

UNIVERSITÄT
LEIPZIG

Algebra 1

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Erzeugendensysteme, Ordnung, zyklische Gruppen

3. Mehr über S_n

- Halbgruppe:

- Halbgruppe: Menge

- Halbgruppe: Menge mit

- Halbgruppe: Menge mit einer

- Halbgruppe: Menge mit einer assoziativen

- Halbgruppe: Menge mit einer assoziativen Verknüpfung

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid:

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe:

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität)

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c =$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle a,

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b,$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element)

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea =$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae =$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente)

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab =$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba =$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*,

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab =$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a,$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in$

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.
- Untergruppe,

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.
- Untergruppe, triviale

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.
- Untergruppe, triviale Untergruppe,

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.
- Untergruppe, triviale Untergruppe, richtige

- Halbgruppe: Menge mit einer assoziativen Verknüpfung
- Monoid: Halbgruppe mit der Einheit
- Gruppe: Monoid sodass alle Elemetne invertierbar sind
  - (Assoziativität) $(ab)c = a(bc)$ für alle $a, b, c \in G$.
  - (Neutrales Element) Es gibt $e \in G$ mit $ea = ae = a$ für alle $a \in G$.
  - (Inverse Elemente) Für jedes $a \in G$ gibt es $b \in G$ mit $ab = ba = e$.
- Eine Gruppe heißt *abelsch*, falls $ab = ba$ für alle $a, b \in G$.
- Untergruppe, triviale Untergruppe, richtige Untegruppe

Beispiele.

Beispiele.

- $GL(n,$

Beispiele.

- $GL(n, \mathbb{K})$

Beispiele.

- $GL(n, \mathbb{K})$ und

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen.

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$,

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$,

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$,

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B.

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) =$

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in$

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C}:$

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| =$

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$.

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch

Beispiele.

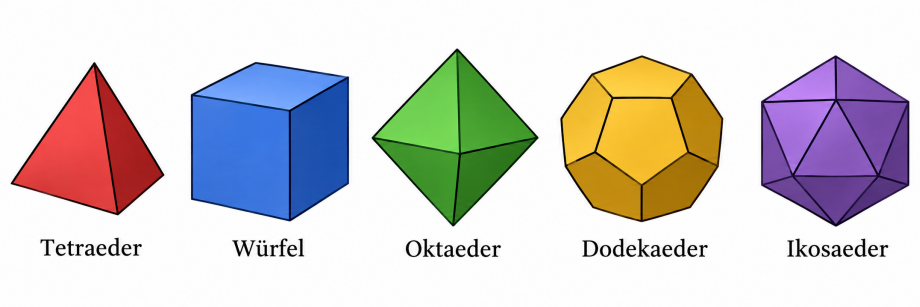
- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

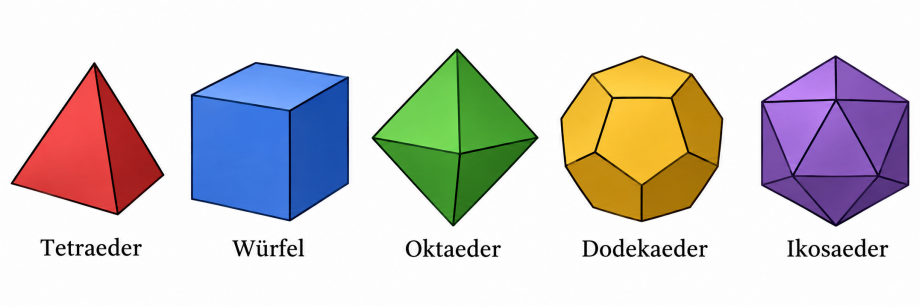
- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.



Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

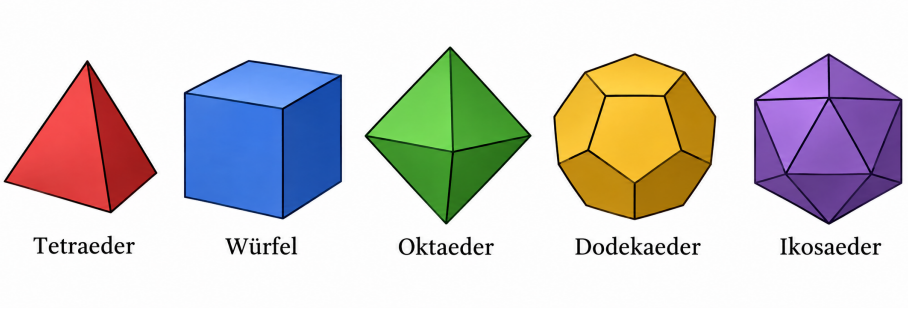


- die

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

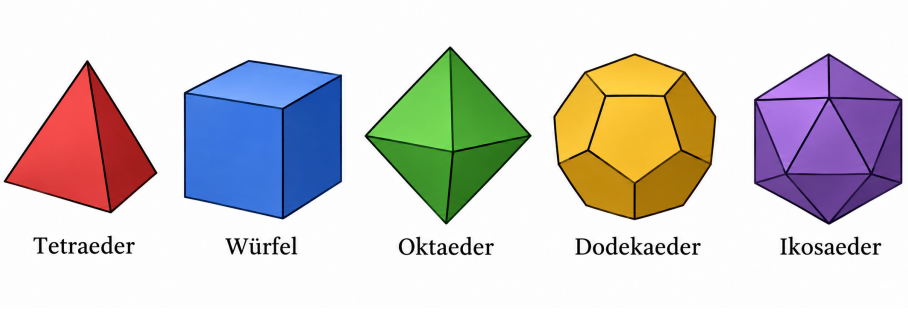


- die Gruppe

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

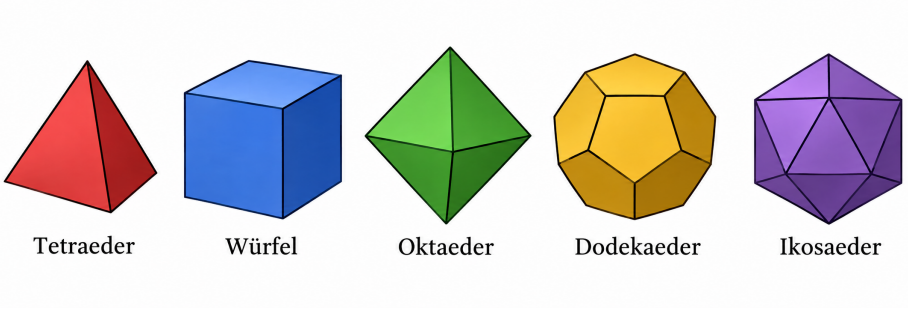
- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.



- die Gruppe aller

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.
- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

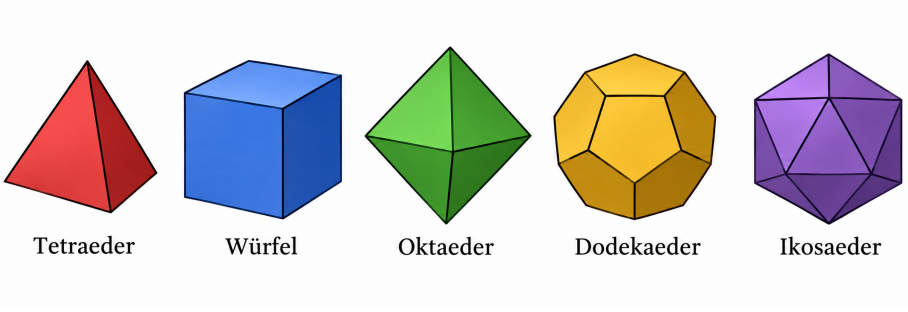


- die Gruppe aller Isometrien,

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

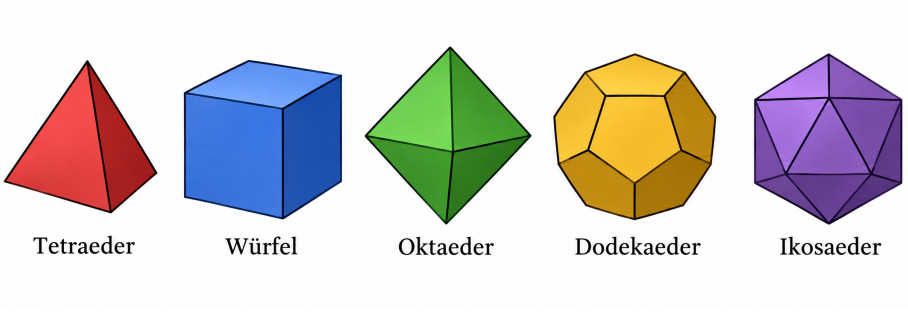


- die Gruppe aller Isometrien, die

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

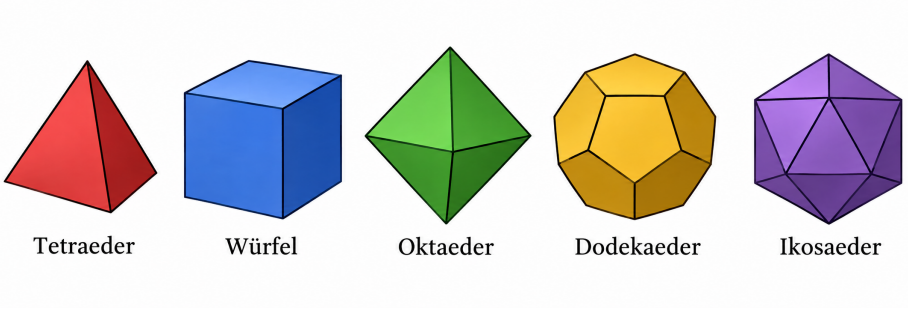


- die Gruppe aller Isometrien, die einen

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

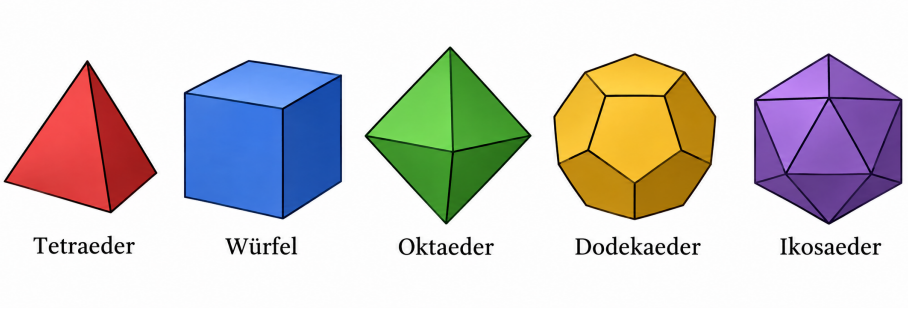


- die Gruppe aller Isometrien, die einen Körper

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

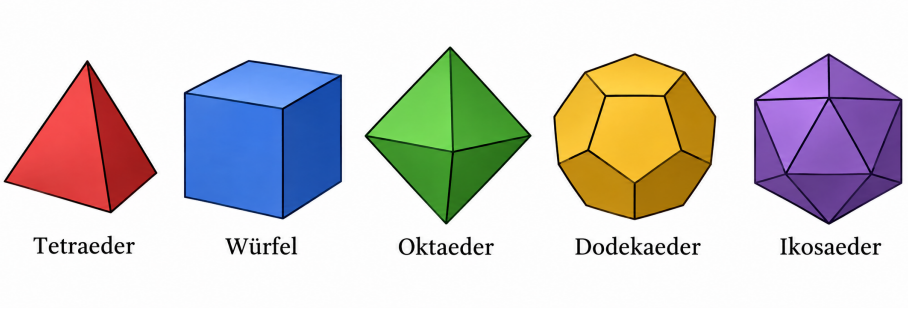


- die Gruppe aller Isometrien, die einen Körper auf

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.

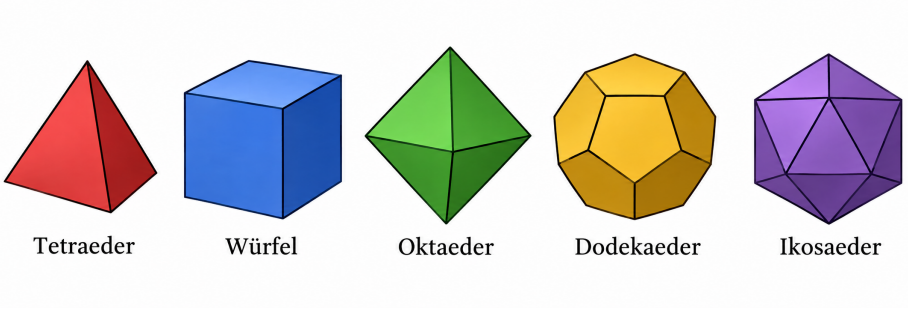


- die Gruppe aller Isometrien, die einen Körper auf sich

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.

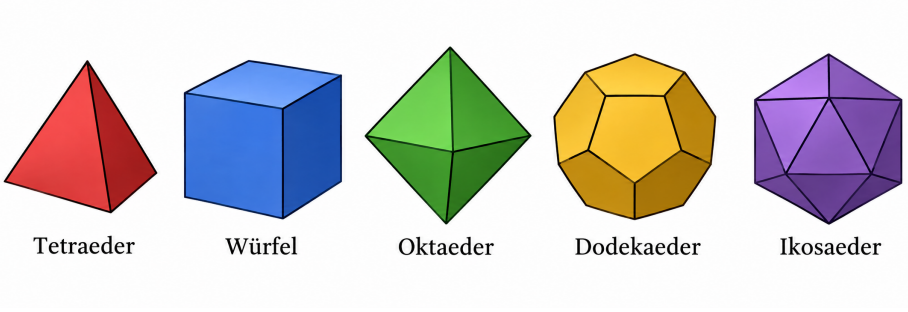
- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.



- die Gruppe aller Isometrien, die einen Körper auf sich selbst

Beispiele.

- $GL(n, \mathbb{K})$ und verschiedene Untergruppen. Insbesondere $O(n)$, $U(n)$, $SO(n)$, $SU(n)$.
- z.B. $U(1) = \{z \in \mathbb{C} \colon |z| = 1\}$. Auch S^1.



- die Gruppe aller Isometrien, die einen Körper auf sich selbst abbilden.

- $\mathrm{Bij}(X)$.

- $\mathrm{Bij}(X)$.
- Insbesondere

- $\mathrm{Bij}(X)$.
- Insbesondere für

- $\mathrm{Bij}(X)$.
- Insbesondere für $X =$

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1,$

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots,$

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$:

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$: $S_n :=$

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$: $S_n := \mathrm{Bij}(X)$.

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$: $S_n := \mathrm{Bij}(X)$.
  - Die

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$: $S_n := \mathrm{Bij}(X)$.
  - Die Elemente

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$: $S_n := \mathrm{Bij}(X)$.
  - Die Elemente heißen

- $\mathrm{Bij}(X)$.
- Insbesondere für $X = \{1, \ldots, n\}$: $S_n := \mathrm{Bij}(X)$.
  - Die Elemente heißen *Permutationen*.

1. Wiederholung

2. Erzeugendensysteme, Ordnung, zyklische Gruppen

3. Mehr über S_n

- Sei

- Sei G

- Sei G eine

- Sei G eine Gruppe

- Sei G eine Gruppe und

- Sei G eine Gruppe und $S \subseteq$

- Sei G eine Gruppe und $S \subseteq G$.

- Sei G eine Gruppe und $S \subseteq G$. Die

- Sei G eine Gruppe und $S \subseteq G$. Die Menge

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem*

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G,

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h.

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g =$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1,$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben:

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G =$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition.

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1,$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0,$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*,

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*, falls

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*, falls sie

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*, falls sie ein

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*, falls sie ein endliches

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*, falls sie ein endliches Erzeugendensystem

- Sei G eine Gruppe und $S \subseteq G$. Die Menge S heißt *Erzeugendensystem* von G, falls jedes $g \in G$ als Produkt von Elementen aus S und deren Inversen geschrieben werden kann.
  - D.h. $g = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ mit $s_i \in S$ und $\varepsilon_i \in \{1, -1\}$.
  - Geschrieben: $G = \langle S \rangle$.
- Beispiele:
  - Jede Gruppe G wird von sich selbst erzeugt.
  - $\mathbb{Z}^2$ ist eine Gruppe mit komponentenweiser Addition. Die Elemente $(1, 0)$ und $(0, 1)$ bilden ein Erzeugendensystem.
- Eine Gruppe heißt *endlich erzeugt*, falls sie ein endliches Erzeugendensystem besitzt.

- Eine

- Eine Gruppe

- Eine Gruppe G

- Eine Gruppe G heißt

- Eine Gruppe G heißt *zyklisch*,

- Eine Gruppe G heißt *zyklisch*, falls

- Eine Gruppe G heißt *zyklisch*, falls sie

- Eine Gruppe G heißt *zyklisch*, falls sie von

- Eine Gruppe G heißt *zyklisch*, falls sie von einem

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird,

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h.

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G =$

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in$

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also

• Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.

- Also $G =$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z},$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch,

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung:

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n :=$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0],$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1],$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots,$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$,

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$ eine

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$ eine zyklische

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$ eine zyklische Gruppe,

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$ eine zyklische Gruppe, erzeugt

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$ eine zyklische Gruppe, erzeugt von

- Eine Gruppe G heißt *zyklisch*, falls sie von einem einzigen Element erzeugt wird, d.h. $G = \langle g \rangle$ für ein $g \in G$.
  - Also $G = \{g^n \mid n \in \mathbb{Z}\}$.

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch, erzeugt von 1 (oder -1).
- Erinnerung: $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$, wobei $[k]$ die Klasse von k modulo n ist.
  - Mit Addition modulo n ist $\mathbb{Z}/n$ eine zyklische Gruppe, erzeugt von $[1]$.

- Die

- Die n-ten

- Die n-ten Einheitswurzeln

- Die n-ten Einheitswurzeln $\mu_n :=$

- Die n-ten Einheitswurzeln $\mu_n := \{z \in$

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n =$

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit

• Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit Multiplikation.

• Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit Multiplikation.

- Ein

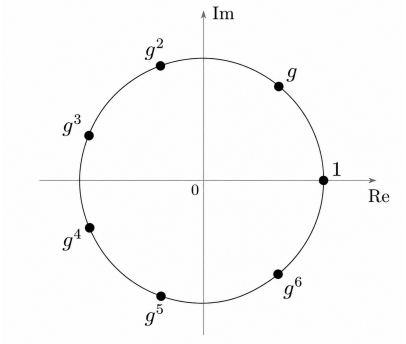
- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit Multiplikation.
  - Ein Erzeuger

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit Multiplikation.
  - Ein Erzeuger ist

- Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit Multiplikation.
  - Ein Erzeuger ist $e^{2\pi i/n}$.

• Die n-ten Einheitswurzeln $\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$ bilden eine zyklische Gruppe mit Multiplikation.

- Ein Erzeuger ist $e^{2\pi i/n}$.



- Sei

- Sei G

- Sei G die

- Sei G die Gruppe

- Sei G die Gruppe der

- Sei G die Gruppe der orientierungserhaltenden

- Sei G die Gruppe der orientierungserhaltenden Isometrien

- Sei G die Gruppe der orientierungserhaltenden Isometrien eines

- Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

- Also:

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

- Also: Rotationen

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

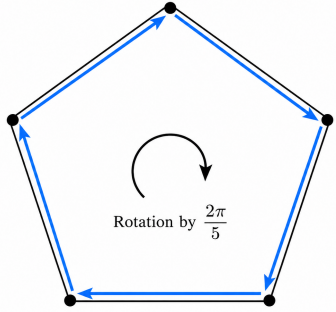
- Also: Rotationen des

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

- Also: Rotationen des n-Ecks.

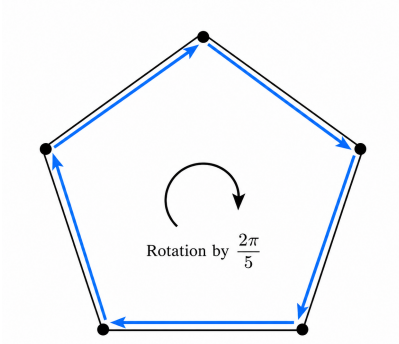
• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

- Also: Rotationen des n-Ecks.



• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

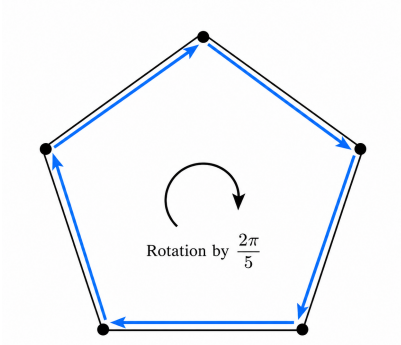
- Also: Rotationen des n-Ecks.



- G

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

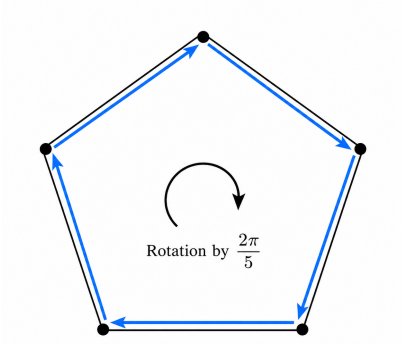
- Also: Rotationen des n-Ecks.



- G ist

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

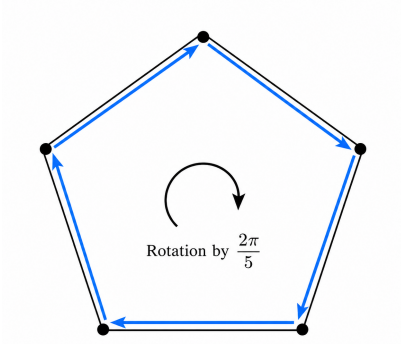
- Also: Rotationen des n-Ecks.



- G ist eine

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

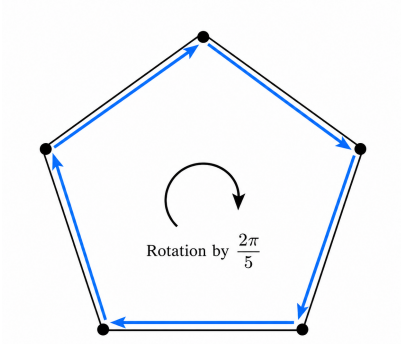
- Also: Rotationen des n-Ecks.



- G ist eine zyklische

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

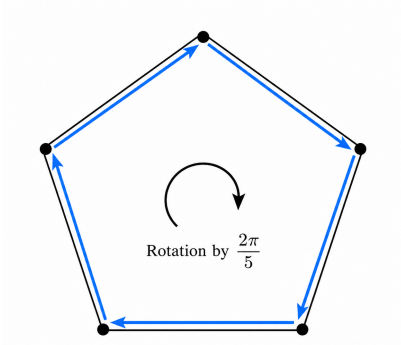
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe,

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

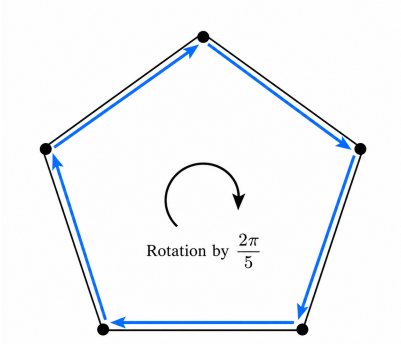
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

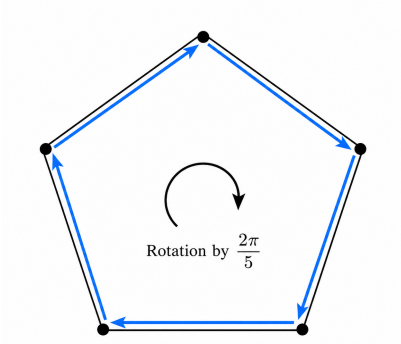
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt von

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

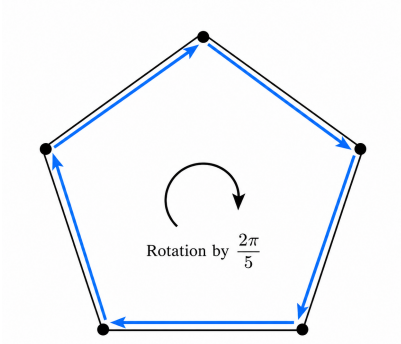
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt von der

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

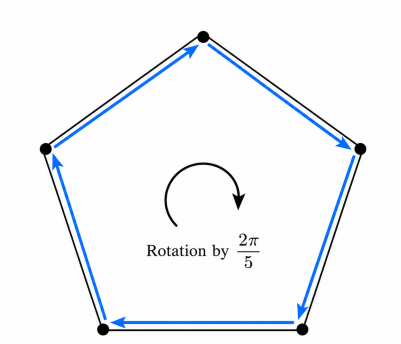
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt von der Drehung

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

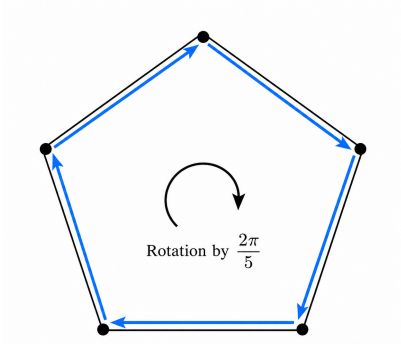
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt von der Drehung um

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

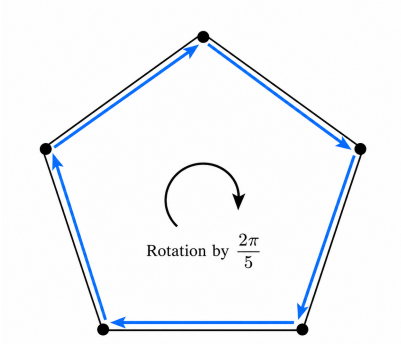
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt von der Drehung um den

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

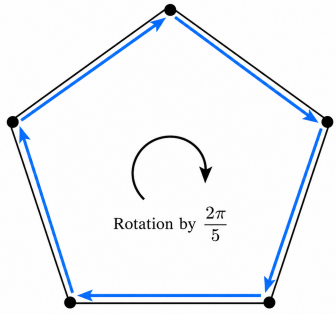
- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt von der Drehung um den Winkel

• Sei G die Gruppe der orientierungserhaltenden Isometrien eines regelmäßigen n-Ecks.

- Also: Rotationen des n-Ecks.



- G ist eine zyklische Gruppe, erzeugt von der Drehung um den Winkel $2\pi/n$.

- Für

- Für a,

- Für $a, b \geqslant$

- Für $a, b \geqslant 1$

- Für $a, b \geqslant 1$ mit

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a,$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) =$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition)

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger:

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1],$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen:

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1],$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]),$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2],$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]),$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots,$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab],$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich.

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k],$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) =$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l],$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$,

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch $ab \mid k - l$.

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch $ab \mid k - l$. Das

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch $ab \mid k - l$. Das bedeutet

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch $ab \mid k - l$. Das bedeutet aber

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch $ab \mid k - l$. Das bedeutet aber $k =$

- Für $a, b \geqslant 1$ mit $\mathrm{ggT}(a, b) = 1$ ist $\mathbb{Z}/a \times \mathbb{Z}/b$ (mit Addition) zyklisch.
  - Erzeuger: $([1], [1])$.
  - zu Zeigen: die Elemente $([1], [1]), ([2], [2]), \ldots, (([ab], [ab])$ sind paarweise unterschiedlich. Wenn $k \leqslant l$ und $([k], [k]) = ([l], [l])$ dann $a \mid k - l$ und $b \mid k - l$, also auch $ab \mid k - l$. Das bedeutet aber $k = l$.

- Die

- Die *Ordnung*

- Die *Ordnung* einer

- Die *Ordnung* einer Gruppe

- Die *Ordnung* einer Gruppe G

- Die *Ordnung* einer Gruppe G ist

- Die *Ordnung* einer Gruppe G ist ihre

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*,

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$.

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung*

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g,

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$,

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\mathrm{ord}(g)$, ist die

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\mathrm{ord}(g)$, ist die kleinste

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\mathrm{ord}(g)$, ist die kleinste Zahl

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n =$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt,

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) :=$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe*

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle :=$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung:

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m,$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m =$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann,

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} =$

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$,

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir die

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir die Gleichheit

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir die Gleichheit durch

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir die Gleichheit durch g^{-n}

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir die Gleichheit durch g^{-n} multiplizieren

- Die *Ordnung* einer Gruppe G ist ihre Kardinalität $|G|$.
  - Eine Gruppe heißt *endlich*, falls $|G| < \infty$.
- Sei $g \in G$. Die *Ordnung* von g, bezeichnet mit $\operatorname{ord}(g)$, ist die kleinste Zahl $n \geqslant 1$ mit $g^n = e$.
  - Falls es kein solches n gibt, setzen wir $\operatorname{ord}(g) := \infty$.
- Die von g erzeugte *zyklische Untergruppe* ist $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
- Bemerkung: für $m, n \in \mathbb{Z}$ gilt $g^m = g^n$ genau dann, wenn $g^{m-n} = e$, weil wir die Gleichheit durch g^{-n} multiplizieren können.

Lemma.

Lemma. Sei

Lemma. Sei $d :=$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann,

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$,

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld} g^r = e$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld} g^r = e$ und es folgt $g^r =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld} g^r = e$ und es folgt $g^r = e$. Das zeigt

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld} g^r = e$ und es folgt $g^r = e$. Das zeigt $r =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$,

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n,

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$,

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d :=$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich,

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt:

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$.

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt man

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt man $\langle g \rangle =$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt man $\langle g \rangle = \{e,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt man $\langle g \rangle = \{e, g,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt man $\langle g \rangle = \{e, g, \ldots,$

Lemma. Sei $d := \operatorname{ord}(g) < \infty$. Es gilt $g^k = e$ genau dann, wenn $d \mid k$

Beweis. • Wenn $d \mid k$ dann $k = dl$ und $g^k = (g^d)^l = e^l = e$.

• Falls $g^k = e$, dann schreiben wir $k = ld + r$ mit $0 \leqslant r < d$ und $g^{ld+r} = e$ also $g^{ld}g^r = e$ und es folgt $g^r = e$. Das zeigt $r = 0$. □

Lemma. Für jedes $g \in G$ gilt $|\langle g \rangle| = \operatorname{ord}(g)$.

Beweis. • Falls $\operatorname{ord}(g) = \infty$, sind alle Potenzen g^n, $n \in \mathbb{Z}$, paarweise unterschiedlich.

• Falls $d := \operatorname{ord}(g) < \infty$ sind die Potenzen $g, g^2, \ldots, g^d$ paarweise unterschiedlich, und für jede Potenz g^k haben wir $g^k = g^{dl+r} = g^r$.

- Dies zeigt: $\langle g \rangle = \{g, g^2, \ldots, g^d\}$. □

• Häufig schreibt man $\langle g \rangle = \{e, g, \ldots, g^{d-1}\}$.

- Beispiel:

- Beispiel: in

- Beispiel: in $\mathrm{SL}(2,$

- Beispiel: in $\mathrm{SL}(2, \mathbb{Z})$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung,

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 \\ \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung:

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ erzeugen

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ erzeugen $\mathrm{SL}(2,$

- Beispiel: in $\mathrm{SL}(2,\mathbb{Z})$ die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ hat unendliche Ordnung, und die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ hat Ordnung 4.
- Übung: die Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ erzeugen $\mathrm{SL}(2,\mathbb{Z})$.

1. Wiederholung

2. Erzeugendensysteme, Ordnung, zyklische Gruppen

3. Mehr über S_n

Notation

Notation

- In

Notation

- In der

Notation

- In der *zweizeiligen Schreibweise*

Notation

- In der *zweizeiligen Schreibweise* geben

Notation

- In der *zweizeiligen Schreibweise* geben wir

Notation

- In der *zweizeiligen Schreibweise* geben wir die

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an.

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel:

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma =$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links).

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau =$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau =$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die *Zyklenschreibweise*:

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.
- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.
- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$,

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt.

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".

  ▶ Im obigen

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".

- Im obigen Beispiel:

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma =$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1$

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".

  ▶ Im obigen Beispiel: $\sigma = (1\,2$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$,

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau =$

Notation

• In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

• Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

• Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".

- Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1\,2)$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1\,2)$ und

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1\,2)$ und $\sigma\tau =$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1\,2)$ und $\sigma\tau = (1$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1\,2)$ und $\sigma\tau = (1\,3)(4$

Notation

- In der *zweizeiligen Schreibweise* geben wir die Bilder aller Elemente an. Zum Beispiel: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

- Die Verknüpfung ist die Komposition von Abbildungen (von rechts nach links). Für $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ gilt $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

- Wir verwenden meistens die *Zyklenschreibweise*: $(a_1\, a_2\, \ldots\, a_k)$ bezeichnet die Permutation $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, die alle anderen Elemente fest lässt. So eine Permutation nennen wir auch ein "Zyklus".
  - Im obigen Beispiel: $\sigma = (1\,2\,3)(4\,5)$, $\tau = (1\,2)$ und $\sigma\tau = (1\,3)(4\,5)$.

- Vorsicht:

- Vorsicht: ▶ ohne

- Vorsicht: ▶ ohne weiteres

- Vorsicht: ▶ ohne weiteres Kontext

- Vorsicht: ▶ ohne weiteres Kontext $(1$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein,

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.

- Vorsicht:
  - ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung:

- Vorsicht:
  - ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind,

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau =$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.
Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1,$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots,$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir a,

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a),$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a),$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) =$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$,

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$,

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) =$

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.
Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist,

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt.

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie -

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von σ

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von σ als

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von σ als Produkt

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von σ als Produkt paarweise

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von σ als Produkt paarweise disjunkter

- Vorsicht: ▶ ohne weiteres Kontext $(1\,2\,3)$ könnte ein Element in S_3 sein, oder S_4 oder...
  - ▶ Die Notation $(1\,2\,3)$ und $(2\,3\,1)$ beschreibt die *gleiche Permutation*.
- Bemerkung: falls σ and τ disjunkte Zyklen sind, dann $\sigma\tau = \tau\sigma$.

Lemma. Jede Permutation $\sigma \in S_n$ ist ein Produkt paarweise disjunkter Zyklen.

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zyklen.

Beweis.

- Für $a \in \{1, \ldots, n\}$ betrachten wir $a, \sigma(a), \sigma^2(a), \ldots$.
  - ▶ falls $\sigma^k(a) = \sigma^l(a)$, $k > l$, dann $\sigma^{k-l}(a) = a$. Da die Menge endlich ist, kommen wir irgendwann wieder bei a an. Dies ergibt einen Zyklus.
- Zwei solche Zyklen sind entweder gleich oder disjunkt. Wir nehmen eine maximale disjunkte Familie - dies gibt uns eine Darstellung von σ als Produkt paarweise disjunkter Zyklen.

- Eindeutigkeit:

- Eindeutigkeit: ▶ Für

- Eindeutigkeit: ▶ Für $\sigma =$

- Eindeutigkeit: ▶ Für $\sigma = e$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma =$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k =$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind,

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 =$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen kommutieren.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen kommutieren. Wir

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen kommutieren. Wir können

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen kommutieren. Wir können also

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.
  - ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.
  - ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.
  - ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein Gegenbeispiel

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein Gegenbeispiel mit

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein Gegenbeispiel mit $k - 1$

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein Gegenbeispiel mit $k - 1$ Zyklen,

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein Gegenbeispiel mit $k - 1$ Zyklen, Widerspruch.

- Eindeutigkeit: ▶ Für $\sigma = e$ ist die Behauptung klar.

  ▶ Sei $\sigma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_l$ ein Gegenbeispiel mit minimalem $k \geqslant 1$.

  ▶ Wähle x mit $\alpha_1(x) \neq x$. Dann gibt es ein i mit $\beta_i(x) \neq x$. Da α_1 und β_i nicht disjunkt sind, gilt $\alpha_1 = \beta_i$.

  ▶ Disjunkte Zyklen kommutieren. Wir können also β_i nach vorne ziehen und kürzen. So erhalten wir ein Gegenbeispiel mit $k - 1$ Zyklen, Widerspruch. □

- Beispiel:

- Beispiel: Für

- Beispiel: Für $\sigma =$

- Beispiel: Für $\sigma = (1$

- Beispiel: Für $\sigma = (1\,2$

- Beispiel: Für $\sigma = (1\,2\,3)(4$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\operatorname{ord}(\sigma) =$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) =$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) =$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l:

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) =$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m =$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann,

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn jeder

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

- Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit:

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3,2,4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche Zahl

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche Zahl m

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche Zahl m ist

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche Zahl m ist $\mathrm{kgV}(l_1,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche Zahl m ist $\mathrm{kgV}(l_1, \ldots,$

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche Zahl m ist $\mathrm{kgV}(l_1, \ldots, l_k)$.

- Beispiel: Für $\sigma = (1\,2\,3)(4\,5)(6\,7\,8\,9)$ gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(3, 2, 4) = 12$.

Lemma. Sei $\sigma \in S_n$ ein Produkt disjunkter Zyklen $\sigma_1, \ldots, \sigma_k$ der Längen $l_1, \ldots, l_k$. Dann gilt $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_k)$.

Beweis. • Die Aussage ist klar für einen Zyklus α der Länge l: $\mathrm{ord}(\alpha) = l$.

• Es gilt $\sigma^m = e$ genau dann, wenn jeder Zykel nach m Anwendungen alle seine Elemente wieder fest lässt.

• Das ist äquivalent mit: $\mathrm{ord}(\sigma_i) \mid m$ für alle i.

• Die kleinste solche Zahl m ist $\mathrm{kgV}(l_1, \ldots, l_k)$. □