

Permutationsgruppen¹

Dozent: Dr. F. M. Schneider
 \LaTeX : rydval.jakub@gmail.com
Version: 1. Juli 2017
Technische Universität Dresden

¹Math Ba ALGSTR: Permutationsgruppen, WS 2015/16

INHALTSVERZEICHNIS

Inhaltsverzeichnis

0	Einleitung	1
1	Permutationen und Permutationsgruppen	4
2	Gruppenwirkungen und Darstellungen	10
3	Erzeugendensysteme & Sims-Ketten	12
4	Automorphismen, invariante Relationen und die Sätze von KRASNER	17
5	k-Abgeschlossene Permutationsgruppen, primitive Gruppen, Automorphismengruppen von Graphen	25
6	POLYAsche Abzähltheorie	36
7	Operationen auf Permutationsgruppen	44
8	Die Sätze von CAUCHY und SYLOW	52
9	Einfache Gruppen	63

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:

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

Wichtige Beispiele:

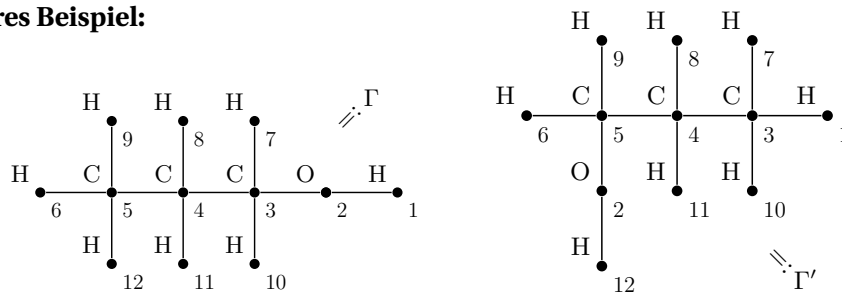
- Symmetrie- bzw. Isometriegruppen (geometrisch),
- Automorphismengruppen (algebraisch/kombinatorisch).

Konkret:

Zu (a): Isometrische Abbildungen der Ebene, die $\triangle_{a,b,c}$ in Drehung bringen: Drehungen um $0^\circ, 120^\circ, 240^\circ$. Spiegelungen um Achsen durch 0, 1, 2 \Rightarrow 6 Symmetrien. Genauer: $G \cong S_3$ (volle symmetrische Gruppe).

Zu (b): Betrachte $\triangle_{a,b,c}$ als Graphen (Punkte & Knoten). Automorphismus ist 1-1-Abbildung auf Punkten, die Knoten in Kanten überführt $\Rightarrow \text{Aut}(\triangle_{a,b,c}) = S_3$.

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:

$$\begin{array}{l} \left. \begin{array}{l} 3: 7 \longleftrightarrow 10 \\ 4: 8 \longleftrightarrow 11 \\ 5: 6, 9, 12 \end{array} \right\} \Rightarrow \text{Aut } \Gamma \cong S_2 \times S_3 \times S_3 \\ \Rightarrow |\text{Aut } \Gamma| = 24 \end{array}$$

0 EINLEITUNG

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

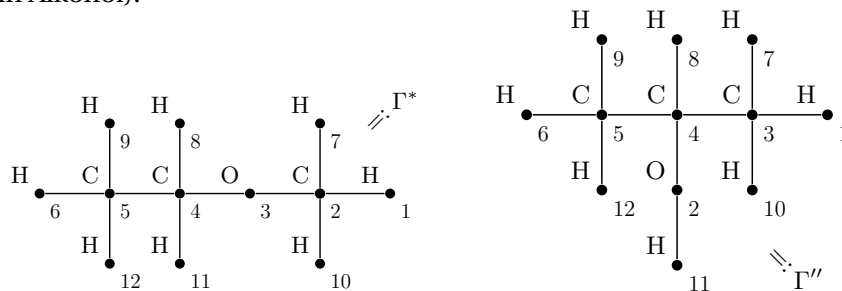
Isomorphieproblem: Wann sind zwei Strukturen im wesentlichen gleich d.h. isomorph? Bemerkung: Isomorphieproblem ist zurückführbar auf Bestimmung der Automorphismengruppe:

$$\left. \begin{array}{l} f: \Gamma \rightarrow \Gamma' \\ f^{-1}: \Gamma' \rightarrow \Gamma \end{array} \right\} \text{ ist als Automorphismus von } \Gamma \sqcup \Gamma' \text{ interpretierbar}$$

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 $\text{Aut } \Gamma''$).

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.

0 EINLEITUNG

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 $M = a, b, c$:

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

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

$$\begin{array}{l} \pi_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \begin{array}{l} \leftarrow \text{Argumentenzeile} \\ \leftarrow \text{Bildzeile} \end{array} \\ \pi_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \\ \vdots \\ \pi_6 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \end{array}$$

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

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

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

1.0.1 Definition. Eine *Permutation* auf einer Menge M ist eine bijektive Abbildung $f: M \rightarrow M$. $S_M := S(M) :=$ 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 $M = \{a_1, \dots, a_n\}$.

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

Beweis. Übungsaufgabe. □

1.0.3 Definition. Der Graph einer Permutation $f: M \rightarrow M$:

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

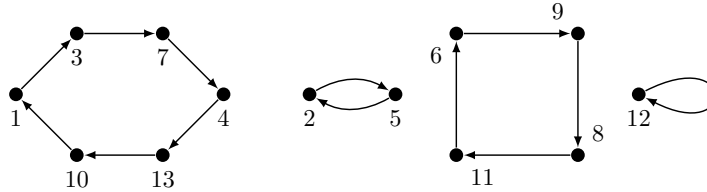
1 PERMUTATIONEN UND PERMUTATIONSGRUPPEN

- 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).

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

$$f = (a_1 \ a_1^f \ a_1^{ff} \ \dots \ a_1^{f^{k_1}}) \cdots (a_l \ a_l^f \ a_l^{ff} \ \dots \ a_l^{f^{k_l}}),$$

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

Beispiel. Sei f wie oben, dann:

$$f = (1 \ 3 \ 7 \ 4 \ 13 \ 10)(2 \ 5)(6 \ 9 \ 8 \ 11)(12).$$

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

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

Beachte: $(a \ b \ c), (b \ c \ a), (c \ a \ b)$ bezeichnen dieselbe Permutation (nur Reihenfolge ist wichtig, nicht der Anfangselement).

1.0.5 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:

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

Fakt: Sei f Permutation mit (verkürzten) Zyklendarstellung

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

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

1.0.6 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 $\text{ord}(f) := \inf\{m \in \mathbb{N} \setminus \{0\} \mid f^m = e\}$, Untergruppe (UG), Normalteiler (NT), konjugierte Elemente etc.

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

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

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

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

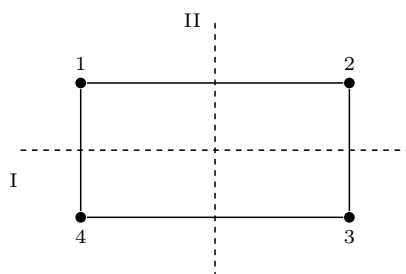
$$a^U := \{a^u \mid u \in U\}, B^g := \{b^g \mid b \in B\}, B^U := \{b^u \mid b \in B, u \in U\}.$$

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

Beweis. Übungsaufgabe! □

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

1 PERMUTATIONEN UND PERMUTATIONSGRUPPEN



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* ($\cong \mathbb{Z}_2 \times \mathbb{Z}_2$).

1.0.10 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*), $1\text{-Orb}(G, M) :=$ Menge aller 1-Bahnen.
 (c) $B \subseteq M$ *invariant* (bzgl. G) $\iff B^G = B$ ($\iff B \subseteq B$).
 (d) G *transitiv*: $\iff \exists a \in M : a^G = M \iff |1\text{-Orb}(G, M)| = 1 \iff \forall a \in M : a^G = M$.
 Bedeutung: Alle Elemente von M haben gleiche „Eigenschaften“ in der Struktur, falls $G = \text{Aut}(\text{Struktur auf } M)$.

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

- (i) G_a ist Untergruppe von G .
 (ii) $G_{a^g} = g^{-1}G_ag$ für jedes $g \in G$.
 (iii) Durch $a \sim b \iff a^G = b^G$ ist eine ÄR auf M definiert und $1\text{-Orb}(G, M) = M/\sim \implies$ die Menge $1\text{-Orb}(G, M)$ 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! □

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

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

Wiederholung Algebra:

1.0.12 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 $k := [G : U] = |G/U| = \text{Anzahl der Nebenklassen von } U \text{ in } G$. Also $G = Ug_1 \sqcup \dots \sqcup Ug_k$ für beliebige Transversale $g_1, \dots, g_k \in G$. Da $|U| = |Ug_i|$ für jedes $i \in \{1, \dots, k\}$ folgt Behauptung. \square

1.0.13 Lemma. Sei $a \in M$, $G \leq S_M$. Durch $a^G \rightarrow G/G_a$, $a^g \mapsto G_ag$ 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. \square

Aus 1.12 und 1.13 folgt:

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

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

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

1.0.15 Beispiel. $G := S_4$ (d.h. $M = \{1, 2, 3, 4\}$). $1^G = \{1, 2, 3, 4\} \implies |G_1| \stackrel{1.14}{=} \frac{|G|}{|1^G|} = \frac{4!}{4} = 6$. 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: $G_{1,2,3} = \{(1)\}$.

1.0.16 Definition. Zwei Permutationsgruppen (G, M) , (H, N) heißen *ähnlich*, wenn eine bijektive Abbildung $f : M \rightarrow N$ und ein Gruppenisomorphismus $\varphi : G \rightarrow H$ 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

1 PERMUTATIONEN UND PERMUTATIONSGRUPPEN

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ g \downarrow & & \downarrow \varphi(g) \\ M & \xrightarrow{f} & N \end{array}$$

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 (\Leftarrow gilt i.a. nicht).

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

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

1.0.18 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 $g_2 = f^{-1}g_1f$. (Sprechweise: g_1 und g_2 sind konjugiert in G).

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

(b) *Aus der Darstellung*

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

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

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

(c) g_1 konjugiert zu g_2 in $G \implies g_1$ und g_2 sind ähnlich (\Leftarrow 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) Untergruppen $(\langle g_1 \rangle, M)$ und $(\langle g_2 \rangle, M)$ sind ähnlich im Sinne von 1.16.

Beweis. Übungsaufgabe! □

2 Gruppenwirkungen und Darstellungen

2.0.1 Definition. Ein (Gruppen-)Homomorphismus $\psi : G \rightarrow S_M$ 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*: $\iff \psi$ ist injektiv.

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

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

- $$\begin{array}{l} \varphi(x, e_G) \\ \parallel \\ \text{(i) } x e_G = x \quad \forall x \in M, \\ \text{(ii) } (xg)g' = x(gg') \quad \forall x \in M, g, g' \in G. \\ \parallel \qquad \parallel \\ \varphi(\varphi(x, g)g') \quad \varphi(x, gg') \end{array}$$

Sprechweise: G *wirkt* (*operiert*) auf M .

Schreibweise: (G, M) Gruppenwirkung.

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

2.0.3 Satz. Jeder Gruppenwirkung entspricht in eindeutiger Weise eine Permutationsdarstellung $\psi : G \rightarrow S_M$ 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).

2.0.4 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) $\psi : G \rightarrow S_G$ ist Permutationsdarstellung (Homo.), $\psi : g \mapsto g^*$.
 (c) $\varphi : G \times G \rightarrow G, (h, g) \mapsto hg$ ist zugehörige Gruppenwirkung.
 (d) ψ oben ist treu (und heißt rechtsreguläre Darstellung v. G).

2.0.5 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) $\varphi(h, e) = he = h$,

2 GRUPPENWIRKUNGEN UND DARSTELLUNGEN

(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 $g_1 = e^{g_1^*} = e^{g_2^*} = g_2$. \square

- 2.0.6 Bemerkungen.** (a) Ist $g \in G \setminus \{e\}$, dann hat $g^* : M \rightarrow M$ keinen Fixpunkt.
 (b) Jedes g^* zerfällt in Produkt von Zyklen der Länge $\text{ord}(g)$. (Zum Beweis: Die Zyklen von g^* sind alle von der Form $(h \ hg \ hg^2 \ \dots \ hg^{n-1})$ für $h \in G$ und $n := \text{ord}(g)$.)
 (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).

2.0.7 Beispiele. (1) Wirkung durch Konjugation: $\varphi : G \times G \rightarrow G, (h, g) \mapsto g^{-1}hg, \psi : G \rightarrow S_G, g \mapsto \psi(g)$ mit $h^{\psi(g)} := g^{-1}hg$.

Menge aller Unter-
gruppen von G

- (2) Wirkung auf Untergruppen: $U \leq G, \varphi : \overbrace{\text{Sub}(G)}^{\text{Menge aller Untergruppen von } G} \times G \rightarrow \text{Sub}(G), (U, g) \mapsto g^{-1}Ug$.
 (3) Wirkung auf Rechtsnebenklassen: $G/U = \{Uh \mid h \in G\}$ Faktorgruppe einer Untergruppe $U \leq G, \varphi : G/U \times G \rightarrow G/U, (Uh, g) \mapsto Uhg$.

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

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

3 Erzeugendensysteme & Sims-Ketten

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

Ausweg:

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

Wiederholung aus Algebra

3.0.1 Definition. $U \subseteq G$ heißt *Erzeugendensystem* einer Gruppe $G : \iff$ jedes $g \in G$ ist als Produkt $g = u_1 \cdots u_m$ mit $u_i \in U$ oder u_i^{-1} ($i \in \{1, \dots, m\}$, $m \in \mathbb{N}$) 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 $g \in S_n$ und $U \subseteq S_n$.
 (P2) Beschreibe Bahnen von $\langle U \rangle$, also $a^{(U)}$ 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 ($i = 1, \dots, r$), sodass $G = T_r \cdot T_{r-1} \cdot \dots \cdot T_1$ (Komplexprodukt) und die Darstellung $g = t_r \cdot t_{r-1} \cdot \dots \cdot t_1$ (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 .

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

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

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

Für Nebenklassenzerlegung $U_{i-1}/U_i = U_i g_{i_1} \sqcup U_i g_{i_2} \sqcup \dots \sqcup U_i g_{i_{n_i}}$ wird Repräsentantensystem (Transversale) $T_i := \{g_{i_1}, \dots, g_{i_{n_i}}\} \subseteq U_{i-1}$ gewählt ($i = 1, \dots, r$). (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!

3.0.3 Satz. Seien G, T_1, \dots, 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 $h_i \in T_i$ ($i \in \{1, \dots, r\}$) 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, \dots, a_r^g)

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

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

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

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

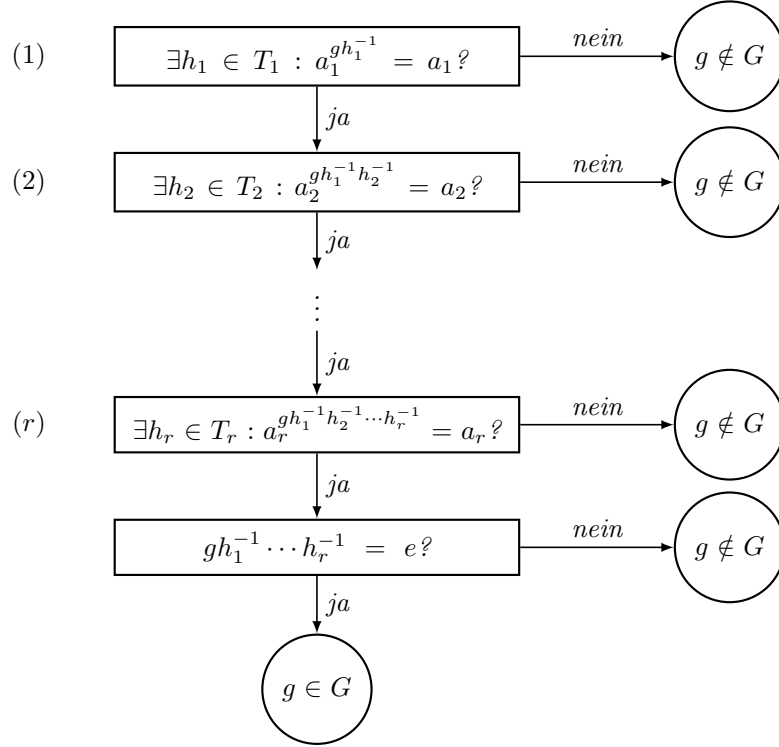
$$h_1 \in U_1 h'_1$$

$$\begin{aligned} & \begin{array}{c} T_1 \text{ Transversale} \\ \implies \\ \text{von } G/U_1 \end{array} \quad h_1 = h'_1 \implies \underbrace{h_r \cdots h_2}_{\in U_2} = \underbrace{h'_r \cdots h'_2}_{\in U_2} \implies h_2 = h'_2 \\ & \quad \vdots \\ & \implies h_i = h'_i \text{ für jedes } i \in \{1, \dots, r\}. \end{aligned}$$

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

3.0.4 Beispiel. $G = S_4$ mit $M = \{1, 2, 3, 4\}$. Es gilt $G_1 \cong S_3$, $G_{1,2} \cong S_2$, $G_{1,2,3} = \{e\}$. $T_1 = \{e, g_1, g_1^2, g_1^3\}$ 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 $g_3 := (3 \ 4) \xrightarrow{3.3}$ Jedes $g \in S_4$ 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.

3.0.5 Folgerung (Testalgorithmus). Für G seien T_1, \dots, 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, \dots, T_r für die Untergruppen falls nur Erzeugendensystem U für G gegeben ist? (vgl Problem 3.1 (P3)) Antwort gibt ein Resultat von SCHREIER:

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

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

ein Erzeugendensystem für die Gruppe V .

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

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

3 ERZEUGENDENSYSTEME & SIMS-KETTEN

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

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

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

□

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

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

Beweis. Zu (a): Für Zyklen gilt $(a_1 \ \dots \ a_k) = (a_1 \ a_2)(a_1 \ a_3) \cdots (a_1 \ a_k)$ (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): $g = (1 \ 2)$, $h = (1 \ 2 \ 3 \ \dots \ n)$, $(2 \ 3) = h^{-1} g h$, $(3 \ 4) = h^{-1} (2 \ 3) h, \dots, (n-1 \ n) = h^{-1} (n-2 \ n-1) h$. Weiter mit (b).

□

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

3.0.9 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 :

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

g heißt *gerade Permutation*, falls $\text{sgn}(g) = 1$ und *ungerade Permutation*, falls $\text{sgn}(g) = -1$.

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

- (1) $\text{sgn}(g) = \prod_{i < j} \frac{j^g - i^g}{j - i} = \prod_{i < j} \frac{j^{gh} - i^{gh}}{j^h - i^h}$ für jedes $h \in S_{\underline{n}}$.
 (2) $\text{sgn}(gh) = \text{sgn}(g)\text{sgn}(h) \forall g, h \in G$. Begründung:

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

- (3) $\text{sgn}(e) = 1$, $\text{sgn}(g^{-1}) = \text{sgn}(g)$. Begründung: $1 = \text{sgn}(e) \stackrel{(2)}{=} \text{sgn}(g)\text{sgn}(g^{-1})$.
 (4) $\text{sgn} : S_{\underline{n}} \rightarrow \{-1, 1\}$ 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: $g = t_1 t_2 \cdots t_q \implies \text{sgn}(g) = \text{sgn}(t_1) \cdots \text{sgn}(t_q) = (-1)^q$.

3.0.10 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): $\text{sgn} : S_{\underline{n}} \rightarrow \{-1, 1\}$ ist Homomorphismus $\implies A_{\underline{n}} = \{g \in S_{\underline{n}} \mid \text{sgn}(g) = 1\} = \text{Ker}(\text{sgn})$ ist ein Normalteiler von $S_{\underline{n}}$. Homomorphiesatz: $S_{\underline{n}}/A_{\underline{n}} \cong \{-1, 1\}$, da sgn surjektiv ist. Also $2 = |S_{\underline{n}}/A_{\underline{n}}| \implies |A_{\underline{n}}| = |S_{\underline{n}}|/2 = n!/2$. \square

3.0.11 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)). $S_{\underline{n}} = V h_1 \sqcup V h_2 = A_{\underline{n}} \underbrace{e}_{=: h_1} \sqcup A_{\underline{n}} \underbrace{(1\ 2)}_{=: h_2 = g_1}$. 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

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

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).

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

- g bewahrt Φ (Φ invariant unter g , Bezeichnung: $g \triangleright \Phi$) : $\Longleftrightarrow \Phi^g \subset \Phi \stackrel{M \text{ endl.}}{\Longleftrightarrow} \Phi^g = \Phi \Longleftrightarrow g$ Automorphismus v. Φ .
D.h. $g \triangleright \Phi \Longleftrightarrow \forall a_1, \dots, a_n \in M : (a_1, \dots, a_n) \in \Phi \Longleftrightarrow (a_1^g, \dots, a_n^g) \in \Phi$.
- Bezeichnung:

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

ist Menge aller endlich-stelligen Relationen auf M . Setze

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

für $\Phi \in R_M$.

- Für $Q \subseteq R_M$:

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

Automorphismen von Q .

- Für $G \subseteq S_M$:

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

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

Invarianten von G .

Einschub:

(1) Sei X Menge. $H : \mathfrak{P}(X) \rightarrow \mathfrak{P}(X)$ 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* : \iff

- (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 $H: \mathfrak{P}(X) \rightarrow \mathfrak{P}(X)$ 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*:

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

Jede Relation induziert eine Galoisverbindung, also auch

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

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

$$\begin{aligned} \varphi &= \text{Aut} : \mathfrak{P}(R_M) \rightarrow \mathfrak{P}(S_M), Q \mapsto \text{Aut}(Q), \\ \psi &= \text{Inv} : \mathfrak{P}(S_M) \rightarrow \mathfrak{P}(R_M), G \mapsto \text{Inv}(G). \end{aligned}$$

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

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

$$\begin{array}{ccc} \{G \subseteq S_M \mid \text{Aut } \text{Inv } G\} & \begin{array}{c} \xrightarrow{\text{Aut}} \\ \xleftarrow{\text{Inv}} \end{array} & \{Q \subseteq R_M \mid \text{Inv } \text{Aut } Q\} \end{array}$$

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

Beweis. Übung! □

4.0.3 Definition. Eine Relation der Form

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

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

Bemerkung. Für $\Phi \subseteq M^n$:

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

4.0.4 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 $a \in M^n$. Z.z.: a^G ist invariant für jedes $g \in G$. Offenbar: $(a^G)^g = a^{Gg} = a^G$ 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 $f : \mathfrak{P}(n\text{-Orb}(G, M)) \rightarrow n\text{-Inv}(G, M), B \mapsto \bigcup B$ bijektiv). □

Folgerung aus 1.4 (Satz von LAGRANGE für Permutationsgruppen):

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

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

Beweis. $\Phi = (a_1, \dots, a_n)^{\tilde{G}} = a^{\tilde{G}}$, $\tilde{G}_a = G_{a_1, \dots, a_n}$ für Wirkung (\tilde{G}, M^n) . 1.14 $\implies |G| = |\tilde{G}| = |\tilde{G}_a| \cdot |a^{\tilde{G}}| \implies \text{Behauptung.}$ □

||

Φ

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

Probleme:

4 AUTOMORPHISMEN, INVARIANTE RELATIONEN UND DIE SÄTZE VON KRASNER

- 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:

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

Beweis. Übung! □

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

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

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

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

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

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

Beschreibung der von G erzeugten Untergruppe

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

$$\text{ich wirke auf jedem Element} \rightarrow (a_1^f, \dots, a_m^f)$$

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

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

Damit folgen alle Gleichungen in (a).

$$\begin{aligned} \text{Zu (b): } G &\subseteq \text{Aut Inv } G \quad (\text{vgl. } 4.2 \text{ (III)}) \\ \Rightarrow \langle G \rangle &\subseteq \langle \text{Aut Inv } G \rangle \stackrel{4.6}{=} \text{Aut Inv } G \stackrel{4.2 \text{ (V)}}{\subseteq} \text{Aut Inv } \langle G \rangle \stackrel{(a)}{=} \langle G \rangle. \end{aligned}$$


□

Erinnerung: Prädikatenkalkül erster Stufe

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

- Für je zwei $x, y \in X$ ist

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

freie Variablen 

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

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


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

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

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

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

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

es gilt 

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

$$F_\varphi(\Phi_1, \Phi_2) = \{(x, y) \in M^2 \mid \exists z \in M : (x, z) \in \Phi_1 \wedge (z, y) \in \Phi_2\}$$

$$=: \Phi_1 \circ \Phi_2 \text{ (Relationenprodukt).}$$

(ii) $\varphi_1(R_1, R_2; x, y) := R_1(x, y) \wedge R_2(x, y)$, $F_{\varphi_1} = \Phi_1 \cap \Phi_2$.

(iii) $\varphi(R_1; x_1, \dots, x_n) := \neg R_1(x_1, \dots, x_n)$,

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

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

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

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

$$F_\varphi(\Phi) = \{(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \in M^{n-1} \mid \exists a_i \in M : (a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \in \Phi\}$$

$$= \text{pr}_{\underline{n} \setminus \{i\}}(\Phi)$$

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

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

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

der Abschluss gegen logische Operationen.

Bemerkung 1. Die Abbildung $\mathfrak{P}(R_M) \rightarrow \mathfrak{P}(R_M), Q \mapsto [Q]$ 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 $\langle R_M, (R_\varphi)_{\varphi \text{ Formel}} \rangle$.

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

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

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

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

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

für alle $g \in G$. Also $F_\varphi(\Phi_1, \dots, \Phi_q) \in \text{Inv } G$. □

4.0.12 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:

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

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

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

Beschreibung der von Q erzeugten Krasner-Algebra

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

$$Q \stackrel{4.2 \text{ (IV)}}{\subseteq} \text{Inv Aut } Q \implies [Q] \subseteq [\text{Inv Aut } Q] \stackrel{4.11}{=} \text{Inv Aut } Q \\ \subseteq \text{Inv Aut } [Q] \stackrel{(a)}{=} [Q].$$

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

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

Dann folgt:

$$\begin{aligned} Q &\stackrel{4.2 \text{ (IV)}}{\subseteq} \text{InvAut } Q \implies [Q] \subseteq \text{InvAut } Q = \text{Inv } G \\ &\stackrel{2. \text{ S.}}{\subseteq} [\mathbf{a}^G] \stackrel{1. \text{ S.}}{\subseteq} [Q] = Q. \end{aligned}$$

□

4.0.13 Lemma. Sei $[Q] = Q \subseteq R_M$, $G = \text{Aut } Q$, $M = \{a_1, \dots, a_m\}$, $\mathbf{a} = (a_1, \dots, a_m)$. Dann gilt $\mathbf{a}^G \in Q$.

Beweis. Definiere

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

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 $\mathbf{a}^G = \gamma$.

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

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

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

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

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

und weiter

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

Also $\sigma \in [Q] = Q$ und $\sigma \subseteq \gamma$. Wegen $\mathbf{a} \in \gamma$ und $s \in \varrho_0$ folgt $\mathbf{a} \in \sigma$. Aber $\mathbf{r} = \mathbf{a}^f \notin \sigma$, weil $(a_{j_1}, \dots, a_{j_t})^f = s^f \notin \varrho_0$. Das heißt: $\mathbf{r} \notin \gamma \setminus \sigma \implies \gamma \not\subseteq \sigma$. Andererseits: $\mathbf{a} \in \sigma \in Q \stackrel{(*)}{\implies} \gamma \subseteq \sigma \implies$ Widerspruch. Also $\mathbf{a}^G = \gamma \in Q$. □

4.0.14 Lemma. Sei $M = \{a_1, \dots, a_m\}$, $[Q] = Q \subseteq R_M$, $G = \text{Aut } Q$, $\mathbf{a} = (a_1, \dots, a_m)$. Dann gilt:

$$\text{Inv } G \subseteq [\mathbf{a}^G].$$

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

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:

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

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

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

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

Dann:

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

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

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

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

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

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

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

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

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

5.0.2 Satz. Es gilt:

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

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

wobei $R_M^{(k)} := \mathfrak{P}(M^k)$, 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 ($G \approx_k H \implies H \subseteq G^{(k)} = G^{(k)}$).

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

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

Beweis. Übungsaufgabe! □

5.0.3 Satz. Sei $G \leq S_M$.

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

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

(b) k -Abschlusskriterium (hinreichend):

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

(c) Charakterisierung:

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

Beweis. Zu (a):

$$\begin{aligned} h \in G^{(k)} &\stackrel{5.2(v)}{\iff} h \in \text{Aut } k\text{-Orb } G \\ &\iff \forall a \in M^k : (a^G)^h = a^G \\ &\iff \forall a \in M^k : a^h \in a^G \end{aligned}$$

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

$$\iff \forall a_1, \dots, a_k \in M \exists g \in G : a^h = a^g.$$

5 K -ABGESCHLOSSENE PERMUTATIONSGRUPPEN, PRIMITIVE GRUPPEN,
AUTOMORPHISMENGRUPPEN VON GRAPHEN

Zu (b): Zu zeigen: $h \in G^{(k)} \implies h \in G$. Sei $h \in G^{(k)}$. Nach (a) gilt: $\forall b \in M \exists g_b \in G : (a_1, \dots, a_{k-1}, b)^h = (a_1, \dots, a_{k-1}, b)^{g_b}$. Sind $b, b' \in M$, dann ist $g_b g_{b'}^{-1} \in G_{a_1, \dots, a_{k-1}} = \{e\}$ 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): „ \implies “ Sei $Q \subseteq R_M^{(k)}$ mit $G = \text{Aut } Q$. Dann folgt:

$$G = \text{Aut } Q \stackrel{4.2 \text{ (II)}}{\supseteq} \text{Aut } k\text{-Inv } G = G^{(k)} \supseteq G.$$

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

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

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

5.0.4 Definition. $G \leq S_M$ heißt

$$\text{semi-regulär} : \iff \forall a \in M : G_a = \{e\},$$

$$\text{regulär} : \iff G \text{ ist semi-regulär und transitiv (vgl. 1.10 (d)).}$$

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

5.0.5 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): $|G| \stackrel{1.14}{=} |G_a| |a^G| = |a^G|$.

Zu (d): G transitiv, d.h. $\exists a \in M : a^G = M$. Nach (c) ist $|M| = |a^G| = |G|$. □

5.0.6 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 $g \in G : g^* : G \rightarrow G, x \mapsto xg$.

5.0.7 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 $a = b$.

5 K -ABGESCHLOSSENE PERMUTATIONSGRUPPEN, PRIMITIVE GRUPPEN, AUTOMORPHISMENGRUPPEN VON GRAPHEN

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

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

- Ein *gefärbter Graph* ist ein Paar (Γ, γ) , wobei:
 - $\Gamma = (V, E)$ Graph,
 - $\gamma : E \rightarrow C$ 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 $f : V \rightarrow V$, so dass:
 - $f \in \text{Aut } \Gamma$,
 - 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) : $\text{Aut}(\Gamma, \gamma)$ (ist tatsächlich eine Gruppe—Übungsaufgabe!).

$$\text{Aut}\left(\begin{array}{c} c \\ \triangle \\ a \quad b \end{array}\right) = S_3 \text{ aber } \text{Aut}\left(\begin{array}{c} c \\ \text{---} \triangle \text{---} \\ a \quad b \end{array}\right) \neq S_3.$$

5.0.8 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:

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

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

5.0.9 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:

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

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

$$\begin{aligned} &\implies (x, x^{g'}) = (x, x^{h_1 g h_2}) \stackrel{h_1 \in G_x}{=} (x, x^{g h_2}) \stackrel{h_2 \in G_x}{=} (x^{h_2}, x^{g h_2}) = (x, x^g)^{h_2} = (x, x^g)^G. \\ &\iff \text{Sei } (x, x^{g'}) \in (x, x^g)^G \implies \exists h_2 \in G : (x, x^{g'}) = (x, x^g)^{h_2} = (x^{h_2}, x^{g h_2}) \implies h_2 \in G_x. \text{ Definiere } h_1 := g' h_2^{-1} g^{-1}. \text{ Dann } x^{h_1} = x^{g' h_2^{-1} g^{-1}} = x^{g h_2 h_2^{-1} g^{-1}} = x \implies x \in G_x. \\ &\text{Außerdem ist } h_1 g h_2 = g'. \quad \square \end{aligned}$$

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

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

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

ist eine Bijektion.

- (b) Elemente von 2-Bahn $\xrightarrow{1:1}$ Rechtsnebenklassen nach „Doppelstabilisator“. Die Abbildung

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

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

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

$$\varphi : (x, x^g)^G \times G \rightarrow (x, x^g)^G, ((x^h, x^{g h}), f) \mapsto (x^{h f}, x^{g h f})$$

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

$$\varphi' : G / G_{x, x^g} \times G \rightarrow G / G_{x, x^g}, (G_{x, x^{g h}}, f) \mapsto G_{x, x^g} h f$$

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 $a^G \rightarrow G/G_a$, $a^h \mapsto G_a h$ 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):

$$\begin{array}{ccc}
 (x, x^g)^G & \xrightarrow{\alpha'} & G/G_{x, x^g} \\
 \downarrow f & & \downarrow f \\
 (x^h, x^{gh}) & \mapsto & (G_{x, x^g} h) \\
 \downarrow & & \downarrow \\
 (x^{hf}, x^{ghf}) & \mapsto & G_{x, x^g} hf \\
 \downarrow f & & \downarrow f \\
 (x, x^g)^G & \xrightarrow{\alpha'} & G/G_{x, x^g}
 \end{array}$$

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

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

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

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

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

(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 $1\text{-Orb}(G_x, M)$ (und $\hat{T} = \{(x, x^g) \mid g \in T\}$ Transversale für $2\text{-Orb}(G, M)$).

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 $B \in 1\text{-Orb}(G_x, M)$ 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 $(x, x^g)^G \in 2\text{-Orb}(G, M)$ und $\kappa((x, x^g)^G) = (x^g)^{G_x} = B$. Restliche Gleichungen: Übung!

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

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

- Vergrößerung der betrachteten Struktur durch Homomorphismus,

- Problem in grober Struktur behandeln.

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

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

d.h. das Diagramm

$$\begin{array}{ccccc} m & & M & \xrightarrow{f} & N & & n \\ \downarrow & & \downarrow g & & \downarrow \varphi(g) & & \downarrow \\ m^g & & M & \xrightarrow{f} & N & & n^{\varphi(g)} \end{array}$$

kommutiert (für jedes $g \in G$).

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

5.0.14 Lemma. Sei $G \leq S_M$, $\Theta \in \mathcal{Q}(M)$. Dann ist durch

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

genau dann eine Gruppenwirkung von G auf M/Θ gegeben, wenn $\Theta \in 2\text{-Inv}(G, M)$. In diesem Fall ist (φ, f) mit $\varphi = \text{id} : G \rightarrow G$ und $f : M \rightarrow M/\Theta, m \mapsto [m]_\Theta$ 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!). \square

5.0.15 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*.

5 K-ABGESCHLOSSENE PERMUTATIONSGRUPPEN, PRIMITIVE GRUPPEN,
AUTOMORPHISMENGRUPPEN VON GRAPHEN

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 $\Theta \in \mathcal{q}(M)$ gilt:

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

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

- (a) G ist imprimitiv.
- (b) Es gibt eine nichttriviale Äquivalenzrelation $\Theta \in \mathcal{q}(M) \cap \text{Inv}(G, M)$ (d.h. $\Delta_M \neq \Theta \neq M^2$).
- (c) Es gibt ein nichttriviales verträgliches Blocksysteem für G .

Beweis. (a) \implies (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 Blocksysteem. Für $g, h \in G$:

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

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

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

(c) \implies (b): Sei \mathcal{B} nichttriviales Blocksysteem, 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: $\Delta_M \neq \Theta \neq M^2$.

(b) \implies (a): $\Theta \in \mathcal{q}(M) \setminus \{\Delta_M, M^2\}$ invariant. Dann gibt es $x \in M$ mit $\{x\} \neq [x]_\Theta \neq M$. Da Θ invariant, ist $B := [x]_\Theta$ Block. Auch: $\{x\} \subsetneq B \subsetneq M \implies B$ nichttrivial. \square

5.0.17 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 $B \times G_B \rightarrow B$, $(b, g) \mapsto b^g$ ist Gruppenwirkung (G_B, B) auf B gegeben (Übung!).

5.0.18 Satz. Sei (G, M) Gruppenwirkung und $\Theta \in \mathcal{q}(M)$ invariant (d.h. $\mathcal{B} := M/\Theta$ ist verträgliches Blocksysteem) (Bemerkung: Dann ist (id_G, f) Homomorphismus von (G, M) nach $(G, M/\Theta)$ mit $f : M \rightarrow M/\Theta, x \mapsto [x]_\Theta$). 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! □

5.0.19 Bemerkungen. Seien $(G, M), (H, N)$ Gruppenwirkungen, $(\varphi, f) : (G, M) \rightarrow (H, N)$ morphismus. Dann gilt:

- (i) $\Theta := \ker f$ ist G -invariant, d.h. M/Θ ist verträgliches Blocksysteem.
- (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:

- $R^{\text{ref}} := R \cup \Delta_M$ ist reflexiver Abschluss,
- $R^{\text{sym}} := R \cup R^{-1}$ ist symmetrischer Abschluss, wobei $R^{-1} = \{(b, a) \mid (a, b) \in R\}$,
- $R^{\text{trans}} := \bigcup_{n \in \mathbb{N} \setminus \{0\}} R^n$ ist transitiver Abschluss, wobei $R^n := R \circ \dots \circ R$ für $n \geq 1$ und

$$R \circ S = \{(a, c) \in M^2 \mid \exists b \in M : (a, b) \in R, (b, c) \in S\},$$

- $R^q := \bigcup \{S \in \mathcal{q}(M) \mid R \subseteq S\}$ die von R erzeugte Äquivalenzrelation auf M (bzgl. \subseteq kleinstes Element von $\mathcal{q}(M)$, das R enthält).

Es gilt:

$$R^q = \left((R^{\text{ref}})^{\text{sym}} \right)^{\text{trans}} \quad (*)$$

(Übung!)

Begiffe:

- R antireflexiv: $\iff R \cap \Delta_M = \emptyset$.
- Graph (M, R) heißt zusammenhängend: $\iff \forall a, b \in M, a \neq b \exists a = a_0, a_1, \dots, a_n = b \in M : \forall i \in \{0, \dots, n-1\} : (a_i, a_{i+1}) \in R$ oder $(a_{i+1}, a_i) \in R \iff R^q = M \times M$.

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

- (A) (G, M) imprimitiv $\iff \exists a \in M \exists U \leq G : G_a \not\leq U \not\leq G$ ($\iff \forall a \in M \dots$ da (G, M) transitiv).

5 K -ABGESCHLOSSENE PERMUTATIONSGRUPPEN, PRIMITIVE GRUPPEN,
AUTOMORPHISMENGRUPPEN VON GRAPHEN

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

(C) **Satz von HIGMAN:**

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

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

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

- (i) U ist nicht transitiv ($B^U = B \subsetneq M$), also $U \subsetneq G$ (da G transitiv).
- (ii) $G_a \subseteq U$, denn $g \in G_a \implies a = a^g \in B^g \implies B \cap B^g \neq \emptyset \xrightarrow{B \text{ Block}} B^g = B \iff g \in G_B = U$.
- (iii) $G_a \not\subseteq U$: G transitiv, $|B| \geq 2 \implies \exists b \in B, a \neq b \exists h \in G : b = a^h$, d.h. $h \notin G_a$.
 $b = a^h \in B^h \xrightarrow{b \in B} B \cap B^h \neq \emptyset \xrightarrow{B \text{ Block}} B = B^h \implies h \in G_B = U$.

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

- Blockeigenschaft: Sei $b \in B \cap B^g, g \in G \implies \exists h, h' \in U : b = a^h, b = a^{h'g} \implies h'gh^{-1} \in G_a \subseteq U \implies g \in (h')^{-1}Uh = U \implies B^g = a^{Ug} \stackrel{g \in U}{=} a^U = B$.
- B nicht trivial: $G_a \subsetneq U \implies \exists h \in U : a^h \neq a \implies |B| = |a^U| \geq 2. U \subsetneq G \implies \exists g \in G \setminus U \implies B \cap B^g = \emptyset$ (denn $B = B^g \xrightarrow{s.o.} g \in U$) $\implies |B| \leq \frac{|M|}{2}$. Also $B \neq M$.

Zu (C): „ \implies “ Sei (G, M) primitiv. Sei $\varrho \in 2\text{-Orb}(G, M)$ antireflexiv (d.h. $\Delta_M \cap \varrho = \emptyset$)
 $\varrho \xrightarrow{2\text{-Bahn}} \iff \varrho \not\subseteq \Delta_M$. Setze:

$$\Theta := \varrho^q \stackrel{(*)}{=} \left((\varrho^{\text{ref}})^{\text{sym}} \right)^{\text{trans}} = ((\Delta_M \cup \varrho) \cup \varrho^{-1})^{\text{trans}}.$$

Da $\text{Inv}(G, M)$ Krasneralgebra ist (vgl. 4.11) folgt $\Theta \in \text{Inv}(G, M) \cap q(M)$. Da (G, M) primitiv, ist $\Theta = \Delta_M$ oder $\Theta = M^2$ (5.16). Weil $\varrho \subseteq \Theta$ und $\varrho \not\subseteq \Delta_M$, ist $\Theta = M \times M$.

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

5.0.21 Folgerung. Jede 2-fach transitive Permutationsgruppe G (d.h. $2\text{-Inv}(G, M) = \{\Delta_M, M^2 \setminus \Delta_M\}$) ist primitiv.

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

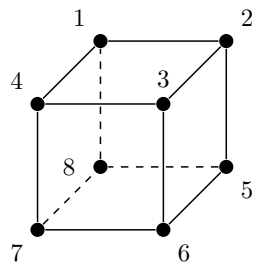
Neues Problem: Wie bestimmt man eigentlich Automorphismengruppen von Graphen?

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

- (1) Wähle $a_1 \in V$ und bestimme eine Menge $T_1 = \{g_{11}, \dots, g_{1n_1}\}$ mit $a_1^G = \{a_1^{g_{11}}, \dots, a_1^{g_{1n_1}}\}$, $n_1 = |a_1^G|$. Dann gilt $G = G_{a_1 T_1}$ (und $|G| = |G_{a_1}| \cdot n_1$). Bemerkung: Die Darstellung $h g_1$ ($h \in G_{a_1}$, $g_1 \in T_1$) 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 $T_2 = \{g_{21}, \dots, g_{2n_2}\}$ mit $a_2^{G_{a_1}} = \{a_2^{g_{21}}, \dots, a_2^{g_{2n_2}}\}$, $n_2 = |a_2^{G_{a_1}}|$. Dann gilt: $G = G_{a_1, a_2} T_2 T_1$ und $|G| = |G_{a_1, a_2}| n_1 n_2$.
- (3) Wiederhole solange, bis Stabilisator G_{a_1, \dots, a_r} bekannt ist (spätestens bis $G_{a_1, \dots, a_r} = \{e\}$).
- (4) Ergebnis: $G = G_{a_1, \dots, a_r} T_r \cdots T_1$ bzw. $|G| = |G_{a_1, \dots, a_r}| n_r \cdots n_1$. Jede Permutation ist eindeutig in der Form $g = h t_r \cdots t_1$ ($h \in G_{a_1, \dots, a_r}$, $t_i \in T_i$ für $i \in \{1, \dots, r\}$) darstellbar.

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

5.0.23 Beispiel. Automorphismengruppe des Würfelgraphen Γ_W :



Anzahl der Automorphismen:

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

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

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

Bestimmung der Automorphismengruppe:

$a_1 = 1$: $a_1^G = \{1, \dots, 8\} = \{a_1^e, a_1^f, a_1^{f^2}, a_1^{f^3}, a_1^{fg}, a_1^{fgf}, a_1^{fgf^2}, a_1^{fgf^3}\}$,
 $T_1 = \{e, f, f^2, f^3, fg, fgf, fgf^2, fgf^3\}$.

$a_2 = 2$: $a_2^{G_{a_1}} = \{2, 4, 8\} = \{a_2^e, a_2^h, a_2^{h^2}\}$, $T_2 = \{e, h, h^2\}$.


$a_3 = 3$: $a_3^{G_{a_1, a_2}} = \{3, 5\} = \{a_3^e, a_3^k\}$, $T_3 = \{e, k\}$.

Jeder Automorphismus von Γ_W ist eindeutig in der Form $t_3 t_2 t_1$ 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 $G \implies$ einfacheres Erzeugendensystem: $\{f, g, h, k\}$.

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

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 ($a \models \varphi \implies a^g \models \varphi$, $(a, b) \models \varphi \implies (a^g, b^g) \models \varphi$, $(a_1, \dots, a_n) \models \varphi \implies (a_1^g, \dots, a_n^g) \models \varphi$).

Beispiele für φ :

- 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

6.0.1 Beispiele (Isomorphietypen von Graphen). Graph $\Gamma = (V, E)$ ohne Schlingen, d.h. $E \subseteq (V \times V) \setminus \Delta_M =: M$. Sei $V := \{1, \dots, n\}$. 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:

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

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

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

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

$$(V, E) \cong (V, E') \iff \exists f \in S_n : E' = E^{\tilde{f}} \iff E' \in E^{\tilde{S}_n}.$$

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

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

Das heißt:

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

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

$$\begin{array}{c} \# \text{Isomorphietypen von Graphen} \\ \Gamma = (V, E) \text{ mit } |E| = k \end{array} = |1\text{-Orb}(\tilde{S}_n^{[k]}, \mathfrak{P}_k(M))|. \quad \begin{array}{l} \nearrow \text{Einschränkung der Wirkung} \\ \text{ } (\tilde{S}_n, \mathfrak{P}(M)) \text{ auf } \mathfrak{P}_k(M) \end{array} \quad \begin{array}{l} \nearrow \text{Menge der } k\text{-elementigen} \\ \text{Teilmengen von } M \end{array}$$

Darstellung oft durch erzeugende Funktion (Polynom):

$$\gamma(x) = \sum_{k=0}^{|M|} t_k x^k \stackrel{\text{Satz von POLYA}}{=} Z(\hat{S}_n).$$

sog. Zyklenzeiger $Z(\hat{S}_n)$
(aus $Z(S_n)$ bestimmbar)

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

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

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

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

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

Andererseits:

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

6.0.4 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 ($k \in \{1, \dots, n\}$, $n := |M|$) Das Polynom (in unbestimmten x_1, \dots, x_n)

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

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

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

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

der *Zykluszeiger* (*Zyklusindex*) von G .

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

Bemerkung: Ähnliche Permutationen haben 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 Zykluszeiger möglich!

(\rightsquigarrow Normalform.)

- 6.0.5 Beispiele.** (a) $G := C_4 = \{g_0, g_1, g_2, g_3\} = \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$
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) $G := S_3$ auf $\underline{3} = \{1, 2, 3\}$. $|S_3| = 3! = 6$. Dann gilt: $Z(G) = \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3)$.
(c) $G := S_3^{[2]}$ induzierte Wirkung von S_3 auf der Menge

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

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.

6.0.6 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. $G = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$, $M = \underline{4}$. Dann: $Z(G) = \frac{1}{4}(x_1^4 + x_1^2x_2 + x_1^2x_2 + x_2^2) \Rightarrow |1\text{-Orb}(G, M)| = \frac{1}{4}(1 \cdot 4 + 2 \cdot 2) = 2$. 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. $\text{coef}_k(\sum_{i=0}^m a_i x^i) := a_k$ ($k \in \{0, \dots, m\}$).

Beispiel. Sei G wie oben. $Z(G, 1+x) = \frac{1}{4}((1+x^4) + 2(1+x^2)(1+x^2) + (1+x^2)^2) \Rightarrow \text{coef}_1(Z(G, 1+x)) = \frac{1}{4}(4 + 2 \cdot 2) = \frac{8}{4} = 2$.

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

$$Z(S_3^{[2]}, 1+x) = \frac{1}{6}((1+x)^6 + 3(1+x^2)^3 + 2(1+x^3)^2)$$

$\Rightarrow \text{coef}_1(Z(S_3^{[2]}, 1+x)) = \frac{1}{6} \cdot 6 = 1$. Das heißt: $S_3^{[2]}$ hat nur eine Bahn, also $S_3^{[2]}$ transitiv auf M (vgl. 6.5).

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

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

erzeugende Funktion für die Zerlegung A/\sim .

Problem: Bestimmung der erzeugenden Funktion.

Wiederholung: Für $f : A \rightarrow B$ 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 Zykluszeiger der gegebenen Gruppe.

Beispiel.

„einfach“	„kompliziert“
(G, M)	$(\tilde{G}, \mathfrak{P}(M))$ (vgl. 6.1, 2.8(a))
Zerlegung von M $1\text{-Orb}(G, M)$	Zerlegung von $\mathfrak{P}(M)$ $1\text{-Orb}(\tilde{G}, \mathfrak{P}(M))$
↓	↓
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)

6.0.8 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).

\implies Zerlegung der 1-Bahnen:

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

Erzeugende Funktion für diese Zerlegung:

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

Beachte:

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

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

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

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

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 $k \in \{0, \dots, m\}$ sei $c_k := \text{coef}_k(Z(g, 1+x))$, d.h. $Z(g, 1+x) = \sum_{k=0}^m c_k(g)x^k$. Dann ist:

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

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

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

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

Mit obigem Lemma folgt:

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

Somit:

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

□

6.0.10 Lemma. (Notation wie in 6.8 und 6.9)

- (a) $c_k(g) \stackrel{\text{Def.}}{=} \text{coef}_k(Z(g, 1+x))$ 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 $g^{\{k\}} : \mathfrak{P}_k(M) \rightarrow \mathfrak{P}_k(M), B \mapsto B^g$).

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:

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

Wir betrachten die (vollständige) Zyklendarstellung von g :

Anzahl der Elemente in Zyklen	$M_1 \quad M_2 \quad M_s$
Menge der Elemente in Zyklen	$m_1 \quad m_2 \quad m_s$

$$g = (\cdots)(\cdots) \cdots (\cdots)$$

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

$$\begin{aligned} Z(g, 1+x) &= (1+x)^{j_1(g)} (1+x^2)^{j_2(g)} \dots (1+x^m)^{j_m(g)} \\ &= (1+x^{m_1}) (1+x^{m_2}) \dots (1+x^{m_s}). \end{aligned}$$

Nun gilt:

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

wobei allgemein gilt (Übung!):

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

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

Bemerkung: Die Abbildung

$$\Phi: \mathfrak{P}(\{1, \dots, s\}) \rightarrow \mathfrak{P}(M), \quad T \mapsto \bigsqcup_{i \in T} M_i$$

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

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

□

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

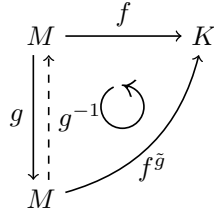
Beweis. Aus Beweis von 6.10: $\Phi: \mathfrak{P}(\{1, \dots, s\}) \rightarrow \mathfrak{P}(M)$, $T \mapsto \bigsqcup_{i \in T} M_i$ ist injektiv, und $\mathfrak{I}(\Phi) = \{B \subseteq M \mid B^g = B\}$. Damit folgt:

$$\chi(\tilde{g}) = |\{B \subseteq M \mid B^g = B\}| = |\mathfrak{I}(\Phi)| \stackrel{\Phi \text{ inj.}}{=} 2^s. \quad \square$$

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

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

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 .



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

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

6.0.13 Beispiel (Isomorphie von Graphen). (vgl. 6.1) Sei $\Gamma = (V, E)$ Graph ohne Schlingen, d.h. $E \subseteq M := (V \times V) \setminus \Delta_V$. $\Gamma \cong \Gamma' \xleftrightarrow{6.1} E' \in E_{\tilde{S}_n}^{\tilde{S}_n} (|V| := \tilde{S}_n, \Gamma' = (V, E'))$.

$$\#\text{Isomorphietypen} = |1\text{-Orb}(\tilde{S}_n, \mathfrak{P}(M))|,$$

$$\#\text{Isomorphietypen von Graphen mit } k \text{ Kanten} = |1\text{-Orb}(S_n^{\{k\}}, \mathfrak{P}_k(M))| = t_k.$$

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

$$t_{S_n^{[2]}}(x) = Z(S_n^{[2]}, 1 + x).$$

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

Hier am Beispiel $n = 4$: $|S_4| = 4!$, 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 $Z(S_4) = \frac{1}{4!}(Z(e) + 6Z(g_2) + 3Z(g_3) + 8Z(g_4) + 6Z(g_5)) = \frac{1}{4!}(x_1^4 + 6x_1^2x_2 + 3x_2^2 + 8x_1x_3 + 6x_4)$. Nun Übergang zu $S_4^{[2]}$. In S_4 : Ähnlichkeit = Konjugiertheit \implies Konjugiertheit bleibt beim Übergang zu $S_4^{[2]}$ erhalten:

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

Also

$$Z(S_4^{[2]}) = \frac{1}{4!}(Z(\hat{e}) + 6Z(\hat{g}_2) + 3Z(\hat{g}_3) + 8Z(\hat{g}_4) + 6Z(\hat{g}_5)),$$

wobei $\tilde{g}: M \rightarrow M, (a, b) \mapsto (a^g, b^g)$ induzierte Wirkung von $g \in S_M$ auf $M = (V \times V) \setminus \Delta_V$, $|M| = 12$. Insbesondere $\hat{e} = e \implies Z(\hat{e}) = x_1^{12}$. $g_2 = (12)(3)(4) \implies$

$$\hat{g}_2 = ((1,2)(2,1))((1,3)(2,3))((1,4)(2,4))((3,1)(3,2))((4,1)(4,2))((3,4)(4,3))$$

$\implies Z(\hat{g}_2) = x_1^2 x_2^5$. 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 $Z(S_4^{[2]}) = \frac{1}{4!}(x_1^{12} + 6x_1^2 x_2^5 + 3x_2^6 + 8x_3^4 + 6x_4^3)$. POLYA-Substitution:

$$\begin{aligned} Z(S_4^{[2]}, 1+x) &= \frac{1}{4!}((1+x)^{12} + 6(1+x)^2(1+x^2)^5 + 3(1+x^2)^6 + 8(1+x^3)^4 + 6(1+x^4)^3) \\ &= 1 + x + 5x^2 + 13x^3 + 27x^4 + 38x^5 + 48x^6 + 38x^7 + 27x^8 + 13x^9 + 5x^{10} \\ &\quad + x^{11} + x^{12}. \end{aligned}$$

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

7.0.1 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:

7.0.2 Definition. Die *direkte Summe* $(G, M) \oplus (H, N)$ zweier Permutationsgruppen (G, M) , (H, N) ist definiert als $(G \times H, M \sqcup N)$ 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 $x \in M \sqcup N$, $(g, h) \in G \times H$. Übung: Nachrechnen, dass dies Wirkung ist!

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

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

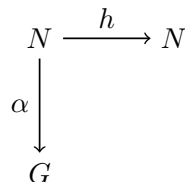
$$G^N \times H = \{(\alpha, h) \mid \alpha : N \rightarrow G, h \in H\}$$

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 *Kranzprodukt* (engl. *Wreath Product*) $G \wr (H, N)$ (auch $G \text{Wr}(H, N)$, $G \wr_N H$).

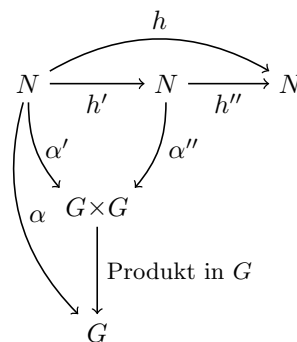
Beweis. • Assoziativität von \cdot : Nachrechnen (Übung!)

- neutrales Element bzgl. \cdot : (ε, e_H) mit $\varepsilon : N \rightarrow G$, $i \mapsto e_G$
- inverses Element zu $(\alpha, h) \in G^N \times H$: $(\bar{\alpha}, h^{-1})$ mit $\bar{\alpha}(i) := \alpha(i^{h^{-1}})^{-1}$ ($i \in N$). □

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



Produkt:



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

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

heißt *reguläres Kranzprodukt* von G und H .

Bemerkung. Sei $N \triangleleft G$. Es gibt eine Einbettung $\Phi: G \rightarrow N \wr (G/N)$. Wähle dazu Abb. $f: G/N \rightarrow G$, sodass $H = Nf(H)$ für alle $H \in G/N$ (Repräsentantenauswahl). Definiere nun $\Phi: G \rightarrow N \wr G/N$ durch $\Phi(g) := (\alpha_g, Ng)$ ($g \in G$), $\alpha_g: G/N \rightarrow N, H \mapsto f(h)gf(Hg)^{-1}$. 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.

7.0.5 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 $D_i := \{(\alpha, e_H) \mid \alpha \in G^N \forall j \in N \setminus \{i\} : \alpha(j) = e_G\}$ 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, \dots, 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) $\Delta(G) := \{(\alpha_g, e_H) \mid g \in G\} \leq D \leq G \wr (H, N)$ (mit $c_g: N \rightarrow G, i \mapsto g$). Es gilt $\Delta(G) \cong G$ und $|\Delta(G) \cap H^*| = 1$ und $H^* \Delta(G) \cong H \times G$.

7.0.6 Definition und Satz. Das *Kranzprodukt* $(G, N) \wr (H, N)$ 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 $(a, b)^{(\varepsilon, e)} = (a^{\varepsilon(b)}, b^{e_H}) = (a, b)$,

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

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: $\alpha \neq \varepsilon \implies \exists b \in N : \alpha(b) \neq e \implies \exists a \in M : a^{\alpha(b)} \neq a \implies (a, b)^{(\alpha, h)} = (a^{\alpha(b)}, b^h) \neq (a, b)$.

□

7.0.7 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 $(\text{Aut } \theta, M \times N) \cong (S_M, M) \wr (S_N, N)$ (Ähnlichkeit, vgl. 1.6).

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

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

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

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

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

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

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

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

Definiere $\alpha : N \rightarrow S_M$ durch

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

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

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

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

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

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

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

$\implies \varphi(\alpha, h) = g$. □

7 OPERATIONEN AUF PERMUTATIONSGRUPPEN

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

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

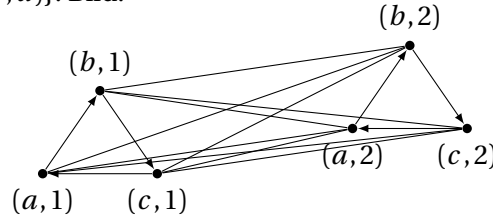
Die Wirkung aus 7.6 definiert einen (injektiven) Homomorphismus $\varphi : \text{Aut } \Gamma_1 \wr (\text{Aut } \Gamma_0, N) \rightarrow \text{Aut } \Gamma$.

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

- $(b, b') \in \Phi_0 \xLeftrightarrow{h \in \text{Aut } \Gamma_0} (b^h, (b')^h) \in \Phi_0 \implies ((a, b)^{(\alpha, h)}, (a', b')^{(\alpha, h)}) \in \Phi$.
- $(a, a') \in \Phi_1 \wedge b = b' \xLeftrightarrow{\alpha(b) \in \text{Aut } \Gamma_1} (a^{\alpha(b)}, (a')^{\alpha(b)}) \in \Phi_1 \wedge b^h = (b')^h \implies ((a, b)^{(\alpha, h)}, (a', b')^{(\alpha, h)}) \in \Phi$.

Also $\varphi(\alpha, h) \in \text{Aut } \Gamma$. □

Konkret: $\Gamma_0 := (N, (N \times N) \setminus \Delta_N)$ 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: $\text{Aut } \Gamma_0 = S_2$, $\text{Aut } \Gamma_1 \cong \mathbb{Z}_3$ und $\varphi : H := \text{Aut } \Gamma_1 \wr (\text{Aut } \Gamma_0, N) \rightarrow \text{Aut } \Gamma =: G$ ist ein Isomorphismus. Denn:

$$\begin{aligned} |G| &= |(a, 1)^G| \cdot |G_{(a, 1)}| = G \cdot |(a, 2)^{G_{(a, 1)}}| \cdot |G_{(a, 1), (a, 2)}| \\ &= 6 \cdot 3 = 18 = 3^2 \cdot 2 = |\mathbb{Z}_3|^2 \cdot |S_2| = |H| \end{aligned}$$

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

7.0.8 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
 $(\alpha, h) \in G^N \times H$:

$$\begin{array}{ccc} N & \xrightarrow{h} & N \\ \alpha \downarrow & & \\ G & & \end{array}$$

Exponentiation:

$$\begin{array}{ccccc} N & \xrightarrow{h} & N & & \\ \downarrow f & \searrow \alpha & \downarrow f & & \\ M \times G & \xrightarrow{\text{Wirkung}} & M & & \\ & (b, g) \mapsto b^g & & & \end{array}$$

$\begin{array}{ccc} b & \xrightarrow{\quad} & b^h \\ \downarrow & & \downarrow \\ (f(b), \alpha(b)) & \xrightarrow{\quad} & f(b)^{\alpha(b)} \end{array}$

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

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

für

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

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 $f : N \rightarrow M, x \mapsto a$ (konstant). Dann ist $f^{(\alpha, h)} = a^{\alpha(b)} \neq a = f(b)$ und daher $f^{(\alpha, h)} \neq f$.

□

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

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

Kranzproduktmultiplikation in dieser Schreibweise:

- Einselement: $((e_G, \dots, e_G), e_H)$,
- Inverses von $((g_1, \dots, g_n), h)$: $((g_1^{-1}, \dots, g_n^{-1}), h^{-1})$,

- Multiplikation:

$$((g'_1, \dots, g'_n), h') \cdot ((g''_1, \dots, g''_n), h'') = ((g'_1 g''_1, \dots, g'_n g''_n), h' h'')$$

Insbesondere lässt sich jedes Element zerlegen in ein Produkt der Form

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

vgl. auch 7.5.

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

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

7.0.11 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

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

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

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

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

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

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

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

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

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

7.0.12 Satz. Die Automorphismengruppe des n -dimensionalen Würfels:

$$\text{Aut } \Phi_1(n) \cong S_{\underline{n}} \uparrow S_{\underline{n}}.$$

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

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

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

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

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

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

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

Dann gilt:

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

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

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

Nach (*) folgt $\Gamma_1(0)^f = \Gamma_1(0^f) = \Gamma_1(0)$ für alle $f \in G_0$ (von jetzt an ist $G := \text{Aut } \Phi_1(n)$), d.h. jedes $f \in G_0$ permutiert die Nachbarn von 0 . Wir erhalten eine Abbildung $\psi : G_0 \rightarrow S_N$, $f \mapsto f|_N$, wobei $N := \Gamma_1(0) = \{(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$. Offenbar ist ψ Homomorphismus, außerdem ist ψ surjektiv.

Sei $g \in S_N$. Da die Abbildung $\theta : \{1, \dots, n\} \rightarrow N$, $i \mapsto (0, \dots, 0, 1, 0, \dots, 0)$ (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 $i \in \underline{n}$:

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

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

Wir zeigen nun: ψ ist auch injektiv. Es genügt zu zeigen: $\ker \psi = \{e\}$. Dazu sei $f \in \ker \psi$, d.h. $f \in G_0$ und $f|_N = \text{id}_N$. Wir zeigen $f|_{\Gamma_i(0)} = \text{id}_{\Gamma_i(0)}$ per Induktion über $i \in \{1, \dots, n\}$.

7 OPERATIONEN AUF PERMUTATIONSGRUPPEN

(IA) Nach Voraussetzung.

(IS) Gelte $f|_{\Gamma_i(\mathbf{0})} = \text{id}|_{\Gamma_i(\mathbf{0})}$ für ein $i \in \{1, \dots, n-1\}$. Für alle $\mathbf{b} \in \Gamma_{i+1}(\mathbf{0})$:

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

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

Wegen $B^n = \bigcup_{i=0}^n \Gamma_i(\mathbf{0})$ folgt $f = \text{id}_{B^n}$. Also ist ψ injektiv und damit ein Isomorphismus. Insbesondere gilt: $|G_0| = |S_N| = n!$.

Außerdem: $\mathbf{a}^G = B^n$ (d.h. G ist transitiv). Für jedes $(a_1, \dots, a_n) \in B^n$ gibt es $g_1, \dots, g_n \in S_2$ mit $a_1 = 0^{g_1}, \dots, a_n = 0^{g_n}$ und es folgt $(a_1, \dots, a_n) = (0^{g_1}, \dots, 0^{g_n}) = (0, \dots, 0)^{(g_1, \dots, g_n), e} \in \mathbf{0}^G$.

Finale: Nach 1.14 gilt $|G| = |G_0| \cdot |\mathbf{0}^G| = n! \cdot |B^n| = n! \cdot 2^n$.

Da φ injektiv ist: $|\mathfrak{I}\varphi| = |S_2 \wr (S_{\underline{n}}, \underline{n})| \stackrel{7.5}{=} 2^n n!$. Wegen $\mathfrak{I}\varphi \subseteq G$ folgt $\mathfrak{I}\varphi = G$. Also: φ ist Isomorphismus von $S_{\underline{n}} \wr (S_{\underline{n}}, \underline{n})$ nach G . \square

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 $\iff \exists n \in \mathbb{N} : |G| = p^n$.

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

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

(Menge aller Fixpunkte).

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

$$|M| \equiv |\text{Fix}(G, M)| \pmod{p}.$$

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

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

□

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

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

8.0.3 Definition und Sätzchen. Sei G Gruppe. Dann ist das Zentrum

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

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

Beweis. Übungsaufgabe!

□

8.0.4 Satz. Sei G p -Gruppe für eine Primzahl p und sei $\{e\} \neq N \triangleleft G$. 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:

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

Mit Lemma 8.1 folgt:

$$|N| \equiv |N \cap Z(G)| \pmod{p}. \quad (*)$$

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

8.0.5 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 $N = G$. \square

8.0.6 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:

8.0.7 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:

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

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: $|Z(G)| = p \implies |G/Z(G)| \stackrel{1.12}{=} |G|/|Z(G)| = p \implies G/Z(G)$ zyklisch $\stackrel{8.7}{\implies} G$ abelsch, d.h. $Z(G) = G$. Widerspruch.

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

Nun zum angekündigten Satz:

8.0.8 Satz (Cauchy). 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

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

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

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

ist invariant unter dieser Wirkung:

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

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

$$|M| = |\text{Fix}(\mathbb{Z}_p, M)| \pmod{p}. \quad (*)$$

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

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

Beobachtung 2: Die Abbildung $f : G^{p-1} \rightarrow M$, $(g_0, \dots, g_{p-2}) \mapsto (g_0, \dots, g_{p-2}, (g_0 \cdots g_{p-2})^{-1})$ 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 $\text{ord}(G) \mid p$ (vgl. ALGZTH) und daher $\text{ord}(g) = p$ (da p Primzahl). \square

8.0.9 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 $\text{ord}(a) = 2$ und $\text{ord}(b) = 3$. Fallunterscheidung:

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

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

8 DIE SÄTZE VON CAUCHY UND SYLOW

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

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

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

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

$$\begin{array}{c} \text{Klassifikations-} \\ \implies \\ \text{-satz für endl.} \\ \text{abelsche Gruppen} \end{array} \quad G \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3.$$

□

Bemerkung: Im 2. Fall kann man auch direkt zeigen: $f: \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow G, (k, l) \mapsto a^k b^l$ 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 $G : \iff |H| = p^{v_p(|G|)}$.

Wir bezeichnen mit:

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

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

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

8.0.10 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 Normalisator von H (in G). Es gilt:

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

Beweis. Übungsaufgabe! □

8.0.11 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:

$$|G/H| \equiv |\text{Fix}(H, G/H)| \pmod{p}. \quad (*)$$

Beobachtung: Für alle $g \in G$ gilt:

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

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

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

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

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

□

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

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. $H \stackrel{8.10}{\triangleleft} N(H) = G$. □

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

Beweis. Nach 8.10 ist $H \triangleleft N(H)$. 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

$$\pi : N(H) \rightarrow N(H)/H, g \mapsto Hg.$$

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

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

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

8.0.14 Folgerung. Sei G endliche Gruppe und $H \in \text{Sub}_p(G)$ 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 $H = H_m \leq H_{m+1} \leq \dots \leq H_n \leq G$, sodass $|H_i| = p^i$ für jedes $i \in \{m, \dots, n\}$.

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

Induktionsanfang: Fall $i = m$ ist klar.

Induktionsschritt: Sei $i \in \{m, \dots, n-1\}$ und seien $H = H_m \leq H_{m+1} \leq \dots \leq H_i \leq G$, sodass $|H_j| = p^j$ für jedes $j \in \{m, \dots, i\}$. 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 $|H_{i+1}| = |H_i| \cdot p = p^{i+1}$. □

8.0.15 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 $\text{Syl}_p(G) \neq \emptyset$.
- (b) $\text{Syl}_p(G) = \max(\text{Sub}_p(G), \subseteq)$, 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* : $\iff \exists g \in G : g^{-1}Ug = V$.

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

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

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

8 DIE SÄTZE VON CAUCHY UND SYLOW

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

$$p \nmid \frac{|G|}{|K|} \stackrel{\text{LAGR.}}{=} [G : K] = |G/K|.$$

Da H p -Gruppe ist, können wir Folgerung 8.12 anwenden, und schließen: $\text{Fix}(H, G/K) \neq \emptyset$. Sei $g \in G$ mit $Kg \in \text{Fix}(H, G/K)$, 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:

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

□

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

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

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

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

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

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

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

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

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

Wir zeigen: $\text{Fix}(P, \text{Syl}_p(G)) = \{P\}$. Offenbar: $P \in \text{Fix}(P, \text{Syl}_p(G))$, da $g^{-1}Pg = P$ für alle $g \in P$. Sei $H \in \text{Fix}(P, \text{Syl}_p(G))$. 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: $P, H \in \text{Syl}_p(N(H))$. Nach Satz 8.16, SYLOW II sind P und H konjugiert in $N(H)$, d.h. es gibt $g \in N(H)$ mit $P = g^{-1}Hg \stackrel{g \in N(H)}{=} H$. Das zeigt die Behauptung. Aus (*) folgt: $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$.

8 DIE SÄTZE VON CAUCHY UND SYLOW

Zu (b): Nach Satz 8.16, SYLOW II ist $(G, \text{Syl}_p(G))$ transitiv. Sei $H \in \text{Syl}_p(G)$. Dann gilt:

$$G_H = \{g \in G \mid g^{-1}Hg = H\} = N(H).$$

Daher $|G| \stackrel{1.14}{=} |H^G| \cdot |G_H| = |\text{Syl}_p(G)| \cdot |N(H)|$. Es folgt:

$$|\text{Syl}_p(G)| = \frac{|G|}{|N(H)|} \stackrel{\text{LAGR.}}{=} [G : N(H)].$$

Letzte Aussage: $|\text{Syl}_p(G)| \cdot [N(H) : H] = [G : N(H)] \cdot [N(H) : H] \stackrel{\text{ALGZTH}}{=} [G : H]$. Also
 $|\text{Syl}_p(G)| = [G : N(H)] \stackrel{\text{LAGR.}}{=} \frac{|G|}{|H|} = \frac{|G|}{p^{v_p(|G|)}}.$ \square

8.0.19 Satz. Sei G endliche Gruppe und seien p und q verschiedene Primzahlen mit $|\text{Syl}_p(G)| = 1 = |\text{Syl}_q(G)|$. 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:

$$\underbrace{g^{-1}h^{-1}g}_{\in Q}h \in P \cap Q \implies g^{-1}h^{-1}gh = e, \text{ d.h. } gh = hg.$$

\square

8.0.20 Satz. Sei G endliche Gruppe, p_1, \dots, p_n seien die paarweise verschiedene Primteiler von $|G|$. Gilt $\text{Syl}_{p_i}(G) = \{P_i\}$ für jedes $i \in \{1, \dots, n\}$, dann ist die Abbildung

$$\varphi : P_1 \times \dots \times P_n \rightarrow G, (g_1, \dots, g_n) \mapsto g_1 \cdots g_n$$

ein Gruppenisomorphismus.

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

$$\text{ord}(g_1 \cdots g_n) = \text{ord}(g_1) \cdots \text{ord}(g_n).$$

Beweis. Sei $m_1 := \text{ord}(g_1), \dots, m_n := \text{ord}(g_n)$, $m := m_1 \cdots m_n$. Dann $(g_1 \cdots g_n)^m \stackrel{\text{komm.}}{=} g_1^m \cdots g_n^m \stackrel{m_i \mid m}{=} e$. Daher $k := \text{ord}(g_1 \cdots g_n) \mid m$. Für $i \in \{1, \dots, n\}$:

$$\begin{aligned} e &= (g_1 \cdots g_n)^{km_1 \cdots m_{i-1} m_{i+1} \cdots m_n} \\ &\stackrel{\text{komm.}}{=} g_1^{km_1 \cdots m_{i-1} m_{i+1} \cdots m_n} \cdots g_n^{km_1 \cdots m_{i-1} m_{i+1} \cdots m_n} \\ &= g_i^{km_1 \cdots m_{i-1} m_{i+1} \cdots m_n} \end{aligned}$$

$\implies m_i \mid km_1 \cdots m_{i-1} m_{i+1} \cdots m_n \stackrel{m_1, \dots, m_n \text{ teilerfremd}}{\implies} m_i \mid k$. Nochmal Teilerfremdheit liefert: $m = m_1 \cdots m_n \mid k$. Also $m = k$. \square

Beweis von Satz 8.20. φ ist Homomorphismus:

$$\begin{aligned}\varphi((g_1, \dots, g_n)(h_1, \dots, h_n)) &= \varphi((g_1 h_1, \dots, g_n h_n)) \\ &= g_1 h_1 \cdots g_n h_n \stackrel{8.19}{=} g_1 \cdots g_n h_1 \cdots h_n \\ &= \varphi((g_1, \dots, g_n)) \cdot \varphi((h_1, \dots, h_n))\end{aligned}$$

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

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

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

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

Surjektivität von φ :

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

$$\stackrel{\varphi \text{ ist}}{\stackrel{\text{injektiv}}{\implies}} G = \varphi(P_1 \times \dots \times P_n).$$

Somit ist φ ein Isomorphismus. □

8.0.21 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):

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

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

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

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

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

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

- (1) $|\text{Syl}_q(G)| = p \xrightarrow[\text{Teil (a)}]{8.18} p \equiv 1 \pmod{q} \iff q \mid (p-1)$. Widerspruch.
- (2) $|\text{Syl}_q(G)| = p^2 \xrightarrow[\text{Teil (a)}]{8.18} p^2 \equiv 1 \pmod{q}$
 $\iff q \mid (p^2 - 1) = (p+1)(p-1)$
 $\iff q \mid (p+1) \vee q \mid (p-1)$.

Widerspruch.

Also $|\text{Syl}_p(G)| = 1$. Sei $\text{Syl}_p(G) = \{P\}$ und $\text{Syl}_q(G) = \{Q\}$. 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. \square

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.

8.0.23 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 $\text{ord}(g) = \max\{\text{ord}(h) \mid h \in G\}$. Zu zeigen: $G = \langle g \rangle$. Sei dazu $h \in G$. Nach dem Satz von LAGRANGE: $\exists m, n \in \mathbb{N} : \text{ord}(g) = p^m, \text{ord}(h) = p^n$. 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, \dots, p_n die paarweise verschiedene Primteiler von $|G|$. Nach Voraussetzung: $|\text{Syl}_{p_i}(G)| = 1$ für jedes $i \in \{1, \dots, n\}$. Sei $i \in \{1, \dots, n\}$ und $\text{Syl}_{p_i}(G) = \{P_i\}$. Nach Schritt 1: P_i ist zyklisch, d.h. $P_i = \langle g_i \rangle$ für ein $g_i \in P_i$ und daher $\text{ord}(g_i) = |P_i| = p_i^{v_{p_i}(|G|)}$. Nach Satz 8.20:

$$\begin{aligned} G \cong P_1 \times \dots \times P_n &\stackrel{\text{Schritt 1}}{\cong} \mathbb{Z}_{p_1^{v_{p_1}(|G|)}} \times \dots \times \mathbb{Z}_{p_n^{v_{p_n}(|G|)}} \\ &\stackrel{\text{teilerfr.}}{\cong} \mathbb{Z}_{p_1^{v_{p_1}(|G|)}} \dots p_n^{v_{p_n}(|G|)}. \end{aligned} \quad (\square)$$

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

$$\text{ord}(g_1 \cdots g_n) = \text{ord}(g_1) \cdots \text{ord}(g_n) = p_1^{v_{p_1}(|G|)} \cdots p_n^{v_{p_n}(|G|)} = |G|$$

$\implies G$ ist zyklisch. \square

8.0.24 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 $\text{ord}(g) = \max\{\text{ord}(h) \mid h \in G\}$. Für alle $h \in \langle g \rangle$ ist $h^{\text{ord}(g)} = e$ (da $\text{ord}(h) \mid \text{ord}(g)$ nach dem Satz von LAGRANGE). Nach Voraussetzung (für $n := \text{ord}(g) = |\langle g \rangle|$):

$$\{x \in G \mid x^{\text{ord}(g)} = e\} = \langle g \rangle. \quad (*)$$

Für jedes $h \in G$ ist $\text{ord}(h)$ eine p -Potenz (da G eine p -Gruppe ist) und $\text{ord}(h) \leq \text{ord}(g)$. Daher $\text{ord}(h) \mid \text{ord}(g)$, also $h^{\text{ord}(g)} = e \stackrel{(*)}{\implies} h \in \langle g \rangle$. Also ist $H = \langle g \rangle$ zyklisch.
Schritt 2: Sei p Primteiler von $|G|$, $P \in \text{Syl}_p(G)$. Dann $g^{|P|} = e$ für jedes $g \in P$. Nach Voraussetzung:

$$\{x \in G \mid x^{|P|} = e\} = P. \quad (**)$$

Sei $P' \in \text{Syl}_p(G)$. 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 $|P'| = p^{v_p(|G|)} = |P|$). Das Zeigt: $|\text{Syl}_p(G)| = 1$. Rest wie letzter Teil im Schritt 2 im Beweis von 8.23. Erinnerung:

$$\begin{aligned} G &\stackrel{8.20}{\cong} P_1 \times \dots \times P_n \stackrel{\text{Schritt 1}}{\cong} \mathbb{Z}_{p_1^{v_{p_1}(|G|)}} \times \dots \times \mathbb{Z}_{p_n^{v_{p_n}(|G|)}} \\ &\stackrel{\text{teilerfr.}}{\cong} \mathbb{Z}_{p_1^{v_{p_1}(|G|)} \dots p_n^{v_{p_n}(|G|)}} = \mathbb{Z}_{|G|}. \end{aligned}$$

□

9 Einfache Gruppen

9.0.1 Definition und Sätzchen. Sei G Gruppe.

G ist einfach $\iff \{e\}$ und G sind die einzigen Normalteiler von G

^{Übung³}
 $\iff \forall H \text{ Gruppe } \forall h : G \rightarrow H \text{ Homomorphismus:}$
 $h \text{ ist injektiv oder konstant.}$

9.0.2 Bemerkungen. (1) Für endliche abelsche Gruppe G gilt:

G ist einfach $\iff \{e\}$ und G sind die einzigen Untergruppen von G

$\iff^4 |G| = 1$ oder $|G|$ ist eine Primzahl

$\iff^5 |G| = 1$ oder $G \cong \mathbb{Z}_p$ für eine Primzahl p .

(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.

9.0.3 Satz. Sei G endliche Gruppe. Dann existiert Kette von Untergruppen:

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G,$$

sodass G_i/G_{i-1} einfach ist für jedes $i \in \{1, \dots, n\}$.

Beweis. Da G endlich ist, ist $n := \sup\{m \in \mathbb{N} \mid \exists \{e\} \neq G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{m-1} \triangleleft G\} < \infty$.

Sei $\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$. Behauptung: $\forall i \in \{1, \dots, n\}$: G_i/G_{i-1} einfach. Sei $i \in \{1, \dots, n\}$. Annahme: G_i/G_{i-1} nicht einfach. Dann:

$$\exists N \triangleleft G_i/G_{i-1} : N \neq \{e_{G_i/G_{i-1}}\} = \{G_{i-1}\}.$$

Dann $\pi^{-1}(N) \triangleleft G_i$ (sonst $N = \pi(\pi^{-1}(N)) = \pi(G_i) = G_i/G_{i-1}$ und $G_{i-1} = \text{Ker } \pi \triangleleft \pi^{-1}(N)$). Also:

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{i-1} \triangleleft \pi^{-1}(N) \triangleleft G_i \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G.$$

Diese Kette hat ein Glied mehr als die ursprüngliche. Widerspruch zur Definition von n . Daher ist G_i/G_{i-1} einfach. \square

³Hinweis: Für eine Richtung den Kern anschauen, für die andere Richtung Faktorgruppe benutzen.

⁴Hinweis: Eine Richtung mit dem Satz von LAGRANGE (1.12), die andere mit dem Satz von CAUCHY (8.8.)

⁵Hinweis: Beweis mit dem Klassifikationssatz oder direkt.

⁶Fun Fact: Letzte Lücke im Beweis wurde 2002 geschlossen.

Die entstehenden Faktoren G_i/G_{i-1} ($i \in \{1, \dots, n\}$) sind (bis auf Isomorphie und Permutation der Reihenfolge) eindeutig bestimmt:

9.0.4 Satz (Jordan-Hölder). Sei G endliche Gruppe. Sind

$$\begin{aligned}\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_{n-1} \trianglelefteq G_n = G, \\ \{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_{m-1} \trianglelefteq H_m = G,\end{aligned}$$

sodass $\forall i \in \{1, \dots, n\}: G_i/G_{i-1}$ einfach und $\forall j \in \{1, \dots, m\}: H_j/H_{j-1}$ einfach, dann gilt: $m = n$ und es gibt $\pi \in S_n$ mit

$$\forall i \in \{1, \dots, n\}: G_i/G_{i-1} \cong H_{i\pi}/H_{i\pi-1}.$$

Beweis. Eventuell später. □

Nächstes Ziel: Einfachheit alternierender Gruppen.

9.0.5 Lemma. Sei $n \in \mathbb{N}$ mit $n \geq 3$. Die Gruppe A_n wird erzeugt von der Menge

$$E := \{(a \ b \ c) \mid a, b, c \in \underline{n}, |\{a, b, c\}| = 3\}.$$

Beweis. Zunächst: $E \subseteq A_n$. Denn: $(a \ b \ c)(b \ a) = (a)(b \ c)$, daher

$$\begin{aligned}\text{sgn}((a \ b \ c)) &= \text{sgn}((a \ b \ c)(b \ a)(b \ a)) \\ &\stackrel{\text{Homom.}}{=} \underbrace{\text{sgn}((a \ b \ c)(b \ a))}_{=-1} \cdot \underbrace{\text{sgn}((b \ a))}_{=-1} = 1,\end{aligned}$$

d.h. $(a \ b \ c) \in A_n$ für alle $(a \ b \ c) \in E$. Zu zeigen:

$$\forall a, b, c, d \in \underline{n}, a \neq b, c \neq d: (a \ b)(c \ d) \in \langle E \rangle. \quad (*)$$

Fallunterscheidung:

- $(a \ b)(a \ b) = e \in \langle E \rangle,$
- $(a \ b)(a \ c) = (a \ b \ c) \in E \subseteq \langle E \rangle,$
- $(a \ b)(c \ d) = (a \ b \ c)(a \ d \ c) \in \langle E \rangle.$

Aussage des Lemmas: Sei $g \in A_n$. Dann gibt es Transpositionen $h_1, h_2, \dots, h_{2t-1}, h_{2t}$ mit

$$g = \underbrace{h_1 h_2}_{\substack{\in \langle E \rangle \\ \text{nach } (*)}} \cdots \underbrace{h_{2t-1} h_{2t}}_{\substack{\in \langle E \rangle \\ \text{nach } (*)}} \in \langle E \rangle.$$

□

9.0.6 Lemma. Sei $n \in \mathbb{N}$ mit $n \geq 5$. Je zwei Elemente von

$$E := \{(a \ b \ c) \mid a, b, c \in \underline{n}, |\{a, b, c\}| = 3\}$$

sind konjugiert in A_n .

Beweis. Sei $(a \ b \ c) \in E$. Zeige: $(a \ b \ c)$ ist konjugiert zu $(1 \ 2 \ 3)$ in A_n . Aussage des Lemmas folgt dann mit 1.19 (a). Da $(a \ b \ c)$ und $(1 \ 2 \ 3)$ ähnlich sind, sind sie konjugiert in S_n (vgl. 1.19 (c)), d.h. $\exists h \in S_n : (1 \ 2 \ 3) = h(a \ b \ c)h^{-1}$. Ist $h \in A_n$, dann fertig. Annahme: $h \notin A_n$, d.h. $\text{sgn}(h) = -1$. Setze $\tilde{h} := (4 \ 5)h$. Dann $\text{sgn}(\tilde{h}) = \text{sgn}((4 \ 5)) \cdot \text{sgn}(h) = 1$, also $\tilde{h} \in A_n$, und

$$\begin{aligned}\tilde{h}(a \ b \ c)\tilde{h}^{-1} &= (4 \ 5)h(a \ b \ c)h^{-1}(4 \ 5) \\ &\stackrel{(*)}{=} (4 \ 5)(1 \ 2 \ 3)(4 \ 5) \\ &= (1 \ 2 \ 3).\end{aligned}$$

□

9.0.7 Folgerung. A_5 ist einfach.

Erinnerung (vgl. 3.8): Ein Zyklus ist genau dann eine gerade Permutation, wenn er ungerade Länge hat, denn:

$$\begin{aligned}(a_1 \ \cdots \ a_k) &\stackrel{3.9}{=} (a_1 \ a_2)(a_1 \ a_3) \cdots (a_1 \ a_{k-1})(a_1 \ a_k) \\ &= (a_k \ a_{k-1})(a_{k-1} \ a_{k-2}) \cdots (a_3 \ a_2)(a_2 \ a_1) \Big\}^{(k-1) \text{ Faktoren.}}\end{aligned}$$

Beweis von 9.7. Jedes Element von A_5 ist von einem der folgenden Typen (für $\{a, b, c, d, e\} = \{1, 2, 3, 4, 5\}$).

Maximum der Zyklenlängen in Zykeldarstellung	Typ (Zykeldarstellung)
1	$e = (a)(b)(c)(d)(e)$
2	$(a \ b)(c \ d)(e) \rightarrow \text{Typ (I)}$
3	$(a \ b \ c)(d)(e) \rightarrow \text{Typ (II)}$
4	
5	$(a \ b \ c \ d \ e) \rightarrow \text{Typ (III)}$

Sei $\{e\} \neq N \triangleleft A_5$.

Behauptung: N enthält ein Element von $E := \{(a \ b \ c) \mid a, b, c \in \underline{5}, |\{a, b, c\}| = 3\}$.

Beweis. Sei $g \in N \setminus \{e\}$. Fallunterscheidung:

Fall 1: g hat Typ (I), also $g = (a \ b)(c \ d)$. Dann

$$\underbrace{((a \ b \ e)g(a \ b \ e)^{-1})}_{=(a \ e \ b)(c)(d) \in E} g \in N \text{ (da } N \triangleleft A_5\text{)}.$$

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 $g = (a \ b \ c \ d \ e)$. Dann

$$\underbrace{((a \ b \ e)g(a \ b \ e)^{-1})}_{=(a)(b \ c \ e)(d) \in E} g \in N \text{ (da } N \triangleleft A_{\underline{5}}\text{)}.$$

Also $N \cap E \neq \emptyset$. □

Nach Behauptung: $N \cap E \neq \emptyset$. Wegen Lemma 9.6 und $N \triangleleft A_{\underline{5}}$, 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. □

9.0.8 Lemma. Sei $n \in \mathbb{N}$, $n \geq 5$. Dann: $\forall g \in A_{\underline{n}} : \forall A_{\underline{n}} \setminus \{e\} \exists n \in A_{\underline{n}} \setminus \{g\} :$

- (i) g und h sind konjugiert in $A_{\underline{n}}$, und
- (ii) $\exists i \in \{1, \dots, n\} : i^g = i^h$.

Beweis. Sei $g \in A_{\underline{n}} \setminus \{e\}$. Sei m die maximale Länge eines Zyklus in der Zykeldarstellung von g . Klar: $m \geq 2$. Fallunterscheidung:

$m \geq 3$: Sei $g = (a_1 \ \dots \ a_m)g'$ Zykeldarstellung von g . Wähle $b, c \in \{1, \dots, n\} \setminus \{a_1, a_2, a_3\}$, $b \neq c$. Dann $(a_3 \ b \ c) \in A_{\underline{n}}$ (vgl. 9.5) und daher $h := (a_3 \ b \ c)g(a_3 \ b \ c)^{-1} \in A_{\underline{n}}$ konjugiert zu g in $A_{\underline{n}}$. Nun:

- $a_1^h = a_1^{(a_3 \ b \ c)g(a_3 \ b \ c)^{-1}} = a_2 = a_1^g$,
- $a_2^h = a_2^{(a_3 \ b \ c)g(a_3 \ b \ c)^{-1}} = c \neq a_3 = a_2^g \implies g \neq h$.

$m = 2$: Dann $h = (a_{11} \ a_{12})(a_{21} \ a_{22})(a_{31} \ a_{32}) \dots (a_{k1} \ a_{k2})$ für paarweise verschiedene $a_{11}, a_{12}, \dots, a_{k1}, a_{k2} \in \underline{n}$. Fallunterscheidung ($k \geq 2$, da g gerade Permutation ist):

$k \geq 3$: Dann $(a_{11} \ a_{12})(a_{21} \ a_{31}) \in A_{\underline{n}}$ und daher

$$h := (a_{11} \ a_{12})(a_{21} \ a_{31})g(a_{11} \ a_{12})(a_{21} \ a_{31}) \in A_{\underline{n}}$$

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 $g = (a_{11} \ a_{12})(a_{21} \ a_{22})$. Dann $(a_{11} \ a_{21} \ a_{12}) \in A_{\underline{n}}$ (vgl. 9.5), also $h := (a_{11} \ a_{21} \ a_{12})h(a_{11} \ a_{12} \ a_{21}) \in A_{\underline{n}}$ 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 $b \in \{1, \dots, n\} \setminus \{a_{11}, a_{12}, a_{21}, a_{22}\}$.

□

9.0.9 Lemma. Sei $n \in \mathbb{N}$ mit $n \geq 3$, und $i \in \{1, \dots, n\}$. Dann gilt: $(A_{\underline{n}})_i \cong A_{\underline{n-1}}$.

Beweis. Betrachte Injektion $f : \{1, \dots, n-1\} \rightarrow \{1, \dots, n\}$ mit

$$f(j) := \begin{cases} j & \text{falls } j < i, \\ j+1 & \text{falls } j \geq i \ (j \in \{1, \dots, n-1\}). \end{cases}$$

Dann $\mathfrak{I}(f) = \{1, \dots, n\} \setminus \{i\}$. Betrachte injektiven Homomorphismus $\Phi : S_{n-1} \rightarrow S_n$ mit

$$j^{\Phi(g)} := \begin{cases} f(f^{-1}(j)^g) & \text{falls } j \neq i, \\ i & \text{sonst,} \end{cases}$$

für $j \in \{1, \dots, n\}$ und $g \in S_{n-1}$. Dann $\mathfrak{I}(\Phi) = (S_n)_i$. Und: Φ bildet Transpositionen auf Transpositionen ab. Genauer:

$$\Phi((j \ k)) = (f(j) \ f(k))$$

für alle $j, k \in \{1, \dots, n-1\}$, $j \neq k$. Folgerung:

$$\begin{aligned} g \in A_{n-1} &\iff g \text{ ist Produkt einer geraden Anzahl von Transpositionen} \\ &\implies \Phi(g) \text{ ist Produkt einer geraden Anzahl von Transpositionen} \\ &\iff \Phi(g) \in A_n. \end{aligned}$$

Also $\Phi(A_{n-1}) \subseteq A_n \cap (S_n)_i = (A_n)_i$. Und:

$$|(A_n)_i| = \frac{|A_n|}{|i^{A_n}|} \stackrel{A_n \text{ ist transitiv}}{=} \frac{\frac{n!}{2}}{n} = \frac{(n-1)!}{2} = |A_{n-1}|.$$

Also $\Phi(A_{n-1}) = (A_n)_i$. Damit ist $A_{n-1} \cong (A_n)_i$. □

9.0.10 Satz. Sei $n \in \mathbb{N}$ mit $n \geq 5$. Dann ist A_n einfach.

Beweis. Induktion über $n \geq 5$:

Induktionsanfang: Folgerung 9.7.

Induktionsschritt: Sei $n \geq 6$ und Einfachheit von A_{n-1} vorausgesetzt. Sei $\{e\} \neq N \triangleleft A_n$.

Sei $g \in N \setminus \{e\}$. Nach Lemma 9.8: $\exists h \in A_n \setminus \{g\}$:

- (i) g und h konjugiert in A_n ,
- (ii) $\exists i \in \{1, \dots, n\} : i^g = i^h$.

Wegen (i) und $N \triangleleft A_n$ ist $h \in N$. Wegen (ii) ist $g h^{-1} \in (A_n)_i =: H_i$ für ein $i \in \{1, \dots, n\}$. Also: $e \neq g h^{-1} \in N \cap H_i \implies N \cap H_i \neq \{e\}$. Wegen $N \triangleleft A_n$ ist $(N \cap H_i) \triangleleft H_i$ (ganz

allgemein gilt $N \triangleleft G, H \leq G \implies N \cap H \triangleleft H$). Weil $H_i = (A_n)_i \stackrel{9.9}{\cong} A_{n-1}$ 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 $N \triangleleft A_n$ enthält N jeden Zyklus der Länge 3. Mit Lemma 9.5 folgt: $N = A_n$. Das zeigt: A_n ist einfach. □