# Vorlesung "Mathematische Strukturen"

Sommersemester 2011

Prof. Barbara König
Übungsleitung: Mathias Hülsbusch





## Mengen

**Menge**

Menge $M$ von Elementen, wird beschrieben als Aufzählung

$$M = \{0, 2, 4, 6, 8, \dots\}$$

oder als Menge von Elementen mit einer bestimmten Eigenschaft

$$M = \{n \mid n \in \mathbb{N}_0 \text{ und } n \text{ gerade}\}.$$

Allgemeines Format:

$$M = \{x \mid P(x)\}$$

($M$ ist Menge aller Elemente $x$, die die Eigenschaft $P$ erfüllen.)





## Mengen

Bemerkungen:

- Die Elemente einer Menge sind ungeordnet, d.h., ihre Ordnung spielt keine Rolle. Beispielsweise gilt:

$$\{1,2,3\} = \{1,3,2\} = \{2,1,3\} = \{2,3,1\} = \{3,1,2\} = \{3,2,1\}$$

- Ein Element kann nicht "mehrfach" in einer Menge auftreten. Es ist entweder in der Menge, oder es ist nicht in der Menge. Beispielsweise gilt:

$$\{1,2,3\} \neq \{1,2,3,4\} = \{1,2,3,4,4\}$$





## Mengen

**Element einer Menge**

Wir schreiben $a \in M$, falls ein Element $a$ in der Menge $M$ enthalten ist.

**Anzahl der Elemente einer Menge**

Für eine Menge $M$ gibt $|M|$ die Anzahl ihrer Elemente an.

**Teilmengenbeziehung**

Wir schreiben $A \subseteq B$, falls jedes Element von $A$ auch in $B$ enthalten ist. Die Beziehung $\subseteq$ heißt auch Inklusion.

**Leere Menge**

Mit $\emptyset$ oder $\{\}$ bezeichnet man die leere Menge. Sie enthält keine Elemente und ist Teilmenge jeder anderen Menge.

## Mengen

**Vereinigung**

Die Vereinigung zweier Mengen $A, A$ ist die Menge $M$, die die Elemente enthält, die in $A$ oder $B$ vorkommen. Man schreibt dafür $A \cup B$.

$$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$$

**Schnitt**

Der Schnitt zweier Mengen $A, B$ ist die Menge $M$, die die Element enthält, die sowohl in $A$ als auch in $B$ vorkommen. Man schreibt dafür $A \cap B$.

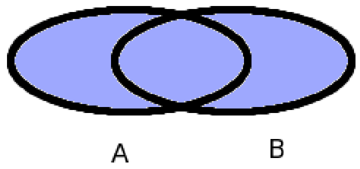
$$A \cap B = \{x \mid x \in A \text{ und } x \in B\}$$



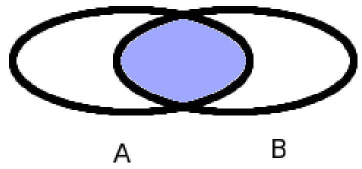


## Mengen

Veranschaulichung von Vereinigung und Schnitt durch Venn-Diagramme:




Blau eingefärbte Fläche entspricht der Vereinigung $A \cup B$




Blau eingefärbte Fläche entspricht dem Schnitt $A \cap B$





## Mengen

**Mengendifferenz**

Seien $A, B$ zwei Mengen. Dann bezeichnet $A \backslash B$ die Menge aller Elemente, die in $A$ vorkommen und in $B$ nicht vorkommen.

$$A \backslash B = \{x \mid x \in A \text{ und } x \notin B\}$$

Beispiele:

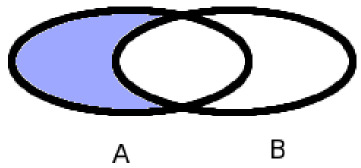
- $\{0, 1, 2, 3, 4, 5\} \backslash \{0\} = \{1, 2, 3, 4, 5\}$
- $\{a, b, c\} \backslash \{c, d\} = \{a, b\}$





## Mengen

Veranschaulichung der Mengendifferenz durch ein Venn-Diagramm:




Blau eingefärbte Fläche entspricht der Mengendifferenz $A \backslash B$

## Mengen

### Potenzmenge

Sei $M$ eine Menge. Die Menge $\mathcal{P}(M)$ ist die Menge aller Teilmengen von $M$.

$$\mathcal{P}(M) = \{A \mid A \subseteq M\}$$

Beispiel:
$\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Es gilt: $|\mathcal{P}(M)| = 2^{|M|}$ (für eine endliche Menge $M$).





## Mengen

### Kreuzprodukt (kartesisches Produkt)

Seien $A, B$ zwei Mengen. Die Menge $A \times B$ ist die Menge aller Paare $(a, b)$, wobei die erste Komponente des Paars aus $A$, die zweite aus $B$ kommt.

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Beispiel:
$\{1,2\} \times \{3,4,5\} = \{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5)\}$

Es gilt: $|A \times B| = |A| \cdot |B|$ (für endliche Menge $A, B$).





## Mengen

Bemerkungen:

- Wir betrachten nicht nur Paare, sondern auch sogenannte Tupel, bestehend aus mehreren Komponenten. Ein Tupel $(a_1, \ldots, a_n)$ bestehend aus $n$ Komponenten heißt auch $n$-Tupel.
- In einem Tupel sind die Komponenten geordnet! Es gilt z.B.:

$$(1,2,3) \neq (1,3,2) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0$$

- Eine Komponente kann "mehrfach" in einem Tupel auftreten. Tupel unterschiedlicher Länge sind immer verschieden. Beispielsweise:

$$(1,2,3,4) \neq (1,2,3,4,4)$$

Runde Klammern $(,)$ und geschweifte Klammern $\{,\}$ stehen für ganz verschiedene mathematische Objekte!





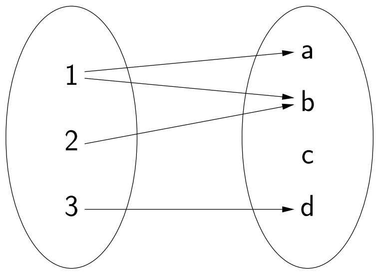
## Relationen

### Relation zwischen der Menge $A$ und der Menge $B$

Eine Teilmenge $R \subseteq A \times B$ des Kreuzprodukts von $A$ und $B$ heißt Relation zwischen $A$ und $B$.

Beispiel:
$A = \{1,2,3\}$ $B = \{a, b, c, d\}$ $R = \{(1,a), (1,b), (2,b), (3,d)\}$

Relationen können auf folgende Weise graphisch dargestellt werden:



## Relationen

Schreibweise: wir notieren folgendermaßen, dass ein Paar in einer Relation liegt

- Standard-Schreibweise: $(2, b) \in R$
- Infix-Schreibweise: $2\,R\,b$

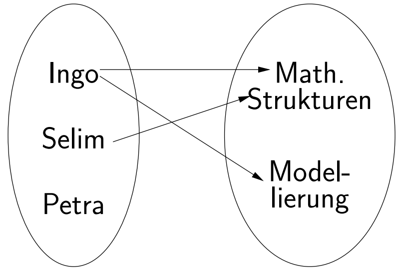
  Für Relationen wie $=, <, \leq, >, \geq$ wird fast immer die Infix-Schreibweise verwendet
  (Beispielsweise $2 < 5$, $7 \geq 3$)





## Relationen

Weiteres Beispiel: Zuordnung von Studierenden zu Veranstaltungen




$$\begin{aligned} A &= \{\text{Ingo}, \text{Selim}, \text{Petra}\} \\ B &= \{\text{Math.Strukturen}, \text{Modellierung}\} \\ R &= \{(\text{Ingo}, \text{Math.Strukturen}), (\text{Ingo}, \text{Modellierung}), \\ &\quad (\text{Selim}, \text{Math.Strukturen})\} \end{aligned}$$





## Relationen

Wir sehen uns nun einige besondere Arten von Relationen an:

- Funktionen
- Äquivalenzrelationen
- Ordnungen





## Funktionen

**Funktion von der Menge $A$ in die Menge $B$**

Eine Relation $f \subseteq A \times B$ heißt Funktion, wenn folgendes gilt:

- für jedes Element $a \in A$ gibt es genau ein Element $b \in B$ mit $(a, b) \in R$.

Anschaulich: jedes Element in der Menge $A$ hat genau einen ausgehenden Pfeil. (Die vorherigen Beispiels-Relationen waren also keine Funktionen.)

## Funktionen

### Notation von Funktionen

$$\begin{aligned} f\colon A &\to B \\ a &\mapsto f(a) \end{aligned}$$

Die Funktion $f$ bildet ein Element $a \in A$ auf ein Element $f(a) \in B$ ab. Dabei ist $A$ der Definitionsbereich und $B$ der Wertebereich.

Beispiel (Quadratfunktion):

$$f\colon \mathbb{Z} \to \mathbb{N}_0, \quad f(n) = n^2$$
$$\dots, -3 \mapsto 9, -2 \mapsto 4, -1 \mapsto 1, 0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 4, 3 \mapsto 9, \dots$$

Dabei ist $\mathbb{N}_0$ die Menge der natürlichen Zahlen (mit der Null) und $\mathbb{Z}$ die Menge der ganzen Zahlen.



Organisatorisches Einführung Grundlagen Algebraische Strukturen Kombinatorik Graphen Zusammenfassung

## Funktionen

### Bild und Urbild einer Menge

Sei $f\colon A \to B$ eine Funktion und $A' \subseteq A$. Dann nennt man die Menge

$$f(A') = \{f(a) \mid a \in A'\}$$

das Bild von $A'$ unter der Funktion $f$.

Sei nun $B' \subseteq B$. Die Menge

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

heißt das Urbild von $B'$ unter der Funktion $f$.



Organisatorisches Einführung Grundlagen Algebraische Strukturen Kombinatorik Graphen Zusammenfassung

## Funktionen

### Injektive Funktion

Eine Funktion $f\colon A \to B$ heißt injektiv, falls es keine Elemente $a_1, a_2 \in A$ gibt mit $a_1 \neq a_2$ und $f(a_1) = f(a_2)$.

Anschaulich: auf kein Element im Wertebereich zeigt mehr als ein Pfeil.

### Surjektive Funktion

Eine Funktion $f\colon A \to B$ heißt surjektiv, falls es für jedes $b \in B$ (mindestens) ein $a \in A$ gibt mit $f(a) = b$.

Anschaulich: auf jedes Element im Wertebereich zeigt (mindestens) ein Pfeil.



Organisatorisches Einführung Grundlagen Algebraische Strukturen Kombinatorik Graphen Zusammenfassung

## Funktionen

### Bijektive Funktion

Eine Funktion $f\colon A \to B$ heißt bijektiv, falls sie injektiv und surjektiv ist.

Anschaulich: auf jedes Element im Wertebereich zeigt genau ein Pfeil. D.h., es gibt eine eins-zu-eins-Zuordnung zwischen den Elementen des Definitionsbereichs und des Wertebereichs

## Funktionen

Bemerkung: Die bijektiven Funktionen sind genau die invertierbaren Funktionen. Zu einer bijektiven Funktion $f\colon A \to B$ gibt es eine Umkehrfunktion $f^{-1}\colon B \to A$ mit folgenden Eigenschaften:

- $f^{-1}(f(a)) = a$ für alle $a \in A$
- $f(f^{-1}(b)) = b$ für alle $b \in B$

Beispiel: Die Funktion

$$f\colon \mathbb{Z} \to \mathbb{Z} \qquad z \mapsto z - 1$$

hat als Umkehrfunktion

$$f^{-1}\colon \mathbb{Z} \to \mathbb{Z} \qquad z \mapsto z + 1$$





## Funktionen

**Verknüpfung von Funktionen**

Gegeben seien zwei Funktionen $f\colon A \to B$ und $g\colon B \to C$. Mit $g \circ f$ bezeichnen wir die Verknüpfung oder Hintereinanderausführung von $f$ und $g$. Diese Funktion ist wie folgt definiert:

$$\begin{array}{rcl} g \circ f\colon A & \to & C \\ a & \mapsto & g(f(a)) \end{array}$$

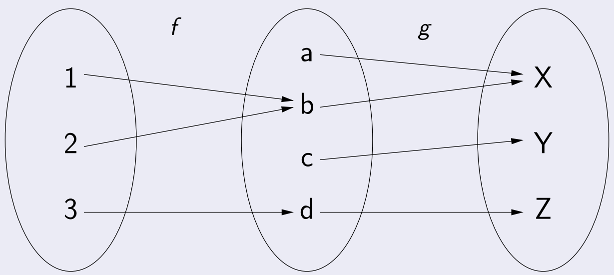
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$





## Funktionen

**Beispiel: Funktionsverknüpfung**

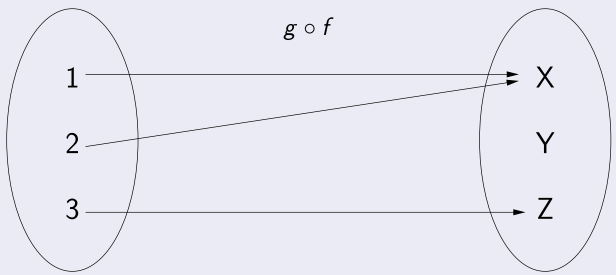







## Funktionen

**Beispiel: Funktionsverknüpfung**



## Relationen

Wir betrachten nun spezielle Relationen, die nur auf einer Menge $A$ definiert sind.

**Äquivalenzrelation**

Eine Relation $R \subseteq A \times A$ heißt Äquivalenzrelation, falls folgendes gilt:

- Reflexivität: für alle $a \in A$ gilt $(a, a) \in R$.
- Transitivität: falls für beliebige $a, b, c \in A$ $(a, b) \in R$ und $(b, c) \in R$ gilt, so muss auch $(a, c) \in R$ gelten.
- Symmetrie: falls für beliebige $a, b \in A$ $(a, b) \in R$ gilt, so muss auch $(b, a) \in R$ gelten.





## Relationen

Beispiel für eine Äquivalenzrelation:

$$R = \{(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid x, y \text{ haben denselben Divisionsrest bei ganzzahliger Division durch } 3\}$$

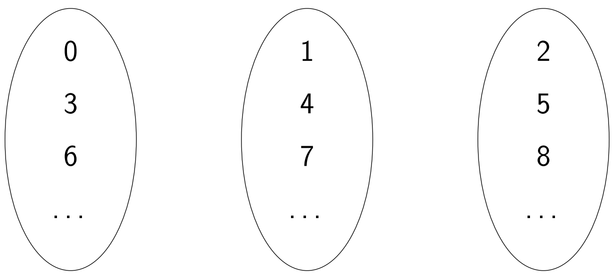




## Relationen

Bemerkung:

- Durch eine Äquivalenzrelation $R \subseteq A \times A$ zerfällt die Menge $A$ in sogenannte Äquivalenzklassen.
- Graphische Darstellung von Äquivalenzklassen für das vorherige Beispiel:








## Relationen

**Äquivalenzklassen**

Sei $R \subseteq A \times A$ eine Äquivalenzrelation und $a \in A$. Die Äquivalenzklasse von $a$ ist

$$[a]_R = \{a' \in A \mid a \, R \, a'\}$$

Für zwei Element $a, b \in A$ gilt entweder $[a]_R = [b]_R$ oder $[a]_R \cap [b]_R = \emptyset$.

## Relationen

**(Partielle) Ordnung**

Eine Relation $R \subseteq A \times A$ heißt (partielle) Ordnung, falls folgendes gilt:

- Reflexivität: für alle $a \in A$ gilt $(a, a) \in R$.
- Transitivität: falls für beliebige $a, b, c \in A$ $(a, b) \in R$ und $(b, c) \in R$ gilt, so muss auch $(a, c) \in R$ gelten.
- Antisymmetrie: falls für beliebige $a, b \in A$ $(a, b) \in R$ und $(b, a) \in R$ gilt, so muss $a = b$ gelten, d.h., $a$ und $b$ müssen dann gleich sein.





## Relationen

Bei der Definition einer Ordnung hat sich gegenüber der Definition einer Äquivalenzrelation nur die letzte Eigenschaft geändert (Antisymmetrie versus Symmetrie).

Achtung: Antisymmetrie ist nicht das Gegenteil von Symmetrie! Jede Gleichheitsrelation erfüllt beide Eigenschaften.





## Relationen

Beispiel für eine Ordnung:

Wir betrachten die Potenzmenge $\mathcal{P}(M)$ einer festen Menge $M$ und die Mengeninklusion $\subseteq$.





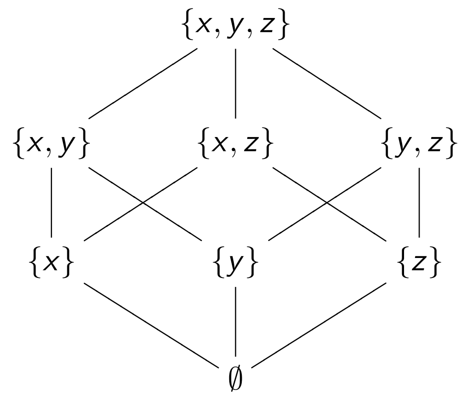
## Relationen

Ordnungen werden graphisch als sogenannte Hasse-Diagramme dargestellt:

Falls $a\,R\,b$ (und $a \neq b$) gilt, dann:

- liegt $a$ unterhalb von $b$ *und*
- wenn keine Elemente "zwischen" $a$ und $b$ liegen (bezüglich $R$), dann werden beide mit einer Linie verbunden.

Beispiel: $\mathcal{P}(\{x, y, z\})$ und Inklusion $\subseteq$



## Zahlen

Wir betrachten folgende spezielle Mengen von Zahlen:

**Natürliche Zahlen mit 0**

$\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, \ldots\}$

**Ganze Zahlen**

$\mathbb{Z} = \{\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$





## Zahlen

**Rationale Zahlen**

$\mathbb{Q}$: die Menge aller Brüche (= Menge aller Kommazahlen mit endlicher oder periodischer Dezimaldarstellung)

$$2 \quad -4 \quad \frac{1}{2} \quad \frac{27}{7} \quad 0,75 \quad 32,333417 \quad \frac{1}{3} = 0,3333\ldots = 0,\overline{3}$$

**Reelle Zahlen**

$\mathbb{R}$: die Menge aller reellen Zahlen (= Menge aller Kommazahlen mit beliebiger – auch unendlicher, nicht-periodischer – Dezimaldarstellung)

$$2 \quad -4 \quad \frac{1}{2} \quad \pi = 3,14159\ldots \qquad e = 2,718281\ldots$$





## Zahlen

**Division mit Rest**

Seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen mit $a \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $z, r \in \mathbb{Z}$ mit $0 \leq r < |a|$ und

$$z \cdot a + r = b$$

- $z$ heißt Ergebnis der ganzzahligen Division von $b$ durch $a$ und man schreibt $z = b \text{ div } a$.
- $r$ heißt Rest der ganzzahligen Division von $b$ durch $a$ und man schreibt $r = b \bmod a$.

Dabei ist $|a|$ der Absolutwert von $a$, beispielsweise ist $|-7| = 7$. Im folgenden wird $a$ aber immer eine positive ganze Zahl sein.





## Zahlen

Konkret (z.B. bei Verwendung eines Taschenrechners) lassen sich ($b$ div $a$) und ($b$ mod $a$) folgendermaßen berechnen (für den Fall, dass $a > 0$):

$$b \text{ div } a = \left\lfloor \frac{b}{a} \right\rfloor \qquad b \bmod a = b - a \cdot \left\lfloor \frac{b}{a} \right\rfloor$$

Dabei steht $\lfloor q \rfloor$ mit $q \in \mathbb{R}$ für die Abrundung von $q$ nach unten. D.h., $\lfloor q \rfloor$ ist die größte ganze Zahl, die kleiner gleich $q$ ist.

Beispiele: $\lfloor 3 \rfloor = 3$, $\lfloor 5,17 \rfloor = 5$, $\lfloor \pi \rfloor = 3$, $\lfloor -1 \rfloor = -1$, $\lfloor -0,7 \rfloor = -1$

## Zahlen

Ein Spezialfall der Division mit Rest ist die Teilbarkeit:

**Teilbarkeit**

Seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen. Man sagt, $a$ teilt $b$, wenn es ein $z \in \mathbb{Z}$ gibt mit $a \cdot z = b$.
Wir schreiben auch $a \mid b$ und nennen $a$ Teiler von $b$.

Bemerkung: Hier wird auch $a = 0$ erlaubt.

Die Relation $\mid$ (Teilbarkeit) ist eine partielle Ordnung, wenn man sie auf die natürlichen Zahlen einschränkt.





## Zahlen

Gelten folgende Beziehungen?

| | |
|---|---|
| $2 \mid 18$ | (Ja, $z = 9$) |
| $-7 \mid 14$ | (Ja, $z = -2$) |
| $3 \mid 10$ | (Nein) |
| $0 \mid 0$ | (Ja, $z$ beliebig) |
| $0 \mid 7$ | (Nein) |
| $7 \mid 0$ | (Ja, $z = 0$) |





## Zahlen

**Primzahl**

Eine Zahl $p \in \mathbb{N}_0$ heißt Primzahl, wenn folgendes gilt:

- $p \neq 0$ und $p \neq 1$
- die einzigen Teiler von $p$ in den natürlichen Zahlen sind 1 und $p$ selbst.

Primzahlen: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \dots$

Es gibt unendlich viele Primzahlen.





## Zahlen

**Eindeutigkeit der Primfaktorzerlegung**

Sei $n \in \mathbb{N}_0$ mit $n \neq 0$ eine natürliche Zahl. Ein Produkt $p_1 \cdot \dots \cdot p_m = n$ von Primzahlen heißt Primfaktorzerlegung von $n$.

Jede Zahl $n \neq 0$ besitzt eine solche Primfaktorzerlegung.
Wenn man zudem verlangt, dass die Primfaktoren in aufsteigender Reihenfolge angeordnet sind ($p_i \leq p_j$ für $i < j$), so ist die Primfaktorzerlegung einer Zahl eindeutig.

Bemerkungen:

- Die Primfaktorzerlegung von 1 ist das leere Produkt.
- Wenn wir auch die 1 als Primzahl einführen würden, so würden wir die die Eindeutigkeit der Primfaktorzerlegung verlieren. ($7 = 1 \cdot 7 = 1 \cdot 1 \cdot 7 = \dots$).

## Zahlen

**Größter gemeinsamer Teiler**

Seien $a, b \in \mathbb{N}_0$. Eine Zahl $d \in \mathbb{N}_0$ heißt größter gemeinsamer Teiler von $a$ und $b$ ($d = ggT(a, b)$), falls folgendes gilt:

- $d \mid a$ und $d \mid b$, d.h., $d$ teilt sowohl $a$ als auch $b$.
- für jede andere natürliche Zahl $d'$, die $a$ und $b$ teilt, gilt: $d' \leq d$.





## Zahlen

**Kleinstes gemeinsames Vielfaches**

Seien $a, b \in \mathbb{N}_0$. Eine Zahl $m \in \mathbb{N}_0$ mit $m \neq 0$ heißt kleinstes gemeinsames Vielfaches von $a$ und $b$ ($m = kgV(a, b)$), falls folgendes gilt:

- $a \mid m$ und $b \mid m$, d.h., sowohl $a$ als auch $b$ teilen $m$.
- für jede andere natürliche Zahl $m'$, die von $a$ und $b$ geteilt wird, gilt: $m \leq m'$.





## Zahlen

Wie bestimmt man den größten gemeinsamen Teiler?

**Bestimmung von $d = ggT(a, b)$ – Methode 1**

- Bestimme die Primfaktorzerlegungen von $a$ und $b$
- Betrachte alle Primfaktoren $p$, die in beiden Zerlegungen vorkommen: angenommen $p$ kommt in $a$ $k$-mal und in $b$ $\ell$-mal vor. Dann kommt $p$ in $d$ genau $\min(k, \ell)$-mal vor.

Beispiel: $ggT(12, 30)$

- $12 = 2 \cdot 2 \cdot 3$, $30 = 2 \cdot 3 \cdot 5$
- $ggT(12, 30) = 2 \cdot 3 = 6$.





## Zahlen

**Bestimmung von $d = ggT(a, b)$ – Methode 2**

- $ggT(0, a) = a$
- $ggT(a, b) = ggT(b, a)$
- $ggT(a, b) = ggT(a - b, b)$, falls $b \leq a$

Wende diese Regeln zur $ggT$-Berechnung so lange an, bis ein Ausdruck der Form $ggT(0, a)$ erreicht wird.

$$ggT(12, 30) = ggT(30, 12) = ggT(18, 12) = ggT(6, 12)$$
$$= ggT(12, 6) = ggT(6, 6) = ggT(0, 6) = 6$$

## Zahlen

Bemerkung:

Die Methode 2 ist bei weitem effizienter, insbesondere, wenn man die dritte Regel durch

$$ggT(a,b) = ggT(a \bmod b, b) \quad \text{falls } b \le a$$

ersetzt.





## Zahlen

Der $ggT$ und die $ggT$-Berechnung sind ein wichtiges Werkzeug für das Lösen bestimmter Gleichungen.

**Lösen diophantischer Gleichungen**

Gegeben seien $a, b, c \in \mathbb{Z}$. Wir suchen Lösungen $x, y \in \mathbb{Z}$ der Gleichung

$$a \cdot x + b \cdot y = c$$

Es gilt:

- Diese Gleichung hat genau dann eine Lösung, wenn $ggT(a,b) \mid c$.





## Zahlen

Für Gleichungen der Form $a \cdot x + b \cdot y = ggT(a,b)$ kann man $x, y$ dadurch bestimmen, dass man die $ggT$-Berechnung "rückwärts" nachvollzieht.

Beispiel: Lösen von $30 \cdot x + 12 \cdot y = 6$.

$$\begin{aligned} ggT(12,30) &= ggT(12,18) = ggT(6,12) = ggT(6,6) \\ &= ggT(6,0) = ggT(0,6) = 6 \end{aligned}$$

Dabei wurden die Zahlen folgendermaßen ermittelt:
$18 = 30 - 12$, $6 = 18 - 12$.

Damit kann man einsetzen:

$$6 = 18 - 12 = (30 - 12) - 12 = 30 \cdot 1 + 12 \cdot (-2)$$

Und damit hat man eine Lösung $x = 1$, $y = -2$.





## Zahlen

Gleichungen der Form $a \cdot x + b \cdot y = c$ mit $c \neq ggT(a,b)$ (aber $ggT(a,b) \mid c$) kann man folgendermaßen lösen:

- Zunächst die Gleichung $a \cdot x' + b \cdot y' = ggT(a,b)$ lösen.
- Dann die Lösungen $x', y'$ mit $c/ggT(a,b)$ multiplizieren, das ergibt die Lösungen $x, y$.

Beispiel: Lösen von $30 \cdot x + 12 \cdot y = 24$
$\rightsquigarrow$ Lösen von $30 \cdot x' + 12 \cdot y' = 6$ ergibt $x' = 1$, $y' = -2$.
$\rightsquigarrow$ mit $24/6 = 4$ multiplizieren ergibt $x = 4$, $y = -8$.

## Zahlen

**Teilerfremdheit**

Zwei Zahlen $a, b \in \mathbb{N}_0$ heißen teilerfremd, falls $ggT(a, b) = 1$.

**Eulersche $\varphi$-Funktion**

Die Eulersche $\varphi$-Funktion $\varphi\colon \mathbb{N}_0 \to \mathbb{N}_0$ ist folgendermaßen definiert:

- $\varphi(n)$ mit $n \in \mathbb{N}_0$ ist die Anzahl der Zahlen zwischen 1 und $n$, die zu $n$ teilerfremd sind.

$$\varphi(n) = |\{m \in \mathbb{N}_0 \mid 1 \leq m \leq n \text{ und } ggT(m, n) = 1\}|$$



Organisatorisches Einführung Grundlagen Algebraische Strukturen Kombinatorik Graphen Zusammenfassung

## Zahlen

Beispiele (Eulersche $\varphi$-Funktion):

| $n$ | $\varphi(n)$ | $n$ | $\varphi(n)$ |
|---|---|---|---|
| 0 | 0 | 7 | 6 |
| 1 | 1 | 8 | 4 |
| 2 | 1 | 9 | 6 |
| 3 | 2 | 10 | 4 |
| 4 | 2 | 11 | 10 |
| 5 | 4 | 12 | 4 |
| 6 | 2 | 13 | 12 |

Für eine Primzahl $p$ gilt $\varphi(p) = p - 1$.