



UNIVERSITÄT
LEIPZIG

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

Übersicht

1. Ziele dieses Moduls
2. Aussagenlogik
3. Einige arithmetische Grundlagen

1. Ziele dieses Moduls

2. Aussagenlogik

3. Einige arithmetische Grundlagen

Unsere Beschränkungen und Ziele

- Verschiedene Studiengänge (Informatik, Lehramtsstudenten, Mathematik)
- Einführung in die Mathematik und genaues mathematisches Denken
 - ▶ Was wir genau tun, ist weniger wichtig

- Inhalte:
 - ▶ Logik (später: Strukturen, die in einem Computer programmiert werden können, die Logik darstellen: Verbands, Boolesche Algebren)
 - ▶ Elementare Mengenlehre
 - ▶ Mathematische Strukturen, die in einem Computer programmiert und in Algorithmen verwendet werden können (Gruppen, Ringe, Körper, Graphen)
 - ▷ Insbesondere: Modulo Arithmetik, Euklidischer Algorithmus

1. Ziele dieses Moduls

2. Aussagenlogik

3. Einige arithmetische Grundlagen

Ziele für Heute

- Standardnotation lesen und schreiben
- Einführung in mathematisches Denken
- Einführung in die Formalisierung von Begriffen wie "Wahrheit" in der Mathematik
- Zunächst wollen wir versuchen, zu klären, was eine mathematische Aussage ist. Fangen wir mit einem Beispiel aus dem Gesetz an.

StGB § 211 — Mord

- Der Mörder wird mit lebenslanger Freiheitsstrafe bestraft.
- Mörder ist, wer
 - ▶ aus Mordlust, zur Befriedigung des Geschlechtstrieb, aus Habgier oder sonst aus niedrigen Beweggründen,
 - ▶ heimtückisch oder grausam oder mit gemeingefährlichen Mitteln oder
 - ▶ um eine andere Straftat zu ermöglichen oder zu verdecken,einen Menschen tötet.

- Aussagen
 - ▶ Anton ist Mörder
 - ▶ Anton tötet aus Habgier
 - ▶ Anton tötet heimtückisch
 - ▶ Anton bekommt lebenslange Freiheitsstrafe
- Aussagenkombinationen
 - ▶ Anton tötet heimtückisch **oder** Anton tötet aus Habgier
 - ▶ **Wenn** Anton ist Mörder **dann** Anton bekommt lebenslange Freiheitsstrafe
- Der letzte Satz erfasst einen Teil des Gesetzes. Er erlaubt uns, eine Folgerung zu ziehen. Wenn wir wissen, dass die Aussage “Anton ist Mörder” dann wissen wir auch, dass die Aussage “Anton bekommt lebenslange Freiheitsstrafe” ist wahr.

StVO I, § 30(3) — Sonn- und Feiertagsfahrverbot (editiert)

An Sonn- und Feiertagen dürfen (...) Lastkraftwagen nicht verkehren. Dies gilt nicht für

- die Beförderung von frischer Milch und frischen Milcherzeugnissen,
- die Beförderung von frischem Fleisch und frischen Fleischerzeugnissen.

- Aussagen:
 - ▶ "Es ist Sonntag"
 - ▶ "Mein Auto ist ein Lastkraftwagen",
 - ▶ "Mein Auto darf heute nicht verkehren",
 - ▶ "Mein Auto befördert frische Milch"
- Aussagenkombination:
 - ▶ "Mein Auto befördert frische Milch" **oder** "Mein Auto befördert frisches Fleisch".
 - ▶ **Wenn** "Es ist Sonntag" **und** ("Mein Auto befördert frische Milch" **oder** "Mein Auto befördert frisches Fleisch") **dann nicht wahr das** "Mein Auto darf nicht verkehren".

Definition (informel) Aussage = Äußerung die entweder wahr oder falsch ist.

- genau ein Wahrheitswert; obwohl darf unbekannt sein
- 1 = wahr, 0 = falsch
- Beispiele von Aussagen:
 - ▶ “LKW L-DS 2022 befördert frische Milch”,
 - ▶ “16.11.2022 war ein Feiertag in Sachsen”,
 - ▶ “2 ist eine Primzahl”,
 - ▶ “ $2 + 2 = 5$ ”,
 - ▶ “Der einzige Planet in der Milchstraße, auf dem es Leben gibt, ist die Erde.”
 - ▶ “Jede gerade natürliche Zahl $n > 2$ ist Summe zweier Primzahlen”,
- Keine Aussagen: “Hallo!”, “Wie heißt du?”, “Bitte nehmen Sie Platz”, “Dieser Satz ist falsch”.

- Am meistens verwenden wir die große Buchstaben A, B, C, \dots für Aussagen.
 - ▶ Z.B. sei A die Aussage "Der einzige Planet in der Milchstraße mit Leben ist die Erde." und sei B die Aussage " $2 + 2 = 5$ ",
- Junktoren:
 - ▶ **Negation** $\neg F$ gelesen als **nicht F** oder auch **nicht wahr dass F**
 - ▶ **Konjunktion** $F \wedge G$ gelesen als **F und G**
 - ▶ **Disjunktion** $F \vee G$ gelesen als **F oder G**
 - ▷ Gedankenstütze: Konjunktion $A \wedge B$ (und = unten offen), Disjunktion $A \vee B$ (oder = oben offen)
 - ▶ **Implikation** $F \Rightarrow G$ oder auch $F \rightarrow G$ gelesen als **wenn F dann G** oder auch **F impliziert G** . Die Aussage F heißt hier die **Vorbedingung** und G heißt die **Folgerung**.
 - ▶ **Äquivalenz** $F \iff G$ oder auch $F \leftrightarrow G$ gelesen als **F genau dann, wenn G** oder auch **F ist äquivalent zu G**

Wenn wir den Wahrheitswert von Grundaussagen kennen, dann können wir auch sagen, was der Wahrheitswert ihrer beliebigen Kombination ist. Wir verwenden die folgenden Regeln.

| A | B | $\neg A$ | $A \wedge B$ | $A \vee B$ | $A \Rightarrow B$ | $A \iff B$ |
|-----|-----|----------|--------------|------------|-------------------|------------|
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |

- Die meisten Verständnisschwierigkeiten gehen von der Implikation aus.
 - ▶ A wahr, B wahr: $A \Rightarrow B$ wahr
 - ▶ A wahr B falsch: $A \Rightarrow B$ falsch
 - ▶ A falsch, B beliebig: $A \Rightarrow B$ wahr.
- **Beispiel.** Nehmen wir an, wir haben eine Aussage “Falls es heute um 8Uhr geregnet hat, dann habe ich einen Regenschirm mit.”
 - ▶ $A \Rightarrow B$, A = “Heute um 8Uhr hat es geregnet”, B = “Ich habe einen Regenschirm mit”.
 - ▶ Falls es nicht regnet, dann stimmt diese Aussage. Unabhängig davon ob ich einen Regenschirm habe oder nicht.
- **Beispiel.** “Falls ich 200cm groß bin, dann lebe ich auf dem Mars”.
 - ▶ Ich bin nicht 200cm groß, also diese Aussage ist wahr.

- A wahr, B wahr: $A \Rightarrow B$ wahr.
- **Beispiel.** “Falls ich in Leipzig wohne dann Frankreich und Spanien haben eine gemeinsame Landgrenze.”
 - ▶ $A \Rightarrow B$. A = “Ich wohne in Leipzig”, B = “Frankreich und Spanien haben eine gemeinsame Landgrenze.”.
 - ▶ A und B sind wahr, deswegen $A \Rightarrow B$ ist auch wahr.
 - ▶ Ein nachweisbarer Zusammenhang ist nicht erforderlich.
- **Beispiel.** “Falls ich in Leipzig wohne dann Frankreich und Spanien haben keine gemeinsame Landgrenze.” ist eine falsche Aussage.

Definition (informel) - Atome & Formeln Atome = primitive Aussagen wie A, B , Formeln = Kombinationen von Atomen, z.B. $(A \wedge B) \vee C$.

- Wahrheitswert von Atom = Gültigkeit fachlicher “Aussage”,
- Wahrheitswert von Formel = ergibt sich aus Wahrheitswert der vorkommenden Atome, unter Anwendung der oben genannten Regeln.
- Die Rangfolge von logischen Operationen lautet: Negationen werden zuerst ausgeführt, dann Konjunktionen (und), dann Disjunktionen (oder), dann Implikation, dann Äquivalenz.
- **Beispiel.** Wir betrachten die Formel $(A \vee B \Rightarrow C) \wedge \neg B$.
 - Falls z.B. $A = 0, B = 1, C = 0$, dann $A \vee B = 1, (A \vee B \Rightarrow C) = 0, (A \vee B \Rightarrow C) \wedge \neg B = 0$.

Definition Eine Formel ist

- eine **Tautologie** (oder **tautologisch**), falls sie unabhängig von der Belegung der Atome wahr ist.

“Tautologien sind immer wahr.”

- **unerfüllbar** (oder **Kontradiktion**), falls sie unabhängig von der Belegung der Atome falsch ist.

“Unerfüllbare Formeln sind immer falsch.”

- **erfüllbar**, falls sie nicht unerfüllbar ist, d. h. es gibt eine Belegung der Atome, so dass die Formel wahr ist,
- **widerlegbar**, falls sie keine Tautologie ist., d. h. es gibt eine Belegung der Atome, so dass die Formel falsch ist.

• Die einfachste Methode, um zu überprüfen, ob eine gegebene Formel tautologisch (oder unerfüllbar oder erfüllbar oder widerlegbar) ist, ist die Verwendung der so genannten **Wahrheitstabelle** - tabellarische Auflistung **aller** Möglichkeiten. Schritte:

- ▶ Identifikation aller Atome A_1, \dots, A_n
- ▶ Auflistung aller 2^n Wahrheitswertbelegungen für A_1, \dots, A_n .

| A_1 | A_2 | \dots | A_{n-1} | A_n | \dots |
|---------|---------|---------|-----------|---------|---------|
| 0 | 0 | \dots | 0 | 0 | \dots |
| 0 | 0 | \dots | 0 | 1 | \dots |
| \dots | \dots | \dots | \dots | \dots | \dots |
| 1 | 1 | \dots | 1 | 1 | \dots |

- ▶ Berechnung der Wahrheitswerte der Teilformeln

- **Beispiel** Die Formel $A \wedge B \Rightarrow A \vee B$ ist eine Tautologie. (d.H. diese Formel gilt immer, unabhängig davon was A und B sind)

| A | B | $A \wedge B$ | $A \vee B$ | $A \wedge B \Rightarrow A \vee B$ |
|-----|-----|--------------|------------|-----------------------------------|
| 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 |

Definition Zwei Formeln sind **äquivalent** genau dann, wenn (gdw) deren Wahrheitswerte für alle Belegungen der Atome übereinstimmen.

- **Beispiel.** Die Aussagen $A \Rightarrow B$ und $\neg A \vee B$ sind äquivalent.

► Die Wahrheitstabelle für die Aussage $A \Rightarrow B$ haben wir schon gesehen. Hier ist die Wahrheitstabelle für die Aussage $\neg A \vee B$:

| A | B | $\neg A$ | $\neg A \vee B$ |
|-----|-----|----------|-----------------|
| 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 |

► Wir sehen also dass die zwei Wahrheitstabellen sind gleich, was bedeutet dass die zwei Aussagen äquivalent sind.

- Man nennt die Äquivalenz von $A \Rightarrow B$ und $\neg A \vee B$ die “Elimination von \Rightarrow ”.
- Wenn wir zwei Formeln haben, F und G , dann sind F und G äquivalent genau dann wenn die Formel $F \iff G$ eine Tautologie ist.
 - ▶ Z.B. die Formel $(\neg A \vee B) \iff (A \Rightarrow B)$ ist eine Tautologie. Wir können diese Formel auch als $\neg A \vee B \iff A \Rightarrow B$ schreiben.
- Ähnlich zeigen wir dass die Formeln $(A \wedge B) \wedge C$ und $A \wedge (B \wedge C)$ äquivalent sind. Diese Äquivalenz heißt “Assoziativität von \wedge ”.
 - ▶ Assoziativität erlaubt uns zu schreiben z.B. $A \wedge B \wedge C$. Es ist unerheblich, wo sich die Klammern befinden und welche Operationen (also entweder $A \wedge B$ oder $B \wedge C$) zuerst durchgeführt werden.

- Die Formeln $(A \rightarrow B) \rightarrow C$ und $A \rightarrow (B \rightarrow C)$ sind nicht äquivalent.

| A | B | C | $(A \rightarrow B) \rightarrow C$ | $A \rightarrow (B \rightarrow C)$ |
|-----|-----|-----|-----------------------------------|-----------------------------------|
| 0 | 0 | 0 | 0 | 1 |

- Wenn wir eine große Formel F haben und darin eine Unterformel U sehen, können wir U durch eine äquivalente Unterformel U' ersetzen und erhalten so eine neue Formel F' die zu F äquivalent ist.
- Dieser “Substitutionsprinzip” eröffnet uns die Möglichkeit die Formeln zu vereinfachen, und zu zeigen dass zwei Formeln äquivalent sind, durch **Äquivalenzketten**.
- **Beispiel.** $F = (A \Rightarrow B) \vee \neg B$ ist eine Tautologie.
 - ▶ Tatsächlich durch die “Elimination von \Rightarrow ” ist F mit $(\neg A \vee B) \vee \neg B$ äquivalent. Und durch die “Assoziativität von oder”, $(\neg A \vee B) \vee \neg B$ ist mit $\neg A \vee (B \vee \neg B)$ äquivalent.
 - ▶ $B \vee \neg B$ ist immer wahr (“Ausgeschlossenes Drittes”), weswegen $\neg A \vee (B \vee \neg B) = \neg A \vee 1 = 1$.
- Mehr Äquivalenzen werden auf dem Übungsblatt aufgelistet.

1. Ziele dieses Moduls

2. Aussagenlogik

3. Einige arithmetische Grundlagen

- Wir werden die Arithmetik häufig z.B. zur Illustrierung von Beweistechniken verwenden, also rekapitulieren wir einige arithmetische Grundlagen, die wir hoffentlich schon kennen.
- In diesem Modul, das Symbol $:=$ ist ein Zeichen dafür, dass die linke Seite zum ersten Mal in einem gegebenen Kontext definiert wird.
 - ▶ Z.B. “Sei $a := 5$ ”, oder “Wir definieren die Formel F wie folgt: $F := A \vee B$ ”.
 - ▶ Sie müssen dieses Symbol in Lösungen nicht benutzen, z.B. Sei $a = 5$ ist auch akzeptabel.
- Einige Zahlenmengen
 - ▶ $\mathbb{N} := \{0, 1, 2, 3, \dots\}$ die natürlichen Zahlen
 - ▶ $\mathbb{N}_+ := \{1, 2, 3, \dots\}$ die positiven natürlichen Zahlen
 - ▶ $\mathbb{Z} := \{0, 1, -1, 2, -2, \dots\}$ die ganzen Zahlen
 - ▶ $\mathbb{Z} \setminus \{0\} := \{1, -1, 2, -2, \dots\}$ die ganzen Zahlen außer 0.

- Seien $a, b \in \mathbb{Z}$ (gelesen “seien a und b Elemente von \mathbb{Z} ”). Wir sagen dass a teilt b , oder a ist ein Teiler von b , geschrieben $a \mid b$, falls es existiert $k \in \mathbb{Z}$ mit $ak = b$.
- Sehr häufig benutzen wir die folgende Eigenschaften:
 - ▶ Seien $d, a, b \in \mathbb{Z}$. Falls $d \mid a$ und $d \mid b$ dann $d \mid a + b$.
 - ▷ Beweis: Falls $d \mid a$ und $d \mid b$ dann existieren $k, l \in \mathbb{Z}$ so dass $a = dk, b = dl$, woraus folgt $a + b = d(k + l)$, was bedeutet, dass $d \mid a + b$.
 - ▶ Seien $d, a, b \in \mathbb{Z}$. Falls $d \mid a$ dann $d \mid ab$.
 - ▷ Beweis: Falls $d \mid a$ dann existiert $k \in \mathbb{Z}$ so dass $a = dk$, also $ab = dkb$, was bedeutet $d \mid ab$.

- Seien $a, b \in \mathbb{N}_+$. Dann können wir immer die Division mit Rest durchführen, d.h. wir schreiben $b = qa + r$, für irgendwelche $q, r \in \mathbb{N}$, wobei $r < a$.

- ▶ r heißt der Rest, und q heißt der Ganzzahlquotient. Diese Zahlen r und q sind eindeutig.

- ▶ Z.B. $a = 7, b = 45, 45 = 6 \cdot 7 + 3$.

- Falls wir die Division mit Rest für $a, b \in \mathbb{Z} \setminus \{0\}$ durchführen möchten, schreiben wir $b = qa + r$, wobei $q \in \mathbb{Z}, r \in \mathbb{N}$ und $|r| < |a|$.

- ▶ Z.B. $a = 7, b = -45, -45 = -7 \cdot 7 + 4$.

- Seien $a, b \in \mathbb{N}$. Der grösste gemeinsame Teiler von a und b ist die grösste natürliche Zahl d mit der Eigenschaft, dass $d \mid a$ und $d \mid b$. Sie wird mit $\text{ggT}(a, b)$ bezeichnet.

- ▶ z.B. $\text{ggT}(10, 17) = 1, \text{ggT}(49, 14) = 7, \text{ggT}(0, a) = a, \text{ggT}(0, 0)$ definieren wir auch als 0.

- Wenn $a, b \in \mathbb{Z}$ dann definieren wir $\text{ggT}(a, b) := \text{ggT}(|a|, |b|)$. Also wenn $a, b \in \mathbb{Z}$, ist $\text{ggT}(a, b) \in \mathbb{N}$.
 - ▶ z.B. $\text{ggT}(-49, -14) = 7$.
- Der ggT wird mit dem **Euklidischem Algorithmus** berechnet - das wir in den Übungseinheiten besprochen.



UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski
Mathematisches Institut

grabowski@math.uni-leipzig.de