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 $\mathcal{B} = \{\text{geordnete Basen von } K^n\}$ 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

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

□

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 $\mathrm{Bij}(G)$. □

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 $\underbrace{g_1, g_2 \in \mathrm{Stab}_G(x)}_{\text{bedeutet } g_1x=x, g_2x=x}$, zu zeigen ist $g_1^{-1}g_2 \in \mathrm{Stab}_G(x)$

$$\overset{g_1^{-1}\cdot}{\implies} x = ex = g_1^{-1}g_1x = g^{-1}x$$

Damit gilt $(g_1^{-1} \cdot g_2^{-1})x = g_1^{-1}(g_2x) = g_1^{-1}x = x$

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

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

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

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 $\implies \#{}^{G}\!/_{G_x} = \#G \cdot x$.

□

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

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

Beweis. Aus Proposition 5 folgt (a), Lemma 9 gibt (b). □

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 (p**-Gruppe**)**.** 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 nichttrivial 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)

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

ist ungleich 1!

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

Klassengleichung modulo p :

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

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

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

($\implies \#G$ 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 $n \in \mathbb{N}$, $S_n = \text{Bij}(\{1, ..., n\})$, 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. □

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

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

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

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

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

Beweis.

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

□

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

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

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

$$i_n := i \longmapsto i_2 = \sigma(i) \longmapsto i_3 = \sigma^2(i) \longmapsto \cdots \longmapsto i_r = \sigma^{r-1}(i)$$

$$\overset{\sigma}{\underset{(mit\ \#\{1\cdots n\}=r)}{\curvearrowright}}$$

Beweis. (a)

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

Falls $\sigma(i) \in \text{supp}(\sigma)$, 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 $\sigma^{j_1}(i) = \sigma^{j_2}(i)$

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

$\Longrightarrow$ 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

$$i_1 \longmapsto i_2 \longmapsto \cdots \longmapsto i_r$$

$\square$

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

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

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

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

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

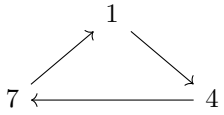
2-Zykel heißen **Transposition**. Konvention: $(\cdot) := \text{id}_{\{1,...,n\}}$ (leerer Zykel). Beachte:

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

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

(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.

$$(1\ 4\ 7) = (7\ 1\ 4) = (4\ 7\ 1) =$$



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

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

(a) Für $j \in \{1, ..., t\}$ $\exists!$ Zykel $\sigma_j \in S_n$ mit $\operatorname{supp}(\sigma_j) = I_j$, und $\sigma_j|_{I_j} = \sigma|_{I_j}$

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

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

(d) Für σ gilt: $\operatorname{ord}(\sigma) = \operatorname{kgV}(\#I_j \mid j \in \{1, ..., t\})$

Beweis. (a) Sei r_j die Länge von I_j. Sei $i_j \in I_j$, dann ist (vgl. Beweis von Korollar 19)

$$\sigma_j := (i_j, \sigma(i_j), \sigma^2(i_j), ..., \sigma^{r_j - 1}(i_j)) \in S_n$$

ein r_j-Zykel und $\sigma|_{I_j} = \sigma_j$

(b) Die (σ_j) kommutieren paarweise, denn deren Träger, die Mengen I_j, sind paarweise disjunkt.

Um $\sigma = \sigma_1 \cdot ... \cdot \sigma_t$ zu prüfen, wende beide Abbildungen an auf $i \in \{1, ..., n\}$.

- Fall $j \in \{1, ..., t\} : i \in J$
  $(*)$ Es gilt $\sigma_{j'}(i) = i$ für $j' \neq j$ (da $I_{j'} \cap I_j = \emptyset$)

$$\implies \sigma(i) = \sigma_j(i) \overset{(*)}{=} \left(\sigma_j \cdot \textstyle\prod_{j' \neq j} \sigma_{j'}\right)(i)$$

$$\overset{\sigma_j \text{ kommutieren}}{=} (\sigma_1 \cdot ... \cdot \sigma_j \cdot ... \cdot \sigma_t)(i)$$

- Fall $0 : i \in \{1, ..., n\} \setminus \bigcup_{j \in \{1, ..., t\}} I_j$. Dann: $\sigma(i) = i$ (1-elementige Bahn).
  Da $i \notin I_j : \sigma_j(i) = i, \forall j \in \{1, \ldots, t\}$. also $(\sigma_1 \cdot \ldots \cdot \sigma_t)(i) = i = \sigma(i)$

(c) Es gelte $\sigma = \sigma'_1 \cdot \ldots \sigma'_{t'}$ mit paarweise disjunkten Zykeln $\sigma = \sigma'_1 \cdot \ldots \sigma'_{t'}$ der Länge ≥ 2. Sei $I'_{j'} := \operatorname{supp}(\sigma'_{j'})$ für $j' \in \{1, \ldots, t'\}$. Dann:

$$\sigma|_{I'_{j'}} = \sigma'_{j'}|_{I'_{j'}}$$

$\implies I'_{j'}$ ist Bahn von $\langle\sigma\rangle$ der Länge ≥ 2. $\implies t' = t$ und nach Umindizieren der $I'_{j'}$ gelte

$$I'_j = I_j \text{ für } j \in \{1, \ldots, t\}$$

und $\sigma_j|_{I_j} = \sigma|_{I_j} = \sigma'_j|_{I_j} \overset{\sigma_j, \sigma'_j \text{ sind } r_j = \#I_j\text{-Zykel}}{\Longrightarrow} \sigma_j = \sigma' j$

(d) (Übung). □

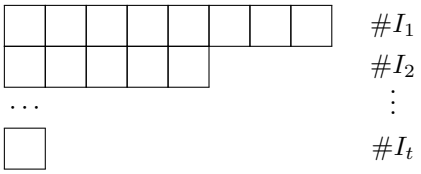
Beispiel 0.23.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 8 & 4 & 1 & 6 & 3 & 7 \end{pmatrix} \in S_8$$

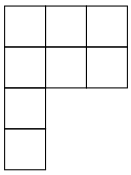
$\implies \langle\sigma\rangle$-Bahnen: $\{1, 2, 5\}, \{3, 8, 7\}, \{4\}, \{6\}$ und $\sigma = (1\ 2\ 5)(3\ 8\ 7)$

Definition 0.24 (**Young-Diagramm/Partition**). Sei $\sigma \in S_n$, seien $I_1, ..., I_t$ die Bahnen von $\langle\sigma\rangle$ (auch Bahnen der Länge 1), und gelte o.E. $\#I_1 \geq \#I_2 \geq \cdots \geq \#I_t$.

(a) Das Young-Diagramm zu σ ist das Diagramm der Form:



im obigen Beispiel 23



(b) Eine Partition von n ist ein Tupel $(n_1, ..., n_t)$ aus $\mathbb{N}$ mit $n_1 \geq \cdots \geq n_t$ unt $n = n_1, + \cdots + n_t$. (Young-Diagramm: Möglichkeit eine Partition zu veranschaulichen z.B. ist $(\#I_1, ..., \#I_t)$ eine Partition von n)

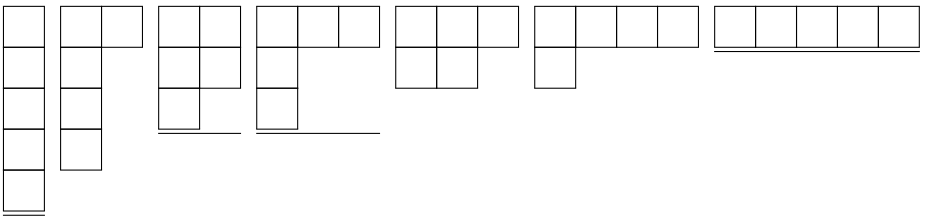
Satz 0.25 (Übung)**.**

(a) Seien $i_1, ..., i_r$ aus $\{1, \ldots, n\}$ paarweise verschiedene Elemente. Dann gilt $\forall\sigma \in S_n$:

$$\sigma \circ (i_1\ i_2 \cdots\ i_r) \circ \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2) \cdots\ \sigma(i_r))$$

(b) σ_1 und σ_2 aus S_n liegen in dieselben Konjugationsklasse $\iff$ sie haben dasselbe Young-Diagramm.

Beispiel. S_5 hat 7 Youngdiagramme



also auch 7 Konjugationsklassen.

Definition (**Signum-Funktion/Alternierende Gruppe**). Sei sgn : $S_n \to \{\pm 1\}$ die Signum-Funktion aus der linearen Algebra. sgn ist eindeutig bestimmt durch:

(i) sgn ist ein Gruppenhomomorphismus.

(ii) $\text{sgn}(\tau) = -1$, für τ eine Transposition.

(jedes $\sigma \in S_n$ lässt sich schreiben als Produkt von Transpositionen) A_n = Kern(sgn) = die alternierende Gruppe auf n Elementen

$$A_n = \{\tau_1 \cdot ... \cdot \tau_{2m} \mid \tau_i \in S_n, \text{sgn}(\tau) = -1, m \in \mathbb{N}\}$$

Proposition 0.26 (Formeln für sgn)**.** *(Übung)*

(a) Jeder r-Zykel σ ist ein Produkt von $r-1$ Transpositionen, und also gilt $\operatorname{sgn}(\sigma) = (-1)^{r-1}$

(b) Hat σ die Zykeldarstellung $\sigma = \sigma_1 \cdot ... \cdot \sigma_t$ mit Zykellängen r_i (von σ_i), $i \in \{1, \dots, t\}$, so gilt $\operatorname{sgn}(\sigma) = (-1)^{r_1 + \dots + r_t - t}$

Bemerkung. Man kann sgn durch (b) bestimmen und kann dann nachprüfen: σ ist ein Gruppenhomomorphismus.

Lemma 0.27. *Sei $C_3 = \{\sigma \in A_n \mid \sigma$ ist 3-Zykel$\}$ und sei $C_{2,2} = \{\sigma \in A_n \mid \sigma = \tau_1 \cdot \tau_2$ mit τ_1, τ_2 disjunkt.$\}$, dann*

(a) Für $n \geq 3$ gilt $A_n = \langle C_3 \rangle =: H_3$

(b) Für $n \geq 5$ gilt $A_n = \langle C_{2,2} \rangle =: H_{2,2}$

(c) Für $n \geq 5$ sind C_3 und $C_{2,2}$ A_n-Konjugationsklassen.

Beweis.

$$A_n = \{\underbrace{\tau_1 \cdot ... \cdot \tau_{2m}}_{\text{gerade Anzahl}} \mid \tau_i \in S_n \text{ Transpositionen.}\}$$

(a) Zeige: $\tau, \tau' \in H_3$ für τ, τ' beliebige Transpositionen in S_n

(i) $\tau = \tau'$:
$\tau \cdot \tau' = \mathrm{id} = \sigma^3$ für jeden 3-Zykel $\sigma \in H_3$

(ii) $\tau \neq \tau'$ und τ, τ' nicht disjunkt:
also $\tau = (a\ b)$, $\tau' = (b\ c)$ mit $\#\{a, b, c\} = 3, a, b, c \in \{1, \dots, n\}$.

$$\tau\tau' = (a\ b\ c) = (a\ b)(b\ c) \quad \begin{smallmatrix} a \leftarrow b \leftarrow c \\ c \leftarrow c \leftarrow b \\ b \leftarrow a \leftarrow a \end{smallmatrix}$$

(iii) $\tau \neq \tau'$ und τ, τ' disjunkt also $\tau = (a\ b), \tau' = (c\ d), \#\{a, b, c, d\} = 4, \{a, b, c, d\} \subseteq \{1, \dots, n\}$.

$$(a\ c\ b)(a\ c\ d) \overset{(\text{Übung})}{=} (a\ b)(c\ d)$$

(b) Zeige $\tau \cdot \tau \in H_{2,2}$ für $\tau, \tau' \in S_n$ Transpositionen.

- Fall (iii) trivial.
- Fall (i) trivial
$$(\tau_1 \cdot \tau_2)(\tau_1 \cdot \tau_2) \in \langle C_{2,2} \rangle = H_{2,2}$$
- Fall (ii) $\tau = (a\ b), \tau' = (b\ c)$ (wie oben). Wegen $n \geq 5$, finde $d \neq e \in \{1, \dots, n\} \setminus \{a, b, c\}$. Dann
$$\tau \cdot \tau' = ((a\ b)(d\ e))((b\ c)(d\ e))$$

(c) C_3 ist A_n-Konjugationsklasse.

Zu zeigen $(a\ b\ c)$ ($\{a,b,c\} \in \{1,\dots,n\}$ 3 elementig) ist konjugiert zu $(1\ 2\ 3)$.

Wahle $\sigma \in S_n$ mit $\sigma(1) = a, \sigma(2) = b, \sigma(3) = c$.

$$\overset{\text{Satz } 25}{\Longrightarrow} \sigma(1\ 2\ 3)\sigma^{-1} \overset{(*)}{(} \underbrace{a}_{\sigma(1)}\ \underbrace{b}_{\sigma(2)}\ \underbrace{c}_{\sigma(3)})$$

Aber $\operatorname{sgn}(\sigma)$ ist unklar $+1, -1$?

Beachte: $(*)$ gilt auch für $\sigma(4\ 5)$ und: entweder gilt $\operatorname{sgn}(\sigma) = 1$ oder $\operatorname{sgn}(\sigma(4\ 5)) = 1 \implies (1\ 2\ 3) \in A_n$ konjugiert zu $(a\ b\ c)$

Für $C_{2,2}$: zu zeigen $(a\ b)(c\ d)$ A_n-konjugiert zu $(1\ 2)(3\ 4)$ für $\{a,b,c,d\} \subseteq \{1,\dots,n\}$ 4-elementig.

Wähle $\sigma \in S_n$ mit $\sigma(1) = a, \sigma(2) = b, \sigma(3) = c, \sigma(4) = d$

$$\implies \sigma(1\ 2)(3\ 4)\sigma^{-1} \overset{(**)}{=} (a\ b)(c\ d)$$

und $(*)$ gilt auch für $\sigma(1\ 2)$ ... etc. (Schließe wie für C_3.)

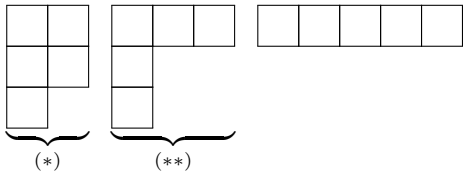
□

Definition 0.28 (**Einfache Gruppe**)**.** Eine Gruppe G heißt **einfach** $\iff \{e\}$ und G sind die einzigen Normalteiler von G. (d.h. G hat keine nicht-trivialen Normalteiler)

Satz 0.29. *Für $n \geq 5$ ist A_n einfach.*

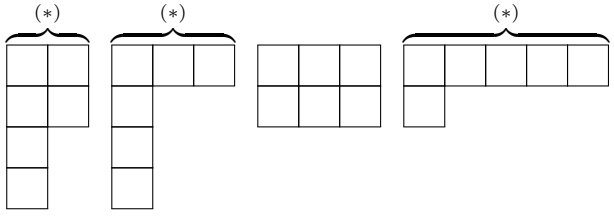
Beweis. Sei $N \trianglelefteq A_n$ ein Normalteiler und $\{e\} \subsetneq N$ und sei $\sigma \in N \setminus \{e\}$.

- $n = 5$:



  $(*)$ Doppeltranspositionen bilden A_5-Konjugationsklasse und erzeugen A_5 (Lemma 27). Falls Doppeltranspositionen in N, so folgt $N = A_5$.
  $(**)$ 3-Zykel bilden A_5-Konjugationsklasse und erzeugen A_5 (Lemma 27). Falls σ ein $3-Zykel \implies N = A_5$.
  Gelte $\sigma = 5\text{-Zykel} = (a\ b\ c\ d\ e)$. Nun: $N \ni \underbrace{(a\ b\ c)\sigma(a\ b\ c)^{-1}}_{\in N}\underbrace{\sigma}_{\in N} \overset{\text{Übung}}{=}$
  $(a\ b\ d)$ 3-Zykel

- $n = 6$: möglichen Youngdiagramme: (zu $\sigma \in A_6 \setminus \{e\}$)



$(*)$ wurden schon im A_5-Fall erklärt.

Sei also $\sigma^2 = (a\,b\,c)(d\,e\,f) \in N$, mit $\{a, \dots f\} = \{1, \dots, 6\}$. Sei $\tau = (a\,b\,c)$, berechne $\tau(\sigma)(\tau^{-1})$ (Satz 25)

$$\underbrace{\underbrace{\tau\sigma\tau^{-1}}_{\in N}\underbrace{\sigma}_{\in N}}_{\in N} = \underset{f \longleftarrow f \longleftarrow \quad e \longleftarrow e \longleftarrow f}{(b\ d\ c)(a\ e\ f)(a\ c\ b)(e\ d\ f)} \overset{\text{Übung}}{=} (a\ b\ e\ c\ d) \in 5 - \text{Zykel}$$

wurde schon bei $n = 5$ geklärt.

- $n \geq 6$: o.E. (Permutation von $1, ..., n$) $\sigma(1) \neq 1$ Wähle $\{j, k\} \in \{1, \dots, n\} \setminus \{1, \sigma(1)\}$. Sei $\tau := (\sigma(1)\ j\ k) \implies \sigma^{-1}\tau\sigma\tau^{-1} \in N$ Dann:
  (i) $\varphi := \tau\sigma\tau^{-1}\sigma^{-1} \in N$
  (ii) $\varphi(\sigma(n)) = \tau\sigma\tau^{-1}(1) \underset{1 \notin \text{supp}(\tau^{-1})}{\overset{1 \notin \text{supp}(\tau)}{=}} \tau\sigma(1) = j \neq \sigma(1)$, also $\varphi \neq \text{id}$.
  (iii) $\#\,\text{supp}(\varphi) \leq 6$, denn:

$$\varphi = \underbrace{\tau}_{\text{3-Zykel}} \cdot \sigma \underbrace{\underbrace{\tau^{-1}}_{\text{3-Zykel}}\ \sigma^{-1}}_{\text{3-Zykel}}$$

  o.E: $\text{supp}(\varphi) \subseteq \{1, \dots, 6\} \implies \varphi \in A_6 \setminus \{e\}$
- Fälle $n \leq 6$: Nurmalteiler, der von φ erzeugt wird enthält 3-Zykel oder Doppeltransposition. Dann fertig wegen Lemma 27. □

Bemerkung. Es gibt eine Klassifikation aller endlich einfachen Gruppen: Liste:

- $\mathbb{Z}/(p), p$ prim
- $A_n, n \geq 5$
- endliche Gruppen vom Lie typ:
  (i) $\text{SL}_\text{n}(K)/Z(\text{SL}_\text{n}(K))$ bis auf einige kleine $\#K$ sind einfach (endlich falls K endlich).
  (ii) Weitere Untergruppen von SL_n, welche zu "linearen algebraischen Gruppen" korrespondieren.
- 26 weitere.

0.3 Sylow Theoreme

Satz 0.30 (Sylow I; nach Wieland)**.** *Sie G eine endliche Gruppe, p eine Primzahl, $k \in \mathbb{N}$ sodass $p^k | \#G$, sei*

$$n_k := \#\{H \leq G \mid \#H = p^k\}$$

Dann ist

$$n_k \equiv 1 \mod p$$

insbesondere $\exists H \leq G$ mit $\#H = p^k$

Übung (Vorbereitung)**.** Sei p eine Primzahl, $k \in \mathbb{N}_0, m \in \mathbb{N}$, dann:

$$\binom{mp^k}{p^k} = m \cdot u$$

wobei $\mathbb{N} \ni u \equiv 1 \mod p$.