# Lernziele der 10. Woche

Die Studierenden sollen:

- die abstrakte Definition einer Gruppe kennen und anwenden können, z. B. zeigen, dass eine durch eine Tabelle definierte Operation eine Gruppenoperation ist.
- grundlegende Eigenschaften von Gruppen (z. B. Satz A1 und dessen Folgerungen) anwenden können.
- Permutationen multiplizieren und invertieren können.
- beweisen können, dass jede Gruppe eine Untergruppe der Permutationsgruppe ist (wird auch in Anwesentheitsaufgaben besprochen)
- zeigen können, dass eine „mod $q$“-Relation eine Äquivalenzrelation ist.
- zeigen können, dass $\mathbb{Z}_q$ eine Gruppe und ein Ring ist.

# Neues Thema: abstrakte Algebra: Gruppen- und Körpertheorie

**Def.** *Eine Gruppe besteht aus einer nicht leeren Menge $G$ und einer Abbildung $\cdot : G \times G \to G$ (wir werden $a \cdot b$ oder $ab$ statt $\cdot(a, b)$ schreiben; die Abbildung heißt Multiplikation) mit folgenden Eigenschaften*

(G1): $a(bc) = (ab)c$ *(für alle $a, b, c \in G$) Assoziativität*

(G2): *Es gibt $e \in G$ mit $ea = a$. (für alle $a \in G$) Existenz eines neutralen Elementes*

(G3): *Für jedes $a \in G$ gibt es ein $b \in G$ mit $ba = e$. Existenz eines inversen Elements*

**Def.** *Gilt ausserdem $ab = ba$, so heißt die Gruppe eine abel'sche (oder eine kommutative) Gruppe.*
**Bemerkung** *In einer abel'sche Gruppe bezeichnet man die Multiplikation oft mit $+$.*

# Bereits bekannte Beispiele

1. $(\mathbb{Z}, +)$: $G := \mathbb{Z}$, „ $\cdot$ “ := „ $+$ “
   (G1): Addition von reellen (und, desqegen, von ganzen) Zahlen ist assoziativ.
   (G2): $e := 0$, weil $0 + a = a$.
   (G3): $a^{-1} := -a$, weil $a + (-a) = 0$.
2. Ebenso: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$. Hier stets $e = 0$, $a^{-1} = -a$
3. Gegenbeispiel: $(\mathbb{R}, \cdot)$ ist keine Gruppe. Betrachten wir $(\mathbb{R}, \cdot)$ und versuchen wir zu verstehen, warum $(\mathbb{R}, \cdot)$ keine Gruppe ist:
   - Die Multiplizieren-Operation „$\cdot$“ in $\mathbb{R}$ ist wohldefiniert: für alle $a, b \in \mathbb{R}$ ist $a \cdot b$ auch ein Element von $\mathbb{R}$.
   - (G1) ist erfüllt
   - (G2) ist ebenfalls erfüllt: Für das Element $e := 1 \in \mathbb{R}$ gilt das Erwünschte $e \cdot a = a$. Also gibt es ein neutrales Element (im Satz A1 werden wir zeigen, dass das neutrale Element eindeutig ist)
   - (G3) ist aber nicht erfüllt: für das Element $0 \in \mathbb{R}$ gibt es KEIN $b \in G$ mit $b \cdot 0 =$ „neutrales Element“, weil $b \cdot 0 = 0$, und 0 ist kein neutrales Element in $(\mathbb{R}, \cdot)$.

# Bsp: Jeder Vektorraum ist eine abelsche Gruppe bzgl. „+“

Sei $(V, +, \cdot)$ ein Vektorraum. Dann ist $(V, +)$ eine kommutative Gruppe. In der Tat sind die ersten vier Axiome des Vektorraums (siehe Vorl. 3 LAAG 1)

I Für alle $u, v, w \in V$ gilt $(u + v) + w = u + (v + w)$

II Für alle $u, v \in V$ gilt $u + v = v + u$

III Es existiert ein $\vec{0} \in V$, so dass für alle $v \in V$ gilt $\vec{0} + v = v$

IV Für jedes $v \in V$ existiert ein $-v \in V$, so dass gilt $-v + v = \vec{0}$

Wir sehen, dass $I = G1$, $III = G2$, $IV = G3$, und $II = \text{Kommutativität}$.

# Weitere Beispiele

$(\mathbb{Q}_{>0}, \cdot)$, (wobei $\cdot$ die übliche Multiplikation ist),
$(\mathbb{R}_{>0}, \cdot)$,
$(\mathbb{C} \setminus \{0\}, \cdot)$ sind Gruppen.

- wohldefiniert (z.B. für $(\mathbb{Q}_{>0}, \cdot)$: Produkt von zwei positiven rationalen Zahlen ist eine positive rationale Zahl.
- (G1): Multiplikation von reellen oder komplexen Zahlen ist assoziativ.
- (G2): $e := 1$, weil $1 \cdot a = a$.
- (G3) $a^{-1} = \frac{1}{a}$, weil $\frac{1}{a} \cdot a = 1$.

# Die Gruppe $GL_n$

Alle Gruppen aus den obigen Beispielen sind abel'sch (kommutativ). Jetzt geben wir ein paar nichtkommutative Beispiele:

Sei $n \in \mathbb{N}$. Als Menge $G$ nehmen wir

$G := GL_n := \{A \in Mat(n,n) \mid \det(A) \neq 0\}$ (=die Menge aller nichtausgearteten $n \times n-$Matrizen). Als Operation „$\cdot$" nehmen wir die Matrix-Multiplikation.

Die Operation ist wohldefiniert: Produkt von zwei nichtausgearteten Matrizen ist nichtausgeartet (weil $\det(AB) \overset{\text{Satz } 19}{=} \underbrace{\det(A)}_{\neq 0} \cdot \underbrace{\det(B)}_{\neq 0} \neq 0$)

(G1): Matrizenprodukt ist assoziativ (Folgerung aus Satz 14 )

(G2): $e := Id$. In der Tat, $Id \cdot A = A$ (für jede Matrix $A$)

(G3): Die inverse Matrix $B := A^{-1}$ hat die gewünschte Eigenschaft $BA = Id$.

Die Gruppe ist nichtkommutativ für $n > 2$.

**Satz A1** *Sei $(G, \cdot)$ eine Gruppe. Dann gilt:*

(i) *Es gibt NUR EIN neutrales Element $e \in G$ (so dass $e \cdot a = a$ für jedes $a \in G$). Es gilt: $a \cdot e = a$ für alle $a \in G$.*

(ii) *Zu jedem $a \in G$ existiert nur ein $b \in G$, für das $b \cdot a = e$ gilt. Für dieses $b$ gilt auch: $a \cdot b = e$.*
*Bezeichnung: Das Element $b \in G$ mit $b \cdot a = a \cdot b = e$ wird mit $a^{-1}$ (bzw. mit $-a$, falls $\cdot = +$) bezeichnet.*

**Beweis:** Zeige zunächst:
$(*)$ $a, b \in G$ und $b \cdot a = e \Rightarrow a \cdot b = e$ ($\Rightarrow$ 2. Behauptung in (ii))
Denn: Nach (G3) existiert zu $b \in G$ ein $c \in G$ mit $c \cdot b = e$. Es gilt:
$a \cdot b = e \cdot (a \cdot b) = (c \cdot b) \cdot (a \cdot b) \overset{(G1)}{=} c \cdot ((b \cdot a) \cdot b) = c \cdot (e \cdot b) = c \cdot b = e$.
$(*)$ ist bewiesen.
Beweis von (i) : Sei $\tilde{e} \in G$ ein Element, so dass (G2) gilt. Z.z.: $e = \tilde{e}$. Es gilt: $e \overset{(G2) \text{ für } \tilde{e}}{=} \tilde{e} \cdot e \overset{(*)}{=} e \cdot \tilde{e} \overset{(G2) \text{ für } e}{=} \tilde{e}$.
Sei $a \in G$. Wir zeigen $a \cdot e = a$. Nach (G3) existiert ein $b \in G$ mit $b \cdot a = e$ und nach $(*)$ folgt $a \cdot b = e$. Also
$a \cdot e = a \cdot (b \cdot a) \overset{(G1)}{=} (a \cdot b) \cdot a = e \cdot a \overset{(G2)}{=} a$. $(i)$ ist bewiesen.
Beweis von (ii): Seien $a, b, \tilde{b} \in G$ und es gelte: $b \cdot a = e = \tilde{b} \cdot a$. Z.z.: $b = \tilde{b}$. Es gilt: $\tilde{b} \overset{(i)}{=} \tilde{b} \cdot e \overset{(*)}{=} \tilde{b} \cdot (a \cdot b) \overset{(G1)}{=} (\tilde{b} \cdot a) \cdot b = e \cdot b \overset{(G2)}{=} b$ □

**Folgerung** *Sei $(G, \cdot)$ Gruppe, $a, b \in G$. Dann gilt:*

(a) $(a^{-1})^{-1} = a$

(b) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ *(Vergl. mit „Coxeter“-Regel)*

(c) $a \cdot e = a = e \cdot a$

**Bemerkung.** Ähnliche Aussagen für nichtausgeartete Matrizen haben wir in Siehe Satz 15 und dessen Folgerungen bewiesen.

**Beweis:**
(a) Z.z.: $a$ ist das Inverse von $a^{-1}$, d.h. $a \cdot a^{-1} = e$. Nach Definition gilt $a^{-1} \cdot a = e$, und nach Satz A1, Aussage (ii), folgt daraus $a \cdot a^{-1} = e$.
(b) Z.z.: $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$. Wir rechnen:
$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) \overset{(G1)}{=} b^{-1}(\cdot a^{-1} \cdot a) \cdot b = b^{-1} \cdot e \cdot b \overset{(G1,G2)}{=} b^{-1} \cdot b = e$
(c) Wir haben eigentlich $(c)$ als Teil des Satz A1(i) gezeigt. Wir zeigen es noch einmal:
Z.z.: $a \cdot e = a$. Wir haben: $e \cdot a^{-1} = a^{-1}$. Dann ist

$$\begin{array}{ccc} (e \cdot a^{-1})^{-1} & = & (a^{-1})^{-1} \\ \| \ (b) & & \\ (a^{-1})^{-1} \cdot e^{-1} & \overset{(a)}{=} & a \cdot e \end{array}$$

□

# Endliche Gruppen (= endlich viele Elemente)

Man muss die Menge beschreiben (z.B. auflisten, d.h. $G = \{e, a_1, a_2, a_3, ..., a_m\}$ ) und die Multiplikation angeben z.B. mit einer Tabelle, auf $(i, j)-$ Stelle steht $a_i \cdot a_j$

| | $e$ | $a_1$ | $a_2$ | ... | $a_j$ | ... | $a_m$ |
|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a_1$ | $a_2$ | | $a_j$ | | $a_m$ |
| $a_1$ | $a_1$ | | | | | | |
| | | | | | | | |
| $a_i$ | $a_i$ | | | | $a_i \cdot a_j$ | | |
| $\vdots$ | | | | | | | $\vdots$ |
| $a_m$ | $a_m$ | | | | | | |

**Bemerkung.** Beliebige Tabelle gibt i.d.R. keine Gruppenoperation, denn *(G2) (bzw. Satz A1(i)): erste Zeile ( bzw. Spalte) wiederholt und die Null-Zeile (bzw. die Null-Spalte).* Außerdem (Sudoku-Regel): (G3): in jeder Zeile und in jeder Spalte steht jedes Element. Tatsächlich, die Gleichungen $ax = b$ und $xa = b$ sind immer lösbar: $x = a^{-1}b$ und $x = ba^{-1}$; wird auch nachher (Seite 19) besprochen.

Bemerkung. Eigentlich, besagt (G3) nur, dass in jeder Zeile das Neutralelement $e$ steht. Die Sudoku-Regel folgt aus allen drei Gruppenaxiomen (G2).

Ausserdem soll (G1) (Assoziativität) erfüllt sein

# Gruppenoperationstabellen für kleinere $m$

1. Triviale Gruppe $G = \{e\}$ (mit $e \cdot e := e$), deren Tabelle

| | $e$ |
|---|---|
| $e$ | $e$ |

2. Gruppe aus zwei Elementen $G = \{e, a\}$ mit $a \cdot a := e$.

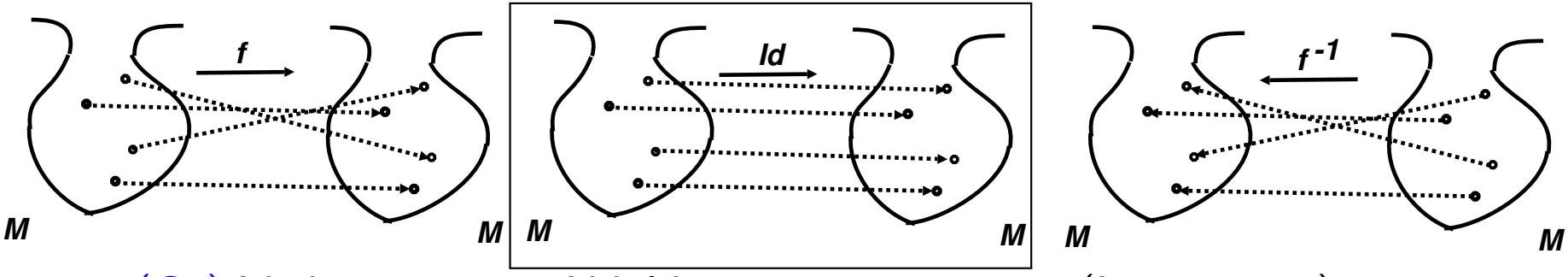
| | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

3. Gruppe aus drei Elementen

| | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

**Wicht. Bsp.** $M$ sei eine nicht leere Menge. Sei $\mathcal{S}_M = \{f : M \to M, \text{ so dass } f \text{ bijektiv ist }\}$. $\mathcal{S}_M$ mit der $\cdot := \circ$ (Verkettung, Komposition, Hintereinanderausführung) ist eine Gruppe.

**Wiederholung (Vorlesung 10)** Bijektion *ist eine injektive surjektive Abbildung, d.h. für jedes $a \in M$ gibt es genau ein $b \in M$ s.d. $f(b) = a$.*




(G1) Verkettung von Abbildungen ist assoziativ (Lemma 17 )

(G2) Die Identitätsabbildung $Id$, $Id(x) = x$ ist ein neutrales Element. Tatsächlich, $Id \circ f(x) = Id(f(x)) = f(x)$.

(G3) Sei $f : M \to M$ eine Bijektion. Dann existiert nach Lemma 13 die eindeutige inverse Abbildung $f^{-1} : M \to M$ (mit der Eigenschaft $f^{-1} \circ f = Id$); diese Abbildung ist bijektiv und ist deswegen ein Element von $\mathcal{S}_M$. Da $f^{-1} \circ f = Id$ (= neutrales Element), erfüllt $f^{-1}$ Eigenschaft (G3)

# Permutationen

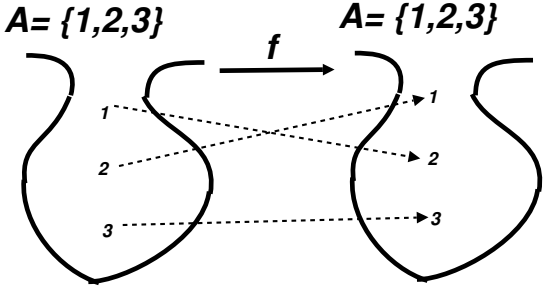
Die Menge $M$ bestehe aus $n < \infty$ Elementen.

**Bezeichnung.** Die Gruppe $\left( \underbrace{\{f : M \to M,\ f \text{ ist bijektiv}\}}_{\text{aller Bijektionen } f : M \to M}, \circ \right)$ bezeichnet man mit $\mathcal{S}_n$ und nennt sie die Gruppe von Permutationen von $M$.

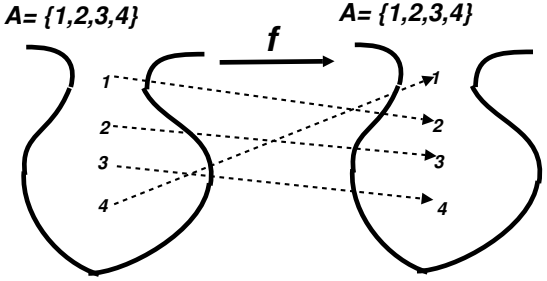
OBdA ist $M = \{1, 2, 3, ..., n\}$. Dann kann man das Element $f \in \mathcal{S}_n$ als $2 \times n$-Tabelle schreiben (Matrixform):

$$f \longleftrightarrow \begin{pmatrix} 1 & 2 & ... & n \\ f(1) & f(2) & ... & f(n) \end{pmatrix}.$$

**Bsp:** $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$:




**Bsp:** $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.



# Multiplizieren und Invertieren von Permutationen

$$f := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

**Frage:** Was ist $f(1)$? **Anwort:** 3
**Frage:** Was ist $f(3)$? **Anwort:** 1

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

# Bitte üben: Multiplizieren Sie die Permutationen.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

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

# Bitte noch einmal üben: Multiplizieren Sie die Permutationen.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Wie invertiert man eine Permutation?

1: Man muss die Zeilen umtauschen

2: Und dann die Spalten sortieren, s.d. oben (1 2 3 ... n) steht.

**Bsp:** $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

Tatsächlich: falls $f(i) = j$, dann $f^{-1}(j) = i$.

# Bitte üben.

Invertieren Sie bitte

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$$

Permutation ist ja eine Abbildung. In unserem Fall, die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$$

steht für die (bijektive) Abbildung $\pi : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ s.d.

$$\pi(1) = 3\,,\ \pi(2) = 1\,,\ \pi(3) = 5\,,\ \pi(4) = 4\,,\ \pi(5) = 2$$

Und beim Umkehren einer Abbildung wird aus $\pi(x) = y$ eben $\pi^{-1}(y) = x$:

$$\pi^{-1}(3) = 1\,,\ \pi^{-1}(1) = 2\,,\ \pi^{-1}(5) = 3\,,\ \pi^{-1}(4) = 4\,,\ \pi^{-1}(2) = 5$$

Man muß also in der obigen Notation einfach die beiden Zeilen vertauschen, schon hat man die Umkehrpermutation, die aber nicht nach unsere Vorschriften geschrieben ist

$$\pi^{-1} = \begin{pmatrix} 3 & 1 & 5 & 4 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

oder, indem man die Eingaben in natürlicher Weise ordnet:

$$\text{Antwort: } \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$$

# Welche Gleichungen kann man in Gruppen lösen?

Z.B. die Gleichungen der Form $x \cdot g = f$ ($g, h \in G$ sind gegeben; $x \in G$ wird gesucht).
Die Lösung ist dann $x = f \cdot g^{-1}$: wenn wir $x = f \cdot g^{-1}$ in $x \cdot g = f$ einsetzen, bekommen wir

$$(f \cdot g^{-1}) \cdot g \overset{(G1)}{=} f \cdot \underbrace{(g^{-1} \cdot g)}_{e} \overset{\text{Satz A1(i)}}{=} f$$

wie gewünscht; also ist $f \cdot g^{-1}$ tatsächlich eine Lösung.
Ferner gilt: erfüllt $x$ die Gleichung $x \cdot g = f$, so gilt nach Multiplizieren von rechts die beide Seiten der Gleichung mit $g^{-1}$:
$x \cdot \underbrace{g \cdot g^{-1}}_{e} = f \cdot g^{-1}$; also $x \overset{\text{muss}}{=} f \cdot g^{-1}$.

**Bsp:** Man finde $X \in \mathcal{S}_4$ s.d. $X \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

**Lösung:** Wir multiplizieren von rechts mit $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$:

$X \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$. Wegen der Assoziativität:

$\iff X = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

Die Gleichungen der Form $x \cdot g = f$ ($g, h \in G$ sind gegeben; $x \in G$ wird gesucht).
hat die Lösung $x = f \cdot g^{-1}$: wenn wir $x = f \cdot g^{-1}$ in $x \cdot g = f$ einsetzen, bekommen wir

$$(f \cdot g^{-1}) \cdot g \overset{(G1)}{=} f \cdot \underbrace{(g^{-1} \cdot g)}_{e} \overset{\text{Satz A1(i)}}{=} f$$

wie gewünscht; also ist $f \cdot g^{-1}$ tatsächlich eine Lösung.

**Vorsicht:** In dem Fall $x \cdot g = f$ müssen wir die Gleichung **von rechts** mit $g^{-1}$ multiplizieren, weil die Gruppenoperation i.a. nicht kommutative ist. Also ist
$g^{-1} \cdot f$ eventuell keine Lösung von $x \cdot g = f$, denn es keine Gründe gibt, warum die Gleichung $g^{-1} \cdot f \cdot g = f$ richtig sein soll (und Beispiele von Gruppen gibt, wo das nicht immer der Fall ist)

**Bezeichnung:** $|G|$ oder $\#G$ ist Anzahl von Elemente in der Menge $G$.
**Satz A2** $|\mathcal{S}_n| = n! := 1 \cdot 2 \cdot 3 \cdot ... \cdot n$

Zuerst Vorarbeit:

# Beschränkung einer Abbildung — Wiederholung

Sei $f : A \to B$, $A_1 \subseteq A$. $f$ beschränkt auf $A_1$ (bez: $f_{|A_1}$) ist die Abbildung $f : A_1 \to B$, $f_{|A_1}(a) := f(a) \quad (\forall a \in A_1)$.

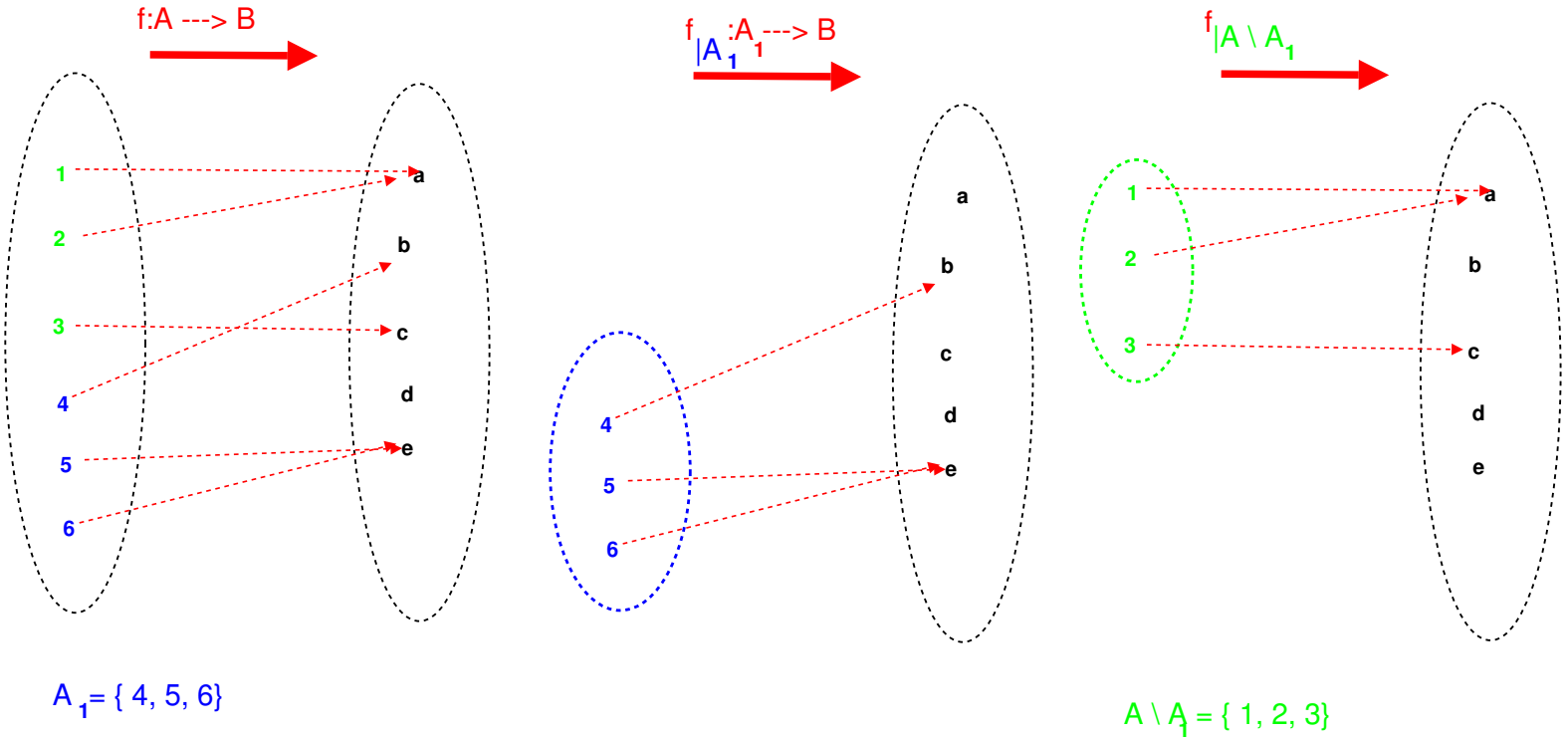



Abbildung: **Bsp:** $A_1 \subseteq A$, $f_{|A_1} : A_1 \to B$, und $f_{|A \setminus A_1} : A \setminus A_1 \to B$

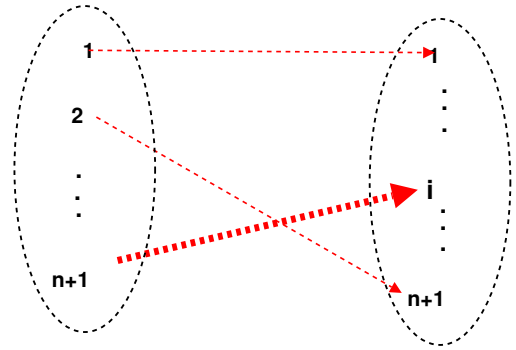
**Bemerkung:** Ist $f_{|A_1} = g_{|A_1}$ und $f_{|A \setminus A_1} = g_{|A \setminus A_1}$, so ist $f = g$.

**Beweis von Satz A2:** Wir beweisen die stärkere Aussage: Angenommen, $|A| = |B| = n$. Dann ist $\#\underbrace{\{f : A \to B \mid f\text{- bijektiv}\}}_{\mathcal{F}_n} = n!$. (Satz A2 = Aussage für $A = B$).

**Induktion nach $n$:** (IA) : $\exists$ nur eine Abbildung von $\{a\}$ nach $\{b\}$.
(IS: $n \longrightarrow n+1$) : OBdA ist $A = B = \{1, ..., n+1\}$.

**Schema:** Wir betrachten $n+1$ Teilmengen $\mathcal{F}^1, ..., \mathcal{F}^{n+1} \subseteq \mathcal{F}_{n+1}$ und zeigen, dass sie disjunkt sind, also $\mathcal{F}^i \cap \mathcal{F}^j = \varnothing$ für $i \neq j$, dass $\mathcal{F}^1 \cup \mathcal{F}^2 \cup ... \cup \mathcal{F}^{n+1} = \mathcal{F}_{n+1}$ ist, und dass $\#\mathcal{F}^i = n!$. Daraus wird die Aussage folgen, weil dann ist
$\#\mathcal{F}_{n+1} = \#\mathcal{F}^1 + \cdots + \#\mathcal{F}^{n+1} = (n+1) \cdot n! = (n+1)!$ .

Für jedes $i \in \{1, ..., n+1\}$ betrachte man
$\mathcal{F}^i := \{f \in \mathcal{F}_{n+1} \mid f(n+1) = i\}$.
Offensichtlich, $\mathcal{F}^i \cap \mathcal{F}^j = \varnothing$ für $i \neq j$,
und $\mathcal{F}^1 \cup \mathcal{F}^2 \cup ... \cup \mathcal{F}^{n+1} = \mathcal{F}_{n+1}$.




$\forall f \in \mathcal{F}^j$ gilt: $f_{|A\setminus\{n+1\}}$ ist Bijektion auf $B \setminus \{i\}$. Nach (IV) ist $\#\mathcal{F}^j = n!$. Dann ist

$$\#\mathcal{F}_{n+1} = \#\left(\mathcal{F}^1 \cup \mathcal{F}^2 \cup ... \cup \mathcal{F}^{n+1}\right) = \#\mathcal{F}^1 + \#\mathcal{F}^2 + ... + \#\mathcal{F}^{n+1} \overset{(IV)}{=}$$
$$\underbrace{n! + n! + ... + n!}_{n+1} = n! \cdot (n+1) = (n+1)!$$

□

# Def.

*Sei $(G, \cdot)$ eine Gruppe. Eine Untergruppe der Gruppe $G$ ist eine nicht leere Teilmenge $G' \subseteq G$ mit den Eigenschaften.*

(i) Für alle $a, b \in G'$ ist $a \cdot b \in G'$. (Geschlossen bzgl. Multiplikation)

(ii) Für jedes $a \in G'$ ist $a^{-1} \in G'$ (Geschlossen bzgl. Invertieren)

**Satz A3.** *Eine Untergruppe einer Gruppe ist eine Gruppe (bzgl. der induzierten Multiplikation.)*

**Beweis.** Wegen (i) ist die Beschränkung der Operation „$\cdot$“ auf $G'$ wohldefiniert – Produkt von zwei Elementen aus $G'$ ist ein Element von $G'$. Wir müssen nur (G1,G2,G3) zeigen.
(G1) ist offensichtlich. Wir beweisen (G2). Z.z.: $e \in G'$. Nehme ein $a \in G'$. Nach (ii) ist $a^{-1} \in G'$. Nach (i) ist $a^{-1}a = e \in G'$. (G3) folgt direkt aus (ii) . □

**Def.** *Sei $(G, \cdot)$ eine Gruppe, und $(H, *)$ eine Menge mit einer Multiplikation $* : H \times H \to H$. Eine Bijektion $\phi : G \to H$ heißt ein Isomorphismus, falls für alle $a, b \in G$ gilt: $\phi(a \cdot b) = \phi(a) * \phi(b)$.*

**Lemma A1** *Ist $\phi : G \to H$ ein Isomorphismus, so ist $H$ auch eine Gruppe.*

**Beweis.** Wir müssen (G1), (G2), (G3) nachweisen.

(G1): Betrachte $a', b', c' \in H$. Z.z.: $(a' * b') * c' = a' * (b' * c')$. Da $\phi$ surjektiv ist, gibt es $a, b, c \in G$ mit $\phi(a) = a'$, $\phi(b) = b'$, $\phi(c) = c'$. Dann ist

$$\begin{array}{ccccc} \phi((a \cdot b) \cdot c) & = & \phi(a \cdot b) * c' & = & (a' * b') * c' \\ \| \ (G1) & & & & \\ \phi(a \cdot (b \cdot c)) & = & a' * \phi(b \cdot c) & = & a' * (b' * c') \end{array}$$

. (G1) ist bewiesen.

(G2): Setze $e' := \phi(e)$. Z.z.: $e' * a' = a'$ für alle $a' \in H$. Da $\phi$ surjektiv ist, gibt es $a$ mit $\phi(a) = a'$.

$$\begin{array}{ccc} \phi(e \cdot a) & = & e' * a' \\ \| & & \\ \phi(a) & = & a' \end{array}$$

. (G2) ist bewiesen.

(G3): Nehme ein $a' \in H$. Da $\phi$ surjektiv ist, gibt es $a \in G$ mit $\phi(a) = a'$. Nach (G3) gibt es ein $b \in G$ mit $b \cdot a = e$. Es gilt:

$$\begin{array}{ccccc} \phi(b \cdot a) & = & \phi(b) * \phi(a) & = & b' * a' \\ \| & & & & \\ \phi(e) & = & & & e' \end{array}$$

, d.h. $b' * a' = e'$. □

Wie kann man beweisen, dass $(H, *)$ eine Gruppe ist? (z.B. wenn die Multiplikation $*$ mit Hilfe einer Tabelle gegeben ist)
(G2) ist einfach nachzuweisen: irgendeine Zeile muss die 0-Zeile wiederholen.
(G3) ist einfach nachzuweisen: In jeder Spalte muss $e$ stehen.
Wie beweist man Assoziativität?
Man kann

**Satz A3**: *Untergruppe einer Gruppe ist eine Gruppe.*

**Wicht. Bsp.**: $(\mathcal{S}_M, \circ)$ *ist eine Gruppe,*
und **Lemma A1**: *Ist eine Gruppe* $(G, \cdot)$ *zu* $(H, *)$ *isomorph, so ist* $(H, *)$ *eine Gruppe*

benutzen.
Man muss eine Untergruppe von geeigneten $\mathcal{S}_M$ finden, die zu $(H, *)$ isomorph ist.

# Exkurs in die Mengenlehre: Äquivalenzrelationen

Sei $A$ eine Menge. Eine Relation auf dieser Menge ist eine Teilmenge $R$ der Menge $A \times A$.

**Wiederholung:** Das Produkt von Mengen $A$, $B$ (Bez: $A \times B$) ist die Menge aller Paare $(a, b)$, wobei $a \in A$, $b \in B$ ist. Also ist die Menge $A \times A$ die Menge aller Paare von Elementen aus $A$.

**Warum das Wort „Relation“?**

**Bsp.** Man kann „$\leq$“ als eine Relation $R$ auf der Menge $\mathbb{R}$ der reellen Zahlen wie folgt verstehen:

$R := \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \leq b\}$.

**Zum Bsp.** $(1, 2) \in R$ (weil $1 \leq 2$); $(-1, -1) \in R$ (weil $-1 \leq -1$); aber $(2, 1) \notin R$ (weil $2 \not\leq 1$).

Dann gilt nach Konstruktion von diesem $R$ : $(a, b) \in R \iff a \leq b$.

**Bsp.** Die Gleicheit „$=$“ kann man auch als eine Relation auf der Menge $\mathbb{R}$ der reellen Zahlen verstehen. In diesem Fall ist

$R = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a = b\}$.

Dann gilt nach Konstruktion von diesem $R$ : $(a, b) \in R \iff a = b$.

Für endlichen Mengen können wir eine Relation als eine Liste von allen Elementen von $R$ darstellen. Z.B.:
$R := \{(a, a), (a, b), (b, b), (b, a), (c, c)\}$ ist eine Relation auf der drei-elementigen Menge $M := \{a, b, c\}$.

(Wir schreiben $a \sim b$ und sagen, dass die Elemente $a$, $b$ in Relation zueinander stehen, falls $(a, b) \in R$ .)
Diese Schreibweise ist mit den Beispielen oben kompatibel (in der Relation „kleiner oder gleich“ oder in der Relation „gleich“ bedeutet $a \sim b$ dass $a \leq b$ bzw. $a = b$.)
Eine Relation heißt eine Äquivalenzrelation, falls sie die folgenden Eigenschaften hat:

- **(Reflexivität)** $\forall a \in A$ ist $a \sim a$.
- **(Symmetrie)** $\forall a, b \in A$ gilt: ist $a \sim b$, so ist $b \sim a$.
- **(Transitivität)** $\forall a, b, c \in A$ gilt: ist $a \sim b$ und ist $b \sim c$ so ist $a \sim c$.

- **(Reflexivität)** $\forall a \in A$ ist $a \sim a$.
- **(Symmetrie)** $\forall a, b \in A$ gilt: ist $a \sim b$, so ist $b \sim a$.
- **(Transitivität)** $\forall a, b, c \in A$ gilt: ist $a \sim b$ und ist $b \sim c$ so ist $a \sim c$.

**Bsp (Wikipedia).** $A$ sei die Menge aller Nutztiere in einem landwirtschaftlichen Betrieb.
Wir definieren nun eine Relation: zwei Tiere stehen in Relation zueinander, wenn sie von derselben Art sind.
Die Kuh Erna zum Beispiel steht mit dem Ochsen Bruno in Relation, aber nicht mit dem Huhn Betti.
Dies ist eine Äquivalenzrelation: Jedes Tier ist von derselben Art wie es selbst (= "reflexiv"). Ist ein Tier von derselben Art wie das andere, dann ist das andere auch von derselben Art wie das eine (= "symmetrisch"). Wenn Erna und Lisa von derselben Art sind und Lisa und Bruno von derselben Art, dann sind Erna und Bruno von derselben Art (z.B. Rinder; = "transitiv").

- **(Reflexivität)** $\forall a \in A$ ist $a \sim a$.
- **(Symmetrie)** $\forall a, b \in A$ gilt: ist $a \sim b$, so ist $b \sim a$.
- **(Transitivität)** $\forall a, b, c \in A$ gilt: ist $a \sim b$ und ist $b \sim c$ so ist $a \sim c$.

**Bsp.** Triviale Relation. Jedes Element steht nur mit sich selbst in Relation. $R = \{(a, a) \mid a \in A\}$ (Das Beispiel „Gleicheit“ oben ist eine solche Relation.)
**Bsp.** Alle Elemente stehen in Relation. $R = A \times A$.
**NichtBsp.** Die Relation „$\leq$“ auf $\mathbb{R}$ (d.h. $R = \{(a, b) \mid a \leq b\}$) ist keine Äquivalenzrelation. In der Tat,

- **(Reflexivität)** ist erfüllt: $a \leq a$.
- **(Transitivität)** ist auch erfüllt: wenn $a \leq b$ und $b \leq c$ ist, so ist $a \leq c$.
- **(Symmetrie)** ist aber nicht erfüllt: Man kann (mehrere) Beispiele von $a, b \in \mathbb{R}$ finden, sodass $a \leq b$, aber $b \not\leq a$, zum Beispiel $a = 1$ und $b = 2$.

# Äquivalenzrelation auf drei-elementiger Menge aus dem Bsp. oben

**Wir zeigen, dass $R := \{(a,a),(a,b),(b,b),(b,a),(c,c)\}$ eine Äquivalenzrelation auf der Menge $M := \{a,b,c\}$ ist.**

- **(Reflexivität)** $x \sim x$ Da $(a,a),(b,b),(c,c) \in R$, ist die Relation reflexiv.
- **(Symmetrie)** ist $x \sim y$, so ist $y \sim x$. Die einzigen in Frage kommenden Paare sind $(a,b)$ und $(b,a)$. Da beide in $R$ liegen, ist die Symmetrieeigenschaft erfüllt.
- **(Transitivität)** Ist $x \sim y$ und $y \sim z$ so ist $x \sim z$ Da die Reflexivität erfüllt ist, reicht es zu zeigen: es gibt keine verketteten Paare $x \sim y$ und $y \sim z$ so dass $x, y, z$ paarweise verschieden sind.

# Transitivität ausführlicher:

$R := \{(a,a),(a,b),(b,b),(b,a),(c,c)\}$
Eine Relation $R \subseteq M \times M$ ist transitiv falls für jede $x, y, z \in M$ gilt: Ist $x \sim y$ und $y \sim z$ so ist $x \sim z$
Für $x = a$: Für $x \sim y$ und $y \sim z$ gibt es folgende Möglichkeiten:
$a \sim b$ und $b \sim b$ (in diesem Fall ist tatsächlich $a \sim b$.)
$a \sim a$ und $a \sim b$ (in diesem Fall ist tatsächlich $a \sim b$.)
$a \sim a$ und $a \sim a$ (in diesem Fall ist tatsächlich $a \sim a$.)
$a \sim b$ und $b \sim a$ (in diesem Fall ist tatsächlich $a \sim a$.)
Für $x = b$: Für die $x \sim y$ und $y \sim z$ gibt es folgende Möglichkeiten:
$b \sim a$ und $a \sim b$ (in diesem Fall ist tatsächlich $b \sim b$.)
$b \sim a$ und $a \sim a$ (in diesem Fall ist tatsächlich $b \sim a$.)
$b \sim b$ und $b \sim b$ (in diesem Fall ist tatsächlich $b \sim b$.)
$b \sim b$ und $b \sim a$ (in diesem Fall ist tatsächlich $b \sim a$)
Für $x = c$: Für $x \sim y$ und $y \sim z$ gibt es nur diese Möglichkeiten:
$c \sim c$ und $c \sim c$ (in diesem Fall ist tatsächlich $c \sim c$.)

# $GL_n$

**Bsp:** Wir betrachten $GL_n := \{A \in Mat(n,n) \mid det(A) \neq 0\}$ (die Bedingung $\det(A) \neq 0$ bedeutet nach Satz 18/Lemma 20, dass $A$ nichtausgeartet ist).
Wir definieren die folgende Relation auf $GL_n$:
$A \sim B \iff \det(A^{-1}B) > 0$.
Das ist eine Äquivalenzrelation:

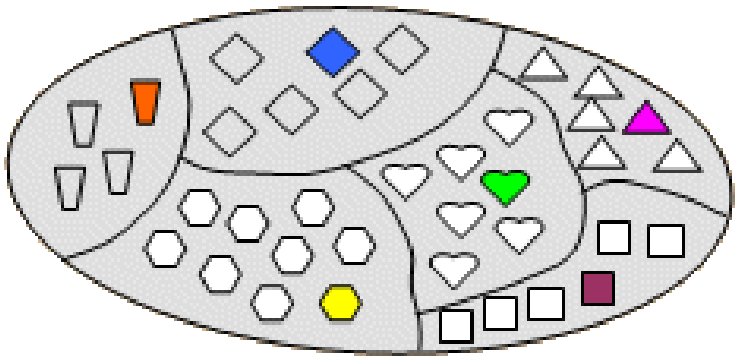
- **(Reflexivität)** $\forall A \in GL_n$ ist $\det(A^{-1}A) = \det(Id) = 1 > 0$, also $A \sim A$.
- **(Symmetrie)** $\forall A, B \in GL_n$ gilt: Ist $A \sim B$, also ist $\det(A^{-1}B) = \frac{\det(B)}{\det(A)} > 0$, so ist $\det(B^{-1}A) = \frac{\det(A)}{\det(B)} > 0$, also $B \sim A$.
- **(Transitivität)** $\forall A, B, C \in GL_n$ gilt: Ist $\det(A^{-1}B) = \frac{\det(B)}{\det(A)} > 0$ und $\det(B^{-1}C) = \frac{\det(C)}{\det(B)} > 0$ so ist $\frac{\det(B)}{\det(A)} \frac{\det(C)}{\det(B)} = \frac{\det(C)}{\det(A)} = \det(A^{-1}C) > 0$, also $A \sim C$.

# Zerlegung einer Menge: http://henked.de/begriffe/aequivalenzrelation.htm

Eine Zerlegung einer nichtleeren Menge $M$ ist eine Menge $\mathbb{M} = \{M_1, M_2, ...\}$ von Teilmengen von $M$ mit den Eigenschaften:

(I) $\bigcup_{M \in \mathbb{M}} M := \underbrace{M_1 \cup M_2 \cup ...}_{\text{falls endlich}} = M$

(II) $M_i \cap M_k = \varnothing$, falls $M_i \neq M_k$.



(**In Worten:** Jedes Element von $M$ ist in genau einer dieser Teilmengen von $\mathbb{M}$ enthalten.)

**Bemerkung: Jede Zerlegung induziert eine Äquivalenzrelation.**

**Beweis:** Sei $\mathbb{M}$ eine Zerlegung von $M$. Wir definieren die Relation $R \subseteq M \times M$ wie folgt: $x \sim y \iff x, y \in M_i$ für ein $M_i \in \mathbb{M}$.

- **Reflexivität:** $x \sim x$ offensichtlich.
- **Symmetrie:** Falls $x, y$ in der gleichen Menge $M_i$ liegen, so liegen $y, x$ auch in der gleichen Menge $M_i$
- **Transitivität:** Liegen $x, y$ in der gleichen Menge $M_i$, und liegen $y, z$ in der gleichen Menge $M_j$, so gilt $M_i = M_j$, weil $y$ nur in einer Menge $M_i$ liegt. Dann ist $x \sim z$.

# Jede Äquivalenzrelation induziert eine Zerlegung

Sei $R$ eine Äquivalenzrelation auf $M \neq \varnothing$. Dann definiert man für jedes $x \in M \quad [x] := \{y \in M \mid x \sim y\} \subseteq M$ und
$\mathbb{M} := \{[x] | x \in M\}$.

**Satz A4.** $\mathbb{M}$ ist eine Zerlegung von $M$

**Beweis:** Z.z.: (I) $\bigcup_{x \in M} [x] = M$ und (II) $[x] \cap [y] \neq \varnothing \iff [x] = [y]$.

(I) Da $y \sim y$ ist, ist $y \in [y]$ und deswegen $y \in \bigcup_{x \in M} [x]$.

(II) $\Longleftarrow$: offensichtlich, da $[x] \neq \varnothing$ ist.
$\Longrightarrow$: Angennomen $[x] \cap [y] \neq \varnothing$,also $\exists z \in [x] \cap [y]$. Dann ist $z \sim x$ und $z \sim y$.Z.z.: (a) $[x] \subseteq [y]$, d.h. $w \sim x \Longrightarrow w \sim y$; und (b) $[y] \subseteq [x]$,d.h. $w \sim y \Longrightarrow w \sim x$.

(a) Aus $w \sim x$ und $\underbrace{x \sim z}_{\text{Symmetrie}} \overset{\text{Transitivität}}{\Longrightarrow} w \sim z$. Also $w \sim z$ und

$z \sim y \overset{\text{Transitivität}}{\Longrightarrow} w \sim y$, also $w \in [y]$.

(b) ist analog. □

# Bsp. Die Äquivalentrelation
$R := \{(a, a), (a, b), (b, b), (b, a), (c, c)\}$

Die Äquivalenzklasse von $a$ besteht aus den Elementen, die zu $a$ äquivalent sind. In unserem Fall ist sie $\{a, b\}$. Also, $[a] = \{a, b\}$.
Die Äquivalenzklasse von $b$ ist gleich Äquivalenzklasse von $a$, weil $a \sim b$.
Die Äquivalenzklasse von $c$ besteht aus den Elementen, die zu $c$ äquivalent sind. In unserem Fall ist sie $\{c\}$. Also, $[c] = \{c\}$.

# Wicht. Bsp.: Äquivalenzklassen in $GL_n$

**Wiederholung.** $GL_n := \{A \in Mat(n,n) \mid det(A) \neq 0\}$; $A \sim B \iff \det(A^{-1}B) > 0$.
Bestimmen wir jetzt die Äquivalenzklasse bzgl. dieser Äquivalenzrelation.
Ich behaupte, dass es zwei Äquivalenzklassen gibt.
$GL_n^+ := \{A \in GL_n \mid \det(A) > 0\}$ und $GL_n^- := \{A \in GL_n \mid \det(A) < 0\}$.
In der Tat, zwei Matrizen aus $GL_n^+$, z.B. $A$ und $B$, sind zueinander äquivalent: $\det(A^{-1}B) = \frac{\det(B)}{\det(A)} > 0$ weil $\det(A) > 0$, $\det(B) > 0$.
Zwei Matrizen aus $GL_n^-$, z.B. $A$ und $B$, sind ebenfalls zueinander äquivalent: $\det(A^{-1}B) = \frac{\det(B)}{\det(A)} > 0$ weil $\det(A) < 0$, $\det(B) < 0$.
Wenn $A$ in $GL_n^+$ und $B$ in $GL_n^-$ liegt, dann ist $A$ zu $B$ nicht äquivalent: $\det(A^{-1}B) = \frac{\det(B)}{\det(A)} < 0$.
Also ist die Äquivalenzklasse einer Matrix mit $\det > 0$, z.B. der Matrix $Id$, $[Id] := \{A \in GL_n \mid \det(A) > 0\}$.
Die Äquivalenzklasse einer Matrix $B$ mit $\det(B) < 0$ ist $[B] := \{A \in GL_n \mid \det(A) < 0\}$.
**Bemerkung.** In diesem Bsp ist offensichtlich, dass $[Id] \cup [B] = GL_n$ und $[Id] \cap [B] = \varnothing$, weil jede Matrix mit $\det \neq 0$ entweder $\det > 0$ oder $\det < 0$ hat.

# Die Menge $\mathbb{Z}_q$

Es sei $M = \mathbb{Z}$ (Die Menge der ganzen Zahlen), $q \in \mathbb{N}$ eine fest gewählte Zahl, $q \neq 0$. Definiere die Relation $\overset{\text{mod } q}{\equiv}$ wie folgt:
$a \overset{\text{mod } q}{\equiv} b \iff q \mid a - b$ , d.h. $a - b = q \cdot k$ für irgendein $k \in \mathbb{Z}$.
**Bsp.** Sei $q = 5$. Dann ist $-3 \overset{\text{mod } 5}{\equiv} 2 \overset{\text{mod } 5}{\equiv} 7 \overset{\text{mod } 5}{\equiv} 12$. (Eigentlich, für jedes $k \in \mathbb{Z}$ ist $2 \overset{\text{mod } 5}{\equiv} 5k + 2$, weil $5 \mid 5k = 2 - (5k + 2)$ )

**Lemma A2.** *Die Relation $\overset{mod\ q}{\equiv}$ ist eine Äquivalenzrelation*

**Beweis.** (Reflexivität): $a \overset{\text{mod } q}{\equiv} a$, weil $a - a = 0 = q \cdot 0$.
(Symmetrie): Z.z: Ist $a \overset{\text{mod } q}{\equiv} b$, so ist $b \overset{\text{mod } q}{\equiv} a$.
In der Tat, $a - b = q \cdot k \implies b - a = q \cdot (-k)$.
(Transitivität): Z.z.: Ist $a \overset{\text{mod } q}{\equiv} b$ und $b \overset{\text{mod } q}{\equiv} c$, so ist $a \overset{\text{mod } q}{\equiv} c$.
Tatsächlich, ist $a = q \cdot k_1 + b$ und ist $b = q \cdot k_2 + c$, so ist
$a = q \cdot k_1 + q \cdot k_2 + c$, also $a - c = q(k_1 + k_2)$. □

**Bsp.** *Bezüglich* $\overset{mod\ 5}{\equiv}$ *gibt es genau* 5 *Äquivalenzklassen:* $[0]$, $[1]$, $[2]$, $[3]$, $[4]$. *Tatsächlich, jedes* $a \in \mathbb{Z}$ *kann man in der Form* $k \cdot 5 + r$ *darstellen,wobei* $0 \leq r < 5$*(dividieren mit Rest), also* $[a] = [r]$, *und diese* 5 *Teilmengen sind verschieden.*

**Bsp.** *Bezüglich* $\overset{mod\ q}{\equiv}$ *gibt es genau* $q$ *Äquivalenzklassen:* $[0]$, ... , $[q-1]$.

# Gruppenstruktur auf $\mathbb{Z}_q$

Addition $\overset{\text{mod } q}{+}$ auf $\mathbb{Z}_q$ : $[a] \overset{\text{mod } q}{+} [b] := [a+b]$.

**Bemerkung** Die Addition $\overset{\text{mod } q}{+}$ ist wohldefiniert: falls wir statt $a$ und $b$ andere Repräsentanten der Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird das Ergebnis nicht geändert. Tatsächlich,

$[a + k_1 \cdot q] \overset{\text{mod } q}{+} [b + k_2 \cdot q] = [a + b + (k_1 + k_2) \cdot q] = [a + b]$.

**Bsp.** $[1] \overset{\text{mod } 5}{+} [2] = [3]$, $[2] \overset{\text{mod } 5}{+} [3] = [5] = [0]$, $[5] \overset{\text{mod } 5}{+} [6] = [1]$.

**Lemma A3** $(\mathbb{Z}_q, \overset{mod\ q}{+})$ *ist eine abel'sche Gruppe*

**Beweis.** (G1): $[a] \overset{\text{mod } q}{+} ([b] \overset{\text{mod } q}{+} [c]) = [a] \overset{\text{mod } q}{+} [b+c] =$

$[a + (b + c)] = [(a + b) + c] = [a + b] \overset{\text{mod } q}{+} [c] = ([a] \overset{\text{mod } q}{+} [b]) \overset{\text{mod } q}{+} [c]$.

(G2): $[0] \overset{\text{mod } q}{+} [a] = [0 + a] = [a]$, also $e = [0]$.

(G3): $[-a] \overset{\text{mod } q}{+} [a] = [0]$.

Abel'sch: $[a] \overset{\text{mod } q}{+} [b] = [a + b] = [b + a] = [b] \overset{\text{mod } q}{+} [a]$. □

**Def.** Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir mit 0 bezeichen;

(R2) die Multiplikation „$\cdot$" ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

**Bsp.** $(\mathbb{R}, \cdot, +)$ und $(\mathbb{C}, \cdot, +)$ sind kommutative Ringe.

**Lemma A4.** $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

**Beweis.** $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.
Wir addieren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. □

# Kommutativer Ring $(\mathbb{Z}_q, +, \cdot)$

Wir werden auf $\mathbb{Z}_q$ die Struktur eines kommutativen Rings definieren. $(\mathbb{Z}, \overset{\text{mod } q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze $[a] \overset{\text{mod } q}{\cdot} [b] := [a \cdot b]$.

**Bsp.** $[1] \overset{\text{mod } q}{\cdot} [2] = [2]$, $[2] \overset{\text{mod } q}{\cdot} [3] = [6] = [1]$, $[4] \overset{\text{mod } q}{\cdot} [3] = [12] = [2]$.

**Bemerkung** Die Multiplikation $\overset{\text{mod } q}{\cdot}$ ist wohldefiniert:falls wir statt $a$ und $b$ die anderen Repräsentanten der Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird das Ergebnis nicht geändert. Tatsächlich,

$$[a + k_1 \cdot q] \overset{\text{mod } q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$$
$$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b].$$

# Beweis von (R2) und (R3)

ist wie in Lemma A3

(R3) $[a] \overset{\text{mod } q}{\cdot} ([b] \overset{\text{mod } q}{+} [c]) = [a \cdot (b + c)] = [a \cdot b + a \cdot c] = [a] \overset{\text{mod } q}{\cdot} [b] \overset{\text{mod } q}{+} [a] \overset{\text{mod } q}{\cdot} [c]$.

# Rechnen Sie selbst in $\mathbb{Z}_5$

$$[2] \cdot [5] + [6] \cdot [3] + [7] \cdot [4] =$$
$$= [2] \cdot [0] + [1] \cdot [3] + [2] \cdot [-1] = [0] + [3] - [2]$$
$$= [6] \quad (= [1] = [-4] = [11] = [1298347746542831]).$$

# Rechnen Sie bitte noch einmal in $\mathbb{Z}_5$

$$[153] \cdot [1723] + ([1600] \cdot [371] - [3]) \cdot [6] =$$

$$[3] \cdot [3] + ([0] - [3]) \cdot [1] = [9 - 3] = [6] = [1]$$