Algebra 1 Vorlesungsmitschrieb nach Vorlesung von Prof. Gebhard Böckle

Yousef Khell

November 17, 2023

Inhaltsverzeichnis

Kapitel 1

Gruppentheorie

1.1 Gruppen und Monoide

Notation.

- $\mathbb{N} = \{1, 2, ...\}$
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
- $\#X =$ die Kardinalität/Mächtigkeit einer Menge X

Definition 1.1 (Monoid). Ein Tripel $(M, e, \circ)$ mit

- M einer Menge.
- e einem Element aus M,
- $\circ : M \times M \to M$ einer zweistelligen Verknüpfung

heißt **Monoid** falls gilt

(M1) Assoziativität:

$$\forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$$

(M2) Neutrales Element:

$$\forall a \in M : a \circ e = a = e \circ a$$

Wir nennen ein $a \in M$ **invertierbar**, falls

$$\exists b, b' \in M : b \circ a = e = a \circ b'$$

(b bzw. b' heißen dann Links- bzw. Rechtsinverse)

Bemerkung. $b = b'$, denn

$$b' = e \circ b' = (b \circ a) \circ b' = b \circ (a \circ b') = b \circ e = b$$

Definition 1.2 (**Gruppe**)**.** Eine **Gruppe** ist ein Monoid, in dem alle Elemente invertierbar sind.

Bemerkung 1.3 (zur Assoziativität)**.** Seien $a_1, ..., a_n \in M$, und setzt man in

$$a_1 \circ \cdots \circ a_n$$

Klammern, sodass $\circ$ jeweils 2 Elemente verknüpft, so ist wegen (M1) das Ergebnis unabhängig von der Wahl der Klammerung, and also lässt man i.a. die Klammern weg. (Die Reihenfolge ist aber schon wichtig!)

Definition 1.4 (**Abelsche Gruppe/Monoid**)**.** Ein Monoid bzw. eine Gruppe M heißt **abelsch** (oder kommutativ) $:\Longleftrightarrow \forall a, b \in M$:

$$a \circ b = b \circ a$$

Proposition 1.5 (Eindeutigkeit des neutralen Elements bzw. der neutralen Elementen)**.** *Sei M ein Monoid, dann*

(a) Erfüllt $e' \in M$ die Bedingung $e' \circ a = a \forall a \in M$, so gilt $e' = e$.

(b) Ist $a \in M$ invertierbar, so ist sein Inverses eindeutig.

Beweis.

(a) Nach Konstruktion $e = e' \circ e = e'$.

(b) Gelte $a \circ b' = e$ und b sei ein Inverses von a, dann:

$$b' = e \circ b' = (b \circ a) \circ b' = b \circ (a \circ b') = b \circ e = b.$$

$\square$

Satz 1.6 (ohne Beweis)**.** *Sei $(G, e, \circ)$ ein Tripel mit G eine Menge, $e \in G$, $\circ : G \times G \to G$ eine assoziative Verknüpfung sodass:*

- *e ist Linkseins, d.h.*
$$\forall g \in G : e \circ g = g$$

- *jedes g hat ein Linksinverses*
$$\forall g \in G \exists h \in G : h \circ g = e$$

So ist $(G, e, \circ)$ eine Gruppe.

Hinweis (Nutzen von Satz 6)**.** Es müssen weniger Axiome geprüft werden.

Notation.

(i) $ab := a \circ b$

(ii) $a^0 = e, a^1 = a, a^{n+1} = a^n a, n \in N$

(iii) $a^n = (a^{-n})^{-1}, n < 0$

(iv) Ist $\circ$ kommutativ, so schreibt man oft $+$

Übung (Rechenregeln)**.**

(i) $a^n a^m = a^{n+m}, (a^n)^m = a^{nm}, \forall m, n \in \mathbb{N}_0$

(ii) Ist a invertierbar, so gelten die Regeln $\forall n, m \in \mathbb{Z}$

Proposition 1.7 (Übung)**.** *Sei G eine Gruppe, seien $g, h \in G$, dann:*

(a) Die Glecihung $xg = h$ besitzt genau eine Lösung (in G), nämlich $x = hg^{-1}$.

(b) Es gilt $(gh)^{-1} = h^{-1}g^{-1}$

(c) Die Rechtstranslation (um g) $r_g : G \to G, x \mapsto xg$ und die Linkstranslationen (um g) $\ell_g : G \to G, x \mapsto gx$ sind bijektiv.

Beispiel. 1) $(\mathbb{N}_0, 0, +), (\mathbb{N}_0, 1, \cdot)$ sind kommutative Monoide.

2) Jede Gruppe ist ein Monoid.

3) Ist X eine Menge, $\mathrm{Abb}(X, X)$ bzw. $\mathrm{Bij}(X, X)$ die Menge aller Abbildungen bzw. Bijektionen von X in sich, so gilt:

   (a) $(\mathrm{Abb}(X, X), \mathrm{id}_X, \circ)$ ist ein Monoid.
   (b) $(\mathrm{Bij}(X, X), \mathrm{id}_X, \circ)$ ist eine Gruppe.

   Schreibe $S_n := \mathrm{Bij}(\{1, ..., n\}, \{1, ..., n\})$ für die Gruppe der Permutationen von $\{1, ..., n\}$.

4) Ist $(V, \langle\cdot, \cdot\rangle)$ ein Euklidischer Raum, so sind

   (i) $O(V) := \{\varphi \in \mathrm{End}_{\mathbb{R}}(V) | \varphi \text{ orthogonal}\}$ und $SO(V) := \{\varphi \in O(V) | \det(\varphi) = 1\}$ Gruppen.
   (ii) Ist $V = \mathbb{R}^2$ und $P_n := \{\cos \frac{2\pi j}{n}, \sin \frac{2\pi j}{n} \mid j = 0, ..., n-1\}$, dann ist
      (a) $C_n := \{\varphi \in SO(V) \mid \varphi(P_n) = P\}$ die Gruppe der Drehungen um 0 von Winkel $\frac{2\pi j}{n}, (j = 0, ..., n = 1)$ und
      (b) $D_n := \{\varphi \in O(V) \mid \varphi(P_n) = P\}$ die [[Diedergruppe]] der Ordnung $2n$

      (Übung) $\#C_n = n, \#D_n = 2n$.

   Gruppen beschreiben oft Symmetrien eines geometrischen Objekts.

5) Ist M ein Monoid, so ist $M^\times := \{a \in M \mid a \text{ invertierbar}\}$ eine Gruppe, also $(M^\times, e, \circ)$.

Definition 1.8 (Ring). Ein [[Ring]] ist ein [[Tupel]] $(R, 0, 1, +, \cdot)$, sodass

(R1) $(R, 0, +)$ eine [[abelsche Gruppe]],

(R2) $(R, 1, \cdot)$ ein Monoid,

(R3) Es gelten die Distributivgesetze

Definition 1.9 (Ordnung einer Gruppe). Ist M ein Monoid oder eine Gruppe, so heißt
$$\mathrm{ord}(M) := \#M$$
die Ordnung von M.

Definition 1.10 (Untermonoid/Untergruppe). Seien M ein Monoid, G eine Gruppe, dann

(a) $N \subseteq M$ heißt Untermonoid (UM) wenn:

- $e \in N$
- $\forall n, n' \in N : n \circ n' \in N$

(b) $H \subseteq G$ heißt Untergruppe (UG) wenn:

- $e \in H$
- $\forall h, h' \in H : h \circ h' \in H$

So schreiben wir $N \leq M, H \leq G$.

Übung 1.11. (i) $N \leq M \implies (N, e, \cdot\,|_{N\times N}\colon N \times N \to N)$ ist Monoid

(ii) $H \leq G \implies (H, e, \cdot\,|_{H\times H}\colon H \times H \to H)$ ist Monoid

Beispiel. Sei K ein Körper, dann ist

(i) $SL_n(K) \leq GL_n(K)$

(ii) $SO(V) \leq O(V) \leq \mathrm{Aut}_{\mathbb{R}}(V)$

Proposition 1.12 (Übung). *Sind $(H_i)_{i\in I}$ Untergruppen von G, so ist*

$$\bigcap_{i\in I} H_i \leq G.$$

Beispiel. Sei G eine Gruppe, $g \in G, S \leq G$, dann:

(i) $C_G(g)$ **Zentralisator** von $g \in G$, also

$$C_G(g) = \{h \in G \mid hg = gh\} \leq G$$

(ii) $C_G(S)$ **Zentralisator** von S, also

$$C_G(S) = \{h \in G \mid hs = sh \forall s \in S\} = \bigcap_{s\in S} C_G(s) \leq G$$

(iii) $Z(G)$ **Zentrum** von G, also

$$Z(G) = C_G(G) \underset{\text{komm.}}{\leq} G$$

(iv) (Übung) $Z(GL_n(K)) = K^\times \mathbf{1}_n$

Lemma 1.13. *Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge, dann $\exists$ kleinste Untergruppe $\langle S\rangle \leq G$, die S umfasst.*

Beweis. Definiere

$$\langle S\rangle := \bigcap \{H \leq G \mid S \subseteq H\}.$$

□

Übung 1.14. Sei M ein Monoid, $S \subseteq M$ eine Teilmenge, ein Wort aus S ist ein Ausdruck

$$s_1 \cdot \cdots \cdot s_n, s_i \in S, n \in N$$

Dann gilt: $\{\text{Worte in } S \cup \{e\}\} = \langle S \rangle \leq M$ ist das kleinste Untermodnoid von M, das S umfasst. Und ist G eine Gruppe, so gilt $\{\text{Worte in } S \cup S^{-1} \cup \{e\}\} = \langle S \rangle \leq G$ ist die kleinste Untergruppe von G, die S umfasst.

Definition 1.15 (**Erzeugendensystem**)**.** Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. S heißt Erzeugendensystem von $G \iff \langle S \rangle = G$.

Beispiel (Übung)**.** Seien $E_{ij} \in M_{n\times n}(K)$ die Elementarmatrizen mit 1 an der Stelle (i, j) und 0 sonst. Dann ist

$$\{\mathbf{1}_n + aE_{ij} \mid a \in K, i, j \in \{1, ..., n\}, i \neq j\}$$

ein Erzeugendensystem von $SL_n(K)$ (Gauß-Algorithmus)

Lemma 1.16. *Sei G eine Gruppe, $g \in G$, dann gilt*

$$\langle g \rangle = \langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Beweis. (Nach Übung 14)

$$\langle \{g\} \rangle = \{\text{Worte in } \{g, g^{-1}, e\}\}$$

$$= \{g^{i_1}, ..., g^{i_n} \mid n \in \mathbb{N} i_1, ..., i_n \in \{0, \pm 1\}\}$$

$$= \{g^{i_1+\cdots+i_n} \mid n \in \mathbb{N} i_1, ..., i_n \in \{0, \pm 1\}\}$$

$$= \{g^n | n \in \mathbb{Z}\}$$

□

Bemerkung. $\langle g \rangle$ ist abelsch.

Definition 1.17 (**Ordnung eines Gruppenelements, Zyklische Gruppe**)**.** Sei G eine Gruppe, $g \in G$

(a) Die Ordnung von g ist

$$\text{ord}(g) = \#\langle g \rangle = \#\{g^n \mid n \in \mathbb{Z}\} \in \mathbb{N} \cup \{\infty\}$$

(b) g hat endliche Ordnung $\iff \text{ord}(g) \in \mathbb{N}$

(c) G ist zyklisch $\iff \exists g \in G : G = \langle g \rangle$

Proposition 1.18. *Zyklische Gruppen sind abelsch.*

Beweis. G zyklisch $\implies \exists g \in G : G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Dann:

$$g^n g^m = g^{n+m} \overset{+\text{komm. in } \mathbb{Z}}{=} g^{m+n} = g^m g^n.$$

□

Proposition 1.19. *Sei G eine Gruppe, $g \in G, n := \operatorname{ord}(g)$ und*

$$n' = \sup\{m \in \mathbb{N} \mid e, g, g^2 ..., g^{m-1} \text{ paarw. versch.}\}$$

Dann gelten:

(a) $n' = \infty = \sup \mathbb{N}$ *oder* $g^{n'} = e$ *und* $\langle g \rangle = \{e, g, g^2 ..., g^{n'-1}\}$. *Insbesondere ist* $n' = n$

(b) Falls $n = \operatorname{ord}(g) < \infty$, *so gilt für* $m, m' \in \mathbb{Z}$:

$$g^m = g^{m'} \iff m \equiv m' \mod n$$

Insbesondere ist $g^m = e \iff n \mid m$

(c) Für $s \in \mathbb{Z}$ *gilt*

$$\operatorname{ord}(g^s) = \frac{n}{\operatorname{ggT}(n, s)}$$

Beweis.

(a) Gelte $n' < \infty$:

Definition von $n' \implies g^{n'} \in \{e, g, ..., g^{n'-1}\}$ Annahme: $g^{n'} = g^i$ für ein $i \in \{1, ..., n'-1\}$ Multipliziere mit $g^{-i} \implies g^{n'-i} = g^0 = e$ und $0 < n'-i < n'$, d.h. $g^{n'-i} \in \{e, ..., g^{n'-1}\} \implies \{g^0, ..., g^{n'-1}\}$ nicht paarweise verschieden (Widerspruch) Sei schließlich $m \in \mathbb{Z}$ beliebig, Division mit Rest:

$$m = qn' + r : q, r \in \mathbb{Z}, 0 \leq r \leq n' - 1$$

$$\implies g^m = g^{qn'+r} = (g^{n'})^q g^r = g^r \in \{g^0, ..., g^{n-1}\}$$

Also: $\langle g \rangle = \{e, ..., g^{n'-1}\}$ sind paarweise verschieden. $\implies \operatorname{ord}(g) = \#\langle g \rangle = n'$

(b) Seien $m, m' \in \mathbb{Z}$, schreibe $m' - m = qn' + r, (q, r \in \mathbb{Z}, 0 \leq r \leq n' - 1)$, dann:

$$g^{m'} = g^m \iff g^{m'-m} = g^0 = e \iff g^{qn'+r} = e$$

$$\iff g = e \underset{e,...,g^{n-1}\text{paarw. versch.}}{\overset{1.\ n=n'}{\iff}} r = 0$$

$$\iff m' - m \text{ ist Vielfaches von } n = n' \iff m \equiv m \mod n$$

(c) Bestime die $m \in \mathbb{Z}$ mit $(g^s)^m = e$

$$(g^s)^m = e \iff g^{sm} \underset{2.}{=} e \iff n \mid sm$$

$$\underset{\operatorname{ggT}(n,s)|n,s}{\iff} \frac{n}{\operatorname{ggT}(n, s)} \mid \frac{s}{\operatorname{ggT}(n, s)} m \iff \frac{n}{\operatorname{ggT}(n, s)} \mid m$$

Da $\frac{n}{\operatorname{ggT}(n,s)}, \frac{s}{\operatorname{ggT}(n,s)}$ teilerfremd sind

$$\overset{2.}{\iff} \operatorname{ord}(g^s) = \frac{n}{\operatorname{ggT}(n, s)} \square.$$

□

Beispiel.
$$\operatorname{ord}(g) = 6 \implies \operatorname{ord}(g^2) = 3 = 6/\operatorname{ggT}(6,2) = 6/2$$

Korollar 1.20. *Sei G eine Gruppe, dann*

(a) Für $g \in G$ gilt:

$$\operatorname{ord}(g) = \infty \iff g^n, n \in \mathbb{Z} \textit{ sind paarw. verschieden}$$

(b) Ist G zyklisch und $G \leq G$ eine Untergruppe, so ist H zyklisch.

Beweis.

(a) $\Longleftarrow$ vgl. 19(a) $\implies$ wissen nach 19(a), dass $e, g, ..., g^n, ...$ paarw. versch. sind. Multipliziere mit $g^{-m}, (m \in \mathbb{N}) \implies g^{-m}, g^{-m+1}, ..., g^0, g^1, ...$ sind paarw. versch.

(b) Sei $g \in G$ ein Erzeuger von $G, H \leq G$ eine UG von G und ohne Einschränkung $H \supsetneq \{e\}$

$$\implies \exists m \in \mathbb{Z} \setminus \{0\} : g^m \in H \setminus \{e\}$$

H ist Gruppe $\implies g^m, (g^m)^{-1} = g^{-m} \in H$

Sei $t \in \min\{m \in \mathbb{N} \mid g^m \in H\}$. Behauptung: $\langle g^t \rangle = H$.

- "$\subseteq$": Klar, da $g^t \in H$ also auch $\langle g^t \rangle \subseteq H$ (H ist UG die t enthält)
- "$\supseteq$": Sei $g^m \in H$, Division mit Rest: $m = tq+r : q, r \in \mathbb{Z}, 0 \leq r \leq t-1$

$$\implies H \ni g^m = g^{tq+r} = \underbrace{(g^t)}_{\in H}{}^q g^r \implies g^r = (g^m)((g^t)^q)^{-1} \in H$$

Nach Def von t muss gelten: $r = 0$, da $r = 1, ..., t-1$ verboten. Also ist $g^m = (g^t)^q \in \langle g^t \rangle$.

□

Korollar 1.21 (Übung)**.** *Untergruppen von $\mathbb{Z}$ sind die Mengen $\mathbb{Z}n = \{an \mid a \in \mathbb{Z}\}, (n \in \mathbb{N}_0)$*

Wiederholung (Vorbereitung)**.**

- Äquivalenzrelationen
- Äquivalenzklassen
- Repräsentantensysteme

Bemerkung.

- $X = \bigsqcup_{r \in \mathcal{R}} [r]_\sim$
- Falls $\#X < \infty : \# = \sum_{r \in \mathcal{R}} \#[r]_\sim$

Satz 1.22 (Satz von Lagrange)**.** *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe, dann gilt $\#H \mid \#G$.*

Beweis.

1) Definiere $\sim$ auf G durch $g \sim g' :\iff \exists h \in H : g' = gh$ $\sim$ ist eine Äquivalenzrelation:

   - reflexiv: $g \sim g$ denn $g = ge, e \in H$
   - symmetrisch: gelte $g' = gh$ für ein $h \in H$

   $$\underset{\_\cdot h^{-1}}{\Longrightarrow} g'h^{-1} = g \underset{H \text{ Gruppe}}{\Longrightarrow} h^{-1} \in H \Longrightarrow g' \sim g$$

   - transitiv: gelte $g \sim g', g' \sim g''$, d.h. $\exists h \in H : g' = gh, \exists h' \in H" g'' = g'h$

   $$\Longrightarrow g'' = g'h' = (gh)h' = g(hh') \Longrightarrow g \sim g''$$

2) Äquivalenzklassen: Für $g \in G$ ist

   $$[g]_\sim = \{g' \in G \mid \exists h \in H : g' = gh\} = \{gh \mid h \in H\} =: gH$$

3) Beachte G endlich $\Longrightarrow$ $H \subseteq G$ endlich (und ebenso jede Teilmenge von G) Behauptung: $\#gH = \#H \forall g \in G$ Grund: Die Abbildungen

   $$\ell_g : H \to gH, h \mapsto gh, \ell_{g^{-1}} : gH \to H, x \mapsto g^{-1}x$$

   sind zueinander invers (Übung) und also biijektiv. $\Longrightarrow \#H = \#gH$.

4) Sei $\mathcal{R} \subseteq G$ ein Repräsentantensystem zu $\sim$

   $\Longrightarrow \#G = \sum_{g \in \mathcal{R}} \#[g]_\sim = \sum_{g \in \mathcal{R}} \#gH = \sum_{g \in \mathcal{R}} \#H \overset{3)}{=} \#\mathcal{R}\#H$
   $\Longrightarrow \#H$ teilt $\#G$. $\square$

Notation. Seien G eine Gruppe, $H \leq G$ eine Untergruppe und $\sim$ wie im Beweis vom Satz 22.

- Schreibe ${}^{G}\!/_{H}$ für die Menge aller Äquivalenzklassen also für $\{gH \mid g \in G\}$
- Schreibe $[G : H] := \#{}^{G}\!/_{H} = \#\mathcal{R}$ (Index von H in G)

Lagrange sagt: $\#G = \#{}^{G}\!/_{H} \cdot \#H = [G : H] \cdot \#H$

Übung 1.23. Seien $H' \leq H \leq G$ Untergruppen, dann ist $H' \leq G$ und

$$[G : H'] = [G : H] \cdot [H : H']$$

Korollar 1.24. *Sei G eine endliche Gruppe, dann gelten:*

(a) $\forall g \in G : \operatorname{ord}(g) \mid \operatorname{ord}(G) = \#G$

(b) Ist $\operatorname{ord}(G)$ *eine Primzahl, so ist G zyklisch*

Beweis.

(a) $\langle g \rangle \leq G$ ist eine Untergruppe $\underset{\text{Lagrange}}{\Longrightarrow} \operatorname{ord}(g) = \#\langle g \rangle \mid \#G = \operatorname{ord}(G)$

(b) Sei $p = \mathrm{ord}(G) \in \mathbb{P}$ eine Primzahl, sei $g \in G \setminus \{e\}$ $(\#G \geq 2)$ Nach 1. gilt $\underbrace{\mathrm{ord}(g)}_{\neq 1 \text{ da } g \neq e} \mid \mathrm{ord}(G) = p$

Folglich: $p = \mathrm{ord}(g) = \mathrm{ord}(G)$, d.h. $\langle g \rangle \leq G$ ist Inklusion gleichmächtiger endlicher Mengen, also $\langle g \rangle = G$. □

Definition 1.25 (Gruppenexponent). Sei G eine Gruppe, der Exponent von G ist $\exp(G) = \min\{n \in \mathbb{N} \mid \forall g \in G : g^n = e\}$ (wobei $\min \emptyset = \infty$).

Beispiel (Übung)**.**

(i) $\exp(C_n) = n$

(ii) $\exp D_n = \mathrm{kgV}(2, n)$

(iii) $\exp(S_3) = 6$

(iv) $\exp(S_4) = 12$

(v) $\exp(G) = 2 \implies G$ abelsch

(vi) $\mathbb{F}_p$ Körper mit p Elementen und $0 \neq V$ ein $\mathbb{F}_p$-[[Vektorraum]], so gilt $\exp(V, 0, +) = p$

Satz 1.26. *Sei G eine endliche Gruppe, es gelten*

(a) $\exp(G) \mid \mathrm{card}(G)$

(b) $\exp(G) = \mathrm{kgV}(\{\mathrm{ord}(g) \mid g \in G\})$

Beweis.

(a) Folgt aus (b) und $\mathrm{ord}(g) \mid \mathrm{ord}(G) \forall g \in G$ nach Korollar 24.

(b) $\mathrm{ord}(g) \mid \exp(G), \forall g \in G$, denn nach Definition gilt:

$$g^{\exp(G)} = e \underset{19}{\implies} \mathrm{ord}(g) \mid \exp(G)$$

folglich: $N := \mathrm{kgV}(\{\mathrm{ord}(g) \mid g \in G\})$ teilt $\exp G$.

Behauptung: $\exp G \leq N$, (dann fertig)

Wir zeigen: $g^N = e \implies \exp G \leq N$. Dies folgt aus $g^{\mathrm{ord}(g)} = e$ und $\mathrm{ord}(g) \mid N = \mathrm{kgV}(...)$. □

Übung 1.27. Sei G eine endliche Gruppe, dann gelten:

(a) Sind $g, h \in G : gh = hg$ und gilt $\mathrm{ggT}(\mathrm{ord}(g), \mathrm{ord}(h)) = 1$, so gilt

$$\mathrm{ord}(gh) = \mathrm{ord}(g)\mathrm{ord}(h)$$

(b) Gelte $p^f \mid \exp G$ für p eine Primzahl und $f \in \mathbb{N}$, dann $\exists g \in G : \mathrm{ord}(g) = p^f$

(c) Ist G abelsch, so $\exists g \in G : \exp(G) = \mathrm{ord}(g)$

Satz 1.28. *Sei G eine endliche abelsche Gruppe, dann ist G genau dann zyklisch, wenn* $\mathrm{ord}(G) = \exp(G)$

Beweis.

- “ $\Longrightarrow$ ”: Sei $g \in G$ Erzeuger $\underset{19}{\Longrightarrow}$ $\mathrm{ord}(G) = \mathrm{ord}(g)$

$$\mathrm{ord}(g) \mid \exp G, \exp G \mid \mathrm{ord}(G) \implies \exp G = \mathrm{ord}(G)$$

- “ $\Longleftarrow$ ”: Wähle nach 27.3 ein $g \in G$ mit $\mathrm{ord}(g) = \exp(G)$, nach Voraussetzung ist $\exp(G) = \mathrm{ord}(g) \implies \mathrm{ord}(g) = \mathrm{ord}(G) \implies \langle g \rangle \subseteq G$ ist Gleichheit, d.h. $\langle g \rangle = G$.

□

1.2 Gruppenhomomorphismen

Seien im Weiteren M, M' Monoide und G, G' Gruppen.

Definition 1.29 (**Monoid-/Gruppenhomomorphismus**).

(a) Eine Abbildung $\varphi : M \to M'$ heißt **Monoidhomomorphismus**, falls

  (i) $\varphi(e) = e'$ und

  (ii) $\forall m, \tilde{m} \in M : \varphi(m \circ \tilde{m}) = \varphi(m) \circ' \varphi(\tilde{m})$

(b) Sind M, M' Gruppen, so heißt ein Gruppenhomomorphismus $\iff$ (ii) gilt.

Bemerkung 1.30.

(a) Ist $\varphi : M \to M'$ ein Gruppenhomomorphismus, so gilt $\varphi(e) = e'$ und $\varphi(m^{-1}) = \varphi(m)^{-1}, \forall m \in M$.

(b) (Übung) Die Verkettung von Monoid- bzw. Gruppenhomomorphismen ist wieder ein solcher.

Beweis. Zu (a):

$$e' \circ' \varphi(e) = \varphi(e) = \varphi(e \circ e) = \varphi(e) \circ' \varphi(e)$$

Kürzen $\implies e' = \varphi(e)$. Und

$$\varphi(m^{-1}) \circ' \varphi(m) = \varphi(m^{-1} \circ m) = \varphi(e) = e'$$

Eindeutigkeit des Inverses $\implies \varphi(m^{-1}) = \varphi(m)^{-1}$. □

Beispiel 1.31. (a) Für $g \in G$ ist die Abbildung

$$\varphi : \mathbb{Z} \to G, n \mapsto g^n$$

ein Gruppenhomomorphismus mit $\mathrm{Bild}(\varphi) = \langle g \rangle$.

(b) Sei K ein Körper, V, W K-Vektorräume, $\varphi : V \to W$ ein Vektorraumhomomorphismus, dann ist

$$\varphi : (V, 0_V, +_V) \to (W, 0_W, +_W)$$

ein Gruppenhomomorphismus.

(c) Die Vorzeichenfunktion (Aus der linearen Algebra)

$$\mathrm{sgn} : S_n \to \{\pm 1\}, \sigma \mapsto \mathrm{sgn}(\sigma)$$

ist ein Gruppenhomomorphismus.

Definition 1.32 (**Kern/Bild**)**.** Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus.

(a) Der Kern von φ ist $\mathrm{Kern}(\varphi) := \{g \in G \mid \varphi(g) = e'\}$

(b) Das Bild von φ ist $\mathrm{Bild}(\varphi) := \{\varphi(g) \in G' \mid g \in G\}$

Proposition 1.33 (Übung)**.** *Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus, dann*

(a) Für $H \leq G$ eine Untergruppe ist $\varphi(G) \leq G'$ eine Untergruppe.

(b) Für $H' \leq G'$ eine Untergruppe ist $\varphi^{-1}(H') \leq G$ eine Untergruppe.
Insbesondere sind $\mathrm{Bild}(\varphi) \leq G', \mathrm{Kern}(\varphi) \leq G$ Untergruppen.

(c) φ ist injektiv (ein Gruppenmonomorphismus) $\iff \mathrm{Kern}(\varphi) = \{e\}$.

(d) φ ist surjektiv (ein Gruppenepimorphismus) $\iff \mathrm{Bild}(\varphi) = G'$

Bemerkung. (a), (b) und (d) gelten auch für Monoide.

Definition 1.34 (**Gruppenisomorphismus**)**.** Ein Gruppenhomomorphismus φ ist ein Gruppenisomorphismus, wenn φ bijektiv ist. ($\iff \mathrm{Kern}(\varphi) = \{e\}$ und $\mathrm{Bild}(\varphi) = G'$).

Bemerkung (Übung)**.** Definiere ein Monoidhomomorphismus analog zu Definition 24.

Notation. Wir schreiben $G \cong G'$ (G ist isomorph zu G') wenn $\exists$ Gruppenisomorphismus $\varphi : G \to G'$.

Definition 1.35 (**Gruppenautomorphismus**)**.** (a) Ein Gruppenisomorphismus $\varphi : G \to G$ heißt Gruppenautomorphismus.

(b) $\mathrm{Aut}(G) := \{\varphi : G \to G \mid \varphi$ ist ein Gruppenautomorphismus$\}$.

Bemerkung 1.36 (Übung)**.** (a) $\mathrm{id}_G : G \to G \in \mathrm{Aut}(G)$

(b) Verkettung von Gruppenisomorphismen (oder Automorphismen) ist wieder ein solcher.

(c) Ist $\varphi : G \to G'$ ein Gruppenisomorphismus, so gelten

  (i) $\#G = \#G'$.

  (ii) G abelsch $\iff G'$ abelsch.

  (iii) $S \subseteq G$ ein Erzeugendensystem $\iff \varphi(S) \subseteq G'$ ein Erzeugendensystem.

Proposition 1.37. *$(\mathrm{Aut}(G), \mathrm{id}_G, \circ)$ und $(\mathrm{Aut}(M), \mathrm{id}_M, \circ)$ sind Gruppen.*

Beweis. (Übung) Zeige:

$$\mathrm{Aut}(G) \leq \mathrm{Bij}(G), \mathrm{Aut}(M) \leq \mathrm{Bij}(M)$$

sind Untergruppen. □

Beispiel 1.38 (Übung)**.**

(a) $\mathrm{Aut}((\mathbb{Z}, 0, +)) = \{\mathrm{id}_{\mathbb{Z}}, -\mathrm{id}_{\mathbb{Z}}\} \cong C_2$

(b) Für $\mathbb{Z}_n := \mathbb{Z}/_{(n)}$ der Ring der Restklassen modulo n gilt

$$(\mathbb{Z}_n, \overline{0}, +) \cong C_n \text{ und } \mathrm{Aut}(\mathbb{Z}_n, \overline{0}, +) \cong \mathbb{Z}_n^\times$$

z.B. Erzeuger von $\mathbb{Z}_n$ sind Reste $\overline{a}$, sodass $\mathrm{ggT}(a, n) = 1$

(c) Sei G beliebig, zu $g \in G$ definiere den **Konjugationsautomorphismus** (**Konjugation** mit g)

$$c_g : G \to G, h \mapsto g \circ h \circ g^{-1}$$

(i) $c_g \circ c_{g'} = g_{g \circ g'}, \forall g, g' \in G$

(ii) $c_e = \mathrm{id}_G$ und $c_g \in \mathrm{Aut}(G), \forall g \in G$

(iii) $c. : G \to \mathrm{Aut}(G), g \mapsto c_g$ ist ein Gruppenhomomorphismus.

(iv) $\mathrm{Kern}(c.) = Z(G)$ (Zentrum von G).

Bemerkung. $\mathrm{Bild}(c.) =: \mathrm{Inn}(G)$ die Gruppe der **inneren Automorphismen** von G

Lemma 1.39. *Seien $\varphi, \varphi' : G \to G'$ Gruppenhomomorphismen. Sei $S \subseteq G$ ein Erzeugendensystem. Dann gilt*

$$\varphi(s) = \varphi'(s) \forall s \in S \iff \varphi = \varphi' \quad (*)$$

Analoge Aussage gilt für Monoide

Beweisskizze. (Übung)

- " $\Longleftarrow$ ": Klar.
- " $\Longrightarrow$ ":

  1) Zeige $H := \{g \in G \mid \varphi(g) = \varphi'(g)\} i \leq G$ ist eine Untergruppe.
  2) Da $S \subseteq$ nach Definition von H und Voraussetzung von " $\Longrightarrow$ ", folgt $G = \langle S \rangle \subseteq H \leq G$

□

Normalteiler (Normal Subgroup)

Notation. Für $X \subseteq G$ und $g \in G$ setze

$$\ell_g(X) = \{gx \mid x \in X\} = gX \text{ und } r_g(X) = \{xg \mid x \in X\} = Xg$$

Gruppenverknüpfung assoziaativ $\implies$

(i) $c_g(X) = \{gxg^{-1} \mid x \in X\} = (gX)g^{-1} = g(Xg^{-1})$.

(ii) $g(hX) = (gh)X$ und $(Xg)h = X(gh)$.

Bemerkung. Ist $H \leq G$ eine Untergruppe, dann heißt gH **Linksnebenklasse** und Hg **Rechtsnebenklasse**.

Definition 1.40 (**Normalteiler**)**.** Eine Untergruppe $N \leq G$ heißt Normalteiler (N.T.) $\iff$ $\forall g \in G : Ng = gN$. (Diese Definition ist auch für Monoide sinnvoll)

Lemma 1.41. *Für eine Untergruppe $N \leq G$ sind äquivalent:*

(i) $\forall g \in G : gN = nG$

(ii) $\forall g \in G : gNg^{-1} = N$

(iii) $\forall g \in G : gNg^{-1} \subseteq N$

Beweis.
- "$(ii) \implies (iii)$": Klar.
- "$(iii) \implies (i)$": Rechtsmultiplikation mit g liefert aus (iii):

  $$(gNg^{-1})g = gN(g^{-1}g) = gNe = gN \subseteq Ng$$

  Für die andere Inklusion betrachte (iii) für g^{-1}:

  $$g^{-1}Ng \subseteq N \underset{\text{Linksmult. mit } g}{\implies} Ng \subseteq gN$$

- "$(i) \implies (ii)$": Wende auf (i) Rechtsmultiplikation mit g^{-1} an. ($r_{g^{-1}} : G \to G$ ist eine bijektive Abbildung.)

$\square$

Notation.

$H \leq G$ bedeuteg $H \subseteq G$ ist eine Untergruppe.

$H \trianglelefteq G$ bedeuteg $H \subseteq G$ ist ein Normailteiler.

Satz 1.42. *Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus, so ist* $\mathrm{Kern}(\varphi) \trianglelefteq G$ *ein Normalteiler.*

Beweis. Sei $g \in G$ beliebig, zu zeigen ist $g \circ \mathrm{Kern}(\varphi) \circ g^{-1} \subseteq \mathrm{Kern}(\varphi)$

Sei $h \in \mathrm{Kern}(\varphi)$, zu zeigen ist $ghg^{-1} \in \mathrm{Kern}(\varphi)$. Damit:

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) \underset{h \in \mathrm{Kern}(\varphi)}{=} \varphi(g) \circ e' \circ \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1})$$

$$= \varphi(gg^{-1}) = \varphi(e) = e'.$$

$\implies \mathrm{Kern}(\varphi) \trianglelefteq G$. $\square$

Übung 1.43.

(a) Ist $N' \trianglelefteq G'$ und $\varphi : G \to G'$ Gruppenhomomorphismus, so gilt $\varphi^{-1}(N') \trianglelefteq G$.

(b) Ist $h \leq G$ eine Untergruppe mit $[G : H] = \#{}^{G}\!/\!_{H} = 2$, so folgt $H \trianglelefteq G$.

(c) Ist G abelsch, so ist jede Untergruppe $H \leq G$ ein Normalteiler.

(d) Der **Kommutator** zu $g, h \in G$ ist $ghg^{-1}h^{-1}$, die **Kommutatoruntergruppe** von G ist

$$[G, G] := \langle ghg^{-1}h^{-1} \mid g, h \in G\rangle$$

Es gilt $[G, G] \trianglelefteq G$.

Beispiel. Es gibt Beispiele für folgende Aussagen:

(i) $\exists H \leq G : H \ntrianglelefteq G$

(ii) $\varphi : G \to G'$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $\varphi(G) \ntrianglelefteq G'$

(iii) $\exists N \trianglelefteq G$ und $H \trianglelefteq N$, so dass $H \ntrianglelefteq G$.

Beweis.

(i) $G = S_3 = \mathrm{Bij}(\{1, 2, 3\}) \supseteq H = \{\mathrm{id}, \sigma\}$ mit $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Dann $H \leq G$ Klar, aber $H \ntrianglelefteq G$, denn für $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ gilt $\tau\sigma\tau^{-1}$ (Übung) $\implies \tau H \tau^{-1} \nsubseteq H$

(ii) Betrachte $\varphi : H \to G$ Inklusion mit G, H aus (i), dann gilt $H \trianglelefteq H$ aber $\varphi(H) = H$ nein Nullteiler von $G = S_3$.

(iii) Später.

$\square$

Satz 1.44. *Sei $N \trianglelefteq G$ ein Normalteiler, dann gelten:*

(a) Aus $gN = g'N$ und $hN = h'N$ für $g, g', h, h' \in G$ folgt $ghN = g'h'N$ und insbesondere ist die Verknüpfung

$$\circ : \underbrace{{}^{G}\!/\!_{N}}_{\{gN \mid g \in G\}} \times {}^{G}\!/\!_{N} \longrightarrow {}^{G}\!/\!_{N},\ (gN, hN) \longmapsto gN \circ hN = ghN$$

wohl-definiert.

(b) ${}^{G}\!/\!_{N}, \underbrace{N}_{=eN}, \circ)$ ist eine Gruppe.

(c) $gN = g'N \iff g^{-}1g' \in N$.

(d) $\pi : G \to {}^{G}\!/\!_{N}, g \mapsto gN$ ist ein Gruppenhomomorphismus mit $\mathrm{Kern}(\pi) = N$.

Beweis. (a) Es gelten (Formeln von Definition 40)

$$(gh)N = g(hN) \overset{N \trianglelefteq G}{=} g(Nh) = (gN)h$$
$$= (g'N)h = g'(Nh) = g'(hN) = g'(h'N) = (g'h')N \implies (a)$$

(b) Überlege Gruppenaxiome.

- Assoziativität (Übung)
- Linkseins ist $N = eN$, denn

$$N \circ (gN) = eN \circ gN \overset{\text{wohl-def.}}{=} (e \circ g)N = gN$$

- Linksinverses zu gN ist $g^{-1}N$, denn

$$(g^{-1}N) \circ gN \underset{\text{nach Def.}}{=} (g^{-1}g)N \underset{\text{Gruppe}}{=} eN = N$$

(c) $gN = g'N \underset{g^{-1}\circ\_}{=} N = g^{-1}g'N \underset{e \in N}{\implies} N \ni g^{-1}g'e$, d.h. $g^{-1}g' \in G$.

$$g^{-1}g' \in N \underset{\substack{\ell_{g^{-1}g'}: N \to N \\ \text{ist bijektiv.}}}{\implies} N = g^{-1}N \underset{g^{-1}\circ\_}{\implies} gN = g'N$$

(d) $\pi : G \to G/N, g \mapsto gN$ ist Gruppenhomomorphismus, denn

$$\pi(gg') = gg'N \underset{\text{Def. von } \circ}{=} gN \circ g'N = \pi(g) \circ \pi(g')$$

$$g \in \mathrm{Kern}(\pi) \iff gN = eN \underset{(c)}{\iff} e^{-1}g = g \in N$$

□

Bemerkung (Bezeichnung)**.** G/N (bzw. $(G/N, eN, \circ)$) heißt **Faktorgruppe** von G modulo N.

Bemerkung (Übung)**.** G abelsch $\implies G/N$ abelsch.

Satz 1.45 (Homomorphiesatz für Gruppen)**.** *Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus mit $N = \mathrm{Kern}(\varphi)$, dann existiert genau ein Gruppenhomomorphismus $\overline{\varphi} : G/N \longrightarrow G'$, sodass*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\ G/N \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

kommutiert, d.h. $\overline{\varphi} \circ \pi = \varphi$. (wobei $\pi : G \longrightarrow G/N, g \mapsto gN$ aus Satz 44). Die Abbildung $\overline{\varphi}$ ist injektiv und $\overline{\varphi}$ bijektiv $\iff \varphi$ surjektiv.

Beweis.
- Existenz von $\overline{\varphi}$: Definiere $\overline{\varphi}(gN) = \varphi(g), \forall g \in G$.

- $\overline{\varphi}$ wohl-definiert: Es gilt: $gN = g'N \iff N = g^{-1}g'N \underset{44c}{\iff} g^{-1}g' \in N$. Damit

$$\implies \varphi(g') = \varphi(gg^{-1}g') = \varphi(g)\varphi(\underbrace{g^{-1} \circ g'}_{\in N = \mathrm{Kern}(\varphi)}) = \varphi(g)e = \varphi(g).$$

- $\overline{\varphi}$ Gruppenhomomorphismus:

$$\overline{\varphi}(gN \circ g'N) \underset{\text{Def. von } \circ}{=} \overline{\varphi}(gg'N) \underset{\text{Def. von } \overline{\varphi}}{=} \varphi(gg') \underset{\varphi \text{ Hom.}}{=} \varphi(g)\varphi(g')$$

$$\underset{\text{Def. von } \overline{\varphi}}{=} \overline{\varphi}(gN)\overline{\varphi}(g'N).$$

- $\overline{\varphi} \circ \pi = \varphi$: (Aus der Definition von $\overline{\varphi}$):

$$\underbrace{\overline{\varphi}(gN)}_{\overline{\varphi}(\pi(g))} = \varphi(g)$$

- $\overline{\varphi}$ injektiv: $\overline{\varphi}(gN) = e \iff \varphi(g) = e \iff g \in N = \mathrm{Kern}(\varphi) \underset{44c}{\iff} gN = eN = N$.
- $\overline{\varphi}$ eindeutig: Folgt aus der Surjektivität von π.
- Zusatz φ surjektiv $\iff \overline{\varphi}$ Isomorphismus (Übung): Verwende $\mathrm{Bild}(\varphi) = \mathrm{Bild}(\overline{\varphi})$ und $\overline{\varphi}$ injektiv.

□

Satz 45' (Homomorphiesatz'). *(Übung) Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus und $N \trianglelefteq G$, so dass $N \subseteq \mathrm{Kern}(\varphi)$, dann existiert genau ein Gruppenhomomorphismus*

$$\overline{\varphi} : {}^{G}\!/\!_{N} \longrightarrow G' \textit{ mit } \overline{\varphi} \circ \pi = \varphi.$$

wobei $\pi : G \to {}^{G}\!/\!_{N}, g \mapsto gN$

Notation. Für $n \in \mathbb{N}$ sei $\mathbb{Z}_n = {}^{\mathbb{Z}}\!/\!_{(n)} = {}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ der Restklassenring. ($n\mathbb{Z} \subseteq \mathbb{Z}$ eine Untergruppe)

Korollar 1.46. *Sei G eine zyklische Gruppe,*

(a) Falls $m := \mathrm{ord}(G) \in \mathbb{N} \implies G \cong \mathbb{Z}_m = {}^{\mathbb{Z}}\!/\!_{(m)}$.

(b) Falls $\mathrm{ord}(G) = \infty \implies G \cong \mathbb{Z}$.

Beweis. Sei $g \in G$ ein Erzeuger und betrachte

$$\varphi : \mathbb{Z} \to G, n \mapsto g^n$$

φ ist surjektiv, da $\mathrm{Bild}(\varphi) = \langle g^n \mid n \in \mathbb{Z} \rangle = G$.

$$\underset{\text{Satz 45}}{\implies} \overline{\varphi} : {}^{\mathbb{Z}}\!/\!_{\mathbb{Z}m} \xrightarrow{\cong} G$$

für $m \in \mathbb{N}_0$, so dass $\mathrm{Kern}(\varphi) = \mathbb{Z}m$.

- Fall (b): $\operatorname{ord}(G) = \infty \implies \operatorname{Kern}(\varphi) = \{0\} \implies \varphi : \mathbb{Z} \to G$ ist ein Isomorphismus.
- Fall (a): $\operatorname{ord}(G) = m \in \mathbb{N}$ dann ist $\overline{\varphi}$ der gewünschte Isomorphismus.

□

Korollar 1.47. *Für zyklische Gruppen G, H gilt $G = H \iff \#G = \#H$*

Übung. (a) $G/[G,G]$ ist eine abelsche Gruppe.

(b) Für $N \trianglelefteq G$ gilt:

$$G/N \text{ abelsch } \iff [G,G] \leq N$$

Einschub: Faktorringe

Definition 1.48 (Ideal). Sei R ein kommutativer Ring. $I \subseteq R$ heißt Ideal wenn

(i) I ist Untergruppe von $(R, 0, +)$

(ii) $RI := \{ri \mid r \in R, i \in I\} \subseteq I$

Beispiel. 1) $\mathbb{Z}n \subseteq \mathbb{Z}$ ist ein Ideal $\forall n \in \mathbb{Z}$.

2) $Ra \subseteq R$ für $a \in R$ ist ein *Ideal* von R.

Satz 1.49. *Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal, und $R/I = \{r + I \mid r \in R\}$ die Nebenklassenmenge von R modulo I (für die Gruppe $(R, 0, +)$). Dann:*

(a) Die Verknüpfungen

$$+ : R/I \times R/I \longrightarrow R/I, (r + I, s + I) \longmapsto (r + s) + I$$

$$\cdot : R/I \times R/I \longrightarrow R/I, (r + I, s + I) \longmapsto rs + I$$

sind wohl-definiert auf R/I

(b) $(R/I, \overline{0}, \overline{1}, +, \cdot)$ ist ein kommutativer Ring ($\overline{r} := r+I$ Notation für die Klasse von r) der Restklassenring von R modulo I.

(c) $\pi : R \longrightarrow R/I, r \longmapsto r + I$ ist ein surjektiver Ringhomomorphismus.

Beweis. (a) "+" wohl-definiert folgt aus Satz 44. ($I \subseteq (R, 0, +)$ Ideal!)

"·" wohl-definiert: Gelte $a + I = a' + I$ und $b + I = b' + I$.

$$\implies a'b' + I = ab + aj + bi + ij + I = ab + I$$

(b) (Übung)

(c) Wie in 45 (d)

□

Die Isomorphiesätze

Satz 1.50 (**Erster Isomorphiesatz**). *Sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $H \leq G$ eine Untergruppe, dann gelten:*

(a) $HN = \{hn \mid h \in H, n \in N\} \subseteq G$ ist ein Untergruppe.

(b) $H \cap N \subseteq H$ ist ein Normalteiler (und (Übung) $N \trianglelefteq HN$)

(c) Die folgende Abbildung ist wohl-definiert und ein Gruppenisomorphismus

$$H/_{H \cap N} \longrightarrow HN/_N, h(H \cap N) \longmapsto hN$$

Beweis. (a) Seien $hn, h'n' \in HN$, dann:

$$(h'n')(hn)^{-1} = h' \underbrace{n'n^{-1}h^{-1}}_{\in Nh^{-1} \underset{N \trianglelefteq G}{=} h^{-1}N} = h'h^{-1}\tilde{n} \underset{H \text{ U.G.}}{=} (h'h^{-1})\tilde{n} \in HN$$

und $e = ee = HN$

(b) Zu zeigen: für $h \in H$ gilt $h(H \cap N)h^{-1} \subseteq H \cap N$

Dazu:

$$\begin{array}{r} h(H \cap N)h^{-1} \subseteq hHh^{-1} = H \\ h(H \cap N)h^{-1} \subseteq hNh^{-1} \underset{N \trianglelefteq G}{=} N \end{array} \implies h(H \cap N)h^{-1} \subseteq H \cap N.$$

(c) Betrachte die Verkettung von Gruppenhomomorphismen

$$\varphi : H \xrightarrow[h \longmapsto h]{\text{Inklusion}} HN \xrightarrow[x \longmapsto xN]{} HN/_N$$

dann ist φ ein Gruppenautomorphismus.

φ ist surjektiv: Jede Klasse in $HN/_N$ ist von der Form

$$hnN = \underbrace{hN}_{=\varphi(h)}$$

für ein $h \in H$. Nach Homomorphiesatz: nur noch zu zeigen $\text{Kern}(\varphi) = H \cap N$: für $h \in H$:

$$h \in \text{Kern}(\varphi) \iff \varphi(h) = eN \iff hN = eN \underset{44(c)}{\implies} h \in N \underset{h \in H}{\implies} h \in N \cap H$$

Umgekehrt: $h \in N \cap H \implies h \in N \implies hN = eN = N.$

$\square$

Satz 1.51 (**Zweiter Isomorphiesatz**). *Sei G eine Gruppe und $N \trianglelefteq G$ ein Normailteiler, und sei $\pi : G \longrightarrow G/_N, g \longmapsto \overline{g} = gN$ die Faktorabbildung.*

(a) Sei $X := \{H \leq G \mid N \subseteq H\}$, und sei $\overline{X} := \left\{\overline{H} \leq {}^{G}\!/_{N}\right\}$, dann ist die Abbildung

$$\psi : X \longrightarrow \overline{X}, H \longmapsto \pi(H) = {}^{H}\!/_{N} =: \overline{H}$$

eine Bijektion mit inverser Abbildung

$$\nu : \overline{X} \longrightarrow X, \overline{H} \longmapsto \pi^{-1}(\overline{H}).$$

Dabei gilt:

$$X \ni H \trianglelefteq G \iff \overline{X} \ni \pi(H) \trianglelefteq {}^{G}\!/_{N}$$

(b) Ist $H \in X$ ein Normalteiler von G, so ist

$${}^{G}\!/_{H} \longrightarrow \left({}^{G}\!/_{N}\right)\Big/\left({}^{H}\!/_{N}\right), g \longmapsto \underbrace{\overline{g}}_{gN}\,\underbrace{\overline{H}}_{\pi(H)}$$

wohl-definiert und ein Gruppenisomorphismus.

Beweis. (a) Nach Proposition 33 sind ψ und ν wohl-definiert.

- $\nu \circ \psi = \mathrm{id}_X$: Sei $H \leq G$ mit $N \subseteq H$, zu zeigen ist $\pi^{-1}(\pi(H)) = H$. Es gilt:

$$g \in \pi^{-1}(\pi(H)) \iff \pi(g) \in \pi(H) \iff gN \in \bigcup_{h \in H} hN$$

$$\iff \exists h \in H : gN = hN \underset{44(c)}{\implies} h^{-1}g \in N \subseteq H \implies g \in hH = H.$$

  („ $\Longleftarrow$ " klar: $g \in H \implies g \in \pi^{-1}(\pi(H))$).

- $\psi \circ \nu = \mathrm{id}_{\overline{X}}$: Für $\overline{H} \in \overline{X}$ (d.h. $\overline{H} \leq {}^{G}\!/_{N}$) ist zu zeigen $\pi(\pi^{-1}(\overline{H})) = \overline{H}$. Dies gilt, denn π ist surjektiv.

- Schließlich: Sei $H \in X$, zu zeigen ist $H \trianglelefteq G \iff \pi(H) \trianglelefteq {}^{G}\!/_{N}$

$$H \trianglelefteq G \iff \forall g \in G : gHg^{-1} \subseteq H$$

$$\underset{\pi : G \to \overline{G} \text{ surj.}}{\implies} \forall \overline{g} \in {}^{G}\!/_{N} : \overline{g}\pi(H)\overline{g} \subseteq \pi(H) \implies \pi(H) \trianglelefteq \overline{G}$$

  Umgekehrt: Falls $\pi(H) \trianglelefteq\trianglelefteq \overline{G}$ und $g \in G$:

$$\pi(gHg^{-1}) = \overline{g}\pi(H)\overline{g}^{-1} \leq \pi(H)$$

$$\implies gHg^{-1} \subseteq \pi^{-1}(\pi(gHg^{-1})) \subseteq \pi^{-1}(\pi(H)) \underset{\nu \circ \psi = \mathrm{id}_X}{=} H$$

(b) Sei $H \trianglelefteq G$ ein Normalteiler mit $N \subseteq H$, so dass nach (a)

$$\overline{H} = \underbrace{{}^{H}\!/_{N}}_{\pi(H)} \trianglelefteq \underbrace{{}^{G}\!/_{N}}_{\pi(G)}$$

ein Normalteiler ist. Betrachte den verketteten Gruppenautomorphismus

$$\varphi : G \xrightarrow[g \longmapsto gN]{\pi} {}^{G}\!/_{N} \xrightarrow[\overline{g} \longmapsto \overline{g}\overline{H}]{\pi'} \left({}^{G}\!/_{N}\right)\Big/\left({}^{H}\!/_{N}\right)$$

π, π' sind surjektive Gruppenhomomorphismen nach Satz 44(d) $\implies$ die Verkettung φ ist ein surjektiver Gruppenhomomorphismus.

Nach Homomorphiesatz für Gruppen bleibt zu zeigen: $\mathrm{Kern}(\varphi) = H$:

$$g \in \mathrm{Kern}(\varphi) \underset{\pi'(\pi(g))=e}{\iff} \pi(g) \in \mathrm{Kern}(\pi') \iff gN \in {}^{H}\!/\!{}_{N}$$

$$\iff gN \subseteq H \underset{N \leq H}{\iff} g \in H.$$

□

(Semi-)direkte Produkte

Lemma 1.52 (Übung). *Seien $(G_1, e_1, \circ_1)$ und $(G_2, e_2, \circ_2)$ Gruppen, dann ist $G = (G_1 \times G_2, (e_1, e_2), \circ)$ eine Gruppe mit*

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 \circ h_1, g_2 \circ h_2)$$

Analog für $k \geq 2$ Faktoren. Dabei sind $G_1 \times \{e_2\} \trianglelefteq G$ und $\{e_1\} \times G_2 \trianglelefteq G$ Nullteiler von G.

Definition 1.53 (**Direktes Produkt**). Die Gruppe G aus Lemma 52 heißt das direkte Produkt von G_1 und G_2, Notation $G_1 \times G_2$.

Beispiel.

$$(\mathbb{R}^n, \underline{0}, +) = (\mathbb{R}, 0, +) \times \cdots \times (\mathbb{R}, 0, +) = \bigtimes_{i=1}^{n} (\mathbb{R}, 0, +)$$

Proposition 1.54. *Sei G eine Gruppe, seien $N_1, N_2 \trianglelefteq G$ Nullteiler mit $N_1 \cap N_2 = \{e\}$, dann gelten:*

(a) $\forall n_1 \in N_1, n_2 \in N_2 : n_1 n_2 = n_2 n_1$

(b) $N_1 N_2 \trianglelefteq G$ *ist ein Normalteiler in* G

(c) $\psi : N_1 \times N_2 \to N_1 N_2, (n_1, n_2) \mapsto n_1 n_2$ *ist ein Gruppenisomorphismus. (Insbesondere gilt $\# N_1 N_2 = \# N_1 \# N_2$)*

Zusatz: Gilt $G = N_1 N_2$, so folgt $G \cong N_1 \times N_2$ via ψ.

Beweis. (a) Seien $n_1 \in N_1, n_2 \in N_2$, setze $x = n_1 n_2 n_1^{-1} n_2^{-1}$. Nun:

$$x = (n_1 n_2 n_1^{-1}) n_2^{-1} \in (n_1 N_2 n_1^{-1}) N_2 \subseteq N_2 N_2 = N_2$$

analog

$$x = n_1 (n_2 n_1^{-1} n_2^{-1}) \in N_1 (n_2 N_1 n_2^{-1}) \overset{N_2 \trianglelefteq G}{\subseteq} N_1 N_1 = N_1$$

damit ist $x \in N_1 \cap N_2 = \{e\} \implies x = e \implies n_1 n_2 = n_2 n_1$.

(b) Für $g \in G$:

$$g N_1 N_2 g^{-1} = g N_1 g^{-1} g N_2 g^{-1} \subseteq N_1 N_2$$

(c) ψ ist wohl-definiert: klar. ψ ein Gruppenhomomorphismus folgt aus (a)

$$\psi((n_1, n_2) \circ (n_1', n_2')) = \psi((n_1 \circ n_1', n_2 \circ n_2')) = n_1 n_1' n_2 n_2'$$

$$\underset{(a)}{=} n_1 n_2 n_1' n_2' = \psi(n_1, n_2) \circ \psi(n_1', n_2')$$

$\{(e, e)\} = \mathrm{Kern}(\psi)$:

$$\psi(n_1, n_2) = e \iff n_1 n_2 = e \iff n_1 = n_2^{-1} \in N_1 \cap N_2 = \{e\}$$

$$\iff n_1 = n_2 = e$$

$\mathrm{Bild}(\psi) = N_1 N_2$.

$\square$

Korollar 1.55 (Übung)**.** *Sei G eine endliche Gruppe. Seien $N_1, ..., N_k \trianglelefteq G$ Normalteiler von G und gelte:*

(i) $\forall i \neq j : \mathrm{ggT}(\#N_i, \#N_j) = 1$

(ii) $\prod_{j=1}^{k} \#N_j = \#G$

Dann ist

$$\psi : \bigtimes_{j=1}^{k} N_j \longrightarrow G, (n_1, ..., n_k) \longmapsto n_1 \cdot ... \cdot n_k = \prod_{j=1}^{k} n_j$$

ein Gruppenisomorphismus.

Übung. Spezialfall: $n = \prod_{i=1}^{k} p_i^{f_i}$ für $p_1, ..., p_k$ paarweise verschiedene Primzahlen, dann gilt:

$$\bigtimes_{i}^{k} \mathbb{Z}/_{(p_i^{f_i})} \cong \mathbb{Z}/_{(n)}$$

ist Folge von Korollar 55.

Lemma 1.56. *Seien $H = (H, e_H, \circ_H), N = (N, e_N, \circ_N)$ Gruppen und sei $\varphi : H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Definiere*

$$G := N \rtimes H := N \rtimes_\varphi H = (N \times H, \underbrace{(e_n, e_H)}_{=:e}, \circ)$$

mit $\circ$ der Verknüpfung auf G definiert durch

$$(n_1, h_1) \circ (n_2, h_2) = (n_1 \circ_N \varphi(h_1)(n_2), h_1 \circ_H h_2)$$

Dann ist G eine Gruppe und es gelten:

- $N' := \{(n, e_H) \mid n \in N\} \cong N$ *ist ein Normalteiler in G,*
- $H' := \{(e_N, h) \mid h \in H\} \cong H$ *ist eine Untergruppe von G,*
- $N'H' = G$ *und* $N' \cap H' = \{e\}$,

- *$G \to H, (n,h) \mapsto h$ ist ein Gruppenepimorphismus (surj.) mit Kern N'.*

Definition 1.57 (Semi-direktes Produkt). Die Gruppe $G = N \rtimes H$ heißt das semi-direkte Produkt von N mit H (bezüglich φ).

Satz 1.58. *Sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler, $H \leq G$ eine Untergruppe, dann gelten:*

(a) $\varphi : H \to \mathrm{Aut}(N), h \mapsto (\underbrace{c_h|_N : N \to N, n \mapsto hnh^{-1}}_{\text{Konjugation mit } h})$ ist wohl-definiert und ein Gruppenhomomorphismus.

(b) Gelten zusätzlich (i) $NH = G$, (ii) $N \cap H = \{e\}$, so ist

$$\psi : N \rtimes_\varphi H \to G, (n,h) \mapsto n \circ_G h$$

ein Gruppenisomorphismus.

Beweis. Siehe Jantzen, Schwermer - Algebra. □

Beispiele.

1. Seien $A_n = \mathrm{Kern}(\mathrm{sign} : S_n \to \{\pm 1\})$ die Untergruppe der geraden Permutationen und τ eine beliebige Transposition, dann gilt:
$$S_n \cong A_n \rtimes \{\mathrm{id}, \tau\}$$

2. V Sei ein endlich dimensionaler euklidischer Vektorraum und $\sigma \in \mathrm{O}(V)$ eine Spiegelung, dann gilt
$$\mathrm{O}(V) \cong \mathrm{SO}(V) \rtimes \{\mathrm{id}, \sigma\}$$

3. Sei K ein Körper, dann gilt
$$\mathrm{GL}_n(K) \cong \mathrm{SL}_n(K) \rtimes H \cong \mathrm{SL}_n(K) \rtimes K^\times$$
wobei
$$H = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \;\middle|\; a \in K^\times \right\} \cong K^\times$$

4. Sei $\sigma \in A_4$ ein 3-Zykel, z.B. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, und V ist die kleinsche Vierergruppe
$$V = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq A_4,$$
dann gilt
$$A_4 \cong V \rtimes \{\mathrm{id}, \sigma, \sigma^2\}$$

Beweis. (Übung) eventuell noch 12 Tage warten. □

Kapitel 2

Gruppen Strukturtheorie

2.1 Strukturtheorie zu Gruppen ("Einige Aussagen")

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

Definition 2.1 (**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 2.2 (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 2.3 (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

$$\overset{\text{Übung}}{\Longleftrightarrow} \forall g \in G \setminus \{e\} : \exists x \in X : \underbrace{gX \neq X}_{\varphi_g(x) \neq \mathrm{id}_X(x)}$$

Beispiel 2.4.

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 2.5. *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 2.6 (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 2.7 (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 2.8. *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 $g_1^{-1}g_2 \in \mathrm{Stab}_G(x)$

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

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 2.9 (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 2.10. 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 2.11. *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) $\#X = \#X^G + \sum_{i\in\{1,\ldots,n\}} \underbrace{[G : G_{x_i}]}_{=\#G\cdot x}$

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 2.12 (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 2.13 (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 2.14. *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 :

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

Übung 2.15 (Satz von Cauchy)**.** (?) Sei p eine Primzahl und G endlich, dann gilt:

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

($\implies$ $\#G$ 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!

2.2 Permutationsgruppen

Sei $n \in \mathbb{N}$, $S_n = \mathrm{Bij}(\{1, ..., n\})$, 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 2.16. $\#S_n = n!$

Beweis. (Übung) Betrachte die möglichen "Wertetabellen" für Permutationen. □

Definition 2.17. Für $\sigma, \tau \in S_n$ definiere

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

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

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

Lemma 2.18 (Andere Interpretation des Trägers)**.** *Sei $\sigma \in S_n$, dann gilt für die Wirkung von $\langle\sigma\rangle$:* $\mathrm{supp}(\sigma) =$ *Vereinigung der Bahnen von $\langle\sigma\rangle$ auf $\{1, ..., n\}$ der Länge ≥ 2.*

Beweis.

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

□

Korollar 2.19. *Für $\sigma \in S_n$ gelten:*

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

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

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

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

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

□

Lemma 2.20. *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 $\sigma(\tau(i)) = \sigma(i) = i = \tau(i) = \tau(\sigma(i))$. □

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

Definition 2.21. 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 2.22 (**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 $I_{j'} \cap I_j = \emptyset$)

$$\Longrightarrow \sigma(i) = \sigma_j(i) \overset{(*)}{=} \Big(\sigma_j \cdot \textstyle\prod_{j' \neq j} \sigma_{j'}\Big)(i)$$

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

- Fall 0 : $i \in \{1, ..., n\} \setminus \bigcup_{j \in \{1, \ldots, t\}} I_j$. 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:

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

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

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

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

(d) (Übung). $\square$

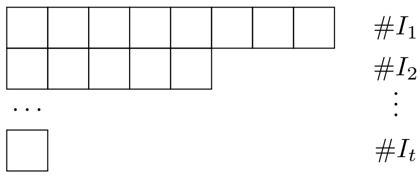
Beispiel 2.23.

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

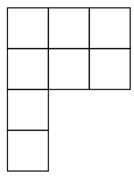
$\Longrightarrow$ $\langle\sigma\rangle$-Bahnen: $\{1,2,5\}, \{3,8,7\}, \{4\}, \{6\}$ und $\sigma = (1\ 2\ 5)(3\ 8\ 7)$

Definition 2.24 (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)

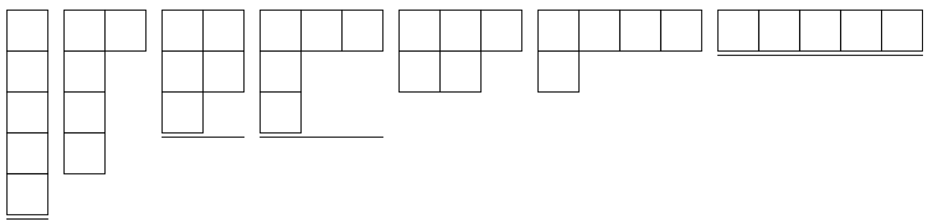
Satz 2.25 (Übung)**.**

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

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

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

Proposition 2.26 (Formeln für sgn)**.** *(Übung)*

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

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

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

Lemma 2.27. *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.

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

(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 $\#\{a, b, c\} = 3, a, b, c \in \{1, \ldots, n\}$.

$$\tau\tau' = (a\ b\ c) = \underset{\substack{a \leftarrow b \leftarrow c \\ c \leftarrow c \leftarrow b \\ b \leftarrow a \leftarrow a}}{(a\ b)(b\ c)}$$

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

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

(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.)

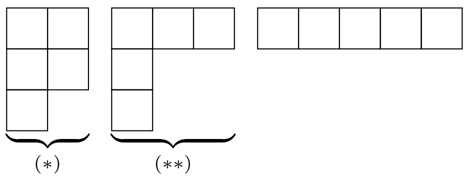
□

Definition 2.28 (**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 2.29. *Für $n \geq 5$ ist A_n einfach.*

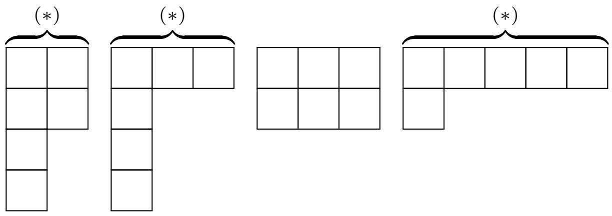
Beweis. Sei $N \trianglelefteq A_n$ ein Normalteiler und $\{e\} \subsetneq N$ und sei $\sigma \in N \setminus \{e\}$.

- $n = 5$:



$(*)$ 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 σ = 5-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)

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

  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:

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

  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) $\mathrm{SL_n}(K)/Z(\mathrm{SL_n}(K))$ bis auf einige kleine $\#K$ sind einfach (endlich falls K endlich).
  (ii) Weitere Untergruppen von $\mathrm{SL_n}$, welche zu “linearen algebraischen Gruppen” korrespondieren.
- 26 weitere.

2.3 Sylow Theoreme

Satz 2.30 (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 $\mathbb{N} \ni u \equiv 1 \mod p$.