

Lineare Algebra I

für die Fachrichtung Informatik

Wintersemester 2023/24

Der Ring der ganzen

Zahlen

$(\mathbb{Z}, +, \cdot)$

Äquivalenzrelationen
und
Quotientenmengen

z.B.

$\mathbb{R}$

$$\sqrt{2}, \pi \in \mathbb{R}$$

$$\frac{\sqrt{2}}{\pi} \in \mathbb{R}$$

$$\frac{\pi}{\sqrt{2}} \in \mathbb{R}$$

$\mathbb{Z}$

$$7, 2 \in \mathbb{Z}$$

$$\frac{7}{2} \notin \mathbb{Z}$$

Teilbarkeit: $a, m \in \mathbb{Z}$

Wir sagen: m ist Teiler von a

$\Leftrightarrow$ a ist Vielfaches von m

$\Leftrightarrow$ a ist durch m teilbar

$\Leftrightarrow$ m teilt a

$\Leftrightarrow$ $m \mid a$

$\Leftrightarrow \exists k \in \mathbb{Z} : a = mk$

Lemma 3.4.3

$$(a) \quad \forall a \in \mathbb{Z} : 1 \mid a$$

$$\text{Bw:} \quad a = 1 \cdot a.$$

$$(b) \quad \forall a \in \mathbb{Z} : (0 \mid a \iff a = 0)$$

$$\text{"} \Rightarrow \text{"} : 0 \mid a \Rightarrow \exists k \in \mathbb{Z} \quad a = 0 \cdot k = 0. \quad \text{"} \Leftarrow \text{"} : a = 0 \cdot 0 \quad \checkmark$$

$$(c) \quad \forall a \in \mathbb{Z} : a \mid a \quad (\text{Reflexivität von } \mid)$$

$$a = a \cdot 1$$

$$(d) \quad \forall a, b, c \in \mathbb{Z} : (a \mid b \text{ und } b \mid c) \Rightarrow (a \mid c) \quad (\text{Transitivität von } \mid)$$

$$b = a \cdot k$$

$$c = b \cdot l \quad \Rightarrow \quad c = a(k \cdot l)$$

$$(e) \quad \forall a, b \in \mathbb{Z} : (a \mid b \text{ und } b \mid a) \iff |a| = |b|$$

$$\Leftarrow: |a| = |b|$$

$$\Rightarrow a = bk \quad k \in \{-1, 1\} \Rightarrow b | a.$$

$$ak = b \Rightarrow a | b.$$

$$\Rightarrow: a | b \text{ und } b | a \quad (\text{z.z.: } |a| = |b|)$$

$$b = ak$$

$$a = bl$$

$$\Rightarrow a = bl = akl.$$

$$a - akl = 0$$

$$\Rightarrow a(1 - kl) = 0.$$

$$\text{1. Fall: } a = 0.$$

$$\Rightarrow b = 0, k = 0.$$

$$|a| = 0 = |b|.$$

$$\text{2. Fall: } 1 - kl = 0$$

$$kl = 1$$

$$\Rightarrow k \in \{-1, 1\}$$

$$|a| = |b|.$$



Def 3.4.16 (Primzahl)

$p \in \mathbb{Z}$ heißt **Primzahl**

$$: \Leftrightarrow p > 1 \quad \text{und} \quad \left(\forall m \in \mathbb{N} : (m|p \Rightarrow m=1 \text{ oder } m=p) \right)$$

Satz 3.4.17 (Fundamentalsatz der Arithmetik)

Anm: $x^n + y^n \neq z^n \quad n > 2$
Fermat
 $x, y, z > 0$

Jede natürliche Zahl $n \in \mathbb{N}$ lässt sich eindeutig

als endliches Produkt von Primzahlen schreiben.

Diese Darstellung ist eindeutig bis auf Umordnung (Permutation) der Primfaktoren.

Lemma 3.4.18 Lemma von Euklid

$$p \text{ Primzahl} \Rightarrow \left(\forall a, b \in \mathbb{Z} : p|(ab) \Rightarrow p|a \text{ oder } p|b \right)$$

Lemma 3.4.1 (Division mit Rest)

Gegeben $a \in \mathbb{Z}$, $m \in \mathbb{N}$,

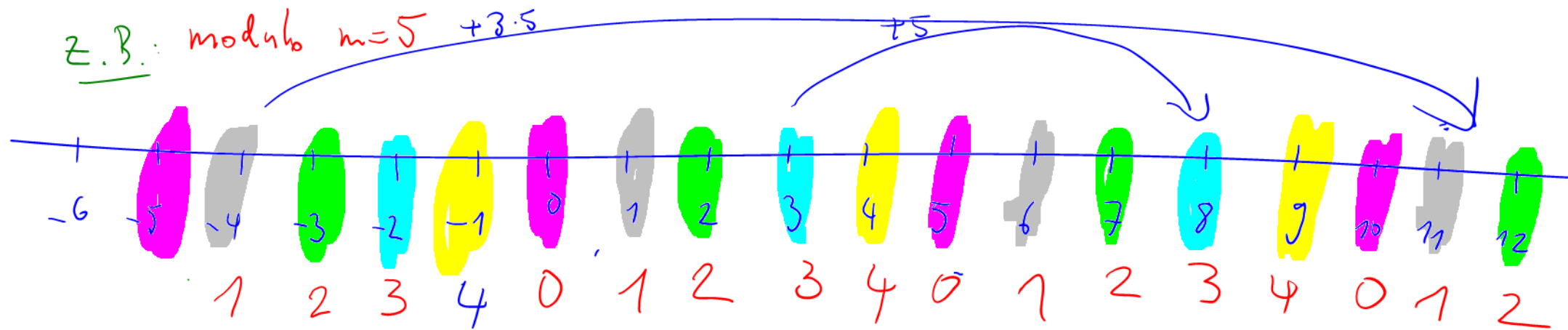
Dann existieren $k, r \in \mathbb{Z}$ mit

$$a = m k + r \quad \text{mit} \quad 0 \leq r < m$$

Diese Darstellung ist eindeutig.

$r = \text{Rest von } a \text{ modulo } m$.

Bw: Skript.



$$7 = 5 \cdot 1 + 2$$

$$-3 = 5(-1) + 2$$

$$12 = 5 \cdot 2 + 2$$

$$8 - 3 = 5$$

$$8 \equiv_5 3$$

$$3 \equiv_5 8$$

$$11 - (-4) = 15$$

$$11 \equiv_5 -4$$

$$-4 \equiv_5 11$$

Def 3.4.4: Es sei $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$

Wir sagen: a und b sind **Kongruent modulo m**

$\Leftrightarrow$

$$a \equiv_m b$$

$\Leftrightarrow$

$$a \equiv b \pmod{m}$$

$\Leftrightarrow$

$$m \mid (a-b)$$

• $a \equiv_m b \Leftrightarrow a \equiv_{-m} b$

• Falls $m \in \mathbb{N}$: $a \equiv_m b \Leftrightarrow a$ und b haben den gleichen Rest modulo m

• $\forall a, b \in \mathbb{Z}: a \equiv_1 b \quad 1 \mid (a-b)$

• $\forall a, b \in \mathbb{Z}: (a \equiv_0 b \Leftrightarrow a = b)$

Lemma 3.4.8: Es sei $m \in \mathbb{Z}$

$$\forall a \in \mathbb{Z}: a \equiv_m a \quad (\equiv_m \text{ ist reflexiv})$$

$$\text{Bw: } m \mid (a-a) \Leftrightarrow m \mid 0, \text{ weil } 0 = m \cdot 0.$$

$$\forall a, b \in \mathbb{Z}: a \equiv_m b \Rightarrow b \equiv_m a \quad (\equiv_m \text{ ist symmetrisch})$$

$$a \equiv_m b \Rightarrow m \mid (a-b) \Rightarrow m \mid (b-a) \Rightarrow b \equiv_m a.$$

$$\forall a, b, c \in \mathbb{Z}: (a \equiv_m b \text{ und } b \equiv_m c) \Rightarrow a \equiv_m c$$

($\equiv_m$ ist transitiv)

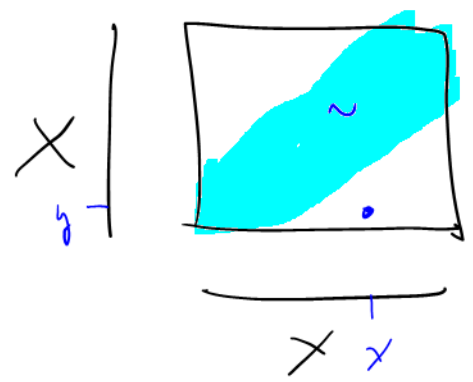
$$a \equiv_m b, \text{ d.h. } m \mid (a-b), \text{ d.h. } a-b = m \cdot k$$

$$b \equiv_m c, \text{ d.h. } m \mid (b-c), \text{ d.h. } b-c = m \cdot l$$

$$a-c = (a-b) + (b-c) = m \cdot k + m \cdot l = m \cdot (k+l) \Rightarrow m \mid a-c \Rightarrow a \equiv_m c.$$

Def: Äquivalenzrelation

Es sei X eine Menge.



(a) $\sim \subseteq X \times X$ heißt **Relation** auf X
(wir schreiben $x \sim y \iff (x, y) \in \sim$)

(b) Eine Relation $\sim$ heißt **reflexiv**, wenn $\forall x \in X: x \sim x$

(c) Eine Relation $\sim$ heißt **symmetrisch**, wenn
$$\forall x, y \in X: x \sim y \Rightarrow y \sim x$$

(d) Eine Relation $\sim$ heißt **transitiv**, wenn
$$\forall x, y, z \in X: (x \sim y \text{ und } y \sim z) \Rightarrow x \sim z$$

(e) Eine Relation heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

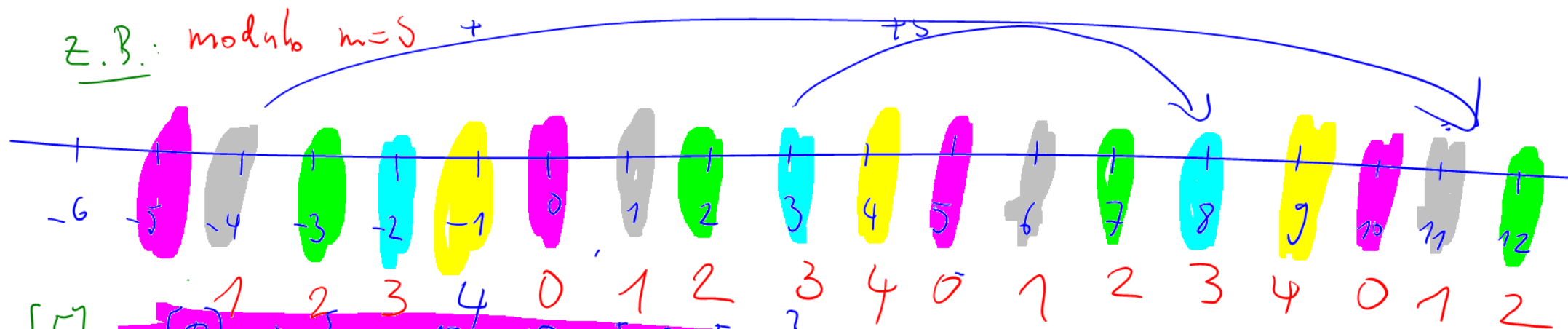
(f) Es sei $\sim$ eine Äquivalenzrelation auf X und $x \in X$.

Dann heißt $[x]_{\sim} := \{y \in X \mid x \sim y\}$ **Äquivalenzklasse** von x .

z.B.: $X = \mathbb{Z}$

$\sim = \equiv_5$

z.B.: modulo $m=5$ +



$[5]_5 = [0]_5 = \{ \dots, -15, -10, -5, 0, 5, \dots \}$

$[6]_5 = [1]_5 = \{ \dots, -14, -9, -4, 1, 6, \dots \}$

$[7]_5 = [2]_5 = \{ \dots, -8, -3, 2, 7, 12, \dots \}$

$[18]_5 = [3]_5 = \{ \dots, -2, 3, 8, 13, 18, \dots \}$

$[19]_5 = [4]_5 = \{ \dots, -6, -1, 4, 9, 14, 19, \dots \}$

z.B.: $\mathbb{Q} \neq \mathbb{Z} \times \mathbb{N}$

$\frac{2}{4}$

$\frac{1}{2}$

$\frac{4}{8}$

Wichtiges Beispiel (3.4.9)

Es sei $g: X \rightarrow Q$ eine Funktion.

Dann ist

$$x \sim_g y : \Leftrightarrow g(x) = g(y)$$

eine Äquivalenzrelation auf X .

Satz 3.4.10

Quotientenmengen

und Quotientenabbildungen

Sei X eine Menge und $\sim$ eine Äquivalenzrelation.

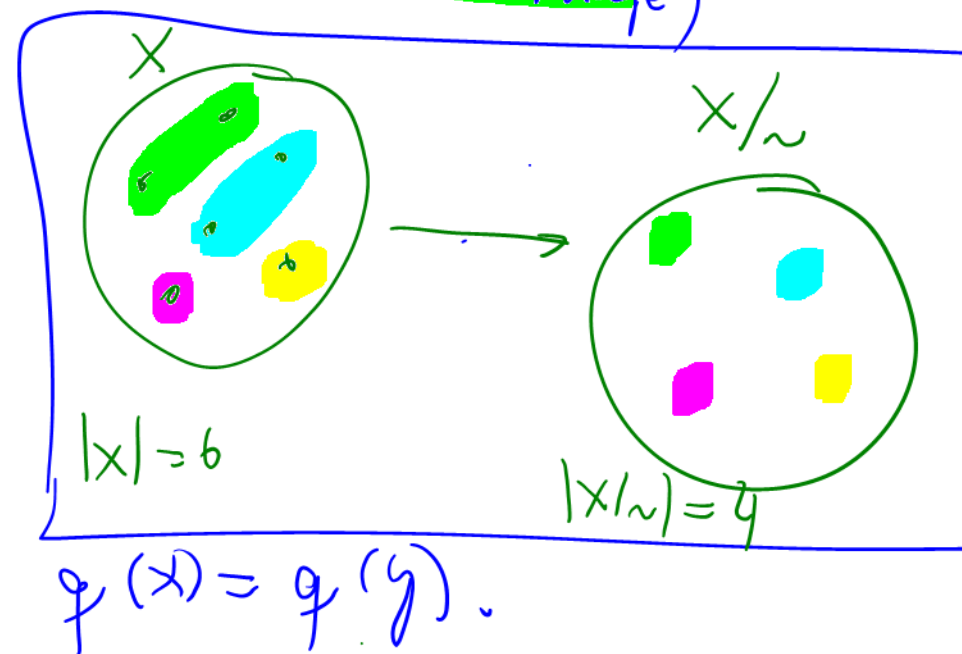
Dann gibt es eine Menge $X/\sim$ (Quotientenmenge
= Faktormenge)

und eine surjektive Abbildung

$$q: X \longrightarrow X/\sim$$

mit

$$\forall x, y \in X \quad x \sim y \iff$$



Bw:

$$X/_\sim := \{ [x]_\sim \mid x \in X \} \subseteq \mathcal{P}(X).$$

$$g: \begin{pmatrix} X & \longrightarrow & X/_\sim \\ x & \longmapsto & [x]_\sim \end{pmatrix} \quad \text{surjektiv nach Konstruktion.}$$

$$[x]_\sim := \{ z \in X \mid x \sim z \}$$

$$z, z_i \quad \forall x, y \in \mathbb{Z}: x \sim y \iff [x]_\sim = [y]_\sim$$

$\Rightarrow$:

Wir nehmen an, $x \sim y$. (z.z. $[x]_\sim = [y]_\sim$)

" $\subseteq$ ":

$$\text{Sei } z \in [x]_\sim$$

$$x \sim z$$

$$x \sim y$$

$$\sim \text{symm.} \Rightarrow y \sim x$$

$$x \sim z$$

$$\left. \begin{array}{l} y \sim x \\ x \sim z \end{array} \right\} \xrightarrow{\sim \text{trans}} y \sim z.$$

$$\text{z.z.: } z \in [y]_\sim$$

$$\text{z.z.: } y \sim z$$

" $\supseteq$ ":

Sei $z \in [y]_{\sim}$.

$$y \sim z.$$

z. z.: $z \in [x]_{\sim}$

$$x \sim z.$$

$$\left. \begin{array}{l} x \sim y \\ y \sim z \end{array} \right\} \xrightarrow{\text{Trans.}} x \sim z.$$

$$[x]_{\sim} = [y]_{\sim}$$

$\Leftarrow$:

$$[x]_{\sim} = [y]_{\sim}$$

z. z.: $x \sim y$.

$x \sim x$, weil $\sim$ reflexiv.

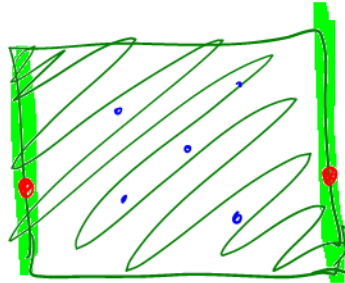
$$x \in [x]_{\sim} = [y]_{\sim} \Rightarrow x \sim y.$$



Anmerkung:

$$X = \square \in \mathbb{R}^2$$

$\sim$

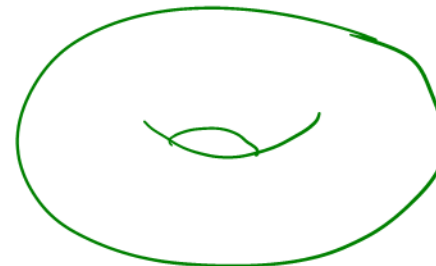
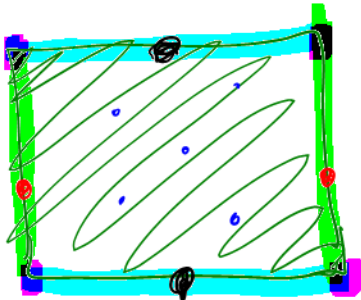


$$X/\sim$$



$$X = \square \in \mathbb{R}^2$$

$\sim$



$$X = \text{---} \text{---} \quad [0, 1]$$

$$0 \sim 1$$

$$x \sim x$$

$$X/\sim$$



... zurück zu $\mathbb{Z}$.

Definition: $m \in \mathbb{N}_0$

$$\mathbb{Z}/m\mathbb{Z} := \mathbb{Z}/\equiv_m$$

= Menge aller Äquivalenzklassen bzgl. $\equiv_m$

$$\mathbb{Z}/m\mathbb{Z}, \quad \mathbb{Z}/m, \quad \mathbb{Z}_m$$

$$q: \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

$$x \longmapsto q(x) = [x]_{\equiv_m} = [x]_m = [x]_{m\mathbb{Z}} = [x]$$

Satz 3.4.12 (Ringstruktur auf $\mathbb{Z}/m\mathbb{Z}$)

Es sei $m \in \mathbb{N}_0$.

Dann gibt es genau eine Möglichkeit

$$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

und $\cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$

so zu definieren, dass $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein Ring wird
und

$$\begin{array}{ccc} \varphi : (\mathbb{Z}, +, \cdot) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z}, +, \cdot) \\ x & \longmapsto & [x]_m \end{array}$$

ein Ringhomomorphismus ist.

$$\begin{aligned} [x-y]_m &= [x]_m - [y]_m \\ [x+y]_m &= [x]_m + [y]_m \\ [x \cdot y]_m &= [x]_m \cdot [y]_m \\ [1]_m &= 1 \text{ in } \mathbb{Z}/m\mathbb{Z} \\ [0]_m &= 0 \text{ in } \mathbb{Z}/m\mathbb{Z} \end{aligned}$$

Bw: Jedes Element in $\mathbb{Z}/m\mathbb{Z}$ ist von der Form $[x]_m$.

$$[x]_m + [y]_m = [x+y]_m$$

$$[x]_m \cdot [y]_m = [x \cdot y]_m$$

→ Eindeutigkeit der Ringstruktur
auf $\mathbb{Z}/m\mathbb{Z}$.

Wieso existiert die Ringstruktur?

Definition:

$$[x]_m + [y]_m := [x+y]_m$$

$$[x]_m \cdot [y]_m := [x \cdot y]_m$$

Frage: Ist dies wohldef?

Einschub:

$$f: \left(\begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Q} \\ \frac{m}{n} & \longmapsto & \frac{m^2 + n^2}{n^2} \end{array} \right), m \in \mathbb{Z}, n \in \mathbb{N}$$

$$\frac{m_1}{n_1} = \frac{m_2}{n_2} \Rightarrow \frac{m_1^2 + n_1^2}{n_1^2} = \frac{m_2^2 + n_2^2}{n_2^2}, \quad \text{wohl def.}$$

$$g: \left(\begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{Q} \\ \frac{m}{n} & \longmapsto & \frac{m^2}{n} \end{array} \right)$$

NICHT

wohl definiert!

hängt von

Repräsentanten ab!

$$g\left(\frac{4}{3}\right) = \frac{16}{3}$$

$$g\left(\frac{8}{6}\right) = \frac{64}{6} \neq \frac{16}{3}$$

$$g\left(\frac{1}{1}\right) = 1$$

$$g\left(\frac{2}{2}\right) = \frac{4}{2} \neq 1$$

Fortsetzung Beweis

+ wohldef.

$$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

$$[x_1]_m = [x_2]_m, \quad [y_1]_m = [y_2]_m \quad \left(\text{z.z.: } [x_1 + y_1]_m = [x_2 + y_2]_m \right)$$

$$m \mid x_1 - x_2 \quad m \mid y_1 - y_2$$

$$x_1 - x_2 = mk \quad y_1 - y_2 = ml$$

$$(x_1 + y_1) - (x_2 + y_2) = x_1 - x_2 + y_1 - y_2 = mk + ml = m(k+l)$$

$$\Rightarrow x_1 + y_1 \equiv_m x_2 + y_2 \quad \Rightarrow [x_1 + y_1]_m = [x_2 + y_2]_m.$$

• wohldef

$$\cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

$$[x_1]_m = [x_2]_m, \quad [y_1]_m = [y_2]_m \quad \left(\text{z.z.: } [x_1 \cdot y_1]_m = [x_2 \cdot y_2]_m \right)$$

$$m \mid x_1 - x_2 \quad m \mid y_1 - y_2$$

$$\text{z.z. } m \mid x_1 y_1 - x_2 y_2$$

$$x_1 - x_2 = mk \quad y_1 - y_2 = ml$$

$$\begin{aligned}
 x_1 y_1 - x_2 y_2 &= x_1 y_1 - x_1 y_2 + x_1 y_2 - x_2 y_2 \\
 &= x_1 (y_1 - y_2) + (x_1 - x_2) y_2 \\
 &= x_1 m l + m k y_2 \\
 &= m (x_1 l + k y_2) .
 \end{aligned}$$

