Grundkurs Theoretische Informatik

Mengentheoretisch-algebraische Grundlagen

S. Gerber

Universität Leipzig
Institut für Informatik

Inhaltsverzeichnis

Literatur

Aho, A.V.; Ullman, J.D.: Grundlagen der Informatik, Bonn 1995

Asser, G.: Grundbegriffe der Mathematik, V.d.Wiss., Berlin, 1973

Bauer, F.L.: Informatik, Springer, Berlin, 1971

Cap, C.H.: Theoretische Grundlagen der Informatik, Springer, Wien 1993

Schöning, U.: Theoretische Informatik, BI, Mannheim, 1992

Völz, H.: Grundlagen der Informatik, Akademie-V., Berlin, 1991

1. AUSSAGEN UND AUSSAGENVERBINDUNGEN

Die Informatik wird als Wissenschaft von der automatisierten Informationsverarbeitung und den informationsverarbeitenden Systemen charakterisiert. Zum einen ist sie wie die Mathematik eine Strukturwissenschaft, andererseits benutzt sie ingenieurwissenschaftliche Methoden. Untersuchungsgegenstand sind letztlich Verhaltensweisen von Systemen, die in der Wirklichkeit oder unserem Denken existieren und in Abhängigkeit von ihrer Umgebung im Rahmen einer Zeitskala Zustandsänderungen durchlaufen. Diese Zustandsänderungen erzeugen einen Prozeß, der von der Umgebung wahrgenommen wird und auf diese einwirkt.
Um solche Systeme zu beschreiben, bedarf es eines Formalismus (Sprache), in der Sachverhalte über das System und der von ihm erzeugten Prozesse ausgedrückt werden können. Aus derartigen Sachverhaltsbeschreibungen, die realiter zutreffen oder vorausgesetzt werden, sollen neue Sachverhalte abgeleitet werden. Dazu bedarf es logischer Regeln, die ihrerseits einem Formalismus unterliegen. Im Prozeß der Anwendung dieser Regeln auf die beschriebenen Sachverhalte erhalten wir dann einen Beweis für den abgeleiteten Sachverhalt. Mit diesen für unsere Wissenschaft notwendigen Formalismen, Sprache und Logik, wollen wir uns im weiteren beschäftigen.
Die Beschreibung der Sachverhalte erfolgt durch Aussagen und Aussagenverbindungen. Unter einer Aussage verstehen wir ganz allgemein ein sprachliches Gebilde zur Mitteilung eines Sachverhaltes, der zutrifft oder nicht zutrifft, oder wie wir sagen, wahr oder falsch ist. Dabei ist es zunächst gleichgültig, ob diese Eigenschaft jetzt oder später nachgewiesen werden kann oder nicht. "Am 20. Oktober 2001 regnet es in Leipzig." - wäre damit eine Aussage. Im Gegensatz dazu ist der Satz "Wieviele Studenten studieren in Leipzig?" keine Aussage.
In der Logik, die wir beim Umgang mit diesen Aussagen benutzen, abstrahieren wir zunächst von den inhaltlichen Bedeutungen der in den sprachlichen Gebilden ausgedrückten Sachverhalte und beschränken uns auf deren Wahrheitswert. Diesem wiederum legen wir das **Prinzip der Zweiwertigkeit** (Eine Aussage kann wahr oder falsch sein.) und das **Prinzip vom ausgeschlossenem Widerspruch** (Eine Aussage kann nicht zugleich wahr und falsch sein.) zugrunde. Dabei wird nicht vorausgesetzt, daß man entscheiden kann, ob der Satz wahr oder falsch ist: z.B. "Am 10.07.1645 betrug die Temperatur in Leipzig um 7 Uhr 14^o C" ist in dem genannten Sinn eine Aussage.
Bezeichnen A und B zwei Aussagen, so lassen sich neue Aussagen gewinnen, indem man sie durch gewisse Wörter zu Aussagenverbindungen zusammenfaßt:
"A und B"(Konjunktion), "A oder B"(Disjunktion oder Alternative), "wenn A, so B"(Implikation), "A genau dann, wenn B"(Äquivalenz), "nicht A"(Negation) usw.
Von diesen Aussagenverbindungen wollen wir einige präzisieren, indem wir festlegen, daß ihr Wahrheitswert, d.h. ob sie wahr oder falsch sind, nur von den Wahrheitswerten der in ihnen verknüpften Aussagen abhängt (Extensionalitätsprinzip). Die Festlegung geschieht durch Tabellen. Dabei bezeichnen wir den Wahrheitswert "wahr" mit L und den Wahrheitswert "falsch" mit 0. Außerdem werden wir die umgangssprachlichen Bindewörter durch gewisse Zeichen abkürzen:

A	B	A und B $A \wedge B$	A oder B $A \vee B$	wenn A, so B $A \rightarrow B$	A genau dann, wenn B $A \leftrightarrow B$
0	0	0	0	L	L
0	L	0	L	L	0
L	0	0	L	0	0
L	L	L	L	L	L

A	nicht A $\sim A$ (oder auch $\neg A$)
0	L
L	0

Aus diesen Aussageverbindungen lassen sich durch Zusammensetzen weitere kompliziertere aufbauen. Wir betrachten zwei Beispiele:

Beispiele

$((A \rightarrow B) \wedge (B \rightarrow A)) \rightarrow (A \leftrightarrow B)$

A	B	A→B	B→A	(A→B)∧(B→A)	A↔B	((A→B)∧(B→A))→ (A↔B)
0	0	L	L	L	L	L
0	L	L	0	0	0	L
L	0	0	L	0	0	L
L	L	L	L	L	L	L

$(A \wedge (A \rightarrow B)) \rightarrow B$

A	B	$A \rightarrow B$	$A \wedge (A \rightarrow B)$	$(A \wedge (A \rightarrow B)) \rightarrow B$
0	0	L	0	L
0	L	L	0	L
L	0	0	0	L
L	L	L	L	L

Wir haben zwei Aussagenverbindungen gefunden, deren Wahrheitswert immer L ist, unabhängig von den Wahrheitswerten der verwendeten Grundaussagen A und B. Derartige Verbindungen heißen allgemeingültige Verbindungen oder Tautologien. Alle Sätze der Mathematik sind solche Tautologien, darauf beruht ihre Allgemeingültigkeit innerhalb der Mathematik.

Neben den bereits verwendeten Aussageverbindungen brauchen wir noch weitere, für die wir auch Abkürzungen einführen wollen.
Generalisierung $\forall$ x A bedeute: Für jedes Ding x sei die Aussage A (über x) wahr,
Partikularisierung $\exists$ x A bedeute: Es gibt (mindestens) ein Ding x, für das die Aussage A (über x) wahr ist.
Statt $\forall$ wird in der Literatur auch $\wedge$ und statt $\exists$ auch $\vee$ verwendet.
Das Definitionszeichen $=_{def}$ bedeutet, daß das durch die links stehende Bezeichnung zu definierende Objekt (definiendum) durch die rechts stehenden Bezeichnungen bereits eingeführter Objekte (definiens) festgelegt wird. Das definiendum kann stets durch das definiens ersetzt werden. Häufig schreiben wir einfach = .
Da im Umgang mit Aussagenverbindungen hinsichtlich ihres Wahrheitswertes nur die Wahrheitswerte der in ihnen verknüpften Aussagen von Interesse sind, können wir von den konkreten Aussagen zu ihren Wahrheitswerten abstrahieren. Wie üblich, führen wir für Aussagen bzw. deren Wahrheitswerte Variable (Aussagen- oder Wahrheitswertvariable) ein und bezeichnen sie im folgenden durch p, q, p_i, q_i (i nat.Zahl). Aus Aussagenverbindungen entstehen unter Verwendung von Variablen und Konstante für Wahrheitswerte aussagenlogische Formeln (Ausdrücke), wie z.B. (p $\rightarrow$ q), $(p_1 \wedge p_2) \leftrightarrow (p_2 \wedge p_1)$.
Jede Formel erhält eindeutig einen Wert (Wahrheitswert) zugeordnet, wenn die Variablen ihrerseits mit Wahreitswerten belegt werden. Bei vorgegebener Variablenbelegung mit Wahrheitswerten 0 bzw. L kann der Wert einer Formel durch Anwendung der oben eingeführten Verknüpfungen entsprechend der Wahrheitstabellen bestimmt werden.
Eine logische Formel heißt erfüllbar, wenn es eine Variablenbelegung gibt, bei der die Formel den Wert wahr (L) erhält.
Eine Formel heißt allgemeingültig (Tautologie), wenn sie bei jeder Variablenbelegung den Wert wahr (L) annimmt.
Besitzt eine Formel keine erfüllende Belegung, dann bezeichnen wir sie als Kontradiktion.
Mit Hilfe bestimmter Regeln können aus allgemeingültigen Formeln neue Formeln gewonnen (geschlossen) werden, die dann auch allgemeingültig sind. Auf diese Weise erhält man Beweise für gewisse Aussagenverbindungen, wenn andere bereits als allgemeingültig nachgewiesen wurden bzw. als solche angenommen werden.
Folgt aus der Gültigkeit einer Aussage A in einem gewissen Bereich (d.h., unter gewissen Voraussetzungen) die Gültigkeit einer Aussage B in diesem Bereich, so schreiben wir A $\Rightarrow$ B (aus A folgt B). Steht das Zeichen $\Longleftrightarrow$ zwischen zwei Aussagen, so soll die links stehende Aussage genau dann wahr sein, wenn es die rechts stehende Aussage ist.
Eine häufig verwendete Regel ist z.B. der Modus Ponens : Wenn A und (A $\rightarrow$ B) bewiesen sind, so ist auch B bewiesen, kann geschlossen (gefolgert) werden. (In Zeichen: A, (A $\rightarrow$ B) $\Rightarrow$ B).
Weitere Schlußregeln sind:
Wenn A und B bewiesen sind, dann ist es auch (A $\wedge$ B). (In Zeichen:
A, B $\Rightarrow$ (A $\wedge$ B).)
(A $\rightarrow$ B) kann geschlossen werden aus ($\sim$ B $\rightarrow\sim$ A) (Kontraposition) (In Zeichen:
$(\sim B \rightarrow \sim A) \Rightarrow (A \rightarrow B)$.)

Das Prinzip der Fallunterscheidung besagt, daß aus (A $\rightarrow$ B) und ($\sim A \rightarrow$ B) auf B geschlossen werden kann. (In Zeichen: $(A \rightarrow B), (\sim A \rightarrow B) \Rightarrow B$.)
Eine weitere wichtige Regel ist der indirekte Schluß, wenn aus der Annahme $\sim$ A eine Kontradiktion (Widerspruch) geschlossen werden kann, dann ist A bewiesen.
Ausführlicher beschäftigen wir uns mit solchen Schlußregeln und den ihnen zugrundeliegenden Prinzipien in der Vorlesung "Logik" im 3.Semester. Hier beschränken wir uns zunächst auf das inhaltliche Folgern nach den üblichen Schlußweisen, wie sie aus der Schulmathematik bekannt sind.

2. MENGENBEGRIFF UND MENGENBILDUNG

Als Begründer der Mengenlehre wird der Hallenser Mathematiker Georg Cantor (1845-1918) angesehen, der 1895 im ersten Teil seiner Arbeit "Beiträge zur Begründung der transfiniten Mengenlehre" die folgende Definition gab:
"Eine Menge ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens - welche die Elemente der Menge genannt werden - zu einem Ganzen."
Man erkennt sofort, daß es sich bei dieser Definition nicht um eine Definition im in der Mathematik heute üblichen Sinne handelt, sondern eher um eine Beschreibung des Begriffes der Menge. Um diese Beschreibung zu präzisieren, gehen wir von einem gewissen Grundbereich I aus, der aus gewissen wohlunterschiedenen Objekten besteht, z.B. alle Städte, alle reellen Zahlen, alle Funktionen, alle Menschen usw. Diese Objekte des Grundbereiches nennen wir auch Urelemente oder Individuen, statt Grundbereich I sagen wir auch Individuenbereich I. Um solche Urelemente zu einer Menge zusammenzufassen, betrachten wir eine Aussage H(x), die auf jedes Urelement x zutrifft (für dieses Urelement wahr ist) oder nicht zutrifft. Genau die Urelemente, für die H(x) wahr ist, fassen wir zu einem Ganzen zusammen und nennen dieses Ganze eine Menge.
Wir legen also fest, d.h. wir postulieren:
Es gibt eine Menge M, so daß für alle Dinge x gilt: wenn x ein Urelement ist, so ist x Element von M genau dann, wenn H(x) wahr ist.
Statt "x ist Element von M" schreiben wir: x $\in$ M und für $\sim$ (x $\in$ M) auch x $\notin$ M.
Damit stellen wir unseren Betrachtungen folgendes Mengenbildungsaxiom voran:
Mengenbildungsaxiom:
Es sei H(x) eine Aussage, die für jedes Urelement x zutrifft oder nicht. Dann setzen wir voraus, daß die Aussagenverbindnung $\exists M \forall$ x (x Urelement $\rightarrow$ (x $\in M \leftrightarrow$ H(x))) wahr ist.

Beispiel 1.1.
I sei die Gesamtheit aller Punkte einer Ebene. H(x) sei die Aussage: "x hat von einem fest gewählten Punkt P dieser Ebene den Abstand a". Dann ist M die Menge der Punkte, die auf der Peripherie des Kreises um P mit Radius a liegen.

Beispiel 1.2.
I sei irgend ein Grundbereich. H(x) sei die Aussage: "x ist sich selbst gleich", d.h. x=x. Dann gehört jedes Urelement zu dieser Menge. Wir wollen diese Menge aller Urelemente mit U bezeichnen, also: x Urelement $\Leftrightarrow$ x $\in$ U.

Beispiel 1.3.
I sei irgend ein Grundbereich. H(x) sei die Aussage: "x ist sich selbst nicht gleich", d.h. $\sim$ (x=x). Dann gibt es kein Urelement, das dieser Menge angehört. Wir nennen diese nach dem Mengenbildungsaxiom existierende Menge die leere Menge und bezeichnen sie mit $\emptyset$.

Nach Beispiel 1.2. können wir das Mengenbildungsaxiom auch in folgender Form schreiben:
$\exists\, M\ \forall\, \mathrm{x}(\mathrm{x} \in U \rightarrow (\mathrm{x} \in M \leftrightarrow \mathrm{H(x)}))$.
Führen wir noch als Abkürzung für $\forall\, \mathrm{x}(\mathrm{x} \in U \rightarrow$ die Bezeichnung $\forall$ x $\in$ U: ein, so lautet das Mengenbildungsaxiom:
A x 1: $\exists\, M\ \forall$ x $\in$ U: (x $\in M \leftrightarrow$ H(x)).
Nachdem durch das Mengenbildungsaxiom die Existenz von Mengen postuliert ist, müssen wir festlegen, wann zwei Mengen einander gleich sind. Für die Urelemente war gefordert, daß sie wohlunterschieden sind, daß also die Gleichheit (Identität) der Objekte, die als Urelemente auftreten, feststeht bzw. gegeben ist. Die Mengen sind dagegen definierte mathematische Objekte, die von den Urelementen zu unterscheiden sind. Deshalb muß für sie eine Gleichheit definiert werden. Das geschieht durch das Extensionalitätsprinzip:
Zwei Mengen M und N sind genau dann gleich, wenn sie die gleichen Elemente enthalten.
A x 2: (M = N) $\leftrightarrow \forall$ x $\in$ U: (x $\in M \leftrightarrow$ x $\in$ N).
Für $\sim$ (M = N) schreiben wir M $\neq$ N.

Anmerkung 1.1.
Zwei Mengen sind also gleich, wenn sie den gleichen Umfang (Extension = Ausdehnung) haben, unabhängig davon, mit welcher Aussage H(x) sie definiert wurden, d.h. unabhängig vom Inhalt der Aussage. Daher geben alle mathematischen Begriffsbildungen, die auf Mengen beruhen, nur den Begriffsumfang aber nicht den Begriffsinhalt wieder. (Unterscheidung von Begriffsinhalt und Begriffsumfang geht auf Aristoteles 384 - 322 v.d.Z. zurück.)

Anmerkung 1.2.
Wegen des Extensionalitätsprinzips sind wir auch berechtigt, den vom Begriffsinhalt eingeführten Individuenbereich I der Urelemente mit der Menge U aller Urelemente zu identifizieren:

I = U.

Zur Vereinfachung der Bezeichnung von Mengen wird oft noch die Mengenbildungsklammer benutzt. Wegen des Mengenbildungsaxioms und des Extensionalitätsprinzips ist die Menge M mit

$\forall$ x $\in$ I:(x $\in$ M $\leftrightarrow$ H(x))

eindeutig bestimmt. Wir bezeichnen sie mit {x | H (x)}.

Definition 1.1.

x' $\in$ {x | H(x)} genau dann, wenn H(x').

Demnach können wir schreiben:

$I =_{def}$ { x | x = x } und $\emptyset =_{def}$ {x | $\sim$ (x = x) }.

Mengen, die nur endlich viele Elemente enthalten, führen wir ein durch:

Definition 1.2.

$\{a_1, a_2, \dots, a_n\} =_{def}$ {x | x = $a_1 \vee$ x = a_2 $\vee$ ... $\vee$ x = a_n}.

Anmerkung 1.3.
Es ist also sehr wohl das Urelement a und die Menge { a } zu unterscheiden, beides sind verschiedene mathematische Objekte. Besteht der Individuenbereich I aus allen Menschen, die bisher gelebt haben, so ist auch der Dichter Goethe ein Urelement. Bildet man nun die Menge M $=_{def}$ {x | x hat Faust 1 und 2 geschrieben }, so enthält die Menge M nur den Dichter Goethe als Element. Während aber das Urelement die Person des Dichters ist, ist M nur eine Eigenschaft des Dichters, deren Umfang nur aus dem Dichter Goethe besteht.

Neben dem Mengenbildungs- und Extensionalitätsaxiom werden zur strengen Begründung einer Mengentheorie noch weitere Axiome benötigt. Wir verweisen hier lediglich noch auf das Aussonderungsaxiom hin.
A x 3: Zu jeder Menge M und jeder Aussage H(x) gibt es eine Menge N $=_{def}$ {x | x $\in M \wedge$ H(x)}, mit der Elemente von M, die die Eigenschaft H(x) besitzen, zur Menge N zusammengefaßt werden.

Mengen höherer Stufen
Bisher haben wir Mengen über einem Grundbereich I betrachtet. Diese Mengen können selbst wieder als Grundbereich aufgefaßt werden, über dem dann Mengensysteme oder Mengen zweiter Stufe gebildet werden können. Die Elemente dieser Mengen zweiter Stufe sind also Mengen über dem Grundbereich I oder Mengen erster Stufe.

Sind z.B. x, y, z Urelemente, so ist $\{\{ x \},\{ x,y \}\}$ eine Menge zweiter Stufe, die als Elemente die Mengen $\{ x \}$ und $\{ x,y \}$ erster Stufe enthält.
Das Verfahren der Mengenbildung kann unter Beachtung der Stufe fortgesetzt werden.Es ist zu beachten, daß bei diesem Aufbau das Extensionalitätsprinzip zunächst nur innerhalb der gleichen Stufe eingeführt ist, und daß die in den einzelnen Stufen existierenden leeren Mengen deshalb als nicht vergleichbar zu betrachten sind.
Russelsches Paradoxon: Man bilde die Menge M aller Mengen X, die sich nicht selbst als Element enthalten, d.h. $M =_{def} \{X \mid X \notin X\}$. Für $M = X$ ergibt sich der Widerspruch: $M \in M \leftrightarrow M \notin M$. Demnach führt die Mengenbildung mit der Aussage $(X \notin X)$ zu Schwierigkeiten. Zur Überwindung der Probleme sei auf die gesonderte Vorlesung Mengentheorie hingewiesen.

3. MENGENALGEBRA

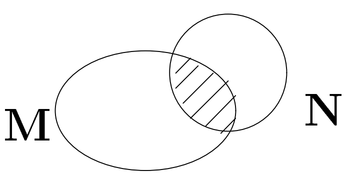
Wir geben uns für das Folgende einen Grundbereich I fest vor und betrachten nur Mengen erster Stufe über I. Dann können wir aus je zwei Mengen M und N neue Mengen mittels “Durchschnittsbildung“, “Vereinigung“ und “Mengendifferenz“ definieren.

Definition 3.1.

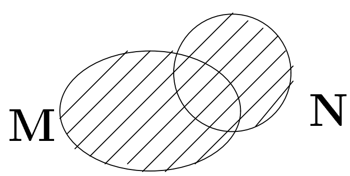
Durchschnitt: $M \cap N =_{def} \{ x \mid x \in M \wedge x \in N\}$
Vereinigung: $M \cup N =_{def} \{x \mid x \in M \vee x \in N\}$
Mengendifferenz: $M \setminus N =_{def} \{x \mid x \in M \wedge x \notin N\}$.

Veranschaulichung:

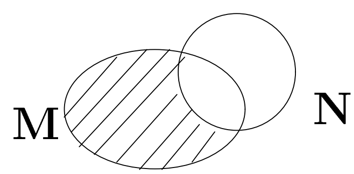
$M \cap N$



$M \cup N$



$M \setminus N$



Definition 3.2.
Zwei Mengen M und N heißen disjunkt oder durchschnittsfremd genau dann, wenn ihr Durchschnitt leer ist:
M, N disjunkt genau dann, wenn $M \cap N = \emptyset$.

Satz 3.1.
Für die Booleschen Operationen $\cap$ und $\cup$ gilt: Für jede Menge M und jede Menge N und jede Menge S:
1) $M \cap N = N \cap M$ und $M \cup N = N \cup M$ (Kommutativgesetze)
2) $(M \cap N) \cap S = M \cap (N \cap S)$ und $(M \cup N) \cup S = M \cup (N \cup S)$ (Assoziativgesetze)
3) $M \cap (N \cup S) = (M \cap N) \cup (M \cap S)$ und $M \cup (N \cap S) = (M \cup N) \cap (M \cup S)$ (Distributivgesetze)
4) $M \cap M = M$ und $M \cup M = M$ (Idempotenz).

Beweis:
Wir beweisen das erste der beiden Distributivgesetze. $Q =_{def} M \cap (N \cup S)$ und $R =_{def} (M \cap N) \cup (M \cap S)$, dann ist Q = R zu zeigen. Nach D.1.1. gilt:
$Q = R \Leftrightarrow \forall x \in I\ (x \in Q \leftrightarrow x \in R)$,
d.h. die Aussage $x \in Q \leftrightarrow x \in R$ muß für alle $x \in I$ wahr sein.
Nun ist nach Definition $x \in Q \Leftrightarrow x \in M \wedge (x \in N \vee x \in S)$ und
$$x \in R \Leftrightarrow \quad (x \in M \wedge x \in N) \vee (x \in M \wedge x \in S).$$

Wir stellen folgende Tabelle auf:

A x∈M	B x∈N	C x∈S	D=A∧B x∈M ∧ x∈N	E=A∧C x∈M ∧ x∈S	F=B∨C x∈N ∨ x∈S	A∧F x∈Q	D∨E x∈R	x∈ Q ↔ x∈R
0	0	0	0	0	0	0	0	L
0	0	L	0	0	L	0	0	L
0	L	0	0	0	L	0	0	L
0	L	L	0	0	L	0	0	L
L	0	0	0	0	0	0	0	L
L	0	L	0	L	L	L	L	L
L	L	0	L	0	L	L	L	L
L	L	L	L	L	L	L	L	L

Damit ist der Beweis erbracht.

Die Operationen $\cap$ und $\cup$ wurden bisher nur für Mengen über I erklärt. Sie lassen sich auch auf Systeme von Mengen über I ausdehnen.

Definition 3.3.
Es sei γ ein nichtleeres System von Mengen über I. Dann sei:
$\bigcap\limits_{M\in\gamma} M =_{def} \{$x $|\forall$ M $\in \gamma$: x $\in$ M$\}$ und $\bigcup\limits_{M\in\gamma} M =_{def} \{$x $|\exists$ M $\in \gamma$: x $\in$ M$\}$.
Es gilt dann der Satz:

Satz 3.2.
Besteht das Mengensystem γ nur aus zwei Mengen: $\gamma = \{M_1, M_2\}$, so gilt:
$\bigcap\limits_{M\in\{M_1,M_2\}}$ M $= M_1 \cap M_2$ und $\bigcup\limits_{M\in\{M_1,M_2\}} = M_1 \cup M_2$.

Beweis:

x$\in M_1$	x $\in M_2$	x$\in M_1 \cap M_2$	x$\in M_1 \cup M_2$	x$\in \bigcap M$	x $\in \bigcup M$	$A_i \leftrightarrow B_i$
				$M \in \gamma$	$M \in \gamma$	
		A_1	A_2	B_1	B_2	i=1,2
0	0	0	0	0	0	L
0	L	0	L	0	L	L
L	0	0	L	0	L	L
L	L	L	L	L	L	L

Außer den genannten Operationen führen wir noch eine zweistellige oder binäre Relation für Mengen ein, die mengentheoretische Inklusion, (Einbettung) also eine Aussage über je zwei Mengen:

Definition 3.4.
M $\subseteq$ N $\Leftrightarrow \forall$ x $\in$ I:(x $\in$ M $\rightarrow$ x $\in$ N).
M Teilmenge von N genau dann, wennn M $\subseteq$ N.

Es gelten folgende Sätze:

Satz 3.3.
Für jede Menge M gilt: M $\subseteq$ M. (Reflexivität der Relation $\subseteq$).

Beweis:

x $\in$ M	x$\in$ M $\rightarrow$ x $\in$ M
0	L
L	L

Satz 3.4.
Für je drei Mengen M, N, R gilt: wenn M $\subseteq$ N und N $\subseteq$ R, so M $\subseteq$ R. (Transitivität der Relation $\subseteq$).

Beweis:
Zum Beweis ist zu zeigen, daß folgende Aussage wahr ist:
$\forall$ x $\in$ I:(((x $\in$ M $\to$ x $\in$ N) $\wedge$ (x $\in$ N $\to$ x $\in$ R)) $\to$ (x $\in$ M $\to$ x $\in$ R))
Als Übungsaufgabe war gezeigt worden, daß die Aussagenverbindung
((A $\to$ B) $\wedge$ (B $\to$ C)) $\to$ (A $\to$ C) allgemeingültig ist.
Daher gilt die obige Aussage mit den speziellen Teilaussagen A $=_{def}$ x $\in$ M,
B $=_{def}$ x $\in$ N, C $=_{def}$ x $\in$ R für alle Urelemente x.

Satz 3.5.
Für je zwei Mengen M und N gilt: wenn M $\subseteq$ N und N $\subseteq$ M, so M = N. (Antisymmetrie der Relation $\subseteq$).

Beweis:
Es ist zu zeigen, daß folgende Aussage wahr ist:
$\forall$ x $\in$ I:(((x $\in M$ $\to$ x $\in$ N) $\wedge$ (x $\in N$ $\to$ x $\in$ M)) $\to$ (x $\in M$ $\leftrightarrow$ x $\in$ N)).
Setzen wir wieder A $=_{def}$ x $\in$ M und B $=_{def}$ x $\in$ N, so folgt die Behauptung aus der Allgemeingültigkeit von ((A $\to$ B) $\wedge$ (B $\to$ A)) $\to$ (A $\leftrightarrow$ B).

Anmerkung 3.1.
Für Mengensysteme γ gilt:
1. $\forall$ P $\in$ γ: ($\bigcap\limits_{M\in\gamma}$ M $\subseteq$ P $\wedge$ P $\subseteq$ $\bigcup\limits_{M\in\gamma}$ M).

Beweis:
Aus x $\in$ $\bigcap\limits_{M\in\gamma}$ M folgt für jede Menge P des Systems γ: x $\in$ P.
Aus x $\in$ P und P $\in$ γ folgt: $\exists P \in \gamma$: x $\in$ P also x $\in$ $\bigcup\limits_{M\in\gamma}$ M.
Ferner gilt:
2. $\forall$ M $\in$ γ: N $\subseteq$ M $\Rightarrow$ N $\subseteq$ $\bigcap\limits_{M\in\gamma}$ M und $\forall$ M $\in$ γ: M $\subseteq$ N $\Rightarrow$ $\bigcup\limits_{M\in\gamma}$ M $\subseteq$ N.

Beweis:
Aus x $\in$ N folgt: $\forall$ M $\in$ γ: x $\in$ M also x $\in$ $\bigcap\limits_{M\in\gamma}$ M.
Aus x $\in$ $\bigcup\limits_{M\in\gamma}$ M folgt: $\exists$ M $\in$ γ: x $\in$ M also x $\in$ N.

Bemerkung: Für Mengensysteme γ schreiben wir für $\bigcap\limits_{M\in\gamma}$ M bzw. $\bigcup\limits_{M\in\gamma}$ M abkürzend $\cap\gamma$ bzw. $\cup\gamma$.

Anmerkung 3.2.
$\cap\gamma$ (bzw. $\cup\gamma$) ist die bzgl. Inklusion größte (bzw. kleinste) Menge, die in allen Mengen von γ enthalten ist (bzw. diese umfaßt).

Anmerkung 3.3.
Jede zweistellige Relation, die die in den Sätzen S.1.3. bis S.1.5. genannten Eigenschaften der Reflexivität, Transitivität und Antisymmetrie hat, heißt Halbordnungsrelation.

Satz 3.6.
Für jede Menge M gilt: $\emptyset \subseteq$ M.

Beweis:
Da die Aussage x $\in \emptyset$ für alle x den Wahrheitswert 0 hat, hat für jede Menge M und alle x die Aussage (x $\in \emptyset \rightarrow$ x $\in$ M) den Wahrheitswert L.
Als Spezialfall der Mengendifferenz kann eingeführt werden das Komplement einer Menge.

Definition 3.5.
Komplement einer Menge N bzgl. einer Menge M.
Wenn N $\subseteq$ M, dann heißt (M - N) das Komplement von N bezüglich M.
Durch $\bar{N}$ wird das Komplement von N bzgl. der Universe I bezeichnet.

Satz 3.7. Für beliebige Mengen M, N gilt:
a) $\bar{\Phi}$ = I
b) $M \cap \bar{M} = \emptyset$
c) $M \subseteq N \leftrightarrow \bar{N} \subseteq \bar{M}$

Satz 3.8. die Morgan Regeln für zwei bzw. mehrere Mengen M, N:
a) $\overline{M \cup N} = \bar{M} \cap \bar{N}$
b) $\overline{M \cap N} = \bar{M} \cup \bar{N}$

Weiter gilt für beliebige Mengen M,N,S der
Satz 3.9.
a) M - N = M $\cap \bar{N}$
b) $M \cap N \subseteq (M \cap S) \cup (N \cap \bar{S})$
c) $(M \cup S) \cap (N \cup \bar{S}) \subseteq M \cap N$

Ist M eine Menge, so heißt das System aller Teilmengen von M die Potenzmenge $\wp$ (M) von M:

Definition 3.6. Potenzmenge
$\wp(M) =_{def} \{N \mid N \subseteq M\}$.
Die Potenzmenge von M wird auch durch 2^M bezeichnet, da für endliche M die Potenzmenge von M soviel Elemente besitzt, wie die Zweierpotenz der Anzahl der Elemente von M angibt.

Für Potenzmengen der Mengen M, N gelten die Eigenschaften

Satz 3.10. $\wp(M) \cap \wp(N) = \wp(M \cap N)$

a) $\wp(M) \cup \wp(N) \subseteq \wp(M \cup N)$ bzw. für Mengensysteme γ

b) $\bigcap\limits_{M \in \gamma} \wp(M) = \wp(\bigcap\limits_{M \in \gamma} \wp(M)) \subseteq \wp(\bigcup\limits_{M \in \gamma} M)$

c) $M \subseteq N \Rightarrow \wp(M) \subseteq \wp(N)$

Ist M eine Menge, $\wp$ (M) die Potenzmenge von M, so heißt ein Mengensystem $\gamma \subseteq \wp$ (M) eine Zerlegung oder Partition von M, wenn M durch γ in paarweise disjunkte nichtleere Teilmengen aufgespalten wird.

Definition 3.7. Zerlegung

γ Zerlegung von M genau dann, wenn 1.) $\gamma \subseteq \wp$ (M) $\setminus \{\emptyset\}$

2.) $\forall$ N, R $\in \gamma$: ((N $\neq$ R) $\rightarrow$ (N $\cap$ R = $\emptyset$))

3.) $\bigcup\limits_{N \in \gamma}$ N = M.

Es ist wohl zu unterscheiden: γ enthält nicht die leere Menge $\emptyset$ als Element, dagegen ist wegen S.1.6. natürlich die leere Menge zweiter Stufe $\emptyset'$ Teilmenge von γ, d.h.: $\emptyset \notin \gamma$ aber $\emptyset' \subseteq \gamma$.

Kuratowski gab 1920 folgende
Definition 3.8. des geordneten Paares [x, y]

Für alle x, y $\in$ I sei [x, y] $=_{def}$ {{x}, {x, y}}.

x heißt die erste Komponente und y die zweite Komponente des geordneten Paares. Das geordnete Paar selbst ist als Menge zweiter Stufe über I definiert. Diese Definition läßt sich sofort auf geordnete Paare von zwei Mengen der gleichen Stufe k über I verallgemeinern. Man benötigt aber sehr oft geordnete Paare, die aus Mengen verschiedener Stufe gebildet werden. Um auch solche geordneten Paare mengentheoretisch im Rahmen des hier gewählten Aufbaus angeben zu können, führen wir eine Stufenhebung durch Bildung von Einermengen ein.
Ist X eine Menge der Stufe k, so ist {X} eine Menge der Stufe k+1, die genau das eine Element X enthält. Bilden wir {{X}}, so ist das wieder eine Einermenge der Stufe k+2, die genau das eine Element {X} enthält. Das Verfahren können wir beliebig fortsetzen.

Satz 3.11.
Für geordnete Paare gilt:
a) [X,Y] = [X',Y'] $\Longleftrightarrow$ X = X' $\wedge$ Y = Y'
b) [X,Y] = [Y,X] $\Longleftrightarrow$ X = Y

Anmerkung 3.4.
Die Definition des geordneten Paares läßt sich erweitern zur Definition des geordneten n-Tupels $[X_1, X_2, ..., X_n]$:
Für alle natürlichen Zahlen n $\geq$ 3 und alle Mengen $X_1, X_2, ..., X_{n+1}$ sei:
$[X_1, X_2, X_3] =_{def} [[X_1, X_2], X_3]$ und
$[X_1, X_2, ..., X_{n+1}] =_{def} [[X_1, X_2, ..., X_n], X_{n+1}]$.
Durch vollständige Induktion folgt dann leicht:
$[X_1, X_2, ..., X_n] = [Y_1, Y_2, ..., Y_m] \Leftrightarrow$ n = m $\wedge \forall$ i $\in$ {1, ... , n}: $X_i = Y_i$.

Sind M und N zwei Mengen über dem Individuenbereich I (mit positiver Stufe), so besteht das kartesische Produkt M $\times$ N (Kreuzprodukt) dieser Mengen aus allen geordneten Paaren, deren erste Komponente ein Element aus M und deren zweite Komponente ein Element aus N ist. Es ist auch zugelassen, daß M = N ist. Diese Definition läßt sich in Hinblick auf Anmerkung 1.8. in naheliegender Weise zum k-fachen kartesischen Produkt der Mengen $M_1, M_2, ..., M_k$ (positiver Stufe) erweitern:

Definition 3.9.
Es seien M, N, $M_1, M_2, ...M_{k+1}$ Mengen (positiver Stufe) über einem Individuenbereich I.
$M \times N =_{def} \{p \mid \exists X \exists Y (X \in M \wedge Y \in N \wedge p = [X, Y])\}$,
$\times_{i=1}^{2} M_i =_{def} M_1 \times M_2$ und $\times_{i=1}^{k+1} M_i =_{def} (\times_{i=1}^{k} M_i) \times M_{k+1}$.

Gilt $M_1 = M_2 = ... = M_k = M$, so sei $M^k =_{def} \times_{i=1}^{k} M_i$.
Die Elemente von $\times_{i=1}^{k} M_i$ sind also alle geordnete k-Tupel
$[X_1, X_2, ..., X_k]$ mit $\forall$ i $\in$ {1, 2, ... , k}: $X_i \in M_i$.

Beispiele

1) M = {a, b, c} , N = {1, 2}.
   M $\times$ N = {[a,1],[a,2],[b,1],[b,2],[c,1],[c,2]}.
2) M = N = {1,2}. M $\times$ N = {[1,1], [1,2], [2,1], [2,2]}.
3) M = {1,2} und N = $\wp$ (M).
   M $\times \wp$ (M) = {[1, $\emptyset$], [1, {1}], [1, {2}], [1, {1,2}], [2, $\emptyset$], [2,{1}], [2, {2}], [2, {1,2}]}.
4) M sei die Menge der reellen Zahlen, dann ist M^n die Menge aller geordneten n-Tupel, deren Komponenten reelle Zahlen sind.
5) M sei eine nichtleere Menge beliebiger positiver Stufe über I. Dann ist M^2 $\times$ M = M^3 die Menge aller 3-Tupel, man sagt dazu auch Tripel (4-Tupel werden auch Quadrupel genannt), deren Komponenten Elemente aus M sind. Hingegen ist M $\times M^2$ die Menge aller geordneten Paare, deren erste Komponente Elemente aus M und deren zweite Komponente geordnete Paare von Elementen aus M sind. Ist also M $\neq \emptyset$, so ist $M \times M^2 \neq M^2 \times M$.

Für das Kartesische Produkt (Kreuzprodukt) gelten für beliebige Mengen M_i , N folgende Beziehungen

Satz 3.12.
$(M_1 \cup M_2) \times N = (M_1 \times N) \cup (M_2 \times N)$,
$N \times (M_1 \cup M_2) = (N \times M_1) \cup (N \times M_2)$,
$(M_1 \backslash M_2) \times N = (M_1 \times N) \backslash (M_2 \times N)$,
$N \times (M_1 \backslash M_2) = (N \times M_1) \backslash (N \times M_2)$,
$(M_1 \cap M_2) \times N = (M_1 \times N) \wedge (M_2 \times N)$,
$N \times (M_1 \cap M_2) = (N \times M_1) \wedge (N \times M_2)$,
$(M_1 \cap M_2) \times (M_3 \cap M_4) = (M_1 \times M_3) \wedge (M_2 \times M_4)$ gilt nicht für $\cup$,
$M_1 \subseteq M_2 \Longrightarrow M_1 \times N \subseteq M_2 \times N$ und $N \times M_1 \subseteq N \times M_2$,
$M_1 \times M_2 = \emptyset \Longleftrightarrow M_1 = \emptyset \vee M_2 = \emptyset$.

4. KORRESPONDENZEN UND FUNKTIONEN

Im Folgenden seien wieder M und N zwei nicht notwendig verschiedene Mengen beliebiger gleicher Stufe über einem Individuenbereich I.

Definition 4.1.
F heißt Korrespondenz (mehrdeutige Abbildung) aus M in N genau dann, wenn F $\subseteq$ M $\times$ N ist.
Eine Korrespondenz aus M und N ist also eine Menge von geordneten Paaren [x,y] mit x $\in$ M $\wedge$ y $\in$ N. Zur vollständigen Bestimmung einer Korrespondenz aus M in N ist nicht nur die Angabe von F, sondern auch die von M und N nötig.

Anmerkung 4.1.
Statt [x,y] $\in$ F schreibt man auch: xFy. Also:
xFy $\Leftrightarrow$ [x,y] $\in$ F $\wedge$ F $\subseteq$ M $\times$ N.
Ist F eine Korrespondenz aus M in N, so führt man folgende Begriffe ein:
y ist ein Bild von x bei F oder x ist ein Urbild von y bei F genau dann, wenn xFy.
Die Menge aller Bilder y eines Elementes x $\in$ M bei F heißt
volles Bild von x bei F und wird mit B_F (x) bezeichnet: B_F (x) $=_{def}$ {y | xFy}.
Die Menge aller Urbilder x eines Elementes y $\in$ N bei F heißt
volles Urbild von y bei F und wird mit U_F (y) bezeichnet: U_F (y) $=_{def}$ {x | xFy}.
Die Menge aller Urbilder bei F heißt Definitions- oder Vorbereich von F und wird mit Vb(F) bzw. Dom(F) bezeichnet:
Vb(F) $=_{def}$ {x |$\exists$ y (y $\in$ N $\wedge$ xFy)}.
Die Menge aller Bilder bei F heißt Werte- oder Nachbereich von F und wird mit Nb(F) bzw. Range(F)bezeichnet:
Nb(F) $=_{def}$ {y |$\exists$ x (x $\in$ M $\wedge$ xFy)}.

In den folgenden Fällen spricht man von Korrespondenzen aus bzw. von M in bzw. auf N:

	in N	auf N
aus M	Vb(F) $\subseteq$ M Nb(F) $\subseteq$ N	Vb(F) $\subseteq$ M Nb(F) = N
von M	Vb(F) = M Nb(F) $\subseteq$ N	Vb(F) = M Nb(F) = N

Da Korrespondenzen auf Mengen erklärt sind, sind zwei Korrespondenzen F aus M in N und F' aus M' in N' genau dann gleich, wenn M = M' und N = N' und F = F' gilt.

Ist F eine Korrespondenz aus M in N, so läßt sich in eindeutiger Weise eine Korrespondenz aus N in M bilden, die mit F^{-1} bezeichnet wird und die die zu F inverse Korrespondenz (Umkehrkorrespondenz) heißt:

Definition 4.2.
F sei Korrespondenz aus M in N.
$F^{-1} =_{def} \{p \mid \exists$ x $\exists$ y ([x,y] $\in$ F $\wedge$ p = [y,x])$\}$ ist Korrespondenz aus N in M und heißt inverse Korrespondenz zu F.
Nach Definition 4.2. gilt:
Vb(F^{-1}) = Nb(F), Nb(F^{-1}) = Vb(F), $(F^{-1})^{-1}$ = F

Ist F Korrespondenz aus M in N und G Korrespondenz aus N in P, so kann man durch Nacheinanderausführung (Verkettung oder Komposition) von F und G eine Korrespondenz aus M in P erhalten:

Definition 4.3.
F sei Korrespondenz aus M in N, G sei Korrespondenz aus N in P.
F $\cdot G =_{def}$ $\{$[x,y] $|x \in$ M $\wedge$ y $\in$ P $\wedge$ $\exists$ z (z $\in$ N $\wedge$ [x,z] $\in$ F $\wedge$ [z,y] $\in$ G$\}$
ist Korrespondenz aus M in P.
Bemerkung:
a) F $\cdot$ G ist immer definiert, im Sonderfall gilt F $\cdot$ G = $\emptyset$.
b) Wenn F bzw. G Korrespondenzen aus M in N (bzw. aus N in M) und F $\cdot$ G = Id_M, so heißt G Rechtsinverse von F und F Linksinverse von G.
Für Korrespondenzen gelten folgende Eigenschaften:

Satz 4.1.
Ist F_1 Korrespondenz aus M in N, F_2 Korrespondenz aus N in P und F_3 Korrespondenz aus P in Q, dann ist:
$F_1 \cdot (F_2 \cdot F_3) = (F_1 \cdot F_2) \cdot F_3$ (Assoziativgesetz)

Beweis:
Es sei [x,y] $\in F_1 \cdot (F_2 \cdot F_3)$. Dann gilt:
$\exists y_1 \in$ N: ([x,y_1] $\in F_1 \wedge [y_1, y] \in F_2 \cdot F_3$).
Wegen $[y_1, y] \in F_2 \cdot F_3$ folgt:
$\exists y_2 \in P : ([y_1, y_2] \in F_2 \wedge [y_2, y] \in F_3)$.
Wegen [x, y_1] $\in F_1$ und $[y_1, y_2] \in F_2$ ergibt sich: [x, y_2] $\in F_1 \cdot F_2$,
und wegen $[y_2, y] \in F_3$ schließlich [x,y] $\in (F_1 \cdot F_2) \cdot F_3$.
Damit ist für diese Mengen gezeigt: $F_1 \cdot (F_2 \cdot F_3) \subseteq (F_1 \cdot F_2) \cdot F_3$.
Entsprechend zeigt man $(F_1 \cdot F_2) \cdot F_3 \subseteq F_1 \cdot (F_2 \cdot F_3)$,
woraus folgt: $F_1 \cdot (F_2 \cdot F_3) = (F_1 \cdot F_2) \cdot F_3$. (Antisymmetrie der Inklusion)
Da beide Mengen Teilmengen von MxQ sind und als Korrespondenzen aus M in Q definiert sind, ergibt sich die Gleichheit der Korrespondenzen.

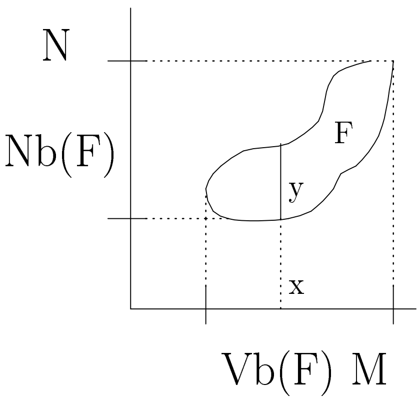
Satz 4.2.
Ist F Korrespondenz aus M in N, G Korrespondenz aus N in P, so gilt für die Korrespondenzen (F $\cdot$ G $)^{-1}$ und $G^{-1} \cdot F^{-1}$ aus P in M: (F $\cdot G)^{-1} = G^{-1} \cdot F^{-1}$.

Beweis:
Nach Definition ist F $\cdot$ G Korrespondenz aus M in P und (F $\cdot G)^{-1}$ Korrespondenz aus P in M. Entsprechend folgt, daß auch $G^{-1} \cdot F^{-1}$ Korrespondenz aus P in M ist.
Es sei [x,y] $\in (F \cdot G)^{-1}$, dann ist [y,x] $\in F \cdot G$, d.h.:
$\exists z \in$ N:([y,z] $\in F \wedge$ [z,x] $\in G$), mit y $\in$ M $\wedge$ x $\in$ P.
Daraus folgt: [z,y] $\in F^{-1} \wedge$ [x,z] $\in G^{-1} \wedge$ [x,y] $\in G^{-1} \cdot F^{-1}$.
Also gilt für die Mengen: (F $\cdot G)^{-1} \subseteq G^{-1} \cdot F^{-1}$.
Entsprechend zeigt man: $G^{-1} \cdot F^{-1} \subseteq (F \cdot G)^{-1}$. Insgesamt also: $(F \cdot G)^{-1} = G^{-1} \cdot F^{-1}$.
Aus der Gleichheit dieser Mengen folgt dann wegen der anfangs gemachten Bemerkung die Gleichheit der Korrespondenzen.

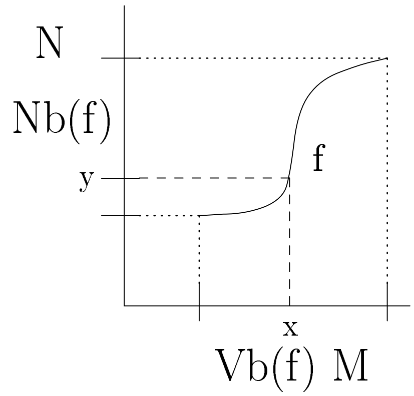
Ein besonders wichtiger Spezialfall sind die eindeutigen Korrespondenzen (Funktionen) oder (eindeutige) Abbildungen. Das sind solche, bei denen jedes Element x $\in$ M höchstens ein Bild besitzt.

Definition 4.4.
Eine Korrespondenz F aus M in N heißt Funktion aus M in N genau dann, wenn $\forall$ x $\forall$ y $\forall$ z ((x $\in$ M $\wedge$ y $\in$ N $\wedge$ z $\in$ N $\wedge$ xFy $\wedge$ xFz) $\to$ y=z).
Ist also F Funktion aus M in N, so ist für jedes x $\in$ Vb(F) das volle Bild B_F (x) eine aus genau einem Element aus N bestehende Menge. Zu jedem x $\in$ Vb(F) existiert also genau ein y $\in$ Nb(F). Dieses Element y $\in$ N heißt Wert der Funktion F an der Stelle x und wird mit F(x) bezeichnet. Ist also F Funktion und x $\in$ Vb(F), so gilt: B_F (x) = {F(x)}. Eine Funktion F mit Vb(F) $\subset$ M (echte Teilmenge von M) heißt partielle Funktion.
Wir werden zur Unterscheidung vorzugsweise Funktionen mit kleinen Buchstaben f, g,... bezeichnen.

Korrespondenzen F und Funktionen f können als Punktmengen in der Ebene wie folgt veranschaulicht werden:



(x,y) $\in$ F



f(x) = y

Bemerkung:
Der Funktionsbegriff war im 17. Jahrhundert ursprünglich als eine durch einen analytischen Ausdruck bestimmte gesetzmäßige Abhängigkeit einer Größe von einer anderen eingeführt worden.

Ist f eine Funktion von M in N, so schreibt man häufig auch:
f: M $\rightarrow$ N oder M $\rightarrow_f$ N. Die Menge aller Funktionen von M in N wird durch
$N^M =_{def} \{f | f : M \rightarrow N\}$ bezeichnet.
Ist f eine Funktion aus M auf N, so sagt man: "f ist surjektiv" oder "f ist eine Surjektion".
Unter den Funktionen oder eindeutigen Abbildungen sind wiederum die besonders interessant, deren Umkehrkorrespondenz ebenfalls eine eindeutige Abbildung ist. Sie heißen eineindeutige Abbildungen oder 1-1- Abbildungen.

Definition 4.5.
f heißt 1-1-Abbildung aus M in N genau dann, wenn f $\subseteq$ M $\times$ N $\wedge$ f eindeutig $\wedge f^{-1}$ eindeutig.

Ist f eine 1-1-Abbildung von M in N, so heißt f injektiv oder eine Injektion. Eine Abbildung, die sowohl injektiv als auch surjektiv ist, heißt bijektiv oder eine Bijektion. Eine Bijektion ist also eine 1-1-Abbildung von M auf N.

Anmerkung 4.2.
Ist f eine eindeutige Abbildung aus M in N und M' Teilmenge von M: M' $\subseteq$ M, so ist das Bild von M' bei f definiert durch:
f(M') $=_{def}$ {y |$\exists$ x(x $\in$ M' $\wedge$ y = f(x))}.

Beispiele

1) M sei eine beliebige Menge. Die Abbildung $Id_M =_{def}$ {p |$\exists$ x $\in$ M: p= [x,x]} ist eine bijektive Abbildung, also eine 1-1-Abbildung von M auf M, und heißt Identität auf M.

2) Mit Nz werde die Menge der natürlichen Zahlen bezeichnet, mit Nz^+ die Menge der positiven natürlichen Zahlen:
Nz = {0, 1, 2, 3, ...}, Nz^+ = {1, 2, 3, ...}.
Ein Abschnitt der Menge Nz^+ (Bezeichnung AbNz^+) ist eine Teilmenge von Nz^+, für die gilt:
$\forall$ n $\in$ Nz^+ :((n $\in$ $AbNz^+ \wedge n \neq 1) \rightarrow$ n-1 $\in$ $AbNz^+$).
Beispiele für Abschnitte:
$\emptyset$, {1, 2, 3, 4} , {n | n $\in$ Nz $\wedge$ 1 $\leq$ n $\leq$ m}, Nz^+.

Ferner sei M eine beliebige nichtleere Menge. Jede eindeutige Abbildung f von einem Abschnitt AbNz^+ in die Menge M heißt Folge von Elementen aus M. Zur Bezeichnung der Glieder der Folge verwendet man Indizes:
$a_n =_{def}$ f(n) $\in$ M.

Ist der Abschnitt die leere Menge, so heißt die Folge leere Folge und Vor- und Nachbereich von f sind leer. Ist der Abschnitt Nz^+ selbst, so heißt die Folge unendliche Folge, in allen anderen Fällen heißt sie endliche Folge.
Zwei Folgen f und g sind genau gleich, wenn f und g eindeutige Abbildungen von demselben Abschnitt AbNz^+ in dieselbe Menge M sind und es gilt:
$\forall$ n $\in$ AbNz^+ : f(n) = g(n).

3) Indizes werden auch noch an anderer Stelle verwendet. Sind N und M beliebige nichtleere Mengen und f eine eindeutige Abbildung von N in M, so sei wieder
$\forall$ n $\in$ N: $b_n =_{def}$ f(n).
Das Bild der Menge N (vgl. Anmerkung 4.2.) f(N) $\subseteq$ M wird dann auch mit $(b_n)_{n\in N}$ bezeichnet und heißt Familie von Elementen aus M, N heißt Indexmenge dieser Familie.
Familien mit denselben Indexmengen sind gleich, wenn sie gliedweise übereinstimmen, d.h. $(a_n)_{n\in N} = (b_n)_{n\in N} \Leftrightarrow \forall_n(n \in N \rightarrow a_n = b_n)$

$(a_m)_{m\in M}$ heißt Teilfamilie von $(b_n)_{n\in N}$ genau dann,
wenn $M \subseteq N \land \forall_m(m \in M \to a_m = b_m)$.
Falls b_n selbst wieder Mengen sind, dann heißt $(b_n)_{n\in N}$ eine Mengenfamilie.

Satz 4.3.
Ist f eindeutige Abbildung aus M in N und g eindeutige Abbildung aus N in P, so ist f · g eindeutige Abbildung aus M in P, und für alle x ∈ Vb(f · g) ⊆ M gilt:
(f · g) (x) = g(f(x)).

Beweis:
Da f und g Korrespondenzen sind, ist f · g ebenfalls eine Korrespondenz aus M in P. Ist Vb(f · g) = ∅, so ist der Satz richtig. Ist Vb(f · g) ≠ ∅, dann gibt es x ∈ Vb(f · g) und das volle Bild B_f (x) ist nicht leer. Es sei nun:
$[x, y_1] \in f \cdot g$ und $[x, y_2] \in f \cdot g$, dann ist $y_1 = y_2$ zu zeigen.
$[x, y_1] \in f \cdot g \Rightarrow \exists\ z_1 \in N : [x, z_1] \in f \land [z_1, y_1] \in g$,
$[x, y_1] \in f \cdot g \Rightarrow \exists z_2 \in N : [x, z_2] \in f \land [z_2, y_2] \in g$.
Da f bzw. g eindeutig, gilt $z_1 = z_2$ bzw. $y_1 = y_2$.
Ferner gilt: $z_1 = f(x)$ und $y_1 = g(z_1)$, also $y_1 = g(f(x))$ und $g(f(x)) = (f \cdot g)(x)$.

Satz 4.4.
Ist f eineindeutige Abbildung aus M in P und g eineindeutige Abbildung aus P in N, so ist f · g eineindeutige Abbildung aus M in N.
Beweis: Wegen S.4.3. ist f · g eindeutige Abbildung aus M in N. Nach Voraussetzung ist g^{-1} eindeutige Abbildung aus N in P und f^{-1} eindeutige Abbildung aus P in M. Daher ist nach S.4.3. $g^{-1} \cdot f^{-1}$ eindeutige Abbildung aus M in N.
Nach S.4.2. gilt aber $(f \cdot g)^{-1} = g^{-1} \cdot f^{-1}$, also f · g ist eineindeutige Abbildung aus M in N.

Beispiel:
Sei M ≠ ∅ und T(M) die Menge aller eineindeutigen Abbildungen von M auf sich selbst, d.h. T(M) $=_{def}$ {f | f eineindeutige Abbildung von M auf M }. Die Menge T(M) besitzt Gruppeneigenschaft und wird die Permutationsgruppe von M genannt. Die Abbildungen f selbst heißen Permutationen oder Transformationen von M.

5. RELATIONEN UND OPERATIONEN

Es sei M eine beliebige Menge.

Definition 5.1.
Jede Teilmenge R $\subseteq M^n$ heißt n-stellige Relation über M:
Ist N $\subseteq$ M, so heißt die über N erklärte n-stellige Relation
R$|_N =_{def}$ R $\cap N^n$ die Einschränkung von R auf N.
Gilt $[x_1, ..., x_n] \in$ R so sagt man: "die Elemente $x_1, ...x_n$ stehen in der Relation R", und schreibt auch R$(x_1, ..., x_n)$.
Da Relationen als Mengen definiert sind, ist es auch sinnvoll, vom Durchschnitt, der Vereinigung und dem Enthaltensein von Relationen zu sprechen.
Einstellige Relationen werden auch Eigenschaften genannt. Besonders wichtig sind zweistellige oder binäre Relationen über M. Binäre Relationen sind Korrespondenzen aus M in M, wir schreiben deshalb statt [x,y] $\in$ R wie bei Korrespondenzen: xRy bzw. R(x,y). Für binäre Relationen werden gewisse Eigenschaften eingeführt, die wir teilweise schon benutzt haben.

Definition 5.2.
R sei binäre Relation über M, dann heißt:
R reflexiv $\Leftrightarrow \forall$ x $\in$ M: (xRx)
R irreflexiv $\Leftrightarrow \forall$ x $\in$ M: ($\sim$ xRx)
R symmetrisch $\Leftrightarrow \forall$ x, y $\in$ M: (xRy $\rightarrow$ yRx)
R antisymmetrisch $\Leftrightarrow \forall$ x, y $\in$ M: ((xRy $\wedge$ yRx) $\rightarrow$ x=y)
R asymmetrisch $\Leftrightarrow \forall$ x, y $\in$ M: (xRy $\rightarrow\sim$ yRx)
R transitiv $\Leftrightarrow \forall$ x, y, z $\in$ M: ((xRy $\wedge$ yRz) $\rightarrow$ xRz)
R eindeutig $\Leftrightarrow \forall$ x, y, z $\in$ M: ((xRy $\wedge$ xRz) $\rightarrow$ y=z)
R voreindeutig $\Leftrightarrow \forall$ x, y, z $\in$ M: ((xRz $\wedge$ yRz) $\rightarrow$ x=y) .

Da Relationen (Relationen ohne Angabe der Stellenzahl sollen immer zweistellige (binäre) Relationen sein) spezielle Korrespondenzen sind, ist für zwei Relationen R und S über M auch R $\cdot$ S und R^{-1} erklärt.
Insbesondere ist die Identität $Id_M =_{def} \{[x, x]|x \in M\}$ ebenfalls Relation über M. Die leere Menge $\emptyset$ wird mit Nullrelation und die Menge M^2 Allrelation über M genannt.

Besonders gilt der Satz 5.1.
R sei Relation über M.
R reflexiv $\Leftrightarrow Id_M \subseteq$ R
R symmetrisch $\Leftrightarrow R^{-1} =$ R
R antisymmetrisch $\Leftrightarrow R \cap R^{-1} \subseteq Id_M$
R asymmetrisch $\Leftrightarrow R \cap R^{-1} = \emptyset$
R transitiv $\Leftrightarrow R \cdot R \subseteq R$.

Besondere Relationen
Im folgenden ist R eine Relation über einer nichtleeren Menge M.

Definition 5.3.
R heißt Äquivalenzrelation genau dann, wenn R reflexiv und R transitiv und R symmetrisch ist.

Ist R Äquivalenzrelation über M, so ist R auch Korrespondenz aus M in M. Da R reflexiv ist, folgt $Id_M \subseteq$ R, und da Id_M bijektiv ist, ist R Korrespondenz von M auf M. Daher gibt es zu jedem x $\in$ M ein nichtleeres volles Bild B_R (x) $\subseteq$ M und
B_R (x) $\neq \emptyset$.
B_R (x) heißt Restklasse oder Äquivalenzklasse von x nach (modulo) R.
Jedes Element y $\in B_R$ (x) heißt Repräsentant dieser Restklasse. Das Mengensystem aller Restklassen nach R wird mit M/R $=_{def} \{B_R(x)|\ x \in M\}$ bezeichnet und heißt Restsystem (Quotient oder Faktormenge) von M nach R.

Satz 5.2.
a) R Äquivalenzrelation über M $\Leftrightarrow R^{-1} \cup R \cdot R \cup Id_M \subseteq R$
b) Ist R Äquivalenzrelation über M $\neq \emptyset$, so ist M /R Zerlegung von M.

Beweis b):

1) Wegen $\forall$ x $\in$ M: xRx gilt x $\in B_R$ (x), also $\forall$ x $\in$ M: B_R (x) $\neq \emptyset$.
2) Es sei B_R (x) $\in$ M/R $\wedge B_R$ (y) $\in$ M/R $\wedge B_R$ (x) $\cap B_R$ (y) $\neq \emptyset$, d.h.
$\exists$ z (z $\in B_R$ (x) $\cap B_R$ (y)). Wegen z $\in B_R$ (x) $\leftrightarrow$ xRz und z $\in B_R$ (y) $\leftrightarrow$ yRz folgt aus der Symmetrie zRy und aus der Transitivität xRy. Ist u ein beliebiges Element aus B_R (x), u $\in B_R$ (x), d.h. xRu, so gilt wieder wegen der Symmetrie uRx und wegen der Transitivität: (uRx $\wedge$ xRy) $\rightarrow$ uRy, also B_R (x) $\subseteq B_R$ (y).
Entsprechend zeigt man B_R (y) $\subseteq B_R$ (x), also B_R (x) $= B_R$ (y). Damit ist gezeigt:
B_R (x) $\neq B_R$ (y) $\Rightarrow B_R$ (x) $\cap B_R$ (y) $= \emptyset$.
3) Wegen: $\forall$ x $\in$ M: x $\in B_R$ (x) folgt: M $\subseteq \bigcup_{x\in M} B_R$ (x) , und wegen $\bigcup_{x\in M} B_R$ (x) $\subseteq$ M auch die Gleichheit.

Satz 5.3.
Zu jeder Zerlegung γ von M $\neq \emptyset$ gibt es eine eindeutig bestimmte Äquivalenzrelation R über M mit M/R $= \gamma$.

Beweis:
γ sei eine Zerlegung von M. Wir definieren eine Relation R über M wie folgt:
$\forall$ x $\forall$ y ((x $\in$ M $\wedge$ y $\in$ M) $\rightarrow$ (xRy $\leftrightarrow$ $\exists$ N (N $\in \gamma \wedge$ x $\in$ N $\wedge$ y $\in$ N))).

1) R ist reflexiv. x sei ein beliebiges Element von M. Wegen $\bigcup_{N\in\gamma}$ N = M gibt es N' $\in \gamma$ mit x $\in$ N'. Daher gilt: $\exists$ N' (N' $\in$ $\gamma \wedge$ x $\in$ N' $\wedge$ x $\in$ N') d.h. xRx.
2) R ist transitiv. Es sei xRy und yRz. Dann gilt:
$\exists N_1(N_1 \in \gamma \wedge$ x $\in N_1 \wedge$ y $\in N_1) \wedge \exists N_2$ ($N_2 \in \gamma \wedge$ y $\in N_2 \wedge$ z $\in N_2$).
Wegen Y $\in N_1 \wedge$ y $\in N_2$ folgt y $\in N_1 \cap N_2 \neq \emptyset$. Da γ Zerlegung ist, folgt $N_1 = N_2 = N$, also x $\in N \wedge$ z $\in N \wedge N \in \gamma$, d.h. xRz.
3) R ist symmetrisch. Es sei xRy, d.h. $\exists$ N(N $\in \gamma \wedge$ x $\in$ N $\wedge$ y $\in$ N). Dann gilt aber auch $\exists$ N(N $\in \gamma \wedge$ y $\in$ N $\wedge$ x $\in$ N), also yRx. Wegen 1), 2) und 3) ist R Äquivalenzrelation über M.
4) N sei eine beliebige Menge aus γ. Da γ Zerlegung ist, gilt N $\neq \emptyset$. Es gibt also ein Element x $\in$ N $\subseteq$ M, und weiter: $\forall$ y $\in$ M: y $\in$ N $\leftrightarrow$ xRy,
also y $\in$ N $\leftrightarrow$ y $\in B_R$ (x). Daher gibt es zu jeder Menge N aus γ eine Restklasse B_R (x) mit N = B_R (x).
5) B_R (x) sei Restklasse nach R. Da γ Zerlegung ist, gibt es N $\in \gamma$ und x $\in$ N. Für jedes Element y $\in$ M gilt: y $\in B_R$ (x) $\leftrightarrow$ xRy, und nach der Definition von R folgt:
$\exists$ N'(N' $\in \gamma \wedge$ x $\in$ N' $\wedge$ y $\in$ N'). Wegen x $\in$ N $\cap$ N' und γ Zerlegung folgt
N = N', d.h. $\forall$ y $\in$ M: y $\in B_R$ (x) $\leftrightarrow$ y $\in$ N, also B_R (x) = N. Jedes volle Bild B_R (x) ist Element von γ.

Aus 4) und 5) folgt γ = M/R.

Anmerkung 5.1.
Es sei M eine nichtleere Menge und R Äquivalenzrelation über M. Wir betrachten die Korrespondenz ω_R von M auf M/R:
$\omega_R =_{def} \{[x, B_R(x)] \mid x \in M\}$. Da jedes x $\in$ M genau auf seine Restklasse B_R (x) abgebildet wird, ist ω_R eine eindeutige Abbildung von M auf M/R.

Definition 5.4.
Ist M eine nichtleere Menge und R Äquivalenzrelation über M, so heißt ω_R die zu R gehörige natürliche (kanonische) Abbildung (Funktion).

Satz 5.4.
Es sei f eine eindeutige Abbildung von M $\neq \emptyset$ in N. Die Relation R_f über M mit
$\forall$ x, y $\in$ M: xR_fy $\leftrightarrow$ f(x) = f(y) ist (die durch f induzierte) Äquivalenzrelation R_f.

Beweis:
Weil f Abbildung von M ist, ist der Vorbereich von f die Menge M selbst. Daher gibt es zu jedem x $\in$ M ein u $\in$ N mit u = f(x). Wegen f(x) = f(x) gilt für jedes x $\in$ M: xRx, d.h. R ist reflexiv.
Gilt xRy und yRz, so folgt: f(x) = f(y) = f(z), also xRz, R ist transitiv.

Gilt xRy, d.h. f(x) = f(y), so folgt aus f(y) = f(x) auch yRx, R ist symmetrisch und damit Äquivalenzrelation.

Satz 5.5. (Abbildungssatz)
Es sei M eine nichtleere Menge und f eine eindeutige Abbildung von M in N, R_f die durch f induzierte Äquivalenzrelation und ω_R die zu R_f gehörende natürliche Abbildung. Dann gibt es eine eineindeutige Abbildung f'von M/R_f in N (Injektion) mit
$f = \omega_R \cdot f'$.
(Jede eindeutige Abbildung von einer Menge in eine andere kann immer aus einer kanonischen und einer eineindeutigen Abbildung zusammengesetzt werden).

$$\begin{tikzcd}
M \arrow[rr, "f"] \arrow[dr, "\omega_R"'] & & N \\
& M / R_f \arrow[ur, "f'"'] &
\end{tikzcd}$$

Beweis:
Wir erklären zunächst die Abbildung f'. f' $(B_R$ (x)) $=_{def}$ f(x). Wegen der Wahl von R_f ist f' $(B_R$ (x)) unabhängig von der Auswahl der Repräsentanten x aus B_R (x) und eindeutig bestimmt. Da der Vorbereich von f die Menge M ist, ist der Vorbereich von f' die Menge M/R_f. Ferner gilt für alle x $\in$ M:
$(\omega_R \cdot$ f') (x) = f' $(\omega_R$ (x)) = f' $(B_R$ (x)) = f(x), also f = $\omega_R \cdot$ f'.
Ist f' $(B_R$(x)) = f' $(B_R$(y)), so f(x) = f(y) also xR_fy und deshalb B_R(x) = B_R(y), f' ist 1-1-Abbildung.

Wichtiges Beispiel für eine Äquivalenzrelation:

Beispiel 5.1.
Zwei Mengen heißen gleichmächtig (äquivalent) (M $\sim$ N) genau dann, wenn eine Bijektion von M auf N existiert.
Gleichmächtigkeit ist eine Äquivalenzrelation.

Anmerkung 5.2.

1) Da für jede Menge M Id_M bijektiv ist, gilt M $\sim$ M.
2) Ist M $\sim$ N und N $\sim$ P, so gibt es eine Bijektion f von M auf N und eine Bijektion g von N auf P. Dann ist f $\cdot$ g Bijektion von M auf P, also M $\sim$ P.
3) Da mit f auch f^{-1} eine Bijektion ist, folgt aus M $\sim$ N auch N $\sim$ M.

Die Äquivalenzklassen gleichmächtiger Mengen heißen Kardinalzahlen.
Eine Menge M heißt unendliche Menge, wenn es eine echte Teilmenge N von M gibt,

die zu M gleichmächtig ist, d.h. M unendlich $\Leftrightarrow \exists$ N (N $\subseteq$ M $\wedge$ N $\neq$ M $\wedge$ N $\sim$ M). (Dedekind).
Jede Menge M, die nicht unendlich ist, heißt <u>endlich</u>.
Eine Menge heißt <u>abzählbar unendlich</u>, wenn sie gleichmächtig zur Menge der natürlichen Zahlen ist. Eine abzählbare Menge ist endlich oder abzählbar unendlich, sonst heißt die Menge <u>überabzählbar</u>.
Eine Kardinalzahl heißt unendlich oder <u>transfinit</u>, wenn sie einen unendlichen Repräsentanten hat.
Bei endlichen Kardinalzahlen sind die Repräsentanten endlich und die Kardinalzahl ist umkehrbar eindeutig der Anzahl der Elemente der Repräsentanten zugeordnet. Deshalb können die natürlichen Zahlen auch als Kardinalzahlen endlicher Mengen definiert werden.

Weitere wichtige Relationen:

<u>Definition 5.5.</u>
Q sei Relation auf M. Q heißt <u>Quasihalbordnungsrelation</u> (<u>Quasiordnung</u>) auf M genau dann, wenn Q reflexiv und transitiv ist.

Jede Äquivalenzrelation ist Quasihalbordnungsrelation aber nicht umgekehrt.

<u>Satz 5.6.</u>
Es sei M eine nichtleere Menge, Q Quasihalbordnungsrelation auf M. Die Relation R mit $\forall$ x, y $\in$ M: xRy $\leftrightarrow$ (xQy $\wedge$ yQx) ist Äquivalenzrelation über M und heißt die <u>zu Q gehörige Äquivalenzrelation</u>.

<u>Beweis:</u>

1) Da Q reflexiv ist, gilt für jedes x $\in$ M: xQx $\Rightarrow$ xQx $\wedge$ xQx $\Rightarrow$ xRx, d.h., R ist reflexiv.
2) xRy $\wedge$ yRz $\Rightarrow$ xQy $\wedge$ yQx $\wedge$ yQz $\wedge$ zQy $\Rightarrow$ xQz $\wedge$ zQx wegen der Transitivität von Q, also xRz, d.h., R ist transitiv.
3) xRy $\Rightarrow$ xQy $\wedge$ yQx $\Rightarrow$ yQx $\wedge$ xQy $\Rightarrow$ yRx, d.h., R ist symmetrisch.

Verlangt man, daß eine Quasihalbordnungsrelation auch symmetrisch ist, so erhält man eine Äquivalenzrelation. Nimmt man aber statt der Symmetrie die Antisymmetrie dazu, so erhält man einen neuen Typ:

<u>Definition 5.6.</u>
R sei Relation auf M. R heißt Halbordnungsrelation (partielle Ordnung) auf M genau dann, wenn R reflexiv, transitiv und antisymmetrisch ist.

Halbordnungsrelationen werden oft mit $\subseteq$ bezeichnet.
Die Relation x $\subset$ y $=_{def}$ x $\subseteq$ y $\wedge$ x $\neq$ y heißt die zur Halbordnungsrelation $\subseteq$ gehörende

irreflexive Halbordnung (asymmetrisch).

Beispiel 5.2.

1) Ist I eine Menge und $\wp$ (I) Potenzmenge von I, so ist die Inklusion $\subseteq$ Halbordnungsrelation über $\wp$ (I).
2) $\underline{Nz^+}$ sei die Menge der positiven natürlichen Zahlen. Die Relation | (a teilt b) mit $\forall$ a, b $\in$ $\underline{Nz^+}$: a | b$=_{def}$ $\exists$ c (c $\in$ $\underline{Nz^+}$ $\wedge$ b= c $\cdot$ a) ist wegen
$\forall$ a $\in$ $\underline{Nz^+}$: a | a, $\forall$ a, b, c $\in$ $\underline{Nz^+}$: (a | b $\wedge$ b | c) $\to$ a | c und
$\forall$ a, b $\in$ $\underline{Nz^+}$: (a | b $\wedge$ b |a) $\to$ a = b Halbordnungsrelation über $\underline{Nz^+}$.

Definition 5.7.

Ist M eine nichtleere Menge, N Teilmenge von M und R Halbordnungsrelation über M, so führt man folgende Begriffe ein:

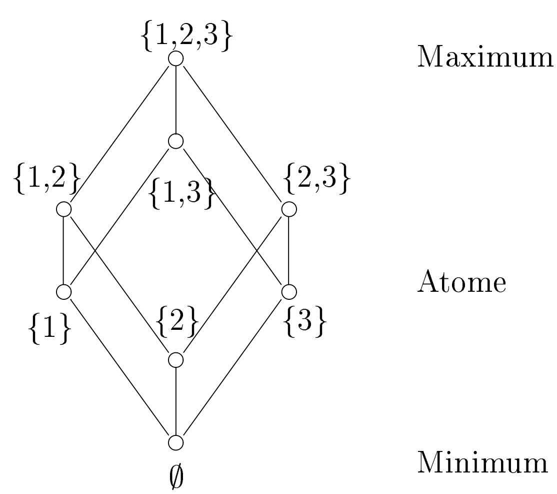
1.) x uS N (x heißt untere Schranke von N) genau dann, wenn x $\in$ M $\wedge\forall$ z $\in$ N: (xRz).
2.) x oS N (x heißt obere Schranke von N) genau dann, wenn x $\in$ M $\wedge\forall$ z $\in$ N: (zRx).
3.) x inf N (x heißt untere Grenze (infimum) von N) genau dann, wenn x $\in$ M $\wedge\forall$ z $\in$ N: (xRz $\wedge\forall$ y $\in$ M: ($\forall$ z' $\in$ N: yRz' $\to$ yRx)).
4.) x sup N (x heißt obere Grenze (supremum) von N) genau dann, wenn x $\in$ M $\wedge\forall$ z $\in$ N: (zRx $\wedge\forall$ y $\in$ M: ($\forall$ z' $\in$ N: z'Ry $\to$ xRy)).
(inf N ist also die größte untere Schranke und sup N die kleinste obere Schranke von N. Beide Schranken sind eindeutig bestimmt.)

5.) x heißt minimales Element genau dann, wenn U_R (x) = {x}, d.h., $\forall$ y $\in$ M: (yRx $\to$ y = x)
6.) x heißt maximales Element genau dann, wenn B_R (x) = {x}, d.h., $\forall$ y $\in$ M: (xRy $\to$ y = x)
7.) x heißt kleinstes Element, Minimum oder Nullelement, genau dann, wenn B_R (x) = M, d.h., $\forall$ y $\in$ M: (xRy)
8.) x heißt größtes Element, Maximum oder Einselement genau dann, wenn U_R (x) = M, d.h., $\forall$ y $\in$ M: (yRx)
(Es existiert höchstens ein Minimum oder Maximum, aber es kann mehrere minimale und maximale Elemente geben.)

Anmerkung 5.3.

a) Jedes Nullelement ist minimales Element.
   x sei Nullelement, dann gilt: B_R (x) = M. Ist y ein beliebiges Element aus U_R (x) (U_R (x) ist nicht leer, da R reflexiv), so folgt: yRx. Wegen y $\in$ M und B_R (x) = M gilt auch xRy, woraus wegen der Antisymmetrie x = y folgt, d.h. U_R (x) = {x}.
b) Jedes Einselement ist maximales Element.
   Der Beweis erfolgt analog zu a).
c) Gibt es in M ein Nullelement x, so ist dieses eindeutig bestimmt.
   x sei Nullelement, dann gilt: B_R (x) = M. Ist y ebenfalls Nullelement, also B_R (y) = M, so folgt aus x, y $\in$ M wegen Antisymmetrie xRy und yRx, also x = y.
d) Gibt es in M ein Einselement, so ist dieses eindeutig bestimmt.
   Der Beweis erfolgt analog zu c).

Beispiel 5.3.
Wir betrachten die in Beispiel 5.2.2 erklärte Halbordnung. Ist $\{a_1, ..., a_n\} \subseteq Nz^+$ eine endliche Menge positiver natürlicher Zahlen, so ist bezüglich der Teilbarkeitsrelation inf $\{a_1, ..., a_n\}$ der größte gemeinsame Teiler und sup $\{a_1, ..., a_n\}$ das kleinste gemeinschaftliche Vielfache der Zahlen $a_1, ..., a_n$.
1 ist Nullelement und damit zugleich das einzige minimale Element, maximale Elemente gibt es nicht.
Endliche nichtleere Halbordnungsrelationen R über M lassen sich durch Hasse-Diagramme graphisch veranschaulichen. Dabei entsprechen die Elemente aus M Punkten der Ebene, die miteinander verbunden werden (Nachbarn), wenn sie in der Relation R stehen. Das Maximum steht ganz oben, das Minimum ganz unten. Die oberen Nachbarn des Mimimums heißen Atome. Für die Inklusionsbeziehung über der Menge $\wp(\{1, 2, 3\})$ entsteht so das Hasse-Diagramm:



Definition 5.8.
R sei Relation auf M. R heißt Ordnungsrelation (Ordnung, totale Ordnung)auf M genau dann, wenn R Halbordnungsrelation auf M ist und $\forall$ x, y $\in$ M: (xRy $\vee$ yRx), d.h., alle Elemente der Halbordnung sind paarweise vergleichbar.

Anmerkung 5.4.
Die Eigenschaft $\forall$ x, y $\in$ M: (xRy $\vee$ yRx) heißt Linearität der Relation R. Da jede Ordnungsrelation auch Halbordnungsrelation ist, sind für Ordnungsrelationen auch die Begriffe nach Definition 5.7. erklärt. Bei Ordnungsrelationen fallen Nullelement und minimales Element einerseits und Einselement und maximales Element andererseits zusammen. Ist nämlich x minimales Element, d.h. U_R (x) = {x} und y $\in$ M beliebig gewählt, so gilt: xRy $\vee$ yRx wegen der Linearität. Ist y $\neq$ x, so folgt wegen U_R(x) = {x} daraus xRy. Daher liegt jedes von x verschiedene Element aus M in B_R (x), und da R reflexiv ist, folgt M $\subseteq$ B_R (x). Trivialerweise gilt aber B_R (x) $\subseteq$ M, also B_R(x) = M, x ist Nullelement. Entsprechend zeigt man die andere Aussage.

Definition 5.9.

Sei R eine Ordnung auf M.
a) M heißt dicht bzgl. R, wenn M mindestens zwei Elemente hat und
$\forall$ x, y $\in$ M: ((xRy $\wedge$ x $\neq$ y) $\to$ $\exists$ z $\in$ M: (x $\neq$ z $\wedge$ y $\neq$ z $\wedge$ xRz $\wedge$ zRy)) gilt.
b) M heißt diskret bzgl. R, wenn keine Teilmenge N von M bzgl. $R|_N$ dicht ist.

Satz 5.7.
Sei R eine Ordnung auf M.
Jede endliche nichtleere Teilmenge von M hat bzgl. R ein kleinstes und ein größtes Element. (Der Beweis kann induktiv über die Anzahl der Elemente geführt werden.)

Weiter führen wir eine Wohlordnung ein nach
Definition 5.10.
R sei Relation auf M. R heißt Wohlordnung auf M genau dann, wenn R Ordnungsrelation auf M ist und jede nichtleere Teilmenge von M ein kleinstes Element (bezüglich R) besitzt.

Beispiel 5.4.
Die Relation $\geq$ (größer oder gleich) ist auf der Menge der reellen Zahlen eine Ordnungsrelation. Desgleichen ist die Einschränkung dieser Relation auf die Teilmenge der ganzen Zahlen eine Ordnungsrelation und die Einschränkung auf die natürlichen Zahlen sogar eine Wohlordnung.

Definition 5.11.
Sei R Halbordnung in M und N Teilmenge von M.
N heißt Kette von M bzgl. R genau dann, wenn R $|_N$ (Einschränkung von R auf N) eine (lineare) Ordnung auf N ist.
Die Kette N heißt wohlgeordnet, wenn R $|_N$ eine Wohlordnung ist.
Darüber gilt der
Satz 5.8. (Zornsches Lemma, Maximalprinzip)
R sei Halbordnung in M.
Wenn jede wohlgeordnete Kette N von M bzgl. R eine obere Schranke besitzt, dann hat M bzg. R ein maximales Element.

Anmerkung 5.5.
Der Satz läßt sich hinsichtlich der vorausgesetzten Wohlordnung abschwächen (Schwaches Maximalprinzip), wenn von N jeweils die Existens eines Supremums (obere Grenze) bzgl. R gefordert wird. In diesem Fall spricht man von einer induktiven Halbordnung bzw. von einer bzgl. R induktiv geordneten Menge.

Über Wohlordnungen gilt der folgende
Satz 5.9. (Wohlordnungssatz)
Sei R Ordnung auf M. Dann sind folgende Aussagen äquivalent:
a) Jede nichtleere Teilmenge von M besitzt ein kleinstes Element.
b) Für jedes echte Anfangsstück A von M (A echte Teilmenge von M, deren Elemente x vor einem Element y aus M liegen, d.h., xRy gilt) besitzt M \ A (Differenz) ein kleinstes Element.
c) Jede bzgl. R absteigende Folge von Elementen aus M ist endlich.
$(a_i > a_{i+1} \Leftrightarrow a_{i+1} \ R \ a_i \wedge a_{i+1} \neq a_i)$

Weiter sei R eine Relation über einer nichtleeren Menge M. Wir werden zeigen, daß sich jede derartige Relation in eine transitive Relation, die transitive Hülle von R, einbetten läßt. Da R Korrespondenz aus M in M ist, ist R · R erklärt und Korrespondenz aus M in M, also Relation über M. Wir können daher mittels R eine unendliche Folge von Relationen durch eine rekursive Definition bilden:
$R^1 =_{def} R$; $\forall$ m $\in$ $\underline{Nz^+}$: $R^{m+1} =_{def} R^m \cdot R$.
Es gilt dann:

Satz 5.10.
$\forall$ n, m $\in$ $\underline{Nz^+}$: $R^n \cdot R^m = R^{n+m}$

Beweis:
Der Beweis erfolgt induktiv über m.
Induktionsanfang: m = 1. $R^n \cdot R^1 = R^n \cdot R = R^{n+1}$ nach Definition.
Induktionsvoraussetzung: Es sei richtig:
$\forall$ k((1 $\leq$ k $\leq$ m) $\rightarrow$ $(R^n \cdot R^k = R^{n+k})$).

Induktionsschluß: Es sei k = m+1. Wir verwenden die Definition und die in S 4.1. gezeigte Assoziativität.
$R^n \cdot R^{m+1} = R^n \cdot (R^m \cdot R) = (R^n \cdot R^m) \cdot R.$
Nach Induktionsvoraussetzung folgt dann weiter:
$R^n \cdot R^{m+1} = R^{n+m} \cdot R = R^{(n+m)+1} = R^{n+(m+1)}$ wegen der Assoziativität der Addition natürlicher Zahlen. Damit gilt die Behauptung auch für k = m+1 und nach dem Induktionsprinzip für alle m $\in$ $\underline{Nz^+}$ bei beliebigen n $\in$ $\underline{Nz^+}$.

Wir betrachten nun die Relation $R^+ = \bigcup\limits_{i=1}^{\infty} R^i$, die wie folgt definiert ist :
$R^+ =_{def} \{$p $|\exists$ i (i $\in$ $\underline{Nz^+}$ $\wedge$ p $\in R^i)\}$.
Es gilt also: $\forall$ x, y $\in$ M: xR^+ y $\leftrightarrow \exists$ i (i $\in$ $\underline{Nz^+}$ $\wedge$ xR^i y).
Wir zeigen folgende Sätze:

<u>Satz 5.11. (Transitivität)</u>
Für jede Relation R über M gilt: $R^+ \cdot R^+ \subseteq R^+$, d.h. R^+ ist transitiv.

<u>Beweis:</u>
Aus x $(R^+ \cdot R^+)$ y folgt: $\exists$ z $\in$ M: (xR^+ z $\wedge$ zR^+y) und daraus weiter:
$\exists$ n (n $\in$ $\underline{Nz^+}$ $\wedge$ xR^nz) und $\exists$ m(m $\in$ $\underline{Nz^+}$ $\wedge$ zR^my) also:
$\exists$ z (z $\in$ M $\wedge$ xR^nz $\wedge$ zR^my), d.h. x$(R^n \cdot R^m)$y $\Rightarrow$ xR^{n+m}y $\Rightarrow$ xR^+y.
Damit ist gezeigt: $R^+ \cdot R^+ \subseteq R^+$ und nach S 5.1. ist R^+ transitiv.

<u>Satz 5.12. (Einbettung)</u>
Für jede Realtion R über M gilt: R $\subseteq R^+$.

<u>Beweis:</u>
xRy $\Leftrightarrow$ xR^1 y $\Rightarrow \exists$ n(n $\in$ $\underline{Nz^+}$ $\wedge$ xR^ny) $\Leftrightarrow$ xR^+y.

<u>Satz 5.13. (Monotonie)</u>
Für jede Relation R über M und jede Relation Q über M gilt: R $\subseteq$ Q $\Rightarrow R^+ \subseteq Q^+$.

<u>Beweis:</u>
1) Wir zeigen durch vollständige Induktion über n:
R $\subseteq$ Q $\Rightarrow \forall$ n $\in$ $\underline{Nz^+}$: $R^n \subseteq Q^n$.
Induktionsanfang: n = 1. Wegen R = R^1 und Q = Q^1 gilt $R^1 \subseteq Q^1$ nach Voraussetzung. Induktionsvoraussetzung: Es sei richtig: $\forall$ k((1 $\leq$ k $\leq$ n) $\rightarrow$ $(R^k \subseteq Q^k)$).
Induktionsschluß: k = n+1.
xR^{n+1}y $\Leftrightarrow$ x$(R^n \cdot R)$y $\Leftrightarrow \exists$ z $\in$ M: (xR^nz $\wedge$ zRy) (1)
Wegen xR^nz folgt nach Induktionsvoraussetzung xQ^nz (2)
Wegen zRy folgt nach Voraussetzung zQy (3)

Aus (2) und (3) folgt x($Q^n \cdot Q$)y also xQ^{n+1}y, und aus (1) weiter: $R^{n+1} \subseteq Q^{n+1}$. Also gilt die Behauptung auch für k = n+1 und nach dem Induktionsprinzip für alle n $\in$ <u>Nz^+</u>.

2) Wir zeigen nun: R $\subseteq$ Q $\Rightarrow$ $R^+ \subseteq Q^+$.

xR^+ y $\Leftrightarrow \exists$ n(n $\in$ <u>Nz^+</u> $\wedge$ xR^n y) $\Rightarrow \exists$ n(n $\in$ <u>Nz^+</u> $\wedge$ xQ^ny) $\Leftrightarrow$ xQ^+y, also $R^+ \subseteq Q^+$.

<u>Satz 5.14. (Abgeschlossenheit)</u>

Für jede Relation R über M gilt: $(R^+)^+ = R^+$.

<u>Beweis:</u>

Aus Satz 5.12. folgt: $R^+ \subseteq (R^+)^+$, so daß nur noch $(R^+)^+ \subseteq R^+$ nachzuweisen ist.
Dazu zeigen wir zunächst durch vollständige Induktion über n:
$\forall$ n(n $\in$ <u>Nz^+</u> $\rightarrow (R^+)^n \subseteq R^+$).
Induktionsanfang: n = 1. $(R^+)^1 = R^+ \subseteq R^+$ nach Satz 3.3.
Induktionsvoraussetzung: $\forall$ k((1 $\leq$ k $\leq$ n) $\rightarrow (R^+)^k \subseteq R^+$).
Induktionsschluß: k = n + 1.
x$(R^+)^{n+1}$ y $\Leftrightarrow$ x $((R^+)^n \cdot R^+)$y $\leftrightarrow \exists$ z(z $\in$ M $\wedge$ x$(R^+)^n$ z $\wedge$ z R^+ y).
Nach Induktionsvoraussetzung folgt daraus: xR^+z und weiter x($R^+ \cdot R^+$)y und nach Satz 5.11.: xR^+y. Folglich gilt die Behauptung auch für k = n + 1 und nach dem Induktionsprinzip für alle n $\in$ <u>Nz^+</u>.
Es sei nun x$(R^+)^+$y. Dann gilt: $\exists$ n(n $\in$ <u>Nz^+</u> $\wedge$ x $(R^+)^n$ y) also: xR^+y, d.h., $(R^+)^+ \subseteq R^+$.

Da jede Relation R über M Teilmenge von M $\times$ M ist, ist $\wp$ (M $\times$ M) die Menge aller Relationen über M. Durch die Bildung von R^+ für jede Relation R über M wird eine eindeutige Abbildung f von $\wp$ (M $\times$ M) in $\wp$ (M $\times$ M) definiert:
$\forall$ R $\in \wp$ (M $\times$ M): f(R) = R^+.
Eindeutige Abbildungen von einer Menge in die gleiche Menge heißen auch <u>einstellige Operationen</u> auf dieser Menge. Daher ist $^+$ auch einstellige Operation auf der Menge aller Relationen über M. Jede einstellige Operation, die die Eigenschaften von S 5.12., 5.13., 5.14. besitzen, heißen <u>Hüllenoperationen</u>, und da das Ergebnis der Operation$^+$ wegen S 5.11 eine transitive Relation ist, heißt R^+ transitive Hülle von R.

Wir zeigen noch folgenden Satz:

<u>Satz 5.15.</u>

Für jede Relation R über M gilt: Ist R transitiv, so ist $R^+ = R$.

Beweis:
Wegen der Einbettung gilt $R \subseteq R^+$, so daß nur noch $R^+ \subseteq R$ gezeigt werden muß. Da R transitiv ist, gilt nach S 5.1. R · R ⊆ R. Daraus folgt wie bei dem Beweis zu S 5.13. zunächst ∀ n(n ∈ $\underline{Nz^+} \to R^n \subseteq R$) und dann $R^+ \subseteq R$.

Sei R wieder eine Relation über M. Bildet man nun R^+ und nimmt alle Paare [x,x] mit x ∈ M hinzu, d.h., bildet man $R^* =_{def} R^+ \cup Id_M$, so erhält man wieder eine Relation über M. Diese ist wie R^+ transitiv (weil die Paare [x,x] die Transitivität nicht stören) und zusätzlich reflexiv.
Wenn man nun analog zu den bekannten Potenzgesetzen für natürliche Zahlen definiert: $R^\circ = Id_M$, so gilt, wie man sich leicht überzeugt, Satz 5.10. nun für Exponenten n,m ∈ Nz einschließlich der Null, und es ergibt sich $R^* = \bigcup\limits_{i=0}^{\infty} R^i$.

Wir fassen zusammen in
Definition 5.12.
Es sei R eine Relation über M.
Dann heißt die Relation $R^+ =_{def} \{p \mid \exists\, i\ (i\ \in \underline{\mathrm{Nz}^+} \land p \in R^i)\}$ die transitive Hülle von R, und die Relation $R^* =_{def} \{p \mid \exists\, i\ (i \in \underline{Nz} \land p \in R^i)\}$ die reflexiv-transitive Hülle von R.

Wir hatten Relationen als spezielle Korrespondenzen eingeführt. Entsprechend sind Operationen spezielle eindeutige Abbildungen, also spezielle Funktionen.

Definition 5.13.
Es sei M eine nichtleere Menge. φ heißt k-stellige (vollständige) Operation auf M genau dann, wenn φ eine eindeutige Abbildung von M^k in M ist.
φ heißt k-stellige partielle Operation auf M genau dann, wenn φ eine eindeutige Abbildung aus M^k in M ist.
Jede k-stellige Operation ist also auch eine (k+1)-stellige Relation über M, da in Anmerkung 3.4. geordnete (k+1)-Tupel als geordnete Paare von k-Tupeln und Elementen aus N definiert sind. Nach Definition ist der Vorbereich Vb(φ) einer k-stelligen Operation auf M die Menge M^k, hingegen ist der Vorbereich einer k-stelligen partiellen Operation eine Teilmenge von M^k.
Besonders wichtig sind wieder die zweistelligen Operationen. Wir bezeichnen sie mit ∘ und schreiben statt [x,y] ∈ ∘ wie bei den zweistelligen Relationen x ∘ y.

Anmerkung 5.6.
Für zweistellige Operationen sind folgende Begriffsbildungen üblich: ∘ und ∘′ seien zwei zweistellige Operationen auf M:
∘ kommutativ ⇔ ∀ x, y ∈ M: x ∘ y = y ∘ x
∘ assoziativ ⇔ ∀ x, y, z ∈ M: (x ∘ y) ∘ z = x ∘ (y ∘ z)
∘ linksseitig distributiv bezüglich ∘′ ⇔ ∀ x, y, z ∈ M: x ∘ (y ∘′ z) = (x ∘ y) ∘′ (x ∘ z)
∘ rechtsseitig distributiv bezüglich ∘′ ⇔ ∀ x, y, z ∈ M: (x ∘′ y) ∘ z = (x ∘ z) ∘′ (y ∘ z)

$\circ$ distributiv bezüglich $\circ' \Leftrightarrow \circ$ ist linksseitig und rechtsseitig distributiv bezüglich $\circ'$
$\circ$ idempotent $\Leftrightarrow \forall$ x $\in$ M: x $\circ$ x = x
$\circ$ linksseitig kürzbar $\Leftrightarrow \forall$ x, y, z $\in$ M: (x $\circ$ y = x $\circ$ z $\rightarrow$ y = z)
$\circ$ rechtsseitig kürzbar $\leftrightarrow \forall$ x, y, z $\in$ M: (x $\circ$ z = y $\circ$ z $\rightarrow$ x = y)
$\circ$ kürzbar $\Leftrightarrow \circ$ ist linksseitig und rechtsseitig kürzbar
$e_l \in$ M linksneutrales Element von $\circ \Leftrightarrow \forall$ x $\in$ M: $e_l \circ$ x = x
$e_r \in$ M rechtsneutrales Element von $\circ \Leftrightarrow \forall$ x $\in$ M: x $\circ e_r$ = x
e$\in$M neutrales Element von $\circ \Leftrightarrow$ e ist linksneutrales und rechtsneutrales Element von$\circ$
$0_l \in$ M linkes Nullelement von $\circ \Leftrightarrow \forall$ x $\in$ M: $0_l \circ$ x = 0_l
$0_r \in$ M rechtes Nullelement von $\circ \Leftrightarrow \forall$ x $\in$ M: x $\circ$ $0_r = 0_r$
0 $\in$ M Nullelement von $\circ \Leftrightarrow$ 0 ist linkes und rechtes Nullelement von $\circ$
$\circ$ linksseitig monoton bzgl. einer binären Relation R auf M $\Leftrightarrow$
$\forall$ x, y, z $\in$ M (xRy $\rightarrow$ (x $\circ$ z) R (y $\circ$ z))
$\circ$ rechtsseitig monoton bzgl. einer binären Relation R auf M $\Leftrightarrow$
$\forall$ x, y, z $\in$ M (xRy $\rightarrow$ (z $\circ$ x) R (z $\circ$ y))
$\circ$ monoton bzgl. einer binären Relation R auf M $\Leftrightarrow \circ$ linksseitig und rechtsseitig monoton bzgl. R

Satz 5.16.
Jede zweistellige kommutative und bezüglich $\circ'$ linksseitig distributive Operation $\circ$ ist distributiv bezüglich $\circ'$

Beweis:
(x $\circ'$ y) $\circ$ z = z $\circ$ (x $\circ'$ y) = (z $\circ$ x) $\circ'$ (z $\circ$ y) = (x $\circ$ z) $\circ'$ (y $\circ$ z).

Satz 5.17.
Gibt es zu einer zweistelligen Operation $\circ$ auf M sowohl ein linksneutrales Element e_l als auch ein rechtsneutrales Element e_r, so gilt: $e_l = e_r = e$ und e ist das einzige linksneutrale und das einzige rechtsneutrale Element von $\circ$.(Analoges gilt für das Nullelement.)

Beweis:
e_l linksneutral $\Rightarrow \forall$ x $\in$ M: $e_l \circ$ x = x $\Rightarrow e_l \circ e_r = e_r$.
e_r rechtsneutral $\Rightarrow \forall$ x $\in$ M: x $\circ e_r$ = x $\Rightarrow e_l \circ e_r = e_l$ also $e_r = e_l$.
e'_l sei ebenfalls linksneutral $\Rightarrow \forall$ x $\in$ M: $e'_l \circ$ x = x $\Rightarrow e'_l \circ e_r = e_r$ und da e_r rechtsneutral ist, $e'_l \circ e_r = e'_l$, also $e'_l = e_r = e_l$. e'_r sei ebenfalls rechtsneutral, dann folgt entsprechend aus $e_l \circ e'_r = e_l$ und $e_l \circ e'_r = e'_r$ auch $e'_r = e_l = e_r$, womit der Satz bewiesen ist.

Satz 5.18.
Ist $\circ$ eine kürzbare zweistellige Operation auf M, so gibt es auf M zwei partielle Umkehrfunktionen $\circ_1$ und $\circ_2$ von $\circ$:
$\forall$ x, y, z $\in$ M: (z $\circ_1$ y = x $\leftrightarrow$ x $\circ$ y = z) $\wedge$ (x $\circ_2$ z = y $\leftrightarrow$ x $\circ$ y = z).

Beweis:
Damit $\circ_1$ und $\circ_2$ partielle Operationen sind, ist die Eindeutigkeit nachzuweisen. Aus z $\circ_1$ y = x_1 und z $\circ_2$ y = x_2 folgt nach Definition: $x_1\circ$ y = z und $x_2\circ$ y = z also $x_1\circ$ y = $x_2\circ$ y, woraus wegen der Kürzbarkeit $x_1 = x_2$ folgt. Entsprechend zeigt man die Eindeutigkeit von $\circ_2$.

Definition 5.14.
$\circ$ sei eine kürzbare zweistellige Operation auf M. $\circ$ heißt umkehrbar auf M, wenn die beiden Umkehroperationen (vollständige) Operationen auf M sind.

Anmerkung 5.7.
Ist $\circ$ eine zweistellige Operation auf M und M' eine Teilmenge von M, so definieren wir (analog zu Anmerkung 4.2.):
M' $\circ$ m' $=_{def}$ $\{$z $|$ z $\in$ M $\wedge\exists$ x $\exists$ y (x $\in$ M' $\wedge$ y $\in$ M' $\wedge$ z = x $\circ$ y)$\}$.

Definition 5.15.
Es sei $\circ$ eine zweistellige Operation auf M und M' Teilmenge von M.
Dann heißt M' stabil (abgeschlossen) bezüglich $\circ$ genau dann, wenn M' $\circ$ M' $\subseteq$ M' gilt.
Die Bedeutung stabiler Teilmengen wird aus dem folgenden Satz ersichtlich.

Satz 5.19.
Es sei $\circ$ eine zweistellige Operation auf M und M' bezüglich $\circ$ stabile Teilmenge von M. Dann wird durch $\circ$ auf M' eine Operation $\circ'$ induziert: $\forall$ x, y $\in$ M': x $\circ'$ y = x $\circ$ y.
$\circ'$ heißt die Einschränkung von $\circ$ auf M' und wird durch $\circ\,|_{M'}$ bezeichnet.

Beweis:
Da $\circ$ Operation auf M und M' $\subseteq$ M, so ist x $\circ'$ y = x $\circ$ y $\in$ M eindeutig bestimmt. Aus x, y $\in$ M' folgt weiter: x $\circ'$ y = x $\circ$ y $\in$ M' $\circ$ M' $\subseteq$ M', also ist $\circ'$ eindeutige Abbildung von M' $\times$ M' in M' und damit Operation auf M'.

Anmerkung 5.8.
Häufig verwendet man für $\circ'$ und $\circ$ das gleiche Zeichen, obgleich es im Falle M $\neq$ M' verschiedene Operationen sind.

Beispiele 5.5.
1) M sei die Menge der rationalen Zahlen, M' die zur Menge Nz der natürlichen Zahlen isomorphe Teilmenge der rationalen Zahlen (d.h. diejenigen rationalen Zahlen, deren Wert gleich dem Wert einer natürlichen Zahl ist). + bezeichne die zweistellige Operation der Addition rationaler Zahlen. M' ist bezüglich + stabil (die Summe zweier natürlicher Zahlen ist eine natürliche Zahl), daher existiert die Einschränkung von + auf M', die üblicherweise mit dem gleichen Zeichen bezeichnet wird, obgleich es sich um verschiedene Operationen handelt.

2) M sei die Menge $\underline{Nz^+}$ der positiven natürlichen Zahlen. Auf $\underline{Nz^+}$ betrachten wir folgende zweistellige Operation: $\forall$ x, y $\in \underline{Nz^+}$: x $\circ$ y $=_{def}$ x^y.
Offensichtlich ist $\circ$ eine eindeutige Abbildung von $\underline{Nz^+} \times \underline{Nz^+}$ in $\underline{Nz^+}$, also eine Operation.
$\circ$ ist nicht kommutativ: $\exists$ x, y $\in \underline{Nz^+}$: $x^y \neq y^x$.
$\circ$ ist nicht assoziativ: $\exists$ x, y, z $\in \underline{Nz^+}$: $x^{(y^z)} \neq (x^y)^z$
$\circ$ ist bezüglich + (Addition) nicht linksseitig und auch nicht rechtsseitig distributiv:
$\exists$ x, y, z $\in \underline{Nz^+}$: $x^{(y+z)} \neq x^y + x^z$ und $\exists$ x, y, z $\in \underline{Nz^+}$: $(x+y)^z \neq x^z + y^z$.
$\circ$ ist bezüglich $\cdot$ (Multiplikation) rechtsseitig distributiv: $\forall$ x, y, z $\in \underline{Nz^+}$. $(x \cdot y)^z = x^z \cdot y^z$.
$\circ$ ist bezüglich $\cdot$ nicht linksseitig distributiv: $\exists$ x, y, z $\in \underline{Nz^+}$. $x^{(y \cdot z)} \neq x^y \cdot x^z$.
$\circ$ ist rechtsseitig kürzbar: $\forall$ x, y, z $\in \underline{Nz^+}$: $x^z = y^z \rightarrow x = y$.
$\circ$ ist nicht linksseitig kürzbar: $\exists$ x, y, z $\in \underline{Nz^+}$: $x^y = x^z \ \wedge y \neq z$
$\circ$ besitzt kein linksneutrales Element.
$\circ$ besitzt ein rechtsneutrales Element: $e_r = 1$, $\forall$ z $\in \underline{Nz^+}$: $z^1 = z$.
$\circ$ besitzt ein linkes Nullelement: $0_1 = 1$, $\forall$ z $\in \underline{Nz^+}$: $1^z = 1$.
$\circ$ besitzt kein rechtes Nullelement.
Da $\circ$ nur rechtsseitig kürzbar ist, existiert nur eine partielle Umkehroperation $\circ_1$ auf $\underline{Nz^+}$: z $\circ_1$ y $=_{def}$ $\sqrt[y]{z}$.

Schränkt man $\circ$ auf die stabile Teilmenge $\underline{Nz^+} \setminus \{1\}$ ein, so ist die Einschränkung auch linksseitig kürzbar und es existiert auf $\underline{Nz^+} \setminus \{1\}$ auch die zweite partielle Umkehroperation: x $\circ_2$ z $=_{def}$ ^{x}log z. Dann gilt: x^y = z $\Leftrightarrow x = \sqrt[y]{z} \Leftrightarrow$ y = ^{x}log z.

6. ALGEBRAISCHE STRUKTUREN

Von den Objekten, die zu Mengen zusammengefaßt wurden, haben wir zunächst nur angenommen, daß sie wohl unterscheidbar sind. Durch Relationen und Operationen werden sie zueinander in Beziehung gesetzt. Die Mengen selbst werden durch derartige Beziehungen strukturiert und beschreiben damit konkrete Strukturen bzw. deren Abstraktionen. Mengen, die auf diese Weise als Objektbereiche von bestimmten Relationen und Operationen strukturiert sind, werden algebraische Strukturen genannt.

Definition 6.1.
M sei eine nichtleere Menge, $(f_i)_{i \leq s}$ eine endliche Familie von Operationen auf M, d.h., $f_i : M^{m_i} \rightarrow M$ und $(R_j)_{j \leq t}$ eine endliche Familie von Relationen über M, d.h., $R_j \subseteq M^{n_j}$, mit $m_i, n_j \in$ Nz, dann heißt das (s+t+1)-Tupel S = (M, $f_1, ..., f_s, R_1, ..., R_t$) algebraische Struktur (Algebra) über M.

M heißt Trägermenge von S m_i bzw. n_j die Stelligkeit (Arität) der Operationen bzw. Relationen aus S. Das Tupel $(m_1, ..., m_s; n_1, ..., n_t)$ wird der Typ (Signatur) von S genannt.
Falls nur Relationen vorgegeben werden, spricht man auch von Relational.
Mit Hilfe der Relationen und Operationen werden Eigenschaften der Objekte aus M beschrieben. Später werden auch Strukturen mit mehreren Trägermengen (Sorten) betrachtet.

Beispiele:
a) (Nz, + , $\cdot$, $\leq$) Natürliche Zahlen mit Addition, Multiplikation und kleiner-gleich Beziehung vom Typ (2,2;2)
b) $(2^M, \cap, \cup, -, \subseteq)$ Boolsche Algebra mit Durchschnitt, Vereinigung und Komplement als Operation und Inklusion als Relation vom Typ (2,2,1;2)

Definition 6.2.
Eine Struktur S' = (M', $f'_1, ..., f'_s, R'_1, ..., R'_t$) heißt Unterstruktur von S = (M, $f_1, ..., f_s, R_1, ..., R_t$), wenn M' $\subseteq$ M, die Typen von S' und S übereinstimmen und f'_i bzw. R'_j die Einschränkungen von f_i bzw. R_j auf M' sind.

Im Folgenden sind S = (M, $f_1, ..., f_s, R_1, ...R_t$) und S' = (M', $f'_1, ..., f'_s, R'_1, ...R'_t$) Strukturen gleichen Typs $(m_1, ..., m_s; n_1, ..., n_t)$. Wir betrachten nun Abbildungen über solchen Strukturen.

Definition 6.3.
a) Eine Funktion φ von M in M' heißt Homomorphismus von S in S', wenn:
   1.) $\varphi\ (f_i(x_1, ..., x_{m_i})) = f_i'(\varphi(x_1), ..., \varphi(x_{m_i}))$ für alle $1 \leq$ i $\leq$ s, $x_1, ..., x_{m_i} \in$ M und
   2.) wenn $[x_1, ..., x_{n_j}] \in R_j$, dann auch $[\varphi(x_1), ..., \varphi(x_{n_j})] \in R_j'$ für alle $1 \leq$ j $\leq$ t, $x_1, ...x_{n_j} \in$ M.
b) φ heißt starker Homomorphismus, wenn zusätzlich zu 2) für alle $1 \leq$ j $\leq$ t, $y_1, ..., y_{n_j} \in$ M' mit $[y_1, ..., y_{n_j}] \in R_j'$ auch $x_1, ..., x_{n_j} \in M$ existieren, so daß $\varphi(x_i) = y_i$ für alle $1 \leq$ i $\leq n_j$ und $[x_1, ..., x_{n_j}] \in R_j$ gilt.
c) S' heißt homomorphes Bild von S (S $\rightrightarrows$ S'), wenn ein Homomorphismus von S auf S' existiert (surjektiv).
d) S' heißt isomorph zu S (S $\approx$ S'), wenn eine bijektive Funktion (Isomorphismus) φ von M auf M' existiert, für die die Eigenschaft a1.) und $[x_1, ..., x_{n_j}] \in R_j \ \leftrightarrow [\varphi(x_1), ...\varphi(x_{n_j})] \in R_j'$ für alle $1 \leq$ j $\leq$ t, $x_1, ..., x_{n_j} \in M$ gilt.

Eigenschaften
1.) Wenn φ Homomorphismus von S in S' und ψ Homomorphismus von S' in S", dann ist $\varphi \cdot \psi$ Homomorphismus von S in S".
2.) Wenn φ Isomorphismus von S auf S', dann ist φ^{-1} Isomorphismus von S' auf S.
3.) Die Relation $\rightrightarrows$ ist reflexiv und transitiv, d.h.,S$\rightrightarrows$S, (S $\rightrightarrows$ S' $\wedge$ S'$\rightrightarrows$ S")$\rightarrow$ S $\rightrightarrows$ S".
4.) Die Relation $\approx$ ist eine Äquivalenzrelation.

Definition 6.4.: Kongruenzrelation und Faktorstruktur
a) Sei S = (M, $f_1, ..., f_s, R_1, ..., R_t$) eine Struktur und R eine Relation über M. R heißt stabil (kompatibel) bzgl. einer Operation f_i von S, wenn für alle $x_1, y_1, ..., x_{m_i},\ y_{m_i} \in$ M aus $\{[x_k, y_k] \mid 1 \leq$ k $\leq m_i\} \in$ R folgt: $[f_i(x_1, ..., x_{m_i}), f_i(y_1, ..., y_{m_i})] \ \in$ R.
b) Eine Äquivalenzrelation R $\subseteq M^2$ auf M heißt Kongruenzrelation der Struktur S = (M, $f_1, ..., f_s, R_1, ...R_t$), wenn R stabil bzgl. jeder Operation f_i von S ist.
c) Die Struktur S$|_R \ =_{def}$ (M$|_R$, $f_1^*, ..., f_s^*, R_1^*, ..., R_t^*$) heißt Faktorstruktur nach der Kongruenzrelation R der Struktur S = (M, $f_1, ..., f_s, R_1, ...R_t$), wenn gilt:
   1.) M$|_R$ = {[x] $_R$ | x $\in$ M} Faktormenge von M nach R,
   2.) $f_i^*\ ([x_1]_R, ..., [x_{m_i}]_R) = [f_i(x_1, ..., x_{m_i})]_R$ und
   3.) $[[x_1]_R, ..., [x_{n_j}]_R] \ \in R_j^*$ genau dann, wenn $y_1 \in [x_1]_R, ...y_{n_j} \in\ [x_{n_j}]_R$ existieren mit $[y_1, ..., y_{n_j}] \ \in R_j$.
   (Dabei bezeichnet [x]$_R$ die Restklasse B_R(x) von x nach R.)

Satz 6.1.
Sei S = (M, $f_i, ..., f_s, R_1, ...R_t$) eine Struktur und R $\subseteq M^2$ Kongruenzrelation von S. Die Funktion φ (kanonische Abbildung) von M in M$|_R$ mit φ(x) = [x]$_R$ für alle x $\in$ M ist Homomorphismus von S in S$|_R$.

Beweis
Nach Definition der Faktorstruktur und Konstruktion von φ gilt:

a) $\varphi(f_i(x_1,...,x_{m_i})) = [f_i(x_1,...,x_{m_i})]_R = f_i^*([x_1]_R,...,[x_{m_i}]_R) = f_i^*(\varphi(x_1),...,\varphi(x_{m_i}))$ für alle $1 \leq$ i $\leq$ s, $x_1,...,x_{n_i} \in$ M, d.h., die Eigenschaft 1.) des Homomorphismus ist erfüllt.

b) Aus $[x_1,...,x_{n_j}] \in R_j$ und $x_i \in [x_i]_R$ (R Äquivalenzrelation) folgt $[[x_1]_R,...,[x_{n_j}]_R] \in R_j^*$ und damit auch $[\varphi(x_1),...,\varphi(x_{n_j})] \in R_j^*$ für alle $1 \leq$ j $\leq$ t, $x_1,...,x_{n_j} \in$ M, d.h., die Eigenschaft 2.) des Homomorphismus ist erfüllt.

Beispiele:

1.) Sei Nz die Menge der natürlichen Zahlen und + die für diese erklärte Addition. Für geordnete Paare [a,b] natürlicher Zahlen führen wir die Operation $\oplus$ mit [a,b] $\oplus$ [c,d] $=_{def}$ [a+c , b+d] ein und betrachten die Struktur Z = (Nz^2, $\oplus$). Auf Nz^2 ist $\sim$ mit

   [a,b] $\sim$ [c,d] genau dann, wenn a+d = b+c

   eine Äquivalenzrelation. Mit der Operation $+_z$ definiert durch $[[a,b]]_\sim +_z [[c,d]]_\sim =_{def} [[a,b] \oplus [c,d]]_\sim$ ist $\sim$ Kongruenzrelation der Struktur Z und die Struktur $(\mathrm{Nz}^2|_\sim, +_z)$ Faktorstruktur Z $|_\sim$ von Z. Die Elemente dieser Struktur entsprechen gerade den ganzen Zahlen mit deren Addition.

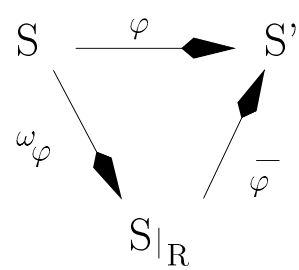
2.) In Analogie zu Beispiel 1.) führen wir ein [a,b] $\oplus$ [c,d] $=_{def}$ [$a\cdot$ d + b $\cdot$ c, b $\cdot$ d] wo $\cdot$ die Multiplikation für natürliche Zahlen bezeichnet. Die Äquivalenzrelation [a,b] $\sim$ [c,d] $=_{def}$ [a $\cdot$ d = b $\cdot$ c] ist Kongruenzrelation der Struktur (Nz^2 , $\oplus$) und die Struktur $(\mathrm{Nz}^2|_\sim, \oplus_r)$ mit $[[a,b]]_\sim \oplus_r [[c,d]]_\sim =_{def} [[a,b] \oplus [c,d]]_\sim$ ist Faktorstruktur von $(\mathrm{Nz}^2, \oplus)$. Die Elemente dieser Struktur entsprechen den positiven rationalen Zahlen.

Satz 6.2. (Homomorphiesatz)
Es seien S = (M, $f_i,...,f_s,R_1,...,R_t$) und S' = (M', $f_i',...,f_s',R_1',...R_t'$) zwei Strukturen gleichen Typs.
Zu jedem (starken) Homomorphismus φ von S auf S' existiert eine Kongruenzrelation R von S, so daß die kanonische Abbildung $\bar{\varphi}$ von der Faktorstruktur S$|_R$ in S' mit $\bar{\varphi}$ ([x]$_R$)= $\varphi(x)$ ein (Isomorphismus) Homomorphismus von S$|_R$ auf S' ist.

Beweis:
Als Kern von φ bilden wir zunächst die Relation R mit [x,y] $\in$ R genau dann, wenn φ (x) = φ (y) für alle x, y $\in$ M. R ist als Äquivalenzrelation stabil bzgl. jeder Operation f_i von S, denn mit $[x_k, y_k] \in$ R, d.h., $\varphi(x_n) = \varphi(y_k)$, und wegen Homomorphieeigenschaft 1) von φ gilt $f_i'(\varphi(x_1),...,\varphi(x_{m_i})) = f_i'(\varphi(y_1),...,\varphi(y_{m_i}))$ und damit $\varphi(f_i(x_1,...,x_{m_i})) = \varphi(f_i(y_1,...,y_{m_i}))$, d.h., $[f_i(x_1,...,x_{m_i}), f_i(y_1,...,y_{m_i})] \in$ R. R ist also eine Kongruenzrelation von S.
Weiter bilden wir die Faktorstruktur S$|_R$ = (M$|_R$, $f_i^*,...,f_s^*,R_1^*,...,R_z^*$).
Für die kanonische Abbildung $\bar{\varphi}$ von S$|_R$ in S' gilt dann $\bar{\varphi}(f_i^*([x_1]_R,...,[x_{m_i}]_R)) = \bar{\varphi}([f_i(x_1,...x_{m_i})]_R) = \varphi(f_i(x_1,...,x_{m_i})) = f_i'(\varphi(x_1),...,\varphi(x_{m_i})) = f_i'(\bar{\varphi}([x_1]_R,...,\bar{\varphi}([x_{m_i}]_R))$

bzw. aus $[[x_1]_R, ..., [x_{n_j}]_R] \in R_j^*$ folgt $[\bar{\varphi}[x_1]_R, ..., \bar{\varphi}[x_{n_j}]_R] \in R'_j$.
Also ist $\bar{\varphi}$ Homomorphismus von $S|_R$ auf S'.
Da die Bedingung 3) für die Faktorstruktur auch in der umgekehrten Richtung gilt, erhält man im Falle des starken Homorphismus φ einen Isomorphismus von $S|_R$ auf S'.

Folgerung 6.3.
Zu jedem (starken) Homomorphismus φ von S auf S' existiert ein (Isomorphismus) Homomorphismus $\bar{\varphi}$ von der Faktorstruktur $S|_R$ von S zum Kern R von φ auf S', so daß für die von φ erzeugte kanonische Abbildung ω_φ gilt: $\varphi = \omega_\varphi \cdot \bar{\varphi}$.



Die kanonische Abbildung, die auch ein Homomorphismus von S auf $S|_R$ ist, wird definiert durch ω_φ (x) = $[x]_R$, d.h., x wird die Restklasse $[x]_R$ nach R zugeordnet.

Folgerung 6.4.
Zu jeder Kongruenzrelation R von S kann jeder starke Homomorphismus φ von S auf eine typgleiche Struktur S' durch Verkettung der von φ erzeugten kanonischen Abbildung ω_φ von S auf die Faktorstruktur $S|_R$ und einem Isomorphismus von $S|_R$ auf S' erzeugt werden.

Folgerung 6.5.
Die Kongruenzrelationen einer Struktur S können durch die homomorphen Bilder von S und umgekehrt dargestellt werden. (Homomorphismen zwischen algebraischen Strukturen können auf die Faktorstrukturen nach einer beliebigen Kongruenzrelation bezogen werden.)

Beispielstrukturen
Wichtige algebraische Strukturen, die später noch ausführlich behandelt werden, sind z.B.:

1.) Graphen:
Die Struktur (M,R) vom Typ (;2) wird gerichteter Graph genannt. Die Elemente der Menge M heißen Knoten, die aus R Kanten. Knoten a,b $\in$ M können als Punkte der Ebene und Kanten [a,b] $\in$ R als gerichtete Verbindungslinien (Pfeile, Bögen) von a nach b aufgefaßt werden. Durch Bedingungen an die Knotenrelation R können spezielle Typen von Graphen, wie Bäume, Netzpläne u.a., ausgezeichnet werden.
2.) Halbgruppen:

Die Struktur (M,f) vom Typ (2;) wird Halbgruppe genannt, wenn die zweistellige Operation f über M die Bedingung der Assoziativität erfüllt, d.h., $f(x, f(y,z)) = f(f(x,y), z)$ für alle $x,y,z \in M$. So ist z.B. die Menge der natürlichen Zahlen zusammen mit der Addition bzw. Multiplikation eine solche Halbgruppe. Spezielle Halbgruppen (Worthalbgruppen) spielen eine wichtige Rolle bei der Beschreibung von formalen Sprachen (z.B. Programmiersprachen).

3.) Verbände:

Eine Struktur $(M, \cap, \cup)$ vom Typ (2,2;) heißt Verband, wenn die beiden zweistelligen Operationen $\cap$ (Infimum), $\cup$ (Supremum) über M für alle $x,y \in M$ die folgenden Bedingungen erfüllen:

$x \cup y = y \cup x, \qquad x \cap y = y \cap x$ (Kommutativität)

$x \cup (y \cup z) = (x \cup y) \cup z, \qquad x \cap (y \cap z) = (x \cap y) \cap z$ (Assoziativität)

$x \cap (x \cup y) = x, \qquad x \cup (x \cap y) = x$ (Absorption, Verschmelzung)

Von besonderer Bedeutung sind spezielle Verbände (z.B. vollständige Verbände), die u.a. bei der Beschreibung der Semantik (der inhaltlichen Bedeutung) von Programmiersprachen eingesetzt werden.

7. GRAPHEN, VERBÄNDE, BOOLSCHE ALGEBREN

Graphen und ihre Spezialfälle sind universelle algebraische Strukturen, die in der Informatik zur Beschreibung von Daten bzw. Objekten herangezogen werden.

Definition 7.1.

a) Ist M eine nichtleere Menge und R eine binäre Relation über M, so heißt die Struktur G = (M,R) gerichteter Graph.
Die Elemente von M heißen Knotenpunkte des Graphen und die Elemente von R Bögen, Pfeile oder gerichtete Kanten des Graphen.

b) (M',R') heißt Untergraph von (M,R) genau dann, wenn M' $\subseteq$ M und R' = R $\cap$ (M' $\times$ M'), d.h. R' ist die Einschränkung R$|_{M'}$ von R auf M'.

c) (M',R') heißt Teilgraph von (M,R) genau dann, wenn M' $\subseteq$ M und R' $\subseteq$ R.

d) a $\in$ M heißt Nachfolger von b $\in$ M genau dann, wenn [b,a] $\in$ R.

e) a $\in$ M heißt Vorgänger von b $\in$ M genau dann, wenn [a,b] $\in$ R.

f) Der Bogen [a,b] $\in$ R heißt Schleife, falls a = b.

Definition 7.2.

Sei G = (M,R) gerichteter Graph.

a) Eine endliche Folge $(a_0, ..., a_n)$ von Elementen aus M mit $a_0 = a$ und $a_n = b$, wo $[a_i, a_{i+1}] \in$ R für alle 0 $\leq$ i < n heißt (endlicher) Weg in G der Länge n von a nach b.
Die Menge aller endlichen Wege in G von a nach b wird durch W_G(a,b) und die Menge aller endlichen Wege in G durch W(G) bezeichnet.

b) Eine endliche Folge $(a_0, ..., a_k)$ von Elementen aus M mit $a_0 = a$ und $a_k = b$ und $[a_i, a_{i+1}] \in R \cup R^{-1}$ für alle 0 $\leq$ i < k heißt Kette von a nach b.

c) Ein Weg (Kette) $(a_0, ..., a_n)$ heißt wiederholungsfrei , wenn $a_i \neq a_j$ $(\{a_i, a_{in}\} \neq \{a_j, a_{jn}\})$ für alle 0 $\leq$ i $\neq$ j < n.

d) Ein wiederholungsfreier Weg (Kette) $(a_0, ..., a_n)$ heißt Elementarkreis (Zyklus), wenn $a_0 = a_n$.

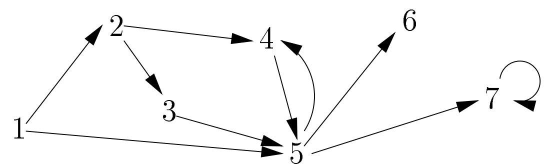
e) Ein Graph (M,R) heißt (stark) zusammenhängend, falls zu je zwei verschiedenen Elementen a, b aus M eine (Weg)Kette von a nach b existiert.

f) Ein Graph G heißt kreisfrei (zyklenfrei), wenn es in G keine Elementarkreise (Zyklen) gibt.

g) a $\in$ M heißt Eingangselement oder minimales Element von (M,R), wenn a in (M,R) keinen Vorgänger hat.
b $\in$ M heißt Ausgangselement oder maximales Element von (M,R), wenn b in (M,R) keinen Nachfolger hat.

Beispiel

Graphen mit endlicher Knotenmenge lassen sich durch Punkte (Knotenpunkte) und Pfeile (Bögen, gerichtete Kanten) in der Ebene veranschaulichen.
M={1, 2, 3, 4, 5, 6, 7}, R = {[1,2], [1,5], [2,3], [2,4], [3,5], [4,5], [5,4], [5,6], [5,7], [7,7]}
Der Graph (M,R) läßt sich durch folgende Figur veranschaulichen.



(2, 3, 5, 4) ist ein wiederholungsfreier Weg von 2 nach 4.
(2, 4, 5, 4) ist ein Weg von 2 nach 4.
(6, 5, 7) und (6, 5, 4, 2, 3, 5, 7) sind Ketten von 6 nach 7.
(7, 7) ist Schleife und (4, 5, 4) ein Elementarkreis.
(M, R) ist zusammenhängend, aber nicht kreisfrei.
1 ist minimales und 6 ist maximales Element.
(M',R') mit M' = {1, 2, 3, 4}, R' = {[1,2], [2,3], [2,4]}ist Untergraph von (M,R).
(M',R') mit M' = M, R' = {[1,2], [2,3], [4,5]} ist Teilgraph von (M,R).

Satz 7.1.

(M,R) sei ein Graph. In (M,R) gibt es genau dann einen Weg von a nach b, wenn [a,b] ∈ R^+ (transitive Hülle von R).

Beweis:

1) Wenn es einen Weg $(a_0, ..., a_k) \in$ W(a,b) mit $a_0 = a$ und $a_k = b$ gibt, dann folgt:
   $[a_0, a_1] \in$ R, $[a_1, a_2] \in$ R also $[a_0, a_2] \in R^2$ und wegen $[a_2, a_3] \in$ R auch:
   $[a_0, a_3] \in R^3$. Durch Induktion folgt dann $[a_0, a_k] \in R^k \subseteq R^+$.
2) Wenn [a,b] ∈ R^+, dann gibt es eine natürliche Zahl k > 0 mit (a,b) ∈ R^k.
   Ist k=1, so [a,b] ∈ R und (a,b) ∈ W(a,b).
   Ist k=2, so gibt es $a_1 \in$ M und $[a, a_1] \in$ R und $[a_1, b] \in$ R und $(a, a_1,$ b) ∈ W(a,b).
   Mit Induktion folgt daraus: $(a, a_1, ..., a_{k-1}, b) \in$ W(a,b).

Anmerkung

Zu jedem Weg W von a nach b in einem Graphen (M,R) gibt es genau eine positive natürliche Zahl k mit [a,b] ∈ R^k. k = l(w) heißt Länge des Weges von a nach b (Anzahl der Bögen auf diesem Weg).

Satz 7.2.
(M,R) sei ein Graph. (M,R) ist genau dann kreisfrei, wenn $R^+ \cap Id_M = \emptyset$.

Beweis:
a) Es sei $R^+ \cap Id_M \neq \emptyset$, dann gibt es a $\in$ M und [a,a] $\in R^+$. Es gibt also eine positive natürliche Zahl k, so daß [a,a] $\in R^k$. Unter all diesen natürlichen Zahlen sei k so gewählt, daß [a,a] $\notin R^i$ für alle 1 $\leq$ i $<$ k, was wegen der Wohlordnung der natürlichen Zahlen bezüglich $\leq$ möglich ist. Nach Satz 7.1. gibt es dann einen Weg $(a_0, ...a_k) \in$ W(a,a) mit $a_0 = a_k = a$. Außerdem sind die Elemente $a_0, ..., a_{k-1}$ paarweise verschieden. Angenommen, es gäbe i, j $\in$ {0, ... , k-1} mit i $<$ j und $a_i = a_j$, so wäre im Falle i=0 auch $(a_j, ..., a_k)$ ein Weg der Länge k-j von a nach a und im Falle i $\neq$ 0 auch $(a_0, ..., a_{i-1}, a_j, ..., a_k)$ ein Weg der Länge k-j+i $<$ k, d.h., in beiden Fällen wäre [a,a] $\in R^{k-j+i}$ im Widerspruch zur Wahl von k.
Daher ist $(a_0, ..., a_k)$ Elementarkreis in (M,R) und der Graph ist nicht kreisfrei.
b) Gibt es in (M,R) einen Elementarkreis $(a_0, ..., a_k)$ mit $a_0 = a_k = a$, so gilt: [a,a] $\in Id_M \cap R^+$, d.h., $R^+ \cap Id_M \neq \emptyset$.

Satz 7.3.
(M,R) sei ein Graph. Gibt es a $\in$ M mit für alle a $\neq$ b $\in$ M $\setminus$ {a}: ([a,b] $\in R^+$), so ist (M,R) zusammenhängend.

Beweis:
Angenommen, es gibt ein derartiges Element a mit der angegebenen Eigenschaft. Wir zeigen: Sind x und y zwei verschiedene aber beliebige Elemente aus M, so gibt es eine Kette von x nach y. Wir unterscheiden drei Fälle:
1) x = a. Nach Voraussetzung ist [a,y] $\in R^+$, d.h., es gibt einen Weg von a nach y, also eine Kette von x nach y.
2) y = a. Durch Vertauschung der Bezeichnung erhält man 1).
3) x $\neq a$ und y $\neq a$. Dann gilt: [a,x] $\in R^+ \wedge$ [a,y] $\in R^+$, d.h., es gibt Wege $(a, a_1, ..., a_{k-1},$ x) und $(a, b_1, ..., b_{i-1}$, y). Dann ist aber (x, $a_{k-1}, ...a_1, a, b_1, b_{i-1}$, y) eine Kette von x nach y.

Anmerkung
Ein Graph (M,R) läßt sich auch als Struktur (M,K,f) aus zwei disjunkten Trägermengen M (Knotenmenge) und K (Kantenmenge) mit M $\cap$ K = $\emptyset$ und einer Funktion f von K in die Menge M^2 darstellen.
Durch f wird jeder Kante k $\in$ K ein Paar [a,b] von Knoten aus M zugeordnet, die man Endpunkte (a Anfangspunkt, b Endpunkt) der Kante k nennt.

Definition 7.3.

a) Ein Graph (M,R) heißt ungerichteter Graph, wenn R symmetrisch ist.

b) Eine Struktur (M,K,f) heißt ungerichteter Graph, wenn $M \cap K = \emptyset$ und f eine Funktion von K in die Potenzmenge 2^M über M mit $1 \leq |\, f(k) \,| \leq 2$ (Einermenge oder Zweiermenge) für alle $k \in K$. Mit f(k) = {a,b} sind $a,b \in M$ die Endpunkte der Kante. f(k) = {a} ist eine Schleife.

(Beide Definitionen sind gleichberechtigt.)

Anmerkung

Sei G= (M,R) ein Graph und ein Knotenpaar [a,b] stehe in der Relation $\sim$ genau dann, wenn a und b durch einen Weg verbunden sind oder a = b ist.
Dann ist $\sim$ Äquivalenzrelation über M und jede (Äquivalenz-)Klasse der Faktorstruktur $G|_\sim$ erzeugt einen maximalen zusammenhängenden Untergraphen (Komponente) von G.

Bezeichnungen

Mit d_G(a,b) bezeichnen wir die Länge des kürzesten Weges (Distanz) von a nach b in G. Falls a und b durch keinen Weg verbunden sind, ist $d_G(a,b) = \infty$
$d_{max}(G) = \max \{d_G(a,b) < \infty \mid a,b \in M\}$ bezeichnet die größte Distanz in G.

Definition 7.4.

a) Ein Graph (M,R) heißt Netzplan, wenn (M,R) endlich und kreisfrei mit genau einem minimalen und genau einem maximalen Element ist.

b) Ist (M,R) Netzplan und $a \in M$, so ist die Stufe S(a) von a in (M,R) definiert als Länge des längsten Weges vom minimalen Element nach a. Das minimale Element hat die Stufe 0.

Beispiel

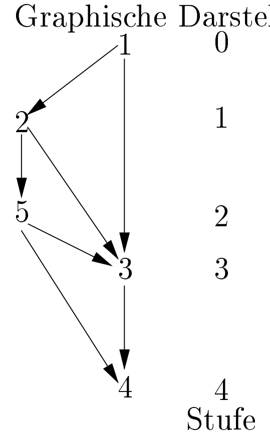
Der Graph (M,R) mit M = {1, 2, 3, 4, 5}, R = {[1,2], [1,3], [2,3], [2,5], [3,4], [5,3], [5,4]} ist Netzplan. 1 ist minimales Element.

Bestimmung der Stufe:

$S(i) = \sup \{j \mid [1,i] \in R^j\}$.

i	S(i)	
1	0	minimales Element
2	1	
3	3	
4	4	maximales Element
5	2	

Graphische Darstellung:



Definition 7.5.
Sei G = (M, R) ein (gerichteter) Graph und für a, b $\in$ M bezeichne W_G (a,b) die Menge aller Wege von a nach b in G.

a) Der Knoten b $\in$ M heißt erreichbar vom Knoten a $\in$ M, falls W_G (a,b) $\neq \emptyset$ oder a = b gilt.
Die Knotenmenge N $\subseteq$ M heißt erreichbar vom Knoten a $\in$ M, falls jeder Knoten aus N von a erreichbar ist.
Die Knotenmenge N' $\subseteq$ M heißt erreichbar von der Knotenmenge N $\subseteq$ M, falls jeder Knoten N' von einem Knoten aus N erreichbar ist.

b) Eine (nichtleere) Knotenmenge B $\subseteq$ M heißt Basis (Knotenbasis) von G, falls M erreichbar von B und M von keiner echten Teilmenge B' $\subset$ B von B erreichbar ist.
(Eine Basis ist eine kleinste nichtleere Teilmenge von M, von der aus alle Knoten von M erreichbar sind.)

Satz 7.4.: Basissatz

1.) Jeder endliche Graph besitzt eine Basis.
2.) B ist Basis von G= (M,R) genau dann, wenn M erreichbar von B und für alle a $\neq$ b $\in$ B gilt: W_G (a,b) $\cup$ W_G (b,a) = $\emptyset$
3.) Jeder endliche kreisfreie Graph besitzt genau eine Basis.

Beweis:

1.) Ausgehend von der endlichen Knotenmenge M, welche von M aus erreichbar ist, wird M sukzessiv verkleinert, bis eine Basis gefunden ist.
2.) Wir nehmen an, daß B' $\subset$ B Basis von G ist. Dann ist jeder Knoten b $\in$ B $\setminus$ B' von einem a $\in$ B' erreichbar mit a $\neq$ b, d.h., W_G (a,b) $\neq \emptyset$, also ein Widerspruch zur rechten Seite von 2.
Die umgekehrte Richtung ergibt sich unmittelbar nach Definition 7.5.
3.) Wir konstruieren als Basis B=$\{$a | a $\in$ M minimal$\}$, d.h., B ist die Menge aller Knoten ohne Vorgänger (Menge der Eingangselemente).
B ist nach 2.) eine Basis, da alle a $\neq$ b $\in$ B minimal, d.h., W_G (a,b) $\cup$ W_G(b,a) = $\emptyset$ und M erreichbar von B, da es wegen der Kreisfreiheit zu jedem b $\in$ M$\setminus$ B einen wiederholungsfreien Weg von einem minimalen Element geben muß. B ist auch die einzige Basis, denn alle minimalen Elemente gehören zu jeder Basis.

Endliche Graphen können durch Matrizen wie folgt dargestellt werden.
Definition 7.6. Adjazenz- und Inzidenzmatrix
Sei G= (M,R) ein endlicher (gerichteter) Graph mit nichtleerer Kantenmenge R =$\{r_1, ..., r_n\}$ und der Knotenmenge M= $\{a_1, ...a_m\}$.

a) Die Funktion A_G von I_M^2 (I_M Indexmenge von M) in die Menge $\{0,1\}$ heißt Adjazenzmatrix von G, wenn

$$A_G(\text{i,k}) = \begin{cases} 1 & \text{falls} \quad [a_i, a_k] \in \text{R} \\ 0 & \qquad\qquad \text{sonst} \end{cases}$$

b) Die Funktion I_G von $I_M \times I_R$ in die Menge {-1, 0, 1} heißt Inzidenzmatrix von G, wenn

$$I_G(\text{i, j}) = \begin{cases} 1 & \\ -1 & \text{falls} \\ 0 & \end{cases} \quad \begin{matrix} a_i \text{ Anfangspunkt von } r_j \\ a_i \text{ Endpunkt von } r_j \\ \text{sonst} \end{matrix}$$

Beispiele:
Der Graph G (M,R) mit M= {1,2,3,4,5}, R= {[3,1], [1,2], [3,2], [4,3], [2,5], [5,4]} kann durch die Inzidenzmatrix I_G bzw. durch die Adjazenzmatrix A_G repräsentiert werden.

$$I_G = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 & 0 \\ 1 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{pmatrix}, \quad A_G = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Satz 7.5.
Wenn A_G^k die k-te Potenz der Adjazenzmatrix A_G des endlichen Graphen G = (M,R) bezeichnet, dann beschreibt A_G^k die Adjazenzmatrix des Graphen (M,R^k)
(Anmerkung: A_G^k (i,j) = Anzahl der Wege von a_i nach a_j der Länge k in G mit M = $\{a_1, ..., a_n\}$)

Folgerung:
In jedem kreisfreien endlichen gerichteten Graphen gibt es einen Weg größter Länge, d.h., es existiert ein l mit $A_G^l \neq 0$ und $A_G^k = 0$ für alle k > l. (0 Nullmatrix)

Satz 7.6.
G_1 und G_2 seien endliche gerichtete Graphen und I_{G_1}, A_{G_1} bzw. I_{G_2}, A_{G_2} ihre Inzidenz- bzw. Adjazenzmatrizen. Dann sind folgende Aussagen äquivalent:
a) G_1 isomorph G_2
b) I_{G_1} kann durch Vertauschen von Zeilen und Spalten in I_{G_2} transformiert werden.
c) A_{G_1} kann durch gleichzeitiges Vertauschen von i-ten Zeilen und i-ten Spalten in A_{G_2} transformiert werden.

Häufig werden spezielle Klassen bzw. Eigenschaften von Graphen ausgezeichnet. So werden Graphen, deren Knoten so als Punkte der euklidschen Ebene dargestellt werden können, daß sich keine zwei Kanten als Verbindungsgeraden der Eckpunkte überschneiden, als planar bezeichnet.

Ein ungerichteter Graph (M,R) heißt n-chromatisch (n-färbbar), wenn es eine Zerlegung von M in n Klassen so gibt, daß alle a,b $\in$ M mit [a,b] $\in$ R zu verschiedenen Klassen dieser Zerlegung gehören.
Ein Teilgraph G' von G mit k Knoten, dessen Knoten alle paarweise durch Kanten verbunden sind, heißt eine k-Clique von G.
Ein Kreis des gerichteten Graphen G = (M,R) heißt ein Hamilton-Kreis, wenn dabei jeder Knoten aus M genau einmal durchlaufen wird.
Ein Weg in G, bei dem jede Kante von G genau einmal durchlaufen wird und dessen Anfangs- und Endknoten gleich sind, wird ein Eulerscher Weg genannt.
Eine Teilmenge R' der Kantenmenge R eines Graphen G = (M,R) heißt Match, wenn jeder Knoten von M zu höchstens einer Kante aus R' gehört.
Von besonderer Bedeutung sind zyklenfreie, zusammenhängende Graphen, die auch als Bäume bezeichnet werden.

Definition 7.7.

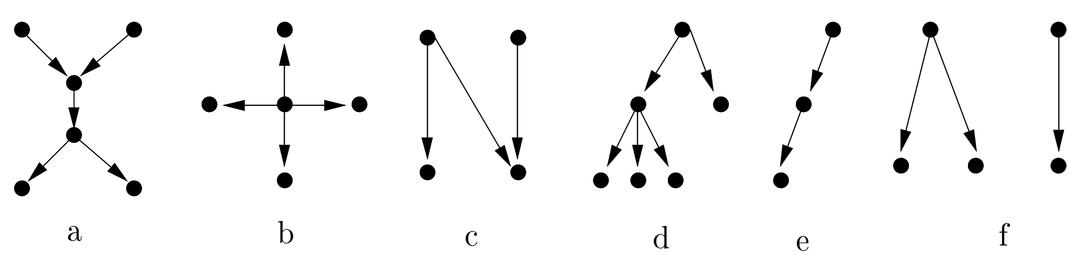
a) Ein gerichteter Graph G heißt Baum (Tree), falls G zyklenfrei und zusammenhängend ist.

b) Ein gerichteter Graph G =(M,R) heißt Wurzelbaum (Arboreszens), falls G ein Baum ist und in M bzgl. R genau ein minimales Element (Wurzel) existiert.

c) Ein gerichteter Graph G heißt ein Wald, falls jede Komponente von G ein Baum ist.
(Ein Baumtupel $[T_1, ...T_n]$ wird auch als ein geordneter Wald bezeichnet).

Beispiele:

Die nachfolgend dargestellten endlichen Graphen a,b,c sind Bäume; d,e sind Wurzelbäume und f ist ein Wald.



Definition 7.8.
Es sei G= (M,R) ein Baum.

a) Unter dem Grad d_G(k) eines Knotens k $\in$ M versteht man die Anzahl der Nachfolger von k (d.h. die Anzahl der von k ausgehenden Kanten).
b) G heißt g-beschränkt, wenn der Grad jedes Knotens maximal g ist, d.h., g ist der maximale Knotengrad des Baumes G mit d_G(k) $\leq$ g für alle k $\in$ M.
   Im Spezialfall g=2 heißt der Baum ein Binärbaum, d.h., jeder Knoten besitzt höchstens zwei Nachfolger. Oft wird dabei zusätzlich eine Ordnung der Nachfolger festgelegt, so daß man von einem linken bzw. rechten Nachfolger (Sohn) sprechen kann.
   Die maximalen Elemente des Baumes (ohne Nachfolger) mit dem Knotengrad d_G(k) =0 werden Blätter genannt, die Menge aller Blätter wird auch als Krone bezeichnet.
   Minimale (Wurzeln) und maximale (Blätter) Knoten werden auch als Endknoten bezeichnet. Die anderen Knoten nennt man innere Knoten. Wenn ihre Nachfolger selbst keine Blätter sind, dann bilden alle Knoten, die von diesen erreichbar sind Unterbäume, die als Nachfolgebäume bezeichnet werden.
c) G heißt gleichverzweigt (perfekt), wenn alle Knoten, die nicht Blätter sind, denselben Knotengrad g besitzen. Man spricht dann auch von g-gleichverzweigt bzw. von einem vollständigen (perfekten) g-Baum.

Für Bäume gelten zunächst folgende Eigenschaften:
Satz 7.7.
Es sei G=(M,R) ein endlicher Baum

a) Wenn G kein Punktgraph (M keine Einermenge), dann hat G mindestens zwei Endpunkte.
b) |R| = |M| -1, d.h., G besitzt genau eine Kante weniger als Knotenpunkte.
c) Zwischen zwei verschiedenen Knoten gibt es genau eine wiederholungsfreie Kette.
d) G besitzt keinen zusammenhängenden echten Teilgraphen mit derselben Knotenmenge, d.h., keine Kante kann weggelassen werden, ohne die Baumeigenschaft zu verletzen.
e) Wenn x,y $\in$ M und (x,y) $\notin$ R, dann enthält der Graph G'=(M,R $\cup$ {(x,y)}) genau einen Zyklus.

Beweis:

a) Würde es nur einen oder keinen Endpunkt geben, dann würde wegen der Zusammenhangseigenschaft unbeschränkte Nachfolger- bzw. Vorgängerbildung möglich sein, woraus wegen der Zyklenfreiheit die Unendlichkeit von M folgen würde.
b) Die Aussage ist für |M|=1 offenbar richtig (Punktgraph). Dann schließen wir mit Induktionsprinzip wie folgt:

Unter der Annahme, daß die Aussage für $|M| = n$ richtig ist, betrachten wir für $|M| = n+1$ den Untergraph G'=(M',R') mit $M' = M \setminus \{k\}$, $R' = R|M'$, der aus G durch Weglassen des nach a) existierenden Endknotens $k \in M$ und der mit diesem verbundenen Kante entsteht. G' ist ebenfalls ein Baum mit $|R'| = n-1$ und $|M'| = n$. Damit gilt aber auch $|R| = n$.

c) d) e) können direkt aus der Tatsache gefolgert werden, daß G zyklenfrei und zusammenhängend ist.

Für endliche Bäume kann aus der Kantenzahleigenschaft und einer der Baumeigenschaften die andere geschlossen werden. Darüber gilt der

Satz 7.8.

a) Ein endlicher gerichteter Graph G =(M,R) ist genau dann ein Baum, wenn G zyklenfrei ist und die Eigenschaft $|M|-1=|R|$ gilt.

b) Ein endlicher gerichteter Graph G= (M,R) ist genau dann ein Baum, wenn G zusammenhängend ist und die Eigenschaft $|M|-1=|R|$ gilt.

Bemerkung:

Es ist lediglich zu zeigen, daß G bei a) zusammenhängend bzw. bei b) zyklenfrei ist. Die Gegenrichtung gilt per Definition und Satz 7.7.b).

Für Wurzelbäume kann man folgende Begriffe einführen:

Definition 7.9.

Sei G=(M,R) ein endlicher Wurzelbaum.

a) Unter der Stufe S_G (k) eines Knotens k versteht man den um 1 erhöhten Abstand zur Wurzel. Die Wurzel selbst hat die Stufe 1.
Unter der Höhe h_G von G versteht man die maximale Stufe seiner Knoten aus M.

b) Ein Wurzelbaum G heißt ausgeglichen, falls sich die Stufe aller Blätter höchstens um 1 von der Höhe von G unterscheiden, d.h., $h_G - 1 \leq S_G(k) \leq h_G$ für alle $k \in M$ mit $d_G(k) = 0$.
Ein ausgeglichener Wurzelbaum heißt vollständig ausgeglichen, falls sich die Knotenzahl der Nachfolgerbäume (Unterbäume) zu einem Knoten höchstens um 1 unterscheiden.

Wurzelbäume besitzen die Eigenschaften nach

Satz 7.9.

Es sei G=(M,R) ein Wurzelbaum mit der Wurzel $k \in M$. Dann gilt:

a) Jeder von der Wurzel k verschiedene Knoten x aus M hat genau einen Vorgänger.

b) Zu jedem $x \neq k$ aus M gibt es genau einen wiederholungsfreien Weg von k nach x.

Beweis:

a) Würde es einen von der Wurzel verschiedenen Knoten mit zwei Vorgängern geben, denn gäbe es wegen des Zusammenhangs Ketten von der Wurzel zu diesen beiden Vorgängerknoten und damit im Widerspruch zu Satz 7.7c zwei Ketten zwischen der Wurzel und den betrachteten Knoten.

b) Nach Satz 7.7c) gibt es genau eine wiederholungsfreie Kette, also höchstens einen Weg. Die Kette ist aber auch ein Weg, da sonst ein Knoten in der Kette entgegen a) zwei Vorgänger haben müßte.

Die im Zusammenhang mit Halbordnungen nach Definition 5.7. eingeführten zweistelligen Operationen $\cap$ Infimum (größte untere Schranke) und $\cup$ Supremum (kleinste obere Schranke) auf einer Menge M führen zum Begriff des Verbandes nach

Definition 7.10.

Es sei M eine nichtleere Menge und $\cap$, $\cup$ zwei zweistellige Operationen auf M.
Die Struktur V =(M, $\cap, \cup$) vom Typ (2,2;) heißt ein Verband, wenn für alle Elemente x,y,z $\in$ M folgende Eigenschaften erfüllt sind

a) $x \cup y = y \cup x$, $x \cap y = y \cap x$ (Kommutativität von $\cap$ und $\cup$)

b) $x \cap (y \cap z) = (x \cap y) \cap z$, $x \cup (y \cup z) = (x \cup y) \cup z$ (Assoziativität von $\cap$ und $\cup$)

c) $x \cap (x \cup y) = x,\ x \cup (x \cap y) = x$ (Verschmelzungs- oder Absorptionsgesetze)

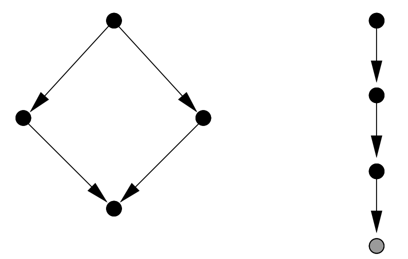
In einem Verband V = (M, $\cap, \cup$) kann man in natürlicher Weise eine Halbordnung $\leq_V$ mit x $\leq_V$ y genau dann wenn x $\cap$ y = x erklären. Die Reflexivität von $\leq_V$ folgt nach Anwendung beider Absorptionsgesetze für x = y, die Transitivität von $\leq_V$ ist aus der Assoziativität von $\cap$ zu schließen.
Umgekehrt kann man zu einer Halbordnung (M, $\leq$), in der je zwei Elemente ein Infimum inf und ein Supremum sup besitzen, durch x $\cap$ y $=_{def}$ inf ({x,y}) und x $\cup$ y $=_{def}$ sup ({x,y}) einen Verband $V_{\leq} =_{def}$ (M, $\cap, \cup$) definieren.
Die Verbandeigenschaften a,b,c können aus der Antisymmetrie, Transitivität, Reflexivität der Halbordnung geschlossen werden.

Damit ergibt sich folgender
Satz 7.10.

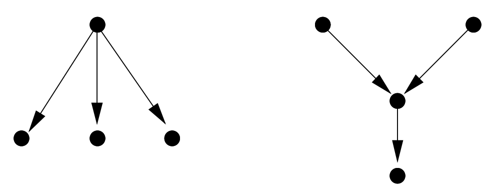
a) Wenn die Struktur V= (M, $\cap, \cup$) ein Verband ist, dann ist (M, $\leq_V$) eine Halbordnung, in der je zwei Elemente von M ein Supremum und ein Infimum besitzen.

b) Wenn (M, $\leq$) eine Halbordnung ist, in der je zwei Elemente von M ein Supremum und ein Infimum besitzen, dann ist $V_{\leq}$ = (M, inf, sup) ein Verband.

Bemerkung:
Lineare Ordnung mit Infimum als Minimum und Supremum als Maximum bilden einen Verband.
Beispiele für Verbände mit endlich vielen Elementen sind z.B.



Im Gegensatz dazu sind



keine Verbände.
Von besonderer Bedeutung sind die vollständigen Verbände.

Definition 7.11.
Ein Verband V=(M, $\cap, \cup$) heißt vollständig, wenn jede nichtleere Teilmenge von M bezüglich der Halbordnung $\leq_V$ ein Infimum und ein Supremum besitzt.

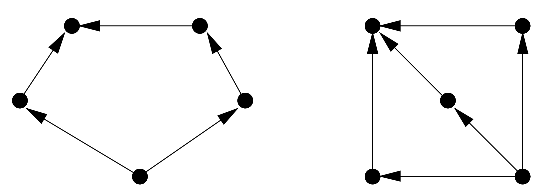
Bemerkung:
a) Endliche Verbände (mit endlicher Trägermenge) sind vollständig, da je zwei Elemente nach Satz 7.10.a) immer ein Infimum und ein Supremum besitzen.
b) Der zur Halbordnung $(Q_{34}, \leq)$ über der Menge Q_{34} der rationalen Zahlen zwischen 3 und 4 gehörige Verband ist nicht vollständig, da z.B. die Menge $\{x \mid x \in Q_{34} \wedge x < \pi\}$ kein Supremum und die Menge $\{ x \mid x \in Q_{34} \wedge x > \pi\}$ kein Infimum besitzt.
c) Der Potenzmengenverband $(2^M, \cap, \cup)$ und der Verband zur Halbordnung $(R_{0,1}, \leq)$ über der Menge der reellen Zahlen zwischen 0 und 1 sind vollständig.
Vollständige Verbände besitzen eine wichtige Eigenschaft, die bei der Beschreibung formaler Sprachen wesentlich benutzt wird.

Satz 7.11. (Fixpunktsatz)
Es sei V = (M, $\cap, \cup$) ein vollständiger Verband und (M, $\leq_V$) die zugeordnete Halbordnung.
Zu jedem (Verbands-) Homomorphismus φ von M auf sich, für den mit x $\leq_V$ y auch φ(x) $\leq_V$ φ(y) gilt, hat die Gleichung φ(x) = x eine Lösung in M. (x heißt Fixpunkt von φ)

Beweis:
Wir zeigen, daß für x = sup ({y $\in$ M | y $\leq_V$ φ(y)}) gilt φ(x) = x. Zunächst gilt für jedes y mit obiger Eigenschaft y $\leq_V$ x und damit φ(y) $\leq_V$ φ(x).
φ(x) ist eine obere Schranke, weil für alle y $\in$ M gilt: y $\leq_V$ φ(y) $\leq_V$ φ(x), also auch x $\leq_V$ φ(x).
φ(x) ist demnach ein derartiges y, also φ(x) $\leq_V$ x wegen Supremumeigenschaft.
Zusammen ergibt sich φ(x) = x.

Für Verbände geben wir weiter die
Definition 7.12.
a) Ein Verband V= (M, $\cap, \cup$) heißt distributiv, wenn jede der beiden Operationen $\cap, \cup$ bzgl. der anderen distributiv ist, d.h., für alle x, y, z $\in$ M gilt:
$x \cap (y \cup z) = (x \cap y) \cup (x \cap z),\ x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$
b) Sei V= (M, $\cap, \cup$) ein Verband mit dem kleinsten Element 0 und dem größten Element 1 aus M und x, y $\in$ M. y heißt Komplement von x, falls
x $\cap$ y = 0 und x $\cup$ y = 1
c) Ein Verband V= (M, $\cap, \cup$) heißt komplementär, wenn jedes Element aus M mindestens ein Komplement besitzt.

Beispiele:
a) Der Potenzmengenverband ($2^M, \cap, \cup$) ist distributiv.
b) Jeder Verband V mit linearer Ordnung $\leq_V$ ist distributiv.
c) Die Verbände



mit 5 Elementen sind die kleinsten nichtdistributiven Verbände.

Für distributive Verbände V= (M, $\cap, \cup$) gelten folgende Eigenschaften:
a) Aus a $\cap$ x = a $\cap$ y und a $\cup$ x = a $\cup$ y folgt x = y für alle a, x, y $\in$ M.
b) Jedes Element von M besitzt höchstens ein Komplement.

Verbände, die distributiv und komplementär sind, werden auch als Boolsche Algebren bezeichnet. Wenn wir das wegen Distributivität eindeutig bestimmte Komplement von x $\in$ M mit $\bar{x}$, das kleinste Element mit 0 und das größte mit 1 bezeichnen, dann gelten in der Boolschen Algebra B=(M, $\cap, \cup$, 0, 1, $^-$) die folgenden Beziehungen:
$\bar{0}$=1, $\bar{1}$=0, $\bar{x} = x, x = y \;\Leftrightarrow\; \bar{x} = \bar{y}$,
$\overline{(x \cup y)} = \bar{x} \cap \bar{y}$, $\overline{(x \cap y)} = \bar{x} \cup \bar{y}$, $x \leq_B y \;\Leftrightarrow\; \bar{y} \leq_B \bar{x}$,
$x \leq_B y \;\Leftrightarrow\; x \cap \bar{y} = \emptyset$ und $x \leq_B y \;\Leftrightarrow\; \bar{x} \cup y = 1$.

Wenn man $\cap$ als logische Konjunktion, $\cup$ als logische Disjunktion, $^-$ als logische Negation, 0 als Wahrheitswert Falsch und 1 als Wahheitswert Wahr interpretiert, dann beschreibt ($\{0{,}1\}$, $\cap, \cup$, 0, 1, $^-$) die der zweiwertigen Aussagenlogik zugrunde liegende algebraische Struktur.

8. ORDINAL- UND KARDINALZAHLEN

Früher hatten wir Kardinalzahlen als Äquivalenzklassen gleichmächtiger Mengen (Mengen mit gleichem Umfang) eingeführt. Die den Äquivalenzklassen zugrunde liegende Äquivalenzrelation muß in einer bestimmten Grundmenge definiert sein. Da wir aber keine Einschränkung bei den betrachteten Mengen angegeben haben, müßten wir bei der obigen Definition der Kardinalzahlen von der Gesamtheit aller Mengen ausgehen, die aber im Rahmen unseres Mengenbegriffs selbst keine Menge sein kann.
Diesen Umstand könnte man zunächst dadurch beheben, daß man sich auf solche Mengen bezieht, die Teilmenge einer gegebenen Grundmenge sind. Damit sind dann allerdings nur Kardinalzahlen erfaßbar, die kleiner oder gleich der Kardinalzahl der Potenzmenge dieser Grundmenge sind.
In der axiomatischen Mengenlehre werden nach J.v. Neumann als Kardinalzahl einer Menge ein spezieller Repräsentant aus der Klasse aller zu dieser Menge gleichmächtigen Mengen definiert. Derartige als Kardinalzahlen bezeichnete Mengen besitzen die Eigenschaft, daß zwei Mengen dann und nur dann dieselbe Kardinalzahl besitzen, wenn sie gleichmächtig sind. Jeder Menge M wird damit in eindeutiger Weise ihre Kardinalzahl | M | mit der eben erwähnten Eigenschaft zugeordnet.
Bezogen auf endliche Mengen, können wir deren Kardinalzahlen mit den natürlichen Zahlen identifizieren, da endliche Mengen dann und nur dann gleichmächtig sind, wenn sie die gleiche Anzahl von Elementen besitzen. Die Zahl 0 ist dann die Kardinalzahl der leeren Menge, die Zahl 1 die Kardinalzahl aller Einermengen, usw.
Für Kardinalzahlen kann eine Halbordnungsrelation $\leq$ (reflexiv, transitiv, antisymmetrisch) eingeführt werden, wobei $k_1 \leq k_2$ genau dann gilt, wenn für beliebige Mengen M_1, M_2 mit $k_i = |M_i|$ die Menge M_1 gleichmächtig einer Teilmenge von M_2 ist ($M_1 < M_2$).
Wenn $\sim$ die Äquivalenzrelation der Gleichmächtigkeit bezeichnet, dann folgt aus
$M_1 < M_2$ und $M_2 < M_1$ die Eigenschaft $M_1 \sim M_2$ (Bernsteinscher Äquivalenzsatz).
Aus der Tatsache, daß für beliebige Mengen M_1, M_2 stets $M_1 < M_2$ oder $M_2 < M_1$ gilt, folgt bei Übergang zu den Kardinalzahlen k_1, k_2 deren Vergleichbarkeit bzgl. $\leq$, d.h., $k_1 \leq k_2$ oder $k_2 \leq k_1$. Zusammen mit der Antisymmetrie von $\leq$ folgt daraus wiederum, daß die kleinste Kardinalzahl in einer beliebigen Menge von Kardinalzahlen eindeutig bestimmt ist, falls es eine solche überhaupt gibt. Übertragen auf nichtleere endliche Mengen von Kardinalzahlen existiert dann immer eindeutig eine kleinste, d.h., $\leq$ ist eine Wohlordnung.
Andererseits gilt für jede Menge M, daß deren Kardinalzahl immer kleiner als die Kardinalzahl der Potenzmenge von M ist, d.h., zu jeder Menge von Kardinalzahlen gibt es immer eine Kardinalzahl, die größer als alle Kardinalzahlen dieser Menge ist. Die Gesamtheit aller Kardinalzahlen kann demnach selbst keine Menge sein.
Die kleinste Kardinalzahl k' in der Gesamtheit aller Kardinalzahlen, die größer als eine vorgegebene Kardinalzahl k sind, wird unmittelbarer Nachfolger von k genannt. Falls k natürliche Zahl, dann ist k'=k+1 der unmittelbare Nachfolger von k. Die Menge der natürlichen Zahlen ist also die kleinste Gesamtheit von Kardinalzahlen, die die Zahl 0

(Kardinalzahl der leeren Menge) und mit einer Zahl k auch deren unmittelbaren Nachfolger (k+1) enthält.
Die Kardinalzahl der Menge aller natürlichen Zahlen, d.h., aller endlichen Kardinalzahlen, als die kleinste sogenannte transfinite Kardinalzahl, wird durch $\aleph_0$ (aleph 0) bezeichnet. Jede Menge mit der Kardinalzahl $\aleph_0$ ist gleichmächtig mit der Menge der natürlichen Zahlen, d.h., abzählbar unendlich.
Der unmittelbare Nachfolger von $\aleph_0$ ist die Kardinalzahl der Potenzmenge der Menge der natürlichen Zahlen (spezielle Kontinuumshypothese), die mit $2^{\aleph_0}$ oder $\aleph_1$ (aleph 1) bezeichnet wird. Daß dies nicht nur für $\aleph_0$, sondern für beliebige transfinite Kardinalzahlen gilt, ist die Aussage der allgemeinen Kontinuumshypothese. $\aleph_1$ ist die Kardinalzahl der Menge aller reellen Zahlen.
Für Kardinalzahlen kann man eine Arithmetik einführen, in der Eigenschaften von Operationen über Mengen untersucht werden. So ist z.B. die Kardinalzahl $|M_1 \times M_2|$ des Kreuzproduktes der Mengen M_1, M_2 die größere der beiden Kardinalzahlen $|M_1|$ bzw. $|M_2|$, falls wenigstens eine der Mengen M_1, M_2 unendlich ist. Daraus folgt z.B., daß für jede unendliche Menge M auch die Menge M^n aller n-Tupel von Elementen aus M mit der Menge M gleichmächtig ist, d.h., die gleiche Kardinalzahl besitzt ($|M| = |M^n|$, wo n nat. Zahl).
Zur Charakterisierung der Ordinalzahlen betrachten wir Wohlordnungen, d.h., Strukturen (M, $\leq$), wo $\leq$ als binäre Relation über M reflexiv, transitiv, antisymmetrisch, linear und bzgl. $\leq$ ein kleinstes (erstes) Element in jeder Teilmenge von M existiert. Zwei solche Strukturen $(M_1, \leq_1)$ und $(M_2, \leq_2)$ heißen ähnlich, wenn es eine Bijektion φ von M_1 auf M_2 gibt, so daß für alle x, y $\in M_1$ gilt: x $\leq_1$ y genau dann, wenn φ(x) $\leq_2$ φ(y).
Damit erhält man eine Äquivalenzrelation in der Gesamtheit aller wohlgeordneten Mengen. Jeder solchen wohlgeordneten Menge (M, $\leq$) wird jetzt eine Ordinalzahl $|(M, \leq)|$ zugeordnet, wobei zwei wohlgeordnete Mengen genau dann die gleiche Ordinalzahl besitzen, wenn sie im obigen Sinne ähnlich sind. In Analogie zu den Kardinalzahlen nennt man die wohlgeordnete Menge (M, $\leq$) einen Repräsentanten der Ordinalzahl $|(M, \leq)|$.
Da endliche Mengen sich bis auf Ähnlichkeit nur auf eine Weise wohlordnen lassen, besitzen zwei endliche wohlgeordnete Mengen genau dann dieselbe Ordnungszahl, wenn ihren Grundmengen dieselbe Kardinalzahl zugeordnet ist, also beide Mengen über die gleiche Anzahl von Elementen verfügen. Ordinalzahlen endlicher wohlgeordneter Mengen können also mit den natürlichen Zahlen identifiziert werden. D.h., natürliche Zahlen können sowohl zur Anzahlbestimmung (Kardinalzahl) als auch zum Zählen (Ordinalzahl) verwendet werden. Für unendliche Mengen besteht aber ein wesentlicher Unterschied zwischen Kardinal- und Ordinalzahlen.
Die Gesamtheit aller Ordinalzahlen bildet im Sinne unserer Mengenlehre selbst keine Menge, sondern eine Klasse. Jede wohlgeordnete Menge ist isomorph zu einer Ordinalzahl. Umgekehrt sind Ordinalzahlen Äquivalenzklassen isomorpher Wohlordnungen.
Eine wohlgeordnete Menge $(M_1, \leq_1)$ ist (ihrer Ordnung nach) kleiner oder gleich ($<$) einer wohlgeordneten Menge $(M_2, \leq_2)$, wenn $(M_1, \leq_1)$ einem Anfangsstück von $(M_2, \leq_2)$ (Teilmenge N_2 von M_2, die mit x $\in M_2$ auch alle y $\in M_2$ mit y $\leq_2$ x enthält und deren

Wohlordnung durch Einschränkung von $\leq_2$ auf N_2 entsteht) ähnlich ist. Die Relation $<$ läßt sich von den wohlgeordneten Mengen repräsentantenweise auf die Ordinalzahlen übertragen, womit eine Wohlordnung in der Gesamtheit der Ordinalzahlen begründet wird. Für endlichen Ordinalzahlen stimmt die Ordnung mit der natürlichen Ordnung für natürliche Zahlen überein.
Die kleinste transfinite Ordinalzahl ω_0 kann durch die Menge aller natürlichen Zahlen mit der vorher erwähnten üblichen Ordnung repräsentiert werden. Der unmittelbare Nachfolger von ω_0 kann durch die wohlgeordnete (in der gegebenen Anschreibung) Menge $(0, 1, 2, \ldots , \omega_0)$ repräsentiert werden.
Neben den transfiniten Ordnungszahlen, die einen unmittelbaren Vorgänger besitzen (isolierte Zahlen), gibt es auch transfinite Ordnungszahlen, die keinen unmittelbaren Vorgänger haben (Limeszahlen).
Wie für Kardinalzahlen kann auch für Ordinalzahlen eine entsprechende Arithmetik eingeführt werden. Für endliche Kardinal- bzw. Ordinalzahlen stimmt diese Arithmetik mit der üblichen Arithmetik natürlicher Zahlen überein.

9. INDUKTION UND REKURSION

Neben der Tatsache, daß nach Kapitel 8 natürliche Zahlen zur Angabe der Elementezahl endlicher Mengen (d.h. Kardinalzahlen) und zum Durchnumerieren der Elemente endlicher Mengen (d.h. Ordinalzahlen) benutzt werden, sind insbesondere auch für die Informatik deren Eigenschaften bzgl. ausführbarer Operationen (d.h. Struktureigenschaften) von Interesse. Als derartige Operationen kommen zunächst die zweistelligen Verknüpfungen Addition und Multiplikation in Betracht. Um die Grundeigenschaften natürlicher Zahlen festzulegen, reicht aber zunächst eine einstellige Operation (Nachfolgerbildung succ) aus.
Nach Peano lassen sich die natürlichen Zahlen beschreiben als Objekte der algebraischen Struktur (N, succ) vom Typ (1;) mit der Nachfolgerfunktion succ: $N \rightarrow N$ und den Eigenschaften:

Ax 1) $0 \in N$; d.h., N ist eine nichtleere Menge

Ax 2) Wenn succ x = succ y, dann ist x=y für alle $x,y \in N$; d.h., succ ist injektiv.

Ax 3) succ $x \neq 0$ für alle $x \in N$; d.h., 0 liegt nicht im Bildbereich von succ.

Ax 4) Für jede Teilmenge (Eigenschaft) $M \subseteq N$, die 0 enthält und mit $x \in M$ auch succ $x \in M$, gilt M=N; d.h., jedes Element von N kann ausgehend von 0 durch fortgesetzte Nachfolgerbildung erhalten werden.

Die Aussagen Ax 1) bis Ax 4) werden als Peanosches Axiomensystem und die Menge der natürlichen Zahlen als ein Modell dieses Systems bezeichnet. Die Struktur (N, 0, succ) mit den Eigenschaften Ax 1 - Ax 4 wird vielfach auch Peano-Algebra genannt. Das Objekt succ x heißt unmittelbarer Nachfolger von x und wird häufig auch durch x+1 bezeichnet.
Wenn y= succ x, dann heißt x unmittelbarer Vorgänger von y und wird durch y-1 bezeichnet. Aus den genannten Peanoschen Axiomen , die wir als Struktureigenschaft voraussetzen, ergeben sich weitere Eigenschaften als Folgerungen.

9.1.: 0 ist die einzige natürliche Zahl, die keinen unmittelbaren Vorgänger hat.
(Jede von 0 verschiedene natürliche Zahl besitzt genau einen unmittelbaren Vorgänger.)

9.2.: Jede natürliche Zahl ist von ihrem unmittelbaren Nachfolger verschieden.

9.3.: Wenn eine Eigenschaft (Aussage) H für die Zahl 0 zutrifft und für jede Zahl x aus der Gültigkeit von H für x auch ihre Gültigkeit für den unmittelbaren Nachfolger succ x folgt, dann gilt die Eigenschaft H für alle natürlichen Zahlen aus N, d.h., $H(0) \wedge \forall x\colon (x \in N \wedge H(x) \rightarrow H(\text{succ } x)) \rightarrow \forall x\colon (x \in N \rightarrow H(x))$

Die Eigenschaft 9.3., die auch als Induktionsprinzip bezeichnet wird, ergibt sich aus dem Axiom Ax 4) und wird wesentlich zum Beweis von Eigenschaften bzw. zur impliziten Definition von weiteren Operationen bzw. Relationen über natürliche Zahlen benutzt.

Dazu beweisen wir den

Satz 9.4. (Dedekindscher Rechtfertigungssatz):

Es sei g eine zweistellige Operation über N mit g(x,y) $\in$ N für alle x,y $\in$ N und a ein beliebiges festes Element aus N.

Dann existiert genau eine auf N definierte einstellige Funktion f mit f(0) = a und f(succ x) = g(f(x),x) für alle x $\in$ N.

Beweis:

1.) Sei Dom f = {x | x $\in$ N $\wedge$ f(x) $\in$ N} $\subseteq$ N der Definitionsbereich von f. Dann gilt nach Definition 0 $\in$ Dom f. Wenn y $\in$ Dom f und x = succ y, dann ist f(x) = g(f(y),y) $\in$ N also x $\in$ Dom f. Nach Axiom Ax 4 also Dom f = N, d.h., zu jedem x $\in$ N existiert ein f(x) $\in$ N.

2.) Eindeutigkeit von f: Angenommen es gibt zwei verschiedene Funktionen f $\neq$ f', die beide die Definitionsgleichungen erfüllen. Sei x $\in$ N die kleinste Zahl mit f(x) $\neq$ f'(x). Nach Definition ist x $\neq$ 0. Wir betrachten den unmittelbaren Vorgänger y von x = succ y mit f(y) = f'(y). Dann muß aber auch f(x) = g(f(y),y) = g(f'(y),y) = f'(x) sein im Widerspruch zur Annahme über x.

Beispiele 9.1.

a) Die Addition add für natürliche Zahlen kann somit wie folgt definiert werden.
   $\text{add}_x(0)$ = x, add_x(succ y) = succ add_x(y) für alle x,y $\in$ N.
   (Hier wird add in parametrisierter Form mit einstelligem Argument verwendet als x+y = add_x(y). Die Funktion succ kann auch als zweistellige Funktion mit unberücksichtigtem zweiten Argument aufgefaßt werden.)
   Sei $N_x = \{y | y \in N \wedge\ y \in \text{Dom add}_x\}$ die Menge aller y aus N, wo add_x(y) definiert ist. Nach Definition von add_x ist 0 $\in N_x$ und mit y $\in N_x$ ist auch succ y $\in N_x$, da succ für alle natürlichen Zahlen erklärt ist. Damit ist nach Axiom Ax 4 bzw. Eigenschaft 9.3. auch x+y= add_x (y) für alle y erklärt.

b) Die Multiplikation mult für natürliche Zahlen ist demnach wie folgt zu definieren:
   mult_x(0)= 0, mult_x(succ y)= add_x (mult_x(y)) für alle x,y $\in$ N als x $\times$ y = mult_x(y).

c) Die Potenzfunktion exp für natürliche Zahlen kann mit 1 = succ 0 wiederum wie folgt definiert werden:
   exp_x(0) = 1, exp_x(succ y) = mult_x (exp_x(y)) für alle x,y $\in$ N als x^y = exp_x(y).

Nach dem Satz 9.4. werden durch die angegebenen Gleichungen (Rekursionsgleichungen) eindeutig die Funktionen add_x, mult_x, exp_x für jede x $\in$ N definiert. Der entsprechende Nachweis folgt allgemein wie im Beispiel a) dem Induktionsprinzip. Im Zusammenhang mit berechenbaren Funktionen werden wir weitere Rekursionsmöglichkeiten kennenlernen.

Bei Anwendung des Induktionsprinzips zum Beweis einer Eigenschaft H(x) für alle x $\in$ N genügt es nach Eigenschaft 9.3. zu zeigen, daß H(0) gültig ist (Induktionsanfang) und unter der Voraussetzung, daß H(x) gilt (Induktionsvoraussetzung) auch die Gültigkeit von H(succ x) (Induktionsbehauptung) gefolgert werden kann (Induktionsschritt).
Man spricht dann von einem Beweis für H(x) durch vollständige Induktion. Die Richtigkeit der Beweisführung ergibt sich dabei aus dem Axiom Ax 4), welches auch Induktionsaxiom genannt wird.

Beispiel 9.2.
Wir zeigen die Kommutativität der Addition, d.h., $\mathrm{add}_x(y) = \mathrm{add}_y(x)$ für alle x,y $\in$ N. Zunächst zeigen wir diese Eigenschaft für y = 0. Für x = 0 ist add_0 (0) = add_0 (0) erfüllt. Wir nehmen an, daß $\mathrm{add}_x(0) = \mathrm{add}_0(\mathrm{x})$ gilt und zeigen $\mathrm{add}_{succ\ x}(0)$ = add_0(succ x) wie folgt:
Mit succ x = y gilt $\mathrm{add}_y(0)$ = succ x und weiter add_0(succ x) = succ add_0(x) = succ $\mathrm{add}_x(0)$ = succ x, wobei wir die Induktionsvoraussetzung $\mathrm{add}_x(0) = \mathrm{add}_0(\mathrm{x})$ und die Definition von add benutzt haben. Damit ist als Induktionsanfang $\mathrm{add}_x(0) = \mathrm{add}_0(\mathrm{x})$ für y = 0 und alle x $\in$ N gezeigt.
Wenn wir nun von der Annahme (Induktionsvoraussetzung) add_x(y) = add_y(x) ausgehen, ist im Induktionsschritt add_x(succ y) = $\mathrm{add}_{succ\ y}$(x) zu zeigen. Das ergibt sich mit Definition von add und dem induktiven Nachweis von succ add_y(x) = $\mathrm{add}_{succ\ y}$(x) aus add_x(succ y) = succ add_x(y) = succ add_y (x) = $\mathrm{add}_{succ\ y}$(x).
Nach Induktionsprinzip gilt damit die Kommutativität von add für alle natürlichen Zahlen.
Analog zeigt man die Eigenschaften
$\mathrm{add}_x(\mathrm{add}_y(\mathrm{z})) = \mathrm{add}_{add_x(y)}$ (z) (Assoziativität von add) bzw.
$\mathrm{mult}_x(\mathrm{add}_y(\mathrm{z})) = \mathrm{add}_{mult_x(y)}$ (mult_x(z)) (Distributivität von mult bzgl. add).

Die natürlichen Zahlen als Objekte der Struktur (N, 0, succ) können ausgehend von 0 durch fortgesetzte Anwendung der Nachfolgerfunktion succ gebildet werden, womit eine Ordnungsrelation $\leq$ in der obigen Struktur erklärt wird durch
x $\leq$ y genau dann, wenn es ein z $\in$ N gibt mit add_x(z) = y.
Jede nichtleere Teilmenge M von N besitzt bzgl. $\leq$ ein (kleinstes) Element x $\in$ M mit x $\leq$ y für alle y $\in$ M (Prinzip der kleinsten Zahl). Die Relation $\leq$ ist damit eine Wohlordnung in N. Diese Wohlordnung liegt dem vorher besprochenem Induktionsprinzip zugrunde.
Bezogen auf beliebige Wohlordnungen $\leq$ in N erhalten wir verallgemeinert die (ordnungstheoretische) Induktion als Eigenschaft
(H(0) $\wedge\forall$ x y $\in$ N: ((x < y $\rightarrow$ H(x)) $\rightarrow$ H(y))) $\rightarrow$ $\forall$ x $\in$ N: H(x)
für beliebige Aussagen H über N, wo < die irreflexive Relation zur Wohlordnung $\leq$ und 0 das Minimum von N bzgl. $\leq$ bedeutet. Hier muß H(0) nicht besonders gefordert werden, da die Gültigkeit der Aussage H für das Minimum in der Induktionsannahme bereits enthalten ist.

Übertragen auf beliebige wohlgeordnete Mengen erhalten wir das Prinzip der <u>transfiniten Induktion</u>.

Sei M eine nichtleere Menge und $\leq$ eine Wohlordnung in M. Gilt die Aussage H über M für das Minimum bzgl. $\leq$ und kann aus H(x) für alle x $<$ y, auch H(y) gefolgert werden, dann gilt H(x) für alle x $\in$ M.

Der Zusammenhang zu den natürlichen Zahlen als Ordinalzahlen ist über die Wohlordnung $\leq$ gegeben. Das Rekursionsprinzip kann damit auf Funktionen über beliebigen nichtleeren Mengen erweitert werden, soweit der Definitionsbereich der Funktion wohlgeordnet ist. Eine Funktion f: M $\rightarrow$ N mit $\leq$ Wohlordnung in M wird eindeutig festgelegt, wenn f(Min) für das Minimum bzgl. $\leq$ bekannt ist und f(y) durch die Werte f(x) für x $<$ y bestimmt werden kann.

Allgemein gilt darüber der

<u>Satz 9.5. (Rekursionsprinzip)</u>

Zu jeder nichtleeren Menge N, jeder Wohlordnung (M, $\leq$) und jeder Funktion
g: M $\times$ 2^N $\rightarrow$ N existiert genau eine Funktion f: M $\rightarrow$ N mit
$\forall\, x(x \in M \rightarrow f(x) = g(x,\ f(M_{x,\leq})))$,
wo $M_{x,\leq} = \{y \in M \mid y < x\}$ Abschnitt in M bzgl. $\leq$.

10. FREIE HALBGRUPPEN UND SPRACHEN

Unter einer Zeichengestalt verstehen wir eine Klasse von für das menschliche Auge gleichgestalteten Zeichen.
Zeichengestalten können verknüpft oder verkettet werden, indem man die sie repräsentierenden Zeichen ohne Beachtung des Zwischenraumes hintereinander schreibt. Dadurch entsteht aus zwei Zeichen eine neue Zeichengestalt. Wir sprechen deshalb einfach von der Verkettung zweier Zeichengestalten. Das Verketten von Zeichengestalten ist offenbar eine vollständige binäre assoziative Operation, die aber nicht kommutativ ist.
Die Menge aller Zeichengestalten mit dieser vollständigen assoziativen binären Operation ist eine algebraische Struktur, die man als Halbgruppe bezeichnet.
Es ist zweckmäßig, noch ein neutrales Element ϵ für die Verkettung einzuführen. Für jede Zeichengestalt z gelte: z ϵ = ϵ z = z . ϵ heißt die leere Zeichengestalt und ist eindeutig bestimmt. Man beachte, daß ϵ eine Konstante, d.h. ein Name (Bezeichnung) für die leere Zeichengestalt und z eine Variable also ein Name für eine beliebige Zeichengestalt ist. Das neutrale Element einer Halbgruppe nennt man auch Einselement der Halbgruppe. Somit bilden alle Zeichengestalten mit der Operation der Verkettung eine Halbgruppe mit Einselement.
Wie bei jeder binären Operation lassen sich Potenzen erklären: Für jede Zeichengestalt z sei:
$z^0 =_{def} \epsilon$ und $\forall$ n $\in$ Nz: $z^{n+1} =_{def} z^n z$.
Wegen der Assoziativität gelten die Potenzgesetze:
$\forall$ n, m $\in$ Nz: $z^n z^m = z^{n+m} \wedge (z^n)^m = z^{n \cdot m}$.
In der Praxis wird man nicht die Menge Z aller Zeichengestalten betrachten. Man wählt vielmehr eine gewisse nichtleere Teilmenge B $\subseteq$ Z aus und betrachtet die durch Verkettung von Zeichengestalten aus B erzeugbaren Zeichengestalten. Um diese Menge zu definieren, führen wir zunächst die Verkettung von Mengen von Zeichengestalten ein durch:
$\forall$ A, C $\subseteq$ Z: A $\cdot$ C $=_{def} \{z_1 z_2 \mid z_1 \in A \wedge z_2 \in C\}$
Dadurch wird $\cdot$ in der Potenzmenge 2^Z zu einer vollständigen und offenbar auch assoziativen Operation, so daß auch die Potenzmenge von Z eine Halbgruppe mit dem Einselement $\{\epsilon\}$ bildet. Deshalb lassen sich wieder Potenzen erklären:
$\forall$ A $\subseteq$ Z: $A^0 =_{def} \{\epsilon\}$ (gilt auch für A = $\emptyset$) und $\forall$ n $\in$ Nz: $A^{n+1} =_{def} A^n \cdot A$.
Wegen der Assoziativität gelten auch für diese Operation die Potenzgesetze.

Definition 10.1.
Ist B eine Teilmenge von Zeichengestalten, so heißt die Menge von Zeichengestalten $B^* =_{def} \{z \mid \exists\, i \in \underline{\mathrm{Nz}} \wedge z \in B^i\} = \bigcup_{i \in Nz} B^i$ der Stern von B.
Die Sternbildung erfolgt also völlig analog zur Bildung der transitiven Hülle einer binären Relation. Auch bei der Sternbildung gelten wieder die Hülleneigenschaften:

Für beliebige A, B, $\subseteq$ Z gilt:
(1) $B \subseteq B^*$ (Einbettung)
(2) $A \subseteq B \Rightarrow A^* \subseteq B^*$ (Monotonie)
(3) $(B^*)^* = B^*$ (Abgeschlossenheit).
Aus (3) folgt sofort: $B^* \cdot B^* = (B^*)^* = B^*$, also ist B^* stabile Teilmenge von Z und deshalb die Einschränkung der Verkettung auf B^* eine (vollständige) Operation auf B^*, also ist B^* mit der Verkettung eine Halbgruppe, die wegen $\epsilon \in \{\epsilon\} = B^0 \subseteq B^*$ ein Einselement besitzt. Sie heißt die von B erzeugte Halbgruppe.

Beispiel 10.1.
a) A = { = , |||}. Dann ist:
A^0 = { ϵ } , die Einermenge der leeren Zeichengestalt,
A^2 = { = = , = |||, ||| = , ||||||}.
b) B = {||, |||}. Dann ist:
B^0 = { ϵ },
B^2 = {||||, |||||, ||||||}.

Beide Beispiele zeigen einen wesentlichen Unterschied. Während A^2 aus 4 Zeichengestalten besteht, umfaßt B^2 nur 3 Zeichengestalten, da zwei der bildbaren Zeichengestalten einander gleich sind. Zu jedem geordneten n-Tupel von Elementen aus A gibt es genau eine Zeichengestalt, die durch Verkettung dieser Elemente in der festgelegten Reihenfolge entsteht, und verschiedenen n-Tupeln entsprechen auch verschiedene Zeichengestalten. Im Gegensatz dazu können verschiedene n-Tupel aus Elementen von B auf die gleiche Zeichengestalt führen.

Definition 10.2.
Es sei (N, $\cdot$) eine Halbgruppe mit dem Einselement ϵ. (N, $\cdot$) heißt freie Halbgruppe mit dem Einselement ϵ genau dann, wenn es eine Teilmenge B $\subseteq$ N $\setminus$ $\{\epsilon\}$ gibt mit folgender Eigenschaft: Zu jedem Element p $\in$ N $\setminus$ $\{\epsilon\}$ gibt es genau eine positive Zahl n und ein geordnetes n-Tupel $[b_1, ..., b_n]$ von Elementen aus B mit p = $b_1 \cdot b_2 \cdot ... \cdot b_n$. B heißt Basis (Erzeugendensystem) der freien Halbgruppe.
Ist B eine endliche Menge, so heißt die freie Halbgruppe (N, $\cdot$) endlich erzeugbar.

Satz 10.1.
Ist (N, $\cdot$) eine freie Halbgruppe mit Einselement ϵ und der Basis B, so gilt :
$\forall$ n, m $\in$ Nz: (n $\neq$ m $\rightarrow B^n \cap B^m = \emptyset$).

Beweis:
1) Ist B = $\emptyset$, so gilt nach Definition: $B^0 = \{\epsilon\}$ und
$\forall$ n $\in$ Nz$^+$: $B^n = \emptyset$, d.h. n $\neq$ m $\Rightarrow B^n \cap B^m = \emptyset$.
2) Es sei B $\neq \emptyset$
a) n, m > 0. Es sei $B^n \cap B^m \neq \emptyset$. Dann gibt es p $\in B^n \cap B^m$ und wegen p $\in B^n$ gibt es Elemente $b_1, ..., b_n \in B$ und wegen p $\in B^m$ auch die Elemente $b'_1, ..., b'_m \in B$ und es gilt: p = $b_1 \cdot ... \cdot b_n = b'_1 \cdot ... \cdot b'_m$.
Aus der nach Voraussetzung geforderten Gleichheit der Tupel $[b_1, ..., b_n]$ und $[b'_1, ..., b'_m]$ folgt n = m und $b_i = b'_i$ für 1 $\leq$ i $\leq$ n.
Also: $B^n \cap B^m \neq \emptyset \Rightarrow$ n = m, d.h. n $\neq$ m $\Rightarrow B^n \cap B^m = \emptyset$.
b) n > 0 und m = 0. Wegen B $\neq \emptyset$ und $\epsilon \notin B$ ist $\epsilon \notin B^n \neq \emptyset$.
Da $B^m = \{\ \epsilon\ \}$ gilt auch in diesem Fall $B^n \cap B^m = \emptyset$.
Damit ist der Satz bewiesen.

Satz 10.2.
Ist [N , $\cdot$] eine freie Halbgruppe mit der Basis B, so ist B die einzige Basis von [N , $\cdot$].

Beweis:
a) Ist $B = \emptyset$, so N = $\{\epsilon\}$. Ist B' ebenfalls Basis, so folgt wegen $B' \subseteq \{\epsilon\}\backslash\{\epsilon\}$.
$B' = \emptyset = B$.
b) Es sei B $\neq \emptyset$ und B' ebenfalls Basis. Für alle $b \in B$ gilt $b \neq \epsilon$. Daher gibt es für jedes $b \in B$ eine natürliche Zahl n und Elemente b'_i mit i $\in$ {1, ... , n} und $b = b'_1 \cdot ... b'_n$, d.h. $b \in B'^n$. Aus dem gleichen Grund gibt es aber auch zu jedem b'_i eine positive natürliche Zahl k_i mit $b'_i \in B^{k_i}$. Daher gilt auch:
$b = b'_1 ... b'_n \in B^r$ mit r = $\sum\limits_{i=1}^{n} k_i$. Nach Satz 10.1. folgt dann: 1 = $\sum\limits_{i=1}^{n} k_i$,
n = 1 und $k_1 = 1$, d.h. b = $b'_1 \in B'$. Also ist $B \subseteq B'$
Genau so zeigt man: $B' \subseteq B$, also demnach $B = B'$.

Für unsere weiteren Betrachtungen sind nun solche (nichtleeren) Mengen von Zeichengestalten B wichtig, für die bezüglich der Verkettung B^* eine freie Halbgruppe mit der Basis B ist. Wir führen dazu folgende Begriffe ein:

Definition 10.3.
Ist B eine nichtleere Menge von Zeichengestalten und $(B^*, \cdot)$ mit der Operation Verkettung eine freie Halbgruppe mit der Basis B, so heißt B ein Alphabet, die Elemente von B Atomgestalten oder Grundzeichen, die Elemente von B^* Zeichenreihen oder Wörter über B, und Wortmengen L $\subseteq B^*$ (formale) Sprachen über dem Alphabet B.
Offensichtlich ist aus Beispiel 10.1. die Menge A ein Alphabet. Die Menge B ist dagegen kein Alphabet.

Satz 10.3.
Ist B $\neq \{\epsilon\}$ eine Menge von Zeichen, für die gilt:
$\forall$ u, v, x, y ((u, v $\in B^* \wedge$ x, y $\in B \wedge$ ux = vy) $\rightarrow$ (u = v $\wedge$ x = y)),
so ist B ein Alphabet und B^* mit der Operation der Verkettung eine freie Halbgruppe mit der Basis B.

Beweis:
Ist $B = \emptyset$, so liegt der für uns uninteressante triviale Fall $B^* = \{ \epsilon \}$ vor. Wir können also $B \neq \emptyset$ voraussetzen.
1) $\epsilon \notin B$. Denn wäre $\epsilon \in B$, so folgt wegen $B \neq \emptyset$ und $B \neq \{\epsilon\}$, daß es in B ein Element $b \neq \epsilon$ gibt. Dann gilt aber $\epsilon\, b = b\, \epsilon$ mit $\epsilon \neq b$ im Widerspruch zur Voraussetzung. Also gilt: $B \subseteq B^* \backslash \{\epsilon\}$.
2) Es sei $p \in B^* \backslash \{\epsilon\}$, dann gibt es n $\in$ Nz und $p \in B^n$. Wegen $B^0 = \{\epsilon\}$ und $p \neq \epsilon$ folgt dann: n $\geq$ 1, d.h. es gibt $b_1, ..., b_n \in B$ mit $p = b_1 b_2 ... b_n$. Angenommen, es gäbe m $\in$ $\underline{Nz^+}$ und $b'_1, ..., b'_m$ *in* B mit $p = b'_1 ... b'_m$. Ohne Beschränkung der Allgemeinheit können wir m $\geq$ n voraussetzen. Wir zeigen durch vollständige Induktion: n = m und $\forall$ i $\in$ {1, ... , n}: $b_i = b_i$'.
Induktionsanfang: n = 1 und $p = b_1 = b'_1 ... b'_m$. Wegen $\epsilon\, b_1 = b'_1 ... b'_m$ folgt dann aus der Voraussetzung des Satzes: $b_1 = b'_m$ und $\epsilon = b'_1 ... b'_{m-1} \in B^{m-1}$.
Aus $\epsilon \in B^{m-1}$ folgt m - 1 = 0, also m = 1. Dann gilt: n = m = 1 und $b_1 = b'_1$.
Induktionsvoraussetzung: Für alle k mit 1 $\leq$ k $\leq$ n gelte: wenn $p \in B^k$, so gibt es genau ein k-Tupel $[b_1, ... b_k]$ von Elementen aus B und $p = b_1 ... b_k$ und für alle j $\neq$ k gilt: $p \notin B^j$.
Induktionsschluß: $p \in B^{n+1}$. Dann gibt es $w \in B^n$ und $b \in B$ und $p = wb$. Aus $wb = b'_1 ... b'_m$ folgt dann: $b = b'_m$ und $w = b'_1 ... b'_{m-1}$. Nach Induktionsvoraussetzung gilt wegen $w \in B^n$: m - 1 = n, das n-Tupel $[b'_1, ..., b'_n]$ ist eindeutig bestimmt und für alle j mit j $\neq$ n ist $w \notin B^j$. Dann gilt aber auch für $p \in B^{n+1}$: das (n+1)-Tupel $[b'_1, ..., b'_{n+1}]$ mit n + 1 = m ist eindeutig bestimmt und für alle j $\neq$ n + 1 gilt $p \notin B^j$. Der Satz ist damit bewiesen. B^* ist bezüglich der Verkettung eine freie Halbgruppe mit der Basis B, also B Alphabet.
Ist also B Alphabet, so gibt es zu jedem Wort $w \in B^*$ genau eine natürliche Zahl n mit $w \in B^n$. Gilt $p \in B^n$ und $w \in B^m$, so folgt: $pw \in B^n \cdot B^m = B^{n+m}$. Das gibt Anlaß zu folgender Definition:

Definition 10.4.
Ist B^* Wortmenge über dem Alphabet B, so heißt die jedem Wort w $\in B^*$ eindeutig zugeordnete natürliche Zahl n, für die gilt: w $\in B^n$ die Länge von w und wird mit l(w) bezeichnet.
Wie bereits bemerkt, gilt dann:
l(pw) = l(p) + l(w), l(ϵ) = 0, l(px) = l(p)+1.

Die Algebra [Nz, +] mit der Operation der Addition ist ebenfalls eine freie Halbgruppe mit der Basis $B = \{1\}$. Durch die Funktion l(x) wird dann die freie Halbgruppe B^* mit der Operation der Verkettung eindeutig auf [Nz , +] operationstreu abgebildet.

Es werden noch folgende Begriffe eingeführt:
Definition 10.5.
Es sei B Alphabet und B^* die Wortmenge über B.
w $\in B^*$ heißt Teilzeichenreihe (Teilwort) von z $\in B^*$ genau dann, wenn
$\exists$ u, v $\in B^*$: z = uwv.
w $\in B^*$ heißt Anfangsstück (Anfangswort) von z $\in B^*$ genau dann, wenn
$\exists$ v $\in B^*$: z = wv.
w $\in B^*$ heißt Endstück (Endwort) von z $\in B^*$ genau dann, wenn $\exists$ u $\in B^*$: z = uw.
w $\in B^*$ heißt echtes Teil- bzw. Anfangs- bzw. Endwort von z $\in B^*$ genau dann, wenn w ist Teil- bzw. Anfangs- bzw. Endwort von z und w $\neq \epsilon$ und w $\neq$ z.

Sei B^* die Wortmenge über einem Alphabet B. Jedes geordnete Paar $[a, w]$ mit $a \in B$ und $w \in B^*$ bestimmt auf B^* eine einstellige Operation, wir bezeichnen sie mit ${}^a/_w$, die man Einsetzung von w für a nennt. Ist $\epsilon \neq z \in B^*$, so gibt es genau eine Zerlegung $z = b_1 b_2 ... b_n$ mit n = l(z) und $b_i \in$ B für 1 $\leq$ i $\leq$ n. Aus dieser Zerlegung läßt sich offensichtlich in eindeutiger Weise eine Zerlegung $z = u_0 a u_1 a ... a u_m$ mit $u_i \in (B \setminus \{a\})^*$ für alle 0 $\leq$ i $\leq$ m erhalten, d.h. die u_i enthalten kein Grundzeichen $a \in$ B.

Definition 10.6.a) Einsetzung

$$z\ {}^a/_w =_{def} \begin{cases} z & \text{falls } m = 0 \text{ oder } z = \epsilon \\ u_0 w u_1 w ... w u_m & \text{falls } m > 0 \text{ und } z = u_0 a u_1 a ... a u_m. \end{cases}$$

Es wird also für jedes in z vorkommende Grundzeichen a das Wort w eingesetzt. Offenbar ist $z\ {}^a/_w$ eindeutig bestimmt und heißt das durch Einsetzen von w für a in z entstandene Wort.
Außer dieser einfachen Einsetzung verwendet man noch die simultane Einsetzung.

Es sei $\{a_1, ..., a_n\} \subseteq$ B eine aus n Elementen bestehende Teilmenge von B. Jedem a_i aus dieser Menge sei eindeutig ein Wort $w_i \in B^*$ zugeordnet. Dann existiert wieder eine eindeutige Zerlegung für jedes Wort $z \in B^*$:
$z = u_o a_{i_1} u_1 a_{i_2} ... a_{i_k} u_k$ mit $a_{i_j} \in \{a_1, ..., a_n\} \wedge u_j \in (B \setminus \{a_1, ..., a_n\})^*$ für alle 1 $\leq$ j $\leq$ k.
Die geordneten Paare $[a_i, w_i]$ sind dann Paare mit paarweise verschiedenen ersten Komponenten.

Definition 10.6.b) simultane Einsetzung

$$z\,{}^{a_1}/_{w_1},\ldots,{}^{a_n}/_{w_n} =_{def} \begin{cases} z & \text{falls } k=0 \text{ oder } z=\epsilon \\ u_0w_{i_1}u_1w_{i_2}\ldots w_{i_k}u_k & \text{falls } k>0 \text{ und } z=u_0a_{i_1}u_1a_{i_2}\ldots a_{i_k}u_k. \end{cases}$$

Die simultane Einsetzung ist von einer Folge einfacher Einsetzungen wohl zu unterscheiden, läßt sich jedoch durch einfache Einsetzung mit Umbenennung beschreiben.

Beispiel 10.2.
Sei $B = \{a,\ b,\ c,\ (,),+,\ *\}$ und $z = ((a+b)\ *c)$.
Wir bilden: $z\ a/a*c),\ b/\ (b*c,\ */\ \epsilon,\ c/\epsilon$.
Die Zerlegung ist: $z = ((a+b)*c)$.
Das Ergebnis lautet: $u_0\ a*\ c)\ u_1\ (b*c\ u_2\ \epsilon\ u_3\ \epsilon\ u_4 = ((a*c)\ +\ (b*c))$ mit
$u_0 = ((\ ,\ u_1 = +,\ u_2 = u_3 = \epsilon,\ u_4 =)$
Im Gegensatz dazu erhält man bei der Folge einfacher Einsetzungen:
$((((z\ a/a*c))\ b/\ (b*c)\ \ */\epsilon)\ c/\epsilon)$ der Reihe nach:
$((a+b)*c), ((a*c)+b)*c), ((a*c)+(b*c)\ *c), ((ac)+(bc)c), ((a)+(b))$.

Anmerkung
B = {|} sei ein einelementiges Alphabet. Jeder natürlichen Zahl n > 0 kann genau ein Wort $|^n$ aus B^* umkehrbar eindeutig zugeordnet werden. Die Wörter aus B^* können daher als Zahlwörter (Namen für Zahlen) verwendet werden. Dann lassen sich Addition und Multiplikation natürlicher Zahlen durch Verkettung und Einsetzung darstellen:
$2+3=5$ entspricht $||\cdot||| = |||||$
$2\cdot 3 = 6$ entspricht $||\ {}^{|}/_{|||} = ||||||$

Eine weitere semiotische Operation ist die Spiegelung $^\sim$. Sie ist wie folgt definiert:
Definition 10.7.
$\tilde{\epsilon} =_{def} \epsilon$ und $\tilde{z} =_{def} b_nb_{n-1}\ldots b_1$ für z = $b_1\ldots b_n$ und $b_i \in$ B ($1 \le$ i $\le$ n)

Eigenschaften
1) l($\tilde{z}$) = l (z), d.h. bei einer Spiegelung ändert sich die Länge nicht
2) $\tilde{\tilde{z}}$ = z, d.h. zweimalige Spiegelung ergibt die Identität
(die Spiegelung ist involutorisch)
3) $\widetilde{wz} = \tilde{z}\tilde{w}$, d.h. die Spiegelung ist ein Antihomomorphismus
(operationstreu mit Vertauschung der Operanden).

Wir betrachten noch die vierstellige Relation der Ersetzung nach
Definition 10.8.
Die Wörter z, w, w′, z′ $\in B^*$ stehen in der Relation "Ersetzung": Ers(z, w, w′, z′) genau dann, wenn es eine natürliche Zahl n $\in$ Nz und Zerlegungen z = $x_0x_1\ldots x_{2n}$ und $z' = x'_0x'_1\ldots x'_{2n}$ gibt, so daß gilt: $x_{2i} = x'_{2i}$ für $0 \le$ i $\le$ n und x_{2i-1} = w und x'_{2i-1} = w′ für n > 0 und $1 \le$ i $\le$ n.
(Anschaulich bedeutet das, in z wird an keiner Stelle oder an beliebigen Stellen, an

denen das Teilwort w vorkommt, dieses Teilwort gestrichen und dafür w′ eingetragen. Das Ergebnis ist das Wort z′.)
Das Wort z′ ist also i.a. nicht eindeutig durch z, w, w′ bestimmt. Deshalb ist die Ersetzung auch keine Operation (im Gegensatz zur Einsetzung), sondern eine Relation.

Beispiel 10.3.
Sei $B = \{$a, b, c, d$\}$, z = abcbcbd, w = bcb und w′ = b.
Ersetzungsmöglichkeiten:
1) Zerlegung: $\underbrace{abcbcbd}_{x_0}$, $z' = abcbcbd$, Ers($abcbcbd$, bcb, b, $abcbcbd$)
2) Zerlegung: $\underbrace{a}_{x_0}\underbrace{bcb}_{x_1}\underbrace{cbd}_{x_2}$ $z' = abcbd$,Ers ($abcbcbd$, bcb, b, $abcbd$)
3) Zerlegung: $\underbrace{abc}_{x_0}\underbrace{bcb}_{x_1}\underbrace{d}_{x_2}$ $z' = abcbd$,Ers ($abcbcbd$, bcb, b, $abcbd$)

Eigenschaft:
Offensichtlich gilt für z,w, w′ $\in B^*$ immer:
Ers (z,w,w′, z),
Ers (z,z,w′,w′),
Ers (z,w,w,z).

Übungsaufgaben

Grundkurs Theoretische Informatik
Mengentheoretisch-algebraische Grundlagen

Aufgabenblatt I

1) Mittels Wahrheitstabellen ist zu prüfen, welche der folgenden Aussageverbindungen allgemeingültig sind:
   a) $(A \rightarrow B) \leftrightarrow (\sim B \rightarrow \sim A)$
   b) $(A \rightarrow B) \rightarrow (B \rightarrow A)$
   c) $(\sim A \rightarrow B) \rightarrow (\sim B \rightarrow A)$
   d) $((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$
   e) $(A \rightarrow B) \leftrightarrow (\sim A \vee B)$
   f) $\sim (A \vee B) \leftrightarrow (\sim A \wedge \sim B)$
   g) $\sim (A \wedge B) \leftrightarrow (\sim A \vee \sim B)$
   h) $\sim (A \vee B) \leftrightarrow (\sim A \vee \sim B)$
2) Die Relation = erfüllt die folgenden Gesetze:
   a) $x = x$ (Reflexivität)
   b) $x_1 = x_2 \rightarrow x_2 = x_1$ (Symmetrie)
   c) $x_1 = x_2 \wedge x_2 = x_3 \rightarrow x_1 = x_3$ (Transitivität)
   d) $x_1 = x_2 \wedge x_1 = x_3 \rightarrow x_2 = x_3$ (Drittengleichheit)
   Man beweise, daß aus Gesetzen (a) und (d) die Gesetze (b,c) folgen.
3) Es sind folgende Mengen über dem Individuenbereich I der ganzen Zahlen zu bilden:
   $M_1 =_{def} \{x \mid (x^2 - 3x + 2)(x - 3) = 0\}$,
   $M_2 =_{def} \{x \mid ((x > 5 \wedge x < 7)) \vee ((x > -5) \wedge (x \leq 0))\}$,
   $M_3 =_{def} \{x \mid (x > 0) \wedge (x \leq 3)\}$,
   $M_4 =_{def} \{x \mid (x < -2) \wedge (x^2 < 3)\}$.
   Welche der Mengen sind gleich?
4) A und B seien endliche Mengen und N(X) die Zahl der Elemente der Menge X. Man zeige die Gleichung
   $N(A \cup B) = N(A) + N(B) - N(A \cap B)$.
5) Man zeige, daß eine Menge mit n Elementen 2^n verschiedene Teilmengen enthält.
6) Man zeige: Es sei I ein Individuenbereich, M und N sind Mengen über I. Dann ist allgemeingültig:
   $(M \subseteq N) \leftrightarrow (M \cap N = M)$ und
   $(M \subseteq N) \leftrightarrow (M \cup N = N)$.

Grundkurs Theoretische Informatik
Mengentheoretisch-algebraische Grundlagen

Aufgabenblatt II

1) Man zeige: I sei ein Individuenbereich, M, N, Q Mengen über I. Dann ist M ∪ N im folgendem Sinn die "kleinste" Menge, die sowohl M als auch N enthält:
   $\forall$ M, N, Q : ((M ⊆ Q) ∧ (N ⊆ Q) → M ∪ N ⊆ Q)
2) Man zeige: Sind M, N, Q Mengen über I, so gilt:
   $\forall$ M, N, Q: (N ⊆ M → Q ∩ N ⊆ Q ∩ M)
   $\forall$ M, N, Q: (N ⊆ M → Q ∪ N ⊆ Q ∪ M)
   $\forall$ M, N, Q: (N ⊆ M → Q \ M ⊆ Q \ N)
3) Es seien M und N Mengen über I.
   Welche der Mengen P, Q, R sind gleich?
   $P =_{def} I\backslash(M \cup N)$, $Q =_{def} (I\backslash M) \cup (I\backslash N)$
   $R =_{def} (I\backslash M) \cap (I\backslash N)$? (vergl. Aufgabe 1)
4) Es sei $R + S =_{def} (R\backslash S) \cup (S\backslash R)$, R, S Mengen. Man zeige, daß die folgenden Beziehungen gelten.
   a) R+ S = S + R
   b) R + (S + T) = (S + R) + T
   c) R + R = ∅
   d) S + T = (S ∪ T) \ (S ∩ T)
5) Man gebe eine notwendige und eine hinreichende Bedingung dafür an, daß die folgende Beziehung gilt: S + T = S ∪ T

Aufgabenblatt III

1) Es sei F Korrespondenz aus M in N und G Korrespondenz aus N in Q.
   Man zeige: Vb (F · G) $\subseteq$ Vb (F).
   Läßt sich die Aussage verschärfen, wenn G Korrespondenz von N in Q ist?
2) a, b, c seien drei Geraden einer Ebene, die sich paarweise in drei verschiedenen Punkten schneiden. In der gleichen Ebene seien die Punkte p und q gegeben.
   p und q sind zwei verschiedene Punkte, die auf keiner der Geraden a, b, c liegen.
   A sei die Menge der Punkte der Geraden a, B sei Menge der Punkte der Geraden b, C Menge der Punkte der Geraden c. Folgende Korrespondenzen seien definiert:
   F Korrespondenz aus A in B $=_{def}$ xFy $\leftrightarrow \exists$ h (h ist Gerade $\wedge$ x,y,p auf h)
   G Korrespondenz aus B in C $=_{def}$ yGz $\leftrightarrow \exists$ h' (h' ist Gerade $\wedge$ y,z,q auf h')
   a) Ist F eindeutig ?
   b) Ist F 1-1-Abbildung ?
   c) Ist F Korrespondenz von A auf B ?
   d) Bestimme Vb (F · G) und Nb (F · G)
3) Man zeige: R sei (binäre) Relation über M. Dann gilt:
   R reflexiv $\leftrightarrow Id_M \subseteq$ R , R symmetrisch $\leftrightarrow R^{-1} \subseteq$ R
   R antisymmetrisch $\leftrightarrow R \cap R^{-1} \subseteq Id_M$, R asymmetrisch $\leftrightarrow R \cap R^{-1} = \emptyset$
   R transitiv $\leftrightarrow R \cdot R \subseteq R$.
4) Man zeige: Sind R und S Äquivalenzrelationen über einer Menge M, so gilt:
   R · S Äquivalenzrelation über M $\leftrightarrow$ R · S = S · R
5) Es sei Q Quasihalbordnungsrelation über M und R die zu Q gehörige Äquivalenzrelation, M / R die Quotientenmenge von M nach R.
   Man zeige: Q' $=_{def}$ $\{[B_R(a), B_R(b)]$ | aQb$\}$ ist Halbordnungsrelation über M / R.
   (B_R(x) volles Bild von x bei R)
6) Man zeige: Wenn R endliche nichtleere Halbordnung, dann besitzt R maximale Elemente
7) Es sei R folgende Relation über der Menge P der rationalen Zahlen:
   R $=_{def}$ $\{$[a,b] | a, b $\in$ P $\wedge$ a + b $\leq$ 5$\}$
   Ist R reflexiv? Ist R symmetrisch? Ist R transitiv?
   Ist R antisymmetrisch? Ist R asymmetrisch?

Aufgabenblatt IV

1) Es sei M die Menge aller Aussagen. Auf M sei folgende Relation R definiert: aRb $\leftrightarrow$ (a $\rightarrow$ b).
   Man bestimme die Hülle R^* von R.
2) Es sei M = $\{a_1, a_2, a_3, a_4, a_5\}$ und R = $\{[a_1, a_3]$, $[a_1, a_4]$, $[a_2, a_3]$, $[a_2, a_4]$, $[a_3, a_5]$, $[a_4, a_5]\}$
   Man bilde $\bar{R} = R^* \cup Id_M$ und zeige, daß $\bar{R}$ Halbordnungsrelation ist.
   (R^* transitive Hülle von R).
3) Man zeige: Für jede Teilmenge N $\subseteq$ M existiert höchstens ein inf(N) bzgl. einer Halbordnungsrelation R auf M
4) Man beweise: Wenn R eine symmetrische Relation ist, dann ist auch $R \cup R^2 \cup ... R^n$ eine symmetrische Relation.
5) Es seien X, Y und Z Teilmengen von U mit den Eigenschaften Y $\cap$ Z = $\emptyset$ und Y $\cup$ Z = X. Man gebe eine bijektive Funktion f von $\wp(X)$ auf $\wp(Y) \times \wp(Z)$ an. ($\wp$ (M) Potenzmenge M)
6) Man zeige, daß eine Menge von n Elementen 2^{n-1} -1 Partitionen mit zwei Äquivalenzklassen (ungleich $\emptyset$) besitzt.
7) X sei eine endliche Menge und f: X $\rightarrow$ X sei eine Injektion, dann ist f eine Bijektion.
   Man zeige an einem Beispiel, daß dies nicht für unendliche Mengen gilt.

Grundkurs Theoretische Informatik
Mengentheoretisch-algebraische Grundlagen

Aufgabenblatt V

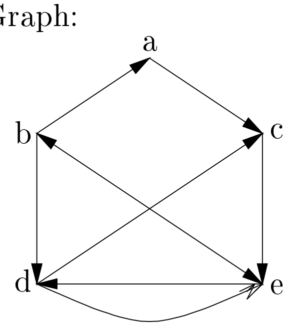
1) Es sei m eine positive ganze Zahl. Zwei ganze Zahlen a,b heißen kongruent modulo m ($a \equiv b \bmod m$), wenn m ein Teiler von (a-b) ist. Zeigen Sie, daß die damit erklärte binäre Relation auf der Menge der ganzen Zahlen eine Äquivalenzrelation ist.
2) Es sei f eine einstellige Operation über einer nichtleeren endlichen Menge M, und R die wie folgt definierte binäre Relation:
   $[x,y] \in R$ genau dann, wenn es eine natürliche Zahl n gibt mit $f^n\ (x) = y$.
   Zeigen Sie die Reflexivität und Transitivität von R.
   (Bemerkung: $f^\circ\ (x) = x$, $f^{n+1}\ (x) = f(f^n\ (x)) = f^n \circ f\ (x))$
3) Es seien f, g zwei einstellige Operationen über reellen Zahlen mit $f(x) = x^2 + 3x + 1$ und $g(x) = 2x-3$.
   Welche Operationen ergeben sich durch Komposition $f \circ g$ und $g \circ f$?
4) Es sei $(M, \leq_M)$ eine lineare Ordnung.
   Zeigen Sie die Äquivalenz folgender Bedingungen:
   a) Jede Teilmenge $N \subseteq M$ besitzt ein kleinstes Element.
   b) Es gibt eine Injektion f: $\underline{Nz} \to M$, so daß für alle natürlichen Zahlen $n, m \in \underline{Nz}$ gilt:
      $m < n \to f(m) <_M f(n)$.
5) Es sei $(M, \leq)$ eine lineare Ordnung und $N \subseteq M$ eine endliche nichtleere Teilmenge von M. Zeigen Sie, daß N ein kleinstes und ein größtes Element besitzt.

Aufgabenblatt VI

1) Welche der definierten Eigenschaften sind für die Operationen
größter gemeinsamer Teiler (ggT) zweier ganzer Zahlen und
Multiplikation ($*$) zweier (m,n) Matrizen ganzer Zahlen
erfüllt?
2) Untersuchen Sie, ob das Hintereinanderschreiben der Zifferndarstellungen natürlicher Zahlen aus $\underline{\mathrm{Nz}}^+$ als binäre Operation assoziativ, kommutativ, umkehrbar, kürzbar ist. Gibt es in $\underline{\mathrm{Nz}}^+$ bezüglich dieser Operation links- bzw. rechtsneutrale Elemente?
($13 \circ 6 =_{def} 136$)
3) Gegeben seien die Operationen
$\circ_1$ Arithmetisches Mittel rationaler Zahlen $a \circ_1 b =_{def} \frac{a+b}{2}$
$\circ_2$ Geometrisches Mittel nichtnegativer reeller Zahlen $a \circ_2 b =_{def} \sqrt{a \cdot b}$
$\circ_3$ Harmonisches Mittel positiver reeller Zahlen $a \circ_3 b =_{def} \frac{2 \cdot a \cdot b}{a+b}$.
Untersuchen Sie diese Operationen auf Kommutativität, Assoziativität, Umkehrbarkeit. Zeigen Sie, daß keine dieser Operationen ein neutrales Element besitzt und daß alle Operationen idempotent sind.
4) Gegeben seien die Operationen
$a \circ_1 b =_{def} a - b$, $a \circ_2 b =_{def} 2a + b$, $a \circ_3 b =_{def} a + b - (a \cdot b)$
Welcher der Operationen sind kommutativ, welche sind assoziativ? Zeigen Sie, daß die Operation $\circ_3$ nicht umkehrbar und bei $\circ_2$ jede Gleichung $a \circ_2 x = c$ für x eindeutig lösbar, aber nicht jede Gleichung $y \circ b = c$ für y lösbar ist.
Existieren Eins- oder Nullelemente?

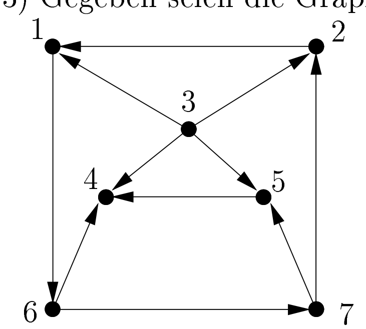
Aufgabenblatt VII

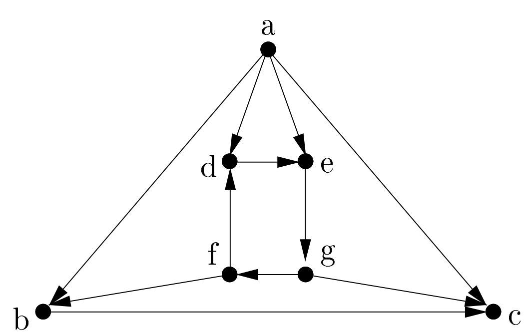
1) Geben Sie alle zusammenhängenden ungerichteten kreisfreien Graphen mit 5 Knoten an.
2) Gegeben sei der Graph:



a) Ist der Graph stark zusammenhängend?
b) Wieviele wiederholungsfreie Ketten und Wege existieren von b nach e ?
c) Bilden Sie den Untergraphen mit den Knoten a, c, e, d. Ist dieser Graph noch zusammenhängend bzw. stark zusammenhängend ?

3) Gegeben seien die Graphen:





Sind diese Graphen isomorph und wenn ja, warum ?

4) Zeigen Sie, daß ein ungerichteter Graph, in dem es zwei unterschiedliche Wege von einem Knoten zu einem anderen Knoten gibt, nicht kreisfrei ist ! Gilt dies auch für gerichtete Graphen ?
5) Zeigen Sie, daß es zu jedem Weg von a nach b in einem gerichteten Graphen (M,R) genau eine natürliche Zahl k > 0, gibt, so daß (a,b) $\in R^k$ ist.
6) Zeigen Sie, daß ein gerichteter Graph (M,R) genau dann stark zusammenhängend ist, wenn $M^2 \subseteq$ (R $\cup R^{-1}$ $)^*$!

Aufgabenblatt VIII

1) Geben Sie ein Verfahren zur Bestimmung der Basis eines endlichen Graphen an und implementieren Sie dieses Verfahren auf einem Rechner.

2) Zeigen Sie, daß die Elemente A_G^k (i,j) der k-ten Potenz der Adjazenzmatrix eines endlichen Graphen G mit der Anzahl der Wege der Länge k in G vom Knoten i zum Knoten j übereinstimmen.

3) Zeigen Sie, daß ein endlicher Graph genau dann kreisfrei ist, wenn eine natürliche Zahl l existiert mit $A_G^l \neq 0$ und $A_G^n = 0$ für alle n > l. (A_G bezeichnet die Adjazenzmatrix von G und 0 die Nullmatrix.)

4) Zeigen Sie, daß zwei endliche Graphen G_1 , G_2 genau dann isomorph sind, wenn sich ihre Inzidenzmatrizen I_{G_1} , I_{G_2} durch Vertauschen von Zeilen und Spalten ineinander überführen lassen.

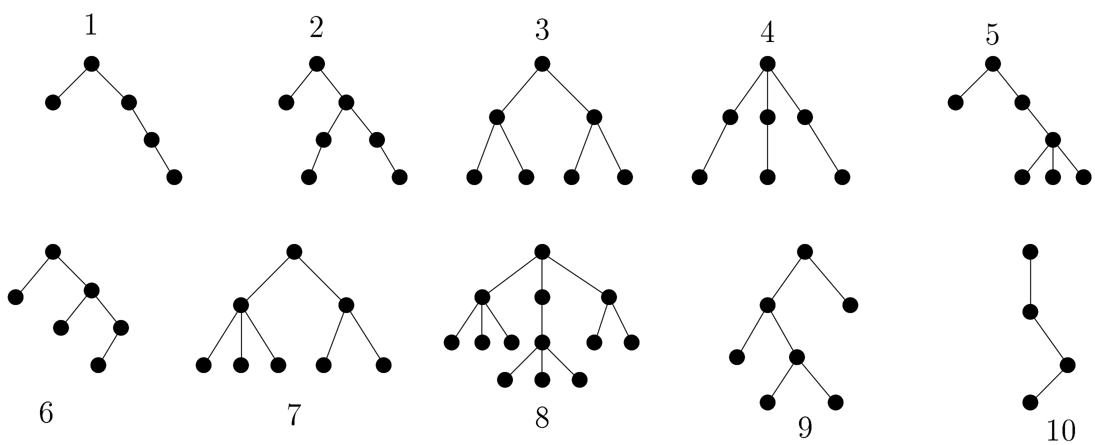
5) Zeigen Sie, daß zwei endliche Graphen G_1 , G_2 genau dann isomorph sind, wenn sich ihre Adjazenzmatrizen A_{G_1} , A_{G_2} durch gleichzeitiges Vertauschen von Zeilen und Spalten ineinander überführen lassen.

Grundkurs Theoretische Informatik
Mengentheoretisch-algebraische Grundlagen

Aufgabenblatt IX

1) Es sei G= (M,R) ein endlicher gerichteter Graph.
   a) Zeigen Sie, daß G Baum genau dann, wenn G zyklenfrei und $|M|$ -1 = $|R|$
   b) Zeigen Sie, daß G Baum genau dann, wenn G zusammenhängend und $|M|$ -1 = $|R|$

2) Welche der nachfolgenden Wurzelbäume sind
   a) ausgeglichen? b) vollständig ausgeglichen? c) gleichverzweigt?



3) In der Menge Nz^+ der natürlichen Zahlen größer als 0 sei für alle x,y $\in Nz^+$
   x $\leq$ y genau dann, wenn x Teiler von y ist.
   Zeigen Sie, daß Nz^+ bzgl. $\leq$ einen distributiven Verband $V_{\leq} = (Nz^+, \cap, \cup)$ bildet.

4) Zeigen Sie, daß eine endliche Halbordnung, in der ein Einselement existiert, und je zwei Elemente eine untere Grenze besitzen, einen Verband bildet.

5) Es sei B= (X, $\cap, \cup$, 0, 1, $^-$) eine Boolsche Algebra.
   Beweisen Sie, daß für jede natürliche Zahl n >0 und alle $x_i \in X$ die Gleichung

$$\overline{\bigwedge_{i=1}^{n} x_i} = \bigvee_{i=1}^{n} \bar{x}_i$$

   gilt.
   (Bemerkung: $\bigwedge_{i=1}^{1} x_i = \bigvee_{i=1}^{1} x_i = x_1$, $\bigwedge_{i=1}^{n+1} x_i = (\bigwedge_{i=1}^{n} x_i) \cap x_{n+1}$, $\bigvee_{i=1}^{n+1} x_i = (\bigvee_{i=1}^{n} x_i) \cup x_{n+1}$)

Aufgabenblatt X

1.) Zeigen Sie, daß aus der Gleichmächtigkeit der Mengen A und B die Gleichheit der Kardinalzahlen ihrer Potenzmengen folgt, d.h., $(\mathrm{A} \sim \mathrm{B}) \rightarrow |2^A| = |2^B|$.

2.) Zeigen Sie durch vollständige Induktion die Assoziativität der Funktion add, d.h., $\mathrm{add}_x\ (\mathrm{add}_y\ (\mathrm{z})) = \mathrm{add}_{\mathrm{add}_x(\mathrm{y})}\ (\mathrm{z})$ für alle x, y, z $\in$ N

3.) Geben Sie unter Benutzung der Funktion mult eine Rekursionsgleichung zur Definition der Fakultätsfunktion fac: $\mathrm{N} \rightarrow \mathrm{N}$ an.

4.) Zeigen Sie, daß die Sternbildung B^* die Eigenschaften der Einbettung $B \subseteq B^*$, Monotonie $A \subseteq B \Rightarrow A^* \subseteq B^*$ und Abgeschlossenheit $(B^*)^* = B^*$ erfüllt.

5.) Sei $(\mathrm{M}, \cdot)$ eine Halbgruppe und $(\mathrm{N}, +)$ die Halbgruppe der natürlichen Zahlen bzgl. der Addition.
Zeigen Sie: $\mathrm{X} \subseteq \mathrm{M}$ ist Basis von $(\mathrm{M}, \cdot)$ genau dann, wenn $\mathrm{X}^+ = \mathrm{M}$ und jede Funktion φ_0: $\mathrm{X} \rightarrow \mathrm{N}$ zu einem Homomorphismus φ von M in N erweitert werden kann.

INDEX