Erläuterung der Seiten- und Gleichungsnummerierung:
L: Teil "Lineare Algebra" in AD.
L1: Kapitel L1, "Mathematics before Numbers", in AD
a: erste Seite im handschriftlichen Skript zu Kapitel L1

Gleichungen die auf Seite L1a (Kapitel L1, Seite a) stehen, werden zitiert als
(1), (2) falls die Zitate auf derselben Seite stehen;
(a.1), (a.2) falls die Zitate auf anderen Seiten (z.B. b,c) desselben Kapitels L1 stehen;
(L1a.1), (L1a.2) falls die Zitate auf Seiten anderer Kapitel (z.B. L2, C3) stehen.

L1 Mathematische Grundbegriffe

L1.1 Mengen und Abbildungen

Zwei Mengen: $A = \{\times, +, \Delta\}$ $\quad B = \{\circ, \square\}$

kartesisches Produkt:

$$A \times B = \{(a,b) \mid a \in A,\ b \in B\} = \{(\times,\circ),\ (\times,\square),\ (+,\circ),\ (+,\square),\ (\Delta,\circ),\ (\Delta,\square)\} \quad (1)$$

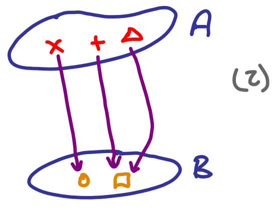
'ist Element von'

Abbildung:

Definitionsmenge, Zielmenge, Name der Abbildung

$$F : A \longrightarrow B$$
$$a \longmapsto F(a)$$

Argument, Zielelement



$F(A) = B$ (2)

Beispiel: $F : \mathbb{N}_0 \longrightarrow \{1,-1\}$
$n \longmapsto F(n) = (-1)^n$

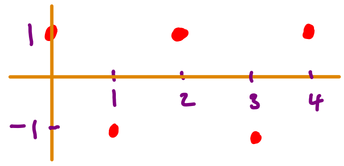
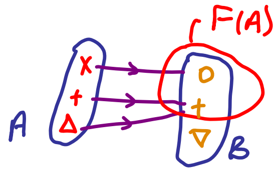


Bild v. A: $F(A) = \{F(a) \mid a \in A\} \subseteq B$

'ist eine Teilmenge von, oder ist gleich'

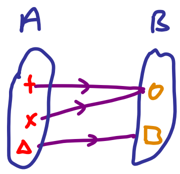


Eine Abbildung ist...

surjektiv falls $\forall\, b \in B$ gilt: $b = F(a)$ für **mindestens** ein $a \in A$

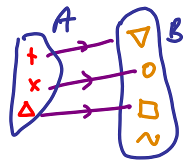
'für alle'

'alle Elemente v. B werden erreicht'



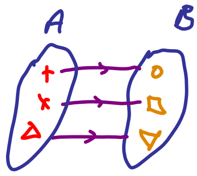
injektiv falls $\forall\, b \in B$ gilt: $b = F(a)$ für **höchstens** ein $a \in A$

'kein Element v. B wird mehr als einmal erreicht'



bijektiv falls $\forall\, b \in B$ gilt: $b = F(a)$ für **genau** ein $a \in A$
(injektiv und surjektiv)

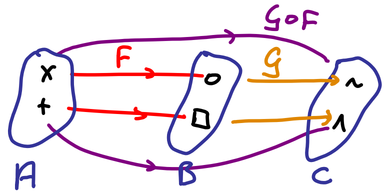
'1-zu-1-Abbildung'



Verkettung / Komposition

Lic

$$F: A \to B, \quad a \mapsto F(a) \qquad , \qquad g: B \to C, \quad b \mapsto g(b) \qquad g \circ F: A \to C, \quad a \mapsto g(F(a))$$

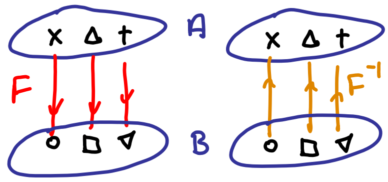


Beispiel: $A, B, C = \mathbb{Z}$

$$F(a) = a+1 \qquad g(b) = 2b \quad , \quad (g \circ F)(a) = 2(a+1)$$

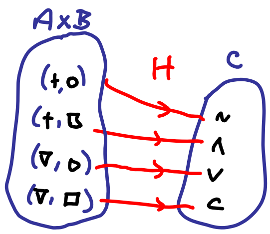
Inverse einer bijektiven Abbildung:

$$F: A \to B, \quad a \mapsto F(a) \qquad F^{-1}: B \to A, \quad F(a) \mapsto F^{-1}(F(a)) = a$$



Binäre Verknüpfung:
Definitionsmenge ist ein kartesisches Produkt:

$$H: A \times B \to C, \quad (a, b) \mapsto c = H(a,b)$$

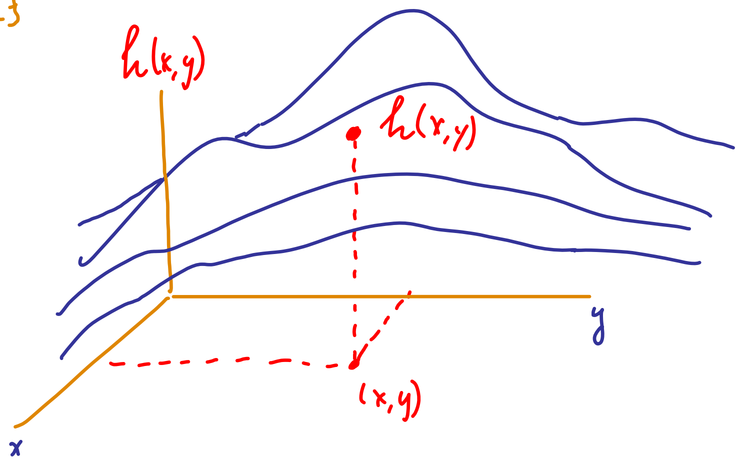


Beispiel einer binären Verknüpfung: Höhe eines Gebirges

Lid

$$h: \overbrace{\mathbb{R} \times \mathbb{R}}^{\mathbb{R}^2 = \{(x,y) \mid x, y \in \mathbb{R}\}} \to \mathbb{R}$$

$$(x,y) \mapsto h(x,y)$$



L1.2 Gruppe: (einfachste Struktur die 'Operationen' mit Elementen erlaubt)

L1e

kartesisches Produkt

Definition: Eine 'Gruppe' $\mathcal{G} = (A, \bullet)$ ist eine Menge A ausgestattet mit einer binären Verknüpfung,

$$\bullet : A \times A \longrightarrow A \qquad (1)$$

$$(a, b) \longmapsto a \bullet b \qquad (2)$$

und folgenden Eigenschaften ('Gruppenaxiome'):

'für alle'

i) Abgeschlossenheit: $\forall a, b \in A, \quad a \bullet b \in A$ (3)

ii) Assoziativität: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ (4)

'es existiert'

iii) neutrales Element: $\exists e \in A$, so dass $a \bullet e = e \bullet a = a, \quad \forall a \in A$ (5)

iv) inverses Element: $\forall a \in A \ \exists \ b \in A$ mit $a \bullet b = e = b \bullet a$ (6)

$a^{-1} \equiv b$

'links wird definiert durch rechts' (7)

Falls $a \bullet b = b \bullet a$ 'kommutative Gruppe', 'Abelsche Gruppe'

Falls $a \bullet b \neq b \bullet a$ 'nicht-kommutative Gruppe', 'nicht-Abelsche Gruppe' (8)

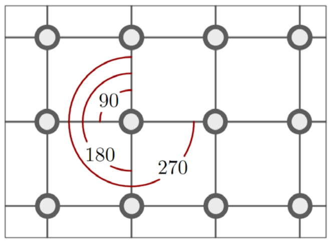
Beispiel 1: Rotationen eines Gitters um eine feste Achse um 0, 90, 180, 270 Grad

L1f

$\tau(\phi) \equiv$ Rotation um ϕ, $\quad \tau(\phi + 360) = \tau(\phi)$ (1)

$R_{90} \equiv \{\tau(\phi) \mid \phi \in \{0, 90, 180, 270\}\}$ (2)

'linke Seite ist Kurznotation für rechte Seite,
bzw. wird durch rechte Seite definiert'



Verknüpfung v. zwei Rotationen aus C sei die Rotation um die Summe der Winkel:

$$\bullet : R_{90} \times R_{90} \longrightarrow R_{90} \qquad (3)$$

z.B.: $(\tau(\phi), \tau(\phi')) \longmapsto \tau(\phi) \bullet \tau(\phi') \equiv \tau(\phi + \phi')$ (4)

$$\tau(0) \bullet \tau(90) = \tau(90) \qquad (5)$$

$$\tau(90) \bullet \tau(180) = \tau(270) \qquad (6)$$

$$\tau(270) \bullet \tau(180) = \tau(90) \qquad (7)$$

Verknüpfungstabelle:

$\bullet$	0	90	180	270
0	0	90	180	270
90	90	180	270	0
180	180	270	0	90
270	270	0	90	180

(bestimmt Gruppe vollständig)

$(R_{90}, \bullet)$ ist eine kommutative Gruppe.

Neutrales element: $\tau(0)$ $\qquad$ (Inverse von $\tau(\phi)$) $= \tau(360 - \phi)$

Beispiel 2: Addition ganzer Zahlen modulo q

L1g

Definition: für $p, q \in \mathbb{Z}$ sei $p \bmod q \equiv$ positiver Rest v. (p geteilt durch q) (1)

Beispiele: $5 \bmod 4 = 1$ $\quad 9 \bmod 4 = 1$ (2)

$7 \bmod 4 = 3$ $\quad -3 \bmod 4 = (-4+1) \bmod 4 = 1$ (3)

Definition: $\mathbb{Z}_q \equiv \{0, 1, 2, \ldots, q-1\}$ (4)

Verknüpfung v. zwei Elementen v. $\mathbb{Z}_q$ sei ihre Summe modulo q:

$$\bullet: \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_q \quad (5)$$

$$(p, p') \mapsto p \bullet p' = (p+p') \bmod q \quad (6)$$

z.B. für q = 4:

$$0 \bullet 1 = (0+1) \bmod 4 = 1 \quad (7)$$

$$1 \bullet 2 = (1+2) \bmod 4 = 3 \quad (8)$$

$$3 \bullet 2 = (3+2) \bmod 4 = 1 \quad (9)$$

Verknüpfungstabelle für q = 4:

•	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(bestimmt Gruppe vollständig)

$(\mathbb{Z}_q, \bullet)$ ist eine kommutative Gruppe. (10)

Ihre Verknüpungstabelle hat dieselbe Struktur wie die von $(R_{90}, \bullet)$

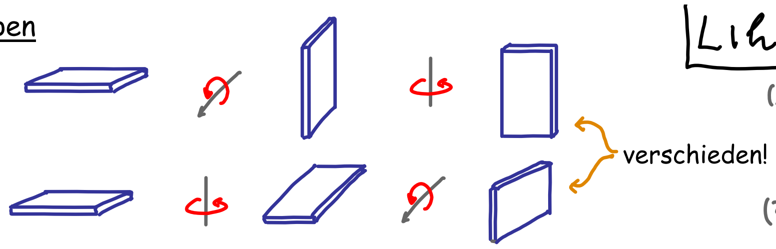
Folglich sind die beiden Gruppen 'isomorph': $(\mathbb{Z}_q, \bullet) \cong (R_{90}, \bullet)$ [AD-Buch, S. 9-10]

Beispiele von nicht-kommutativen Gruppen

L1h

Rotationen in drei Dimensionen:

Rotationen um verschiedene Achsen sind nicht-kommutativ (Reihenfolge ist nicht egal):



(1)

(2)

Permutationsgruppe

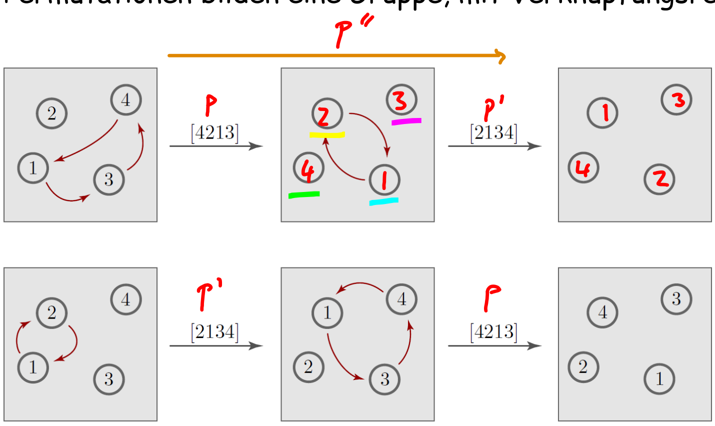
z.B. von 4 unterscheidbaren (nummerierten) Objekten

Kurznotation:

Beispiel einer Permutation: 'Ersetze 1 durch 4, 2 durch 2, 3 durch 1, 4 durch 3 ': [4 2 1 3]

(Die Ersetzungsregel bezieht sich nur auf die Nummern der Kugeln; sie gilt, egal wo die Kugeln liegen!) (3)

Permutationen bilden eine Gruppe, mit Verknüpfungsregel: $p'' = p' \circ p$ = erst P, dann P' (4)



$$\overset{p''}{[4123]} = \overset{p'}{[2134]} \circ \overset{p}{[4213]} \quad (5)$$

verschieden!

$$\overset{p'''}{[2413]} = \overset{p}{[4213]} \circ \overset{p'}{[2134]} \quad (6)$$

L1.3 Körper

L1i

Algebraische Struktur, die Addition, Subtraktion, Multiplikation und Division erlaubt.

Körper: $F = (A, +, \bullet)$ (zwei Verknüpfungsregeln: Addition & Multiplikation) (1)

- Addition: $(A, +)$ bildet eine kommutative Gruppe, mit neutralem Element = 0. (2)
  (additives Inverse v. a) $= -a$ Subtraktion: $a - b \equiv a + (-b)$ (3)

- Multiplikation: $(A \setminus \{0\}, \bullet)$ bildet eine kommutative Gruppe, mit neutralem Element = 1. (4)
  Multiplik. Inverse v. $a = a^{-1}$ Division: $a/b \equiv a \cdot b^{-1}$ (5)

- Für das neutrale Element d. Addition, 0 gilt: $0 \cdot a \equiv 0 \quad \forall a \in A$ (6)
  Also hat 0 kein multiplikatives Inverse $\cancel{\frac{1}{0}}$ [sonst würde gelten: $0^{-1} \cdot 0 \cdot a = 0^{-1} \cdot 0$
  $\Rightarrow a = 1 \quad \forall a \in A$]

- Distributivitätsaxiom: $a \cdot (b + c) = a \cdot b + a \cdot c$ (7)

$\mathbb{Z}$ (ausgestattet mit der üblichen Definition von Addition und Multiplikation ganzer Zahlen)
ist <u>kein</u> Körper, denn Multiplikation hat kein Inverses in $\mathbb{Z}$ (8)

Beispiele von Körpern:

L1j

<u>Rationale Zahlen:</u> $\mathbb{Q} \equiv \{ q/p \mid q, p \in \mathbb{Z},\ p \neq 0 \}$ (1)

<u>Reelle Zahlen:</u> $\mathbb{R}$ = { alle Zahlen, die als Limes von 'Folgen von rationalen Zahlen' dargestellt werden können } (2)

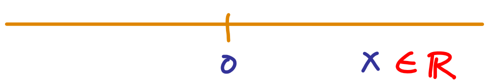
z.B.: $\mathbb{Q} \not\ni \sqrt{2} = 1{,}4142\ldots$ (3)

kann approximiert werden durch die Folge

$$\left\{ \begin{array}{lll} 1{,}4 = \frac{14}{10} & \in \mathbb{Q} \\ 1{,}41 = \frac{141}{100} & \in \mathbb{Q} \\ 1{,}414 = \frac{1414}{1000} & \in \mathbb{Q} \\ 1{,}4142 = \frac{14142}{10000} & \in \mathbb{Q} \\ \vdots & \end{array} \right.$$

(4)

$\mathbb{R}$ = { alle Zahlen, die gebraucht werden, um eine Linie zu Parametrisieren }



Komplexe Zahlen: $\mathbb{C}$

L1k

Ausgangsfrage: was sind die Lösungen der Gleichung $x^2 = -1$? $x \notin \mathbb{R}$ (1)

Lösungsansatz: erweitere unser Zahlensystem um eine neue Zahl, die 'imaginäre Einheit', i .

Definiere i als eine Zahl, deren Quadrat -1 liefert: $\boxed{i^2 \equiv -1}$ (2a)

Dasselbe gilt für $-i$: $(-i)^2 = -1$ (2b)

$\pm i$ sind Wurzeln von -1. Notationskonvention: $i \equiv \sqrt{-1}$ $(\notin \mathbb{R})$ (3)

Wurzel von negativen Zahlen: Sei $r > 0$: $\sqrt{-r} \equiv \sqrt{-1}\sqrt{r} = i\sqrt{r}$ (4)

Menge aller komplexen Zahlen: $\mathbb{C} \equiv \{ z = x + iy \mid x, y \in \mathbb{R} \}$ (5)

jede kompl. Zahl wird dargestellt durch zwei reelle Zahlen:

$x \equiv \mathrm{Re}(z) =$ 'Realteil v. z' (6)

$y \equiv \mathrm{Im}(z) =$ 'Imaginärteil v. z' (7)

L1l

Def. v. Addition:

(analog den üblichen Regeln für einen Körper)

$$z + z' = (x+iy) + (x'+iy') \overset{!}{\equiv} (x + x') + i(y + y')$$ (1)

Bsp: $(1+2i) + (2-3i) = 3 + i(-1) = 3 - i$

Def. v. Multiplikation:

(analog den üblichen Regeln für einen Körper)

$$z z' = (x+iy)(x'+iy') \equiv (xx' + xiy' + iyx' + \overset{\overset{(R.2)}{=-1}}{i^2} yy')$$ (2)

$$= (xx' - yy') + i(xy' + yx')$$ (3)

Bsp: $(1+2i)(2-3i) = (2-(-6)) + i(1\cdot(-3)+4) = 8 + i$

Neutrales Element der Addition: 0 Additives Inverse: $-z = -x - iy$ (4)

Neutrales Element der Multiplikation: 1

Falls $z \neq 0$, was ist das multiplikatives Inverse: $z^{-1} = ?$ (5)

Was sind Re(z^{-1}), Im(z^{-1}) ?

Definiere zunächst: 'komplex Konjugierte' von $z = x+iy$: $\quad z^* \equiv \bar{z} \equiv x - iy$ (1)

dann:

$$\underline{z\bar{z}} \overset{(1)}{=} (x+iy)(x-iy) \overset{(\ell.3)}{=} (x\cdot x - y\cdot(-y)) + i(\cancel{x\cdot(-y)} + \cancel{y\cdot x}) = \overbrace{x^2+y^2}^{\geq 0} \in \mathbb{R} \qquad (2)$$

für $z \neq 0$:

$$(2)\cdot\frac{1}{x^2+y^2}: \quad z\cdot\underbrace{\bar{z}\,\frac{1}{x^2+y^2}}_{\equiv z^{-1}} \overset{(2)}{=} 1 \qquad (3)$$

Inverse: $z^{-1} \overset{(3)}{\equiv} \frac{\bar{z}}{x^2+y^2} = \frac{x-iy}{x^2+y^2}$, $\quad \mathrm{Re}(z^{-1}) = \frac{x}{x^2+y^2}$, $\quad \mathrm{Im}(z^{-1}) = \frac{-y}{x^2+y^2}$ (4)

Check: $z z^{-1} \overset{(4)}{=} (x+iy)\frac{x-iy}{x^2+y^2} \overset{(2)}{=} \frac{x^2+y^2}{x^2+y^2} = 1 \;\checkmark$ (5)

Merkregel für Inverse:
'mache den Nenner reell' ! $\quad z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{x^2+y^2} \overset{\checkmark}{=} (4)$ (6)

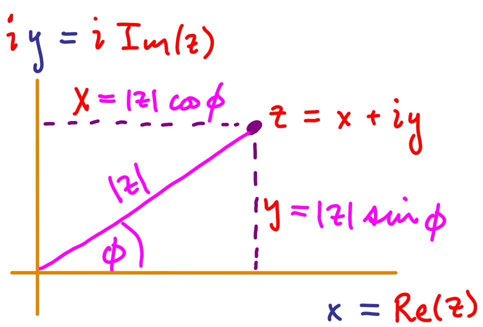
Bsp: $z = 2-3i$, $\quad z^{-1} = \frac{1}{2-3i}\,\frac{2+3i}{2+3i} = \frac{2+3i}{4+9} = \frac{1}{13}(2+3i)$ (7)

Komplexe Ebene:

Identifikation einer komplexen Zahl mit 'geordnetem Paar' von zwei reellen Zahlen:

$$I: \mathbb{C} \to \mathbb{R}^2 = \{(x,y) \mid x,y \in \mathbb{R}\} \qquad (1)$$

$z \mapsto (x,y) =$ Punkt in zwei-dimensionaler Ebene ('komplexe Ebene') (2)



Polardarstellung:

Betrag v. z (Abstand zum Ursprung):

$$|z| \equiv \sqrt{x^2+y^2} = \sqrt{z\bar{z}} \qquad (3)$$

$$z = x + iy \qquad (4)$$

$$= |z|(\cos\phi + i\sin\phi) \qquad (5)$$

Reelle Achse: $z = x$ 'rein reell'

Imaginäre Achse: $z = iy$ 'rein imaginär'

ZL1

Zusammenfassung: L1

Gruppe: $\mathcal{G} = (A, \bullet)$ Verknüpfung: $\bullet : A \times A \longrightarrow A, \quad (a,b) \longmapsto a \bullet b$

(i) Abgeschlossenheit, (ii) Assoziativität, (iii) neutrales Element, (iv) inverses Element

---

Körper: $F = (A, +, \bullet)$ (zwei Verknüpfungsregeln: Addition & Multiplikation, beide liefern jeweils eine kommutative Gruppe)

Algebraische Struktur, die Addition, Subtraktion, Multiplikation und Division erlaubt.

Beispiele: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

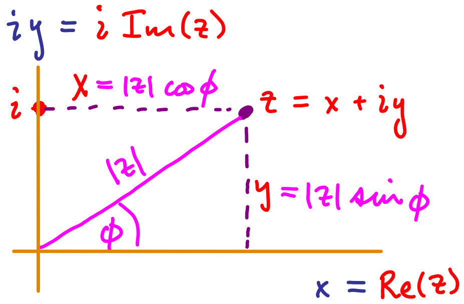
Komplexe Zahlen: $\mathbb{C} = \{ z = x + iy \mid x, y \in \mathbb{R} \} \longrightarrow \mathbb{R}^2 = \{ (x,y) \mid x, y \in \mathbb{R} \}$

$i^2 = -1, \quad i = \sqrt{-1}$

$$z + z' = (x + x') + i(y + y')$$

$$z \cdot z' = (xx' - yy') + i(xy' + x'y)$$

$$z^* = \bar{z} \equiv x - iy, \quad z\bar{z} = x^2 + y^2 = |z|^2$$



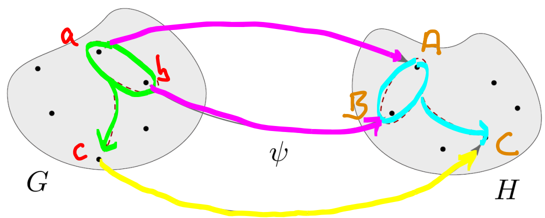
L10

Optional: Homomorphismus

$(\mathcal{G}, \bullet)$ und $(H, \bullet)$

$a \cdot b = c$ $\quad A \bullet B = C$

seien zwei Gruppen mit *a priori* unabhängigen Verknüpfungsregeln.



Def: Eine Abbildung $\psi : \mathcal{G} \longrightarrow H, \quad a \longmapsto \psi(a)$ (1)

ist ein 'Homomorphismus', falls $\psi(a \cdot b) = \psi(a) \bullet \psi(b) \quad \forall\, a, b \in \mathcal{G}$ (2)

'bewahrt die Form' verknüpfen, dann abbilden = abbilden, dann verknüpfen

Beispiel: $(\mathcal{G}, \cdot) = (\mathbb{Z}, +)$, $(H, \bullet) = (2\mathbb{Z}, +)$ (3)

Addition ganzer Zahlen, Addition gerader Zahlen

Die Abbildung $\psi : \mathcal{G} \to H, \quad n \mapsto \psi(n) = 2n$ ist ein Homomorphismus, (4)

denn $\psi(n+m) = 2(n+m)$ ist gleich $\psi(n) + \psi(m) = 2n + 2m = 2m + 2n$ (5)

verknüpfen, dann abbilden — abbilden, dann verknüpfen

Die Abbildung $\phi : \mathcal{G} \to H, \quad n \mapsto \phi(n) = 2n^2$ ist kein Homomorphismus, (6)

denn $\phi(n+m) = 2(n+m)^2$ ist nicht gleich $\phi(n) + \phi(m) = 2n^2 + 2m^2 = 2n^2 + 2m^2$ (7)

verknüpfen, dann abbilden — abbilden, dann verknüpfen

LIP

Optional: Isomorphismus

Def: Eine Abbildung $\psi : G \longrightarrow H \, , \quad a \longmapsto \psi(a)$ (1)

heisst ein 'Isomorphismus' ('identische Form') zwischen den Gruppen G und H ist,
falls sie ein bijektiver Homomorphismus ist. Wir schreiben dann: $G \cong H$ (2)

Isomorphe Gruppen sind praktisch 'identisch'.

$(R_{90}, \bullet) \cong (\mathbb{Z}_4, \cdot)$

Konkret: es existiert eine 1-zu-1 Zuordnung ihrer Elemente, die ihre Verknüpfungstabellen aufeinander abbildet (d.h. sie haben 'dieselbe' Verknüpfungstabelle, alle Eigenschaften der einen Gruppe gelten auch für die andere).

•	0	90	180	270
0	0	90	180	270
90	90	180	270	0
180	180	270	0	90
270	270	0	90	180

•	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Gruppentheorie: sehr wichtig in der Physik !

- Diskrete Translationen, Reflektionen (Kristallstrukturen)
- Translationen in Raum oder Zeit
- Rotationen (Quantenmechanische Theorie des Drehimpulses, Spin)
- Lorentz-Gruppe, Poincare-Gruppe (spezielle Relativitätstheorie)