UNIVERSITÄT
LEIPZIG

Vorlesung 12 - Boolesche Algebren, Kommutative Gruppen

Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

1. Wiederholung

2. Boolsche Algebren - Isomorphiesatz von Stone

3. Kommutative Gruppen

- Ein Verband $(M, \preceq)$ heißt **Boolesche Algebra** gdw. er distributiv und komplemetiert ist, und zusätzlich $\bot \neq \top$.
- Beispiel: $(P(X), \subseteq)$, $X \neq \emptyset$.

Satz. Sei $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass

- $\sqcap$ und $\sqcup$ assoziativ, kommutativ, distributiv und absorptiv sind, und
- Die operation $\cdot^*$ jedes Element $x \in M$ auf sein Komplement abbildet, d.H.

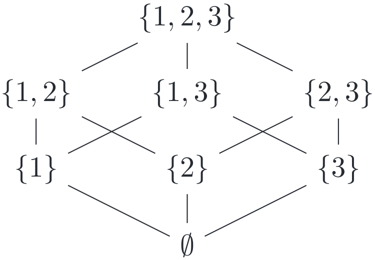
$$x \sqcap x^* = \bot \qquad \text{und} \qquad x \sqcup x^* = \top \ .$$

Dann ist $(M, \preceq)$, mit $x \preceq y$ gdw. $x = x \sqcap y$, eine Boolesche Algebra.

- Wir wenden uns nun zu dem wichtigsten Ergebnis über endliche Boolesche Algebren: Jede endliche Boolesche Algebra ist isomorph zu $\mathcal{P}(A)$, wo A ist eine endliche Menge.
- Ein Element $x \in M \setminus \{\perp\}$ ist ein Atom gdw. für alle $y \in M$ mit $y \preceq x$ gilt $y \in \{\perp, x\}$
- Atome sind also die direkten Nachbarn des kleinsten Elements $\perp$ im Hasse-Diagramm, und die minimalen Elemente in $M \setminus \{\perp\}$.
- Beispiel. Die Boolesche Algebra der Wahrheitswerte hat nur das Atom 1.

$$\begin{tikzcd} 1 \arrow[d, no head] \\ 0 \end{tikzcd}$$

- **Beispiel.** Die Potenzmenge von $M = \{1, 2, 3\}$ hat die Atome $\{1\}$, $\{2\}$ und $\{3\}$.



Satz. Sei $(M, \preceq)$ eine endliche Boolesche Algebra.

- Für jedes $m \in M$ und jedes Atom $a \in M$, gilt $a \wedge m \in \{\perp, a\}$
- Für alle Atome $a, b \in M$ mit $a \neq b$, gilt $a \wedge b = \perp$
- Für jedes $m \in M \setminus \{\perp\}$ existiert ein Atom $a \in M$ mit $a \preceq m$.

Beweis.

- Wir haben $a \wedge m \preceq a$. Da a Atom ist, gilt $a \wedge m \in \{\perp, a\}$.
- Wenn a und b Atome sind, dann folgt $a \wedge b \preceq a$ und $a \wedge b \preceq b$.

  Also $a \wedge b \in \{\perp, a\}$ und $a \wedge b \in \{\perp, b\}$. Wegen $a \neq b$ gilt $a \wedge b = \perp$.

Noch zu beweisen:

- Für jedes $m \in M \setminus \{\perp\}$ existiert ein Atom $a \in M$ mit $a \preceq m$.
- Da M is endlich, finden wir eine Kette

$$m = m_0 > m_1 > m_2 > m_3 > \cdots$$

mit der Eigenschaft dass die einzige Elemente $x \in M$ mit $m_i \geq x \geq m_{i+1}$ sind m_i und m_{i+1}.

Da M ist endlich, die Kette muss mit $\perp$ terminieren, und das letzte Element anders als $\perp$ ist ein Atom mit der gewischten Eigenschaft. $\square$

Satz. (Isomorphiesatz von Stone) Sei $(M, \leq)$ eine endliche Boolesche Algebra und sei A die Menge von Atomen von M. Dann sind $(M, \leq)$ und $(\mathcal{P}(A), \subseteq)$ isomorph.

Der Isomorphismus schickt $m \in M$ auf die Menge $A_m \subset A$ von Atomen a mit $a \leq m$.

Beweis.

- Wir müssen zeigen, dass die Abbildung $m \mapsto A_m$ eine ordnungserhaltende Bijektion ist.
  - ▶ Die Ordnungserhaltung ist klar: wenn $m \leq n$, dann liegen alle Atome, die unter m liegen, auch unter n, also $A_m \subseteq A_n$.
- Für die Injektivität reicht es zu zeigen, dass $m = \sup A_m$. Wir zeigen dies zunächst für $m := \top$. Offensichtlich ist $A_\top$ die Menge aller Atome.
  - ▶ Sei $s := \sup A_\top$. Wenn $s \neq \top$ dann $s^c \neq \bot$, also es existiert ein Atom $a \leq s^c$. Aber dann $a \leq s \wedge s^c$, was ein Widerspruch ist.

- Zeigen wir jetzt für beliebige m, dass $m = \sup A_m$.
  - Seien $a_1, \ldots, a_k$ alle Atome von M. Wir haben $m = \top \wedge m = (a_1 \vee \ldots \vee a_k) \wedge m = (a_1 \wedge m) \vee \ldots (a_k \wedge m)$.
  - Jedes element $a_i \wedge m$ ist entweder $\perp$ (wenn a_i ist nicht unten m), oder a_i (wenn a_i ist unten m).
  - Also $(a_1 \wedge m) \vee \ldots (a_k \wedge m)$ ist genau gleich dem Infimum der Atome, die unter m liegen.
- Für die Surjektivität reicht es zu zeigen, dass, wenn X eine Menge von Atomen ist, dann für $m := \sup X$ gilt $A_m = X$.
  - Offensichtlich gilt $X \subseteq A_m$. Nehmen wir an, dass es existiert $a \in A_m \setminus X$. Wir haben $m = \sup X = \sup A_m$. Insbesondere $\sup X \geq a$.
  - Es folgt $a = \sup X \wedge a = (x_1 \wedge a) \vee (x_2 \wedge a) \vee \ldots \vee (x_l \wedge a)$. Aber $x_i \wedge a \in \{\perp, x_i\}$. Da $a \notin X$, es folgt $x_i \wedge a = \perp$, und deswegen $a = \perp$. Das ist ein Widerspruch.

$\square$

Satz. (Isomorphiesatz von Stone) Sei $(M, \leq)$ eine endliche Boolesche Algebra und sei A die Menge von Atomen von M. Dann sind $(M, \leq)$ und $(\mathcal{P}(A), \subseteq)$ isomorph.

- Gilt dieser Satz für unendliche Boolsche Algebren?
- Nein. Sei $M \neq \emptyset$ eine unendliche Menge und

$$E := \{X \in \mathcal{P}(M) \mid X \text{ endlich}\} \cup \{X \in \mathcal{P}(M) \mid M \setminus X \text{ endlich}\}$$

  - E ist eine Boolsche unter-Algebra von $\mathcal{P}(M)$, da die Operationen $\vee, \wedge$, und Komplement die Elemente von E erhalten.
  - Wenn M abzählabr ist, dann ist auch E abzählbar.
  - Aber $\mathcal{P}(X)$ kann nicht abzählbar sein. Es folgt dass E kann nicht isomorph zu $\mathcal{P}(X)$ sein.

Satz. (Isomorphiesatz von Stone) Sei $(M, \leq)$ eine endliche Boolesche Algebra und sei A die Menge von Atomen von M. Dann sind $(M, \leq)$ und $\big(\mathcal{P}(A), \subseteq\big)$ isomorph.

- Dieser Satz vermittelt uns ein gutes konzeptionelles Verständnis der Aussagenlogik.
- Er motiviert auch die grundlegenden Definitionen der Wahrscheinlichkeitstheorie: In der Wahrscheinlichkeitstheorie beginnen wir mit einer Menge X von atomaren Ereignissen und jedes der Ereignisse x hat eine Wahrscheinlichkeit p_x.

- Kommutative Gruppen sind eine Abstraktion von $(\mathbb{Z}, +)$.
  - Wir haben ein spezielles Element 0 mit der Eigenschaft $x + 0 = x$ für alle $x \in \mathbb{Z}$.
  - Für jedes $x \in \mathbb{Z}$ können wir ein Element y finden, so dass $x + y = 0$ (“additive Inverse von x”),
  - Für alle x, y haben wir $x + y = y + x$.
- Eine algebraische Struktur $(M, \oplus, \cdot^*, e)$ des Typs $(0, 1, 1, 1)$ ist eine kommutative oder auch Abelsche Gruppe gdw. für alle $x, y, z \in M$ gilt:
  - $x \oplus (y \oplus z) = (x \oplus y) \oplus z$, (Assoziativität)
  - $x \oplus y = y \oplus x$, (Kommutativität)
  - $e \oplus x = x$, (neutrales Element)
  - $x \oplus x^* = e$. (inverse Elemente)

Beispiele von kommutativen Gruppen.

- $(\mathbb{Z}, +, (-\cdot), 0)$,
  - Auch $(\mathbb{Q}, +, (-\cdot), 0)$, $(\mathbb{R}, +, (-\cdot), 0)$,
- $(\mathbb{Q} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$
  - Auch $(\mathbb{R} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$
- $(\mathbb{N}, +, (-\cdot), 0)$ ist keine kommutative Gruppe, denn es gibt kein $n \in \mathbb{N}$, so dass $1 + n = 0$).
  - $(\mathbb{Q}, \cdot, \cdot^{-1}, 1)$ ist auch keine kommutative Gruppe, denn es gibt kein $q \in \mathbb{Q}$, so dass $0 \cdot q = 1$).

Wir schreiben am meistens $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, etc. da die inverse Operation und 0 sind eindeutig bestimmt.

- D.H. wir können die kommutative Gruppen auch wie folgt definieren. $(M, +)$ ist eine kommutative Gruppe, gdw.
  - für alle $x, y, z \in M$ gilt $(x + y) + z = x + (y + z)$
  - für alle $x, y \in M$ gilt $x + y = y + x$
  - es gibt $0 \in M$, so dass für alle $x \in M$ gilt $x + 0 = x$
  - für alle $x \in M$ gibt es y so dass $x + y = 0$.
- Kein Problem mit der Wohldefiniertheit im vierten Punkt: Die ersten drei implizieren, dass 0 eindeutig ist: $0 = 0 + 0' = 0'$.
- Die inverse ist auch eindeutig: Wenn $0 = x + y = x + z$ dann $z = 0 + z = (y + x) + z = y + (x + z) = y$.

Wir werden häufig das folgende Lemma verwenden.

Lemma. Sei $(M, +)$ eine kommutative Gruppe und $x, y \in M$. Dann existiert genau ein $z \in M$, so dass $x + z = y$.

Beweis. Wir definieren $z := (-x) + y$. Dann
$x + z = x + ((-x) + y) = (x + (-x)) + y = 0 + y = y$.

Für eindeutigkeit, wenn $x + z = x + z'$ dann auch $(-x) + (x + z) = (-x) + (x + z')$, aber mit Assoziativität es folgt $z = z'$. $\square$

- Im Beweiss haben wir auch die folgende Eigenschaft gesehen: in jeder kommutativen Gruppe wenn wir Elemente $m, x, y \in M$ mit $m + x = m + y$ haben, dann gilt $x = y$.

  Wir werden häufig die Notation $x - y$ für $x + (-y)$ benutzen.
- Üblicherweise wird die Kardinalität einer Gruppe als Ordnung der Gruppe bezeichnet.

Wenn wir zwei Gruppen $(A, +_A)$ und $(B, +_B)$ haben, können wir auch das karthesische Produkt $A \times B$ als eine Gruppe betrachten. Die Operation ist $(a_1, b_1) + (a_2, b_2) := (a_1 +_A a_2, b_1 +_B b_2)$.

- Beispiele: $(\mathbb{R}^2, +)$, $(\mathbb{R}^n, +)$, $(\mathbb{R}\, times \mathbb{Z}, +)$

Die Gruppen der Residuen modulo n

- Die Gruppe der Residuen Modulo n ist die Gruppe $\mathbb{Z}/n$ mit Elementen $\{0, 1, 2, \ldots, n-1\}$. Die operation ist “Addition modulon n”. Z.B. Wenn $n = 5$ dann $4 + 3 = 2$.
- Wir schreiben häufig z.B. $4 + 3 \equiv 7 \equiv 2 \mod 5$.
- Jede endliche okmmutative Gruppe ist isomorph zu einem kartesischen Produkt von Gruppen der Form $\mathbb{Z}/n\mathbb{Z}$.
  - Z.B. $\mathbb{Z}/5 \times \times \mathbb{Z}/5 \times \mathbb{Z}/25 \times \mathbb{Z}/7$.
  - Dies ist ein sehr wichtiger Satz, der normalerweise in einem Kurs über lineare Algebra bewiesen wird. Wir werden ihn in diesem Kurs nicht beweisen.

Isomorphismen und Homomoprhismen

- Ein Isomorphismus von Gruppen $(M,+)$ und $(N,+)$ ist eine Bijektion $\varphi\colon M \to N$, so dass $\varphi(a+b) = \varphi(a) + \varphi(b)$ für alle $a, b \in M$ gilt.
  - ▶ Daraus folgt, dass $\varphi(0_M) = 0_N$, $\varphi(-x) = -\varphi(x)$ für alle $x \in M$.
- Führen wir nun einen weiteren nützlichen Begriff ein: Gruppenhomomoprhismus: Ein Homomorphismus von $(M,+)$ zu $(N,+)$ ist eine Funktion $\varphi\colon M \to N$, so dass für alle $a, b \in M$ gilt $\varphi(a+b) = \varphi(a) + \varphi(b)$ und außerdem $\varphi(0_M) = 0_N$ un d $\varphi(-x) = -\varphi(x)$ für alle $x \in M$.
- Die Eigenschaften $\varphi(0_M) = 0_N$ und $\varphi(-x) = -\varphi(x)$ müssen wir nicht verlangen, sie folgen automatisch aus $\varphi(a+b) = \varphi(a) + \varphi(b)$.

UNIVERSITÄT
LEIPZIG

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Łukasz Grabowski
Mathematisches Institut

grabowski@math.uni-leipzig.de