Technische Universität Ilmenau 15. Juli 2019

Vorlesung

Grundlagen und Diskrete Strukturen

Prof. Matthias Kriesell

Vorlesungsmitschrift von
Adrian Schollmeyer

Inhaltsverzeichnis

Vorgeplänkel

Buchempfehlungen

- Meinel, Mundhenk, Mathematische Grundlagen der Informatik, 5. Auflage (2011), Viewig/Teubner

Wikipedia

- inzwischen akzeptable Quelle

1. Aussagen

1.1. Aussage. Ein Satz, der *wahr* oder *falsch* ist, d. h. er hat den Wahrheitswert „wahr“ bzw. „falsch“ (w/f, t/f, 1/0).

Beispiele

- „5 ist Primzahl“; Aussage, wahr
- „4 ist Primzahl“; Aussage, falsch
- „Jede gerade ganze Zahl größer 2 ist Summe zweier Primzahlen“; Aussage (Goldbach-Vermutung, seit 1742 unbewiesen)
- „Dieser Satz ist falsch“; Satz, jedoch keine Aussage (d.h. formalerer Zugang ist wünschenswert)

1.1. Verknüpfungen von Aussagen

Seien p, q Aussagen, dann seien auch die folgenden Sätze Aussagen:

- „$(p \wedge q)$“ („und“)
- „$(p \vee q)$“ („oder“)
- „$(\neg p)$“ („nicht“, Negation)
- „$(p \implies q)$“ („impliziert“)
- „$(p \iff q)$“

Tabelle 1.1.: Festlegung der Wahrheitswerte

p	q	$p \wedge q$	$p \vee q$	$p \implies q$	$p \iff q$
f	f	f	f	w	w
f	w	f	w	w	f
w	f	f	w	f	f
w	w	w	w	w	w

1.2. Aussagenlogische Variable. Variablen, die den Wert w oder f annehmen.

1.3. Aussagenlogische Formel. Verknüpfung von aussagenlogischen Variablen mit (kleineren) Formeln nach obigem Muster.

1.4. Belegung. Zuordnung von w bzw. f an die einzelnen aussagenlogischen Variablen einer Funktion.

1.5. Tautologie. Aussagenlogische Formel, die für jede Belegung den Wahrheitswert w hat.

1.6. Kontradiktion. Aussagenlogische Formel, die für jede Belegung den Wahrheitswert f hat.

1.7. Wahrheitswerteverlauf. Zuordnung des Wahrheitswertes einer Formel an jede Belegung ihrer Variablen.

$(p \implies q) \iff ((\neg q) \implies (\neg p))$ hat folgenden Wahrheitswerteverlauf (wwv):

p	q	$p \implies q$	$(\neg q) \implies (\neg p)$	$(p \implies q) \iff ((\neg q) \implies (q))$
f	f	w	w	w
f	w	w	w	w
w	f	f	f	w
w	w	w	w	w

1.8. Zwei Formeln heißen **logisch äquivalent**, falls $p \iff q$ eine Tautologie ist, d. h. wenn p und q den gleichen Wahrheitswerteverlauf haben.

$$p \equiv q$$

In diesem Sinn ist $(p \implies q) \equiv ((\neg q) \implies (\neg p))$ (sogenannte Kontraposition). Auch $(p \wedge (p \implies q)) \implies q$ ist ebenfalls eine Tautologie. Eine Formel p impliziert eine Formel q, falls $p \implies q$ eine Tautologie ist. In diesem Sinne impliziert $p \wedge (p \implies q)$ die Formel q (sogenannter *Modus ponens*).

Regeln zur Verknüpfung

$$p \wedge q \equiv q \wedge p \qquad \cdots \wedge \text{ kommutativ} \qquad (1.1)$$
$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \qquad \cdots \wedge \text{ assoziativ} \qquad (1.2)$$
$$p \vee q \equiv q \vee p \qquad \cdots \vee \text{ kommutativ} \qquad (1.3)$$
$$(p \vee q) \vee r \equiv p \vee (q \vee r) \qquad \cdots \vee \text{ assoziativ} \qquad (1.4)$$
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \qquad \cdots \wedge, \vee \text{ distributiv} \qquad (1.5)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \qquad (1.6)$$

De-Morgansche Regeln:

$$\neg (p \wedge q) \equiv (\neg p) \vee (\neg q) \qquad (1.7)$$
$$\neg (p \vee q) \equiv (\neg p) \wedge (\neg q) \qquad (1.8)$$

Doppelte Negation:

$$\neg (\neg p) \equiv p \qquad (1.9)$$

Andere Schreibweisen für Implikationen und Äquivalenzen:

$$p \implies q \equiv (\neg p) \vee q \qquad (1.10)$$
$$p \iff q \equiv (p \implies q) \wedge (q \implies p) \qquad (1.11)$$

1.2. Aussageformen/Prädikate

1.9. Eine **Aussageform/ein Prädikat** über den *Universen* $U_1, \ldots, U_n$ ist ein Satz mit den Variablen $x_1, \ldots, x_n$, der bei Ersetzung von x_j durch ein Objekt aus U_j (für jedes j) stets zu einer Aussage wird.

Beispiele:

- „x ist prim“ ist eine Aussageform in der Variablen x über dem Universum U der natürlichen Zahlen.
- „$x < y$“ ist eine Aussageform in den Variablen x und y über den Universen U_1, U_2 der reellen Zahlen.
- „x ist falsch“ ist keine (wohl) keine Aussageform über dem Universum aller Sätze.

Ersetzt man in der Aussageform „$x < y$“ nur x durch eine reelle Zahl, so entsteht eine Aussageforn in der Variablen y über dem Universum U der reellen Zahlen (über $\mathbb{R}$).

1.10. Allquantor. Sei $p(x)$ Prädikat in der Variablen x über dem Universum U.
„$\forall x : p(x)$“ ist die Aussage (!) „für alle x aus U ist $p(x)$ wahr.“Ihr Wahrheitswert ist wahr, falls $p(x)$ den Wahrheitswehrt *wahr* hat für alle x aus U, und falsch, falls $p(x)$ den Wahrheitswert *falsch* hat für *mindestens* ein x aus U.

1.11. Existentialquantor. Sei $p(x)$ Prädikat in der Variablen x über dem Universum U.
„$\exists x : p(x)$“ ist die Aussage (!) „es existiert ein x aus U, für das $p(x)$ wahr ist.“Ihr Wahrheitswert ist wahr, falls $p(x)$ den Wahrheitswert *wahr* hat für mindestens ein x aus U, und falsch, falls $p(x)$ den Wahrheitswert *falsch* hat für alle x aus U.

Ist z. B. U das leere Universum (ohne Objekte), so gilt für jede Aussageform $p(x)$:

$$\forall x : p(x) \qquad w \tag{1.12}$$
$$\exists x : p(x) \qquad f \tag{1.13}$$

Ist U ein endliches Universum, etwa mit Objekten $O_1, O_2, \ldots, O_n$, so gilt:

$$\forall x : p(x) \equiv p(O_1) \wedge p(O_2) \wedge \cdots \wedge p(O_n) \tag{1.14}$$
$$\exists x : p(x) \equiv p(O_1) \vee p(O_2) \vee \cdots \vee p(O_n) \tag{1.15}$$

Daher gibt es als Alternativschreibweisen ein großes $\bigwedge$ anstelle von $\forall$ und ein großes $\bigvee$ anstelle von $\exists$.

Regeln

$$\forall x : (p(x) \wedge (q(x))) \equiv (\forall x : p(x)) \wedge (\forall x : q(x)) \tag{1.16}$$
$$\neg(\forall x : p(x)) \equiv \exists x : (\neg p(x)) \tag{1.17}$$
$$\exists x : (p(x) \vee q(x)) \equiv (\exists x : p(x)) \vee (\exists x : q(x)) \tag{1.18}$$
$$\neg(\exists x : p(x)) \equiv \forall x : (\neg p(x)) \tag{1.19}$$

Gleichartige Quantoren dürfen bei Aneinanderreihungen Vertauscht werden, jedoch nicht verschiedenartige.

Beispiel 1:

$$\forall x \exists y : x < y \text{ vs. } \exists y \forall x : x < y \tag{1.20}$$
$$\text{vs. } \exists x \forall y : x < y \tag{1.21}$$

Beispiel 2: „Jede gerade Zahl > 2 ist Summe zweier Primzahlen."

$$\forall z \exists a \exists b : z > 2 \wedge z \text{ ist gerade } \implies z = a + b \wedge a \text{ prim } \wedge b \text{ prim} \tag{1.22}$$

$$\underset{\substack{z>2\\ z|0}}{\forall} z \quad \underset{\text{ist prim}}{\exists} a \quad \underset{\text{ist prim}}{\exists} b : z = a + b \tag{1.23}$$

Alternativ kann man anstelle von „ist prim" auch sagen, dass a, b aus dem Universum der Primzahlen stammt.

Beispiel 3: Eine Funktion $f : \mathbb{R} \to \mathbb{R}$ heißt *stetig* im Punkt x_0, falls zu jedem $\varepsilon > 0$ ein $\delta > 0$ existiert mit:

$$|f(x) - f(x_0)| < \varepsilon \text{ für alle } x \text{ mit } |x - x_0| < \delta \tag{1.24}$$

Wird zu:

$$\underset{\varepsilon>0}{\forall} \varepsilon \underset{\delta>0}{\exists} \delta \forall x : |x - x_0| < \delta \implies |\, f(x) - f(x_0) \,| < \varepsilon \tag{1.25}$$

$$\underset{\varepsilon>0}{\forall} \varepsilon \underset{\delta>0}{\exists} \delta \underset{|x-x_0|<\delta}{\forall} x : |f(x) - f(x_0)| < \varepsilon \tag{1.26}$$

2. Mengen

Literaturempfehlung

- A. Doxiadis, C. Papapdimitrion, „Logicomix“, Atrium 2010

2.1. Definition der Menge nach Cantor

2.1. Eine **Menge** ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens.
Von jedem Objekt steht fest, dass es zu einer Menge gehört oder nicht.

Beispiel:

- $\{1; 2; 3; 4\}$: Menge der ganzen Zahlen von 1 bis 4.
- $\{M; A; T; H; E; I; K\}$: Menge der Buchstaben des Wortes MATHEMATIK.
- $\{A; I; E; H; K; M; T\}$: Menge der Buchstaben des Wortes MATHEMATIK.
- $\{x \in \mathbb{Z} \mid x \text{ ist Primzahl}\}$: Menge der Primzahlen (deskriptive Beschreibung)
- $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$: Menge der reellen Zahlen zwischen 0 und 1
- $[0; 1]$: Menge der reellen Zahlen zwischen 0 und 1 (Intervallschreibweise für geschlossenes Intervall)

2.2. Probleme der naiven Mengenlehre

Wunsch 0 Es gibt eine Menge.

Wunsch 1 „$x \in y$“ (d. h. x ist ein Element von y) soll Prädikat über dem Universum U aller Mengen sein, d. h. für zwei Mengen A und B soll $A \in B$ stets eine Aussage sein, also den Wahrheitswert w oder f haben.

Wunsch 2 Aussonderung mittels Aussageform: Ist $p(x)$ ein Prädikat über dem Universum aller Mengen, so soll es eine Menge geben, die aus genau denjenigen Mengen besteht, für die $p(x)$ wahr ist („Bindeglied zur natürlichen Sprache“).

Problem: Wegen Wunsch 1 ist $p(x) :=$ „$\neg(x \in x)$“ Aussageform. Wegen Wunsch 2 bilden diejenigen Mengen, für die $p(x)$ wahr ist, eine Menge, nämlich $M = \{x : p(x) \text{ wahr}\} = \{x \mid x \notin x\}$.

Frage: Ist $M \in M$?
Wäre $M \in M$, so wäre $p(M)$ wahr, folglich $M \notin M$.
Wäre $M \notin M$, so wäre $p(M)$ wahr, folglich $M \in M$.

- Nach Definition von M
- Nach Definition von $p(x)$

In beiden Fällen entsteht ein Widerspruch, also ist $M \in M$ keine Aussage, entgegen Wunsch 1 (Russelsches Paradoxon)

„Lösung“: Aussondern nur aus („gesicherten“) Mengen des Universums, nicht jedoch ganz U.

Wunsch 2' Ist A eine Menge und $p(x)$ ein Prädikat über U (wahlweise auch über A), dann soll es auch eine Menge geben, die aus genau denjenigen Mengen *aus* A besteht, für die $p(x)$ wahr ist.

$$\{x \in A : p(x) \text{ ist wahr}\} \tag{2.1}$$

Wunsch 3 Zwei Mengen sind gleich, genau dann, wenn sie die selben Elemente haben.

$$A = B \iff (\forall x : x \in A \iff x \in B) \tag{2.2}$$

Sind zum Beispiel A und B durch $p(x)$ bzw. $q(x)$ beschrieben, d. h.

$$A = \{x \in C : p(x) \text{ wahr}\}$$

und

$$B = \{x \in C : q(x) \text{ wahr}\}$$

dann gilt

$$A = B \iff (\forall x : x \in A \iff x \in B) \tag{2.3}$$

$$\iff \left(\underset{x \in C}{\forall} x : x \in A \iff x \in B\right) \tag{2.4}$$

$$\iff \underset{x \in C}{\forall} x : (p(x) \iff q(x)) \tag{2.5}$$

Wie kommt man (ausgehend von der „einen“ Menge in Wunsch 0) zu einer neuen Menge?

Wunsch 4 A heißt **Teilmenge** von B, wenn gilt:

$$\forall x : x \in A \implies x \in B \qquad \text{Schreibweise: } A \subseteq B \tag{2.6}$$

B heißt **Obermenge** von A:

$$B \supseteq A \tag{2.7}$$

Zu jeder Menge A soll es eine Menge geben, die genau aus den Teilmengen von A besteht. Diese Menge heißt **Potenzmenge** von A und wird mit $\mathfrak{P}(A)$ bezeichnet.

- X sei Menge $\implies$ $\mathfrak{P}(X)$ ist „größer“ als X
- X ist n-elementig $\implies$ $\mathfrak{P}(x)$ ist 2^n-elementig.

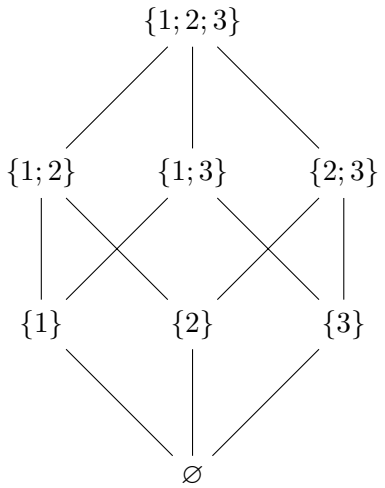
Aus den bisherigen Wünschen folgt: Es gibt eine Menge ohne Elemente, die sogenannte leere Menge $\varnothing$: Sei A irgendeine Menge (existiert nach Wunsch 0). Die Aussageform $p(x) :=$ „$x \in x \wedge x \notin x$“ ist stets falsch. Wegen Wunsch 2 ist $\{x \in A : p(x) \text{ wahr}\}$ eine Menge ohne Elemente (Wunsch 3).

Es gilt für jede Menge A: $\varnothing \subseteq A$, $\varnothing \subseteq \varnothing$, (nicht jedoch $\varnothing \in \varnothing$!)

Beispiel:

$$\mathfrak{P}(\{1;2;3\}) = \{\varnothing;\{1\};\{2\};\{3\};\{1;2\};\{1;3\};\{2;3\};\{1;2;3\}\}$$

2.2.1. Darstellung einer Potenzmenge im Hasse-Diagramm



2.3. Mengenoperation

2.2. Seien A, B Mengen.

$$p(x) := x \in B$$

ist Prädikat.
Dann ist $\{x \in A : p(x) \text{ wahr}\}$ eine Menge, die **Schnittmenge** von A und B.

$$A \cap B$$

2.3. A und B heißen **disjunkt**, falls $A \cap B = \varnothing$ ist.

2.4. Man fordert dagegen axiomatisch: Zu Mengen A und B gibt es eine Menge, die aus genau denjenigen Elementen besteht, die Elemente von A oder von B sind.
Bezeichnung: $A \cup B$

Sei A eine Menge (von Mengen).

2.5. Sei $\Cap A$ die Menge aller Mengen, die in jeder Menge aus A als Element enthalten sind.

2.6. Sei $\Cup A$ die Menge aller Mengen, die in wenigstens einer Menge aus A als Element enthalten sind.

Formal:

$$\Cap A := \{x : \forall B \in A : x \in B\} \text{ durch Aussonderung} \tag{2.8}$$
$$\Cup A := \{x : \exists B \in A : x \in B\} \text{ axiomatisch} \tag{2.9}$$

Beispiel:

$$A = \{\{1;2;3;4\},\{3;5;7\},\{3;10\}\} \tag{2.10}$$
$$\Cap A = \{3\} \tag{2.11}$$
$$\Cup A = \{1;2;3;4;5;7;10\} \tag{2.12}$$

Stets gilt: $\Cup\varnothing = \varnothing$ und $\Cap\varnothing = \varnothing$. Manchmal bleibt der Durchschnitt von $\varnothing$ auch undefiniert.

2.3.1. Regeln und Sätze

$$A \cap B = B \cap A \text{ (Kommutativität)} \tag{2.13}$$
$$A \cup B = B \cup A \tag{2.14}$$
$$A \cap (B \cap C) = (A \cap B) \cap C \text{ (Assoziativität)} \tag{2.15}$$
$$A \cup (B \cup C) = (A \cup B) \cup C \tag{2.16}$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ (wechselseitige Distributivität)} \tag{2.17}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{2.18}$$
$$\tag{2.19}$$

Beweise sind möglich über ein Venn-Diagramm[1] sowie formal über Aussagenlogik. Die Gleichheit zweier Mengen X und Y kann durch den Nachweis von $X \subseteq Y \wedge Y \subseteq X$ bewiesen werden. Im Beispiel wird ein Distributivgesetz bewiesen:

„$\subseteq$“: Sei $x \in A \cap (B \cup C)$

$$\implies x \in A \wedge x \in (B \cup C) \tag{2.20}$$
$$\implies x \in A \wedge (x \in B \vee x \in C) \tag{2.21}$$
$$\implies (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \tag{2.22}$$
$$\implies x \in (A \cap B) \vee x \in (A \cap C) \tag{2.23}$$
$$\implies x \in \big((A \cap B) \cup (A \cap C) \big) \tag{2.24}$$

Folglich gilt:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \square \tag{2.25}$$

Der Beweis geht auch in umgekehrter Reihenfolge.

2.7. Für Mengen A, B sei

$$A \setminus B := \{x \in A \mid x \notin B\} \tag{2.26}$$

die **Differenz**, gesprochen „A ohne B).“

2.8.

$$A \triangle B := (A \setminus B) \cup (B \setminus A) \tag{2.27}$$

ist die **symmetrische Differenz**.

[1] Siehe …

2.9. Sei M fest vorgegeben.
Zu $A \subseteq M$ sei das **Komplement** von A bezüglich M definiert durch:

$$\overline{A} := M \setminus A \tag{2.28}$$

Damit erhält man z. B. De-Morgansche Regeln:

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \tag{2.29}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{2.30}$$

2.4. (Geordnete) Paare und n-Tupel

2.10. Paar. Zu zwei Mengen A, B gebe es eine Menge, die genau aus den zwei Elementen A und B besteht.

Schreibweise: $\{A, B\}$ bzw. $\{A\}$ im Fall $A = B$.
Beispielsweise gilt:

$$\Cup\{A, B\} = A \cup B \tag{2.31}$$
$$\Cap\{A, B\} = A \cap B \tag{2.32}$$

2.11. Sei

$$(x, y) := \big\{ \{x\}, \{x, y\} \big\}$$

Dies definiert das **geordnete Paar** (x, y).

Es gilt: $(x, y) = (a, b) \iff x = y \wedge y = b$.
Analog dazu kann man auch Tripel, Quadrupel, Quintupel, n-Tupel definieren:

$$(a, b, c) := \big\{ a, (b, c) \big\} \tag{2.33}$$

Allen ist gemein:

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \tag{2.34}$$
$$\iff x_1 = y_1 \wedge x_1 = y_2 \wedge \cdots \wedge x_n = y_n \tag{2.35}$$
$$\iff \forall i \in \{1, \ldots, n\} : x_i = y_i \tag{2.36}$$

3. Relationen

3.1. Allgemein

3.1. Zu zwei Mengen A, B sei $A \times B = \big\{ (a, b) : a \in A, b \in B \big\}$. Eine Teilmenge $R \subseteq A \times B$ heißt **Relation** von A nach B.

Beispiel:

$$A := \{\text{Peter}, \text{Paul}, \text{Mary}\} \tag{3.1}$$
$$B := \{\text{C++}, \text{Basic}, \text{Lisp}\} \tag{3.2}$$
$$R := \big\{ (\text{Peter}, \text{C++}), (\text{Paul}, \text{C++}), (\text{Paul}, \text{Basic}), (\text{Mary}, \text{Basic}), (\text{Mary}, \text{Lisp}) \big\} \tag{3.3}$$

TODO: Graphen übernehmen

$$(x, y) \in R \quad x \text{ steht in Relation zu } y. \qquad xRy \tag{3.4}$$
$$(x, y) \notin R \quad x \text{ steht nicht in Relation zu } y. \qquad x \not R y \tag{3.5}$$

Ist $A = B$, so heißt $R \subseteq A \times A$ eine **Relation auf** A.

Allgemein gilt: Eine Teilmenge $R \subseteq A_1 \times \cdots \times A_n$ heißt *n-stellige Relation*. Alle im Folgenden betrachteten Relationen sind zweistellig (binär).

Beispiele:

(1) $R := A \times B$ ist die „All-Relation“ (alles steht in Relation zu allem).

(2) $R := \varnothing$ ist analog dazu die „Null-Relation“.

(3) “Gleichheitsrelation“ =:

$$R := = := \big\{ (a, b) \in A \times B : a = b \big\}$$

- Gleichheitsrelation
- Logisches =

(4) ...TBD

(5) ...TBD

(6) ...TBD

(7) ...TBD

(8) $\left\{ \left(x, x^2\right) : x \in \mathbb{R} \right\} \subseteq \mathbb{R} \times \mathbb{R}$ (Graph der Normalparabel). Funktionen sind damit auch (spezielle) Relationen.

(9) ...TBD

3.2. Eigenschaften von Relationen auf A

(i) R **reflexiv** : $\iff xRx$ für alle $x \in A$ (x steht in Relation zu sich selbst)

(ii) R **symmetrisch** : $\iff xRy \implies yRx$ für alle $x, y \in A$

(iii) R **antisymmetrisch** : $\iff (xRy \wedge yRx) \implies x = y$ für alle $x, y \in A$

(iv) R **transitiv** : $\iff (xRy \wedge yRz) \implies xRz$ für alle $x, y, z \in A$

(v) R **total** : $\iff xRy \vee yRx$ für alle $x, y \in A$

- R **Äquivalenzrelation** : $\iff R$ reflexiv, symmetrisch, transitiv
- R **Halbordnung** : $\iff R$ reflexiv, antisymmetrisch, transitiv
- R **Quasiordnung** : $\iff R$ reflexiv, transitiv
- R **Totalordnung** : $\iff R$ Halbordnung, total

3.2.1. Äquivalenzrelationen

3.2. $\mathscr{C} \subseteq \mathfrak{P}(A)$ heißt **Partition** von A, falls gilt:

(i) $\biguplus \mathscr{C} = A$ (jedes Element aus A ist in einer Schublade)

(ii) $\varnothing \notin \mathscr{C}$

(iii) $X \cap Y = \varnothing$ für $X \neq Y$ und $X, Y \in \mathscr{C}$ (alle sind disjunkt, daher ist wegen (i) jedes Element in genau einer Schublade)

Satz 3.1. *Sei $\sim$ eine Äquivalenzrelation auf A. Für x aus A sei*

$$[x]_{/\sim} := \{y \in A : y \sim x\}$$

die sogenannte ***Äquivalenzklasse*** *zu x bezüglich $\sim$.*
Dann ist die Menge

$$\mathscr{C}_{/\sim} := \left\{ [x]_{/\sim} : x \in A \right\}$$

eine Partition von A.

Beweis. ⚡: $\mathscr{C}_{/\sim}$ ist Partition, d. h. (i), (ii), (iii) müssen nachgewiesen werden. TBD □

Beispiel: Sei $m \in \mathbb{Z}$. Man schreibe $x \equiv y \mod m$ (x kongruent $y \mod m$), falls $m \mid x-y$ (d. h. $\exists \lambda \in \mathbb{Z} : \lambda m = x - y$ bzw. m ist Teiler von $x - y$).
$\equiv (\mod m)$ ist eine Äquivalenzrelation, denn:

- „$\equiv$ reflexiv“: Wegen

Satz 3.2. *Ist $\mathscr{C}$ eine Partition von A, so wird durch $x \sim_{\mathscr{C}} y \iff$ es gibt ein $D \in \mathscr{C}$ mit $x, y \in D$ eine Äquivalenzrelation $\sim_{\mathscr{C}}$ auf A definiert.*

Beweis.

„$\sim_{\mathscr{C}}$ reflexiv“

Wegen $\biguplus \mathscr{C} = A$ gibt es zu $x \in A$ ein $D \in \mathscr{C}$ mit $x \in D$

Folglich ist $x, x \in D$, also $x \sim_{\mathscr{C}} x$

„$\sim \mathscr{C}$ symmetrisch“

Aus $x \sim_{\mathscr{C}} y$ folgt:

$$x, y \in D \text{ für ein } D \in \mathscr{C} \tag{3.6}$$
$$\text{also: } y, x \in D \tag{3.7}$$
$$\text{folglich: } y \sim_{\mathscr{C}} x \tag{3.8}$$

„$\sim_{\mathscr{C}}$ transitiv“

Aus $x \sim_{\mathscr{C}} y$ und $y \sim_{\mathscr{C}} x$ folgt:

$$x, y \in D \text{ und } y, z \in F \text{ für geeignete Klassen } D, f \in \mathscr{C} \tag{3.9}$$

Wegen $y \in D \cap F$ folgt mit (iii):

$$D = F, \text{ also } x, z \in D \tag{3.10}$$

Also:

$$x \sim_{\mathscr{C}} z \tag{3.11}$$

□

$$\sim \mapsto \mathscr{C}_{/\sim} \tag{3.12}$$
$$\mathscr{C} \mapsto \sim_{\mathscr{C}} \tag{3.13}$$

3.2.2. Halbordnungen

Sei $\leq$ eine Halbordnung auf X (d. h. reflexiv, transitiv, antisymmetrisch). Sei $A \subseteq X$ und $b \in X$.

3.3. b heißt **minimal** in $A \iff b \in A$ und $(c \leq b \implies c = b)$ für jedes $c \in A$.

3.4. b heißt **maximal** in $A \iff b \in A$ und $(b \leq c \implies c = b)$ für alle $c \in A$.

3.5. b heißt **kleinstes** in $A \iff b \in A$ und $b \leq c$ für alle $c \in A$.

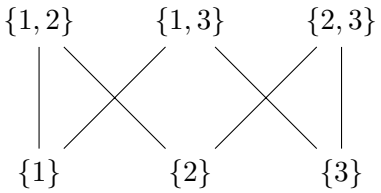
3.6. b heißt **größtes** in $A \iff b \in A$ und $c \leq b$ für alle $c \in A$.

3.7. b ist **untere Schranke** von $A \iff b \leq c$ für alle $c \in A$.

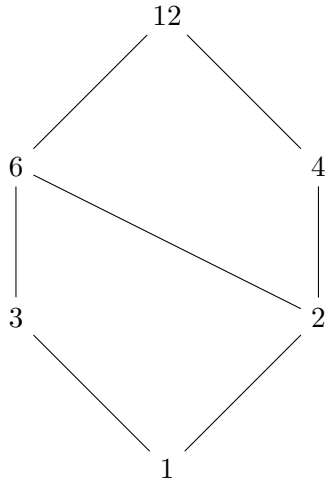
3.8. b ist **obere Schranke** von $A \iff c \leq b$ für alle $c \in A$.

Beispiel. Betrache die Halbordnung

$$\subseteq \text{ auf der Menge } \Big\{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\Big\}$$



- $\{1\},\{2\},\{3\}$ sind minimal
- es gibt keine kleinsten Elemente
- $\{1,2\},\{1,3\},\{2,3\}$ sind maximal



Teiler von 12:

- 1 ist minimal
- 1 ist kleinstes
- 12 ist maximal

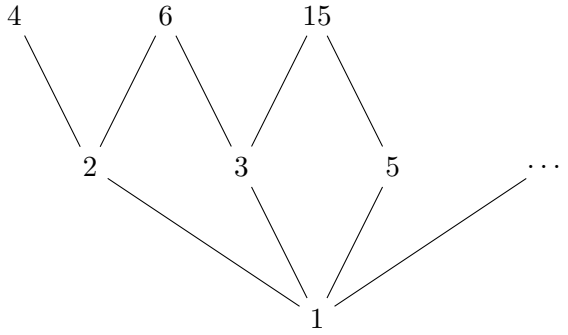
Primzahlen

- 2 ist minimal und kleinstes
- es gibt keine maximalen oder größten Elemente

Die Primzahlen > 0, mit der Teilbarkeitsordnung $|$:

- paarweise unvergleichbar bzgl. $|$

Die natürlichen Zahlen > 0, mit Teilbarkeitsordnung



Ist b ein Kleinstes in A und b' auch Kleinstes in A, so folgt:

$$b \leq b' \qquad b' \leq b$$

Also:

$$b = b'$$

Also besitzt jedes $A \subseteq X$ höchstens ein kleinstes Element. Ist b das kleinste Element von A, so gilt $b \in A$ und $b \leq c$ für alle $c \in A$. Aus $c \leq b$ für $c \in A$ folgt also $c = b$, d. h. b ist auch minimal in A.

3.9. b ist die **kleinste obere Schranke** $\iff$ b ist kleinstes Element von $\{b' : b' \text{ obere Schranke von } A\}$.
Jede Menge A besitzt höchstens eine kleinste obere Schranke; sie wird dann auch das **Supremum** von A genannt, Bezeichnung $\sup A$, aber auch $\bigvee A$.

Zum Beispiel ist für $\mathbb{R}$ mit der natürlichen Ordnung $\sup(0,1) = 1$ (Supremum des offenen Intervalls $(0,1)$). $\sup[0,1] = 1$, denn 1 ist größtes Element von $[0,1]$ und größte Elemente sind per se Suprema.

3.10. b ist die **größte untere Schranke** $\iff$ b ist größtes Element von $\{b' : b' \text{ untere Schranke von } A\}$.
Jede Menge A besitzt höchstens eine größte untere Schranke; sie wird dann auch das **Infimum** von a genannt, Bezeichnung $\inf A$ oder auch $\bigwedge A$.

Zum Beispiel ist (analog zum Supremum) für $\mathbb{R}$ mit der natürlichen Ordnung $\inf(0,1) = 0$ (Infimum des offenen Intervalls $(0,1)$).

Satz 3.3. *Sei X Menge. $\subseteq$ ist eine Halbordnung auf $\mathfrak{P}(X)$. Ist $\mathfrak{A} \subseteq \mathfrak{P}(X)$, so gilt:*

(i) $\sup \mathfrak{A} = \Cup \mathfrak{A}$

(ii) $\inf \mathfrak{A} = \Cap \mathfrak{A}$

Beweis. $B := \Cup \mathfrak{A}$ ist obere Schranke von $\mathfrak{A}$, denn für jedes $C \in \mathfrak{A}$ gilt:

$$C \subseteq \Cup \mathfrak{A}$$

denn aus $x \in C$ folgt $x \in D$ für ein $D \in \mathfrak{A}$ (nämlich $D = C$), also $x \in \Cup \mathfrak{A}$.

B ist kleinste obere Schranke von *fracA*, dann ist B' irgendeine obere Schranke von $\mathfrak{A}$, so gilt $A \subseteq B'$ für alle $A \in \mathfrak{A}$, also gilt auch $\Cup \mathfrak{A} \subseteq B'$, d. h. $B \subseteq B'$

Dies zeigt (i). Der zweite Teil folgt analog. □

Satz 3.4. | *(Teilbarkeit) ist eine Halbordnung auf $\mathbb{N}$. Dann gilt für $a, b \in \mathbb{N} \setminus \{0\}$:*

(i) $\sup\{a,b\} = \mathrm{kgV}(a,b)$ *(kleinstes gemeinsames Vielfaches)*

(ii) $\inf\{a,b\} = \mathrm{ggT}(a,b)$ *(größter gemeinsamer Teiler)*

Beweis. „(i)“: Sei $c := \sup\{a, b\}$. c ist obere Schranke von $\{a, b\}$ bezüglich der Teilbarkeit, d. h. $a \mid c$ und $b \mid c \implies c$ ist gemeinsames Vielfaches von a, b.

Sei c' weiteres gemeinsames Vielfaches von $a, b \implies a \mid c'$ und $b \mid c' \implies c'$ ist obere Schranke von $\{a, b\}$ bezüglich $|$.

$\implies c \mid c'$, weil c kleinste obere Schranke von $\{a, b\}$ ist (bezüglich $|$).

$\implies c \leq c'$

$\implies c = \text{kgV}$

„(ii)“ analog. □

3.3. Definition der Zahlen

Zu einer Menge X sei $X^+ := X \cup \{X\}$.

$$0 := \varnothing \tag{3.14}$$
$$1 := 0^+ = 0 \cup \{0\} = \varnothing \cup \{\varnothing\} = \{\varnothing\} \tag{3.15}$$
$$2 := 1^+ = 1 \cup \{1\} = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} \tag{3.16}$$
$$3 := 2^+ = 2 \cup \{2\} = \{\varnothing, \{\varnothing\}\} \cup \{\{\varnothing, \{\varnothing\}\}\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \tag{3.17}$$
$$4 := \ldots \tag{3.18}$$

- Es gilt: $0 \in 1 \in 2 \in 3 \in \ldots$
- Es gilt: $0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \ldots$

3.11. Eine Menge heißt induktiv, falls sie die $\varnothing$ Menge (als Element) enthält und mit jedem X auch X^+.

Wunsch Es gibt eine induktive Menge. Der Durchschnitt einer Menge von induktiven Mengen ist wieder induktiv. Ist nun M induktiv, dann ist

$$\mathbb{N}_M := \bigcap \{A \subseteq M : A \text{ induktiv}\} \neq \varnothing \text{ (denn } M \text{ selbst ist darin)}$$

ebenfalls induktiv.

Ist M' eine weitere induktive Menge, so ist $M' \cap M$ induktiv und Teilmenge von M. Folglich:

$$\mathbb{N}_M \overset{\text{Def. } \mathbb{N}_M}{\subseteq} M' \cap M \subseteq M' \tag{3.19}$$

Insbesondere ist

$$\mathbb{N}_M \subseteq \mathbb{N}'_M \subseteq \mathbb{N}_M \tag{3.20}$$

D. h. die Konstruktion ist unabhängig von M.

Wir können daher definieren (!):

3.12.

$$\mathbb{N} := \mathbb{N}_M \tag{3.21}$$

für beliebige induktive Menge M. $\mathbb{N}$ ist Teilmenge jeder induktiven Menge (die „kleinste“ induktive Menge).
Die Elemente von $\mathbb{N}$ heißen *natürliche Zahlen*; jede natürliche Zahl $\neq 0$ ist Nachfolger einer anderen natürlichen Zahl (d. h. zu $x \in \mathbb{N} \setminus \{0\}$ existiert ein $y \in \mathbb{N}$ mit $y^+ = x$).

Satz 3.5 (Vollständige Induktion I)**.** *Sei $p(x)$ eine Aussageform über $\mathbb{N}$. Ist $p(0)$ wahr und impliziert für jedes $n \in \mathbb{N}$ die Wahrheit von $p(n)$ auch die Wahrheit von $p(n^+)$ („$n+1$“), dann ist die Aussage $p(n)$ für jedes $n \in \mathbb{N}$ wahr.*

$$p \implies q \implies r \tag{3.22}$$

$$\text{impliziert } p \implies r \tag{3.23}$$

$$p(0) \implies p(1) \implies p(2) \implies p(3) \implies \dots \tag{3.24}$$

Beweis.

$$M := \{n \in \mathbb{N} : p(x) \text{ ist wahr}\} \tag{3.25}$$

$$M \text{ induktiv, denn enthält } 0 \text{ und mit } n \text{ auch } n^+ \tag{3.26}$$

$$\implies \mathbb{N} \subseteq M \subseteq M \tag{3.27}$$

also:

$$M = \mathbb{N} \tag{3.28}$$

□

Satz 3.6 (Anordnung der natürlichen Zahlen)**.**

(i) Für $m, n \in \mathbb{N}$ gilt: $m \in n \iff m \subseteq n \wedge m \neq n$ (Schreibweise: $\subsetneq, \subset$, „m echte Teilmenge von n“)

(ii) $\subseteq$ ist Totalordnung auf $\mathbb{N}$

(iii) Jede nichtleere Teilmenge von $\mathbb{N}$ hat ein kleinstes Element.

(Ohne Beweis; der Beweis ist eine (technische) vollständige Induktion.)

Satz 3.7 (Vollständige Induktion II)**.** *Sei $p(x)$ eine Aussageform über $\mathbb{N}$. Für jedes $n \in \mathbb{N}$ impliziere die Wahrheit von $p(x)$ für alle $x < n$ die Wahrheit von $p(x)$. Dann gilt $p(n)$ für jedes $n \in \mathbb{N}$.*

Beweis. (*Übung*) □

3.13. Man nennt eine *totale Halbordnung* eine *Wohlordnung* auf A, falls jede nichtleere Teilmenge von A ein kleinstes Element besitzt.
Z. B. ist $\mathbb{N}$ durch die natürliche Ordnung $\leq$ wohlgeordnet ($\mathbb{R}$ dagegen nicht).

Wunsch 10 Äquivalent zum Auswahlaxiom sind:

Wohlordnungssatz Jede Menge besitzt eine Wohlordnung.

Lemma 3.8 (Zorn)**.** *Besitzt jede totalgeordnete Teilmenge einer nichtleeren halbgeordneten Menge eine obere Schranke, so besitzt X ein maximales Element.*

Aus dem Zornschen Lemma folgt zum Beispiel:

- Jeder Vektorraum besitzt ein maximale linear unabhängige Menge (sog. Basic).

4. Funktionen

Alternativschreibweisen für „es existiert genau ein Element“: $\exists!$ bzw. $\exists_1$

4.1. Seien A, B Mengen. Eine Relation $f \subseteq A \times B$ heißt *Funktion* von A nach B, Schreibweise:

$$f\colon A \to B$$

falls es zu jedem $x \in A$ *genau ein* $y \in B$ mit $(x, y) \in f$ gibt, d. h.:

$$\forall x \in A : \exists y \in B : (x, y) \in f \wedge \forall z \in B : (x, z) \in f \implies z = y$$

Statt $(x, y) \in f$ (oder xfy) schreibt man gerne $f(x) = y$, bzw.: Das eindeutig zu $x \in A$ bestimmte $y \in B$ mit $(x, y) \in f$ wird mit $f(x)$ bezeichnet („f von x“).

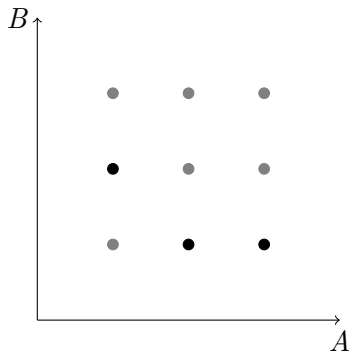


Abbildung 4.1.: Darstellung einer Funktion

- f heißt *injektiv*, falls für alle $x_1, x_2 \in A$ aus $f(x_1) = f(x_2)$ stets $x_1 = x_2$ folgt.
- f heißt *surjektiv*, falls zu jedem $y \in B$ ein $x \in A$ mit $f(x) = y$ existiert.
- f heißt *bijektiv*, falls f injektiv und surjektiv ist.
- Ein $x \in A$ mit $f(x) = y$ heißt ein *Urbild* von $y \in B$. Urbilder sind also alle x zu seinem bestimmten y.

Daraus folgt:

$$f \text{ ist injektiv} \iff \text{jedes } y \in B \text{ hat höchstens ein Urbild} \tag{4.1}$$

$$f \text{ ist surjektiv} \iff \text{jedes } y \in B \text{ hat wenigstens ein Urbild} \tag{4.2}$$

$$\implies f \text{ ist bijektiv} \iff \text{jedes } y \in B \text{ hat genau ein Urbild} \tag{4.3}$$

- Die Menge aller Urbilder von y wird mit $f^{-1}(y) \subseteq A$ bezeichnet.
- Die Menge aller Urbilder von Argumenten $z \in Y \subseteq B$ wird mit $f^{-1}(Y)$ bezeichnet (also $f^{-1}(\{y\}) = f^{-1}(y)$).

Daraus folgt:

$$f \text{ injektiv} \iff \forall y \in B : f^{-1}(y) \text{ hat höchstens ein Element} \tag{4.4}$$
$$f \text{ surjektiv} \iff \forall y \in B : f^{-1}(y) \text{ hat wenigstens ein Element} \tag{4.5}$$
$$f \text{ bijektiv} \iff \forall y \in B : f^{-1}(y) \text{ hat genau ein Element} \tag{4.6}$$

Satz 4.1. *Eine Funktion $f : A \to B$ ist genau dann bijektiv (eine Bijektion), wenn die Umkehrrelation f^{-1} (siehe Kapitel 3) eine Funktion ist. In diesem Fall ist f^{-1} auch bijektiv und heißt* Umkehrfunktion *von f.*

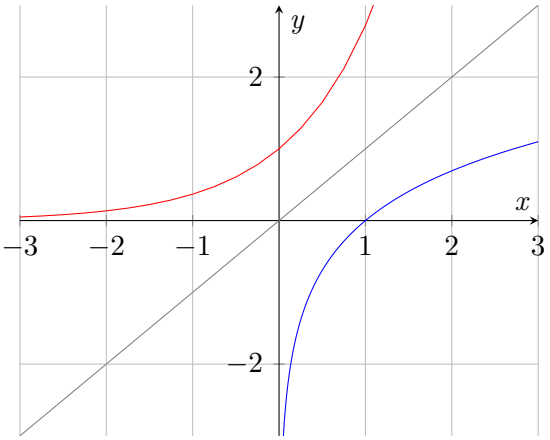


Abbildung 4.2.: Die e-Funktion (bijektiv) und ihre Umkehrfunktion (bijektiv).

Beispiel:

$$f\colon \mathbb{R} \to \mathbb{R} \qquad f(x) := x^2$$

Diese Funktion ist nicht injektiv, denn $f^{-1}(1)$ hat zwei Elemente ($\{+1, -1\}$), und nicht surjektiv, denn $f^{-1}(-1)$ hat kein Element.

Dagegen ist $f\colon \mathbb{R} \to \mathbb{R}_{\geq 0}, f(x) := x^2$, surjektiv (denn jedes $x \in \mathbb{R}_{\geq 0}$ hat ein Urbild, nämlich $\sqrt{x}$), aber nicht injektiv denn 1 hat zwei Urbilder.

$f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, f(x) := x^2$ ist injektiv und surjektiv, also bijektiv. Der Status von Injektivität und Surjektivität kann je nach Kontext auch bei gleicher Funktionsgleichung wechseln.

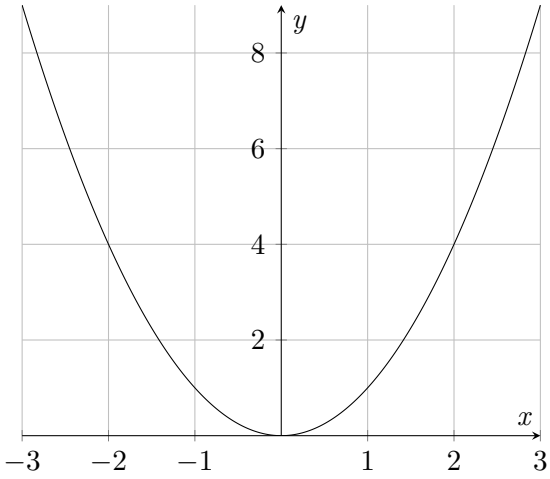


Abbildung 4.3.: Die Normalparabel $f\colon \mathbb{R} \to \mathbb{R}, f(x) = x^2$

Beispiel: Sei A Menge $\neq \varnothing$, $\mathfrak{P}(A)$ ihre Potenzmenge. Dann ist:[1]

$$f\colon \mathfrak{P}(x) \times \mathfrak{P}(A) \to \mathfrak{P}(A) \qquad f((X, Y)) := X \cap Y$$

- f ist immer surjektiv, denn für $Z \in \mathfrak{P}(A)$ ist $f((Z, Z)) = Z \cap Z = Z$, also ist (Z, Z) ein Urbild von Z.
- f ist nicht injektiv, denn (für $Z \neq A$) (Z, A) ist ein weiteres Urbild von Z, denn $f((Z, A)) = Z \cap A = Z$.

Konkret: $A = \{1, 2, 3\}$, dann ist z. B.:

$$f^{-1}(\{1,2,3\}) = \{(X, Y) \in \mathfrak{P}(A) \times \mathfrak{P}(A) : X \cap Y = \{1,2\}\} \tag{4.7}$$

$$= \Big\{\big(\{1,2\},\{1,2\}\big), \big(\{1,2\},\{1,2,3\}\big), \big(\{1,2,3\},\{1,2\}\big)\Big\} \tag{4.8}$$

Zurück zum Allgemeinen:

> **4.2.** Ist $f\colon A \to B$ eine Funktion, so heißt $f(x)$ das *Bild* von x unter f. Für $X \subseteq A$ heißt $f(X) := \{f(x) : x \in X\}$ das *Bild* (oder auch *Bildmenge*) von X unter f.

Damit gilt beispielsweise: $f(\{x\}) = \{f(x)\}$.

Satz 4.2. *Zwei Funktionen $f\colon A \to B$, $g : A \to B$ sind genau dann gleich, wenn gilt:*

$$\forall x \in A : f(x) = g(x) \tag{4.9}$$

[1] $\mathfrak{P}(A) \times \mathfrak{P}(A)$ ist Menge aller Paare von Teilmengen von A

4.3. Seien $f : A \to B$ und $g : B \to C$ Funktionen. Dann wird durch $g \circ f : A \to C, (g \circ f)(x) := g(f(x))$ (für $x \in A$)[a] eine Funktion $g \circ f$ definiert, die sogenannte Hintereinanderschaltung/Konkatenation/Verkopplung/Verkullerung/Verkettung/….

[a] „g Kuller f“, „g nach f“

Satz 4.3. *$f : A \to B, g : B \to C$ seien bijektive Funktionen. Dann ist $g \circ f : A \to C$ bijektiv.*

Beweis.

„$g \circ f$ injektiv“:

$$\text{Seien } x \neq x' \in A \overset{f \text{ injektiv}}{\Longrightarrow} f(x) \neq f(x') \tag{4.10}$$

$$\overset{g \text{ injektiv}}{\Longrightarrow} g(f(x)) \neq g(f(x')) \tag{4.11}$$

$$\Longrightarrow (g \circ f)(x) \neq (g \circ f)(x') \quad \checkmark \tag{4.12}$$

„$g \circ f$ surjektiv“:

$$\text{Zu } z \in C \text{ existiert ein } y \in B \text{ mit } g(y) = z \text{ (denn: } g \text{ ist surjektiv)} \tag{4.13}$$

$$\text{Zu } y \in B \text{ existiert ein } x \in A \text{ mit } f(x) = y \text{ (denn: } f \text{ ist surjektiv)} \tag{4.14}$$

$$\Longrightarrow (g \circ f)(x) = g(f(x)) = g(y) = z \tag{4.15}$$

□

4.4. Eine Funktion f ist eine Injektion, falls sie injektiv ist.

4.5. Eine Funktion f ist eine Surjektion, falls sie surjektiv ist.

4.6. Eine Funktion f ist eine Bijektion, falls sie bijektiv ist.

Für zwei Mengen A und B wird definiert:

- A ist höchstens so mächtig wie B, falls eine Injektion von A nach B existiert.

$$|A| \leq |B|$$

- A ist gleichmächtig zu B, falls eine Bijektion von A nach B existiert.

$$|A| = |B|$$

Durch $|\cdot| \leq |\cdot|$ wird eine Quasiordnung (auf jeder Menge irgendwelcher Mengen) definiert.

„reflexiv“:

$$|A| \leq |A|, \text{ denn } f\colon A \to A, f(x) := x \text{ ist Injektion} \tag{4.16}$$

f heißt auch Identität auf A, Bezeichnung id_A.

„transitiv“:

$$\text{Aus } |A| \leq |B| \text{ und } |B| \leq |C| \text{ folgt:} \tag{4.17}$$
$$\text{Es gibt Injektionen } f\colon A \to B \text{ und } g : B \to C \tag{4.18}$$
$$\implies g \circ f\colon A \to C \text{ Injektion } (\textbf{??}) \tag{4.19}$$

Durch $|\,.\,| = |\,.\,|$ wird eine Äquivalenzrelation (auf jeder Menge irgendwelcher Mengen) definiert.

„reflexiv“:

$$|A| = |A|, \text{ denn } id_A \text{ ist Bijektion.} \tag{4.20}$$

„transitiv“:

$$\text{Aus } |A| = |B| \text{ und } |B| = |C| \text{ folgt:} \tag{4.21}$$
$$\text{Es gibt Bijektionen } f\colon A \to B \text{ und } g : B \to C \tag{4.22}$$
$$\implies g \circ f\colon A \to C \text{ Bijektion } (\textbf{??}) \tag{4.23}$$
$$\implies |A| = |C| \tag{4.24}$$

„symmetrisch“:

$$\text{Aus } |A| = |B| \text{ folgt:} \tag{4.25}$$
$$\text{Es gibt eine Bijektion } f\colon A \to B \tag{4.26}$$
$$\implies f^{-1} : B \to A \text{ Bijektion} \tag{4.27}$$
$$\implies |B| = |A| \tag{4.28}$$

4.7. Eine Menge heißt *Ordinalzahl*, falls $\in$ transitiv auf ihr selber und jeder ihrer Elemente ist.

Beispiel: Jedes $n \in \mathbb{N}$ ist Ordinalzahl.

4.8. Die kleinste zu einer Menge X gleichmächtige Ordinalzahl heißt *Kardinalzahl* bzw. *Kardinalität* von X. Bezeichnung:

$$|X|$$

4.9. Eine Menge X heißt *endlich*, falls sie gleichmächtig zu einer natürlichen Zahl ist.

4.10. Eine Menge X heißt *abzählbar* (bzw. *höchstens abzählbar*), falls sie höchstens so mächtig wie die natürlichen Zahlen $\mathbb{N}$ ist. Insbesondere sind endliche Mengen abzählbar, d. h.

$$|X| \leq |\mathbb{N}|$$

4.11. Eine Menge X heißt *überabzählbar*, falls

$$|X| \not\leq |\mathbb{N}|$$

Ist zum Beispiel $\mathbb{Z}$ die Menge der ganzen Zahlen und $G = \{x \in \mathbb{Z} : 2 \mid x\}$ die Menge der geraden Zahlen, so ist $|G| = |\mathbb{Z}|$ (nicht: „$|G| < |\mathbb{Z}|$“).

Beweis.

$$f\colon \mathbb{Z} \to G, f(x) := 2x \text{ ist bijektiv} \tag{4.29}$$

„f injektiv“:

$$f(x) = f(y) \tag{4.30}$$
$$2x = 2y, \text{ also} \tag{4.31}$$
$$x = y \ \checkmark \tag{4.32}$$

„f surjektiv“:

$$\text{Ist } y \in G, \text{ so} \tag{4.33}$$
$$2 \mid y, \text{ also} \tag{4.34}$$
$$y = 2\lambda \text{ für ein } \lambda \in \mathbb{Z} \tag{4.35}$$
$$\Longrightarrow f(\lambda) = 2\lambda = y \tag{4.36}$$

□

Außerdem: $|\mathbb{Z}| = |\mathbb{N}|$.

4.12. Eine Menge X heißt DEDEKIND-endlich, falls es keine Injektion von X in eine echte Teilmenge von X gibt.

Beispiel:

- Hotel mit 8 Zimmer, alle belegt.
- Ein neuer Gast kommt, ich kann ihn nicht unterbringen

Hilberts Hotel:

- Hotel mit $|\mathbb{N}|$ Zimmern, alle belegt
- Ein neuer Gast kommt, ich kann ihn unterbringen:
  - Der Gast aus Zimmer i zieht nach Zimmer $i+1$, so wird Zimmer 0 frei.
- Abzählbar viele Gäste kommen, ich kann sie unterbringen:
  - Der Gast in Zimmer i zieht nach Zimmer $2i+1$
  - dadurch werden die geraden Zimmer frei

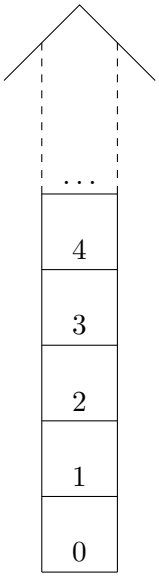


Abbildung 4.4.: Hilberts Hotel

4.13. Eine Relation $R \subseteq A \times B$ heißt *Matching* von A nach B, falls zu jeden $a \in A$ höchstens ein $b \in B$ mit $(a, b) \in R$ existiert und zu jedem $b \in B$ höchstens ein $a \in A$ mit $(a, b) \in R$ existiert.

Satz 4.4. *Für zwei Mengen A, B gilt: $|A| \leq |B|$ oder $|B| \leq |A|$.*

Beweis. Die Menge M aller Matchings von A nach B ist durch $\subseteq$ halbgeordnet.

Wir suchen bezüglich $\subseteq$ ein maximales Matching. Dieses existiert in Folge des ZORNschen Lemmas (Satz 3.8).

$\lightning$: Jede totalgeordnete Teilmenge K von M hat eine obere Schranke.

$\biguplus K$ ist kleinste obere Schranke von K bzgl. $\subseteq$

(4.37)

Frage: ist $\biguplus K$ ein Matching?

Angenommen (reductio ad absurdum), dass nicht …

$$\text{Dann } \exists a \in A \text{ und zwei verschiedene } b, b' \in B \text{ mit} \tag{4.38}$$
$$(a, b), (a, b') \in \biguplus K \tag{4.39}$$
$$\text{oder aber } \exists b \in B \text{ und zwei verschiedene } a, a' \in B \text{ mit} \tag{4.40}$$
$$(a, b), (a', b) \in \biguplus K \tag{4.41}$$

O. B. d. A. tritt Ersteres ein.

$$\text{Zu } (a, b)\, \exists R \in K : (a, b) \in R \tag{4.42}$$
$$\text{Weil } K \text{ geordnet ist, gilt } R \subseteq R' \vee R' \subseteq R \tag{4.43}$$
$$\implies (a, b), (a, b') \in R \text{ oder } \in R' \tag{4.44}$$
$$\implies R \text{ oder } R' \text{ kein Matching } \lightning \tag{4.45}$$

Folglich ist $\biguplus K$ ein Matching. Also gelten die Vorraussetzungen des ZORNschen Lemmas.

Also enthält M ein maximales Matching, etwa M.

(4.46)

Fall 1: Zu jeden $a \in A$ gibt es exakt ein $b \in B$ mit $(a, b) \in M'$. Dann ist M' eine Funktion von A nach B und sogar Injektion (weil Matching). $\implies |A| \leq |B|$.

Fall 2: Zu jedem $b \in B$ gibt es exakt ein $a \in A$ mit $(a, b) \in M'$. Dann ist die Umkehrrelation M'^{-1} eine Funktion von B nach A und injektiv. $\Longrightarrow$ $|B| \leq |A|$.

Tritt weder Fall 1 noch Fall 2 ein, so gibt es ein $a \in A$ mit $(a, b') \notin M \, \forall b' \in B$ und es gibt ein $b \in B$ mit $(a', b) \notin M' \, \forall a' \in A$.

Daraus folgt:

$$M' \cup \{(a, b)\} \text{ ist ein Matching,} \tag{4.47}$$

$$\text{jedoch } M' \supset M', \text{ im Widerspruch zur Maximalität von } M' \text{ (in } M) \tag{4.48}$$

□

Satz 4.5 (Cantor). *Für jede Menge X gilt:*

$$|X| < |\mathfrak{P}(X)| \tag{4.49}$$

d. h.

$$|X| \leq |\mathfrak{P}(X)| \tag{4.50}$$

und

$$|X| \neq |\mathfrak{P}(X)| \tag{4.51}$$

Beweis. (Übungen) □

Satz 4.6 (Cantor/Schröder/Bernstein). *Sind A und B Mengen mit $|A| \leq |B|$ und $|B| \leq |A|$, so ist $|A| = |B|$.*

Beweis. Seien zunächst A und B disjunkt (d. h. $A \cap B = \varnothing$).

Nach Vorraussetzung existieren Injektionen $f : A \to B$, $g : B \to A$.

Man betrachte $f \cup g$ (als Netzwerk) (siehe Abbildung 4.5).

- f und g
- Aus $x \in A$ weist genau ein roter Pfeil fort
- Auf $y \in B$ weist höchstens ein roter Pfeil zu
- Aus $y \in B$ weist genau ein blauer Pfeil fort
- Auf $x \in A$ weist höchstens ein blauer Pfeil zu

Die „Komponenten“ von $f \cup g$ sind …

… einseitig unendliche Strahlen (beginnend in A oder B)

… zweiseitig unendliche Strahlen

… Kreise gerader Länge

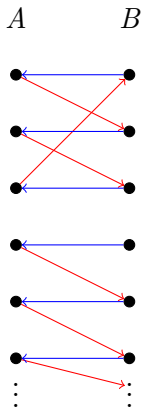


Abbildung 4.5.: Darstellung der Injektionen f und g. Der obere Teil der Punkte zeigt einen Kreis gerader Länge, der untere Teil einen unendlichen Strahl.

Das Netzwerk $f \cup g$ „zerfällt“ in derartige Teile.

Sei A' die Menge der $a \in A$, die nicht auf einem in B beginnenden unendlichen Strahl liegen. Man setze $h(a) = f(a)$ für jedes derartige $a \in A'$ und $h(c) := g^{-1}(c)$ für jedes $c \in A \setminus A'$, wobei $g^{-1}(c)$ das eindeutig bestimmte Urbild von c unter g sei.

Somit ist $h : A \to B$ eine Bijektion. Folglich: $|A| = |B|$ ✓

Im allgemeinen Fall betrachte man

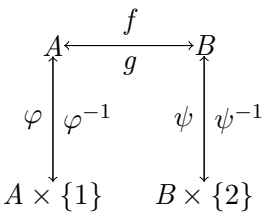
$$\varphi : A \to A \times \{1\}, \qquad \varphi(a) := (a, 1) \tag{4.52}$$

$$\text{und } \psi : B \to B \times \{2\}, \qquad \psi(b) := (b, 2) \tag{4.53}$$

φ und ψ sind Bijektionen, $A \times \{1\}$ und $B \times \{2\}$ sind disjunkt.

φ ist injektiv, denn für $x \neq y$ ist $\varphi(x) = (x, 1) \neq (y, 1) = \varphi(y)$, φ ist surjektiv, denn für $(a, 1) \in A \times \{1\}$ ist $\varphi(a) = (a, 1)$.

Nach Vorraussetzung existieren Injektionen $f : A \to B$ und $g : B \to A$.



- $\psi \circ f \circ \varphi^{-1} : A \times \{1\} \to B \times \{2\}$ ist injektiv
- $\varphi \circ g \circ \psi^{-1} : B \times \{2\} \to A \times \{1\}$ ist injektiv

Folglich gibt es eine Bijektion $h : A \times \{1\} \to B \times \{2\}$ (nach erstem Teil des Beweises). $\psi^{-1} \circ h \circ \varphi : A \to B$ ist folglich eine Bijektion $\implies |A| = |B|$. □

4.1. Mengenfamilien

4.14. Seien M (Grundmenge) und I (Indexmenge) Mengen. Eine Funktion $f\colon I \to M$ heißt auch *Familie* (über M mit Indexmenge I).

$$(f_i)_{i\in I}$$

wobei $f_i = f(i)$.
Ist $I = \{1, 2, \dots, n\}$, so schreibt man auch $(f_1, f_2, \dots, f_n)$ statt $(f_i)_{i\in\{1,\dots,n\}}$.

Beispiel: $(A_i)_{i\in\{1,2,3\}}$ mit $A_1 := \varnothing, A_2 := \varnothing, A_3 := \{17, 18\}$ definiert eine „Mengenfamilie“ mit Indexmenge $\{1, 2, 3\}$, nämlich $(\varnothing, \varnothing, \{17, 18\})$.

4.15. Eine Familie über M mit Indexmenge $\mathbb{N}$ heißt auch *Folge* über M.
Schreibweise:

$$(a_0, a_1, a_2, \dots,)$$

Beispielsweise wird durch $a_i := 2i$ mit $i \in \mathbb{N}$ die Folge der geraden natürlichen Zahlen definiert $((0, 2, 4, 6, \dots))$.

4.16. Für eine Mengenfamilie $(A_i)_{i\in I}$ mit Indexmenge I sei

$$\prod_{i\in I} A_i = \Big\{ f\colon I \to \Cup\{A : i \in I\} : f(i) \in A_i \Big\} \tag{4.54}$$

das *Produkt* von $(A_i)_{i\in I}$.

Die Elemente von $\prod_{i\in I} A_i$ sind folglich Familien $(f_i)_{i\in I}$ mit $f(i) \in A_i$.

Beispiele

- $I = \{1, 2, 3\},\ A_i := \mathbb{R}$, dann ist $\displaystyle\prod_{i\in I} A_i = \Big\{(x_1, x_2, x_3) : x_1, x_2, x_3 \in \mathbb{R}\Big\}$
- $I = \mathbb{N},\ A_i := \mathbb{Q}$, dann ist $\displaystyle\prod_{i\in I} A_i = \Big\{(a_0, a_1, \dots) : a_i \in \mathbb{Q} \quad \forall i \in \mathbb{N}\Big\}$

Ist $(A_i)_{i\in I}$ konstant, etwa $A_i = A$ für alle $i \in I$, so schreibt man anstelle von $\prod_{i\in I} A_i$:

$$A^I$$

So zum Beispiel $\mathbb{R}^{\{1,2,3\}}$ statt $\prod_{i\in\{1,2,3\}} \mathbb{R}$ bzw. $\mathbb{R}^3$ oder auch $\mathbb{Q}^{\mathbb{N}}$ für die Menge aller rationalen Folgen.
A^I ist daher die Menge aller Abbildungen von I nach A.
Im Fall $I = \{1, 2, 3, \dots, n\}$ schreibt man auch anstelle von $\prod_{i\in\{1,2,\dots,n\}} A_i$:

$$A_1 \times A_2 \times A_3 \times \cdots \times A_n$$

5. Gruppen / Ringe / Körper

5.1. Eine *Operation* auf einer Menge A ist eine Funktion $f : A \times A \to A$. Schreibweise: xfy statt $f(x, y)$.

Statt f schreibt man meist $+, \cdot, -, /, \circ, \times, \%, :, \heartsuit, \ldots$.

5.2. Eine Menge G mit einer Operation $\cdot$ heißt *Gruppe*, falls gilt:

(i) $\forall a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ($\cdot$ assoziativ)

(ii) $\exists e \in G : \forall a \in G : e \cdot a = a \cdot e = a$. Dadurch ist e eindeutig bestimmt. Ist $e' \in G$ mit $\forall a \in G : e' \cdot a = a \cdot e' = a$, so gilt $e' = e' \cdot e = e$. e heißt *neutral* und wird gerne mit 1 bezeichnet.

(iii) $\forall a \in G \exists b \in G : a \cdot b = b \cdot a = e$ (wobei e das neutrale Element aus (ii) sei). Auch b ist hierdurch eindeutig bestimmt: Gilt auch für b' : $a \cdot b' = b' \cdot a = e$, so folgt: $b \overset{(ii)}{=} b \cdot e = b \cdot (a \cdot b') \overset{(i)}{=} (b \cdot a) \cdot b' = e \cdot b' \overset{(ii)}{=} b'$. b heißt *invers* zu a, Schreibweise: a^{-1} (also $a \cdot a^{-1} = a^{-1} \cdot a = 1$).

Multiplikative Schreibweise: Operationen $\cdot$ oder ähnlich.

$$1, a^{-1}$$

Additive Schreibweise: Operationen $+$ oder ähnlich.

$$0, -a$$

Die Bedingungen (i), (ii), (iii) lauten dann:

(i) $\forall a, b, c \in G : a + (b + c) = (a + b) + c$

(ii) $\exists 0 \in G \forall a \in G : a + 0 = 0 + a = a$

(iii) $\forall a \in G \exists -a \in G : a + (-a) = -a + a = 0$

Achtung: Es wird nicht verlangt, dass $\forall a, b \in G : a \cdot b = b \cdot a$.

5.3. Eine Gruppe G heißt *abelsch* oder *kommutativ*, falls gilt:

$$\forall a, b \in G : a \cdot b = b \cdot a$$

Solche Gruppen werden meist additiv $(+, 0, -a)$ notiert.

Beispiel: Sei X Menge, S_X sei die Menge aller Bijektionen von X nach X (siehe Abbildung 5.1), die sogenannten *Permutationen* von X. S_X ist eine Gruppe mit $\circ$ (Konkatenation, s. o.), denn: Die Konkatenation von Permutationen von X ist wieder eine solche (siehe **??**), denn:

(i) $\forall f, g, h \in S_X : f \circ (g \circ h) = (f \circ g) \circ h$

Beweis. Für jedes $x \in X$ ist
$(f \circ (g \circ h))(x) \overset{\text{Def.}}{=} f((g \circ h)(x)) \overset{\text{Def.}}{=} f(g(h(x)))$ und
$((f \circ g) \circ h)(x) \overset{\text{Def.}}{=} (f \circ g)(h(x)) = f(g(h(x)))$ □

(ii) Die Funktion $id_X : X \to X, id_X(x) := x$ ist neutral bezüglich $\circ$.

Beweis. Für jedes $x \in X$ und $f \in S_X$ gilt: $(f \circ id_X)(x) \overset{\text{Def.}}{=} f(id_X(x)) \overset{\text{Def.}}{=} f(x)$ und $(id_X \circ f)(x) \overset{\text{Def.}}{=} id_X(f(x)) \overset{\text{Def.}}{=} f(x)$, also $f \circ id_X = f$ und $id_X \circ f = f$ □

(iii) Zu $f \in S_X$ ist $f^{-1} \in S_X$ die Inverse zu f bezügich $\circ$.

Beweis. Für $x \in X$ betrachte $\left(f \circ f^{-1}\right)(x) \overset{\text{Def.}}{=} f\left(f^{-1}(x)\right) = f(y)$, wobei y das (einzige) Urbild von x unter f ist. Folglich gilt $f(y) = x$, also $\left(f \circ f^{-1}\right)(x) = x$.
Ähnlich zeigt man: $\left(f^{-1} \circ f\right)(x) = x$. Also: $f \circ f^{-1} = id_X$ und $f^{-1} \circ f = id_X$. □

Beispiel:

- $X = \{1, \ldots, 5\}$
- Abbildung 5.2
- ...

Insbesondere gilt:

$$f \circ g \neq g \circ f$$

Folglich ist die Gruppe $S_{\{1,\ldots,5\}}$ mit $\circ$ nicht abelsch.

Für allgemeines X und $a_1, \ldots, a_n$ paarweise verschiedene Elemente aus X definiere: $f : X \to X$ durch:

$$f(x) = \begin{cases} a_{n+1} & \text{, falls } x = a_j \text{ für ein } j \in \{1, \ldots, n-1\} \\ a_1 & \text{, falls } x = a_n \\ x & \text{, sonst} \end{cases}$$

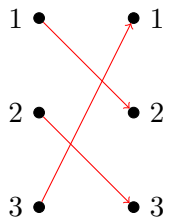


Abbildung 5.1.: Eine Bijektion von X nach X.

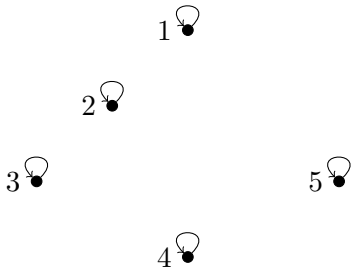


Abbildung 5.2.: Identität id_X

Abbildung 5.3.: TBD Verkopplung von Funktionen

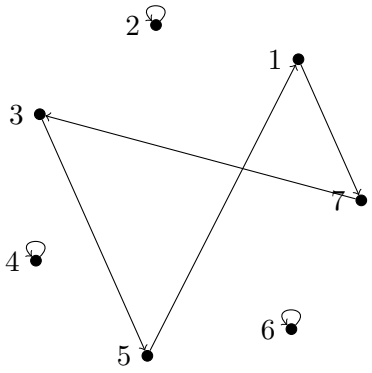


Abbildung 5.4.: Beispiel einer Funktion $f\colon X \to X$

Siehe dazu Abbildung 5.4. f wird bezeichnet durch $(a_1, \ldots, a_n)$ oder auch $(a_1 \ldots a_n)$. Zum Beispiel[1]: $f = (1\,5\,2) \circ (3\,4)\,; g = (1\,5\,4\,2)$

$$f \circ g = (1\,5\,2) \circ (3\,4) \circ (1\,5\,4\,2) \tag{5.1}$$
$$= (1\,2\,5\,3\,4) \tag{5.2}$$

Tabellarische Schreibweise: Für $f \in S_{\{1,\ldots,n\}}$ schreibe:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix} \tag{5.3}$$

z. B.:
$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \tag{5.4}$$

Beispiel:

$$(1\,2\,3) \circ (1\,2) = (1\,3) \circ (2) \tag{5.5}$$
$$= (1\,3) \tag{5.6}$$
$$(1\,2) \circ (1\,2\,3) = (1) \circ (2\,3) \tag{5.7}$$
$$= (2\,3) \tag{5.8}$$
$$(1\,3) \neq (2\,3) \tag{5.9}$$

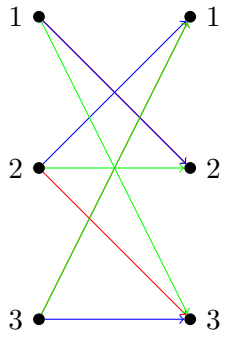


Abbildung 5.5.: Verkullerung von f und g zu $f \circ g$.

5.4. $H \subseteq G$ ist *Untergruppe* der Gruppe G mit $\cdot$, falls gilt:

(i) $1 \in H$ (alternativ: $H \neq \varnothing$)

(ii) $\forall a, b \in H : a \cdot B \in H$ (Abschlusseigenschaft)

(iii) $\forall a \in H : a^{-1} \in H$ (Abschlusseigenschaft)

(Äquivalent: $\cdot$ „eingeschränkt“ auf H ist Operation auf H und H mit dem eingeschränkten $\cdot$ ist eine Gruppe)

[1] Siehe dazu Abbildung 5.3

Nur, weil er kein $\mathfrak{H}$ zeichnen kann...

Der Durchschnitt irgendwelcher Untergruppen von G ist eine Untergruppe von G. Sei $\heartsuit$ eine Menge von Untergruppen von G.
Zeige $\Cap\heartsuit$ ist Untergruppe von G.

„(i)“:

$$\text{Es ist } 1 \in H \text{ für jedes } H \in \heartsuit, \text{ also } 1 \in \Cap\heartsuit \tag{5.10}$$

„(ii)“:

$$\text{Für } a, b \in \Cap\heartsuit \text{ folgt :} \tag{5.11}$$
$$\forall H \in \heartsuit : a, b \in H \tag{5.12}$$
$$\text{also } \forall H \in \heartsuit : a \cdot b \in H \tag{5.13}$$
$$\text{also } a \cdot b \in \Cap\heartsuit \tag{5.14}$$

„(iii)“:

$$\text{Für } a \in \Cap\heartsuit \text{ folgt } a \in H \text{ für jedes } H \in \heartsuit \tag{5.15}$$
$$\text{also } \forall H \in \heartsuit : a^{-1} \in H \tag{5.16}$$
$$\text{also } a^{-1} \in \Cap\heartsuit \quad \square \tag{5.17}$$

20. 11. 2018 bei Samuel Mohr

Satz 5.1. *Ist $\mathfrak{H}$ eine Menge von Untergruppen, so auch $\Cap\mathfrak{H}$.*

Folgerung: Für $A \subseteq G$, $(G, \cdot)$ Gruppe, ist

$$\langle A \rangle_G := \Cap \{H \subseteq G : A \subseteq H\}$$

eine Untergruppe.

> **5.5.** Gegeben sind G, H Gruppen mit $\cdot_G$, $\cdot_H$, sowie $\varphi : G \to H$ Abbildung. Falls $\forall a, b \in G : \varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$, dann ist φ *Homomorphismus* zwischen G und H.

Es ist also egal, ob die Operation zunächst in G und dann in H oder umgekehrt ausgeführt wird.[2]

Satz 5.2. *Sei $\varphi : G \to H$ Homomorphismus zwischen G und H mit $\cdot_G, \cdot_H$. Dann*

(1) $\varphi(1_G) = 1_H$

(2) $\forall a \in G : (\varphi(a))^{-1} = \varphi\left(a^{-1}\right)$

[2] Siehe dazu Abbildung 5.6

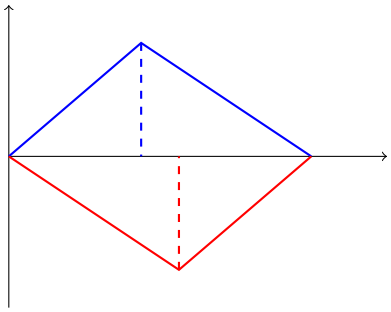


Abbildung 5.6.: Ein Homomorphismus

Beweis.

„1“:

$$\begin{aligned} \varphi(1_G) &= \varphi(1_G \cdot 1_G) && (5.18)\\ &= \varphi(1_G) \cdot \varphi(1_G) && (5.19)\\ \Longrightarrow\ 1_H \cdot \varphi(1_G) &= \varphi(1_G) \cdot \varphi(1_G) && (5.20)\\ &= 1_H \cdot 1_H && (5.21)\\ &= 1_H\ \checkmark && (5.22) \end{aligned}$$

„2“:

$$\begin{aligned} \varphi(a) \cdot \varphi\left(a^{-1}\right) &= \varphi\left(a \cdot a^{-1}\right) && (5.23)\\ &= \varphi(1_G) = 1_H && (5.24)\\ \varphi\left(a^{-1}\right) \cdot \varphi(a) &= \varphi\left(a^{-1} \cdot a\right) && (5.25)\\ &= \varphi(1_G) = 1_H && (5.26)\\ \Longrightarrow\quad \text{also ist}\ \ (\varphi(a))^{-1} &= \varphi\left(a^{-1}\right) && (5.27) \end{aligned}$$

□

Satz 5.3. *$\varphi : G \to H$ Homomorphismus zur $(G, \cdot_G)$ und $(H, \cdot_H)$. Dann ist*

(1) $\varphi(G) := \{\varphi(x) : x \in G\} \leq H$

(2) *Kern* $\varphi := \{x \in G : \varphi(x) := 1_H\} \leq G$

(3) *φ injektiv* $\iff$ *Kern* $\varphi = \{1_G\}$

Beweis.

„1“:

$$\bullet\ 1_H \in \varphi(G), \text{ da vorheriger Satz (1)} \tag{5.28}$$
$$\bullet \text{ ist } a, b \in \varphi(G), \text{ etwa} \tag{5.29}$$
$$a = \varphi(x), b = \varphi(y) \text{ für geeignete } x, y \in G \tag{5.30}$$
$$\Longrightarrow\ a \cdot b = \varphi(x) \cdot \varphi(y) \tag{5.31}$$
$$= \varphi(x \cdot y) \in \varphi(G) \tag{5.32}$$
$$\bullet \text{ ist } a \in \varphi(G), \text{ etwa } a = \varphi(x), \text{ so} \tag{5.33}$$
$$a^{-1} = \varphi(x^{-1}) \in \varphi(G) \tag{5.34}$$

„2“:

$$\bullet\ 1_G \in \text{ Kern } \varphi, \text{ da } \varphi(1_G) = 1_H \tag{5.35}$$
$$\bullet \text{ Sind } a, b \in \text{ Kern } \varphi, \text{ so ist} \tag{5.36}$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \tag{5.37}$$
$$\overset{\text{Def.}}{=} 1_H \cdot 1_H = 1_H, \tag{5.38}$$
$$\text{also } a \cdot b \in \text{ Kern } \varphi \tag{5.39}$$
$$\bullet \text{ und } \varphi(a^{-1}) = (\varphi(a))^{-1} \tag{5.40}$$
$$= 1_H^{-1} = 1_H \tag{5.41}$$
$$\text{also } a^{-1} \in \text{ Kern } \varphi \tag{5.42}$$

„3“:

„$\rightarrow$“:

$$\text{Sei } \varphi \text{ injektiv und } x \in \text{ Kern } \varphi \tag{5.43}$$
$$\Longrightarrow\ \varphi(x) = 1_H, \text{ außerdem } \varphi(1_G) = 1_H \tag{5.44}$$
$$\Longrightarrow\ x = 1_G \tag{5.45}$$
$$\Longrightarrow\ \text{Kern } \varphi = \{1_G\} \tag{5.46}$$

„$\leftarrow$“:

$$\text{Sei Kern } \varphi = \{1_G\} \text{ und } x, y \in G \text{ mit } \varphi(x) = \varphi(y) \tag{5.47}$$
$$\Longrightarrow\ \varphi(x) \cdot (\varphi(y))^{-1} = \varphi(x) \cdot (\varphi(x))^{-1} \tag{5.48}$$
$$= 1_H \tag{5.49}$$
$$\text{und } \varphi(x) \cdot (\varphi(y))^{-1} = \varphi(x) \cdot \varphi(y^{-1}) \tag{5.50}$$
$$= \varphi\left(x \cdot y^{-1}\right) \tag{5.51}$$
$$\Longrightarrow\ x \cdot y^{-1} \in \text{ Kern } \varphi \tag{5.52}$$
$$\Longrightarrow\ x \cdot y^{-1} = 1_G \tag{5.53}$$
$$\Longrightarrow\ x = y \tag{5.54}$$

□

5.1. Isomorphismen

5.6. Ein *Isomorphismus* zwischen Gruppen $(G, \cdot_G)$ und $(H, \cdot_H)$ ist ein bijektiver Homomorphismus. G, H heißen *isomorph* ($G \cong H$), falls es einen Isomorphismus zwischen G und H gibt.

Bis auf den Namen der Elemente sind die Gruppen also gleich.
$\cong$ ist eine Äquivalenzrelation.

Beweis.

„reflexiv“:

$$G \cong G, \text{ da } id_G \text{ Isomorphismus } \checkmark \tag{5.55}$$

„symmetrisch“:

$$G \cong H \tag{5.56}$$
$$\implies \exists \varphi : G \to H \text{ Isomorphismus} \tag{5.57}$$
$$\text{Beh.: } \varphi^{-1} : H \to G \text{ ist Isomorphismus} \tag{5.58}$$
$$\text{Bew.: } \varphi^{-1} \text{ bijektiv klar} \tag{5.59}$$
$$\varphi^{-1} \text{ Homomorphismus} \tag{5.60}$$
$$\text{Seien } a, b \in H \text{ und } x = \varphi^{-1}(a), y = \varphi^{-1}(b) \tag{5.61}$$
$$\implies \varphi(x) = a, \varphi(y) = b \tag{5.62}$$
$$\implies \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = a \cdot b \tag{5.63}$$
$$\implies \varphi^{-1}(a \cdot b) = \varphi^{-1}(\varphi(x \cdot y)) = x \cdot y = \varphi^{-1}(a) \cdot \varphi^{-1}(b) \tag{5.64}$$
$$\implies \varphi^{-1} \text{ Isomorphismus} \tag{5.65}$$
$$\implies H \cong G \ \checkmark \tag{5.66}$$

„transitiv“:

$$G \cong H \cong J \tag{5.67}$$
$$\implies \exists \varphi : G \to H \text{ und } \psi : H \to J \text{ Isomophismen} \tag{5.68}$$
$$\psi \circ \varphi : G \to J \text{ Isomorphismus, weil} \tag{5.69}$$
$$(\psi \circ \varphi)(a \cdot b) = \psi(\varphi(a \cdot b)) \tag{5.70}$$
$$= \psi(\varphi(a) \cdot \varphi(b)) \tag{5.71}$$
$$= (\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b) \quad \forall a, b \in G \tag{5.72}$$
$$\psi \circ \varphi \text{ bijektiv} \tag{5.73}$$
$$\implies G \cong J \tag{5.74}$$

□

Satz 5.4. *Jede Gruppe G (mit $\cdot$) ist isomorph zu einer Untergruppe von*

$$S_G = \{f \colon G \to G \mid f \text{ bijektiv}\}$$

Beweis.

$$\text{Zu } a \in G \text{ sei} \tag{5.75}$$
$$f_a : G \to G, f_a(x) = a \cdot x \tag{5.76}$$
$$^* \ f_a \text{ bijektiv} \tag{5.77}$$
$$\text{Beweis injektiv: } f_a(x) = f_a(y) \implies ax = ay \implies x = y \ \checkmark \tag{5.78}$$
$$\text{Beweis surjektiv: zu } y \in G \text{ setze } x = a^{-1}y \tag{5.79}$$
$$\implies f_a(x) = a \cdot a^{-1} \cdot y = y \tag{5.80}$$
$$^{**} \ f_a \circ f_b = f_{a \cdot b} \tag{5.81}$$
$$\text{Beweis: } (f_a \circ f_b)(x) = f_a(f_b(x)) \tag{5.82}$$
$$= a \cdot (b \cdot x) = (a \cdot b) \cdot c = f_{a \cdot b}(x) \tag{5.83}$$
$$\tag{5.84}$$

Wegen Gleichung 5.77 ff. ist durch $\varphi(a) = f_a$ eine Abbildung von G nach S_G definiert.
Wegen Gleichung 5.81 ff. gilt

$$\varphi(a) \circ \varphi(b) = f_a \circ f_b \qquad = f_{a \cdot b} = f(a \cdot b) \tag{5.85}$$

d. h. φ ist Homomorphismus von G nach S_G.
Damit gilt:

$$H := \varphi(G) \tag{5.86}$$
$$= \{\varphi(a) \mid a \in G\} \tag{5.87}$$
$$= \{f_a \mid a \in G\} \tag{5.88}$$
$$\leq S_G \tag{5.89}$$
$$\implies \hat{\varphi} : G \to H \tag{5.90}$$
$$\text{mit } \hat{\varphi}(a) = \varphi(a) \quad \forall a \in G \tag{5.91}$$
$$\implies \hat{\varphi} \text{ surjektiv, Homomorphismus} \tag{5.92}$$

Es bleibt zu zeigen, dass $\hat{\varphi}$ injektiv ist.

$$f_a = id_G \tag{5.93}$$
$$\iff \forall x \in G : f_a(x) = x \tag{5.94}$$
$$\iff \forall x \in G : a \cdot x = x \tag{5.95}$$
$$\iff a = 1_G \tag{5.96}$$
$$\text{also Kern } \hat{\varphi} = \{1_G\} \tag{5.97}$$
$$\implies \hat{\varphi} \text{ injektiv} \tag{5.98}$$
$$\text{Also: } G \cong H \leq S_G \tag{5.99}$$

□

5.2. Arithmetik von $\mathbb{N}$

- $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ werde definiert durch

$$m + 0 := m \quad \forall m \in \mathbb{N}$$

und

$$m + n^+ := (m + n)^+ \quad \forall m \in \mathbb{N}$$

(rekursive bzw. induktive Definition), $n \in \mathbb{N}$
Daraus:

- $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ durch

$$m \cdot 0 := 0 \quad \forall m \in \mathbb{N}$$

und

$$m \cdot n^+ := m \cdot n + m \quad \forall m \in \mathbb{N}$$

, $n \in \mathbb{N}$

Satz 5.5. *$\mathbb{N}$ mit $+$ erfüllt (i)[3], (ii)[4] aus der Definition Gruppe". Außerdem ist $+$ kommutativ.*

$\mathbb{N}$ mit $\cdot$ erfüllt (i), (ii) aus der Definition „Gruppe". Außerdem ist $\cdot$ kommutativ.

Beweis. Wir zeigen zunächst $m + n = n + m \quad \forall m, n \in \mathbb{N}$.

$$\lightning: \quad \forall n \in \mathbb{N} : m + n = n + m \tag{5.100}$$

Beweis induktiv über m.

(1) Induktionsanfang:

$$m = 0 \tag{5.101}$$

$$\lightning: \quad \forall n \in \mathbb{N} : 0 + n = n + 0 \tag{5.102}$$

Dies zeige man induktiv über n.

(2) Induktionsanfang:

$$n = 0 \tag{5.103}$$

$$\text{In der Tat gilt:} \quad 0 + 0 = 0 + 0 \ \checkmark \tag{5.104}$$

(2) Induktionsvorraussetzung:

$$\text{Gelte } 0 + n = n + 0 \text{ für ein } n \in \mathbb{N} \tag{5.105}$$

[3] Assoziativität
[4] Existenz eines neutralen Elements

(2) Induktionsschluss:

$$0 + n^+ \overset{\text{Def.}+}{=} n^+ + 0 \tag{5.106}$$
$$\overset{\text{IV}}{=} (n+0)^+ \tag{5.107}$$
$$\overset{\text{Def.}+}{=} n^+ \tag{5.108}$$
$$\overset{\text{Def.}+}{=} n^+ + 0 \ \checkmark \tag{5.109}$$

(1) Induktionsvorraussetzung:

$$\text{Gelte } \forall n \in \mathbb{N} : m + n = n + m \text{ für ein } m \tag{5.110}$$

(1) Induktionsschluss:

$$\lightning: \quad \forall n \in \mathbb{N} m^+ + n = n + m^+ \text{ induktiv über } n \tag{5.111}$$

(3) Induktionsanfang:

$$\lightning: \quad m^+ + 0 = 0 + m^+ \text{ (bewiesen in Gleichung 5.102 ff.)} \tag{5.112}$$

(3) Induktionsvorraussetzung:

$$\text{Gelte } m^+ + n = n + m^+ \text{ für ein } n \in \mathbb{N} \tag{5.113}$$

(3) Induktionsschluss:

$$\lightning: \quad m^+ + n^+ = n^+ + m^+ \tag{5.114}$$
$$m^+ + n^+ \overset{\text{Def.}+}{=} \left(m^+ + n\right)^+ \tag{5.115}$$
$$\overset{\text{IV}}{\underset{(3)}{=}} \left(n + m^+\right)^+ \tag{5.116}$$
$$= \left((n+m)^+\right)^+ \tag{5.117}$$
$$n^+ + m^+ \overset{\text{Def.}+}{=} \left(n^+ + m\right)^+ \tag{5.118}$$
$$\overset{\text{IV}}{\underset{(1)}{=}} \left(m + n^+\right)^+ \tag{5.119}$$
$$= \left((m+n)^+\right)^+ \tag{5.120}$$

Dies zeigt: + kommutativ.

(5.121)

Jetzt:

$$\lightning: \quad \forall l, m \in \mathbb{N} : l + (m+n) = (l+m) + n, \text{ induktiv über } n \in \mathbb{N} \tag{5.122}$$

Induktionsanfang:

$$\text{Es ist } l+(m+0) \overset{\text{Def. }+}{=} l+m \tag{5.123}$$
$$= (l+m) \overset{\text{Def. }+}{=} (l+m)+0 \ \checkmark \tag{5.124}$$

Induktionsvorraussetzung:

$$\text{Gelte } \forall l, m \in N : l+(m+n) = (l+m)+n \text{ für ein } n \in \mathbb{N} \tag{5.125}$$

Induktionsschluss:

$$l+\left(m+n^+\right) \overset{\text{Def. }+}{=} l+(m+n)^+ \tag{5.126}$$
$$\overset{\text{Def. }+}{=} (l+(m+n))^+ \tag{5.127}$$
$$\overset{\text{IV}}{=} ((l+m)+n)^+ \tag{5.128}$$
$$\overset{\text{Def. }+}{=} (l+m)+n^+ \ \checkmark \tag{5.129}$$
$$\tag{5.130}$$

Dies zeigt den ersten Teil des Satzes.
Der Beweis des zweiten Teils verläuft ähnlich. □

Satz 5.6 (Streichungsregel)**.** *Für $a, b \in \mathbb{N}$ gilt: Aus $a+n = b+n$ folgt $a = b$.*

Beweis. (Induktiv über n mithilfe von $\forall a, b \in \mathbb{N} : a^+ = b^+ \implies a = b$) □

5.3. Konstruktion und Arithmetik von $\mathbb{Z}$

Man betrache $\mathbb{N} \times \mathbb{N} = \left\{ (a,b) : a \in \mathbb{N}, b \in \mathbb{N} \right\}$. a beschreibt den positiven Anteil, b beschreibt den negativen Anteil der ganzen Zahl. (a,b) wird interpretiert als $a-b$:

- $(0,3)$ entspricht der ganzen Zahl -3.
- $(2,5)$ entspricht auch der ganzen Zahl -3.

(a',b') ist folglich „gleich“ (a,b), wenn $a-b = a'-b'$ gilt.
Durch

$$(a,b) \sim (a',b') \iff a+b' = a'+b$$

wird eine Äquivalenzrelation auf $\mathbb{N}^2$ definiert. Die Äquivalenzklassen von $\sim$ heißen *ganze Zahlen*. Die Menge $\mathbb{Z}$ der ganzen Zahlen ist folglich

$$\mathbb{Z} = \left\{ \left[(a,b)\right]_{/\sim} : (a,b) \in \mathbb{N} \times \mathbb{N} \right\} \tag{5.131}$$

Man definiere zwei Operationen $+, \cdot$ auf $\mathbb{Z}$ wie folgt:

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \tag{5.132}$$
$$\left[(a,b)\right]_{/\sim} + \left[(c,d)\right]_{/\sim} := \left[(a+c, b+d)\right]_{/\sim} \tag{5.133}$$

Zu zeigen ist hier die *Wohldefiniertheit*, d. h. die rechte Seite hängt nicht von der Wahl der Repräsentanten $(a,b),(c,d)$ links ab. D. h. $\big[(a,b)\big]_{/\sim} = \big[(a',b')\big]_{/\sim}$ und $\big[(c,d)\big]_{/\sim} = \big[(c',d')\big]_{/\sim}$ impliziert $\big[(a+c,b+d)\big]_{/\sim} = \big[(a'+c',b'+d')\big]_{/\sim}$:

$$a+b'=a'+b \wedge c+d'=c+d \implies (a+c)+(b'+d')=(a'+c')+(b+d) \ \checkmark \tag{5.134}$$

$$\cdot : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z} \tag{5.135}$$

$$\big[(a,b)\big]_{/\sim}\cdot\big[(c,d)\big]_{/\sim} := \big[(ac+bd,ad+bc)\big]_{/\sim} \tag{5.136}$$

ist ebenfalls wohldefiniert. Dazu zeige man:

$$a+b'=a'+b \wedge c+d'=c'+d \implies ac+bd+a'd'+b'c'=a'c'+b'd'+ad+bc \tag{5.137}$$

TBD RECHNE SELBST, VERDAMMT!

(5.138)

Die ganzen Zahlen $\mathbb{Z}$ mit $+$ bilden eine Gruppe, neutrales Element:

$$\big[(0,0)\big]_{/\sim} \text{ (ohne Beweis)}$$

5.4. Konstruktion und Arithmetik von $\mathbb{Q}$

Man betrachte

$$\mathbb{Z}\times(\mathbb{Z}\setminus\{0\}) = \Big\{(a,b) : a\in\mathbb{Z}, b\in\mathbb{Z}\setminus\{0\}\Big\}$$

„$(a,b)\cong\frac{a}{b}$“

Durch

$$(a,b)\sim(a',b') : \iff a\cdot b' = a'\cdot b$$

wird eine Äquivalenzrelation auf $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ definiert. Die Äquivalenzklassen heißen *rationale Zahlen*. Schreibweise:

$$\frac{a}{b} \text{ statt } \big[(a,b)\big]_{/\sim}$$

Bezeichnung:

$$\mathbb{Q} := \Big\{\frac{a}{b} : a,b\in\mathbb{Z}, b\neq 0\Big\} \tag{5.139}$$

Arithmetik:

$$+ : \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q} \tag{5.140}$$

$$\frac{a}{b}+\frac{c}{d} := \frac{ad+bc}{bd} \text{ (ist wohldefiniert)} \tag{5.141}$$

$$\cdot : \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q} \tag{5.142}$$

$$\frac{a}{b}\cdot\frac{c}{d} := \frac{a\cdot c}{b\cdot d} \tag{5.143}$$

In Klassenschreibweise:

$$\big[(a,b)\big]_{/\sim} + \big[(c,d)\big]_{/\sim} := \big[(ad+bc,bd)\big]_{/\sim} \tag{5.144}$$

$$\big[(a,b)\big]_{/\sim} \cdot \big[(c,d)\big]_{/\sim} := \big[(ac,bd)\big]_{/\sim} \tag{5.145}$$

Reelle Zahlen erhält man aus $\mathbb{Q}$ durch DEDEKIND-Schnitte[5].

5.5. Ringe und Körper

(i) – (iv): R mit $+$ ist kommutative Gruppe.

5.7. Ein *Ring* ist eine Menge R mit zwei Operationen $+, \cdot$ und den folgenden Eigenschaften:

(i) $\forall a,b,c \in R : a+(b+c) = (a+b)+c$

(ii) $\exists 0 \in R : \forall a \in R : a+0 = 0+a = a$

(iii) $\forall a \in R : \exists -a \in R : a+(-a) = (-a)+a = 0$

(iv) $\forall a,b \in R : a+b = b+a$

(v) $\forall a,b,c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ($\cdot$ assoziativ)

(vi) $\forall a,b,c \in R : (a+b) \cdot c = a \cdot c + b \cdot c$ und $a \cdot (b+c) = a \cdot b + a \cdot c$ ($+, \cdot$ distributiv)

R heißt Ring mit $1 \neq 0$, falls außerdem gilt:

(vii) Es gibt ein (multiplikativ) neutrales Element $1 \in R$, $1 \neq 0$, existiert mit $\forall a \in R : a \cdot 1 = 1 \cdot a = a$

R heißt kommutativer Ring, falls (i) bis (vi) gelten und

(viii) $\forall a,b \in R : a \cdot b = b \cdot a$

5.8. Ein kommutativer Ring mit $1 \neq 0$ heißt *Körper*, falls gilt:

(ix) Zu $a \in R, a \neq 0$ gibt es ein $a^{-1} \in R$ mit $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Beispiel: $\mathbb{Z}$ mit $+, \cdot$ ist ein kommutativer Ring mit $1 \neq 0$, jedoch kein Körper ((ix) ist verletzt für $a = 2$)

Beispiel: $\mathbb{Q}$ ist ein Körper, ebenso $\mathbb{R}$ (die reellen Zahlen) und $\mathbb{C}$ (die komplexen Zahlen).

[5] Siehe https://de.wikipedia.org/wiki/Reelle_Zahl

Beispiel: Sei $m > 1$ aus Z und $\mathbb{Z}_m$ sei die Menge der Restklassen modulo m, d. h.

$$\mathbb{Z}_m = \left\{ [a]_{/\equiv \mod m} (= \overline{a}) : a \in \mathbb{Z} \right\} \tag{5.146}$$

$$\text{wobei } \overline{a} = \left\{ b \in \mathbb{Z} : b \equiv a \mod m \right\} \tag{5.147}$$

$$\iff m \mid (b - a) \tag{5.148}$$

$$\iff b, a \text{ lassen denselben Rest bei der Teilung durch } m \tag{5.149}$$

Wir definieren Operationen $+, \cdot$ auf $\mathbb{Z}_m$:

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, \overline{a} + \overline{b} = \overline{a + b} \text{ (wohldefiniert)} \tag{5.150}$$

$$\text{Wohldefiniertheit: Aus } a - a' = \lambda m \text{ und } b - b' = \mu m \text{ folgt } (a + b) - \left(a' + b\right) = \nu \cdot m \tag{5.151}$$

$$a - a' = \lambda m \text{ und } b - b' = \mu m \tag{5.152}$$

$$\implies \left(a - a'\right) + \left(b - b'\right) = \lambda m + \mu m \tag{5.153}$$

$$\implies (a + b) - \left(a' + b'\right) = (\lambda + \mu) \cdot m \tag{5.154}$$

$$\implies \nu = \lambda + \mu \text{ (tut es)} \tag{5.155}$$

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, \overline{a} \cdot \overline{b} = \overline{a \cdot b} \text{ (ebenfalls wohldefiniert)} \tag{5.156}$$

Satz 5.7. *$\mathbb{Z}_m$ mit $+, \cdot$ ist ein kommutativer Ring mit $\overline{1} \neq \overline{0}$.*

Beweis. (i), …, (iv), (v)

„(vi)“:

$$\left(\overline{a} + \overline{b}\right) \cdot \overline{c} = \left(\overline{a + b}\right) \cdot \overline{c} \tag{5.157}$$

$$\overset{\text{(vi) für } \mathbb{Z}}{=} \overline{a \cdot c + b \cdot c} \tag{5.158}$$

$$= \overline{a \cdot c} + \overline{b \cdot c} \tag{5.159}$$

$$= \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c} \ \checkmark \tag{5.160}$$

„(viii)“:

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} \tag{5.161}$$

$$= \overline{b \cdot a} \tag{5.162}$$

$$= \overline{b} \cdot \overline{a} \tag{5.163}$$

□

$\mathbb{Z}_m$ ist im Allgemeinen kein Körper: Beispielsweise besesitzt $\overline{2}$ in $\mathbb{Z}_6$ ($m = 6$) kein multiplikativ Inverses. In Tabelle 5.1 sieht man in der Zeile zu $\overline{2}$ sofort, dass $\overline{1}$ nicht auftritt.

Tabelle 5.1.: Multiplikation auf $\mathbb{Z}_6$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

5.9. Ein *Nullteiler* im Ring R ist ein $a \in R$, $a \neq 0$, zu dem es ein $b \in R$, $b \neq 0$ mit $a \cdot b = 0$ gibt.
Körper besitzen keinen Nullteiler.

Beispiel: Man Betrachte $\mathbb{Z}_5$ in Tabelle 5.2. Es gilt $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{2} = \overline{1}$, $\overline{4} \cdot \overline{4} = \overline{1}$. Folglich ist $\mathbb{Z}_5$ ein Körper.

Tabelle 5.2.: Multiplikation auf $\mathbb{Z}_5$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Gleichungen der Form $\overline{a} \cdot \overline{x} = \overline{b}$ mit $\overline{a} \neq \overline{0}$ besitzen eine Lösung $\overline{x} = \overline{a}^{-1} \cdot \overline{b}$.

Beispiel: Man betrache $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. $\mathbb{Z}_2$ ist ein Körper.

Tabelle 5.3.: Addition und Multiplikation auf $\mathbb{Z}_2$

$+$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\cdot$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{1}$

Beispiel: $\mathbb{Z}_4$ ist kein Körper, denn $\overline{2}$ ist Nullteiler.

Satz 5.8 (Division mit Rest)**.** *Zu $a, b \in \mathbb{Z}, b \neq 0$, gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$.*

Beweis. „Existenz“: Die Menge $M := \{a - qb : q \in \mathbb{Z}, a - qb \geq 0\}$ ist eine nichtleere Menge nichtnegativer ganzer Zahlen. ✓

M besitzt daher ein kleinstes Element r (siehe Wohlordnung von $\mathbb{N}$, **??**) und es gilt

$$r = a - qb \text{ für ein } q \in \mathbb{Z} \tag{5.164}$$
$$\text{also } a = qb + r \tag{5.165}$$
$$\text{Wäre } r \geq |b| \tag{5.166}$$
$$\text{dann wäre } r - |b| \geq 0 \tag{5.167}$$
$$\text{und } r - |b| = \begin{cases} a - (q+1)\, b & \text{für } b \geq 0 \\ a - (q-a)\, b & \text{für } b \leq 0 \end{cases} \tag{5.168}$$
$$\text{folglich } r - |b| \in M \tag{5.169}$$
$$\text{jedoch } r - |b| < r \;\lightning \text{ Wahl von r.} \tag{5.170}$$

„Eindeutigkeit“:

$$\text{Sei } q', r' \in \mathbb{Z} \text{ ein zweites Paar} \tag{5.171}$$
$$\text{mit } a = q'b + r' \text{ und } 0 \leq r' < |b| \tag{5.172}$$
$$\implies a - a(=0) = qb + r - \left(q'b + r'\right) \tag{5.173}$$
$$= \left(q - q'\right) b + \left(r - r'\right) \tag{5.174}$$
$$\implies q - q' = 0 \tag{5.175}$$
$$\implies q = q' \tag{5.176}$$
$$\text{und } r' = a - q'b = a - qb = r \tag{5.177}$$

□

Satz 5.9. *Sei $m > 1$. Dann ist*

$$\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$$

wobei $\forall i, j \in \left\{0, 1, \ldots, m-1\right\} : \bar{i} \neq \bar{j}$, d. h. $|\mathbb{Z}_m| = m$.

Es ist $\mathbb{Z}_m$ ein Körper genau dann, wenn m eine Primzahl ist.

Beweis.

$$\text{Sei } \overline{a} \in \mathbb{Z}_m \tag{5.178}$$
$$\Longrightarrow \text{ existiert } q, r \in \mathbb{Z} \tag{5.179}$$
$$\text{mit } a = qm + r \tag{5.180}$$
$$\text{und } 0 \leq r < m \tag{5.181}$$
$$\Longrightarrow \overline{a} = \overline{qm + r} = \overline{q} \cdot \overline{m} + \overline{r} \tag{5.182}$$
$$\overset{\overline{m}=\overline{0}}{=} \overline{q} \cdot \overline{0} + \overline{r} \tag{5.183}$$
$$= \overline{0} + \overline{r} \tag{5.184}$$
$$\text{also } \overline{a} = \overline{r} \in \left\{\overline{0}, \ldots, \overline{m-1}\right\} \tag{5.185}$$
$$\text{Für } i \neq j \text{ aus } \left\{0, \ldots, m-1\right\} \tag{5.186}$$
$$\text{o. B. d. A. } i > j \tag{5.187}$$
$$0 < i - j < m - 1 \tag{5.188}$$
$$\text{also } m \nmid i - j \tag{5.189}$$
$$\text{also } \bar{i} \neq \bar{j} \tag{5.190}$$

Ist m keine Primzahl, so besitzt $\mathbb{Z}_m$ Nullteiler (s. o.).

Sei jetzt m eine Primzahl und $\overline{a} \neq \overline{0}$. Finde multiplikativ Inverse zu $\overline{a}$.

$$f\colon \mathbb{Z}_m \to \mathbb{Z}_m \tag{5.191}$$
$$f(\overline{x}) := \overline{a} \cdot \overline{x} \text{ ist injektiv, denn:} \tag{5.192}$$
$$\text{Seien } \overline{x} \neq \overline{y} \text{ aus } \mathbb{Z}_m, \text{ o. B. d. A.} \tag{5.193}$$
$$x > y \tag{5.194}$$
$$\text{und } x, y \in \left\{0, \ldots, m-1\right\} \tag{5.195}$$

Annahme:

$$f(\overline{x}) = f(\overline{y}) \tag{5.196}$$
$$\Longrightarrow \overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y} \tag{5.197}$$
$$\Longrightarrow \overline{a}\,(\overline{x} - \overline{y}) = \overline{0} \tag{5.198}$$
$$\Longrightarrow \overline{a\,(x - y)} = \overline{0} \tag{5.199}$$
$$\Longrightarrow m \mid a\,(x - y) \tag{5.200}$$

Mithilfe des Satzes von der eindeutigen Primfaktorzerlegung (s. u.)

$$\Longrightarrow m \mid a \text{ oder } m \mid x - y \tag{5.201}$$
$$\text{jedoch } m \nmid a \text{ wegen } \overline{a} \neq \overline{0} \tag{5.202}$$
$$\text{und } m \nmid x - y \text{ wegen } x - y < m \;\lightning \tag{5.203}$$
$$\text{Folglich ist } f \text{ injektiv} \tag{5.204}$$
$$\text{also } f \text{ bijektiv (denn } \mathbb{Z}_m \text{ (Dedekind)-endlich).} \tag{5.205}$$

Insbesondere gibt es (genau) ein $\overline{x}$ mit

$$f(\overline{x}) = \overline{1} \tag{5.206}$$
$$\text{also } \overline{a} \cdot \overline{x} = \overline{1} \tag{5.207}$$
$$\text{Somit } \overline{x} = \overline{a}^{-1} \tag{5.208}$$

$\overline{x}$ ist multiplikativ Inverses von $\overline{a}$.

$$\text{Somit ist } \mathbb{Z}_m \text{ ein Körper} \tag{5.209}$$

□

Satz 5.10. *Im Allgemeinen gilt: Genau dann gibt es einen endlichen Körper mit q Elementen, wenn q eine Primzahlpotenz ist.*

Satz 5.11 (Zerlegung in Primfaktoren)**.** *Jede Zahl $n \geq 1$ lässt sich als Produkt von Primzahlen darstellen. Diese Darstellung ist bis auf die Reihenfolgen der Faktoren eindeutig.*

Dabei ist das Produkt von 0 Primzahlen $= 1$ und von einer Primzahl $p = p$:

$$1 = \prod_{\emptyset}, 2 = 2, 3 = 3, 4 = 2 \cdot 2, 5 = 5, 6 = 2 \cdot 3, 7 = 7, 8 = 2 \cdot 2 \cdot 2, 9 = 3 \cdot 3, \ldots$$

a^n ist induktiv definiert durch $a^0 := 1$ und $a^{n+1} := a \cdot a^n$ für $n \geq 0$.

5.6. Polynomringe in einer Unbekannten

5.10. Sei K Körper. Eine Folge $p = (a_0, a_1, \ldots) \in K^{\mathbb{N}}$ über K heißt *formale Potenzreihe.*
Schreibweise:

$$K\big[\,[x]\,\big] \text{ statt } K^{\mathbb{N}}$$

wobei x die formale Potenzreihe $x = (0, 1, 0, 0, \ldots)$ bezeichnet.

Ist $a \in K$, so bezeichnet a ebenfalls die formale Potenzreihe $(a, 0, 0, 0, \ldots)$.

5.11. $p \in K\big[[x]\big]$ heißt ein *Polynom*, falls ein $d \in \mathbb{N}$ existiert mit $a_j = 0$ für $j > d$. Für $p \neq 0$ heißt das kleinste derartige d der *Grad* von p (Bezeichnung: $\operatorname{grad} p = d$). Das Nullpolynom $p = 0$ hat (in dieser Vorlesung) keinen Grad. Je nach Lehrbuch wird jedoch auch beispielsweise -1 oder $-\infty$ angenommen.
Die Menge aller Polynome in $K\big[[x]\big]$ bezeichnet man mit $K[x]$.

$$\begin{aligned} x^2+2x+1 &= (1,2,1,0,0,0,0,\dots) && \text{Grad } 2\\ x &= (0,1,0,0,\dots) && \text{Grad } 1\\ 3x^2+4x+5 &= (5,4,3,0,0,\dots) && \text{Grad } 2 \end{aligned}$$

Satz 5.12. *$K[[x]]$ wird mit $+,\cdot$ wie folgt zu einem kommutativen Ring mit 1:*

$$+ : K[[x]] \times K[[x]] \to K[[x]] \tag{5.210}$$
$$(a_0,a_1,\dots)+(b_0,b_1,\dots) := (a_0+b_0, a_1+b_1,\dots) \text{ „punktweise“} \tag{5.211}$$
$$\cdot : K[[x]] \times K[[x]] \to K[[x]] \tag{5.212}$$
$$(a_0,a_1,\dots)\cdot(b_0,b_1,\dots) := (c_0,c_1,\dots) \tag{5.213}$$
$$\text{mit } c_k := \sum_{j=0}^{k} a_j b_{k-j} \tag{5.214}$$

Beispiel:

$$\begin{aligned} (3x^3+4x)\cdot(x+3) &= (0,4,0,3,0,\dots)\cdot(3,1,0,0,\dots) && (5.215)\\ &= (0,12,4,9,3,0,0,0,\dots) && (5.216)\\ &= 3x^4+9x^3+4x^2+12x && (5.217) \end{aligned}$$

	3	1	0	0
0	0	0		
4	12	4		
0	0	0		
3	9	3		
0				
0				

Bei der Berechnung in der Tabelle erhält man die Faktoren durch diagonale Addition ($0=0$, $12+0=12$, $0+4=0$, $9+0=9$, $3=3$)

$$\begin{aligned} x^n &= (0,0,\dots,1(i=n),0,0,\dots) && (5.218)\\ x^2\cdot(a_0,a_1,a_2,\dots) &= (0,0,1,0,0,\dots)\cdot(a_0,a_1,a_2,\dots) && (5.219)\\ &= (0,0,a_0,a_1,a_2,\dots) && (5.220) \end{aligned}$$

Man interpretiere $a \in K$ als die formale Potenzreihe $(a, 0, 0, \dots)$. Dann ist

$$
\begin{aligned}
(a_0, a_1, a_2, \dots) &= \sum_{j=0}^{\infty} a_j \cdot x^j && (5.221)\\
&= (a_0, 0, 0, \dots) && (5.222)\\
&+ (0, a_1, 0, \dots) && (5.223)\\
&+ (0, 0, a_2, \dots) && (5.224)\\
&\vdots && (5.225)\\
&= (a_0, a_1, a_2, \dots) && (5.226)
\end{aligned}
$$

wobei a_j und x^j Polynome sind.

5.12. Für ein $f \in K\big[[x]\big]$ sei

$$\operatorname{supp} f = \big\{ i \in \mathbb{N} : f_i \neq 0 \big\} \tag{5.227}$$

der *Träger* (support) von f.

Die Menge $K[x] = \Big\{ f \in K\big[[x]\big] : \operatorname{supp} f \text{ endlich} \Big\}$ bildet einen Ring mit $+, \cdot$ (einen *Unterring* von $K\big[[x]\big]$), denn: Sind $f, g \in K[x]$ mit $c = \max(\operatorname{supp} f \cup \{0\}), d = \max(\operatorname{supp} g \cup \{0\})$, ist $k > c \wedge k > d$, so ist $f_k = 0$ und $g_k = 0$, also auch $f_k + g_k = 0$, also $(f+g)_k = 0$, also $\operatorname{supp}\{f+g\} \subseteq \big\{0, \dots, \max\{c, d\}\big\}$.

Ist $k > c + d$, so ist für $i, j \geq 0$ mit $i + j = k$ stets $i > c \vee j > d$, also $f_i = 0$ oder $g_j = 0$, also $f_i \cdot g_j = 0$, also $\sum\limits_{\substack{i-j\geq 0 \\ i+j=k}} f_i \cdot g_j = 0$, also $\operatorname{supp} f \cdot g \subseteq \big\{0, \dots, c + d\big\}$.

Folglich ist $f + g \in K[x]$ und $f \cdot g \in K[x]$ $\forall f, g \in K[x]$.

Satz 5.13. *Seien $f, g \in K[x] \setminus \{0\}$. Dann gilt*

(i) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\}$

(ii) $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$

Beweis.

„(i)“:

$$
\begin{aligned}
&\operatorname{supp}\big\{f+g\big\} \subseteq \Big\{0, \dots, \max\big\{\operatorname{grad} f, \operatorname{grad} g\big\}\Big\} && (5.228)\\
\Longrightarrow\ &\operatorname{grad}(f+g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\} && (5.229)
\end{aligned}
$$

„(ii)“:

$$\text{Analog zu „(i)“ zeige man: } \operatorname{grad} f\cdot g \le \operatorname{grad} f + \operatorname{grad} g \tag{5.230}$$

$$\text{Es ist } (f\cdot g)_{\operatorname{grad} f+\operatorname{grad} g} = \sum_{\substack{i,j\ge 0\\ i+j=\operatorname{grad} f+\operatorname{grad} g}} f_i\cdot g_j \tag{5.231}$$

$$(f_i\cdot g_j = 0, \text{ falls } i>\operatorname{grad} f \vee j>\operatorname{grad} g) \tag{5.232}$$

$$= f_{\operatorname{grad} f}\cdot g_{\operatorname{grad} g} \tag{5.233}$$

$$\neq 0 \ (k \text{ hat keine Nullteiler}) \tag{5.234}$$

	g_0	g_1	$\dots$	$g_{\operatorname{grad} f}$	0	$\dots$	0
f_0							
f_1							
$\vdots$							
$f_{\operatorname{grad} f}$							
0							

□

5.13. Für $f\neq 0$ aus $K[x]$ heißt $f_{\operatorname{grad} f}$ der *Leitkoeffizient* von f.

Der vorangegangene Satz gilt auch dann noch, wenn K ein kommutativer Ring mit $1\neq 0$ ohne Nullteiler ist (ein sogenannter *Integritätsring*).

Satz 5.14 (Division mit Rest für Polynome)**.** *Sind $a,b\in K[x], b\neq 0$, so existieren eindeutig bestimmte Polynome $q,r\in K[x]$ mit $a=qb+r$ mit $r=0$ oder $\operatorname{grad} r<\operatorname{grad} b$.*

Beweis. Für $a=0$ nehme man $q=0, r=0$.

Existenz induktiv über $\operatorname{grad} a$:

Induktionsanfang:

$$\text{Für } a=0 \tag{5.235}$$

$$\text{oder } \operatorname{grad} a<b \tag{5.236}$$

$$\text{nehme man } q=0 \tag{5.237}$$

$$\text{und } r=a \tag{5.238}$$

Induktionsschritt:

$$\text{Für } \operatorname{grad} a \geq \operatorname{grad} b \tag{5.239}$$

$$\text{betrachte } p = \underbrace{a_{\operatorname{grad} a} \cdot b_{\operatorname{grad} b}^{-1}}_{\text{als Polynom}} \cdot x^{\operatorname{grad} a - \operatorname{grad} b} \tag{5.240}$$

$$\implies \operatorname{grad}(a - pb) < \operatorname{grad} a \tag{5.241}$$

$$\overset{\text{IV}}{\implies} a' = q' \cdot b + r' \tag{5.242}$$

$$\text{für gewisse } q', r' \in K[x] \text{ mit } r' = 0 \vee \operatorname{grad} r' \operatorname{grad} b \tag{5.243}$$

$$\implies a = a' + pb = q'b + r' + pb \tag{5.244}$$

$$= \underbrace{\left(q' + p\right)}_{:=q} \cdot \underbrace{b + r'}_{:=r} \tag{5.245}$$

$$= qb + r, r = 0 \vee \operatorname{grad} r < \operatorname{grad} b \tag{5.246}$$

Eindeutigkeit:

$$\text{Gelte für } q, r \text{ und } q', r' \colon q = qb + r \text{ und } r = 0 \vee \operatorname{grad} r < \operatorname{grad} b \tag{5.247}$$

$$\text{und } a = q'b + r' \text{ und } r' = 0 \vee \operatorname{grad} r' < \operatorname{grad} b \tag{5.248}$$

$$\implies 0 = \left(q - q'\right) b + \left(r - r'\right) \tag{5.249}$$

$$\text{Wäre } r \neq r' \tag{5.250}$$

$$\text{so } r - r' \neq 0 \tag{5.251}$$

$$\text{so ist } \operatorname{grad} b > \operatorname{grad}\left(r - r'\right) \tag{5.252}$$

$$= \operatorname{grad}\left(-\left(r - r'\right)\right) \tag{5.253}$$

$$= \operatorname{grad}\left(q - q'\right) b \tag{5.254}$$

$$= \operatorname{grad}\left(q - q'\right) + \operatorname{grad} b \tag{5.255}$$

$$\geq \operatorname{grad} b \tag{5.256}$$

$$\text{also } \operatorname{grad} b > \operatorname{grad} b \; \lightning \tag{5.257}$$

$$\text{Folglich ist } r = r' \tag{5.258}$$

$$\implies \left(q - q'\right) b = 0 \tag{5.259}$$

$$\overset{\text{(Übung)}}{\implies} q - q' = 0 \text{ oder } b = 0 \tag{5.260}$$

$$\overset{b \neq 0}{\implies} q - q' = 0 \tag{5.261}$$

$$\implies q = q' \tag{5.262}$$

□

Erklärungen:

- Gleichung 5.240 bewirkt, dass a und pb denselben Leitkoeffizienten haben.
- Die Polynome aus Gleichung 5.253 und Gleichung 5.254 sind gleich, deshalb auch ihre Grade.

6. Boolesche Algebra

6.1. Eine Menge B mit Operationen $\vee, \wedge : B \times B \to B$ (sprich: „sup“, „inf“) und Abbildung $^- : B \to B$ (schreibe $\overline{x}$, „x-quer“) heißt BOOLE*sche Algebra*, falls gilt:

(i) $a \vee b = b \vee a$ und
$a \wedge b = b \wedge a \quad \forall a, b \in B$

(ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ und
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad \forall a, b, c \in B$

(iii) $\exists \bot \in B : a \vee \bot = \bot \vee a = a$ („bottom“)
$\exists \top \in B : a \wedge \top = \top \wedge a = a$ („top“)
Es existieren also zwei eindeutig bestimmte neutrale Elemente $\bot$ und $\top$

(iv) $a \vee \overline{a} = \top \quad \forall a \in B$
$a \wedge \overline{a} = \bot \quad \forall a \in B$

Mit „$(B, \vee, \wedge, ^-)$“ ist auch „$(B, \wedge, \vee, ^-)$“ eine boolesche Algebra (der zu „$(B, \vee, \wedge, ^-)$“ *duale* boolesche Algebra).

Beispiel: M Menge, $B := \mathfrak{P}(M), \cup, \cap$ (statt $\vee, \wedge$), $\overline{a} := M \setminus a$ ist eine boolesche Algebra, $\top = M, \bot = \varnothing$.

Beispiel: $B = \{0,1\}^m = \big\{(a_1, \ldots, a_m) : a_i \in \{0,1\} \forall i \in \{1, \ldots, m\}\big\}$. Man definiere $+, \cdot$ auf $\{0,1\}$ durch

$+$	0	1
0	0	1
1	1	1

und

$\cdot$	0	1
0	0	0
1	0	1

Ferner $\overline{0} := 1$ und $\overline{1} := 0$. Setze (punktweise) fort zu Operationen auf B:

$$(a_1, \ldots, a_m) + (b_1, \ldots, b_m) := (a_1 + b_1, \ldots, a_m + b_m) \tag{6.1}$$

$$(a_1, \ldots, a_m) \cdot (b_1, \ldots, b_m) := (a_1 \cdot b_1, \ldots, a_m \cdot b_m) \tag{6.2}$$

$$\overline{(a_1, \ldots, a_m)} := (\overline{a_1}, \ldots, \overline{a_m}) \tag{6.3}$$

Dies liefert eine boolesche Algebra auf B

$$\bot = (0, \ldots, 0) \tag{6.4}$$

$$\top = (1, \ldots, 1) \tag{6.5}$$

Beispiel: Sei T_m die Menge der positiven Teiler von $m \geq 2$. kgV, ggT anstelle von $\vee, \wedge$ sowie $\overline{x} := \frac{m}{x}$ liefert eine boolesche Algebra mit $\top = m$ und $\bot = 1$, sofern m *quadratfrei*, d. h. keine Quadratzahl > 1 ist ein Teiler von m.

Satz 6.1. *$\bot$, $\top$ sind durch (iii) eindeutig bestimmt.*

Beweis. (wie beim neutralen Element in Gruppen, siehe Punkt iii auf Seite 36) □

Satz 6.2. *$\overline{a}$ ist durch die Gleichung in (iv) bestimmt, d. h. aus $a \vee b = \top$ und $a \wedge b = \bot$ folgt $b = \overline{a}$.*

Beweis.

$$b \overset{\text{(iii)}}{=} b \wedge \top \tag{6.6}$$

$$\overset{\text{(iv)}}{=} b \wedge (a \vee \overline{a}) \tag{6.7}$$

$$\overset{\text{(ii)}}{=} (b \wedge a) \vee (b \wedge \overline{a}) \tag{6.8}$$

$$\underset{\text{aus b, (i)}}{\overset{\text{Vss.}}{=}} \bot \vee (b \wedge \overline{a}) = b \wedge \overline{a} \tag{6.9}$$

$$\overline{a} \overset{\text{(iii)}}{=} \overline{a} \wedge T \tag{6.10}$$

$$\underset{\text{aus b}}{\overset{\text{Vss.}}{=}} \overline{a} \wedge (a \vee b) \tag{6.11}$$

$$\overset{\text{(ii)}}{=} (\overline{a} \wedge a) \vee (\overline{a} \wedge b) \tag{6.12}$$

$$\overset{\text{(iv), (i)}}{=} \bot \vee (\overline{a} \wedge b) \tag{6.13}$$

$$= \overline{a} \wedge b \tag{6.14}$$

$$\text{Folgich ist } b = \overline{a} \tag{6.15}$$

□

Lemma 6.3. *In einer booleschen Algebra $B, \vee, \wedge, \overline{\ }$ gilt:*

(i) $\forall a \in B : a \vee \top = \top$ *(Dominanz)*
$\forall a \in B : a \wedge \bot = \bot$

(ii) $\forall a, b \in B : a \vee (a \wedge b) = a$ *(Absorption)*
$\forall a, b \in B : a \wedge (a \vee b) = a$

(iii) Aus $a, b, x \in B : a \wedge x = b \wedge x$ und $a \vee x = b \vee x$ folgt $a = b$ (Streichungsregel)

(iv) $\forall a, b, c \in B : a \vee (b \vee c) = (a \vee b) \vee c$ *(Assoziativität)*
$\forall a, b, c \in B : a \wedge (b \wedge c) = (a \wedge b) \wedge c$

(v) $\forall a, b \in B : \overline{a \vee b} = \overline{a} \wedge \overline{b}$ *(DEMORGAN)*
$\forall a, b \in B : \overline{a \wedge b} = \overline{a} \vee \overline{b}$

Beweis.

„(i)“:

$$\begin{aligned} a \vee \top &= (a \vee \top) \wedge \top && (6.16)\\ &= (a \vee \top) \wedge (a \vee \overline{a}) && (6.17)\\ &= a \vee (\top \wedge \overline{a}) && (6.18)\\ &= a \vee \overline{a} && (6.19)\\ &= \top \ \checkmark && (6.20) \end{aligned}$$

Der zweite Teil ergibt sich aus der Dualität.

„(ii)“:

$$\begin{aligned} a \vee (a \wedge b) &= (a \wedge \top) \vee (a \wedge b) && (6.21)\\ &= a \wedge (\top \vee b) && (6.22)\\ &= a \wedge \top && (6.23)\\ &= a \ \checkmark && (6.24) \end{aligned}$$

Der zweite Teil ergibt sich aus der Dualität.

„(iii)“:

Aus den Vorraussetzungen folgt zunächst:

$$\begin{aligned} (a \wedge x) \vee (a \wedge \overline{x}) &= (b \wedge x) \vee (b \wedge \overline{x}) && (6.25)\\ (a \wedge x) \vee (a \wedge \overline{x}) &= a \wedge (x \vee \overline{x}) && (6.26)\\ &= a \wedge \top && (6.27)\\ &= a && (6.28)\\ (b \wedge x) \vee (b \wedge \overline{x}) &= b \wedge (x \vee \overline{x}) && (6.29)\\ &= b \wedge \top && (6.30)\\ &= b && (6.31)\\ \text{also } a &= b \ \checkmark && (6.32) \end{aligned}$$

„(iv)“:

$$\text{ZZ:}\quad a \vee (b \vee c) = (a \vee b) \vee c \tag{6.33}$$
$$(a \vee (b \vee c)) \wedge a = a \text{ (Absorption)} \tag{6.34}$$
$$((a \vee b) \vee c) \wedge a = a \wedge ((a \vee b) \vee c) \tag{6.35}$$
$$= \big(a \wedge (a \vee b)\big) \vee (a \wedge c) \tag{6.36}$$
$$= a \vee (a \wedge c) \tag{6.37}$$
$$= a \tag{6.38}$$
$$\big(a \vee (b \vee c)\big) \wedge \overline{a} = (a \wedge \overline{a}) \vee \big((b \vee c) \wedge \overline{a}\big) \tag{6.39}$$
$$= \bot \vee \big((b \vee c) \wedge \overline{a}\big) \tag{6.40}$$
$$= (b \vee c) \wedge \overline{a} \tag{6.41}$$
$$\big((a \vee b) \vee c\big) \wedge \overline{a} = \big((a \vee b) \wedge \overline{a}\big) \vee (c \wedge \overline{a}) \tag{6.42}$$
$$= \big((a \wedge \overline{a}) \vee (b \wedge \overline{a})\big) \vee (c \wedge \overline{a}) \tag{6.43}$$
$$= \big(\bot \vee (b \wedge \overline{a})\big) \vee (c \wedge \overline{a}) \tag{6.44}$$
$$= (b \wedge \overline{a}) \vee (c \wedge \overline{a}) \tag{6.45}$$
$$= (b \vee c) \wedge \overline{a} \tag{6.46}$$

Also gilt nach Steichungsregel:

$$a \vee (b \vee c) = (a \vee b) \vee c \ \checkmark \tag{6.47}$$

Der zweite Teil ergibt sich aus der Dualität.

„(v)“:

$$\text{ZZ:}\quad \left\{\begin{array}{ll} \overline{a \vee b} \vee \big(\overline{a} \wedge \overline{b}\big) & = \top \\ (a \vee b) \wedge \big(\overline{a} \wedge \overline{b}\big) & = \bot \end{array}\right\} \implies \overline{a} \wedge \overline{b} = \overline{a \vee b} \tag{6.48}$$

In der Tat:

$$(a \vee b) \vee \big(\overline{a} \wedge \overline{b}\big) = a \vee \big(b \vee \big(\overline{a} \wedge \overline{b}\big)\big) \tag{6.49}$$
$$= a \vee \big((b \vee \overline{a}) \wedge \big(b \vee \overline{b}\big)\big) \tag{6.50}$$
$$= a \vee (b \vee \overline{a}) \tag{6.51}$$
$$= (a \vee \overline{a}) \vee b \tag{6.52}$$
$$= \top \vee b \tag{6.53}$$
$$= \top \tag{6.54}$$

Dies gilt für beliebige a und b, also auch für $\overline{a}$ und $\overline{b}$.

$$\big(\overline{a} \vee \overline{b}\big) \vee \Big(\overline{\overline{a}} \wedge \overline{\overline{b}}\Big) = \top \tag{6.55}$$
$$\text{Dualisierung:}\quad \implies \big(\overline{a} \wedge \overline{b}\big) \wedge (a \wedge b) = \bot \tag{6.56}$$
$$\text{also:}\quad (a \vee b) \wedge \big(\overline{a} \wedge \overline{b}\big) = \bot \tag{6.57}$$

Der zweite Teil ergibt sich aus der Dualität. □

Satz 6.4. *Sei B mit $\vee, \wedge, \,^{-}$ Boolesche Algebra. Dann wird durch $a \leq b \iff a \vee b = b$ eine Ordnung auf B definiert. Es gilt:*

(i) $a \vee b = b \iff a \wedge b = a$

(ii) $a \vee b = \sup\{a, b\}$ *(bzgl. $\leq$)*

(iii) $a \wedge b = \inf\{a, b\}$ *(bzgl. $\leq$)*

Beweis.

„$\leq$ reflexiv“:

$$\begin{aligned} a \vee a &= (a \vee a) \wedge \top && (6.58)\\ &= (a \vee a) \wedge (a \vee \overline{a}) && (6.59)\\ &= a \vee (a \wedge \overline{a}) && (6.60)\\ &= a \vee \bot && (6.61)\\ &= a \ \checkmark && (6.62) \end{aligned}$$

„$\leq$ antisymmetrisch“:

$$\begin{aligned} a \leq b \leq a &\implies a \vee b = a \text{ sowie } b \vee a = b && (6.63)\\ &\implies a = b \ \checkmark && (6.64) \end{aligned}$$

„$\leq$ transitiv“:

$$\begin{aligned} a \leq b \leq c &\implies a \vee b = b \text{ sowie } b \vee c = c && (6.65)\\ \implies a \vee c &= a \vee (b \vee c) && (6.66)\\ &= (a \vee b) \vee c && (6.67)\\ &= b \vee c && (6.68)\\ &= c && (6.69)\\ &\implies a \leq c \ \checkmark && (6.70) \end{aligned}$$

„(i)“:

$$\begin{aligned} a \vee b = b &\implies a \wedge b = a \wedge (a \vee b) = a \text{ und} && (6.71)\\ a \wedge b = a &\implies a \vee b = (a \wedge b) \vee b = b \ \checkmark \text{ (Absorption)} && (6.72) \end{aligned}$$

„(ii)“:

$$
\begin{aligned}
& a \vee b \text{ ist obere Schranke von } a, b, && (6.73)\\
\text{denn } & a \leq a \vee b && (6.74)\\
\text{wegen } & a \vee (a \vee b) = (a \vee a) \vee b && (6.75)\\
& = a \vee b, && (6.76)\\
\text{ebenso } & b \leq a \vee b && (6.77)\\
& a \vee b \text{ ist sogar kleinste obere Schranke,} && (6.78)\\
\text{d. h. aus } & a \leq z \text{ und } b \leq z && (6.79)\\
\text{folgt } & a \vee b \leq z, && (6.80)\\
\text{denn } a \leq z \text{ und } b \leq z & \implies a \vee z = z \text{ und } b \vee z = z && (6.81)\\
\implies & (a \vee b) \vee z = a \vee (b \vee z) && (6.82)\\
& = a \vee z && (6.83)\\
& = z && (6.84)\\
\implies & a \vee b \leq z \ \checkmark && (6.85)
\end{aligned}
$$

„(iii)“:

Ähnlich, siehe Übung (nicht ganz symmetrisch, benutze (i)).

(6.86)

□

Die bezüglich $\leq$ minimalen Elemente von $B \setminus \{\bot\}$ heißen *Atome* von B mit $\vee, \wedge, \bar{}$. Die bezüglich $\leq$ maximalen Elemente von $B \setminus \{\top\}$ heißen *Coatome*.

Man betrachte $B = \mathfrak{P}(\{1,2,3\})$ mit $\cap, \cup, \bar{}$, wobei $\forall a \subseteq M : \overline{a} := \{1,2,3\} \setminus a$. Man erhält $\subseteq$ als Ordnung von B, denn $a \cup b = b \iff a \subseteq b$. Hasse-Diagramm siehe Abbildung 6.1.

Ist allgemein $B = \mathfrak{P}(M)$, M endlich, so sind die Atome von B mit $\cup, \cap, \bar{}$ die 1-elementigen Teilmengen von M, die Coatome sind die $(|M|-1)$-elementigen Teilmengen von M.

Satz 6.5. *Sei B mit $\vee, \wedge, \bar{}$ eine boolesche Algebra und $b \in B \setminus \{\bot\}$. Seien $a_1, \ldots, a_k$ diejenigen Atome a mit $a \leq b$.*

Dann folgt:

$$b = \underbrace{a_1 \vee \cdots \vee a_k}_{=c}$$

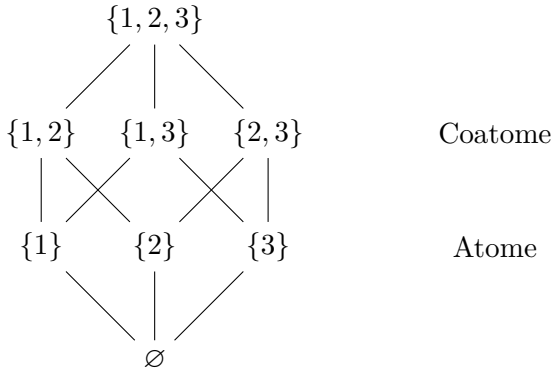


Abbildung 6.1.: Hasse-Diagramm von $\mathfrak{P}(\{1,2,3\})$.

Beweis.

$$b \wedge c = b \wedge (a_1 \vee \cdots \vee a_k) \tag{6.87}$$
$$= (b \wedge a_1) \vee \cdots \vee (b \wedge a_k) \tag{6.88}$$
$$= a_1 \vee \cdots \vee a_k \tag{6.89}$$
$$= c \tag{6.90}$$
$$\lightning: \quad b \wedge \overline{c} = \bot \tag{6.91}$$
$$\text{Aus } b \wedge \overline{c} \neq \bot \tag{6.92}$$
$$\text{folgt } \exists a \text{ Atom} : a \leq b \wedge \overline{c} \tag{6.93}$$
$$\implies a \leq b \tag{6.94}$$
$$\implies a = a_j \text{ für } j \in \{1, \ldots, k\} \tag{6.95}$$
$$\text{o. B. d. A. } j = 1 \tag{6.96}$$
$$\implies a_1 = a_1 \wedge \left(b \wedge \underbrace{\overline{c}}_{= \overline{a_1 \vee \ldots a_k}} \right) \tag{6.97}$$
$$= \underbrace{a_1 \wedge b \wedge \overline{a_1}}_{a_1 \wedge \overline{a_1} = \bot} \wedge \cdots \wedge \overline{a_k} \tag{6.98}$$
$$= \bot \ \lightning, \text{ denn } \bot \text{ ist kein Atom} \tag{6.99}$$

Folglich:

$$b \wedge c = c \text{ und } c \wedge c = c \tag{6.100}$$
$$b \wedge \overline{c} = \bot \text{ und } c \wedge \overline{c} = \bot \tag{6.101}$$
$$\implies b = c \tag{6.102}$$

□

Seien B mit $\vee, \wedge, \ ^{-}$ und $\dot{B}$ mit $\dot{\vee}, \dot{\wedge}, \ \dot{^{-}}$ boolesche Algebren.

Diese heißen *isomorph* zueinander, wenn eine Bijektion $\varphi : B \to \dot{B}$ existiert mit

$$\forall a, b \in B : \varphi(a \vee b) = \varphi(a) \dot{\vee} \varphi(b) \tag{6.103}$$
$$\forall a, b \in B : \varphi(a \wedge b) = \varphi(a) \dot{\wedge} \varphi(b) \tag{6.104}$$
$$\varphi(\overline{a}) = \dot{\overline{\varphi(a)}} \tag{6.105}$$

Ein soches φ heißt *Isomorphismus*.

Satz 6.6 (STONE)**.** *Ist B mit $\vee, \wedge, \bar{}$ boolesche Algebra und die Menge A ihrer Atome endlich, so ist B isomorph zur booleschen Algebra $\mathfrak{P}(A), \cup, \cap, \dot{\bar{}}$ wobei $\dot{\overline{x}} := A \setminus x$ für $x \in \mathfrak{P}(A)$, d. h. $x \subseteq A$.*

Beweis. Für $X = \{x_1, \ldots, x_l\}$, so schreibe $\bigvee X := x_1 \vee \cdots \vee x_l$ ($\vee$ assoziativ, kommutativ). $\bigvee \varnothing = \bot$. Es gilt z. B. $\bigvee X \vee \bigvee Y = \bigvee (X \cup Y)$. Für $b \in B$ sei $\varphi(b)$ die Menge aller Atome a mit $a \leq b$.

$$\implies \bigvee \varphi(b) = b \tag{6.106}$$
$$\text{Dies definiert } \varphi : B \to \mathfrak{P}(A) \tag{6.107}$$
$$\text{z}\!\!\!/: \quad \varphi \text{ ist Isomorphismus} \tag{6.108}$$

„φ injektiv“:

$$\varphi(b) = \varphi(b') \tag{6.109}$$
$$\implies \bigvee \varphi(b) = \bigvee \varphi(b') \tag{6.110}$$
$$\overset{(6.106)}{\implies} b = b' \ \checkmark \tag{6.111}$$

„φ surjektiv“:

$$\text{Für } X \subseteq A \tag{6.112}$$
$$\text{gilt } \varphi\left(\bigvee X\right) = X \tag{6.113}$$
$$\text{denn ist } a \in X, \text{ so ist } a \leq \bigvee X \tag{6.114}$$
$$\text{und ist } a \in A \setminus X, \text{ so ist } a \wedge \left(\bigvee X\right) = \bot \neq \bigvee X \tag{6.115}$$
$$\text{also } a \nleq \bigvee X \tag{6.116}$$

Folglich ist φ eine Bijektion. ✓

$$\varphi(x \vee y) \overset{(6.106)}{=} \varphi\left(\overbrace{\bigvee \varphi(x)}^{=x} \vee \overbrace{\bigvee \varphi(y)}^{=y}\right) \tag{6.117}$$
$$= \varphi\left(\bigvee (\varphi(x) \vee \varphi(y))\right) \tag{6.118}$$
$$\overset{(6.106)}{=} \varphi(x) \cup \varphi(y) \tag{6.119}$$

Für beliebiges $a \in B$ gilt:

$$a \leq x \wedge y \implies a \leq x \text{ und } a \leq y \tag{6.120}$$
$$\implies a \text{ untere Schranke von } \{x, y\} \tag{6.121}$$
$$\text{Folglich: } \varphi(x \wedge y) = \varphi(x) \cap \varphi(y) \tag{6.122}$$
$$\text{Für } a \in A, x \in B \text{ gilt dann } a \in \varphi(\top) = \varphi(x \vee \overline{x}) \tag{6.123}$$
$$= \varphi(x) \cup \varphi(\overline{x}) \tag{6.124}$$
$$\text{Aus } a \in \varphi(x) \cup \varphi(\overline{x}) = \varphi(x \wedge \overline{x}) \tag{6.125}$$
$$= \varphi(\bot) \tag{6.126}$$
$$= \varnothing \; \lightning \tag{6.127}$$

Also ist jedes $a \in A$ genau eine der Mengen $\varphi(x), \varphi(\overline{x})$.

$$\implies \varphi(\overline{x}) = A \setminus \varphi(x) \tag{6.128}$$
$$= \overline{\varphi(x)}^{\cdot} \tag{6.129}$$
$$\tag{6.130}$$

Somit ist φ tatsächlich ein Isomorphismus. □

Aus dem Satz folgt unmittelbar: Jede boolesche Algebra mit endlichem B ist isomorph zu $\mathfrak{P}(M)$ mit $\cup, \cap, \overline{\ }$, wobei $\overline{x} := M \setminus x$ und M endlich ist. Insbesondere ist dann $|B|$ eine Zweierpotenz.

Beispiel: Sei T_m die Menge der positiven Teiler von m und m quadratfrei. Sei $A = \{p_1, \ldots, p_k\}$ die Menge der Primteiler von m, also $m = p_1 \cdot \cdots \cdot p_k$.

$$\varphi : T_m \to \mathfrak{P}(A), \tag{6.131}$$
$$\varphi(x) = \{p_j : p_j \mid x, j \in \{1, \ldots, k\}\} \text{ ist Bijektion} \tag{6.132}$$
$$\varphi(\mathrm{kgV}(x, y)) = \varphi(x) \cup \varphi(y) \tag{6.133}$$
$$\varphi(\mathrm{ggT}(x, y)) = \varphi(x) \cap \varphi(y) \tag{6.134}$$
$$\varphi(m/x) = A \setminus \varphi(x) \tag{6.135}$$
$$\text{d. h. } T_m \text{ mit } \mathrm{kgV}, \mathrm{ggT}, \text{ wobei } \overline{x} := m/x \tag{6.136}$$
$$\text{ist boolesche Algebra.} \tag{6.137}$$

6.1. Aussagenlogik als boolesche Algebra

Sei X eine endliche Menge von Variablen. Eine aussagenlogische Formel[1] F in X ist…

… *atomar*, wenn sie die Gestalt „x“ (mit $x \in X$) oder „f“[2] oder „w“[3] hat.

[1] siehe **??**
[2] „immer falsch“
[3] „immer wahr“

… *zusammengesetzt*, wenn sie die Gestalt „$(P \vee Q)$“ oder „$(P \wedge Q)$“ oder „$\neg(P)$“ für gewisse Formeln P, Q in X hat.

Der *Wahrheitswert* von F unter der *Belegung* $\beta : X \to \{f, w\}$ der Variablen ergibt sich wie in Kapitel 1. Bezeichnung: $W_F(\beta)$. Der *Wahrheitswerteverlauf* ist die so definierte Funktion $W_F : \{f, w\}^X \to \{f, w\}$. Folglich gibt es $2^{\left(2^{|x|}\right)}$ verschiedene Wahrheitswerteverläufe.

Aussagenlogische Formeln F, F' sind also *logisch äquivalent* ($F \equiv F'$) genau dann, wenn $W_F = W_{F'}$ gilt (d. h. $\forall \beta : X \to \{f, w\} : W_F(\beta) = W_{F'}(\beta)$).

Bezeichner (wie üblich): $[F]_{/\equiv}$ — Diejenige Äquivalenzklasse von aussagenlogischen Formeln in X (bzgl. $\equiv$), die F enthält. Es gibt $2^{\left(2^{|X|}\right)}$ viele Äquivalenzklassen.

$$[F]_{/\equiv} \underbrace{\vee}_{\text{sup}} [F]_{/\equiv} := \left[\left(F \underbrace{\vee}_{\text{oder}} F'\right)\right]_{/\equiv} \qquad \text{wohldefiniert} \tag{6.138}$$

$$[F]_{/\equiv} \underbrace{\wedge}_{\text{inf}} [F]_{/\equiv} := \left[\left(F \underbrace{\wedge}_{\text{und}} F'\right)\right]_{/\equiv} \qquad \text{wohldefiniert} \tag{6.139}$$

$$\overline{[F]_{/\equiv}} := [\neg(F)]_{/\equiv} \qquad \text{wohldefiniert} \tag{6.140}$$

liefert eine boolesche Algebra mit der Menge $B = \left\{ [F]_{/\equiv} : F \text{ aussagenlogische Formel} \right\}$ aller Äquivalenzklassen (bzgl. $\equiv$) von Formeln in X.

$$\bot = [f]_{/\equiv} \qquad \text{(Menge aller Kontradiktionen)} \tag{6.141}$$

$$\top = [w]_{/\equiv} \qquad \text{(Menge aller Tautologien)} \tag{6.142}$$

Für die Ordnung $\leq$ von B (s. o.) ergibt sich:

$$[F]_{/\equiv} \leq \left[F'\right]_{/\equiv} \overset{\text{Def.}}{\iff} [F]_{/\equiv} \vee \left[F'\right]_{/\equiv} = \left[F'\right]_{/\equiv} \tag{6.143}$$

$$\text{d. h. } \left[(F \vee F')\right]_{/\equiv} = \left[F'\right]_{/\equiv} \tag{6.144}$$

$$\text{d. h. } W_{F \vee F'} = W_{F'} \tag{6.145}$$

$$\text{d. h. } F \vee F' \equiv F' \tag{6.146}$$

$$\text{also } (F \implies F') \text{ ist stets wahr} \tag{6.147}$$

Aus Tabelle 6.1 folgt also:

$$[F]_{/\equiv} \leq \left[F'\right]_{/\equiv}, \text{ falls } W_{F \to F'} \text{ konstant } w \tag{6.148}$$

$$\left[F \implies F'\right]_{/\equiv} = [w]_{\equiv} \tag{6.149}$$

Tabelle 6.1.: Wahrheitswerteverläufe von $F \vee F'$, $F \vee F' \iff F'$ und $F \implies F'$.

F	F'	$F \vee F'$	$F \vee F' \iff F'$	$F \implies F'$
f	f	f	w	w
f	w	w	w	w
w	f	w	f	f
w	w	w	w	w

Man rechnet nach:

$$[F]_{/\equiv} \leq \left[F'\right]_{/\equiv} \iff W_F^{-1}(\{w\}) \subseteq W_{F'}^{-1}(\{w\}) \tag{6.150}$$

Die Atome von $(B, \vee, \wedge, \bar{\ })$ sind genau diejenigen $[F]_{/\equiv}$, mit $\left|W_F^{-1}(\{w\})\right| = 1$, d. h. $W_F(\beta) = w$ für genau ein $\beta : X \to \{f, w\}$. Die Atome können besonders einfach repräsentiert werden. Für $X = \{x_1, \ldots, x_n\}$ ist $x_1 \wedge x_2 \wedge \cdots \wedge x_n = F$ ein solcher Repräsentant, ebenso wie alle F', die sich durch Ersetzen einiger x_j durch $(\neg x_j)$ daraus ergeben (z. B. $x_1 \wedge (\neg x_2) \wedge (\neg x_3) \wedge x_4 \wedge \cdots \wedge x_{n-1} \wedge (\neg x_n)$). Diese Formeln heißen *Minterme*.

Aus dem Satz über Atome einer booleschen Algebra folgt: Zu jedem $[F]_{/\equiv}$ existieren Atome $[F_1]_{/\equiv}, \ldots, [F_k]_{/\equiv}$ mit

$$[F]_{/\equiv} = [F_1]_{/\equiv} \vee \cdots \vee [F_k]_{/\equiv} = [F_1 \vee \cdots \vee F_k]_{/\equiv} \tag{6.151}$$

Folglich gibt es zu jeder Formel F Minterme $F_1, \ldots, F_k$ mit $F \iff F_1 \vee \cdots \vee F_k$. Eine Formel der Gestalt $F_1 \vee \cdots \vee F_k$ mit Mintermen $F_1, \ldots, F_k$ heißt in *disjunktiver Normalform* (DNF).

Analog: $x_1 \vee x_2 \vee \cdots \vee x_n$ sowie alle Formeln, die daraus durch Ersetzen einiger x_j durch $\neg x_j$ hervorgehen, heißen *Maxterme*. Die durch Maxterme repräsentierten Formelklassen sind genau die Coatome von $(B, \vee, \wedge, \bar{\ })$. Zu jeder Formel F gibt es Maxterme $F_1, \ldots, F_k$ mit

$$F \iff F_1 \wedge \ldots \wedge F_k \tag{6.152}$$

Diese Form heißt *konjunktive Normalform* (KNF).

Beispiel: $X = \{x, y\}$. Es gibt $\left|\{f, w\}^{\{x,y\}}\right| = 4$ Belegungen $\beta : \{x, y\} \to \{w, f\}$. Daher gibt es $2^4 = 16$ Wahrheitswerteverläufe für aussagenlogische Formeln in $\{x, y\}$. B wie oben hat daher 16 Elemente. $\top$ ist repräsentiert durch w, denn $W_w(\beta) = w$ für alle vier Belegungen von x, y. Die Belegungen notieren wir so: $\beta(x)\,\beta(y)$, also vier Möglichkeiten *ff*, *fw*[4], *wf*, *ww*. Die Wahrheitswerteverläufe so:

$$W_F(ff)\ W_F(fw)\ W_F(wf)\ W_f(ww)$$

.

[4] hier: $\beta(x) = f$ und $\beta(y) = w$

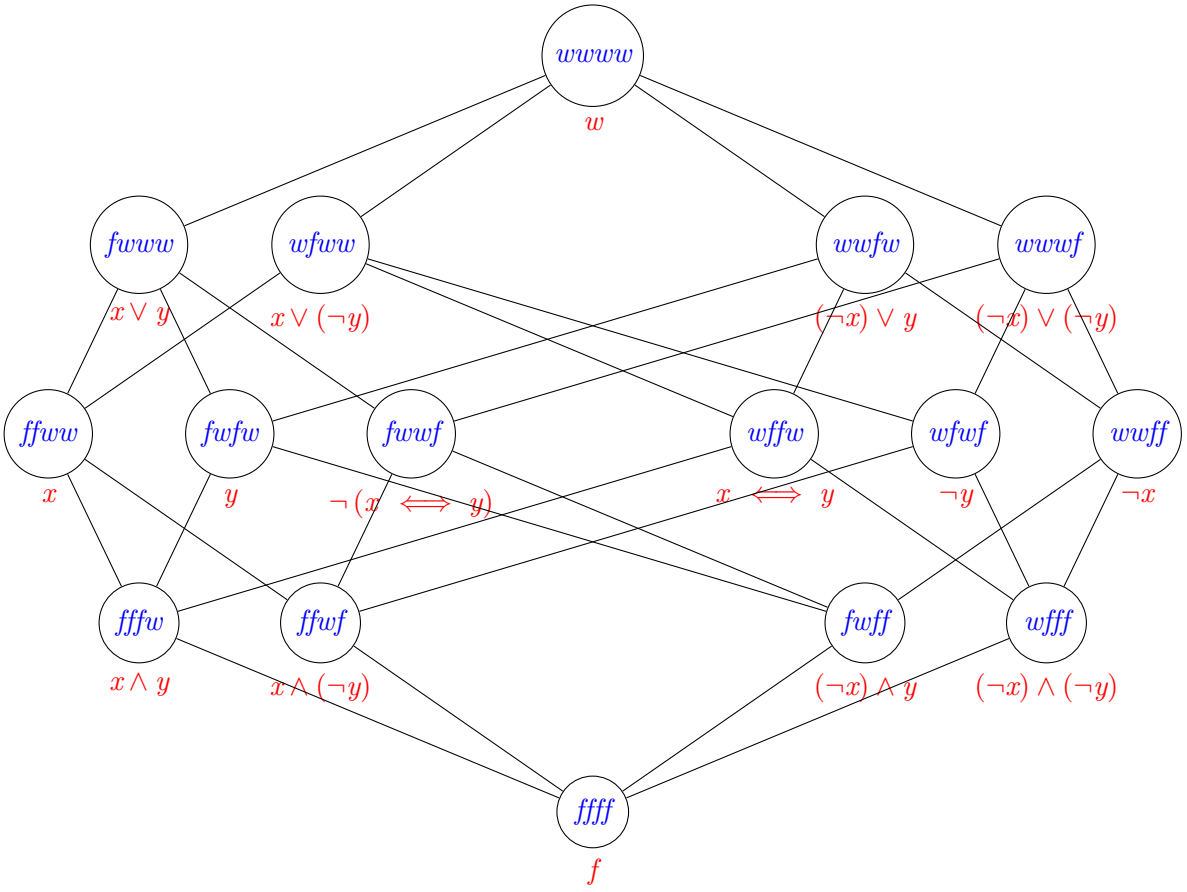


Abbildung 6.2.: 4D-Würfel der Ordnung $\leq$

7. Endliche diskrete Wahrscheinlichkeitsräume

7.1. Ein (endlicher, diskreter) *Wahrscheinlichkeitsraum* ist ein Paar (Ω, p) aus einer endlichen Menge Ω von *Elementarereignissen* und einer Funktion $p : \Omega \to \underset{\subseteq \mathbb{R}}{[0,1]}$ mit $\sum_{\omega \in \Omega} p(\omega) = 1$.

p heißt eine *Verteilung* auf Ω.
$A \subseteq \Omega$ heißt *Ereignis*, $p(A) := \sum_{\omega \in A} p(\omega)$ heißt *Wahrscheinlichkeit* von A.
Für Ereignisse $A, B, A_1, \ldots, A_k$ gilt z. B.

(i) $A \subseteq B \implies p(A) \leq p(B)$ (A *Teilereignis* von B)

(ii) $p(A \cup B) + p(A \cap B) = p(A) + p(B)$

(iii) Sind $A_1, \ldots, A_k$ paarweise disjunkt, so gilt $p(A_1 \cup \cdots \cup A_k) = p(A_1) + \cdots + p(A_k)$

(iv) $p(A_1 \cup \cdots \cup A_k) \leq p(A_1) + \cdots + p(A_k)$

(v) $p(A) + p\left(\underbrace{\Omega \setminus A}_{\text{Gegenereignis}}\right) = 1$

Beispiel:

$$\Omega = \{1, \ldots, 6\} \qquad \text{(Ergebnisse beim Würfeln)} \tag{7.1}$$

$$p = \left(\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}\right) \tag{7.2}$$

$$p(\{2,4,6\}) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2} \tag{7.3}$$

$$p = \left(\frac{1}{4}, \frac{1}{10}, \frac{1}{5}, \frac{1}{4}, \frac{1}{10}, \frac{1}{10}\right) \tag{7.4}$$

$$p(\{2,4,6\}) = \frac{9}{20} \tag{7.5}$$

Beispiel:

$$\Omega \neq \varnothing \tag{7.6}$$

$$p(\omega) = \frac{1}{|\Omega|} \qquad \text{definiert die sog. Gleichverteilung auf } \Omega \tag{7.7}$$

$$\text{Für } A \subseteq \text{ gilt dann:} \tag{7.8}$$

$$p(A) = \frac{|A|}{|\Omega|} \tag{7.9}$$

Satz 7.1. *Sind* $(\Omega_1, p_1), \ldots, (\Omega_n, p_n)$ *Wahrscheinlichkeitsräume, so ist durch*

$$p((\omega_1, \ldots, \omega_m)) = p_1(\omega_1) \cdot \cdots \cdot p_m(\omega_m) \tag{7.10}$$

für $(\omega_1, \ldots, \omega_m) \in \Omega \times \cdots \times \Omega_m$ *eine Verteilung auf* $\Omega = \Omega_1 \times \cdots \times \Omega_m$ *gegeben. Für* $A_1 \subseteq \Omega_1, \ldots, A_m \subseteq \Omega_m$ *gilt:*

$$p(A_1 \times \cdots \times A_m) = p_1(A_1) \cdot \cdots \cdot p_m(A_m) \tag{7.11}$$

$A_1 \times \cdots \times A_m$ *ist ein sogenanntes* Rechteckereignis.

Beweis.

$$\text{Offenbar: } p : \Omega \to [0,1] \tag{7.12}$$

$$\text{Seien } A_1, \ldots, A_m \text{ wie oben} \tag{7.13}$$

$$\Longrightarrow \prod_{j=1}^{m} p_j(A_j) = \prod_{j=1}^{m} \sum_{\omega_j \in A_j} p_j(\omega_j) \tag{7.14}$$

$$\text{Ausmultiplizieren:} \quad = \sum_{\substack{(\omega_1,\ldots,\omega_m) \\ \in A_1 \times \cdots \times A_m}} \underbrace{\prod_{j=1}^{m} p_j(\omega_j)}_{= p((\omega_1,\ldots,\omega_m))} \tag{7.15}$$

$$= \sum_{(\omega_1,\ldots,\omega_m) \in A_1 \times \cdots \times A_m} p((\omega_1, \ldots, \omega_m)) \tag{7.16}$$

$$\text{Summenkonvention:} \quad = p(A_1 \times \cdots \times A_m) \tag{7.17}$$

Insbesondere gilt für $\Omega = \Omega_1 \times \ldots \Omega_m$:

$$p(\Omega) = \prod_{j=1}^{m} p_j(\Omega_j) = 1 \tag{7.18}$$

$$\text{weil } (\Omega_j, p_j) \text{ Wahrscheinlichkeitsraum} \tag{7.19}$$

□

(Ω, p) aus dem Satz heißt *Produktraum* von $(\Omega_1, p_1), \dots (\Omega_m, p_m)$.

$$(\Omega_1, p_1) := (\Omega_2, p_2) = \left(\{1, \dots, 6\}, \left(\frac{1}{6}, \frac{1}{6}, \dots, \frac{1}{6}\right)\right) \quad \text{(Doppelwurf)} \tag{7.20}$$

$$A = \{i\} \times \Omega_2 = \{(i,1), (i,2), \dots, (i,6)\} \tag{7.21}$$

$$B = \Omega_1 \times \{j\} = \{(1,j), (2,j), \dots, (6,j)\} \tag{7.22}$$

$$A \cap B = \{(i,j)\} \tag{7.23}$$

$$p(A) = p_1(\{i\}) \cdot p_2(\Omega_2) \tag{7.24}$$

$$= \frac{1}{6} \cdot 1 = \frac{1}{6} \tag{7.25}$$

$$p(B) = P_1(\Omega_1) \cdot p_2(\{j\}) \tag{7.26}$$

$$= 1 \cdot \frac{1}{6} = \frac{1}{6} \tag{7.27}$$

$$p(A \cap B) = p(\{i\} \times \{j\}) \tag{7.28}$$

$$= p_1(\{i\}) \cdot p_2(\{j\}) \tag{7.29}$$

$$= \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36} \tag{7.30}$$

$$\implies p(A \cap B) = p(A) \cdot p(B) \tag{7.31}$$

7.2. Die Ereignisse $A, B \subseteq \Omega$ heißen *(stochastisch) unabhängig*, falls $p(A \cap B) = p(A) \cdot p(B)$ gilt.

7.3. Sei (Ω, p) ein Wahrscheinlichkeitsraum, $B \subseteq \Omega$ mit $p(B) > 0$. Dann ist $p_B : B \to [0,1]$, $p_B(\omega) = \frac{p(\omega)}{p(B)}$ Verteilung auf B, die sogenannte durch B *bedingte Verteilung*.
Es gilt: $p_B(A \cap B) = \frac{p(A \cap B)}{p(B)} =: p(A \mid B)$ für $A \subseteq \Omega$.
$p(A \mid B)$ heißt *bedingte Wahrscheinlichkeit* von A unter B. B ist das *bedingende Ereignis*.

Beweis.

$$p_B(A \cap B) = \sum_{\omega \in A \cap B} p_B(\omega) \tag{7.32}$$

$$\text{Nach Definition:} \quad = \sum_{\omega \in A \cap B} \frac{p(\omega)}{p(B)} \tag{7.33}$$

$$= \frac{1}{p(B)} \sum_{\omega \in A \cap B} p(\omega) \tag{7.34}$$

$$= \frac{1}{p(B)} p(A \cap B) \tag{7.35}$$

$$= \frac{p(A \cap B)}{p(B)} \tag{7.36}$$

Speziell für $A = B$:

$$p_B(B) = \frac{p(B \cap B)}{p(B)} \tag{7.37}$$

$$= \frac{p(B)}{p(B)} \tag{7.38}$$

$$= 1 \tag{7.39}$$

$$\text{d. h. } (B, p_B) \text{ ist Wahrscheinlichkeitsraum} \tag{7.40}$$

□

Satz 7.2 (Bayes, kleine Version)**.** *Sei* (Ω, p) *ein Wahrscheinlichkeitsraum und* $A, B \subseteq \Omega$ *mit* $p(A) > 0$*.*

$$\implies p(A \mid B) = \frac{p(B \mid A) \cdot p(A)}{p(B)} \tag{7.41}$$

Beweis.

$$\frac{p(B \mid A) \cdot p(A)}{p(B)} \overset{\text{Def.}}{=} \frac{\frac{p(B \cap A)}{p(A)} \cdot p(A)}{p(B)} \tag{7.42}$$

$$= \frac{p(B \cap A)}{p(A)} \tag{7.43}$$

$$= \frac{p(A \cap B)}{p(A)} \tag{7.44}$$

$$= p(A \mid B) \tag{7.45}$$

□

Satz 7.3 (Totale Wahrscheinlichkeit)**.** *Sei* (Ω, p) *ein Wahrscheinlichkeitsraum. Seien* $A_1, \ldots, A_k$ *paarweise disjunkt mit* $p(A_j) > 0$ *und* $\biguplus_{j=1} A_j = \Omega$*. Dann gilt für* $B \subseteq \Omega$*:*

$$p(B) = \sum_{j=1}^{k} p(B \mid A_j) \cdot p(A_j) \tag{7.46}$$

Beweis.

$$\sum_{j=1}^{k} p(B \mid A_j) \cdot p(A_j) = \sum_{j=1}^{k} \frac{p(B \cap A_j)}{p(A_j)} \cdot p(A_j) \tag{7.47}$$

$$= \sum_{j=1}^{k} p(B \cap A_j) \tag{7.48}$$

$$= p\left(\dot{\bigcup}_{j=1}^{k} B \cap A_j\right) \tag{7.49}$$

$$= p(B) \tag{7.50}$$

□

Satz 7.4 (Bayes, erweiterte Form)**.** Vss*: wie im vorangeganenen Satz,* $p(B) > 0$*.*

$$\forall i \in \{1, \ldots, b\} : p(A_i \mid B) = \frac{p(B \mid A_i) \cdot p(A_i)}{\sum_{j=1}^{k} (B \mid A_j) \cdot p(A_j)} \tag{7.51}$$

Beweis. Sofort aus den beiden vorangegangenen Sätzen. □

7.4. Sei (Ω, p) Wahrscheinlichkeitsraum. Eine Funktion $X : \Omega \to \mathbb{R}$ heißt *Zufallsvariable* (kurz: ZVA).

Weil Ω endlich ist, ist auch $X(\Omega) = \{X(\omega) : \omega \in \Omega\}$ endlich.

Durch $p_X(x) := p(X = x) := p(\{w \in \Omega : X(\omega) = x\})$ wird ein Wahrscheinlichkeitsraum auf (jeder endlichen Obermenge von) $X(\Omega)$ definiert, nämlich $(X(\Omega), p_X)$, denn $p_X : X(\Omega) \to [0, 1]$ und

$$\sum_{x \in X(\Omega)} p_X(X = x) = \sum_{x \in X(\Omega)} p(\{\omega \in \Omega : X(\omega) = x\}) = \sum_{\omega \in \Omega} p(\omega) = 1 \tag{7.52}$$

p_X heißt die *Verteilung der Werte von X*. $X(\Omega)$ ist dabei meist wesentlich kleiner als Ω.

Sei $(\Omega, p) := \left(\{1, \ldots, 6\}, \left(\frac{1}{6}, \ldots, \frac{1}{6}\right)\right) \times \left(\{1, \ldots, 6\}, \left(\frac{1}{6}, \ldots, \frac{1}{6}\right)\right)$. $X : \Omega \to \mathbb{R}$, $X((i, j)) := i + j \in \{2, \ldots, 12\}$.

Tabelle 7.1.: Wahrscheinlichkeitsverteilung von X

x	2	3	4	5	6	7	8	9	10	11	12
$p(X = x)$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

Zufallsvariablen $X_1, \ldots, X_n : \Omega \to \mathbb{R}$ heißen *stochastisch unabhängig*, falls

$$p(X_1 = x_1 \wedge X_2 = x_2 \wedge \cdots \wedge X_n = x_n) = p(X_1 = x_1) \cdot p(X_2 = x_2) \cdot \cdots \cdot p(X_n = x_n) \tag{7.53}$$

$$\widehat{=} \{\omega \in \Omega : X_1(\omega) = x_1 \wedge \cdots \wedge X_n(\omega) = x_n\} \tag{7.54}$$

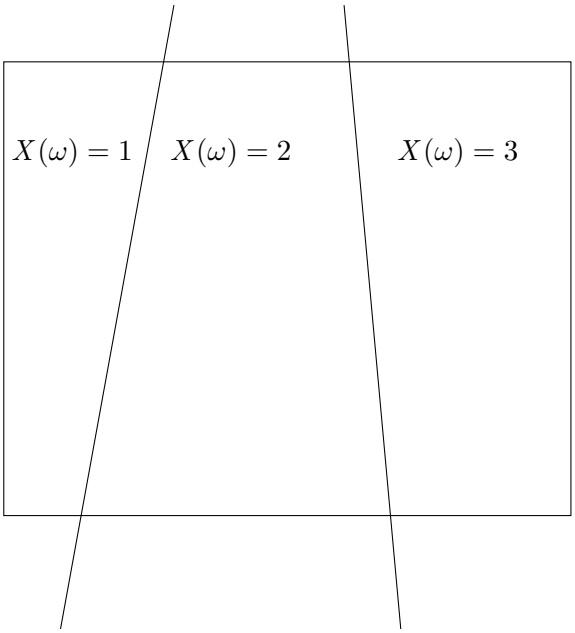


Abbildung 7.1.: Aufteilung des Wahrscheinlichkeitsraumes durch X

Beispiel: Sei X die Würfelnummer beim Doppelwurf und

$$Y(i,j) := \begin{cases} 0 & \text{, falls } i \text{ gerade} \\ 1 & \text{, sonst} \end{cases} \tag{7.55}$$

$$\implies p(Y=0) = \frac{1}{2} \tag{7.56}$$

$$= p(Y=1) = \frac{1}{2} \tag{7.57}$$

$$p(X=2 \wedge Y=0) = 0 \tag{7.58}$$

$$p(X=2) \cdot p(Y=0) = \frac{1}{36} \cdot \frac{1}{2} = \frac{1}{72} \neq 0 \tag{7.59}$$

$$\implies X, Y \text{ stochastisch abhängig} \tag{7.60}$$

7.5. Der Erwartungswert einer Zufallsvariablen X in einem Wahrscheinlichkeitsraum Ω ist:

$$E(X) := \sum_{\omega \in \Omega} p(\omega) \cdot X(\omega) = \int X \, \mathrm{d}p \tag{7.61}$$

[1] Das Integral da ist eigentlich Käse…

Sei $X : \Omega \to \mathbb{R}$ konstant $= c$.

$$\implies E(X) = \sum_{\omega \in \Omega} p(\omega) \cdot c \tag{7.62}$$

$$= c \cdot \sum_{\omega \in \Omega} p(\omega) \tag{7.63}$$

$$= c \cdot 1 = c \tag{7.64}$$

Sei X Zufallsvariable, $\alpha \in \mathbb{R}$.

$$\implies (\alpha \cdot X)(\omega) := \alpha \cdot X(\omega) \tag{7.65}$$

definiert eine Zufallsvariable $\alpha \cdot X$.

$$E(\alpha \cdot X) = \sum_{\omega \in \Omega} p(\omega) \cdot (\alpha \cdot X)(\omega) \tag{7.66}$$

$$= \sum_{\omega \in \Omega} p(\omega) \cdot \alpha \cdot X(\omega) \tag{7.67}$$

$$= \alpha \cdot \sum_{\omega \in \Omega} p(\omega) \cdot X(\omega) \tag{7.68}$$

Seien X, Y Zufallsvariablen. Durch $(X + Y)(\omega) := X(\omega) + Y(\omega)$ wird die Zufallsvariable $X + Y$ definiert.

$$E(X + Y) = \sum_{\omega \in \Omega} p(\omega) \cdot (X + Y)(\omega) \tag{7.69}$$

$$= \sum_{\omega \in \Omega} p(\omega) \cdot (X(\omega) + Y(\omega)) \tag{7.70}$$

$$= \sum_{\omega \in \Omega} p(\omega) \cdot X(\omega) + \sum_{\omega \in \Omega} p(\omega) \cdot Y(\omega) \tag{7.71}$$

$$= E(X) + E(Y) \tag{7.72}$$

Satz 7.5 (Linearität des Erwartungswertes)**.** *Sind X, Y Zufallsvariablen und $\alpha, \beta \in \mathbb{R}$, so gilt:*

$$E(\alpha X + \beta Y) = \alpha E(X) + \beta E(Y) \tag{7.73}$$

Es gilt außerdem:

$$E(X) \overset{Def.}{=} \sum_{\omega \in \Omega} p(\omega) \cdot X(\omega) \tag{7.74}$$

$$= \sum_{x \in X(\Omega)} x \cdot p(X = x) \tag{7.75}$$

7.6. Die Varianz einer Zufallsvariablen X:

$$\operatorname{Var}(X) := E\Big((X - E(X))^2\Big) \tag{7.76}$$

ist die erwartete (bzw. mittlere) quadratische Abweichung von X und $E(X)$.

$$\begin{aligned}
\operatorname{Var}(X) &= E((X - E(X)(X - E(X)))) && (7.77)\\
&= E\Big(X^2 - 2XE(X) + (E(X))^2\Big) && (7.78)\\
&= E\big(X^2\big) - 2E(X \cdot E(X)) + E\Big((E(X))^2\Big) && (7.79)\\
&= E\big(X^2\big) - 2E(X)\,E(X) + (E(X))^2 && (7.80)\\
&= E\big(X^2\big) - (E(X))^2 && (7.81)
\end{aligned}$$

Für eine $0,1$-wertige Zufallsvariable gilt: $X^2 = X$, also $\operatorname{Var}(X) = E(X) - (E(X))^2$.

Drogentest (Nachtrag zur bedingten Wahrscheinlichkeit): Der Test liefert mit 99% Wahrscheinlichkeit die richtige Antwort, d. h. positiv, falls Abhängigkeit besteht, mit Wahrscheinlichkeit 99% und negativ, falls keine Abhängigkeit besteht, mit Wahrscheinlichkeit 99%.

Annahme: $0,5\%$ aller Testpersonen sind abhängig.

Wie wahrscheinlich ist es nun, dass eine Testperson, die positiv getestet wird, auch wirklich abhängig ist?

$$\begin{aligned}
p(\text{abh.} \mid \text{pos.}) &= \frac{p(\text{pos.} \mid \text{abh.}) \cdot p(\text{abh.})}{p(\text{pos.} \mid \text{abh.}) \cdot p(\text{abh.}) + p(\text{pos.} \mid \text{n. abh.}) \cdot p(\text{n. abh.})} && (7.82)\\
&= \frac{0,99 \cdot 0,005}{0,99 \cdot 0,005 + 0,01 \cdot 0,995} && (7.83)\\
&= 33,2\% && (7.84)
\end{aligned}$$

7.1. Der Binomialkoeffizient

Sie N Menge und $k \in \mathbb{N}$.

$$\binom{N}{k} := \Big\{X \subseteq N \colon |X| = k\Big\} \tag{7.85}$$

Für $n \in \mathbb{N}$ sei

$$\begin{aligned}
\binom{n}{k} &:= \left|\binom{\{1,\dots,n\}}{k}\right| && (7.86)\\
&= \left|\binom{N}{k}\right|, \text{ falls } \ |N| = n. && (7.87)
\end{aligned}$$

Satz 7.6.

$$\binom{n}{0} = \binom{n}{n} = 1 \quad \forall n \geq 0 \tag{7.88}$$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad \forall n \geq 1, k \geq 1, k \leq n-1 \tag{7.89}$$

Beweis. Für jedes N ist

$$\binom{N}{0} = \{\varnothing\} \tag{7.90}$$

$$\text{und } \binom{N}{n} = \{N\}, \tag{7.91}$$

$$\text{also } \binom{n}{0} = \binom{n}{n} = 1 \tag{7.92}$$

Also gilt der erste Teil der Behauptung.

Habe N n viele Elemente, $n \geq 1$.

$$\text{Sei } z \in N \tag{7.93}$$

$$\text{Setze } M = N \setminus \{z\} \tag{7.94}$$

$$\text{Für } X \in \binom{N}{k} \tag{7.95}$$

$$\text{setze } f(X) = X \setminus \{z\} \tag{7.96}$$

$$= \begin{cases} \binom{M}{k} & \text{, falls } z \notin X \\ \binom{M}{k-1} & \text{, falls } z \in X \end{cases} \tag{7.97}$$

$$\text{Dies definiert } f\colon \binom{N}{k} \to \binom{M}{k} \dot{\cup} \binom{M}{k-1} \tag{7.98}$$

$$\not{z}\text{:} \quad f \text{ bijektiv} \tag{7.99}$$

„injektiv“:

$$\text{Aus } f(X) = f(Y) \tag{7.100}$$
$$\text{folgt } X \setminus \{x\} = Y \setminus \{z\} \tag{7.101}$$
$$\text{Wegen } |X| = |Y| = k \tag{7.102}$$
$$\text{folgt } |X \setminus \{z\}| = \begin{cases} k & \text{, falls } z \notin X \\ k-1 & \text{, falls } z \in X \end{cases} \tag{7.103}$$
$$\text{sowie } |Y \setminus \{z\}| = \begin{cases} k & \text{, falls } z \notin Y \\ k-1 & \text{, falls } z \in Y \end{cases} \tag{7.104}$$
$$\text{Wegen } |X \setminus \{z\}| = |Y \setminus \{z\}| \tag{7.105}$$
$$\text{folgt } (z \in X \wedge z \in Y) \text{ oder } (z \notin X \wedge z \notin Y) \tag{7.106}$$

Im ersten Fall folgt:

$$X \overset{z \in X}{=} (X \setminus \{z\}) \cup \{z\} \tag{7.107}$$
$$\overset{X\setminus\{z\}=Y\setminus\{z\}}{=} (Y \setminus \{z\}) \cup \{z\} \tag{7.108}$$
$$= Y \tag{7.109}$$

Im zweiten Fall folgt:

$$X \overset{z \notin X}{=} X \setminus \{z\} \tag{7.110}$$
$$= Y \setminus \{z\} \tag{7.111}$$
$$= Y \tag{7.112}$$

In beiden Fällen:

$$X = Y \tag{7.113}$$

„surjektiv“:

$$\text{Für } Z \in \binom{M}{k} \tag{7.114}$$
$$\text{folgt } Z \in \binom{N}{k} \tag{7.115}$$
$$\text{und } f(Z) = Z \tag{7.116}$$
$$\text{Für } Z \in \binom{M}{k-1} \tag{7.117}$$
$$\text{folgt } Z \dot{\cup} \{z\} \in \binom{N}{k} \tag{7.118}$$
$$\text{und } f(Z \cup \{z\}) = Z \tag{7.119}$$

Also ist f bijektiv, somit

$$\left|\binom{N}{k}\right| = \left|\binom{M}{k} \cup \binom{M}{k-1}\right| \tag{7.120}$$

$$= \left|\binom{M}{k}\right| + \left|\binom{M}{k-1}\right| \tag{7.121}$$

$$\text{also } \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \tag{7.122}$$

□

Aus dieser Rekursionsformel ergibt sich das sogenannte PASCAL*sche Dreieck* (sh. TODO).

Satz 7.7.

$$\binom{n}{0} = \binom{n}{n} \text{ für } n \geq 0 \tag{7.123}$$

$$\text{und } \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \text{ für } k \geq 1, k \leq n-1 \tag{7.124}$$

Beweis.

$$\binom{n}{0} = \frac{n!}{0!\,(n-0)!} \tag{7.125}$$

$$= \frac{n!}{n!} = 1 \tag{7.126}$$

$$\text{und } \binom{n}{n} = \frac{n!}{n!\,(n-n)!} \tag{7.127}$$

$$= 1 \tag{7.128}$$

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{k\,(n-1)!}{k\,(k-1)!\,(n-1-(k-1))!} + \frac{(n-1)!}{k!\,(n-1-k)!\,(n-k)!} \tag{7.129}$$

$$= \frac{k\,(n-1)! + (n-1)!\,(n-k)}{k!\,(n-k)!} \tag{7.130}$$

$$= \frac{(k+n-k)\,(n-1)!}{k!\,(n-k)!} \tag{7.131}$$

$$= \frac{n!}{k!\,(n-k)!} \tag{7.132}$$

$$= \binom{n}{k} \tag{7.133}$$

□

Die Zahlen $\binom{n}{k}$ heißen *Binomialkoeffizienten.*

Binomialsatz:

$$(a+b)^0 = 1 \tag{7.134}$$
$$(a+b)^1 = a+b \tag{7.135}$$
$$(a+b)^2 = a^2+2ab+b^2 \tag{7.136}$$
$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 \tag{7.137}$$
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{(n-k)} \tag{7.138}$$

Beweis.

Ausmultiplizieren:

$$(a+b)^n = \sum_{(\alpha_1,\ldots,\alpha_n)\in\{a,b\}^n} \prod_{j=1}^{n} \alpha_j \tag{7.139}$$
$$= \sum_{k=0}^{n} \sum_{\substack{(\alpha_1,\ldots,\alpha_n)\in\{a,b\}^n \\ \alpha_i=a \text{ für genau} \\ k \text{ viele } i\in\{1,\ldots,n\}}} \prod_{j=1}^{n} a_j \tag{7.140}$$
$$= \sum_{k=0}^{n} \sum_{\substack{(\alpha_1,\ldots,\alpha_n)\in\{a,b\}^n \\ \alpha_i=a \text{ für genau} \\ k \text{ viele } i\in\{1,\ldots,n\}}} a^k b^{n-k} \tag{7.141}$$
$$= \sum_{k=0}^{n} \sum_{J\in\binom{\{1,\ldots,n\}}{k}} a^k b^{n-k} \tag{7.142}$$
$$= \sum_{k=0}^{n} a^k b^{n-k} \sum_{J\in\binom{\{1,\ldots,n\}}{k}} 1 \tag{7.143}$$
$$= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{7.144}$$

□

7.2. Bernoulli-Verteilung

Sei (Ω, p) Wahrscheinlichkeitsraum. Die Zufallsvariable $X : \Omega \to \{0, 1\}$ heißt BERNOULLI-*verteilt* mit Erfolgswahrscheinlichkeit p^*, falls gilt

$$p(X = 1) = p^* \tag{7.145}$$
$$p(X = 0) = 1 - p^* \tag{7.146}$$
$$\tag{7.147}$$

Dann ist

$$E(X) = \sum_{\omega \in \Omega} X(\omega)\, p(\omega) \tag{7.148}$$
$$= 1 - p(X = 1) + 0 \cdot p(X = 0) \tag{7.149}$$
$$= p^* \tag{7.150}$$
$$\operatorname{Var}(X) = E\left(X^2\right) - E(X)^2 \tag{7.151}$$
$$= p^* - p^{*2} \tag{7.152}$$
$$= p^*(1 - p^*) \tag{7.153}$$

Seien $X_1, \ldots, X_n$ unabhängige Bernoulli-verteilte Zufallsvariablen mit (gleicher) Erfolgswahrscheinlichkeit p^*. Setze $X = X_1 + \cdots + X_n : \Omega \to \{0, 1, 2, \ldots, n\}$. Es gilt

$$p(X = k) = \sum_{J \in \binom{\{1,\ldots,n\}}{k}} p(X_j = 1 \text{ für } j \in J \text{ und } X_j = 0 \text{ für } j \notin J) \tag{7.154}$$

$$\overset{\substack{X_1,\ldots,X_n \text{ statist.} \\ \text{unabh.}}}{=} \sum_{J \in \binom{\{1,\ldots,n\}}{k}} \prod_{j=1}^{n} \begin{cases} p(X_j = 1) & \text{für } j \in J \\ p(X_j = 0) \end{cases} \tag{7.155}$$

$$= \sum_{J \in \binom{\{1,\ldots,n\}}{k}} p^{*k}(1 - p^*)^{n-k} \tag{7.156}$$

$$= \binom{n}{k} p^{*k}(1 - p^*)^{n-k} \tag{7.157}$$

Eine Zufallsvariable $X : \Omega \to \{0, 1, \ldots, n\}$ heißt *binomialverteilt* in den Parametern n und p^*, falls

$$p(X = h) = \binom{n}{k} p^{*k}(1 - p^*)^{n-k} \tag{7.158}$$
$$\tag{7.159}$$

Schreibweise:

$$X \sim B(n, p)$$

Übungsaufgabe: Man bestimme $\mathrm{Var}(X)$; $E(X) = E(X_1 + \cdots + X_n) = E(X_1) + \cdots + E(X_n) = p^* + \cdots + p^* = np^*$.

7.3. Multimonialverteilung

7.7.

$$\begin{bmatrix} n \\ k_1, \ldots, k_1 \end{bmatrix} := \frac{n!}{k_1! k_2! \cdot \cdots \cdot k_r!} \tag{7.160}$$

wobei $k_1, \ldots, k_r \geq 0$ und $k_1 + \cdots + k_r = n$.

$$\left(\begin{array}{c} N \\ k_1, \ldots, k_r \end{array} \right) := \text{ Menge der Abbildungen } f\colon N \to \{1, \ldots, r\} \text{ mit} \tag{7.161}$$

$$\mid f^{-1}(\{j\}) = \{x \in N : f(x) = j\} \mid = k_j \quad \forall j \in \{1, \ldots, r\} \tag{7.162}$$

$$\left(\begin{array}{c} n \\ k_1, \ldots, k_r \end{array} \right) := \left| \left(\begin{array}{c} \{1, \ldots, n\} \\ k_1, \ldots, k_r \end{array} \right) \right| \tag{7.163}$$

Man erhält (ohne Beweis):

$$\binom{n}{k_1, \ldots, k_r} = \left[\begin{array}{c} n \\ k_1, \ldots, k_r \end{array} \right] \tag{7.164}$$

Beispiel:

$$\left[\begin{array}{c} n \\ k \end{array} \right] = \left[\begin{array}{c} n \\ k, n-k \end{array} \right] \tag{7.165}$$

Sei $X_j \sim B(n, p_j)$ binomialverteilt in den Parametern n, p_j für $j \in \{1, \ldots, r\}$. Seien $X_1, \ldots, X_r$ stochastisch unabhängig. Dann gilt:

$$p(X_1 = k_1 \text{ und } \ldots \text{ und } X_r = k_r) = \frac{n!}{k_1! \cdot \cdots \cdot k_r!} \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_r^{k_r}, \tag{7.166}$$

$$\text{wobei } k_1 + k_2 + \cdots + k_r = n \tag{7.167}$$

7.8. Eine Zufallsvariable

$$X : \Omega \to \mathbb{R}^d \tag{7.168}$$

heißt *d-dimensionale Zufallsvariable*.

$$X(\omega) = \begin{pmatrix} X_1(\omega) \\ \vdots \\ X_j(\omega) \end{pmatrix} \tag{7.169}$$

Setze $p(X = x) := p(\{\omega \in \Omega : X(\omega) = x\})$ (die sogenannte *multivariale*).

$$(x_1, \ldots, x_d) \in \mathbb{R}^d \tag{7.170}$$

$$X_1(\omega) = x_1 \wedge \cdots \wedge X_j(\omega) = x_d \tag{7.171}$$

Gilt $p(X = (k_1, \ldots, k_d)) = \frac{n!}{k_1! \cdot \ldots \cdot k_d!} \cdot p_1^{k_1} \cdot \ldots \cdot p_d^{k_d}$ für $k_1, \ldots, k_d \geq 0$ aus N mit $k_1 + \cdots + k_d = n$ (für feste $p_1, \ldots, p_d \geq 0$ mit $p_1 + \cdots + p_d = 1$), so heißt X *multimonialverteilt* in den Parametern $p_1, \ldots, p_d$.

7.4. Hypergeometrische Verteilung

Es sei eine Urne mit zwei Sorten Kugeln.

- N: Gesamtzahl der Kugeln
- M: Anzahl der Kugeln der Sorte 1
- $N - M$: Anzahl der Kugeln der Sorte 2
- n: Stichprobengröße
- X: Anzahl der Kugeln von Sorte 1 einer n-elementigen zufälligen Stichprobe

$$p(X = k) = \frac{\binom{M}{k}\binom{N-M}{n-k}}{\binom{N}{n}} \tag{7.172}$$

$$\text{Sorte 1: } k \in \binom{M}{k} \tag{7.173}$$

$$\text{Sorte 2: } n - k \in \binom{N-M}{n-k} \tag{7.174}$$

Eine Zufallsvariable $X : \Omega \to \{0, \ldots, M\}$ mit

$$p(X = k) = \frac{\binom{M}{k} \cdot \binom{N-M}{n-k}}{\binom{N}{n}} \tag{7.175}$$

heißt *hypergeometrisch verteilt* in den Parametern N, M, n.

$$E(X) = n \cdot \frac{M}{N} \tag{7.176}$$

$$\operatorname{Var}(X) = n \cdot \frac{M}{N} \left(1 - \frac{M}{N}\right) \binom{N-n}{N-1} \tag{7.177}$$

8. Elementare Graphentheorie

8.1. Ein *Graph* $G = (V, E)$ ist ein Paar, bestehend aus einer endlichen Menge V von Ecken und einer Menge $E \subseteq \{\{x, y\} : x \neq y \text{ aus } V\}$ von *Kanten*.
Schreibweise: xy statt $\{x, y\}$, folglich $xy = yx$.

8.2. Eine Folge $W = x_0 \dots x_l$ von paarweise verschiedenen Ecken mit $x_{i-1}x_i \in E$ für $i \in \{i, \dots, l\}$ heißt ein *Weg von* x_0 *nach* x_l der Länge l ($l \geq 0$), oder kurz x_0, x_l-*Weg*.

Durch

$$a \sim b \iff \exists a, b\text{-Weg in } G \tag{8.1}$$

wird eine Äquivalenzrelation auf V definiert.

8.3. Ein Graph H heißt *Teilgraph* des Graphen G, falls $V(H) \subseteq V(G)$ und $E(H) \subseteq E(G)$.

Für $A \subseteq V(G)$ heißt $G[A] := (A, \{xy \in E(G) : x, y \in A\})$ der von A *induzierte* Teilgraph.
Für $F \subseteq E(G)$ heißt $G[F] := (V(G), F)$ der von F *induzierte* Teilgraph.
Für $A \subseteq V(G)$ sei $G - A := G[V(G) \setminus A]$, für $F \subseteq E(G)$ sei $G - F := G[E(G) \setminus F]$.
Ist $W = x_0 \dots x_l$ ein Weg, so definiere

$$V(W) = \{x_0, \dots, x_l\}, \tag{8.2}$$
$$E(W) = \{x_0x_1, x_1x_2, \dots, x_{l-1}x_l\} \tag{8.3}$$

Auch der Teilgraph $H = (V(W), E(W))$ heißt ein x_0x_l-Weg der Länge l.
Die Äquivalenzklassen von $\sim$ heißen *Zusammenhangskomponenten* von G (s. o.). Auch die von ihnen induzierten Teilgraphen heißen Zusammenhangskomponenten.
G heißt *k-zusammenhängend*, falls $G - S$ zusammenhängend ist für jedes $S \subseteq V(G)$ mit $|S| < k$ sowie $|V(G)| > k$ gilt.
Ein Graph heißt *planar*, falls er sich „überschneidungsfrei in die Ebene (oder Kugeloberfläche) zeichnen lässt."

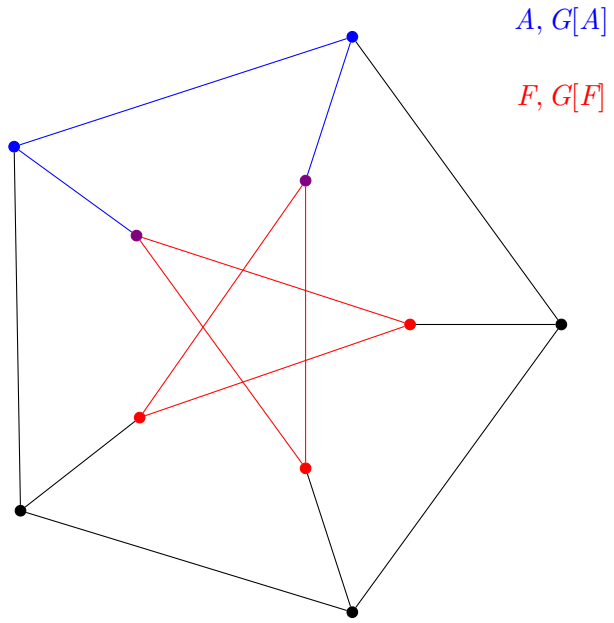


Abbildung 8.1.: Subgraphen in einem PETERSEN-Graph

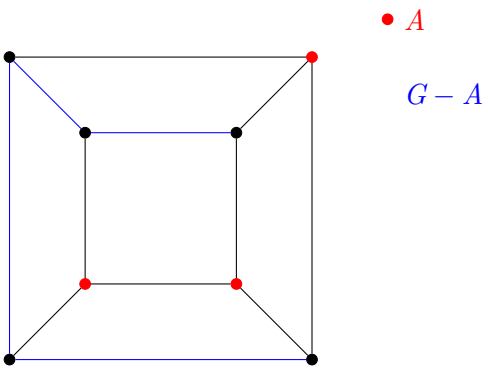


Abbildung 8.2.: Ein Graph $G - A$ in einem Graphen G

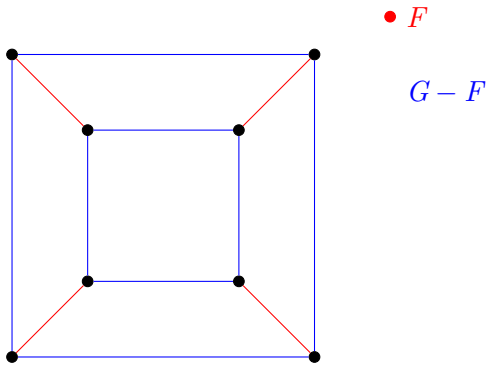


Abbildung 8.3.: Ein Graph $G - F$ in einem Graphen G

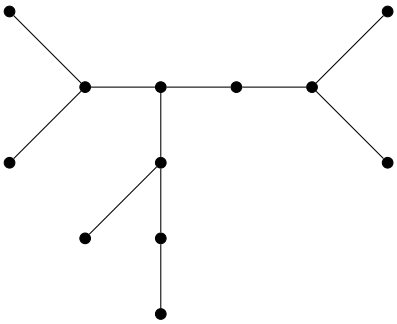


Abbildung 8.4.: Ein 1-zusammenhängender, jedoch nicht 2-zusammenhängender Graph

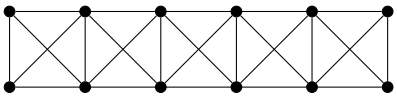


Abbildung 8.5.: Ein 2-zusammenhängender, jedoch nicht 3-zusammenhängender Graph

Abbildung 8.6.: Ein planarer Graph

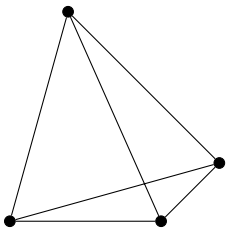


Abbildung 8.7.: Ein nicht planarer Graph

Nicht k-zusammenhängend zu sein ist „leicht zu zertifizieren“. k-zusammenhängend zu sein ist „etwas schwerer“ zu zertifizieren: Dazu generiere man alle Graphen $G - S$ mit $|S| < k$; diese sind (im Falle, dass G k-zusammenhängend ist) zusammenhängend. Das sind $\binom{n}{k-1} + \binom{n}{k-2} + \cdots + \binom{n}{0}$ viele, wenn G n Ecken hat.

Planar zu sein, ist durch Zeichnen des Graphen leicht zu verifizieren. Nicht planar zu sein, scheint schwerer zu verifizieren.

Satz 8.1 (Menger)**.** *Ein Graph G ist genau dann k-zusammenhängend, wenn $|V(G)| > k$ und für je zwei (nicht benachbarte) Ecken $a \neq b$ k viele* offen-disjunkte *a, b-Wege existieren, d. h. Wege, die außer a und b paarweise keine Ecken gemeinsam haben.*

(Ohne Beweis, aus der Existenz von jeweils k Wegen wie oben folgt jedoch leicht, dass G k-zusammenhängend ist; Gegenrichtung ist schwieriger)

Das Zertifikat für einen k-zusammenhängenden Graphen ist ein Wegesystem für jedes Eckenpaar. Damit gibt es „nur noch“ $\binom{n}{2}$ viele Teilzertifikate.

8.1. Minoren

8.4. Ein Graph H heißt *Minor* des Graphen G, falls es eine Familie $(V_x)_{x \in V(X)}$ von paarweise disjunkten Teilmengen von V_x von $V(G)$ gibt mit:

(i) $\forall x \in V(A) : G[V_x]$ ist zusammenhängend und nichtleer

(ii) $\forall xy \in E(H)$ sind V_x, V_y *benachbart*, d. h. es gibt (wenigstens) eine Kante $ab \in E(G)$ mit $a \in V_x$ und $b \in V_y$.

Schreibweise: $H \preccurlyeq G$; $\preccurlyeq$ reflexiv und transitiv (ohne Beweis), also Quasiordnung.

Ist H ein Teilgraph von G, so ist H auch ein Minor von G, denn:

$$(V_x)_{x \in V(H)}\,,\ V_x = \{x\} \tag{8.4}$$

erfüllt sowohl (i) also auch (ii) Kriterien.

Zwei Graphen G, H heißen *isomorph* (gleichgestaltig, $G \cong H$), wenn es eine Bijektion $\varphi : V(G) \to V(H)$ gibt mit $\forall x \neq y \in V(G) : xy \in E(G) \iff \varphi(x)\varphi(y) \in E(H)$. Dabei ist $\cong$ eine Äquivalenzrelation.

Im Fall $H \cong G$ ist $H \preccurlyeq G$ (rechne selbst) sowie $G \preccurlyeq H$. Folglich sind isomorphe Graphen wechselseitig Minoren voneinander, jedoch nicht unbedingt gleich.

8.5. Für $xy \in E(G)$ entstehe $G_{/xy}$ aus $G - \{x, y\}$ durch Hinzufügen einer neuen Ecke v und aller Kanten vz mit $xz \in E(G - xy)$ oder $yz \in E(G - xy)$. *Dies entspricht informell etwa dem Vorgang, die beiden Ecken der Kante xy „zusammenzuziehen“, sodass aus ihnen eine einzelne Ecke wird. Gibt es nun zwischen zwei benachbarten Ecken mehrere „gleiche“ Kanten, so werden diese zu einer „vereinigt“.*

Somit gilt: H ist Minor von G genau dann, wenn sich ein Teilgraph von G schrittweise auf einen zu H isomorphen Graphen kontrahieren lässt.

Satz 8.2 (Wagner/Kuratowski)**.** *G ist genau dann planar, wenn weder K_5[1] noch $K_{3,3}$[2] Minor von G ist.*

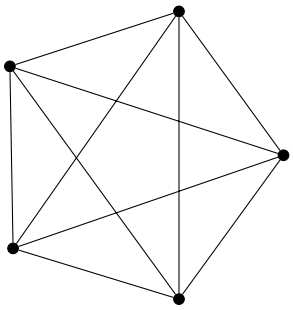


Abbildung 8.8.: Graph K_5

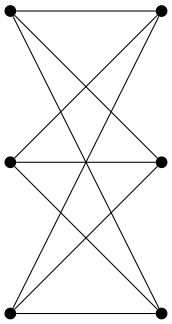


Abbildung 8.9.: Graph $K_{3,3}$

Nicht planar zu sein, lässt sich folglich durch Angabe eines Minor K_5 oder $K_{3,3}$ zertifizieren. Beispielsweise ist der Petersen-Graph[3] nicht planar, da dieser K_5 als Minor hat.

Planarität lässt sich komplett kombinatorisch beschreiben.

8.6. Eine Quasiordnung $\preccurlyeq$ auf A (d. h. $\leq$ ist reflexiv und transitiv) heißt *Wohlquasiordnung* (WQO) auf A, falls es zu jeder Folge $a_0, a_1, a_2, \ldots$ von Elementen aus A ein Indexpaar $i < j$ gibt mit $a_i \leq a_j$.

Satz 8.3 (Minorensatz, Robertson/Seymour, 1989–2006)**.** *Die Klasse der endlichen Graphen ist durch $\preccurlyeq$ wohlquasigeordnet.*

Anders ausgedrückt: Sind $G_0, G_1, G_2, \ldots$ endliche Graphen, so gibt es ein $i < j$, mit $G_i \preccurlyeq G_j$.

Sei $\leq$ eine Quasiordnung auf A und ein $c \in A$ quasiminimal : $\iff$ $x \leq c \implies c \leq x \quad \forall x \in A$.

[1] Siehe Abbildung 8.8
[2] Siehe Abbildung 8.9
[3] Siehe Abbildung 8.1

Lemma 8.4. *Sei A durch $\leq$ wohlquasigeordnet. Dann existiert zu jedem $a \in A$ ein quasiminimales Element $c \leq a$.*

Beweis. Angenommen, die Behauptung gelte nicht.

$$\implies a_0 := a \quad \text{nicht quasiminimal} \tag{8.5}$$
$$\overset{\text{Def.}}{\implies} \exists a_1 \leq a_0 : a_0 \not\leq a_1 \tag{8.6}$$
$$\implies a_1 \text{ nicht quasiminimal} \tag{8.7}$$
$$\overset{\text{Def.}}{\implies} \exists a_2 \leq a_1 : a_1 \not\leq a_2 \tag{8.8}$$
$$\implies a_2 \text{ nicht quasiminimal} \tag{8.9}$$
$$\vdots \tag{8.10}$$

Man erhält $a_0, a_1, a_2, \ldots$ mit $a = a_0 \geq a_1 \geq a_2 \geq \ldots$ und $a_0 \not\leq a_1 \not\leq a_2 \not\leq \ldots$.

$$\overset{\text{Def.}}{\implies} \exists i < j : a_i \leq a_j \tag{8.11}$$
$$\implies a_i \geq a_{i+1} \geq a_{i+2} \cdots \geq a_j \geq a_i \tag{8.12}$$

Aus der Transitivität von $\leq$ folgt:

$$\implies a_{i+1} \geq a_i \;\lightning \tag{8.13}$$

□

Lemma 8.5. *Ist $\leq$ eine Wohlquasiordnung auf A und $S \subseteq A$, $S \neq A$, gegen $\leq$* abgeschlossen[4]*, so existiert ein* endliches *$F \subseteq A$ mit:*

$$\forall x \in F : a \in S \iff x \not\leq a \tag{8.14}$$

Beweis. Sei $M = \{c \in A \setminus S : c \text{ quasiminimal in } A \setminus S\}$. Durch

$$c \sim c' \iff c \leq c' \text{ und } c' \leq c \tag{8.15}$$

wird eine Äquivalenzrelation auf M definiert. Elemente verschiedener Äquivalenzklassen sind unvergleichbar, denn aus $c \leq c'$ folgt $c' \leq$ (weil c' quasiminimal ist), also $[c]_{/\sim} = [c']_{/\sim}$.

Gäbe es unendlich viele Klassen, so auch unendlich viele paarweise unvergleichbare Elemente, also auch $a_0, a_1, a_2, a_3, \ldots$ mit $\forall i \neq j \in \mathbb{N} : a_i \not\leq a_j$. $\lightning \leq$ WQO

Also hat $\sim$ nur unendlich viele Äquivalenzklassen. Man wähle aus jeder Klasse genau einen Vertreter. Sei F die Menge dieser Vertreter. Dann leistet F das Gewünschte.

„⇒“: Sei $a \in S$. Wäre $x \leq a$ für ein $x \in F$, so $x \in S$, jedoch $F \subseteq M \subseteq A \setminus S$, d. h. $x \notin S$ $\lightning$

[4] d. h. aus $x \leq y \in S$ folgt $x \in S$.

„⇐“: Sei $a \notin S$.

$$\implies a \in A \setminus S \tag{8.16}$$

$$\overset{\text{Satz 8.4}}{\implies} \exists c \in M : c \leq a \tag{8.17}$$

Nach der Wahl von F existiert ein Vertreter $x \in F$ mit $x \leq c$ und $c \leq x$.

$$\implies x \leq c \leq a \tag{8.18}$$

$$\implies x \leq a \tag{8.19}$$

□

Daraus folgt, dass zu jeder echten Klasse von endlichen Graphen $\mathfrak{H}$, die gegen $\preccurlyeq$ abgeschlossen ist, existiert eine endliche Menge F von endlichen Graphen mit:

$$G \in \mathfrak{H} \iff H \not\preccurlyeq \quad \forall H \in F \tag{8.20}$$

Beweis. Man spezialisiere das vorangegangene Lemma auf die Menge aller Graphen G mit $V(G) \subseteq \mathbb{N}$. □

F heißt auch *Kuratowski-Menge* für die Klasse $\mathfrak{H}$.

$\mathfrak{H}$ ist genau dann $\preccurlyeq$-abgeschlossen, wenn die Löschung von Ecken/Kanten und die Kontraktion von Kanten in einem Graphen aus $\mathfrak{H}$ stets wieder einen Graphen aus $\mathfrak{H}$ ergibt.

Die Eigenschaft, überschneidungsfrei in die Ebene (äquivalent, auf der Kugeloberfläche) zeichenbar zu sein, definiert eine $\preccurlyeq$-abgeschlossene Klasse; $\{K_5, K_{3,3}\}$ ist eine Kuratowski-Menge hierfür. Entsprechend gibt es auch für den Torus und (und andere Oberflächen) eine Kuratowski-Menge. Diese ist jedoch nicht bekannt und enthält wenigstens 20 000 viele Graphen. Für die Kleinsche Flasche kennt man die Kuratowski-Menge (circa 135 Graphen).

Das Problem, der Entscheidung, ob ein (fester) Graph Minor des Eingabegraphen ist, in $O\left(|V(G)|^3\right)$ lösbar. Also kann auch in kubischer Zeit getestet werden, ob ein Eingabegraph in einer festen $\preccurlyeq$-abgeschlossenen Klasse $\mathfrak{H}$ liegt.

8.2. Bäume

8.7. Ein *Baum* T ist ein zusammenhängender Graph mit $\forall e \in E(T) : T - e$ *nicht* zusammenhängend.

Es gibt viele weiter Charakterisierungen, z. B.

- zusammenhängend und „kreisfrei[5]“
- zusammenhängend und $|V(G)| - 1 = |E(G)|$

[5] siehe Abschnitt 8.2.3

- zusammenhängend und maximal (bzgl. „Kanten hinzufügen“) in der Eigenschaft, keinen Kreis zu haben

8.8. Ein *Wald* ist ein Graph, dessen Komponenten Bäume sind.
Ein zusammenhängender Wald ist ein Baum.

Ein Wald ist ein „kreisfreier“ Graph.

8.9. Ein *Teilwald/ Teilbaum* ist ein Teilgraph von G, der ein Wald/Baum ist.

8.10. Ein aufspannender Teilgraph von G ist ein Teilgraph von H von G mit $V(H) = V(G)$

8.11. Ein *Spannbaum* von G ist ein aufspannender Teilgraph von G.

Satz 8.6. *Sei x_0 Ecke des Graphen G.*
⊛ Wenn es unter den bereits gewählten Ecken $x_0, \dots, x_l$ eine Ecke x_t gibt, die einen Nachbarn $y \in V(G) \setminus \{x_0, \dots, x_l\}$ gibt, dann setze man $x_{l+1} := y$ und setze $f(l+1) = t$; iteriere ⊛.[6]
Das Verfahren endet mit einem Spannbaum

$$T := \left(\{x_0, \dots, x_l\}, \left\{x_t x_{f(t)} : t \in \{1, \dots, l\}\right\}\right) \tag{8.21}$$

derjenigen Komponente von G, die x_0 enthält.

Beweis. Das Verfahren endet, weil G endlich ist.
Sei $T_S := \left(\{x_0, \dots, x_l\}, \left\{x_t x_{f(t)} : t \in \{1, \dots, s\}\right\}\right)$. Man zeige T_S ist ein Teilbaum von G induktiv über s.
Das Verfahren ist richtig für $T_S = (\{x_0\}, \varnothing)$. ✓
T_{S+1} entsteht aus T_S durch das Hinzufügen einer Ecke x_{S+1} und einer Kante $x_{S+1}x_{f(S+1)}$.[7] Zwischen je zwei Ecken x_i, x_j mit $i \neq j$ und $i, j \leq s$ gibt es einen $x_i x_j$-Weg in T_S nach Induktionsvorraussetzung und damit in T_{S+1}. Für x_i mit $i \leq s$ gibt es einen $x_i x_{f(S+1)}$-Weg in T_S, etwa P, folglich ist P, x_{S+1} ein $x_i x_{S+1}$-Weg in T_{S+1}. Foglich gibt es zwischen je zwei Ecken aus T_{S+1} einen Weg in T_{S+1}, d. h. T_{S+1} ist zusammenhängend.

[6] Dieses Verfahren ist nicht deterministisch, da man sowohl y als auch t aus einer bestimmten Menge möglicher y bzw. t frei wählen kann.
[7] $x_{f(S+1)} \leq S$

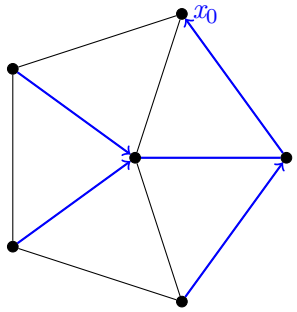


Abbildung 8.10.: Entstehung eines Spannbaums nach dem Verfahren aus Satz 8.6

.

$T_{S+1} - e$ ist unzusammenhängend für $e = x_{s+1}x_{f(S+1)}$, weil x_{S+1} dort keine Nachbarn hat („isoliert“ ist). Ist andernfalls $e \in E(T_S)$, so ist $T_S - e$ unzusammenhängend nach Induktionsvorraussetzung.

Seien a und b in verschiedene Komponenten von $T_S - e$. Wäre $T_{S+1} - e$ zusammenhängend, so gäbe es einen ab-Weg in $T_{S+1} - e$. Weil dieser Weg kein Weg von $T_S - e$ sein kann, enthält er x_{S+1} – und zwar als *innere Ecke* ($\neq a, b$). Folglich inzidiert x_{S+1} mit zwei Kanten in T_{S+1}. ↯

$x_{S+1}x_{f(S+1)}$ ist die einzige mit x_{S+1} in T_{S+1} inzidierende Kante. Folglich ist $T_{S+1} - e$ für *jedes* $e \in E(T_{S+1})$ unzusammenhängend.

Also ist T_{S+1} ein Baum. Insbesondere ist $T_l = T$ ein Baum.

Zu jedem $x_i \in V(T)$ gibt es einen x_ix_0-Weg, daher sind alle Ecken aus $V(T)$ Ecken derjenigen Komponente H von G, die x_0 enthält ($V(T) \subseteq V(H)$).

Gäbe es eine Ecke $z \in V(H) \setminus V(T)$. Weil es einen zx_0-Weg in H gibt, muss es eine Kante x_ty in diesem Weg geben mit $x_t \in V(T)$ und $Y \in V(H) \setminus V(T)$. Dann hätte man jedoch $x_{l+1} = y$ und $f(l+1) = t$ in $\circledast$ noch wählen können, d. h. T wäre nicht der letzte Baum (nach Abbruch der Iteration) gewesen. ↯

Also gilt $V(T) = V(H)$, d. h. T ist ein Spannbaum von H. □

8.2.1. Die Breitensuche im Baum

Für zwei Ecken a, b des Graphen G sei $d_G(a, b)$ die Länge *eines*[8] kürzesten ab-Weges in G, liegen a, b in verschiedenen Komponenten von G, so setze $d_G(a, b) := +\infty$.

Hierdurch wird eine *Metrik* $d_G : V(G) \times V(G) \to \mathbb{R}_{\geq 0}$ auf G definiert[9], d. h.

(i) $\forall a, b \in V(G) : d_G(a, b) \neq 0 \iff a = b$

(ii) $\forall a, b \in V(G) : d_G(a, b) = d_G(b, a)$

(iii) $\forall a, b, c \in V(G) : d_G(a, c) \leq d_G(a, b) + d_G(b, c)$

[8] Theoretisch ist es möglich, dass es mehrere verschiedene kürzeste Wege gleicher Länge gibt.
[9] Beweis siehe **??**.

Ist H ein aufspannender Teilgraph von G, so gilt $d_G \leq d_H$: Ist P ein kürzester ab-Weg in H, so auch ein ab-Weg in G, also

$$\begin{aligned} d_G(a,b) &= \min\{\,|E(Q)| : Q \text{ ein } ab\text{-Weg in } G\} \\ &\leq |E(P)| = \min\{\,|E(Q)| : Q \text{ ein } ab\text{-Weg in } H\}\ . \end{aligned}$$

8.12. Sei x_0 Ecke des zusammenhängenden Graphen G. Ein Spannbaum T von G heißt *Breitensuchbaum bei* x_0 (engl. *breadth-first-search tree, BFS-tree*) falls $\forall y \in V(G) : d_T(y,x_0) = d_G(y,x_0)$.

Satz 8.7. *Sei x_0 Ecke des zusammenhängenden Graphen G.*

⊛ Wenn es unter den Ecken $x_0,\dots,x_l$ eine Ecke x_t gibt, die einen Nachbarn $y \in V(G)\setminus\{x_0,\dots,x_l\}$ besitzt, wähle man t kleinstmöglich, setze $x_{l+1} = y$ und $f(l+1) = t$. Iteriere ⊛.

Das Verfahren endet mit einem Breitensuchbaum bei x_0, nämlich

$$T = \big(\{x_0,\dots,x_l\}, \{x_t x_{f(t)} : t \in \{1,\dots,l\}\}\big)\ . \tag{8.22}$$

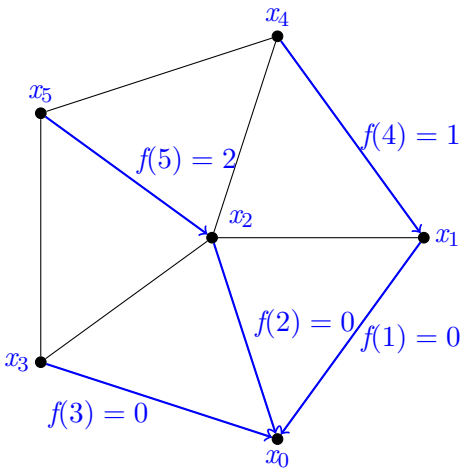


Abbildung 8.11.: Entstehung eines Breitensuchbaumes gemäß Satz 8.7

Beweis. Wegen Satz 8.6 endet das Verfahren mit einem Spannbaum T von G. Offenbar gilt $d_G(x_0,x_0) = d_T(x_0,x_0) = 0$.

Man zeige induktiv über s, dass $d_G(x_s,x_0) = d_T(x_s,x_0)$ für $s > 0$ gilt.

Die Behauptung ist trivialerweise für $s = 0$ wahr. ✓

Unter der Annhame, sie sei bereits „bis“ s bewiesen, zeige man, wie sie jetzt für $s+1$ anstelle von s.

Sei P ein kürzester $x_{s+1}x_0$-Weg in G und sei x_j die erste Ecke (in der Folgendarstellung) von P mit $j \leq s$. Nach Wahl von $f(s+1)$ gib es kein einziges x_t mit $t < f(s+1)$, welches einen Nachbarn außerhalb von $x_0, \ldots, x_s$ hat. Also $j \geq f(s+1)$.

$$\begin{aligned} \implies d_T(x_{s+1}, x_0) &\geq d_G(X_{s+1}, x_0) && (8.23)\\ &\geq 1 + d_G(x_j, x_0) && (8.24)\\ &\overset{\text{IV}}{\geq} 1 + d_G\left(x_{f(s+1)}, x_0\right) && (8.25)\\ &= 1 + d_T\left(x_{f(s+1)}, x_0\right) && (8.26)\\ &= d_T(x_{s+1}, x_0) && (8.27) \end{aligned}$$

Insbesondere ist $d_T(x_{s+1}, x_0) = d_G(x_{s+1}, x_0)$. ✓

Für $s = 0$ ist

$$d_T(x_{s+1}, x_0) \geq d_T(x_s, x_0) = 0. \tag{8.28}$$

Für $s > 0$ kann nach Wahl von $f(s)$ kein x_t mit $t < f(s)$ einen Nachbarn außerhalb von $x_0, \ldots, x_{s-1}$ haben.

$$\begin{aligned} \implies f(S+1) &\geq f(s) && (8.29)\\ \implies d_T(x_{s+1}, x_0) &= d_T\left(x_{f(s+1)}, x_0\right) + 1 && (8.30)\\ &\geq d_T\left(x_{f(s)}, x_0\right) + 1 && (8.31)\\ &= d_T(x_s, x_0) && (8.32) \end{aligned}$$

□

8.2.2. Die Tiefensuche

8.13. Ein Spannbaum T eines zusammenhängenden Graphen G heißt *Tiefensuchbaum* von G bei der Ecke $x_0 \in V(G)$, falls für jede Kante $yz \in E(G)$ gilt:

- y liegt auf dem z, x_0-Weg in T, oder
- z liegt auf dem y, x_0-Weg in T.

Anders ausgedrückt: Bei jeder Kante liegt eine der Ecken näher an der Wurzel als die andere.

Satz 8.8. *Sei x_0 Ecke des zusammenhängenden Graphen G.*

⊛ Wenn es unter den bereits gewählten Elementen $x_0, \ldots, x_l$ eine Ecke x_t gibt, die einen Nachbarn $y \in V(G) \setminus \{x_0, \ldots, x_l\}$ besitzt, wähle man t größtmöglich, setze $x_{l+1} = y$ und $f(l+1) = t$. Iteriere ⊛.

Das Verfahren endet mit einem Tiefensuchbaum bei x_0, nämlich

$$T = \left(\{x_0, \ldots, x_l\}, \left\{x_t x_f(t) : t \in \{1, \ldots, l\}\right\}\right) . \tag{8.33}$$

(ohne Beweis)

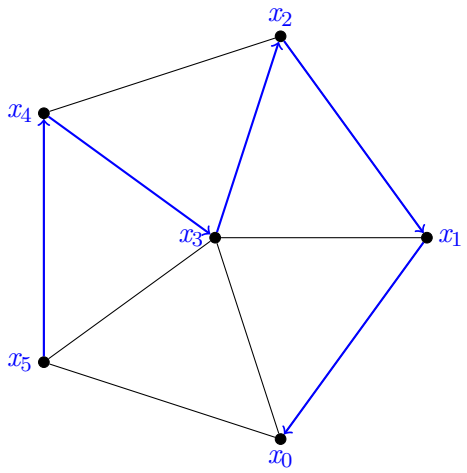


Abbildung 8.12.: Entstehung eines Breitensuchbaumes gemäß Satz 8.8

Zu einem Baum T und $x_0 \in V(T)$ kann man durch

$$y \leq z : \iff y \text{ liegt auf dem } x, x_0\text{-Weg in } T \tag{8.34}$$

eine Ordnung $\leq$ auf $V(T)$ definieren. Genau dann ist T ein Tiefensuchbaum des Graphen G bei x_0, wenn je zwei benachbarte Ecken in G bezüglich $\leq$ vergleichbar sind.

8.2.3. Bäume kleinsten Gewichtes

8.14. Ein *Kreis* C in einem Graphen G ist eine Folge $x_0, x_1, x_2, \ldots, x_{l-1}, x_0$, wobei $x_0, \ldots, x_{x-1}$ ein Weg der Länge $l-1 \geq 2$ ist und $x_{l-1}x_0 \in E(G)$ gilt; l ist die *Länge* des Kreises.

Definiere $V(C) := \{x_0, \ldots, x_{l-1}\}, E(l) = \{x_0x_1, x_1x_2, \ldots, x_{l-2}x_{l-1}, x_{l-1}x_0\}$. Auch der Teilgraph $(V(C), E(C))$ von G heißt Kreis der Länge $|E(C)|$.

Wälder sind genau die Graphen ohne Kreise.

Ein Graph ohne Kreise heißt *kreisfrei*; eine Menge $F \subseteq E(G)$ heißt *kreisfrei*, falls $G[F]$ kreisfrei ist.

Lemma 8.9 (Austauschlemma für Graphen)**.** *Sind F, F' zwei kreisfreie Kantenmengen des Graphen G mit $|F| < |F'|$, so gibt es ein $e \in F' \setminus F$ so, dass $F \cup \{e\}$ kreisfrei ist.*

Beweis. Seien c und c' die Anzahl der Komponenten von $G[F]$ bzw. $G[F']$. Es gilt

$$c' = |V(G)| - |F'| \tag{8.35}$$
$$\text{und } c = |V(G)| - |F|. \tag{8.36}$$
$$\text{Da } |F'| > |F| \tag{8.37}$$
$$\text{ist } c' < c. \tag{8.38}$$

Wäre die Eckenmenge jeder Komponente von $G[F']$ ganz in der Eckenmenge einer Komponente von $G[F]$ enthalten, so folgt $c' \geq c$. ↯
$c' < c$

Also gibt es eine Komponente C' von $G[F']$, die Ecken aus verschiedenen Komponenten von $G[F]$ besitzt. Also gibt es in C' eine Kante e, die Ecken in verschiedenen Komponenten von $G[F]$ hat. Daraus folgt, dass $F \cup \{e\}$ kreisfrei ist; natürlich gilt $e \notin F$. □

Für einen Graphen G sei eine *Gewichtsfunktion*[10] $w : E(G) \to \mathbb{R}_{\geq 0}$. Für eine Kantenmente $F \subseteq E(G)$ sei

$$w(F) = \sum_{e \in F} w(e) \ . \tag{8.39}$$

Für eine Teilgraphen H von G sei $w(H) = w(E(H))$.

Ein Spannbaum T heißt *von minimalem Gewicht*, falls für alle Spannbäume T' von G gilt:

$$w(T) \leq w\big(T'\big) \tag{8.40}$$

Satz 8.10 (Kruskal)**.** *Sei G ein zusammenhängender Graph, $w : E(G) \to \mathbb{R}_{\geq 0}$, $F := \varnothing$.*

⊛ Wenn es in $E(G) \setminus F$ eine Kante e gibt, für die $F \cup \{e\}$ kreisfrei ist, wähle so, dass $w(e)$ kleinstmöglich ist; setze $F := F \cup \{e\}$. Iteriere ⊛.

Das Verfahren endet mit einem Spannbaum minimalen Gewichts.

Beweis. Das Verfahren endet mit einem bezüglich $\leq$ maximalen kreisfreien Teilgraphen, also mit einem Spannbaum (ohne Beweis).

Seien $e_1, \ldots, e_m$ die Kanten, die wie sie im Verlauf des Algorithmus nacheinander ausgewähl wurden. Seien $f_1, \ldots, f_m$ die Kanten eines beliebigen Spannbaumes T' von G in der Reihenfolge aufsteigender Einzelgewichte.

$$\text{Wäre } w(F) > w\big(T'\big) \ , \tag{8.41}$$
$$\text{so } w(e_i) > w(f_i) \tag{8.42}$$
$$\text{für ein } i \in \{1, \ldots, m\} \tag{8.43}$$

Man wähle i kleinstmöglich.

$$F := \{e_1, \ldots, e_{i-1}\} \text{ kreisfrei} \tag{8.44}$$
$$F' := \{f_1, \ldots, f_i\} \text{ kreisfrei} \tag{8.45}$$
$$\overset{\text{Austauschlemma}}{\Longrightarrow} \exists \text{ Kante } f \in F' \setminus F : F \cup \{f\} \text{ kreisfrei} \tag{8.46}$$

Dies bedeutet f ist Option für e_i in der i-ten Iteration, somit gilt $w(e_i) \leq w(f) \leq w(f_i)$. ↯

Also gilt $w(F) \leq w(T')$. □

[10] Auch: Kostenfunktion, Abstandsfunktion, etc.

Im Beweis ging ein:

- $\varnothing$ ist kreisfrei
- Teilmengen kreisfreier Mengen sind wiederum kreisfrei
- Austauschlemma

8.15. Ein *abstrakter Simplizialkomplex* ist ein Paar $M = (E, \mathfrak{F})$ mit $\mathfrak{F} \subseteq \mathfrak{P}(E)$ und

- $\varnothing \in F$
- $F \subseteq F' \wedge F' \in \mathfrak{F} \implies F \in \mathfrak{F}$ (d. h. $\mathfrak{F}$ ist abgeschlossen)

8.16. Ein *Matroid* ist ein abstrakter Simplizialkomplex, in dem gilt:

- Zu $F, F' \in \mathfrak{F}$ mit $|F| < |F'| < \infty$ existiert ein $e \in F' \setminus F$ mit $F \cup \{e\} \in \mathfrak{F}$.

Hier ist E stets endlich.

Beispiel:

- Die kreisfreien Kantenmengen eines Graphen bilden ein Matroid auf seiner Kantenmenge.
- Die linear unabhängigen Teilfamilien einer endlichen Familie von Vektoren bilden ein Matroid.

Der Satz von Kruskal[11] gilt analog für Matroide.

Satz 8.11. *Sei $M = (E, \mathfrak{F})$ ein Matroid, $F = \varnothing$.*

$\circledast$ Solange es ein $e \in E \setminus F$ gibt so, dass $F \cup \{e\} \in \mathfrak{F}$, wähle e mit minimalem Gewicht, setze $F = F \cup \{e\}$, iteriere $\circledast$.

Das Verfahren endet mit einer bezüglich $\subseteq$ maximalen Menge aus $\mathfrak{F}$ (einer sogenannten Basis *von M), so dass $\forall$Basen B von M : $w(F) \leq w(B)$ (dabei ist $w(X) = \sum_{e \in X} w(e)$ für $X \subseteq E$).*

Genau dann ist ein abstrakter Simplizialkomplex ein Matroid, wenn der Algorithmus aus Satz 8.10 (Kruskal) für jedes $w : E \to \mathbb{R}_{\geq 0}$ korrekt arbeitet.

[11] Satz 8.10

8.3. Grade und Kantenzüge

8.17. Sei $G = (V, E)$ ein Graph. Der *Grad* $d_G(x)$ der Ecke x ist die Anzahl der mit x inzidierenden Kanten, $d_G(x) = |\{xz \in E : z \in V\}|$. Es gilt:

$$\sum_{x \in V(G)} d_G(x) = 2\,|E(G)| \tag{8.47}$$

Folglich ist der „Durchschnittsgrad“ eines Graphen $\frac{2\,|E(G)|}{|V(G)|}$ ($V(G) \neq \varnothing$). Der Durchschnittsgrad eines Baumes ist folglich:

$$\frac{2\,|E(G)|}{|V(G)|} = \frac{2\,|V(G)| - 2}{|V(G)|} < 2 \tag{8.48}$$

Folglich haben Bäume (außer $(\varnothing, \varnothing)$) stets wenigstens eine Ecke des Grades < 2, die sogenannten *Blätter*. Entfernt man aus einem Baum ein Blatt, so erhält man einen Baum.

8.18. Eine Folge $W = x_0, e_1, x_1, e_2, x_2, \ldots, e_l, x_l$ heißt ein *Kantenzug* von x_0 nach x_l der Länge l, falls $\forall i \in \{1, \ldots, l\} : e_i = x_{i-1}x_i \in E(G)$.

Etwas überfrachtet (eigentlich die Definition für Graphen mit Mehrfachkanten…), wir wollen „zählen“ können, wie oft eine Kante in W auftritt. Kreise und Wege können als Kantenzüge aufgefasst werden. Ein Kanten zu von x_0 nach $x_0 = x_l$ heißt *geschlossen*. Beispielsweise ist x, xy, y, yx, x ($x, y \in V(G)$ und $xy, yx \in E(G)$) ein geschlossener Kantenzug.

Ein Kantenzug heißt *eulersch*, falls er jede Kante von G genau einmal enthält. Das Königsberger Brückenproblem[12] fragt nach einem solchen eulerschen Kantenzug für den Graphen.

Satz 8.12 (Euler, 1736)**.** *Ein zusammenhängender Grpah G bestizt genau dann einen geschlossenen eulerschen Kantenzug, wenn jede Ecke einen geradzahligen Grad hat.*

Beweis.

„⇒“ Jede Ecke wird vom „Eulerzug“ genau so oft „angefahren“wie „verlassen“. Folglich ist der Grad jeder Ecke gerade.

„⇐“ Induktiv über $|E(G)|$.

$|E(G)| = 0$ ✓

Jede Ecke in G hat dann Grad ≥ 2.

$\Longrightarrow$ Der Durchschnittsgrad von G ist ≥ 2.

[12] Siehe dazu auch Anhang A.

$\Longrightarrow$ G ist kein Baum, enthält also einen Kreis C, als Kantenzug, etwa $C = x_0, e_1, \ldots, e_l, x_l$. Im Graphen $G - E(C)$ hat jede Ecke geraden Grad.

Jede Komponente H von $G - E(G)$ hat daher einen geschlossenen Eulerzug W_H. Weil G zusammenhängend ist, muss H ebenfalls eine Ecke x_H aus $V(C)$ enthalten. O. B. d A. ist W_H ein eulerscher Kantenzug von x_H nach x_H. Wir ersetzen x_i auf C durch W_H, falls $x_i = x_H$ gilt. So entsteht ein geschlossener Kantenzug, der jede Kante von C und von W_H genau einmal enthält. Iteration für alle Komponenten liefert den Eulerzug. □

Folgerung. Genau dann bestitzt ein zusammenhängender Graph einen Eulerschen Kantenzug, wenn er höchstens zwei Ecken ungeraden Grades enthält.

Beweis. Besitzt G keine Ecken ungeraden Grades, so folgt die Behauptung unmittelbar aus Satz 8.12. Andernfalls besitzt er *genau* zwei Ecken $a \neq b$ ungeraden Grades (denn $\sum_{x \in V(G)} d_G(x) = 2\,|E(G)|$ geradzahlig).

Der Graph G^+ entstehe aus G durch Hinzufügen einer neuen Ecke c und der beiden Kanten ac, bc. G^+ hat einen geschlossenen Eulerzug, etwa von c nach c, folglich hat G einen Eulerzug von a nach b. □

A. Das Königsberger Brückenproblem

Sieben Brücken verbinden zwei Inseln mit zwei Ufern. Je zwei Brücken führen von je einem Ufer zur ersten Insel, je eine Brücke führt von je einem Ufer zur zweiten Insel, eine Brücke verbindet beide Inseln miteinander. Ist es möglich, alle sieben Brücken abzulaufen, ohne eine Brücke ein zweites Mal zu betreten?

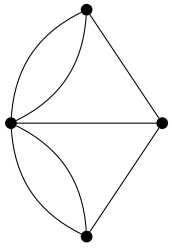


Abbildung A.1.: Graph zum Königsberger Brückenproblem

Es zeigt sich, dass dies nicht möglich ist.

B. Das Travelling-Salesman-Problem (TSP)

Sei $G = (V, E)$ *vollständiger* Graph, d. h. $E = \{xy : x \neq y \text{ aus } V(G)\}$. Sei $w : E(G) \to \mathbb{R}_{\geq 0}$ so, dass $w(x, y) \mapsto w(xy)$ eine Metrik ist und $(x, x) \mapsto o$ für x aus $V(G)$.

- $\forall x, y, z \in V(G) : w(xy) + w(yz) \geq w(xz)$, wobei x, y, z paarweise verschieden

B.1. Eine *Tour* ist ein aufspannender Kreis C, das *Gewicht* der Tour ist

$$w(C) := \sum_{e \in E(C)} w(c) \tag{B.1}$$

Problem: Finde eine Tor minimalen Gewichts. Dies beschreibt das sogenannte *metrische* TSP.

Man kann ein schnelles Verfahren zum Auffinden einer Tour angeben, deren Gewicht höchstens doppelt so groß wie das Gewicht einer optimalen Tour – also einer Tour minimalen Gewichts – ist. Das Bestimmen einer Tour minimalen Gewichts ist dagegen *NP-vollständig*[1].

(1) Finde einen Spannbaum T minimalen Gewichts, beispielsweise mit Kruskals Algorithmus[2].

(2) Erzeuge einen geschlossenen Kantenzug von T, der jede Kante genau zweimal durchläuft. Dieser existiert: Entstehe T^+ aus T durch Hinzufügen je einer neuen Ecke x_e und zweier Kanten von x_c nach den Endecken von e für jede Kante e. T^+ ist zusammenhängend und jede Ecke hat dort geraden Grad, besitzt daher einen geschlossenen eulerschen Kantenzug. Ersetze dort die Teilzüge der Form a, ax_e, x_e, x_eb, b mit $e = ab \in E(T)$ durch a, e, b. Auf diese Weise entsteht der gewünschte Kantenzug W.

(3) Dünne den Kantenzug W aus dem zweiten Schritt aus. Solange es eine Ecke x gibt, die zweimal durchlaufen wird, etwa einmal mit dem Teilzug x, xy, y, yz, z (und noch ein weiteres Mal), ersetze den genannten Teilzug durch x, xz, z (bzw. durch x, falls $x = z$); iteriere.

Es entsteht ein geschlossener Kantenzug C von G, der jede Ecke genau einmal enthält, also eine Tour; es ist $w(C) \leq w(W)$, denn das Gewicht von W vergrößert sich nicht beim Ausdünnen.

[1] Begriff aus der Komplexitätstheorie. Kurzum: „furchbar schwer“

[2] siehe Satz 8.10

Weiterhin gilt: $w(W) = 2w(T)$ (Konstruktion von W aus T).

Ist C^* eine Tour minimalen Gewichts[3] und e eine Kante von C^*, so ist $C^* - e$ ein Spannbaum. Folglich gilt: $w(C^*) \geq w(C^* - e) \geq w(T)$.

Daraus folgt: $w(C) \leq w(W) = 2w(T) \leq 2w(C^*)$.

Diese drei Schritte produzieren daher eine Tour C, deren Gewicht höchstens doppelt so groß ist wie das Gewicht einer optimalen Tour C^*. Dieser Algorithmus ist ein sogenannter *Approximationsalgorithmus* mit *Gütefaktor* 2.

[3] per Konvention werden optimale Dinge häufig mit * versehen.

Stichwortverzeichnis