0.1 Strukturtheorie zu Gruppen ("Einige Aussagen")

Sei im Weiteren M ein Monoid, G eine Gruppe und X eine Menge.

Definition 0.1 (**Wirkung**)**.** Eine Abbildung

$$\lambda : M \times X \to X, (m, x) \mapsto m \cdot x := \lambda(m, x)$$

heißt Linkswirkung (left action, Linksoperation) von M auf X, wenn es gelten $\forall x \in X, m, m' \in M$:

(i) Neutrales Element: $e \cdot x = x$

(ii) Assoziativität: $m \cdot (m' \cdot x) = (m \cdot m') \cdot x$

Bezeichnung. Ist M eine Gruppe, so heißt λ auch Gruppenwirkung und X heißt Links-M-Menge.

Bemerkung. Analog kann man auch Rechtswirkungen

$$\rho : X \times M \to X, (x, m) \mapsto x \cdot m$$

definieren. (Axiome: $x \cdot e = c$ und $(x \cdot m) \cdot m' = x \cdot (m \cdot m')$)

Bemerkung (Übung)**.** Jede Links-G-Wirkung kann man in eine Rechts-G-Wirkung überführen: zu $\lambda : G \times X \to X$ definiere $\rho : X \times G \to X$ durch

$$\rho(x, g) := \lambda(g^{-1}, x) \iff x \cdot g := g^{-1} \cdot x$$

Proposition 0.2 (Alternative Beschreibung von Wirkungen)**.**

(a) Sei $\lambda : G \times X \to X$ eine Linkswirkung, dann ist

$$\varphi : G \to \mathrm{Bij}(X), g \mapsto (\varphi_g : X \to X, x \mapsto gx)$$

ein wohl-definierter Gruppenhomomorphismus.

(b) Sei $\varphi : G \to \mathrm{Bij}(X)$ ein Gruppenhomomorphismus, dann ist

$$\lambda : G \times X \to X, (g, x) \mapsto \varphi(g)(x)$$

eine Linkswirkung von G auf X.

Beweis. (a) Für $g \in G$ sei $\varphi_g : X \to X, x \mapsto gx$, dann gelten: $\varphi_e : X \to X, x \mapsto ex = x$ ist id_X (Axiom (i)), und

$$(*) \quad \varphi_g \circ \varphi_{g'} = \varphi_{gg'}$$

denn $\forall x \in X$:

$$(\varphi_g \circ \varphi_{g'})(x) = \varphi_g(\varphi_{g'}(x)) = g(g'x) \overset{(ii)}{=} (gg')x = \varphi_{gg'}(x)$$

Damit folgen:

1. $\varphi_g \circ \varphi_{g^{-1}} = \underbrace{\varphi_e}_{\mathrm{id}_X} = \varphi_{g^{-1}} \circ \varphi_g \implies \varphi_g$ ist eine bijektive Abbildung mit Inverse $\varphi_{g^{-1}}$, d.h.
$$\varphi : G \to \mathrm{Bij}(X), g \mapsto \varphi_g$$
ist wohl-definiert.
2. φ ist ein Gruppenhomomorphismus: folgt aus $(*)$ (Verknüpfung in $\mathrm{Bij}(X)$ ist die Verkettung von Abbildungen.)

(b) Übung.

□

Bemerkung. (a) Das Analogon von Proposition 2 gilt auch für Monoide. Die Linkewirkungen eines Monoids M auf X entsprechen Monoidhomomorphismen $M \to (\mathrm{Abb}(X, X), \mathrm{id}_X, \circ)$

(b) Eine Gruppe kann auch auf "Objekten" mit mehr Struktur als eine Menge wirken, z.B. auf eine Gruppe!

Beispiel. G wirkt auf eine Gruppe N heißt, man hat einen Gruppenhomomorphismus $G \to \mathrm{Aut}(N)$ (vgl. Lemma 1.56)

Definition 0.3 (Eigenschaften von Wirkungen)**.** Sei $\lambda : G \times X \to X$ eine Linkswirkung von G auf X.

(a) Die Bahn zu $x \in X$ ist $Gx = \{gx \mid g \in G\}$. Die Länge der Bahn zu x ist $\#Gx$

(b) λ ist transitiv $\iff \forall y, z \in X \exists g \in G : gy = z \overset{\text{Übung}}{\iff} \forall y \in X : Gy = X \overset{\text{Übung}}{\iff} \exists x \in X : Gx = X$

(c) λ ist n-fach transitiv ($n \in \mathbb{N}$), wenn für alle Paare von n-Tupeln $(x_1, ..., x_n), (y_1, ..., y_n) \in X^n$ mit $\#\{x_1, ..., x_n\} = \#\{y_1, ..., y_n\}$ gilt $\exists g \in G : gx_i = y_i, \forall i$.

(d) Die Wirkung heißt treu, wenn der induzierte Gruppenhomomorphismus $\varphi : G \to \mathrm{Bij}(X)$ (aus Proposition 2) injektiv ist
$$\overset{\text{Übung}}{\iff} \forall g \in G \setminus \{e\} : \exists x \in X : \underbrace{gX \neq X}_{\varphi_g(x) \neq \mathrm{id}_X(x)}$$

Beispiel 0.4.

1. Ist V ein K-Vektoraum, so wirkt das Monoid $(K, 1, \cdot)$ auf V durch Skalarmultiplikation $(\lambda, v) \mapsto \lambda v$
2. Die folgenden 3 Beispiele sind Linkswirkungen von $\mathrm{GL_n}(K)$:
   (i) $\mathrm{GL_n}(K) \times K^n \to K^n, (g, v) \mapsto gv$. (Übung: Es gibt die Bahnen $\{0\}, K^n \setminus \{0\}$)
   (ii) Sei $\mathcal{B} = \{$geordnete Basen von $K^n\}$ und
   $$\mathrm{GL_n}(K) \times \mathcal{B} \to \mathcal{B}, (g, (b_1, ..., b_n)) \mapsto (gb_1, ..., gb_n)$$
   die Wirkung ist treu und transitiv.

(iii) $\mathrm{GL_n}(K) \times \mathrm{End}_K(K^n) \to \mathrm{End}_K(K^n), (A, B) \mapsto ABA^{-1}$ die Wirkung ist nicht treu $Z(\mathrm{GL_n}(K))$ wirkt trivial. (Übung: Bahnen stehen in Bijektion zu den Frobeniusnormalformen von Matrizen.)

3. $S_n \times \{1, ..., n\} \to \{1, ..., n\}, (\sigma, i) \mapsto \sigma(i)$ Wirkung ist treu und n-fach transitiv.

4. Abstrakte Beispiele: Sei $H \leq G$ eine Untergruppe.

   (i) $\lambda : H \times G \to G, (h, g) \mapsto hg$. Die Bahnen sind die Mengen Hg, also die Rechtsnebenklassen zu H (treu?) Menge der Rechtsnebenklassen

   $$H \backslash G := \{Hg \mid g \in G\}$$

   (ii) $\rho : G \times H \to G, (g, h) \mapsto gh$ Bahnen = Linksnebenklassen zu H und

   $$G/H = \{gH \mid g \in G\}$$

   (iii) $c. : G \times G \to G, (g, g') \mapsto gg'g^{-1}$ ist eine Linkswirkung, denn der nach Proposition 2 zugehörige Gruppenhomomorphismus ist $c : G \to \mathrm{Aut}(G), g \mapsto c_g$.

   (iv) $G \times G/H \to G/H, (g, g'H) \mapsto gg'H$ Die Klassen gH heißen Linksnebenklassen wegen der Links-G-Wirkung auf ihnen.

Proposition 0.5. *Sei X eine Links-G-Menge (zu der Wirkung $\lambda : G \times X \to X, (g, x), \mapsto gx$) definiere Relation $\sim$ auf X durch*

$$x \sim y \iff \exists g \in G : gx = y$$

dann gelten:

(a) $\sim$ ist eine Äquivalenzrelation.

(b) Die Äquivalenzklasse zu $x \in X$ bezüglich $\sim$ ist die Bahn Gx. Insbesondere ist X die disjunkte Vereinigung seiner Bahnen. (Ist $(x_i)_{i \in I}$ ein Repräsentantensystem der G-Bahnen, so gilt also $\#X = \sum_{i \in I} \#Gx$)

Beweis. (a) $\sim$ ist eine Äquivalenzrelation: Prüfe

- $\sim$ reflexiv: $ex = x \implies x \sim x$.
- $\sim$ symmetrisch: Gelte $x \sim y$, d.h. $\exists g \in G : gx = y$, dann gilt $x = ex = g^{-1}(gx) = g^{-1}y \implies y \sim x$.
- $\sim$ transitiv: Gelte $x \sim y$ und $y \sim z$, d.h. $\exists g, h' \in G : gx = y, g'y = z$

$$\implies (g'g)x = g'(gx) = g'y = z \implies x \sim z$$

(b) Sei $x \in X$, dann ist

$$\{y \in X \mid x \sim y\} = \{y \in X \mid \exists g \in G : y = gx\} = \{gx \mid g \in G\} = Gx.$$

$\square$

Satz 0.6 (**Satz von Cayley**). *Jede Gruppe G (jedes Monoid M) ist isomorph zu einer Untergruppe (einem Untermonoid) von* $(\mathrm{Bij}(G), \mathrm{id}_G, \circ)$ *(bzw.* $(\mathrm{Abb}(G, G), \mathrm{id}_G, \circ)$*).*

Beweis. (Für Gruppen, Rest ist eine Übung) Definiere die Wirkung $\lambda G \times G \to G, (g, h) \mapsto gh$, dann erhalten wir den induzierten Gruppenhomomorphismus $\varphi : G \to \mathrm{Bij}(G)$, wir zeigen φ ist injektiv: Sei $g \in G \setminus \{e\}$, dann gilt $ge = g \neq e \implies$ Wirkung treu, also φ ist ein Gruppenmonomorphismus. D.h. G "ist" Untergruppe von $\mathrm{Bij}(G)$. $\square$

Definition 0.7 (**Stabilisator**). Sei X eine Links-G-Menge und $x \in X$, dann heißt

$$G_x := \mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$$

Stabilisator von x (unter G). Warnung: $G_x \neq G \cdot x$.

Beispiel. $\mathrm{Stab}_{S_n}(\{n\}) = \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}$ mit der üblichen S_n-Wirkung auf $\{1, ..., n\}$.

Übung. G-Wirkung auf einer Menge X ist treu

$$\iff \bigcap_{x \in X} \mathrm{Stab}_G(x) = \{e\}$$

Proposition 0.8. *Sei X eine links-G-Menge, $x \in X, g \in G$, dann gilt*

(a) $\mathrm{Stab}_G(x) \leq G$ *ist eine Untergruppe.*

(b) $\mathrm{Stab}_G(gx) = g\,\mathrm{Stab}_G(x) g^{-1}$

Beweis.

(a) $e \in \mathrm{Stab}_G(x)$, denn $ex = x$. Seien $\underbrace{g_1, g_2 \in \mathrm{Stab}_G(x)}_{\text{bedeutet } g_1 x = x, g_2 x = x}$, zu zeigen ist $g_1^{-1} g_2 \in \mathrm{Stab}_G(x)$

$$\stackrel{g_1^{-1}\cdot}{\implies} x = ex = g_1^{-1} g_1 x = g^{-1} x$$

Damit gilt $(g_1^{-1} \cdot g_2^{-1})x = g_1^{-1}(g_2 x) = g_1^{-1} x = x$

(b) Sei $h \in G$, dann:

$$h \in \mathrm{Stab}_G(gx) \iff hgx = gx \stackrel{g^{-1}\cdot}{\iff} g^{-1} hgx = x$$

$$\iff g^{-1} hg \in \mathrm{Stab}_G(x) \underset{\text{Konj. mit } g}{\iff} h \in g\,\mathrm{Stab}_G(x) g^{-1}.$$ $\square$

Proposition 0.9 (Bahngleichung). *Sei X eine links-G-Menge, $x \in X$, dann gilt:*

- $\psi : {}^{G}\!/_{G_x} \to Gx, hG_x \mapsto hx$ *ist wohl-definiert und eine Bijektion.*
- *Ist G endlich, so folgt* $\#G \cdot x = [G : G_x]$.

Beweis.

- ψ injektiv und wohl definiert: Seien $g, h \in G$, dann

$$hx = gx \iff g^{-1}hx = x \iff g^{-1}h \in G_x \leq G$$
$$\iff g^{-1}hG_x = G_x \iff hG_x = gG_x$$

- ψ surjektiv nach Definition von $G \cdot x$.
- Aussage über Mächtigkeiten: ψ bijektiv $\implies \# {}^{G}/_{G_x} = \# G \cdot x$.

$\square$

Bemerkung. Die Abbildung ψ ist ein Homomorphismus von links-G-Mengen (ein Isomorphismus!), ${}^{G}/_{G_x}$ und $G \times x \subseteq X$ sind links-G-Mengen und ψ erfüllt:

$$\psi(g \cdot hG_x) = g \cdot \psi(hG_x)$$

(beides ist $= gx \cdot x$)

Definition 0.10. Sei X eine links-G-Menge,

(a) Man sagt G operiert frei auf $X \iff \forall x \in X : G_x = \{e\}$

(b) Die Menge der Fixpunkte der G-Wirkung ist

$$X^G := \{x \in X \mid G_x = G\}$$

Beispiel. $\mathrm{GL_n}(K)$ operiert frei auf der Menge der geordneten Basen von K^n.

Korollar 0.11. *Sei X eine links-G-Menge. Sei $x_1, ..., x_n$ ein Repräsentantensystem der Bahnen der Länge ≥ 2. Dann:*

(a) $X = X^G \sqcup \bigsqcup_{i \in \{1,\ldots,n\}} G \cdot x_i$

(b) $\# X = \# X^G + \sum_{i \in \{1,\ldots,n\}} \underbrace{[G : G_{x_i}]}_{= \# G \cdot x}$

Beweis. Aus Proposition 5 folgt (a), Lemma 9 gibt (b). $\square$

Anwendung. Sei $X := G$. Sei die G-Wirkung durch Konjugation gegeben, d.h.

$$g \underbrace{\circ}_{\text{Wirk.}} h = ghg^{-1}$$

Die Bahnen unter dieser G-Wirkung heißen Konjugationsklassen. Die Konjugationsklasse zu $h \in G = X$ ist

$$G_h := \{ghg^{-1} \mid g \in G\}$$

Bahnen der Länge 1 sind Fixpunkte unter Konjugation mit allen $g \in G$

$$= \{h \in G \mid \forall g \in G : \underbrace{ghg^{-1} = h}_{gh = hg}\} =: Z(G) \text{ das Zentrum von } G$$

Stabilisator zu $h \in G$ (unter Konjugationswirkung)

$$= \{g \in G \mid ghg^{-1} = h\} = C_G(h) \text{ Zentralisator von } h$$

Aus Korollar 11 ergibt sich nun:

Satz 0.12 (Klassengleichung)**.** *Sei G endlich. Ist $g_1, ..., g_n$ ein Repräsentantensystem der Konjugationsklassen der Länge ≥ 2, so gilt:*

$$\# \underbrace{G}_{X} = \# \underbrace{Z(G)}_{X^G} + \sum_{i=1}^{n} [G : \underbrace{C_G(g_i)}_{C_g}]$$

Definition 0.13. Sei p eine Primzahl, eine Gruppe G heißt p-Gruppe $\iff$ $\# = p^m$ füe ein $m \in \mathbb{N}$

Beispiel.

$$\mathbb{Z}/_{(p^m)} \text{ oder } U_3(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{F}_p \right\}$$

Korollar 0.14. *Ist G eine p-Gruppe, so gilt $p | \# Z(G)$, (d.h. $Z(G)$ ist nicht-trivial und also eine p-Gruppe)*

Beweis. Seien $g_1, ..., g_n$ wie im Satz 12. Dann gilt: $C_G(g_i) < G$ ist eine echte Untergruppe. (sonst $g_i = Z(G)$, ist ausgeschlossen)

$$\underset{\text{Lagrange}}{\Longrightarrow} [G : C_G(g_i)] \text{ teilt } \#G = p^m$$

ist ungleich 1!

$$\Longrightarrow \; p | [G : C_G(g_i)], \forall i \in \{1, ..., n\}$$

Klassengleichung modulo p :

$$\underbrace{0}_{\#G} \cong \#Z(G) + \sum_{i=1}^{n} \underbrace{0}_{[G:C_G(g_i)]} \quad \text{mod } p \implies p | \#Z(G).$$

□

Übung 0.15 (Satz von Cauchy)**.** (?) Sei p eine Primzahl und G endlich, dann gilt:

$$p | \#G \implies \exists g \in G : \operatorname{ord}(g) = p.$$

($\implies$ $\#G$ und $\# \exp(G)$ haben dieselben Primteiler)

Idee: Verwende Induktion über $\#G$ und die Klassengleichung. In Induktionsschritt 2 Fälle:

1. $\exists H < G$ echte Untergruppe mit $p | \#H$
2. $\neg \exists H < G$ echte Untergruppe mit $p | \#H$

Im 2. Fall wende Klassengleichung mod p an!

0.2 Permutationsgruppen

Sei $n \in \mathbb{N}$, $S_n = \operatorname{Bij}(\{1, ..., n\})$, Notation für $\sigma \in S_n$, d.h. $\sigma : \{1, ..., n\} \to \{1, ..., n\}$ bijektiv ist

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Dabei gilt: $(\sigma(1), ..., \sigma(n))$ ist eine Permutation von $\{1, ..., n\}$, d.h.

$$\#\{\sigma(1), ..., \sigma(n)\} = n$$

Korollar 0.16. $\#S_n = n!$

Beweis. (Übung) Betrachte die möglichen "Wertetabellen" für Permutationen. $\square$

Definition 0.17. Für $\sigma, \tau \in S_n$ definiere

(a) $\operatorname{supp}(\sigma) =$ Träger von $\sigma, \operatorname{supp}(\sigma) := \{i \in \{1, ..., n\} \mid \sigma(i) \neq i\}$

(b) σ und τ sind disjunkt $\iff \operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$

Bemerkung. $\operatorname{supp}(\sigma) = \emptyset \iff 0 = \mathrm{id}$

Lemma 0.18 (Andere Interpretation des Trägers)**.** *Sei $\sigma \in S_n$, dann gilt für die Wirkung von $\langle\sigma\rangle$: $\operatorname{supp}(\sigma) =$ Vereinigung der Bahnen von $\langle\sigma\rangle$ auf $\{1, ..., n\}$ der Länge ≥ 2.*

Beweis.

- "$\subseteq$": Sei $i \in \operatorname{supp}(\sigma) \implies \sigma(i) \neq i \implies \{i, \sigma(i), \sigma^2(i), ..., \sigma^m(i), ...\}$ ist Bahn von $\langle\sigma\rangle = \{\sigma^j \mid j \in \mathbb{N}_0\} = \{\mathrm{id}, \sigma, ..., \sigma^{r-1}\}$ der Länge ≥ 2. für $r = \operatorname{ord}(\sigma)$.
- "$\supseteq$": Sei $i \notin \operatorname{supp}(\sigma) \implies \sigma(i) = i \implies \sigma^j(i) = i, \forall j \in \mathbb{N} \implies$ Bahn von i unter $\langle\sigma\rangle$ ist 1-elementig.

$\square$

Korollar 0.19. *Für $\sigma \in S_n$ gelten:*

(a) $i \in \operatorname{supp}(\sigma) \iff \sigma(i) \in \operatorname{supp}(\sigma)$

(b) Auf jeder $\langle\sigma\rangle$-Bahn (durch $i \in \{1, ..., n\}$) wirkt σ als "zyklische Permutation", d.h.

$$\begin{tikzcd} i_n := i \arrow[r, mapsto] & i_2 = \sigma(i) \arrow[r, mapsto] & i_3 = \sigma^2(i) \arrow[r, mapsto] & \cdots \arrow[r, mapsto] & i_r = \sigma^{r-1}(i) \arrow[llll, bend left, "\substack{\sigma \\ (\textit{mit } \#\{1\cdots n\}=r)}"] \end{tikzcd}$$

Beweis. (a)

$$i \in \operatorname{supp}(\sigma) \implies \sigma(i) \neq i \underset{\sigma \text{ anwenden}}{\implies} \sigma(\sigma(i)) \neq \sigma(i) \implies \sigma(i) \in \operatorname{supp}(\sigma)$$

Falls $\sigma(i) \in \operatorname{supp}(\sigma)$, so gilt $\sigma(\sigma(i)) \neq \sigma(i) \underset{\sigma^{-1} \text{ anwenden}}{\implies} \sigma(i) \neq i$

(b) Sei r die Länge der Bahn durch i unter $\langle\sigma\rangle$. Dann sind $i_{j+1} := \sigma^j(i), j = 0, ..., r-1$ *paarweise verschieden.* Sonst $\exists 0 \leq j_1 < j_2 \leq r-1$ mit $\sigma^{j_1}(i) = \sigma^{j_2}(i)$

$$\underset{\sigma^{-1} \text{ anwenden}}{\implies} i = \sigma^{j_2 - j_1}(i) \quad (*)$$

$\implies$ Bahn durch i hat höchstens $j_2 - j_1 < r$ Elemente, die Bahn ist wegen $(*)$

$$= \{i, \sigma(i), ..., \sigma^{j_2 - j_1}(i)\}$$

Und nun: Wiederholtes Anwenden von σ gibt den Zykel

$$\begin{tikzcd} i_1 \arrow[r, mapsto] & i_2 \arrow[r, mapsto] & \cdots \arrow[r, mapsto] & i_r \arrow[lll, bend left] \end{tikzcd}$$ $\square$

Lemma 0.20. *Sind $\sigma, \tau \in S_n$ disjunkt, so gilt $\sigma\tau = \tau\sigma$.*

Beweis. Zeige $\sigma \circ \tau = \tau \circ \sigma$ als Abbildungen $\{1, ..., n\} \to \{1, ..., n\}$, sei $i \in \{1, ..., n\}$

- Fall 1: $i \in \operatorname{supp}(\sigma) \implies \sigma(i) \in \operatorname{supp}(\sigma) \implies i, \sigma(i) \notin \operatorname{supp}(\tau)$. Also $\tau(i) = i, \tau(\sigma(i)) = \sigma(i)$
- Fall 2: $i \in \operatorname{supp}(\tau)$ analog zu Fall 1.
- Fall 3: $i \notin \operatorname{supp}(\sigma) \cup \operatorname{supp}(\tau) \implies \sigma(i) = i = \tau(i)$.

Also $\sigma(\tau(i)) = \sigma(i) = i = \tau(i) = \tau(\sigma(i))$. $\square$

(Folge: σ, τ disjunkt $\implies \operatorname{ord}(\sigma\tau) = \operatorname{kgV}(\operatorname{ord}(\sigma), \operatorname{ord}(\tau))$)

Definition 0.21. Seien $i_1, ..., i_r \in \{1, ..., n\}$ paarweise verschieden. Der r-Zykel

$$(i_1\ i_2\ \cdots\ i_r)(j) = \begin{cases} j & j \notin \{i_1, ..., i_r\} \\ i_{s+1} & j = i_s\ (s \in \{1, ..., n\}) \\ i_1 & j = i_r \end{cases}$$

2-Zykel heißen Transposition. Konvention: $(\cdot) := \mathrm{id}_{\{1,...,n\}}$ (leerer Zykel). Beachte:

(i) $(i) = (\cdot)$ für $i \in \{1, ..., n\}$

(ii) $\operatorname{supp}(i_1\ i_2\ \cdots\ i_r) = \begin{cases} \{i_1, ..., i_r\} & r \geq 2 \\ \emptyset & r = 1 \end{cases}$

(iii) $(i_1\ i_2\ \cdots\ i_r) = (i_r\ i_1\ i_2\ \cdots i_{r-1})$ (Notation ist nicht eindeutig, können Einträge zyklisch weiterschieben.) z.B.

$$(1\ 4\ 7) = (7\ 1\ 4) = (4\ 7\ 1) = \begin{tikzcd} & 1 \arrow[dr] & \\ 7 \arrow[ur] & & 4 \arrow[ll] \end{tikzcd}$$

(iv) $\operatorname{ord}(i_1\ \cdots\ i_r) = r$, z.B. $\operatorname{ord}(1\ 2) = 2$

Satz 0.22 (Zykeldarstellung)**.** *Sei $\sigma \in S_n$, seien $I_1, ..., I_t \subseteq \{1, ..., n\}$. Die verschiedenen Bahnen von $\langle\sigma\rangle$ der Länge ≥ 2, dann:*

(a) $\exists!$ Zykel σ_j der Länge $\#I_j$ mit $\operatorname{supp}(\sigma_j) = I_j$, so dass $\sigma_j|_{I_j} = \sigma|_{I_j}$

(b) $\sigma = \sigma_1 \cdot ... \cdot \sigma_t$ und die σ_i kommutieren paarweise.

(c) Die Darstellung in (b) ist bis auf Permutation der Faktoren eindeutig.

(d) Es gilt mit der Notation aus (b):

$$\operatorname{ord}(\sigma) = \operatorname{kgV}(\#I_1, ..., \#I_t)$$