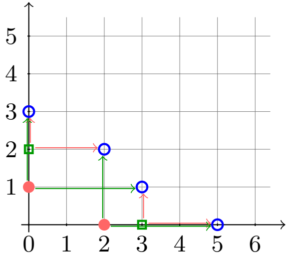
Beispiel 1

Polynome als Funktionen (mit Ableitung, Tangenten, ...) sind nicht unbedingt Stoff der Diskreten Mathematik; ein Beispiel für eine diskrete Betrachtung sind dagegen die sogenannten *Newton-Polytope*:

$$\begin{array}{ll}
y - x^2: & y^2 + x^3: \\
& \\
+y \mapsto (1,0,1) & +y^2 \mapsto (1,0,2) \\
-x^2 \mapsto (-1,2,0) & +x^3 \mapsto (1,3,0)
\end{array}$$

Die Monome über $\{x, y\}$ werden also als (Faktor, x-Potenz, y-Potenz) dargestellt.

Beispiel 2



Die blauen Kreise entstehen durch Vektoraddition der grünen Quadrate und der roten Punkte und stellen die Polytope des Produkts

$$\left(y - x^2\right)\left(y^2 + x^3\right) = y^3 + yx^3 - y^2x^2 - x^5$$

dar (Minkowski-Addition).

3. Komplexität: Ein warnendes Beispiel

$$
\begin{aligned}
(k+2)\cdot\Big(1 \quad &- \quad \big(wz+h+j-q\big)^2 \\
&- \quad \big((gk+2g+k+1)(h+j)+h-z\big)^2 \\
&- \quad \big(2n+p+q+z-e\big)^2 \\
&- \quad \big(16(k+1)^3(k+2)(n+1)^2+1-f^2\big)^2 \\
&- \quad \big(e^3(e+2)(a+1)^2+1-o^2\big)^2 \\
&- \quad \big((a^2-1)y^2+1-x^2\big)^2 \\
&- \quad \big(16r^2y^4(a^2-1)+1-u^2\big)^2 \\
&- \quad \big(n+l+v-y\big)^2 \\
&- \quad \Big(\big((a+u^2(u^2-a))^2-1\big)\big(n+4dy\big)^2+1-\big(x+cu\big)^2\Big)^2
\end{aligned}
$$

$$
\begin{aligned}
&- \Big((a^2-1)l^2+1-m^2\Big)^2\\
&- \Big(q+y(a-p-1)+s\big(2ap+2a-p^2-2p-2\big)-x\Big)^2\\
&- \Big(z+pl\big(a-p\big)+t\big(2ap-p^2-1\big)-pm\Big)^2\\
&- \Big(ai+k+1-l-i\Big)^2\\
&- \Big(p+l\big(a-n-1\big)+b\big(2an+2a-n^2-2n-2\big)-m\Big)^2\ \Bigg)
\end{aligned}
$$

Die positiven Werte, die dieses Polynom mit $(a,\ldots,z)\in\mathbb{N}_0{}^{26}$ annimmt, sind genau alle Primzahlen.
Deshalb empfiehlt sich oft die Verwendung eines symbolischen Mathematikprogramms, z. B. Maple.

4. Mathematische und notationelle Grundlagen

4.1 Mengen

Beispiel 3

$$A_1 = \{2, 4, 6, 8\};$$
$$A_2 = \{0, 2, 4, 6, \ldots\} = \{n \in \mathbb{N}_0; n \text{ gerade}\}$$

Bezeichnungen:

$x \in A \Leftrightarrow A \ni x$	x Element A
$x \notin A$	x nicht Element A
$B \subseteq A$	B Teilmenge von A
$B \subsetneq A$	B echte Teilmenge von A
$\emptyset$	leere Menge, dagegen:
$\{\emptyset\}$	Menge mit leerer Menge als Element

Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \ldots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
- $\mathbb{Z} =$ Menge der ganzen Zahlen
- $\mathbb{Q} =$ Menge der Brüche (rationalen Zahlen)
- $\mathbb{R} =$ Menge der reellen Zahlen
- $\mathbb{C} =$ Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ Restklassen bei Division durch n
- $[n] = \{1, 2, \ldots, n\}$

Operationen auf Mengen:

- $|A|$ Kardinalität der Menge A
- $A \cup B$ Vereinigungsmenge
- $A \cap B$ Schnittmenge
- $A \setminus B$ Differenzmenge
- $A \vartriangle B := (A \setminus B) \cup (B \setminus A)$ symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$ kartesisches Produkt
- $A \uplus B$ Disjunkte Vereinigung: die Elemente werden nach ihrer Herkunft unterschiedlich gekennzeichnet
- $\bigcup_{i=0}^{n} A_i$ Vereinigung der Mengen $A_0, A_1, \ldots, A_n$
- $\bigcap_{i \in I} A_i$ Schnittmenge der Mengen A_i mit $i \in I$
- $\mathsf{P}(M) := 2^M := \{N; N \subseteq M\}$ Potenzmenge der Menge M

Beispiel 4

Für $M = \{a, b, c, d\}$ ist

$$
\begin{array}{rcll}
P(M) & = & \{ & \emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \\
 & & & \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \\
 & & & \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \\
 & & & \{a, b, c, d\} \\
 & & \} &
\end{array}
$$

Satz 5

Die Menge M habe n Elemente, $n \in \mathbb{N}$. Dann hat $P(M)$ 2^n Elemente!

Beweis:

Sei $M = \{a_1, \ldots, a_n\}$, $n \in \mathbb{N}$. Um eine Menge $L \in P(M)$ (d.h. $L \subseteq M$) festzulegen, haben wir für jedes $i \in [n]$ die (unabhängige) Wahl, a_i zu L hinzuzufügen oder nicht. Damit ergeben sich $2^{|[n]|} = 2^n$ verschiedene Möglichkeiten. $\square$

Bemerkungen:

1. Der obige Satz gilt auch für $n = 0$, also die leere Menge $M = \emptyset$.
2. Die leere Menge ist in jeder Menge als Teilmenge enthalten.
3. $P(\emptyset)$ enthält als Element genau $\emptyset$ (also $P(\emptyset) \neq \emptyset$).

4.2 Relationen und Abbildungen

Seien $A_1, A_2, \ldots, A_n$ Mengen. Eine Relation über $A_1, \ldots, A_n$ ist eine Teilmenge

$$R \subseteq A_1 \times A_2 \times \ldots \times A_n = \bigtimes_{i=1}^{n} A_i$$

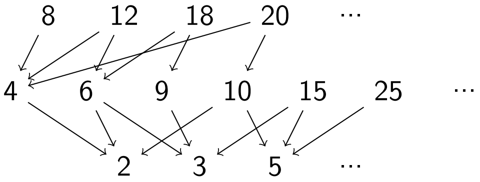
Andere Schreibweise (Infixnotation) für $(a, b) \in R$: aRb.

Eigenschaften von Relationen ($R \subseteq A \times A$):

- reflexiv: $(a, a) \in R \quad \forall a \in A$
- symmetrisch: $(a, b) \in R \Rightarrow (b, a) \in R \quad \forall a, b \in A$
- asymmetrisch: $(a, b) \in R \Rightarrow (b, a) \notin R \quad \forall a, b \in A$
- antisymmetrisch: $\big[(a, b) \in R \wedge (b, a) \in R\big] \Rightarrow a = b \quad \forall a, b \in A$
- transitiv: $\big[(a, b) \in R \wedge (b, c) \in R\big] \Rightarrow (a, c) \in R \quad \forall a, b, c \in A$
- Äquivalenzrelation: reflexiv, symmetrisch und transitiv
- Partielle Ordnung (aka *partially ordered set, poset*): reflexiv, antisymmetrisch und transitiv

Beispiel 6

$(a, b) \in R$ sei $a|b$ „a teilt b“, $a, b \in \mathbb{N} \setminus \{1\}$.
Die graphische Darstellung ohne reflexive und transitive Kanten heißt Hasse-Diagramm:



Im Diagramm wird $a|b$ durch einen Pfeil $b \longrightarrow a$ dargestellt.
Die Relation $|$ stellt eine *partielle Ordnung* dar.

Definition 7

Sei $R \subseteq A \times B$ eine binäre Relation. Dann heißt

$$\{a \in A;\ (\exists b \in B)[(a,b) \in R]\}$$

das Urbild der Relation R und

$$\{b \in B;\ (\exists a \in A)[(a,b) \in R]\}$$

das Bild der Relation R.

Definition 8

Sei $R \subseteq A \times B$ eine binäre Relation. Dann heißt

$$R^{-1} := \{(b,a);\ (a,b) \in R\}$$

die inverse (oder auch konverse) Relation zu R.

Definition 9

Seien $R \subseteq A \times B$ und $S \subseteq B \times C$ binäre Relationen. Dann heißt

$$R \circ S := \{(a, c) \in A \times C;\ (\exists b \in B)[(a, b) \in R \text{ und } (b, c) \in S]\}$$

das Produkt der Relationen R und S. Es wird oft auch einfach durch RS bezeichnet.

Satz 10

Das Relationenprodukt $\circ$ ist assoziativ und distributiv über $\cup$ und $\cap$.

Beweis:

Hausaufgabe! $\square$