

# Lineare Algebra I

## Woche 05

10.11.2025 und 11.11.2025

## § 7.2 Gruppen

## Definition 7.21

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

## Beispiel 7.22

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

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

## Beispiel 7.22

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

$+_m$	0	1	$\dots$	$m-1$
0				
1				
$\vdots$				
$m-1$				

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

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

## Beispiel 7.22

- 5 Ist  $X$  eine Menge und  $(G, \star)$  eine Gruppe, dann ist  $(G^X, \star)$  eine Gruppe.
  
- 6  $(X^X, \circ)$  ist **keine Gruppe**, sobald  $X$  zwei oder mehr Elemente hat.

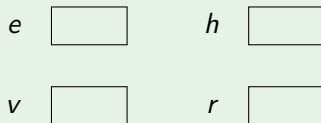
Wenn  $X$  jedoch null- oder einelementig ist, dann ist  $(X^X, \circ)$  eine Gruppe.

## Beispiel 7.22

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

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

$K_4$  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.

# 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  $X \rightarrow H$ , die nur Funktionswerte in der Einheitengruppe von  $H$  annehmen.
- ③ Es sei  $X$  eine Menge. Die Einheitengruppe des Monoids  $(X^X, \circ)$  besteht genau aus den invertierbaren (bijektiven) Funktionen  $X \rightarrow X$ .



# Gruppenkriterium mit Translationen („Sudoku-Kriterium“)

## Lemma 7.25

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

# Gruppenkriterium mit Translationen

## Beispiel 7.26

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

$\star$	$\boxtimes$	$\bullet$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\blacktriangleright$
$\blacklozenge$	$\bullet$	$\blacktriangleright$	$\heartsuit$	$\otimes$	$\blacklozenge$	$\boxtimes$
$\boxtimes$	$\heartsuit$	$\otimes$	$\bullet$	$\blacktriangleright$	$\boxtimes$	$\blacklozenge$
$\heartsuit$	$\boxtimes$	$\bullet$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\blacktriangleright$
$\bullet$	$\blacklozenge$	$\heartsuit$	$\blacktriangleright$	$\boxtimes$	$\bullet$	$\otimes$
$\otimes$	$\blacktriangleright$	$\boxtimes$	$\blacklozenge$	$\heartsuit$	$\otimes$	$\bullet$
$\blacktriangleright$	$\otimes$	$\blacklozenge$	$\boxtimes$	$\bullet$	$\blacktriangleright$	$\heartsuit$

$\square$	$\boxtimes$	$\bullet$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\blacktriangleright$
$\blacklozenge$	$\blacklozenge$	$\bullet$	$\heartsuit$	$\blacklozenge$	$\heartsuit$	$\bullet$
$\boxtimes$	$\boxtimes$	$\bullet$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\blacktriangleright$
$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
$\bullet$	$\bullet$	$\blacklozenge$	$\heartsuit$	$\bullet$	$\heartsuit$	$\blacklozenge$
$\otimes$	$\otimes$	$\bullet$	$\boxtimes$	$\heartsuit$	$\heartsuit$	$\otimes$
$\blacktriangleright$	$\blacktriangleright$	$\blacklozenge$	$\otimes$	$\bullet$	$\heartsuit$	$\boxtimes$

# Gruppenkriterium mit Translationen

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

$\star$	$\heartsuit$	$\boxtimes$	$\bullet$
$\heartsuit$	$\bullet$	$\boxtimes$	$\heartsuit$
$\boxtimes$	$\heartsuit$	$\bullet$	$\boxtimes$
$\bullet$	$\boxtimes$	$\heartsuit$	$\bullet$

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

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

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

## 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  $S(X) := \{f: X \rightarrow X \mid f \text{ ist bijektiv}\}$ .

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

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

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

Jedes  $\sigma \in S_n$  heißt eine **Permutation** von  $\llbracket 1, n \rrbracket$ .

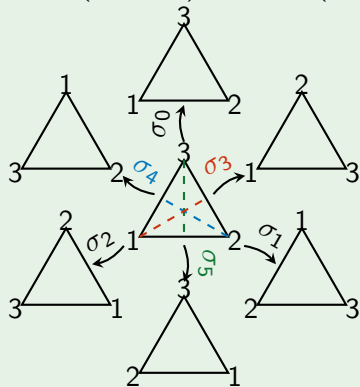
Darstellung einer Permutation  $\sigma \in S_n$  durch Angabe der Funktionswerte:

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

# die symmetrische Gruppe vom Grad 3

## Beispiel 7.31

$$\begin{array}{lll} \sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & \text{Drehungen} \\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & \text{Spiegelungen} \end{array}$$



# Transpositionen sind die Bausteine aller Permutationen

## Definition 7.32

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

Es gibt also Zahlen  $i, j \in \llbracket 1, n \rrbracket$  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 verschiedene Transpositionen.

Transpositionen sind

## Satz 7.33

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



# Zerlegung in Transpositionen

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

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

# Fehlstand und Signum einer Permutation

## Definition 7.35

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

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

$$\operatorname{sgn} \sigma := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

## Beispiel 7.36

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

## Bemerkung 7.37, Lemma 7.38 und Satz 7.40

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

- $\operatorname{sgn} \sigma = (-1)^{\text{Anzahl der Fehlstände von } \sigma} =:$  **Parität von  $\sigma$**
- $\sigma$  heißt eine **gerade Permutation** im Fall  $\operatorname{sgn} \sigma = 1$ .  
 $\sigma$  heißt eine **ungerade Permutation** im Fall  $\operatorname{sgn} \sigma = -1$ .
- $\operatorname{sgn} \operatorname{id} = 1$
- $\operatorname{sgn} \tau = -1$  für jede Transposition  $\tau$
- $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = (\operatorname{sgn} \sigma_1) \cdot (\operatorname{sgn} \sigma_2)$
- $\sigma = \tau_1 \circ \cdots \circ \tau_r$  (Komposition von  $r \in \mathbb{N}_0$  Transpositionen in  $S_n$ )  
impliziert  $\operatorname{sgn} \sigma = (-1)^r$

## § 7.4 Untergruppen

## Definition 7.42

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

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

## 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  $G$ .

## 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.

## 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  $a \star b^{-1} \in U$ .

Beweis.

## 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  $(G, \star)$ .
- ②  $(\mathbb{Q}_{>0}, \cdot)$  ist eine Untergruppe von  $(\mathbb{Q}_{\neq 0}, \cdot)$ .
- ③ Für jedes  $m \in \mathbb{N}$  ist  $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$  eine Untergruppe der Gruppe  $(\mathbb{Z}, +)$ .



## 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  $(H, \star)$ :

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

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

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

# 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:

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

# Darstellung der erzeugten Untergruppe

$$\langle E \rangle := \bigcap \{ U \mid (U, \star) \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U \} =: \bigcap \mathcal{R}$$
$$M := \{ a_1 \star \cdots \star a_n \mid \exists n \in \mathbb{N}_0 \, \forall i = 1, \dots, n (a_i \in E \cup E') \}$$

Beweis.

# Darstellung der erzeugten Untergruppe

$$\langle E \rangle := \bigcap \{ U \mid (U, \star) \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U \} =: \bigcap \mathcal{R}$$
$$M := \{ a_1 \star \cdots \star a_n \mid \exists n \in \mathbb{N}_0 \, \forall i = 1, \dots, n (a_i \in E \cup E') \}$$

Beweis.

## erzeugte Untergruppen in $S_3$

### Beispiel 7.51

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

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

$$\langle \{\sigma_3\} \rangle =$$

$$\langle \{\sigma_1\} \rangle =$$

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



# 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 ...

- ❶  $a \star U$  eine **Linksnebenklasse von  $U$**
- ❷  $U \star a$  eine **Rechtsnebenklasse von  $U$**

## Satz 7.55

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

- ❶ Die Linksnebenklassen  $a \star U$  und  $b \star U$  sind gleich oder disjunkt.
- ❷ Die Rechtsnebenklassen  $U \star a$  und  $U \star b$  sind gleich oder disjunkt.

Beweis.

# 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  $G$ :

$$a \sim^U b \Leftrightarrow a \star U = b \star U \Leftrightarrow b \in a \star U \Leftrightarrow a \in b \star U$$

$$a \stackrel{U}{\sim} b \Leftrightarrow U \star a = U \star b \Leftrightarrow b \in U \star a \Leftrightarrow a \in U \star b$$

Die Faktormengen werden bezeichnet mit

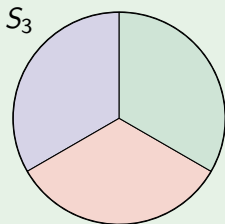
$$G / U := G / \sim^U = \{a \star U \mid a \in G\}$$

$$U \backslash G := G / \stackrel{U}{\sim} = \{U \star a \mid a \in G\}$$

- 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 $S_3$

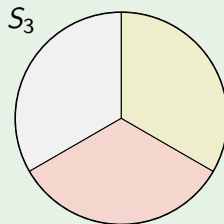
Beispiel 7.59 zur Untergruppe  $U = \{\sigma_0, \sigma_5\} \subseteq S_3$



$$\begin{aligned}\sigma_0 \circ U &= \{\sigma_0 \circ \sigma_0, \sigma_0 \circ \sigma_5\} \\ &= \{\sigma_0, \sigma_5\}\end{aligned}$$

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

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



$$\begin{aligned}U \circ \sigma_0 &= \{\sigma_0 \circ \sigma_0, \sigma_5 \circ \sigma_0\} \\ &= \{\sigma_0, \sigma_5\}\end{aligned}$$

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

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

# 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.