Lineare Algebra I

Woche 05

10.11.2025 und 11.11.2025

§ 7.2 Gruppen

Gruppe

Definition 7.21

Ein Monoid $(H, \star)$ heißt eine **Gruppe**, wenn jedes Element aus H ein Inverses besitzt.

Beispiel 7.22

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind Gruppen.

2. $(\mathbb{Q}_{\neq 0}, \cdot)$, $(\mathbb{R}_{\neq 0}, \cdot)$ und $(\mathbb{C}_{\neq 0}, \cdot)$ sind Gruppen.

Gruppe

Beispiel 7.22 $(\mathbb{Z}_m, +_m)$ add. Gr. mod m !

3. Für $m \in \mathbb{N}$ bildet die Menge $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ mit der Verknüpfung $+_m$ (**Addition modulo m**) eine Gruppe.

Fall $m=2$ bereits bekannt (Beispiel 7.2)

Folie 08

$+_m$	0	1	$\cdots$	$m-1$
0	0	1	$\cdots$	$m-1$
1	1	2	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$		1
$m-1$	$m-1$	0	1	$\cdots$

4. Für $m \in \mathbb{N}$ bildet die Menge $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ mit der Verknüpfung $\cdot_m$ (**Multiplikation modulo m**) keine Gruppe außer im Fall $m = 1$.

$m=1$

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

mult. Monoid $(\mathbb{Z}_m, \cdot_m)$

Gruppe

Beispiel 7.22

z.B. $X \to (\mathbb{Q}, +)$

5. Ist X eine Menge und $(G, \star)$ eine Gruppe, dann ist $(G^X, \star)$ eine Gruppe. Inverses Element in $(G^X, *)$ zu $f: X \to G$:
$f': X \to G$ mit $f'(x) := f(x)'$
$(f' * f)(x) = f'(x) * f(x) = f(x)' * f(x) = e$
$(f * f')(x) \quad - \quad - \quad = e$
6. $(X^X, \circ)$ ist keine Gruppe, sobald X zwei oder mehr Elemente hat.
denn dann ex. nicht-bijektive Funktionen!

   Wenn X jedoch null- oder einelementig ist, dann ist $(X^X, \circ)$ eine Gruppe.

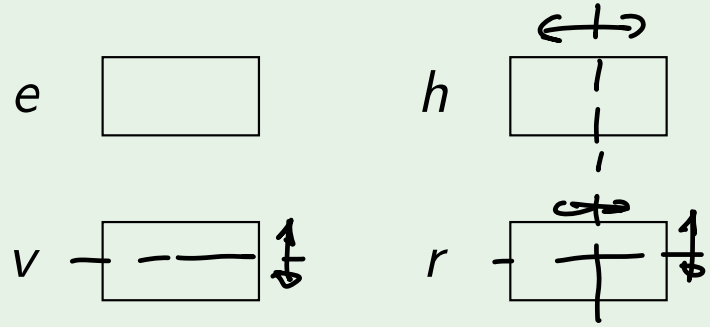
Beispiel 7.22

7. Die **Kleinsche Vierergruppe** K_4 ist eine kommutative Gruppe mit vier Elementen und der folgenden Verknüpfungstafel:

$\circ$	e	h	v	r
e	e	h	v	r
h	h	e	r	v
v	v	r	e	h
r	r	v	h	e

Jedes El. ist selbstinvers.

K_4 kann verstanden werden als die Symmetriegruppe eines Rechtecks:



Einheitengruppe eines Monoids

Lemma 7.23

Es sei $(H, \star)$ ein Monoid. Dann ist das Untermonoid der invertierbaren Elemente

$$E := \{a \in H \mid a \text{ ist invertierbar}\}$$

eine Gruppe, genannt die **Einheitengruppe** von $(H, \star)$.

Beweis. Lemma 7.16 : E ist Untermonoid von $(H, \star)$. Alle El. von E sind nach Vor. invertierbar, also ist E sogar eine Gruppe.

Einheitengruppe eines Monoids

Beispiel 7.24

1. $(\mathbb{Q}_{\neq 0}, \cdot)$, $(\mathbb{R}_{\neq 0}, \cdot)$ bzw. $(\mathbb{C}_{\neq 0}, \cdot)$ sind die Einheitengruppen der Monoide $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ bzw. $(\mathbb{C}, \cdot)$.

2. Es sei X eine Menge und $(H, \star)$ ein Monoid. Die Einheitengruppe von $(H^X, \star)$ besteht genau aus denjenigen Funktionen $X \to H$, die nur Funktionswerte in der Einheitengruppe von H annehmen.
   Inverse zu $f: X \to H$ ist $f^{-1}: X \to H$ mit
   $f^{-1}(x) := f(x)^{-1}$

3. Es sei X eine Menge. Die Einheitengruppe des Monoids $(X^X, \circ)$ besteht genau aus den invertierbaren (bijektiven) Funktionen $X \to X$.
   Inverse zu $f: X \to X$ ist $f^{-1}: X \to X$.

Gruppenkriterium mit Translationen („Sudoku-Kriterium“)

notwendiges Kriterium

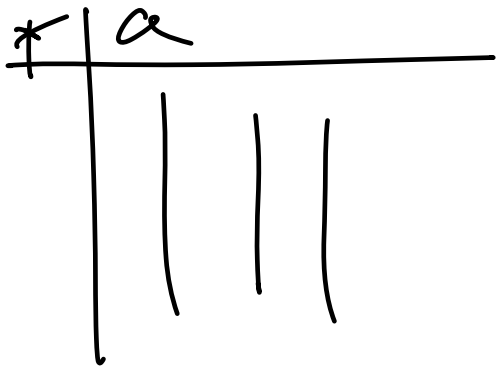
Lemma 7.25

1. Ist $(G, \star)$ eine Gruppe, so sind alle Rechtstranslationen $\star_a$ und alle Linkstranslation ${}_a\star$ bijektive Abbildungen $G \to G$.

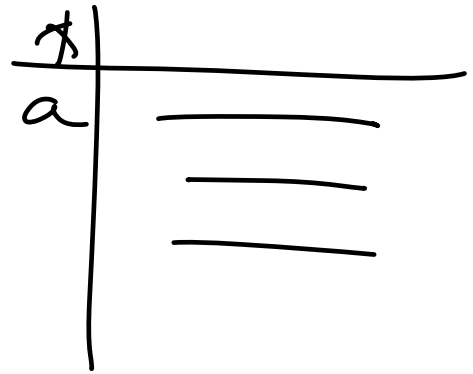
hinreichendes Kriterium

2. Ist $(H, \star)$ eine Halbgruppe mit $H \neq \emptyset$ und sind alle Rechtstranslationen $\star_a$ und alle Linkstranslationen ${}_a\star$ surjektive Abbildungen, dann ist $(H, \star)$ eine Gruppe.

Das gilt auch für unendliche Mengen!



pro Spalte eine Rechtstr.



pro Zeile eine Lchtstr

Gruppenkriterium mit Translationen

Beispiel 7.26

Ist die Menge $\{\heartsuit, \boxtimes, \CIRCLE, \otimes, \blacklozenge, \rhd\}$ mit den Verknüpfungen $\star$ bzw. $\square$ eine Gruppe? (Assoziativität wurde bereits geprüft und bestätigt.)

$\star$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\blacklozenge$	$\CIRCLE$	$\rhd$	$\heartsuit$	$\otimes$	$\blacklozenge$	$\boxtimes$
$\boxtimes$	$\heartsuit$	$\otimes$	$\CIRCLE$	$\rhd$	$\boxtimes$	$\blacklozenge$
$\heartsuit$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\CIRCLE$	$\blacklozenge$	$\heartsuit$	$\rhd$	$\boxtimes$	$\CIRCLE$	$\otimes$
$\otimes$	$\rhd$	$\boxtimes$	$\blacklozenge$	$\heartsuit$	$\otimes$	$\CIRCLE$
$\rhd$	$\otimes$	$\blacklozenge$	$\boxtimes$	$\CIRCLE$	$\rhd$	$\heartsuit$

In jeder Zeile und jeder Spalte kommen alle Elemente vor. Gruppe ✓

$\square$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\blacklozenge$	$\blacklozenge$	$\CIRCLE$	$\heartsuit$	$\blacklozenge$	$\heartsuit$	$\CIRCLE$
$\boxtimes$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
$\CIRCLE$	$\CIRCLE$	$\blacklozenge$	$\heartsuit$	$\CIRCLE$	$\heartsuit$	$\blacklozenge$
$\otimes$	$\otimes$	$\CIRCLE$	$\boxtimes$	$\heartsuit$	$\heartsuit$	$\otimes$
$\rhd$	$\rhd$	$\blacklozenge$	$\otimes$	$\CIRCLE$	$\heartsuit$	$\boxtimes$

keine Gruppe

Gruppenkriterium mit Translationen

Assoziativität der Verknüpfung ist Voraussetzung für die Anwendung des Gruppenkriteriums! Die Menge $\{\heartsuit, \boxtimes, \CIRCLE\}$ mit der Verknüpfung $\star$

$\star$	$\heartsuit$	$\boxtimes$	$\CIRCLE$
$\heartsuit$	$\CIRCLE$	$\boxtimes$	$\heartsuit$
$\boxtimes$	$\heartsuit$	$\CIRCLE$	$\boxtimes$
$\CIRCLE$	$\boxtimes$	$\heartsuit$	$\CIRCLE$

ist keine Gruppe, da $\star$ nicht assoziativ ist!

$$(\heartsuit \star \heartsuit) \star \boxtimes = \CIRCLE \star \boxtimes = \heartsuit$$
$$\heartsuit \star (\heartsuit \star \boxtimes) = \heartsuit \star \boxtimes = \boxtimes$$

Kommutativität

Definition 7.27

1. Es sei M eine Menge mit einer Verknüpfung $\star$. Die Elemente $a, b \in M$ **vertauschen** oder **kommutieren** bzgl. der Verknüpfung $\star$, wenn $a \star b = b \star a$ gilt.

2. Die Verknüpfung $\star$ auf der Menge M heißt **kommutativ** oder **abelsch**, wenn $a \star b = b \star a$ für alle $a, b \in M$ gilt.

3. Eine Halbgruppe bzw. ein Monoid bzw. eine Gruppe $(H, \star)$ heißt **kommutativ** oder **abelsch**, wenn die Verknüpfung $\star$ kommutativ ist.

§ 7.3 Die symmetrische Gruppe

die symmetrische Gruppe

Definition 7.30

Es sei X eine Menge und $S(X) := \{f : X \to X \mid f \text{ ist bijektiv}\}$.

1. $(S(X), \circ)$ heißt die **symmetrische Gruppe** auf X.

   Jedes Element von $S(X)$ heißt eine **Permutation** von X.

2. Ist $X = [\![1, n]\!]$ für $n \in \mathbb{N}_0$, so schreiben wir statt $S([\![1, n]\!])$ auch S_n und sprechen von der **symmetrischen Gruppe vom Grad n**.

   Jedes $\sigma \in S_n$ heißt eine **Permutation** von $[\![1, n]\!]$.

$\#S_n = n!$ für $n \in \mathbb{N}_0$

Darstellung einer Permutation $\sigma \in S_n$ durch Angabe der Funktionswerte:

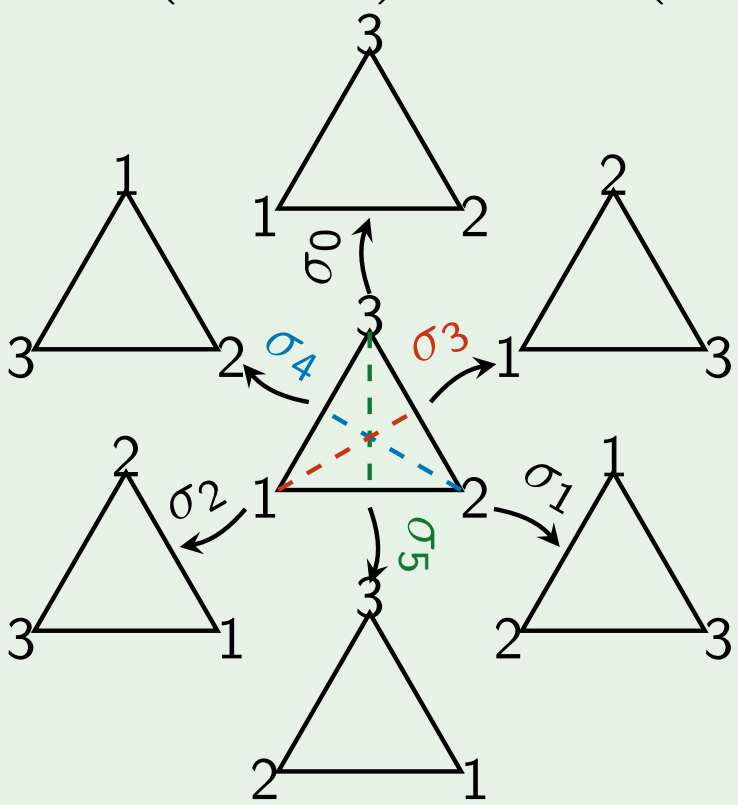
$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

die symmetrische Gruppe vom Grad 3

Beispiel 7.31

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$ Drehungen

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$ Spiegelungen



$\sigma_4 \circ \sigma_3 = \sigma_2$

$\sigma_3 \circ \sigma_4 = \sigma_1$

S_3 ist nicht kommutativ!

Transpositionen sind die Bausteine aller Permutationen

gibt es nur bei $n \geq 2$

Definition 7.32

Eine Permutation $\sigma \in S_n$, $n \in \mathbb{N}$, heißt eine **Transposition**, wenn sie genau zwei Elemente von $[\![1, n]\!]$ vertauscht und den Rest unverändert lässt:

Es gibt also Zahlen $i, j \in [\![1, n]\!]$ mit $i \neq j$, sodass $\sigma(i) = j$ und $\sigma(j) = i$ gilt und ansonsten $\sigma(k) = k$.

Wir schreiben dann $\sigma = \tau(i, j)$.

Es gibt $\binom{n}{2} = \frac{1}{2} n(n-1)$ verschiedene Transpositionen.

Transpositionen sind selbstinvers: $\tau^2 = \mathrm{id}$

Satz 7.33

Es sei $n \in \mathbb{N}_0$. Jede Permutation $\sigma \in S_n$ lässt sich als Komposition von $0 \leqslant r \leqslant n - 1$ Transpositionen schreiben (bzw. $r = 0$ im Fall $n = 0$).

schwache Schranke

Zerlegung in Transpositionen

Beispiel 7.34: $n = 4$, $r = n - 1 = 3$ Transpositionen benötigt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \xrightarrow{\tau(4,1)\circ} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\xrightarrow{\tau(3,1)\circ} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\xrightarrow{\tau(2,1)\circ} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\tau(2,1) \circ \tau(3,1) \circ \tau(4,1) \circ \sigma = \mathrm{id}$$

$$\sigma = \tau(4,1) \circ \tau(3,1) \circ \tau(2,1)$$

Fehlstand und Signum einer Permutation

Definition 7.35

Es sei $n \in \mathbb{N}_0$ und σ eine Permutation in S_n.

1. Ein Indexpaar $(i, j) \in [\![1, n]\!]^2$ heißt ein **Fehlstand** von σ, wenn $i < j$ und $\sigma(i) > \sigma(j)$ gilt.
2. Das **Signum** von σ ist definiert als die Zahl

$$\operatorname{sgn} \sigma := \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \mathbb{Q}, \quad \in \{\pm 1\}$$

Beispiel 7.36

Fehlst. $(1,2), (1,3), (2,3)$

$$\operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \frac{2-3}{2-1} \cdot \frac{1-3}{3-1} \cdot \frac{1-2}{3-2}$$

$$= (-1)^3 = -1$$

Eigenschaften von Signum

Bemerkung 7.37, Lemma 7.38 und Satz 7.40

Es sei $n \in \mathbb{N}_0$ und σ eine Permutation in S_n.

- $\operatorname{sgn}\sigma = (-1)^{\text{Anzahl der Fehlstände von } \sigma} =:$ **Parität von σ**
- σ heißt eine **gerade Permutation** im Fall $\operatorname{sgn}\sigma = 1$.
  σ heißt eine **ungerade Permutation** im Fall $\operatorname{sgn}\sigma = -1$.
- $\operatorname{sgn}\mathrm{id} = 1$
- $\operatorname{sgn}\tau = -1$ für jede Transposition τ
- $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = (\operatorname{sgn}\sigma_1) \cdot (\operatorname{sgn}\sigma_2)$

sgn ist verträglich mit $\circ$ und $\cdot$

- $\sigma = \tau_1 \circ \cdots \circ \tau_r$ (Komposition von $r \in \mathbb{N}_0$ Transpositionen in S_n) impliziert $\operatorname{sgn}\sigma = (-1)^r$

§ 7.4 Untergruppen

Untergruppe

Definition 7.42

Es sei $(G, \star)$ eine Gruppe.

UG

1. Eine Teilmenge $U \subseteq G$ heißt eine **Untergruppe von** $(G, \star)$, wenn U bzgl. $\star$ abgeschlossen und wenn $(U, \star)$ selbst wieder eine Gruppe ist. Manchmal schreibt man dies als $(U, \star) \leqslant (G, \star)$.

   kurz: $U * U \subseteq U$

2. Eine Untergruppe $(U, \star)$ von $(G, \star)$ heißt **echt**, wenn $U \subsetneq G$ gilt.

Es muss nicht gefordert werden, dass e dasselbe ist!

Lemma 7.43

Es sei U eine Untergruppe der Gruppe $(G, \star)$. Dann ist das neutrale Element e_U von $(U, \star)$ gleich dem neutralen Element e von $(G, \star)$. Außerdem gilt für alle $a \in U$, dass das Inverse von a in U übereinstimmt mit dem Inversen von a in G.

Übung! Konsequenz: schreibe e und $^{-1}$

Untergruppenkriterium

Satz 7.44

Es sei $(G, \star)$ eine Gruppe und $U \subseteq G$.

Dann sind äquivalent:

1. $(U, \star)$ ist eine Untergruppe von $(G, \star)$.
2. $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a \star b' \in U$.

Beweis. (1) $\Rightarrow$ (2)

$U \neq \emptyset$, denn jede Gr. enthält ein neutrales Element.

$a, b \in U \Rightarrow b' \in U$.

U ist bzgl. $\star$ abgeschlossen:

$\Rightarrow \quad a \star b' \in U$.

Untergruppenkriterium

Satz 7.44

Es sei $(G, \star)$ eine Gruppe mit dem neutralen Element e sowie $U \subseteq G$.

Dann sind äquivalent:

1. $(U, \star)$ ist eine Untergruppe von $(G, \star)$.
2. $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a \star b' \in U$.

Beweis. ② ⇒ ①

- U enthält ein $a \in U \subseteq G$. Nach Vor. enthält U auch $e = a * a' \in U$, also $\boxed{e \in U}$
- $\boxed{U' \subseteq U}$, denn $b \in U \Rightarrow b' = e * b' \in U$
- $\boxed{U * U \subseteq U}$, denn für $a, b \in U \Rightarrow b' \in U$
  $\Rightarrow a * b = a * (b')' \in U$.

Untergruppe

Prüfung durch UG-Kriterium:

Beispiel 7.45

1. Es sei $(G, \star)$ eine Gruppe mit dem neutralen Element e. Dann sind $(\{e\}, \star)$ und $(G, \star)$ die **trivialen Untergruppen** von $(G, \star)$.

   Minimum — Max. alle UG von G bzgl. $\leq$ und $\subseteq$

2. $(\mathbb{Q}_{>0}, \cdot)$ ist eine Untergruppe von $(\mathbb{Q}_{\neq 0}, \cdot)$.

   $\neq \emptyset$ und $a \cdot b^{-1} \in \mathbb{Q}_{>0}$

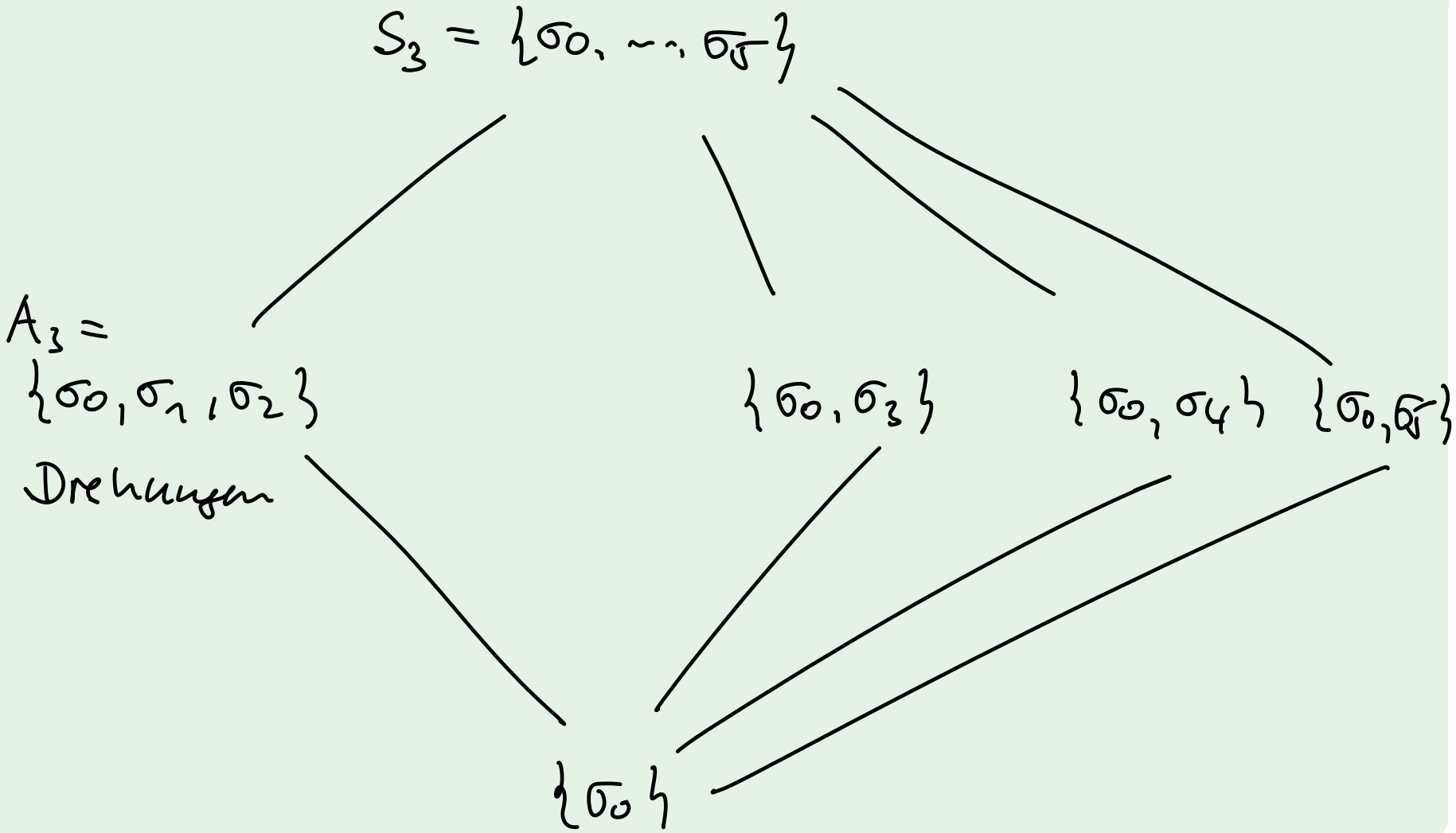
3. Für jedes $m \in \mathbb{N}$ ist $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$ eine Untergruppe der Gruppe $(\mathbb{Z}, +)$. $\neq \emptyset$

   $mz_1 + (-mz_2) = m(z_1 - z_2) \in m\mathbb{Z}$

   Kommutation — Komm. von $+$ — $z_1 + \dots + z_1$ (m-mal)

Untergruppe

alle Untergruppen von S_3



„Untergruppe sein“ ist Ordnungsrelation

Bemerkung 7.46

1. Die Menge aller Untergruppen einer Gruppe $(G, \star)$ ist durch die Untergruppenhalbordnung partiell geordnet. Diese Ordnung stimmt mit der Inklusionshalbordnung überein.

2. Ist $U \subseteq H$ ein Untermonoid des Monoids $(H, \star)$ und ist $(U, \star)$ zusätzlich eine Gruppe, dann sprechen wir auch kurz von einer **Untergruppe** $(U, \star)$ **des Monoids** $(H, \star)$.

   Das trifft genau dann zu, wenn $(U, \star)$ eine Gruppe ist und das neutrale Element $e \in H$ enthält.

3. Die Einheitengruppe E eines Monoids $(H, \star)$ ist die größte Untergruppe von $(H, \star)$:
   E ist Max. von $\{U \leq H \mid U \text{ ist UG von } (H,*)\}$ bzgl. $\leq$ und $\subseteq$
   Alle weiteren Untergruppen von $(H, \star)$ sind also Teilmengen (und sogar Untergruppen) von E.

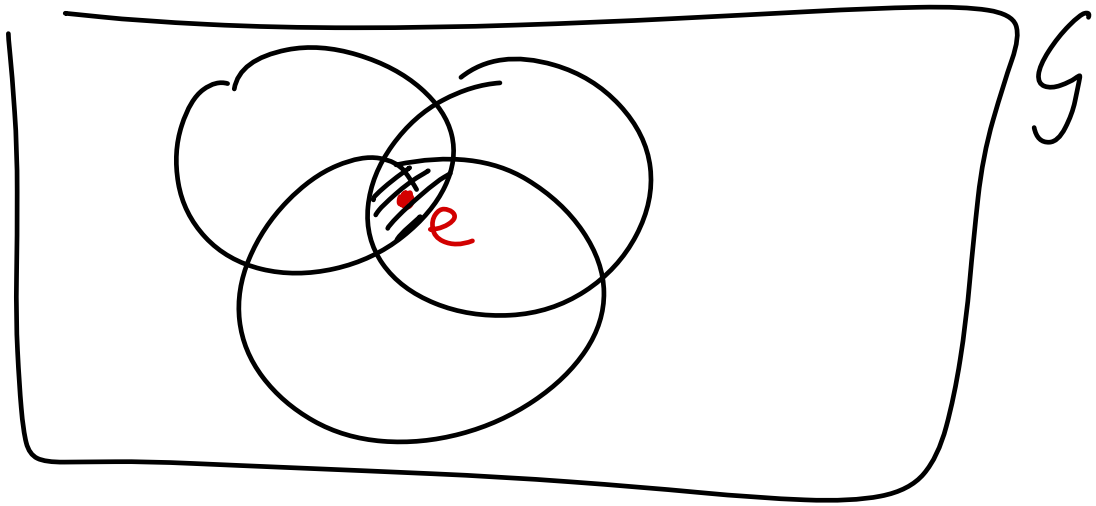
Durchschnitt von Untergruppen

Lemma

Es sei $(G, \star)$ eine Gruppe und $(U_i, \star)_{i \in I}$ eine nichtleere Familie von Untergruppen.

Dann ist auch $\bigcap_{i \in I} U_i$ mit $\star$ eine Untergruppe von $(G, \star)$.

Beweis. Übung



Hüllenbildung: erzeugte Untergruppe

Definition 7.48

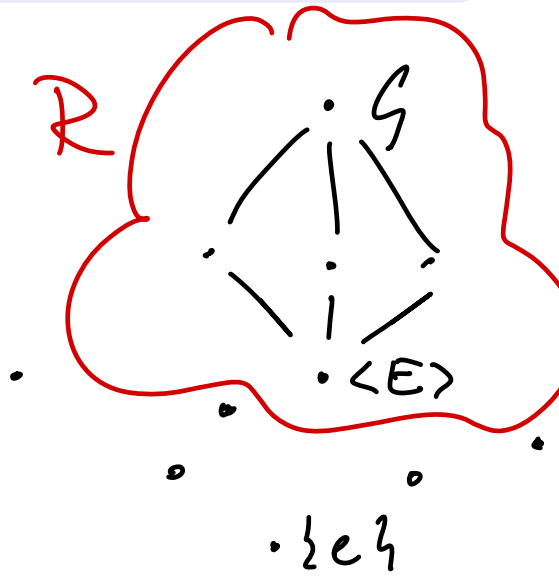
Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$.

Die Menge

$$\langle E \rangle := \bigcap \underbrace{\{U \mid U \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U\}}_{\mathcal{R}}$$

heißt die **von E erzeugte Untergruppe in $(G, \star)$**.

$\langle E \rangle$ ist das Minimum von $\mathcal{R}$ in der Menge aller UG von $(G, *)$ bzgl. $\leq$ (und $\subseteq$)



Wie berechnen?

Darstellung der erzeugten Untergruppe

Satz 7.50

Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$.

Dann gilt für die von E erzeugte Untergruppe:

$$\langle E \rangle = \left\{ a_1 \star \cdots \star a_n \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1, \ldots, n \, (a_i \in E \cup E') \right\}$$

$\langle \{a_1, a_2\} \rangle = \langle a_1, a_2 \rangle$

$n = 0$: e

$n = 1$: a_1, a_2, a_1', a_2'

$n = 2$: $a_2 * a_2$ $a_2 * a_1'$, $a_2 * a_2$, ...

i. A. nicht alle verschieden

Darstellung der erzeugten Untergruppe

$$\langle E\rangle := \bigcap \overbrace{\{U \mid (U,\star) \text{ ist Untergruppe von } (G,\star) \text{ und } E \subseteq U\}}^{\mathcal{R}} =: \bigcap \mathcal{R}$$

$$M := \{a_1 \star \cdots \star a_n \mid \exists n \in \mathbb{N}_0 \; \forall i = 1,\dots,n \; (a_i \in E \cup E')\}$$

Beweis. $M \subseteq \langle E\rangle$: Es sei $U \in \mathcal{R}$ beliebig.

Wir zeigen $M \subseteq U$ per Induktion nach $n \in \mathbb{N}_0$:

$n=0$: $e \in U$ ✓ da U UG und $E \subseteq U$

$n=1$: $a_1 \in E \cup E' \subseteq U$

Ind. schritt: $a_1 * \cdots * a_n * a_{n+1}$

$= (\underbrace{a_1 * \cdots * a_n}_{\in U}) * \underbrace{a_{n+1}}_{\in E \cup E' \subseteq U} \in U$, da U UG

$\Rightarrow M \subseteq \bigcap \mathcal{R} = \langle E\rangle$.

Darstellung der erzeugten Untergruppe

$$\langle E\rangle := \bigcap\left\{U \,\middle|\, (U,\star) \text{ ist Untergruppe von } (G,\star) \text{ und } E \subseteq U\right\} =: \bigcap \mathcal{R}$$

$$M := \left\{a_1 \star \cdots \star a_n \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1,\ldots,n \,(a_i \in E \cup E')\right\}$$

Beweis. $\langle E\rangle \subseteq M$:

Wir zeigen: M ist UG von G mit UG-Kriterium:

- $M \neq \emptyset$, denn $e \in M$ (für $n=0$).
- Sind $a_1 * \cdots * a_n$ und $b_1 * \cdots * b_m$ beide in M.

Dann ist auch $(a_1 * \cdots * a_n) * (b_1 * \cdots * b_m)'$
$= (a_1 * \cdots * a_n) * (b_m' * \cdots * b_1') \in M$

Außerdem $E \subseteq M$ ($n=1$). D.h. $M \in \mathcal{R}$.

Damit $\langle E\rangle = \bigcap \mathcal{R} \subseteq M$.

erzeugte Untergruppen in S_3

Beispiel 7.51

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{Drehungen}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{Spiegelungen}$$

$\langle\{\sigma_3\}\rangle = \{ \underbrace{\sigma_3^0}_{=\sigma_0=\mathrm{id}}, \sigma_3, \underbrace{\sigma_3^{-1}}_{=\sigma_3}, \underbrace{\sigma_3 \circ \sigma_3}_{=\sigma_0}, \dots \} = \{\sigma_0, \sigma_3\}$

$\langle\{\sigma_1\}\rangle = \{ \underbrace{\sigma_1^0}_{=\sigma_0}, \sigma_1, \underbrace{\sigma_1^{-1}}_{=\sigma_2}, \underbrace{\sigma_1 \circ \sigma_1}_{=\sigma_2}, \underbrace{\sigma_1 \circ \sigma_1^{-1}}_{=\sigma_0}, \dots \} = \{\sigma_0, \sigma_1, \sigma_2\}$

$\langle\{\sigma_1, \sigma_3\}\rangle = \dots = S_3$

zyklische Untergruppen

Definition 7.48

Die von einem einzelnen Element $a \in G$ erzeugte Untergruppe $\langle a \rangle$ heißt eine **zyklische Untergruppe von** $(G, \star)$.

Eine Gruppe $(G, \star)$ heißt **zyklisch** (**erzeugt**), wenn es ein Element $a \in G$ mit $G = \langle a \rangle$ gibt.

Beispiel 7.51

1. In der Gruppe $(\mathbb{Z}, +)$ erzeugt das Element $m \in \mathbb{Z}$ die zyklische Untergruppe $\langle m \rangle = m\,\mathbb{Z}$.

2. Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch. Sie hat die Erzeuger 1 und -1, es gilt also $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

§ 7.5 Untergruppen induzieren Äquivalenzrelationen

Links- und Rechtsnebenklassen einer Untergruppe

Definition 7.54

Es sei U eine Untergruppe der Gruppe $(G, \star)$. Für $a \in G$ heißt ...

1. $a \star U \subseteq G$ eine **Linksnebenklasse von U**
2. $U \star a \subseteq G$ eine **Rechtsnebenklasse von U**

Satz 7.55

Es sei $(G, \star)$ eine Gruppe, U eine Untergruppe und $a, b \in G$.

1. Die Linksnebenklassen $a \star U$ und $b \star U$ sind gleich oder disjunkt.
2. Die Rechtsnebenklassen $U \star a$ und $U \star b$ sind gleich oder disjunkt.

Beweis. ①: $a*U$, $b*U$ seien nicht disjunkt.
Es ex. $c \in (a*U) \cap (b*U)$. D.h. es ex. $u_1, u_2 \in U$ mit
$c = a*u_1 = b*u_2$. Für beliebiges $u \in U$ ist
$\Rightarrow a*u = a_1 * \underbrace{u_1 * u_1'}_{=e} * u = b*\underbrace{u_2 * u_1'}_{\in U} * u \in b*U$.
$\Rightarrow a*U \subseteq b*U$. Analog: $b*U \subseteq a*U$.

eine Untergruppe induziert zwei Äquivalenzrelationen

Folgerung 7.57

Es sei $(G, \star)$ eine Gruppe und U eine Untergruppe.

1. Folgende zwei Relationen sind Äquivalenzrelationen auf G:

$$a \sim^U b \quad \Leftrightarrow \quad a \star U = b \star U \quad \Leftrightarrow \quad b \in a \star U \quad \Leftrightarrow \quad a \in b \star U$$
$$a \,{}^U\!\sim b \quad \Leftrightarrow \quad U \star a = U \star b \quad \Leftrightarrow \quad b \in U \star a \quad \Leftrightarrow \quad a \in U \star b$$

   Die Faktormengen werden bezeichnet mit

$$G / U := G / \sim^U = \{a \star U \mid a \in G\}$$
$$U \setminus G := G / {}^U\!\sim = \{U \star a \mid a \in G\}$$

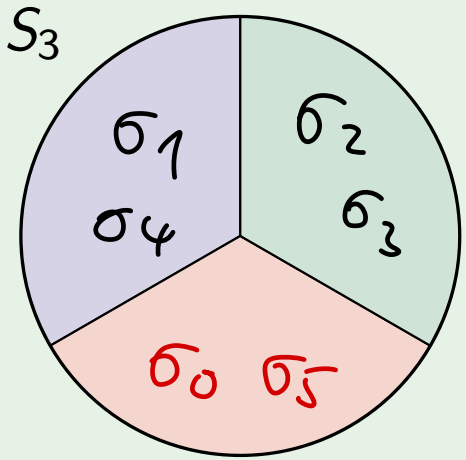
2. Jede der Äquivalenzklassen ist gleichmächtig zu U.

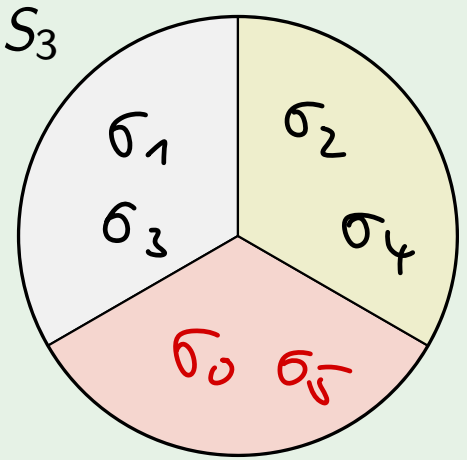
3. Ist L ein Repräsentantensystem der Linksnebenklassen, dann ist $R := L'$ ein Repräsentantensystem der Rechtsnebenklassen.

Links- und Rechtsnebenklassen in S_3

nicht kommutativ

Beispiel 7.59 zur Untergruppe $U = \{\sigma_0, \sigma_5\} \subseteq S_3$





$$\begin{aligned}\sigma_0 \circ U &= \{\sigma_0 \circ \sigma_0, \sigma_0 \circ \sigma_5\} \\ &= \{\sigma_0, \sigma_5\} \\ \sigma_1 \circ U &= \{\sigma_1 \circ \sigma_0, \sigma_1 \circ \sigma_5\} \\ &= \{\sigma_1, \sigma_4\} \\ \sigma_2 \circ U &= \{\sigma_2 \circ \sigma_0, \sigma_2 \circ \sigma_5\} \\ &= \{\sigma_2, \sigma_3\}\end{aligned}$$

$$\begin{aligned}U \circ \sigma_0 &= \{\sigma_0 \circ \sigma_0, \sigma_5 \circ \sigma_0\} \\ &= \{\sigma_0, \sigma_5\} \\ U \circ \sigma_1 &= \{\sigma_0 \circ \sigma_1, \sigma_5 \circ \sigma_1\} \\ &= \{\sigma_1, \sigma_3\} \\ U \circ \sigma_2 &= \{\sigma_0 \circ \sigma_2, \sigma_5 \circ \sigma_2\} \\ &= \{\sigma_2, \sigma_4\}\end{aligned}$$

Satz von Lagrange

Satz 7.60

Es sei $(G, \star)$ eine endliche Gruppe und U eine Untergruppe.

Dann gilt $\#U \mid \#G$.

Beweis. Übung

Gruppen mit Prim-Kardinalität sind zyklisch

Folgerung 7.61

Es sei $(G, \star)$ eine endliche Gruppe, deren Kardinalität eine Primzahl ist. Dann gilt:

1. G besitzt nur die trivialen Untergruppen $\{e\}$ und G.
2. G ist zyklisch, und jedes Element $a \in G \setminus \{e\}$ ist ein Erzeuger.
3. G ist abelsch.

Beweis.

1. Nach dem Satz von Lagrange 7.60 kommen als Kardinalität von U nur 1 oder $\#G$ in Frage.
2. Für $a \in G \setminus \{e\}$ ist $\langle a \rangle$ eine Untergruppe von G, die von $\{e\}$ verschieden ist. Es muss also $\langle a \rangle = G$ gelten.
3. Zyklisch erzeugte Gruppen sind immer abelsch.