ÜBER ALGEBRAISCHE STRUKTUREN

A Aussagenlogik

1. Definitionen und Beispiele

Im folgenden sollen a, b , c, ... Aussagen bedeuten, denen man die Eigenschaft wahr (Wahrheitswert 1) oder falsch (Wahrheitswert 0) zuordnen kann.

Beispiele: a := Hans ist zu Hause
b := Hans ist in der Schule
c := Hans isst einen Apfel

Gegenbeispiele: x ist eine Primzahl, Wie viele Menschen gibt es auf der Erde?

Eine neue Aussage kann definiert werden, indem man ihre Wahrheitswerte für alle Kombinationen der Wahrheitswerte der Ausgangsaussagen definiert. Die Darstellung erfolgt in der sog. Wahrheitstafel (Wertetafel).

Definition 1: "Negation" Für die Verneinung einer Aussage a schreibt man $\neg$ a.
Pascal: NOT

Wahrheitstafel:

a	**$\neg$ a**
1	0
0	1

Beispiel: $\neg$ b = Hans ist nicht in der Schule

Verknüpft man zwei (und später endlich viele) Aussagen a und b miteinander, so entsteht eine **zusammengesetzte Aussage**

Definition 2: "Konjunktion" Für "a und b" (sowohl a als auch b) schreibt man a $\wedge$ b.
Pascal: AND

Wahrheitstafel:

a	**b**	**a $\wedge$ b**
1	1	1
1	0	0
0	1	0
0	0	0

Beispiel: a $\wedge$ b = Hans ist zu Hause und ist in der Schule
b $\wedge$ c = Hans ist in der Schule und isst einen Apfel

Definition 3: "Adjunktion" Für "a oder b" (nicht ausschl. oder) schreibt man $a \vee b$.
Pascal: OR

Wahrheitstafel:

a	b	a v b
1	1	1
1	0	1
0	1	1
0	0	0

Beispiel: $a \vee b$ = Hans ist zu Hause oder ist in der Schule
$b \vee c$ = Hans ist in der Schule oder isst einen Apfel

2. Logische Formeln und Gesetze, weitere Definitionen

Definition: Zwei **zusammengesetzte** Aussagen p und q heissen **logisch gleichwertig** oder **äquivalent**, wenn sie bei **jeder** Kombination der Wahrheitswerte ihrer Bestandteile jeweils den **gleichen** Wahrheitswert haben.
Schreibweise: $p = q$ (Vergleiche später: $\Leftrightarrow$ bei Aussageformen)

Beispiel: $p := a \wedge c$ = Hans ist zu Hause und isst einen Apfel
$q := c \wedge a$ = Hans isst einen Apfel und ist zu Hause

a	c	$p = a \wedge c$	$q = c \wedge a$
1	1	1	1
1	0	0	0
0	1	0	0
0	0	0	0

Hier gilt also: $p = q$

Es gilt also das Kommutativgesetz für $\wedge$:

(K1) $a \wedge b = b \wedge a$

Analog erkennt man zuerst vom deutschen Sprachgebrauch und dann mit math. Beweis der Wahrheitstafel, dass folgende Gesetze gelten: (vgl. auch Aufblatt 1, Nr 2)

(K2) $a \vee b = b \vee a$

(A1) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

(Assoziativgesetze)

(A2) $(a \vee b) \vee c = a \vee (b \vee c)$

(Ab1) $a \wedge (a \vee b) = a$ Absorptionsgesetze

(Ab2)	$a \vee (a \wedge b) = a$	(Verschmelzungsgesetze)
(D1)	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	Distributivgesetze
(D2)	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$	
(I1)	$a \wedge a = a$	Idempotenz
(I2)	$a \vee a = a$	
	$\neg(\neg a) = a$	Doppelte Verneinung
(M1)	$\neg(a \wedge b) = \neg a \vee \neg b$	de Morgan
(M2)	$\neg(a \vee b) = \neg a \wedge \neg b$	

Bemerkung: $\neg$ bindet stärker als $\wedge$ und $\vee$.

Beweise mit Hilfe der Wahrheitstafel: exemplarisch für (A2) und (M1):

für (A2):

a	**b**	**c**	**$a \vee b$**	**$p:=(a\vee b)\vee c$**	**$b\vee c$**	**$q:=a\vee(b\vee c)$**
1	1	1	1	**1**	1	**1**
1	1	0	1	**1**	1	**1**
1	0	1	1	**1**	1	**1**
0	1	1	1	**1**	1	**1**
1	0	0	1	**1**	0	**1**
0	1	0	1	**1**	1	**1**
0	0	1	0	**1**	1	**1**
0	0	0	0	**0**	0	**0**

gleiche Wahrheitstafel für p und q , also p = q.

für (M1):

a	**b**	**$a \wedge b$**	**$p:= \neg(a\wedge b)$**	**$\neg a$**	**$\neg b$**	**$q:= \neg a \vee \neg b$**
1	1	1	**0**	0	0	**0**
1	0	0	**1**	0	1	**1**
0	1	0	**1**	1	0	**1**
0	0	0	**1**	1	1	**1**

gleiche Wahrheitstafel für p und q , also p = q.

Definition 4: Eine zusammengesetzte Aussage, die für jede Kombination der Wahrheitswerte der Grundaussagen wahr ist, heisst Tautologie e (griechisch: dasselbe sagen).

Bemerkung: Jedes vorher angegebene Gesetz ist eine Tautologie, z.B.
$p:= [\neg(\neg a) = a]$ ist Tautologie, also p = e.
(Beweis: selber)

Behauptung: $a \vee \neg a = e$

Beweis:

$\mathbf{a}$	$\neg \mathbf{a}$	$\mathbf{a} \vee \neg \mathbf{a}$
1	0	1
0	1	1

<u>Definition 5</u>: Eine zusammengesetzte Aussage, die für <u>jede</u> Kombination der Wahrheitswerte der Grundaussagen <u>falsch</u> ist, heisst <u>Kontradiktion</u> n (lateinisch: Widerspruch)

<u>Behauptung</u>: $a \wedge \neg a = n$

Beweis:

$\mathbf{a}$	$\neg \mathbf{a}$	$\mathbf{a} \wedge \neg \mathbf{a}$
1	0	0
0	1	0

Für e und n gelten die folgenden Gesetze: (vgl. Aufblatt 1, Aufgabe 2e))

(N1)	$a \wedge n = n$	(N2)	$a \vee n = a$
(E1)	$a \wedge e = a$	(E2)	$a \vee e = e$

<u>Definition 6</u>: "Disjunktion" Für "entweder a oder b" (ausschl. oder) schreibt man $a \underline{\vee} b$.
Pascal: XOR

Wahrheitstafel:

$\mathbf{a}$	$\mathbf{b}$	$\mathbf{a} \underline{\vee} \mathbf{b}$
1	1	0
1	0	1
0	1	1
0	0	0

Beispiel: $a \underline{\vee} b$ = Entweder ist Hans zu Hause oder er ist in der Schule

<u>Behauptung</u>: $a \underline{\vee} b = (a \wedge \neg b) \vee (\neg a \wedge b)$ (vgl. Aufblatt1, Nr1, Nr 22)

Beweis: Aufblatt1, Nr 2f), erster Teil

3. Logikkalkül, weitere Definitionen

Man kann Aussagen durch wiederholte Verwendung der Zeichen $\wedge$, $\vee$, $\neg$ und $\underline{\vee}$ ('Junktoren') verknüpfen und so immer kompliziertere Aussagen bilden. Mit Hilfe der Gesetze aus Kapitel 2 gelingt es oft, Vereinfachungen herbeizuführen.

Beispiele:

1) $\neg (a \wedge \neg b) = \neg a \vee b$ (mit M1)

2) $(a \wedge b) \vee a = a \vee (a \wedge b) = a$ (mit K2 und Ab2)

3) $\neg (\neg a \wedge \neg b) = \neg (\neg a) \vee \neg (\neg b) = a \vee b$ (mit M1 und dopp. Vern.)

4) $(a \wedge b) \vee (a \vee b) = ((a \wedge b) \vee a) \vee b = a \vee b$

5) $(a \wedge b) \underline{\vee} (\neg a \wedge \neg b) = ((a \wedge b) \wedge \neg (\neg a \wedge \neg b)) \vee (\neg (a \wedge b) \wedge (\neg a \wedge \neg b)) = \ldots = (a \wedge b) \vee (\neg a \wedge \neg b)$

Beispiel 1) hat in der Logik eine spezielle Bedeutung: vgl. Aufblatt 1, Bsp 15:
a = Das Haus brennt, b = Die Feuerwehr kommt
$\neg (a \wedge \neg b)$ = Es ist nicht so, dass das Haus brennt und die Feuerwehr nicht kommt.
Wie ist es denn? Entweder brennt das Haus nicht oder das Haus brennt, dann kommt aber die Feuerwehr. Das bedeutet also:
Wenn das Haus brennt, dann kommt die Feuerwehr. Dies führt zu einer neuen Definition.

Definition 7: "Subjunktion" Für " Wenn a, so b" schreibt man $a \to b$.
Pascal: IF a THEN b.
$a \to b := \neg a \vee b$

Wahrheitstafel für Subjunktion:

a	**b**	$\neg a \vee b$	$a \to b$
1	1	1	1
1	0	0	0
0	1	1	1
0	0	1	1

Nebenbei: $a \to b = \neg a \vee b$ ist also eine **Tautologie**.

Beachte: Die Subjunktion $a \to b$ ist also nur dann falsch, wenn a wahr und b falsch ist!

Beispiele:

a := Der Riese ist gross	1
b := Der Mond besteht aus Käse	0
c := 6 ist eine Primzahl	0

a) $a \to b$ = Wenn der Riese gross ist, so besteht der M aus Käse 0
b) $b \to a$ = Wenn der M aus Käse besteht, so ist der Riese gross 1
c) $b \to c$ = Wenn der M aus Käse besteht, so ist 6 eine Primzahl 1
d) $b \to \neg a$ = Wenn der M aus Käse besteht, so ist der R nicht gross 1

Definition 8: "Bijunktion" Für "Genau dann, wenn a, so b" schreibt man $a \leftrightarrow b$.
Definition mit Wahrheitstafel:

a	**b**	**$a \leftrightarrow b$**
1	1	1
1	0	0
0	1	0
0	0	1

Bemerkung: Statt "Genau dann, wenn a, so b" sagt man auch etwa "Dann und nur dann, wenn a, so b"

Beispiele: Aussagen a, b und c definiert wie im vorherigen Beispiel.

$a \leftrightarrow b$ = Genau dann, wenn der R gross ist, besteht der M aus Käse 0

$b \leftrightarrow a$ = Genau dann, wenn der M aus Käse besteht, so ist der R gross 0

$b \leftrightarrow c$ = Genau dann, wenn der M aus Käse besteht, so ist 6 eine Primzahl 1

Aufgabe: Zeige: $a \leftrightarrow b = (a \rightarrow b) \wedge (b \rightarrow a)$ ist Tautologie
Lösung: Aufblatt 2, Nr 7a.

In der formalen Logik wird nur die Form der Verknüpfung studiert, nicht der innere Zusammenhang der Aussage (Gegensatz zur Umgangssprache).
Im Logikkalkül binden $\wedge$ und $\vee$ stärker als $\rightarrow$ und $\leftrightarrow$ (und damit $\neg$ stärker als $\rightarrow$ und $\leftrightarrow$).

Beispiele:
1) $a \rightarrow (\neg a) := a \rightarrow \neg a$
2) $(a \wedge b) \rightarrow (a \vee c) := a \wedge b \rightarrow a \vee c$
3) $[(a \rightarrow b) \wedge (b \rightarrow c)] \rightarrow (a \rightarrow c) := (a \rightarrow b) \wedge (b \rightarrow c) \rightarrow (a \rightarrow c)$

Zu Beispiel 3): Beweise mit Wahrheitstafel und Logikkalkül:
Die Aussage $(a \rightarrow b) \wedge (b \rightarrow c) \rightarrow (a \rightarrow c)$ ist eine Tautologie!

Mit Wahrheitstafel:

					p	q	
a	**b**	**c**	$a \rightarrow b$	$b \rightarrow c$	$(a\rightarrow b) \wedge (b\rightarrow c)$	$a \rightarrow c$	**$p \rightarrow q$**
1	1	1	1	1	1	1	**1**
1	1	0	1	0	0	0	**1**
1	0	1	0	1	0	1	**1**
0	1	1	1	1	1	1	**1**
1	0	0	0	1	0	0	**1**
0	1	0	1	0	0	1	**1**
0	0	1	1	1	1	1	**1**
0	0	0	1	1	1	1	**1**

Mit Logikkalkül: $((\neg a \vee b) \wedge (\neg b \vee c)) \rightarrow (\neg a \vee c) = \neg((\neg a \vee b) \wedge (\neg b \vee c)) \vee (\neg a \vee c)$
$= \neg(\neg a \vee b) \vee \neg(\neg b \vee c) \vee (\neg a \vee c) = (a \wedge \neg b) \vee (b \wedge \neg c) \vee (\neg a \vee c) =$ (Assoz.gesetz für $\vee$)
$= (a \wedge \neg b) \vee ((b \wedge \neg c) \vee c) \vee \neg a = (a \wedge \neg b) \vee ((b \vee c) \wedge (\neg c \vee c)) \vee \neg a =$
$= (a \wedge \neg b) \vee (b \vee c) \vee \neg a = ((a \vee \neg a) \wedge (\neg b \vee \neg a)) \vee (b \vee c) = (\neg b \vee b) \vee \neg a \vee c = e$

B Aussageformen und Mengenlehre

4. Aussageformen

Definition: Eine Aussageform enthält Variabeln. Sie wird durch Einsetzen von Elementen einer vorgegebenen Grundmenge G zu einer (wahren oder falschen) Aussage.

Bezeichnung: a(x), b(x), ... bei einer Variablen
a(x,y), b(x,y), ... bei zwei Variablen
a(x,y,z), ...

Beispiele:
1) a(x) := x ist eine Primzahl G = {1,2, ...,10}
2) b(x,y) := x ist grösser als y G = Menge der Schüler/innen R4b
3) c(heute) := Heute ist Sonntag G = {Mo, Di, ..., So}

Definition: Diejenigen Elemente von G, die die Aussageform zu einer wahren Aussage machen, werden zur Erfüllungsmenge E (für Gleichungen und Ungleichungen: zur Lösungsmenge L) zusammengefasst.

Beispiele:
1) Erfüllungsmenge A von a(x): A = { 2, 3, 5, 7}
2) Erfüllungsmenge B von b(x,y): B = { (.....,.....), (.....,........), ... }
geordnete Paare als Elemente von B.
3) Erfüllungsmenge C von c(heute): C = { So }

5. Verknüpfung von Aussageformen

Aussageformen können wie Aussagen miteinander verknüpft werden.

Beispiele: a(x) := 6 ist durch x teilbar := $x \mid 6$ (x ist Teiler von 6) , G = $\mathbb{N}$
b(x) := $x \mid 16$

Erfüllungsmengen: A = {1, 2, 3, 6}, B = { 1, 2, 4, 8, 16 }

1) $a(x) \wedge b(x) = x \mid 6 \;\wedge\; x \mid 16$ = x ist Teiler von 6 und x ist Teiler von 16
Erfüllungsmenge E = { 1 , 2 } = $A \cap B$

2) $a(x) \vee b(x) = x \mid 6 \;\vee\; x \mid 16$ = x ist Teiler von 6 oder x ist Teiler von 16
Erfüllungsmenge E = { 1, 2, 3, 4, 6, 8, 16 } = $A \cup B$

3) $\neg$ a(x) = 6 ist nicht durch x teilbar
E = {4, 5, 7, 8, 9, ...} = $\mathbb{N} \setminus A = \overline{A}$ (A Komplement)

4) $a(x) \underline{\vee} b(x)$ = Entweder ist 6 durch x oder 16 durch x teilbar
E = {3, 4, 6, 8, 16} = $(A \cup B) \setminus (A \cap B)$

Satz 1: A sei die Erfüllungsmenge der Aussageform a(x), B sei diejenige von b(x). Dann gilt:

a) $A \cap B$ ist Erfüllungsmenge von $a(x) \wedge b(x)$.

b) $A \cup B$ ist Erfüllungsmenge von $a(x) \vee b(x)$.

c) $\overline{A}$ ist Erfüllungsmenge von $\neg a(x)$.

d) $(A \cap \overline{B}) \cup (\overline{A} \cap B) = (A \cup B) \setminus (A \cap B)$ ist Erfüllungsmenge von $a(x) \underline{\vee} b(x)$. (vgl. auch Aufgabenblatt 3, Nr. 3)

Beweis: a) Sei $x_0 \in$ Erfüllungsmenge von $a(x) \wedge b(x)$. Dann ist also $a(x_0) \wedge b(x_0)$ wahr. Also ist sowohl $a(x_0)$ als auch $b(x_0)$ wahr. Daher ist $x_0 \in A$ und $x_0 \in B$, also $x_0 \in A \cap B$.

b) bis d): selber.

Implikation $\Rightarrow$

Beispiel: $a(x) :=$ x ist teilbar durch 6 $= 6 \mid x$, $G = \mathbb{N}$

$b(x) := 3 \mid x$

Die Subjunktion $\rightarrow$ lässt eine neue Aussageform entstehen:

1) $a(x) \rightarrow b(x)$ = Wenn x teilbar durch 6, so ist x teilbar durch 3.

2) $b(x) \rightarrow a(x)$ = Wenn x teilbar durch 3, so ist x teilbar durch 6.

Wir untersuchen nun Beispiele 1) und 2) auf Wahrheitswert (beim Einsetzen von Elementen aus G):

Zu 1):

$x_0 = 12$	$a(12) \rightarrow b(12)$	wahr, da a(12) wahr und b(12) wahr
$x_0 = 3$	$a(3) \rightarrow b(3)$	wahr, da a(3) falsch
$x_0 = 2$	$a(2) \rightarrow b(2)$	wahr, da a(2) falsch

Der Fall $a(x_0)$ wahr und $b(x_0)$ falsch tritt nie ein! Hier ist also $a(x) \rightarrow b(x)$ für alle $x \in G$ wahr. Dieser Sachverhalt wird ausgedrückt durch $a(x) \Rightarrow b(x)$.

Definition: "Implikation" oder "Folgerung"

Aus a(x) folgt b(x), wenn für jede beliebige Einsetzung $x_0 \in G$ gilt:

$a(x_0) \rightarrow b(x_0)$ ist wahr.

Schreibweise: $a(x) \Rightarrow b(x)$

Bemerkung: Statt " aus ..... folgt" sagt man auch etwa "wenn.......dann" oder "wenn........so".

Zu 2):

$x_0 = 12$	$b(12) \rightarrow a(12)$	wahr, da b(12) wahr und a(12) wahr
$x_0 = 3$	$b(3) \rightarrow a(3)$	falsch, da b(3) wahr und a(3) falsch
$x_0 = 2$	$b(2) \rightarrow a(2)$	wahr, da b(2) falsch

Hier darf also das Zeichen $\Rightarrow$ nicht gebraucht werden. Man schreibt dann:

$b(x) \not\Rightarrow a(x)$

Definition: $b(x) \Rightarrow a(x)$ heisst Umkehrung von $a(x) \Rightarrow b(x)$.

In unserem Beispiel gilt also die Umkehrung $b(x) \Rightarrow a(x)$ von $a(x) \Rightarrow b(x)$ **nicht!**

Beispiel: $c(x) :=$ x ist ein Luzerner G = Menge aller Menschen
$d(x) :=$ x ist ein Schweizer

3) Gilt $c(x) \Rightarrow d(x)$?
Ja, denn jeder Luzerner ist ein Schweizer. Alle andern Fälle brauchen nicht beachtet zu werden, da die Subjunktion $0 \rightarrow 1$ bzw. $0 \rightarrow 0$ wahr ist.

4) Behauptung: $d(x) \not\Rightarrow c(x)$
Beweis: x_0 sei Berner. $d(x_0)$ ist wahr, $c(x_0)$ ist falsch, also $1 \rightarrow 0$, also falsch. Also gilt die Behauptung.

Implikation und Lösungsmenge

$a(x) \Rightarrow b(x)$ gilt, falls $a(x_0) \rightarrow b(x_0)$ wahr für alle $x_0 \in G$. Es gibt zwei Fälle:
(1) $a(x_0)$ ist falsch. Dann ist $a(x_0) \rightarrow b(x_0)$ immer wahr.
(2) $a(x_0)$ ist wahr. Dann ist $x_0 \in$ Erfüllungsmenge A von a(x). Damit $a(x_0) \rightarrow b(x_0)$ wahr ist, muss $b(x_0)$ wahr sein, d.h. aber $x_0 \in$ Erfüllungsmenge B von b(x). Also $A \subset B$.

Es gilt also der

Satz 2: A sei Erfüllungsmenge von a(x), B sei Erfüllungsmenge von b(x).
$a(x) \Rightarrow b(x)$ darf genau dann geschrieben werden, falls $A \subset B$ gilt.

Kontrolle bei Beispielen:

1) $A = \{ 6, 12, 18, 24, ...\} = \{x \mid x = 6n \wedge n \in \mathbb{N} \}$
$B = \{ 3, 6, 9, 12, ...\} = \{x \mid x = 3n \wedge n \in \mathbb{N} \}$
$A \subset B$, also $a(x) \Rightarrow b(x)$
2) $B \not\subset A$, also $b(x) \not\Rightarrow a(x)$
3) C = Menge aller Luzerner, D = Menge aller Schweizer
$C \subset D$, also $c(x) \Rightarrow d(x)$.
4) $D \not\subset C$, also $d(x) \not\Rightarrow c(x)$.

Liegt eine Folgerung $a(x) \Rightarrow b(x)$ vor, dann ist b(x) eine notwendige Bedingung für a(x).
(Wenn $a(x_0)$ wahr ist, muss $b(x_0)$ wahr sein).
Umgekehrt ist a(x) eine hinreichende Bedingung für b(x).
(Wenn $a(x_0)$ wahr ist, reicht dies hin, dass $b(x_0)$ wahr ist).
Abgekürzt: "hinreichend" $\Rightarrow$ "notwendig"

Beispiel: 6 ist Teiler von n $\Rightarrow$ 2 ist Teiler von n ($G = \mathbb{N}$)

Mögliche Formulierungen:

(1) Aus 6 ist Teiler von n folgt 2 ist Teiler von n.

(2) Notwendige Bedingung dafür, dass eine natürliche Zahl durch 6 teilbar ist, ist ihre Teilbarkeit durch 2.

(3) Hinreichende Bedingung dafür, dass eine natürliche Zahl durch 2 teilbar ist, ist ihre Teilbarkeit durch 6.

(4) Damit eine natürliche Zahl durch 6 teilbar ist, muss sie notwendigerweise durch 2 teilbar sein.

<u>Aequivalenz</u> $\Leftrightarrow$

<u>Definition:</u> "Aequivalenz"

Genau dann (Dann und nur dann) folgt a(x) aus b(x), wenn für jede Einsetzung $x_0 \in G$ gilt: $a(x_o) \leftrightarrow b(x_0)$ ist wahr.

Zeichen: $a(x) \Leftrightarrow b(x)$

Beispiele:

1) a(x) := x ist teilbar durch 15 b(x):= x ist teilbar durch 3 und 5
   $x_0 = 30$ a(30) wahr, b(30) wahr, also $a(x_o) \leftrightarrow b(x_0)$ wahr.
   $x_0 = 12$ a(12) falsch, b(12) falsch, also $a(x_o) \leftrightarrow b(x_0)$ wahr.

2) $c(x) := x(x+6)=0$ $d(x) := 3x(x+6)=0$

3) e(x,y):= x ist Vater von y f(x,y):= y ist Kind des Mannes x

Lässt man das Zeichen $\Leftrightarrow$ sinngemäss für <u>Aussagen</u>verknüpfungen zu, so stimmt die hier definierte Aequivalenz mit unserer Aequivalenz " = " überein: vgl. auch Aufblatt2, Aufgabe 4. Sind p und q zusammengesetzte Aussagen, so gilt:

$p = q$ ist gleichwertig wie $p \leftrightarrow q$ ist wahr.

$p = q$ ist gleichwertig wie $p \Leftrightarrow q$

<u>Satz3</u>: $(a(x) \Leftrightarrow b(x)) \Leftrightarrow (a(x) \Rightarrow b(x) \wedge b(x) \Rightarrow a(x))$

Beweis: selber (Verwende Aufblatt2, Nr 7a)

Aequivalenz und Lösungsmenge

Satz 4: A sei Erfüllungsmenge von a(x), B sei Erfüllungsmenge von b(x)
$a(x) \Leftrightarrow b(x)$ darf genau dann geschrieben werden, falls A = B.

Beweis: Nach Satz 3 ist $a(x) \Leftrightarrow b(x)$ äquivalent zu $(a(x) \Rightarrow b(x)) \wedge (b(x) \Rightarrow a(x))$
Nach Satz 2 gilt dann: $(A \subset B) \wedge (B \subset A)$. Also ist A = B.

Kontrolle bei Beispiel 1):

$A = \{x \mid x = 15n,\ n \in \mathbb{N}\}$, $B = \{x \mid x = 3m \wedge x = 5l,\quad m, l \in \mathbb{N}\}$

$A \subset B$: $x \in A \Rightarrow x = 15n \Rightarrow x = 3 \cdot 5n \wedge x = 5 \cdot 3n \Rightarrow$ für m:=5n und l:=3n gilt
$x = 3m \wedge x = 5l \Rightarrow x \in B$

$B \subset A$: $x \in B \Rightarrow x = 3m \wedge x = 5l \Rightarrow 3m = 5l \Rightarrow m = \frac{5}{3}l \Rightarrow$ Da $m \in \mathbb{N}$, so muss l die
Form $l = 3n$ mit $n \in \mathbb{N}$ haben $\Rightarrow x = 5 \cdot 3n = 15n \Rightarrow x \in A$

6. Quantoren

Es gibt Sätze, in denen Variabeln auftreten, die aber trotzdem Aussagen sind (denen man also Wahrheitswert 1 oder 0 zuordnen kann)

Beispiele:	Wahrheitswert
1. 1 ist Teiler jeder natürlichen Zahl n	1
2. Für alle x, y aus den rationalen Zahlen $\mathbb{Q}$ gilt: $x + y = y + x$	1
3. Für alle natürlichen Zahlen n und m ist die Summe $n + m = 5$	0
4. 1000 ist grösser als jede natürliche Zahl n	0
5. Es gibt eine rationale Zahl x, die grösser als 5 ist	1
6. Es gibt natürliche Zahlen n und m, so dass $n + m = 5$ ist	1
7. Es gibt eine ganze Zahl x, so dass für alle ganzen Zahlen y die Summe $x + y = y$ ist	1

Beispiele 1 bis 4 enthalten die Worte "für alle", "für jede", .. ., es sind sogenannte **All-Aussagen**. Jede solche Aussage ist die Abkürzung für Aussagen, die mit $\wedge$ verknüpft sind:

Beispiel 1: $(1 \mid 1) \wedge (1 \mid 2) \wedge (1 \mid 3) \wedge \ldots$ $\qquad$ | : ist Teiler von

Beispiel 4: $(1000>1) \wedge (1000>2) \wedge \ldots$

Definition: Eine All-Aussage wird mit dem Zeichen $\forall$ geschrieben ($\forall$: All-Quantor).
Die Variable, auf die sich $\forall$ bezieht, heisst gebundene Variable.

Beispiele: Wahrheitswert

1.	$\forall\, n \in \mathbb{N}:\ 1 \mid n$	1
2.	$\forall\, x, y \in \mathbb{Q}:\ x + y = y + x$	1
3.	$\forall\, n, m \in \mathbb{N}:\ n + m = 5$	0
4.	$\forall\, n \in \mathbb{N}:\ 1000 > n$	0

Es gilt: Ist A die Erfüllungsmenge der Aussageform a(x), so ist die All-Aussage
$\forall\, x \in A: a(x)$ wahr . {gelesen: "für alle x aus A gilt a(x)"

Beispiele 5 bis 7 enthalten die Worte "es gibt", "es existiert", .. ., es sind sogenannte **Existenz-Aussagen**. Jede solche Aussage ist die Abkürzung für Aussagen, die mit $\vee$ verknüpft sind:

Beispiel 5: $0/1 > 5 \ \vee\ 0/2 > 5 \ \vee\ 0/3 > 5 \ \vee \ldots.$
$1/1 > 5 \ \vee\ 1/2 > 5 \ \vee\ 1/3 > 5 \ \vee \ldots.$
.....

Beispiel 7: $\ldots (-3 + y = y) \vee (-2 + y = y) \vee (-1 + y = y) \vee (0 + y = y) \vee (1 + y = y) \vee \ldots$

Definition: Eine Existenz-Aussage wird mit dem Zeichen $\exists$ geschrieben ($\exists$: Existenz-Quantor).
Die Variable, auf die sich $\exists$ bezieht, heisst gebundene Variable.

Beispiele: Wahrheitswert

5.	$\exists\, x \in \mathbb{Q}:\ x > 5$	1
6.	$\exists\, n \in \mathbb{N},\ \exists\, m \in \mathbb{N}:\ n + m = 5$	1
7.	$\exists\, x \in \mathbb{Z},\ \forall\, y \in \mathbb{Z}:\ x + y = y$	1

Es gilt: Entsteht aus der Aussageform a(x) für mindestens ein Element $x_0 \in G$ (G: Grundmenge) eine wahre Aussage, so ist die Existenzaussage $\exists\, x \in G: a(x)$ wahr .

Gesetze für Quantoren

Beispiele:

	Wahrheitswert		Wahrheitswert
8. $\forall\, n \in \mathbb{N}, \forall\, x \in \mathbb{Q}:\ n + x = x + n$	1	12. $\exists\, n \in \mathbb{N}, \exists\, x \in \mathbb{Z}:\ n + x = 10$	1
9. $\forall\, x \in \mathbb{Q}, \forall\, n \in \mathbb{N}:\ n + x = x + n$	1	13. $\exists\, x \in \mathbb{Z}, \exists\, n \in \mathbb{N}:\ n + x = 10$	1
10. $\forall\, n \in \mathbb{N}, \forall\, x \in \mathbb{Z}:\ x > n$	0	14. $\exists\, x \in \mathbb{Z}, \exists\, y \in \mathbb{Q}:\ x + y < y + x$	0
11. $\forall\, x \in \mathbb{Z}, \forall\, n \in \mathbb{N}:\ x > n$	0	15. $\exists\, y \in \mathbb{Q}, \exists\, x \in \mathbb{Z}:\ x + y < y + x$	0
7. $\exists\, x \in \mathbb{Z},\ \forall\, y \in \mathbb{Z}:\ x + y = y$	1 (x=0)	7'. $\forall\, y \in \mathbb{Z},\ \exists\, x \in \mathbb{Z}:\ x + y = y$	1 (x_1=0,...)
16. $\forall\, n \in \mathbb{N}, \exists\, x \in \mathbb{Z}:\ n + x = 10$	1	17. $\exists\, x \in \mathbb{Z}, \forall\, n \in \mathbb{N}:\ n + x = 10$	0

Es gilt: (nach Assoziativgesetz und Kommutativgesetz von $\wedge$ und $\vee$)

Gleiche Quantoren vor einer Aussageform dürfen vertauscht werden!
Verschiedene Quantoren vor einer Aussageform dürfen nicht immer vertauscht werden!

	Aussagenlogik	Mengenalgebra	Algebra (z.B. M=$\mathbb{Z}$)
Elemente von M	Aussagen a,b,c...	Mengen A,B,C, ...	Zahlen a,b,c, ...
Verknüpfungen $*_1$	Konjunktion $\wedge$	Durchschnitt $\cap$	Multiplikation $\cdot$
$*_2$	Adjunktion $\vee$	Vereinigung $\cup$	Addition $+$
	Negation $\neg$	Komplement $\overline{}$	
Abgeschlossenheit	$a \wedge b \in M$ $a \vee b \in M$	$A \cap B \in M$ $A \cup B \in M$	$a \cdot b \in M$ $a + b \in M$
Kommutativ (K)	$a \wedge b = b \wedge a$ $a \vee b = b \vee a$	$A \cap B = B \cap A$ $A \cup B = B \cup A$	$a \cdot b = b \cdot a$ $a + b = b + a$
Assoziativ (A)	$(a\wedge b)\wedge c=a\wedge(b\wedge c)$ $(a\vee b)\vee c=a\vee(b\vee c)$	$(A\cap B)\cap C=A\cap(B\cap C)$ $(A\cup B)\cup C=A\cup(B\cup C)$	$(a\cdot b)\cdot c=a\cdot(b\cdot c)$ $a+b)+c=a+(b+c)$
Absorption (Ab)	$a \wedge (a \vee b) = a$ $a \vee (a \wedge b) = a$	$A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$	
Distributiv (D)	$a\wedge(b\vee c) = (a\wedge b)\vee(a\wedge c)$ $a\vee(b\wedge c) = (a\vee b)\wedge(a\vee c)$	$A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$ $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$	$a\cdot(b+c)=a\cdot b+ a\cdot c$
De Morgan (M)	$\neg(a\wedge b) = \neg a \vee \neg b$ $\neg(a\vee b) = \neg a \wedge \neg b$	$\overline{A\cap B}=\overline{A}\cup\overline{B}$ $\overline{A\cup B}=\overline{A}\cap\overline{B}$	
Neutrales Element bez. * (N)	bez. $\wedge$: Tautologie $a \wedge e = e \wedge a = a$ bez: $\vee$: Kontradikt. $a \vee n = n \vee a = a$	bez. $\cap$: Grundm. $A\cap G = G\cap A = A$ bez. $\cup$: Leere M. $A\cup\{\ \}=\{\ \}\cup A = A$	bez. $\cdot$: Zahl 1 $a \cdot 1 = 1 \cdot a = a$ bez. + : Zahl 0 $a + 0 = 0 + a = a$
Inverse Elemente (In) a^{-1} zu a			bez. $\cdot$: ex. nicht bez: + : (-a) $a+(-a)=(-a)+a= 0$

Definition

1. Falls in M für $*_1$ und $*_2$ Abg. , (K), (A) und (Ab) gelten, so ist < M; $*_1$, $*_2$ > ein **Verband**.
   Falls zusätzlich noch (D) gilt, so ist < M; $*_1$, $*_2$ > ein **distributiver Verband**.
2. Falls in M für * Abgeschlossenheit, (A), (N) und (In) gelten, so ist < M; * > eine **Gruppe**. Falls zusätzlich noch (K) gilt, so ist < M; * > eine **kommutative Gruppe**.

C DER BEWEIS

8. Definitionen und Beweisregeln

Definition: Ein Beweis ist eine *Folge von wahren Aussagen*. Jede Aussage geht nach bestimmten *Regeln* entweder direkt oder aus vorausgehenden Aussagen hervor.

<u>Beweisregeln</u>

1. Ein *Axiom* darf hingeschrieben werden.
   Axiom: Mathematischer Grundsatz, der als *wahr vorausgesetzt* wird. Axiome stehen zu Beginn jeder mathematischen Theorie, z.B.
   - Eine Gerade ist durch zwei Punkte bestimmt.
   - Eine Ebene ist durch drei nicht auf einer Geraden liegenden Punkte bestimmt.

2. Eine *Tautologie* (mit Aussagenvariabeln a, b, c, ...) darf hingeschrieben werden.

3. In einer Tautologie dürfen die Aussagenvariabeln a, b, c, ... durch beliebige Aussagen ersetzt werden.

4. Kommt $a \leftrightarrow b$ in einem Beweis vor, so darf a durch b ersetzt werden.

5. *Abtrennungsregel* (Modus ponens: vgl. Aufgabenblatt 2, Nr. 7c)
   Sind in einem Beweis a und $a \rightarrow b$ vorhanden, so darf man zu b übergehen.

   Schreibweise: $$\frac{\begin{array}{l} a \\ a \rightarrow b \end{array}}{b}$$

6. Regeln zur *Konjunktion*: $$\frac{\begin{array}{l} a \\ b \end{array}}{a \wedge b} \qquad \frac{a \wedge b}{a}$$

7. *Kontraposition* (vgl. Aufgabenblatt 2, Nr. 7b)
   $$\frac{a \rightarrow b}{\neg b \rightarrow \neg a}$$ (vgl. indirekter Beweis, Kapitel 9)

8. Regeln für die *Quantoren*

$$\frac{\neg \forall x \in M\colon a(x)}{\exists x \in M\colon \neg a(x)} \qquad \frac{\forall x \in M\colon a(x)}{a(x_0)} \qquad \frac{\exists x \in M\colon a(x)}{a(x_0)} \qquad \frac{a(x_0)}{\exists x \in M\colon a(x)}$$

$x_0 \in M$ beliebig (zweite Regel); $x_0 \in M$ fest (dritte Regel)

9. Beweisverfahren

Die meisten mathematischen Sätze können als Implikation $a \Rightarrow b$ aufgefasst werden. Selten wird aber diese Folgerung in <u>einem</u> Schritt bewiesen.

a) Der direkte Beweis

Es gilt: (vgl. Beispiel 3), p.6) $(a \to c) \wedge (c \to b) \to (a \to b)$ ist eine Tautologie. Also ist die Schreibweise $(a \to b) \wedge (b \to c) \Rightarrow (a \to c)$ korrekt. Ist also die linke Seite wahr, so auch die rechte:

$$\begin{array}{l} a \to c \\ c \to b \\ \hline a \to b \end{array}$$

<u>Beispiel</u>: Voraussetzung a: n ist eine gerade ganze Zahl
Behauptung b: n^2 ist eine gerade ganze Zahl
Zu zeigen: $a \Rightarrow b$ (es gilt sogar: $a \Leftrightarrow b$)

Beweis: $a \Leftrightarrow c1{:}\ \exists\, k \in \mathbb{Z}{:}\ n = 2k \Leftrightarrow c2{:}\ \exists\, k \in \mathbb{Z}{:}\ n^2 = 4k^2 \Leftrightarrow c3{:}\ \exists\, k \in \mathbb{Z}{:}\ n^2 = 2(2k^2)$
$\Leftrightarrow c4{:}\ \exists\, m \in \mathbb{Z}{:}\ n^2 = 2m$ (denn $m := 2k^2$) $\Leftrightarrow b$

b) Widerlegung durch Gegenbeispiel

Aus den Regeln für Quantoren folgt: Eine Aussageform a(x) ist dann als nicht allgemeingültig über der Grundmenge G erkannt, wenn es $x_0 \in G$ gibt, so dass $a(x_0)$ falsch ist.

<u>Beispiel</u>: a(x): x ist ungerade Primzahl, G: Menge aller Primzahlen
Behauptung: $\forall\, x \in G{:}\ a(x)$

Die Behauptung ist falsch, denn für $x_0 = 2$ ist a(2) falsch.

c) Beweis indirekt (Beweis durch Gegenannahme)

Es soll $a \Rightarrow b$ bewiesen werden.

1. Art:
$$\begin{array}{l} a \\ \neg b \to a \wedge \neg a \\ \hline b \end{array}$$

2. Art:
$$\begin{array}{l} \neg b \wedge a \\ c \wedge \neg c \\ \hline b \end{array}$$

Beispiel 1: Voraussetzung a: Summe der Innenwinkel beim Dreieck ist 180°
Behauptung b: Es gibt kein Dreieck, das mehr als einen stumpfen Winkel besitzt.
Beweis: Gegenannahme $\neg b$: Dreieck hat z.B. zwei stumpfe Winkel
Dann ist die Winkelsumme > 180°, also $a \wedge \neg a$ (Kontradiktion)
Also gilt die Behauptung b.

Beispiel 2: Es gibt keine rationale Zahl, deren Quadrat 2 ist.

Voraussetzung $a(x)$: $x^2 = 2$, Behauptung $b(x)$: $x \notin \mathbb{Q}$ $(G = \mathbb{Q})$
Beweis(s. bereits in Klasse 3): Gegenannahme $\neg$ b: $x \in \mathbb{Q}$
c: $x = \frac{p}{q} \wedge p \in \mathbb{N} \wedge q \in \mathbb{N} \wedge \text{ggT}(p,q)=1$ (d.h. Bruch ist vollständig gekürzt)
$\Rightarrow x^2 = 2 \wedge x^2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2 \Rightarrow p^2$ ist gerade $\Rightarrow$ <u>p ist gerade</u>
$\Rightarrow p = 2m \ (m \in \mathbb{N}) \Rightarrow p^2 = 4m^2 = 2q^2 \Rightarrow q^2 = 2m^2 \Rightarrow q^2$ ist gerade
$\Rightarrow$ <u>q ist gerade</u> $\Rightarrow \neg$ c: p und q haben Teiler 2, also Kontradiktion
Also gilt die Behauptung b.

d) Beweis mit vollständiger Induktion über $\mathbb{N}$

Induktion: Schluss vom Speziellen auf das Allgemeine
Dieser Beweis bedarf der Axiome von Peano, die die natürliche Zahlenmenge begründen (s. auf der Website mathematik.ch)

Satz: $a(n)$ sei eine Aussageform über $G = \mathbb{N}$:

I	$a(1)$	'Verankerung'
II	$\forall k \in \mathbb{N}: a(k) \rightarrow a(k+1)$	'Induktionsschluss'
	$\forall n \in \mathbb{N}: a(n)$	

Beispiel 1: Behauptung: $\forall n \in \mathbb{N}$: $8 \mid 9^n - 1$ (d.h. $a(n) = 9^n - 1$ ist teilbar durch 8) (*)

Beweis mit vollständiger Induktion:

I Verankerung: (*) gilt für n=1: $8 \mid 9 - 1$ ist wahr
II Induktionsschluss: Es genügt, a(k) für beliebiges k als wahr <u>vorauszusetzen</u> und zu zeigen, dass dann auch a(k+1) wahr ist.
Induktionsvoraussetzung: (*) gelte für n=k, d.h. $8 \mid 9^k - 1$
zu zeigen: Dann gilt (*) auch für n=k+1, d.h. $8 \mid 9^{k+1} - 1$
in der Tat: $9^{k+1} - 1 = (9^k - 1) \cdot 9 + 9 - 1$
$(9^k - 1)$ ist nach Vor. durch 8 teilbar, also ist auch $(9^k - 1) \cdot 9$ durch 8 teilbar; da auch 9-1 durch 8 teilbar, so ist der ganze rechte Teil durch 8 teilbar
Also gilt $\forall k \in \mathbb{N}: a(k) \rightarrow a(k+1)$

Aus I $\wedge$ II folgt die Behauptung.