Mathematik Begabtenkurs JWG März 2017

Maximilian Starke

18. März 2017

Teil I

Aussagenlogik in der Mathematik

1 Aussagen

Definition 1.1 Eine Aussage ist ein wohldefinierter mathematischer Ausdruck, der entweder 1 (= wahr, true) oder 0 (= falsch, false) ist. Formal handelt es sich um einen verketteten Funktionsaufruf von endlicher Tiefe.

Beispiel 1.2 1 ist eine wahre Aussage. 0 ist eine falsche Aussage. Die Tiefe des verketteten Funktionsaufrufes ist jeweils *null*. Auch $(5 \mid 21) = wahr$ ist eine (zugegebenermaßen *falsche*) Aussage. Hier beträgt die Tiefe *zwei*, da auf oberster Ebene eine Gleichheit behauptet wird und auf der linken Seite auf nächst tieferer Ebene eine Teilerbeziehung (5 teilt 21). $5 \mid 21$ ist bekanntlich falsch, $falsch = wahr$ und damit die gesamte Aussage ist folglich auch falsch.

(a) 7 ist eine Primzahl.

(b) 2 ist Teiler von 4.

(c) $1 = 2 - 1$

(d) $3 \cdot 7 = 21$

(e) Es gibt unendlich viele Primzahlen.

(f) 6 ist eine ungerade Zahl.

(g) 3 lässt sich als Summe von geraden Zahlen darstellen.

(h) $5 + 6 = 10$

(i) $80 \div 7 = 10$

(j) $2 + x = 5$

(k) $2 \cdot (x + 3) = 2 \cdot x + 6$

(l) 3 ist kein Teiler von 4 und $p = wahr$.

(m) Für alle natürlichen Zahlen n gilt: $2 \cdot n = n + n$

(n) Es existiert eine natürliche Zahl x mit $234 < x < 235$.

Beispiele (a) bis (e) sind wahre Aussagen und (f) bis (i) falsche Aussagen. Dagegen sind (j) bis (l) keine Aussagen. (m) ist eine wahre Aussage, (n) wiederum eine falsche Aussage.

2 Operationen auf Aussagen

Auf Aussagen werden eine Reihe von Operationen (auch *Abbildungen* oder *Funtionen* genannt) definiert. Mittels der so eingeführten *(Funktions-)* Symbole, die häufig Operatoren genannt werden, können aus vorhandenen Aussagen neue konstruiert werden. Seien im Folgenden A und B Aussagen. Dafür schreibt man auch $A, B \in \{wahr, falsch\}$ oder $A, B \in \{W, F\}$ oder $A, B \in \{0, 1\}$ oder noch kürzer, aber weniger gebräuchlich $A, B \in 2$, sofern 2 mit $2 := \{0, 1\}$ eingeführt wird.

Definition 2.1 (Negation) $\neg : \{0,1\} \to \{0,1\} : A \mapsto \neg A$ mit $\neg 0 := 1$ und $\neg 1 := 0$

Oder als Tabelle:

A	$\neg A$
0	1
1	0

Oder in Worten:
Die Negation von einer wahren Aussage ist als falsch definiert, die Negation der falschen Aussage ist wahr.

Den Ausdruck $\neg A$ liest man als „nicht A“.

Definition 2.2 (Konjunktion, Disjunktion, Implikation, Äquivalenz) Neben der einstelligen Negation gibt es mehrere allgemein gebräuchliche zweistellige Operationen auf Aussagen:

Konjunktion: $\wedge : 2 \times 2 \to 2 : (A, B) \mapsto A \wedge B$	(sprich „A und B“)
Disjunktion: $\vee : 2 \times 2 \to 2 : (A, B) \mapsto A \vee B$	(sprich „A oder B“)
Implikation: $\Rightarrow : 2 \times 2 \to 2 : (A, B) \mapsto A \Rightarrow B$	(sprich „wenn A, dann B“, auch „A impliziert B“)
Äquivalenz: $\Leftrightarrow : 2 \times 2 \to 2 : (A, B) \mapsto A \Leftrightarrow B$	(sprich „A genau dann, wenn B“, auch „A ist äquivalent zu B“)

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Bemerkung 2.3 Häufig entstehen Fehler, indem nicht beachtet wird, dass eine **oder**-Verknüpfung stets genau dann wahr ist, wenn *mindestens eine* ihrer Teilaussagen wahr ist. Dagegen benutzt man in der Mathematik die Formulierung „**entweder** A **oder** B“, um auszudrücken, dass *genau eine* von beiden Aussagen wahr ist, auch *exklusives Oder* genannt.

Eine noch häufigere Fehlerquelle ist die Implikation. $A \Rightarrow B$ ist genau dann falsch, wenn A wahr und B falsch ist, in Symbolen $(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$. Dann und nur dann besteht ein Widerspruch der Wahrheitswertebelegung für A und B zu der angegebenen Implikation. Bei einer Implikation $A \Rightarrow B$ nennt man die Prämisse A auch **hinreichende Bedingung** und die Konklusion B **notwendige Bedingung**. Es reicht also aus, wenn die hinreichende Bedingung falsch oder die notwendige Bedingung wahr ist, damit die Implikation wahr ist.

Bemerkung 2.4 Insbesondere die Operationen $\Rightarrow$ und $\Leftrightarrow$ können auch als Relationen aufgefasst werden. Diese Intuition entspricht schon eher dem Gebrauch der Symbole beim mathematisch korrekten Schließen bzw. Beweisen. Die Bedeutung von Implikation und Äquivalenz ändert sich dadurch nicht wesentlich.

Satz 2.5 *Ähnlich wie für Addition und Multiplikation gelten für Konjunktion und Disjunktion Assoziativ-, Kommutativ- sowie Distributivgesetze. Seien A, B und C Aussagen. Dann gilt:*

Idempotenz:	$A \wedge A \Leftrightarrow A$	$A \vee A \Leftrightarrow A$
Assoziativität:	$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$	$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$
Kommutativität:	$A \wedge B \Leftrightarrow B \wedge A$	$A \vee B \Leftrightarrow B \vee A$
Distributivität:	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

Beweis. Der Beweis ist trivial und erfolgt über Wahrheitstabellen. *(siehe Übungsaufgaben)* ∎

Proposition 2.6 (Ersetzungsregeln und De Morgan)

Es gelten folgende Ersetzungsregeln für Implikation und Äquivalenz sowie die De Morgan'schen Gesetze für Und und Oder:

Implikation	$A \Rightarrow B$
$\Leftrightarrow$	$\neg A \vee B$
$\Leftrightarrow$	$\neg(A \wedge \neg B)$
Äquivalenz	$A \Leftrightarrow B$
$\Leftrightarrow$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
$\Leftrightarrow$	$(A \wedge B) \vee (\neg A \wedge \neg B)$
$\Leftrightarrow$	$(A \vee \neg B) \wedge (\neg A \vee B)$

Regeln von De Morgan
$(\neg A \wedge \neg B) \Leftrightarrow \neg(A \vee B)$
$(\neg A \vee \neg B) \Leftrightarrow \neg(A \wedge B)$

Beweis. Der Beweis ist wie bei Satz 2.5 trivial und erfolgt über Wahrheitstabellen. *(siehe Übungsaufgaben)* ∎

3 Prädikate und Aussageformen

Oft sagt man in der Mathematik etwas *über Objekte* aus, seien es Zahlen oder gar andere Objekte wie Graphen, Gruppen, Vektorräume, und vieles mehr. Dazu führt man häufig Variablen ein, gern mit x bezeichnet. Zum Beispiel kann folgendes gefragt werden:

Sei x eine natürliche Zahl. Das Quadrat von x ist Teiler von 100.
Bestimmen Sie alle x, für die obige … (ja, was denn? … Aussage???) gilt.

Offenbar wird mit „Das Quadrat von x ist Teiler von 100." etwas Bestimmtes *über* x ausgesagt, aber laut Definition 1.1 ist es keine Aussage. Die richtige Bezeichnung lautet hier *Prädikat*. Intuitiv kann man ein Prädikat als Aussage in Abhängigkeit von einem Objekt über das Objekt verstehen. Informell kann man sich merken „Prädikat = Aussage + Variablen". Ein Prädikat beschreibt eine Eigenschaft von Objekten.

Definition 3.1 (Prädikat) Ein Prädikat ist eine Funktion (oftmal mit P bezeichnet), deren Zielbereich die Menge der Aussagen $\{0, 1\}$ ist. Sei M eine nichtleere Menge. $P : M \to \{0, 1\}$

Bemerkung 3.2 Ein Prädikat kann einstellig oder (endlich) mehrstellig sein. Einstellige Prädikate sagen über ein Objekt etwas aus, k-stellige Prädikate über ein Tupel von k Objekten. Sämtliche Funktionen sind Prädikate, sofern sie jeweils nur auf wahr oder falsch abbilden.

Beispiel 3.3 Ein einstelliges Prädikat P ist beispielsweise definiert durch

$$P(x) := 2 \mid x$$

Man kann in diesem Fall auch „... ist eine gerade Zahl" für P schreiben. Ein weiteres einstelliges Prädikat ist „... ist ein Teiler von 14". Dieses ist offensichtlich für die Zahlen 1, 2, 7 und 14 wahr und für alle anderen Zahlen falsch. Ein zweistelliges Prädikat ist beispielsweise „ist Teiler von". In Symbolen:

$$P(x, y) := x \mid y$$

Hier müssen für zwei Variablen Werte eingesetzt werden, damit eine Aussage entsteht. So ist dann zum Beispiel $P(3, 21) = wahr$, weil 3 ein Teiler von 21 ist und $P(5, 7) = falsch$, weil 5 kein Teiler von 7 ist.

Definition 3.4 (Aussageform) Eine Aussageform ist ein Prädikat, bei dem alle Variablen aussagenlogische Variablen sind, also nur die Werte wahr und falsch annehmen dürfen.

Beispiel 3.5 Seien A, B und C aussagenlogische Variablen. Dann ist

$$(A \Rightarrow (B \vee C)) \wedge B \wedge (A \vee \neg B)$$

eine Aussageform. Oft wird nach Lösungen für eine solche Aussageform gefragt. Zum Bestimmen aller Lösungen der obigen Aussageform kann man alle möglichen Belegungen der drei Variablen einsetzen und jeweils das Ergebnis ausrechnen. Man kann jedoch auch durch geschicktes Hinsehen die Lösung(en) ablesen:

- Die Aussageform ist eine Und-Verknüpfung mehrerer Teilaussagen, u.a. taucht die Variable B dort einzeln auf. Wenn die Und-Verknüpfung wahr sein soll, müssen alle Teilformeln, also auch B, wahr sein.

- Wir wissen, dass wenn es überhaupt eine Lösung gibt, $B = wahr$ gilt und betrachten als nächstes den rechten Ausdruck $A \vee \neg B$. Da B wahr ist, ist $\neg B$ falsch. Also muss A wahr sein, damit die Formel erfüllbar sein kann.

- Wir wissen bisher, dass $A = wahr \wedge B = wahr$ gilt. Leicht ist zu sehen, dass dann auch für C beliebig der linke Ausdruck $A \Rightarrow (B \vee C)$ wahr ist.

Die Aussageform von Beispiel 3.5 hat also genau zwei gültige Variablenbelegungen, nämlich $(A, B, C) = (1, 1, 0)$ und $(A, B, C) = (1, 1, 1)$

Definition 3.6 (Tautologie) Eine Tautologie ist eine Aussageform, die für alle Variablenbelegungen wahr ist.

Beispiel 3.7 $A \vee \neg A$ ist eine Tautologie wie auch $(A \Rightarrow B) \vee (B \Rightarrow A)$.

4 Quantoren

Eine Möglichkeit, um aus Prädikaten wieder Aussagen zu konstruieren, sind Quantoren. Oft möchte man eine Aussage über die Gesamtheit aller Objekte einer Menge z.B. über die Gesamtheit der natürlichen Zahlen treffen oder eine Existenzaussage über ein Objekt innerhalb einer Menge. Zum Beispiel ist die Aussage „Es existiert eine natürliche Zahl x mit $x \geq 1024$" eine solche Konstruktion.

Für eine Menge M von Objekten und ein Prädikat $P : M \to \{0, 1\}$ schreibt man:

mathematische Schreibweise	Bedeutung
$\forall x \in M : P(x)$	Für alle Objekte x aus der Menge M gilt $P(x)$
$\exists x \in M : P(x)$	Es existiert ein Objekt x in der Menge M, für welches $P(x)$ gilt.

Teil II
Rechnen mit Kongruenzen

Vielleicht ist dem einen oder anderen schon einmal aufgefallen, dass, wenn er zwei gerade Zahlen addiert oder subtrahiert, das Ergebnis stets auch eine gerade Zahl ist. Ebenso fällt beim Addierten zweier ungerader Zahlen auf, dass das Ergebnis eine gerade Zahl ist. Addiert man jedoch eine gerade Zahl zu einer ungeraden, dann ist das Ergebnis eine ungerade Zahl. Im folgenden Teil wollen wir uns etwas Klarheit darüber verschaffen.

5 Teiler

Definition 5.1 Seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen. a heißt genau dann Teiler von b, wenn es eine ganze Zahl $m \in \mathbb{Z}$ gibt, sodass $a \cdot m = b$ gilt. In Symbolen

$$a \mid b :\Leftrightarrow \exists m \in \mathbb{Z} : a \cdot m = b$$

Ist dagegen a kein Teiler von b, schreibt man auch $a \nmid b$.

Bemerkung 5.2 Es gilt $a \nmid b \Leftrightarrow \neg(a \mid b)$ sowie $a \nmid b \Leftrightarrow \forall m \in \mathbb{Z} : a \cdot m \neq b$.

Definition 5.3 Der größte gemeinsame Teiler $ggT(a, b)$ zweier natürlicher Zahlen $a, b \in \mathbb{N}$ ist die größte natürliche Zahl d, für die $(d \mid a) \wedge (d \mid b)$ gilt.

Lemma 5.4 *Wenn eine ganze Zahl m zwei ganze Zahlen a und b teilt, dann teilt m auch deren Summe.*

$$(m \mid a) \wedge (m \mid b) \quad \Rightarrow \quad (m \mid (a + b))$$

Beweis.

$$\begin{aligned}
&(m \mid a) \wedge (m \mid b) \\
\Longrightarrow\ &\exists x : a = x \cdot m \ \wedge\ \exists y : b = y \cdot m \\
\Longrightarrow\ &\exists x, y : a + b = x \cdot m + y \cdot m = (x + y) \cdot m \\
\Longrightarrow\ &\exists z : a + b = z \cdot m, \quad (z := x + y) \\
\Longrightarrow\ &m \mid (a + b)
\end{aligned}$$

■

Definition 5.5 (Modulooperator) Man definiert eine Operation **mod** so, dass $a \bmod b$ der Rest beim Teilen von a durch b ist.
$\mathrm{mod} : \mathbb{Z} \times \mathbb{N}^+ \to \mathbb{N} : (a, b) \mapsto a \bmod b$ mit $(a \bmod b = r) \wedge (0 \leq r < b) \wedge (\exists k \in \mathbb{Z} : a = k \cdot b + r)$

Bemerkung 5.6 Der Rest $r = a \bmod b$ aus Definition 5.5 ist eindeutig bestimmt.

Beweis. Angenommen, es gäbe zwei Reste r_1, r_2 mit $r_1 \neq r_2$, welche die Bedingungen in Definition 5.5 erfüllen. Dann gibt es zwei ganze Zahlen k_1 und k_2 mit $k_1 \cdot b + r_1 = a = k_2 \cdot b + r_2$. Daraus folgt $r_1 - r_2 = (k_2 - k_1) \cdot b$. Wegen $r_1 \neq r_2$ gilt $|r_1 - r_2| \neq 0$. Dann muss b ein Teiler von $|r_1 - r_2|$ sein. Weil aber $0 \leq r_i < b$ für $i = 1, 2$ gilt, folgt dann auch $|r_1 - r_2| < b$. Das steht im Widerspruch zur Aussage, dass b die Zahl $|r_1 - r_2|$ teilt.
$\Longrightarrow$ Es gibt keine zwei verschiedenen Reste. ■

Durch diesen Beweis haben wird uns klargemacht, dass **mod** auch wirklich eine *Funktion* ist, indem wir nachgewiesen haben, dass **mod** rechtseindeutig ist.

Definition 5.7 Für zwei ganze Zahlen a und b, welche beim Teilen durch m den gleichen Rest lassen, schreiben wir auch $a \equiv b \pmod{m}$ (sprich „a ist kongruent zu b modulo m“). Formal lautet das:

$$a \equiv b \pmod{m} :\Leftrightarrow a \bmod m = b \bmod m$$

Man sagt auch, dass a und b in derselben Restklasse mod m liegen.

Satz 5.8 *Für Zahlen $a, b \in \mathbb{Z}$ und ein Modular $m \in \mathbb{N}^+$ gelten folgende Beziehungen:*

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m \tag{1}$$
$$(a - b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m \tag{2}$$
$$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m \tag{3}$$
$$** (a \div b) \bmod m = ((a \bmod m) \div (b \bmod m)) \bmod m \tag{4}$$

Bemerkung 5.9 Gleichung (4) ist mit etwas größerer Vorsicht zu genießen. Wenn man $1 \div x$ als „multiplikatives Inverses von x modulo m“ interpretiert, ist es auch sinnvoll, Reste von gebrochenen Zahlen zu betrachten. Dies allerdings führt für unseren Kurs ein bisschen zu weit, weswegen wir Gleichung (4) zunächst nicht vordergründig behandeln werden.

Beispiel 5.10 Mittels der Rechenregeln von Satz 5.8 ist es möglich, den Rechenaufwand erheblich zu reduzieren, wenn nicht nach exakten Zahlen sondern bestimmten Resten gefragt wird. So ist zum Beispiel $(25497 + 45038 + 45938 + 1234) \bmod 3 = (0 + 2 + 2 + 1) \bmod 3 = 2$. Die Summe dieser beachtlich großen Zahlen lässt also beim Teilen durch 3 den Rest 2. Dafür haben wir die Zahlen nur kurz angesehen und auch keinen Taschenrechner oder großen Zettel benötigt, um sie explizit zu addieren.

Beispiel 5.11 Wie lautet die letzte Ziffer von 2017^{2017}?

Dazu betrachten wir die Zahl $2017^{2017} \bmod 10$. Das ist ein Produkt von 2017 gleichen Zahlen. Laut Satz 5.8 ist dann die letzte Ziffer von 2017^{2017} gleich der letzten Ziffer von 7^{2017}. Weiterhin gilt $7^{2017} \equiv 7^{2\cdot 1008+1} \equiv 7 \cdot (7^2)^{1008} \equiv 7 \cdot 49^{1008} \equiv 7 \cdot (-1)^{1008} \equiv 7 \cdot 1^{504} \equiv 7 \pmod{10}$. Die letzte Ziffer lautet 7.

6 Aussagen über Teiler und Faktoren

Satz 6.1 (Der euklidische Algorithmus)

$$\begin{aligned} \forall a \neq 0 &: ggT(a, 0) = a \\ \forall b \neq 0 &: ggT(a, b) = ggT(b, a \bmod b) \end{aligned}$$

Beweis. Den trivialen Fall in der ersten Zeile wollen wir hier direkt überspringen. Betrachten wir den Schritt, welcher in der zweiten Zeile vollzogen wird:

$$a \quad = \quad k \cdot b \quad + \quad r$$

Man kann den euklidischen Algorithmus anwenden, indem man ein $k \in \mathbb{Z}$ sucht, sodass obige Gleichung mit einem Rest r mit $0 \leq r < b$ erfüllt ist. Dann hat man $a \bmod b = r$ bestimmt. Die Behauptung lautet nun, dass der größte gemeinsame Teiler von a und b gleich dem größten gemeinsamen Teiler von b und $(a \bmod b)$ ist.

Nach Lemma 5.4 wissen wir, dass jeder gemeinsame Teiler von a und b auch ein Teiler von r ist. Insbesondere ist also der größte gemeinsame Teiler von a und b ein Teiler von r und natürlich auch von b. Also ist er kleiner oder gleich dem größten gemeinsamen Teiler von b und r ($ggT(a, b) \leq ggT(b, r)$). Andersherum gilt aber wegen Lemma 5.4 auch, dass jeder gemeinsame Teiler von b und r, also insbesondere der größte gemeinsame Teiler beider Zahlen, ein Teiler von a (und von b sowieso) ist. Also ist dieser Teiler kleiner oder gleich dem größten gemeinsamen Teiler von a und b ($ggT(b, r) \leq ggT(a, b)$). Aus $ggT(a, b) \leq ggT(b, r)$ und $ggT(b, r) \leq ggT(a, b)$ folgt unmittelbar $ggT(a, b) = ggT(b, r)$ und damit die Behauptung. ∎

Korollar 6.2 (Lemma von Bézout) *Es seien $m, n \in \mathbb{N}$ mit der Einschränkung, dass nicht beide 0 sind. Dann gibt es ganze Zahlen $a, b \in \mathbb{Z}$ mit $ggT(m, n) = am + bn$.*

*Beweis (**Zusatz für Interessierte).* mittels Induktion über n.
Induktionsanfang: Für $n = 0$ gilt $ggT(m, n) = 1m + 0n$.
Induktionsvoraussetzung: $\forall n < n_0$ gibt es ganze Zahlen a, b mit $ggT(m, n) = am + bn$
Induktionsbehauptung: Es gibt ganze Zahlen a, b mit $ggT(m, n_0) = am + bn_0$
Induktionsbeweis: Man bestimme Zahlen q, r mit $m = q \cdot n_0 + r$ und $r < n_0$. Weil $r < n_0$ gibt es Zahlen $a', b' \in \mathbb{Z}$ mit $ggT(n_0, r) = a'n_0 + b'r$. Mit Satz 6.1 folgt:
$ggT(m, n_0) = ggT(n_0, r) = a'n_0 + b'r = a'n_0 + b'(m - qn_0) = b'm + (a' - b'q)n_0$
Mit $a := b'$ und $b := a' - b'q$ folgt die [Induktions-] Behauptung. ∎

Korollar 6.3 (Lemma von Euklid) *Wenn eine Primzahl das Produkt zweier natürlicher Zahlen teilt, dann teilt sie auch mindestens einen der Faktoren.*

Beweis. Seien $m, n \in \mathbb{N}$ zwei natürliche Zahlen. Weiterhin sei p eine Primzahl mit $p \mid mn$. Angenommen p ist kein Teiler von n. (Andernfalls wäre unser Beweis fertig.) Dann bleibt $p \mid m$ zu zeigen. Wir wissen bereits, dass $ggT(p, n) = 1$. Damit gibt es wegen Lemma 6.2 zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $1 = ap + bn$. Multipliziert man diese Gleichung mit m, so ergibt sich $m = p(am) + bmn$. Laut Voraussetzungen teilt p den Summanden bmn und offensichtlich auch $p(am)$. Wegen Lemma 5.4 teilt p also auch m. ∎

Teil III
Der nun folgende Teil des Dokumentes ist noch in Arbeit und besteht größtenteils aus Ideensammlungen und Auflistungen möglicher Themen für die Förderung begabter Schüler

Teil IV
Elementare Beweismethoden

direkter Beweis, indirekter Beweis, vollständige Induktion
$0 + 1 + 2 + \cdots + n = n \cdot (n + 1) \div 2$ □

Teil V
Gleichungen, Ungleichungen und Gleichungssysteme

Lineare Gleichungssysteme, quasi-lineare GS:
$x^2y - 2xy = 6$
$x^2 + 3x = 36 \div y$

Teil VI
Mengen

zurzeit für die Schüler eher unwichtig