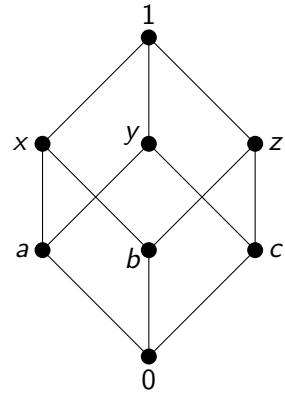
DHBW
Duale Hochschule
Baden-Württemberg
Mannheim



Modul: Mathematik 1

Lehreinheit: Logik und Algebra

Dozent: Dr. Wolfgang Weiss (w.square.dhbw@gmail.com)

Klausur: Vorbereitung mit Übungsaufgaben und Musterlösungen in Lerngruppen und in der Vorlesung
Erlaubte Hilfsmittel: Ein DIN-A4-Blatt mit eigenen Notizen, Taschenrechner

Vorwort

Bei der Vorbereitung und kontinuierlichen Verbesserung dieser Vorlesung habe ich außerordentlich hilfreiche Unterstützung erlebt. Ich bin sehr dankbar für den Rat und das Feedback von Studierenden, Professoren, Kolleginnen und Kollegen an der Dualen Hochschule Baden-Württemberg in Mannheim, insbesondere von Bernhard Drabant, Regina Griesinger, Matthias Heiler, Rainer Hoch und Robert Lang.
Ebenso dankbar bin ich für zahlreiche Anregungen zu Inhalt und Didaktik der mathematischen Grundlagen dieser Vorlesung, die ich von Kolleginnen und Kollegen bei der SAP SE und Studierenden und Professoren an anderen Hochschulen und Universitäten erhalten habe, u.a. von Andreas Deutesfeld, Marcel Erné, Robert Graeff, Joachim Hilgert, Karl-Hermann Neeb, Charlotte Reuschel und Johanna Reuschel.

Dossenheim, im September 2021 Wolfgang Weiss

Inhalt

Literatur (1/3)

- Aigner, Martin, und Behrends, Ehrhard (Hrsg.). Alles Mathematik. Von Pythagoras zum CD-Player. Vieweg–Teubner GWV Fachverlage, Wiesbaden, 2009, doi: https://doi.org/10.1007/978-3-658-09990-9
- Beutelspacher, Albrecht und Zschiegner, Marc-Alexander. Diskrete Mathematik für Einsteiger, Springer Spektrum, Wiesbaden, 4. Aufl. 2011, doi: https://doi-org.ezproxy-dhma-2.redi-bw.de/10.1007/978-3-8348-9941-5
- Haggarty, Rod. Diskrete Mathematik für Informatiker, Addison Wesley Pearson Education, München 2004
- Hilgert, Inge und Hilgert, Joachim. Mathematik - Ein Reiseführer, Springer, Berlin Heidelberg, 2012, doi: https://doi.org/10.1007/978-3-8274-2932-2
- Hilgert, Joachim, Hoffmann, Max, und Panse, Anja. Einführung in mathematisches Denken und Arbeiten, Springer, Berlin Heidelberg, 2015, doi: https://doi.org/10.1007/978-3-662-45512-8

Literatur (2/3)

- Hofstadter, Douglas R.. Gödel, Escher, Bach — ein Endloses Geflochtenes Band, Stuttgart, Klett Cotta, 16. Aufl. 2001
- Holey, Thomas und Wiedemann, Armin. Mathematik für Wirtschaftswissenschaftler, Springer Gabler, BA Kompakt, Berlin Heidelberg, 4. Aufl. 2016, doi: https://doi-org.ezproxy-dhma-2.redi-bw.de/10.1007/978-3-662-48143-1
- M. H. Ibrahim, R. Missaoui and J. Vaillancourt. 'Cross-Face Centrality: A New Measure for Identifying Key Nodes in Networks Based on Formal Concept Analysis', in IEEE Access, vol. 8, pp. 206901-206913, 2020, doi: 10.1109/ACCESS.2020.3038306.

Literatur (3/3)

- Knebl, Helmut. Algorithmen und Datenstrukturen, Springer Vieweg, Wiesbaden, 2. Aufl. 2021, doi: https://doi-org.ezproxy-dhma-1.redi-bw.de/10.1007/978-3-658-32714-9
- Lau, Dietlinde. Algebra und Diskrete Mathematik 1, Springer, Berlin Heidelberg, 3. Aufl., 2011, doi: https://doi-org.ezproxy-dhma-1.redi-bw.de/10.1007/978-3-642-19443-6
- Teschl, Gerald und Teschl, Susanne. Mathematik für Informatiker, Band 1: Diskrete Mathematik und Lineare Algebra, Springer, Berlin Heidelberg, 4. Aufl., 2013, doi: https://doi-org.ezproxy-dhma-1.redi-bw.de/10.1007/978-3-642-37972-7
- Teschl, Gerald, und Teschl, Susanne.: Mathematik für Informatiker, Band 2: Analysis und Statistik, Springer, Berlin Heidelberg, 3. Aufl., 2014, doi: https://doi-org.ezproxy-dhma-1.redi-bw.de/10.1007/978-3-642-54274-9

Mathematik-Videos und Online-Tools

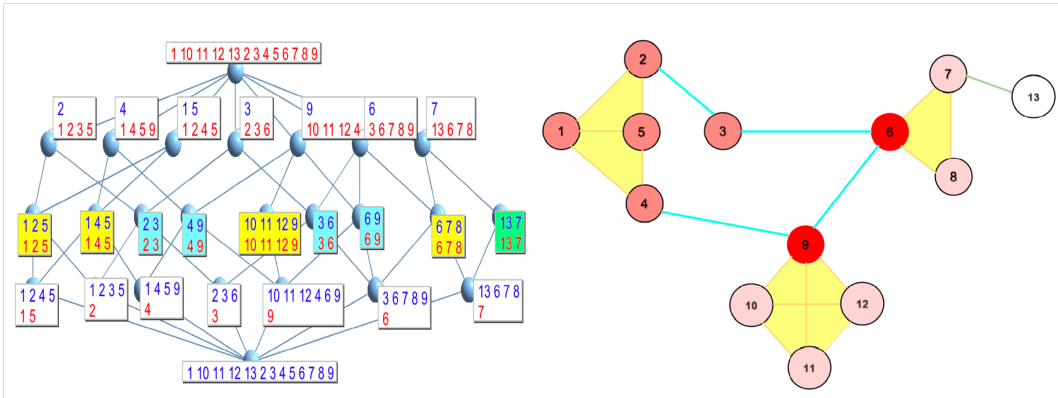
- Jung, Daniel. https://www.youtube.com/channel/UCPtUzxTfdaxAmr4ie9bXZVA
- Loviscach, Jörn. https://j3l7h.de/
- Numberphile – Haran, Brady.
  https://www.youtube.com/channel/UCoxcjq-8xIDTYp3uz647V5A
- Spannagel, Christian.
  https://www.ph-heidelberg.de/mathematik/personen/lehrende/spannagel.html
- Weitz, Edmund. http://weitz.de/haw-videos/
- WolframAlpha. http://www.wolframalpha.com/
- 3Blue1Brown – Sanderson, Grant.
  https://www.youtube.com/channel/UCYO_jab_esuFRV4b17AJtAw

Relevanz von Mathematik in IT, Wirtschaft, Naturwissenschaften etc.

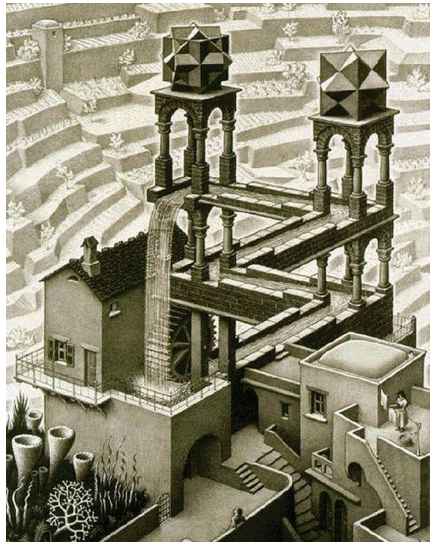
- **IT und Wirtschaft:** Datenmodellierung, Korrektheit und Effizienz von Algorithmen, Kryptographie, Artificial Intelligence, Software Engineering, Kostenrechnung, Enterprise Resource Planning (ERP), Statistik, Simulationen, Communities in Sozialen Medien
- **Naturwissenschaft und Technik:** 'Mathematik als Sprache', Modelle für Erklärung und Simulation von Naturphänomenen und technischen Prozessen (z.B. in den Biowissenschaften für die virale Verbreitung von COVID-19 oder das Data Mining zur Krebs-Früherkennung)
- **Politik und Gesellschaft:** Erfolgsfaktoren der Digitalisierung und ihrer gesellschaftlichen Akzeptanz, Bildung, Transparenz von wissenschaftlichen Studien
- **Grundlagen der Mathematik, Philosophie, Kunst und Musik:** Theoriebildung mit Axiomen und Beweisen, Strukturen in Kunst (Symmetrien etc.) und Musik (Harmonielehre), Erforschung der Grenzen menschlicher Erkenntnis gemeinsam mit Logik und Erkenntnistheorie

Beispiel: Analyse der Verbreitung von COVID-19

Quelle: Ibrahim, Missaoui and Vaillancourt, 2020



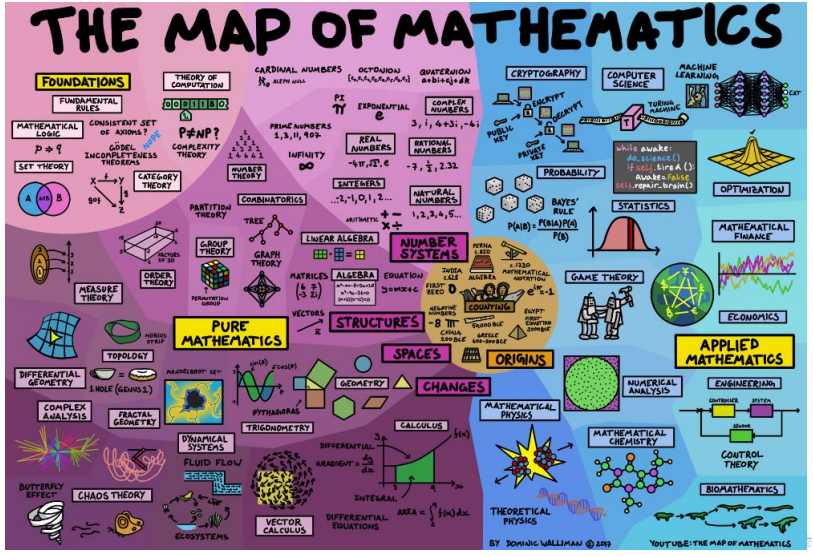
M. C. Escher



Copyright: M. C. Escher

Map of Mathematics (Domain of Science)

https://www.youtube.com/watch?v=OmJ-4B-mS-Y&feature=youtu.be



Einleitung: Methodik und Lernziele

Lernen mit digitalen Formaten und Fokus auf präzise Argumentation

- Englisch als Fachsprache für Recherchen und Anwendungen der Mathematik.
- Lernziel: Selbständige Recherche mit Google, Wikipedia, z.B.
  https://de.wikipedia.org/wiki/Hashfunktion, https://en.wikipedia.org/wiki/Hash_function
  https://en.wikipedia.org/wiki/Marginal_revenue
- Lernziel: Verwendung von Tools (WolframAlpha etc.) und Bewertung von Algorithmen (z.B. Korrektheit und Genauigkeit).
- Lernziel: Präzise Argumentation in Diskussionen und Beiträgen zu Projekten. In Übungen und Klausur Fokus nicht auf Auswendiglernen sondern auf exakte und nachvollziehbare Argumente bei Berechnungen und Beweisen.
- 'Comprehension is key': Verständnis der Vorlesung und Erfolg in der Klausur nur mit regelmäßiger Bearbeitung von Übungen in Lerngruppen möglich.
- Fokus auf Minimal Viable Scope (MVS), zusätzlich Ausblicke ($>$ MVS).

Schreibweisen für Zahlen und Mengen

1. $\mathbb{N} = \{1, 2, \ldots\}$ Menge der **natürlichen Zahlen** (engl. natural numbers)
2. $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ Menge der **ganzen Zahlen** (integers)
3. $\mathbb{Q} = \{q \mid q = \frac{n}{m}, n \in \mathbb{Z},\ m \in \mathbb{N}\}$ Menge der **rationalen Zahlen** (Brüche) (rational numbers, fractions)
4. $\mathbb{R}$ Menge der **reellen Zahlen** (real numbers), mit den Teilmengen
   - $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ der positiven reellen Zahlen,
   - $\mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ der nichtnegativen reellen Zahlen und
   - $\mathbb{N}_0 = \{n \in \mathbb{Z} \mid x \geq 0\}$ der nichtnegativen ganzen Zahlen.
5. Für $a, b \in \mathbb{R}$ mit $a < b$ ist $[a, b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}$ das **abgeschlossene** und $(a, b) := \{x \in \mathbb{R} \mid a < x < b\}$ das **offene Intervall** mit den Grenzen a und b. Analog dazu sind $[a, \infty) := \{x \in \mathbb{R} \mid a \leq x\}$ und $(a, \infty) := \{x \in \mathbb{R} \mid a < x\}$ sowie $(-\infty, b] := \{x \in \mathbb{R} \mid x \leq b\}$ und $(-\infty, b) := \{x \in \mathbb{R} \mid x < b\}$ definiert.
6. Für Relationen von Mengen A und B werden folgende Notationen verwendet:
   - $A \subseteq B$, **Teilmenge** (subset)
   - $A \cap B$, **Durchschnitt** (intersection), und $A \cup B$, **Vereinigung** (union)
   - $A \setminus B$, **Komplement** (complement)

Kapitel 1

Grundlagen der Mathematik — Logik und Mengenlehre

Abschnitt 1

Elementare Logik — 'Wahr oder nicht wahr - das ist hier die Frage'

Elementare Logik — 'Wahr oder nicht wahr - das ist hier die Frage'

Definition (1.1)

Eine **Aussage** (engl. proposition) *a* ist ein Satz (einer natürlichen oder künstlichen Sprache), von dem man eindeutig entscheiden kann, ob er wahr (true, Bezeichnung: 1) oder falsch (false, Bezeichnung: 0) ist.

Axiome für Aussagen

Für eine Aussage *a* setzt man voraus:

- *a* ist wahr oder falsch ("tertium non datur").
- *a* kann nicht gleichzeitig wahr und falsch sein.

Bitte beachten: "Tertium non datur" kennzeichnet die klassische zweiwertige Logik. In Mathematik, Philosophie und Informatik werden tlw. auch andere Modelle mit mehr als zwei Wahrheitswerten verwendet, z.B. ein dritter Wert für "unbekannt" oder unendlich viele Werte im Intervall $[0, 1]$ in der Fuzzy Logic.

Aussagen in Mathematik, Naturwissenschaften und Gesellschaft

Beispiele (1.2)

Welche der folgenden Sätze sind Aussagen? Und welche Aussagen sind wahr? Wie kann ggf. überprüft werden, ob sie wahr oder falsch sind?

- Oslo ist die Hauptstadt von Norwegen.
- Guten Abend!
- Heute ist Montag.
- Person A hat mehr als 100.000 Follower auf Instagram.
- Alle Studierenden der DHBW MA nutzen täglich WhatsApp.
- Luft-Temperatur an Wetterstation X im Odenwald, 28.01.2021, 7:00 Uhr CET: 2°C
- Die Zahl 3 ist der größte gemeinsame Teiler (ggT) von 15 und 30.
- Es gibt unendlich viele Primzahlen.
- Der Bubble Sort Algorithmus ist korrekt in der Sortierung einer Liste von Zahlen nach ihrer Größe.

Aussagen: Musterlösung für Teile von (1.2)

- Oslo ist die Hauptstadt von Norwegen.
  Aussage ist wahr, kann mit Atlas oder Wikipedia überprüft werden.
- Guten Abend!
  Keine Aussage, sondern ein Gruß.
- Heute ist Montag.
  Satz ist mit Kontext (Ort und Zeit) eine Aussage, andernfalls nicht.
- Alle Studierenden der DHBW MA nutzen täglich WhatsApp.
  Aussage, die z.B. durch ein einziges Gegenbeispiel einer Studierenden, die an einem Tag nicht WhatsApp verwendet, widerlegt (falsifiziert) werden kann.
- Die Zahl 3 ist der größte gemeinsame Teiler (ggT) von 15 und 30.
  Falsche Aussage, da 15 ein größerer gemeinsamer Teiler von 15 und 30 ist.
- Es gibt unendlich viele Primzahlen.
  Dieser Satz von Euklid wird im Rahmen dieser Vorlesung bewiesen, s. Satz (1.22).

Aussagen in Mathematik, Naturwissenschaften und Gesellschaft

Beispiele (1.3)

- Seit den 1970er Jahren findet ein globaler Klimawandel statt (z.B. im statistischen Mittel höhere Wintertemperaturen in Mitteleuropa).
- Die Teilnehmer bei den Kundgebungen von “Fridays for Future“ in Deutschland sind alle wahlberechtigt.
- Wachstum des Bruttoinlandsprodukts (BIP, engl. GDP) eines Landes ist gleichbedeutend mit einem höheren verfügbaren Einkommen für alle Bevölkerungsschichten (“trickle down effect“)
- Das BIP-Wachstum reflektiert weder das verfügbare Einkommen aller Bevölkerungsschichten noch die Nachhaltigkeit von Wirtschaft und Gesellschaft bei Umwelt, Klima, Gesundheit und sozialer Gerechtigkeit.

Beispiele (1.4)

- "Alle Kreter lügen", nach Epimenides von Knossos (ca. 600 v. Chr.)
- "Ich lüge gerade" (bzw. "Dieser Satz ist falsch"), Lügner (Pinocchio) Paradoxon

Negation

Definition (1.5)

Die **Negation** einer Aussage a ist genau dann wahr, wenn a falsch ist. Die Negation von a wird symbolisch mit $\neg a$ oder $\overline{a}$ bezeichnet (gelesen "nicht a" oder "non a").

Wahrheitswertetabelle (truth table)

a	$\neg a$
0	1
1	0

Beispiele (1.6)

- Zur Aussage "Person A hat mehr als 100.000 Follower auf Instagram" ist die Negation "Person A hat nicht mehr als 100.000 Follower auf Instagram".
- Für $x \in \mathbb{R}$ ist $\neg(x \leq 0)$ gleichbedeutend mit $x > 0$.
- Für $n, p \in \mathbb{N}$ gilt $\neg(n < p)$ genau dann, wenn $n \geq p$ erfüllt ist.

Negation

Beispiele (1.7)

- Zur Aussage “Alle Studierenden der DHBW MA nutzen täglich WhatsApp“ ist die Negation “Mindestens ein*e Studierende*r der DHBW MA nutzt nicht täglich WhatsApp“.
- “Die ganze Zahl n ist nicht durch 2 teilbar“ ist Negation von “Die ganze Zahl n ist durch 2 teilbar“.
- “Es gibt endlich viele Primzahlen“ ist Negation von “Es gibt unendlich viele Primzahlen“.

Konjunktion und Disjunktion

Definition (1.8)

Seien a und b Aussagen.

- $a \wedge b$ (**Konjunktion,** a **und** b, engl. and) ist genau dann wahr ist, wenn beide Aussagen wahr sind.
- $a \vee b$ (**Disjunktion,** a **oder** b, engl. or) ist genau dann wahr ist, wenn mindestens eine der beiden Aussagen wahr ist.
- $a \oplus b$ (**exklusives oder**, engl. exclusive or) ist genau dann wahr, wenn entweder a oder b (aber nicht beide gleichzeitig) wahr sind.

a	b	$a \wedge b$	$a \vee b$	$a \oplus b$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

Konjunktion und Disjunktion

Beispiele (1.9)

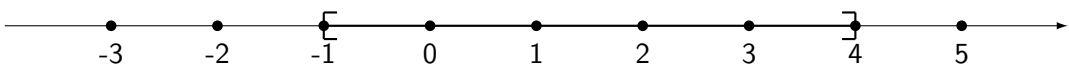
1. Für welche Zahlen $p \in \mathbb{N}$ ist die Konjunktion von (p ist eine Primzahl) und $(5 < p < 10)$ wahr?
2. Nennen Sie bitte zwei Beispiele von Zahlen $x \in \mathbb{R}$, für die die Konjunktion

$$(-1 \leq x) \wedge (x \leq 4)$$

   wahr ist. Beschreiben Sie die Menge aller reellen Zahlen, die diese Konjunktion erfüllen, und skizzieren Sie das Ergebnis auf der reellen Zahlenachse.
3. Für welche $x \in \mathbb{R}$ ist die Disjunktion $(x^2 \leq 4) \vee (-x > 2)$ gültig?
4. Geben Sie die natürlichen Zahlen $n \in \mathbb{N}$ an, für die gilt: $(n \leq 4) \oplus (n \geq 3)$

Musterlösung (1.9)

1. Für $p \in \mathbb{N}$ ist die Konjunktion (p prim) $\wedge$ ($5 < p < 10$) gleichbedeutend mit $p = 7$, da nur ungerade Zahlen als Primzahlen in Frage kommen, 9 durch 3 teilbar ist und deshalb 7 die einzige Primzahl im Intervall $(5, 10)$ ist.
2. $(-1 \leq x) \wedge (x \leq 4)$: Beispiele sind -1 und π, Ergebnismenge ist $[-1, 4]$.



3. Für $x \in \mathbb{R}$ ist die Disjunktion $(x^2 \leq 4) \vee (-x > 2)$ gültig, wenn mindestens eine der beiden Bedingungen erfüllt ist.
   - Die Bedingung $x^2 \leq 4$ beschreibt alle Zahlen im Intervall $[-2, 2]$.
   - Die Aussage $-x > 2$ trifft auf die Zahlen in $(-\infty, -2)$ zu.

   Die Disjunktion beschreibt also alle Zahlen $x \leq 2$, d.h. es ist das Intervall $(-\infty, 2]$.
4. $(n \leq 4) \oplus (n \geq 3)$ gilt für $1, 2$ und alle natürlichen Zahlen $n \geq 5$.

Äquivalenz

Definition (1.10)

Aussagen a und b werden als **gleich** oder **logisch äquivalent** bezeichnet, wenn sie für jede Kombination der Wahrheitswerte der Eingangsaussagen die gleichen Wahrheitswerte annehmen.

$$a \Leftrightarrow b$$

Man sagt: "a **genau dann, wenn** b" bzw. "a ist **notwendig und hinreichend** für b" ("if and only if" bzw. "necessary and sufficient")

a	b	$a \Leftrightarrow b$
0	0	1
0	1	0
1	0	0
1	1	1

Äquivalenz

Notation

Für Aussagen a und b werden folgende Schreibweisen (abhängig vom Kontext) synonym verwendet

- $a \Leftrightarrow b$
- $a \equiv b$
- $a = b$

Zu beachten: In der formalen Logik entsprechen diese Bezeichnungen verschiedenen Varianten von "Gleichheit".

Beispiele (1.11)

- "Heute ist Montag" $\Leftrightarrow$ "Morgen ist Dienstag"
- Für $p \in \mathbb{N}$ gilt: $((p \text{ prim}) \wedge (5 < p < 10)) \Leftrightarrow p = 7$

Logikgesetze

Satz (1.12)

Seien a, b und c Aussagen.

Kommutativgesetze $a \vee b \equiv b \vee a$ *und* $a \wedge b \equiv b \wedge a$

Assoziativgesetze $a \vee (b \vee c) \equiv (a \vee b) \vee c$ *und* $a \wedge (b \wedge c) \equiv (a \wedge b) \wedge c$

Distributivgesetze $a \vee (b \wedge c) \equiv (a \vee b) \wedge (a \vee c)$ *und* $a \wedge (b \vee c) \equiv (a \wedge b) \vee (a \wedge c)$

De Morgan'sche Regeln $\overline{a \wedge b} \equiv \overline{a} \vee \overline{b}$ *und* $\overline{a \vee b} \equiv \overline{a} \wedge \overline{b}$

Beweis.

Vergleich von Wahrheitswertetabellen, z.B. von $a \vee b$ und $b \vee a$, vgl. Beispiel (1.13). □

Hinweis:

Analoge Aussagen werden später im Zusammenhang mit Mengenoperationen (Vereinigung, Durchschnitt, Komplement) behandelt, vgl. Satz (1.39).

Logikgesetze: Beispiel eines Beweises

Beispiel (1.13)

Beweis des Kommutativgesetzes $a \vee b \equiv b \vee a$ mit Wahrheitswertetabellen:

a	b	$a \vee b$	$b \vee a$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	1

Die Wahrheitswerte der Spalten 3 und 4 stimmen überein, d.h. das Kommutativgesetz ist gültig. Das kann auch über folgende erweiterte Tabelle nachgewiesen werden, in der alle Werte der letzten Spalte gleich 1 sind.

a	b	$a \vee b$	$b \vee a$	$a \vee b \equiv b \vee a$
0	0	0	0	1
0	1	1	1	1
1	0	1	1	1
1	1	1	1	1

Implikation

Definition (1.14)

Seien a und b Aussagen. Die **Implikation** $a \Rightarrow b$ ist definiert durch:

a	b	$a \Rightarrow b$
0	0	1
0	1	1
1	0	0
1	1	1

Man sagt: "a **impliziert** b", "**aus** a **folgt** b", "a **ist hinreichend für** b", bzw. "b **ist notwendig für** a" ("a implies b", "a is sufficient for b" bzw. "b is necessary for a").

Beispiele (1.15)

- (Alle Studierenden der DHBW MA nutzen täglich WhatsApp) $\Rightarrow$ (Studierende A an der DHBW MA benutzt heute WhatsApp)
- (Es gibt unendlich viele Primzahlen) $\Rightarrow$ (Es existiert eine Primzahl $p > 100.000$)

Äquivalenz und Implikation

Satz (1.16)

1. *Die Äquivalenz von zwei Aussagen a und b kann in zwei Implikationen aufgeteilt werden, die beide gültig sein müssen:*

$$(a \Leftrightarrow b) \equiv ((a \Rightarrow b) \wedge (b \Rightarrow a))$$

2. *Die Implikation ist transitiv, d.h. für Aussagen a, b, c gilt:*

$$((a \Rightarrow b) \wedge (b \Rightarrow c)) \Rightarrow (a \Rightarrow c)$$

Die Ergebnisse dieses Satzes (die Zerlegung einer Äquivalenz in zwei Implikationen sowie die schrittweise Verkettung von Implikationen mit Hilfe der Transitivität) werden sehr oft in mathematischen Argumentationen genutzt, vgl. Beispiel (1.17).

Äquivalenz und Implikation

Beweis.

Teil 1: Zu zeigen: $(a \Leftrightarrow b) \equiv ((a \Rightarrow b) \wedge (b \Rightarrow a))$

a	b	$a \Leftrightarrow b$	$a \Rightarrow b$	$b \Rightarrow a$	$(a \Rightarrow b) \wedge (b \Rightarrow a)$
0	0	1	1	1	1
0	1	0	1	0	0
1	0	0	0	1	0
1	1	1	1	1	1

Vergleich der Spalten 3 und 6 liefert die Behauptung.

Teil 2: Übung

□

Äquivalenz und Implikation

Beispiel (1.17)

Für $p \in \mathbb{N}$ gilt:

$$((p \text{ prim}) \wedge (20 < p < 25)) \Leftrightarrow (p = 23)$$

Beweis durch Aufteilen der Äquivalenz in zwei Implikationen:

1. Die rechte Seite ist notwendig für die linke Seite (d.h., die Implikation von links nach rechts ist wahr), da $21 = 3 \cdot 7$ keine Primzahl ist und 23 somit die einzige Primzahl zwischen 20 und 25 ist.
2. Umgekehrt ist die rechte Seite hinreichend für die linke Seite (d.h., die Implikation von rechts nach links ist wahr), da für $p = 23$ auch die linke Aussage gilt.

Implikation und Negation

Satz (1.18)

Seien a, b Aussagen.

1. *Aus $a \Rightarrow b$ folgt im Allgemeinen nicht $b \Rightarrow a$*
2. $(a \Rightarrow b) \equiv (\neg b \Rightarrow \neg a)$

Beweis.

Für 2. vergleiche in der Wahrheitswertetabelle die Spalten 3 und 7:

a	b	$a \Rightarrow b$	$b \Rightarrow a$	$\neg b$	$\neg a$	$\neg b \Rightarrow \neg a$
0	0	1	1	1	1	1
0	1	1	0	0	1	1
1	0	0	1	1	0	0
1	1	1	1	0	0	1

Gegenbeispiel zu 1: (Alle Studierenden der DHBW MA nutzen täglich WhatsApp) $\Rightarrow$ (Studierende A an der DHBW MA benutzt heute WhatsApp). Die umgekehrte Richtung ist falsch, wenn eine einzige Studierende an einem Tag kein WhatsApp nutzt.

Beweisverfahren

Motivation für logisch-mathematische Beweise

- Herleitung von mathematischen Gesetzen aus Axiomen (z.B. für reelle Zahlen oder für euklidische bzw. nicht-euklidische Geometrien)
- Prüfung der Korrektheit von Algorithmen (z.B. für Sortierung)

Definition (1.19)

Sei $p \Rightarrow q$ eine Implikation (mit der **Prämisse** p und der **Konklusion** q).

- **Direkter Beweis** (modus ponens, direct proof): Aus der Annahme "p ist wahr" wird abgeleitet "q ist wahr". Damit ist ausgeschlossen, dass p wahr und q falsch ist (s. Wahrheitswertetabelle Zeile 3), d.h. $p \Rightarrow q$ ist wahr.
- **Indirekter Beweis** (Umkehrschluss, Kontraposition, modus tollens, proof of the contrapositive): Aus der Annahme "q ist falsch" wird abgeleitet "p ist falsch". Damit ist die Implikation $(\neg q \Rightarrow \neg p)$ mit direktem Beweis hergeleitet, d.h. $p \Rightarrow q$ ist wahr.

Lemma (1.20)

Seien $m, n \in \mathbb{Z}$.

1. *Wenn m und n ungerade sind, dann ist auch mn ungerade.*
2. *Wenn n^2 ungerade ist, dann ist n ungerade.*

Beweis.

1. m, n ungerade $\Rightarrow$ Es existieren $a, b \in \mathbb{Z}$ mit $m = 2a + 1$ und $n = 2b + 1$, also

$$mn = (2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2\underbrace{(2ab + a + b)}_{c} + 1.$$

   Folglich ist für $c := 2ab + a + b$ das Produkt $mn = 2c + 1$ ungerade.

2. Indirekter Beweis: Annahme, dass n gerade ist. Dann existiert $a \in \mathbb{Z}$ mit $n = 2a$ und $n^2 = 4a^2 = 2(2a^2)$, d.h. die Zahl n^2 ist gerade. Also ist die Implikation (n ist gerade $\Rightarrow$ n^2 gerade) wahr und damit im Umkehrschluss die Behauptung.

Definition (1.21)

Der **Widerspruchsbeweis** einer Aussage a (reductio ad absurdum, proof by contradiction) leitet aus der Annahme "a ist falsch" eine Aussage b ab, die im Widerspruch zu bekannten Tatsachen steht. Folglich ist b falsch. Da die Implikation $\neg a \Rightarrow b$ als wahr bewiesen wurde, muss $\neg a$ falsch sein, d.h., a ist wahr.

Satz (1.22, Euklid von Alexandria, ca. 325 — 270 v.Chr.)

Es gibt unendlich viele Primzahlen.

Widerspruchsbeweis

Beweis.

Annahme: Es gibt nur endlich viele Primzahlen $p_1 < \ldots < p_k$.
Setze $n := p_1 \cdots p_k + 1$. Offensichtlich gilt:
(*) Wenn n durch eine der Primzahlen $p_1, \ldots, p_k$ geteilt wird, bleibt 1 als Rest.
Aufgrund von (*) ist n nicht durch eine Primzahl teilbar. Dann muss entweder n eine Primzahl sein (im Widerspruch zu $n > p_k$) oder $n = m_1 m_2$ ist ein Produkt von natürlichen Zahlen $m_i, (i = 1, 2)$.
(**) Behauptung: Für jede natürliche Zahl $m > 1$ ist der kleinste Teiler $d > 1$ eine Primzahl.
Indirekter Beweis: Annahme d ist keine Primzahl. Dann gibt es natürliche Zahlen $1 < d_1 < d$, $1 < d_2 < d$ mit $d = d_1 d_2$. Folglich sind d_1 und d_2 Teiler von m, die kleiner als d sind im Widerspruch zur Minimum-Eigenschaft von m. QED (**)
Wegen (**) existieren Primteiler q_i von $m_i, (i = 1, 2)$. Bei Division von $n = m_1 m_2$ durch $q_i, (i = 1, 2)$ gibt es keinen Rest im Widerspruch zu (*).

Aussageformen

Definition (1.23)

Sei a eine Aussage.

- Wenn in a eine Konstante durch eine Variable x ersetzt wird, dann wird dadurch eine **Aussageform** $a(x)$ erzeugt.
- Eine Aussageform $a(x)$ wird zu einer Aussage, wenn für die Variable x eine Konstante eingesetzt wird (auch **Belegung der Variablen** genannt).
- Für Aussageformen können genau wie bei Aussagen Verknüpfungen (Negation, Konjunktion, Disjunktion, Äquivalenz etc.) gebildet werden, deren Wahrheitswerte bei Belegung der Variablen entsprechend der Verknüpfung ermittelt werden.

Aussageformen

Beispiele (1.24)

Seien $a_1(x) : x^2 = 4$ und $a_2(x) : x^2 < 4$ Aussageformen.

- Bestimme für $i = 1$ und $i = 2$ jeweils die Negation $\neg a_i$.
- Bestimme für die Variablenwerte $x = 1$ und $x = 2$ die Aussagen $a_i(1)$ und $a_i(2)$ $(i = 1, 2)$. Welche dieser Aussagen sind nicht wahr?
- Bestimme die Disjunktion $a_1 \vee a_2$.
- Für welche $x \in \mathbb{Z}$ ist $(a_1 \vee a_2)(x)$ wahr?

Aussageform: Musterlösung (1.24)

Gegeben die Aussageformen $a_1(x) : x^2 = 4$ und $a_2(x) : x^2 < 4$.

- Negationen: $\neg a_1 : x^2 \neq 4$ und $\neg a_2 : x^2 \geq 4$
- Aussagen mit Variablenwerten $x = 1$ und $x = 2$:
  $a_1(1) : 1^2 = 4$ (nicht wahr)
  $a_1(2) : 2^2 = 4$ (wahr)
  $a_2(1) : 1^2 < 4$ (wahr)
  $a_2(2) : 2^2 < 4$ (nicht wahr)
- Disjunktion $a_1 \vee a_2 : (x^2 = 4) \vee (x^2 < 4)$.
- $(a_1 \vee a_2)(x)$ ist wahr für $x \in \{2, 1, 0, -1, -2\}$.

Quantoren

Definition (1.25)

Sei $a(x)$ eine Aussageform.

- Die **All-Aussage** $\forall x : a(x)$ “Für alle x (aus einer bestimmten Menge) gilt $a(x)$“ ist wahr genau dann, wenn $a(x)$ für alle in Frage kommenden x wahr ist. (“for all x the proposition $a(x)$ is valid (or true)“)
- Die **Existenz-Aussage** $\exists x : a(x)$ “Es gibt ein x (aus einer bestimmten Menge), für das gilt $a(x)$“ ist wahr genau dann, wenn $a(x)$ für (mindestens) ein in Frage kommendes x wahr ist. (“there exists an x such that $a(x)$“)
- Die **Existenz und Eindeutigkeits-Aussage** $\exists! x : a(x)$ “Es gibt genau ein x, für das gilt $a(x)$“ ist wahr genau dann, wenn $a(x)$ für genau ein in Frage kommendes x wahr ist. (“there exists one and only one x such that $a(x)$“)

Quantoren und Negation

Beispiele (1.26)

Zu beachten: Bei mehreren Quantoren kommt es auf die Reihenfolge an.

1. $\forall n \in \mathbb{N}\, \exists p \in \mathbb{N} : n < p$ (Wahre Aussage, z.B. mit der Wahl von $p := n + 1$.)
2. $\exists p \in \mathbb{N}\, \forall n \in \mathbb{N} : n < p$ (Falsche Aussage: Es gibt keine größte natürliche Zahl.)

Satz (1.27)

Die Negation einer All-Aussage ist eine Existenz-Aussage und die Negation einer Existenz-Aussage ist eine All-Aussage.

- $\neg(\forall x : a(x)) \equiv \exists x : \neg a(x)$
- $\neg(\exists x : a(x)) \equiv \forall x : \neg a(x)$

Beispiel (1.28)

$\neg$(Alle Studierenden nutzen täglich WhatsApp) $\equiv$ (Es gibt eine*n Studierende*n, die/der an mindestens einem Tag kein WhatsApp benutzt)

Beispiel (1.29)

Negation von Aussagen der Prädikatenlogik (d.h. Aussageformen mit Quantoren), z.B. für die zweite Aussage aus Beispiel (1.26):

$$\neg(\exists p \in \mathbb{N}\, \forall n \in \mathbb{N} : n < p) \equiv \forall p \in \mathbb{N}\, \exists n \in \mathbb{N} : n \geq p$$

Schrittweise Umwandlung der Aussage durch "Negation in die Klammer ziehen":

1. Nach Satz (1.27) All-Aussagen in Existenz-Aussagen umwandeln und Existenz-Aussagen in All-Aussagen. Dabei bleiben die Eigenschaften der Variablen erhalten, z.B. wird $\exists p \in \mathbb{N}$ zu $\forall p \in \mathbb{N}$ und $\forall n \in \mathbb{N}$ zu $\exists n \in \mathbb{N}$.
2. Anschliessend Anwendung der Negation auf die Aussagen ohne Quantoren, z.B. wird $n < p$ umgewandelt in $n \geq p$.

Quantoren kommen in komplexen Aussagen vor, dabei ist der Geltungsbereich zu beachten (analog zu lokalen Variablen in Programmiersprachen).

Definition (1.30)

Seien $d, m, n \in \mathbb{N}$. Die Zahl d heißt **größter gemeinsamer Teiler** von m und n, Bezeichnung $ggT(m, n)$, (greatest common divisor, $gcd(m, n)$):
$((d \mid m) \wedge (d \mid n)) \wedge (\forall d' \in \mathbb{N} : (d' \mid m) \wedge (d' \mid n) \Rightarrow d' \leq d))$

Beispiele (1.31)

- Das **Lügner bzw. Pinocchio-Paradoxon** hat bereits Grenzen der Logik gezeigt. **Kurt Gödel** hat 1931 mit dem nach ihm benannten **Unvollständigkeitssatz** eine Verallgemeinerung davon hergeleitet, die die Existenz unendlich vieler wahrer Aussagen nachweist, die nicht innerhalb einer mathematisch-logischen Theorie beweisbar oder widerlegbar sind. Damit ist es unmöglich geworden, alle wahren Aussagen aus endlich vielen Axiomen herzuleiten. In der Logik sind daraufhin komplexe Theorien für die Erforschung beweisbarer Aussagen entwickelt worden.
- Der **Intuitionismus** verzichtet auf das Axiom “tertium non datur“ und lässt zu, dass eine Aussage weder wahr noch falsch, sondern “bisher nicht bewiesen oder widerlegt“ sein kann. Mit diesem Ansatz, der Widerspruchsbeweise ausschliesst, wurde eine Variante der Mathematik entwickelt, die nur konstruktive (algorithmische) Beweise verwendet, aber keine reinen Existenzbeweise.

Abschnitt 2

Mengenlehre — Objekte und Mengen

Mengenlehre — Objekte und Mengen

Definition (1.32)

Eine **Menge** (set) ist jede Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens — welche die **Elemente** dieser Menge genannt werden — zu einem Ganzen. (Georg Cantor, 1845 – 1918)

Bemerkungen

Die Definition von Cantor wird in der "Naiven Mengenlehre" verwendet und ist ausreichend für große Bereiche der Mathematik und für diesen Kurs. Beachte aber das **Russell'sches Paradoxon:** "Ein Barbier rasiert alle Männer eines Dorfes, die sich nicht selbst rasieren. Rasiert dieser Barbier sich selbst?"
Es gibt dabei auch eine Analogie zum Lügner- bzw. Pinocchio-Paradoxon, da eine Selbstreferenzierung vorliegt. In der axiomatischen Mengenlehre sind weitergehende Theorien entwickelt worden, die diese Paradoxien vermeiden.

Beschreibung von Mengen

Mengen können auf zwei Arten beschrieben werden:

- Aufzählung der Elemente der Menge (list of elements)
- Angabe der Eigenschaft (property), die die Elemente der Menge erfüllen sollen.

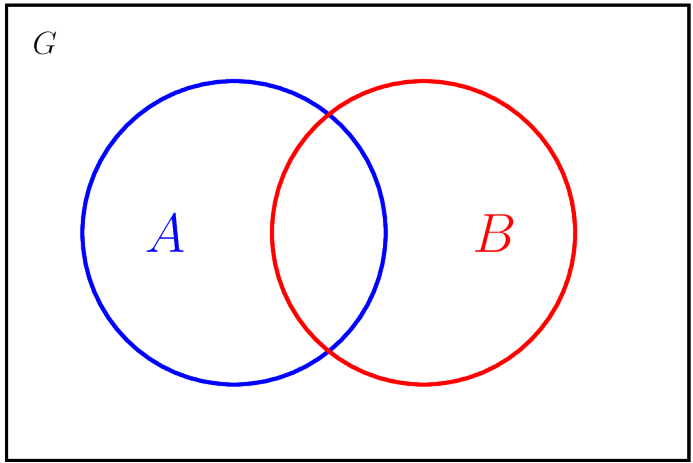
Bezeichnungen:

- Grossbuchstaben $A, B, \ldots$ für Mengen, Kleinbuchstaben $a, b, \ldots$ für Elemente
- x ist (nicht) Element von A: $x \in A$, $(x \notin A)$
- Für die Eigenschaft E, die die Elemente der Menge M erfüllen, gilt $M = \{x \mid E\}$.

Beispiele (1.33)

- $A = \{1, 2, 5\}$
- $B = \{n \in \mathbb{N} \mid n < 4\}$
- $C = \{x \in \mathbb{Z} \mid x^2 = 4\}$
- $D = \{2, -2\}$

Venn-Diagramme



Teilmengen, leere Menge und Potenzmenge

Definition (1.34)

Seien A, B und X Mengen.

- $A \subseteq B$ (A ist **Teilmenge** (subset) von B) $:\Leftrightarrow \forall x \in A : x \in B$
  In Worten: Jedes Element von A ist Element von B. In diesem Fall heißt B auch **Obermenge** (superset) von A.
- $A = B$ (A und B sind **gleich** (equal)) $:\Leftrightarrow A \subseteq B \wedge B \subseteq A$
- $A \neq B$ (A und B sind **ungleich** (not equal)) $:\Leftrightarrow \neg(A = B)$
- $A \subset B$ (A ist **echte Teilmenge** (proper subset) von B) $:\Leftrightarrow A \subseteq B \wedge A \neq B$
- Notation: $A \not\subseteq B :\Leftrightarrow \neg(A \subseteq B)$
- $\emptyset = \{x \in \mathbb{N} \mid x \neq x\}$ ist die **leere Menge** (empty set), die aus keinem Element besteht,
- $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ ist die **Potenzmenge** (power set) von X.

Teilmengen, leere Menge und Potenzmenge

Beispiele (1.35)

Beweisen Sie diese Aussagen, indem Sie für jedes (bzw. ein) Element der Teilmengen nachweisen, dass es (nicht) in der größeren Menge enthalten ist. Bei echten Teilmengen nennen Sie ein Element der Obermenge, das nicht in der Teilmenge enthalten ist.

1. $\{1, 2, 5\} \subseteq \{1, 2, 5, 6\}$
2. $\{1, 6\} \not\subseteq \{1, 2, 5\}$
3. $\{1, 2, 5\} \subseteq \{1, 2, 5\}$
4. $\{1, 2, 5\} \subseteq \{5, 2, 1\}$, d.h. auf die Reihenfolge der Aufzählung kommt es nicht an.
5. $\{2, 5\} \subset \{1, 2, 5\}$
6. Was ist $\mathcal{P}(\{0\})$?

Teilmengen, leere Menge und Potenzmenge: Musterlösung (1.35)

1. $\{1,2,5\} \subseteq \{1,2,5,6\}$:
   Sei $x \in \{1,2,5\}$. Dann gilt auch $x \in \{1,2,5,6\}$, damit ist die Teilmengenrelation bewiesen. ✓
2. $\{1,6\} \not\subseteq \{1,2,5\}$:
   $6 \in \{1,6\}$ aber $6 \notin \{1,2,5\}$. ✓
3. $\{1,2,5\} \subseteq \{1,2,5\}$:
   Die Mengen sind gleich, also ist die linke Seite Teilmenge der rechten Seite. ✓
4. $\{1,2,5\} \subseteq \{5,2,1\}$:
   Sei $x \in \{1,2,5\}$ Dann gilt auch $x \in \{5,2,1\}$. ✓
5. $\{2,5\} \subset \{1,2,5\}$:
   Sei $x \in \{2,5\}$. Dann gilt auch $x \in \{1,2,5\}$, d.h. die linke Seite ist Teilmenge der rechten. Da 1 in der rechten aber nicht in der linken Seite enthalten ist, liegt eine echte Teilmenge vor. ✓
6. $\mathcal{P}(\{0\}) = \{\emptyset, \{0\}\}$. Zu beachten: $\mathcal{P}(\{0\})$ besteht aus zwei Elementen.

Transitivität vonTeilmengen und die leere Menge als Teilmenge

Satz (1.36)

1. *Die Teilmengenrelation $\subseteq$ ist transitiv, d.h. für beliebige Mengen A, B, C gilt:*

$$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$$

2. *$\emptyset$ ist Teilmenge jeder Menge*

Beweis.

1. Sei $x \in A$. Wegen $A \subseteq B$ gilt damit $x \in B$. Wegen $B \subseteq C$ gilt dann $x \in C$. Aus der Transitivität der Implikation (vgl. Satz (1.16)) folgt $(x \in A \Rightarrow x \in C)$ und damit $A \subseteq C$.
2. Sei X eine Menge. Dann gilt $(x \in \emptyset \Longrightarrow x \in X)$, da die Prämisse stets falsch ist und damit die Implikation wahr ist.

Binäre Mengenoperationen

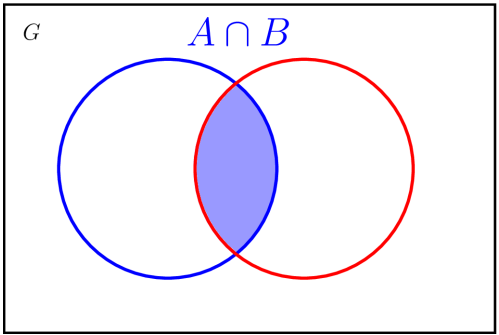
Definition (1.37)

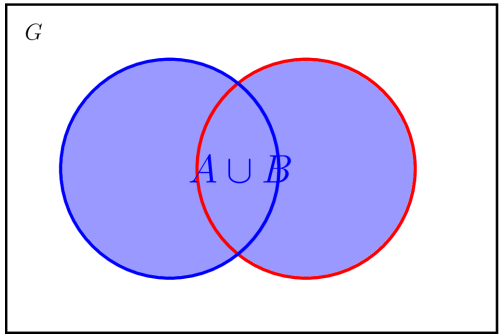
Seien A, B und G Mengen mit $A \subseteq G$ und $B \subseteq G$

- $A \cap B := \{x | (x \in A) \wedge (x \in B)\}$ **Durchschnitt** (intersection)
- $A \cup B := \{x | (x \in A) \vee (x \in B)\}$ **Vereinigung** (union)
- $A \backslash B := \{x | (x \in A) \wedge (x \notin B)\}$ **Komplement** (complement)
- $\overline{A} := G \backslash A$
- $A \Delta B := A \oplus B := (A \backslash B) \cup (B \backslash A)$ **symmetrische Differenz** (symmetric difference)

Binäre Mengenoperationen

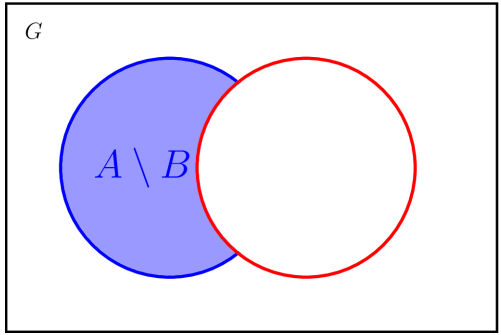
Durchschnitt und Vereinigung



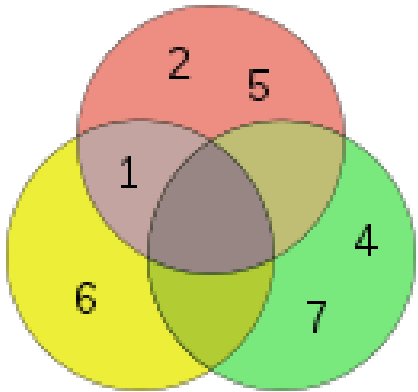


Binäre Mengenoperationen

Komplement



Binäre Mengenoperationen



Binäre Mengenoperationen

Beispiele (1.38)

Beweisen Sie folgende Aussagen über die Gleichheit von Mengen, indem Sie jeweils nachweisen, dass die Menge auf der linken Seite der Gleichung eine Teilmenge der Menge auf der rechten Seite ist und umgekehrt.

- $\{1,2,5\} \cap \{1,6\} = \{1\}$
- $\{1,2,5\} \cap \{4,7\} = \emptyset$
- $\{1,2,5\} \cup \{4,7\} = \{1,2,4,5,7\}$
- $\{1,2,5\} \backslash \{1,6\} = \{2,5\}$
- $\{1,2,5\} \Delta \{1,6\} = \{2,5,6\}$

Musterlösung (1.38)

- $\{1,2,5\} \cap \{1,6\} = \{1\}$:
  Zu zeigen: $\{1,2,5\} \cap \{1,6\} \subseteq \{1\}$
  Sei $x \in \{1,2,5\} \cap \{1,6\} \subseteq \{1\}$. Dann muss $x = 1$ gelten, da $2, 5$ und 6 jeweils nur in einer der beiden Mengen vorkommen. Folglich ist $x \in \{1\}$.
  Zu zeigen: $\{1,2,5\} \cap \{1,6\} \supseteq \{1\}$
  Sei $y \in \{1\}$. Dann ist $y = 1 \in \{1,2,5\}$ und $y = 1 \in \{1,6\}$, damit auch im Durchschnitt $\{1,2,5\} \cap \{1,6\}$.
- $\{1,2,5\} \cap \{4,7\} = \emptyset$:
  Keines der Elemente von $\{1,2,5\}$ kommt in $\{4,7\}$ vor und außerdem kommt keines der Elemente von $\{4,7\}$ in $\{1,2,5\}$ vor. Deshalb ist der Durchschnitt die leere Menge.

Musterlösung (1.38)

- $\{1,2,5\} \cup \{4,7\} = \{1,2,4,5,7\}$
  Zu zeigen: $\{1,2,5\} \cup \{4,7\} \subseteq \{1,2,4,5,7\}$
  Sei $x \in \{1,2,5\} \cup \{4,7\}$. Dann ist $x \in \{1,2,5\}$ oder $x \in \{4,7\}$. In beiden Fällen ist $x \in \{1,2,4,5,7\}$.
  Zu zeigen: $\{1,2,5\} \cup \{4,7\} \supseteq \{1,2,4,5,7\}$
  Sei $y \in \{1,2,4,5,7\}$. Falls $y = 4$ oder $y = 7$ gilt, ist $y \in \{4,7\}$. In den anderen Fällen ist $y \in \{1,2,5\}$.
- $\{1,2,5\} \setminus \{1,6\} = \{2,5\}$
  Zu zeigen: $\{1,2,5\} \setminus \{1,6\} \subseteq \{2,5\}$
  Sei $x \in \{1,2,5\} \setminus \{1,6\}$. Dann ist $x \neq 1$ und es bleiben nur die Möglichkeiten $x = 2$ oder $x = 5$ übrig. Folglich ist $x \in \{2,5\}$.
  Zu zeigen: $\{1,2,5\} \setminus \{1,6\} \supseteq \{2,5\}$
  Sei $y \in \{2,5\}$. Dann ist $y \neq 1$ und deshalb $y \in \{1,2,5\} \setminus \{1,6\}$.

Musterlösung (1.38)

- $\{1,2,5\}\Delta\{1,6\} = \{2,5,6\}$
  Da für den Durchschnitt gilt $\{1,2,5\} \cap \{1,6\} = \{1\}$, besteht die symmetrische Differenz aus allen Elementen $x \in \{1,2,5\} \cup \{1,6\}$ mit $x \neq 1$, das ist gerade die Menge $\{2,5,6\}$

Gesetze für Mengenoperationen

Satz (1.39)

Seien A, B und C Mengen.

Idempotenzgesetze $A \cap A = A = A \cup A$

Kommutativgesetze $A \cup B = B \cup A$ *und* $A \cap B = B \cap A$

Assoziativgesetze $A \cup (B \cup C) = (A \cup B) \cup C$ *und* $A \cap (B \cap C) = (A \cap B) \cap C$

Distributivgesetze $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan'sche Regeln $\overline{A \cap B} = \overline{A} \cup \overline{B}$ *und* $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Beweis.

Diese Gesetze beruhen auf den entsprechenden Logikgesetzen aus Satz (1.12). Das Kommutativgesetz für OR-Aussagen angewendet auf $(x \in A) \vee (x \in B)$ liefert:
$(x \in A \cup B) \Leftrightarrow (x \in A \vee x \in B) \Leftrightarrow (x \in B \vee x \in A) \Leftrightarrow (x \in B \cup A)$ □

Cartesisches Produkt

Definition (1.40)

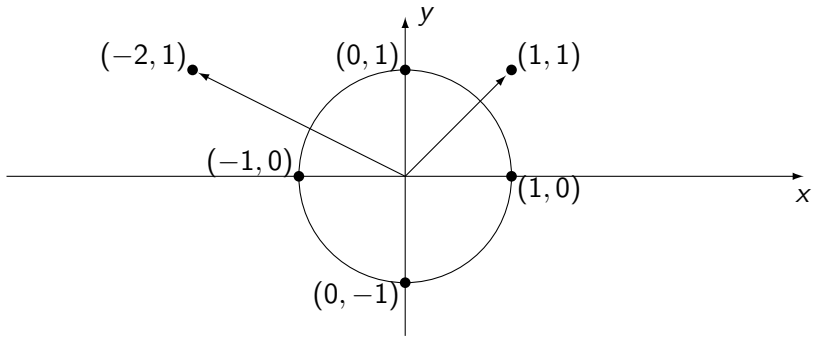
Seien X und Y nichtleere Mengen.

- Ein Paar (x, y) mit $x \in X$ und $y \in Y$ und festgelegter Reihenfolge der beiden Elemente heißt **geordnetes Paar** oder **Tupel** (ordered pair, ordered set, tuple)
- $X \times Y := \{(x, y) \mid x \in X, y \in Y\}$ **cartesisches Produkt** (cartesian product) von X und Y.

Beispiele (1.41)

- $(1, 2) \neq (2, 1)$, d.h. bei Tupeln kommt es auf die Reihenfolge der Aufzählung an (im Unterschied zu Mengen, z.B. bei der Menge $\{1, 2\}$).
- $\{1, 2\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
- $\{1\} \times \{3, 4\} = \{(1, 3), (1, 4)\} \neq \{(3, 1), (4, 1)\} = \{3, 4\} \times \{1\}$
- $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ (reelle Zahlenebene)

Reelle Zahlenebene $\mathbb{R}^2$



Addition von Vektoren (Zahlenpaaren): $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
Skalarmultiplikation (Streckung) eines Vektors mit einer Zahl $a \in \mathbb{R}$: $a(x, y) = (ax, ay)$
Betrag (Länge) eines Vektors: $|(x, y)| = \sqrt{x^2 + y^2}$,
Einheitskreis $U = \{(x, y) \in \mathbb{R}^2 : |(x, y)| = 1\}$
Vergleichbarkeit von Vektoren: $(x_1, y_1) \leq (x_2, y_2) :\Longleftrightarrow x_1 \leq x_2 \wedge y_1 \leq y_2$

Reelle Zahlenebene $\mathbb{R}^2$

Beispiele (1.42)

Bitte berechnen Sie die folgenden Operationen und Aussagen für Vektoren in $\mathbb{R}^2$.
Hinweis: Der Betrag von $(x, y) \in \mathbb{R}^2$ ist definiert durch $|(x, y)| := \sqrt{x^2 + y^2}$.

1. Addition von Vektoren: $(-1, 3) + (2, 0) \neq (1, 2)$
2. Skalarmultiplikation eines Vektors mit einer Zahl: $2(-2, 1) = (-4, 2)$
3. Betrag (Länge) eines Vektors: $|(-1, 3)| = \sqrt{10}$
4. Einheitskreis:

$$\left(\frac{-\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right) \in U = \{(x, y) \in \mathbb{R}^2 : |(x, y)| = 1\}$$

5. Vergleich von Vektoren:
   - $(-3, -3) \leq (2, 0)$
   - $(1, 3) \not\leq (2, 0)$, d.h. $(1, 3)$ und $(2, 0)$ sind unvergleichbar.

Abbildungen und Funktionen

Definition (1.43)

- Eine **Abbildung** oder **Funktion** f (mapping, map, function) bildet jedes Element x einer **Definitionsmenge** X (domain) auf ein Element $y = f(x)$ in einer **Wertemenge** Y (co-domain, value set) ab.
- Notation: $f : X \to Y$, $x \mapsto f(x)$
- Das Element $f(x) \in Y$ heißt **Bildpunkt** (image, value, output) von $x \in X$ und x heißt **Urbildpunkt** oder **Argument** (pre-image, input, argument) von $f(x)$. Der **Graph** von f ist $\text{graph}(f) := \{(x, y) \in X \times Y \mid y = f(x)\}$.
- Funktionen $f : X \to Y$ und $g : X \to Y$ sind **gleich** ($f = g$), wenn $f(x) = g(x)$ für alle $x \in X$. Funktionen mit verschiedenen Definitions- oder Wertebereichen sind stets ungleich.

Beispiele (1.44)

Die Funktionen $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$, und $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, sind ungleich: $f \neq g$.

Abbildungen und Funktionen: Bild- und Urbildpunkte

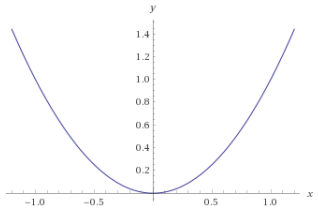
Hinweis: Für eine Abbildung $f : X \to Y$ ist zu beachten:

1. Für jedes $x \in X$ gibt es nur einen Bildpunkt $f(x)$.
2. Für $f(x) \in Y$ kann es mehrere Urbildpunkte geben.
3. Für $y \in Y$ muss es keinen Urbildpunkt geben.

Beispiel (1.45)

Normalparabel 2. Ordnung $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$

1. Für $x_1 = 1$ gibt es nur ein Bildpunkt: $g(1) = 1$.
2. Für $g(1) = 1$ gibt es mehrere Urbildpunkte: $x_1 = 1$ und $x_2 = -1$.
3. Für $y_0 = -0,1$ gibt es keinen Urbildpunkt $x \in \mathbb{R}$ mit $g(x) = -0,1$.



Betrag, Floor, Ceil & Truncation

Definition (1.46)

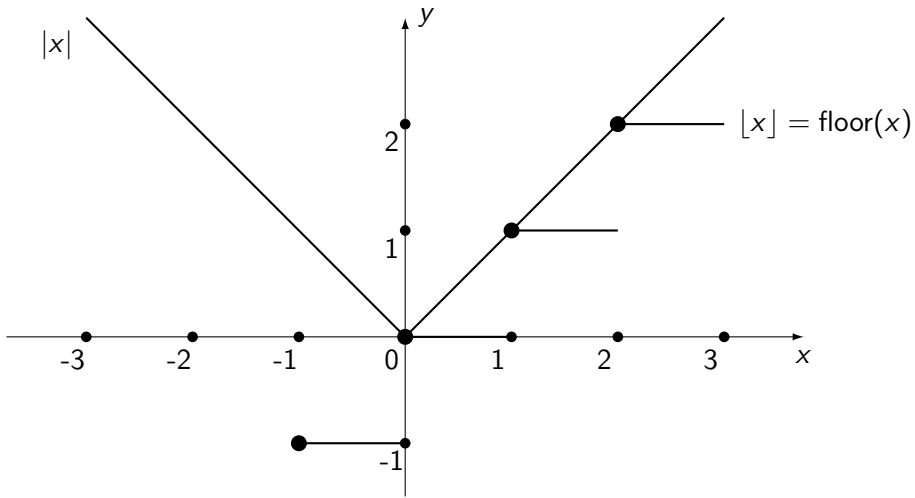
- **Betragsfunktion** (absolute value) $|.| : \mathbb{R} \to \mathbb{R}, x \mapsto |x|$
- Sei $x \in \mathbb{R}$.
  - $\lfloor x \rfloor := \text{floor}(x) := \max\{m \in \mathbb{Z} \mid m \leq x\}$
  - $\lceil x \rceil := \text{ceil}(x) := \min\{n \in \mathbb{Z} \mid n \geq x\}$
  - Für $n \in \mathbb{N}$ ist die **bis zur n−ten Dezimalstelle gerundete Zahl** (truncation)

$$\text{trunc}(x, n) := \begin{cases} \lfloor 10^n x \rfloor \cdot 10^{-n} & \text{falls } x \geq 0, \\ \lceil 10^n x \rceil \cdot 10^{-n} & \text{sonst.} \end{cases}$$

  - Für $n = 0$ ist $\text{trunc}(x) := \text{trunc}(x, 0)$ der **ganzzahlige Anteil von** x.

Zu beachten: $\text{trunc}(x)$ rundet für positive und negative Zahlen zur 0, während $\lfloor x \rfloor$ bzw. $\lceil x \rceil$ jeweils stets nach unten bzw. oben runden.

Betrag, Floor, Ceil & Truncation



Kardinalität endlicher Mengen

Definition (1.47)

Wenn A eine endliche Menge ist mit n verschiedenen Elementen $a_1, \ldots, a_n$ für ein $n \in \mathbb{N}$, dann wird die Anzahl der Elemente bzw. die **Kardinalität von** A mit $|A| = n$ bezeichnet.

Im weiteren Verlauf dieser Vorlesung werden auch Kardinalitäten unendlicher Mengen untersucht, s. (1.107).

Verallgemeinerungen der Mengenoperationen für mehr als zwei Mengen:

Definition (1.48)

Seien $A_1, \ldots, A_n$, B_n $(n \in \mathbb{N})$ und C_i $(i \in I)$ Mengen, I eine Indexmenge

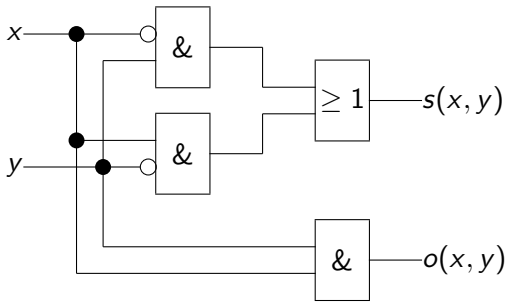
- $\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$
- $\bigcap_{i=1}^{\infty} B_i = B_1 \cap B_2 \cap \ldots$
- $\bigcap_{i \in I} C_i = \{x \mid \forall j \in I, x \in C_j\}$
- $\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$
- $\bigcup_{i=1}^{\infty} B_i = B_1 \cup B_2 \cup \ldots$
- $\bigcup_{i \in I} C_i = \{x \mid \exists j \in I, x \in C_j\}$

Abschnitt 3

Boolesche Algebren — Modellierung logischer Schaltungen

Boolesche Algebren — Modellierung logischer Schaltungen

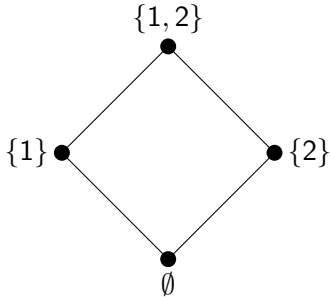
Beim Entwurf von logischen Schaltungen und digitalen Schaltkreisen (z.B. für Rechenoperationen von Computern oder für komplexe Strom-Netzwerke) werden mathematische Modelle mit binären Variablen eingesetzt, die nur die Werte 0 und 1 annehmen und auf die elementare Operationen (“und“, “oder“, “nicht“) angewendet werden können. Dafür ist das Konzept einer **Booleschen Algebra** sehr passend mit Hilfe von Ausdrücken und Formeln, die analog zu logischen Ausdrücken und zu Mengenoperationen gebildet sind und für die entsprechende Gesetze gelten.



Hasse-Diagramme von $\mathcal{P}(\{1,2\})$ und der.Booleschen Algebra B_4

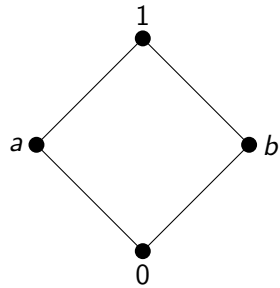
Beispiele (1.49)

$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$



$\emptyset \subset \{1\}, \emptyset \subset \{2\}, \{1\} \subset \{1,2\}, \{2\} \subset \{1,2\}$

$B_4 = \{0, 1, a, b\}$



$0 < a, 0 < b, a < 1, b < 1$

- Kombination von Relationen, z.B. $0 < a \wedge a < 1 \Rightarrow 0 < 1$.
- Operationen $\cup$ und $\cap$ für $\vee$ (Addition, Supremum, OR) und $\wedge$ (Multiplikation, Infimum, AND), z.B. $\{1\} \cup \{2\} = \{1,2\}, \{1\} \cap \{2\} = \emptyset, a \vee b = 1, a \wedge b = 0$.

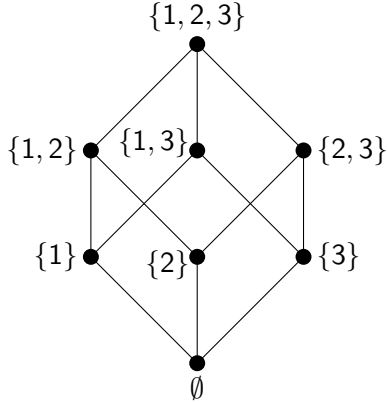
Boolesche Algebren

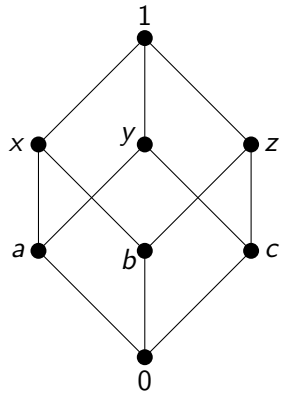
Definition (1.50)

Eine **Boolesche Algebra** (boolean algebra) $(B, \vee, \wedge, \neg, 0, 1)$ ist eine algebraische Struktur über einer Menge B mit folgenden Operationen
$\vee : B^2 \to B, (a, b) \mapsto a \vee b$ (Addition, Supremum),
$\wedge : B^2 \to B, (a, b) \mapsto a \wedge b$ (Multiplikation, Infimum),
$\neg : B \to B, a \mapsto \neg a$ (Komplement)
und neutralen Elementen $0, 1 \in B$, so dass für alle $a, b, c \in B$ gilt:

1. Kommutativität: $a \vee b = b \vee a$ und $a \wedge b = b \wedge a$
2. Assoziativität: $a \vee (b \vee c) = (a \vee b) \vee c$ und $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
3. Distributivität: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ und $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
4. Idempotenz $a \vee a = a$ und $a \wedge a = a$
5. Neutrale Elemente: $a \vee 0 = a$ und $a \wedge 1 = a$
6. Komplement: $a \vee (\neg a) = 1$ und $a \wedge (\neg a) = 0$

Boolesche Algebren und Mengenlehre: $\mathcal{P}(\{1,2,3\}) =: B_8$





- Kombination von Relationen, z.B. $0 < a \wedge a < y \Rightarrow 0 < y$.
- 0 ist das kleinste Element von B_8 und 1 das größte.
- Operationen $\cup$ und $\cap$ für $\vee$ (Addition, Supremum, OR) und $\wedge$ (Multiplikation, Infimum, AND), $\{1\} \cup \{3\} = \{1,3\}, \{1,3\} \cap \{2,3\} = \{3\}, a \vee c = y, y \wedge z = c$.

Boolesche Algebren: Alternative Schreibweisen

Notation

Sei B eine Boolesche Algebra und $a, b \in B$.

- $a \wedge b = a \cdot b = ab = a \otimes b$
- $a \vee b = a + b = a \oplus b$
- $\neg a = \overline{a}$

Hinweis

Die alternativen Schreibweisen sind durch Anwendungen von Booleschen Algebren in anderen mathematischen Gebieten (Mengenlehre, Zahlentheorie etc.) motiviert, von denen einige im Verlauf des Kurses behandelt werden.

Boolesche Algebren und Aussagenlogik

Beispiele (1.51)

Für $B_2 = \{0, 1\}$ seien a, b Variablen mit Werten in B_2. Mit den üblichen Regeln für Supremum und Infimum bzw. für die Negation kann die Struktur einer Booleschen Algebra auf B_2 definiert werden:

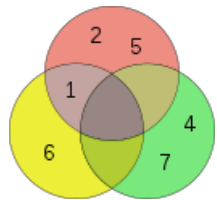
a	b	$a \wedge b$	$a \vee b$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

a	$\neg a$
0	1
1	0

Wenn a und b als logische Aussagen und ihre Werte als Wahrheitswerte 0 oder 1 interpretiert werden, dann entspricht das genau den Wahrheitswertetabellen der Aussagenlogik. Die Logikgesetze (z.B. Kommutativgesetze) entsprechen den definierenden Eigenschaften einer Booleschen Algebra.

Beispiele (1.52)

Für eine Menge X ist die Potenzmenge $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ mit den Operationen Vereinigung, Durchschnitt und Komplement sowie den neutralen Elementen $\emptyset$ und X eine Boolesche Algebra. Die Gesetze für Mengenoperationen (z.B. Kommutativgesetze) entsprechen den definierenden Eigenschaften einer Booleschen Algebra.



Hinweis (>MVS): Jenseits dieses Kurses kann gezeigt werden, dass jede endliche Boolesche Algebra die Struktur einer Potenzmenge hat. Darüberhinaus gilt für unendliche Boolesche Algebren, dass sie dieselbe Struktur haben wie eine Teilmenge einer Potenzmenge ("Darstellungssatz von Stones").

Satz (1.53)

Für eine Boolesche Algebra B ist das Komplement jedes Elements $a \in B$ eindeutig bestimmt und es gilt $\overline{\overline{a}} = a$.

Beweis.

Seien $a, b \in B$ und b ein Komplement von a.

1. Zu zeigen: $b = \overline{a}$.
   $b = b1 = b(a \vee \overline{a}) = ba \vee b\overline{a} = ab \vee \overline{a}b = 0 \vee \overline{a}b$
   Da auch $\overline{a}$ ein Komplement von a ist, gilt weiter:
   $0 \vee \overline{a}b = a\overline{a} \vee \overline{a}b = \overline{a}a \vee \overline{a}b = \overline{a}(a \vee b) = \overline{a}1 = \overline{a}$
2. Zu zeigen: $\overline{\overline{a}} = a$.
   Es gilt $\overline{a} \vee a = 1$ und $\overline{a} \cdot a = 0$ (wegen Kommutativität), folglich ist a ein Komplement von $\overline{a}$.
   Außerdem ist $\overline{a} \vee \overline{\overline{a}} = 1$ und $\overline{a} \cdot \overline{\overline{a}} = 0$, d.h. $\overline{\overline{a}}$ ist ein Komplement von $\overline{a}$.
   Mit Teil 1 folgt die Behauptung.

Satz (1.54)

Jede gültige Formel für Boolesche Algebren geht in eine andere gültige Formel über, wenn man überall die Symbole $\vee$ *und* $\wedge$ *sowie* 0 *und* 1 *gleichzeitig vertauscht.*

Beispiele (1.55)

- Für neutrale Elemente wird aus Formel $a \vee 0 = a$ durch Vertauschung $a \wedge 1 = a$.
- *De Morgan'sche Regeln:* $\overline{a \wedge b} = \overline{a} \vee \overline{b}$ und $\overline{a \vee b} = \overline{a} \wedge \overline{b}$
- Involution: $\overline{0} = 1$ und $\overline{1} = 0$

Beweis der Involution $\overline{0} = 1$

Wegen der Komplementeigenschaft von $\overline{0}$ gelten $0 \vee \overline{0} = 1$ und $0 \wedge \overline{0} = 0$.
Gleichzeitig gelten für die neutralen Elemente $0 \vee 1 = 1$ und $0 \wedge 1 = 0$.
Aufgrund der Eindeutigkeit des Komplements folgt $\overline{0} = 1$.

Boolesche Funktionen: Modellierung von Schaltungen

Definition (1.56)

Sei $B_2 = \{0, 1\}$ und $n \in \mathbb{N}$. Eine ***n*-stellige Boolesche Funktion** (boolean function), ist eine Abbildung

$$f : (B_2)^n \to B_2, (x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n) \in B_2$$

Hinweis

Eine Boolesche Funktion bildet jeweils n Bits auf ein einziges Bit ab, d.h., sie ist ein Modell für eine Schaltung, die aus mehreren Eingabebits ein einziges Ausgabebit berechnet (z.B.die Quersumme der Eingabebits modulo 2).

2-stellige Boolesche Funktionen

Beispiele (1.57)

Tabelle aller 2-stelligen Boolesche Funktionen

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Einige 2-stellige Boolesche Funktionen entsprechen bekannten logischen Ausdrücken:

- $f_8(x, y) = x \wedge y$
- $f_{14}(x, y) = x \vee y$
- $f_{11}(x, y) = x \Rightarrow y$

Boolesche Funktionen und Boolesche Terme (Formeln, Ausdrücke)

Definition (1.58)

(Boolesche) Terme bzw. **Formeln** oder **Ausdrücke** (boolean expressions) sind rekursiv definiert:

1. (Basis clause) Die Konstanten $0, 1$ sowie die Variablen $x_1, \ldots, x_n$ sind Boolesche Terme
2. (Recursion clause) Wenn a und b Boolesche Terme sind, so auch $(a), \neg a, a \wedge b, a \vee b, a \Rightarrow b, a \Leftrightarrow b, a \oplus b$

Jeder Boolesche Term entsteht, indem die Regel (2) endlich oft angewendet wird, wobei die Booleschen Terme aus (1) als Ausgangspunkt dienen.

Hinweis

Terme entsprechen den logischen Ausdrücken der Aussagenlogik. Wenn ein Term a Variablen $x_1, \ldots, x_n$ enthält, können Wahrheitswerte für a entsprechend der Belegung der Variablen $x_1, \ldots, x_n$ berechnet werden.

Boolesche Funktionen und Terme: Überblick

Boolesche Funktionen und Terme sind "zwei Seiten einer Medaille":

- Aus einem Term a mit Variablen $x_1, \ldots, x_n$ kann eine zugehörige Boolesche Funktionen f_a konstruiert werden, deren Funktionswerte mit den Wahrheitswerten von a übereinstimmt: Bei konkreter Belegung der Variablen $x_1, \ldots, x_n$ mit 0 oder 1 errechnet sich der Funktionswert $f_a(x_1, \ldots, x_n)$ aus der Formel bzw. dem Term a.
- Aus einer Booleschen Funktion f lassen sich zugehörige Terme konstruieren, deren Wahrheitswerte mit den Funktionswerten von f übereinstimmen. Dabei ist diese Zuordnung nicht eindeutig, d.h., verschiedene Terme können dieselbe Funktion beschreiben.

Das Zusammenspiel von Booleschen Funktionen und Termen wird in der Informatik dafür genutzt, mit Hilfe von **Normalformen** (z.B. Disjunktive Normalform, s.u.) und **Vereinfachungen von Termen** (z.B. Quine-McCluskey Verfahren, s.u.) die **technische Implementierung** der zugehörigen Booleschen Funktionen zu **optimieren**. Damit können z.B. Schaltungen mit möglichst wenigen standardisierten Bauelementen entworfen werden.

Normalformen

Standardisierte Terme für Boolesche Funktionen

Beispiele (1.59)

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Konstruiere eine zugehörigen Term a mit Hilfe der Zeilen mit Funktionswert 1:

$$f_a(x,y,z) = (\overline{x} \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge y \wedge z) \vee (x \wedge y \wedge z)$$

Normalformen

Im Allgemeinen bestehen Terme aus (eventuell negierten) Variablen, die durch Operatoren wie z.B. $\wedge$, $\vee$, oder $\Rightarrow$ verknüpft sind. Der Zweck der Normalformen liegt darin, als Operatoren nur $\wedge$ oder $\vee$ zu verwenden und die Konjunktionen und Disjunktionen "voneinander zu trennen". Zunächst ein paar hilfreiche Begriffe für die atomaren und zusammengesetzten Bausteine der Terme:

Definition (1.60)

- Ein **Literal** ist eine Boolesche Variable x oder deren Komplement $\overline{x}$. Notation:

$$x^{\alpha} = \begin{cases} \overline{x} & \text{für } \alpha = 0 \\ x & \text{für } \alpha = 1 \end{cases} \quad (\alpha \in \{0,1\})$$

- Ein **Minterm** oder **Vollkonjunktion** ist ein Term aus Literalen, die durch $\wedge$ verknüpft sind, wobei alle Variablen genau einmal vorkommen (ggf. als Negation).

Disjunktive und Konjunktive Normalformen

Beispiele (1.61)

1. $(\overline{x} \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge y \wedge z) \vee (x \wedge y \wedge z) = (x^0 y^1 z^0) \vee (x^0 y^1 z^1) \vee (x^1 y^1 z^1)$
2. $f_{11}(x, y) = (x \Rightarrow y) = (\overline{x} \wedge \overline{y}) \vee (\overline{x} \wedge y) \vee (x \wedge y) = (x^0 y^0) \vee (x^0 y^1) \vee (x^1 y^1)$
3. $f_7(x, y) = \overline{(x \wedge y)} = (x^0 y^0) \vee (x^0 y^1) \vee (x^1 y^0)$ "*NAND*"
4. $f_1(x, y) = \overline{(x \vee y)} = (x^0 y^0)$ "*NOR*"

Satz (1.62)

Für jede n-stellige Boolesche Funktion existiert eine **Disjunktive Normalform (DNF)***:*

$$f(x_1, \ldots, x_n) = \bigvee_{(a_1, \ldots, a_n) \in {B_2}^n} f(a_1, \ldots, a_n) \cdot {x_1}^{\alpha_1} \cdots {x_n}^{\alpha_n}$$

Die dazu duale **Konjunktive Normalform (KNF)** *ist*

$$f(x_1, \ldots, x_n) = \bigwedge_{(a_1, \ldots, a_n) \in {B_2}^n} f(a_1, \ldots, a_n) \vee {x_1}^{\alpha_1} \vee \cdots \vee {x_n}^{\alpha_n}$$

Konstruktion von Disjunktiven Normalformen

Algorithmus

Gegeben eine Boolesche Funktion $f : (B_2)^n \to B_2, (x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n) \in B_2$.

1. *Suche Zeilen mit Funktionswert* 1.
   Beispiel 1: Zeilen 3, 4 und 8.
2. *Bestimme für jede dieser Zeilen einen Minterm, der den Wert* 1 *liefert.*
   Beispiel 1, Zeile 3: $x^0 y^1 z^0$
3. *Die Minterme werden durch* $\vee$ *verknüpft.*
   Beispiel 1: $(x^0 y^1 z^0) \vee (x^0 y^1 z^1) \vee (x^1 y^1 z^1)$

Hinweise

- Mit entsprechenden dualen Methoden werden Konjunktive Normalformen gebildet.
- Die Normalformen haben den Vorteil der einheitlichen Struktur, können aber relativ viele Minterme enthalten, die jeweils Schaltelementen entsprechen. Die Zahl und Komplexität der verwendeten Terme (Schaltelemente) kann mit dem Quine-McCluskey-Verfahren (s.u.) reduziert werden.

Quine-McCluskey-Verfahren

Vereinfachung von DNF's

Beispiele (1.63)

x	y	z	$g(x,y,z)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

$$\begin{aligned} \text{DNF: } g(x,y,z) &= (\overline{x}\overline{y}\overline{z}) \vee (\overline{x}\overline{y}z) \vee (\overline{x}y\overline{z}) \vee (xy\overline{z}) \vee (xyz) \\ &= x^0y^0z^0 \vee x^0y^0z^1 \vee x^0y^1z^0 \vee x^1y^1z^0 \vee x^1y^1z^1 \end{aligned}$$

Quine-McCluskey-Verfahren

Vereinfachung von DNF's

Schritt 1:

Zusammenfassen von Konjunktionen mit Hilfe der Regeln für Boolesche Algebren:

- $x^1 y^0 \vee x^1 y^1 = x^1 (y^0 \vee y^1) = x^1 \wedge 1 = x^1$ (Ausklammern mit Distributivität)
- $x^1 y^1 = y^1 x^1$ (Kommutativität)
- $x^1 \vee x^1 = x^1$ (Idempotenz)

Schritt 2:

Elimination von Konjunktionen, die für keine Kombination von Variablenwerten einen zusätzlichen Wert 1 erzeugen

Quine-McCluskey-Verfahren

Beispiel für Schritt 1

$$g(x,y,z) = \underbrace{(x^0y^0z^0)}_{1.} \vee \underbrace{(x^0y^0z^1)}_{2.} \vee \underbrace{(x^0y^1z^0)}_{3.} \vee \underbrace{(x^1y^1z^0)}_{4.} \vee \underbrace{(x^1y^1z^1)}_{5.}$$

Nr. der zusammgefassten Konjunktionen	Konjunktion
1., 2.	x^0y^0
1., 3.	x^0z^0
3., 4.	y^1z^0
4., 5.	x^1y^1

Zwischenergebnis: $g(x,y,z) = x^0y^0 \vee x^0z^0 \vee y^1z^0 \vee x^1y^1$

Quine-McCluskey-Verfahren

Beispiel für Schritt 2

Elimination von Konjunktionen, die keinen zusätzlichen Wert 1 erzeugen

x	y	z	$g(x,y,z)$	x^0y^0	x^0z^0	y^1z^0	x^1y^1
0	0	0	1	1	1	0	0
0	0	1	1	1	0	0	0
0	1	0	1	0	1	1	0
0	1	1	0	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	0	1	0	0	1	1
1	1	1	1	0	0	0	1

Elimination von Spalte y^1z^0 ergibt: $g(x,y,z) = x^0y^0 \vee x^0z^0 \vee x^1y^1$
Alternative Lösung mit Elimination von Spalte x^0z^0: $g(x,y,z) = x^0y^0 \vee y^1z^0 \vee x^1y^1$

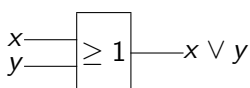
Bemerkungen

- Wegen der Kommutativität der Disjunktion ist die Reihenfolge der Minterme ohne Bedeutung und kann nach praktischen Gesichtspunkten gewählt werden.
- Eine interessante geometrische Interpretation des Verfahrens mit Hilfe der Eckpunkte, Seitenkanten und Seitenflächen eines Würfels wird in (Lau, 2011, S.43) vorgestellt.
- Der Algorithmus des Verfahrens erlaubt effiziente Implementierungen.

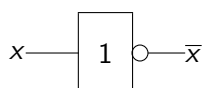
Definition (1.64)

- **Logische Schaltungen** (combinatorial circuits) sind technische Realisierungen von Booleschen Funktionen und werden für das Design von Halbleitern verwendet. Die Zustände 0 und 1 in der Booleschen Algebra B_2 entsprechen bei Computern Spannungs-Zuständen $0 = U_{min}$ und $1 = U_{max}$ (unter Berücksichtigung von Toleranzbereichen um diese Spannungen).
- Die Booleschen Funktionen Konjunktion, Disjunktion und Negation werden durch **Gatter** bzw. **gates** realisiert:

AND gate



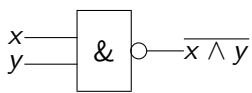
OR gate



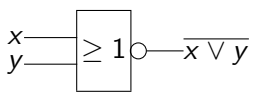
NOT gate

Beispiele (1.65)

- Gates können hintereinander geschaltet werden. Zur Vereinfachung werden vor- oder nachgeschaltete *NOT* gates am Eingang bzw. am Ausgang als Kreis dargestellt.
- *NAND*-Funktion $\overline{(x \wedge y)}$ und *NOR*-Funktion $\overline{(x \vee y)}$:



NAND gate



NOR gate

Funktionale Vollständigkeit: Reduktion auf wenige Operationen

> MVS

Für die industrielle Fertigung von Halbleitern ist es aus wirtschaftlichen Gründen wichtig, mit wenig verschiedenen Gates auszukommen. Mit Hilfe der DNF können alle Booleschen Funktionen auf $\wedge, \vee$ und $\neg$ zurückgeführt werden. Darüberhinaus lassen sie sich sogar als Hintereinanderausführung von ausschließlich *NAND*-Funktionen bzw. ausschließlich *NOR*-Funktionen konstruieren (s.u.)., d.h. mit einem einzigen Typ von Gates können alle logischen Schaltungen gebaut werden.

Definition (1.66)

Eine Menge von Booleschen Operationen heißt **funktional vollständig** (functionally complete), wenn sich alle Booleschen Funktionen mit Verknüpfungen aus dieser Menge darstellen lassen.

Satz (1.67)

- *Die Menge* $\{\wedge, \vee, \neg\}$ *ist funktional vollständig.*
- *Sowohl* $\{NAND\}$ *als auch* $\{NOR\}$ *sind funktional vollständig.*

Beweis.

Der erste Teil folgt aus dem Satz über die Disjunktive Normalform. Für den Beweis der funktionalen Vollständigkeit von $\{NAND\}$ wird folgende Notation verwendet:

$$NAND(x, y) := \overline{x \wedge y}$$

Zu zeigen: Die Konjunktion läßt sich mit $NAND$ beschreiben. Für diesen Nachweis ist die De Morgan'sche Regel $\overline{a \wedge b} = \overline{a} \vee \overline{b}$ hilfreich:

$$x \wedge y = (x \wedge y) \vee 0 = \overline{\overline{(x \wedge y)} \wedge \overline{0}} = \overline{\overline{(x \wedge y)} \wedge 1} = NAND(NAND(x, y), 1)$$

Analog zeigt man, dass Disjunktion und Negation allein mit $NAND$ dargestellt werden können (Übung), □

Anwendung: Halb-Addierer (1/2)

Definition (1.68)

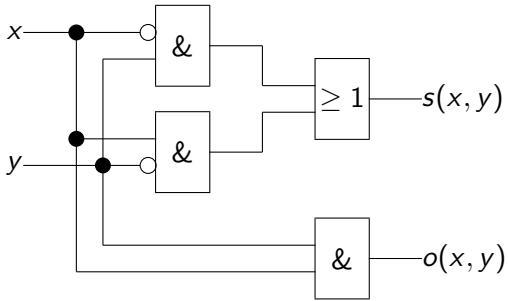
Ein **Halb-Addierer** (half adder) implementiert die Addition von zwei einstelligen Binärzahlen mit Übertrag, d.h. $0+0=0,\ 0+1=1,\ 1+0=1,\ 1+1=10$.
Wertetabelle für Eingänge x, y und Ausgänge s (sum) und o (overflow):

x	y	$s(x,y)$	$o(x,y)$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Die DNF der Ausgänge können direkt aus der Tabelle ermittelt werden:

$$s(x,y) = (\overline{x} \wedge y) \vee (x \wedge \overline{y}),\ o(x,y) = (x \wedge y)$$

Anwendung: Halb-Addierer (2/2)



Weitere Anwendungen

> MVS

- Für elementare Rechenoperationen mehrstelliger Binärzahlen werden Volladdierer und Multiplikatoren konstruiert, die auf Halb-Addierern aufbauen.
- Logische Schaltungen für die Anzeige von Zahlen auf elektronischen Geräten laßen sich ebenfalls mit einfachen Booleschen Funtkionen und (Vereinfachungen) der DNF implementieren.
- Neben dem Quine-McCluskey-Verfahren gibt es weitere Vereinfachungen von DNF's bzw. KNF's, z.B. das graphische Verfahren von **Karnaugh und Veitch**, s. (Beutelspacher, Zschiegner, 2011).
- Die Prinzipien von Booleschen Algebren und logischen Schaltungen sind die Grundlage für die Digitaltechnik in zahlreichen weiteren technischen Anwendungsgebieten.

Abschnitt 4

Vollständige Induktion — Beweise für unendliche viele natürliche Zahlen

Vollständige Induktion — Beweise für unendliche viele natürliche Zahlen

Motivation und Beispiele

In Mathematik, Informatik und Naturwissenschaften werden oft Aussagen formuliert, die für unendlich viele natürliche Zahlen gelten:

- Für alle $n \in \mathbb{N}$ gilt $\sum_{i=1}^{n}(2i-1) = n^2$.
- Jede natürliche Zahl $n > 1$ besitzt eine bis auf Reihenfolge der Faktoren eindeutige Darstellung als Produkt von Primzahlen.

Einerseits können diese Aussagen unmöglich für alle $n \in \mathbb{N}$ einzeln bewiesen werden. Andererseits sind sie mit Hilfe von $\mathbb{N}$ durchnummeriert und deshalb bietet es sich an, das Konstruktionsprinzip von $\mathbb{N}$ für den Beweis aller Aussagen zu verwenden (**Beweisprinzip der vollständigen Induktion**, Principle of Mathematical Induction):

1. Anfang mit dem Beweis für die erste Aussage (**Induktionsanfang**)
2. Nachweis, dass aus dem Beweis einer beliebigen Aussage der Beweis der nächsten in der Reihenfolge der Nummerierung folgt (**Induktionsschritt**)

Vollständige Induktion: Beispiel

Beispiel (1.69)

Für $n \in \mathbb{N}$ gilt $\sum_{i=1}^{n}(2i-1) = n^2$

1. Induktionsanfang: Für $n = 1$ gilt $\sum_{i=1}^{n}(2i-1) = 1 \cdot (2-1) = 1 = 1^2 = n^2$.
2. Induktionsschritt $n \to n+1$:
   Nach Induktionsannahme ist $\sum_{i=1}^{n}(2i-1) = n^2$ wahr. Dann gilt

$$\begin{aligned}
\sum_{i=1}^{n+1}(2i-1) &= \underbrace{\sum_{i=1}^{n}(2i-1)}_{n^2} + (2(n+1)-1) && \text{Letzten Summanden abtrennen} \\
&= n^2 + (2(n+1)-1) && \text{Nach Induktionsannahme} \\
&= n^2 + (2n+1) && \text{Ausmultiplizieren in der Klammer} \\
&= (n+1)^2 && \text{Binomische Formel}
\end{aligned}$$

Vollständige Induktion: Hinweis

Auf den Induktionsanfang kann man nicht verzichten, wie diese "Formel" zeigt, für die der Induktionsschritt beweisbar ist, obwohl sie ungültig ist:

$$\sum_{i=1}^{n}(2i-1) = n^2 + 1$$

Angenommen $\sum_{i=}^{n}(2i-1) = n^2+1$ ist wahr für $n \in \mathbb{N}$. Dann gilt

$$\sum_{i=1}^{n+1}(2i-1) = \sum_{i=1}^{n}(2i-1) + (2(n+1)-1) = (n^2+1) + (2n+1) = (n+1)^2 + 1$$

Warum ist diese Formel trotzdem ungültig?

Vollständige Induktion

Satz (1.70)

Sei $X \subseteq \mathbb{N}$ eine Teilmenge der natürlichen Zahlen mit folgenden Eigenschaften:

1. $1 \in X$
2. *Wenn $n \in X$, dann gilt auch $n + 1 \in X$.*

Dann ist $X = \mathbb{N}$.

Beweis.

Widerspruchsbeweis: Leite aus $\neg(p \Rightarrow q)$ einen Widerspruch ab.
Angenommen 1. und 2. sind erfüllt aber $X \neq \mathbb{N}$.
Dann gibt es ein kleinstes $b \in A := \mathbb{N} \setminus X$, d.h. b ist minimal mit $b \notin X$.
Nach 1. ist $1 < b$ bzw. $b - 1 \in \mathbb{N}$.
Da b minimal ist mit $b \notin X$ gilt $b - 1 \in X$.
Aus 2. folgt $b = (b - 1) + 1 \in X$ im Widerspruch zu $b \notin X$.
Also ist die Annahme falsch und $X = \mathbb{N}$. □

Hinweis: Das Argument in Zeile 3 ist fundamental für viele Aussagen der Algebra.

Beispiel (1.71)

Für alle $n \in \mathbb{N}$ ist $5^n - 1$ durch 4 teilbar.

Beweis.

1. Induktionsanfang: $5^1 - 1 = 4$ ist durch 4 teilbar.
2. Induktionsschritt: Sei $5^n - 1$ durch 4 teilbar.
   Dann existiert ein $k \in \mathbb{N}$ mit $5^n - 1 = 4k$ und es gelten:

$$5^{n+1} - 1 = 5^{n+1} - 5^n + \underbrace{5^n - 1}_{4k} = 5^n(5-1) + 4k = 4\underbrace{(5^n + k)}_{m}$$

   Mit $m := 5^n + k$ ist also $5^{n+1} - 1 = 4m$ durch 4 teilbar.

□

Vollständige Induktion: Beispiele

Satz (1.72)

Fundamentalsatz der Zahlentheorie: *Jede natürliche Zahl $n > 1$ besitzt eine bis auf Reihenfolge der Faktoren eindeutige Darstellung als Produkt von Primzahlen.*

Notation

Für die Primfaktorzerlegung einer natürlichen Zahl $n \in \mathbb{N}$ werden folgende Schreibweisen verwendet:

- $n = p_1 \cdots p_k$ mit Primzahlen $p_1, \ldots, p_k$ (Wiederholungen möglich)
- $n = {p_1}^{\alpha_1} \cdots {p_s}^{\alpha_s}$ mit Primzahlen $p_1 < \cdots < p_s$ und Exponenten $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$
- $n = \prod_{i=1}^{s} {p_i}^{\alpha_i}$

Generell wird die **Teilbarkeitsrelation** wie folgt bezeichnet:
Sei $d \in \mathbb{N}$ ein **Teiler** von n (d.h., $\exists q \in \mathbb{N}$ mit $n = qd$). Dann schreibt man $d \mid n$.

Beweis.

Teil 1: Existenz der Primfaktorzerlegung

1. Induktionsanfang: $n = 2$ ist das Produkt von genau einer Primzahl.
2. Induktionsschritt: Nach Annahme ist jedes $1 < m \leq n$ Produkt von Primzahlen.
   Hilfssatz: Für jede Zahl $1 < x \in \mathbb{N}$ ist der kleinste Teiler $d > 1$ von x eine Primzahl.
   Beweis: Andernfalls gäbe es $d_1, d_2 \in \mathbb{N}$ mit $1 < d_1 < d$ und $1 < d_2 < d$ sowie $d = d_1 d_2$, damit wäre aber d nicht minimal im Widerspruch zur Voraussetzung.
   Aus dem Hilfssatz folgt: $n + 1$ hat einen Primfaktor p_1. Folglich gilt $\frac{n+1}{p_1} \in \mathbb{N}$.
   Fall 1: $1 = \frac{n+1}{p_1}$. Dann ist $n + 1 = p_1$ und damit ist die Behauptung bewiesen.
   Fall 2: $1 < \frac{n+1}{p_1} < n + 1$. Nach Induktionsannahme gibt es Primzahlen $p_1, \ldots, p_k$ mit $m := \frac{n+1}{p_1} = p_2 \cdots p_k$, d.h. $n + 1 = p_1 \cdots p_k$.

Auch die Eindeutigkeit der Primfaktorzerlegung kann mit vollständiger Induktion bewiesen werden. Für den Induktionsschritt ist das folgende Ergebnis hilfreich, das auf Sätzen aus der Zahlentheorie aufbaut, die später bewiesen werden:

Lemma (1.73)

Für eine Primzahl p und $m, n, q_1, \dots q_k \in \mathbb{N}$ mit $k \in \mathbb{N}$ gelten:

1. $p \mid mn \Longrightarrow (p \mid m) \vee (p \mid n)$.
2. $p \mid (q_1 \cdots q_k) \Longrightarrow \exists s \leq k : p \mid q_s$

Teil 2 folgt aus Teil 1 mit vollständiger Induktion (Übung).

Beweis.

Fallunterscheidung für Teil 1:
Fall 1: p ist ein Teiler von n. Dann ist der Beweis bereits abgeschlossen.
Fall 2: p ist kein Teiler von m. Es bleibt zu zeigen: $p \mid n$.
Wegen $p \mid mn$ existiert ein $q \in \mathbb{N}$ mit $mn = pq$.
Sei $d = \mathrm{ggT}(p, m)$ der größte gemeinsame Teiler von p und m (Nachweis von Existenz und Eindeutigkeit später mit dem Euklidischen Algorithmus).
Da p prim ist, gilt $d = 1$.
Aus dem Satz von Bézout (Beweis später) folgt, dass $x, y \in \mathbb{Z}$ existieren mit $1 = px + my$. Daraus folgt

$$n = n(px + my) = npx + nmy = pnx + mny = pnx + pqy = p(nx + qy)$$

und schließlich $p \mid n$. □

Beweis des Fundamentalsatzes — Teil 2: Eindeutigkeit der Primfaktorzerlegung
Induktion über die Länge der Primfaktorzerlegung von n.
Induktionsnannahme $A(m)$: Für Primfaktorzerlegungen $n = p_1 \cdots p_m = q_1 \cdots q_k$ mit $m \leq k$ gilt

- $m = k$
- Die Primzahlmengen $\{p_i \mid i = 1, \ldots, m\}$ und $\{q_j \mid j = 1, \ldots, k\}$ lassen sich eindeutig aufeinander abbilden.

Induktionsanfang $m = 1$: Aus dem Lemma folgt, dass es ein $s \leq k$ gibt mit $p_1 \mid q_s$.
Da q_s prim ist, gilt $p_1 = q_s$ und damit $1 = \frac{p_1}{p_1} = \frac{p_1}{q_s} = \frac{n}{q_s} = \frac{1}{q_s} q_1 \cdots q_k$.
Daraus folgt $k = 1$ und wegen $1 \leq s \leq k$ auch $1 = s$.
Schließlich liefert die Zuordnung $p_1 \mapsto q_s$ die gesuchte eindeutige Abbildung der Primzahlmengen.

Vollständige Induktion: Beispiele

Induktionsschritt $m \to m+1$: Sei $A(m)$ wahr und $(p_1 \cdots p_m) \cdot p_{m+1} = q_1 \cdots q_k =: y$. Mit $x := (p_1 \cdots p_m)$ ist also $x \cdot p_{m+1} = y$ und daher $p_{m+1} \mid y = q_1 \cdots q_k$. Das Lemma impliziert die Existenz von $s \leq k$ mit $p_{m+1} \mid q_s$. Da q_s prim ist gilt $p_{m+1} = q_s$ und

$$(p_1 \cdots p_m) = \frac{1}{p_{m+1}}(p_1 \cdots p_m) \cdot p_{m+1} = \frac{1}{q_s} q_1 \cdots q_k$$

Auf der rechten Seite ist q_s herausgekürzt und es liegt deshalb nur ein Produkt von $k-1$ Primzahlen vor.
Nach Induktionsannahme $A(m)$ angewendet auf diese Darstellung ist $m = k-1$ und die Primzahlmengen $\{p_i \mid i = 1, \ldots, m\}$ und $\{q_j \mid j = 1, \ldots, k, j \neq s\}$ lassen sich eindeutig aufeinander abbilden. Mit der Zuordnung $p_{m+1} \mapsto q_s$ kann diese Abbildung auf die Gesamtmengen $\{p_i \mid i = 1, \ldots, m+1\}$ und $\{q_j \mid j = 1, \ldots, k\}$ erweitert werden und der Induktionsschritt ist vollständig bewiesen.

Abschnitt 5

Relationen und Abbildungen — Modellierung von Objektbeziehungen und Veränderungsprozessen

Relationen und Abbildungen — Modellierung von Objektbeziehungen und Veränderungsprozessen

Motivation

Für die Modellierung der **Beziehungen zwischen Objekten der realen und digitalen Welt** (Geschäftspartner, Instagram Follower, Elementarteilchen, Knoten in Computernetzwerken etc.) bieten die Konzepte der **Relationen** und **Abbildungen** sehr mächtige Werkzeuge. In der **klassischen Physik** hat das von Descartes (1596 – 1650) etablierte **cartesische Koordinatensystem** (in heutiger Terminologie ein **cartesisches Produkt**) analytische Verfahren ermöglicht, die mit der von Newton und Leibniz entwickelten Differential- und Integralrechnung zur revolutionären Entwicklung der Naturwissenschaften geführt haben. Auch heute verwenden viele Disziplinen von **Artificial Intelligence** über **Biotechnologie** bis zur **Quantenphysik** diese Methoden und veranlassen weitere Forschungen. Ebenso beruht in der **Enterprise IT** die **Digitalisierung der Geschäftsprozesse** auf Relationen und Abbildungen (z.B. bei Datenmodellierung und effizienten Algorithmen).

Cartesisches Produkt

Definition (1.74)

Seien $A, A_1, \ldots, A_n$ Mengen ($n \in \mathbb{N}$).

- $A_1 \times \cdots \times A_n := \prod_{i=1}^{n} A_i := \{(a_1, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$ **cartesisches Produkt** (cartesian product) besteht aus n-**Tupeln** (n tuples) $(a_1, \ldots, a_n)$, dabei kommt es auf die Reihenfolge der Elemente $a_1, \ldots, a_n$ an.
- $A^1 := A,\ A^2 := A \times A,\ A^n := \underbrace{A \times \cdots \times A}_{n-\text{mal}}$

Beispiele (1.75)

- $\mathbb{R}^2$ (reelle Zahlenebene) und $\mathbb{R}^3$ (euklidischer 3-dimensionaler Raum)
- $\{1\} \times \{3,4\} = \{(1,3),(1,4)\} \neq \{(3,1),(4,1)\} = \{3,4\} \times \{1\}$
- Für $B_2 = \{0,1\}$ ist ${B_2}^3 \neq B_2 \times {B_2}^2$ (warum?)
- $S := \{s \mid s \text{ studiert an DHBW MA}\}$, $F := \{f \mid f \text{ Studiengang der DHBW MA}\}$. Was ist $S \times F$?

Relationen

Definition (1.76)

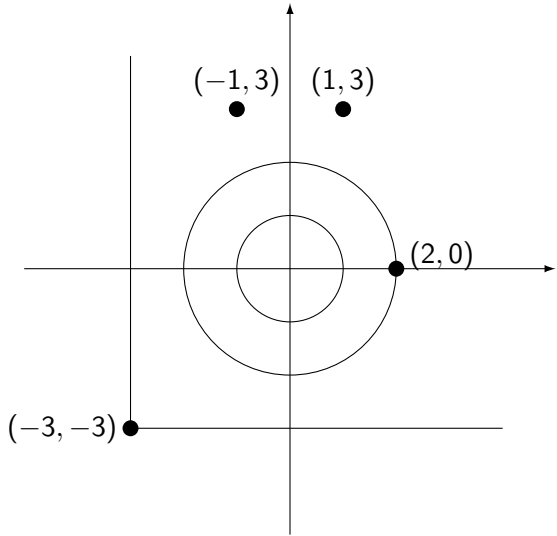
Für $n \in \mathbb{N}$, Mengen $A, A_1, \ldots, A_n$ und $a, b \in A$ wird vereinbart:

- Eine Teilmenge $X \subseteq A_1 \times \cdots \times A_n$ heißt **n-stellige Relation in** $A_1 \times \cdots \times A_n$.
- $R \subseteq A^2$ wird als **binäre Relation in** A bezeichnet. Notation: $aRb :\Longleftrightarrow (a, b) \in R$

Beispiele (1.77)

- $S := \{s \mid s \text{ studiert an DHBW MA}\}$, $F := \{f \mid f \text{ Studiengang der DHBW MA}\}$.
  $R := \{(s, f) \in S \times F \mid s \text{ studiert Studiengang } f \text{ an DHBW MA}\}$
  $T := \{(s, s') \in S^2 \mid s \text{ folgt } s' \text{ auf Twitter}\}$
- Uhrzeiten: Für Zeiten t_1, t_2 in Stunden sei $t_1 \sim t_2 :\Leftrightarrow \exists z \in \mathbb{Z} : t_1 = t_2 + 24z$
- In $\mathbb{R}$ sind $\leq$ und $=$ binäre Relationen.
- $\leq$ in $\mathbb{R}^2 : \forall (x, y), (x', y') \in \mathbb{R}^2 : (x, y) \leq (x', y') :\Leftrightarrow (x \leq x') \wedge (y \leq y')$
- Vektoren mit gleichem Betrag in $\mathbb{R}^2$: $(x, y)A(x', y') :\Leftrightarrow |(x, y)| = |(x', y')|$, d.h. $\sqrt{x^2 + y^2} = \sqrt{x'^2 + y'^2}$

Relationen in der reellen Zahlenebene $\mathbb{R}^2$



Beispiel (1.78)

Bei der Digitalisierung von Geschäftsprozessen eines Unternehmens E spielen Relationen zwischen Entitäten wie "Kunde", "Auftrag", "Material", "Lieferant" etc. eine zentrale Rolle. Eine einfache Datenmodellierung enthält z.B. folgende Objekte:

- $CUSTOMERS := \{c \mid c \text{ Kunde von } E\}$
- $ORDERS := \{o \mid o \text{ Auftrag von Kunde } c \text{ für } E\}$
- $MATERIALS := \{m \mid m \text{ Material, das in Aufträgen für } E \text{ verwendet wird }\}$
- $VENDORS := \{v \mid v \text{ Lieferant, der Materialen an } E \text{ liefert}\}$

Zwischen diesen Objekten bestehen folgende Relationen:

- $R_1 := \{(c, o) \in CUSTOMERS \times ORDERS \mid o \text{ Auftrag von Kunde } c\}$
- $R_2 := \{(o, m) \in ORDERS \times MATERIALS \mid m \text{ wird in } o \text{ verwendet}\}$
- $R_3 := \{(m, v) \in MATERIALS \times VENDORS \mid m \text{ wird von } v \text{ geliefert}\}$

Exercise

Define a data model (incl. entities/tables and relations between them) for a digital platform offering flights between various destinations:

- *CUSTOMERS* (Customers)
- *GEOCITY* (Destinations of locations)
- *CARRIERS* (Airlines)
- *PLANFLI* (Potential flights between destinations, incl. max. number of seats)
- *ACTFLI* (Actual flights including date, price and number of booked seats)
- *BOOKINGS* (Bookings of customers incl. order date)

Relations play a major role in Enterprise IT even beyond well established data modeling of master and transaction data in relational databases:

- Agile business processes: Enable customizing via table entries instead of program changes. This approach supports seamless changes of business processes without time consuming compilation and software lifecycle management efforts.
- Performance: Fast analytical and transactional scenarios using column store databases with appropriate data models.

Beispiele (1.79)

Einteilung der Bluthochdruckwerte nach WHO/ISH

Grad der Hypertonie	systolisch
Grad 0 (keine Hypertonie)	< 140
Grad 1	$140 - 159$
Grad 2	$160 - 179$
Grad 3	≥ 180

Für eine Stichprobe (d.h., einer Menge von Patienten) S und $x, y \in S$ wird mit

$$xHy :\Longleftrightarrow \text{ Blutdruck von } x \text{ hat denselben Grad wie der Blutdruck von } y$$

eine Relation H zur Clusterung der Blutdruckwerte definiert, die für statistische und therapeutische Zwecke verwendet ist.

Relationen: Teilbarkeit und Lexikographische Ordnung

Beispiele (1.80)

- **Teilbarkeit:** Für $a, b \in \mathbb{N}$ gilt a **teilt** b (Notation: $a \mid b$) $:\Longleftrightarrow \exists q \in \mathbb{N} : b = q \cdot a$
- **Lexikographische Ordnung** (bzw. "Telefonbuchordnung"): Für das Alphabet $A = \{a, b, c, \ldots, z\}$ wird die übliche Ordnung $a < b < \cdots < z$ verwendet und ein **Wort über** A definiert als endliche Zeichenkette aus A. Die **Menge aller Wörter** wird mit A^* bezeichnet und für $w \in A^*$ sei $l(w)$ die **Länge** von w. Für **das leere Wort** Λ ist die Länge 0 festgelegt.
  Für Wörter $v = v_1 \ldots v_m \in A^*$ und $w = w_1 \ldots w_n \in A^*$ ist die lexikographische Ordnung rekursiv definiert über die Länge von v:
  1. Für $l(v) = 0$ ist $v = \Lambda \leq w$.
  2. Für $l(v) > 0$ sei $v \leq w :\Longleftrightarrow (v_1 < w_1) \vee ((v_1 = w_1) \wedge v_2 \ldots v_m \leq w_2 \ldots w_n)$

Ordnungsrelationen

Definition (1.81)

Eine binäre Relation $R \subseteq A^2$ in einer Menge A heißt

reflexiv	$\forall a \in A : aRa$
symmetrisch	$\forall a, b \in A : aRb \Longrightarrow bRa$
antisymmetrisch	$\forall a, b \in A : (aRb \wedge bRa) \Longrightarrow (a = b)$
transitiv	$\forall a, b, c \in A : aRb \wedge bRc \Longrightarrow aRc$
linear	$\forall a, b \in A : aRb \vee bRa$
Halbordnung	R ist reflexiv, antisymmetrisch und transitiv
Äquivalenzrelation	R ist reflexiv, symmetrisch und transitiv

Halbgeordnete Mengen (partially ordered sets, "posets") sind Verallgemeinerungen der natürlichen, reellen oder komplexen Zahlen mit der üblichen Relation $\leq$, während Äquivalenzrelationen (equivalence relations) Abstraktionen von $=$ bzw $\Longleftrightarrow$ sind.

Ordnungsrelationen

Beispiele (1.82)

Bestimmen Sie die Eigenschaften dieser Relationen:

- $T := \{(s, s') \in S^2 \mid s \text{ folgt } s' \text{ auf Twitter}\}$
- Uhrzeiten: Für Zeiten t_1, t_2 in Stunden sei $t_1 \sim t_2 :\Longleftrightarrow \exists z \in \mathbb{Z} : t_1 = t_2 + 24z$
- $\leq$ in $\mathbb{R}$ und $\mathbb{R}^2$
- Teilbarkeit: Für $a, b \in \mathbb{N}$ ist $a \mid b :\Longleftrightarrow \exists q \in \mathbb{N} : b = q \cdot a$
- Lexikographische Ordnung auf der Menge von Wörtern A^* über einem Alphabet A.
- $\mathrm{Id}_{\mathbb{R}} := \Delta_{\mathbb{R}} := \{(x, y) \in \mathbb{R}^2 \mid x = y\} \subset \mathbb{R}^2$ (Identität oder Diagonale)
- $R := \mathbb{R}^2 \subseteq \mathbb{R}^2$ (Allrelation)

Der folgende Satz klärt den Zusammenhang zwischen Booleschen Algebren und Halbordnungen und motiviert die Verwendung von Hasse-Diagrammen:

Satz (1.83)

In jeder Boolesche Algebra B wird durch

$$a \leq b :\Leftrightarrow a = a \wedge b$$

eine Halbordnung $\leq$ definiert, bei der für je zwei Elemente $a, b \in B$ gilt:

- $\sup(a, b) = a \vee b$
- $\inf(a, b) = a \wedge b$

Beweis.
Übung. □

Äquivalenzklassen

Definition (1.84)

Für eine Äquivalenzrelation R auf einer Menge A und $a \in A$ heißt

$$\overline{a} := [a] := [a]_R := \{b \in A \mid aRb\}$$

Äquivalenzklasse von a. Ein Element $b \in [a]_R$ wird als **Repräsentant** der Klasse bezeichnet.

Beispiele (1.85)

- Für Uhrzeiten: $t_1 \sim t_2 :\Leftrightarrow \exists z \in \mathbb{Z} : t_1 = t_2 + 24z$ sind die Äquivalenzklassen alle 'gleichen' Uhrzeiten an verschiedenen Tagen (Stunden zwischen 0 und 23 Uhr).
- Menge $A = \{0, 1, 2\}$ und Äquivalenzrelation

$$R = \{(0,0), (1,1), (2,2), (0,1), (1,0)\}.$$

Es gibt zwei Äquivalenzklassen von R: $[0] = \{0, 1\}, [2] = \{2\}$

Äquivalenzklassen

Satz (1.86)

Für eine Äquivalenzrelation R auf einer Menge A gelten:

1. $\bigcup_{a \in A} [a]_R = A$
2. $\forall a, b \in A : [a]_R = [b]_R \iff aRb$
3. $\forall a, b \in A : [a]_R \cap [b]_R = \emptyset \ \vee \ [a]_R = [b]_R$

Beweis.

Übung □

Definition (1.87)

Sei A eine nichtleere Menge. Eine Familie von nichtleeren Mengen $\mathcal{P} = \{A_i \mid i \in I\}$ nennt man eine **Partition** oder **Zerlegung** oder **Klasseneinteilung** von A, wenn gelten:

- $\bigcup_{i \in I} A_i = A$
- $\forall i, j \in I : A_i \cap A_j = \emptyset \ \vee \ A_i = A_j$

Korollar (1.88)

Sei A eine nichtleere Menge und R eine Äquivalenzrelation auf A.

- *Die Äquivalenzklassen von R bilden eine Partition von A:*

$$\mathcal{P}_R := \{[a]_R \mid a \in A\}$$

- *Für eine Partition $\mathcal{P} = \{A_i \mid i \in I\}$ von A ist die Relation*

$$R_{\mathcal{P}} := \{(a, b) \in A^2 \mid \exists i \in I : (a, b) \in A_i\}$$

  eine Äquivalenzrelation auf A.

- *Es gilt $R = R_{\mathcal{P}_R}$.*

Beweis.

Teil 1 folgt unmittelbar aus (1.86). Die anderen Teile bitte als Übung beweisen.

Äquivalenzrelation: Kongruenz

Beispiel (1.89)

Eine sehr wichtige Äquivalenzrelation auf $\mathbb{Z}$ ist die Kongruenz: Für $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ heißt a **kongruent** b **modulo** n , wenn gilt:

$$a \equiv_n b :\Longleftrightarrow a = b (\text{mod } n) :\Longleftrightarrow n \mid (a - b)$$

Die Kongruenz kann auch dadurch charakterisiert werden, dass für a und b bei Division durch n derselbe Rest übrig bleibt:

$$a \equiv_n b \Longleftrightarrow \exists k, l \in \mathbb{Z}\ \exists r \in \mathbb{N}_0 : (0 \leq r < n) \wedge (a = kn + r) \wedge (b = ln + r)$$

Für $a \in \mathbb{Z}$ ist die **Rest- bzw. Kongruenzklasse von** a **modulo** n (congruence class):

$$[a] = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : x = kn + a\} = \{kn + a \mid k \in \mathbb{Z}\}$$

Übungsaufgabe: Nachweis, dass $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$ definiert.

Kongruenzklassen

Beispiele (1.90)

Bitte begründen bzw. beschreiben Sie folgende Kongruenzrelationen bzw. Kongruenzklassen::

1. $25 = 1 \mod 12$ (Uhrzeiten oder Monate)
2. $366 = 2 \mod 7$ (Wochentage)
3. $30 = 4 \mod 26$ (Codierung von Buchstaben des Alphabets)
4. $17 = -3 \mod 5$
5. Beschreiben Sie für $n = 5$ und die Relation $\equiv_5$ die Restklasse [4] als Teilmenge der ganzen Zahlen.

Beispiel 3 ist sehr relevant in der Codierungstheorie, um z.B. Wörter mit Buchstaben aus einem Alphabet mit 26 Zeichen als Zahlen darzustellen. Darüberhinaus spielen diese Kongruenzrelationen eine grosse Rolle in der Kryptographie (vgl. die Erklärungen zum RSA-Algorithmus im weiteren Verlauf dieser Vorlesung).

Musterlösung (1.90)

1. $25 = 1 \mod 12 : 25 - 1 = 24 \wedge 12 \mid 24 \Rightarrow \text{true}$
2. $366 = 2 \mod 7 : 366 - 2 = 364 \wedge 7 \mid 364 \Rightarrow \text{true}$
3. $54 = 2 \mod 26 : 54 - 2 = 52 \wedge 26 \mid 52 \Rightarrow \text{true}$
4. $17 = -3 \mod 5 : 17 - (-3) = 20 \wedge 5 \mid 20 \Rightarrow \text{true}$
5. Für die Relation $\equiv_5$ ist die Restklasse $[4]$ als Teilmenge von $\mathbb{Z}$ gegeben durch

$$[4] = \{4, 9, -1, 14, -6, ...\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : x = k \cdot 5 + 4\}.$$

Quotientenmengen

Definition (1.91)

Sei R eine Äquivalenzrelation auf A. Die Menge

$$A/R := \{[a]_R \mid a \in A\}$$

wird als **Quotientenmenge** oder **Faktormenge** (factor set) von A nach R bezeichnet.

Beispiele (1.92)

- Für $n \in \mathbb{N}$ ist $\mathbb{Z}_n := \mathbb{Z}/\equiv_n$.
- Die Restklasse $[5] \in \mathbb{Z}_6$ als Teilmenge der ganzen Zahlen ist

$$[5] = \{5, 11, -1, 17, -7, ...\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : x = k \cdot 6 + 5\}.$$

Addition von Kongruenzklassen

Mit den Kongruenzklassen in $\mathbb{Z}_n$ kann man sehr sehr gut rechnen. Zunächst wird die Addition untersucht, die Multiplikation folgt im Abschnitt 'Modulare Arithmetik'.

Definition (1.93)

Für $n \in \mathbb{N}$ ist die **Addition von Kongruenzklassen** definiert durch die Addition der Repräsentanten der Kongruenzklassen, d.h. für alle $x, y \in \mathbb{Z}$ ist

$$[x] + [y] := [x + y]$$

Lemma (1.94)

Die Addition von Kongruenzklassen ist unabhängig von der Wahl der Repräsentanten.

Beweis.

Für $x' \in [x]$ und $y' \in [y]$ ist zu zeigen: $[x + y] = [x' + y']$ bzw. $x + y \equiv_n x' + y'$
Wegen $x \equiv_n x' \wedge y \equiv_n y'$ gilt auch $n \mid (x - x') + (y - y') = (x + y) - (x' + y')$ und damit $x + y \equiv_n x' + y'$.

Addition von Kongruenzklassen: $\mathbb{Z}_6$

Beispiel (1.95)

Additionstafel von $\mathbb{Z}_6$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Addition von Kongruenzklassen: Prüfziffern (1/3)

Beispiel (1.96)

Prüfziffern in Zahlencodes dienen dazu, die häufigsten Fehler beim Datenaustausch und bei der manuellen Eingabe von Zahlen zuverlässig zu erkennen, z.B. **Einzelfehler** (fehlerhafte Ziffern an einer Stelle) und **Vertauschung von zwei Ziffern**. Algorithmen für Prüfziffern werden z.B. eingesetzt für

- die Europäische Artikelnummer (EAN) (mit 8 oder 13 Stellen),
- das Einheitliche Kontonummernsystem (EKONS) der Banken, und
- die Internationale Standard Buchnummer (ISBN) (mit 10 oder 13 Stellen).

Bei diesen Algortihmen wird sehr oft die **Addition von Kongruenzklassen** verwendet und weiter unten am Beispiel von ISBN-10 detailliert erläutert. Die Nachweise, dass Einzelfehler und Vertauschung von zwei Ziffern garantiert erkannt werden, beruhen auf Ergebnissen der Algebra, die jenseits des Rahmens dieser Vorlesung liegen.
Für mehr Details sie (Beutelspacher und Zschiegner), (Teschl und Teschl) und Wikipedia: https://de.wikipedia.org/wiki/Internationale_Standardbuchnummer.

Addition von Kongruenzklassen: Prüfziffern (2/3)

Die Internationale Standard Buchnummer der Länge 10 (ISBN-10) enthält eine Prüfziffer am Ende, für deren Berechnung Kongruenz modulo 11 verwendet wird. Eine ISBN-10-Nummer ist von dieser Form:

$$z_1 - z_2 z_3 z_4 - z_5 z_6 z_7 z_8 z_9 - z_{10}$$

Die Ziffer z_1 verschlüsselt das Herkunftsland (z.B: $z_1 = 3$ für Deutschland, Österreich und Schweiz) und die drei Ziffern $z_2 z_3 z_4$ den Verlag. Die Prüfziffer z_{10} ist eine gewichtete Quersumme der ersten 9 Ziffern, d.h. es muss gelten:

$$z_{10} = \sum_{i=1}^{9} (i \cdot z_i) \pmod{11}$$

Addition von Kongruenzklassen: Prüfziffern (3/3)

Z.B. hat das Buch "Gödel, Escher, Bach" von Douglas R. Hofstadter die ISBN 3-608-93037-X (das Symbol X steht für 10 mod 11) und die Prüfziffer ergibt sich aus:

$$\begin{aligned} z_{10} &= (1 \cdot 3 + 2 \cdot 6 + 4 \cdot 8 + 5 \cdot 9 + 6 \cdot 3 + 8 \cdot 3 + 9 \cdot 7) \mod 11 \\ &= (3 + 12 + 32 + 45 + 18 + 24 + 63) \mod 11 \\ &= (3 + 1 + 10 + 1 + 7 + 2 + 8) \mod 11 \\ &= 32 \mod 11 \\ &= 10 \mod 11 \end{aligned}$$

Abbildungen

Satz (1.97)

Seien D und W Mengen und $f : D \to W$ eine Abbildung.

1. *Die Abbildung f definiert durch*

$$\forall x \in D \, \forall y \in W : (x, y) \in R_f :\Longleftrightarrow y = f(x)$$

eine Relation $R_f \subseteq D \times W$, für die gilt:

$$\forall x \in D \, \exists! y \in W : (x, y) \in R_f \tag{1}$$

R_f wird auch als **Graph von** *f bezeichnet mit der Notation graph(f).*

2. *Jede Relation $R \subseteq D \times W$ mit der Eigenschaft (1) definiert eine Abbildung $f_R : D \to W$, so dass für alle $x \in D$ und $y \in W$ gilt: $(x, y) \in R \Longleftrightarrow y = f_R(x)$.*
3. *Ferner sind $f_{R_f} = f$ und $R_{f_R} = R$.*

Injektivität, Surjektivität und Konkatenation von Abbildungen

Definition (1.98)

Seien A, B, C Mengen und $f : A \to B$ und $g : B \to C$ Abbildungen.

- f ist **injektiv**, wenn gilt: $\forall a, a' \in A : f(a) = f(a') \Rightarrow a = a'$.
- f ist **surjektiv**, wenn gilt: $\forall b \in B \; \exists a \in A : b = f(a)$.
- f ist **bijektiv**, wenn injektiv und surjektiv ist.
- Die **Konkatenation** oder **Verknüpfung** von g und f ist definiert durch:

$$g \circ f : A \to C, x \mapsto g(f(x)) =: (g \circ f)(x)$$

Die Eigenschaften der Injektivität und Surjektivität sind sowohl durch die Funktionsgleichung $y = f(x)$ (z.B. $y = x^2 - 1$) als auch durch die Definitions- und Wertemengen bestimmt. In anderen Worten: Dieselbe Funktionsgleichung kann mit einer Definitionsmenge zu einer injektiven Funktion gehören und mit einer anderen zu einer nicht-injektiven Funktion, analog gilt das auch für surjektive Funktionen.

Injektive und surjektive Abbildungen

Satz (1.99)

Jede streng monotone (steigende oder fallende) reelle Funktion $f : X \to \mathbb{R}$ mit einer Definitionsmenge $X \subseteq \mathbb{R}$ ist injektiv.

Beweis.

Seien $a, a' \in X$ mit $f(a) = f(a')$.
Zu zeigen: $a = a'$.
Indirekter Beweis: Annahme $a \neq a'$. Folglich gilt $a < a'$ oder $a > a'$.
Fall 1: $a < a'$.
Fall 1.1: f ist streng monoton steigend. Dann gilt $f(a) < f(a')$, also $f(a) \neq f(a')$ im Widerspruch zur Voraussetzung. Q.E.D.
Fall 1.2: f ist streng monoton fallend. Dann gilt $f(a) > f(a')$, also ebenfalls $f(a) \neq f(a')$ im Widerspruch zur Voraussetzung. Q.E.D.
Fall 2 ($a > a'$) wird analog bewiesen.

□

Injektive und surjektive Abbildungen

Beispiele (1.100)

Untersuchen Sie die folgenden Funktionen auf Injektivität und Surjektivität:

- $f_1 : \mathbb{R} \to \mathbb{R},\ x \mapsto -x + 1$
- $f_2 : [0,1] \to \mathbb{R},\ x \mapsto -x + 1$
- $f_3 : [0,1] \to [0,1],\ x \mapsto -x + 1$
- $f_4 : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$
- $f_5 : [0,2] \to \mathbb{R},\ x \mapsto x^2$
- $f_6 : [-2,2] \to [0,4],\ x \mapsto x^2$

Musterlösungen (1.100)

- $f_1 : \mathbb{R} \to \mathbb{R}$, $x \mapsto -x + 1$:
  Für die Injektivität ist zu zeigen: $\forall x_1, x_2 \in \mathbb{R}$ mit $f_1(x_1) = f_1(x_2)$ folgt $x_1 = x_2$.
  Beweis:
  Seien $x_1, x_2 \in \mathbb{R}$ mit $-x_1 + 1 = f_1(x_1) = f_1(x_2) = -x_2 + 1$.
  Also folgt $-x_1 = -x_2$ und damit $x_1 = x_2$, d.h. f_1 ist injektiv.
  Alternative Lösung: Der Graph von f_1 ist eine Gerade mit Steigung -1, also ist f_1 streng monoton fallend und wegen Satz (1.99) injektiv.
  Surjektivität: Die Gleichung

$$y = -x + 1$$

  hat für jedes $y \in \mathbb{R}$ eine Lösung, die durch Auflösen der Gleichung nach x berechnet werden kann:

$$x = -y + 1$$

  Folglich existiert für alle $y \in \mathbb{R}$ ein $x \in \mathbb{R}$ mit $y = -x + 1 = f_1(x)$, d.h. die Funktion f_1 ist surjektiv.

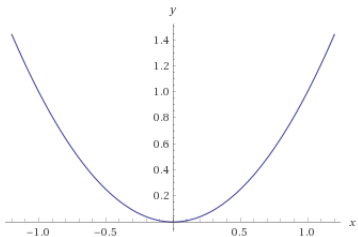
Musterlösungen (1.100)

- $f_2 : [0,1] \to \mathbb{R}$, $x \mapsto -x + 1$: Als Einschränkung von f_1 auf das Intervall $[0,1]$ ist auch f_2 injektiv. Die Gleichung $-1 = -x + 1$ hat aber keine Lösung in $[0,1]$, d.h. es gibt kein $x \in [0,1]$ mit $-1 = -x + 1 = f_2(x)$. Demnach ist f_2 nicht surjektiv.
- $f_3 : [0,1] \to [0,1]$, $x \mapsto -x + 1$: Analog zu f_2 ist auch f_3 injektiv.
  Die Gleichung $y = -x + 1$ hat für jedes $y \in [0,1]$ eine Lösung innerhalb des Intervalls $[0,1]$, da $x = -y + 1$ dann ebenfalls in $[0,1]$ liegt. Deshalb ist die Funktion f_3 surjektiv.
  Alternativ kann man mit Hilfe des Graphen der Geraden argumentieren: Aus dem Graphen ist unmittelbar zu erkennen, dass die Endpunkte des Intervalls $[0,1]$ aufeinander abgebildet werden (in umgekehrter Reihenfolge), außerdem liegen alle Zwischenwerte in $[0,1]$ auf dem Graphen zwischen 1 und 0. Auch damit ist gezeigt, dass f_3 surjektiv ist.

Beispiele: Betragsfunktion und Floor-Funktion

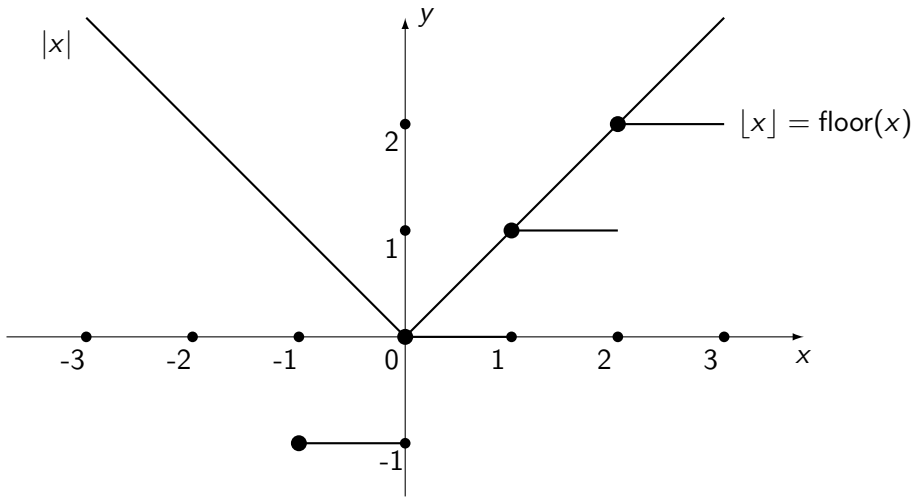
Beispiele (1.101)

- Die quadratische Funktion $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ ist weder injektiv noch surjektiv, s. Beispiel (1.45).



- Die Betragsfunktion $|.| : \mathbb{R} \to \mathbb{R}, x \mapsto |x|$ und die Floor-Funktion $x \mapsto \lfloor x \rfloor$ sind beide weder injektiv noch surjektiv, da sie weder streng monoton steigend oder fallend sind noch alle Zahlen im Wertebereich als Funktionswerte annehmen (s.u.).

Betragsfunktion, Floor-Funktion



Beispiele: Quotientenabbildungen

Beispiel (1.102)

Für jedes $n \in \mathbb{N}$ ist die **Quotientenabbildung**

$$\pi_n : \mathbb{Z} \to \mathbb{Z}_n, a \mapsto [a]_n$$

surjektiv, aber nicht injektiv.
Gegenbeispiel: $n = 3, x_1 = 2, x_2 = 5$:

$$\pi_n(2) = [2] = [5] = \pi_n(5)$$

Konkatenation von Abbildungen

Beispiele (1.103)

Bestimmen Sie für die Funktionen $f_i : \mathbb{R}^+ \to \mathbb{R}$ und $g_i : \mathbb{R} \to \mathbb{R}$ $(i \leq 3)$ jeweils die Konkatenation $g_i \circ f_i$:

- $f_1(x) = 2x,\ g_1(x) = 3x + 3$
- $f_2(x) = -x + 2,\ g_2(x) = x^2 - 4$
- $f_3(x) = \sqrt{x},\ g_3(x) = x^2$

Musterlösungen (1.103)

- $f_1(x) = 2x,\ g_1(x) = 3x + 3$:

$$(g_1 \circ f_1)(x) = g_1(f_1(x)) = 3(2x) + 3 = 6x + 3$$

- $f_2(x) = -x + 2,\ g_2(x) = x^2 - 4$:

$$(g_2 \circ f_2)(x) = g_2(f_2(x)) = (-x + 2)^2 - 4 = (x^2 - 4x + 4) - 4 = x^2 - 4x$$

Bijektive Abbildungen

Satz (1.104)

Sei $f : A \to B$ eine Abbildung.

- *Wenn f bijektiv ist, dann gibt es eine eindeutig bestimmte* **Umkehrabbildung** $g : B \to A$ **von** f *(inverse mapping) mit*

$$(\forall a \in A : g(f(a)) = a) \wedge (\forall b \in B : f(g(b)) = b) \tag{2}$$

  Notation: $f^{-1} := g$

- *Wenn eine Abbildung $g : B \to A$ mit die Eigenschaft (2) gibt, dann ist f bijektiv.*

Beispiele (1.105)

Bestimme die Umkehrabbildungen:

- $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$
- $p : \mathbb{R}^+ \to \mathbb{R}^+, x \mapsto x^2$ (rechter Ast der quadratischen Normalparabel)
- $\exp : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto e^x$ (Exponentialfunktion bzw. e-Funktion)

Musterlösung (1.105)

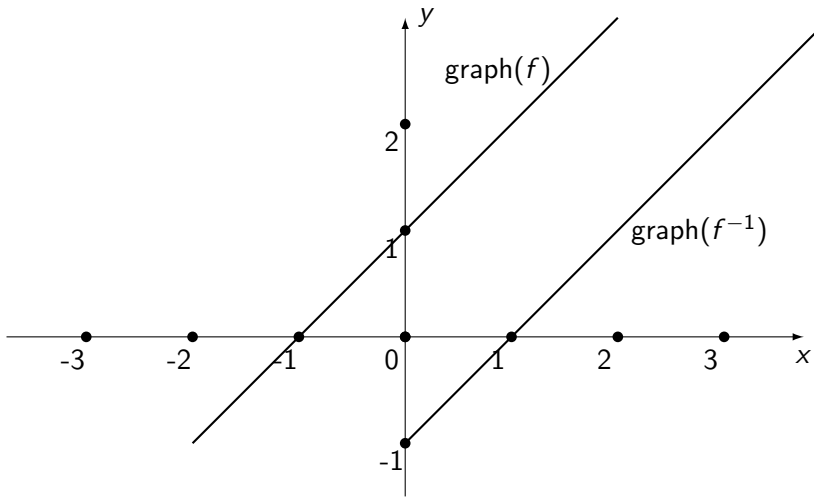
Umkehrabbildung von $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$:
Der Graph von f ist eine Parallele zur Winkelhalbierenden, die um 1 nach oben verschoben ist. Offensichtlich ist f streng monoton steigend und damit injektiv, außerdem auch surjektiv, insgesamt also bijektiv.
Deshalb existiert eine Umkehrabbildung f^{-1}, deren Graph durch Spiegelung an der Winkelhalbierenden entsteht. Also ist der Graph von f^{-1} eine Parallele zur Winkelhalbierenden, die um 1 nach unten verschoben ist, d.h.

$$f^{-1} : \mathbb{R} \to \mathbb{R}, y \mapsto y - 1.$$

Rechnerisch ergibt sich die Umkehrabbildung dadurch, dass die Addition von 1 zur Winkelhalbierenden bei der Funktion f durch eine entsprechende Subtraktion wieder aufgehoben wird. Damit gilt für alle $x, y \in \mathbb{R}$:

$$f^{-1}(f(x)) = (x + 1) - 1 = x \quad \text{und} \quad f(f^{-1}(y)) = (y - 1) + 1 = y$$

Umkehrabbildung einer Geraden



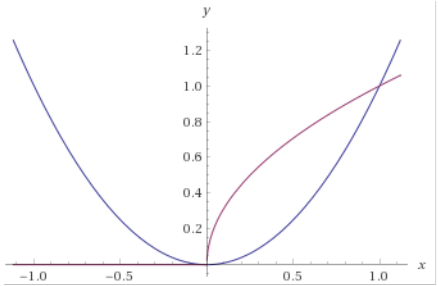
Musterlösung (1.105)

Die Umkehrfunktion der Funktion $p : \mathbb{R}^+ \to \mathbb{R}^+, x \mapsto x^2$, d.h. des rechten Astes der quadratischen Normalparabel, führt auf die **(positive) Quadratwurzelfunktion**

$$s : \mathbb{R}^+ \to \mathbb{R}^+, y \mapsto \sqrt{y}.$$

Ihr Graph G entsteht durch Spiegelung des rechten Parabel-Astes an der ersten Winkelhalbierenden. Da der Parabel-Ast streng monoton steigend ist, entsteht durch Spiegelung ebenfalls der Graph einer Funktion. Offensichtlich gilt für alle $x, y \in \mathbb{R}^+$:

$$x = \sqrt{x^2} = s(p(x)) \quad \text{und} \quad y = (\sqrt{y})^2 = p(s(y))$$

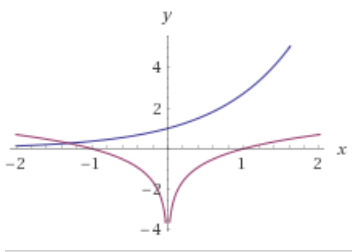


Musterlösung (1.105)

Die Umkehrfunktion der Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto e^x$ ist der natürliche Logarithmus:

$$\ln : \mathbb{R}^+ \to \mathbb{R},\ y \mapsto \ln(x)$$

Graphen von $e^x, \ln(x)$ und $\ln(-x)$:



Hashfunktionen für effiziente Suche und Kryptograhie (1/4)

Beispiel (1.106)

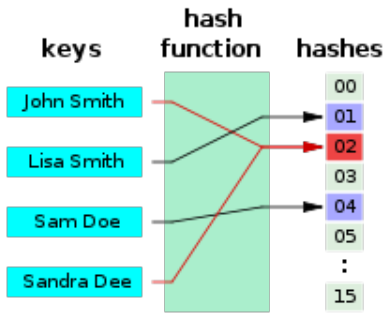
Für effiziente Speicherung und Suche von großen Datenmengen werden oft **Hashfunktionen** eingesetzt, die auch in der Kryptograhie z.B. bei digitalen Signaturen eine zentrale Rolle spielen. Eine Hashfunktion

$$h : K \to \{0, \ldots, n-1\}$$

bildet eine (potentiell sehr große) Menge K von keys (z.B. Namen von Personen) in ein Intervall von natürlichen Zahlen ab. Dabei ist $n \in \mathbb{N}$ oft wesentlich kleiner als $|K|$, die Kardinalität von K (vgl. Definition (1.47)), um die schnelle Suche eines keys in der Menge $\{0, \ldots, n-1\}$ zu ermöglichen. Zusätzlich zu den Hashwerten werden oft Attribute in einer Tabelle gespeichert, z.B. die Kontaktdaten einer Person.
Bei $n < |K|$ sind **Kollisionen** möglich, denn für zwei keys $k_1 \neq k_2$ können deren Hashwerte gleich sein, d.h. $h(k_1) = h(k_2)$. Die Funktion h ist dann nicht injektiv und ein Rückschluss auf k_1 bzw. k_2 ist nicht eindeutig möglich. Gegen solche Kollisionen gibt es Vermeidungsstrategien (s.u.).

Hashfunktionen für effiziente Suche und Kryptograhie (2/4)

Hashfunktion mit Kollisionen:



Von Jorge Stolfi - Eigenes Werk, Gemeinfrei,
https://commons.wikimedia.org/w/index.php?curid=6601264

Hashfunktionen für effiziente Suche und Kryptograhie (3/4)

Hashfunktionen verwenden oft die Addition von Kongruenzklassen. Dafür werden z.B. Wörter über einem Alphabet $\{a, b, \ldots, z\}$ mit den Positionen der Buchstaben im Alphabet codiert, z.B.

$$c(ANNE) = (1, 14, 14, 1).$$

Allgemein ist für ein Wort k die Codierung $c(k)_i$ die Position des i-ten Buchstabens von k. Außerdem sei $l(k)$ die Länge des Worts k. Dann ist der Hashwert

$$h(k) = \sum_{i=1}^{l(k)} c(k)_i \mod n.$$

Damit gilt z.B. für $n = 16$:

$$h(ANNE) = 1 + 14 + 14 + 1 \mod 16 = 30 \mod 16 = 14$$

Hashfunktionen für effiziente Suche und Kryptograhie (4/4)

Kollisionen erlauben keinen Rückschluss auf verschiedene keys mit denselben Hashwerten. Zur Vermeidung von Kollisionen werden Hash-Algorithmen mit Fallunterscheidungen ergänzt, die z.B. bei der Erzeugung eines Hashwertes im Falle einer Kollision eine Konstante addieren, ggf. auch rekursiv. Natürlich werden dann auch Abbruchbedingungen zur Vermeidung von unendlichen Rekursionen benötigt.
In der Praxis wird für $n \in \mathbb{N}$ z.B. ein Wert wie

$$n = 2^{128} = 2^{2^7}$$

gewählt und der Hash-Algorithmus wird so konstruiert, dass er für die Eingabedaten möglichst wenig Kollisionen erzeugt.
Weitere Informationen zu Hashfunktionen in (Teschl und Teschl) sowie Wikipedia:

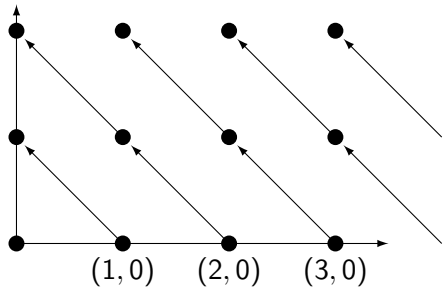
- https://de.wikipedia.org/wiki/Hashfunktion
- https://en.wikipedia.org/wiki/Hash_function

Definition (1.107)

Wenn sich die Elemente einer unendlichen Menge C mit Hilfe von $\mathbb{N}$ nummerieren lassen, d.h., wenn es eine bijektive Abbildung $f : \mathbb{N} \to C$ gibt, dann wird C als **abzählbar unendlich** bzw. **abzählbar** (countable) bezeichnet. In diesem Fall wird die Kardinalität von A mit $|A| = \aleph_0$ ($\aleph$: Hebräischer Buchstabe aleph) beschrieben.

Beispiele (1.108)

- Cantor'sche Diagonalabzählung: Bijektive Abbildung $f : \mathbb{N} \to \mathbb{N}^2$ nach Skizze.



- $\mathbb{R}$ ist nicht abzählbar, d..h. $|\mathbb{R}| > \aleph_0$
- Hilberts Hotel:
  https://en.wikipedia.org/wiki/Hilbert%27s_paradox_of_the_Grand_Hotel

Kapitel 2

Algebraische Strukturen

Abschnitt 1

Modulare Arithmetik — Vom Euklidischen Algorithmus zur modernen Kryptographie

Modulare Arithmetik — Vom Euklidischen Algorithmus zur modernen Kryptographie

Motivation

Kryptographische Methoden verwenden z.B. bei **Public-Key-Verfahren** zahlentheoretische Eigenschaften von Zahlenpaaren, von denen jeweils eine Zahl nur dem Sender bzw. Empfänger einer Nachricht bekannt sind. Dabei liefern die Division mit Rest und die modulare Arithmetik die Rechtfertigung für die Korrektheit der Verfahren, die bei heutigen Rechnerarchitekturen und ausreichend großen Zahlen hinreichende Sicherheit bieten, z.B. dadurch, dass eine Entschlüsselung mit massiv parallelen Systemen mindestens 10 Minuten benötigt (work factor of brute-force key search attack).

Dieser Abschnitt fokussiert sich auf die **Grundlagen der Modularen Arithmetik** und den **Euklidischen Algorithmus** und liefert einen Ausblick zur Kryptographie, für weiterführende Aspekte sei auf die Literatur verwiesen, z.B. in (Beutelspacher, Zschiegner, 2011).

Division mit Rest

Satz (2.1)

Für je zwei $a, b \in \mathbb{Z}$ mit $a \neq 0$ gibt es eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit

$$b = qa + r \text{ und } 0 \leq r < |a|$$

Definition

Bei der Division mit Rest wird der Rest $r =: b$ **mod** a mit "b **modulo** a" bezeichnet.

Korollar (2.3)

- *b mod a ist die kleinste nichtnegative Zahl r, so dass $b - r$ durch a teilbar ist.*
- *Zusammenhang mit der Kongruenz modulo a: Für alle $b, b' \in \mathbb{Z}$ gilt*

$$b \bmod a = b' \bmod a \iff a \mid (b - b') \iff b = b' (\text{mod } a)$$

Division mit Rest

Beispiele (2.4)

Bitte bestätigen oder widerlegen:

1. $17 \mod 5 = 2$
2. $17 = 2 \pmod 5$
3. $17 = -3 \pmod 5$
4. $(38 + 22) \mod 9 = 7$
5. $365 \mod 7 = 1$
6. $4711 \mod 1024 = 615$

Division mit Rest: Beweis des Satzes

Ein ausführlicher Beweis für Existenz und Eindeutigkeit der Division mit Rest in Satz (2.1) wird in (Beutelspacher, Zschiegner, 2011) vorgestellt. An dieser Stelle sei nur das folgende hilfreiche Zwischenergebnis genannt:

Lemma (2.5)

Für alle $a, b, b' \in \mathbb{Z}$ *gilt:* $a \mid b \ \wedge \ a \mid b' \Longrightarrow a \mid (b + b') \ \wedge \ a \mid (b - b')$

Beweis.

Sei nach Voraussetzung $a \mid b$ und $a \mid b'$. Dann gibt es ganze Zahlen $q, q' \in \mathbb{Z}$ mit $b = qa$ und $b' = q'a$. Addition bzw. Subtraktion ergeben:

$$b + b' = qa + q'a = (q + q')a \ \text{ und } \ b - b' = qa - q'a = (q - q')a$$

Daraus folgt die Behauptung. □

Division mit Rest

Beispiel (2.6)

Behauptung: $a \mid 235 \ \wedge \ a \mid 252 \Longrightarrow a = 1 \ \vee \ a = 17$
Nach dem Lemmma gilt:

$$a \mid (252 - 235) = 17$$

Da 17 eine Primzahl ist folgt $a = 1$ oder $a = 17$,

Größter gemeinsamer Teiler

Definition (2.7)

Seien $a, b \in \mathbb{Z}$ nicht beide gleich Null. Der **größte gemeinsame Teiler** von a und b (greatest common divisor) wird mit $\mathbf{ggT}(a, b)$ bzw. $\mathbf{gcd}(a, b)$ bezeichnet und ist die größte natürliche Zahl d mit der Eigenschaft $d \mid a$ und $d \mid b$.

Beispiele (2.8)

Bitte bestätigen oder widerlegen:

1. $\mathrm{ggT}(6, 9) = 2$
2. $\mathrm{ggT}(38, 10) = 2$
3. $\mathrm{ggT}(36, 54) = 9$

Hinweis

Im Folgenden werden Lösungsstrategien zur Reduktion und zur algorithmischen Berechnung des ggT sehr großer Zahlen vorgestellt.

Satz (2.9)

Seien $a, b \in \mathbb{Z}, a \neq 0$ *und* $q, r \in \mathbb{Z}$ *mit* $b = qa + r$. *Dann gilt:* $ggT(a, b) = ggT(a, r)$

Beispiel (2.10)

Die Reduktion $\mathrm{ggT}(1587, 17459) = \mathrm{ggT}(1587, 2)$ beruht auf $17459 = 11 \cdot 1587 + 2$.

Beweis.

Behauptung: $D_{ab} := \{d \in \mathbb{N} : d \mid a \wedge d \mid b\} = \{d \in \mathbb{N} : d \mid a \wedge d \mid r\} =: D_{ar}$
"$D_{ab} \subseteq D_{ar}$": Für $d \in D_{ab}$ gilt auch $d \mid qa$ und deshalb $d \mid (b - qa) = r$, d.h., $d \in D_{ar}$.
"$D_{ar} \subseteq D_{ab}$": Für $d \in D_{ar}$ gilt auch $d \mid qa$ und deshalb $d \mid (qa + r) = b$, d.h., $d \in D_{ab}$.
Schließlich folgt $\mathrm{ggT}(a, b) = \max(D_{ab}) = \max(D_{ar}) = \mathrm{ggT}(a, r)$ □

Euklidischer Algorithmus

Satz (2.11)

Für $a, b \in \mathbb{Z}$ mit $a > 0$ ermöglicht der **Euklidische Algorithmus** *die digitale Berechnung von $ggT(a, b)$ durch eine rekursive Division mit Rest:*

1. $r_0 := b, r_1 := a$
2. *Berechne für $k \geq 2$ den Rest $r_k := r_{k-2}$ mod r_{k-1} mit Hilfe der Division $r_{k-2} = q_k r_{k-1} + r_k$ und $0 \leq r_k < r_{k-1}$.*
3. *Ende der Rekursion, wenn der Rest das erste Mal gleich Null ist, d.h. $r_{n+1} = 0$ und $r_n \neq 0$ für ein $n \in \mathbb{N}$. Andernfalls weiter mit Schritt 2 und Index $k + 1$.*

Dann gilt für den letzten von Null verschiedenen Rest: $ggT(a, b) = r_n$

Beweis.

Der Rest nimmt wegen $0 \leq r_k < r_{k-1}$ bei jedem Schritt ab, d.h., nach $n \leq a$ Schritten ist die Rekursion beendet. Nach dem Satz vorher gilt $\text{ggT}(r_{k-1}, r_{k-2}) = \text{ggT}(r_{k-1}, r_k)$. Folglich ist beim Abbruch der Rekursion $\text{ggT}(a, b) = \ldots = \text{ggT}(r_n, 0) = r_n$ □

Euklidischer Algorithmus

Beispiel (2.12)

Berechnung von $\mathrm{ggT}(38, 75)$:

1. $r_0 := 75, r_1 := 38$
2. $r_2 := r_0 \bmod r_1 = 75 \bmod 38 = 37$ wegen $75 = 1 \cdot 38 + 37$
3. $r_3 := r_1 \bmod r_2 = 38 \bmod 37 = 1$ wegen $38 = 1 \cdot 37 + 1$
4. $r_4 := r_2 \bmod r_3 = 37 \bmod 1 = 0$ wegen $37 = 37 \cdot 1 + 0$
5. Ende der Rekursion, da $r_4 = 0$. Ergebnis: $\mathrm{ggT}(38, 75) = r_3 = 1$

Übungen

1. $\mathrm{ggT}(63, 217)$
2. $\mathrm{ggT}(462, 1071)$
3. $\mathrm{ggT}(1024, 2076)$

Euklidischer Algorithmus

Hinweis

- In Wikipedia wird eine sehr hilfreiche graphische Interpretation des Euklidischen Algorithmus vorgestellt:
  https://en.wikipedia.org/wiki/Euclidean_algorithm
  Bei dieser Graphik wird z.B. ein Rechteck mit den Kantenlängen 462 und 1071 nacheinander in Quadrate mit den Kantenlängen 462 (2x), 147 (3x) und 21 (7x) aufgeteilt, die jeweils den Resten im Euklidischen Algorithmus entsprechen. Die kleinsten Quadrate in dieser Folge (Kantenlänge 21) entsprechen $\mathrm{ggT}(462, 1071)$.
- Wähle $r_0 > r_1$, ansonsten vertauscht der erste Schritt die Reihenfolge.

Größter gemeinsamer Teiler: Lemma von Bézout

Satz (2.13)

Seien $a, b \in \mathbb{Z}$ und $d = ggT(a, b)$. Dann existieren $a', b' \in \mathbb{Z}$ mit $d = aa' + bb'$.

Beispiel (2.14)

Es ist $\text{ggT}(8, 5) = 1$. Setze $a' := 2$ und $b' := -3$. Dann ist $1 = 8 \cdot 2 + 5 \cdot (-3)$.

Korollar (2.15)

1. *Wenn a und b positiv sind, muss einer der Zahlen a', b' aus dem Lemma von Bézout negativ sein.*
2. *Wenn $a, n \in \mathbb{N}$ teilerfremd sind, dann gibt es $a', n' \in \mathbb{Z}$ mit $1 = aa' + nn'$ bzw. $a \cdot a' \equiv_n 1$.*

Hinweise

- Ein Beweis von (2.13) ist in (Beutelspacher, Zschiegner, 2011, S. 70).
- Nach Folgerung 2. ist a invertierbar bzgl. der Multiplikation in $\mathbb{Z}_n$ (Details s.u.).

Modulare Arithmetik

Wiederholung

- Für $n \in \mathbb{N}$ ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$, bei der für alle $a, b \in \mathbb{Z}$ und für deren Kongruenzklassen $[a]$ bzw. $[b]$ gilt:

$$[a] = [b] \iff a \equiv_n b :\iff a = b (\text{mod } n) :\iff n \mid (a - b)$$

- $a \equiv_n b \iff \exists x, y \in \mathbb{Z}\ \exists r \in \mathbb{N}_0 : (0 \leq r < n) \wedge (a = xn + r) \wedge (b = yn + r)$
- Für $a \in \mathbb{Z}$ besteht die Kongruenzklasse $[a]$ aus den Elementen $a + kn$ mit $k \in \mathbb{Z}$.
- Die Addition von Kongruenzklassen $[x] + [y] := [x + y]$ ist unabhängig von der Wahl der Repräsentanten.

Definition (2.16)

Für $n \in \mathbb{N}$ ist die **Addition** in $\mathbb{Z}_n$ definiert durch $[x] + [y] := [x + y]$ für alle $x, y \in \mathbb{Z}$. Zu jedem $[x] \in \mathbb{Z}_n$ ist die Restklasse $[-x]$ das **additive Inverse**, d.h. $[x] + [-x] = [0]$.

Modulare Arithmetik: Addition von Kongruenzklassen

Additionstafel von $\mathbb{Z}_6$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Die additiven Inversen in $\mathbb{Z}_6$ ergeben sich jeweils aus folgenden Gleichungen:

$$[0] = [0] + [0] = [1] + [5] = [2] + [4] = [3] + [3] = [4] + [2] = [5] + [1]$$

Modulare Arithmetik: Multiplikation von Kongruenzklassen

Analog zur Addition kann man Kongruenzklassen in $\mathbb{Z}_n$ auch multiplizieren:

Definition (2.17)

Für $n \in \mathbb{N}$ ist die **Multiplikation von Kongruenzklassen** definiert durch die Multiplikation der Repräsentanten der Kongruenzklassen, d.h. für alle $x, y \in \mathbb{Z}$ ist

$$[x] \cdot [y] := [x \cdot y]$$

Lemma (2.18)

Die Multiplikation von Kongruenzklassen ist unabhängig von der Wahl der Repräsentanten.

Beweis.

Für $x' \in [x]$ und $y' \in [y]$ ist zu zeigen: $[x \cdot y] = [x' \cdot y']$ bzw. $xy \equiv_n x'y'$.
$x \equiv_n x' \iff n \mid (x - x') \implies n \mid (x - x')y \iff xy \equiv_n x'y$
$y \equiv_n y' \iff n \mid (y - y') \implies n \mid x'(y - y') \iff x'y \equiv_n x'y'$
Daraus folgt $xy \equiv_n x'y \equiv_n x'y'$.

Beispiel: Multiplikation in $\mathbb{Z}_6$

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Hinweise

- In den Zeilen [2], [3] und [4] kommen einige Zahlen doppelt vor, andere gar nicht.
- In Zeile [5] kommen alle Zahlen genau einmal vor.
- Das Produkt einiger von [0] verschiedener Zahlen ist gleich [0], z.B. $[4] \cdot [3]$.

Modulare Arithmetik: Reduktion grosser Zahlen

Hinweise

Mit Hilfe der Multiplikation in $\mathbb{Z}_n$ können exakte Algorithmen zur Lösung von Gleichungen mit sehr grossen Zahlen erstellt werden, ohne dass Rundungsfehler bei der Division mit grossen Zahlen auftreten. Das ist z.B. die Grundlage für moderne kryptographische Verfahren, deren Korrektheit auf zahlentheoretischen Eigenschaften beruht, z.B. dass zwei Zahlen zueinander teilerfremd sind. Im Folgenden wird die Reduktion großer Zahlen mit Hilfe der Kongruenzen analysiert, später dann weitere Eigenschaften für die Lösung von Gleichungen.

Beispiele (2.19)

Beweise oder widerlege:

- $12^9 = 1 (\text{mod } 11)$
- $10^k = 1 (\text{mod } 9)\ \forall k \in \mathbb{N}$
- $13 \cdot 15 = 1 \cdot 3 (\text{mod } 12)$
- $135^4 \text{ mod } 12 = 9 \text{ mod } 12$

Modulare Arithmetik: Reduktion grosser Zahlen

Beispiele (2.20)

1. Berechnen Sie: $(29 \cdot 9 + 4 \cdot 8) \mod 5$
2. Berechnen Sie: $13^4 \mod 7$
3. Berechnen Sie in $\mathbb{Z}_7$: $[3]^{15} \cdot [2]$

Musterlösung (2.20)

1.

$$\begin{aligned}(29 \cdot 9 + 4 \cdot 8) \mod 5 &= (4 \cdot 4 + 4 \cdot 3) \mod 5 \\ &= (16 + 12) \mod 5 \\ &= (1 + 2) \mod 5 \\ &= 3 \mod 5\end{aligned}$$

2. $13^4 \mod 7 = 6^4 \mod 7 = (6^2 \cdot 6^2) \mod 7 = (1 \cdot 1) \mod 7 = 1 \mod 7$
3. In $\mathbb{Z}_7$ gilt:

$$3^{15} \cdot 2 = (3^3)^5 \cdot 2 = 27^5 \cdot 2 = 6^5 \cdot 2 = (6^2 \cdot 6^2 \cdot 6) \cdot 2 = (1 \cdot 1 \cdot 6) \cdot 2 = 5$$

Multiplikation von Kongruenzklassen

Satz (2.21)

Für $n \in \mathbb{N}$ und $[a] \in \mathbb{Z}_n$ sind äquivalent:

1. *Die Zahlen a und sind n teilerfremd .*
2. *Es existiert ein* **multiplikatives Inverses** *von $[a]$, d.h. eine Restklasse $[a'] \in \mathbb{Z}_n$ mit $[a] \cdot [a'] = [1]$.*

Beweis.

1. $\Longrightarrow$ 2.: Die Behauptung folgt unmittelbar aus dem Korollar zum Lemma von Bézout.
2. $\Longrightarrow$ 1.: Sei nach 2. eine Restklasse $[a'] \in \mathbb{Z}_n$ mit $[a] \cdot [a'] = [1]$ gegeben.
Zu zeigen: $\mathrm{ggT}(a, n) = 1$ bzw. jeder gemeinsame Teiler d von a und n teilt 1.
Sei d ein gemeinsamer Teiler von a und n. Dann existieren $q_1, q_2 \in \mathbb{Z}$ mit

$$a = q_1 d \text{ und } n = q_2 d.$$

Nach 2. und Definition der Multiplikation in $\mathbb{Z}_n$ existiert ein $k \in \mathbb{Z}$ mit $aa' - 1 = kn$.
Daraus folgt $1 = aa' - kn = q_1 da' - kq_2 d = d(q_1 a' - kq_2)$, also auch $d \mid 1$.

Modulare Arithmetik: Lösung von Gleichungen

Beispiel (2.22)

Welches $x \in \mathbb{Z}_7$ erfüllt diese Gleichung?

$$4 \cdot x = 5$$

Hinweis: Bestimmen Sie zunächst das multiplikative Inverse y von 4 und mulitplizieren Sie dann die Gleichung mit y.

Lösung (2.22)

Lösung der Gleichung in $\mathbb{Z}_7$:

$$4 \cdot x = 5$$

In $\mathbb{Z}_7$ gilt $2 \cdot 4 = 8 = 1$, d.h. $y = 2$ ist das multiplikative Inverse von 4.
Multiplikation der Gleichung mit y liefert:

$$\underbrace{2 \cdot 4}_{1} \cdot x = 2 \cdot 5 = 10 = 3$$

Lösung: $x = 3$

Modulare Arithmetik: Lösung von Gleichungen

Aufgabe (2.23)

Lösen Sie die Gleichung in $\mathbb{Z}_5$:

$$4 \cdot x + 3 = 4$$

Hinweis: Analog zu den Grundrechenarten in $\mathbb{R}$ können Sie in $\mathbb{Z}_5$ durch Addition von additiven Inversen (entsprechend der Subtraktion) und anschließende Multiplikation mit multiplikativen Inversen (entsprechend der Division) die Variable x auf der linken Seite der Gleichung isolieren und damit berechnen.

Lösung (2.23)

Lösung der Gleichung in $\mathbb{Z}_5$:

$$4 \cdot x + 3 = 4$$

In $\mathbb{Z}_5$ ist 2 das eindeutige additive Inverse von 3 (wegen $3 + 2 = 5 \equiv 0 \mod 5$).
Addition von 2 auf beiden Seiten der Gleichung ergibt also:

$$4 \cdot x + \underbrace{3 + 2}_{0} = 4 + 2 = 1$$

In $\mathbb{Z}_5$ ist 4 das eindeutige multiplikative Inverse von 4 (wegen $4 \cdot 4 = 16 \equiv 1 \mod 5$).
Multiplikation mit 4 auf beiden Seiten der Gleichung ergibt:

$$\underbrace{4 \cdot 4}_{1} \cdot x = 4 \cdot 1 = 4$$

Lösung: $x = 4$

Beispiel (2.24)

Eine Dezimalzahl der Form

$$a = (a_n a_{n-1} \dots a_1 a_0)_{10} = \sum_{k=0}^{n} a_k 10^k$$

ist genau dann durch 9 teilbar, wenn ihre Quersumme $(\sum_{k=0}^{n} a_k)$ durch 9 teilbar ist.
Beweis: Nach Beispiel (2.19) gilt

$$10^k = 1 (\text{mod } 9)\ \forall k \in \mathbb{N}$$

Diese Formel angewendet auf die Dezimaldarstellung von a ergibt die Behauptung:

$$a \text{ mod } 9 = (\sum_{k=0}^{n} a_k 10^k) \text{mod } 9 = (\sum_{k=0}^{n} a_k 10^k \text{mod } 9) = (\sum_{k=0}^{n} a_k) \text{mod } 9$$

Multiplikation von Kongruenzklassen: Sätze von Fermat und Euler

Die folgenden Resultate spielen in der Kryptographie eine zentrale Rolle:

Satz (2.25, Kleiner Satz von Fermat)

Für eine Primzahl $p \in \mathbb{N}$ und $m \in \mathbb{Z}$ gelten:

$$m^{p-1} = 1 (mod\ p) \text{ und } m^p = m (mod\ p)$$

Definition (2.26)

Eulersche ϕ-Funktion: $\phi : \mathbb{N} \to \mathbb{N}, n \mapsto \phi(n) := |\{1 \leq t < n \mid \mathrm{ggT}(t, n) = 1\}|$.

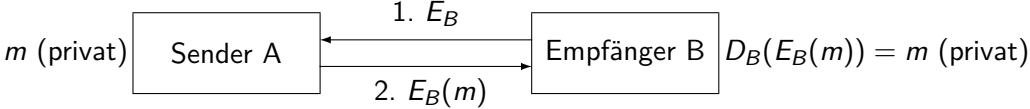
In anderen Worten: $\phi(n)$ ist die Anzahl der zu n teilerfremden Zahlen.

Satz (2.27, Euler)

Sind $m, n \in \mathbb{N}$ zueinander teilerfremd, dann gilt: $m^{\phi(n)} = 1 (mod\ n)$

Kryptographie: Public Key Verschlüsselungsschema

Jeder Teilnehmer T hat einen **öffentlichen Schlüssel** E_T (encryption key) und einen **privaten (geheimen) Schlüssel** D_T (decryption). Sowohl die unverschlüsselten (Original-)Nachrichten als auch die verschlüsselten seien als Zahlen codiert, d.h., Zahlen $m \in \mathbb{Z}$ und Abbildungen $E_T, D_T : \mathbb{Z} \to \mathbb{Z}$ sind gegeben. **Austausch-Schema für öffentliche Schlüssel und verschlüsselte Nachrichten (inkl. Decodierung beim Empfänger):**



- **Entschlüsselungseigenschaft:** Jede Nachricht m kann decodiert werden durch die Konkatenation von D_T und E_T, d.h. $D_T(E_T(m)) = m$.
- **Public-key-Eigenschaft:** Privater Schlüssel D_T kann in einem gegebenen Zeitintervall (z.B. 10 Minuten) nicht aus öffentlichem Schlüssel E_T berechnet werden.

Modulare Arithmetik und Kryptographie: RSA Algorithmus (1/3)

Schlüsselerzeugung: Jeder Teilnehmer T wählt zwei verschiedene, große Primzahlen p_T, q_T und bildet das Produkt $n_T := p_T \cdot q_T$. Wegen des Chinesischen Restsatzes ist die Eulersche ϕ-Funktion davon

$$\phi(n_T) = (p_T - 1) \cdot (q_T - 1)$$

Anschließend wählt T eine natürliche Zahl e_T, die teilerfremd zu $\phi(n_T)$ ist:

$$\mathrm{ggT}(e_T, \phi(n_T)) = 1$$

Im letzten Schritt wird eine Zahl $d_T \in \mathbb{N}$ ermittelt, die das multiplikative Inverse von e_T modulo $\phi(n_T)$ ist (die Existenz ist aufgrund des vorherigen Satzes garantiert, der erweiterte euklidische Algorithmus liefert ein Konstruktionsverfahren), d.h. es gilt:

$$e_T \cdot d_T = 1 (\mathrm{mod}\ \phi(n_T))$$

Folglich existiert $k_T \in \mathbb{Z}$ mit $e_T \cdot d_T = k_T \cdot \phi(n_T) + 1$.

Potenzieren mit e_T modulo n_T definiert die **öffentliche Verschlüsselungs-Funktion** :

$$E_T : \mathbb{N} \to \mathbb{N}, m \mapsto E_T(m) := m^{e_T} \text{mod } n_T$$

Potenzieren mit d_T definiert die **private Entschlüsselungsfunktion**:

$$D_T : \mathbb{N} \to \mathbb{N}, c \mapsto D_T(c) := c^{d_T}$$

Der Satz von Euler liefert $m^{\phi(n_T)} = 1(\text{mod } n_T)$ und damit folgt die **Korrektheit der Entschlüsselung:**

$$D_T(E_T(m)) = (m^{e_T})^{d_T} = m^{e_T \cdot d_T} = m^{k_T \cdot \phi(n_T)+1} = 1^{k_T} \cdot m = m(\text{mod } n_T) \quad (3)$$

Der RSA Algorithmus ist sicher, da bei einem brute-force key search attack die Zahl n_T in ihre Primfaktoren zerlegt werden müsste, um den privaten Schlüssel d_T aus dem öffentlichen Schlüssel e_T zu berechnen. Diese Faktorisierung dauert heute sehr lange bzw. ist bisher unmöglich, der Weltrekord im Faktorisieren liegt bei 232 Dezimalstellen (768 Bits). Empfohlen werden deshalb Zahlen n_T mit 1024 oder 2048 Bits.

Der RSA-Algorithmus kann auch für die **digitale Signatur** und für die **Authentifizierung** verwendet werden, da die Gleichung (3) symmetrisch ist, d.h. die Reihenfolge der Anwendung der Funktionen D_T und E_T kann umgedreht werden:

$$(m^{e_T})^{d_T} = m^{e_T \cdot d_T} = m^{d_T \cdot e_T} = (m^{d_T})^{e_T}$$

Mehr Details dazu siehe (Beutelspacher und Zschiegner) und (Teschl und Teschl).

Abschnitt 2

Graphen und Bäume — Modellierung von Netzwerken, Datenstrukturen und effizienten Algorithmen

Graphen und Bäume — Modellierung von Netzwerken, Datenstrukturen und effizienten Algorithmen

Motivation

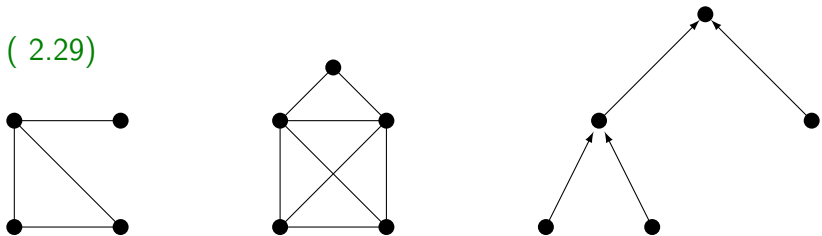
Mit **Graphen** können zahlreiche Anwendungen in Technik und Naturwissenschaften modelliert und digital kontrolliert werden, z.B. im Risiko-Management von Netzwerken für Kommunikations-, Strom- oder Verkehrsverbindungen. Auch die Struktur und die Veränderungsprozesse chemischer Moleküle können mit Hilfe von Graphen analysiert werden. **Bäume** sind spezielle Graphen, die in der Informatik beim Strukturieren großer Datenmengen eine zentrale Rolle spielen. Einige theoretische Erkenntnisse zu Bäumen sind z.B. relevant für die Beurteilung der Effizienz von Such-Algorithmen.

Graphen

Definition (2.28)

- Ein **Graph** $G(V, E)$ bzw. G besteht aus einer endlichen Menge V von **Knoten** (vertex) und einer Menge E von **Kanten** (edge) $\{v, w\}$, die jeweils die Endknoten $v, w \in V$ $(v \neq w)$ miteinander verbinden.
- $H(V', E')$ mit $V' \subseteq V$ und $E' \subseteq E$ heißt **Teilgraph** (subgraph) von G.
- Ein **gerichteter Graph** oder **Digraph** (directed graph) ist ein Graph, in dem jede Kante eine Richtung besitzt, also ein geordnetes Paar (v, w) ist.

Beispiele (2.29)



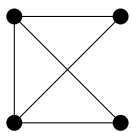
Nachbarn in Graphen

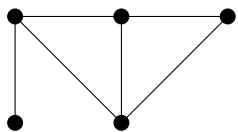
Definition (2.30)

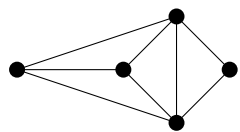
Sei $G(V, E)$ ein Graph.

- Knoten $v, w \in V$ sind **benachbart** oder **adjazent** (adjacent), wenn sie durch eine Kante verbunden sind, d.h. $\{v, w\} \in E$.
- Zwei Kanten mit einem gemeinsamen Endknoten sind **inzident** (incident).
- Ein Endknoten einer Kante $\{v, w\}$ heißt ebenfalls **inzident** zur Kante.
- Für einen Knoten $v \in V$ ist der **Grad** (degree) von v die Anzahl der Kanten, die inzident mit v sind. Notation: $\mathbf{deg}(v)$

Beispiele (2.31)







Graphen: Knotengrade und Kantenanzahl

Satz (2.32)

Sei $G(V, E)$ ein Graph.

1. $\sum_{v \in V} deg(v) = 2\,|E|$
2. *Die Anzahl der Knoten mit ungeradem Grad ist gerade.*

Beweis.

1. Jede Kante hat zwei Endknoten und addiert somit 2 zur Gesamtsumme.
2. Sei d_1 die Summe der ungeraden Grade und d_2 die Summe der geraden Grade:

$$d_1 := \sum_{\deg(v) \text{ ungerade}} \deg(v),\ d_2 := \sum_{\deg(v) \text{ gerade}} \deg(v)$$

Wegen 1. ist $d_1 + d_2 = \sum_{v \in V} \deg(v) = 2\,|E|$ gerade. Als Summe von geraden Zahlen ist d_2 gerade. Folglich ist auch $d_1 = 2\,|E| - d_2$ gerade. Deshalb muss es eine gerade Anzahl von Summanden für d_1 geben.

Digitale Analyse von Graphen: Adjazenzmatrix

Definition (2.33)

Sei $G(V, E)$ ein Graph mit n Knoten, d.h. $V = \{v_1, \ldots, v_n\}$. Die **Adjazenzmatrix** (adjacency matrix) $A = (a_{ij})$ von G ist definiert durch

$$a_{ij} = \begin{cases} 1, & \text{falls } \{v_i, v_j\} \in E \\ 0, & \text{sonst} \end{cases} \quad (\text{für } 1 \leq i, j \leq n)$$

Hinweis

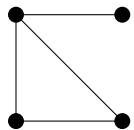
Adjazenzmatrizen ermöglichen eine digitale Darstellung von Graphen, mit deren Hilfe Eigenschaften analysiert und Veränderungen (teil-)automatisiert durchgeführt werden können.

Eine alternative Darstellung sind **Adjazenz-Listen** mit den Listen der Nachbarn pro Knoten. Diese Listen benötigen weniger Speicherplatz als die Matrizen, während die Matrizen über die Matrixmultiplikation spezielle Vorteile bieten (s.u.).

Adjazenzmatrix

Beispiele (2.34)

1. Bestimme die Adjazenzmatrix dieses Graphen:



2. Bestimme den Graphen zur Adjazenzmatrix $A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Kantenzüge

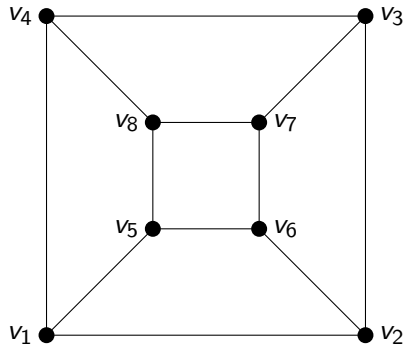
Definition (2.35)

Sei $G(V, E)$ ein Graph mit Knoten $V = \{v_1, \ldots, v_n\}$ und $s \in \mathbb{N}$.

- Ein **Kantenzug** (path) ist eine Folge $(e_i)_{i=1}^{s}$ von inzidenten Kanten $e_i = \{v_{i-1}, v_i\} \in E$ für $1 \leq i \leq s$.
- Die **Länge** eines Kantenzuges ist die Anzahl der durchlaufenen Kanten: $s = l(e_i)$. Ein Spezialfall ist ein Kantenzug der Länge 0, der aus einem einzelnen Knoten $v \in V$ besteht.
- Ein Kantenzug ist **geschlossen**, wenn Anfangs- und Endknoten gleich sind: $(v_0 = v_s)$
- Ein **Weg** (simple path) ist ein Kantenzug, bei dem alle Knoten (bis eventuell auf Anfangs- und Endknoten) verschieden sind: $((i, j < s) \wedge (i \neq j) \Longrightarrow v_i \neq v_j)$
- Ein **Kreis** (cycle) ist ein geschlossener Weg.

Kantenzüge: Beispiele

Beispiele (2.36)



Welche Folgen von Knoten definieren ein (geschlossenen) Kantenzug, Weg oder Kreis?
$s_1 := (v_2, v_7, v_6, v_2), s_2 := (v_1, v_2, v_3, v_2, v_6), s_3 := (v_1, v_2, v_3, v_2, v_6, v_5, v_1),$
$s_4 := (v_1, v_2, v_3, v_7, v_6), s_5 := (v_1, v_2, v_3, v_7, v_6, v_5, v_1)$

Satz (2.37)

Sei $G(V, E)$ ein Graph mit n Knoten und Adjazenzmatrix $A = (a_{ij})$.

1. *Für $s \in \mathbb{N}$ und $i, k \leq n$ gibt in der potenzierten Matrix A^s der Koeffizient $a_{ik}^{(s)}$ die Anzahl der Kantenzüge der Länge s von Knoten v_i zu Knoten v_k an.*
2. *$a_{kk}^{(2)} = deg(v_k)$ für alle $1 \leq k \leq n$.*

Beweis.

Teil 1 beruht auf der Formel für die Berechnung von A^2 (d.h., $a_{ik}^{(2)} = \sum_{j=1}^{n} a_{ij} \cdot a_{jk}$) und Induktion. Dabei gilt für einen Summanden $a_{ij} \cdot a_{jk} = 1$ genau dann, wenn ein Kantenzug von v_i über v_j nach v_k exisitiert.
Teil 2 folgt daraus, dass bei den Diagonalelementen von A^2 die ein- und ausgehenden Kanten von v_k addiert werden: $a_{kk}^{(2)} = \sum_{j=1}^{n} a_{kj} \cdot a_{jk}$ □

Zusammenhang

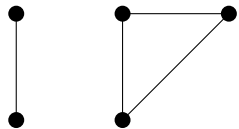
Definition (2.38)

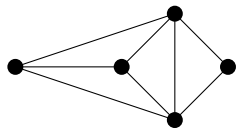
Sei $G(V, E)$ ein Graph und $s \in \mathbb{N}$.

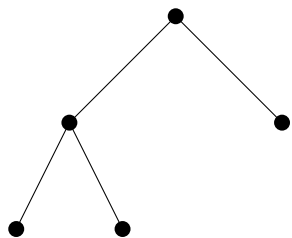
1. Zwei Knoten $v, w \in V$ sind **zusammenhängend** (connected) ($v \sim w$), wenn es einen Weg $(e_i)_{i=1}^{s}$ von v nach w gibt , d.h.$e_i = \{v_{i-1}, v_i\} \in E$ für alle $i \leq s$ und $v = v_0, v_s = w$.
2. Eine Äquivalenzklassen der Relation $\sim$ heißt **Zusammenhangskomponente** (connected component).
3. G ist **zusammenhängend** (connected), wenn je zwei Knoten $v, w \in V$ zusammenhängend sind (d.h., es gibt genau eine Zusammenhangskomponente).
4. G wird als **einfach zusammenhängend** (1-connected) bezeichnet, wenn es eine Kante $e \in E$ gibt, so dass der Graph $G(V, E \setminus \{e\})$ nicht zusammenhängend ist.
5. G wird als **mehrfach zusammenhängend** (k-connected, $k > 1$) bezeichnet, wenn bei Wegfall einer beliebigen Kante $e \in E$ auch der Graph $G(V, E \setminus \{e\})$ zusammenhängend ist.

Zusammenhang: Beispiele

Beispiele (2.39)

$G_1 =$ 

$G_2 =$ 

$G_3 =$ 

Hinweis

- Bei den Äquivalenzrelation-Eigenschaften von $\sim$ sind Reflexivität und Symmetrie offensichtlich gegeben.
- Beim Beweis der Transitivität kann es sein, dass die Konkatenation zweier Wege von Knoten u nach v bzw. von v nach w einige Knoten doppelt enthält. In diesem Fall kann die Konkatenation durch Abschneiden von Kreisen so verkürzt werden, dass ein Weg von u nach w entsteht.

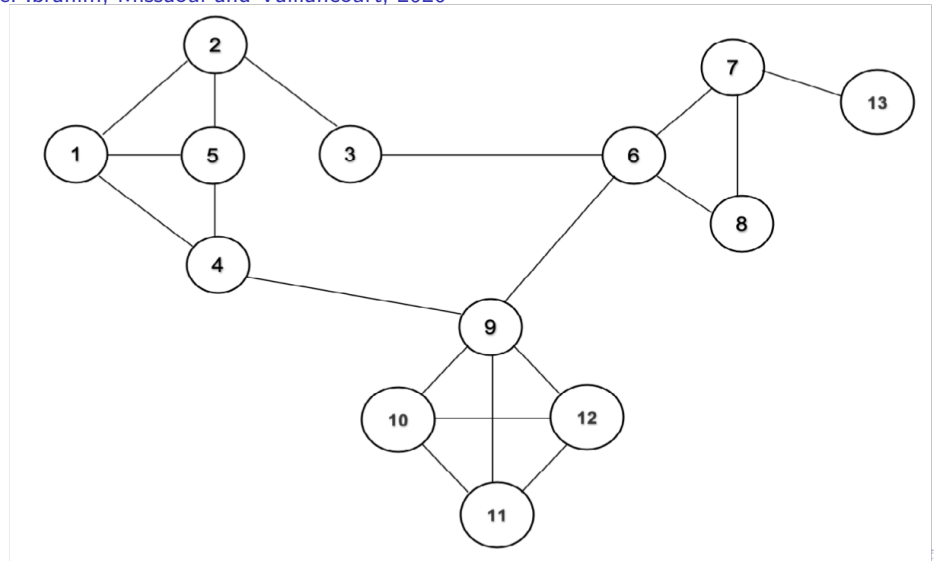
Ausblick: Graphen in Wirtschaft, Technik und aktuellen Forschungen

Beispiele (2.40)

- Der mehrfache Zusammenhang von Graphen ist Im **Risiko-Management von Netzwerken** (Internet, Strom, Gas, etc.) sehr wichtig. Andernfalls kann z.B. ein kleiner Stromausfall zu hohen Ausfallraten bei Millionen Menschen führen, wenn Ersatzleitungen fehlen.
- In sehr aktuellen Forschungen werden **Communities in Sozialen Medien** oder der **Datenverkehr in Internet-Knoten** mit algebraischen Modellen von Netzwerken analysiert, dabei werden Methoden der **Graphentheorie** und der **Formalen Begriffsanalyse** (Formal Concept Analysis) eingesetzt, u.a. auch zur **Performance-Optimierung der digitalen Analyse von Graphen mit sehr vielen Knoten**.
- Analog dazu werden diese Konzepte in den Biowissenschaften verwendet für die **Protein-Protein Interaktion, die virale Verbreitung von COVID-19 oder das Data Mining zur Krebs-Früherkennung**.

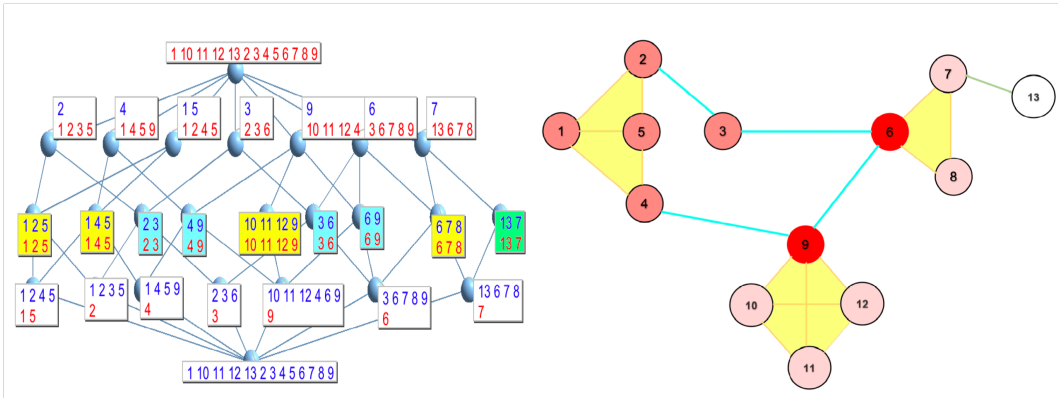
Beispiel: Analyse der Verbreitung von COVID-19

Quelle: Ibrahim, Missaoui and Vaillancourt, 2020



Beispiel: Analyse der Verbreitung von COVID-19

Quelle: Ibrahim, Missaoui and Vaillancourt, 2020



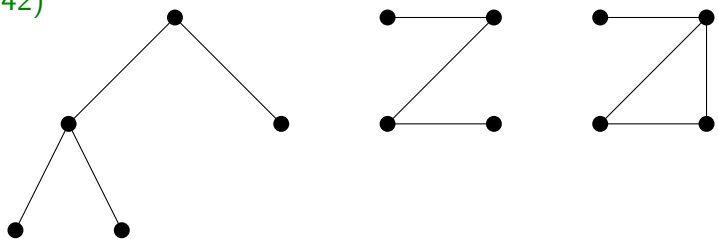
Bäume

Datenstrukturen und effiziente Algorithmen verwenden oft das Konzept von Bäumen, da diese sich einerseits relativ leicht implementieren lassen und da sie andererseits theoretisch fundierte Aussagen zu Korrektheit und durchschnittlicher Dauer der Ausführung von Algorithmen erlauben.

Definition (2.41)

Ein **Baum** (tree) ist ein zusammenhängender Graph ohne Kreise. Ein Graph, dessen Zusammenhangskomponenten Bäume sind, heißt **Wald** (forest).

Beispiele (2.42)



Satz (2.43)

Für einen zusammenhängenden Graphen $T(V, E)$ mit n Knoten sind äquivalent:

1. *T ist ein Baum.*
2. *T hat genau $n-1$ Kanten.*
3. *T ist einfach zusammenhängend.*
4. *Zwischen je zwei Knoten gibt es genau einen Weg.*

Beweis.

Übung (z.B. als Ringschluss 1. $\Longrightarrow$ 2. $\Longrightarrow$ 3. $\Longrightarrow$ 4. $\Longrightarrow$ 1.) □

Vorgänger und Nachfolger in Wurzel-Bäumen

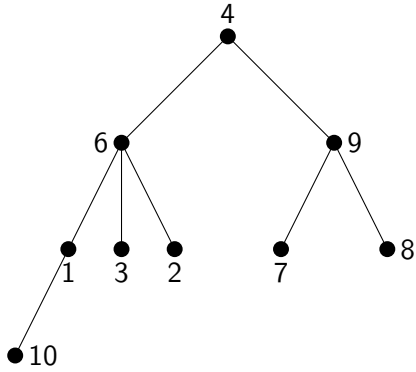
Definition (2.44)

Sei $T(V, E)$ ein Baum mit einem ausgezeichneten Knoten $r \in V$.

1. T bzw. (T, r) wird als **Wurzelbaum** (rooted tree) bezeichnet.
2. Ein Knoten $v \in V$ ist **Vorgänger** (ancestor) eines Knotens $w \in V$ und w ist **Nachfolger** (successor) von v, wenn es einen Weg von r über v nach w gibt: $v \leq w :\Longleftrightarrow (\exists \text{ Weg } (e_i)_{i=1}^{s} \exists j \leq s \text{ mit } r = v_0, v_j = v, v_s = w)$
3. Für $v < w$ (d.h. $v \leq w$ und $v \neq w$) heißt v **echter Vorgänger** (proper ancestor) von w bzw. w **echter Nachfolger** (proper successor)
4. Ein Knoten ohne echte Nachfolger ist ein **Blatt** (leaf).
5. Der **Teilbaum** (subtree) eines Knotens v ist v zusammen mit seinen Nachfolgern.
6. Die **Tiefe** (depth) eines Knotens v ist die Länge eines Weges von der Wurzel zu v.
7. Die **Höhe** (height) eines Knotens v ist die maximale Länge eines Weges von v zu den Blättern des Teilbaums von v.
8. Die **Höhe** (height) des Baums ist Höhe der Wurzel r.

Vorgänger und Nachfolger in Wurzel-Bäumen

Beispiel (2.45)



Binäre Bäume

Definition (2.46)

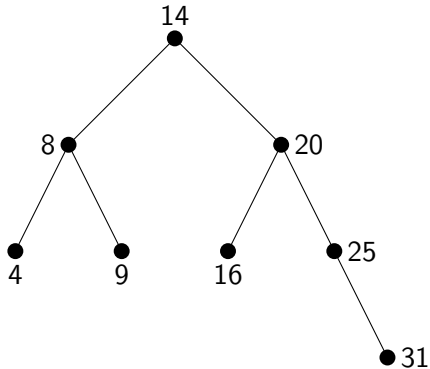
Ein Wurzelbaum wird **binärer Baum** (binary tree) genannt, wenn jeder Knoten v höchstens zwei unmittelbare Nachfolger hat (d.h. einen **linken Nachfolger** v_L und einen **rechten Nachfolger** v_R). Die zugehörigen Teilbäume mit Wurzel v werden als **linker (bzw. rechter) Teilbaum** T_L bzw. T_R bezeichnet.

Beispiele (2.47)

Binäre Bäume werden oft für die Suche verwendet, in diesem Fall werden sie als **binäre Suchbäume** (binary search trees, BST) bezeichnet.

Binäre Suchbäume

Beispiel (2.48)



Suchbaum-Algorithmus

- **Voraussetzung:** Die Knoten im Baum $T(V, E)$ sind linear geordnet (d.h., für alle $v, w \in V$ gilt $v \leq w \vee v \geq w$). Ferner sind für alle $v \in V$ die kleineren Elemente im linken Teilbaum ($v > w \Longrightarrow w \in T_L$) und die größeren im rechten ($v < w \Longrightarrow w \in T_R$) .
- **Suche von Knoten v:** Suchdurchlauf beginnt im Wurzelknoten und ist rekursiv definiert: Falls für den aktuellen Knoten t gilt $t = v$, dann wird der Algorithmus terminiert (STOP, RESULT: 'v found'). Andernfalls setze für $v < t$ die Suche im linken Teilbaum T_L fort und für $v > t$ in T_R. Schließlich STOP, falls der gewählte Teilbaum leer ist (RESULT: 'v not found').

Die Suche mit diesem Algorithmus in einem binären Baum der Höhe h benötigt maximal $h + 1$ Vergleiche. Mit Hilfe der Suche können auch Algorithmen für das Einfügen neuer und das Löschen vorhandener Knoten implementiert werden, die die in der Voraussetzung genannte Struktur des Baums erhalten.

Ausblick: Bäume, Datenstrukturen und Algorithmen

In der Informatik spielt die Optimierung binärer Suchbäume eine zentrale Rolle, um Laufzeiten zu minimieren für das Suchen von Knoten (Datensätzen) und für das Hinzufügen, Ändern und Löschen von Daten (d.h., für die CRUD Operationen Create, Read, Update und Delete). Dabei bestehen Abhängigkeiten von den zu erwartenden Datenmengen und den Häufigkeiten der diversen Zugriffe. Wenn z.B. diese Anfragen nicht gleich verteilt sind, können nach dem Ansatz von Huffmann Daten mit minimaler Zugriffs-Häufigkeit als Blätter mit maximaler Tiefe im Baum und solche mit größerer Häufigkeit nahe der Wurzel mit geringer Tiefe und damit kürzerer Suchlaufzeit platziert werden.

Weiterführende Literatur

In (Knebl) ist ein sehr guter Überblick zur Verwendung von Bäumen für effiziente Algorithmen, ebenso in Wikipedia: https://en.wikipedia.org/wiki/Binary_search_tree

Abschnitt 3

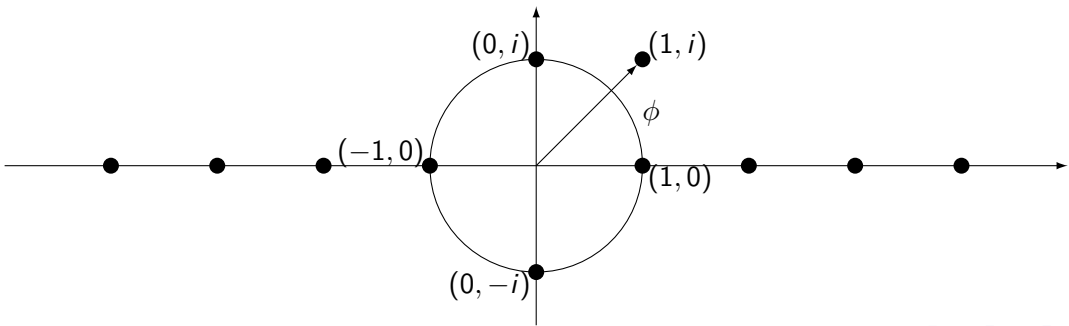
Gruppen, Ringe und Körper — Die Struktur der Zahlen

Motivation

Die aus der Schule bekannten Rechengesetze für reelle Zahlen lassen sich auf viele komplexe Objekte übertragen, z.B. auf Restklassen in der modularen Arithmetik oder auf Matrizen in der linearen Algebra. Für **digitale Anwendungen mit korrekten und effizienten Algorithmen** bietet die **Algebra** mit den weiter unten vorgestellten Konzepten der **(Halb-)Gruppen, Ringe und Körper** eine Grundlage, um Objekte mit diesen Strukturen und Funktionen zwischen diesen Objekten digital zu erfassen und Veränderungen darzustellen bzw. zu prognostizieren. Diese mathematischen Hilfsmittel werden z.B. für realistische Klimamodelle als Basis für aussagekräftigen Prognosen und Modellrechnungen benötigt.

Zahlen und Gleichungen

Gleichungstyp	Menge	Geometrische Darstellung
$3 = 2 + x$	$\mathbb{N}$	Diskrete Punkte auf Zahlengerade nach rechts
$2 = 3 + x$	$\mathbb{Z}$	Diskrete Punkte auf Zahlengerade nach rechts und links
$2 = 3 \cdot x$	$\mathbb{Q}$	Dicht liegende Punkte auf Zahlengerade nach rechts und links
$2 = x^2$	$\mathbb{R}$	Reelle Zahlengerade
$-1 = x^2$	$\mathbb{C}$	Komplexe Zahlenebene



Halbgruppen und Gruppen

Definition (2.49)

Sei G eine nichtleere Menge und $\circ$ eine innere binäre Verknüpfung auf G, d.h., eine Abbildung $\circ : G \times G \to G, (x, y) \mapsto x \circ y = xy$.

1. $(G, \circ)$ **Halbgruppe** (semigroup), wenn $\circ$ das **Assoziativgesetz** erfüllt:

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

2. $(G, \circ)$ **Gruppe** (group)
   - 2.1 G ist Halbgruppe.
   - 2.2 Es gibt ein **neutrales Element**.

$$\exists e \in G \, \forall x \in G : x \circ e = x$$

   - 2.3 Es gibt **inverse Elemente**.

$$\forall x \in G \, \exists x^{-1} \in G : x^{-1} \circ x = e$$

Halbgruppen und Gruppen

Satz (2.50)

In einer Gruppe sind das neutrale Element und das zu jedem Element existierende Inverse eindeutig bestimmt.

Notation

	Allgemein	Additiv	Multiplikativ
Verknüpfung	$\circ$	$+$	$\cdot$
Neutrales Element	e	0	1
Inverses Element	x^{-1}	$-x$	x^{-1}

Definition (2.51)

Eine (Halb-)Gruppe $(G, \circ)$, für die das **Kommutativgesetz**

$$a \circ b = b \circ a \; (\forall a, b \in G)$$

gilt, wird als **kommutative** oder **Abelsche (Halb-)Gruppe** (abelian (semi-)group) bezeichnet.

Halbgruppen und Gruppen: Beispile

Beispiele (2.52)

Welche der folgenden algebraischen Strukturen sind Halbgruppen bzw. Gruppen? Welche sind kommutativ?

1. $(\mathbb{N}, +)$
2. $(\mathbb{Z}, +)$ und $(\mathbb{Z} \setminus \{0\}, \cdot)$
3. $(\mathbb{Q}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$
4. $(\mathbb{R}, +)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$
5. $(\mathbb{C}, +)$ und $(\mathbb{C} \setminus \{0\}, \cdot)$
6. $(\mathbb{Z}_n, +)$ und $(\mathbb{Z}_n \setminus \{[0]\}, \cdot)$ für $n \in \mathbb{N}$
7. $(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$ für p prim
8. $\mathbb{Z}_n^* := \{[m] \in \mathbb{Z}_n \setminus \{[0]\} \mid \mathrm{ggT}(m, n) = 1\}$ (**prime Restklassengruppe modulo** n)

Musterlösung (2.52)

1. - 5.: Die algebraischen Strukturen mit Addition sind alle kommutative Gruppen mit neutralem Element 0 und jeweils zu x inversem Element $-x$.

$$(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$$

$(\mathbb{Z} \setminus \{0\}, \cdot)$ ist zwar kommutative Halbgruppe aber keine Gruppe, da es z.B. zu 2 kein multiplikatives Inverses gibt.

$$(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$$

sind kommutative Gruppen mit neutralem Element 1 und jeweils zu x inversem Element x^{-1}.

Musterlösung (2.52)

6. - 8. Die additiven Strukturen der modulare Arithmetik

$$(\mathbb{Z}_n, +)$$

sind für jedes $n \in \mathbb{N}$ kommutative Gruppen. Die multiplikativen Strukturen

$$(\mathbb{Z}_n \setminus \{[0]\}, \cdot)$$

sind im Allgemeinen kommutative Halbgruppen mit neutralem Element, aber keine Gruppen (Gegenbeispiel: In $\mathbb{Z}_4$ exisitiert kein multiplikatives inverses Element von 2). Demgegenüber ist für eine Primzahl p stets

$$(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$$

eine Gruppe. Allgemeiner ist die prime Restklassengruppe modulo n eine Gruppe:

$$\mathbb{Z}_n^* := \{[m] \in \mathbb{Z}_n \setminus \{[0]\} \mid \mathrm{ggT}(m, n) = 1\}$$

Lineare Abbildungen und Matrizen

Beispiele (2.53)

$\mathrm{Mat}(n, \mathbb{R}) := \{A \mid A = (a_{ij}) n \times n \text{ Matrix}, a_{ij} \in \mathbb{R}\}$ ist kommutative Gruppe bzgl. Matrix-Addition und $\mathrm{Mat}(n, \mathbb{R}) \setminus \{0\}$ ist nicht-kommutative Halbgruppe mit neutralem Element bzgl. Matrix-Multiplikation:

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, D = \begin{pmatrix} 1 & 2 & 0 \\ 6 & 12 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Die Einheitsmatrix (identity matrix) ist das neutrale Element bzgl. der Multiplikation. Für die Matrixelemente $\delta_{i,j}$ von I_n gilt $\delta_{i,j} = 1$ für $i = j$ und $\delta_{i,j} = 0$ für $i \neq j$.

$$I := I_n := (\delta_{i,j}) := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Beispiele (2.54)

$\mathrm{GL}(n,\mathbb{R}) := \{A \in \mathrm{Mat}(n,\mathbb{R}) \mid \det(A) \neq 0\}$ (**General Linear Group**) ist mit der Matrix-Multiplikation eine Gruppe mit neutralem Element.
Welche der folgenden Matrizen gehören zu $\mathrm{GL}(n,\mathbb{R})$?

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, C = \begin{pmatrix} 4 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

Rechenregeln in Gruppen

Satz (2.55)

Ist G eine Gruppe und sind $a, b, x, y \in G$, dann gelten:

1. $(ab)^{-1} = b^{-1}a^{-1}$
2. $(a^{-1})^{-1} = a$
3. *Die Gleichung $ax = b$ hat genau eine Lösung $x = a^{-1}b$.*
4. *Die Gleichung $ya = b$ hat genau eine Lösung $y = ba^{-1}$.*
5. **Kürzungsregeln**:
   - $ax = bx \Longrightarrow a = b$
   - $xa = xb \Longrightarrow a = b$

Hinweis

Diese Rechenregeln gelten für beliebige Gruppen, z.B. auch für 100×100-Matrizen in $\mathrm{GL}(100, \mathbb{R})$. Ein Beweis für diesen Spezialfall ist schwieriger als der abstrakte Beweis für Gruppen allgemein.

Untergruppen

Definition (2.56)

Eine nichtleere Teilmenge S einer Gruppe G mit Verknüpfung $\circ$ wird als **Untergruppe** (subgroup) bezeichnet, wenn S mit der Restriktion von $\circ$ auf $S \times S$ eine Gruppe ist.

Satz (2.57)

Ist G eine Gruppe und $\emptyset \neq S \subseteq G$, dann sind die folgenden Eigenschaften äquivalent:

1. *S ist eine Untergruppe von G*
2. *Für alle $x, y \in S$ sind $x \circ y \in S$ und $x^{-1} \in S$.*
3. *Für alle $x, y \in S$ ist $x \circ y^{-1} \in S$.*

Beispiele (2.58)

Sind folgende Teilmengen jeweils Untergruppen?

- $\mathbb{N} \subset \mathbb{Z}$ bzgl. Addition
- $\mathbb{Q} \subset \mathbb{R}$ bzgl. Addition und $\mathbb{Q} \setminus \{0\} \subset \mathbb{R} \setminus \{0\}$ bzgl. Multiplikation

Definition (2.59)

Für $n \in \mathbb{N}$ wird $S_n := \{s \mid s : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ bijektiv}\}$ als **symmetrische Gruppe** oder auch **Gruppe der Permutationen** bezeichnet mit der Konkatenation von Abbildungen als binäre innere Verknüpfung: $s \circ t(k) = s(t(k))$ für $1 \leq k \leq n$.

Notation für eine Permutation $s \in S_n$:

$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n) \end{pmatrix} = (s(1), s(2), \ldots, s(n))$$

In der einzeiligen Darstellung steht der Wert $s(k)$ an Position k, deshalb ist die Reihenfolge wesentlich, während in der zweizeiligen Darstellung die (vertikal dargestellten) Paare $(k, s(k))$ auch unsortiert sein können.
Das Produkt $s \circ t$ von Permutationen $s, t \in S_n$ erhält man wie folgt:

$$\begin{pmatrix} 1 & \ldots & n \\ s(1) & \ldots & s(n) \end{pmatrix} \begin{pmatrix} 1 & \ldots & n \\ t(1)) & \ldots & t(n) \end{pmatrix} = \begin{pmatrix} 1 & \ldots & n \\ s(t(1)) & \ldots & s(t(n)) \end{pmatrix}$$

Beispiele (2.60)

In der symmetrische Gruppe $S_4 := \{s \mid s : \{1, \ldots, 4\} \to \{1, \ldots, 4\} \text{ bijektiv}\}$ sind folgende Permutationen einer Menge mit 4 Elementen gegeben:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \; t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

1. Berechnen Sie $s \circ t$ und $t \circ s$.
2. Ist S_4 kommutativ?
3. Beschreiben Sie das neutrale Element von S_4.

Lösung (2.60)

1. Berechnung von $s \circ t$ und $t \circ s$:

$$s \circ t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

$$t \circ s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

2. Wegen $s \circ t \neq t \circ s$ ist S_4 nicht kommutativ.
3. Das neutrale Element von S_4 ist die Identität:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Anzahl der Elemente einer symmetrischen Gruppe

Satz (2.61)

Für jedes $n \in \mathbb{N}$ hat die symmetrische Gruppe $n!$ viele Elemente, d.h. es gilt:

$$|S_n| = n!$$

Beweisidee (Überblick)

Beweis mit vollständiger Induktion. Im Induktionsschritt wird die Menge S_{n+1} in $(n+1)$ in gleich große Teilmengen zerlegt, wobei für jedes $k \leq n+1$ die Teilmenge F_k diejenigen Permutationen enthält, die die Zahl k auf 1 abbilden:

$$F_k := \{s \in S_{n+1} \mid s(k) = 1\} \subseteq S_n$$

Die Teilmengen F_k haben paarweise eine leere Schnittmenge und ihre Vereinigung ergibt die Gesamtmenge. Anwendung der Induktionsvoraussetzung auf alle F_k liefert in der Gesamtsumme das gewünschte Ergebnis.

Anzahl der Elemente einer symmetrischen Gruppe: Beweis (1/4)

Induktionsanfang: Für $n = 1$ gilt $|S_n| = 1 = 1! = n!$
Induktionsschritt $n \to n + 1$: Nach Induktionsannahme ist $|S_n| = n!$ wahr.
In der Menge S_{n+1} wird für jedes $k \leq n + 1$ definiert:

$$F_k := \{s \in S_{n+1} \mid s(k) = 1\} \subseteq S_n$$

Bis auf die Benennung der Elemente stimmt jede Teilmenge F_k mit S_n überein. Genauer kann man F_k und S_n mit einer bijektiven Abbildung $f : F_k \to S_n, s \mapsto f(s)$ identifizieren. Die Werte von f für eine Permutation $s \in F_k$ sind schrittweise über folgende Permutationen $f_i(s), i = 1, \ldots, 5$ definiert, das Endergebnis ist $f(s) = f_4(s)$ bzw. $f(s) = f_5(s)$ mit dem optionalen Schritt f_5:

Anzahl der Elemente einer symmetrischen Gruppe: Beweis (2/4)

- $f_1(s)$: In der Definitionsmenge der Permutationen werden k und 1 vertauscht
- $f_2(s)$: Das erste Paar $(k, s(k))$ mit dem konstanten Wert $(k, 1)$ wird abgetrennt.
- $f_3(s)$: Von alle verbleibenden Zahlen im Wertebereich von s wird die Zahl 1 subtrahiert (die Resultate sind positiv, da das Paar $(k, s(k))$ abgetrennt wurde).
- $f_4(s)$: Umbenennung der Zahlen im Definitionsbereich von $k+1$ bis $n+1$: Für $k+1 \leq i \leq n+1$ wird jeweils ein neues Argument $j = i - 1$ gebildet, dabei bleiben die Werte $s(i) - 1$ aus dem vorhergehenden Schritt erhalten. In anderen Worten: Für die neuen Argumente $k \leq j \leq n$ ist $f_4(s(j)) = s(j+1) - 1$.
  Nach diesem Schritt sind für alle $1 \leq i \leq n$ Werte $f_4(s(j)) \leq n$ definiert, außerdem ist $f_4(s) : \{1, \ldots, n\} \to \{1, \ldots, n\}$ eine bijektive Abbildung, da bei jedem Schritt $f_1(s), \ldots, f_4(s)$ die Bijektivität erhalten geblieben ist, und damit gilt $f_4(s) \in S_n$.
- $f_5(s)$: Optionaler Schritt (für bessere Lesbarkeit, entfällt für $k = 1$): Sortierung der ersten Zeile nach aufsteigenden Zahlen und gleichzeitige Verschiebung der Zahlen darunter . Das betrifft die Zahlen $1, \ldots, k-1$, bei denen 1 an die erste Position rückt und die anderen um eine Position nach hinten verschoben werden.

Anzahl der Elemente einer symmetrischen Gruppe: Beweis (3/4)

$$f_1(s) = \begin{pmatrix} k & 2 & \dots & k-1 & 1 & k+1 & \dots & n+1 \\ s(k) & s(2) & \dots & s(k-1) & s(1) & s(k+1) & \dots & s(n+1) \end{pmatrix}$$

$$f_2(s) = \begin{pmatrix} 2 & \dots & k-1 & 1 & k+1 & \dots & n+1 \\ s(2) & \dots & s(k-1) & s(1) & s(k+1) & \dots & s(n+1) \end{pmatrix}$$

$$f_3(s) = \begin{pmatrix} 2 & \dots & k-1 & 1 & k+1 & \dots & n+1 \\ s(2)-1 & \dots & s(k-1)-1 & s(1)-1 & s(k+1)-1 & \dots & s(n+1)-1 \end{pmatrix}$$

$$f_4(s) = \begin{pmatrix} 2 & \dots & k-1 & 1 & k & \dots & n \\ s(2)-1 & \dots & s(k-1)-1 & s(1)-1 & s(k+1)-1 & \dots & s(n+1)-1 \end{pmatrix}$$

Anzahl der Elemente einer symmetrischen Gruppe: Beweis (4/4)

Da f bijektiv ist, haben F_k und S_n gleich viele Elemente. Nach Induktionsvoraussetzung gilt:

$$|F_k| = |S_n| = n!$$

Für alle $k, m \leq n+1$ mit $k \neq m$ und für alle $s \in S_{n+1}$ gilt $s \in F_k \Rightarrow s \notin F_m$. Damit sind die Mengen F_k paarweise disjunkt:

$$\forall k, m : k \neq m \Rightarrow F_k \cap F_m = \emptyset$$

Da jedes Element $s \in S_{n+1}$ mit $k = s^{-1}(1)$ zur Menge F_k gehört, ist S_{n+1} die Vereinigung aller Mengen F_k: $S_{n+1} = F_1 \cup \ldots \cup F_{n+1}$. Deshalb gilt insgesamt die Behauptung:

$$|S_{n+1}| = \sum_{k=1}^{n+1} |F_k| = (n+1) \cdot n! = (n+1)!$$

Ringe: Beziehungen zwischen Addition und Multiplikation

Definition (2.62)

Eine nichtleere Menge R mit zwei inneren binären Verknüpfungen

$$+ : R \times R \to R, (x, y) \mapsto x + y \text{ und } \cdot : R \times R \to R, (x, y) \mapsto x \cdot y = xy$$

wird als **Ring** bezeichnet, wenn gilt:

1. $(R, +)$ ist kommutative Gruppe.
2. $(R \setminus \{0\}, \cdot)$ ist Halbgruppe.
3. Für alle $x, y, z \in R$ sind die **Distributivgesetze** erfüllt:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \text{ und } (x + y) \cdot z = (x \cdot z) + (y \cdot z)$$

Ein Ring heißt **kommutativ**, wenn $(R \setminus \{0\}, \cdot)$ kommutativ ist.

Beispiele (2.63)

$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Z}_n, +, \cdot), \mathrm{Mat}(n, \mathbb{R})$

Definition (2.64)

Ein Ring $(F, +, \cdot)$ wird als **Körper** (field) bezeichnet, wenn $(F \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist.

Beispiele (2.65)

Welche der Ringe $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (p prim), $\mathrm{Mat}(n, \mathbb{R})$, $\mathrm{GL}(n, \mathbb{R})$ ($n \in \mathbb{N}$) sind Körper?

Hinweis

Die Körper $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ unterscheiden sich bzgl. der Lösungen folgender Gleichungen:

$$x^2 = 2 \text{ und } x^2 = -1 \text{ und } x^n = 1 \ (n \in \mathbb{N})$$

In der Körpertheorie wird u.a. die Struktur der Lösungen komplexer Gleichungen analysiert.

Während in der Analysis stetige, differenzierbare und integrierbare Funktionen im Mittelpunkt stehen, liegt der Fokus in der Algebra auf strukturerhaltenden Abbildungen:

Definition (2.66)

Eine Funktion $f : G \to H$ zwischen (Halb-)Gruppen G und H heißt **Homomorphismus von (Halb-)Gruppen**, wenn gilt:

$$\forall x, y \in G : f(x \circ y) = f(x) \circ f(y)$$

Analog wird eine Abbildung zwischen Ringen bzw. Körpern **Homomorphismus von Ringen bzw. Körpern** genannt, wenn sie ein Homomorphismus zwischen den jeweiligen (Halb-)Gruppen bzgl. Addition und Multiplikation ist.

Beispiele (2.67)

- Für die Exponentialfunktion $\exp : \mathbb{R} \to \mathbb{R}^+, x \mapsto e^x$ gilt:

$$\forall x, y \in \mathbb{R} : e^x e^y = e^{x+y}$$

  Damit ist sie ein Gruppen-Homomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R}^+, \cdot)$.
- Die Quotientenabbildung $\pi_n : \mathbb{Z} \to \mathbb{Z}_n, a \mapsto [a]_n$ ist ein Ring-Homomorphismus.

In vielen wissenschaftlichen und technischen Anwendungsbereichen werden Homomorphismen verwendet, um Strukturen und deren Weiterentwicklung zu analysieren, z.B. um Veränderungsprozesse modellieren und digital berechnen zu können.

Weiter viel Spass bei der Mathematik!