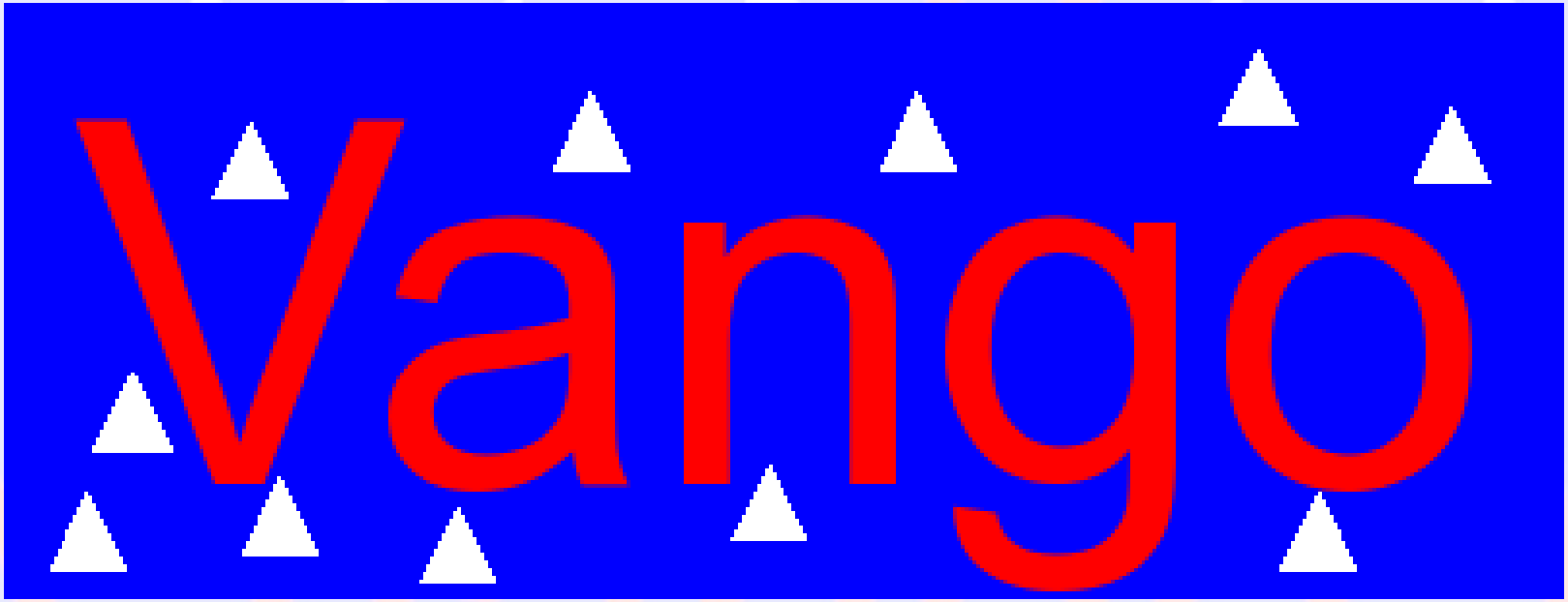


Gruppentheorie

Themenüberblick

1. Definition einer Gruppe
2. Homomorphismen
3. Gruppenoperationen
4. Direktes Produkt
5. Semidirektes Produkt

1. Definition einer Gruppe

Definition Gruppe

Sei G eine Menge und $*$ eine Verknüpfung

$$* : G \times G \to G$$
$$(a\ ,\ b) \mapsto a * b$$

(G, $*$) ist eine Gruppe, wenn folgende Axiome gelten:

- Assoziativität $(a * b) * c = a * (b * c)$ $\forall$ a, b, c $\in$ G
- Neutrales Element $e \in G$ mit $a * e = e * a = a$
- Inverse Elemente $a \in G \Rightarrow a^{-1} \in G$ mit $a * a^{-1} = a^{-1} * a = e$

Gruppe (Beispiel)

$(\mathbb{Z}, +)$ ist eine Gruppe.

Sei $\mathbb{Z}$ eine Menge und $+$ eine Verknüpfung

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a\ ,\ b) \mapsto a + b$$

$(\mathbb{Z}, +)$ ist eine Gruppe, wenn folgende Axiome gelten:

- Assoziativität $(a + b) + c = a + (b + c)$ $\forall$ a, b, c $\in \mathbb{Z}$
- Neutrales Element $0 \in \mathbb{Z}$ mit $a + 0 = 0 + a = a$
- Inverse Elemente $a \in \mathbb{Z} \Rightarrow -a \in \mathbb{Z}$ mit $a + (-a) = (-a) + a = 0$

2. Homomorphismen

Definition Homomorphismus

Seien $(G, *)$ und $(H, \star)$ Gruppen. Eine Funktion

$f : G \longrightarrow \mathrm{H}$ heißt Gruppenhomomorphismus,

wenn für alle $a, b \in G$ gilt:

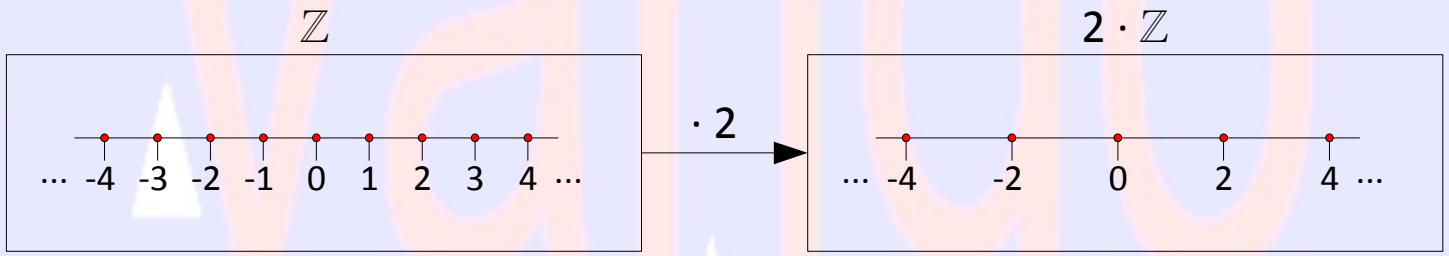
$$f(a * b) = f(a) \star f(b)$$

Gruppenhomomorphismus (Beispiel)

Gruppen: $(\mathbb{Z}, +)$ und $(2 \cdot \mathbb{Z}, +)$.

$$f(a + b) = f(a) + f(b)$$

$f : \mathbb{Z} \longrightarrow 2 \cdot \mathbb{Z}$ ist ein Gruppenhomomorphismus.
$x \mapsto x + x$



$$f(a + b) = (a + b) + (a + b) = (a + a) + (b + b) = f(a) + f(b)$$

Gruppenhomomorphismus (Beispiel)

$(\mathbb{R}^+, \cdot)$ $(\mathbb{R}, +)$

$$f : \mathbb{R}^+ \longrightarrow \mathbb{R}$$
$$x \mapsto \log(x)$$

$$f(a \cdot b) = f(a) + f(b)$$

$$f(a \cdot b) = \log(a \cdot b) = \log(a) + \log(b) = f(a) + f(b)$$

$\Rightarrow$ f ist ein Gruppenhomomorphismus

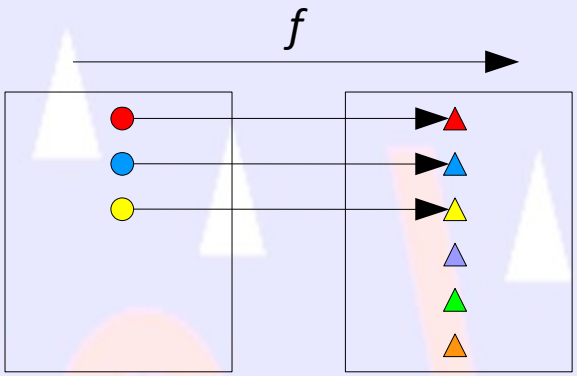
injektiv, surjektiv, bijektiv

- Eine Funktion *f* heißt injektiv, wenn für jedes Bild höchstens ein Urbild existiert.

- Eine Funktion *f* heißt surjektiv, wenn für jedes Bild mindestens ein Urbild existiert.

- Eine Funktion *f* heißt bijektiv, wenn für jedes Bild genau ein Urbild existiert.

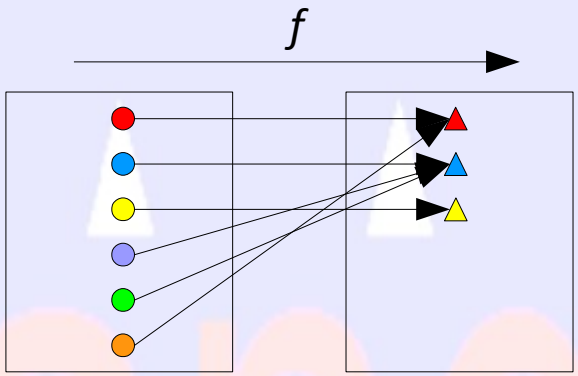
injektiv, surjektiv, bijektiv



injektiv

$f : \mathbb{Z} \rightarrow \mathbb{Z}$

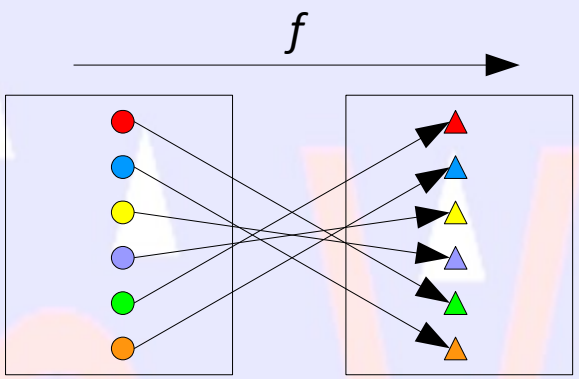
$f(x) = 2x$



surjektiv

$f : \mathbb{R} \rightarrow [-1, 1]$

$f(x) = \sin(x)$



bijektiv

$f : \mathbb{Z} \rightarrow \mathbb{Z}$

$f(x) = x + 3$

Spezielle Homomorphismen

Sei $f : G \longrightarrow H$ ein Gruppenhomomorphismus.

- Monomorphismus: f injektiv
- Epimorphismus: f surjektiv
- Isomorphismus: f bijektiv
- Endomorphismus: $G = H$
- Automorphismus: $G = H$, f bijektiv

Isomorphie

- Zwei Gruppen G, H heißen isomorph zueinander, wenn es einen Isomorphismus $f : G \longrightarrow H$ gibt.

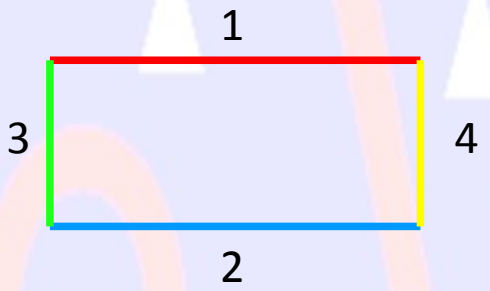
  Schreibweise: $G \cong$ H

- Zwei isomorphe Gruppen haben immer gleich viele Elemente (da f bijektiv ist).

- Zwei isomorphe Gruppen sind bis auf die Bezeichnung der Elemente identisch.

Isomorphie (Beispiel)

$G_1 = (V, \circ)$



$V := \{ 1, a, b, ab \}$

1 ändert nichts (neutral)

a vertauscht Seite 1 und 2

b vertauscht Seite 3 und 4

ab vertauscht Seite 1 und 2 sowie Seite 3 und 4

$G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

$f : V \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$

$1 \mapsto (0, 0)$

$a \mapsto (0, 1)$

$b \mapsto (1, 0)$

$ab \mapsto (1, 1)$

f ist ein Isomorphismus

$\Rightarrow V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

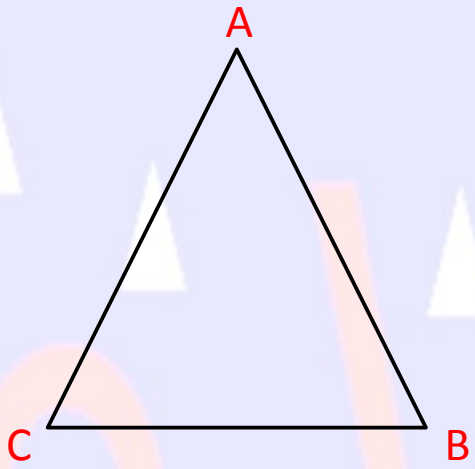
3. Gruppenoperationen

Gruppenoperationen

- Mengen haben keine Verknüpfung
- Rechenoperationen also zunächst nicht möglich
- Idee: Operationen auf einer Menge von einer Gruppe durchführen

Motivation

- Menge = { A, B, C }



- Ziel: „Rechnen“ mit den Punkten
- Eine Möglichkeit dazu wäre:
  Bewegen im Uhrzeigersinn
  - A + 0 = A A + 1 = B A + 2 = C A + 3 = A …
  - B + 0 = B B + 1 = C B + 2 = A B + 3 = B …
  - C + 0 = C C + 1 = A C + 2 = B C + 3 = C …
- $\mathbb{Z}_3$ wäre also als Gruppe geeignet

Definition Gruppenoperation

Sei X eine Menge und $(G, *)$ eine Gruppe.

Eine Operation von G auf X ist eine Funktion

$$\tilde{\rho} : G \times X \to X$$
$$(g\ ,\ x) \mapsto \tilde{\rho}\,(g\ ,\ x) := g.x$$

mit den Eigenschaften:

(1) $e.x = x \qquad \forall\, x \in X \qquad e$ = neutr. Elem. in G

(2) $g_1.(g_2.x) = (g_1 * g_2).x \qquad \forall\, x \in X \qquad \forall\, g_1, g_2 \in G$

Definition Gruppenoperation

Andere Notation:

$$\rho : G \to \{\, f : X \to X \mid f \text{ ist ein Automorphismus} \,\}$$

$$g \mapsto \rho_g : X \to X$$
$$x \mapsto g.x$$

- ρ ist ein Gruppenhomomorphismus
- $\rho_g^{-1} = \rho_{g^{-1}}$

Gruppenoperation (Beispiel)

Sei X = { A, B, C } und $G = (\mathbb{Z}_3, +)$.

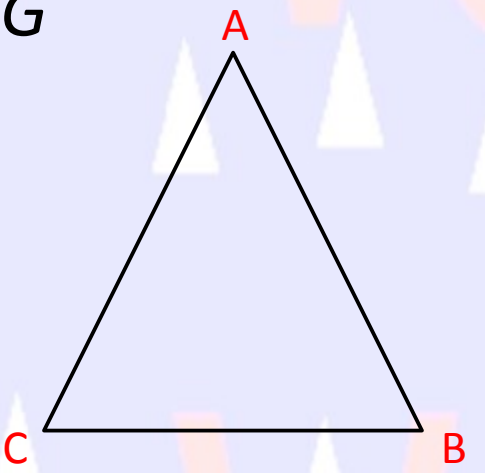
$\tilde{\rho} : G \times X \to X$

$(g\ ,\ x) \mapsto$ g Schritte im Uhrzeigersinn ab x $:= g.x$

Offensichtlich gilt:

(1) $0.x = x \qquad \forall\, x \in X$

(2) $g_1.(g_2.x) = (g_1 + g_2).x \quad \forall\, x \in X \quad \forall\, g_1, g_2 \in G$



Danke für die Aufmerksamkeit!