

## 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

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

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  $\lambda$  auch Gruppenwirkung und  $X$  heißt Links- $M$ -Menge.

**Bemerkung.** Analog kann man auch Rechtswirkungen

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

definieren. (Axiome:  $x \cdot e = x$  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  $\lambda : G \times X \rightarrow X$  definiere  $\rho : X \times G \rightarrow X$  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  $\lambda : G \times X \rightarrow X$  eine Linkswirkung, dann ist

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

ein wohl-definierter Gruppenhomomorphismus.

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

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

eine Linkswirkung von  $G$  auf  $X$ .

*Beweis.* (a) Für  $g \in G$  sei  $\varphi_g : X \rightarrow X, x \mapsto gx$ , dann gelten:  $\varphi_e : X \rightarrow X, x \mapsto ex = x$  ist  $\text{id}_X$  (Axiom (i)), und

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

denn  $\forall x \in X$ :

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

Damit folgen:

1.  $\varphi_g \circ \varphi_{g^{-1}} = \underbrace{\varphi_e}_{\text{id}_X} = \varphi_{g^{-1}} \circ \varphi_g \implies \varphi_g$  ist eine bijektive Abbildung mit Inverse  $\varphi_{g^{-1}}$ , d.h.

$$\varphi : G \rightarrow \text{Bij}(X), g \mapsto \varphi_g$$

ist wohl-definiert.

2.  $\varphi$  ist ein Gruppenhomomorphismus: folgt aus (\*) (Verknüpfung in  $\text{Bij}(X)$  ist die Verkettung von Abbildungen.)

(b) Übung.

□

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

- (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  $G \rightarrow \text{Aut}(N)$  (vgl. Lemma 1.56)

**Definition 0.3** (Eigenschaften von Wirkungen). Sei  $\lambda : G \times X \rightarrow X$  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)  $\lambda$  ist transitiv  $\iff \forall y, z \in X \exists g \in G : gy = z \stackrel{\text{Übung}}{\iff} \forall y \in X : Gy = X \stackrel{\text{Übung}}{\iff} \exists x \in X : Gx = X$
- (c)  $\lambda$  ist  $n$ -fach transitiv ( $n \in \mathbb{N}$ ), wenn für alle Paare von  $n$ -Tupeln  $(x_1, \dots, x_n), (y_1, \dots, y_n) \in X^n$  mit  $\#\{x_1, \dots, x_n\} = \#\{y_1, \dots, y_n\}$  gilt  $\exists g \in G : gx_i = y_i, \forall i$ .
- (d) Die Wirkung heißt **treu**, wenn der induzierte Gruppenhomomorphismus  $\varphi : G \rightarrow \text{Bij}(X)$  (aus Proposition 2) injektiv ist

$$\stackrel{\text{Übung}}{\iff} \forall g \in G \setminus \{e\} : \exists x \in X : \underbrace{gx \neq x}_{\varphi_g(x) \neq \text{id}_X(x)}$$

**Beispiel 0.4.**

- Ist  $V$  ein  $K$ -Vektorraum, so wirkt das Monoid  $(K, 1, \cdot)$  auf  $V$  durch Skalarmultiplikation  $(\lambda, v) \mapsto \lambda v$
- Die folgenden 3 Beispiele sind Linkswirkungen von  $\text{GL}_n(K)$ :
  - $\text{GL}_n(K) \times K^n \rightarrow K^n, (g, v) \mapsto gv$ . (Übung: Es gibt die Bahnen  $\{0\}, K^n \setminus \{0\}$ )
  - Sei  $\mathcal{B} = \{\text{geordnete Basen von } K^n\}$  und

$$\text{GL}_n(K) \times \mathcal{B} \rightarrow \mathcal{B}, (g, (b_1, \dots, b_n)) \mapsto (gb_1, \dots, gb_n)$$

die Wirkung ist treu und transitiv.

- (iii)  $\text{GL}_n(K) \times \text{End}_K(K^n) \rightarrow \text{End}_K(K^n), (A, B) \mapsto ABA^{-1}$  die Wirkung ist nicht treu  $Z(\text{GL}_n(K))$  wirkt trivial. (Übung: Bahnen stehen in Bijektion zu den Frobeniusnormalformen von Matrizen.)
3.  $S_n \times \{1, \dots, n\} \rightarrow \{1, \dots, n\}, (\sigma, i) \mapsto \sigma(i)$  Wirkung ist treu und  $n$ -fach transitiv.
4. Abstrakte Beispiele: Sei  $H \leq G$  eine Untergruppe.
- (i)  $\lambda : H \times G \rightarrow G, (h, g) \mapsto hg$ . Die Bahnen sind die Mengen  $Hg$ , also die Rechtsnebenklassen zu  $H$  (treu?) Menge der Rechtsnebenklassen

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

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

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

- (iii)  $c : G \times G \rightarrow G, (g, g') \mapsto gg'g^{-1}$  ist eine Linkswirkung, denn der nach Proposition 2 zugehörige Gruppenhomomorphismus ist  $c : G \rightarrow \text{Aut}(G), g \mapsto c_g$ .
- (iv)  $G \times G/H \rightarrow G/H, (g, g'H) \mapsto gg'H$  Die Klassen  $gH$  heißen Linksnebenklassen wegen der Links- $G$ -Wirkung auf ihnen.

**Proposition 0.5.** Sei  $X$  eine Links- $G$ -Menge (zu der Wirkung  $\lambda : G \times X \rightarrow X, (g, x) \mapsto gx$ ) 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  $\#X = \sum_{i \in I} \#Gx_i$ )

*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  $(\text{Bij}(G), \text{id}_G, \circ)$  (bzw.  $(\text{Abb}(G, G), \text{id}_G, \circ)$ ).

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

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

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

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

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

**Übung.**  $G$ -Wirkung auf einer Menge  $X$  ist treu

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

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

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

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

*Beweis.*

(a)  $e \in \text{Stab}_G(x)$ , denn  $ex = x$ . Seien  $\underbrace{g_1, g_2 \in \text{Stab}_G(x)}_{\text{bedeutet } g_1x=x, g_2x=x}$ , zu zeigen ist  $g_1^{-1}g_2 \in \text{Stab}_G(x)$

$$\text{Stab}_G(x)$$

$$\xrightarrow{g_1^{-1}} x = ex = g_1^{-1}g_1x = g^{-1}x$$

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

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

$$\begin{aligned} h \in \text{Stab}_G(gx) &\iff hgx = gx \xrightarrow{g^{-1}} g^{-1}hgx = x \\ &\iff g^{-1}hg \in \text{Stab}_G(x) \xleftrightarrow[\text{Konj. mit } g]{} h \in g \text{Stab}_G(x) g^{-1}. \end{aligned} \quad \square$$

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

- $\psi : G/G_x \rightarrow Gx, hG_x \mapsto hx$  ist wohl-definiert und eine Bijektion.
- Ist  $G$  endlich, so folgt  $\#G \cdot x = [G : G_x]$ .

*Beweis.*

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

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

- $\psi$  surjektiv nach Definition von  $G \cdot x$ .
- Aussage über Mächtigkeiten:  $\psi$  bijektiv  $\implies \#G/G_x = \#G \cdot x$ . □

**Bemerkung.** Die Abbildung  $\psi$  ist ein Homomorphismus von links- $G$ -Mengen (ein Isomorphismus!),  $G/G_x$  und  $G \times x \subseteq X$  sind links- $G$ -Mengen und  $\psi$  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,

- Man sagt  $G$  operiert **frei** auf  $X \iff \forall x \in X : G_x = \{e\}$
- Die Menge der **Fixpunkte** der  $G$ -Wirkung ist

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

**Beispiel.**  $\text{GL}_n(K)$  operiert frei auf der Menge der geordneten Basen von  $K^n$ .

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

- $X = X^G \sqcup \bigsqcup_{i \in \{1, \dots, n\}} G \cdot x_i$
- $\#X = \#X^G + \sum_{i \in \{1, \dots, n\}} \underbrace{[G : G_{x_i}]}_{=\#G \cdot x}$

*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  $g \in G$

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

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  $g_1, \dots, g_n$  ein Repräsentantensystem der Konjugationsklassen der Länge  $\geq 2$ , 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  $\iff \# = p^m$  für ein  $m \in \mathbb{N}$

**Beispiel.**

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

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

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

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

ist ungleich 1!

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

Klassengleichung modulo  $p$ :

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

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

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

( $\implies \#G$  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  $p \mid \#H$
2.  $\neg \exists H < G$  echte Untergruppe mit  $p \mid \#H$

Im 2. Fall wende Klassengleichung mod  $p$  an!

## 0.2 Permutationsgruppen

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

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

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

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

**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)  $\text{supp}(\sigma) = \text{Träger von } \sigma, \text{supp}(\sigma) := \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}$
- (b)  $\sigma$  und  $\tau$  sind **disjunkt**  $\iff \text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$

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

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

*Beweis.*

- “ $\subseteq$ ”: Sei  $i \in \text{supp}(\sigma) \implies \sigma(i) \neq i \implies \{i, \sigma(i), \sigma^2(i), \dots, \sigma^m(i), \dots\}$  ist Bahn von  $\langle \sigma \rangle = \{\sigma^j \mid j \in \mathbb{N}_0\} = \{\text{id}, \sigma, \dots, \sigma^{r-1}\}$  der Länge  $\geq 2$ . 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  $i \in \{1, \dots, n\}$ ) wirkt  $\sigma$  als “zyklische Permutation”, d.h.

$$\begin{array}{ccccccc} i_n := i & \longrightarrow & i_2 = \sigma(i) & \longrightarrow & i_3 = \sigma^2(i) & \longrightarrow & \cdots \longrightarrow i_r = \sigma^{r-1}(i) \\ & & \searrow & & \swarrow & & \\ & & \sigma & & & & \\ & & (\text{mit } \#\{1 \cdots n\} = r) & & & & \end{array}$$

*Beweis.* (a)

$$i \in \text{supp}(\sigma) \implies \sigma(i) \neq i \xRightarrow[\sigma \text{ anwenden}]{} \sigma(\sigma(i)) \neq \sigma(i) \implies \sigma(i) \in \text{supp}(\sigma)$$

$$\text{Falls } \sigma(i) \in \text{supp}(\sigma), \text{ so gilt } \sigma(\sigma(i)) \neq \sigma(i) \xRightarrow[\sigma^{-1} \text{ anwenden}]{} \sigma(i) \neq i$$

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

$$\xRightarrow[\sigma^{-1} \text{ anwenden}]{\quad} i = \sigma^{j_2-j_1}(i) \quad (*)$$

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

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

Und nun: Wiederholtes Anwenden von  $\sigma$  gibt den Zykel

$$i_1 \xrightarrow{\quad} i_2 \xrightarrow{\quad} \dots \xrightarrow{\quad} i_r \xrightarrow{\quad} i_1 \quad \square$$

**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  $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ , sei  $i \in \{1, \dots, n\}$

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

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

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

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

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

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

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

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

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

$$(1 \ 4 \ 7) = (7 \ 1 \ 4) = (4 \ 7 \ 1) = \begin{array}{ccc} & 1 & \\ \nearrow & & \searrow \\ 7 & \xleftarrow{\quad} & 4 \end{array}$$

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



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

- (a) Für  $j \in \{1, \dots, t\} \exists!$  Zykel  $\sigma_j \in S_n$  mit  $\text{supp}(\sigma_j) = I_j$ , und  $\sigma_j|_{I_j} = \sigma|_{I_j}$
- (b)  $\sigma = \sigma_1 \cdot \dots \cdot \sigma_t$  und die  $\sigma_i$  kommutieren paarweise.
- (c) Die Darstellung in (b) ist eindeutig bis auf Permutation der Faktoren.
- (d) Für  $\sigma$  gilt:  $\text{ord}(\sigma) = \text{kgV}(\#I_j \mid j \in \{1, \dots, t\})$

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

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

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

- (b) Die  $(\sigma_j)$  kommutieren paarweise, denn deren Träger, die Mengen  $I_j$ , sind paarweise disjunkt.

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

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

$$\implies \sigma(i) = \sigma_j(i) \stackrel{(*)}{=} (\sigma_j \cdot \prod_{j' \neq j} \sigma_{j'})(i)$$

$$\stackrel{\sigma_j \text{ kommutieren}}{=} (\sigma_1 \cdot \dots \cdot \sigma_j \cdot \dots \cdot \sigma_t)(i)$$

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

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

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

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

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

$$\text{und } \sigma_j|_{I_j} = \sigma|_{I_j} = \sigma'_j|_{I_j} \xrightarrow[r_j = \#I_j\text{-Zykel}]{\sigma_j, \sigma'_j \text{ sind}} \sigma_j = \sigma'_j$$

- (d) (Übung). □

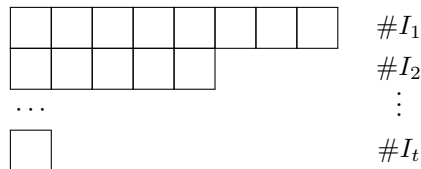
**Beispiel 0.23.**

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

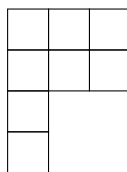
$$\implies \langle \sigma \rangle\text{-Bahnen: } \{1, 2, 5\}, \{3, 8, 7\}, \{4\}, \{6\} \text{ und } \sigma = (1 \ 2 \ 5)(3 \ 8 \ 7)$$

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

(a) Das Young-Diagramm zu  $\sigma$  ist das Diagramm der Form:



im obigen Beispiel 23



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

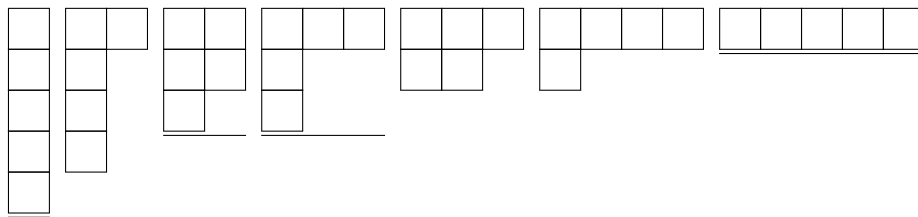
**Satz 0.25** (Übung).

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

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

(b)  $\sigma_1$  und  $\sigma_2$  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  $\text{sgn} : S_n \rightarrow \{\pm 1\}$  die Signum-Funktion aus der linearen Algebra.  $\text{sgn}$  ist eindeutig bestimmt durch:

(i)  $\text{sgn}$  ist ein Gruppenhomomorphismus.

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

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

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

**Proposition 0.26** (Formeln für  $\text{sgn}$ ). (Übung)

- (a) Jeder  $r$ -Zykel  $\sigma$  ist ein Produkt von  $r - 1$  Transpositionen, und also gilt  $\text{sgn}(\sigma) = (-1)^{r-1}$
- (b) Hat  $\sigma$  die Zykeldarstellung  $\sigma = \sigma_1 \cdot \dots \cdot \sigma_t$  mit Zykellängen  $r_i$  (von  $\sigma_i$ ),  $i \in \{1, \dots, t\}$ , so gilt  $\text{sgn}(\sigma) = (-1)^{r_1 + \dots + r_t - t}$

**Bemerkung.** Man kann  $\text{sgn}$  durch (b) bestimmen und kann dann nachprüfen:  $\sigma$  ist ein Gruppenhomomorphismus.

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

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

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

- (i)  $\tau = \tau'$ :  
 $\tau \cdot \tau' = \text{id} = \sigma^3$  für jeden 3-Zykel  $\sigma \in H_3$
- (ii)  $\tau \neq \tau'$  und  $\tau, \tau'$  nicht disjunkt:  
 also  $\tau = (a \ b), \tau' = (b \ c)$  mit  $\#\{a, b, c\} = 3, a, b, c \in \{1, \dots, n\}$ .

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

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

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

- (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  $(1\ 2\ 3)$ .

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

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

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

Beachte:  $(*)$  gilt auch für  $\sigma(4\ 5)$  und: entweder gilt  $\text{sgn}(\sigma) = 1$  oder  $\text{sgn}(\sigma(4\ 5)) = 1 \implies (1\ 2\ 3) \in A_n$  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  $\sigma(1\ 2) \dots$  etc. (Schließe wie für  $C_3$ .)

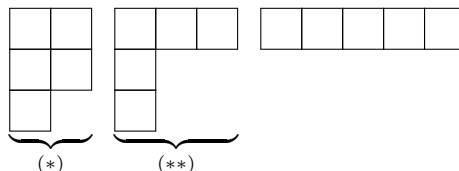
□

**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  $\sigma \in N \setminus \{e\}$ .

- $n = 5$ :

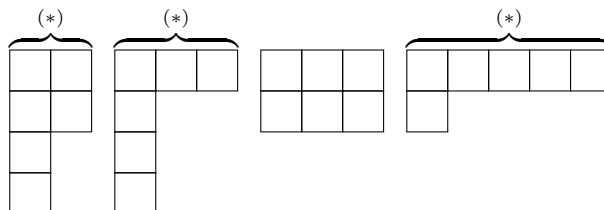


$(*)$  Doppeltranspositionen bilden  $A_5$ -Konjugationsklasse und erzeugen  $A_5$  (Lemma 27). Falls Doppeltranspositionen in  $N$ , so folgt  $N = A_5$ .

$(**)$  3-Zykel bilden  $A_5$ -Konjugationsklasse und erzeugen  $A_5$  (Lemma 27). Falls  $\sigma$  ein 3-Zykel  $\implies N = A_5$ .

Gelte  $\sigma = 5\text{-Zykel} = (a\ b\ c\ d\ e)$ . Nun:  $N \ni \underbrace{(a\ b\ c)\sigma(a\ b\ c)^{-1}}_{\in N} \underbrace{\sigma}_{\in N} \stackrel{\text{Übung}}{=} (a\ b\ d)$  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)

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

$f \leftarrow f \leftarrow e \leftarrow e \leftarrow f$

wurde schon bei  $n = 5$  geklärt.

- $n \geq 6$  : o.E. (Permutation von  $1, \dots, n$ )  $\sigma(1) \neq 1$  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)  $\varphi(\sigma(n)) = \tau\sigma\tau^{-1}(1) \stackrel{1 \notin \text{supp}(\tau)}{=} \tau\sigma(1) = j \neq \sigma(1)$ , also  $\varphi \neq \text{id}$ .  
 $1 \notin \text{supp}(\tau^{-1})$

(iii)  $\#\text{supp}(\varphi) \leq 6$ , denn:

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

o.E:  $\text{supp}(\varphi) \subseteq \{1, \dots, 6\} \implies \varphi \in A_6 \setminus \{e\}$

- Fälle  $n \leq 6$ : Normalteiler, der von  $\varphi$  erzeugt wird enthält 3-Zykel oder Doppeltransposition. Dann fertig wegen Lemma 27.  $\square$

**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)  $\text{SL}_n(K)/Z(\text{SL}_n(K))$  bis auf einige kleine  $\#K$  sind einfach (endlich falls  $K$  endlich).
  - (ii) Weitere Untergruppen von  $\text{SL}_n$ , welche zu "linearen algebraischen Gruppen" korrespondieren.
- 26 weitere.

## 0.3 Sylow Theoreme

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

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

Dann gilt:

$$n_k \equiv 1 \pmod{p}$$

Insbesondere ist  $n_k \neq 0$ , d.h.  $\exists H \leq G$  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  $\mathbb{N} \ni u \equiv 1 \pmod{p}$ .

*Beweis.* (zu 30) Durch Analyse der Wirkung von  $G$  auf  $X := \{S \subseteq G \mid \#S = p^k\}$  gegeben durch

$$\lambda : G \times X \rightarrow X, (g, S) \mapsto g \cdot S = \{g \cdot s \mid s \in S\}$$

(beachte:  $\ell_g : h \mapsto g \cdot h$  ist bijektiv  $\implies \#gS = \#S = p^k$  d.h.  $g \cdot S \in X$ ) Setze  $m := \#G/p^k$ , für  $S \in X$  definiere

$$G_S := \text{Stab}_G(S) = \{g \in G \mid gS = S\}$$

1.  $\forall S \in X : \#G_S \mid p^k$ :

Beachte:  $G_S$  wirkt auf  $S$  (da  $gS = S \forall g \in G_S$ ) durch Linkstranslation:

$$G_S \times S \rightarrow S, (g, s) \mapsto g \cdot s$$

Schreibe  $S$  als disjunkte Vereinigung seiner  $G_S$ -Bahnen.

$$S = \bigsqcup_{i \in \{1, \dots, \ell\}} G_S h_i$$

wobei  $h_1, \dots, h_\ell$  ein Repräsentantensystem der Bahnen ist.

Beachte:  $r_{h_i} : g \mapsto gh_i$  ist bijektiv. Also folgt  $\#G_S h_i = \#G_S$

$$\implies p^k = \#S = \sum_{i=1}^{\ell} \#G_S h_i = \sum_{i=1}^{\ell} \#G_S = \ell \#G_S$$

d.h.  $\#G_S \mid p^k$ .

2. Sei  $X_0 := \{S \in X \mid \#G_S = p^k\}$  und  $X_1 := X \setminus X_0$

Behauptung:  $\#X_0 = m \cdot n_k$

(a) Sei  $H \leq G$  eine Untergruppe mit  $\#H = p^k$ , dann:

$$\{S \in X_0 \mid G_S = H\} = \{Hg \mid g \in G\}$$

Denn:

- “ $\subseteq$ ”: Gelte  $G_S = H$ , d.h.  $H \cdot S = S \implies H \cdot s \subseteq S, \forall s \in S$ .  
Aber:  $\#H \cdot s \underset{r_s \text{ ist bij.}}{=} \#H = p^k = \#S \implies H \cdot s = S \implies s$  (ist das gesuchte  $g$ )
- “ $\supseteq$ ”: Zu zeigen:  $\text{Stab}_G(H \cdot s) = H$ . Sei  $g \in G$ .

$$g \in \text{Stab}_G(Hs) \iff gHs = Hs \underset{r_s \text{ ist bij.}}{\iff} gH = H \underset{H \leq G}{\iff} g \in H$$

(b)

$$\begin{aligned}
X_0 &= \bigsqcup_{H \leq G, \#H=p^k} \{S \in X \mid G_S = H\} \stackrel{(a)}{=} \bigsqcup_{H \leq G, \#H=p^k} \{Hg \mid g \in G\} \\
\#X_0 &= \sum_{H \leq G, \#H=p^k} \underbrace{\#\{Hg \mid g \in G\}}_{=H \backslash G} \stackrel{\text{Lagrange}}{=} \frac{\#G}{\#H} = \frac{\#G}{p^k} = m \\
&= m \left( \sum_{H \leq G, \#H=p^k} 1 \right) = m \cdot n_k
\end{aligned}$$

3.  $pm \mid \#X_1$

(a)  $G$  wirkt auf  $X_1$  (durch  $(g, S) \mapsto gS$ )

d.h. gilt  $S \in X_1$  und  $g \in G$ , so auch  $gS \in X_1$ . Es genügt also zu zeigen:  $\#G_{gS} = \#G_S$

Dazu:

$$G_{gS} = \text{Stab}_G(gS) = g \text{Stab}_G(S) g^{-1} = g G_S g^{-1} \stackrel{\substack{\text{Konj. mit } g \\ \text{ist Gruppenisom.}}}{\cong} G_S.$$

(b) Betrachte nun  $G$ -Bahn durch  $S \in X_1$ , Behauptung:  $\#G \cdot S$  ist Vielfaches von  $p \cdot m$

Dazu: Bahngleichung:

$$\#G \cdot S = \#G / \#G_S = mp^k / \#G_S$$

da  $\#G_S$  echter Teiler von  $p^k$ , also Teiler von  $p^{k-1} \implies \#G_S$  ist Vielfaches von  $mp^k / p^{k-1} = mp$

$$(m \cdot 2^5 / 2^4 = m \cdot 2, \quad m \cdot 2^5 / 2^2 = m \cdot 2^3,)$$

(c) Schreibe nun  $X_1$  als disjunkte Vereinigung seiner Bahnen

$$X_1 = \bigsqcup_{j \in I} G \cdot \underbrace{S_j}_{\text{Bahnrepr.}}$$

und  $\#G \cdot S_j = m \cdot p \cdot a_j, a_j \in \mathbb{N}$

$$\implies \#X_1 = \sum_{j \in J} \#G \cdot S_j = m \cdot p \cdot \underbrace{\sum_{j \in J} a_j}_{=: N \in \mathbb{N}}$$

4.  $\#X = \#X_0 + \#X_1 = m \cdot n_k + m \cdot p \cdot N = m(n_k + pN)$

gleichzeitig:

$$\#X = \#\{S \subseteq G \mid \#S = p^k\} \stackrel{\#G=m \cdot p^k}{=} \binom{m \cdot p^k}{p^k} \stackrel{\text{Übung}}{=} m \cdot u$$

für ein  $u \in \mathbb{N} : u \equiv 1 \pmod{p}$ .

$$\implies m(n_k + pN) = n \cdot u \implies n_k + pN = u \cdot \frac{n}{m} \equiv u \equiv 1 \pmod{p}. \quad \square$$

**Korollar 0.31 (Satz von Cauchy).** Sei  $G$  eine endliche Gruppe mit  $p \mid \#G$  für  $p$  eine Primzahl, dann  $\exists g \in G : \text{ord}(g) = p$

*Beweis.* Nach Sylow I  $\exists H \leq G : \#H = p$ , sei  $g \in H \setminus \{e\}$ . Dann gilt  $\text{ord}(g) = p$ .  
( $\text{ord}(g) \neq 1$  und  $\text{ord}(g) \mid \#G = p$ ).  $\square$

**Definition 0.32 ( $p$ -Sylow Gruppe).** Sei  $G$  endlich, gelte  $\#G = p^f \cdot m$  für  $m, f \in \mathbb{N}$  sodass  $p \nmid m$ . Eine Untergruppe  $H \leq G$  mit  $\#H = p^f$  heißt  $p$ -Sylow (Unter-)Gruppe von  $G$ , schreiben

$$\text{Syl}_p(G) = \{H \leq G \mid H \text{ ist } p\text{-Sylow}\}$$

$$\text{syl}_p(G) = \#\text{Syl}_p(G)$$

**Definition 0.33 (Normalisator).** Der Normalisator einer Untergruppe  $H \leq G$  ist

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}$$

( $c_g$  ist Automorphismus  $\implies \#gHg^{-1} = \#H, \forall g \in G$ )

**Interpretation.** Sei  $X := \{H \mid H \leq G\}$ ,  $X$  ist eine  $G$ -Menge durch Konjugation  $c : G \times X \rightarrow X, (g, H) \mapsto gHg^{-1}$

**Proposition 0.34 (Übung).** (a)  $N_G(H) \underset{\text{für } H \leq G}{=} \text{Stab}_G(H)$

(Insbesondere ist  $N_G(H) \leq G$  eine Untergruppe.)

(b) Es gelten:  $H \trianglelefteq N_G(H)$  und  $N_G(H)$  ist die größte Untergruppe von  $G$ , sodass  $H$  ein Normalteiler in dieser ist.

**Lemma 0.35.** Sei  $H \leq G$  eine  $p$ -Gruppe,  $P \in \text{Syl}_p(G)$  ( $p$  eine Primzahl), dann:

(a) Gilt  $P \leq H$ , so folgt  $P = H$ .

(b) Ist  $H \leq N_G(P)$ , so gilt  $H \leq P$ .

(c) Gilt  $H \not\leq P$ , so folgt  $\text{Stab}_H(P) < H$  (ist echte Untergruppe)

*Beweis.* (a) Schreibe  $\#G = p^f \cdot m$ , so dass  $p \nmid m$  ( $m, f \in \mathbb{N}$ ),  $P$   $p$ -Sylow Untergruppe  $\implies \#P = p^f$ .

$H$  eine  $p$ -Gruppe in  $G \xRightarrow{\text{Lagrange}} \#H \mid p^f \cdot m$ . also  $\#H \mid p^f$

Nun:  $P \subseteq H$  und  $p^f = \#P = \#H \implies P = H$  (und  $\#H = p^f$ )

(b) Sei  $G' = N_G(P)$ . Aus Proposition

$$\implies P \trianglelefteq G' \xrightarrow[\text{Voraussetzung}]{\text{Nach}} H \leq G' \xrightarrow[\text{Isomorphiesatz}]{\text{Erster}} P \trianglelefteq P \cdot H$$

und

$$(P \cdot H)/P \cong H/P \cap H$$



Ordnung ist  $p$ -Potenz, evtl  $p^f$

$$\xRightarrow{\text{Lagrange}} \#P \cdot H = \underbrace{\#P}_{p\text{-Potenz}} \cdot \underbrace{\#P \cdot H / P}_{p\text{-Potenz}}$$

Also ist  $P \cdot H$  eine  $p$ -Gruppe mit  $P \subseteq PH$

$$\xRightarrow{(a)} PH = P \xRightarrow{eH \subseteq P} H \subseteq P$$

(c) Gelte  $H \not\subseteq P$ . zu zeigen:  $\text{Stab}_H(P) < H$

$$\text{Angenommen: } H = \text{Stab}_H(P) = \underbrace{\{h \in H \mid hPh^{-1} = P\}}_{=H \cap \text{Stab}_G(P)} = H \cap N_G(P)$$

Dann folgt

$$H \subseteq N_G(P) \xRightarrow{(b)} H \subseteq G. \quad \square$$

**Satz 0.36 (Sylow II).** Sei  $G$  endlich,  $p$  ein Primteiler von  $\#G$ . Dann:

(a) Je 2  $p$ -Sylow Gruppen von  $G$  sind konjugiert.

(b) Jede  $p$ -Gruppe  $H$  mit  $H \leq G$  liegt in einer  $p$ -Sylow Gruppe von  $G$ .

(c)  $\forall P \in \text{Syl}_p(G) : \text{syl}_p(G) = [G : N_G(P)]$  und insbesondere ( $P \leq N_G(P)$ ) gilt  $\text{syl}_p(G) \mid [G : P]$

*Beweis.* (a)  $X := \text{Syl}_p(G)$  ist  $G$ -Menge via Konjugation ( $P \in \text{Syl}_p(G)$  und  $g \in G \implies \#gPg^{-1} = \#P \implies gPg^{-1} \in \text{Syl}_p(G)$ )

Zu zeigen:  $G$  wirkt transitiv auf  $X$ .

Annahme:  $X$  besteht aus  $t \geq 2$  Bahnen, also

$$X = \bigsqcup_{i \in \{1, \dots, t\}} G \circ P_i$$

für geeignete Repräsentantensystem  $P_1, \dots, P_t \in \text{Syl}_p(G)$  ( $g \circ P = gPg^{-1}$ )

Behauptung:  $p \mid \#G \circ P_i, \forall i \in \{1, \dots, t\}$ .

Dazu: Wähle  $j \neq i$  betrachte die  $P_j$ -Wirkung auf  $G \circ P_i$ . Schreibe wieder  $G \circ P_i$  als disjunkte Vereinigung von  $P_j$ -Bahnen:

$$G \circ P_i = P_j \circ Q_1 \sqcup \dots \sqcup P_j \circ Q_s \quad (*)$$

( $s \in \mathbb{N}$  geeignet,  $Q_\ell \in \text{Syl}_p(G)$  geeignet)

Bahngleichung:

$$\#P_j \circ Q_\ell = \#P_j / \# \text{Stab}_{P_j}(Q_\ell)$$

beachte:  $P_j \notin G \circ P_i$ , d.h.  $P_j \neq Q_\ell$

$$\xRightarrow{35(c)} \text{Stab}_{P_j}(Q_\ell) < P_j \implies \#P_j \circ Q_\ell \neq 1 \text{ und teilt } \#P_j \implies p \mid \#P_j \circ Q_\ell$$

$$\implies p \text{ alle Bahnlängen in } (*) \text{ von } G \circ P \text{ als } P_j\text{-Menge} \implies p \mid \#G \circ P_i, \forall i \implies p \mid \# \text{Syl}_p(G)$$

$$\implies \text{Syl}_p(G) = \bigsqcup_{i \in \{1, \dots, t\}} G \circ P_i$$

Widerspruch zu (0):  $\text{syl}_p(G) \equiv 1 \pmod{p}$ .

- (b) Annahme:  $H \leq G$  eine  $p$ -Gruppe liegt in keiner  $p$ -Sylow. Betrachte Konjugationswirkung von  $H$  auf  $X = \text{Syl}_p(G)$ . Schreibe

$$X = H \circ R_1 \sqcup \dots \sqcup H \circ R_w$$

( $w \in \mathbb{N}$ ) die  $R_i$  sind Repräsentanten der Bahnen. Beachte  $H \not\subseteq R_i$  ( $i \in \{1, \dots, w\}$ ). Wie in (a) gilt  $\text{Stab}_H(R_i) < H$  also, dass  $p \mid \#H \circ R_i, \forall i \implies p \mid \#X$  Widerspruch zu (0).

- (c) Bahngleichung für  $P \in \text{Syl}_p(G)$  (Verwenden (a), d.h.  $G \circ P = \text{Syl}_p(G)$ )

$$\text{syl}_p(G) = \# \text{Syl}_p(G) = \#G / \# \text{Stab}_G(P) : \#G / \#N_G(P) = [G : N_G(P)]$$

( $\text{syl}_p(G)$  teilt  $[G : P]$  schon oben eingesehen, da  $P \leq N_G(P)$ )

□

**Korollar 0.37.** Sei  $G$  endlich und  $p$  ein Primteiler von  $\#G$ , dann  $\text{syl}_p(G) = 1 \iff$  jede  $p$ -Sylow ist ein Nullteiler in  $G$ .

*Beweis.* Für  $P \in \text{Syl}_p(G)$  gilt:

$$P \trianglelefteq G \iff N_G(P) = G \xLeftrightarrow[36(c)] \text{syl}_p(G) = [G : N_G(P)] = 1. \quad \square$$

**Korollar 0.38.** Sei  $G$  endlich, seien  $p_1, \dots, p_t$  die paarweise verschiedenen Primteiler von  $\#G$ . Sei  $P_i \in \text{Syl}_{p_i}(G)$ . Dann gilt: sind  $P_1, \dots, P_t$  Normalteiler von  $G$ , so folgt: die Abbildung  $P_1 \times \dots \times P_t \rightarrow G, (g_1, \dots, g_t) \mapsto g_1 \cdot \dots \cdot g_t$  ist ein Gruppenisomorphismus.

*Beweis.*  $P_i \trianglelefteq G$  für  $i \in \{1, \dots, t\}$

und  $\text{ggT}(\#P_i, \#P_j) = 1$  ( $p_i, p_j$  versch. Primzahlen) und  $\prod_{i=1}^t \#P_i = \#G$

$\implies$  die angegebene Abbildung ist ein Gruppenisomorphismus. □  
Kor. 1.55

**Beispiel.** Ist  $G$  abelsch, so sind alle Untergruppen Normalteiler.

**Korollar 0.39.**  $G$  endlich abelsch und  $p_i$  und  $P_i$  wie in Korollar 38. So gilt:  $\times_{i=1}^t P_i \xrightarrow{\text{wie in Kor. 38}} G$  ist Gruppenisomorphismus. ( $P_i$  sind abelsche  $p_i$ -Gruppen).

**Satz 0.40.** Sei  $G$  eine endliche abelsche  $p$ -Gruppe, dann  $\exists t \in \mathbb{N}, \exists! e_1 \geq e_2 \geq \dots \geq e_t \in \mathbb{N}$ , sodass

$$G \cong \times_{i=1}^t \mathbb{Z}/p^{e_i}$$

**Beispiel.**  $G$  abelsch mit  $\text{ord}(G) = 105 \implies G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

**Wiederholung.**  $G$  heißt einfach  $\iff$  einzige Nullteiler von  $G$  sind  $\{e\}$  und  $G$ .

**Lemma 0.41** (Übung). sei  $G$  endlich,  $\#G = p^f \cdot m$  mit  $f, m \in \mathbb{N}, p$  Primzahl und  $p \nmid m$ . Dann:  $p^f \nmid (m-1)! \implies G$  ist nicht einfach.

*Beweis.* Idee: Sei  $P \in \text{Syl}_p(G)$ , betrachte  $G$ -Wirkung auf  $G/P$  durch Linkstranslation, d.h.

$$\rho : G \rightarrow \text{Bij}(G/P), g \mapsto \ell g$$

Trick: Kern( $\rho$ ) ist der gesuchte Normalteiler.  $\square$

**Satz 0.42.** Ist  $G$  einfache Gruppe mit  $\#G < 60$ , so gilt  $G \cong \mathbb{Z}/p$  für  $p$  eine Primzahl.

*Beweis.* Sei  $G$  einfach mit  $\#G < 60$ . o.E.  $\#G$  keine Primzahl, sonst fertig. o.E.  $G$  ist keine  $p$ -Gruppe für Primzahl  $p$ . (sonst:  $Z(G) \supsetneq \{e\} \xrightarrow[Z(G) \trianglelefteq G]{G \text{ einfach}} G = Z(G)$ ,

d.h.  $G$  abelsch.  $\xRightarrow[G \text{ einfach}]{} G \cong \mathbb{Z}/p$ )

Fall  $\# = p^f m$  mit  $p^f \nmid (n-1)! \implies G$  nicht einfach (Lemma 41)

(Übung) Es bleiben  $\#G \in \{\underbrace{30}_{2 \cdot 3 \cdot 5}, \underbrace{40}_{2^3 \cdot 5}, \underbrace{56}_{2^3 \cdot 7}\}$

Fall 1:  $\#G = 2^3 \cdot 5$ , dann:  $\text{Syl}_5(G) \cong 1(5)$  (Sylow I)

$\text{Syl}_5(G)$  teilt  $\#G/5 = 8$  (Sylow II)

Teiler von 8 : 1, 2, 4, 8 Kongruenz erzwingt  $\text{Syl}_5(G) = 1 \xRightarrow{37}$  die einzige

5-Sylow Untergruppe von  $G$  ist ein Normalteiler (Widerspruch zu  $G$  einfach)

Fall 2:  $\#G = 2^3 \cdot 7$ , dann (Schritte wie im Fall 1 für  $p = 7$ )

$$\text{Syl}_7(G) \in \{1, 8\}$$

(teilt 8,  $\cong 1 \pmod{7}$ )

Fall: Es gibt 8 7-Sylow Untergruppen, isomorph zu  $\mathbb{Z}/7$

Beachte: 2 7-Sylow's schneiden sich nur in  $\{e\}$  (sonst sind sie gleich, Elemente  $\neq e$  sind Erzeuger)

$\implies$  es gibt  $8 \cdot 6$  Elemente in  $G$  der Ordnung 7

$\implies$  Es gibt  $56 - 48 = 8$  Elemente in  $G$  der Ordnung  $\neq 7$

Aber: Es gibt (mindestens) eine 2-Sylow Untergruppe von  $G$  und die hat Ordnung  $8 = 2^3$ .

Es folgt: Die 8 obigen Elemente bilden die einzig mögliche 2-Sylow Untergruppe von  $G$ .

$\implies \text{Syl}_2(G) = 1 \implies$  die 2-Sylow ist ein nicht triviale Normalteiler von  $G$ .

Fall 3 (Übung)  $\square$

**Bemerkung.** Die Zahl 60 ist optimal, denn  $A_5$  ist einfach, nicht zyklisch (von Primzahlordnung) und hat 60 Elemente.

## 0.4 Auflösbare Gruppen

**Definition 0.43.** (a) Eine aufsteigende Folge von Untergruppen  $G_0 < G_1 < G_2 < \dots < G_t = G$  von  $G$  heißt Normalreihe, wenn  $\forall i \in \{1, \dots, t\} : G_{i-1} \trianglelefteq G_i$  ist Normalteiler.

Schreibe auch  $(G_i)_{i=0}^t$  oder  $\&$  für die Folge.

(b) die Faktorgruppe  $(G_i/G_{i-1})_{i=1}^t$  heißen Faktoren der Normalreihe.

- (c) Eine Normalreihe  $\mathcal{G}$  heißt Zerlegungsreihe  $\iff$  alle Faktoren sind einfach.  
(d)  $X$  heißt abelsch  $\iff$  alle Faktoren sind abelsch.  
(e)  $G$  heißt auflösbar  $\iff G$  besitzt eine abelsche Normalreihe.  
(f) Ist  $\mathcal{G}' : G'_0 < G'_1 < \dots < G'_{t'} = G$  eine weitere Normalreihe, so heißt  $\mathcal{G}'$  **echt** feiner als  $\mathcal{G} \iff$

$$\{G_i \mid i \in \{0, \dots, t\}\} \subsetneq \{G'_j \mid j \in \{0, \dots, t'\}\}$$

**Beispiel.**

**Proposition 0.44.** Sei  $G''\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_t = G$  eine Normalreihe, dann:

- (a)  $G$  ist eine Zerlegungsreihe  $\iff G$  besitzt keine echte Verfeinerung.  
(b) Es gilt  $2^t \leq \#G$   
(c) Ist  $G$  endlich, so besitzt  $G$  eine Verfeinerung, die eine Zerlegungsreihe ist.  
(d) Ist  $G$  abelsch, so ist auch Verfeinerung abelsch.

*Beweis.* (a)  $G$  ist keine Zerlegungsreihe  $\iff \exists i \in \{1, \dots, t\} : G_i/G_{i-1}$  nicht einfach  $\iff \exists i \in \{1, \dots, t\} : \overline{H} \trianglelefteq G_i/G_{i-1}$  ein Normalteiler mit  $\overline{H} \neq \{e\}, \overline{H} \subsetneq G_i/G_{i-1}$  <sup>2. Isometriesatz</sup>  $\iff \{e\}i \in \{1, \dots, t\} : \exists H \triangleleft G_i$  ein Normalteiler mit  $G_{i-1} \triangleleft H$   
 $\iff \exists i \in \{1, \dots, t\} : G$  kann zwischen  $G_{i-1}$  und  $G_i$  echt verfeinert werden  
 $\iff G$  besitzt eine echte Verfeinerung.

- (b) Lagrange: (Für  $H \leq G : \#G = \#H \cdot \#G/H$ )

$$\begin{aligned} G = G_t &= \#G_{t-1} \cdot \#G_t/G_{t-1} = \#G_{t-2} \cdot \#G_{t-1}/G_{t-2} \cdot \#G_t/G_{t-1} \\ &\vdots \\ &\prod_{i=1}^t \#G_i/G_{i-1} \geq 2^t \end{aligned}$$

$$\implies t \leq \log_2 \#G$$

- (c) Sei  $G'$  eine Verfeinerung von  $G$ , maximaler Länge  $t'$ . Das gibt es, da  $t' \leq \log_2 \#G$  dieses  $G'$  kann nicht echt verfeinert werden ( $t'$  maximal!)  
 $\implies G'$  ist Zerlegungsreihe, die  $G$  verfeinert.  
(d) Sei  $G$  abelsch und  $G'$  eine Verfeinerung von  $G$ , z.z.  $G'$  ist abelsch. ( $G' : G'_0 = \{e\} \triangleleft G'_1 \triangleleft \dots \triangleleft G'_{t'} = G$ ) Sei  $j \in \{1, \dots, t'\}$ , z.z.  $G'_j/G'_{j-1}$  abelsch. Finde zu  $j, j-1$  ein  $i \in \{1, \dots, t\}$ , sodass

$$\begin{aligned} G \quad \dots \quad G_{i-1} &\triangleleft \quad G_i \quad \dots \\ &= \\ G'_\ell &\leq G'_{j-1} \triangleleft G'_{j'} \end{aligned}$$

□

**Satz 0.45 (Jordan-Hölder).** *Ist  $G$  endlich, so ist die Folge der Faktoren einer Zerlegungsreihe  $G(srqa)$  von  $G$  bis auf Reihenfolge der Faktoren unabhängig von der Wahl der Zerlegungsreihe von  $G$ .*

*Beweis.*

Jantzen Schwermer Satz II. 2.4

Jacobson §4.6

□

**Korollar 0.46.**  *$G$  endlich, dann  $G$  auflösbar  $\iff$  die Faktoren jeder Zerlegungsreihe sind (abelsch und ) von Primzahlordnung.*

*Beweis.*

“ $\implies$ ”: Sei  $\mathcal{G}$  eine abelsche Normalreihe  $\xrightarrow[44]{\implies} \exists$  Zerlegungsreihe  $G'$  die  $G$  verfeinert, diese ist dann (stets) wieder abelsch.

Ihre Faktoren sind einfach und abelsch (und endliche Gruppen), also zyklisch von Primzahlordnung.

Wende nun Jordan-Hölder an.

“ $\impliedby$ ”: Hat man  $G$  wie angegeben (zu  $G$ ), dann ist  $\mathcal{G}$  abelsch, also  $G$  auflösbar.

□

asdasdasd