Inoffizielles Script zur Vorlesung Algebra 1 WS 2011 für IST, Prof. Schmidt

Mitwirkende Autoren:

Mic92

chaosbastler

js75

Revision: 10. Januar 2012

Dieses Script wird fortlaufend mit den Vorlesungen erweitert. Es lohnt sich also ab und an nach Updates zu schauen.
Mitarbeit ist natürlich erwünscht, weitere Informationen auf der Projektseite:
https://github.com/Mic92/Algebra-I

Inhaltsverzeichnis

1 Mengen

1.1 Grundlegendes

Was ist eine Menge?

Eine Menge ist eine Zusammenfassung unterscheidbarer Objekte zu einer Gesamtheit. Die Reihenfolge der Elemente ist irrelevant. Jedes Element ist einzigartig.
Seien A und B Elemente, dann gilt:

$$A = B \Leftrightarrow \{A, B\} = \{A\} \tag{1}$$

$$A \neq B \Leftrightarrow \{A, B\} \neq \{A\} \tag{2}$$

D.h. gleiche Elemente werden in Mengen nur einmal gezählt. 2 Mengen sind genau dann gleich, wenn sie die selben Elemente enthalten.

Besondere Mengen

Die Menge, die keine Elemente enthält, wird als die *leere Menge* bezeichnet, das Symbol hierfür ist: $\{\}$ oder $\varnothing$.
Die *Potenzmenge* einer Menge ist die Menge aller Teilmengen dieser Menge. Sie wird mit $\mathcal{P}(A)$ oder 2^A bezeichnet. Jede Potenzmenge enthält die leere Menge als Element.

Def.: $\mathcal{P}(A) := \{U | U \subseteq A\}$

Beispiel: $A = \{1, 2, 3\} \Rightarrow 2^A = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$

1.2 Mächtigkeit von Mengen

Für endliche (abzählbare) Mengen ist die Mächtigkeit gleichzusetzen mit der Anzahl der Elemente einer Menge. Für unendliche (nicht abzählbare) Mengen müssen andere Definitionen getroffen werden, um deren Mächtigkeit zu beschreiben.

Man schreibt: $|A|$ oder $\#A$

Es gilt: $|2^A| = 2^{|A|}$

Satz von Cantor Die Mächtigkeit der Potenzmenge einer Menge A ist stets größer als die Mächtigkeit der Menge A selber:

$$|2^A| > |A|$$

Dies gilt insbesondere für die leere Menge, da $2^0 > 0$. Außerdem ist für sämtliche endliche Mengen klar: $2^n > n$. Auch bei unendlichen Mengen lässt sich die Gültigkeit des Satzes zeigen.

Gleichmächtigkeit

Seien A und B zwei beliebige Mengen. Dann heißt A gleichmächtig zur Menge B, wenn eine Bijektion ($f : A \to B$) gebildet werden kann. Das bedeutet, dass eine Vorschrift existiert, welches jedem Element der Menge A genau ein Element der Menge B zuordnet. Dabei werden alle Elemente der Menge B einmal erfasst. Diese Vorschrift ist umkehrbar.

Man schreibt: $\#A = \#B$ bzw. $|A| = |B|$

Beispiele: $\#\mathbb{N} = \#\mathbb{Z} = \#\mathbb{Q}$
Jede Menge, die gleichmächtig zur Menge der natürlichen Zahlen ist, wird als *abzählbar* bezeichnet. Die Mächtigkeit der reelen Zahlen hingegen wird als *überabzählbar* bezeichnet.

Erläuterung zu $\#\mathbb{N} = \#\mathbb{Z}$: Der Einwand, dass die natürlichen Zahlen doch "offensichtlich" (von der 0 abgesehen) doppelt so viele seien müssten, wie die ganzen Zahlen zählt bei diesen unendlichen Mengen nicht! Stattdessen sollte man an die Definition

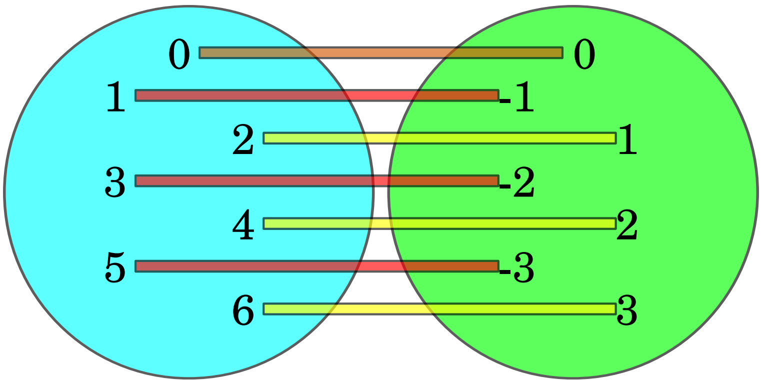
der Gleichmächtigkeit denken: 2 Mengen sind dann gleich, wenn es eine eineindeutige(bijektive) Abbildung gibt. Es werden also die 0 auf die 0, die ungeraden Zahlen auf die positiven Zahlen und die geraden Zahlen auf die negativen Zahlen abgebildet. Dies ist aufgrund der Unendlichkeit der beiden Mengen ohne Probleme möglich.
Auch für die rationalen Zahlen lässt sich ein solches Schema für eine Bijektion finden. Hierauf geht ein Wikipedia-Artikel näher ein:
http://de.wikipedia.org/wiki/Cantors_erstes_Diagonalargument
Und auch bei der Frage, warum die reellen Zahlen nicht abzählbar sind, hilft Wikipedia:
http://de.wikipedia.org/wiki/Cantors_zweites_Diagonalargument

Beispiel für überabzählbare Mengen Ähnlich wie beim vorherige Beispiel widerspricht es auch der Intuition, dass die Menge $\{x|x \in (0,1)\}$ sowie $\{x|x \in \mathbb{R}\}$ gleichmächtig sind. Schließlich ist das Intervall $(0,1)$ ja nur eine Teilmenge der reelen Zahlen.
Tatsächlich kann man schon mit Schulmathematik eine solche Bijektion finden:

$$f(x) = 1/\pi * (arctan(x) + \pi/2)$$

Wer einen Blick auf den Graphen von $arctan(x)$ wirft wird dies schnell einsehen: die Funktion durchläuft sämtliche Werte von $-\infty$ bis ∞ und nimmt dabei nur Werte von $-\pi/2$ bis $\pi/2$ an. Durch Stauchung mit dem Faktor $1/\pi$ sowie Verschiebung nach oben kommt man dann zu obiger Funktion.

Abbildung 1: Beispiel für eine Abbildung $\#\mathbb{N} = \#\mathbb{Z}$



2 Abbildungen

2.1 Definition

Eine *Abbildung* f besteht aus drei Teilen: einer Ausgangsmenge A (genannt *Definitionsbereich*), einer Zielmenge B (genannt *Wertebereich*) und einer Abbildungsvorschrift $x \overset{f}{\mapsto} f(x)$. Jedem Element x aus A kann genau ein Element $y = f(x) =: fx$ aus B zugeordnet werden.

2.1.1 Beispiel

$A =$ Menge von Personen, $B =$ Menge von Jahreszahlen und $x \mapsto fx$
Jeder Person x aus A wird ihr Geburtsjahr $y = fx$ aus B zugeordnet.

2.1.2 Notation

Ist f eine Abbildung mit Ausgangsmenge A und Zielmenge B, so schreiben wir $f\colon A \to B, x \mapsto fx$ anstelle von f.
Mit $\mathrm{Def}(f) := A$ und $\mathrm{Wert}(f) := B$ können wir auch für f die Notation $f\colon \mathrm{Def}(f) \to \mathrm{Wert}(f), x \mapsto fx$ verwenden.

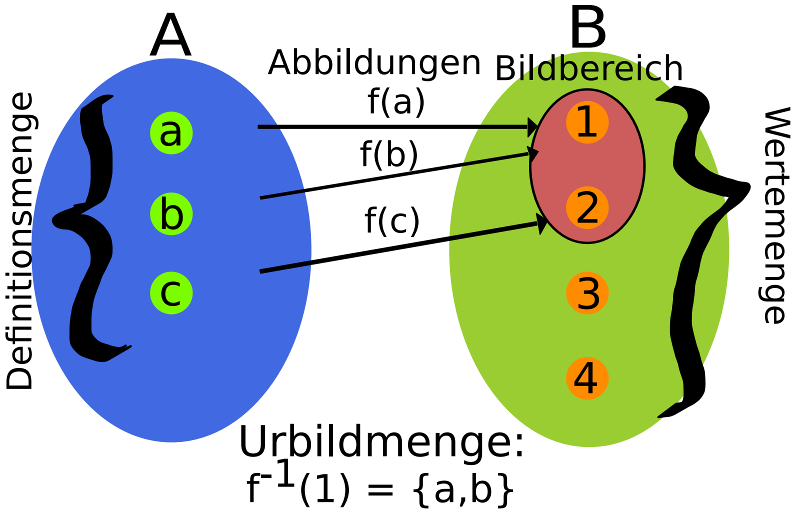
Anmerkungen

(a) Abbildung = map oder mapping

(b) Funktion = function (ist immer eine Abbildung, manchmal synonym, manchmal spezieller)

Von bijektiven Funktionen kann eine *Umkehrfunktion* $f^{-1} : B \to A$ gebildet werden. Deswegen bezeichnet bijektive Funktionen auch als *invertierbar*.
Diese ist nicht zu verwechseln mit dem *Urbild*, was ähnlich geschrieben wird.

Beispiel



Hinweis: Der Begriff *Wertemenge* kann als Synonym sowohl für die *Zielmenge* als auch für den *Bildbereich* verwendet werden. In diesem Skript sind *Zielmenge* und Wertemenge identisch, der *Bildbereich* ist somit eine Teilmenge der *Wertemenge* (siehe auch Abschnitt 2.3).

2.2 Kern einer Funktion

Sei $f : A \longrightarrow B$ eine Abbildungsvorschrift. Dann ist die Menge

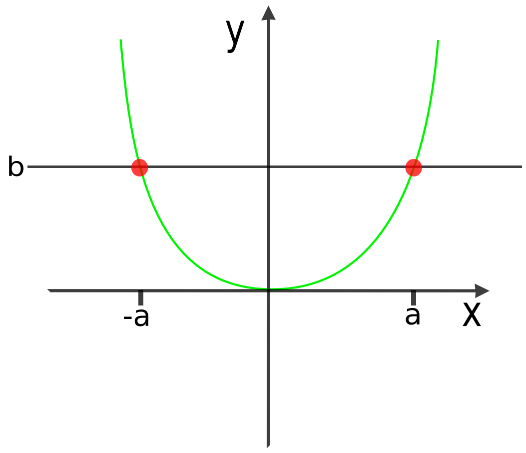
$$\ker(f) := \{(a, b) | f(a) = f(b)\}$$

der sogenannte Kern von f. Umgangssprachlich ausgedrückt: Alle Paare, die den selben Funktionswert besitzen.

2.2.1 Beispiel

$$\begin{aligned} f :&\mathbb{R} \rightarrow \mathbb{R} : x \longmapsto x^2 \\ \ker(f) &= \{(a, b) | f(a) = f(b)\} \\ &= \{(a, b) | a^2 = b^2\} \\ &= \{(a, b) || a| = |b|\} \end{aligned}$$

Ein anschaulicher Erklärungsversuch: Um den Kern dieser Funktion zu bestimmen, zeichnet man eine Parallele zur X-Achse zum Graph der Funktion(vgl. Grafik). Nun untersucht man an der Stelle a, welche Werte den den selben Funktionswert besitzen. Offensichtlich trifft die Parallele zur X-Achse den Graph wiederrum bei -a. Also muss die Menge $\{(0, 0), (1, -1), (-1, 1), (2, -2), ...\} = \{(a, -a) | a \in \mathbb{R}\}$ Teil des Kerns sein. Außerdem muss(wie unter 2.2.3 erläutert wird) auch die Menge $\{(a, a) | a \in \mathbb{R}\}$ im Kern enthalten sein, was insgesamt zu obigem Ergebnis führt.



2.2.2 Rechnerische Behandlung

Je nach Abbildung kann man den Kern auch rechnerisch bestimmen. Hierfür soll das Beispiel noch einmal etwas ausführlicher erläutert werden. Der Ausgangspunkt ist, dass zwei (nicht notwendigerweise verschiedene) Werte x_1, x_2 auf das selbe Element abgebildet werden sollen:

$$f(x_1) = f(x_2)$$

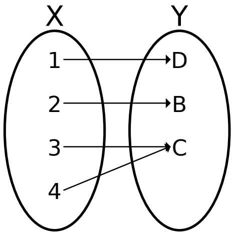
$$x_1{}^2 = x_2{}^2$$

Wurzelziehen führt zu den Lösungen $x_1 = x_2$ sowie $x_1 = -x_2$ Dieses Beispiel ist rechnerisch recht trivial, entscheident ist, dass man den Ansatz verstanden hat: man muss für (möglicherweise unterschiedliche) Werte beim Einsetzen in die Funktion das selbe Ergebnis erhalten. [1]

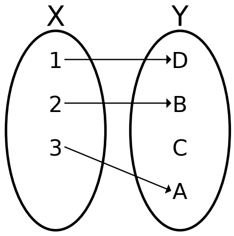
2.2.3 Eigenschaften des Kerns

Wegen $f(a) = f(a)$ muss $\ker(f)$ immer $\{(a, a)|a \in A\}$ enthalten. Anders formuliert: da man bei einer Funktion für ein und den selben Eingabewert immer das selbe herrausbekommt, müssen diese im Kern enthalten sein.

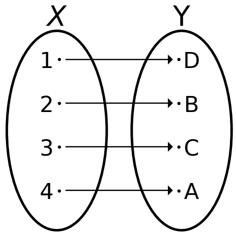
[1] Wenn gewünscht, kann man hier auch ein etwas komplexeres Beispiel (so wie das in der Übung z.B.) einfügen. Sagt einfach irgendwie Bescheid, wenn Bedarf besteht.



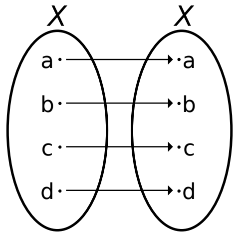
(a) surjektive Abbildung



(b) injektive Abbildung



(c) bijektive Abbildungen



(d) identische Abbildungen

2.3 Typen von Abbildungen

2.3.1 Definition

Seinen A und B zwei Mengen und $f : A \longrightarrow B$ eine Abbildungsvorschrift. Dann gibt es 3 besondere Typen von Abbildungen:

surjektive Abbildung *alle* Elemente von B mindestens einmal erfassen

$$\forall b \in B \exists a \in A : f(a) = b$$

injektive Abbildungen alle Elemente von A erhalten *unterschiedliche* Elemente aus B ("keine Kollisionen")

$$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

bijektive Abbildungen *surjektiv und injektiv* zu gleich: alle A erhalten genau ein B und alle B werden getroffen. Dies impliziert die Umkehrbarkeit der Funktion. Eine Sonderform der bijektiven Abbildung ist die *Identität*. Dabei wird jedes Element sich selbst zugeordnet.

$$\forall b \in B \exists ! a \in A : f(a) = b$$

Ist $f\colon A \to B$ eine Abbildung, so sei für $X \subseteq A$ stets $fX \coloneqq f[X] \coloneqq \{fx | x \in X\}$ die Menge der Bilder von X unter f. Ferner heiße $\mathrm{Bild}(f) = \mathrm{Im}(f) \coloneqq fA$ die *Bildmenge*[2] von f. f ist genau dann surjektiv, wenn (gdw[3]) $fA = B$ gilt, das heißt die Bildmenge von f ist gleich der Zielmenge von f. Daraus folgt: $fX \subseteq fA$

[2] Bild = Image
[3] im englischen Sprachraum *iff* = if and only if

2.3.2 Bezeichnungen

Sind A und B Mengen, so bezeichnen $B^A \coloneqq \mathrm{Abb}(A,B) \coloneqq \mathrm{Map}(A,B)$ die Menge aller Abbildungen von A nach B.

$\mathrm{Surj}(A,B)$ sei die Menge aller surjektiven Abbildungen (*Surjektionen*) von A nach B,

$\mathrm{Inj}(A,B)$ sei die Menge aller injektiven Abbildungen (*Injektionen*) von A nach B,

$\mathrm{Bij}(A,B)$ sei die Menge aller bijektiven Abbildungen (*Bijektionen*) von A nach B.

2.3.3 Mächtigkeit von Definitions- und Wertebereich

Für Surjektionen gilt: $|A| \geqslant |B|$
Für Injektionen gilt: $|B| \geqslant |A|$
Weil für bijektive Abbildungen beide Aussagen gelten müssen gilt:

$$|A| \geqslant |B| \wedge |B| \geqslant |A| \Rightarrow |A| = |B|$$

Analog gilt auch:

$$|A| < |B| \Longleftrightarrow \mathrm{Surj}(A,B) = \varnothing$$

$$|A| > |B| \Longleftrightarrow \mathrm{Inj}(A,B) = \varnothing$$

$$|A| \neq |B| \Longleftrightarrow \mathrm{Bij}(A,B) = \varnothing$$

Die ersten Aussagen schließen von einem Typ von Abbildung auf die Mächtigkeit von Definitions- und Wertebereich. Die drei letzen Aussagen schließen von Definitions- und Wertebereich auf die (nicht) möglichen Typen von Abbildungen.
Würden die Beziehungen zwischen den Mächtigkeiten nicht gelten, würde z.B. die Formel zur Mächtigkeit von $\mathrm{Inj}(A,B)$ zu Widersprüchen führen(vlg. nächstes Kapitel).

2.4 Mächtigkeit von Mengen von Abbildungen

Seien A und B Mengen. Dann bezeichnet B^A oder $\mathrm{Map}(A, B)$ die Menge aller Abbildungen von A nach B.

Satz: Für A, B endliche Mengen gilt:

$$|B^A| = |B|^{|A|}$$

2.4.1 Formeln zur Berechnung der Mächtigkeit von Mengen von Abbildungen

bijektive Abbildungen Sei $|A| = |B|$ endlich. Die Mächtigkeit der Menge aller bijektiven Abbildungen von A nach B entspricht der Anzahl der Permutationen auf einer |A|-elementigen Menge.

$$\begin{aligned} A &\to B \\ |Bij(A, B)| &= (|A|)! = (|B|)! \end{aligned}$$

injektive Abbildungen Seien |A| und |B| endlich. Die Mächtigkeit der Menge aller injektiven Abbildungen von A nach B entspricht einer *Variation* ohne Zurücklegen:

$$\begin{aligned} A &\to B \\ a &= |A| \; b = |B| \\ |Inj(A, B)| &= \binom{b}{a} * a! = \frac{b!}{(b-a)!} \end{aligned}$$

Anmerkung: Für den Sonderfall $|A| = |B|$ führt die Formel auf die Formel für die bijektiven Abbildungen zurück. Das bedeutet, dass im Fall $|A| = |B|$ endlich jede Injektion automatisch auch eine Bijektion ist:

$$|A| = |B| \Longleftrightarrow Inj(A, B) = Bij(A, B) = Surj(A, B)$$

z.B.: $Inj(A, A) = Bij(A, A) =: Perm(A)$ (die Permutation einer Menge ist die Bijektion einer Menge in sich selbst)

surjektive Abbildung Seien |A| und |B| endlich. Die Mächtigkeit der Menge aller surjektiven Abbildungen von A nach B lässt sich mithilfe der Stirlingzahl 2. Art ($S_{n,r}$)

berechnen.

$$
\begin{aligned}
A &\to B \\
a &= |A| \; b = |B| \\
|Surj(A, B)| &= b! \cdot S_{(a,b)} \\
S(a, b) &= \frac{1}{b!} \sum_{j=1}^{b} (-1)^{b-j} \binom{b}{j} j^a
\end{aligned}
$$

Bemerkung: Die Formel für surjektive Abbildung sollte als Ergänzung zum Vorlesungsstoff verstanden werden. Sie wird(soweit wir bisher wissen) nicht als bekannt vorrausgesetzt.

Weitere Bemerkungen Es gilt: $|A| = n \iff Bij(\{1, ..., n\}, A) \neq \emptyset$

2.4.2 Herleitung einer rekursiven Formel für |Surj(A,B)|

Idee:

$$B^A = \dot{\bigcup_{X \subseteq B}} \{f \in B^A | f(A) = X\}$$

Offensichtlich gilt:

$$|f \in B^A | f(A) = X| = |Surj(A, X)| = s(|A|, |X|)$$

Da $\{\{f \in B^A | f(A) = \lambda\} X \subseteq B\}$ eine Partition(d.h. "disjunkte Zerlegung") von B^A ist, gilt nun:

$$|B|^{|A|} = |B^A| = \sum_{x \subseteq B} s(|A|, |X|) = \sum_{i=0}^{|B|} \sum_{X \in \binom{|B|}{i}} s(|A|, i) = \sum_{i=0}^{|B|} \binom{|B|}{i} * s(|A|, i)$$

Es folgt mit $n := |A|$ sowie $k := |B|$:

$$\sum_{i=0}^{k} \binom{k}{i} * s(n, i) = \binom{k}{0} * s(n, 0) + \binom{k}{1} * s(n, 1) + \binom{k}{2} * s(n, 2) + \cdots + \binom{k}{k} * s(n, k) = k^n$$

Weiterhin gilt: $s(0, 0) = 1$ und $s(n, 1) = 1$ sowie $s(n, 0) = 0$ für $n \neq 0$

2.4.3 Anwendung der rekursiven Formel

Exemplarisch soll am Beispiel k=3 die Berechnung mit einer rekursiven Formel gezeigt werden. Die im vorherigen Abschnitt hergeleitete Formel gibt nur implizit s(n,k) an, als erster Schritt soll die Angabe explizit geschehen. Das heißt, die Gleichung wird zunächst einfach umgestellt:

$$s(n,k) = k^n - \binom{k}{1} * s(n,1) - \binom{k}{2} * s(n,2) + ... + \binom{k}{k-1} * s(n,k-1)$$

Also gilt für k = 3:

$$s(n,3) = 3^n - \binom{3}{1} * s(n,1) - \binom{3}{2} * s(n,2)$$

Offensichtlich müssen zur Berechung eines Elementes erst die vorherigen Elemente bestimmt werden:

$$s(n,1) = 1$$
$$s(n,2) = 2^n - \binom{2}{1} * s(n,1) = 2^n - 2$$

Die Ergebnisse können nun eingesetzt werden:

$$s(n,3) = 3^n - \binom{3}{1} * 1 - \binom{3}{2} * (2^n - 2) = 3^n - 3 * 2^n + 3$$

So ergibt sich z.B. für n = 5:

$$s(5,3) = 3^5 - 3 * 2^5 + 3 = 150$$

3 Graphen

3.1 Gerichteter Multigraph

3.1.1 Motivaton

Graphen sind ein gutes Modell für verschiedene Problemstellungen. Wie jedes Modell dienen sie dazu, die Realität zu simplifizieren und auf das Wesentliche zu beschränken. Bei einem Netzwerk wäre eine geeignete Abstraktion, dass man sich auf die Betrachtung von Objekten(die als Knoten bezeichnet werden) und ihrer Verbindungen beschränkt. Die Position der Knoten ist nicht relevant.

3.1.2 Definition

Ein *gerichteter Multigraph* (auch: Netzwerk) $G := (V, E, \sigma, \tau)$ besteht aus einer *Knotenmenge* V, einer *Kantenmenge* E sowie $\sigma, \tau \in V^E$.

- σ wird als Anfangspunktabbildung (source map) von G bezeichnet.
- τ wird als Endpunktabbildung (target map) von G bezeichnet.
- entspricht der Abbildung: $\rho : E \to V \times V, e \mapsto (\sigma e, \tau e)$

G heiße einfach, falls σ injektiv ist.

3.1.3 Erläuterungen zur Definition

Der Begriff (gerichteter) Graph meint im Rahmen der Vorlesung immer einen (gerichteter) Multigraph. Andernfalls wird explizit von einem einfachen Graphen gesprochen.
Im Gegensatz zu ungerichteten Graphen, werden bei der graphischen Darstellung eines Graphen Kanten durch Pfeile(und nicht durch Linien) dargestellt. Dadurch soll verdeutlicht werden, dass man die Kante nur in eine Richtung(nämlich die Pfeilrichtung) "durchlaufen" kann.
Bei einem Multigraphen ist es - im Gegensatz zu einem einfachem Graphen - erlaubt, zwei Knoten auch durch mehrere Kanten zu verbinden. Auch sogenannte Schleifen (eine Kante von einem Knoten auch sich selbst) sind erlaubt. Eine nähere Erläuterung von σ und τ findet anhand des Beispiels b) statt.

3.1.4 Beispiel

a)

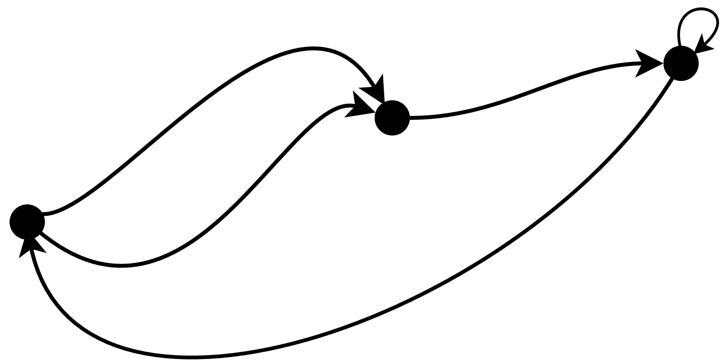


Abbildung 2: Ein Beispiel für einen gerichteten Multigraphen: es sind sowohl Schlingen als auch mehrfache Verbindungen von zwei Knoten erlaubt

b) Sei V Menge und $E \subseteq V \times V$ "binäre Relation auf V"
Dann ist $G(V, E) := (V, E, \sigma, \tau)$
mit $\sigma : E \to V, (p, q) \mapsto p$
und $\tau : E \to V, (p, q) \mapsto q$
Sei V nun z.B. die Menge $\{1, 2, 3\}$. Die Elemente 1,2,3 bezeichnen dabei jeweils die Knoten. Dann ist z.B. $E = \{(1, 1), (1, 2), (1, 3)\}$ die Menge aller Kanten des Graphen. Das heißt, es geht vom Element 1 ein Pfeil zu allen anderen Elementen und zu sich selbst.
Die Funktion σ gibt nun zu einer Kante den Anfangspunkt als Funktionswert zurück, also bei einer Kante (a, b) das Element a):

$$\sigma((1, 1)) = 1$$
$$\sigma((1, 2)) = 1$$
$$\sigma((1, 3)) = 1$$

Die Funktion τ hingegen gibt jeweils den Endpunkt einer Kante zurück, also bei einer

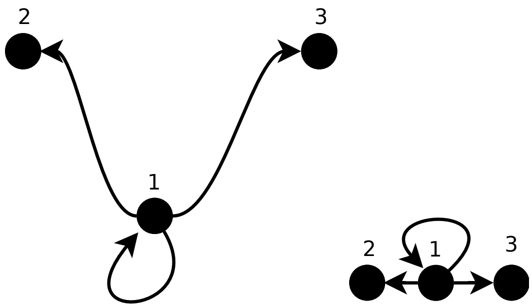


Abbildung 3: 2 Möglichkeiten den Graphen zum Beispiel b) darzustellen

Kante (a, b) das Element b):

$$\tau((1,1)) = 1$$
$$\tau((1,2)) = 2$$
$$\tau((1,3)) = 3$$

planarer Graph Graph, der auf einer Ebene mit Punkten und Linien dargestellt, keine Überscheidungen besitzt.

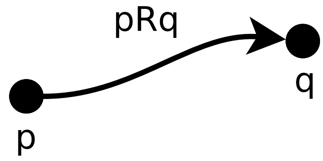


Abbildung 4: Die Notation pRq steht für $(p, q) \in R$, vergleiche auch Vorlesung Mathematik I, Definition 3.1.1

3.2 Binäre Relate als Netzwerke

3.2.1 Definition

Ein *binäres Relat* ist erklärt als Paar $M := (M, R)$, wobei M und R Mengen sind und $R \subseteq M \times M$, d.h. R ist "binäre Relation auf M".
Sei $GM := (M, R, \sigma, \tau)$ mit $\sigma : E \to V, (p, q) \mapsto p$ und $\tau : E \to V, (p, q) \mapsto q$
GM heiße das zu M gehörige Netzwerk bzw. "M=(M,R) als Netzwerke"

Bemerkung Der Begriff "binäres Relat" ist in der Literatur nicht verbreitet, aber für die Vorlesung zweckmäßig.

3.3 Moprhismen zum Vergleich von Graphen

3.3.1 Definition

Seien G und G' zwei Netzwerke(Graphen) sowie $G \overset{\Phi}{\to} G'$
Dann ist $\Phi = (\Phi_{kante}, \Phi_{ecke})$ ein *Morphismus* ein Paar von Abbildungen:

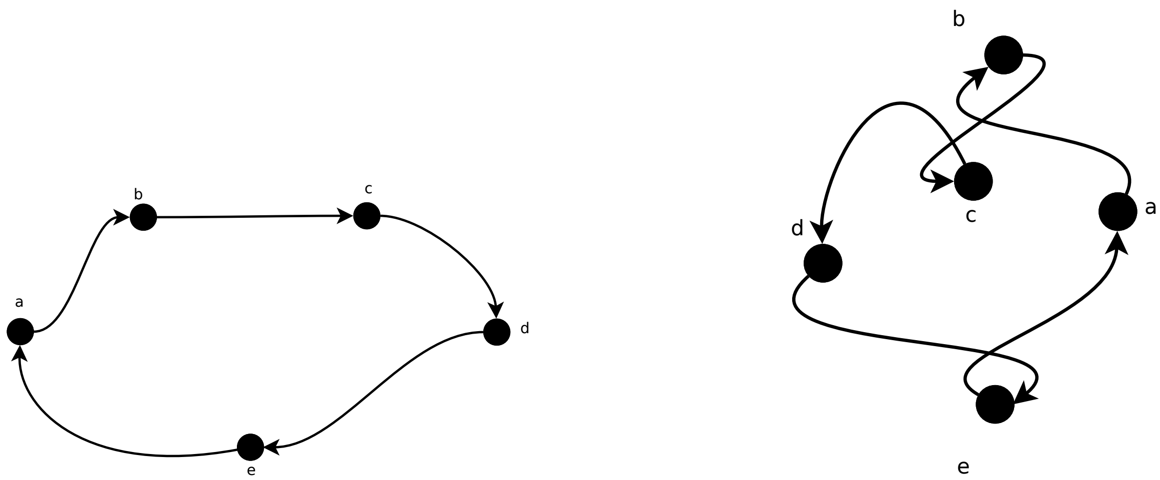
$$\Phi_{vert} : V \to V'$$

$$\Phi_{edge} : E \to E'$$

mit $\tau' \Phi_{edge} e = \Phi_{vert} \tau e$
und $\sigma' \Phi_{edge} e = \Phi_{vert} \sigma e$
D.h. das Bild des Anfangsknoten einer Kante e ist Anfangsknoten der Bildkante.

Merkregel "Fuß und Kopf gehen nicht verloren"

3.3.2 Beispiel



(a) Netzwerk G (b) Netzwerk G'

G und G' sind isomorph, man schreibt $G \cong G'$

4 Teilbarkeit

Seien $a, b \in \mathbb{N}$. Dann ist a *Teiler von* b genau dann, wenn es ein $m \in \mathbb{N}$ gibt, so dass gilt: $a \cdot m = b$.

Bezeichnung: $a \mid b$, $a \leqslant_\tau b$

Beispiel:

$$\begin{aligned} 3 &\mid 6, \text{ denn } 3 \cdot 2 = 6 \\ n &\mid 0, \text{ für alle } n \in \mathbb{N} \\ n &\leqslant_\tau 0, \text{ für alle } n \in \mathbb{N} \\ 0 \mid 0,\ 0 &\nmid k \text{ für alle } k \in \mathbb{N}\backslash\{0\} \text{ (es gibt } m \in \mathbb{N} : 0 \cdot m = 0) \\ 1 &\mid n, \text{ für alle } n \in \mathbb{N} \end{aligned}$$

Bemerkung: $\leqslant_\tau$ ist eine Relation über $\mathbb{N}$:
$\leqslant_\tau$ ist eine Untermenge von $\mathbb{N} \times \mathbb{N}$.
(a, b) ist ein Element von $\leqslant_\tau$, wenn gilt $a \leqslant_\tau b$.

Eigenschaften von Relationen: Wenn $R \subseteq A \times A$ eine Relation ist, dann ist R:

- *symmetrisch*, falls für $(a, b) \in \mathbb{R}$ stets auch $(b, a) \in \mathbb{R}$ gilt, z.B. Rechwinkligkeit: wenn $a \perp b$ ist, dann ist $b \perp a$.
- *antisymmetrisch* falls für $(a, b) \in \mathbb{R}$ und $(b, a) \in \mathbb{R}$ stets folgt: $a \equiv b$
- *reflexiv* falls $(a, a) \in \mathbb{R}$ für alle a in A gilt, z.B. Parallelität: Jede Gerade ist zu sich selbst parallel
- *transitiv* falls aus $(a, b) \in \mathbb{R}$ und $(b, c) \in \mathbb{R}$ folgt: $(a, c) \in \mathbb{R}$, z.B. Kleiner-Gleich "$\leqslant$": Wenn $a \leqslant b$ und $b \leqslant c$, dann gilt $a \leqslant c$.

Eine Ordnung(-srelation) ist eine Relation, die antisymmetrisch, transitiv und reflexiv ist.
Beispiel: $\leqslant_\tau$ (Teiler von), $\leqslant$ (kleiner gleich)

Eine Äquivalenz(-relation) ist eine Relation, die symmetrisch, transitiv und reflexiv ist.
Beispiel: $=, \equiv \pmod n$

T_n sei die Menge der Teiler von $n (n \in \mathbb{N})$.
Beispiel: $T_{12} = \{1, 2, 3, 4, 6, 12\}$

Wir schränken $\leqslant_\tau$ ein auf T_n: $\leqslant_\tau \cap (T_n \times T_n) = \leqslant_\tau^n$

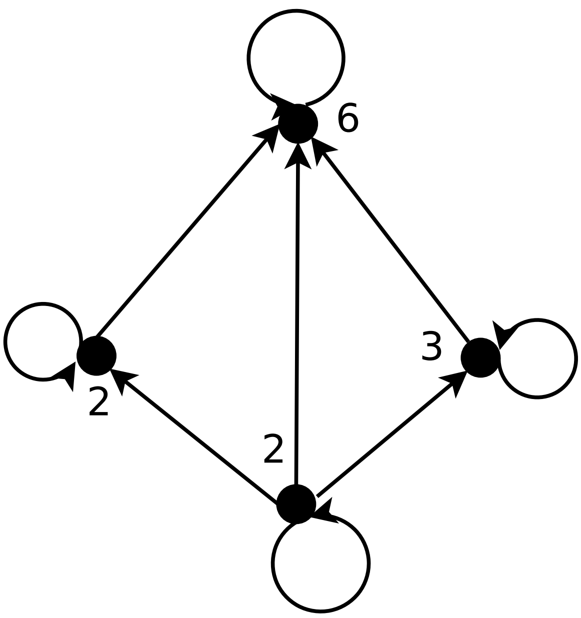
Konvention: wir schreiben $\leqslant_\tau$ statt $\leqslant_\tau \cap (A \times A)$, wenn klar ist, worauf sich $\leqslant_\tau$ bezieht, also was A ist.

$\mathbb{T}_n := (T_n, \leqslant_\tau)$ heißt **Teilerverband** von n.

Achtung: $\mathbb{T}_n$ ist ein binäres Relat. Wir haben bereits definiert, was $G(\mathbb{T}_n) = G(T_n, \leqslant_\tau)$ ist: $G(\mathbb{T}_n) = (T_n, \leqslant_\tau, \sigma, \tau)$ mit:

$$\sigma(a, b) = a$$
$$\tau(a, b) = b$$
$$\forall (a, b) \in \leqslant_\tau$$

Beispiel: $\mathbb{T}_6 = (T_6, \leqslant_\tau), T_6 = 1, 2, 3, 6$
Teilerverband $G(\mathbb{T}_6)$:



Ist R eine Ordnung über A, dann ist $G(A,R)$ eine ungünstige Darstellung.
Besser: Hasse-Diagramm:
$\leqslant_\tau$ ist eine Relation auf $\mathbb{N}$, die gegeben ist durch:
$\leqslant_\tau = \{(a,b) \in \leqslant_\tau \mid$ für alle $c \in \mathbb{N}$ mit $a \leqslant_\tau c \leqslant_\tau b, (a,c),(c,b) \in \leqslant_\tau$ gilt entweder $c = a$ oder $c = b\}$

Beispiel:

- $(1,6) \in \leqslant_\tau$, aber $1 \leqslant_\tau 2 \leqslant_\tau 6$ und $1 \leqslant_\tau 3 \leqslant_\tau 6$, daraus folgt $(1,6) \notin \leqslant_\tau$.
- $(2,6) \in \leqslant_\tau$ und für alle $c \in T_6$ mit $2 \leqslant_\tau c \leqslant_\tau 6$ gilt $c = 2$ oder $c = 6 \to (2,6)$

Hassediagramm zu $\mathbb{T}_n$: Zeichne $G(T_n, \leqslant_\tau)$, so dass der Knoten b über dem Knoten a liegt, falls $(a,b) \in \leqslant_\tau$ und zeichne Kanten (a,b), also a —— b statt $a \longrightarrow b$.

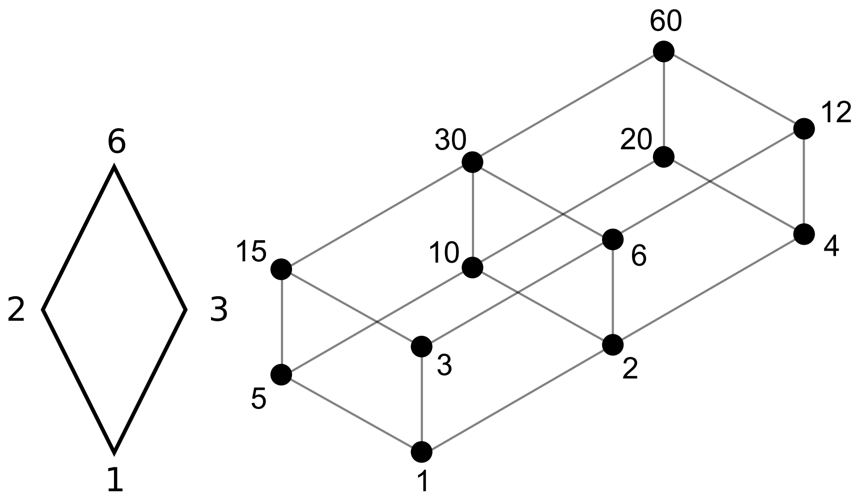


Abbildung 5: Hassediagramm vom Teilerverband 6 und 60