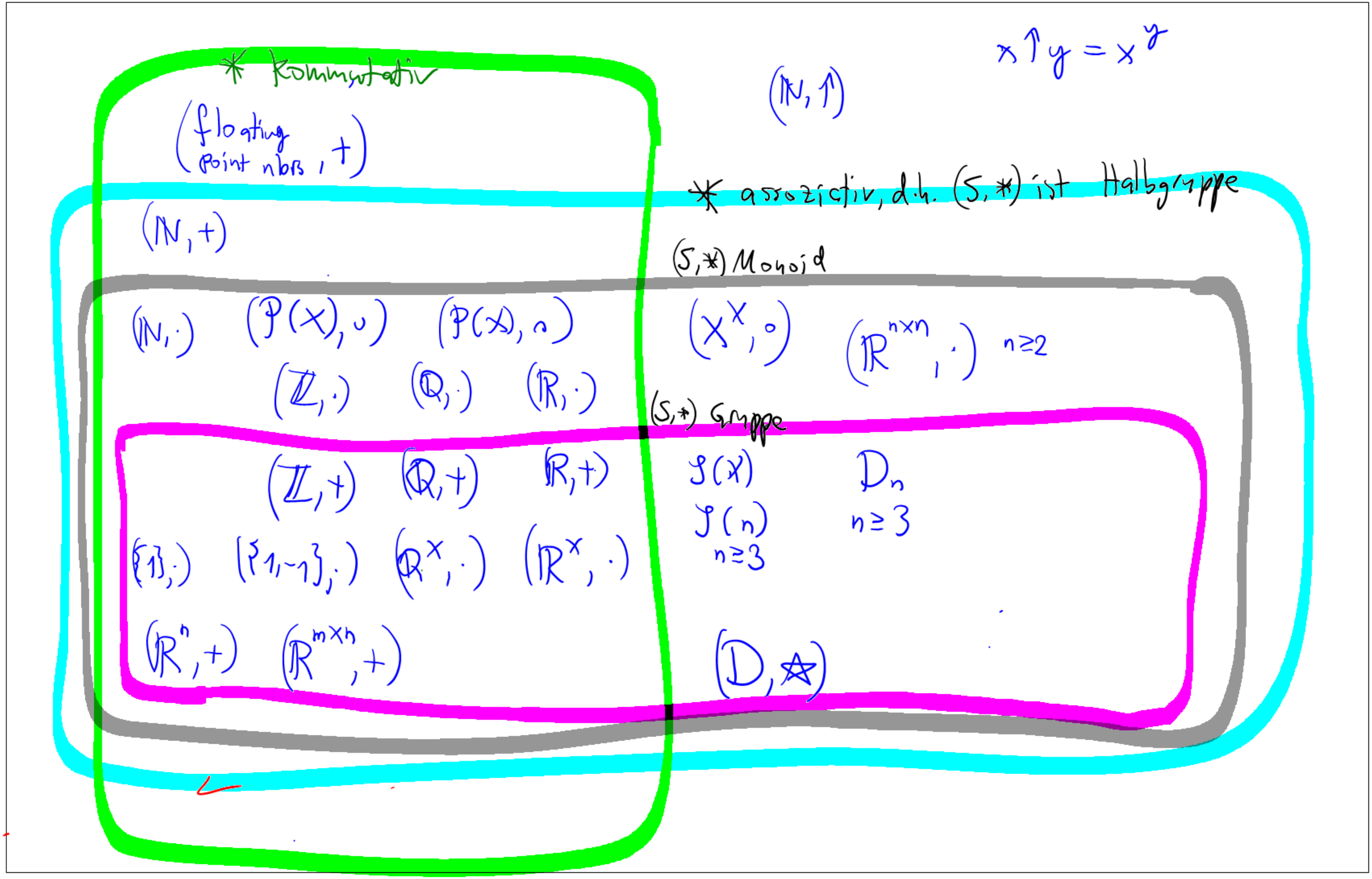
Lineare Algebra I für die Fachrichtung Informatik

Wintersemester 2023/24

Beispiele für Mengen S mit binärer Verknüpfung $*: S \times S \longrightarrow S$



Def: $(G, *)$ ist eine Gruppe, wenn

$$\boxed{(G, *) \text{ ist Monoid mit Neutralelement } e}$$

und $\boxed{\forall x \in G : \exists y \in G \quad x * y = e = y * x}$

__Def:__ $(G, *)$ ist eine Gruppe, wenn

$$\boxed{(G,*) \text{ ist Halbgruppe}}$$

und $\boxed{\exists e \in G : \forall x \in G : x * e = x = e * x}$

und $\boxed{\forall x \in G : \exists y \in G \quad x * y = e = y * x}$

Def: $(G, *)$ ist eine Gruppe, wenn

$$\boxed{* : G \times G \longrightarrow G}$$

und $\boxed{\forall x, y, z \in G: \ (x * y) * z = x * (y * z)}$

und $\boxed{\exists e \in G: \forall x \in G: \ x * e = x = e * x}$

und $\boxed{\forall x \in G: \exists y \in G \ \ x * y = e = y * x}$

Beispiel: X Menge

$$S(X) := \left(\{ f : X \to X \mid f \text{ bijektiv} \}, \circ \right)$$

$$X = \{1, 2, \dots, n\} \qquad n \in \mathbb{N}$$

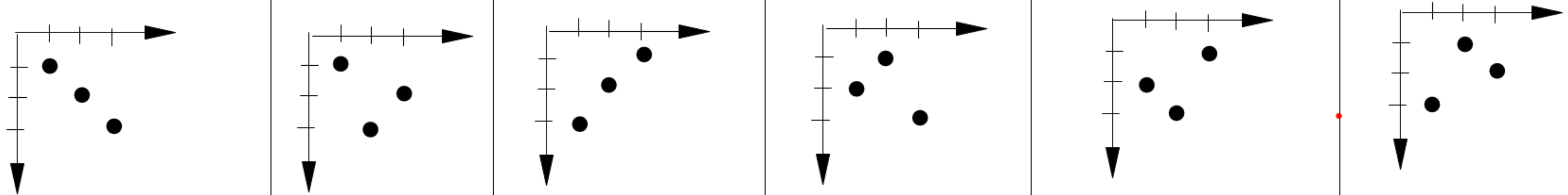
$$S(n) := S(\{1, \dots, n\})$$

$$= \{ \sigma : \{1, \dots, n\} \to \{1, \dots, n\} \mid \sigma \text{ bijektiv} \}$$

$S(n)$ $\quad S_n \quad (\mathrm{Sym}(n)) \quad |S(n)| = n!$

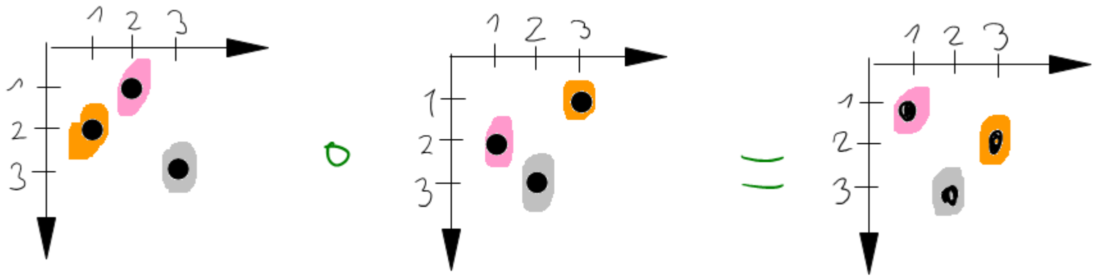
z.B. $S(3)$

id					
$\begin{array}{c\|c\|c}1&2&3\\\hline 1&2&3\end{array}$	$\begin{array}{c\|c\|c}1&2&3\\\hline 1&3&2\end{array}$	$\begin{array}{c\|c\|c}1&2&3\\\hline 3&2&1\end{array}$	$\begin{array}{c\|c\|c}1&2&3\\\hline 2&1&3\end{array}$	$\begin{array}{c\|c\|c}1&2&3\\\hline 2&3&1\end{array}$	$\begin{array}{c\|c\|c}1&2&3\\\hline 3&1&2\end{array}$
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$



$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$	$\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$	$\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$

z.B.:

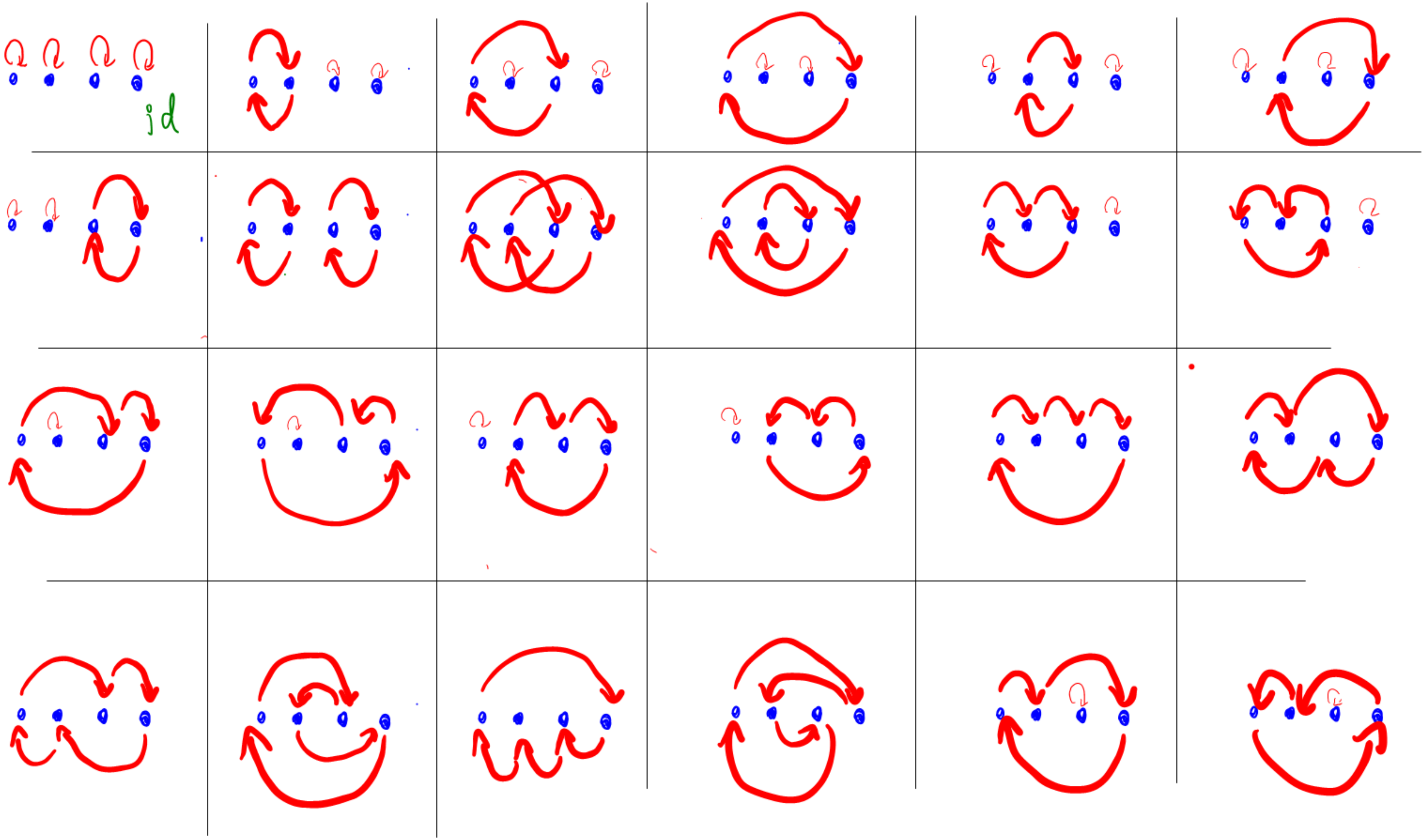


$$\begin{array}{c} 1\\ \downarrow\\ 2\\ \downarrow\\ 1 \end{array} \quad \begin{array}{c} 2\\ \downarrow\\ 3\\ \downarrow\\ 3 \end{array} \quad \begin{array}{c} 3\\ \downarrow\\ 1\\ \downarrow\\ 2 \end{array}$$

$$\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 1 & 3 \end{array} \circ \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 3 & 1 \end{array} = \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 3 & 2 \end{array}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

z.B. $S(4)$ $\quad |S(4)| = 4! = 24$

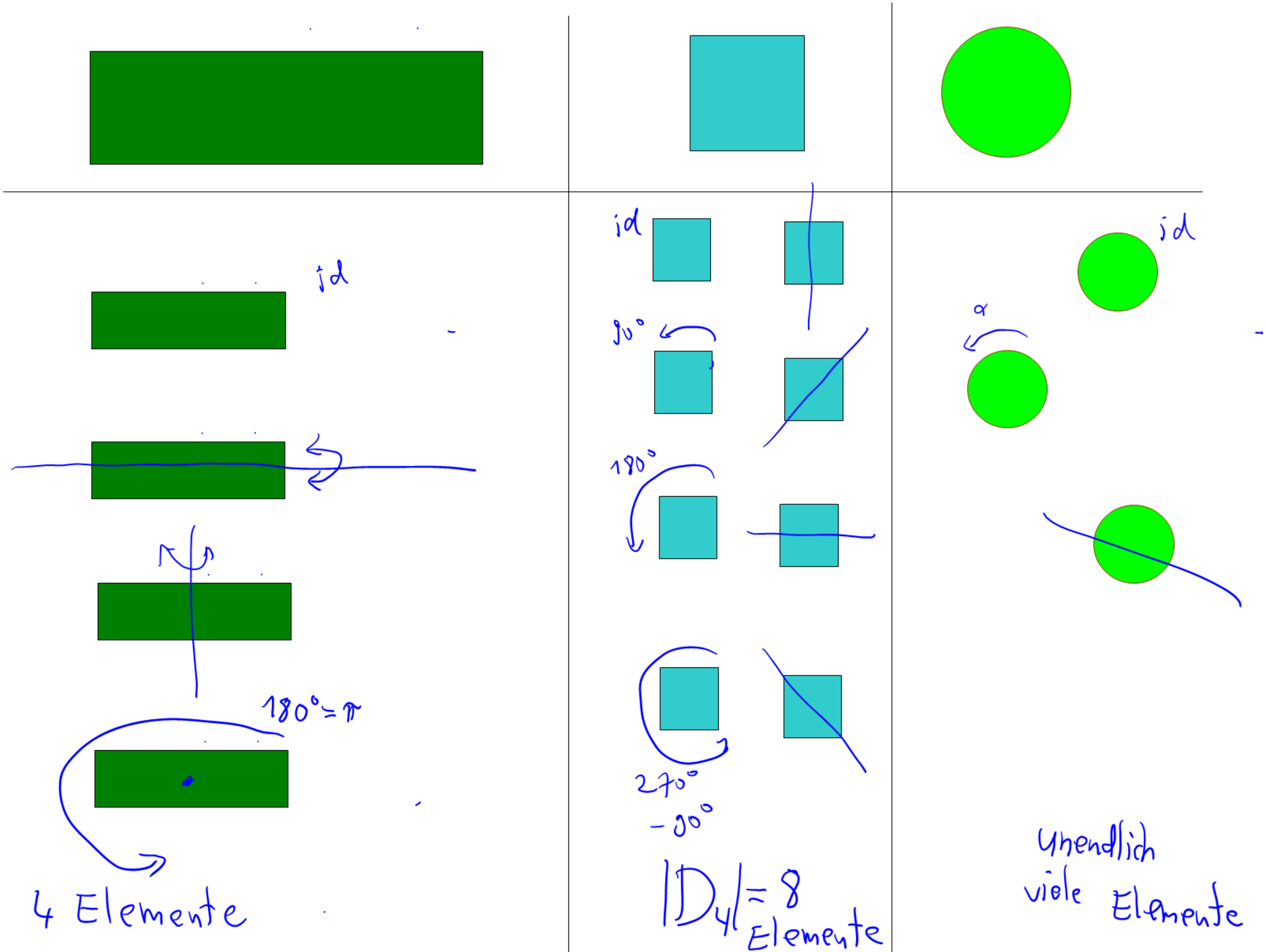


Symmetrie

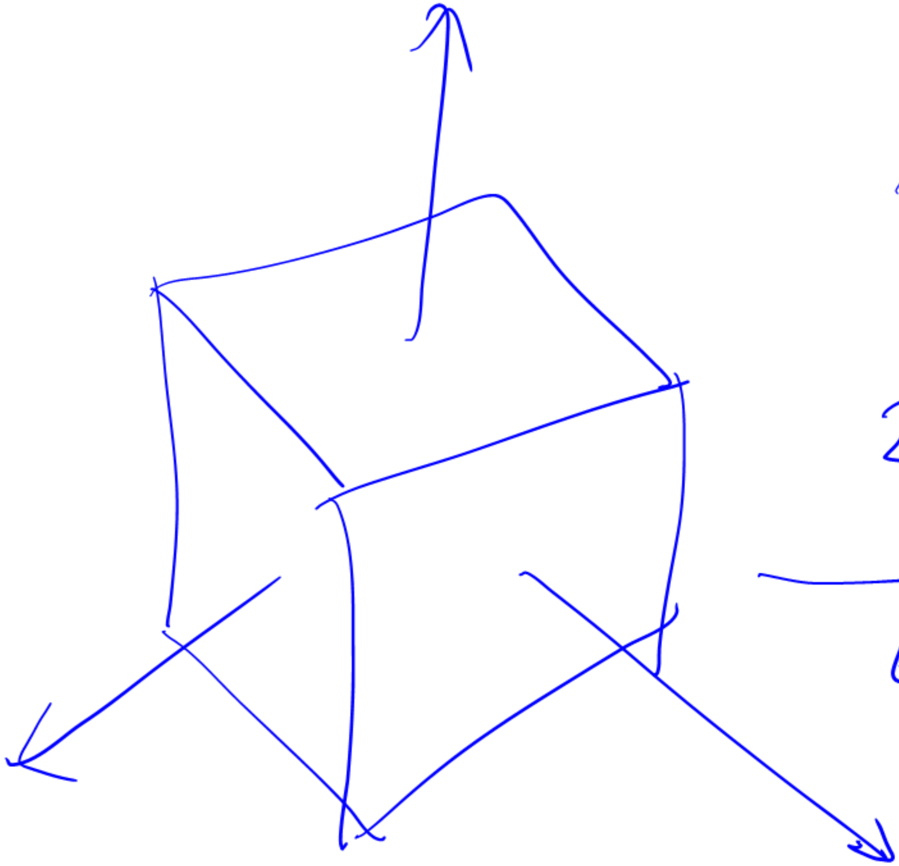
$A \subseteq \mathbb{R}^2$

$$G = \left\{ f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \ \text{Drehung oder Spiegelung} \ \middle| \ f(A) = A \right\}$$

Symmetrie-Gruppe von A


id
180°=π
4 Elemente
id
90°
180°
270°
-90°
|D4|=8
Elemente
id
α
unendlich
viele Elemente

$A \subseteq \mathbb{R}^3$; $A \subseteq \mathbb{R}^n$

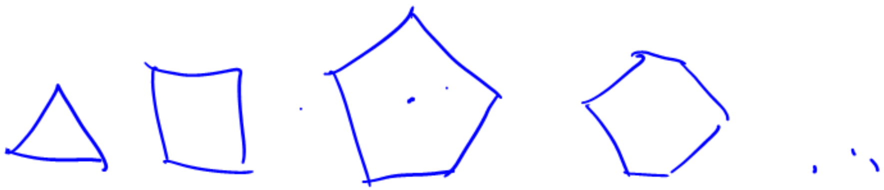


24 Drehungen

24 Spiegelungen

48 Symmetrien

A Regelmäßiges n-Eck



$n=3$ $n=4$ $n=5$ $n=6$ ...

Def: $n \in \mathbb{N}$ $n \geq 3$

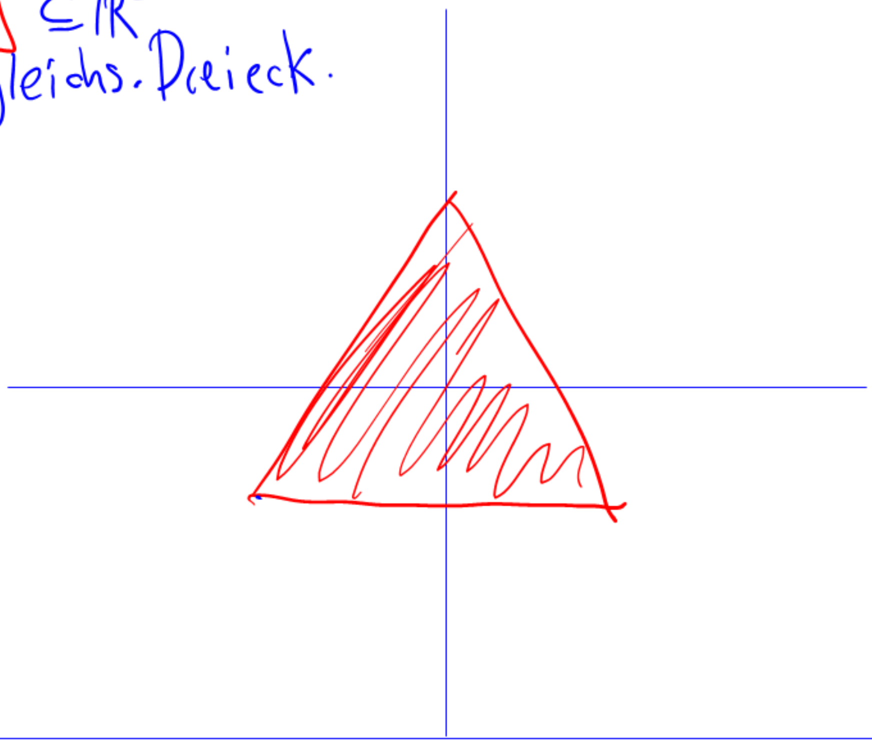
D_n = Symmetriegruppe von A

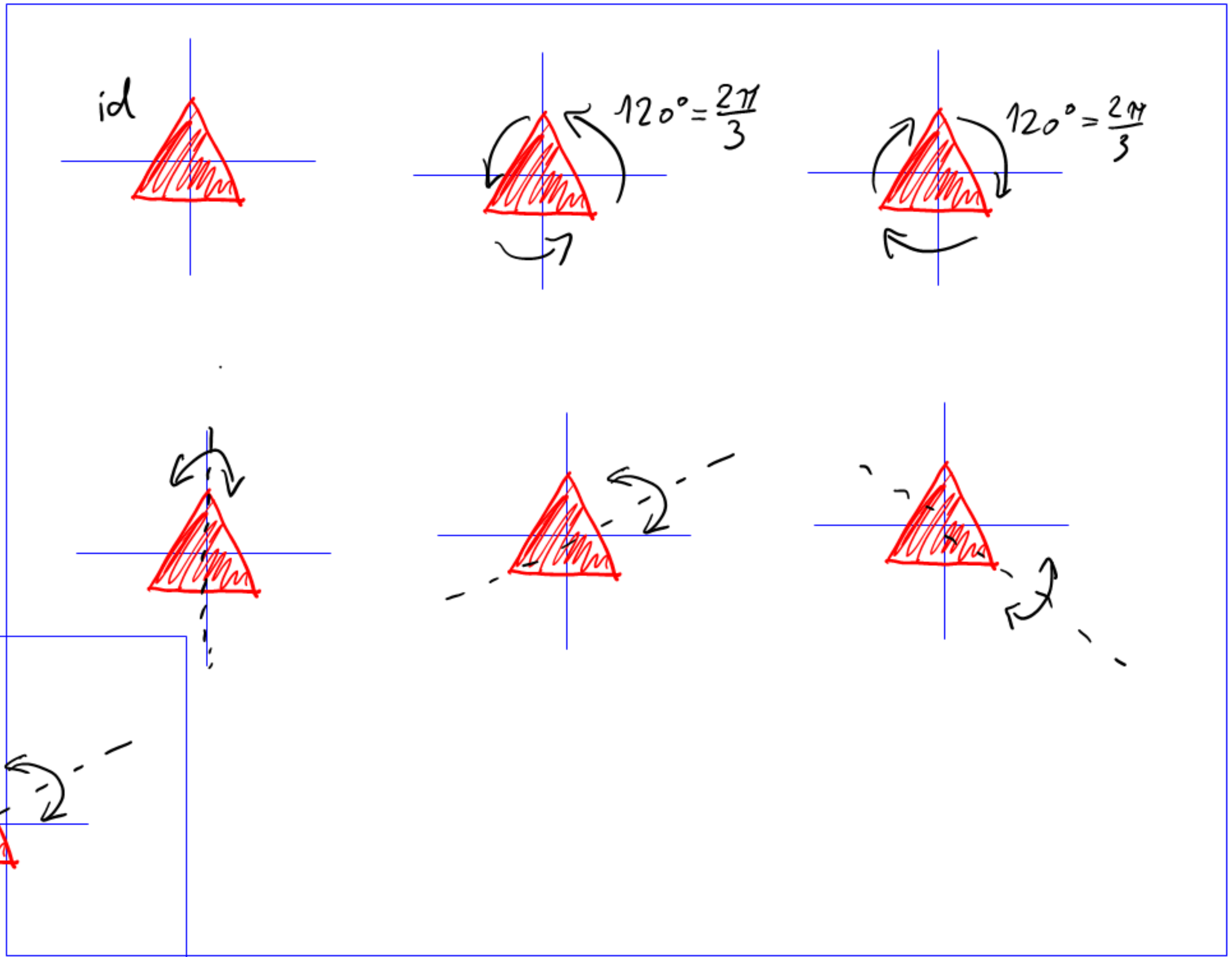
Diedegruppe $|D_n| = n + n$
$= 2n$

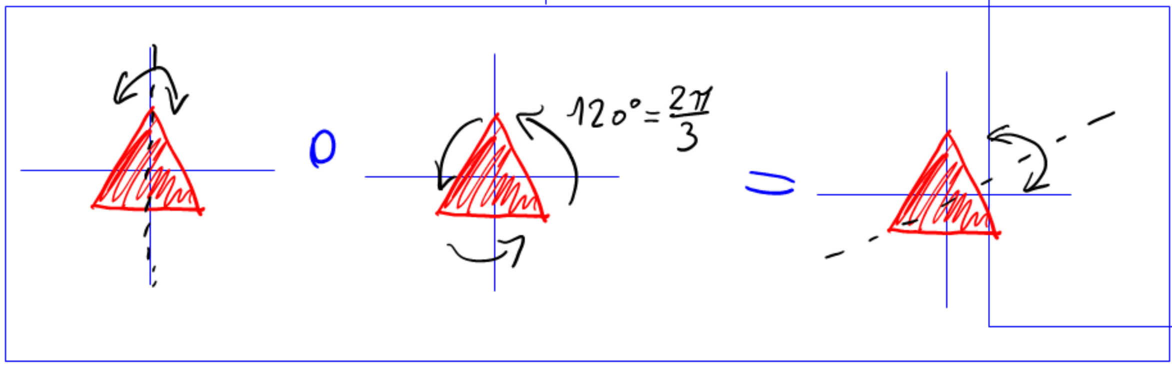
z.B.: $D_3 = \left\{ f : \mathbb{R}^2 \to \mathbb{R}^2 \;\middle|\; \begin{array}{c} \text{Drehung oder Spiegelung} \\ \text{und} \\ f(\Delta) = \Delta \end{array} \right\}$ $\qquad |D_3| = 2 \cdot 3 = 6$

$X = \mathbb{R}^2$

$\Delta \subseteq \mathbb{R}^2$
gleichs. Dreieck.







Youtube-Empfehlung zum Thema

3Blue1Brown

Group theory, abstraction, and the
196,883-dimensional monster

https://youtu.be/mH0oCDa74tE

Def 3.2.5 $(G, *)$ mit Neutralelement $e_G \in G$.

$H \subseteq G$ heißt **Untergruppe** von G, wenn

(i) $\boxed{e_G \in H}$ ← enthält Neutralelement

(ii) $\boxed{\forall a, b \in H: \quad a * b \in H}$ ← abgeschlossen unter $*$

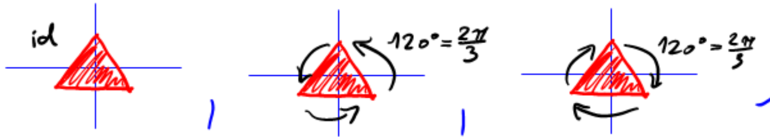
(iii) $\boxed{\forall a \in H: \quad a^{-1} \in H}$ ← abgeschlossen unter $(\,)^{-1}$

Wenn $H \subseteq G$ Untergruppe

$\Longrightarrow$ $(H, *)$ Gruppe

$(\mathbb{R} \setminus \{0\}, \cdot)$ ist keine Untergruppe von $(\mathbb{R}, +)$.

z.B.:

$\{$ 

$\}$ Untergruppe von D_3

$\mathbb{Z}$ Untergruppe von $(\mathbb{Q},+)$

$\mathbb{Q}$ Untergruppe von $(\mathbb{R},+)$

$\{t\in\mathbb{R} \mid t>0\} = (0,\infty) =]0,\infty[$
ist Untergruppe von $(\mathbb{R},\cdot)^\times = (\mathbb{R}\setminus\{0\},\cdot)$

$U \subseteq \mathbb{R}^n$ Untervektorraum
$\Longrightarrow$ U Untergruppe von $(\mathbb{R}^n,+)$

$\mathbb{Z}^n$ Untergruppe von $(\mathbb{R}^n,+)$, aber kein UVR.

Bemerkung: (Kürzungsregel)

Sei $(G, *)$ eine Gruppe und $a, x, y \in G$

Dann gilt: $\boxed{x * a = y * a \implies x = y}$

und $\boxed{a * x = a * y \implies x = y}$

Bw: Ang. $x * a = y * a$ (z.z: $x = y$)

$\leadsto (x * a) * a^{-1} = (y * a) * a^{-1}$

$\Rightarrow x * \underbrace{(a * a^{-1})}_{e} = y * \underbrace{(a * a^{-1})}_{e}$

$\Rightarrow x * e = y * e$

$\Rightarrow x = y$

Achtung:

$(\mathbb{R}, \cdot)$ Monoid

$5 \cdot 0 = 7 \cdot 0$ ✓

$\not\Rightarrow 5 = 7$.

Def 3.2.7

(a) $(G, *_G)$ $(H, *_H)$ Gruppen

$\varphi: G \longrightarrow H$

heißt **Gruppenhomomorphismus**, wenn

$$\boxed{\forall x,y \in G: \varphi(x *_G y) = \varphi(x) *_H \varphi(y)}$$

$$\left(\boxed{\varphi(e_G) = e_H} \right.$$

$$\left. \boxed{\forall x \in G \quad \varphi(x^{-1}) = (\varphi(x))^{-1}} \right)$$

(gilt automatisch Lemma 3.2.8)

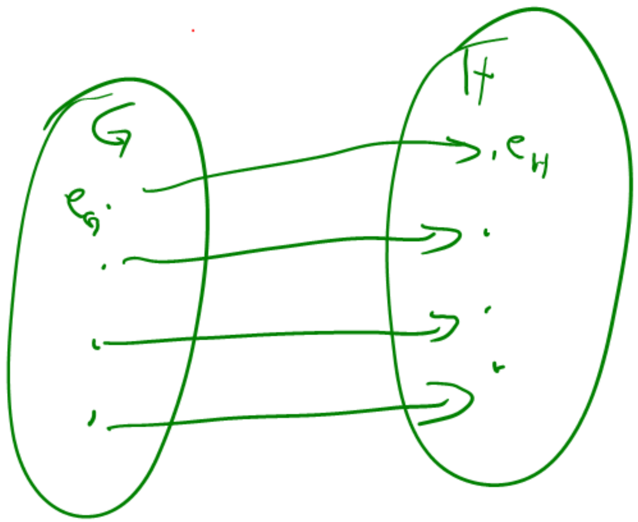
(b) Wenn $\varphi: G \longrightarrow H$ Gruppenhomomorph.

und bijektiv,

dann heißt **Gruppenisomorphismus**.

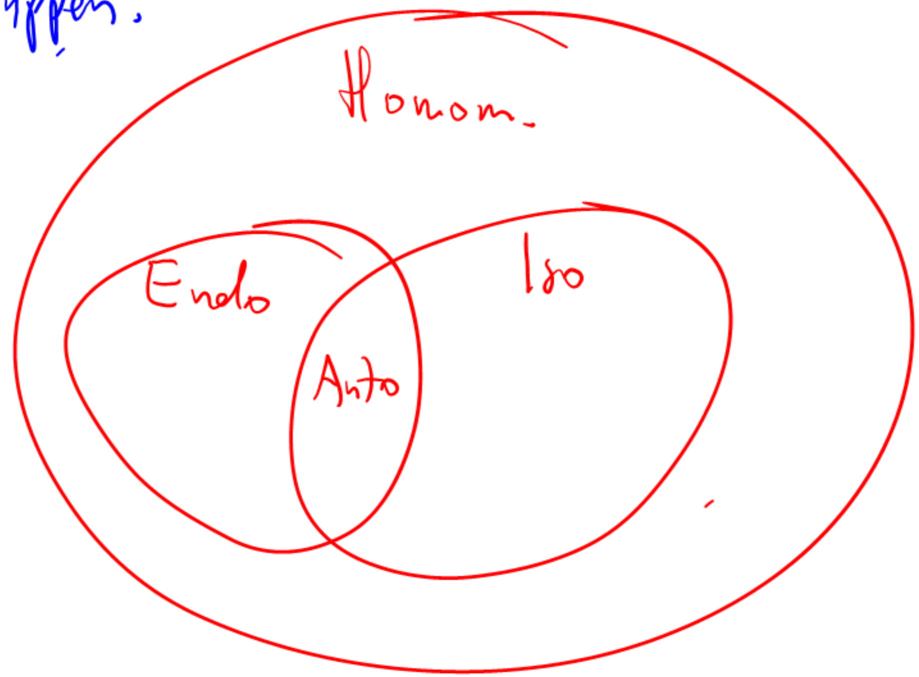
$(G, *)$ und $(H, *)$ heißen **isomorph**.

Schreibweise: $(G, *) \cong (H, *)$



(c) Ein Gruppenhomomorphismus von $(G,*)$ nach $(G,*)$ heißt auch Gruppenendomorphismus.

Einen bijektiven Endomorphismus von Gruppen nennt man auch Automorphismus von Gruppen.



Lemma 3.2.8

$\varphi : (G, *) \longrightarrow (H, *)$ Gruppenhomo.

a) $\boxed{\varphi(e_G) = e_H \quad \forall x \in G \quad \varphi(x^{-1}) = (\varphi(x))^{-1}}$

b) $U \subseteq G$ Untergruppe
$\Rightarrow \varphi(U) \subseteq H$ Untergruppe.
(Spezialfall: $\mathrm{Bild}(\varphi) = \varphi(G)$ Untergruppe von H.)

c) $W \subseteq H$ Untergruppe
$\Rightarrow \varphi^{-1}(W)$ Untergruppe von G.

Spezialfall:

$\ker\varphi := \varphi^{-1}(\{e_H\}) = \{x \in G \mid \varphi(x) = e_H\}$
ist Untergruppe von $(G, *)$.

Bw: (a)

$$\varphi(e_G) * e_H = \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) * \varphi(e_G)$$

Kürzungsregel $\Longrightarrow$ $e_H = \varphi(e_G)$ ✓

$x \in G$. (z.z.: $(\varphi(x))^{-1} = \varphi(x^{-1})$)

$$x^{-1} * x = e_G = x * x^{-1} \quad \Big|\ \varphi$$

$$\varphi(x^{-1} * x) = \underbrace{\varphi(e_G)} = \varphi(x * x^{-1})$$

$$\boxed{\varphi(x^{-1}) * \varphi(x) = e_H = \varphi(x) * \varphi(x^{-1})}$$

$\Longrightarrow \varphi(x^{-1}) = (\varphi(x))^{-1}$ ✓

(b) $U \subseteq G$ Untergruppe

(z.z: $\varphi(U) \subseteq H$ Untergruppe, d.h.
- $e_H \in \varphi(U)$
- $\varphi(U)$ abg. unter $*$
- $\varphi(U)$ abg unter $(\ )^{-1}$.

- $$e_H = \varphi(e_G) \in \varphi(U) \checkmark$$

$a, b \in \varphi(U)$. (z.z: $a *_H b \in \varphi(U)$)

$\exists x \in U \quad a = \varphi(x)$

$\exists y \in U \quad b = \varphi(y)$

$$a * b = \varphi(x) * \varphi(y) = \varphi(\underbrace{x * y}_{\in U}) \in \varphi(U).$$

$a \in \varphi(U)$. z.z: $a^{-1} \in \varphi(U)$.

$\exists x \in U: \quad a = \varphi(x)$.

$$a^{-1} = (\varphi(x))^{-1} = \varphi(\underbrace{x^{-1}}_{\in U}) \in \varphi(U).$$

Teil (c) wird ähnlich bewiesen (siehe Skript) $\square$

z.B.:

$(\mathbb{R},+) \longrightarrow (\mathbb{R},\cdot)^\times : t \longmapsto e^t$ $\boxed{e^{s+t} = e^s \cdot e^t}$

inj, nicht surj.

$(\mathbb{R},+) \cong ((0,\infty),\cdot)$ $\boxed{(\mathbb{R},+) \longrightarrow (\{t\in\mathbb{R} \mid t>0\},\cdot) : t \longmapsto e^t}$ ISO

$\boxed{(\mathbb{C},+) \longrightarrow (\mathbb{C}^\times,\cdot) \quad z \longmapsto e^z}$ (dazu später mehr...) 3.5.8

$\boxed{(\mathbb{Z},+) \longrightarrow ((\mathbb{Z},\cdot)^\times = \{-1,1\},\cdot) \quad k \longmapsto (-1)^k}$ nicht inj.

$\boxed{(H,*) ;\ a\in H. \quad (\mathbb{Z},+) \longrightarrow (H,*) : k \longmapsto a^k}$ 3.1.12

$\boxed{(\mathbb{R}^{m\times n},+) \longrightarrow (\mathbb{R}^{n\times m},+) : A \longmapsto A^T}$ ISO

$\frac{1}{st} = \frac{1}{s}\frac{1}{t}$ $\boxed{(\mathbb{R}^\times,\cdot) \longrightarrow (\mathbb{R}^\times,\cdot) : t \longmapsto \frac{1}{t}}$ Auto

$\boxed{A\in\mathbb{R}^{m\times n} \quad (\mathbb{R}^n,+) \longrightarrow (\mathbb{R}^m,+) : x \longmapsto Ax}$

$\boxed{(G,*) \longrightarrow (H,*) \quad x \longmapsto e_H}$ trivialer Homomorphismus

$\boxed{\mathrm{id}_G : \left((G,*) \longrightarrow (G,*) \quad x \longmapsto x \right)}$ Auto

Lemma 3.2.10 $(G,*)$, $(H,*)$ Gruppen

$\varphi: G \longrightarrow H$ Gruppenhomorphismus

$\ker\varphi = \{x \in G \mid \varphi(x) = e_H\}$ Untergruppe von G

Dann sind äquivalent:

$\boxed{\varphi: G \longrightarrow H \text{ ist injektiv}} \Longleftrightarrow \boxed{\ker\varphi = \{e_G\}}$

Bw: „$\Rightarrow$": Ang. φ inj. (z.z: $\ker\varphi = \{e_G\}$)

„$\supseteq$": $e_G \in \ker\varphi$, weil $\ker\varphi$ Untergruppe.

„$\subseteq$": Sei $x \in \ker\varphi$. (z.z: $x = e_G$)

$$\varphi(x) = e_H = \varphi(e_G) \underset{\varphi \text{ inj}}{\Longrightarrow} x = e_G.$$

„$\Leftarrow$": Ang. $\ker\varphi = \{e_G\}$ (z.z. φ inj)

Ang. $x, y \in G$ mit $\varphi(x) = \varphi(y)$. (z.z: $x = y$)

$$\varphi(x) = \varphi(y) \quad \Big| \text{ mult. von rechts mit } (\varphi(y))^{-1}$$

$$\varphi(x) *_H (\varphi(y))^{-1} = e_H$$

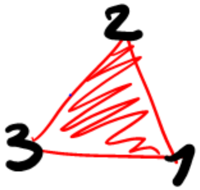
$$\varphi(x) *_H \varphi(y^{-1}) = e_H$$

$$\varphi(x *_G y^{-1}) = e_H$$

$$\Longrightarrow x *_G y^{-1} \in \ker \varphi.$$

$$\Longrightarrow x *_G y^{-1} = e_G \quad \Longrightarrow x = y \quad \blacksquare$$

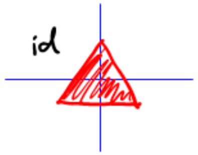
Beispiel: Die Gruppen D_3 und $S(3)$ sind isomorph.



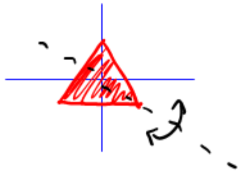
$$D_3 \xrightarrow{\ \cong\ } S(3) \qquad \boxed{\text{Isomorphismus}}$$

$|D_3| = 3 \cdot 2 = 6$

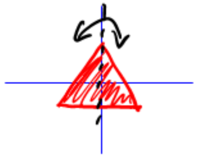
$|S(3)| = 3! = 6$



$\longmapsto \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 2 & 3 \end{array}$

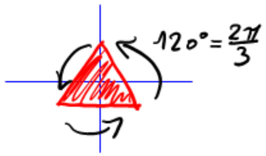


$\longmapsto \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 3 & 2 \end{array}$



$\longmapsto \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 2 & 1 \end{array}$

$\longmapsto \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 1 & 3 \end{array}$



$\longmapsto \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 2 & 3 & 1 \end{array}$

$\longmapsto \begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 3 & 1 & 2 \end{array}$

Anmerkung: Die Gruppe $(D, \star)$ mit der Cayley-Tafel

$D = \{ i, s_1, s_2, s_3, g, u \}$

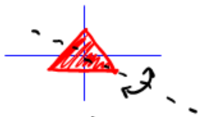
$\star : D \times D \longrightarrow D$

$\star$	i	s_1	s_2	s_3	g	u
i	i	s_1	s_2	s_3	g	u
s_1	s_1	i	g	u	s_2	s_3
s_2	s_2	u	i	g	s_3	s_1
s_3	s_3	g	u	i	s_1	s_2
g	g	s_3	s_1	s_2	u	i
u	u	s_2	s_3	s_1	i	g

ist ebenfalls isomorph zu D_3 und $\mathcal{S}(3)$.

$$D_3 \xrightarrow{\cong} (D, \star)$$

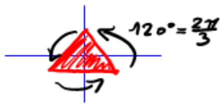
$\longmapsto i$



$\longmapsto s_1$

$\longmapsto s_2$

$\longmapsto s_3$



$\longmapsto g$

$\longmapsto u$

Achtung: $\forall n > 3$

D_n und $S(n)$ sind NICHT isomorph.

$$|D_n| = 2n \neq |S(n)| = n!$$

Aber: $S(4)$ ist isomorph zur Symmetriegruppe des regelmäßigen Tetraeders.