

## 3. Elementare Zahlentheorie

# Zahlenbereiche

## Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ( $\mathbb{N}$  und  $\mathbb{N}_0$ ) mit den Rechenoperationen  $+$  und  $\cdot$  und der Ordnung  $\leq$  konstruieren wir daraus die **ganzen** ( $\mathbb{Z}$ ), die **rationalen** ( $\mathbb{Q}$ ) und schließlich die **reellen Zahlen** ( $\mathbb{R}$ )

## Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ( $\mathbb{N}$  und  $\mathbb{N}_0$ ) mit den Rechenoperationen  $+$  und  $\cdot$  und der Ordnung  $\leq$  konstruieren wir daraus die **ganzen** ( $\mathbb{Z}$ ), die **rationalen** ( $\mathbb{Q}$ ) und schließlich die **reellen Zahlen** ( $\mathbb{R}$ )
- die ganzen Zahlen  $\mathbb{Z}$  erlauben zusätzlich die **Subtraktion** ( $-$ )

## Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ( $\mathbb{N}$  und  $\mathbb{N}_0$ ) mit den Rechenoperationen  $+$  und  $\cdot$  und der Ordnung  $\leq$  konstruieren wir daraus die **ganzen** ( $\mathbb{Z}$ ), die **rationalen** ( $\mathbb{Q}$ ) und schließlich die **reellen Zahlen** ( $\mathbb{R}$ )
- die ganzen Zahlen  $\mathbb{Z}$  erlauben zusätzlich die **Subtraktion** ( $-$ )
- ganz ähnlich erlauben die rationalen Zahlen  $\mathbb{Q}$  die **Division** ( $/$ )

## Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ( $\mathbb{N}$  und  $\mathbb{N}_0$ ) mit den Rechenoperationen  $+$  und  $\cdot$  und der Ordnung  $\leq$  konstruieren wir daraus die **ganzen** ( $\mathbb{Z}$ ), die **rationalen** ( $\mathbb{Q}$ ) und schließlich die **reellen Zahlen** ( $\mathbb{R}$ )
- die ganzen Zahlen  $\mathbb{Z}$  erlauben zusätzlich die **Subtraktion** ( $-$ )
- ganz ähnlich erlauben die rationalen Zahlen  $\mathbb{Q}$  die **Division** ( $/$ )
- $\mathbb{Z}$  und  $\mathbb{Q}$  können als **Abschluss/Erweiterung** der natürlichen Zahlen bezüglich der Subtraktion und Division angesehen werden

## Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ( $\mathbb{N}$  und  $\mathbb{N}_0$ ) mit den Rechenoperationen  $+$  und  $\cdot$  und der Ordnung  $\leq$  konstruieren wir daraus die **ganzen** ( $\mathbb{Z}$ ), die **rationalen** ( $\mathbb{Q}$ ) und schließlich die **reellen Zahlen** ( $\mathbb{R}$ )
- die ganzen Zahlen  $\mathbb{Z}$  erlauben zusätzlich die **Subtraktion** ( $-$ )
- ganz ähnlich erlauben die rationalen Zahlen  $\mathbb{Q}$  die **Division** ( $/$ )
- $\mathbb{Z}$  und  $\mathbb{Q}$  können als **Abschluss/Erweiterung** der natürlichen Zahlen bezüglich der Subtraktion und Division angesehen werden
- die reellen Zahlen  $\mathbb{R}$  **vervollständigen** die rationalen Zahlen bezüglich Grenzwerteigenschaften die im Analysis-Teil der Vorlesung (Sommersemester) relevant werden

## Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ( $\mathbb{N}$  und  $\mathbb{N}_0$ ) mit den Rechenoperationen  $+$  und  $\cdot$  und der Ordnung  $\leq$  konstruieren wir daraus die **ganzen** ( $\mathbb{Z}$ ), die **rationalen** ( $\mathbb{Q}$ ) und schließlich die **reellen Zahlen** ( $\mathbb{R}$ )
- die ganzen Zahlen  $\mathbb{Z}$  erlauben zusätzlich die **Subtraktion** ( $-$ )
- ganz ähnlich erlauben die rationalen Zahlen  $\mathbb{Q}$  die **Division** ( $/$ )
- $\mathbb{Z}$  und  $\mathbb{Q}$  können als **Abschluss/Erweiterung** der natürlichen Zahlen bezüglich der Subtraktion und Division angesehen werden
- die reellen Zahlen  $\mathbb{R}$  **vervollständigen** die rationalen Zahlen bezüglich Grenzwerteigenschaften die im Analysis-Teil der Vorlesung (Sommersemester) relevant werden
- für die Konstruktionen dieser Zahlenbereiche brauchen wir den Begriff der **Äquivalenzrelation**

# Relationen

## Definition (Relation)

Eine **Relation  $R$  auf einer Menge  $A$**  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ .

# Relationen

## Definition (Relation)

Eine **Relation  $R$  auf einer Menge  $A$**  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

# Relationen

## Definition (Relation)

Eine **Relation  $R$  auf einer Menge  $A$**  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer **Menge**  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer Menge  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .

# Relationen

## Definition (Relation)

Eine **Relation  $R$  auf einer Menge  $A$**  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .
- **antisymmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \wedge (b, a) \in R \implies a = b$ .

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer Menge  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .
- **antisymmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \wedge (b, a) \in R \implies a = b$ .
- **transitiv**: für alle  $a, b, c \in A$  gilt  $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$ .

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer Menge  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .
- **antisymmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \wedge (b, a) \in R \implies a = b$ .
- **transitiv**: für alle  $a, b, c \in A$  gilt  $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$ .

## Definition (Spezielle Relationen)

Eine Relation  $R$  auf  $A$  ist eine

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer Menge  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .
- **antisymmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \wedge (b, a) \in R \implies a = b$ .
- **transitiv**: für alle  $a, b, c \in A$  gilt  $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$ .

## Definition (Spezielle Relationen)

Eine Relation  $R$  auf  $A$  ist eine

- **Teilordnung** (auch **Halbordnung**, **Ordnung**, **partielle Ordnung** genannt), falls  $R$  **reflexiv**, **antisymmetrisch** und **transitiv** ist.

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer Menge  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .
- **antisymmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \wedge (b, a) \in R \implies a = b$ .
- **transitiv**: für alle  $a, b, c \in A$  gilt  $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$ .

## Definition (Spezielle Relationen)

Eine Relation  $R$  auf  $A$  ist eine

- **Teilordnung** (auch **Halbordnung**, **Ordnung**, **partielle Ordnung** genannt), falls  $R$  reflexiv, antisymmetrisch und transitiv ist. z. B.  $\leq$  auf  $\mathbb{N}$

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer Menge  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .
- **antisymmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \wedge (b, a) \in R \implies a = b$ .
- **transitiv**: für alle  $a, b, c \in A$  gilt  $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$ .

## Definition (Spezielle Relationen)

Eine Relation  $R$  auf  $A$  ist eine

- **Teilordnung** (auch **Halbordnung**, **Ordnung**, **partielle Ordnung** genannt), falls  $R$  reflexiv, antisymmetrisch und transitiv ist. z. B.  $\leq$  auf  $\mathbb{N}$  und  $\subseteq$  auf  $\mathcal{P}(M)$

# Relationen

## Definition (Relation)

Eine **Relation**  $R$  auf einer Menge  $A$  ist eine Teilmenge der geordneten Paare aus  $A^2$ , d. h.  $R \subseteq A^2$ . Für  $(a, b) \in R$  schreibt man auch  $aRb$ .

## Definition (Eigenschaften von Relationen)

Eine Relation  $R$  auf  $A$  heißt

- **reflexiv**: für alle  $a \in A$  gilt  $(a, a) \in R$ .
- **symmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \implies (b, a) \in R$ .
- **antisymmetrisch**: für alle  $a, b \in A$  gilt  $(a, b) \in R \wedge (b, a) \in R \implies a = b$ .
- **transitiv**: für alle  $a, b, c \in A$  gilt  $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$ .

## Definition (Spezielle Relationen)

Eine Relation  $R$  auf  $A$  ist eine

- **Teilordnung** (auch **Halbordnung**, **Ordnung**, **partielle Ordnung** genannt), falls  $R$  **reflexiv**, **antisymmetrisch** und **transitiv** ist. **z. B.**  $\leq$  auf  $\mathbb{N}$  und  $\subseteq$  auf  $\mathcal{P}(M)$
- **Äquivalenzrelation**, falls  $R$  **reflexiv**, **symmetrisch** und **transitiv** ist.

# Beispiel: Äquivalenzrelation

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

## Beispiel: Äquivalenzrelation

### Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

## Beispiel: Äquivalenzrelation

### Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- Reflexivität:

## Beispiel: Äquivalenzrelation

### Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓
- **Transitivität:**

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓
- **Transitivität:** Falls  $x + y$  und  $y + z$  gerade sind,

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓
- **Transitivität:** Falls  $x + y$  und  $y + z$  gerade sind, dann ist  $x + 2y + z$  gerade

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓
- **Transitivität:** Falls  $x + y$  und  $y + z$  gerade sind, dann ist  $x + 2y + z$  gerade und, da  $2y$  gerade ist, ist auch  $x + z$  gerade.

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓
- **Transitivität:** Falls  $x + y$  und  $y + z$  gerade sind, dann ist  $x + 2y + z$  gerade und, da  $2y$  gerade ist, ist auch  $x + z$  gerade. D. h. aus  $x \equiv_2 y$  und  $y \equiv_2 z$  folgt  $x \equiv_2 z$  für beliebige  $x, y, z \in \mathbb{N}_0$  ✓

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓
- **Transitivität:** Falls  $x + y$  und  $y + z$  gerade sind, dann ist  $x + 2y + z$  gerade und, da  $2y$  gerade ist, ist auch  $x + z$  gerade. D. h. aus  $x \equiv_2 y$  und  $y \equiv_2 z$  folgt  $x \equiv_2 z$  für beliebige  $x, y, z \in \mathbb{N}_0$  ✓

Relation  $\equiv_2$  ist reflexiv, symmetrisch und transitiv und die Beh. folgt.  $\square$

# Beispiel: Äquivalenzrelation

## Paritäten

Wir definieren eine Relation  $\equiv_2$  auf  $\mathbb{N}_0$  durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$  ist gerade  $\iff x, y$  gerade oder beide ungerade

**Behauptung:**  $\equiv_2$  ist eine Äquivalenzrelation auf  $\mathbb{N}_0$ .

**Beweis:** Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:**  $x + x$  ist gerade für jedes  $x \in \mathbb{N}_0$  ✓
- **Symmetrie:**  $x + y = y + x$  für alle  $x, y \in \mathbb{N}_0$  ✓
- **Transitivität:** Falls  $x + y$  und  $y + z$  gerade sind, dann ist  $x + 2y + z$  gerade und, da  $2y$  gerade ist, ist auch  $x + z$  gerade. D. h. aus  $x \equiv_2 y$  und  $y \equiv_2 z$  folgt  $x \equiv_2 z$  für beliebige  $x, y, z \in \mathbb{N}_0$  ✓

Relation  $\equiv_2$  ist reflexiv, symmetrisch und transitiv und die Beh. folgt. □

**Bemerkung:**  $\equiv_2$  zerlegt  $\mathbb{N}_0$  in zwei disjunkte Mengen (gerade und ungerade Zahlen) innerhalb denen jeweils alle Paare in Relation stehen.

## Definition (Partition)

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ ,

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

**1**  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ ,

nichtleere Teilmengen

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ , nichtleere Teilmengen
- 2  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

**1**  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ ,

nichtleere Teilmengen

**2**  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$

paarweise disjunkt

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ , nichtleere Teilmengen
- 2  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$  paarweise disjunkt
- 3 und  $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$ .

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ ,
- 2  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$
- 3 und  $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$ .

nichtleere Teilmengen  
paarweise disjunkt  
Überdeckung von  $A$

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ ,
- 2  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$
- 3 und  $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$ .

nichtleere Teilmengen  
paarweise disjunkt  
Überdeckung von  $A$

Die Teilmengen aus  $\mathcal{Z}$  heißen **Partitionsklassen**.

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ , nichtleere Teilmengen
- 2  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$  paarweise disjunkt
- 3 und  $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$ . Überdeckung von  $A$

Die Teilmengen aus  $\mathcal{Z}$  heißen **Partitionsklassen**.

**Bemerkung:** Disjunkte Vereinigungen werden wir manchmal mit einem Punkt im Vereinigungszeichen anzeigen (z. B.  $\bigcup \{Z : Z \in \mathcal{Z}\}$ ,  $A \cup B$ , ...).

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ , nichtleere Teilmengen
- 2  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$  paarweise disjunkt
- 3 und  $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$ . Überdeckung von  $A$

Die Teilmengen aus  $\mathcal{Z}$  heißen **Partitionsklassen**.

**Bemerkung:** Disjunkte Vereinigungen werden wir manchmal mit einem Punkt im Vereinigungszeichen anzeigen (z. B.  $\bigcup \{Z : Z \in \mathcal{Z}\}$ ,  $A \cup B$ , ...).

## Beispiele

- $\{\{n \in \mathbb{N}_0 : n \text{ gerade}\}, \{n \in \mathbb{N}_0 : n \text{ ungerade}\}\}$  ist Partition von  $\mathbb{N}_0$

# Partitionen

## Definition (Partition)

Ein **Partition/Zerlegung** einer Menge  $A$  ist eine Menge  $\mathcal{Z} \subseteq \wp(A)$  von Teilmengen von  $A$ , sodass

- 1  $Z \neq \emptyset$  für alle  $Z \in \mathcal{Z}$ , nichtleere Teilmengen
- 2  $Z \cap Z' = \emptyset$  für alle verschiedenen  $Z, Z' \in \mathcal{Z}$  paarweise disjunkt
- 3 und  $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$ . Überdeckung von  $A$

Die Teilmengen aus  $\mathcal{Z}$  heißen **Partitionsklassen**.

**Bemerkung:** Disjunkte Vereinigungen werden wir manchmal mit einem Punkt im Vereinigungszeichen anzeigen (z. B.  $\bigcup \{Z : Z \in \mathcal{Z}\}$ ,  $A \cup B$ , ...).

## Beispiele

- $\{\{n \in \mathbb{N}_0 : n \text{ gerade}\}, \{n \in \mathbb{N}_0 : n \text{ ungerade}\}\}$  ist Partition von  $\mathbb{N}_0$
- die Menge  $\mathcal{Z} = \{Z_k : k \in \mathbb{N}_0\}$  bestehend aus den Mengenfamilien  $Z_k = \{A \subseteq \mathbb{N} : A \text{ hat genau } k \text{ Elemente}\}$  partitioniert die Menge der endlichen Teilmengen von  $\mathbb{N}$  in unendlich viele Partitionsklassen

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ .

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert.

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup \{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup \{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓
- **Symmetrie:** Seien  $a, b \in A$  mit  $a \sim_{\mathcal{Z}} b$ .

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup \{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓
- **Symmetrie:** Seien  $a, b \in A$  mit  $a \sim_{\mathcal{Z}} b$ . D. h. es gibt eine Menge  $Z \in \mathcal{Z}$  mit  $a, b \in Z$  und somit  $b \sim_{\mathcal{Z}} a$ . ✓

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup \{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓
- **Symmetrie:** Seien  $a, b \in A$  mit  $a \sim_{\mathcal{Z}} b$ . D. h. es gibt eine Menge  $Z \in \mathcal{Z}$  mit  $a, b \in Z$  und somit  $b \sim_{\mathcal{Z}} a$ . ✓
- **Transitivität:** Seien  $a, b$  und  $c \in A$  mit  $a \sim_{\mathcal{Z}} b$  und  $b \sim_{\mathcal{Z}} c$ .

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup \{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓
- **Symmetrie:** Seien  $a, b \in A$  mit  $a \sim_{\mathcal{Z}} b$ . D. h. es gibt eine Menge  $Z \in \mathcal{Z}$  mit  $a, b \in Z$  und somit  $b \sim_{\mathcal{Z}} a$ . ✓
- **Transitivität:** Seien  $a, b$  und  $c \in A$  mit  $a \sim_{\mathcal{Z}} b$  und  $b \sim_{\mathcal{Z}} c$ . Nach Definition von  $\sim_{\mathcal{Z}}$  gibt es  $Z$  und  $Z' \in \mathcal{Z}$  mit  $a, b \in Z$  und  $b, c \in Z'$ .

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup\{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓
- **Symmetrie:** Seien  $a, b \in A$  mit  $a \sim_{\mathcal{Z}} b$ . D. h. es gibt eine Menge  $Z \in \mathcal{Z}$  mit  $a, b \in Z$  und somit  $b \sim_{\mathcal{Z}} a$ . ✓
- **Transitivität:** Seien  $a, b$  und  $c \in A$  mit  $a \sim_{\mathcal{Z}} b$  und  $b \sim_{\mathcal{Z}} c$ . Nach Definition von  $\sim_{\mathcal{Z}}$  gibt es  $Z$  und  $Z' \in \mathcal{Z}$  mit  $a, b \in Z$  und  $b, c \in Z'$ . Also gilt  $b \in Z \cap Z'$  und da  $\mathcal{Z}$  eine Partition ist (paarweise disjunkte Elemente), folgt  $Z = Z'$ .

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup \{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓
- **Symmetrie:** Seien  $a, b \in A$  mit  $a \sim_{\mathcal{Z}} b$ . D. h. es gibt eine Menge  $Z \in \mathcal{Z}$  mit  $a, b \in Z$  und somit  $b \sim_{\mathcal{Z}} a$ . ✓
- **Transitivität:** Seien  $a, b$  und  $c \in A$  mit  $a \sim_{\mathcal{Z}} b$  und  $b \sim_{\mathcal{Z}} c$ . Nach Definition von  $\sim_{\mathcal{Z}}$  gibt es  $Z$  und  $Z' \in \mathcal{Z}$  mit  $a, b \in Z$  und  $b, c \in Z'$ . Also gilt  $b \in Z \cap Z'$  und da  $\mathcal{Z}$  eine Partition ist (paarweise disjunkte Elemente), folgt  $Z = Z'$ . Somit enthält  $Z$  neben  $a$  und  $b$  auch  $c$  und es folgt  $a \sim_{\mathcal{Z}} c$ .

# Äquivalenzrelationen und Partitionen

## Satz

Sei  $\mathcal{Z}$  eine Partition der Menge  $A$ . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation  $\sim_{\mathcal{Z}}$  auf  $A$ .

**Beweis:** Sei  $\mathcal{Z}$  eine Partition von  $A$  und  $\sim_{\mathcal{Z}}$  wie in der Behauptung definiert. Wir zeigen, dass  $\sim_{\mathcal{Z}}$  reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei  $a \in A$ . Da  $A = \bigcup \{Z : Z \in \mathcal{Z}\}$  gibt es genau eine Menge  $Z \in \mathcal{Z}$  mit  $a \in Z$  und somit gilt  $a \sim_{\mathcal{Z}} a$ . ✓
- **Symmetrie:** Seien  $a, b \in A$  mit  $a \sim_{\mathcal{Z}} b$ . D. h. es gibt eine Menge  $Z \in \mathcal{Z}$  mit  $a, b \in Z$  und somit  $b \sim_{\mathcal{Z}} a$ . ✓
- **Transitivität:** Seien  $a, b$  und  $c \in A$  mit  $a \sim_{\mathcal{Z}} b$  und  $b \sim_{\mathcal{Z}} c$ . Nach Definition von  $\sim_{\mathcal{Z}}$  gibt es  $Z$  und  $Z' \in \mathcal{Z}$  mit  $a, b \in Z$  und  $b, c \in Z'$ . Also gilt  $b \in Z \cap Z'$  und da  $\mathcal{Z}$  eine Partition ist (paarweise disjunkte Elemente), folgt  $Z = Z'$ . Somit enthält  $Z$  neben  $a$  und  $b$  auch  $c$  und es folgt  $a \sim_{\mathcal{Z}} c$ .

Also erfüllt  $\sim_{\mathcal{Z}}$  die notwendigen Eigenschaften einer Äquivalenzrelation.  $\square$

### Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ .

### Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

### Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

### Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
$$Z_a := \{b \in A : a \sim b\}.$$
- $\mathcal{Z}$  ist Partition:

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
$$Z_a := \{b \in A : a \sim b\}.$$
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - nichtleer und  $\bigcup \mathcal{Z} = A$ :  $\sim$  reflexiv

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - nichtleer und  $\bigcup \mathcal{Z} = A$ :  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
$$Z_a := \{b \in A : a \sim b\}.$$
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .

Wir zeigen nun  $Z_a \subseteq Z_b$ :

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .  
Wir zeigen nun  $Z_a \subseteq Z_b$ : Sei  $x \in Z_a$  beliebig

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .

Wir zeigen nun  $Z_a \subseteq Z_b$ : Sei  $x \in Z_a$  beliebig  $\Rightarrow a \sim x$  und wegen der Symmetrie und Transitivität und  $a \sim b$  folgt auch  $b \sim x$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .

Wir zeigen nun  $Z_a \subseteq Z_b$ : Sei  $x \in Z_a$  beliebig  $\Rightarrow a \sim x$  und wegen der Symmetrie und Transitivität und  $a \sim b$  folgt auch  $b \sim x \Rightarrow x \in Z_b$ .

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .

Wir zeigen nun  $Z_a \subseteq Z_b$ : Sei  $x \in Z_a$  beliebig  $\Rightarrow a \sim x$  und wegen der Symmetrie und Transitivität und  $a \sim b$  folgt auch  $b \sim x \Rightarrow x \in Z_b$ .

Da  $x \in Z_a$  beliebig war, gilt  $Z_a \subseteq Z_b$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$   
 $Z_a := \{b \in A : a \sim b\}$ .
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .

Wir zeigen nun  $Z_a \subseteq Z_b$ : Sei  $x \in Z_a$  beliebig  $\Rightarrow a \sim x$  und wegen der Symmetrie und Transitivität und  $a \sim b$  folgt auch  $b \sim x \Rightarrow x \in Z_b$ .

Da  $x \in Z_a$  beliebig war, gilt  $Z_a \subseteq Z_b$  und die gleiche Argumentation zeigt auch  $Z_b \subseteq Z_a$

## Satz

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $A$ . Dann gibt es **genau** eine Partition  $\mathcal{Z}$  von  $A$  mit  $\sim = \sim_{\mathcal{Z}}$ .

**Beweis:** Sei  $\sim$  eine Äquivalenzrelation auf  $A$ . Zuerst zeigen wir die Existenz einer Partition  $\mathcal{Z}$  mit  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit.

- **Definition von  $\mathcal{Z}$ :** Setze  $\mathcal{Z} := \{Z_a : a \in A\}$ , wobei für jedes  $a \in A$ 

$$Z_a := \{b \in A : a \sim b\}.$$
- **$\mathcal{Z}$  ist Partition:** Wir zeigen, dass die Mengen  $Z_a$  nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz  $A$  ergibt.
  - **nichtleer und  $\bigcup \mathcal{Z} = A$ :**  $\sim$  reflexiv  $\Rightarrow a \sim a$  für jedes  $a \in A$   
 $\Rightarrow a \in Z_a$  für jedes  $a \in A \Rightarrow Z_a \neq \emptyset$  für jedes  $a \in A$  und  $\bigcup_{a \in A} Z_a = A$  ✓
  - **disjunkt:** Angenommen  $c \in Z_a \cap Z_b \Rightarrow a \sim c$  und  $b \sim c$  und wegen der Symmetrie und Transitivität von  $\sim$  folgt  $a \sim b$ .

Wir zeigen nun  $Z_a \subseteq Z_b$ : Sei  $x \in Z_a$  beliebig  $\Rightarrow a \sim x$  und wegen der Symmetrie und Transitivität und  $a \sim b$  folgt auch  $b \sim x \Rightarrow x \in Z_b$ .

Da  $x \in Z_a$  beliebig war, gilt  $Z_a \subseteq Z_b$  und die gleiche Argumentation zeigt auch  $Z_b \subseteq Z_a$  und somit  $Z_a = Z_b$ , falls  $Z_a \cap Z_b \neq \emptyset$ . ✓

Als nächstes zeigen wir  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit von  $\mathcal{A}$ .

Als nächstes zeigen wir  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit von  $\mathcal{A}$ .

- $\sim \subseteq \sim_{\mathcal{Z}}$ : Sei  $a \sim b$ , also  $(a, b) \in \sim$ . Dann gilt  $a, b \in Z_a$  und aus der Definition von  $\sim_{\mathcal{Z}}$  folgt  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . ✓

Als nächstes zeigen wir  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit von  $\mathcal{A}$ .

- $\sim \subseteq \sim_{\mathcal{Z}}$ : Sei  $a \sim b$ , also  $(a, b) \in \sim$ . Dann gilt  $a, b \in Z_a$  und aus der Definition von  $\sim_{\mathcal{Z}}$  folgt  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . ✓
- $\sim_{\mathcal{Z}} \subseteq \sim$ : Sei nun  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . Dann existiert ein  $Z \in \mathcal{Z}$  mit  $a, b \in Z$ . Wegen der Definition von  $\mathcal{Z}$  gibt es ein  $a' \in Z$  mit  $Z = Z_{a'}$ .

Als nächstes zeigen wir  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit von  $\mathcal{A}$ .

- $\sim \subseteq \sim_{\mathcal{Z}}$ : Sei  $a \sim b$ , also  $(a, b) \in \sim$ . Dann gilt  $a, b \in Z_a$  und aus der Definition von  $\sim_{\mathcal{Z}}$  folgt  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . ✓
- $\sim_{\mathcal{Z}} \subseteq \sim$ : Sei nun  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . Dann existiert ein  $Z \in \mathcal{Z}$  mit  $a, b \in Z$ . Wegen der Definition von  $\mathcal{Z}$  gibt es ein  $a' \in Z$  mit  $Z = Z_{a'}$ .  
Da also  $a, b$  aus  $Z_{a'}$  sind, folgt  $a' \sim a$  und  $a' \sim b$  und mit Symmetrie und Transitivität von  $\sim$  auch  $a \sim b$ . D. h.  $(a, b) \in \sim$  wie gewünscht. ✓

Als nächstes zeigen wir  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit von  $\mathcal{A}$ .

- $\sim \subseteq \sim_{\mathcal{Z}}$ : Sei  $a \sim b$ , also  $(a, b) \in \sim$ . Dann gilt  $a, b \in Z_a$  und aus der Definition von  $\sim_{\mathcal{Z}}$  folgt  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . ✓
- $\sim_{\mathcal{Z}} \subseteq \sim$ : Sei nun  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . Dann existiert ein  $Z \in \mathcal{Z}$  mit  $a, b \in Z$ . Wegen der Definition von  $\mathcal{Z}$  gibt es ein  $a' \in Z$  mit  $Z = Z_{a'}$ .  
Da also  $a, b$  aus  $Z_{a'}$  sind, folgt  $a' \sim a$  und  $a' \sim b$  und mit Symmetrie und Transitivität von  $\sim$  auch  $a \sim b$ . D. h.  $(a, b) \in \sim$  wie gewünscht. ✓
- **Eindeutigkeit**: Sei  $\mathcal{Y}$  eine weitere Partition mit  $\sim_{\mathcal{Y}} = \sim$ . Aus dem bereits Gezeigten folgt also  $\sim_{\mathcal{Y}} = \sim = \sim_{\mathcal{Z}}$  und somit gilt für alle  $a, b \in A$

$$a \sim_{\mathcal{Y}} b \iff a \sim b \iff a \sim_{\mathcal{Z}} b.$$

Als nächstes zeigen wir  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit von  $\mathcal{A}$ .

- $\sim \subseteq \sim_{\mathcal{Z}}$ : Sei  $a \sim b$ , also  $(a, b) \in \sim$ . Dann gilt  $a, b \in Z_a$  und aus der Definition von  $\sim_{\mathcal{Z}}$  folgt  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . ✓
- $\sim_{\mathcal{Z}} \subseteq \sim$ : Sei nun  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . Dann existiert ein  $Z \in \mathcal{Z}$  mit  $a, b \in Z$ . Wegen der Definition von  $\mathcal{Z}$  gibt es ein  $a' \in Z$  mit  $Z = Z_{a'}$ .  
Da also  $a, b$  aus  $Z_{a'}$  sind, folgt  $a' \sim a$  und  $a' \sim b$  und mit Symmetrie und Transitivität von  $\sim$  auch  $a \sim b$ . D. h.  $(a, b) \in \sim$  wie gewünscht. ✓
- **Eindeutigkeit**: Sei  $\mathcal{Y}$  eine weitere Partition mit  $\sim_{\mathcal{Y}} = \sim$ . Aus dem bereits Gezeigten folgt also  $\sim_{\mathcal{Y}} = \sim = \sim_{\mathcal{Z}}$  und somit gilt für alle  $a, b \in A$

$$a \sim_{\mathcal{Y}} b \iff a \sim b \iff a \sim_{\mathcal{Z}} b.$$

Folglich gilt für alle  $a \in A$  auch

$$Y_a := \{b \in A : a \sim_{\mathcal{Y}} b\} = \{b \in A : a \sim b\} = Z_a.$$

Somit ist  $\{Y_a : a \in A\} = \mathcal{Z}$ .

Als nächstes zeigen wir  $\sim = \sim_{\mathcal{Z}}$  und dann die Eindeutigkeit von  $\mathcal{A}$ .

- $\sim \subseteq \sim_{\mathcal{Z}}$ : Sei  $a \sim b$ , also  $(a, b) \in \sim$ . Dann gilt  $a, b \in Z_a$  und aus der Definition von  $\sim_{\mathcal{Z}}$  folgt  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . ✓
- $\sim_{\mathcal{Z}} \subseteq \sim$ : Sei nun  $a \sim_{\mathcal{Z}} b$ , also  $(a, b) \in \sim_{\mathcal{Z}}$ . Dann existiert ein  $Z \in \mathcal{Z}$  mit  $a, b \in Z$ . Wegen der Definition von  $\mathcal{Z}$  gibt es ein  $a' \in Z$  mit  $Z = Z_{a'}$ .  
Da also  $a, b$  aus  $Z_{a'}$  sind, folgt  $a' \sim a$  und  $a' \sim b$  und mit Symmetrie und Transitivität von  $\sim$  auch  $a \sim b$ . D. h.  $(a, b) \in \sim$  wie gewünscht. ✓
- **Eindeutigkeit**: Sei  $\mathcal{Y}$  eine weitere Partition mit  $\sim_{\mathcal{Y}} = \sim$ . Aus dem bereits Gezeigten folgt also  $\sim_{\mathcal{Y}} = \sim = \sim_{\mathcal{Z}}$  und somit gilt für alle  $a, b \in A$

$$a \sim_{\mathcal{Y}} b \iff a \sim b \iff a \sim_{\mathcal{Z}} b.$$

Folglich gilt für alle  $a \in A$  auch

$$Y_a := \{b \in A : a \sim_{\mathcal{Y}} b\} = \{b \in A : a \sim b\} = Z_a.$$

Somit ist  $\{Y_a : a \in A\} = \mathcal{Z}$ .

Des Weiteren ist  $Y_a$  offensichtlich eine Teilmenge der Menge  $Y \in \mathcal{Y}$ , die  $a$  enthält. Aber wegen der Transitivität von  $\sim_{\mathcal{Y}}$  gilt tatsächlich  $Y_a = Y$ . D. h.

$\{Y_a : a \in A\} = \mathcal{Y}$ , also  $\mathcal{Y} = \mathcal{Z}$  was den Beweis abschließt. □

# Äquivalenzklassen

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

- Die eindeutig bestimmte Partition  $\mathcal{Z}$  aus dem letzten Satz bezeichnet man mit  $A/\sim$  und sie heißt **Faktormenge/Quotientenmenge**.

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

- Die eindeutig bestimmte Partition  $\mathcal{Z}$  aus dem letzten Satz bezeichnet man mit  $A/\sim$  und sie heißt **Faktormenge/Quotientenmenge**.
- Die Elemente von  $A/\sim$  heißen **Äquivalenzklassen**, welche man mit  $[a]$  (manchmal auch  $\bar{a}$ ) statt  $Z_a$  bezeichnet.

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

- Die eindeutig bestimmte Partition  $\mathcal{Z}$  aus dem letzten Satz bezeichnet man mit  $A/\sim$  und sie heißt **Faktormenge/Quotientenmenge**.
- Die Elemente von  $A/\sim$  heißen **Äquivalenzklassen**, welche man mit  $[a]$  (manchmal auch  $\bar{a}$ ) statt  $Z_a$  bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die **Repräsentanten** dieser Äquivalenzklasse und wir sagen, sie sind **äquivalent** zueinander.

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

- Die eindeutig bestimmte Partition  $\mathcal{Z}$  aus dem letzten Satz bezeichnet man mit  $A/\sim$  und sie heißt **Faktormenge/Quotientenmenge**.
- Die Elemente von  $A/\sim$  heißen **Äquivalenzklassen**, welche man mit  $[a]$  (manchmal auch  $\bar{a}$ ) statt  $Z_a$  bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die **Repräsentanten** dieser Äquivalenzklasse und wir sagen, sie sind **äquivalent** zueinander.
- Äquivalenzklassen sind also paarweise disjunkt.

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

- Die eindeutig bestimmte Partition  $\mathcal{Z}$  aus dem letzten Satz bezeichnet man mit  $A/\sim$  und sie heißt **Faktormenge/Quotientenmenge**.
- Die Elemente von  $A/\sim$  heißen **Äquivalenzklassen**, welche man mit  $[a]$  (manchmal auch  $\bar{a}$ ) statt  $Z_a$  bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die **Repräsentanten** dieser Äquivalenzklasse und wir sagen, sie sind **äquivalent** zueinander.
- Äquivalenzklassen sind also paarweise disjunkt.
- Zwei Elemente  $a$  und  $b \in A$  repräsentieren also die gleiche Äquivalenzklasse genau dann, wenn sie äquivalent sind

$$[a] = [b] \iff a \sim b.$$

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

- Die eindeutig bestimmte Partition  $\mathcal{Z}$  aus dem letzten Satz bezeichnet man mit  $A/\sim$  und sie heißt **Faktormenge/Quotientenmenge**.
- Die Elemente von  $A/\sim$  heißen **Äquivalenzklassen**, welche man mit  $[a]$  (manchmal auch  $\bar{a}$ ) statt  $Z_a$  bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die **Repräsentanten** dieser Äquivalenzklasse und wir sagen, sie sind **äquivalent** zueinander.
- Äquivalenzklassen sind also paarweise disjunkt.
- Zwei Elemente  $a$  und  $b \in A$  repräsentieren also die gleiche Äquivalenzklasse genau dann, wenn sie äquivalent sind
$$[a] = [b] \iff a \sim b.$$
- Die Funktion  $a \mapsto [a]$  heißt **kanonische Projektion** von  $A$  nach  $A/\sim$ .

# Äquivalenzklassen

## Definition (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf  $A$ .

- Die eindeutig bestimmte Partition  $\mathcal{Z}$  aus dem letzten Satz bezeichnet man mit  $A/\sim$  und sie heißt **Faktormenge/Quotientenmenge**.
- Die Elemente von  $A/\sim$  heißen **Äquivalenzklassen**, welche man mit  $[a]$  (manchmal auch  $\bar{a}$ ) statt  $Z_a$  bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die **Repräsentanten** dieser Äquivalenzklasse und wir sagen, sie sind **äquivalent** zueinander.
- Äquivalenzklassen sind also paarweise disjunkt.
- Zwei Elemente  $a$  und  $b \in A$  repräsentieren also die gleiche Äquivalenzklasse genau dann, wenn sie äquivalent sind
$$[a] = [b] \iff a \sim b.$$
- Die Funktion  $a \mapsto [a]$  heißt **kanonische Projektion** von  $A$  nach  $A/\sim$ .

**Beispiel:** Partitioniert man  $\mathbb{N}$  in die geraden und ungeraden Zahlen und bezeichnet diese Partition mit  $\mathcal{Z}$ , so ist  $\sim_{\mathcal{Z}}$  die Äquivalenzrelation mit zwei Äquivalenzklassen und zwei Zahlen sind genau dann äquivalent, wenn sie die gleiche Parität haben. Jede ungerade Zahl repräsentiert die Äquivalenzklasse der ungeraden Zahlen usw.

# Wie macht man Funktionen injektiv?

# Wie macht man Funktionen injektiv?

## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \quad :\iff \quad f(a) = f(a').$$

# Wie macht man Funktionen injektiv?

## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \quad :\iff \quad f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

# Wie macht man Funktionen injektiv?

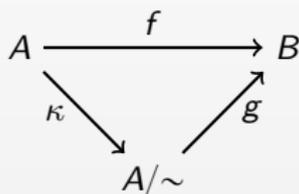
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \quad :\iff \quad f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



# Wie macht man Funktionen injektiv?

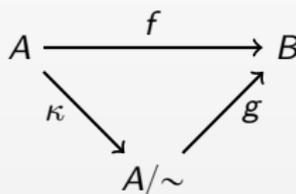
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \iff f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

# Wie macht man Funktionen injektiv?

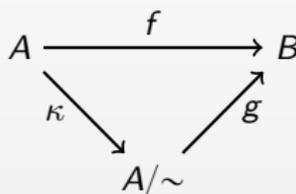
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \iff f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

- 1  $\sim$  ist eine Äquivalenzrelation,

# Wie macht man Funktionen injektiv?

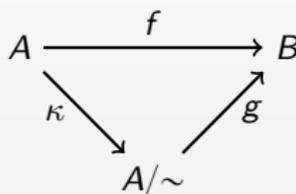
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \iff f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

- 1  $\sim$  ist eine Äquivalenzrelation,



# Wie macht man Funktionen injektiv?

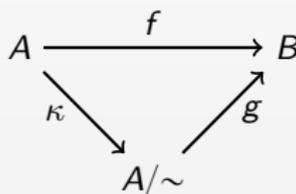
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \iff f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

- 1  $\sim$  ist eine Äquivalenzrelation,
- 2  $g$  ist wohldefiniert



# Wie macht man Funktionen injektiv?

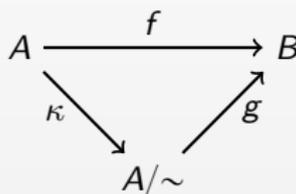
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \quad :\iff \quad f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

- 1  $\sim$  ist eine Äquivalenzrelation, ✓
- 2  $g$  ist **wohldefiniert**, d. h.  $g([a])$  ist unabhängig vom gewählten Repräsentanten!

# Wie macht man Funktionen injektiv?

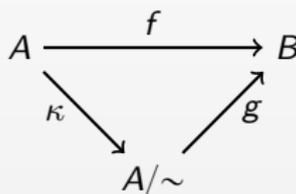
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \iff f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

- 1  $\sim$  ist eine Äquivalenzrelation, ✓
- 2  $g$  ist **wohldefiniert**, d. h.  $g([a])$  ist unabhängig vom gewählten Repräsentanten! ✓

# Wie macht man Funktionen injektiv?

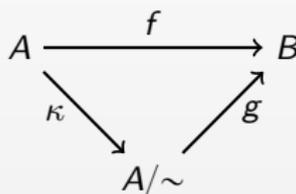
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \iff f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

- 1  $\sim$  ist eine Äquivalenzrelation, ✓
- 2  $g$  ist **wohldefiniert**, d. h.  $g([a])$  ist unabhängig vom gewählten Repräsentanten! ✓
- 3  $g$  ist injektiv.

# Wie macht man Funktionen injektiv?

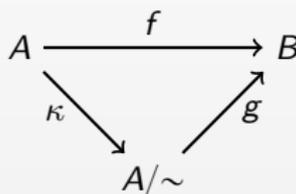
## Satz

Sei  $f: A \rightarrow B$  eine Funktion. Für  $a, a' \in A$  definiere die Relation  $\sim$  durch

$$a \sim a' \iff f(a) = f(a').$$

Dann ist  $\sim$  eine Äquivalenzrelation und  $[a] \mapsto f(a)$  eine injektive Funktion  $g: A/\sim \rightarrow B$ .

Sei  $\kappa$  die kanonische Projektion von  $\sim$ . Dann besagt der Satz, es gibt inj.  $g$  mit  $f = g \circ \kappa$



## Beweis

Zu zeigen ist:

- 1  $\sim$  ist eine Äquivalenzrelation, ✓
- 2  $g$  ist **wohldefiniert**, d. h.  $g([a])$  ist unabhängig vom gewählten Repräsentanten! ✓
- 3  $g$  ist injektiv. ✓



# Ganze Zahlen

**Idee:**

## Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von  $\mathbb{N}_0$  definiert werden. Z. B.  $7 - 12$  liegt nicht in  $\mathbb{N}_0$ .

## Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von  $\mathbb{N}_0$  definiert werden. Z. B.  $7 - 12$  liegt nicht in  $\mathbb{N}_0$ .
- Vervollständige  $\mathbb{N}_0$  für die Abgeschlossenheit der Subtraktion.

# Ganze Zahlen

## Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von  $\mathbb{N}_0$  definiert werden. Z. B.  $7 - 12$  liegt nicht in  $\mathbb{N}_0$ .
- Vervollständige  $\mathbb{N}_0$  für die Abgeschlossenheit der Subtraktion.
- Definiere die ganze Zahl  $z$  als Menge der Paare  $(a, b) \in \mathbb{N}_0^2$  mit „ $a - b = z$ “ (z. B.  $(7, 12)$  und  $(0, 5)$  sind Repräsentanten von  $-5$ ).

## Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von  $\mathbb{N}_0$  definiert werden. Z. B.  $7 - 12$  liegt nicht in  $\mathbb{N}_0$ .
- Vervollständige  $\mathbb{N}_0$  für die Abgeschlossenheit der Subtraktion.
- Definiere die ganze Zahl  $z$  als Menge der Paare  $(a, b) \in \mathbb{N}_0^2$  mit „ $a - b = z$ “ (z. B.  $(7, 12)$  und  $(0, 5)$  sind Repräsentanten von  $-5$ ).
- Da es aber kein „ $-$ “ in  $\mathbb{N}_0$  gibt, drücken wir diese Beziehung innerhalb von  $\mathbb{N}_0$  durch „umstellen“ wie folgt aus

$$\text{„}a - b = a' - b'\text{“} \quad \iff \quad a + b' = a' + b.$$

# Ganze Zahlen

## Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von  $\mathbb{N}_0$  definiert werden. Z. B.  $7 - 12$  liegt nicht in  $\mathbb{N}_0$ .
- Vervollständige  $\mathbb{N}_0$  für die Abgeschlossenheit der Subtraktion.
- Definiere die ganze Zahl  $z$  als Menge der Paare  $(a, b) \in \mathbb{N}_0^2$  mit „ $a - b = z$ “ (z. B.  $(7, 12)$  und  $(0, 5)$  sind Repräsentanten von  $-5$ ).
- Da es aber kein „ $-$ “ in  $\mathbb{N}_0$  gibt, drücken wir diese Beziehung innerhalb von  $\mathbb{N}_0$  durch „umstellen“ wie folgt aus

$$\text{„}a - b = a' - b'\text{“} \iff a + b' = a' + b.$$

- Damit definieren wir eine Äquivalenzrelation auf  $\mathbb{N}_0^2$  deren Äquivalenzklassen den ganzen Zahlen entsprechen.

# Ganze Zahlen

formale Definition

Idee

Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \iff a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \iff a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \iff a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \Leftrightarrow a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

$$[(a, b)] +_{\mathbb{Z}} [(a', b')] : \Leftrightarrow [(a + a', b + b')], \quad \text{„}(a - b) + (a' - b') = (a + a') - (b + b')\text{“}$$

$$[(a, b)] \cdot_{\mathbb{Z}} [(a', b')] : \Leftrightarrow [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], \quad \text{„}(a - b) \cdot (a' - b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“}$$

$$[(a, b)] \leq_{\mathbb{Z}} [(a', b')] : \Leftrightarrow a + b' \leq a' + b. \quad \text{„}(a - b) \leq (a' - b')\text{“}$$

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \Leftrightarrow a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

$$\begin{aligned} [(a, b)] +_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a+a', b+b')], & \text{„}(a-b) + (a'-b') = (a+a') - (b+b')\text{“} \\ [(a, b)] \cdot_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], & \text{„}(a-b) \cdot (a'-b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“} \\ [(a, b)] \leq_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow a + b' \leq a' + b. & \text{„}(a-b) \leq (a' - b')\text{“} \end{aligned}$$

## Bemerkungen:

- $+_{\mathbb{Z}}$ ,  $\cdot_{\mathbb{Z}}$  und  $\leq_{\mathbb{Z}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \Leftrightarrow a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

$$\begin{aligned} [(a, b)] +_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a+a', b+b')], & \text{„}(a-b) + (a'-b') = (a+a') - (b+b')\text{“} \\ [(a, b)] \cdot_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], & \text{„}(a-b) \cdot (a'-b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“} \\ [(a, b)] \leq_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow a + b' \leq a' + b. & \text{„}(a-b) \leq (a' - b')\text{“} \end{aligned}$$

## Bemerkungen:

- $+_{\mathbb{Z}}$ ,  $\cdot_{\mathbb{Z}}$  und  $\leq_{\mathbb{Z}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- $\mathbb{Z}$  **“erbt”** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{N}_0$

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \Leftrightarrow a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

$$\begin{aligned} [(a, b)] +_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a+a', b+b')], & \text{„}(a-b) + (a'-b') = (a+a') - (b+b')\text{“} \\ [(a, b)] \cdot_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], & \text{„}(a-b) \cdot (a'-b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“} \\ [(a, b)] \leq_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow a + b' \leq a' + b. & \text{„}(a-b) \leq (a'-b')\text{“} \end{aligned}$$

## Bemerkungen:

- $+_{\mathbb{Z}}$ ,  $\cdot_{\mathbb{Z}}$  und  $\leq_{\mathbb{Z}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- $\mathbb{Z}$  **“erbt”** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{N}_0$
- für jedes  $z \in \mathbb{Z}$  gibt es genau ein  $z' \in \mathbb{Z}$  mit  $z + z' = 0$

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \Leftrightarrow a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

$$\begin{aligned} [(a, b)] +_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a+a', b+b')], & \text{„}(a-b) + (a'-b') = (a+a') - (b+b')\text{“} \\ [(a, b)] \cdot_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], & \text{„}(a-b) \cdot (a'-b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“} \\ [(a, b)] \leq_{\mathbb{Z}} [(a', b')] &: \Leftrightarrow a + b' \leq a' + b. & \text{„}(a-b) \leq (a' - b')\text{“} \end{aligned}$$

## Bemerkungen:

- $+_{\mathbb{Z}}$ ,  $\cdot_{\mathbb{Z}}$  und  $\leq_{\mathbb{Z}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- $\mathbb{Z}$  **“erbt”** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{N}_0$
- für jedes  $z \in \mathbb{Z}$  gibt es genau ein  $z' \in \mathbb{Z}$  mit  $z + z' = 0$   $[(a, b)] + [(b, a)] \sim [(0, 0)]$

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \iff a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

$$[(a, b)] +_{\mathbb{Z}} [(a', b')] : \iff [(a+a', b+b')],$$

$$\text{„}(a-b) + (a'-b') = (a+a') - (b+b')\text{“}$$

$$[(a, b)] \cdot_{\mathbb{Z}} [(a', b')] : \iff [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], \quad \text{„}(a-b) \cdot (a'-b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“}$$

$$[(a, b)] \leq_{\mathbb{Z}} [(a', b')] : \iff a + b' \leq a' + b.$$

$$\text{„}(a-b) \leq (a'-b')\text{“}$$

## Bemerkungen:

- $+_{\mathbb{Z}}$ ,  $\cdot_{\mathbb{Z}}$  und  $\leq_{\mathbb{Z}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- $\mathbb{Z}$  **“erbt“** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{N}_0$
- für jedes  $z \in \mathbb{Z}$  gibt es genau ein  $z' \in \mathbb{Z}$  mit  $z + z' = 0$   $[(a, b)] + [(b, a)] \sim [(0, 0)]$
- $z'$  bezeichnen wir mit  $-z$

# Ganze Zahlen

formale Definition

Idee

## Definition ( $\mathbb{Z}$ )

Durch

$$(a, b) \sim (a', b') : \iff a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf  $\mathbb{N}_0^2$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $\mathbb{N}_0^2 / \sim$  mit  $\mathbb{Z}$  und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form  $[(n, 0)]$  bezeichnen wir kürzer durch die natürliche Zahl  $n$  und ganze Zahlen der Form  $[(0, n)]$  als  $-n$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  von  $\mathbb{N}$  erweitert man auf ganz  $\mathbb{Z}$  durch:

$$\begin{aligned} [(a, b)] +_{\mathbb{Z}} [(a', b')] &: \iff [(a+a', b+b')], & \text{„}(a-b) + (a'-b') = (a+a') - (b+b')\text{“} \\ [(a, b)] \cdot_{\mathbb{Z}} [(a', b')] &: \iff [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], & \text{„}(a-b) \cdot (a'-b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“} \\ [(a, b)] \leq_{\mathbb{Z}} [(a', b')] &: \iff a + b' \leq a' + b. & \text{„}(a-b) \leq (a' - b')\text{“} \end{aligned}$$

## Bemerkungen:

- $+_{\mathbb{Z}}$ ,  $\cdot_{\mathbb{Z}}$  und  $\leq_{\mathbb{Z}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- $\mathbb{Z}$  **“erbt”** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{N}_0$
- für jedes  $z \in \mathbb{Z}$  gibt es genau ein  $z' \in \mathbb{Z}$  mit  $z + z' = 0$   $[(a, b)] + [(b, a)] \sim [(0, 0)]$
- $z'$  bezeichnen wir mit  $-z$
- allgemein definieren wir dann die **Subtraktion**  $x - y := x + (-y)$   
 $- : \mathbb{Z}^2 \rightarrow \mathbb{Z}$  mit  $(x, y) \mapsto x + (-y)$

**Idee:**

## Idee:

- vervollständige  $\mathbb{Z}$  für die Abgeschlossenheit bezüglich der Division

## Idee:

- vervollständige  $\mathbb{Z}$  für die Abgeschlossenheit bezüglich der Division
- Definiere die rationale Zahl  $q$  durch ihre Bruchdarstellungen, d. h. das Paar von ganzen Zahlen  $(a, b)$  mit  $b \neq 0$  soll die rationale Zahl  $q = a/b$  repräsentieren und verschiedene Bruchdarstellungen der Selben Zahl  $q$  werden gleich (äquivalent) gesetzt.

## Idee:

- vervollständige  $\mathbb{Z}$  für die Abgeschlossenheit bezüglich der Division
- Definiere die rationale Zahl  $q$  durch ihre Bruchdarstellungen, d. h. das Paar von ganzen Zahlen  $(a, b)$  mit  $b \neq 0$  soll die rationale Zahl  $q = a/b$  repräsentieren und verschiedene Bruchdarstellungen der Selben Zahl  $q$  werden gleich (äquivalent) gesetzt.
- Ähnlich wie bei der Darstellung von „-“, stellen wir um

$$\frac{a}{b} = \frac{a'}{b'} \iff a \cdot b' = a' \cdot b.$$

## Idee:

- vervollständige  $\mathbb{Z}$  für die Abgeschlossenheit bezüglich der Division
- Definiere die rationale Zahl  $q$  durch ihre Bruchdarstellungen, d. h. das Paar von ganzen Zahlen  $(a, b)$  mit  $b \neq 0$  soll die rationale Zahl  $q = a/b$  repräsentieren und verschiedene Bruchdarstellungen der Selben Zahl  $q$  werden gleich (äquivalent) gesetzt.
- Ähnlich wie bei der Darstellung von „-“, stellen wir um

$$\frac{a}{b} = \frac{a'}{b'} \iff a \cdot b' = a' \cdot b.$$

- Damit definieren wir eine Äquivalenzrelation auf der Menge

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$$

deren Äquivalenzklassen den rationalen Zahlen entsprechen.

# Rationale Zahlen

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

$$\text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b$$

$$\text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+_{\mathbb{Q}}$ ,  $\cdot_{\mathbb{Q}}$  und  $\leq_{\mathbb{Q}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+_{\mathbb{Q}}$ ,  $\cdot_{\mathbb{Q}}$  und  $\leq_{\mathbb{Q}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- wir definieren die Subtraktion analog wie in  $\mathbb{Z}$ , d. h. für  $q = [(a, b)]$  setze  $-q = [(-a, b)]$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+$ ,  $\cdot$  und  $\leq_{\mathbb{Q}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- wir definieren die Subtraktion analog wie in  $\mathbb{Z}$ , d. h. für  $q = [(a, b)]$  setze  $-q = [(-a, b)]$
- $\mathbb{Q}$  **“erbt”** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{Z}$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+$ ,  $\cdot$  und  $\leq_{\mathbb{Q}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- wir definieren die Subtraktion analog wie in  $\mathbb{Z}$ , d. h. für  $q = [(a, b)]$  setze  $-q = [(-a, b)]$
- $\mathbb{Q}$  **“erbt“** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{Z}$
- für jedes  $q \in \mathbb{Q} \setminus \{0\}$  gibt es genau ein  $q' \in \mathbb{Q}$  mit  $q \cdot q' = 1$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+$ ,  $\cdot$  und  $\leq_{\mathbb{Q}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- wir definieren die Subtraktion analog wie in  $\mathbb{Z}$ , d. h. für  $q = [(a, b)]$  setze  $-q = [(-a, b)]$
- $\mathbb{Q}$  **“erbt“** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{Z}$
- für jedes  $q \in \mathbb{Q} \setminus \{0\}$  gibt es genau ein  $q' \in \mathbb{Q}$  mit  $q \cdot q' = 1$   $[(a, b)] \cdot [(b, a)] \approx [(1, 1)]$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+$ ,  $\cdot$  und  $\leq_{\mathbb{Q}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- wir definieren die Subtraktion analog wie in  $\mathbb{Z}$ , d. h. für  $q = [(a, b)]$  setze  $-q = [(-a, b)]$
- $\mathbb{Q}$  **“erbt“** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{Z}$
- für jedes  $q \in \mathbb{Q} \setminus \{0\}$  gibt es genau ein  $q' \in \mathbb{Q}$  mit  $q \cdot q' = 1$   $[(a, b)] \cdot [(b, a)] \approx [(1, 1)]$
- $q'$  bezeichnen wir mit  $1/q$  bzw.  $q^{-1}$

# Rationale Zahlen

## Definition ( $\mathbb{Q}$ )

Durch

$$(a, b) \approx (a', b') : \iff a \cdot b' = a' \cdot b \quad \text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge  $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$  mit  $\mathbb{Q}$  und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form  $[(z, 1)]$  bezeichnen wir kürzer durch die ganze Zahl  $z$  und rationale Zahlen der Form  $[(1, z)]$  als  $1/z$  bzw.  $z^{-1}$ .

Die Operationen  $+$  und  $\cdot$  und die Ordnung  $\leq$  aus  $\mathbb{Z}$  erweitert man auf ganz  $\mathbb{Q}$  durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot b' + a' \cdot b, b \cdot b')], \quad \text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] : \iff [(a \cdot a', b \cdot b')], \quad \text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] : \iff a \cdot b' \leq a' \cdot b. \quad \text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+$ ,  $\cdot$  und  $\leq_{\mathbb{Q}}$  sind **wohldefiniert** und wir schreiben einfach  $+$ ,  $\cdot$  und  $\leq$
- wir definieren die Subtraktion analog wie in  $\mathbb{Z}$ , d. h. für  $q = [(a, b)]$  setze  $-q = [(-a, b)]$
- $\mathbb{Q}$  **“erbt“** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von  $\mathbb{Z}$
- für jedes  $q \in \mathbb{Q} \setminus \{0\}$  gibt es genau ein  $q' \in \mathbb{Q}$  mit  $q \cdot q' = 1$   $[(a, b)] \cdot [(b, a)] \approx [(1, 1)]$
- $q'$  bezeichnen wir mit  $1/q$  bzw.  $q^{-1}$
- allgemein definieren wir dann die **Division**  $x/y := x \cdot (y^{-1})$



# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**,

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetz:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetz:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$  erfüllt

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$  erfüllt (K1)–(K4) mit der üblichen Addition und Multiplikation

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetz:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetz:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$  erfüllt (K1)–(K4) mit der üblichen Addition und Multiplikation
- $\mathbb{Z}$  erfüllt

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetz:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetz:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$  erfüllt (K1)–(K4) mit der üblichen Addition und Multiplikation
- $\mathbb{Z}$  erfüllt (K1)–(K4) und

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetz:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetz:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$  erfüllt (K1)–(K4) mit der üblichen Addition und Multiplikation
- $\mathbb{Z}$  erfüllt (K1)–(K4) und den ersten Teil von (K5)

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetz:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetz:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$  erfüllt (K1)–(K4) mit der üblichen Addition und Multiplikation
- $\mathbb{Z}$  erfüllt (K1)–(K4) und den ersten Teil von (K5)
- $\mathbb{Q}$  erfüllt

# Körper

## Definition (Körper)

Sei  $K$  eine Menge

- mit zwei verschiedenen Elementen  $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$ .

Wir sagen  $K$  (genauer  $(K, +, \cdot)$  bzw.  $(K, +, \cdot, 0_K, 1_K)$ ) ist ein **Körper**, wenn für alle  $a, b, c \in K$  die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetz:**  $a + (b + c) = (a + b) + c$  und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetz:**  $a + b = b + a$  und  $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:**  $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:**  $a + 0_K = a$  und  $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein  $-a \in K$  mit  $a + (-a) = 0_K$ .
- falls  $a \neq 0_K$ , dann existiert ein  $a^{-1} \in K$  mit  $a \cdot a^{-1} = 1_K$ .

## Bemerkungen

- für  $0_K$  und  $1_K$  schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$  erfüllt (K1)–(K4) mit der üblichen Addition und Multiplikation
- $\mathbb{Z}$  erfüllt (K1)–(K4) und den ersten Teil von (K5)
- $\mathbb{Q}$  erfüllt (K1)–(K5) und ist ein Körper

# Beispiele: Körper

# Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 =$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0, \quad -1 =$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} =$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$
  - $1 + 1 = 0$  ist erzwungen, da sonst keine  $-1$  existieren würde

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$
  - $1 + 1 = 0$  ist erzwungen, da sonst keine  $-1$  existieren würde
  - $0 \cdot 0 = 1$  würde zu folgendem Widerspruch führen:

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$
  - $1 + 1 = 0$  ist erzwungen, da sonst keine  $-1$  existieren würde
  - $0 \cdot 0 = 1$  würde zu folgendem Widerspruch führen:

$$1 = 0 \cdot 0$$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$
  - $1 + 1 = 0$  ist erzwungen, da sonst keine  $-1$  existieren würde
  - $0 \cdot 0 = 1$  würde zu folgendem Widerspruch führen:

$$1 = 0 \cdot 0 = 0 \cdot (1 + 1)$$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$
  - $1 + 1 = 0$  ist erzwungen, da sonst keine  $-1$  existieren würde
  - $0 \cdot 0 = 1$  würde zu folgendem Widerspruch führen:

$$1 = 0 \cdot 0 = 0 \cdot (1 + 1) \stackrel{(K3)}{=} 0 \cdot 1 + 0 \cdot 1$$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$
  - $1 + 1 = 0$  ist erzwungen, da sonst keine  $-1$  existieren würde
  - $0 \cdot 0 = 1$  würde zu folgendem Widerspruch führen:

$$1 = 0 \cdot 0 = 0 \cdot (1 + 1) \stackrel{(K3)}{=} 0 \cdot 1 + 0 \cdot 1 = 0 + 0$$

## Beispiele: Körper

- neben  $\mathbb{Q}$  sind die bekannten Erweiterungen  $\mathbb{R}$  und  $\mathbb{C}$  Körper
- weitere wichtige Beispiele sind die **endlichen** Körper  $\mathbb{F}_q$  (auch  $GF(q)$ ) mit  $q$  Elementen, wobei  $q = p^n$  für eine Primzahl  $p$  und  $n \in \mathbb{N}$
- der kleinste Körper  $\mathbb{F}_2$  hat zwei Elemente 0 und 1 und ist auf der Menge  $\{0, 1\}$  mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$ ,  $-1 = 1$ , und  $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- $\mathbb{F}_2$  ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf  $1 + 1$  und  $0 \cdot 0$
  - $1 + 1 = 0$  ist erzwungen, da sonst keine  $-1$  existieren würde
  - $0 \cdot 0 = 1$  würde zu folgendem Widerspruch führen:

$$1 = 0 \cdot 0 = 0 \cdot (1 + 1) \stackrel{(K3)}{=} 0 \cdot 1 + 0 \cdot 1 = 0 + 0 = 0$$

# Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf  $\mathbb{N}$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  eine Ordnung  $\leq$  definiert.

# Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf  $\mathbb{N}$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  eine Ordnung  $\leq$  definiert.
- Dabei ist  $\leq$  sogar eine **Totalordnung** (auch **lineare**, **vollständige** oder **totale Ordnung**), d. h. zusätzlich zu den definierenden Ordnungseigenschaften

# Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf  $\mathbb{N}$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  eine Ordnung  $\leq$  definiert.
- Dabei ist  $\leq$  sogar eine **Totalordnung** (auch **lineare**, **vollständige** oder **totale Ordnung**), d. h. zusätzlich zu den definierenden Ordnungseigenschaften (reflexiv, antisymmetrisch, transitiv) gilt für je zwei Elemente  $a$  und  $b$

$$a \leq b \quad \text{oder} \quad b \leq a.$$

# Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf  $\mathbb{N}$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  eine Ordnung  $\leq$  definiert.
- Dabei ist  $\leq$  sogar eine **Totalordnung** (auch **lineare**, **vollständige** oder **totale Ordnung**), d. h. zusätzlich zu den definierenden Ordnungseigenschaften (reflexiv, antisymmetrisch, transitiv) gilt für je zwei Elemente  $a$  und  $b$

$$a \leq b \quad \text{oder} \quad b \leq a.$$

Es sind also **alle** Elemente miteinander vergleichbar (im Gegensatz zur Teilmengenrelation, die nur eine Ordnung aber **keine** Totalordnung ist)

# Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf  $\mathbb{N}$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  eine Ordnung  $\leq$  definiert.
- Dabei ist  $\leq$  sogar eine **Totalordnung** (auch **lineare**, **vollständige** oder **totale Ordnung**), d. h. zusätzlich zu den definierenden Ordnungseigenschaften (reflexiv, antisymmetrisch, transitiv) gilt für je zwei Elemente  $a$  und  $b$

$$a \leq b \quad \text{oder} \quad b \leq a.$$

Es sind also **alle** Elemente miteinander vergleichbar (im Gegensatz zur Teilmengenrelation, die nur eine Ordnung aber **keine** Totalordnung ist) und für zwei verschiedene  $a$  und  $b$  gilt **genau eine** der Beziehungen

$$a < b \quad \text{oder} \quad b < a,$$

wobei  $a < b$  durch  $a \leq b \wedge a \neq b$  definiert ist.

# Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf  $\mathbb{N}$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  eine Ordnung  $\leq$  definiert.
- Dabei ist  $\leq$  sogar eine **Totalordnung** (auch **lineare**, **vollständige** oder **totale Ordnung**), d. h. zusätzlich zu den definierenden Ordnungseigenschaften (reflexiv, antisymmetrisch, transitiv) gilt für je zwei Elemente  $a$  und  $b$

$$a \leq b \quad \text{oder} \quad b \leq a.$$

Es sind also **alle** Elemente miteinander vergleichbar (im Gegensatz zur Teilmengenrelation, die nur eine Ordnung aber **keine** Totalordnung ist) und für zwei verschiedene  $a$  und  $b$  gilt **genau eine** der Beziehungen

$$a < b \quad \text{oder} \quad b < a,$$

wobei  $a < b$  durch  $a \leq b \wedge a \neq b$  definiert ist.

- Darüber hinaus ist es praktisch, wenn die Totalordnung mit den Rechenoperationen „kompatibel“ ist und dies führt zum Begriff des **geordneten Körper**.

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden,

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1$$

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1$$

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1 \iff 1 < 0$$

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1 \iff 1 < 0$$

- (A1) und (A2) implizieren auch  $a \cdot c \geq b \cdot c$  für  $a \leq b$  und  $c \leq 0$ ,

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1 \iff 1 < 0$$

- (A1) und (A2) implizieren auch  $a \cdot c \geq b \cdot c$  für  $a \leq b$  und  $c \leq 0$ , da:

$$a \leq b$$

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1 \iff 1 < 0$$

- (A1) und (A2) implizieren auch  $a \cdot c \geq b \cdot c$  für  $a \leq b$  und  $c \leq 0$ , da:

$$a \leq b \stackrel{(A1)}{\implies} a + ((-a) + (-b)) \leq b + ((-a) + (-b))$$

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1 \iff 1 < 0$$

- (A1) und (A2) implizieren auch  $a \cdot c \geq b \cdot c$  für  $a \leq b$  und  $c \leq 0$ , da:

$$a \leq b \stackrel{(A1)}{\implies} a + ((-a) + (-b)) \leq b + ((-a) + (-b)) \implies -b \leq -a$$

# Geordnete Körper

## Definition (Angeordneter Körper)

Ein Körper  $K$  mit einer totalen Ordnung  $\leq$  auf  $K$  heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle  $a, b, c \in K$  gelten:

(A1) Falls  $a \leq b$ , dann gilt auch  $a + c \leq b + c$ .

(A2) Falls  $a \leq b$  und  $c \geq 0$ , dann gilt auch  $a \cdot c \leq b \cdot c$ .

## Bemerkungen

- $\mathbb{N}_0$ ,  $\mathbb{Z}$  und  $\mathbb{Q}$  mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$  und die Erweiterung  $\mathbb{R}$  sind angeordnete Körper
- $\mathbb{C}$  und endliche Körper können nicht angeordnet werden, z. B. für  $\mathbb{F}_2$  führt sowohl die Festlegung  $0 < 1$  als auch  $1 < 0$  wegen  $1 + 1 = 0$  zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1 \iff 1 < 0$$

- (A1) und (A2) implizieren auch  $a \cdot c \geq b \cdot c$  für  $a \leq b$  und  $c \leq 0$ , da:

$$a \leq b \stackrel{(A1)}{\implies} a + ((-a) + (-b)) \leq b + ((-a) + (-b)) \implies -b \leq -a$$

und Multiplikation mit  $-c \geq 0$  und Anwendung von (A2) ergibt  $b \cdot c \leq a \cdot c$ .

# Reelle Zahlen

- $\mathbb{Q}$  läßt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht

# Reelle Zahlen

- $\mathbb{Q}$  läßt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
- $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt

# Reelle Zahlen

- $\mathbb{Q}$  lässt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
- $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
- auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)

# Reelle Zahlen

- $\mathbb{Q}$  lässt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
- $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
- auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)
- man kann  $\mathbb{Q}$  so zur Menge  $\mathbb{R}$  der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden

# Reelle Zahlen

- $\mathbb{Q}$  lässt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
- $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
- auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)
- man kann  $\mathbb{Q}$  so zur Menge  $\mathbb{R}$  der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
  - die formale Konstruktion von  $\mathbb{R}$  aus  $\mathbb{Q}$  überspringen wir hier

# Reelle Zahlen

- $\mathbb{Q}$  lässt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
- $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
- auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)
- man kann  $\mathbb{Q}$  so zur Menge  $\mathbb{R}$  der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
  - die formale Konstruktion von  $\mathbb{R}$  aus  $\mathbb{Q}$  überspringen wir hier
  - Standardkonstruktionen basieren auf **DEDEKINDSchen Schnitten** oder auf **Äquivalenzklassen von CAUCHY-Folgen** → Analysis

# Reelle Zahlen

- $\mathbb{Q}$  lässt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
- $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
- auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)
- man kann  $\mathbb{Q}$  so zur Menge  $\mathbb{R}$  der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
  - die formale Konstruktion von  $\mathbb{R}$  aus  $\mathbb{Q}$  überspringen wir hier
  - Standardkonstruktionen basieren auf **DEDEKINDSchen Schnitten** oder auf **Äquivalenzklassen von CAUCHY-Folgen** → Analysis
  - dabei erweitert man die Addition, die Multiplikation und die totale Ordnung auf  $\mathbb{R}$  ( $a \leq b$ , wenn  $a$  links von  $b$  auf der Zahlengeraden liegt)

# Reelle Zahlen

- $\mathbb{Q}$  lässt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
  - $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
  - auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)
  - man kann  $\mathbb{Q}$  so zur Menge  $\mathbb{R}$  der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
    - die formale Konstruktion von  $\mathbb{R}$  aus  $\mathbb{Q}$  überspringen wir hier
    - Standardkonstruktionen basieren auf **DEDEKINDSchen Schnitten** oder auf **Äquivalenzklassen von CAUCHY-Folgen** → Analysis
    - dabei erweitert man die Addition, die Multiplikation und die totale Ordnung auf  $\mathbb{R}$  ( $a \leq b$ , wenn  $a$  links von  $b$  auf der Zahlengeraden liegt)
- ⇒ mit der üblichen Addition, Multiplikation und Ordnung ist die Menge der reellen Zahlen  $\mathbb{R}$  ein **angeordneter Körper**

# Reelle Zahlen

- $\mathbb{Q}$  lässt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
  - $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
  - auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)
  - man kann  $\mathbb{Q}$  so zur Menge  $\mathbb{R}$  der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
    - die formale Konstruktion von  $\mathbb{R}$  aus  $\mathbb{Q}$  überspringen wir hier
    - Standardkonstruktionen basieren auf **DEDEKINDSchen Schnitten** oder auf **Äquivalenzklassen von CAUCHY-Folgen**  $\longrightarrow$  **Analysis**
    - dabei erweitert man die Addition, die Multiplikation und die totale Ordnung auf  $\mathbb{R}$  ( $a \leq b$ , wenn  $a$  links von  $b$  auf der Zahlengeraden liegt)
- $\Rightarrow$  mit der üblichen Addition, Multiplikation und Ordnung ist die Menge der reellen Zahlen  $\mathbb{R}$  ein **angeordneter Körper**
- im Gegensatz zu  $\mathbb{Q}$  ist  $\mathbb{R}$  auch noch **vollständig** (siehe Analysis) und bis auf Isomorphie ist  $\mathbb{R}$  der einzige vollständige und angeordnete Körper

# Reelle Zahlen

- $\mathbb{Q}$  läßt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
  - $\mathbb{Q}$  ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
  - auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass  $\sqrt{2}$  keine rationale Zahl ist (aber  $\sqrt{2}$  entspricht einem Punkt auf der Zahlengeraden)
  - man kann  $\mathbb{Q}$  so zur Menge  $\mathbb{R}$  der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
    - die formale Konstruktion von  $\mathbb{R}$  aus  $\mathbb{Q}$  überspringen wir hier
    - Standardkonstruktionen basieren auf **DEDEKINDSchen Schnitten** oder auf **Äquivalenzklassen von CAUCHY-Folgen**  $\longrightarrow$  **Analysis**
    - dabei erweitert man die Addition, die Multiplikation und die totale Ordnung auf  $\mathbb{R}$  ( $a \leq b$ , wenn  $a$  links von  $b$  auf der Zahlengeraden liegt)
- $\Rightarrow$  mit der üblichen Addition, Multiplikation und Ordnung ist die Menge der reellen Zahlen  $\mathbb{R}$  ein **angeordneter Körper**
- im Gegensatz zu  $\mathbb{Q}$  ist  $\mathbb{R}$  auch noch **vollständig** (siehe Analysis) und bis auf Isomorphie ist  $\mathbb{R}$  der einzige vollständige und angeordnete Körper
  - die Zahlen in  $\mathbb{R} \setminus \mathbb{Q}$  heißen **irrationale Zahlen**, z. B.  $\sqrt{2}$ ,  $e$ ,  $\pi$

# $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} ?$

Streng genommen geht aus den vorangegangenen Definitionen von  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$  nicht hervor, dass  $\mathbb{N}$  eine Teilmenge von  $\mathbb{Z}$  oder  $\mathbb{Z}$  eine Teilmenge von  $\mathbb{Q}$  ist. Zum Beispiel wurde  $\mathbb{Z}$  als die Faktormenge einer Äquivalenzrelation auf  $\mathbb{N}_0 \times \mathbb{N}_0$  definiert und diese Faktormenge enthält formal  $\mathbb{N}$  nicht!

# $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} ?$

Streng genommen geht aus den vorangegangenen Definitionen von  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$  nicht hervor, dass  $\mathbb{N}$  eine Teilmenge von  $\mathbb{Z}$  oder  $\mathbb{Z}$  eine Teilmenge von  $\mathbb{Q}$  ist. Zum Beispiel wurde  $\mathbb{Z}$  als die Faktormenge einer Äquivalenzrelation auf  $\mathbb{N}_0 \times \mathbb{N}_0$  definiert und diese Faktormenge enthält formal  $\mathbb{N}$  nicht!

Auf der anderen Seite, haben wir eine injektive Funktion  $n \mapsto [(n, 0)]$  von  $\mathbb{N}$  in diese Faktormenge angegeben, für die sich die auf  $\mathbb{N}$  definierte Addition und Multiplikation erhält, z. B. für die Addition ergibt sich aus der Definition sofort für alle natürlichen Zahlen  $\ell$ ,  $m$  und  $n$ , dass  $\ell + m = n$  genau dann gilt, wenn  $[(\ell, 0)] +_{\mathbb{Z}} [(m, 0)] = [(n, 0)]$ . Diese Einbettung von  $\mathbb{N}$  erlaubt es  $\mathbb{N}$  als Teilmenge von  $\mathbb{Z}$  zu betrachten und wir werden von nun an  $\mathbb{N}$  immer als diese Teilmenge von  $\mathbb{Z}$  ansehen.

# $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} ?$

Streng genommen geht aus den vorangegangenen Definitionen von  $\mathbb{Z}$ ,  $\mathbb{Q}$  und  $\mathbb{R}$  nicht hervor, dass  $\mathbb{N}$  eine Teilmenge von  $\mathbb{Z}$  oder  $\mathbb{Z}$  eine Teilmenge von  $\mathbb{Q}$  ist. Zum Beispiel wurde  $\mathbb{Z}$  als die Faktormenge einer Äquivalenzrelation auf  $\mathbb{N}_0 \times \mathbb{N}_0$  definiert und diese Faktormenge enthält formal  $\mathbb{N}$  nicht!

Auf der anderen Seite, haben wir eine injektive Funktion  $n \mapsto [(n, 0)]$  von  $\mathbb{N}$  in diese Faktormenge angegeben, für die sich die auf  $\mathbb{N}$  definierte Addition und Multiplikation erhält, z. B. für die Addition ergibt sich aus der Definition sofort für alle natürlichen Zahlen  $\ell$ ,  $m$  und  $n$ , dass  $\ell + m = n$  genau dann gilt, wenn  $[(\ell, 0)] +_{\mathbb{Z}} [(m, 0)] = [(n, 0)]$ . Diese Einbettung von  $\mathbb{N}$  erlaubt es  $\mathbb{N}$  als Teilmenge von  $\mathbb{Z}$  zu betrachten und wir werden von nun an  $\mathbb{N}$  immer als diese Teilmenge von  $\mathbb{Z}$  ansehen.

Genauso kann mit Hilfe der Funktion  $z \mapsto [(z, 1)]$  die Menge der ganzen Zahlen in  $\mathbb{Q}$  eingebettet werden, welche wiederum durch  $q \mapsto [(q)_{n \in \mathbb{N}}]$  als eine Teilmenge von  $\mathbb{R}$  aufgefasst werden kann. Von nun an werden wir auf Grund dieser Einbettungen sowohl die rationalen, als auch die ganzen und die natürlichen Zahlen als durch  $\leq$  vollständig geordnete Teilmengen der reellen Zahlen betrachten und die Addition und Multiplikation einfach mit  $+$  und  $\cdot$  bezeichnen. Insbesondere gilt also

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

# Mächtigkeiten von Mengen

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig** : $\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig** : $\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig**  $:\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig** : $\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig**  $:\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.  $M$  hat genau  $n$  Elemente ( $M$  ist  **$n$ -elementig**,  $M$  ist eine  **$n$ -Menge**) und wir schreiben
$$|M| := n.$$

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig**  $:\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.  $M$  hat genau  $n$  Elemente ( $M$  ist  **$n$ -elementig**,  $M$  ist eine  **$n$ -Menge**) und wir schreiben
$$|M| := n.$$
- **unendlich**: falls  $M$  **nicht** endlich ist.

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig**  $:\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.  $M$  hat genau  $n$  Elemente ( $M$  ist  **$n$ -elementig**,  $M$  ist eine  **$n$ -Menge**) und wir schreiben

$$|M| := n.$$

- **unendlich**: falls  $M$  **nicht** endlich ist.
- **abzählbar**: falls  $M$  endlich ist **oder** gleichmächtig mit  $\mathbb{N}$  ist.

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig** : $\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.  $M$  hat genau  $n$  Elemente ( $M$  ist  **$n$ -elementig**,  $M$  ist eine  **$n$ -Menge**) und wir schreiben

$$|M| := n.$$

- **unendlich**: falls  $M$  **nicht** endlich ist.
- **abzählbar**: falls  $M$  endlich ist **oder** gleichmächtig mit  $\mathbb{N}$  ist.
- **überabzählbar**: falls  $M$  **nicht** abzählbar ist.

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig** : $\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.  $M$  hat genau  $n$  Elemente ( $M$  ist  **$n$ -elementig**,  $M$  ist eine  **$n$ -Menge**) und wir schreiben

$$|M| := n.$$

- **unendlich**: falls  $M$  **nicht** endlich ist.
- **abzählbar**: falls  $M$  endlich ist **oder** gleichmächtig mit  $\mathbb{N}$  ist.
- **überabzählbar**: falls  $M$  **nicht** abzählbar ist.

## Bemerkungen

- $M \neq \emptyset$  ist abzählbar genau dann, wenn es eine surjektive Abbildung  $f: \mathbb{N} \rightarrow M$  gibt und  $f$  heißt **Aufzählung** von  $M$

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig** : $\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.  $M$  hat genau  $n$  Elemente ( $M$  ist  **$n$ -elementig**,  $M$  ist eine  **$n$ -Menge**) und wir schreiben
$$|M| := n.$$
- **unendlich**: falls  $M$  **nicht** endlich ist.
- **abzählbar**: falls  $M$  endlich ist **oder** gleichmächtig mit  $\mathbb{N}$  ist.
- **überabzählbar**: falls  $M$  **nicht** abzählbar ist.

## Bemerkungen

- $M \neq \emptyset$  ist abzählbar genau dann, wenn es eine surjektive Abbildung  $f: \mathbb{N} \rightarrow M$  gibt und  $f$  heißt **Aufzählung** von  $M$
- $n \mapsto n - 1$  zeigt  $\mathbb{N}_0$  ist abzählbar

# Mächtigkeiten von Mengen

- Mengen  $A$  und  $B$  sind **gleichmächtig**  $:\Leftrightarrow$  es gibt Bijektion zwischen  $A$  und  $B$
- für  $n \in \mathbb{N}_0$  schreiben wir  $[n]$  als Kurzform für die Menge  $\{1, \dots, n\}$

## Definition

Eine Menge  $M$  heißt:

- **endlich**: falls  $M$  gleichmächtig zu  $[n]$  für ein  $n \in \mathbb{N}_0$ , d. h.  $M$  hat genau  $n$  Elemente ( $M$  ist  **$n$ -elementig**,  $M$  ist eine  **$n$ -Menge**) und wir schreiben
$$|M| := n.$$
- **unendlich**: falls  $M$  **nicht** endlich ist.
- **abzählbar**: falls  $M$  endlich ist **oder** gleichmächtig mit  $\mathbb{N}$  ist.
- **überabzählbar**: falls  $M$  **nicht** abzählbar ist.

## Bemerkungen

- $M \neq \emptyset$  ist abzählbar genau dann, wenn es eine surjektive Abbildung  $f: \mathbb{N} \rightarrow M$  gibt und  $f$  heißt **Aufzählung** von  $M$
- $n \mapsto n - 1$  zeigt  $\mathbb{N}_0$  ist abzählbar
- $n \mapsto (-1)^n \lfloor n/2 \rfloor$  zeigt  $\mathbb{Z}$  ist abzählbar, wobei für  $x \in \mathbb{R}$  mit  $\lfloor x \rfloor$  die größte ganze Zahl  $\leq x$  bezeichnet wird

# Mächtigkeit von $\mathbb{Q}$

# Mächtigkeit von $\mathbb{Q}$

## Satz

Die Menge der rationalen Zahlen  $\mathbb{Q}$  ist abzählbar.

# Mächtigkeit von $\mathbb{Q}$

## Satz

Die Menge der rationalen Zahlen  $\mathbb{Q}$  ist abzählbar.

## Beweis

Wir geben eine Aufzählung  $q_1, q_2, \dots$  der Menge der rationalen Zahlen  $> 0$  an.

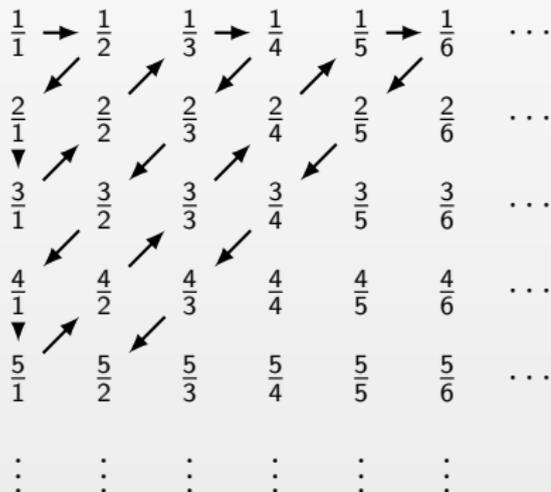
# Mächtigkeit von $\mathbb{Q}$

## Satz

Die Menge der rationalen Zahlen  $\mathbb{Q}$  ist abzählbar.

## Beweis

Wir geben eine Aufzählung  $q_1, q_2, \dots$  der Menge der rationalen Zahlen  $> 0$  an. Man erhält die Aufzählung, indem man im folgenden Bild bei den Bruch  $\frac{1}{1}$  beginnt und den Pfeilen folgt:



### Satz

Die Menge der rationalen Zahlen  $\mathbb{Q}$  ist abzählbar.

Die Aufzählung lautet also

$$q_1 = \frac{1}{1}, \quad q_2 = \frac{1}{2}, \quad q_3 = \frac{2}{1}, \quad q_4 = \frac{3}{1}, \quad q_5 = \frac{2}{2}, \dots$$

## Satz

Die Menge der rationalen Zahlen  $\mathbb{Q}$  ist abzählbar.

Die Aufzählung lautet also

$$q_1 = \frac{1}{1}, \quad q_2 = \frac{1}{2}, \quad q_3 = \frac{2}{1}, \quad q_4 = \frac{3}{1}, \quad q_5 = \frac{2}{2}, \dots$$

Die Tatsache, dass viele rationale Zahlen hierbei doppelt auftreten, zum Beispiel 1 als  $\frac{1}{1}$  und  $\frac{2}{2}$  spielt keine Rolle, da eine Aufzählung nicht injektiv sein muss.

## Satz

Die Menge der rationalen Zahlen  $\mathbb{Q}$  ist abzählbar.

Die Aufzählung lautet also

$$q_1 = \frac{1}{1}, \quad q_2 = \frac{1}{2}, \quad q_3 = \frac{2}{1}, \quad q_4 = \frac{3}{1}, \quad q_5 = \frac{2}{2}, \dots$$

Die Tatsache, dass viele rationale Zahlen hierbei doppelt auftreten, zum Beispiel 1 als  $\frac{1}{1}$  und  $\frac{2}{2}$  spielt keine Rolle, da eine Aufzählung nicht injektiv sein muss. Es ist aber klar, dass jede rationale Zahl  $> 0$  in dieser Aufzählung irgendwann einmal auftritt.

## Satz

Die Menge der rationalen Zahlen  $\mathbb{Q}$  ist abzählbar.

Die Aufzählung lautet also

$$q_1 = \frac{1}{1}, \quad q_2 = \frac{1}{2}, \quad q_3 = \frac{2}{1}, \quad q_4 = \frac{3}{1}, \quad q_5 = \frac{2}{2}, \dots$$

Die Tatsache, dass viele rationale Zahlen hierbei doppelt auftreten, zum Beispiel 1 als  $\frac{1}{1}$  und  $\frac{2}{2}$  spielt keine Rolle, da eine Aufzählung nicht injektiv sein muss. Es ist aber klar, dass jede rationale Zahl  $> 0$  in dieser Aufzählung irgendwann einmal auftritt.

Mit dieser Aufzählung der rationalen Zahlen  $> 0$  können wir nun aber leicht eine Aufzählung aller rationalen Zahlen angeben:

$$0, q_1, -q_1, q_2, -q_2, \dots$$

leistet das Gewünschte. □

# Mächtigkeit von $\mathbb{R}$

Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis. Angenommen, es gibt eine Aufzählung  $s_1, s_2, s_3, \dots$  der reellen Zahlen  $s$  mit  $0 < s < 1$ . Die Zahlen  $s_n$ ,  $n \in \mathbb{N}$  lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben.

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung  $s_1, s_2, s_3, \dots$  der reellen Zahlen  $s$  mit  $0 < s < 1$ . Die Zahlen  $s_n$ ,  $n \in \mathbb{N}$  lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle  $i, j \in \mathbb{N}$  sei  $s_{ij}$  die Ziffer, die in der  $j$ -ten Nachkommastelle der Dezimaldarstellung von  $s_i$  steht:

$$s_1 = 0.s_{11}s_{12}s_{13} \dots$$

$$s_2 = 0.s_{21}s_{22}s_{23} \dots$$

$$\vdots \qquad \qquad \qquad \vdots$$

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung  $s_1, s_2, s_3, \dots$  der reellen Zahlen  $s$  mit  $0 < s < 1$ . Die Zahlen  $s_n$ ,  $n \in \mathbb{N}$  lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle  $i, j \in \mathbb{N}$  sei  $s_{ij}$  die Ziffer, die in der  $j$ -ten Nachkommastelle der Dezimaldarstellung von  $s_i$  steht:

$$\begin{aligned} s_1 &= 0.s_{11}s_{12}s_{13} \dots \\ s_2 &= 0.s_{21}s_{22}s_{23} \dots \\ &\vdots \qquad \qquad \qquad \vdots \end{aligned}$$

Nun definieren wir eine weitere reelle Zahl  $a$ , die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt.

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung  $s_1, s_2, s_3, \dots$  der reellen Zahlen  $s$  mit  $0 < s < 1$ . Die Zahlen  $s_n$ ,  $n \in \mathbb{N}$  lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle  $i, j \in \mathbb{N}$  sei  $s_{ij}$  die Ziffer, die in der  $j$ -ten Nachkommastelle der Dezimaldarstellung von  $s_i$  steht:

$$s_1 = 0.s_{11}s_{12}s_{13} \dots$$

$$s_2 = 0.s_{21}s_{22}s_{23} \dots$$

$$\vdots \qquad \qquad \qquad \vdots$$

Nun definieren wir eine weitere reelle Zahl  $a$ , die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt. Wir geben die Nachkommastellen  $a_1a_2a_3 \dots$  der Zahl  $a$  an.

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung  $s_1, s_2, s_3, \dots$  der reellen Zahlen  $s$  mit  $0 < s < 1$ . Die Zahlen  $s_n$ ,  $n \in \mathbb{N}$  lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle  $i, j \in \mathbb{N}$  sei  $s_{ij}$  die Ziffer, die in der  $j$ -ten Nachkommastelle der Dezimaldarstellung von  $s_i$  steht:

$$\begin{aligned} s_1 &= 0.s_{11}s_{12}s_{13} \dots \\ s_2 &= 0.s_{21}s_{22}s_{23} \dots \\ &\vdots \qquad \qquad \qquad \vdots \end{aligned}$$

Nun definieren wir eine weitere reelle Zahl  $a$ , die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt. Wir geben die Nachkommastellen  $a_1a_2a_3 \dots$  der Zahl  $a$  an. Für  $i \in \mathbb{N}$  sei

$$a_i := \begin{cases} 4, & \text{falls } s_{ii} \neq 4 \text{ ist und} \\ 5, & \text{sonst.} \end{cases}$$

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung  $s_1, s_2, s_3, \dots$  der reellen Zahlen  $s$  mit  $0 < s < 1$ . Die Zahlen  $s_n$ ,  $n \in \mathbb{N}$  lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle  $i, j \in \mathbb{N}$  sei  $s_{ij}$  die Ziffer, die in der  $j$ -ten Nachkommastelle der Dezimaldarstellung von  $s_i$  steht:

$$\begin{aligned} s_1 &= 0.s_{11}s_{12}s_{13} \dots \\ s_2 &= 0.s_{21}s_{22}s_{23} \dots \\ &\vdots \qquad \qquad \qquad \vdots \end{aligned}$$

Nun definieren wir eine weitere reelle Zahl  $a$ , die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt. Wir geben die Nachkommastellen  $a_1a_2a_3 \dots$  der Zahl  $a$  an. Für  $i \in \mathbb{N}$  sei

$$a_i := \begin{cases} 4, & \text{falls } s_{ii} \neq 4 \text{ ist und} \\ 5, & \text{sonst.} \end{cases}$$

Es ist klar, dass  $a = 0.a_1a_2a_3 \dots$  echt zwischen 0 und 1 liegt.

# Mächtigkeit von $\mathbb{R}$

## Satz (CANTOR 1874)

Die Menge der reellen Zahlen  $\mathbb{R}$  ist überabzählbar.

**Beweis:** Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung  $s_1, s_2, s_3, \dots$  der reellen Zahlen  $s$  mit  $0 < s < 1$ . Die Zahlen  $s_n$ ,  $n \in \mathbb{N}$  lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle  $i, j \in \mathbb{N}$  sei  $s_{ij}$  die Ziffer, die in der  $j$ -ten Nachkommastelle der Dezimaldarstellung von  $s_i$  steht:

$$s_1 = 0.s_{11}s_{12}s_{13} \dots$$

$$s_2 = 0.s_{21}s_{22}s_{23} \dots$$

$$\vdots \qquad \qquad \qquad \vdots$$

Nun definieren wir eine weitere reelle Zahl  $a$ , die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt. Wir geben die Nachkommastellen  $a_1a_2a_3 \dots$  der Zahl  $a$  an. Für  $i \in \mathbb{N}$  sei

$$a_i := \begin{cases} 4, & \text{falls } s_{ii} \neq 4 \text{ ist und} \\ 5, & \text{sonst.} \end{cases}$$

Es ist klar, dass  $a = 0.a_1a_2a_3 \dots$  echt zwischen 0 und 1 liegt. Die Zahl  $a$  ist so gewählt, dass es sich an der  $i$ -ten Nachkommastelle von  $s_i$  unterscheidet. Damit ist  $a$  von allen  $s_i$ ,  $i \in \mathbb{N}$  verschieden. □



## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  ist und schreiben  $x \mid y$ .

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  ist und schreiben  $x \mid y$ .
- Falls  $x$  kein Teiler von  $y$  ist, dann schreiben wir  $x \nmid y$ .

# Teilbarkeit

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  ist und schreiben  $x \mid y$ .
- Falls  $x$  kein Teiler von  $y$  ist, dann schreiben wir  $x \nmid y$ .

## Bemerkungen

- jede ganze Zahl  $x \in \mathbb{Z}$  teilt also die 0

$$0 = 0 \cdot x$$

# Teilbarkeit

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  ist und schreiben  $x \mid y$ .
- Falls  $x$  kein Teiler von  $y$  ist, dann schreiben wir  $x \nmid y$ .

## Bemerkungen

- jede ganze Zahl  $x \in \mathbb{Z}$  teilt also die 0
- 0 ist nur Teiler von der 0

$$0 = 0 \cdot x$$

# Teilbarkeit

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  ist und schreiben  $x \mid y$ .
- Falls  $x$  kein Teiler von  $y$  ist, dann schreiben wir  $x \nmid y$ .

## Bemerkungen

- jede ganze Zahl  $x \in \mathbb{Z}$  teilt also die 0
- 0 ist nur Teiler von der 0
- es gilt für alle  $x, y \in \mathbb{Z}$

$$0 = 0 \cdot x$$

$$x \mid y \iff -x \mid y$$

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  und schreiben  $x \mid y$ .
- Falls  $x$  kein Teiler von  $y$  ist, dann schreiben wir  $x \nmid y$ .

## Bemerkungen

- jede ganze Zahl  $x \in \mathbb{Z}$  teilt also die 0
- 0 ist nur Teiler von der 0
- es gilt für alle  $x, y \in \mathbb{Z}$

$$0 = 0 \cdot x$$

$$x \mid y \iff -x \mid y \iff x \mid -y$$

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  ist und schreiben  $x \mid y$ .
- Falls  $x$  kein Teiler von  $y$  ist, dann schreiben wir  $x \nmid y$ .

## Bemerkungen

- jede ganze Zahl  $x \in \mathbb{Z}$  teilt also die 0  $0 = 0 \cdot x$
- 0 ist nur Teiler von der 0
- es gilt für alle  $x, y \in \mathbb{Z}$

$$x \mid y \iff -x \mid y \iff x \mid -y \iff -x \mid -y$$

# Teilbarkeit

## Definition (Teiler)

Eine ganze Zahl  $x \in \mathbb{Z}$  ist ein **Teiler** von  $y \in \mathbb{Z}$ , falls ein  $d \in \mathbb{Z}$  existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch,  $y$  ist ein **Vielfaches** von  $x$  ist und schreiben  $x \mid y$ .
- Falls  $x$  kein Teiler von  $y$  ist, dann schreiben wir  $x \nmid y$ .

## Bemerkungen

- jede ganze Zahl  $x \in \mathbb{Z}$  teilt also die 0  $0 = 0 \cdot x$
- 0 ist nur Teiler von der 0
- es gilt für alle  $x, y \in \mathbb{Z}$

$$x \mid y \iff -x \mid y \iff x \mid -y \iff -x \mid -y$$

- Teilbarkeiten in  $\mathbb{Z}$  lassen sich also auf Teilbarkeiten in  $\mathbb{N}_0$  zurückführen

## Satz

Teilbarkeitsbeziehung | definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

## Satz

Teilbarkeitsbeziehung | definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- reflexiv,

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- reflexiv, da  $x | x$

## Satz

Teilbarkeitsbeziehung | definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- reflexiv, da  $x \mid x$
- transitiv,

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- **reflexiv**, da  $x | x$
- **transitiv**, da  $x | y$  und  $y | z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- **reflexiv**, da  $x | x$
- **transitiv**, da  $x | y$  und  $y | z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x$

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- **reflexiv**, da  $x | x$
- **transitiv**, da  $x | y$  und  $y | z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x | z$

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- reflexiv, da  $x | x$
- transitiv, da  $x | y$  und  $y | z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x | z$
- antisymmetrisch auf  $\mathbb{N}_0$  (aber **nicht** auf  $\mathbb{Z}$ ),

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- **reflexiv**, da  $x | x$
- **transitiv**, da  $x | y$  und  $y | z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x | z$
- **antisymmetrisch auf  $\mathbb{N}_0$**  (aber **nicht** auf  $\mathbb{Z}$ ), da  $x | y$  und  $y | x$  bedeutet  $y = d_1 \cdot x$  und  $x = d_2 \cdot y$  für geeignete  $d_1$  und  $d_2$

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- **reflexiv**, da  $x | x$
- **transitiv**, da  $x | y$  und  $y | z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x | z$
- **antisymmetrisch auf  $\mathbb{N}_0$**  (aber **nicht** auf  $\mathbb{Z}$ ), da  $x | y$  und  $y | x$  bedeutet  $y = d_1 \cdot x$  und  $x = d_2 \cdot y$  für geeignete  $d_1$  und  $d_2$   
 $\implies y = d_1 \cdot d_2 \cdot y$  und  $x = d_1 \cdot d_2 \cdot x$

## Satz

Teilbarkeitsbeziehung  $|$  definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- **reflexiv**, da  $x | x$
- **transitiv**, da  $x | y$  und  $y | z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x | z$
- **antisymmetrisch auf  $\mathbb{N}_0$**  (aber **nicht** auf  $\mathbb{Z}$ ), da  $x | y$  und  $y | x$  bedeutet  $y = d_1 \cdot x$  und  $x = d_2 \cdot y$  für geeignete  $d_1$  und  $d_2$   
 $\implies y = d_1 \cdot d_2 \cdot x$  und  $x = d_1 \cdot d_2 \cdot x \implies d_1 \cdot d_2 = 1$  oder  $y = x = 0$

## Satz

Teilbarkeitsbeziehung | definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- **reflexiv**, da  $x \mid x$
- **transitiv**, da  $x \mid y$  und  $y \mid z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x \mid z$
- **antisymmetrisch auf  $\mathbb{N}_0$**  (aber **nicht** auf  $\mathbb{Z}$ ), da  $x \mid y$  und  $y \mid x$  bedeutet  $y = d_1 \cdot x$  und  $x = d_2 \cdot y$  für geeignete  $d_1$  und  $d_2$   
 $\implies y = d_1 \cdot d_2 \cdot y$  und  $x = d_1 \cdot d_2 \cdot x \implies d_1 \cdot d_2 = 1$  oder  $y = x = 0$

Des Weiteren gilt:

- $x_1 \mid y_1$  und  $x_2 \mid y_2 \implies (x_1 \cdot x_2) \mid (y_1 \cdot y_2)$

## Satz

Teilbarkeitsbeziehung | definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- reflexiv, da  $x \mid x$
- transitiv, da  $x \mid y$  und  $y \mid z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x \mid z$
- antisymmetrisch auf  $\mathbb{N}_0$  (aber **nicht** auf  $\mathbb{Z}$ ), da  $x \mid y$  und  $y \mid x$  bedeutet  $y = d_1 \cdot x$  und  $x = d_2 \cdot y$  für geeignete  $d_1$  und  $d_2$   
 $\implies y = d_1 \cdot d_2 \cdot x$  und  $x = d_1 \cdot d_2 \cdot x \implies d_1 \cdot d_2 = 1$  oder  $y = x = 0$

Des Weiteren gilt:

- $x_1 \mid y_1$  und  $x_2 \mid y_2 \implies (x_1 \cdot x_2) \mid (y_1 \cdot y_2)$
- $(x \cdot y_1) \mid (x \cdot y_2)$  und  $x \neq 0 \implies y_1 \mid y_2$

## Satz

Teilbarkeitsbeziehung | definiert eine Relation auf  $\mathbb{Z}$  (bzw. auf  $\mathbb{N}_0$ ) mit folgenden Eigenschaften:

- reflexiv, da  $x \mid x$
- transitiv, da  $x \mid y$  und  $y \mid z$  bedeutet, dass es  $d_1, d_2$  mit  $y = d_1 \cdot x$  und  $z = d_2 \cdot y$  gibt  $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x \mid z$
- antisymmetrisch auf  $\mathbb{N}_0$  (aber **nicht** auf  $\mathbb{Z}$ ), da  $x \mid y$  und  $y \mid x$  bedeutet  $y = d_1 \cdot x$  und  $x = d_2 \cdot y$  für geeignete  $d_1$  und  $d_2$   
 $\implies y = d_1 \cdot d_2 \cdot y$  und  $x = d_1 \cdot d_2 \cdot x \implies d_1 \cdot d_2 = 1$  oder  $y = x = 0$

Des Weiteren gilt:

- $x_1 \mid y_1$  und  $x_2 \mid y_2 \implies (x_1 \cdot x_2) \mid (y_1 \cdot y_2)$
- $(x \cdot y_1) \mid (x \cdot y_2)$  und  $x \neq 0 \implies y_1 \mid y_2$
- $x \mid y_1$  und  $x \mid y_2 \implies x \mid (y_1 \cdot z_1 + y_2 \cdot z_2)$  für alle  $z_1, z_2$ .

### Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

## Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

### Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) =$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) =$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 =$

# Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 =$

# Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

■  $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) =$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) = 6$  und  $\text{kgV}(24, 18) =$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) = 6$  und  $\text{kgV}(24, 18) = 72$  und  $6 \cdot 72 =$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) = 6$  und  $\text{kgV}(24, 18) = 72$  und  $6 \cdot 72 = 432 =$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) = 6$  und  $\text{kgV}(24, 18) = 72$  und  $6 \cdot 72 = 432 = 24 \cdot 18$

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) = 6$  und  $\text{kgV}(24, 18) = 72$  und  $6 \cdot 72 = 432 = 24 \cdot 18$
- Allgemein gilt tatsächlich (Beweis folgt später):

## Definition (ggT und kgV)

Für ganze Zahlen  $x, y \in \mathbb{Z}$  ist der **größte gemeinsame Teiler** ( $\text{ggT}(x, y)$ ) von  $x$  und  $y$  ist die größte natürliche Zahl  $n \in \mathbb{N}$ , die sowohl  $x$  als auch  $y$  teilt, wobei man für  $x = y = 0$  üblicherweise  $\text{ggT}(0, 0) := 0$  setzt.

Das **kleinste gemeinsame Vielfache** ( $\text{kgV}(x, y)$ ) von  $x$  und  $y$  ist die kleinste natürliche Zahl  $n > 0$ , die sowohl von  $x$  als auch von  $y$  geteilt wird, wobei man für  $x = 0$  oder  $y = 0$  üblicherweise  $\text{kgV}(x, y) := 0$  setzt.

## Beispiele

- $\text{ggT}(18, 45) = 9$  und  $\text{kgV}(18, 45) = 90$  und  $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) = 6$  und  $\text{kgV}(24, 18) = 72$  und  $6 \cdot 72 = 432 = 24 \cdot 18$
- Allgemein gilt tatsächlich (Beweis folgt später):

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|,$$

wobei  $|z|$  der **Absolutbetrag** einer ganzen Zahl  $z \in \mathbb{Z}$  ist.

# Berechnung des ggT

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z}$

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ .

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ . Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y$$

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ . Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y \implies \text{ggT}(x, y) \leq \text{ggT}(x - y, y).$$

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ . Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y \implies \text{ggT}(x, y) \leq \text{ggT}(x - y, y).$$

Auf der anderen Seite teilt auch jeder Teiler von  $x - y$  und  $y$  auch  $x - y + y = x$

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ . Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y \implies \text{ggT}(x, y) \leq \text{ggT}(x - y, y).$$

Auf der anderen Seite teilt auch jeder Teiler von  $x - y$  und  $y$  auch  $x - y + y = x$  und somit gilt auch

$$\text{ggT}(x - y, y) \mid x \quad \text{und} \quad \text{ggT}(x - y, y) \mid y$$

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ . Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y \implies \text{ggT}(x, y) \leq \text{ggT}(x - y, y).$$

Auf der anderen Seite teilt auch jeder Teiler von  $x - y$  und  $y$  auch  $x - y + y = x$  und somit gilt auch

$$\text{ggT}(x - y, y) \mid x \quad \text{und} \quad \text{ggT}(x - y, y) \mid y \implies \text{ggT}(x - y, y) \leq \text{ggT}(x, y).$$

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ . Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y \implies \text{ggT}(x, y) \leq \text{ggT}(x - y, y).$$

Auf der anderen Seite teilt auch jeder Teiler von  $x - y$  und  $y$  auch  $x - y + y = x$  und somit gilt auch

$$\text{ggT}(x - y, y) \mid x \quad \text{und} \quad \text{ggT}(x - y, y) \mid y \implies \text{ggT}(x - y, y) \leq \text{ggT}(x, y).$$

Also muss gelten  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$  □

# Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$  für alle  $x, y \in \mathbb{Z} \implies$  o. B. d. A. seien  $x, y \in \mathbb{N}_0$

## Proposition

Für alle  $x, y \in \mathbb{N}_0$  mit  $x \geq y$  gilt  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ .

## Beweis

Jeder Teiler von  $x$  und  $y$  teilt auch  $x - y$ . Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y \implies \text{ggT}(x, y) \leq \text{ggT}(x - y, y).$$

Auf der anderen Seite teilt auch jeder Teiler von  $x - y$  und  $y$  auch  $x - y + y = x$  und somit gilt auch

$$\text{ggT}(x - y, y) \mid x \quad \text{und} \quad \text{ggT}(x - y, y) \mid y \implies \text{ggT}(x - y, y) \leq \text{ggT}(x, y).$$

Also muss gelten  $\text{ggT}(x, y) = \text{ggT}(x - y, y)$  □

- Proposition liefert rekursiven Algorithmus für die Berechnung des ggT

# Einfacher EUKLIDischer Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):
  - Induktion über  $n =$

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):
  - Induktion über  $n = |x| + |y|$  mit mehreren Vorgängern

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):
  - Induktion über  $n = |x| + |y|$  mit mehreren Vorgängern
  - Induktionsanfang  $x = 0$  oder  $y = 0$  klar wegen der Definition des  $\text{ggT}$

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):
  - Induktion über  $n = |x| + |y|$  mit mehreren Vorgängern
  - Induktionsanfang  $x = 0$  oder  $y = 0$  klar wegen der Definition des  $\text{ggT}$
  - Induktionsschritt für  $|x| > 0$  und  $|y| > 0$  durch Proposition

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):
  - Induktion über  $n = |x| + |y|$  mit mehreren Vorgängern
  - Induktionsanfang  $x = 0$  oder  $y = 0$  klar wegen der Definition des  $\text{ggT}$
  - Induktionsschritt für  $|x| > 0$  und  $|y| > 0$  durch Proposition
- **Problem:** langsamer Algorithmus

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):
  - Induktion über  $n = |x| + |y|$  mit mehreren Vorgängern
  - Induktionsanfang  $x = 0$  oder  $y = 0$  klar wegen der Definition des  $\text{ggT}$
  - Induktionsschritt für  $|x| > 0$  und  $|y| > 0$  durch Proposition
- **Problem:** langsamer Algorithmus – Laufzeit  $O(|x| + |y|)$

# Einfacher EUKLIDISCHER Algorithmus

## Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

## Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$  (Korrektheit):
  - Induktion über  $n = |x| + |y|$  mit mehreren Vorgängern
  - Induktionsanfang  $x = 0$  oder  $y = 0$  klar wegen der Definition des  $\text{ggT}$
  - Induktionsschritt für  $|x| > 0$  und  $|y| > 0$  durch Proposition
- **Problem:** langsamer Algorithmus – Laufzeit  $O(|x| + |y|)$  **keine** polynomielle Laufzeit in der Länge der Eingabe  $\log |x| + \log |y|$

# Warum ist der einfache Algorithmus schlecht?

# Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse

# Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn  $x$  sehr groß und  $y$  sehr klein ist, dann wird sehr oft  $y$  von  $x$  abgezogen

# Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn  $x$  sehr groß und  $y$  sehr klein ist, dann wird sehr oft  $y$  von  $x$  abgezogen
- z. B.  $x = 2^{51}$  und  $y = 2$  resultiert in  $2^{50} \sim 10^{15}$  Subtraktionen für die mein Rechner mehr als **8 Tage** braucht

## Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn  $x$  sehr groß und  $y$  sehr klein ist, dann wird sehr oft  $y$  von  $x$  abgezogen
- z. B.  $x = 2^{51}$  und  $y = 2$  resultiert in  $2^{50} \sim 10^{15}$  Subtraktionen für die mein Rechner mehr als **8 Tage** braucht
- für  $x = 2^{61}$  und  $y = 2$  braucht der Algorithmus dann  $\sim 1000$ -mal so lange, obwohl die Eingabe nur 10 Bit länger geworden ist

# Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn  $x$  sehr groß und  $y$  sehr klein ist, dann wird sehr oft  $y$  von  $x$  abgezogen
- z. B.  $x = 2^{51}$  und  $y = 2$  resultiert in  $2^{50} \sim 10^{15}$  Subtraktionen für die mein Rechner mehr als **8 Tage** braucht
- für  $x = 2^{61}$  und  $y = 2$  braucht der Algorithmus dann  $\sim 1000$ -mal so lange, obwohl die Eingabe nur 10 Bit länger geworden ist  
→ exponentielle Laufzeit

# Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn  $x$  sehr groß und  $y$  sehr klein ist, dann wird sehr oft  $y$  von  $x$  abgezogen
- z. B.  $x = 2^{51}$  und  $y = 2$  resultiert in  $2^{50} \sim 10^{15}$  Subtraktionen für die mein Rechner mehr als **8 Tage** braucht
- für  $x = 2^{61}$  und  $y = 2$  braucht der Algorithmus dann  $\sim 1000$ -mal so lange, obwohl die Eingabe nur 10 Bit länger geworden ist  
→ exponentielle Laufzeit

## Beobachtung

- beim einfachen EUKLIDISCHEN Algorithmus ziehen wir  $y$  solange ab, bis  $z = x - y < y$  erreicht ist

# Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn  $x$  sehr groß und  $y$  sehr klein ist, dann wird sehr oft  $y$  von  $x$  abgezogen
- z. B.  $x = 2^{51}$  und  $y = 2$  resultiert in  $2^{50} \sim 10^{15}$  Subtraktionen für die mein Rechner mehr als **8 Tage** braucht
- für  $x = 2^{61}$  und  $y = 2$  braucht der Algorithmus dann  $\sim 1000$ -mal so lange, obwohl die Eingabe nur 10 Bit länger geworden ist  
→ exponentielle Laufzeit

## Beobachtung

- beim einfachen EUKLIDISCHEN Algorithmus ziehen wir  $y$  solange ab, bis  $z = x - y < y$  erreicht ist
- ⇒ **Division mit Rest** von  $x$  und  $y$  liefert uns dieses  $z$  in einem Schritt

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- $\text{div}: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- $\text{div}: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- $\text{mod}: \mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- $\text{div}: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- $\text{mod}: \mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- $\text{div}: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- $\text{mod}: \mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz:** Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- **div**:  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- **mod**:  $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz**: Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$  ist ein Vielfaches von  $y$ .

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- **div**:  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- **mod**:  $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz**: Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ .

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- **div**:  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- **mod**:  $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz**: Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ . ✓

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- **div**:  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- **mod**:  $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz**: Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ . ✓

- **Eindeutigkeit**: Falls  $qy + r = x = q'y + r'$  wie in (\*),

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- **div**:  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- **mod**:  $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz**: Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ . ✓

- **Eindeutigkeit**: Falls  $qy + r = x = q'y + r'$  wie in (\*), dann gilt  $0 = (q - q')y + (r - r')$  mit  $|r - r'| < |y|$ .

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- $\text{div}: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- $\text{mod}: \mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz:** Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ . ✓

- **Eindeutigkeit:** Falls  $qy + r = x = q'y + r'$  wie in (\*), dann gilt

$$0 = (q - q')y + (r - r') \quad \text{mit} \quad |r - r'| < |y|.$$

$\implies y \mid (r - r')$ , da  $y \mid 0$  und  $y \mid (q - q')y$

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- **div**:  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- **mod**:  $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz**: Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ . ✓

- **Eindeutigkeit**: Falls  $qy + r = x = q'y + r'$  wie in (\*), dann gilt

$$0 = (q - q')y + (r - r') \quad \text{mit} \quad |r - r'| < |y|.$$

$\implies y \mid (r - r')$ , da  $y \mid 0$  und  $y \mid (q - q')y$

$\implies$  wegen  $|r - r'| < |y|$  folgt dann  $r = r'$

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- $\text{div}: \mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- $\text{mod}: \mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz:** Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ . ✓

- **Eindeutigkeit:** Falls  $qy + r = x = q'y + r'$  wie in (\*), dann gilt

$$0 = (q - q')y + (r - r') \quad \text{mit} \quad |r - r'| < |y|.$$

$\implies y \mid (r - r')$ , da  $y \mid 0$  und  $y \mid (q - q')y$

$\implies$  wegen  $|r - r'| < |y|$  folgt dann  $r = r'$

$\implies qy = q'y$  und wegen  $y \neq 0$  folgt  $q = q'$

# Division mit Rest

## Definition und Satz

Für je zwei ganze Zahlen  $x, y \in \mathbb{Z}$  mit  $y \neq 0$  gibt es **eindeutig** bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$ , sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl  $q$  heißt **Quotient** und  $r$  heißt **Rest** der Division.

- **div**:  $\mathbb{Z}^2 \rightarrow \mathbb{Z}$  ordnet  $(x, y)$  den Quotienten  $q$  zu,
- **mod**:  $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$  ordnet  $(x, y)$  den Rest  $r$  zu.

## Beweis

- **Existenz**: Eine der  $|y| \geq 1$  hintereinander liegenden ganzen Zahlen  $x - 0, x - 1, \dots, x - (|y| - 1)$

ist ein Vielfaches von  $y$ .

$\implies$  es gibt  $r \in \{0, 1, \dots, |y| - 1\}$  und  $q \in \mathbb{Z}$  mit  $x - r = q \cdot y$ . ✓

- **Eindeutigkeit**: Falls  $qy + r = x = q'y + r'$  wie in (\*), dann gilt

$$0 = (q - q')y + (r - r') \quad \text{mit} \quad |r - r'| < |y|.$$

$\implies y \mid (r - r')$ , da  $y \mid 0$  und  $y \mid (q - q')y$

$\implies$  wegen  $|r - r'| < |y|$  folgt dann  $r = r'$

$\implies qy = q'y$  und wegen  $y \neq 0$  folgt  $q = q'$  ✓ □

# Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest

# Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest
- Proposition 2:  $\text{ggT}(x, y) = \text{ggT}(\text{mod}(x, y), y)$

# Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest
- Proposition 2:  $\text{ggT}(x, y) = \text{ggT}(\text{mod}(x, y), y)$   
→ Beweis wie bei der Proposition zuvor

# Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest

- Proposition 2:  $\text{ggT}(x, y) = \text{ggT}(\text{mod}(x, y), y)$

→ Beweis wie bei der Proposition zuvor

## Verbesserter rekursiver EUKLIDischer Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x%y,y); /* x%y = mod(x,y) */  
    else  
        return ggT(x,y%x);  
}
```

# Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest

- Proposition 2:  $\text{ggT}(x, y) = \text{ggT}(\text{mod}(x, y), y)$

→ Beweis wie bei der Proposition zuvor

## Verbesserter rekursiver EUKLIDischer Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x%y,y); /* x%y = mod(x,y) */  
    else  
        return ggT(x,y%x);  
}
```

- **Korrektheit:** Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$ ,

# Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest

- Proposition 2:  $\text{ggT}(x, y) = \text{ggT}(\text{mod}(x, y), y)$

→ Beweis wie bei der Proposition zuvor

## Verbesserter rekursiver EUKLIDischer Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x%y,y); /* x%y = mod(x,y) */  
    else  
        return ggT(x,y%x);  
}
```

- **Korrektheit:** Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$ ,

→ Induktionsbeweis wie zuvor mit Proposition 2

# Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest
- Proposition 2:  $\text{ggT}(x, y) = \text{ggT}(\text{mod}(x, y), y)$   
→ Beweis wie bei der Proposition zuvor

## Verbesserter rekursiver EUKLIDischer Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x%y,y); /* x%y = mod(x,y) */  
    else  
        return ggT(x,y%x);  
}
```

- **Korrektheit:** Algorithmus berechnet den  $\text{ggT}(|x|, |y|)$ ,  
→ Induktionsbeweis wie zuvor mit Proposition 2
- mod ist etwas teurer (Laufzeit) als Subtraktion, aber der verbesserte EUKLIDische Algorithmus hat polynomielle Laufzeit in der Länge der Eingabe  $\log |x| + \log |y|$

# Kongruenzen

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ .

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

■  $x \equiv y \pmod{m} \iff m \mid x - y$

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :
  - Reflexivität

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :
  - Reflexivität ✓

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :
  - Reflexivität ✓
  - Symmetrie

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :
  - Reflexivität ✓
  - Symmetrie ✓

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :
  - Reflexivität ✓
  - Symmetrie ✓
  - Transitivität:

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :
  - Reflexivität ✓
  - Symmetrie ✓
  - Transitivität:  $m \mid x - y$  und  $m \mid y - z \Rightarrow m \mid x - y + y - z$

# Kongruenzen

## Definition

Ganze Zahlen  $x, y \in \mathbb{Z}$  sind **kongruent modulo  $m$**  für eine natürliche Zahl  $m \in \mathbb{N}$ , falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h.  $x$  und  $y$  haben denselben Rest bei Division durch  $m$ . In diesem Fall sagen wir auch,  **$x$  ist kongruent zu  $y$  modulo  $m$**  und schreiben

$$x \equiv y \pmod{m}.$$

## Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo  $m$  definiert Äquivalenzrelation auf  $\mathbb{Z}$ :
  - Reflexivität ✓
  - Symmetrie ✓
  - Transitivität:  $m \mid x - y$  und  $m \mid y - z \Rightarrow m \mid x - y + y - z$  ✓

# Restklassen

## Definition (Restklassen)

Für jede natürliche Zahl  $m \in \mathbb{N}$  und jede ganze Zahl  $x \in \mathbb{Z}$  heißt die Äquivalenzklasse

$$[x]_m := \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$$

die Restklasse von  $x$  modulo  $m$ .

# Restklassen

## Definition (Restklassen)

Für jede natürliche Zahl  $m \in \mathbb{N}$  und jede ganze Zahl  $x \in \mathbb{Z}$  heißt die Äquivalenzklasse

$$[x]_m := \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$$

die **Restklasse von  $x$  modulo  $m$** .

## Folgerungen

- für jedes  $m \in \mathbb{N}$  gibt es genau  $m$  verschiedene Restklassen modulo  $m$

$$[0]_m, [1]_m, \dots, [m-1]_m.$$

# Restklassen

## Definition (Restklassen)

Für jede natürliche Zahl  $m \in \mathbb{N}$  und jede ganze Zahl  $x \in \mathbb{Z}$  heißt die Äquivalenzklasse

$$[x]_m := \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$$

die Restklasse von  $x$  modulo  $m$ .

## Folgerungen

- für jedes  $m \in \mathbb{N}$  gibt es genau  $m$  verschiedene Restklassen modulo  $m$

$$[0]_m, [1]_m, \dots, [m-1]_m.$$

- die Restklassen bilden eine Partition von  $\mathbb{Z}$ , d. h. sie sind paarweise disjunkt und

$$\mathbb{Z} = [0]_m \cup \dots \cup [m-1]_m$$

# Restklassen

## Definition (Restklassen)

Für jede natürliche Zahl  $m \in \mathbb{N}$  und jede ganze Zahl  $x \in \mathbb{Z}$  heißt die Äquivalenzklasse

$$[x]_m := \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$$

die **Restklasse von  $x$  modulo  $m$** .

## Folgerungen

- für jedes  $m \in \mathbb{N}$  gibt es genau  $m$  verschiedene Restklassen modulo  $m$

$$[0]_m, [1]_m, \dots, [m-1]_m.$$

- die Restklassen bilden eine Partition von  $\mathbb{Z}$ , d. h. sie sind paarweise disjunkt und

$$\mathbb{Z} = [0]_m \cup \dots \cup [m-1]_m$$

- Menge der Restklassen (Faktormenge der Äquivalenzrelation kongruent modulo  $m$ )

$$\mathbb{Z}/m\mathbb{Z} := \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist wohldefinierte Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist wohldefinierte Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [-\ell]_m = [m - \ell]_m$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist wohldefinierte Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist wohldefinierte Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist wohldefinierte Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist wohldefinierte Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist wohldefinierte Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist wohldefinierte Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist wohldefinierte Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [-\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist **wohldefinierte** Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist **wohldefinierte** Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:

$$[2]_4 \cdot [0]_4 = [0]_4,$$

$$[2]_4 \cdot [1]_4 = [2]_4,$$

$$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4,$$

$$[2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist **wohldefinierte** Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:
- $$[2]_4 \cdot [0]_4 = [0]_4, \quad [2]_4 \cdot [1]_4 = [2]_4,$$
- $$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4, \quad [2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$
- $\Rightarrow [2]_4$  hat kein multiplikativ Inverses in  $\mathbb{Z}/4\mathbb{Z}$

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist **wohldefinierte** Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:
- $$[2]_4 \cdot [0]_4 = [0]_4, \quad [2]_4 \cdot [1]_4 = [2]_4,$$
- $$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4, \quad [2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$
- $\Rightarrow [2]_4$  hat kein multiplikativ Inverses in  $\mathbb{Z}/4\mathbb{Z}$
- Addition und Multiplikation erfüllen das Distributivgesetz

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist **wohldefinierte** Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:
- $$[2]_4 \cdot [0]_4 = [0]_4, \quad [2]_4 \cdot [1]_4 = [2]_4,$$
- $$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4, \quad [2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$
- $\Rightarrow [2]_4$  hat kein multiplikativ Inverses in  $\mathbb{Z}/4\mathbb{Z}$
- Addition und Multiplikation erfüllen das Distributivgesetz

Für jedes  $m \in \mathbb{N}$  heißt  $\mathbb{Z}/m\mathbb{Z}$  mit Verknüpfungen  $+$  und  $\cdot$  **Restklassenring modulo  $m$** .

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [-\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist **wohldefinierte** Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:
- $$[2]_4 \cdot [0]_4 = [0]_4, \quad [2]_4 \cdot [1]_4 = [2]_4,$$
- $$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4, \quad [2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$
- $\Rightarrow [2]_4$  hat kein multiplikativ Inverses in  $\mathbb{Z}/4\mathbb{Z}$
- Addition und Multiplikation erfüllen das Distributivgesetz

Für jedes  $m \in \mathbb{N}$  heißt  $\mathbb{Z}/m\mathbb{Z}$  mit Verknüpfungen  $+$  und  $\cdot$  **Restklassenring modulo  $m$** .

- $\mathbb{Z}/1\mathbb{Z} = \{[0]_1\} = \{\mathbb{Z}\}$  ist **trivial (Nullring)**,

# Modulare Arithmetik

- mit Restklassen kann man gut rechnen
  - $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$  ist **wohldefinierte** Addition auf  $\mathbb{Z}/m\mathbb{Z}$
- Addition auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[0]_m$  ist neutrales Element der Addition auf  $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch  $[z]_m - [z']_m := [z - z']_m$  definiert werden
  - $[-z]_m$  ist invers zu  $[z]_m$ , d. h.  $-[z]_m = [-z]_m$
  - für  $\ell \in \{0, \dots, m-1\}$  gilt  $-[\ell]_m = [-\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$  und  $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$  ist **wohldefinierte** Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
- Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$  ist assoziativ und kommutativ
  - $[1]_m$  ist neutrales Element der Multiplikation auf  $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:
- $$[2]_4 \cdot [0]_4 = [0]_4, \quad [2]_4 \cdot [1]_4 = [2]_4,$$
- $$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4, \quad [2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$
- $\Rightarrow [2]_4$  hat kein multiplikativ Inverses in  $\mathbb{Z}/4\mathbb{Z}$
- Addition und Multiplikation erfüllen das Distributivgesetz

Für jedes  $m \in \mathbb{N}$  heißt  $\mathbb{Z}/m\mathbb{Z}$  mit Verknüpfungen  $+$  und  $\cdot$  **Restklassenring modulo  $m$** .

- $\mathbb{Z}/1\mathbb{Z} = \{[0]_1\} = \{\mathbb{Z}\}$  ist **trivial (Nullring)**, aber  $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$  ist sogar ein Körper

# GAUSSklammer

# GAUSSklammer

## Definition

Sei  $\xi \in \mathbb{R}$  eine reelle Zahl. Dann bezeichnet

## Definition

Sei  $\xi \in \mathbb{R}$  eine reelle Zahl. Dann bezeichnet

- $\lceil \xi \rceil$  die kleinste ganze Zahl  $z \in \mathbb{Z}$  mit  $z \geq \xi$ .

## Definition

Sei  $\xi \in \mathbb{R}$  eine reelle Zahl. Dann bezeichnet

- $\lceil \xi \rceil$  die kleinste ganze Zahl  $z \in \mathbb{Z}$  mit  $z \geq \xi$ .
- $\lfloor \xi \rfloor$  die größte ganze Zahl  $z \in \mathbb{Z}$  mit  $z \leq \xi$ .

# GAUSSklammer

## Definition

Sei  $\xi \in \mathbb{R}$  eine reelle Zahl. Dann bezeichnet

- $\lceil \xi \rceil$  die kleinste ganze Zahl  $z \in \mathbb{Z}$  mit  $z \geq \xi$ .
- $\lfloor \xi \rfloor$  die größte ganze Zahl  $z \in \mathbb{Z}$  mit  $z \leq \xi$ .

## Beobachtung

Für alle  $z \in \mathbb{Z}$  und  $n \in \mathbb{N}$  gilt

$$\operatorname{div}(z, n) = \left\lfloor \frac{z}{n} \right\rfloor$$

# GAUSSklammer

## Definition

Sei  $\xi \in \mathbb{R}$  eine reelle Zahl. Dann bezeichnet

- $\lceil \xi \rceil$  die kleinste ganze Zahl  $z \in \mathbb{Z}$  mit  $z \geq \xi$ .
- $\lfloor \xi \rfloor$  die größte ganze Zahl  $z \in \mathbb{Z}$  mit  $z \leq \xi$ .

## Beobachtung

Für alle  $z \in \mathbb{Z}$  und  $n \in \mathbb{N}$  gilt

$$\operatorname{div}(z, n) = \left\lfloor \frac{z}{n} \right\rfloor \quad \text{und} \quad \operatorname{mod}(z, n) = z - n \cdot \left\lfloor \frac{z}{n} \right\rfloor.$$

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13,$

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$
- 1 und  $n$  heißen auch die **trivialen (natürlichen) Teiler** von  $n \in \mathbb{N}$
- 1,  $-1$ ,  $z$  und  $-z$  sind die **trivialen (ganzen) Teiler** von  $z \in \mathbb{Z}$

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$
- 1 und  $n$  heißen auch die **trivialen (natürlichen) Teiler** von  $n \in \mathbb{N}$
- 1,  $-1$ ,  $z$  und  $-z$  sind die **trivialen (ganzen) Teiler** von  $z \in \mathbb{Z}$

## Definition (teilerfremd)

Zwei ganze Zahlen heißen **teilerfremd** (auch **relativ prim**), falls die 1 der einzige gemeinsame Teiler in  $\mathbb{N}$  ist.

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$
- 1 und  $n$  heißen auch die **trivialen (natürlichen) Teiler** von  $n \in \mathbb{N}$
- 1,  $-1$ ,  $z$  und  $-z$  sind die **trivialen (ganzen) Teiler** von  $z \in \mathbb{Z}$

## Definition (teilerfremd)

Zwei ganze Zahlen heißen **teilerfremd** (auch **relativ prim**), falls die 1 der einzige gemeinsame Teiler in  $\mathbb{N}$  ist. Es gilt also

$$x, y \in \mathbb{Z} \quad \text{sind teilerfremd} \quad \iff \quad \text{ggT}(x, y) = 1$$

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$
- 1 und  $n$  heißen auch die **trivialen (natürlichen) Teiler** von  $n \in \mathbb{N}$
- 1,  $-1$ ,  $z$  und  $-z$  sind die **trivialen (ganzen) Teiler** von  $z \in \mathbb{Z}$

## Definition (teilerfremd)

Zwei ganze Zahlen heißen **teilerfremd** (auch **relativ prim**), falls die 1 der einzige gemeinsame Teiler in  $\mathbb{N}$  ist. Es gilt also

$$x, y \in \mathbb{Z} \quad \text{sind teilerfremd} \quad \iff \quad \text{ggT}(x, y) = 1$$

- Teilerfremdheit ist **nicht** reflexiv, **nicht** transitiv, aber symmetrisch

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$
- 1 und  $n$  heißen auch die **trivialen (natürlichen) Teiler** von  $n \in \mathbb{N}$
- 1,  $-1$ ,  $z$  und  $-z$  sind die **trivialen (ganzen) Teiler** von  $z \in \mathbb{Z}$

## Definition (teilerfremd)

Zwei ganze Zahlen heißen **teilerfremd** (auch **relativ prim**), falls die 1 der einzige gemeinsame Teiler in  $\mathbb{N}$  ist. Es gilt also

$$x, y \in \mathbb{Z} \text{ sind teilerfremd} \iff \text{ggT}(x, y) = 1$$

- Teilerfremdheit ist **nicht** reflexiv, **nicht** transitiv, aber symmetrisch
- Für teilerfremde  $z \in \mathbb{Z}$  und  $m \in \mathbb{N}$  gilt:  
 $(z \cdot x) \equiv (z \cdot y) \pmod{m} \implies x \equiv y \pmod{m}$  für alle  $x, y \in \mathbb{Z}$ .

# Primzahlen

## Definition (Primzahlen)

Eine natürliche Zahl  $p \geq 2$  heißt **Primzahl**, falls 1 und  $p$  die einzigen Teiler von  $p$  in  $\mathbb{N}$  sind.

- Menge der Primzahlen  $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$
- 1 und  $n$  heißen auch die **trivialen (natürlichen) Teiler** von  $n \in \mathbb{N}$
- 1,  $-1$ ,  $z$  und  $-z$  sind die **trivialen (ganzen) Teiler** von  $z \in \mathbb{Z}$

## Definition (teilerfremd)

Zwei ganze Zahlen heißen **teilerfremd** (auch **relativ prim**), falls die 1 der einzige gemeinsame Teiler in  $\mathbb{N}$  ist. Es gilt also

$$x, y \in \mathbb{Z} \text{ sind teilerfremd} \iff \text{ggT}(x, y) = 1$$

- Teilerfremdheit ist **nicht** reflexiv, **nicht** transitiv, aber symmetrisch
- Für teilerfremde  $z \in \mathbb{Z}$  und  $m \in \mathbb{N}$  gilt:  
 $(z \cdot x) \equiv (z \cdot y) \pmod{m} \implies x \equiv y \pmod{m}$  für alle  $x, y \in \mathbb{Z}$ .

Falls  $p \in \mathbb{N}$  eine Primzahl ist, dann ist  $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$  ein Körper.

# Primfaktorzerlegung

## Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl  $n \in \mathbb{N}$  gibt es

- ein  $k \in \mathbb{N}_0$ ,
- paarweise verschiedene Primzahlen  $p_1, \dots, p_k$
- und natürliche Zahlen  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ ,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

# Primfaktorzerlegung

## Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl  $n \in \mathbb{N}$  gibt es

- ein  $k \in \mathbb{N}_0$ ,
- paarweise verschiedene Primzahlen  $p_1, \dots, p_k$
- und natürliche Zahlen  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ ,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

Diese Produktdarstellung von  $n$  heißt **Primfaktorzerlegung** und ist bis auf die Reihenfolge der Faktoren eindeutig.

# Primfaktorzerlegung

## Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl  $n \in \mathbb{N}$  gibt es

- ein  $k \in \mathbb{N}_0$ ,
- paarweise verschiedene Primzahlen  $p_1, \dots, p_k$
- und natürliche Zahlen  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ ,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

Diese Produktdarstellung von  $n$  heißt **Primfaktorzerlegung** und ist bis auf die Reihenfolge der Faktoren eindeutig.

## Bemerkungen

- für  $n = 1$  ist  $k = 0$  und der Satz folgt, da das leere Produkt 1 ist

# Primfaktorzerlegung

## Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl  $n \in \mathbb{N}$  gibt es

- ein  $k \in \mathbb{N}_0$ ,
- paarweise verschiedene Primzahlen  $p_1, \dots, p_k$
- und natürliche Zahlen  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ ,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

Diese Produktdarstellung von  $n$  heißt **Primfaktorzerlegung** und ist bis auf die Reihenfolge der Faktoren eindeutig.

## Bemerkungen

- für  $n = 1$  ist  $k = 0$  und der Satz folgt, da das leere Produkt 1 ist
- für  $n \geq 2$  ist immer  $k \geq 1$

# Primfaktorzerlegung

## Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl  $n \in \mathbb{N}$  gibt es

- ein  $k \in \mathbb{N}_0$ ,
- paarweise verschiedene Primzahlen  $p_1, \dots, p_k$
- und natürliche Zahlen  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ ,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

Diese Produktdarstellung von  $n$  heißt **Primfaktorzerlegung** und ist bis auf die Reihenfolge der Faktoren eindeutig.

## Bemerkungen

- für  $n = 1$  ist  $k = 0$  und der Satz folgt, da das leere Produkt 1 ist
- für  $n \geq 2$  ist immer  $k \geq 1$
- Sicherheit vieler Verschlüsselungsverfahren beruht auf der Annahme, dass für gegebenes  $n$  die Primfaktorzerlegung **nicht** effizient berechenbar ist

# Primfaktorzerlegung

## Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl  $n \in \mathbb{N}$  gibt es

- ein  $k \in \mathbb{N}_0$ ,
- paarweise verschiedene Primzahlen  $p_1, \dots, p_k$
- und natürliche Zahlen  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ ,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

Diese Produktdarstellung von  $n$  heißt **Primfaktorzerlegung** und ist bis auf die Reihenfolge der Faktoren eindeutig.

## Bemerkungen

- für  $n = 1$  ist  $k = 0$  und der Satz folgt, da das leere Produkt 1 ist
- für  $n \geq 2$  ist immer  $k \geq 1$
- Sicherheit vieler Verschlüsselungsverfahren beruht auf der Annahme, dass für gegebenes  $n$  die Primfaktorzerlegung **nicht** effizient berechenbar ist  
→ theoretisch effizient berechenbar mit Quantencomputern

# Primfaktorzerlegung

## Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl  $n \in \mathbb{N}$  gibt es

- ein  $k \in \mathbb{N}_0$ ,
- paarweise verschiedene Primzahlen  $p_1, \dots, p_k$
- und natürliche Zahlen  $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ ,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

Diese Produktdarstellung von  $n$  heißt **Primfaktorzerlegung** und ist bis auf die Reihenfolge der Faktoren eindeutig.

## Bemerkungen

- für  $n = 1$  ist  $k = 0$  und der Satz folgt, da das leere Produkt 1 ist
- für  $n \geq 2$  ist immer  $k \geq 1$
- Sicherheit vieler Verschlüsselungsverfahren beruht auf der Annahme, dass für gegebenes  $n$  die Primfaktorzerlegung **nicht** effizient berechenbar ist
  - theoretisch effizient berechenbar mit Quantencomputern
  - Entscheidungsproblem liegt in **NP**  $\cap$  **coNP**

# Existenz der Primfaktorzerlegung

**Beweis** (Widerspruch)

# Existenz der Primfaktorzerlegung

## **Beweis** (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

# Existenz der Primfaktorzerlegung

## **Beweis** (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist

# Existenz der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist
- $n$  ist keine Primzahl, da sonst  $n = p^\alpha$  mit  $p = n$  und  $\alpha = 1$  eine Primfaktorzerlegung von  $n$  ist

# Existenz der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist
  - $n$  ist keine Primzahl, da sonst  $n = p^\alpha$  mit  $p = n$  und  $\alpha = 1$  eine Primfaktorzerlegung von  $n$  ist
- ⇒  $n$  hat von 1 und  $n$  verschiedene Teiler

# Existenz der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist
  - $n$  ist keine Primzahl, da sonst  $n = p^\alpha$  mit  $p = n$  und  $\alpha = 1$  eine Primfaktorzerlegung von  $n$  ist
- ⇒  $n$  hat von 1 und  $n$  verschiedene Teiler
- ⇒ es gibt  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n \quad \text{und} \quad n = xy$$

# Existenz der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist
  - $n$  ist keine Primzahl, da sonst  $n = p^\alpha$  mit  $p = n$  und  $\alpha = 1$  eine Primfaktorzerlegung von  $n$  ist
- ⇒  $n$  hat von 1 und  $n$  verschiedene Teiler
- ⇒ es gibt  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n \quad \text{und} \quad n = xy$$

Da  $n$  die kleinste Zahl ohne Primfaktorzerlegung ist, gibt es Primfaktorzerlegungen von  $x$  und  $y$ , d. h. für geeignete  $k, \ell \in \mathbb{N}$ , Primzahlen  $p_1, \dots, p_k, q_1, \dots, q_\ell$  und  $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_\ell \in \mathbb{N}$  gilt:

$$x = \prod_{i=1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{j=1}^{\ell} q_j^{\beta_j}.$$

# Existenz der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist
  - $n$  ist keine Primzahl, da sonst  $n = p^\alpha$  mit  $p = n$  und  $\alpha = 1$  eine Primfaktorzerlegung von  $n$  ist
- ⇒  $n$  hat von 1 und  $n$  verschiedene Teiler  
⇒ es gibt  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n \quad \text{und} \quad n = xy$$

Da  $n$  die kleinste Zahl ohne Primfaktorzerlegung ist, gibt es Primfaktorzerlegungen von  $x$  und  $y$ , d. h. für geeignete  $k, \ell \in \mathbb{N}$ , Primzahlen  $p_1, \dots, p_k, q_1, \dots, q_\ell$  und  $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_\ell \in \mathbb{N}$  gilt:

$$x = \prod_{i=1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{j=1}^{\ell} q_j^{\beta_j}.$$

Somit ist  $n = xy = \prod_{i=1}^k p_i^{\alpha_i} \prod_{j=1}^{\ell} q_j^{\beta_j}$

# Existenz der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist
  - $n$  ist keine Primzahl, da sonst  $n = p^\alpha$  mit  $p = n$  und  $\alpha = 1$  eine Primfaktorzerlegung von  $n$  ist
- ⇒  $n$  hat von 1 und  $n$  verschiedene Teiler  
⇒ es gibt  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n \quad \text{und} \quad n = xy$$

Da  $n$  die kleinste Zahl ohne Primfaktorzerlegung ist, gibt es Primfaktorzerlegungen von  $x$  und  $y$ , d. h. für geeignete  $k, \ell \in \mathbb{N}$ , Primzahlen  $p_1, \dots, p_k, q_1, \dots, q_\ell$  und  $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_\ell \in \mathbb{N}$  gilt:

$$x = \prod_{i=1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{j=1}^{\ell} q_j^{\beta_j}.$$

Somit ist  $n = xy = \prod_{i=1}^k p_i^{\alpha_i} \prod_{j=1}^{\ell} q_j^{\beta_j}$  und ggf. durch das Zusammenfassen von Faktoren (falls  $p_i = q_j$ ), erhalten wir eine Primfaktorzerlegung von  $n$ .

# Existenz der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$ , da das leere Produkt eine Primfaktorzerlegung der 1 ist
  - $n$  ist keine Primzahl, da sonst  $n = p^\alpha$  mit  $p = n$  und  $\alpha = 1$  eine Primfaktorzerlegung von  $n$  ist
- ⇒  $n$  hat von 1 und  $n$  verschiedene Teiler  
⇒ es gibt  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n \quad \text{und} \quad n = xy$$

Da  $n$  die kleinste Zahl ohne Primfaktorzerlegung ist, gibt es Primfaktorzerlegungen von  $x$  und  $y$ , d. h. für geeignete  $k, \ell \in \mathbb{N}$ , Primzahlen  $p_1, \dots, p_k, q_1, \dots, q_\ell$  und  $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_\ell \in \mathbb{N}$  gilt:

$$x = \prod_{i=1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{j=1}^{\ell} q_j^{\beta_j}.$$

Somit ist  $n = xy = \prod_{i=1}^k p_i^{\alpha_i} \prod_{j=1}^{\ell} q_j^{\beta_j}$  und ggf. durch das Zusammenfassen von Faktoren (falls  $p_i = q_j$ ), erhalten wir eine Primfaktorzerlegung von  $n$ . 

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem **Lemma von EUKLID**, welches eine Konsequenz des **Lemmas von BÉZOUT** ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als **Linearkombination** von  $x$  und  $y$  dargestellt werden.

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als **Linearkombination** von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als **Linearkombination** von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?)

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)
- Induktion nach  $x + y$  mit mehreren Vorgängern

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)
- Induktion nach  $x + y$  mit mehreren Vorgängern
- Induktionsanfang:  $x = 0$ , klar da dann  $y = 0$  und  $\text{ggT}(0, 0) = 0$

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)
- Induktion nach  $x + y$  mit mehreren Vorgängern
- Induktionsanfang:  $x = 0$ , klar da dann  $y = 0$  und  $\text{ggT}(0, 0) = 0$
- Induktionsschritt:

$$\text{ggT}(x, y) \stackrel{\text{Prop.}}{=} \text{ggT}(x, y)$$

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)
- Induktion nach  $x + y$  mit mehreren Vorgängern
- Induktionsanfang:  $x = 0$ , klar da dann  $y = 0$  und  $\text{ggT}(0, 0) = 0$
- Induktionsschritt:

$$\text{ggT}(x, y) \stackrel{\text{Prop.}}{=} \text{ggT}(x - y, y)$$

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)
- Induktion nach  $x + y$  mit mehreren Vorgängern
- Induktionsanfang:  $x = 0$ , klar da dann  $y = 0$  und  $\text{ggT}(0, 0) = 0$
- Induktionsschritt:

$$\text{ggT}(x, y) \stackrel{\text{Prop.}}{=} \text{ggT}(x - y, y) \stackrel{\text{l.A.}}{=} s'(x - y) + t'y$$

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)
- Induktion nach  $x + y$  mit mehreren Vorgängern
- Induktionsanfang:  $x = 0$ , klar da dann  $y = 0$  und  $\text{ggT}(0, 0) = 0$
- Induktionsschritt:

$$\text{ggT}(x, y) \stackrel{\text{Prop.}}{=} \text{ggT}(x - y, y) \stackrel{\text{l.A.}}{=} s'(x - y) + t'y = s'x + (t' - s')y$$

# Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

## Lemma (BÉZOUT)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  gibt es ganze Zahlen  $s, t \in \mathbb{Z}$ , sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der  $\text{ggT}(x, y)$  kann als Linearkombination von  $x$  und  $y$  dargestellt werden.
- Für teilerfremde  $x, y \in \mathbb{Z}$  gibt es somit  $s, t \in \mathbb{Z}$  mit  $sx + ty = 1$ .

**Beweis** (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?) und  $x \geq y$  (Warum?)
- Induktion nach  $x + y$  mit mehreren Vorgängern
- Induktionsanfang:  $x = 0$ , klar da dann  $y = 0$  und  $\text{ggT}(0, 0) = 0$
- Induktionsschritt:

$$\text{ggT}(x, y) \stackrel{\text{Prop.}}{=} \text{ggT}(x - y, y) \stackrel{\text{l.A.}}{=} s'(x - y) + t'y = s'x + (t' - s')y$$

und die Aussage folgt mit  $s = s'$  und  $t = t' - s'$  □

# Erweiterter EUKLIDISCHER Algorithmus

rekursive Berechnung von  $\text{ggT}(x, y)$ ,  $s$  und  $t$  mit  $\text{ggT}(x, y) = sx + ty$

```
int erwEuklid(int x, int y, int *s, int *t) {
    if ( x==0 ){ *s=0; *t=1; return y; }
    if ( y==0 ){ *s=1; *t=0; return x; }
    int ggT, sp, tp;           /* Zwischenergebnisse speichern */
    if ( x>y ){
        ggT = erwEuklid(x%y, y, &sp, &tp);    /* % = mod, / = div */
        *s = sp; *t = tp - sp*(x/y);         /* s und t verrechnen */
        return ggT;
    }
    else{
        ggT = erwEuklid(x, y%x, &sp, &tp);
        *s = sp - tp*(y/x); *t = tp;         /* s und t verrechnen */
        return ggT;
    }
}
```

# Erweiterter EUKLIDISCHER Algorithmus

rekursive Berechnung von  $\text{ggT}(x, y)$ ,  $s$  und  $t$  mit  $\text{ggT}(x, y) = sx + ty$

```
int erwEuklid(int x, int y, int *s, int *t) {
    if ( x==0 ){ *s=0; *t=1; return y; }
    if ( y==0 ){ *s=1; *t=0; return x; }
    int ggT, sp, tp;                /* Zwischenergebnisse speichern */
    if ( x>y ){
        ggT = erwEuklid(x%y, y, &sp, &tp);    /* % = mod, / = div */
        *s = sp; *t = tp - sp*(x/y);          /* s und t verrechnen */
        return ggT;
    }
    else{
        ggT = erwEuklid(x, y%x, &sp, &tp);
        *s = sp - tp*(y/x); *t = tp;          /* s und t verrechnen */
        return ggT;
    }
}
```

Korrektheit folgt induktiv mit  $x = q \cdot y + r$  für  $q = \text{div}(x, y)$  und  $r = \text{mod}(x, y)$  durch:

$$\text{ggT}(x, y) =$$

# Erweiterter EUKLIDISCHER Algorithmus

rekursive Berechnung von  $\text{ggT}(x, y)$ ,  $s$  und  $t$  mit  $\text{ggT}(x, y) = sx + ty$

```
int erwEuklid(int x, int y, int *s, int *t) {
    if ( x==0 ){ *s=0; *t=1; return y; }
    if ( y==0 ){ *s=1; *t=0; return x; }
    int ggT, sp, tp;                /* Zwischenergebnisse speichern */
    if ( x>y ){
        ggT = erwEuklid(x%y, y, &sp, &tp);    /* % = mod, / = div */
        *s = sp; *t = tp - sp*(x/y);         /* s und t verrechnen */
        return ggT;
    }
    else{
        ggT = erwEuklid(x, y%x, &sp, &tp);
        *s = sp - tp*(y/x); *t = tp;        /* s und t verrechnen */
        return ggT;
    }
}
```

Korrektheit folgt induktiv mit  $x = q \cdot y + r$  für  $q = \text{div}(x, y)$  und  $r = \text{mod}(x, y)$  durch:

$$\text{ggT}(x, y) = \text{ggT}(r, y) =$$

# Erweiterter EUKLIDISCHER Algorithmus

rekursive Berechnung von  $\text{ggT}(x, y)$ ,  $s$  und  $t$  mit  $\text{ggT}(x, y) = sx + ty$

```
int erwEuklid(int x, int y, int *s, int *t) {
    if ( x==0 ){ *s=0; *t=1; return y; }
    if ( y==0 ){ *s=1; *t=0; return x; }
    int ggT, sp, tp;                /* Zwischenergebnisse speichern */
    if ( x>y ){
        ggT = erwEuklid(x%y, y, &sp, &tp);    /* % = mod, / = div */
        *s = sp; *t = tp - sp*(x/y);          /* s und t verrechnen */
        return ggT;
    }
    else{
        ggT = erwEuklid(x, y%x, &sp, &tp);
        *s = sp - tp*(y/x); *t = tp;          /* s und t verrechnen */
        return ggT;
    }
}
```

Korrektheit folgt induktiv mit  $x = q \cdot y + r$  für  $q = \text{div}(x, y)$  und  $r = \text{mod}(x, y)$  durch:

$$\text{ggT}(x, y) = \text{ggT}(r, y) = s'r + t'y$$

# Erweiterter EUKLIDISCHER Algorithmus

rekursive Berechnung von  $\text{ggT}(x, y)$ ,  $s$  und  $t$  mit  $\text{ggT}(x, y) = sx + ty$

```
int erwEuklid(int x, int y, int *s, int *t) {
    if ( x==0 ){ *s=0; *t=1; return y; }
    if ( y==0 ){ *s=1; *t=0; return x; }
    int ggT, sp, tp;                /* Zwischenergebnisse speichern */
    if ( x>y ){
        ggT = erwEuklid(x%y, y, &sp, &tp);    /* % = mod, / = div */
        *s = sp; *t = tp - sp*(x/y);          /* s und t verrechnen */
        return ggT;
    }
    else{
        ggT = erwEuklid(x, y%x, &sp, &tp);
        *s = sp - tp*(y/x); *t = tp;          /* s und t verrechnen */
        return ggT;
    }
}
```

Korrektheit folgt induktiv mit  $x = q \cdot y + r$  für  $q = \text{div}(x, y)$  und  $r = \text{mod}(x, y)$  durch:

$$\text{ggT}(x, y) = \text{ggT}(r, y) = s' r + t' y$$

und wegen  $r = x - q \cdot y$  folgt  $\text{ggT}(x, y) = s' x + (t' - s' \cdot q) y$ .

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl  $p$  einen Faktor  $x$  oder  $y$ , falls  $p$  Teiler des Produkts  $xy$  ist.

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl  $p$  einen Faktor  $x$  oder  $y$ , falls  $p$  Teiler des Produkts  $xy$  ist.

## Beweis

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl  $p$  einen Faktor  $x$  oder  $y$ , falls  $p$  Teiler des Produkts  $xy$  ist.

## Beweis

Wegen BÉZOUTS Lemma (für  $x$  und  $n$ ) gibt es  $s, t \in \mathbb{Z}$  mit

$$sx + tn = \text{ggT}(x, n) = 1$$

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl  $p$  einen Faktor  $x$  oder  $y$ , falls  $p$  Teiler des Produkts  $xy$  ist.

## Beweis

Wegen BÉZOUTS Lemma (für  $x$  und  $n$ ) gibt es  $s, t \in \mathbb{Z}$  mit

$$sx + tn = \text{ggT}(x, n) = 1 \quad \implies \quad sxy + tny = y.$$

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl  $p$  einen Faktor  $x$  oder  $y$ , falls  $p$  Teiler des Produkts  $xy$  ist.

## Beweis

Wegen BÉZOUTS Lemma (für  $x$  und  $n$ ) gibt es  $s, t \in \mathbb{Z}$  mit

$$sx + tn = \text{ggT}(x, n) = 1 \quad \implies \quad sxy + tny = y.$$

Da  $n \mid xy$  gibt es ein  $d \in \mathbb{Z}$  mit  $xy = dn$

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl  $p$  einen Faktor  $x$  oder  $y$ , falls  $p$  Teiler des Produkts  $xy$  ist.

## Beweis

Wegen BÉZOUTS Lemma (für  $x$  und  $n$ ) gibt es  $s, t \in \mathbb{Z}$  mit

$$sx + tn = \text{ggT}(x, n) = 1 \quad \implies \quad sxy + tny = y.$$

Da  $n \mid xy$  gibt es ein  $d \in \mathbb{Z}$  mit  $xy = dn$  und damit erhalten wir

$$y = s \cdot dn + tny = (sd + ty)n.$$

# Lemma von EUKLID

## Lemma (EUKLID)

Für alle ganzen Zahlen  $x, y \in \mathbb{Z}$  und jede natürliche Zahl  $n \in \mathbb{N}$  gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl  $p$  einen Faktor  $x$  oder  $y$ , falls  $p$  Teiler des Produkts  $xy$  ist.

## Beweis

Wegen BÉZOUTS Lemma (für  $x$  und  $n$ ) gibt es  $s, t \in \mathbb{Z}$  mit

$$sx + tn = \text{ggT}(x, n) = 1 \quad \implies \quad sxy + tny = y.$$

Da  $n \mid xy$  gibt es ein  $d \in \mathbb{Z}$  mit  $xy = dn$  und damit erhalten wir

$$y = s \cdot dn + tny = (sd + ty)n.$$

Somit ist  $y$  ein Vielfaches von  $n$ . □

# Eindeutigkeit der Primfaktorzerlegung

**Beweis** (Widerspruch)

# Eindeutigkeit der Primfaktorzerlegung

## **Beweis** (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

# Eindeutigkeit der Primfaktorzerlegung

## **Beweis** (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$ , da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann

# Eindeutigkeit der Primfaktorzerlegung

## **Beweis** (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$ , da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann
- $n$  ist keine Primzahl, da wir sonst eine Primzahl als Produkt von Primzahlen schreiben könnten

# Eindeutigkeit der Primfaktorzerlegung

## **Beweis** (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$ , da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann
- $n$  ist keine Primzahl, da wir sonst eine Primzahl als Produkt von Primzahlen schreiben könnten
- beide Primfaktorzerlegungen können keinen gemeinsamen Primfaktor  $p$  haben, da sonst  $n/p$  eine kleinere Zahl mit mehreren Primfaktorzerlegungen wäre

# Eindeutigkeit der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$ , da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann
  - $n$  ist keine Primzahl, da wir sonst eine Primzahl als Produkt von Primzahlen schreiben könnten
  - beide Primfaktorzerlegungen können keinen gemeinsamen Primfaktor  $p$  haben, da sonst  $n/p$  eine kleinere Zahl mit mehreren Primfaktorzerlegungen wäre
- ⇒ es gibt unterschiedliche Primzahlen  $p$  und  $q$  und  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n, \quad x \neq y \quad \text{und} \quad px = n = qy$$

# Eindeutigkeit der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$ , da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann
  - $n$  ist keine Primzahl, da wir sonst eine Primzahl als Produkt von Primzahlen schreiben könnten
  - beide Primfaktorzerlegungen können keinen gemeinsamen Primfaktor  $p$  haben, da sonst  $n/p$  eine kleinere Zahl mit mehreren Primfaktorzerlegungen wäre
- ⇒ es gibt unterschiedliche Primzahlen  $p$  und  $q$  und  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n, \quad x \neq y \quad \text{und} \quad px = n = qy$$

Insbesondere haben wir

$$p \mid qy \quad \text{und} \quad \text{ggT}(p, q) = 1.$$

Nach dem Lemma von EUKLID ist  $p$  also ein Teiler von  $y$ ,

# Eindeutigkeit der Primfaktorzerlegung

## Beweis (Widerspruch)

Sei  $n$  die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$ , da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann
  - $n$  ist keine Primzahl, da wir sonst eine Primzahl als Produkt von Primzahlen schreiben könnten
  - beide Primfaktorzerlegungen können keinen gemeinsamen Primfaktor  $p$  haben, da sonst  $n/p$  eine kleinere Zahl mit mehreren Primfaktorzerlegungen wäre
- ⇒ es gibt unterschiedliche Primzahlen  $p$  und  $q$  und  $x, y \in \mathbb{N}$  mit

$$1 < x < n, \quad 1 < y < n, \quad x \neq y \quad \text{und} \quad px = n = qy$$

Insbesondere haben wir

$$p \mid qy \quad \text{und} \quad \text{ggT}(p, q) = 1.$$

Nach dem Lemma von EUKLID ist  $p$  also ein Teiler von  $y$ , aber dies widerspricht der obigen Beobachtung, dass wegen der minimalen Wahl von  $n$  keine Primzahl in beiden Primfaktorzerlegungen vorkommt. ⚡

# Wieviele Primzahlen gibt es?

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

**Beweis** (Widerspruch)

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

**Beweis** (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen  $p_1, \dots, p_k$ .

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

**Beweis** (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen  $p_1, \dots, p_k$ .

- **Beobachtung:**  $N$  und  $N + 1$  haben keinen gemeinsamen Teiler  $\geq 2$ , da jeder Teiler auch  $N + 1 - N = 1$  teilt

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

**Beweis** (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen  $p_1, \dots, p_k$ .

- **Beobachtung:**  $N$  und  $N + 1$  haben keinen gemeinsamen Teiler  $\geq 2$ , da jeder Teiler auch  $N + 1 - N = 1$  teilt
- betrachte das Produkt  $N = p_1 \cdot \dots \cdot p_k$

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

**Beweis** (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen  $p_1, \dots, p_k$ .

- **Beobachtung:**  $N$  und  $N + 1$  haben keinen gemeinsamen Teiler  $\geq 2$ , da jeder Teiler auch  $N + 1 - N = 1$  teilt
- betrachte das Produkt  $N = p_1 \cdot \dots \cdot p_k$

$\Rightarrow N$  und  $N + 1$  haben keine gemeinsamen Primfaktoren

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

**Beweis** (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen  $p_1, \dots, p_k$ .

- **Beobachtung:**  $N$  und  $N + 1$  haben keinen gemeinsamen Teiler  $\geq 2$ , da jeder Teiler auch  $N + 1 - N = 1$  teilt
  - betrachte das Produkt  $N = p_1 \cdot \dots \cdot p_k$
- $\Rightarrow N$  und  $N + 1$  haben keine gemeinsamen Primfaktoren
- $\Rightarrow$  alle Primzahlen aus der Primfaktorzerlegung von  $N + 1$  sind verschieden von  $p_1, \dots, p_k$

# Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

**Beweis** (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen  $p_1, \dots, p_k$ .

- **Beobachtung:**  $N$  und  $N + 1$  haben keinen gemeinsamen Teiler  $\geq 2$ , da jeder Teiler auch  $N + 1 - N = 1$  teilt
- betrachte das Produkt  $N = p_1 \cdot \dots \cdot p_k$
- ⇒  $N$  und  $N + 1$  haben keine gemeinsamen Primfaktoren
- ⇒ alle Primzahlen aus der Primfaktorzerlegung von  $N + 1$  sind verschieden von  $p_1, \dots, p_k$
- wegen  $N + 1 > 1$  gibt es auch mindestens einen Primfaktor  $q$  von  $N + 1$

# Wieviele Primzahlen gibt es?

## Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

### Beweis (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen  $p_1, \dots, p_k$ .

- **Beobachtung:**  $N$  und  $N + 1$  haben keinen gemeinsamen Teiler  $\geq 2$ , da jeder Teiler auch  $N + 1 - N = 1$  teilt

- betrachte das Produkt  $N = p_1 \cdot \dots \cdot p_k$

$\Rightarrow N$  und  $N + 1$  haben keine gemeinsamen Primfaktoren

$\Rightarrow$  alle Primzahlen aus der Primfaktorzerlegung von  $N + 1$  sind verschieden von  $p_1, \dots, p_k$

- wegen  $N + 1 > 1$  gibt es auch mindestens einen Primfaktor  $q$  von  $N + 1$

Es gibt also eine weitere Primzahl  $q$  verschieden von  $p_1, \dots, p_k$ .



# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

## Beweis

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?)

# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

## Beweis

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (**Warum?**)
- falls  $x = 0$  oder  $y = 0$ ,

# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

## Beweis

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (**Warum?**)
- falls  $x = 0$  oder  $y = 0$ , dann  $\text{kgV}(x, y) = 0$  und die Formel folgt

# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

## Beweis

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (**Warum?**)
- falls  $x = 0$  oder  $y = 0$ , dann  $\text{kgV}(x, y) = 0$  und die Formel folgt
- seien  $p_1, \dots, p_\ell$  alle gemeinsamen Primfaktoren von  $x$  und  $y$  und

$$x = \prod_{i=1}^{\ell} p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{i=1}^{\ell} p_i^{\beta_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}$$

die Primfaktorzerlegungen von  $x$  und  $y$

# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

## Beweis

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?)
- falls  $x = 0$  oder  $y = 0$ , dann  $\text{kgV}(x, y) = 0$  und die Formel folgt
- seien  $p_1, \dots, p_\ell$  alle gemeinsamen Primfaktoren von  $x$  und  $y$  und

$$x = \prod_{i=1}^{\ell} p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{i=1}^{\ell} p_i^{\beta_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}$$

die Primfaktorzerlegungen von  $x$  und  $y$

Damit folgt

# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

## Beweis

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?)
- falls  $x = 0$  oder  $y = 0$ , dann  $\text{kgV}(x, y) = 0$  und die Formel folgt
- seien  $p_1, \dots, p_\ell$  alle gemeinsamen Primfaktoren von  $x$  und  $y$  und

$$x = \prod_{i=1}^{\ell} p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{i=1}^{\ell} p_i^{\beta_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}$$

die Primfaktorzerlegungen von  $x$  und  $y$

Damit folgt

$$\text{ggT}(x, y) = \prod_{i=1}^{\ell} p_i^{\min(\alpha_i, \beta_i)}$$

$$\text{kgV}(x, y) = \prod_{i=1}^{\ell} p_i^{\max(\alpha_i, \beta_i)} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}.$$

# ggT und kgV und Primfaktoren

## Satz

Für alle ganzen Zahlen  $x$  und  $y \in \mathbb{Z}$  gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

## Beweis

- o. B. d. A.  $x, y \in \mathbb{N}_0$  (Warum?)
- falls  $x = 0$  oder  $y = 0$ , dann  $\text{kgV}(x, y) = 0$  und die Formel folgt
- seien  $p_1, \dots, p_\ell$  alle gemeinsamen Primfaktoren von  $x$  und  $y$  und

$$x = \prod_{i=1}^{\ell} p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{i=1}^{\ell} p_i^{\beta_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}$$

die Primfaktorzerlegungen von  $x$  und  $y$

Damit folgt

$$\text{ggT}(x, y) = \prod_{i=1}^{\ell} p_i^{\min(\alpha_i, \beta_i)}$$

$$\text{kgV}(x, y) = \prod_{i=1}^{\ell} p_i^{\max(\alpha_i, \beta_i)} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}.$$

Da  $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$  folgt die Aussage. □