Zur Erinnerung: Gruppendefinition

G sei Menge $\circ : G \times G \to G$

(i) $\exists e \in G : \forall g \in G : e \circ g = g$

(ii) $\forall g \in G : \exists g' \in G : g' \circ g = e$

(iii) $\forall g_1, g_2, g_3 \in G : (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

$\forall x : \ldots$

Für alle x gilt

$\exists x : \ldots$

Es existiert ein x mit

Eine Gruppe $(G, \circ)$ heißt kommutativ:

wenn $\forall g_1, g_2 \in G : g_1 \circ g_2 = g_2 \circ g_1$

Nächstes Thema: Untergruppen

<u>Def</u> Sei $(G, \circ)$ eine Gruppe und $U \subseteq G$
Ist $(U, \circ)$ eine Gruppe so nennt man
$(U, \circ)$ eine Untergruppe von $(G, \circ)$

<u>Bem</u> Da für $(U, \circ)$ die Verknüpfung von $(G, \circ)$
„geerbt" wird nennt man auch oft U die
Untergruppe.

Satz Sei $U \subseteq G$ und $(G, \circ)$ sei Gruppe

$(U, \circ)$ ist Untergruppe wenn:

(i) $U \neq \{\}$

(ii) $\forall a, b \in U$ gilt $a \circ b \in U$ (Abgeschl. bzg. „$\circ$")

(iii) $\forall a \in U$ gilt $a' \in U$ (Abgeschl. bzg. Inversen)

eindeutige Inverse zu a in $(G, \circ)$

Bew: Abgeschl.: klar wg. (ii)

Neutrales El: Aus (i) folgt $\exists a: a \in U$

Aus (iii) folgt $a' \in U$

Aus (ii) folgt $a' \circ a \in U$, $a' \circ a = e \in U$

Inverse: klar wg. (iii)

Assoziativ: Wird wg. Abgeschl. von $(G, \circ)$ „geerbt"

Def Sei $(G, \circ)$ eine Gruppe und $M \subseteq G$

Die von M erzeugte Untergruppe $\langle M \rangle$ ist eine Teilmenge von G mit

(i) $U \supseteq M$

(ii) Für jede Untergruppe $(U', \circ)$ mit $U' \supseteq M$ gilt $U' \supseteq U$.

Satz: die von M erzeugte Untergruppe ist eindeutig bst.

Bew Angenommen es gibt zwei versch. Mengen $U, \overline{U}$ die (i) und (ii) erfüllen. Dann zu zeigen $U = \overline{U}$

Wg. $(i)_U$ gilt $U \supseteq M$ Wg. $(i)_{\overline{U}}$ gilt $\overline{U} \supseteq M$

$$\left.\begin{array}{l} \text{Wg } (ii)_U \text{ und } \overline{U} \supseteq M \text{ gilt } \overline{U} \supseteq U \\ \text{wg } (ii)_{\overline{U}} \text{ und } U \supseteq M \text{ gilt } U \supseteq \overline{U} \end{array}\right\} \Rightarrow U = \overline{U}$$

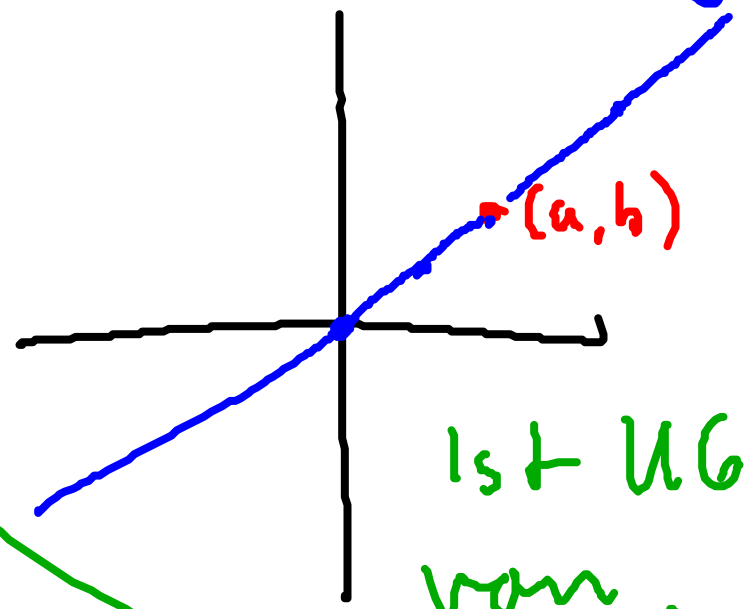
Untergruppen von $(\mathbb{R}^2, \oplus)$

$(\mathbb{R}^2, \oplus)$ selbst ist Untergr.

$(\{(0,0)\}, \oplus)$ ist kleinste Untergr.

$a, b \in \mathbb{R}$ mit $a \neq 0$ oder $b \neq 0$

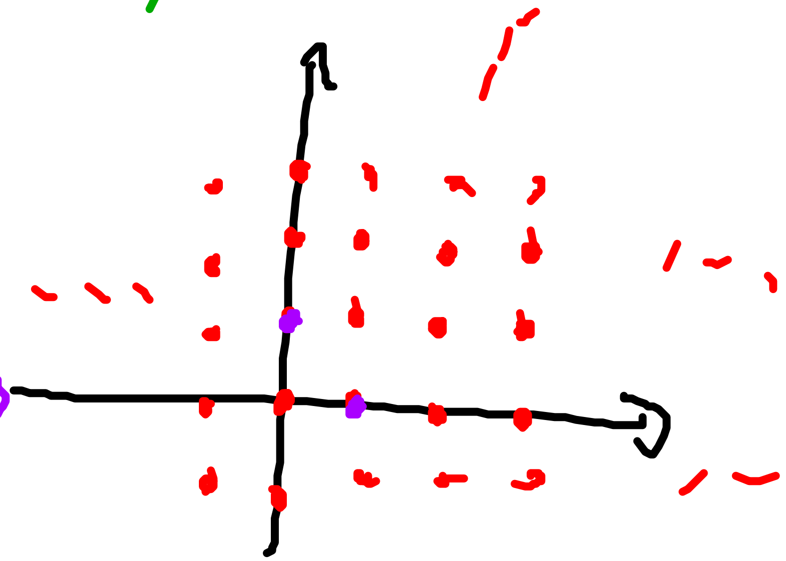
$\{(\lambda a, \lambda b) \mid \lambda \in \mathbb{R}\}$



ist UG von $(\mathbb{R}^2, \oplus)$

$(\mathbb{Z}^2, \oplus)$ ist Untergr.

Erzeugt von $\{(0,1), (1,0)\}$



(i) $\mathbb{Z}^2 \neq \{\}$

(ii) Zu $(a,b), (c,d) \in \mathbb{Z}^2$ ist $(a,b) \oplus (c,d) \in \mathbb{Z}^2$

$(a+c, b+d)$

(iii) Zu $(a,b) \in \mathbb{Z}^2$ ist $(-a,-b) \in \mathbb{Z}^2$

Untergruppen von $(\mathbb{Z},+)$

Bsp $(7\mathbb{Z},+)$ ist Untergruppe von $(\mathbb{Z},+)$

<u>Satz</u> Jede Untergruppe von $(\mathbb{Z},+)$ ist von der Form $(n\mathbb{Z},+)$ für geeignetes n

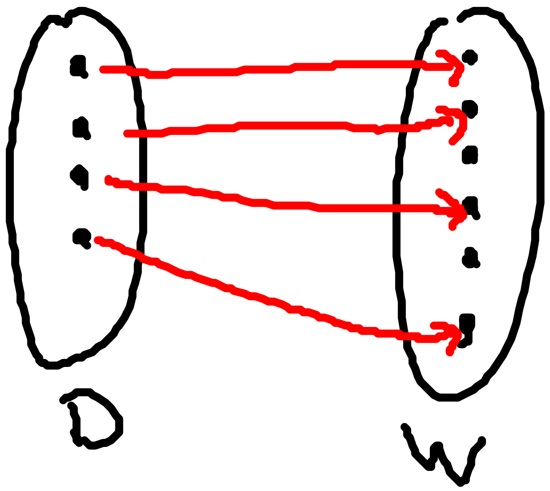
Bem das ist die von $\{n\}$ erzeugte Untergr

<u>Bew</u> $\to$ Übung $\to$ Tipp (ggT)

Injektive, Surjektive, bijektive Funktionen

Sei $f: D \to W$

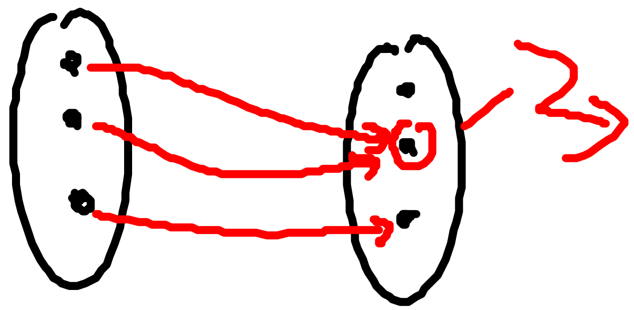
f ist injektiv wenn für $x, y \in D$ mit $x \neq y$ auch $f(x) \neq f(y)$ gilt



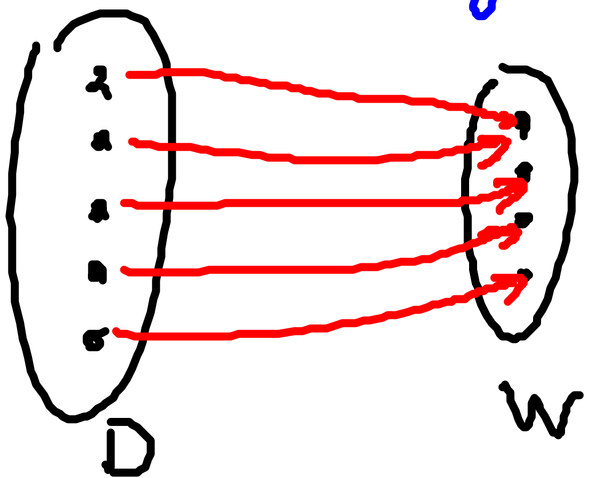
$f: \mathbb{N} \to \mathbb{N}$
$x \to x^2$ ist injektiv

$f: \mathbb{Z} \to \mathbb{N}$
$x \to x^2$ ist nicht injektiv

Verboten:



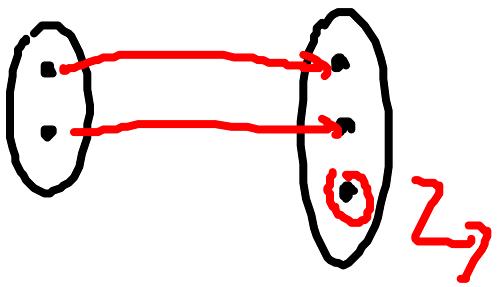
f ist surjektiv wenn für jedes $y \in W$ ein x existiert mit $f(x) = y$.



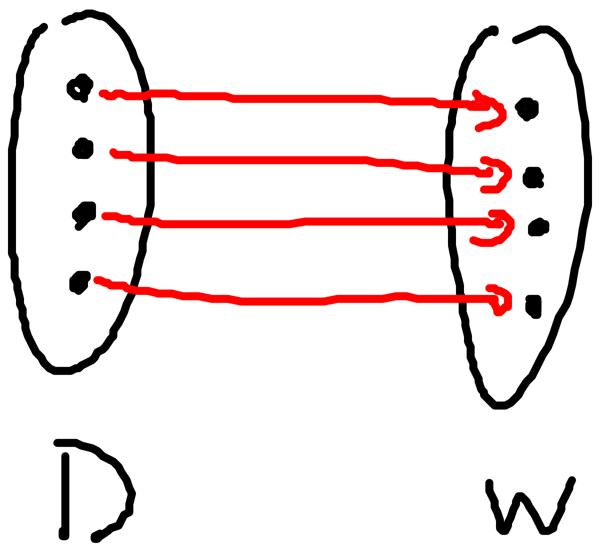
$f: \mathbb{N} \to \mathbb{N}$
$x \to x+1$ ist nicht surjektiv

$f: \mathbb{Z} \to \mathbb{Z}$
$x \to x+1$ ist surjektiv

Verboten



f ist **bijektiv** wenn es injektiv und surjektiv ist.



$$(g \circ f)(x) = g(f(x))$$

Einige Tatsachen für bijekt Abbildunge

- Wenn $f: X \to Y$ bijektiv ist und X endl, dann $|X| = |Y|$
- Ist $f: X \to Y$ bijektiv so existiert eine Umkehrabbildung $f^{-1}: Y \to X$ mit $f^{-1}(f(x))\, x$
- Ist $|X| = |Y|$ endlich so ist gleichwertig
  - $f: X \to Y$ ist injektiv
  - $f: X \to Y$ ist surjektiv
  - $f: X \to Y$ ist bijektiv
- Ist $f: X \to Y$ bijektiv und $g: Y \to Z$ bijekti
  So ist $g \circ f$ bijektiv