Surjektive, injektive und bijektive Funktionen.

Definition. Sei $f : M \to N$ eine Funktion.

Dann heißt f **surjektiv**, falls die Gleichung $f(x) = y$ für jedes $y \in N$ mindestens eine Lösung $x \in M$ besitzt, d.h.

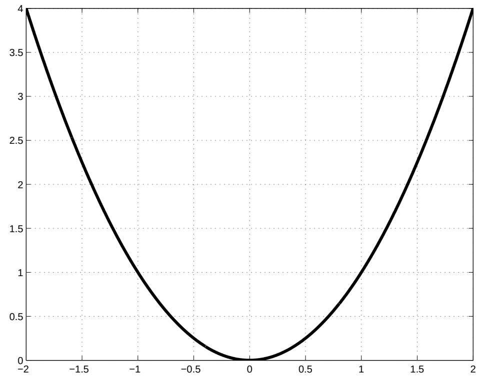
$$\forall y \in N \quad \exists x \in M : y = f(x).$$

Weiterhin heißt f **injektiv**, falls die Gleichung $f(x) = y$ für $y \in N$ höchstens eine Lösung $x \in M$ besitzt, d.h.

$$\forall x_1, x_2 \in M : f(x_1) = f(x_2) \quad \Longrightarrow \quad x_1 = x_2.$$

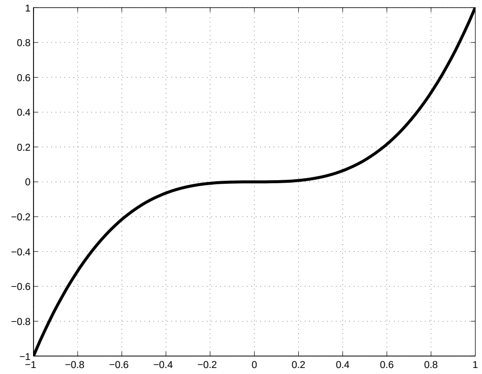
Schließlich heißt f **bijektiv**, falls f injektiv und surjektiv ist. $\square$

Beispiele.



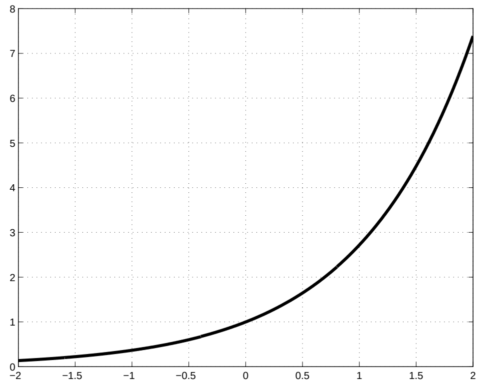
$f : \mathbb{R} \to [0, \infty)$, $f(x) = x^2$

surjektiv, nicht injektiv.



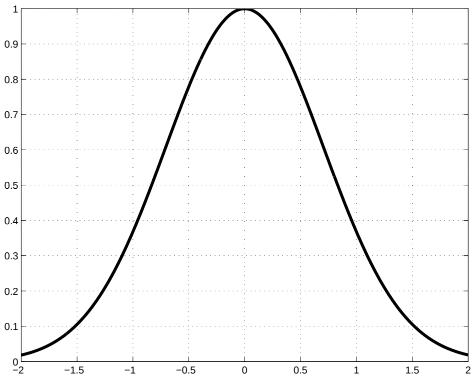
$f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$

bijektiv.



$f : \mathbb{R} \to [0, \infty)$, $f(x) = \exp(x)$

injektiv, nicht surjektiv.



$f : \mathbb{R} \to [0, \infty)$, $f(x) = \exp(-x^2)$

weder injektiv noch surjektiv.

Bemerkungen.

- Eine injektive Funktion $f: M \to N$ lässt sich *invertieren*, denn zu jedem $y \in f(M)$ existiert *genau ein* $x \in M$ mit $y = f(x)$.

- Für eine injektive Funktion $f: M \to N$ wird deren `Umkehrfunktion` $f^{-1}: f(M) \to M$ definiert durch

$$f^{-1}(y) = x \quad \text{für } y \in f(M), \text{ wobei } f(x) = y.$$

- Falls $f: M \to N$ bijektiv ist, so gilt $f(M) = N$ und $f^{-1}(N) = M$, d.h.

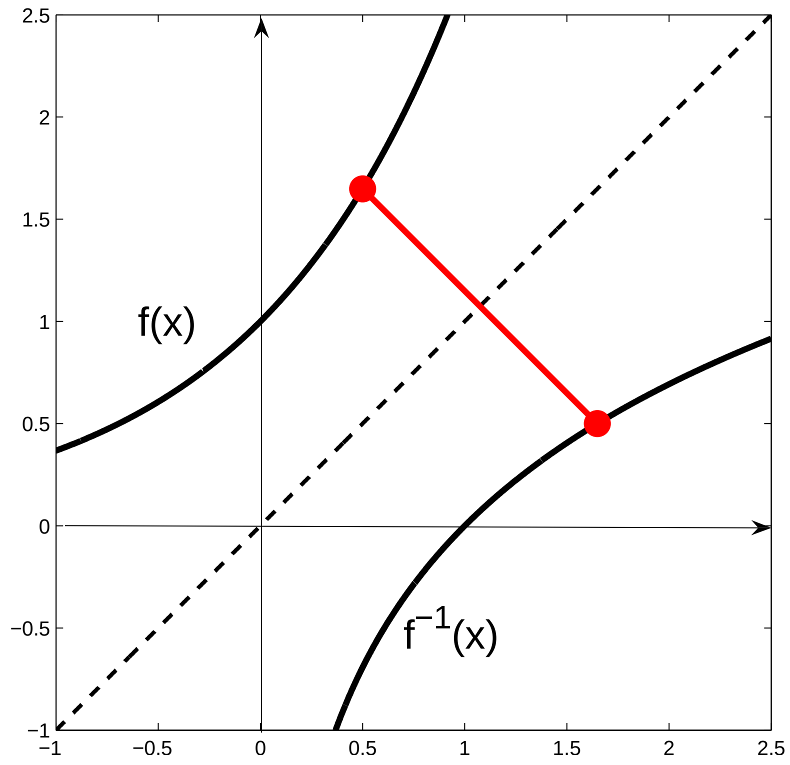
$$M \xrightarrow{f} N \quad \text{und} \quad N \xrightarrow{f^{-1}} M.$$

Beispiel.

- $f: [0,1] \to [0,1]$, definiert durch $f(x) = x^2$.
- $f^{-1}: [0,1] \to [0,1]$ mit $f^{-1}(x) = \sqrt{x}$.
- Dann: $f^{-1}(f(x)) = f^{-1}(x^2) = \sqrt{x^2} = x$ für alle $x \in [0,1]$.
- Ebenso: $f(f^{-1}(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x$ für alle $x \in [0,1]$.

Bemerkung und Beispiel.

Sei $f : M \to N$ eine reellwertige injektive Funktion einer reellen Variablen, d.h. $M, N \subset \mathbb{R}$. Dann erhält man den Graphen der Umkehrfunktion f^{-1} aus dem Graphen von f durch Spiegelung an der Diagonalen $x = y$.



Konstruktion der Umkehrfunktion.

Komposition von Funktionen.

Definition: Seien $f : M \longrightarrow N$ und $g : N \longrightarrow P$ Funktionen. Dann ist die Komposition $g \circ f$ von f und g eine Funktion, definiert durch

$$g \circ f : M \longrightarrow P \qquad (g \circ f)(x) = g(f(x)), \qquad \text{für } x \in M.$$

$$M \quad \xrightarrow{f} \quad N \quad \xrightarrow{g} \quad P$$

$$M \quad \xrightarrow{g \circ f} \quad P$$

Eigenschaften von Kompositionen.

- Assoziativität. Für Funktionen $f : M \longrightarrow N, g : N \longrightarrow P, h : P \longrightarrow Q$ gilt

$$h \circ (g \circ f) = (h \circ g) \circ f$$

- Kompositionen sind im Allgemeinen nicht kommutativ, d.h.

$$g \circ f \neq f \circ g.$$

Gegenbeispiel: Seien $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ Funktionen, definiert durch

$$\begin{aligned} f(x) &= x^2 + 2x, \\ g(x) &= x + 1. \end{aligned}$$

Dann folgt

$$\begin{aligned} (g \circ f)(x) &= g(x^2 + 2x) = x^2 + 2x + 1 = (x + 1)^2, \\ (f \circ g)(x) &= f(x + 1) = (x + 1)^2 + 2(x + 1) = x^2 + 4x + 3, \end{aligned}$$

und somit gilt $g \circ f \neq f \circ g$.

Die symmetrische Gruppe.

Definition: Sei M eine nichtleere Menge. Dann heißt die Menge

$$S(M) = \{f : M \to M \mid f \text{ bijektiv } \}$$

die symmetrische Gruppe von M. Die symmetrische Gruppe $S(M)$ enthält die Identität $\mathrm{id}_M : M \to M$, definiert durch $\mathrm{id}_M(x) = x$ für alle $x \in M$. □

Die symmetrische Gruppe $S(M)$ von M erfüllt die Gruppenaxiome.

(G1) Es gilt das Assoziativgesetz

$$h \circ (g \circ f) = (h \circ g) \circ f \qquad \text{für alle } f, g, h \in S(M).$$

(G2) Die Identität id_M ist das neutrale Element in $S(M)$, d.h. es gilt

$$f \circ \mathrm{id}_M = \mathrm{id}_M \circ f = f \qquad \text{für alle } f \in S(M).$$

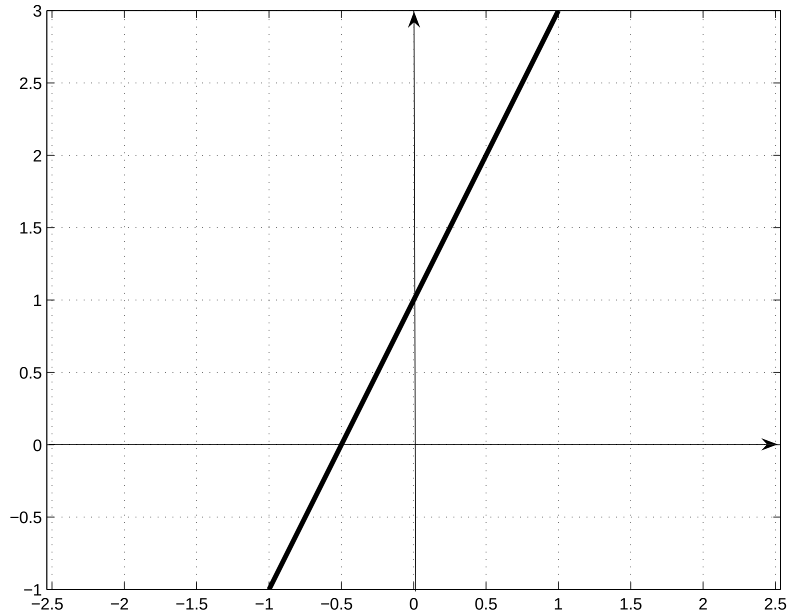
(G3) Jede Funktion $f \in S(M)$ besitzt ein Inverses $f^{-1} \in S(M)$ mit

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_M \qquad \text{für alle } f \in S(M).$$

Elementare reelle Funktionen.

- Affin-lineare Funktionen:

$$f(x) = a_1 x + a_0 \qquad \text{für } a_0, a_1 \in \mathbb{R}.$$

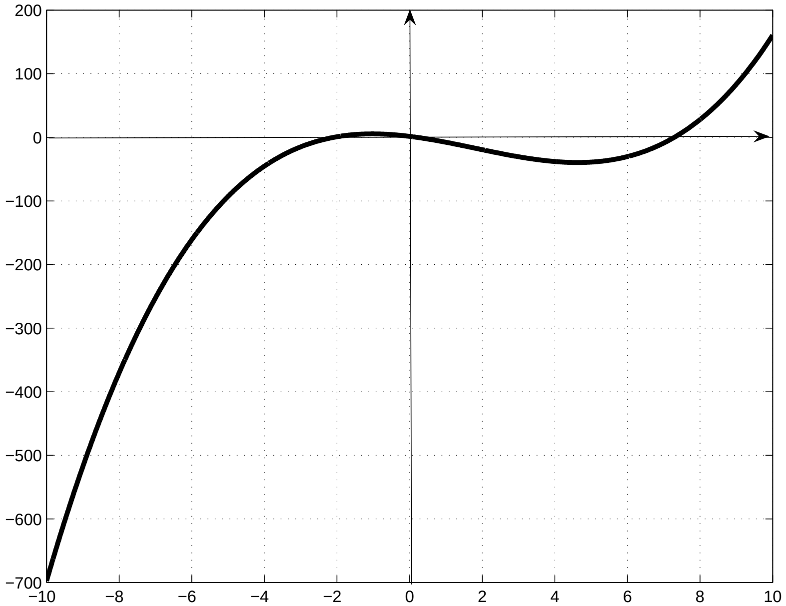


Die affin-lineare Funktion

$$f(x) = 2x + 1.$$

- **Polynome**:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \qquad \text{für } a_0, \ldots, a_n \in \mathbb{R} \text{ mit } a_n \neq 0.$$



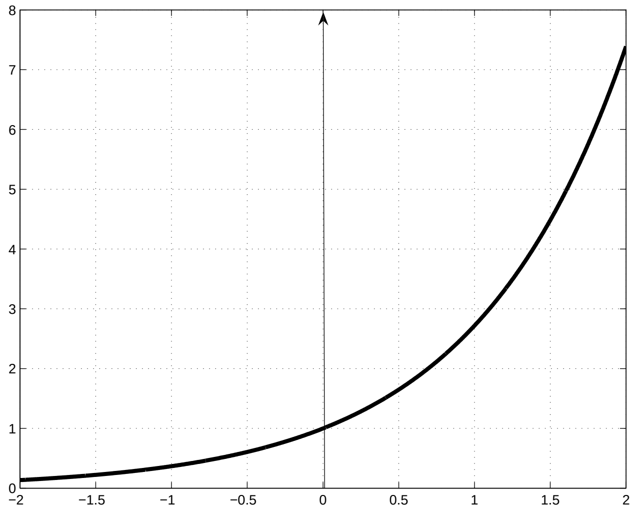
Das kubische Polynom

$$f(x) = 0.5x^3 - 2.7x^2 - 7.1x + 1.5.$$

• Die Exponentialfunktion: $f(x) = a^x$ für Basis $a \in \mathbb{R}$.

Spezialfall: Basis e, wobei die Eulersche Zahl e definiert ist durch

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = 2.718281828459045235 3\ldots$$



Die Exponentialfunktion $f(x) = \exp(x) = e^x$.

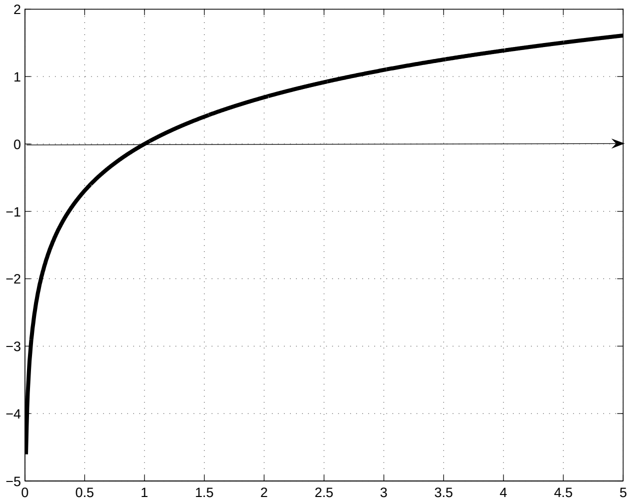
Es gilt die *Funktionalgleichung*

$$a^{x+y} = a^x \cdot a^y \qquad \text{für alle } x, y \in \mathbb{R}.$$

- Der Logarithmus, Umkehrfunktion der (injektiven) Exponentialfunktion,

$$f(x) = \log_a(x) : (0, \infty) \to \mathbb{R} \qquad \text{für Basis } a > 0.$$

Spezialfall: Basis e, $\log(x) = \log_e(x)$, der natürliche Logarithmus.



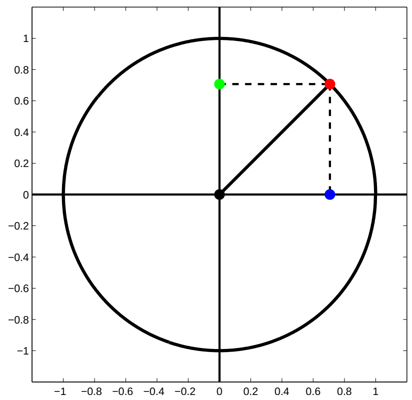
Der natürliche Logarithmus $f(x) = \log(x)$.

Es gilt die *Funktionalgleichung*

$$\log_a(x \cdot y) = \log_a(x) + \log_a(y) \qquad \text{für alle } x, y > 0.$$

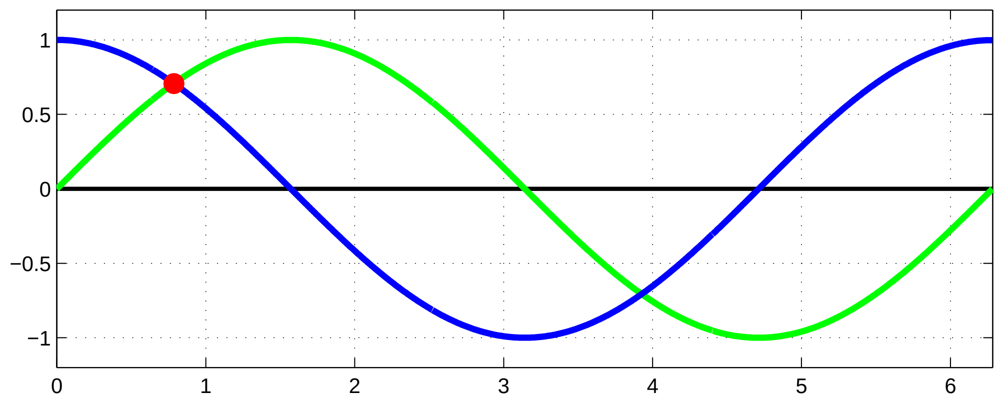
Trigonometrische Funktionen.

$$\begin{aligned} \sin &: [0, 2\pi) \to [-1, 1] \quad (\texttt{Sinus}) \\ \cos &: [0, 2\pi) \to [-1, 1] \quad (\texttt{Cosinus}) \end{aligned}$$



Der Einheitskreis.

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$$



$$\sin : [0, 2\pi) \to [-1, 1];$$

$$\cos : [0, 2\pi) \to [-1, 1].$$

Eigenschaften trigonometrischer Funktionen.

- Für alle $\varphi \in [0, 2\pi)$ gilt

$$\sin^2(\varphi) + \cos^2(\varphi) = 1.$$

- Symmetrie:

$$\begin{aligned} \sin(-\varphi) &= -\sin(\varphi) \qquad \text{für alle } \varphi \in [0, 2\pi) \\ \cos(-\varphi) &= \cos(\varphi) \qquad \text{für alle } \varphi \in [0, 2\pi) \end{aligned}$$

- Periodizität:

$$\begin{aligned} \sin(\varphi) &= \sin(\varphi + 2\pi) \\ \cos(\varphi) &= \cos(\varphi + 2\pi) \end{aligned}$$

somit sind Sinus und Cosinus auf ganz $\mathbb{R}$ definiert,

$$\sin : \mathbb{R} \to [-1, 1] \quad \text{und} \quad \cos : \mathbb{R} \to [-1, 1].$$

Weitere Eigenschaften trigonometrischer Funktionen.

- Wertetafel:

φ	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
$\sin\varphi$	0	$1/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	1
$\cos\varphi$	1	$\sqrt{3}/2$	$\sqrt{2}/2$	$1/2$	0

- Additionstheoreme: Für alle $\alpha, \beta \in \mathbb{R}$ gilt

$$
\begin{aligned}
\cos(\alpha+\beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta \\
\sin(\alpha+\beta) &= \sin\alpha\cos\beta + \cos\alpha\sin\beta
\end{aligned}
$$

2 Zahlenbereiche

2.1 Natürliche Zahlen

Die Menge

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

der natürlichen Zahlen wird formal durch die Peano-Axiome definiert:

(A1) $1 \in \mathbb{N}$;

(A2) $n \in \mathbb{N} \Longrightarrow n+1 \in \mathbb{N}$ für alle $n \in \mathbb{N}$;

(A3) $n \neq m \Longrightarrow n+1 \neq m+1$ für alle $n, m \in \mathbb{N}$;

(A4) $n \in \mathbb{N} \Longrightarrow n+1 \neq 1$ für alle $n \in \mathbb{N}$;

(A5) Für $A \subset \mathbb{N}$ gilt das Vollständigkeitsaxiom:

$$1 \in A \wedge (\forall n : [n \in A \Rightarrow (n+1) \in A]) \qquad \Longrightarrow \qquad A = \mathbb{N}.$$

Bemerkung: Die *Nachfolgeabbildung* $n \mapsto n+1$ ist injektiv.

Beweisprinzip der vollständigen Induktion.

Dabei ist die Gültigkeit einer Aussage $A(n)$ für alle $n \in \mathbb{N}$ zu beweisen, d.h. es ist zu zeigen

$$\forall n \in \mathbb{N} : A(n),$$

wobei $A(n)$ eine Aussageform ist, die von $n \in \mathbb{N}$ abhängt.

Beweisschritte der vollständigen Induktion.

(I1) Induktionsanfang: $n = 1$
Zeige $A(1)$;

(I2) Induktionsannahme:
Es gelte $A(n)$;

(I3) Induktionsschluss: $n \to n + 1$
Zeige die Implikation $A(n) \Longrightarrow A(n + 1)$.

Falls Schritte **(I1)-(I3)** durchführbar, so gilt die Aussage $A(n)$ für alle $n \in \mathbb{N}$.

Beispiel 1.

Bestimme die Anzahl t_n der Teilmengen einer n-elementigen Menge

$$A_n = \{a_1, \ldots, a_n\}.$$

Vorgehen: Betrachte zunächst kleine $n \in N$, z.B. $n = 1, 2, 3$.

- $n = 1$: Die Menge $A_1 = \{a_1\}$ besitzt nur die Teilmengen $\emptyset, \{a_1\}$.
  Somit $t_1 = 2$.

- $n = 2$: Die Menge $A_2 = \{a_1, a_2\}$ besitzt die vier Teilmengen

$$\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\},$$

  und somit gilt $t_2 = 4$.

- $n = 3$: Die Menge $A_3 = \{a_1, a_2, a_3\}$ besitzt $t_3 = 8$ Teilmengen.

Vermutung: Es gilt $t_n = 2^n$ für alle $n \in \mathbb{N}$.

Satz: *Eine n-elementige Menge $A_n = \{a_1, \ldots, a_n\}$ besitzt $t_n = 2^n$ Teilmengen.*

Beweis: durch vollständige Induktion über n.

- Induktionsanfang ($n = 1$): Es gilt $t_1 = 2 = 2^1$.
- Induktionsannahme: Es gelte $t_n = 2^n$ für $n \in \mathbb{N}$.
- Induktionsschluss ($n \to n + 1$):

Zu zeigen: $A_{n+1} = \{a_1, \ldots, a_n, a_{n+1}\}$ hat $t_{n+1} = 2^{n+1}$ Teilmengen.

Schreibe $\mathcal{P}(A) = K_1 \cup K_2$ für die Potenzmenge von A_{n+1}, wobei

$$
\begin{aligned}
T \in K_1 \quad &\Longleftrightarrow \quad a_{n+1} \notin T \\
T \in K_2 \quad &\Longleftrightarrow \quad a_{n+1} \in T
\end{aligned}
$$

Nach Induktionsannahme besitzt K_1 genau $t_n = 2^n$ Elemente.

Ebenso besitzt K_2 nach Induktionsannahme $t_n = 2^n$ Elemente.

Weiterhin gilt $K_1 \cap K_2 = \emptyset$ nach Konstruktion.

Somit hat $\mathcal{P}(A)$ insgesamt $t_{n+1} = t_n + t_n = 2^n + 2^n = 2^{n+1}$ Elemente. ■

Beispiel 2.

Bestimme die Anzahl p_n der verschiedenen Anordnungen (Permutationen) für die Elemente einer n-elementigen Menge $A_n = \{1, \ldots, n\}$.

Vorgehen: Betrachte zunächst kleine $n \in N$, z.B. $n = 1, 2, 3$.

- $n = 1$: Das Element in $A_1 = \{1\}$ besitzt nur eine Anordnung, (1).
  Somit $p_1 = 1$.
- $n = 2$: Für die Elemente in $A_2 = \{1, 2\}$ gibt es zwei Anordnungen,
  $$(1, 2), (2, 1).$$
  Somit gilt $p_2 = 2$.
- $n = 3$: Für die Elemente in $A_3 = \{1, 2, 3\}$ gibt es sechs Anordnungen,
  $$(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1).$$
  Somit gilt $p_3 = 6$.

Vermutung: Es gilt $p_n = n! := 1 \cdot 2 \cdot \ldots \cdot n$ für alle $n \in \mathbb{N}$.

Satz: *Es gibt* $p_n = n!$ *Permutationen für das* n*-tupel* $(1, 2, \ldots, n)$.

Beweis: durch vollständige Induktion über n.

- Induktionsanfang $(n = 1)$: Es gilt $p_1 = 1$.
- Induktionsannahme: Es gelte $p_n = n!$ für $n \in \mathbb{N}$.
- Induktionsschluss $(n \to n + 1)$:

Es gibt nach Induktionsannahme je $n!$ Permutationen für die $(n + 1)$-Tupel

$$\left\{ \begin{array}{c} (i_1, i_2, \ldots, i_{n-1}, i_n, n+1), \\ (i_1, i_2, \ldots, i_{n-1}, n+1, i_n), \\ \vdots \\ (i_1, n+1, i_2, \ldots, i_{n-1}, i_n), \\ (n+1, i_1, i_2, \ldots, i_{n-1}, i_n) \end{array} \right\} \quad i_1, \ldots, i_n \in \{1, \ldots, n\} \text{ paarweise verschieden.}$$

und somit gilt $p_{n+1} = \underbrace{n! + \ldots + n!}_{(n+1)\text{-fach}} = (n + 1) \cdot n! = (n + 1)!$ ■

Folgerung: Eine n-elementige Menge $\{a_1, \ldots, a_n\}$ besitzt genau

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}, \qquad \text{für } n, m \in \mathbb{N}_0 : 0 \le m \le n,$$

m-elementige Teilmengen. Dabei setzt man $0! = 1$.

Beweis: Es gibt $n!$ Permutationen von $(a_1, \ldots, a_n)$, bezeichnet mit

$$(a_{i_1}, \ldots, a_{i_n}), \qquad \text{wobei } \{i_1, \ldots, i_n\} = \{1, \ldots, n\}.$$

Betrachte nun die ersten m Plätze in $(a_{i_1}, \ldots, a_{i_n})$. Die $n!$ möglichen Permutationen

$$(a_{i_1}, \ldots, a_{i_m}, a_{i_{m+1}}, \ldots, a_{i_n})$$

von $(a_1, \ldots, a_n)$ führen genau $m!(n-m)!$-mal auf die gleiche Teilmenge

$$\{a_{i_1}, \ldots, a_{i_m}\} \subset \{a_1, \ldots, a_n\},$$

denn die $m!$ Permutationen der ersten m Plätze und die $(n-m)!$ Permutationen der restlichen $n-m$ Plätze verändern $\{a_{i_1}, \ldots, a_{i_m}\}$ nicht. Somit gibt es $\frac{n!}{m!(n-m)!} = \binom{n}{m}$ m-elementige Teilmengen von $\{a_1, \ldots, a_n\}$. ■

Einschub: Summen, Produkte und Potenzen.

Allgemeine Summen und Produkte.

$$\sum_{k=m}^{n} b_k \quad := \quad b_m + b_{m+1} + \cdots + b_n \quad \text{(falls } m \leq n\text{)}$$

$$\sum_{k=m}^{n} b_k \quad := \quad 0 \quad \text{(falls } m > n\text{, leere Summe)}$$

$$\prod_{k=m}^{n} b_k \quad := \quad b_m \cdot b_{m+1} \cdot \ldots \cdot b_n \quad \text{(falls } m \leq n\text{)}$$

$$\prod_{k=m}^{n} b_k \quad := \quad 1 \quad \text{(falls } m > n\text{, leeres Produkt)}$$

Einschub: Summen, Produkte und Potenzen.

Potenzen.

$$a^n := \begin{cases} \prod_{k=1}^{n} a & \text{für } n \geq 0 \\ 1/(a^{-n}) & \text{für } n < 0 \end{cases}$$

Potenzgesetze.

$$\begin{aligned} a^n \cdot a^m &= a^{n+m} \\ (a^n)^m &= a^{n \cdot m} \end{aligned}$$

Binomialkoeffizienten und deren Eigenschaften.

Definition: *Die Zahlen* $\binom{n}{m}$ *heißen* Binomialkoeffizienten.

Satz:

(a) Für $n, m \in \mathbb{N}$ mit $0 < m \leq n$ gilt die Rekursionsformel

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1},$$

wobei

$$\binom{n}{0} = \binom{n}{n} = 1.$$

(b) Für $n \in \mathbb{N}_0$ und $a, b \in \mathbb{R}$ gilt der Binomische Lehrsatz

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Beweis von Teil (a): Es gilt

$$\begin{aligned}
\binom{n}{m} + \binom{n}{m-1} &= \frac{n!}{m!(n-m)!} + \frac{n!}{(m-1)!(n-m+1)!} \\
&= \frac{n!(n+1-m) + n!m}{m!(n+1-m)!} \\
&= \frac{n!(n+1-m+m)}{m!(n+1-m)!} \\
&= \frac{(n+1)!}{m!(n+1-m)!} \\
&= \binom{n+1}{m}.
\end{aligned}$$

$\blacksquare$

Beweis von Teil (b): durch vollständige Induktion über n.

- Induktionsanfang ($n = 0$): Es gilt

$$(a+b)^0 = \binom{0}{0} a^0 b^0 = 1.$$

- Induktionsannahme: Für $n \geq 0$ gelte

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

- Induktionsschluss ($n \to n+1$):

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \binom{n}{0}a^0 b^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]a^k b^{n+1-k} + \binom{n}{n}a^{n+1}b^0 \\
&= \binom{n+1}{0}a^0 b^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k} + \binom{n+1}{n+1}a^{n+1}b^0 \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}
$$

$\blacksquare$

Direkte Berechnung der Binomialkoeffizienten.

Für $n, m \in \mathbb{N}_0$ mit $m \leq n$ gilt

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

Klassisches Beispiel: Zahlenlotto.

Es gibt

$$\binom{49}{6} = \frac{49!}{6!43!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13983816$$

Möglichkeiten, aus einer 49-elementigen Menge eine 6-elementige Teilmenge auszuwählen.

Mit anderen Worten: Die Wahrscheinlichkeit, beim (klassischen) Zahlenlotto "6 aus 49" die 6 richtigen Zahlen zu tippen, beträgt

$$\frac{1}{\binom{49}{6}} = \frac{1}{13983816} = 0.0000000715112384201851 6\ldots$$

Rekursive Berechnung der Binomialkoeffizienten.

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
$$

Pascalsches Dreieck.

Beispiel:

$$
\begin{aligned}
(a+b)^5 &= 1 \cdot a^0 b^5 + 5 \cdot a^1 b^4 + 10 \cdot a^2 b^3 + 10 \cdot a^3 b^2 + 5 \cdot a^4 b^1 + 1 \cdot a^5 b^0 \\
&= a^5 + 5a^4 b + 10a^3 b^2 + 10a^2 b^3 + 5ab^4 + b^5
\end{aligned}
$$

2.2 Primzahlen

Definition: *Eine natürliche Zahl* $m \in \mathbb{N}$ *heißt* Teiler *von* $n \in \mathbb{N}$, *falls ein* $k \in \mathbb{N}$ *existiert mit*

$$n = k \cdot m.$$

Man schreibt dann auch $m|n$. □

Jede Zahl $n \in \mathbb{N}$ besitzt offensichtlich die beiden Teiler 1 und n, denn es gilt stets

$$n = n \cdot 1 = 1 \cdot n$$

Existiert für $n > 1$ *kein* weiterer Teiler, so nennt man n eine Primzahl.

Die ersten Primzahlen lauten

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Bemerkung: Es gibt unendlich viele Primzahlen. ■

Hauptsatz der Zahlentheorie.

Satz: Jede natürliche Zahl $n \in \mathbb{N}$ läßt sich als Produkt von Primzahlpotenzen schreiben,

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k},$$

wobei p_j Primzahl und $r_j \in \mathbb{N}_0$ für $1 \leq j \leq k$.

Beweis: durch Induktion (Übung!) ■

Bemerkung: In der Primzahldarstellung sind die (paarweise verschiedenen) Basen $p_1, \ldots, p_k$ und deren zugehörige Exponenten $r_1, \ldots, r_k$ eindeutig bestimmt. □