Gruppen

2.1 Def: Eine Verknüpfung auf einer Menge M ist eine Abbildung

$$* : M \times M \longrightarrow M$$
$$(m, n) \longmapsto *(m,n)$$

Notation: $m * n := *(m,n)$

2.2 Def: Eine Verknüpfung $*$ auf M heißt

… assoziativ, falls
$\forall x,y,z \in M: \ (x*y)*z = x*(y*z)$

… kommutativ, falls
$\forall x,y \in M: \ x*y = y*x$

Beispiele:

kommutativ
assoziativ

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \qquad \cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(x, y) \longmapsto x+y \qquad (x, y) \longmapsto x \cdot y$$

$$- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(x, y) \longmapsto x-y$$

usw.

nicht kommutativ
nicht assoziativ (Übung)

2.3 Def: Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung $*$, für die gilt:

(G1) $*$ ist assoziativ

und (G2) $\exists$ neutrales Element:
$\exists e \in G: \forall g \in G:$
$$e * g = g = g * e$$

und (G3) $\exists$ Inverse:
$\forall g \in G: \exists g' \in G:$
$$g * g' = e = g' * g$$

Ist außerdem $*$ kommutativ, ist die Gruppe **abelsch**.

2.4 Notiz:
Das neutrale Element e und das zu einem $g \in G$ inverse Element g' sind eindeutig.

(Seien e, f zwei neutrale Elemente in G. Dann ist
$$e \underset{\uparrow\, f \text{ neutral}}{=} e * f \underset{\uparrow\, e \text{ neutral}}{=} f.$$

Seien g', g'' zwei Inverse zu g. Dann ist
$$g' = \underbrace{g' * g}_{e} * g'' = g''\ )$$

Beispiele:

$(\mathbb{Z}, +)$ ist Gruppe, sogar abelsch

$e = 0$, $g' = -g$

$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ $\Big\}$ abelsche Gruppen (genauso)

$(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ $\Big\}$ abelsche Gruppen

triviale Gruppe := Gruppe mit genau einem Element

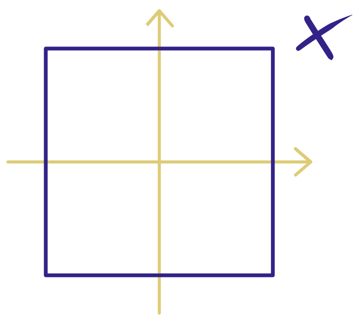
$(\mathbb{N}, +)$ keine Gruppe

$(\mathbb{Z}, \cdot)$ keine Gruppe (keine Inversen)

$(\mathbb{Q}, \cdot)$ keine Gruppe (0 hat kein Inverses)

2.5 Beispiel: Symmetriegruppen

$X \subseteq \mathbb{R}^2$ Teilmenge, z.B.

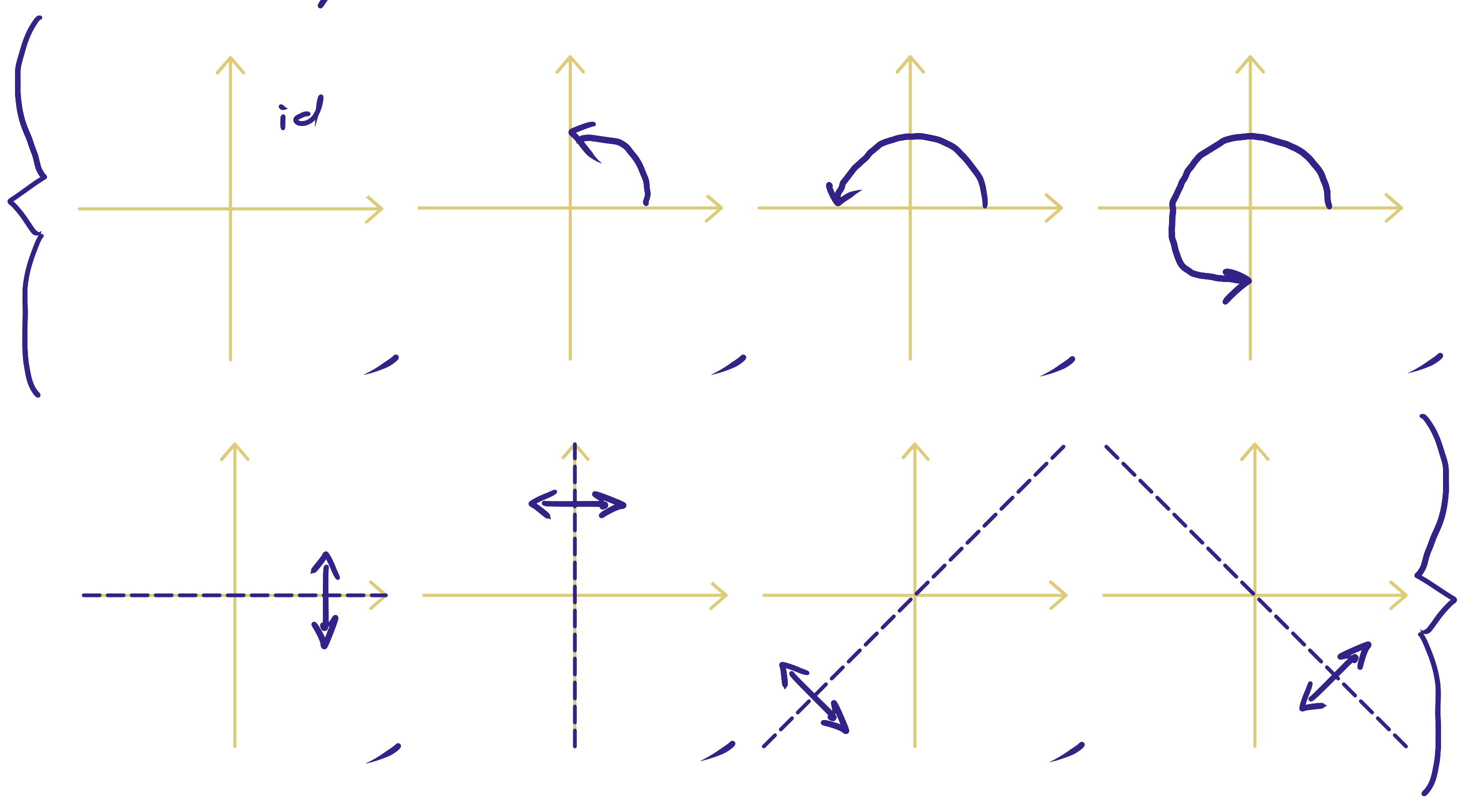


Die Symmetriegruppe von X ist die Menge aller Translationen, Rotationen und Achsenspiegelungen $f: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, für die gilt:

$$f(X) = X,$$

zusammen mit der Komposition als Verknüpfung.

Im Beispiel oben:



2.6 Notation:

übliche Notation für $*$: $\cdot$ oder $+$

	$\cdot$	$+$
neutrales Element:	1	0
Inverses zu g:	g^{-1}	$-g$
für $n \in \mathbb{N}$:	$g^n := \underbrace{g \cdot \ldots \cdot g}_{n \text{ mal } g}$	$ng := \underbrace{g + \ldots + g}_{n \text{ mal } g}$
	$g^0 := 1$	$0g := 0$
	$g^{-n} := (g^n)^{-1}$	$-ng := -(ng)$

Üblicherweise verwenden wir $+$ nur für abelsche Gruppen.

2.7 Satz:

(i) In jeder Gruppe $(G,\cdot)$ gilt:

$$(x\cdot y)^{-1} = y^{-1}\cdot x^{-1}$$

(ii) Ist G abelsch, gilt:

$$(x\cdot y)^n = x^n y^n \quad \text{für alle } n\in\mathbb{Z}$$

Beweis:

i: Wegen der Eindeutigkeit reicht es zu zeigen:

$$\underbrace{(x\cdot y)\cdot(y^{-1}\cdot x^{-1})}_{x\cdot \underbrace{y\cdot y^{-1}}\cdot x^{-1}} \overset{\checkmark}{=} 1 \overset{\checkmark}{=} (y^{-1}\cdot x^{-1})\cdot(x\cdot y)$$

$$x\cdot 1\cdot x^{-1} = x\cdot x^{-1} = 1$$

ii: Für $n\geq 0$ Beweis durch Induktion

IA (Induktionsanfang):

Aussage stimmt für $n=0$.

$$(x\cdot y)^0 = 1$$

$$x^0\cdot y^0 = 1\cdot 1 = 1$$

neutrales Element in G Verknüpfung in G

IV (Induktionsvoraussetzung):
Nehme an, Aussage stimmt für ein bestimmtes n.

IS (Induktionsschluss):
Zeige, dass Aussage unter der IV auch für $n+1$ gilt:

$$
\begin{aligned}
(x\cdot y)^{n+1} &= (x\cdot y)^{n}\cdot(x\cdot y)\\
&\overset{IV}{=} x^{n}\cdot y^{n}\cdot x\cdot y\\
&= x^{n}\cdot x\cdot y^{n}\cdot y\\
&= x^{n+1}\cdot y^{n+1}
\end{aligned}
$$

Für $n \leq 0$ lässt sich die Aussage analog zeigen. $\square$

2.8 Def: Eine *Untergruppe* einer Gruppe $(G,\cdot)$ ist eine Teilmenge $H \subseteq G$, für die gilt:

① · lässt sich zu einer Verknüpfung
$$H \times H \longrightarrow H$$
einschränken, und

② zusammen mit dieser eingeschränkten Verknüpfung ist H eine Gruppe.

2.9 Notiz: Eine Teilmenge $H \subseteq (G,\cdot)$ ist genau dann eine Untergruppe, wenn gilt:

neutrales Element von G

(i) $1_G \in H$

und (ii) $\forall x,y \in H: \quad x \cdot y \in H$

und (iii) $\forall x \in H: \quad x^{-1} \in H$.

Bsp:

$\mathbb{Z} \subseteq (\mathbb{R},+)$ ✓ Untergruppe

$\mathbb{N} \subseteq (\mathbb{R},+)$ ✗ keine Ugruppe (erfüllt nur ①)

$2\cdot\mathbb{Z} \subseteq (\mathbb{Z},+)$ ✓ Untergruppe

gerade ganze Zahlen