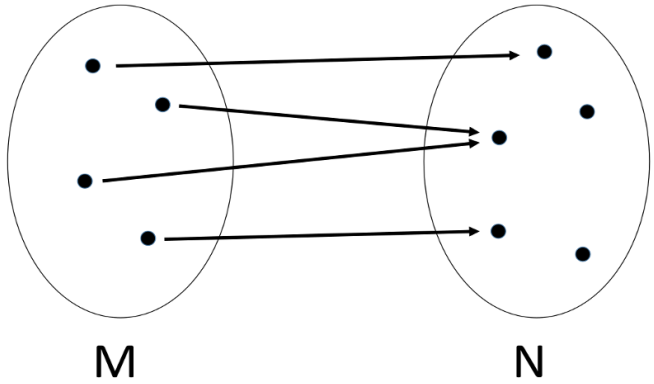
Relationen und Abbildungen

Abbildungen

Abbildungen

Definition:
Seien M und N Mengen. Jedem $x \in M$ wird genau ein $y \in N$ zugeordnet. Diese Zuordnung definiert eine **Abbildung** von M nach N.

Im Grunde genommen ist das ganz einfach. Man sagt jedem Element aus einer Menge, welches andere Element zu ihm dazugehört.



Abbildungen

Schreibweise:
Meistens wird eine Abbildung mit einem Kleinbuchstaben wie f oder g bezeichnet.
Das Element auf das ein $x \in M$ abgebildet wird, wird dann als $f(x)$ bezeichnet.

Insgesamt wird das dann folgendermaßen bezeichnet:
$f : M \to N, x \mapsto f(x)$
Der Pfeil $\to$ wird für Mengen verwendet, $\mapsto$ für die einzelnen Elemente.

Abbildungen

Definitionen:
$D(f) := M$ ist die **Definitionsmenge** von f

$x \in M$ ist das **Argument** von f

$f(M) = \{y \in N |$ es gibt ein $x \in M : y = f(x)\}$ ist die **Bildmenge** von f

Sei $x \in M, y \in N$ und $y = f(x)$,
dann ist y **Bild von x** und x **Urbild von y**.

In der Mathematik muss man sehr genau sein und exakt wissen von was gesprochen wird, deswegen sind all diese Definitionen notwendig!

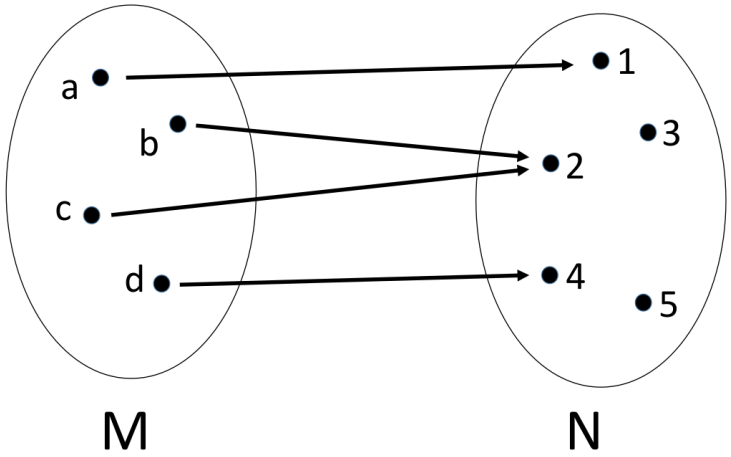
Abbildungen

Definitionen:
Ist $U \subset M$, dann ist die Menge der Bilder von $x \in U$ das **Bild von U.** Dies wird mit $f(U) := \{f(x)|x \in U\}$ bezeichnet.

Ist $V \subset N$, dann ist die Menge der Urbilder von $y \in V$ das **Urbild von V**. Dies wird mit $f^{-1}(V) := \{x \in M|f(x) \in V\}$ bezeichnet.

Abbildungen

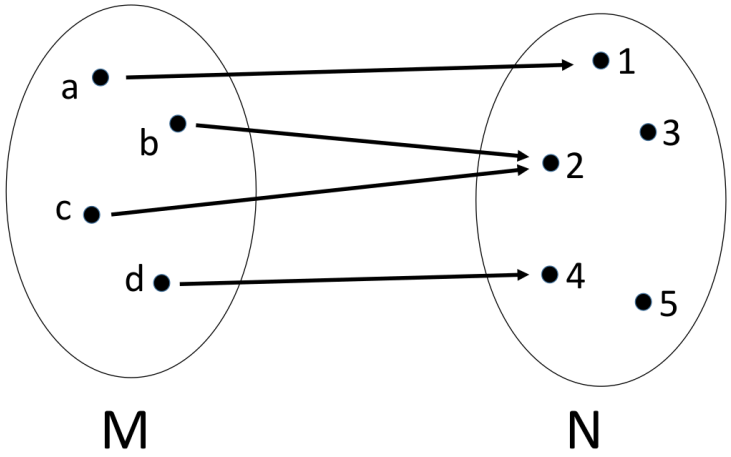
Wir betrachten diese Definitionen anhand eines Beispiels:



Die **Definitionsmenge** ist schlicht M selbst, also die Menge $\{a, b, c, d\}$.
Die **Bildmenge** von f sind diejenige Elemente, die „getroffen“ werden, also $\{1, 2, 4\}$. Betrachten wir a. Das **Bild** von a ist 1. Das **Urbild** von 1 ist a.

Abbildungen

Und nun das Ganze für Mengen:



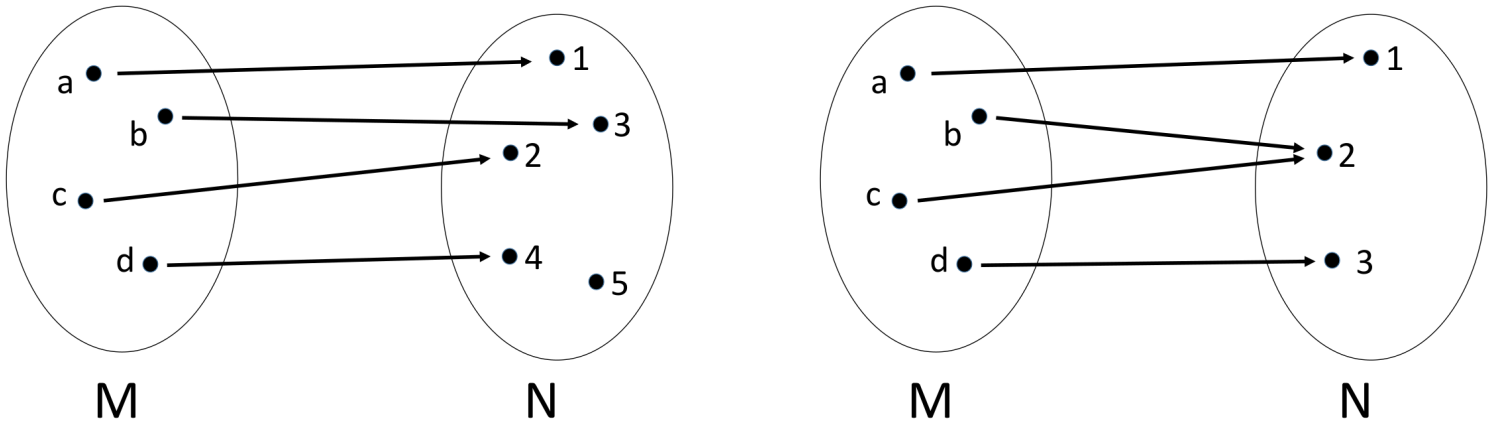
Nehmen wir an wir betrachten die Menge $\{a, b\}$. Das **Bild** davon ist dann $\{1, 2\}$. Allerdings: Das **Urbild** von $\{1, 2\}$ ist $\{a, b, c\}$.

Abbildungen

Definitionen:
Sei $f : M \to N$ eine Abbildung. Dann heißt f:
Injektiv: für alle $x_1, x_2 \in M$ mit $x_1 \neq x_2$ gilt: $f(x_1) \neq f(x_2)$
Surjektiv: für alle $y \in N$ gibt es ein $x \in M$ mit $f(x) = y$
Bijektiv: wenn f injektiv und surjektiv ist

Abbildungen

Beispiele:



Sind diese Beispiele injektiv/surjektiv/bijektiv?

Abbildungen

Beispiele:

- Sei p eine Primzahl, z.B. 5. $h : \mathbb{N}_0 \to 0, 1, 2, ..., p-1$
  $n \longmapsto n \mod p$. Diese Abbildung nennt man *Hashfunktion*.
- Programmiermethode zur Bestimmumg des größten gemeinsamen Teilers zweier ganzer Zahlen
  `int ggt(int m, int n)`,
  in mathematischer Notation $ggt : M \times M \to M, (n, m) \longmapsto ggt(n, m)$,
  mit $M = [-2^{31}, 2^{31} - 1]$

Injektiv, surjektiv, bijektiv?

Abbildungen

Beispiele:

- Die Hashfunktion $h(x) = n \mod p$ ist nicht injektiv, da z.B. $h(0) = h(p)$. Sie ist aber surjektiv, da alle Reste vorkommen. Nicht bijektiv, da nicht injektiv.
- Programmiermethode zur Bestimmung des größten gemeinsamen Teilers zweier ganzer Zahlen ist nicht injektiv, da z. B. $ggt(3, 6) = ggt(9, 12)$. Surjektiv, da alle Zahlen als Teiler vorkommen und $ggt(n, n) = n$. Nicht bijektiv, da nicht injektiv.

Oft ist es einfach, ein Gegenbeispiel zu finden um zu zeigen, dass eine Abbildung nicht injektiv oder nicht surjektiv ist. Versuchen Sie es selbst in Blatt 1, Aufgabe 1! Nicht so einfach, zu zeigen, dass Surjektivität/Injektivität vorliegt.

Umkehrabbildung

Definition:
Ist $f : M \to N, x \longmapsto f(x)$ bijektiv, so wird durch $g : N \to M, y \longmapsto x$ mit $y = f(x)$ eine Abbildung definiert. g heißt Umkehrabbildung zu f, und wird mit f^{-1} notiert.

Abbildungen

Die **Mächtigkeit** einer Menge sagt aus, wie groß eine Menge ist. Bei endlichen Mengen ist das leicht, man zählt einfach die Elemente ab. So hat etwa $M = \{a, b, c, d\}$ die Mächtigkeit $|M| = 4$.

Zwei Mengen M und N haben dieselbe Mächtigkeit, wenn es eine bijektive Abbildung $f : M \to N$ zwischen den Mengen gibt. Man sagt sie haben dieselbe **Kardinalität**.

Unendlich große Mengen, wie $\mathbb{N}$ und $\mathbb{R}$, haben keine endliche Kardinalität. Man sagt, dass $\mathbb{N}$ (und jede dazu bijektive Menge) **abzählbar unendlich** ist. $\mathbb{R}$ hingegen ist **überabzählbar unendlich**.

Abbildungen

Beispiel:
Welche Kardinalität hat $\mathbb{Z}$?

Wir betrachten die Abbildung $f : \mathbb{N}_0 \to \mathbb{Z}$: $0 \longmapsto 0$, $1 \longmapsto 1$, $2 \longmapsto -1$, $3 \longmapsto 2$, $4 \longmapsto -2$, $5 \longmapsto 3$, $6 \longmapsto -3$ usw.
Wir sehen: f ist bijektiv $\Rightarrow$ $\mathbb{Z}$ und $\mathbb{N}$ haben dieselbe Mächtigkeit.

$\Rightarrow$ $\mathbb{Z}$ und $\mathbb{N}$ sind also gleich groß, auch wenn $\mathbb{N}$ eine echte Teilmenge von $\mathbb{Z}$ ist.

Aus der Geschichte der Zahlentheorie

Währinger Straße 33-35

Aus der Geschichte der Zahlentheorie

Frage: Wir kennen abzählbar unendliche Mengen und überabzählbar unendliche Mengen. Gibt es etwas dazwischen?

- **Vermutung von Georg Cantor** (um 1900): Nein.
- **Arbeiten von Kurt Gödel** (1931) und **Paul Cohen** (1963) zeigen: Das ist nicht entscheidbar. Grundaussage: Jedes axiomatische System ist unvollständig. Es gibt wahre Aussagen, die nicht beweisbar sind. (Mathematische Logik)
- **Alan Turing** (1936). Nicht-Entscheidbarkeit des Halteproblems. Gelangt ein Algorithmus zu einem Ende? Das ist nicht für alle möglichen Algorithmen und beliebige Eingaben zu beantworten. (Berechenbarkeitstheorie)
  Aufzählbarkeit – Entscheidbarkeit – Berechenbarkeit
  Weiteres darüber in der VU Theoretische Informatik, 1. Semester Bachelor Informatik

Hintereinanderausführung von Abbildungen

Definition:
Seien $f : M \to N : x \longmapsto f(x)$ und $g : N \to S : y \longmapsto g(y)$ Abbildungen. Dann ist auch $h : M \to S : x \longmapsto g(f(x))$ eine Abbildung. Sie wird mit $h = g \circ f$ bezeichnet.

Beachten Sie:

- erst wird f ausgeführt und dann g
- man sagt auch g nach f.
- Injektiv, surjektiv? Blatt 1, Aufgabe 7

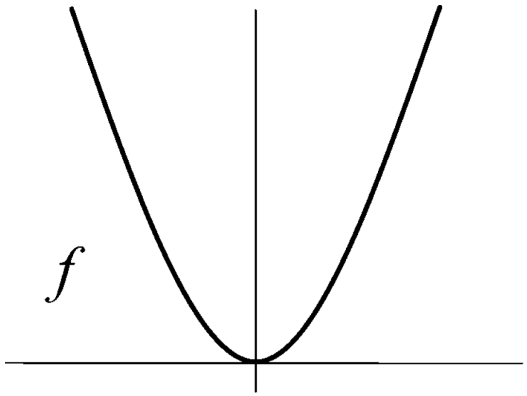
Hintereinanderausführung von Abbildungen

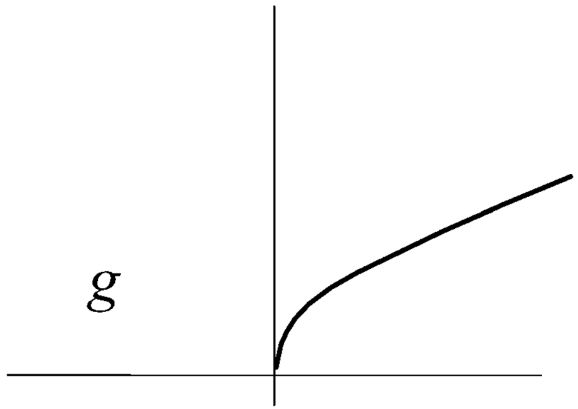
Beispiel:

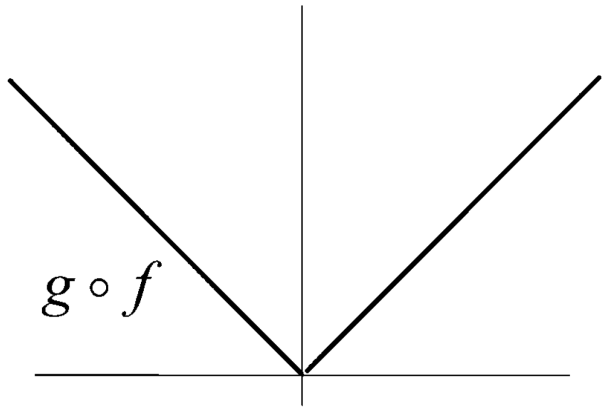
Seien $f : \mathbb{R} \to \mathbb{R} : x \longmapsto x^2$ und $g : \mathbb{R}_{\geq 0} \to \mathbb{R} : x \longmapsto \sqrt{x}$.

Dann ist $h = g \circ f : \mathbb{R} \to \mathbb{R}_0^+ : x \longmapsto \sqrt{x^2} = |x|$.

(Korrektur: Daher im 3. Bild ist $g \circ f$ nur im 1. Quadrant definiert).







Anwendung: Hashing

Hashfunktionen

Abbildungen, die Datensätzen beliebiger Länge (viele Bit) **Hashwerte** fester, meist kürzerer Länge (z.B. 128 Bit) zuordnen.
Dies sind dann Speicheradressen, welche effizientes Suchen von Datensätzen in großen Datenmengen ermöglichen.

Beispiel Hashing

Aufgabe: Finde schnell die Vorwahl von einem beliebigen Ort in Österreich.
Schlüssel (key): Suchbegriff ist in unserem Fall der Ort, mithilfe dessen die Speicheradresse berechnet wird.
Wert (value): gesuchter Wert ist in unserem Fall die Vorwahl.
Idee: Nachdem wir die Speicheradresse mithilfe des Schlüssels berechnen, ist der Zugriff über den Suchbegriff möglich. Wir müssen also nicht mehr die gesamte Datenmenge durchsuchen, sondern können nur die Werte betrachten, welche an der berechneten Speicheradresse zu finden sind.

Die Hashfunktion

Die **Speicheradresse**, die mit Hilfe des Suchbegriffes (sprich Schlüssel k) berechnet wird, wird mittels Hashfunktion (H) ermittelt, welche k als Argument erhält. Der Schlüssel wird also unter der Adresse H(k) abgelegt und kann auch damit wiedergefunden werden.

$$H : K \to A = \{0, 1, 2, ..., N-1\}$$
$$k \mapsto H(k)$$

Beispiel Hashfunktion

Die Hashfunktion:

$$H(k) = \sum_i a_i \mod N \tag{1}$$

a_i = die Zahl für die Stelle des i-ten Buchstaben z.B. k= XYZ würde bedeuten $a_1 = 24$, $a_2 = 25$, $a_3 = 26$.
$N = 7$. Wir berechnen den Wert für die Schlüssel WIEN, GRAZ, SALZBURG und DORNBIRN.
Wir erhalten:
$H(WIEN) = (23 + 9 + 5 + 14) \mod 7 = 2$
$H(GRAZ) = ?$
$H(SALZBURG) = ?$
$H(DORNBIRN) = ?$
Welche Adressen würden für GRAZ, SALZBURG und DORNBIRN mit der gegebenen Hashfunktion berechnet?

Beispiel Hashfunktion

Die Hashfunktion:

$$H(k) = \sum_i a_i \mod N$$

a_i = die Zahl für die Stelle des i-ten Buchstaben z.B. k= XYZ würde bedeuten $a_1 = 24$, $a_2 = 25$, $a_3 = 26$.
$N = 7$. Wir berechnen den Wert für die Schlüssel WIEN, GRAZ, SALZBURG und DORNBIRN.
Wir erhalten:

$H(WIEN) = (23 + 9 + 5 + 14) \mod 7 = 2$
$H(GRAZ) = (7 + 18 + 1 + 26) \mod 7 = 3$
$H(SALZBURG) = (19 + 1 + 12 + 26 + 2 + 21 + 18 + 7) \mod 7 = 1$
$H(DORNBIRN) = (4 + 15 + 18 + 14 + 2 + 9 + 18 + 14) \mod 7 = 3$

Kollision

Wir sehen, dass wir ein Problem haben, da sowohl Dornbirn als auch Graz **demselben Speicherplatz zugeordnet** werden, ein Sachverhalt, der Kollision genannt wird.
Normalerweise gibt es sehr viele Schlüssel, die auf eine kleinere Anzahl verfügbarer Hashwerte (sprich Speicheradressen) mittels H(k) abgebildet werden sollen.

Kollision

Eine einfache Strategie zur Auflösung von Kollisionen ist das **lineare Sondieren**. Dabei wird die nächst größere freie Adresse gewählt.

$$s_i(k) = \big(H(k) + i\big) \mod N, \text{für } i = 1, \cdots, N-1.$$

Hashtabelle

Eine **Hashtabelle** ist eine Datenstruktur, in der die (key, value)- Paare an der mit der Hashfunktion berechneten Adresse abgespeichert werden.
Wir vermeiden die Kollision zwischen GRAZ und DORNBIRN, indem wir DORNBIRN an der Adresse $(3+1) \mod 7 = 4$ abspeichern.

Speicherplatz(n)	Schluessel(k_n)	Wert(v_n)
0		
1	SALZBURG	0662
2	WIEN	01
3	GRAZ	0316
4	DORNBIRN	05572
5		
6		

Quadratisches Sondieren

Bessere Strategie zur Auflösung von Kollisionen:

$$\left.\begin{array}{rcll} s_{2i-1}(k) & = & \left(H(k)+i^2\right) & \mod N \\ s_{2i}(k) & = & \left(H(k)-i^2\right) & \mod N \end{array}\right\} i = 1, \cdots, \frac{N-1}{2}.$$

d.h. für $N = 7$ gilt:
$H(k)+1, H(k)-1, H(k)+4, H(k)-4, H(k)+9, H(k)-9$

Quadratisches Sondieren. Wie gut funktioniert es?

i	1		2		3	
i^2	1		4		9	
$\pm i^2 \bmod 7$	1	6	4	3	2	5

i	1		2	
i^2	1		4	
$\pm i^2 \bmod 5$	1	4	4	1

Abbildung: Adressen für verschiedenes N.

Beachte: Der Modulo Operator bildet positive Reste, d.h. $-1 = (-1) \cdot 7 + 6$.

siehe Blatt 2

Satz von Fermat

Ist N eine Primzahl und es gilt $N \mod 4 = 3$, so gilt

$$\{\pm i^2 \mod N : i = 1, \cdots, \tfrac{N-1}{2}\} = \{1, 2, \cdots, N-1\}.$$

Wähle N gemäß dieser Vorschrift, damit eine gleichmäßige Auslastung der Hashtabelle auch im Fall von Kollisionen gewährleistet ist.

Beispiel zur Äquivalenzrelation

Beispiel zur Äquivalenzrelation

Es sei R die Relation auf der Menge der geordneten Paare von positiven ganzen Zahlen definiert als $((a, b), (c, d)) \in R$ dann und nur dann, wenn $ad = bc$.

Man zeige dass R ist eine Äquivalenzrelation ist.

Lösung

Erst zeigen wir, dass R reflexiv ist:
$((a, b), (a, b)) \in R \; \forall a, b \in \mathbb{Z}^+$ dann und nur dann
wenn $ab = ba \; \forall a, b \in \mathbb{Z}^+$.
Das letzte gilt, weil die Multiplikation in $\mathbb{Z}^+$ kommutativ ist.

Daher ist R reflexiv.

Lösung

Wir zeigen, dass R symmetrisch ist, d.h.
wenn $((a, b), (c, d)) \in R$, dann $((c, d), (a, b)) \in R$.
Wir wissen, dass $ad = bc$ und $cb = da$ dieselbe Relationen sind,
aus dem gleichen Grund wie bei der Reflexivität, weil die
Multiplikation in $\mathbb{Z}^+$ kommutativ ist.

Daher ist R symmetrisch.

Lösung

Wir zeigen, dass R transitiv ist, d.h.
wenn $\forall a, b, c, d \in \mathbb{Z}^+ \; ((a, b), (c, d)) \in R$ und $((c, d), (e, f)) \in R$,
dann $((a, b), (e, f)) \in R \; \forall a, b, c, d \in \mathbb{Z}^+$.
Wir wissen, dass $ad = bc$, und $cf = de \quad \forall a, b, c, d \in \mathbb{Z}^+$.

Multipliziert man diese zwei Gleichungen man, dann bekommt man
$adcf = bcde \Rightarrow af = be \Rightarrow ((a, b), (e, f)) \in R$.

Daher ist R transitiv.

R ist also eine Äquivalenzrelation.