Grundlagen der Programmierung

Mathematische Grundlagen:

Strukturelle Mathematik ♦ Beweise

Zentrale Konzepte

- *bei Algorithmen und bei der Programmierung:*
  - Funktionen, Operationen, Relationen
  - Mengenlehre
  - Kombinatorik (Anzahl von Möglichkeiten)
- *für Korrektheitsbeweise:*
  - Beweisverfahren, *vor allem*
  - vollständige Induktion (*heute*)
  - strukturelle Induktion (*später*)

Kombinatorische Anzahlbestimmung

Anordnung

- Gegeben sind n voneinander unterscheidbare Objekte.

- **Anordnung mit Wiederholung von Elementen**
  Anzahl der verschiedenen Möglichkeiten der Anordnung von k Objekten, wobei jedes Objekt in der Anordnung beliebig oft auftreten darf: n^k

- **Anordnung ohne Wiederholung von Elementen**
  Anzahl der verschiedenen Möglichkeiten der Anordnung der n Objekte (wobei jedes Objekt genau einmal verwendet wird):

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$$

Auswahl

- Gegeben sind *n* voneinander unterscheidbare Objekte.
- **Auswahl ohne Wiederholung**
  Anzahl der Möglichkeiten, *k* Objekte davon auszuwählen, wobei kein Objekt mehrfach ausgewählt werden kann:

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} = \frac{n!}{k! \cdot (n-k)!}$$

$$\binom{n}{2} = \frac{n \cdot (n-1)}{2}$$

Elementare Mengenlehre

Zahlenbereiche

$\mathbb{N}$	Menge der natürlichen Zahlen (inkl. 0)
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{Q}_0^+$	Menge der gebrochenen Zahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{R}_0^+$	Menge der nicht negativen reellen Zahlen

Mengen

- Mengen immer spezifizieren durch
  1. Angabe des Grundbereichs (**Universums**)
  2. Angabe der mengendefinierenden **Eigenschaft**

Beispiele:

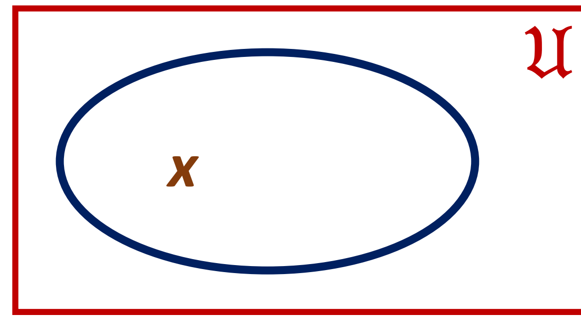
- Menge der Studenten/-innen ist die
  1. Menge der Menschen (**Universum:** Menge aller Menschen),
  2. die an einer HS oder Uni immatrikuliert sind (**Eigenschaft**).
- Menge der geraden Zahlen:

$$M = \{ n \mid n \in \mathbb{Z} \wedge 2 / n \}$$

- *Allgemein:* $M = \{ n \mid n \in \mathfrak{U} \wedge \mathrm{H}(n) \} = \{ n \in \mathfrak{U} \mid \mathrm{H}(n) \}$

Element, Komplementäre, leere Menge

Sei $\boldsymbol{M} = \{\, n \in \mathfrak{U} \mid \mathrm{H}(n) \,\}$.



- **Element der Menge**
  $\boldsymbol{x} \in \boldsymbol{M}$ gdw. $\boldsymbol{x}$ in $\mathfrak{U}$ und H($\boldsymbol{x}$) gilt.

- **Komplementäre Menge** $\overline{\boldsymbol{M}} = \{\, n \in \mathfrak{U} \mid \neg\mathrm{H}(n) \,\}$

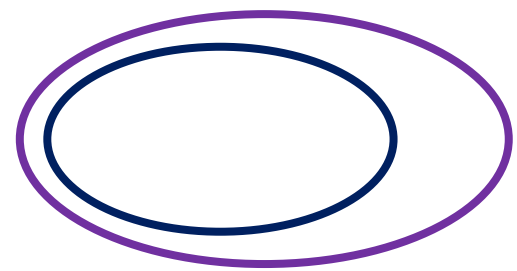
- Die **leere Menge** $\emptyset$ enthält keine Elemente.
  Für jedes Universum $\mathfrak{U}$ gilt: $\overline{\mathfrak{U}} = \emptyset$.

- **Kardinalzahl/Mächtigkeit** $|\boldsymbol{M}|$ einer endlichen Menge M ist die Anzahl ihrer Elemente.

Mengenbeziehungen

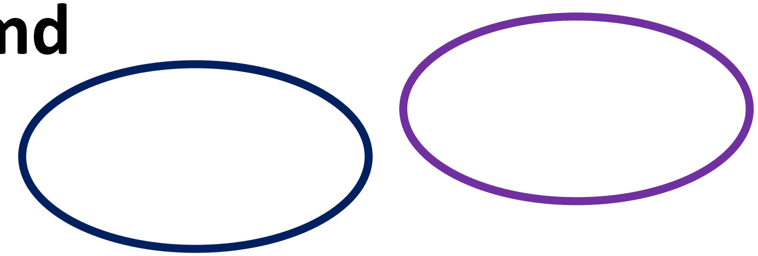
Sei $\boldsymbol{M} = \{\, n \in \mathfrak{U} \mid \mathrm{H}(n) \,\}$.

- $\boldsymbol{N} \subseteq \boldsymbol{M}$ (***N*** **Teilmenge** von ***M***)
  gdw. für alle $x \in \boldsymbol{N}$ auch $x \in \boldsymbol{M}$ gilt.



- $\boldsymbol{N} \subset \boldsymbol{M}$ (***N*** **echte Teilmenge** von ***M***)
  gdw. $\boldsymbol{N} \subseteq \boldsymbol{M}$ und $\boldsymbol{N} \neq \boldsymbol{M}$.

- ***N*** und ***M*** **disjunkt/elementfremd**
  gdw. es kein Element x gibt
  mit $x \in \boldsymbol{N}$ und $x \in \boldsymbol{M}$.



Potenzmenge

- Menge aller Teilmengen:

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

- *Beispiel* für $M = \{1,2,3\}$:

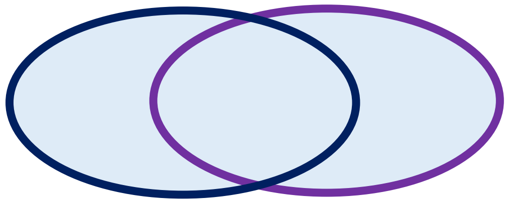
  $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, M\}$

- Sei $|M| = n$. Dann gilt

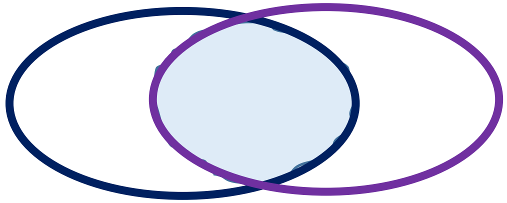
  $|\mathcal{P}(M)| = \sum_{k=0}^{n} \binom{n}{k} = 2^n$ (*Beweis in den Übungen*)

Mengenoperationen

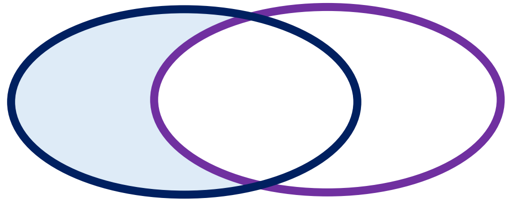
- Vereinigung
  $M \cup N = \{ n \mid n \in M \vee n \in N \}$



- Durchschnitt
  $M \cap N = \{ n \mid n \in M \wedge n \in N \}$



- Differenz
  $M \setminus N = \{ n \mid n \in M \wedge n \notin N \}$



Tupel: Mengen mit Anordnung

- **Endliche Menge**: Menge mit endlich vielen Elementen.

- ***n*-Tupel:** Es gibt ein erstes, zweites usw. und letztes Element einer endlichen Menge mit ***n*** Elementen. Dasselbe Element kann mehrfach auftreten.

- *Schreibweise:* $(x_1, x_2, ..., x_n)$

- $n = 2$: (geordnetes) **Paar** (x_1, x_2)
- $n = 3$: **Tripel** (x_1, x_2, x_3)

Kartesisches Produkt (Kreuzprodukt)

- $\boldsymbol{M_1 \times M_2 \times \ldots \times M_n}$
  $= \{(x_1, x_2, \ldots, x_n) \mid x_i \in M_i$ für alle i, $1 \leq i \leq n\}$

- *Beispiel:*
  Seien $M = \{1,2,3\}$ und $N = \{a,b\}$.

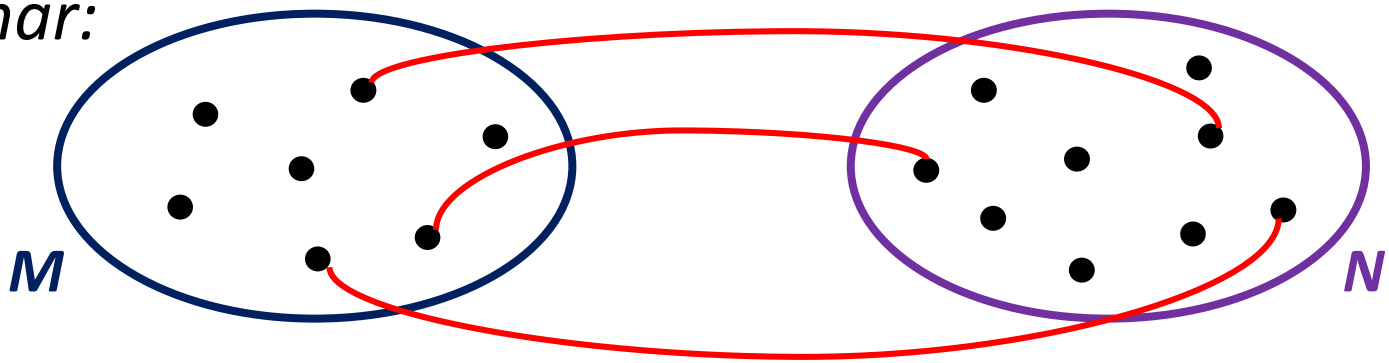
  $M \times N = \{ (1,a), (1,b), (2,a), (2,b), (3,a), (3,b) \}$

- Falls $\boldsymbol{M_1 = M_2 = \ldots = M_n = M}$: $\boldsymbol{M^n}$

Relationen

Relationen (*intuitiv*)

- Beziehungen
  - zwischen zwei Objekten (binäre Relationen)
  - oder mehreren (***n***) Objekten (***n***-stellige Relationen)
- *Beispiele:*
  Verwandtschaft von *n* Personen; Gleichheit oder <-Beziehung zweier Zahlen; Ähnlichkeit zweier Dreiecke
- *binär:*



Relationen (formal)

- *binäre* Relation: $\boldsymbol{R \subseteq M \times N}$
- *n*-stellige Relation: $\boldsymbol{R \subseteq M_1 \times M_2 \times \ldots \times M_n}$
- *n*-stellige Relation über ***M***: $\boldsymbol{R \subseteq M^n}$
- *Beispiele:*
  - Nachfolger-Relation (binäre Relation über $\mathbb{Z}$ oder $\mathbb{N}$)
  - Kleiner-als-Relation (binäre Relation über $\mathbb{Z}$ oder $\mathbb{R}$ oder ...)
  - Quadratzahl-Relation (binäre Relation z.B. über $\mathbb{N}$)
  - Summen-Relation (dreistellige Relation z.B. über $\mathbb{N}$)

Beispiele (formal)

- Nachfolger-Relation über $\mathbb{N}$:
  $R_{succ} = \{ (m,n) \mid n = m + 1 \} = \{(0,1), (1,2), (2,3), ...\}$
- Kleiner-als-Relation über $\mathbb{N}$:
  $R_{<} = \{ (m,n) \mid n - \text{m ist positiv} \}$
  $= \{(0,1), (0,2), ..., (1,2), (1,3), ...\} \supseteq R_{succ}$ **(Teilrelation)**
- Quadratzahl-Relation über $\mathbb{N}$:
  $Q = \{ (m,n) \mid n = m^2 \} = \{(0,0), (1,1), (2,4), (3,9), ...\}$
- Summen-Relation über $\mathbb{N}$:
  $S = \{ (a,b,c) \mid c = a + b \}$
  z.B. $(0,3,3) \in S$, $(1,2,3) \in S$, $(3,3,6) \in S$, $(3,5,8) \in S$

Repräsentation *n*-stelliger als binäre Relationen

- Sei $R \subseteq M_1 \times M_2 \times \ldots \times M_{n\text{-}1} \times M_n$.
- Die binäre Repräsentation von R ist die Relation $\boldsymbol{R^{\mathrm{b}} \subseteq (M_1 \times M_2 \times \ldots \times M_{n\text{-}1}) \times M_n}$ mit
  $(x_1, x_2, \ldots, x_{n\text{-}1}, x_n) \in R$ gdw. $((x_1, x_2, \ldots, x_{n\text{-}1}), x_n) \in R^{\mathrm{b}}$
- *z.B.* Summenrelation:
  $S^{\mathrm{b}} = \{ ((a,b), c) \mid c = a + b \}$
- Binäre Relationen erlauben die Schreibweise
  $x \; R \; y$ für $(x,y) \in R$.

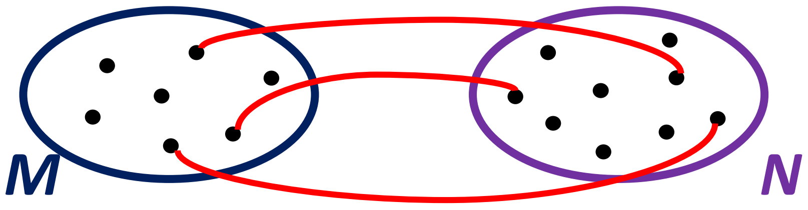
Definitions- und Wertebereich

- Sei R eine binäre Relation von M in N.

- **Definitionsbereich von R**
  D(R) $= \{ x \in M \mid \exists\, y \in N.\ (x,y) \in R \}$

- **Wertebereich von R**
  W(R) $= \{ y \in N \mid \exists\, x \in M.\ (x,y) \in R \}$

- **Bildmenge eines Elements aus D(R)**
  R(x) $= \{ \mathrm{y} \in N \mid (x,y) \in R \}$



Binäre Relationen von/aus und in/auf

- Sei $R \subseteq M \times N$.
- R ist Relation **aus M in N**.
- R ist Relation **von M in N**, falls $\mathbf{D}(R) = M$.
- R ist Relation **aus M auf N**, falls $\mathbf{W}(R) = N$.
- R ist Relation **von M auf N**, falls $\mathbf{D}(R) = M$ **und** $\mathbf{W}(R) = N$.

- *Beispiele:*
  - Quadratzahl-Relation über $\mathbb{N}$: **von** $\mathbb{N}$ **in** $\mathbb{N}$
  - Summen-Relation über $\mathbb{N}$: **von** $\mathbb{N}^2$ **auf** $\mathbb{N}$

Funktionen (Abbildung)

- Eine (totale) Funktion f von M in N, $\boldsymbol{f : M \to N}$, ist eine binäre Relation
  - **von *M*** in N, die
  - **eindeutig** ist.

- Eine Relation $R \subseteq M \to N$ heißt **eindeutig**, falls mit jedem $x \in M$ *höchstens ein* $y \in N$ in Relation R steht:

  Falls $(x,y) \in R$ und $(x,z) \in R$, dann gilt $y = z$.

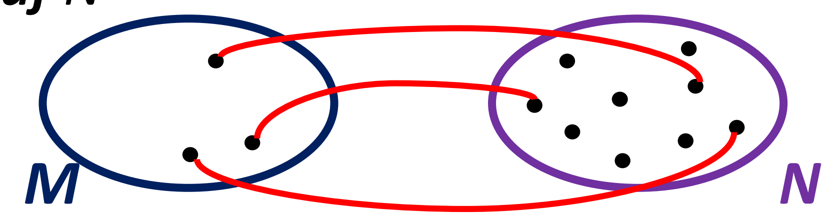
- Daher kann man $R(x) = y$ schreiben. (Oder $x \mapsto y$)

Argument und Bild

- Sei $f : M \to N$ eine Funktion.
- Jedes $x \in \mathrm{D}(f) = M$ heißt **Argument** von f.
- Jedes $y \in \mathrm{W}(f) \subseteq N$ heißt **Bild/Funktionswert** von f.

Eigenschaften von Funktionen

- Sei $f : M \to N$ eine Funktion.
- f ist **surjektiv**, falls **W(*f*) = *N***.
- f ist **injektiv (eineindeutig)**, falls aus $f(x_1) = f(x_2)$ folgt, dass $x_1 = x_2$ gilt.
  - Jedes Element des Wertebereichs ist Bild von genau einem Argument.
- f ist **bijektiv**, falls f surjektiv und injektiv ist.
  - eineindeutige Abbildung *von M **auf** N*



Partielle Funktionen

- Eine partielle Funktion **aus** M in N ist eine eindeutige binäre Relation **aus** M in N.
- $\boldsymbol{f : M \nrightarrow N}$
- *Beispiel:*
  Wurzelfunktion über den natürlichen Zahlen
  $\{ (m,n) \in \mathbb{N}^2 \mid m = n^2 \} = \{(0,0), (1,1), (4,2), (9,3), \ldots\}$
- *Beispiel:*
  Wurzelfunktion über den reellen Zahlen
  - **Einschränkung** auf $\mathbb{R}_0^+$ ist totale Funktion.

Mehrstellige Funktionen

- Eine *n*-stellige Funktion ist eine Funktion, die eine binäre Repräsentation einer (n+1)-stelligen Relation ist.

$$f : (M_1 \times M_2 \times \ldots \times M_{n-1} \times M_n) \longrightarrow N$$

- Diese können als **mehrsortige *n*-stellige Operationen** aufgefasst werden.

- *Beispiel:* $M_1 = \mathbb{N}$, $M_2 = N$ = Menge aller Kreise in der Ebene; $(n, K) \mapsto K'$ (konzentrische Streckung von K um Faktor n)

Operationen

- Eine *n*-stellige Operation ist eine *n*-stellige Funktion über einer Menge *M*.

  $$o : M^n \longrightarrow M$$

- *Beispiel*
  - Addition natürlicher Zahlen

    $+ : \mathbb{N}^2 \longrightarrow \mathbb{N}$ mit $(m,n) \mapsto m+n$

Eigenschaften binärer Relationen

- Sei $R \subseteq M^2$ eine binäre Relation über M .
- R ist **reflexiv** gdw. $(x,x) \in R$ für alle $x \in M$.
- R ist **transitiv** gdw. aus $(x,y) \in R$ und $(y,z) \in R$ folgt, dass auch $(x,z) \in R$.
- R ist **symmetrisch** gdw. aus $(x,y) \in R$ folgt, dass auch $(y,x) \in R$.
- R ist **antisymmetrisch** gdw. aus $(x,y) \in R$ und $(y,x) \in R$ folgt, dass $x = y$.

Ordnungsrelationen

- **Halbordnungsrelation in Menge *M***
  binäre Relation über M, die reflexiv, transitiv und antisymmetrisch ist
  - *z.B.* $\leq, \geq, \subseteq, \supseteq$
- **Ordnungsrelation in *M***
  Halbordnungsrelation R in M, wobei für alle x, y aus M
  $$x \; R \; y \quad \text{oder} \quad y \; R \; x$$
  - *z.B.* $\leq, \geq$ in den Zahlenbereichen
  - <u>nicht</u> $\subseteq, \supseteq$

Äquivalenzrelationen

- Binäre Relation, die reflexiv, transitiv und symmetrisch ist
- *Beispiele:*
  - *Verwandtschaft von Personen*
  - *Ähnlichkeit und Kongruenz geometrischer Figuren*
  - *Gleichheit*
  - *Waren mit gleichem Preis*
  - *Zahlen mit gleichem absoluten Betrag*
  - *...*

Mathematische Beweise

Direkte und indirekte Beweise

Induktionsbeweise

Direkte Beweise

- **Mathematische Sätze** sagen aus, dass unter gewissen
  - **Voraussetzungen** (Liste von Aussagen $A_1, A_2, \ldots, A_k$)
  - eine **Behauptung** (Aussage B)

  gilt.
- **Direkter Beweis**
  - dass die Behauptung aus den Voraussetzungen folgt
  - durch fortgesetzte logische Schlüsse:

$$A_1 \wedge A_2 \wedge \ldots \wedge A_k \Rightarrow \ldots \Rightarrow B$$

Indirekte Beweise

- Hinzunahme der negierten Behauptung zu den Voraussetzungen (**Annahme**)
- Herleiten einer unerfüllbaren Aussage (**Widerspruch**) durch logisches Schließen

$$A_1 \wedge A_2 \wedge \ldots \wedge A_k \wedge \neg B \Rightarrow \ldots \Rightarrow \textbf{false}$$

- *Schema:*
  - **Annahme:** Die Verneinung der Behauptung gilt.
  - Logische Schlüsse bis zu einem Widerspruch.
  - **Die Annahme muss falsch sein, die Behauptung also gelten.**

Vollständige Induktion

- Für Behauptungen über (fast) alle natürlichen Zahlen
- Ist eine Aussage über $\mathbb{N}$ für ein $n_0 \in \mathbb{N}$ wahr und folgt ihre Gültigkeit für jede größere natürliche Zahl aus der Gültigkeit für ihren Vorgänger, dann gilt die Aussage für alle natürlichen Zahlen $n \geq n_0$.

$$[\, B(n_0) \wedge (\forall\, n \geq n_0.\ (B(n) \Rightarrow B(n+1)))\,] \Rightarrow \forall\, n \geq n_0.\ B(n)$$

Induktions-anfang (IA)

Induktions-vorausstzg.

Induktions-behauptung

---- Induktionsschritt (IS) ----

Beispielbeweis

Satz. *Für alle $n \geq 1$ gibt es genau 2^n verschiedene Folgen der Länge n von Binärziffern.*

Beweis (VI nach n):

IA ($n = 1$): Es gibt genau die $2^1 = 2$ Folgen 0 und 1.

IS ($n \to n+1$):

- Nach IV gibt es genau 2^n verschiedene Folgen w der Länge n.
- Für jedes w der Länge n gibt es genau die Folgen $w0$ und $w1$ der Länge $n+1$.
- Somit gibt es genau $2^n + 2^n = 2^{n+1}$ verschiedene Folgen der Länge $n+1$.

Verallgemeinerte Induktion

- Lässt sich eine Aussage über natürliche Zahlen (ab n_0) für jede natürliche Zahl aus der Gültigkeit der Aussage für alle kleineren natürlichen Zahlen (ab n_0) ableiten, so gilt die Aussage für alle natürlichen Zahlen (ab n_0).
- *Beispiel:*
  Sei $fib: \mathbb{N} \to \mathbb{N}$ die Fibonacci-Funktion mit
  $fib(0) = fib(1) = 1$ und $fib(n) = fib(n\text{-}2) + fib(n\text{-}1)$ für $n \geq 2$.
- **Satz.** *Für alle* $n \in \mathbb{N}$ *gilt* $fib(n) \leq 2^n$.
- Für $n \leq 1$: $fib(0) = 1 \leq 2^0$ und $fib(1) = 1 \leq 2^1$.
- Für $n > 1$: $fib(n) = fib(n\text{-}2) + fib(n\text{-}1) \leq 2^{n-2} + 2^{n-1} \leq 2^n$.

  nach IV