Formale Grundlagen

Franz Binder
Institut für Algebra
Johannes Kepler Universität Linz

16. März 2010, Entwurf

1 Aussagenlogik

Aussagen

1.1 Definition. Um eine *Aussage* zu konstruieren muß festgelegt werden,

- was zu tun ist, um einen *Beweis* der Aussage zu konstruieren.

1.2 Notation. Ist A eine Aussage und a eine Beweis von A, so schreiben wir $a : A$ oder $a \in A$.

Implikation

Die grundlegendste Beziehung zwischen Aussagen ist die logische Implikation.

1.3 Definition. A und B seien Aussagen. Dann ist auch $(A \implies B)$ eine Aussage, die logische *Implikation*. Ein Beweis von $(A \implies B)$ ist eine Konstruktion, die jeden Beweis von A in einen Beweis von B transferiert, d.h.

1. Kann man unter der Voraussetzung, daß a ein Beweis von A ist, einen Beweis b von B (in dem a verwendet werden darf) konstruieren, so ist die Konstruktion $a \mapsto b$ ein Beweis von $(A \implies B)$. (*Introduktionsregel*)

2. Ist f ein Beweis von $(A \implies B)$, und ist a ein Beweis von A, so kann man f auf a *anwenden*, und $f(a)$ ist ein Beweis von B. (*Eliminationsregel*)

Die Beweise von Implikationen nennt man daher auch *Funktionen*, und man schreibt $f : A \implies B$, wenn f ein Beweis der Implikation $(A \implies B)$ ist.

1.4 Definition. Ist $f : A \implies B$ und $g : B \implies C$, dann definieren wir die *Hintereinanderausführung von g nach f* durch

$$g \circ f := (a \mapsto g(f(a))).$$

Somit ist dann $g \circ f : A \implies C$.

1.5 Bemerkung. Die obige Definition hätten wir auch durch

$$(g \circ f)(a) := g(f(a))$$

ausdrücken können.

1.6 Definition. Eine Aussage der Form $(A \implies A)$ hat immer den Beweis $(a \mapsto a)$, der mit id_A bezeichnet sei, also

$$\mathrm{id}_A(a) := a.$$

Äquivalente Aussagen

1.7 Definition. Um zu beweisen daß zwei Aussagen A und B *äquivalent* sind $(A \iff B)$, muß man sowohl $A \implies B$ als auch $B \implies A$ beweisen.

Ist also $f : A \implies B$ und $g : B \implies A$, dann ist $(f, g) : A \iff B$.

1.8 Satz. *Die logische Äquivalenz erfüllt die folgenden Bedingungen für beliebige Aussagen A, B, C:*

1. $A \iff A$.
2. $(A \iff B) \implies (B \iff A)$.
3. $(A \iff B) \wedge (B \iff C) \implies (A \iff C)$.

Beweis. 1. $\mathrm{id}_A : A \implies A$, und damit $(\mathrm{id}_A, \mathrm{id}_A) : A \iff A$.

2. Wenn $(f, g) : A \iff B$, dann ist $(g, f) : B \iff A$.

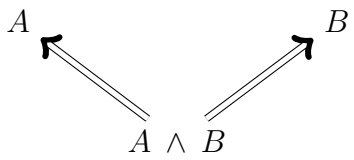
3. Ist $(f, f') : A \iff B$ und $(g, g') : B \iff C$, dann ist $(g \circ f, f' \circ g') : A \iff C$.

□

Konjunktion

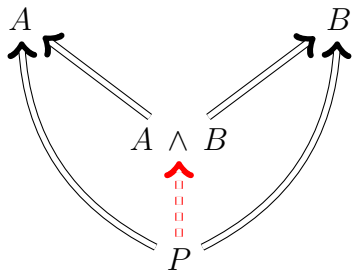
1.9 Definition. Sind A und B Aussagen, dann ist auch deren *Konjunktion* $A \wedge B$ eine Aussage. Um $A \wedge B$ zu beweisen muß man sowohl A als auch B beweisen. Ist also a ein Beweis von A und b ein Beweis von B, dann ist das *Paar* (a, b) ein Beweis von $A \wedge B$.

1.10 Satz. *Ist (a, b) ein Beweis von $A \wedge B$, dann ist a ein Beweis von A. Somit ist die Funktion $(a, b) \mapsto a$ ein Beweis von $A \wedge B \implies A$. Analogerweise ist $(a, b) \mapsto b$ ein Beweis von $A \wedge B \implies B$. Dies läßt sich durch das folgenden Diagramm veranschaulichen:*



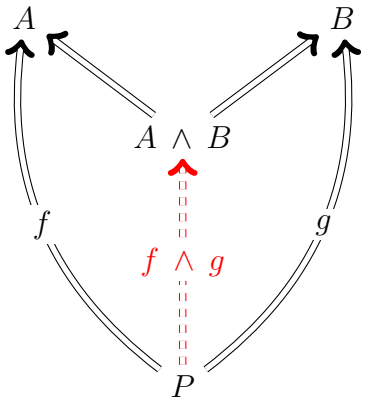
Ist eine Aussage P stärker als $A \wedge B$, dann ist P klarerweise auch stärker als A, und ebenso auch stärker als B. Es gilt aber auch die Umkehrung: Ist P irgendeine Aussage,

welche stärker als A und stärker als B ist, dann ist P auch stärker als $A \wedge B$, was wir durch das folgende Diagramm veranschaulichen:



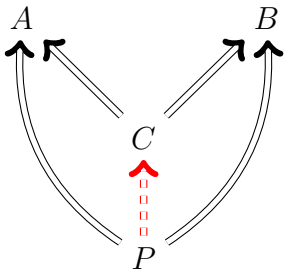
Beweis. Unter den Voraussetzungen $P \implies A$ und $P \implies B$ ist zu zeigen: $P \implies A \wedge B$.
Wir nehmen also P an, und haben $A \wedge B$ zu zeigen.
Dazu sind in diesem Kontext sowohl A als auch B zu zeigen.
Da wir P angenommen haben, folgt A ganz einfach aus $P \implies A$.
Und genauso folgt B aus $P \implies B$. Damit ist alles gezeigt.

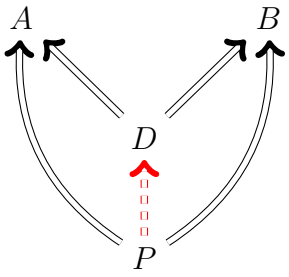
Wir können dies auch etwas konkreter formulieren: Seien $f : P \implies A$ und $g : P \implies B$. Ist dann $p \in P$, dann ist $f(p) \in A$ und $g(p) \in B$. Somit ist die Funktion $f \wedge g$, definiert durch $p \mapsto (f(p), g(p))$, ein Beweis von $P \implies A \wedge B$. Wir veranschaulichen auch dies durch ein Diagramm:



□

1.11 Satz. *C und D seien beide Aussagen, welche die Eigenschaft haben, daß sie stärker als die Aussagen A und B sind, und auch, daß sie schwächer sind als jede weitere Aussage P, welche stärker als die A und B ist. Das heißt, für alle Aussagen P haben wir die Diagramme:*



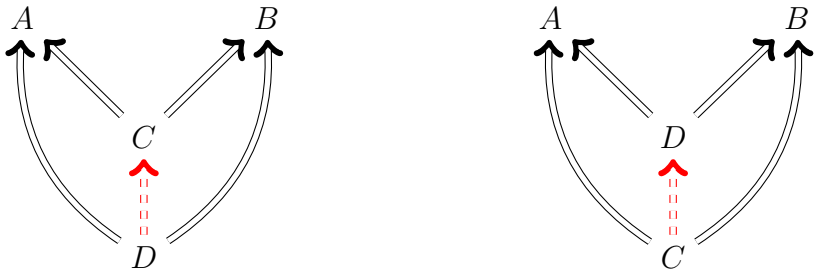


Dann gilt:

$$C \iff D.$$

Somit ist $A \wedge B$ bis auf Äquivalenz die einzige Aussage, welche die besagte Eigenschaft hat.

Beweis. Im Diagramm für C setzen wir stat P die Aussage D ein, und analog im Diagramm für D die Aussage C. Wir erhalten somit:

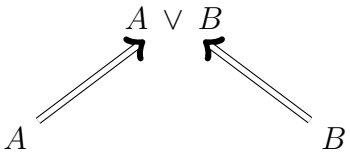


Daraus erkennen wird sofort, daß $C \iff D$. □

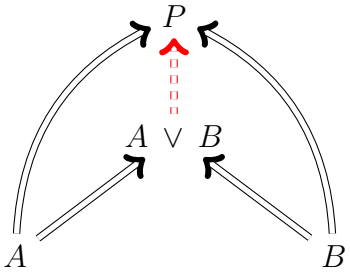
Disjunktion

1.12 Definition. Sind A und B Aussagen, dann ist auch deren *Disjunktion* $A \vee B$ eine Aussage. Um $A \vee B$ zu beweisen, reicht es, wenn A bewiesen wird, und auch, wenn B bewiesen wird. Ist also a ein Beweis von A, dann ist a im wesentlichen auch schon ein Beweis von $A \vee B$, er muß nur noch als solcher gekennzeichnet werden, z.B. als Left a. Ähnliches gilt, wenn b ein Beweis von B ist: dann sei Right b ein Beweis von $A \vee B$.

1.13 Satz. *Ist a ein Beweis von A, dann ist* Left a *ein Beweis von $A \vee B$. Somit ist die Funktion $a \mapsto$* Left a *ein Beweis von $A \implies A \vee B$. Analogerweise ist $b \mapsto$* Right b *ein Beweis von $B \implies A \vee B$. Dies läßt sich durch das folgenden Diagramm veranschaulichen:*



Ist eine Aussage P schwächer als $A \vee B$, dann ist P klarerweise auch schwächer als A, und ebenso auch schwächer als B. Es gilt aber auch die Umkehrung: Ist P irgendeine Aussage, welche schwächer als A und schwächer als B ist, dann ist P auch schwächer als $A \vee B$, was wir durch das folgende Diagramm veranschaulichen:



Beweis. Unter den Voraussetzungen $A \implies P$ und $B \implies P$ ist zu zeigen: $A \vee B \implies P$.
Wir nehmen also $A \vee B$ an, und haben P zu zeigen.
Dazu führen wir eine Fallunterscheidung durch.

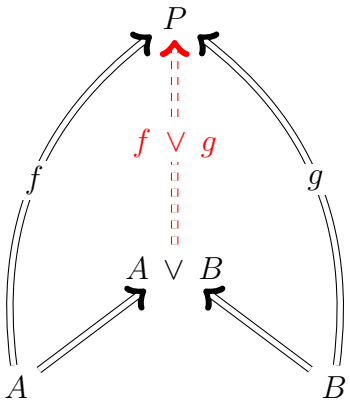
Gilt die Aussage A, dann können wir $A \implies P$ verwenden, und erhalten somit sofort P.

Gilt die Aussage B, dann können wir $B \implies P$ verwenden, und erhalten ebenfalls sofort P. Damit ist alles gezeigt.

Wir können dies auch etwas konkreter formulieren: Seien $f : A \implies P$ und $g : B \implies P$. Ein Beweis von $A \vee B$ hat die Form Left a oder Right b, mit $a \in A$ bzw. $b \in B$. Wir definieren somit die Funktion $f \vee g : A \vee B \to P$ durch

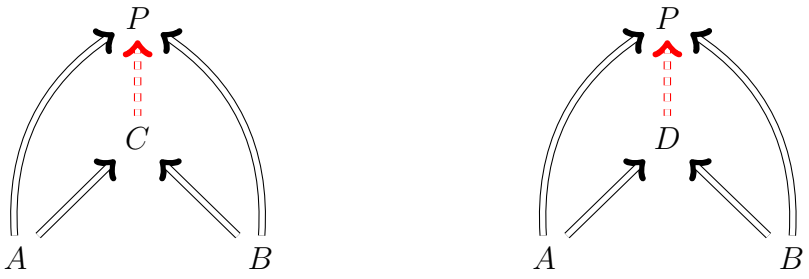
$$\begin{aligned} \text{Left}\, a &\mapsto f(a) \\ \text{Right}\, b &\mapsto g(b) \end{aligned}$$

Wir veranschaulichen auch dies durch ein Diagramm:



□

1.14 Satz. *C und D seien beide Aussagen, welche die Eigenschaft haben, daß sie stärker als die Aussagen A und B sind, und auch, daß sie schwächer sind als jede weitere Aussage P, welche stärker als die A und B ist. Das heißt, für alle Aussagen P haben wir die Diagramme:*

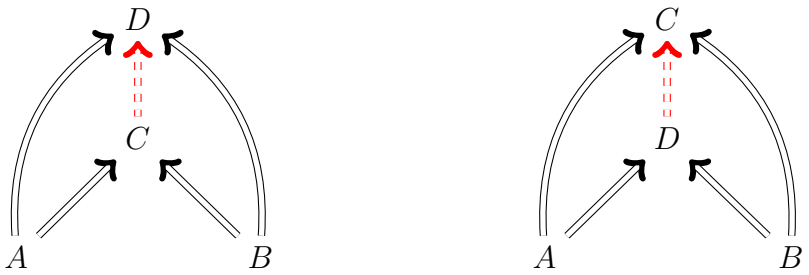


Dann gilt:

$$C \iff D.$$

Somit ist $A \vee B$ bis auf Äquivalenz die einzige Aussage, welche die besagte Eigenschaft hat.

Beweis. Im Diagramm für C setzen wir stat P die Aussage D ein, und analog im Diagramm für D die Aussage C. Wir erhalten somit:



Daraus erkennen wird sofort, daß $C \iff D$. □

2 Mengen

2.1 Definition. Um eine *Menge* zu konstruieren muß festgelegt werden,

1. was zu tun ist, um ein *Element* der Menge zu konstruieren;
2. was es bedeutet, daß zwei Elemente der Menge *gleich* sind;
3. daß dieser Gleichheitsbegriff die Axiome einer Äquivalenzrelation erfüllt.

2.2 Bemerkung. Der erste Teil dieser Definition entspricht exakt der Definition des Begriffs der Aussage. Damit können alle Konstruktionen, die wir für Aussagen kennengelernt haben, auch auf Mengen angewandt werden.

Im Gegensatz zu den Beweisen einer Aussage, sollten die Elemente der Menge jedoch wohlunterscheidbar sein. Daher wird im zweiten Punkt verlangt, daß je zwei Elementen eine Aussage zugeordnet wird, welche dann bedeutet, daß diese beiden Elemente tatsächlich gleich sind. Diese zusätzliche Struktur verleiht vielen Konstruktionen einen deutliche differenzierteren Inhalt.

Dabei kann man aber nicht jede Beziehung zwischen den Elementen als Gleichheitsbegriff verwenden: z.B. sollte jedes Element zu sich selbst gleich sein. Außerdem sollte diese Beziehung symmetrisch sein. Und man sollte Gleichheitsketten bilden können. Diese drei Eigenschaften des Gleichheitsbegriff werden durch die Axiome einer Äquivalenzreltion ausgedrückt:

$$x = x \qquad (\textit{Reflexivität})$$
$$x = y \implies y = x \qquad (\textit{Symmetrie})$$
$$x = y \wedge y = z \implies x = z \qquad (\textit{Transitivität})$$

2.3 Bemerkung. Im einfachsten Fall muß man nicht unterscheiden, ob zwei Elemente wirklich exakt dieselben sind, oder ob sie nur gleich sind. Aber bereits bei den rationalen Zahlen stellt man z.B. fest, daß $\frac{4}{6} = \frac{6}{9}$ ist, obwohl die beiden Brüche verschieden aussehen. Es bedarf doch zumindest einiger Überlegungen, daß die übliche Definition der Gleichheit von rationaler Zahlen tatsächlich zu einer Äquivalenzrelation führt, bzw. daß man sich auf vollständig gekürzte Brüche beschränken kann. In anderen Fällen, z.B. der Menge der reellen Zahlen, Mengen von Funktionen oder von Aussagen, gibt es auch theoretisch nicht die Möglichkeit, eine eindeutige Darstellung zu berechnen.

Abbildungen

2.4 Definition. Sind A und B Mengen, dann heißt eine Funktion $f : A \to B$ *wohldefiniert*, wenn gilt:

$$\underset{\substack{a\epsilon A\\ a'\epsilon A}}{\forall} a = a' \implies f(a) = f(a').$$

Zur einfacheren Unterscheidung nennen wir solche Funktionen auch *Abbildungen*.

2.5 Bemerkung. Probleme mit der Wohldefiniertheit einer Funktion $f : A \to B$ ergeben sich typischerweise nur dann, wenn Elemente von A nicht eindeutig dargestellt werden, z.B. bei einer Darstellung der rationalen Zahlen als (nicht notwendigerweise gekürzter Bruch) könnte man eine Funktion $\frac{p}{q} \mapsto p$ definieren, welche jeder rationalen Zahl, den Zähler zuordnet. Dann hätten beispielsweise $\frac{4}{6}$ und $\frac{6}{9}$ verschiedene Zähler, obwohl sie gleich sind.

Bei den rationalen Zahlen läßt sich das Problem umgehen, indem man immer den Zähler der gekürzten Variante betrachtet. In allgemeineren Fällen (bei Mengen ohne eindeutige Darstellungsmöglichkeit) läßt sich dies jedoch oft nicht erreichen. So läßt sich, abgesehen von der konstanten Abbildung, z.B. keine wohldefinierte Abbildung konstruieren, die jeder Aussage eine Zahl zuordnet.

Ähnliches gilt für die reellen Zahlen. Man kann zeigen, daß jede wohldefinierte Abbildung $\mathbb{R} \to \mathbb{N}$, die man auch tatsächlich berechnen kann, konstant sein muß. Insbesondere ist es daher unmöglich eine Abbildung $b : \mathbb{R} \to \mathbb{N}$ zu programmieren, sodaß $b(x) \geq x$. Es ist allerdings kein Problem, eine nicht-wohldefinierte Funktion mit dieser Eigenschaft zu konstruieren. Diese muß aber ganz wesentlich auf eine spezielle Darstellung einer reellen Zahl Bezug nehmen, und es läßt sich dabei nicht vermeiden, daß es mitunter passiert, daß $b(x) \neq b(y)$, obwohl $x = y$.

2.6 Definition. Seien A und B Mengen. Dann kann man die Menge aller Abbildungen von A nach B betrachten, wobei zwei Abbildungen als gleich gelten sollten, wenn sie stets dieselben Funktionswerte liefern, d.h., sind $f : A \to B$ und $g : A \to B$ zwei Abbildungen, dann definiert man

$$f = g : \iff \underset{a\epsilon A}{\forall} f(a) = g(a).$$

2.7 Satz. *Der Gleichheitsbegriff für Abbildungen von A nach B erfüllt tatsächlich die Axiome für eine Äquivalenzrelation, d.h., seien $f, g, h : A \to B$, dann gelten:*

1. $f = f$.
2. $f = g \implies g = f$.
3. $f = g \wedge g = h \implies f = h$.

Beweis. Jede dieser Bedingungen folgt direkt aus der entsprechenden Bedingung für die Gleichheit in B. □

2.8 Satz. *Sind $f : A \to B$ und $g : B \to C$ Abbildungen, dann ist auch die Hintereinanderausführung $g \circ f : A \to C$ wohldefiniert, und auch assoziativ, d.h., wenn $h : C \to D$ eine weitere Abbildung ist, dann gilt:*

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

2.9 Satz. *Die Hintereinanderausführung von Abbildungen ist auc selbst eine wohldefinierte Abbildung* $\circ : (A \to B) \to (B \to C) \to (A \to C)$. *D.h., sind* $f, f' : A \to B$ *und* $g, g' : B \to C$, *dann gilt*

$$f = f' \wedge g = g' \implies g \circ f = g' \circ f'.$$

Man kann daher auch einfach die Klammern weglassen und $h \circ g \circ f$ schreiben, ohne daß es zu Mehrdeutigkeiten kommen kann.

2.10 Satz. *Für jede Menge* A *ist die Identität* $\mathrm{id}_A : A \to A$ *eine wohldefinierte Abbildung von* A *in sich, und es gilt für alle Mengen* B *und alle Abbildungen* $f : A \to B$ *und* $g : B \to A$*:*

$$f \circ \mathrm{id}_A = f \qquad \textit{und} \qquad \mathrm{id}_A \circ g = g \tag{1}$$

Insbesondere enthält die Menge A^A somit immer ein Element.
Tatsächlich ist die Identität die einzige Abbildung, welche (1) erfüllt.

2.11 Satz. *Sei* $i : A \to A$ *sodaß*

$$\bigwedge_{f:A\to A} f \circ i = f = i \circ f,$$

dann ist $i = \mathrm{id}_A$.

2.12 Definition. Seien $f : A \to B$ und $g : B \to A$ Abbildungen. Dann ist jedenfalls

$$g \circ f : A \to A \qquad \text{und} \qquad f \circ g : B \to B,$$

welche jedoch im allgemeinen nicht mit den Identitäten id_A bzw. id_B des passenden Typs übereinstimmen müssen. Gelten jedoch

$$g \circ f = \mathrm{id}_A \qquad \text{und} \qquad f \circ g = \mathrm{id}_B,$$

dann heißt (f, g) ein Paar *zueinander inverser Abbildungen.*

2.13 Definition. Zwei Mengen A und B heißen *gleichmächtig* wenn es ein Paar (f_1, f_2) zueinander inverser Abbildungen mit $f_1 : A \to B$ und $f_2 : B \to A$ gibt. Wir schreiben dann $A \sim B$.

2.14 Satz. *Die Gleichmächtigkeit von Mengen erfüllt die Axiome einer Äquivalenzrelation, d.h., für alle Mengen* A, B, C *gilt:*

1. $A \sim A$;
2. $A \sim B \implies B \sim A$;
3. $A \sim B \wedge B \sim C \implies A \sim C$.

Beweis. 1. Für jede Menge A ist $(\mathrm{id}_A, \mathrm{id}_A)$ ein Paar zueinander inverser Abbildungen.

2. Sind $f : A \to B$ und $g : B \to A$, und ist (f, g) ist ein Paar zueinander inverser Abbildungen, dann auch (g, f).

3. Sind $f_1 : A \to B$, $f_2 : B \to A$, $g_1 : B \to C$, $g_2 : C \to B$, und sind (f_1, f_2) und (g_1, g_2) Paare zueinander inverser Abbildungen, dann sind $g_1 \circ f_1 : A \to C$ und $f_2 \circ g_2 : C \to A$, und man rechnet leicht nach, daß auch $(g_1 \circ f_1, f_2 \circ g_2)$ ein Paar zueinander inverser Abbildungen ist.

□

2.15 Satz. *Sind (f, g) und (f, g') zwei Paare zueinander inverser Abbildungen, dann ist $g = g'$.*

Beweis. Es seien $f : A \to B$, $g : B \to A$, $g' : B \to A$, $g \circ f = \mathrm{id}_A$, $f \circ g = \mathrm{id}_B$, $g' \circ f = \mathrm{id}_A$ und $f \circ g' = \mathrm{id}_B$. Dann erhalten wir

$$\begin{aligned} g &= g \circ id_B \\ &= g \circ (f \circ g') \\ &= (g \circ f) \circ g' \\ &= \mathrm{id}_B \circ g' \\ &= g'. \end{aligned}$$

□

2.16 Definition. Eine Abbildung $f : A \to B$ heißt *invertierbar* wenn es eine eine Abbildung $g : B \to A$ gibt, sodaß (f, g) ein Paar zueinander inverser Abbildungen ist. Die dadurch eindeutig bestimmte Abbildung g heißt dann das *Inverse* von f und wird mit f^{-1} bezeichnet. Es gilt somit

$$f^{-1} \circ f = \mathrm{id}_A \ \wedge \ f \circ f^{-1} = \mathrm{id}_B \,.$$

2.17 Satz. *A, B, C seien Mengen, und $f : A \to B$, $g : B \to C$ invertierbare Abbildungen. Dann gilt:*

1. $\mathrm{id}_A^{-1} = \mathrm{id}_A$;
2. $(f^{-1})^{-1} = f$;
3. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.