Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kapitel 1: Logik

Referenzen zum Nacharbeiten:

Iwanowski/Lang 1
Meinel 1
Dean 3, 4

Organisationsform dieser Vorlesung

Vorlesung (Präsentation des neuen Stoffs im Frontalunterricht):

2 Lehreinheiten pro Woche bei Prof. Iwanowski

Übungsaufgaben (selbständige Übung des neuen Stoffs):

werden einmal pro Woche ausgegeben zur selbständigen Bearbeitung
(veranschlagter Zeitaufwand inklusive Nacharbeit der Vorlesung:
5 Stunden pro Woche)

Organisationsform dieser Vorlesung

Große Übung für alle:

1 Lehreinheit pro Woche bei Cordula Eichhorn.
Dort werden die Lösungen der Übungsaufgaben für alle vorgeführt.

Tutorien (Arbeiten in Kleingruppen):

1 Lehreinheit pro Woche bei einem Studenten höheren Semesters.
Dieser Student bespricht auch die bearbeiteten Übungsaufgaben.
Jeder Student wird in ein Tutorium eingeteilt (studiengangsabhängig). Das Tutorium selbst sollte nur besucht werden von denen, die Nachhilfe brauchen.

Inhaltlicher Umfang dieser Vorlesung

Inhaltliche Voraussetzungen:

Logisches Denken, Mathematik bis 9. Klasse (Gymnasium)

Lernziele dieser Vorlesung:

Verständnis für Mathematik und Freude daran

Elementare Konzepte: Logik, Mengenlehre, Zahlen

Fortgeschrittene Konzepte: Beweisstrategien, Zahlentheorie, Algebra

Spezielle Gebiete der Diskreten Mathematik: Kombinatorik, Graphentheorie

Direkte inhaltliche Relevanz für folgende Vorlesungen:

Informationstechnik, Digitaltechnik, Programmstrukturen, Grundlagen der Theoretischen Informatik, Algorithmen und Datenstrukturen, Datenbanken, Analysis, Lineare Algebra

Literatur

Lehrbuch, nach dem diese Vorlesung vorgeht:

Sebastian **Iwanowski** / Rainer **Lang**: *Diskrete Mathematik mit Grundlagen,*
Springer-Verlag 2014, ISBN 978-3-658-07130-1 (Print), 978-3-658-07131-8 (Online)

Lehrbücher, die teilweise den Lehrstoff abdecken:

Neville **Dean**: *Diskrete Mathematik,*
Pearson Studium, Reihe "im Klartext" 2003, ISBN 3-8273-7069-8

Albrecht **Beutelspacher** / Marc-Alexander **Zschiegner**:
Diskrete Mathematik für Einsteiger,
Vieweg 2004 (2. Auflage), ISBN 3-528-16989-3

Christoph **Meinel** / Martin **Mundhenk**:
Mathematische Grundlagen der Informatik,
Teubner 2002 (2. Auflage), ISBN 3-519-12949-3

Angelika **Steger**: *Diskrete Strukturen*, Bd.1, Springer 2001, ISBN 3-540-67597-3

Literatur

Weiterführende Lehrbücher, die für einige Kapitel hilfreich sind:

Martin Aigner: *Diskrete Mathematik*,
Vieweg 2001 (4. Auflage), ISBN 3-528-37268-0

Norman Biggs: *Discrete Mathematics*,
Oxford University Press 2002, ISBN 0-19-850717-8

Jiri Matousek / Jaroslav Nesetril:
Diskrete Mathematik - Eine Entdeckungsreise,
Springer-Verlag 2001, ISBN 3-540-42386-9

1. Logik

1.1 Einführung

Was ist das Wesentliche der Mathematik ?

Mathematik ist in erster Linie das Erkennen von:

- Strukturen
- Zusammenhängen
- Verallgemeinerungen
- Gemeinsamkeiten

Was sich auf die Wirklichkeit bezieht,
ist nicht sicher,
und was sicher ist,
ist nicht wirklich.

Erst aus diesen Prinzipien folgert man:

- Rechenregeln
- Vorgehensweisen (Algorithmen)

Formalismen dienen in der Mathematik zu

- einer eindeutigen Ausdrucksweise
- einem besseren Verständnis für den Menschen

1. Logik

1.1 Einführung

Was ist Diskrete Mathematik ?

- Logik
- Mengenlehre
- Diskrete Zahlenbereiche
- Kombinatorik
- Graphentheorie
- Algebra

Was gehört nicht zur Diskreten Mathematik ?

- Analysis / Funktionentheorie
- Lineare Algebra
- Wahrscheinlichkeitsrechnung / Statistik
- ...

1.2 Aussagenlogik

Aussagen und Wahrheitswerte

Was ist eine Aussage ?

- Eine *elementare* Aussage ist ein beliebiges Objekt.
- Elementare Aussagen sind unteilbar.
  - Wegen der Unteilbarkeit heißen elementare Aussagen auch *Atome*

Was ist ein Wahrheitswert ?

- Ein Wahrheitswert ist ein Element aus einer zweielementigen Menge (z.B. dargestellt als {`w`, `f`} oder {0,1}).

Was macht die Aussagenlogik ?

- Die Aussagenlogik beschäftigt sich mit Funktionen, die jeder Aussage einen Wahrheitswert zuordnen.
  - Solche Funktionen heißen *binäre Funktionen*

1.2 Aussagenlogik

Operatoren zwischen Aussagen

Durch Operatoren werden aus alten Aussagen neue Aussagen geschaffen:

Wahrheitswerte für die neuen Aussagen:

p	q	¬p	p ∧ q	p ∨ q	p → q	p ↔ q
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

Einstelliger Operator:

- **Negation (¬)**

Zweistellige Operatoren:

- **Konjunktion (∧)**
- **Disjunktion (∨)**
- **Implikation (→)**
- **Äquivalenz (↔)**

p → q

hinreichend — notwendig

stärker (genauer) — schwächer (ungenauer)

p ↔ q

hinreichend und notwendig

gleichwertig

1.2 Aussagenlogik

Zusammenhang zwischen den Operatoren

Logische Äquivalenzregeln:

$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

Kontraposition

$p \rightarrow q \Leftrightarrow \neg p \vee q$

Ersetzen der Implikation durch ¬ und v

$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

Ersetzen der Äquivalenz durch Implikationen

$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

deMorgansche Regeln

$\neg\neg p \Leftrightarrow p$

Doppelte Negation

Wahrheitswerte für die neuen Aussagen:

p	q	¬p	p ∧ q	p ∨ q	p → q	p ↔ q
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

$p \wedge q \Leftrightarrow q \wedge p$

$p \vee q \Leftrightarrow q \vee p$

Kommutativgesetze

$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

Distributivgesetze

1.2 Aussagenlogik

Zusammenhang zwischen den Operatoren

Logische Schlussregeln:

$(p \rightarrow q) \wedge p \Rightarrow q$

Modus ponens

$(p \rightarrow q) \wedge \neg q \Rightarrow \neg p$

Modus tollens

$(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow (p \rightarrow r)$

Kettenschluss

$(\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q) \Rightarrow p$

Indirekter Beweis

Wahrheitswerte für die neuen Aussagen:

p	q	¬p	p ∧ q	p ∨ q	p → q	p ↔ q
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

$p \wedge q \Rightarrow p$ **$p \wedge q \Rightarrow q$**

Logische Einschränkung

$(p \vee q) \wedge \neg q \Rightarrow p$

Logischer Ausschluss

1.3 Prädikatenlogik

Aussageformen, Variable und Prädikate

Was ist eine Aussageform ?

- Eine (prädikatenlogische) Aussageform ist ein Ausdruck mit Variablen aus bestimmten (aber beliebigen) Definitionsbereichen.
- Die Belegung jeder Variable mit einem zulässigen Wert macht aus einer Aussageform eine Aussage, die wahr oder falsch sein kann.

Was ist ein Prädikat ?

- Ein Prädikat gehört zu einer Aussageform und identifiziert die Wertekonstellationen, die eine Aussageform zu einer wahren Aussage zu machen.
- Für jede Wertekonstellation von Werten aus dem Definitionsbereich der Variablen ist das zu der jeweiligen Aussageform gehörende Prädikat definiert.
- Ein Prädikat ist entweder wahr (erfüllt) oder falsch (nicht erfüllt).

1.3 Prädikatenlogik

Quantoren

- **für Aussageformen, die nur von x abhängen:**

  Der Existenzquantor $\exists x\ (\ldots)$ beschreibt die Aussage, dass es (mindestens) einen Wert für x gibt, der die dahinter stehende Aussageform in x zu einer wahren Aussage macht.

  Der Allquantor $\forall x\ (\ldots)$ beschreibt die Aussage, dass jeder Wert für x die dahinter stehende Aussageform in x zu einer wahren Aussage macht.

  Die Definitionsbereiche für die Variablen dürfen eingeschränkt werden:

  Für den Existenzquantor ist das eine *Verschärfung*,
  für den Allquantor eine *Abschwächung* der Aussage.

1.3 Prädikatenlogik

Quantoren

- **für Aussageformen, die von weiteren Variablen abhängen:**

  Existenzquantor ∃x (...) und Allquantor ∀x (...) beschreiben Aussage*formen*, die nur noch von den restlichen Variablen abhängen, da über x die Aussage bereits gemacht ist.

Beispiel 1.2

$$A^*(z) := \exists x \in D : \forall y \in E : A(x, y, z)$$

Wenn $A(x, y, z)$ die Aussageform ist, dass die Zeugnisnote x für das Fach y an den Studenten z vergeben wird, also D die Menge der möglichen Zeugnisnoten und E die Menge aller Fächer ist, dann ist in diesem Beispiel die Aussageform $A^*(z)$, dass es eine Zeugnisnote gibt, die Student z in allen Fächern erhalten hat. Der Wahrheitswert der Aussageform $A^*(z)$ hängt nur noch davon ab, welcher Student für z eingesetzt wird: Manche Studenten z haben tatsächlich in jedem Fach dieselbe Note erhalten (für diese z ist $A^*(z)$ wahr), andere haben unterschiedliche Noten erhalten (für jene z ist $A^*(z)$ falsch).

Dies macht aus der Aussageform $A(x, y, z)$ durch die Bindung von x und y an Quantoren also eine neue Aussageform $A^*(z)$, deren Wahrheitswert nur noch von der freien Variablen z abhängt. Im Allgemeinen wird aus einer Aussageform durch die Bindung von Quantoren genau dann eine Aussage, wenn *jede Variable* durch einen Quantor gebunden wird.

1.3 Prädikatenlogik

„Rechenregeln“ für die Quantoren:

$\neg\forall x\,(F(x)) \Leftrightarrow \exists x\,(\neg F(x))$

$\neg\exists x\,(F(x)) \Leftrightarrow \forall x\,(\neg F(x))$

Verallgemeinerung von deMorgan

$\forall x\,\forall y\,(F(x,y)) \Leftrightarrow \forall y\,\forall x\,(F(x,y))$

$\exists x\,\exists y\,(F(x,y)) \Leftrightarrow \exists y\,\exists x\,(F(x,y))$

Vertauschung gleicher Quantoren

Was gilt bei der Vertauschung verschiedener Quantoren ? ($\Leftrightarrow$,$\Rightarrow$,$\Leftarrow$,$\not\Leftrightarrow$)

$\exists x\,\forall y\,(F(x,y))$ $\qquad$ $\forall y\,\exists x\,(F(x,y))$

$\exists y\,\forall x\,(F(x,y))$ $\qquad$ $\forall x\,\exists y\,(F(x,y))$

1.3 Prädikatenlogik

„Rechenregeln“ für die Quantoren:

Was gilt bei Hineinziehen von Quantoren in ∧ oder ∨ ? (⇔,⇒,⇐,⇏)

$\forall x\,(F(x)) \vee \forall x\,(G(x))$	$\forall x\,(F(x) \vee G(x))$
$\forall x\,(F(x)) \wedge \forall x\,(G(x))$	$\forall x\,(F(x) \wedge G(x))$
$\exists x\,(F(x)) \vee \exists x\,(G(x))$	$\exists x\,(F(x) \vee G(x))$
$\exists x\,(F(x)) \wedge \exists x\,(G(x))$	$\exists x\,(F(x) \wedge G(x))$

1.3 Prädikatenlogik

Arithmetische Vergleichsprädikate:

Präfix-Notation (Standard in Prädikatenlogik)	Infix-Notation (Standard in Arithmetik)	Postfix-Notation (Standard auf alten Taschenrechnern ohne Klammern)
`lessThan (x,y)`	`x < y`	`x, y, <`
`equal (x,y)`	`x = y`	`x, y, =`

Mit diesen beiden Prädikaten lassen sich alle anderen Vergleichsprädikate bilden:

$x \leq y$ $x \geq y$ $x \neq y$ $x > y$

Wie drückt man mit diesen Prädikaten aus, dass eine Zahl x zwischen y und z liegt ?

1.3 Prädikatenlogik

Übersetzung Umgangssprache in prädikatenlogische Formeln

Umgangssprache	Formel
Objekte mit Eigenschaft E haben auch Eigenschaft F.	$\forall x\ E(x) \rightarrow F(x)$
Nur Objekte mit Eigenschaft E haben auch Eigenschaft F.	$\forall x\ E(x) \Leftrightarrow F(x)$
Höchstens Objekte mit Eigenschaft E haben auch Eigenschaft F.	$\forall x\ F(x) \rightarrow E(x)$
Nur x hat die Eigenschaft F.	$\forall y\ F(y) \Leftrightarrow y=x$
Höchstens x hat die Eigenschaft F.	$\forall y\ F(y) \rightarrow y=x$
Alle Objekte haben die Eigenschaft F.	$\forall x\ F(x)$
Kein Objekt mit Eigenschaft E hat Eigenschaft F.	$\forall x\ E(x) \rightarrow \neg\ F(x)$
Kein Objekt hat die Eigenschaft F.	$\forall x\ \neg\ F(x)$
Einige Objekte mit Eigenschaft E haben auch Eigenschaft F. (wenn es überhaupt Objekte mit Eigenschaft E gibt)	$\exists\ x\ E(x) \wedge F(x)$ (keine Implikation!)
Objekte x mit Eigenschaft E haben Eigenschaft F.	$\forall x\ E(x) \rightarrow F(x)$
Objekte x mit Eigenschaft E sind die Objekte mit Eigenschaft F.	$\forall x\ E(x) \Leftrightarrow F(x)$

1.3 Prädikatenlogik

Übersetzung Umgangssprache in prädikatenlogische Formeln

Umgangssprache	Formel
Für alle Objekte x, für die es ein n gibt mit P(x,n), gibt es ein m mit Q(x,m)	$\forall x \, \forall n \, \exists \, m \; P(x,n) \rightarrow Q(x,m)$

Beispiel:

Alle Leute, die verheiratet sind, haben einen Trauzeugen.

Warnung!

$\forall x \, \forall n \, \forall \, m \; P(x,n) \rightarrow Q(x,m)$	**ist eine stärkere Aussage:** **Jetzt müsste Q(x,m) für alle m gelten, wenn es für x ein n_0 gibt mit $P(x,n_0)$.**
$\forall x \, \exists \, n \, \exists \, m \; P(x,n) \rightarrow Q(x,m)$	**ist eine schwächere Aussage:** **Jetzt müsste Q(x,m) für kein m gelten, selbst wenn es für x ein n_0 gibt mit $P(x,n_0)$: Denn man könnte in P(x,n) einfach ein $n_1 \neq n_0$ einsetzen mit $P(x,n_1) = \bot$, und dann muss Q(x,m) niemals wahr sein.**

Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kapitel 2: Mengenlehre

Referenzen zum Nacharbeiten:

Iwanowski/Lang 2
Meinel 2, 4, 5, 10.2-10.4
(zur Vertiefung: Meinel 10.5-10.8 und Beutelspacher 10)
Dean 2, 5-7
Steger 0.1, 0.2 (als Zusammenfassung), 1.4, 5.2

2. Mengenlehre

2.1 Grundlagen

Definition

Eine Menge ist eine ungeordnete Ansammlung von beliebigen Objekten.
Die Objekte, die in einer Menge enthalten sind, heißen Elemente der Menge.
Schreibweise: $x \in M$ bedeutet: Das Element x ist in Menge M.

Eigenschaften

- Reihenfolge, Einmaligkeit, Anzahl von Elementen

  Die Reihenfolge ist nicht festgelegt: Umordnen erzeugt keine neue Menge.
  Ein Element kann nur einmal in M enthalten sein, egal, wie häufig es erwähnt wird.
  Eine Menge M kann beliebig viele Elemente enthalten, also auch unendlich viele.

- Gleichheit von Mengen

  Zwei Mengen A und B sind genau dann gleich, wenn jedes Element aus A auch in B enthalten ist und jedes Element aus B auch in A enthalten ist.

2. Mengenlehre

2.1 Grundlagen

Darstellung von Mengen

- Elementschreibweise

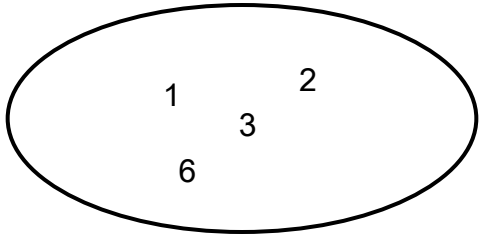
  für endliche Mengen: $\{e_1, e_2, \underbrace{\ldots}, e_n\}$

  Elemente müssen konkret hingeschrieben werden

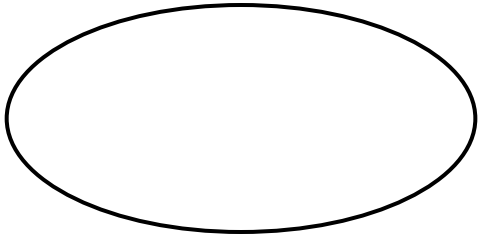
  für beliebige (also auch unendliche) Mengen: $\{x \in \text{Grundmenge: Prädikat } (x)\}$

- Venn-Diagramme

  für endliche Mengen:



  für beliebige Mengen (abstrakt):



2. Mengenlehre

2.1 Grundlagen

Operationen auf Mengen

Menge x Menge → Menge

- Vereinigung $A \cup B$

  Element muss in A oder in B liegen.

- Durchschnitt $A \cap B$

  Element muss in A und in B liegen.

- Differenz $A \setminus B$

  Element muss in A und nicht in B liegen.

- Symmetrische Differenz $A \Delta B$

  Element muss in A oder in B liegen, aber nicht in beiden gleichzeitig.

2. Mengenlehre

2.1 Grundlagen

Operationen auf Mengen

Menge x Menge → {w,f}

- Teilmenge / Obermenge

  $A \subseteq B$ *A ist Teilmenge und B ist Obermenge: Alle Elemente von A liegen auch in B.*

  $A \subsetneq B$ *A ist echte Teilmenge und B ist echte Obermenge: Alle Elemente von A liegen auch in B. A und B sind nicht gleich, d.h. es gibt mindestens ein Element, das in B liegt und nicht in A.*

  $A \subset B$ *wird von manchen Autoren mit „Teilmenge“ gleichgesetzt, von anderen mit „echte Teilmenge“.*

- Unterschied zwischen Elementbeziehung und Teilmengenbeziehung

  Ein beliebiges Objekt x ist Element einer Menge M,
  wenn es in der anderen Menge enthalten ist ($x \in M$).
  Eine Menge A ist Teilmenge einer Menge B,
  wenn alle Elemente von A auch Elemente von B sind ($A \subseteq B$)

2. Mengenlehre

2.1 Grundlagen

Operationen auf Mengen

Menge → Menge

- Bildung der Potenzmenge

  Die Potenzmenge $\wp(A)$ einer Menge A ist die Menge aller Teilmengen von A.

- Bildung der komplementären Menge

  Die zu einer Menge A komplementäre Menge $\bar{A}$ ist die Menge, die aus allen Elementen besteht, die nicht in A enthalten sind.

  Dazu muss man das Universum Ω aller möglichen Elemente definieren: $\bar{A} = \Omega \setminus A$

2. Mengenlehre

2.1 Grundlagen

Operationen auf Mengen

Menge x Menge → Menge

- Kreuzprodukt (kartesisches Produkt)

M x M ist die Menge aller geordneten Paare von Elementen aus M: $M \times M = \{(a,b): a,b \in M\}$

M x N ist die Menge aller geordneten Paare von Elementen aus M und N:

$$M \times N = \{(a,b): a \in M, b \in N\}$$

- Tupel (für mehr als 2 Mengen)

Ein Tupel ist die Verallgemeinerung eines Paares:
Ein n-Tupel hat die Form $(a_1, a_2, \ldots, a_n)$. Es ist Element von $M \times \underbrace{\ldots}_{\text{n mal}} \times M$
Ein Paar ist also ein 2-Tupel.
Analoge Definition: Tupel für verschiedene Mengen.

- Unterschiede zwischen Tupeln und Mengen

Bei den Elementen eines Tupels kommt es auf die Reihenfolge an, bei denen einer Menge nicht.

2. Mengenlehre

2.2 Relationen

Definition und Eigenschaften

Eine Relation auf M ist eine beliebige Teilmenge des Kreuzprodukts M x M.

Mögliche Eigenschaften einer Relation R ⊆ M x M (gelten nicht immer!):

- reflexiv: $\forall x \in M : (x, x) \in R$
- symmetrisch: $\forall x, y \in M : (x, y) \in R \Leftrightarrow (y, x) \in R$
- transitiv: $\forall x, y, z \in M : (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$
- antisymmetrisch: $\forall x, y \in M : (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$
- linear (vollständig): $\forall x, y \in M : (x, y) \in R \vee (y, x) \in R$

2. Mengenlehre

2.2 Relationen

Spezieller Relationstyp: Äquivalenzrelationen

Eine Äquivalenzrelation auf M ist eine Relation R mit folgenden Eigenschaften:

Schreibweise: $(x, y) \in R \Leftrightarrow x \cong y$ (x ist äquivalent zu y)

- reflexiv: $\forall x \in M : x \cong x$
- symmetrisch: $\forall x, y \in M : x \cong y \Leftrightarrow y \cong x$
- transitiv: $\forall x, y, z \in M : x \cong y \wedge y \cong z \Rightarrow x \cong z$

2. Mengenlehre

2.2 Relationen

Spezieller Relationstyp: Äquivalenzrelationen

Eine **Äquivalenzklasse** zu einer Äquivalenzrelation R ⊆ M x M ist eine Menge von Elementen aus M, die paarweise zueinander äquivalent sind, sodass alle Elemente, die zueinander äquivalent sind, in derselben Äquivalenzklasse liegen.

1) *Eine Äquivalenzklasse ist nicht leer und jedes Element liegt in einer Äquivalenzklasse (wg. Reflexivität).*
2) *Kein Element liegt in mehr als einer Äquivalenzklasse (wg.Transitivität).*
3) *Die Tatsache, dass die Äquivalenzklasse eine Menge ist, beruht auf der Symmetrie.*

Eine **Partition** einer Menge M ist eine Zerlegung in nichtleere disjunkte (d.h. elementeverschiedene) Teilmengen.

1. Zu jeder Partition gehört eindeutig eine Äquivalenzrelation.

   Definiere zwei Elemente genau dann als äquivalent, wenn sie in derselben Teilmenge liegen.

2. Zu jeder Äquivalenzrelation gehört eindeutig eine Partition.

   Die Menge der Äquivalenzklassen bildet die Partition.

2. Mengenlehre

2.2 Relationen

Spezieller Relationstyp: Äquivalenzrelationen

Vorgehensweise für konkrete Aufgaben:

- Definition und Nachweis der Eigenschaften von Äquivalenzrelationen

  1) Prüfe für die gesamte Menge nach, ob Reflexivität gilt.

  2) Prüfe für jedes Element nach, ob Symmetrie gilt.

  3) Prüfe für alle aneinanderpassenden Elemente nach, ob Transitivität gilt.

- Bestimmen von Äquivalenzklassen:

  1) Fange mit beliebigem Element an und nimm alle Elemente hinzu, zu dem das Element in Relation steht. ⇒ *1. Äquivalenzklasse*

  2) Fahre mit noch nicht erfassten Element fort und nimm alle Elemente hinzu, zu dem dieses in Relation steht. ⇒ *2. Äquivalenzklasse*

  ⋮

  n) Wenn kein Element mehr übrig ist, sind alle Äquivalenzklassen gebildet.

2. Mengenlehre

2.2 Relationen

Spezieller Relationstyp: Ordnungsrelationen

Eine Ordnungsrelation auf M ist eine Relation R mit folgenden Eigenschaften:

Schreibweise: $(x,y) \in R \Leftrightarrow x \preccurlyeq y$ (x ist kleiner oder gleich y)

- reflexiv: $\forall\, x \in M: x \preccurlyeq x$
- antisymmetrisch: $\forall\, x,y \in M: (x \preccurlyeq y) \wedge (y \preccurlyeq x) \Rightarrow (x = y)$
- transitiv: $\forall\, x,y, z \in M: (x \preccurlyeq y) \wedge (y \preccurlyeq z) \Rightarrow (x \preccurlyeq z)$
- linear: $\forall\, x,y \in M: (x \preccurlyeq y)\ v\ (y \preccurlyeq x)$

Ordnungsrelationen werden auch *totale* Ordnungen genannt.

Bei Wegfall der Eigenschaft *linear* spricht man von *Halbordnungen* oder *partiellen Ordnungen*.

2. Mengenlehre

2.2 Relationen

Spezieller Relationstyp: Ordnungsrelationen

- Maximum und Minimum bezüglich einer Ordnung:

  $x \in M$ ist Maximum $\Leftrightarrow \quad \forall\, y \in M: (y \preccurlyeq x)$

  $x \in M$ ist Minimum $\Leftrightarrow \quad \forall\, y \in M: (x \preccurlyeq y)$

- maximale und minimale Elemente:

  $x \in M$ ist maximal $\Leftrightarrow \quad \forall\, y \in M: (x \preccurlyeq y) \Rightarrow (x = y)$

  $x \in M$ ist minimal $\Leftrightarrow \quad \forall\, y \in M: (y \preccurlyeq x) \Rightarrow (x = y)$

  Jedes Maximum ist maximal und jedes Minimum ist minimal, aber nicht immer umgekehrt!
  Ein Maximum bzw. Minimum ist immer eindeutig, d.h. es kann nicht verschiedene geben.
  Verschiedene maximale bzw. minimale Elemente kann es nur in partiellen Ordnungsrelationen geben, und in diesem Fall gibt es kein Maximum bzw. Minimum.

2. Mengenlehre

2.2 Relationen

Darstellung von Relationen R auf endlichen Mengen M

- Zuordnungsdiagramm (für beliebige Relationen)

  Zeichne 2 Venn-Diagramme für M, eins links, eins rechts:
  Verbinde Element x in linkem Diagramm mit Element y im rechten Diagramm
  genau dann, wenn $(x,y) \in R$

- Partition (nur für Äquivalenzrelationen)

  Bilde die Äquivalenzklassen nach der Methode auf Folie 11

- Hasse-Diagramm (nur für Ordnungsrelationen)

  Zeichne die Elemente von M von oben nach unten, maximale oben, minimale unten:
  Verbinde ein höheres Element x mit einem tieferen y, wenn
  1) $y \preccurlyeq x$ (y ist kleiner oder gleich x)
  2) $(y \preccurlyeq z) \wedge (z \preccurlyeq x) \Rightarrow (y=z) \vee (z=x)$ (kein z liegt zwischen y und x)

2. Mengenlehre

2.2 Relationen

Verallgemeinerung des Kreuzprodukts für <u>verschiedene</u> Mengen:

Menge x Menge → Menge

- Kreuzprodukt (kartesisches Produkt)

  M x N ist die Menge aller Paare von Elementen,
  wobei das erste aus M und das zweite aus N ist: $M \times N = \{(a,b): a \in M, b \in N\}$

Analog:

- Kreuzprodukt für mehr als 2 verschiedene Mengen
- Tupel für mehr als 2 verschiedene Mengen

Verallgemeinerung des Relationsbegriffs für <u>verschiedene</u> Mengen:

Eine Relation **zwischen** M und N ist eine beliebige Teilmenge des Kreuzprodukts M x N.

Analog kann man Relationen zwischen mehr als 2 Mengen definieren (wohl geordnet).

2. Mengenlehre

2.3 Funktionen

Eine **Funktion** ist eine Relation $F \subset M \times N$ (M und N dürfen ungleich sein), in der für **jedes** $m \in M$ ein **eindeutiges** Paar (m,n) existiert:

- Existenz des Funktionswerts (Linksvollständigkeit): $\forall m \in M\ \exists n \in N: (m,n) \in F$
- Eindeutigkeit des Funktionswerts (Rechtseindeutigkeit):
  $\forall m \in M: (m,n_1) \in F \wedge (m,n_2) \in F \Rightarrow n_1 = n_2$

Wenn $(m,n) \in F$, dann heißt $n \in N$ der Funktionswert F(m) von $m \in M$.
M wird Definitionsbereich und N Zielmenge der Funktion F genannt.

Abbildungsschreibweise für Funktionen:

							für die einzelnen Elemente:
F:	M	→	N		m	↦	F(m)
	Definitionsbereich		Zielmenge		Urbild (Argument)		Bild

Die Teilmenge von N, für die es Urbilder in M gibt, heißt Bildmenge F(M) von M.

2. Mengenlehre

2.3 Funktionen

Komposition von Funktionen:

Seien F: A→B und G: B→C Funktionen.
Dann ist G∘F: A→C die Kompositionsfunktion:

$$G \circ F = \{(a,c) \in A \times C \mid \exists b \in B: b=F(a) \wedge c = G(b)\}$$

Für alle $a \in A$ gilt: $G \circ F\ (a) = G(F(a))$

Analog kann man die Komposition von Relationen definieren.

Satz: Die Komposition von 2 Funktionen ist immer eine Funktion.

Inverse Relationen: R^{-1}

Sei $R \subset A \times B$ eine Relation.
Dann ist $R^{-1} \subset B \times A$ mit $(b,a) \in R^{-1} \Leftrightarrow (a,b) \in R$ die zu R inverse Relation.

Frage: Wann ist die Inverse einer Funktion wieder eine Funktion ?

(Antwort auf nächster Folie)

2. Mengenlehre

2.3 Funktionen

Funktionen mit speziellen Eigenschaften

- surjektive Funktionen:

  Eine Funktion F: M→N heißt surjektiv,
  wenn F(M) = N gilt (Rechtsvollständigkeit).

- injektive Funktionen:

  Eine Funktion F: M→N heißt injektiv,
  wenn jedes Bild höchstens ein Urbild hat (Linkseindeutigkeit).

- bijektive Funktionen

  Eine Funktion F: M→N heißt bijektiv, wenn sie surjektiv und injektiv ist.

Satz: Die Inverse F^{-1} einer Funktion F ist genau dann wieder eine Funktion, wenn F bijektiv ist.

2. Mengenlehre

2.3 Funktionen

Mächtigkeit von Mengen

Zwei endliche Mengen gelten als „gleich groß“,
wenn sie die gleiche Anzahl von Elementen enthalten.

Anzahl der Elemente von M: |M|

Zwei unendliche Mengen gelten als „gleich groß“,
wenn es zwischen ihnen eine bijektive Funktion gibt.

Mächtigkeit von M: |M|

- Diese Definition verallgemeinert die für endliche Mengen:
  Sie ist also auch auf **endliche Mengen** anwendbar:

  Seien $A = \{a_1, a_2, \ldots, a_n\}$ und $B = \{b_1, b_2, \ldots, b_n\}$.
  Dann ist $f(a_i) = b_i$ für alle i die gewünschte bijektive Funktion.

  Anm.: Da Mengen ungeordnet sind, ist die bijektive Funktion nicht eindeutig!

für **endliche Mengen:**
Falls |A| > |B|: Jede Funktion f: A → B ist nicht injektiv.
Falls |A| < |B|: Jede Funktion f: A → B ist nicht surjektiv.

2. Mengenlehre

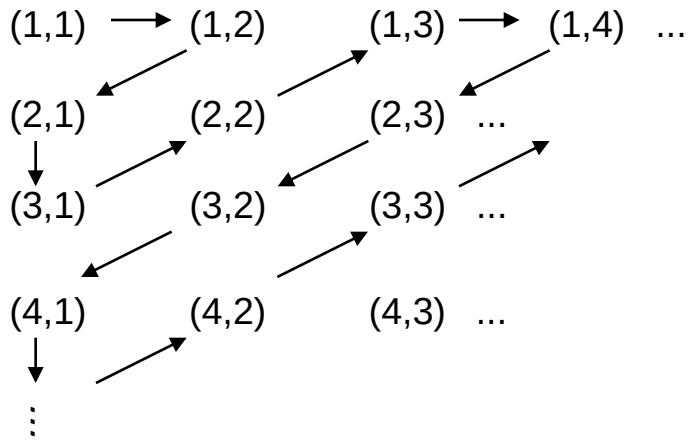
2.3 Funktionen

Mächtigkeit von Mengen

Eine Menge M heißt *abzählbar unendlich*,
wenn es eine bijektive Funktion f: $\mathbb{N} \rightarrow$ M gibt

- Cantorsches Diagonalverfahren für mehrdimensionale abzählbar unendliche Mengen:

Bsp. für $\mathbb{N}\backslash\{0\} \times \mathbb{N}\backslash\{0\}$:



Folgerung:

- $\mathbb{N}$x$\mathbb{N}$ und $\mathbb{Q}$ sind abzählbar

$\mathbb{R}$ ist nicht abzählbar !

2. Mengenlehre

2.4 Boolesche Algebren

Konzept 1: Aussagenlogische Formeln und ihre Operationen:

Aussagenlogische Formeln
haben die Operatoren ¬ (einstellig) und ∧ und ∨ (jeweils zweistellig)
und die Konstanten ⊥ und ⊤, die folgenden Regeln genügen:

$p \wedge q = q \wedge p$
$p \vee q = q \vee p$
Kommutativgesetze

$p \wedge (q \wedge r) = (p \wedge q) \wedge r$
$p \vee (q \vee r) = (p \vee q) \vee r$
Assoziativgesetze

$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$
Distributivgesetze

$p \wedge p = p$
$p \vee p = p$
Idempotenz

$\neg(p \wedge q) = \neg p \vee \neg q$
$\neg(p \vee q) = \neg p \wedge \neg q$
deMorgansche Regeln

$\neg\neg p = p$
Doppelte Negation (Involution)

$p \vee \bot = p$
$p \wedge \top = p$
Neutrale Elemente

$p \wedge \bot = \bot$
$p \vee \top = \top$
“Nullmultiplikation”

$p \wedge \neg p = \bot$
$p \vee \neg p = \top$
Inverses Element (Komplement)

2. Mengenlehre

2.4 Boolesche Algebren

Konzept 2: Mengen eines Ereignisraums Ω und ihre Operationen:

Mengen eines Ereignisraums Ω
haben die Operatoren $\overline{\ }$ (einstellig) und ∩ und ∪ (jeweils zweistellig)
und die Konstanten ∅ und Ω, die folgenden Regeln genügen:

$p \cap q = q \cap p$

$p \cup q = q \cup p$

Kommutativgesetze

$p \cap (q \cap r) = (p \cap q) \cap r$

$p \cup (q \cup r) = (p \cup q) \cup r$

Assoziativgesetze

$p \cap (q \cup r) = (p \cap q) \cup (p \cap r)$

$p \cup (q \cap r) = (p \cup q) \cap (p \cup r)$

Distributivgesetze

$p \cap p = p$

$p \cup p = p$

Idempotenz

$\overline{(p \cap q)} = \overline{p} \cup \overline{q}$

$\overline{(p \cup q)} = \overline{p} \cap \overline{q}$

deMorgansche Regeln

$\overline{\overline{p}} = p$

Doppelte Negation (Involution)

$p \cup \varnothing = p$

$p \cap \Omega = p$

Neutrale Elemente

$p \cap \varnothing = \varnothing$

$p \cup \Omega = \Omega$

"Nullmultiplikation"

$p \cap \overline{p} = \varnothing$

$p \cup \overline{p} = \Omega$

Inverses Element (Komplement)

2. Mengenlehre

2.4 Boolesche Algebren

Formale Zusammenfassung dieser beiden Konzepte:

Eine **Boolesche Algebra** ist eine nichtleere Menge $\mathscr{B}$
mit den Operatoren ~ (einstellig) und $\oplus$ und $\odot$ (jeweils zweistellig)
und den Elementen 0 und 1, die folgenden Regeln genügen:

$p \odot q = q \odot p$
$p \oplus q = q \oplus p$
Kommutativgesetze

$p \odot (q \odot r) = (p \odot q) \odot r$
$p \oplus (q \oplus r) = (p \oplus q) \oplus r$
Assoziativgesetze

$p \odot (q \oplus r) = (p \odot q) \oplus (p \odot r)$
$p \oplus (q \odot r) = (p \oplus q) \odot (p \oplus r)$
Distributivgesetze

$p \odot p = p$
$p \oplus p = p$
Idempotenz

$\sim(p \odot q) = \sim p \oplus \sim q$
$\sim(p \oplus q) = \sim p \odot \sim q$
deMorgansche Regeln

$\sim\sim p = p$
Doppelte Negation (Involution)

$p \oplus 0 = p$
$p \odot 1 = p$
Neutrale Elemente

$p \odot 0 = 0$
$p \oplus 1 = 1$
“Nullmultiplikation”

$p \odot \sim p = 0$
$p \oplus \sim p = 1$
Inverses Element (Komplement)

2. Mengenlehre

2.4 Boolesche Algebren

Was bringt uns der Formalismus ?

Sehr viel: Boolesche Algebren fassen mehrere Konzepte zusammen, die wir bereits kennen !

➔ Einmal verstanden, mehrmals angewendet

➔ Sachverhalte, die aus den Eigenschaften einer Booleschen Algebra folgen, gelten für alle Mengen, die zum Konzept der Booleschen Algebra gehören.

Beispiele für solche Sachverhalte:

Normalformen (konjunktiv oder disjunktiv)

Ordnungsrelationen

Auswertungsalgorithmen (Einsetzen von Werten in Formeln)

Komplexitätsanalysen (Beweise zur Bestimmung von Laufzeit und Platz)

2. Mengenlehre

2.4 Boolesche Algebren für Faule

Der Nachweis folgender Eigenschaften einer Booleschen Algebra reicht aus:

Eine **Boolesche Algebra** ist bereits durch eine Menge $\mathcal{B}$
mit den Operatoren ~ (einstellig) und $\oplus$ und $\odot$ (jeweils zweistellig)
und den Elementen 0 und 1 gegeben, die folgenden Regeln genügen:

$p \odot q = q \odot p$

$p \oplus q = q \oplus p$

Kommutativgesetze

$p \odot (q \oplus r) = (p \odot q) \oplus (p \odot r)$

$p \oplus (q \odot r) = (p \oplus q) \odot (p \oplus r)$

Distributivgesetze

Das heißt:
Bei Erfüllung dieser 4 Grundgesetze sind die anderen Gesetze
Assoziativgesetze, *deMorgansche Regeln*, *Idempotenz*, *Nullmultiplikation*
und *doppelte Negation* automatisch erfüllt.

$p \oplus 0 = p$

$p \odot 1 = p$

Neutrale Elemente

$p \odot \sim p = 0$

$p \oplus \sim p = 1$

Inverses Element (Komplement)

2. Mengenlehre

2.4 Boolesche Algebren: Weitere Beispiele

1. Schaltfunktionen-Algebra

$\mathcal{B}_n = \{f:\{0,1\}^n \rightarrow \{0,1\}\}$

$\sim f(x_1,\ldots,x_n) = 1 - f(x_1,\ldots,x_n)$

$(f \oplus g)(x_1,\ldots,x_n) = \max \{f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)\}$

$(f \odot g)(x_1,\ldots,x_n) = \min \{f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)\}$

Die Funktion $f : \{0,1\}^3 \rightarrow \{0,1\}$ sei definiert durch:

$$f(0,0,0) = 0 \quad f(0,0,1) = 1 \quad f(0,1,0) = 1 \quad f(0,1,1) = 1$$
$$f(1,0,0) = 0 \quad f(1,0,1) = 0 \quad f(1,1,0) = 1 \quad f(1,1,1) = 0$$

f ist ein Element aus $\mathcal{B}_3$

Die Funktion $g : \{0,1\}^3 \rightarrow \{0,1\}$ sei definiert durch:

$$g(0,0,0) = 1 \quad g(0,0,1) = 0 \quad g(0,1,0) = 0 \quad g(0,1,1) = 1$$
$$g(1,0,0) = 1 \quad g(1,0,1) = 1 \quad g(1,1,0) = 0 \quad g(1,1,1) = 0$$

g ist ein Element aus $\mathcal{B}_3$

Nullelement, Einselement ?

2. Mengenlehre

2.4 Boolesche Algebren: Weitere Beispiele

2. Teiler-Algebra

$T_n = \{m \in \mathbb{N}: m \text{ teilt } n\}$ für ein festes $n \in \mathbb{N}$,

(*) für das die Primzahlzerlegung keine mehrfachen Primfaktoren enthält

$\sim p = n / p$

$p \oplus q = ggt(p,q)$

$p \odot q = kgv(p,q)$

Beispiel: $T_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

Nullelement, Einselement ?

Was passiert, wenn (*) verletzt ist?

Beispiel 2.25

Sei $n = 24 = 2 \cdot 2 \cdot 2 \cdot 3$ eine Zahl, die 2 als mehrfachen Primfaktor enthält.

$\mathcal{T}_{24}$ ist keine Boolesche Algebra, weil die Gesetze für inverse Elemente verletzt sind, wie man am Beispiel $p = 4$ ($\sim p = 6$) leicht sehen kann:

$p \otimes \sim p =$	$4 \otimes 6 =$	$\mathrm{kgV}(4,6) =$	$12 \neq 24$	ergibt nicht das Nullelement
$p \oplus \sim p =$	$4 \oplus 6 =$	$\mathrm{ggT}(4,6) =$	$2 \neq 1$	ergibt nicht das Einselement

Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kapitel 3: Beweisverfahren

Referenzen zum Nacharbeiten:

Iwanowski/Lang 3
Meinel 3, 6, 7
Beutelspacher 3 (als unterhaltsame Ergänzung: Beutelspacher 1, 2)
Steger 0.3

3. Beweisverfahren

3.1 Kernstrukturen der Mathematik

- **Voraussetzungen: Axiome**

  Axiome sind Forderungen, die nicht bewiesen werden müssen.
  Sie sind implizite (d.h. häufig nicht erwähnte) Voraussetzungen vieler Aussagen.

- **Benennungen: Definitionen**

  Definitionen sind vereinfachende Schreibweisen. Sie sind keine Aussagen oder Axiome, d.h. weder zu fordern noch zu beweisen.

- **Aussagen: Satz, Lemma, Korollar**

  Sätze, Lemmata oder Korollare sind wahre Aussagen.
  Ob es sich bei einem Sachverhalt um eine Aussage handelt (und nicht um eine Definition oder ein Axiom), ist meistens leicht einzusehen.
  Schwieriger ist es zu beweisen, ob es sich um eine wahre Aussage handelt.

- **Beweise**

  Kette von logischen Schlussfolgerungen, um die Wahrheit einer Aussage, ausgehend von einer Behauptung (häufig in Form von Axiomen) zu belegen.

3. Beweisverfahren

3.1 Kernstrukturen der Mathematik

Das Axiomensystem von Peano für die natürlichen Zahlen:

Gegeben sei eine Menge $\mathbb{N}$ und eine Nachfolgerelation $\sigma \subset \mathbb{N} \times \mathbb{N}$

1) $0 \in \mathbb{N}$
2) Die Nachfolgerelation ist eine Funktion.
3) Die Nachfolgerelation ist injektiv.
4) 0 ist nicht Nachfolger einer natürlichen Zahl.
5) Mit einer endlich oft hintereinandergeschalteten Anwendung der Nachfolgerelation auf 0 kann man *jedes* Element von $\mathbb{N}$ erzeugen.

Satz: Das Axiomensystem von Peano ist minimal.

Die Wegnahme eines einzigen Axioms lässt auch andere Strukturen zu,
welche alle anderen Axiome erfüllen, aber nicht als Repräsentation von $\mathbb{N}$ gewünscht sind.

3. Beweisverfahren

3.2 Vollständige Induktion

Die vollständige Induktion ist ein systematisches Beweisverfahren, welches in der Informatik häufige Verwendung findet.

Grundprinzip (einfachste Variante):

Zu beweisen ist eine Aussage der Form A(n) für ein beliebiges $n \in \mathbb{N}$

1) **Induktionsverankerung:** Beweise: Es gilt A (0)
2) **Induktionsschluss:** Beweise: Aus A (n) folgt A (n+1)

Der Beweis soll die Gültigkeit für A (n) nicht zeigen, sondern voraussetzen.
Zu zeigen ist nur die Gültigkeit von A (n+1).

Der Induktionsschluss muss für wirklich alle n ≥ 0 gelten (keine Einschränkungen!)

Beispiele: siehe Übungsaufgaben

Eigene Übung macht den Meister !

3. Beweisverfahren

3.2 Vollständige Induktion

Verallgemeinertes Grundprinzip:

Zu beweisen ist eine Aussage der Form A(n) für ein beliebiges $n \in \mathbb{N}$

1) Induktionsverankerung: Beweise: Es gilt A (0)

2) Induktionsschluss: Beweise: Aus A (0), ..., A(n) folgt A (n+1)

Anwendungsbeispiele:

1) Primzahlzerlegung (Existenz):

   Jede natürliche Zahl n > 1 kann in ein Produkt $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ zerlegt werden, wobei alle p_i Primzahlen sind. (Beweis durch Induktion über n)

2) Teilbarkeitsnachweis über Quersummenbildung

   Jede natürliche Zahl n ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist. (Beweis durch Induktion über n)

3. Beweisverfahren

3.2 Vollständige Induktion

Induktive Definition für Funktionen $\mathbb{N} \to \mathbb{N}$:

Die Funktion wird in 2 Schritten definiert:

i. Die Funktion wird für eine konstante natürliche Zahl definiert (in der Regel 0 oder 1).

ii. Es wird eine Regel angegeben, wie man aus dem Funktionswert des Vorgängers den Funktionswert des Nachfolgers konstruiert

Beispiele:

1) Fakultät $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$

   i) $0! = 1$
   ii) $n! = n \cdot (n-1)!$

2) Fibonaccizahlen F_n

   i) $F_0 = 0 \quad F_1 = 1$
   ii) $F_n = F_{n-1} + F_{n-2}$

3. Beweisverfahren

3.2 Vollständige Induktion

Verallgemeinerung: Rekursive Definitionen für beliebige Mengen:

Die Menge wird in 2 Schritten definiert:

i. Einige Elemente werden explizit angegeben (*terminale Elemente*)

ii. Es werden Regeln angegeben, wie man neue Elemente aus alten Elementen erzeugen kann (*Rekursionsregeln*).

Beispiele:

1) Grammatikdefinitionen über endlichen Alphabeten

   i) Einige konkrete Wörter werden direkt definiert (Konstante aus Terminalsymbolen).
   ii) Produktionsregeln geben an, wie man aus vorhandenen Wörtern der Grammatik neue Wörter bilden kann.

2) Backus-Naur-Formen für Syntax von Programmiersprachen (wird in anderen Vorlesungen näher besprochen)

3. Beweisverfahren

3.2 Vollständige Induktion

Anwendungen in der Geometrie und Graphentheorie

Beispiel: Färbung von Landkarten

Definitionen:

Eine **Landkarte** ist eine Unterteilung eines zweidimensionalen Gebiets in Zellen (den Ländern), die von eindimensionalen Kurven (den Grenzen) begrenzt werden.
Länder können auch ins Unendliche offen sein.

Eine **zulässige Färbung** einer Landkarte ist eine Zuweisung von Farben an jedes Land der Landkarte derart, dass benachbarte Länder (solche mit einer gemeinsamen Grenze, einzelne Grenzpunkte zählen nicht) unterschiedliche Farben haben.

Satz:

Für jede Landkarte, die dadurch entsteht, dass n Geraden (Kreise) beliebig in eine Ebene gezeichnet werden, existiert eine zulässige Färbung mit 2 Farben.

Beweis: Beutelspacher, Kap. 3.3 (für Geraden)

3. Beweisverfahren

3.3 Beweisstrategien

Direkter Beweis

$(p \rightarrow q) \wedge p \Rightarrow q$

Modus ponens

Beweis durch Kontraposition

$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

Kontraposition

Indirekter Beweis (Widerspruchsbeweis)

$(\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q) \Rightarrow p$

Indirekter Beweis

$(\neg p \rightarrow p) \Rightarrow p$

Widerspruchsbeweis

$(\neg p \rightarrow \bot) \Rightarrow p$

Widerspruchsbeweis

3. Beweisverfahren

3.3 Beweisstrategien

Äquivalenzbeweis

$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

Ersetzen der Äquivalenz durch Implikationen

Beweis durch Fallunterscheidung

$((p_1 \vee p_2) \rightarrow p) \wedge (p_1 \vee p_2) \Rightarrow p$

Fallunterscheidung für 2 Fälle

analog: Fallunterscheidung für mehr als zwei Fälle

Abzählbeweis (Schubfachprinzip, Taubenschlagverfahren)

Gegeben **f: M → N,** wobei **M,N** endlich sind

Dann gilt: **|M| > |N| ⇒ f** ist nicht injektiv

Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kap. 4: Zahlentheorie

Referenzen zum Nacharbeiten:

Iwanowski/Lang 4
Beutelspacher 5
Steger 3

4. Zahlentheorie

In diesem Kapitel repräsentieren die Variablen aller Definitionen und Sätze (Regeln), wenn nicht anders spezifiziert, ***ganze*** *Zahlen (Elemente von $\mathbb{Z}$). Fast alle Definitionen und Sätze können auch auf $\mathbb{N}$ beschränkt werden.*

4.1 Teilbarkeit

Definition von Teilbarkeit

Eine ganze Zahl m ≠ 0 ***teilt*** eine ganze Zahl n, wenn es eine ganze Zahl q gibt mit: n = q·m

$(\forall\, m, n \in \mathbb{Z}: m \mid n :\Leftrightarrow \exists q \in \mathbb{Z}: n = q \cdot m)$

Teilbarkeitssätze über Summen, Differenzen und Produkte

1) $m \mid n_1 \wedge m \mid n_2 \Rightarrow m \mid (n_1 + n_2)$

2) $m \mid n_1 \wedge m \mid n_2 \Rightarrow m \mid (n_1 - n_2)$

3) $m \mid n_1 \Rightarrow m \mid (n_1 \cdot n_2)$

4. Zahlentheorie

4.1 Teilbarkeit

Größenbeschränkungen für Teiler und Vielfache

1) Sei $n \neq 0$: Für jeden echten Teiler $m \neq 1,n,-n$ von n gilt: $m \leq |\, n / 2 \,|$

2) Für zwei Teiler p,q von n mit $p \cdot q = n$ gilt: $(p \leq \sqrt{|n|}) \vee (q \leq \sqrt{|n|})$

3) Die einzigen Vielfachen n von m mit $|\, n \,| \leq |\, m \,|$ sind $-m$, 0 und m

4. Zahlentheorie

4.1 Teilbarkeit

Zahlendarstellungen mit Hilfe von Zahlenbasen

$n = \pm (a_i \cdot b^i + a_{i-1} \cdot b^{i-1} + \ldots + a_0 \cdot b^0)$ wobei $\forall j \in \{0,\ldots,i\}: a_j \in \{0,1,\ldots,b-1\}$

Kurzdarstellung: $n = \pm [a_i\ a_{i-1}\ \ldots\ a_0]_b$

Dezimale Darstellung: $b = 10$

Binäre Darstellung: $b = 2$

Definition der Quersumme $Q_b(n)$ in Abhängigkeit von der Zahlenbasis b:

Es sei $n = \pm [a_i\ a_{i-1}\ \ldots\ a_0]_b$ $Q_b(n) := a_i + a_{i-1} + \ldots + a_0$

Quersummenregeln

$3 \mid n \Leftrightarrow 3 \mid Q_{10}(n)$

$9 \mid n \Leftrightarrow 9 \mid Q_{10}(n)$

Allgemein: Für alle Teiler t von b-1 gilt:

$t \mid n \Leftrightarrow t \mid Q_b(n)$

Für die *binäre* Quersumme gibt das keine hilfreiche Quersummenregel.

4. Zahlentheorie

4.1 Teilbarkeit

Definition von ggT und kgV

$a = ggT(m,n) :\Leftrightarrow (a \mid m) \wedge (a \mid n) \wedge [(b \mid m) \wedge (b \mid n) \Rightarrow (b \leq a)]$

$a = kgV(m,n) :\Leftrightarrow (m \mid a) \wedge (n \mid a) \wedge (a > 0) \wedge [(m \mid b) \wedge (n \mid b) \wedge (b \neq 0) \Rightarrow (a \leq |b|)]$

Zusammenhang zwischen ggT und kgV

$\forall\, m,n \in \mathbb{N}\setminus\{0\}: \qquad ggT(m,n) \cdot kgV(m,n) = m \cdot n$

Teilbarkeitsregel für teilerfremde Zahlen

Definition: Zwei ganze Zahlen m,n heißen teilerfremd $:\Leftrightarrow ggT(m,n) = 1$

Satz: Für zwei teilerfremde Zahlen m,n und eine ganze Zahl a gilt :
$m \mid a \wedge n \mid a \Rightarrow m \cdot n \mid a$

4. Zahlentheorie

4.2 Teilen mit Rest

Definition von ganzzahligem Quotienten und Rest

(1) Sei $n = q \cdot m + r$ für ganze Zahlen n,m,q,r, $0 \leq r < |m|$

Dann ist q der ganzzahlige Quotient von n geteilt durch m ($q = n \text{ DIV } m$)

Dann ist r der ganzzahlige Rest von n geteilt durch m ($r = n \text{ MOD } m$)

Eindeutigkeit und Existenz von ganzzahligem Quotienten und Rest

Für beliebige zwei ganze Zahlen n und $m \neq 0$ gibt es die Darstellung (1)

Die Darstellung (1) ist eindeutig,
d.h. q und r sind zu gegebenen n,m eindeutig bestimmt.

4. Zahlentheorie

4.2 Teilen mit Rest

Euklidischer Algorithmus zur Bestimmung von ggT und kgV

Satz: Sei $n = q \cdot m + r$ für ganze Zahlen n,m,q,r, $0 \leq r < m$

Dann gilt: $ggT(n,m) = ggT(m,r)$

Seien $n,m > 0$:

Algorithmus:

1) Berechne q und r für n und m

2) Falls r = 0: Setze ggT := m, fertig!
   Anderenfalls: Setze n := m und m := r und gehe zu 1)

Was machen wir, wenn n oder m negativ sind?

4. Zahlentheorie

4.3 Primzahlen

In diesem Abschnitt repräsentieren die Variablen aller Definitionen und Sätze (Regeln), wenn nicht anders spezifiziert, ***natürliche*** *Zahlen (Elemente von $\mathbb{N}$).*

Definition

Eine natürliche Zahl p > 1 heißt Primzahl, wenn p und 1 die einzigen Teiler von p sind
(p heißt Primzahl :⇔ $(p \in \mathbb{N}) \wedge (p > 1) \wedge (((n \in \mathbb{N}) \wedge (n \mid p)) \Rightarrow ((n = 1) \vee (n = p)))$)

Bestimmung von Primzahlen: Sieb des Eratosthenes

1) Füge alle Zahlen von 2 bis n in das Sieb ein.
2) Setze p := 2.
3) Solange $p \leq \sqrt{n}$, führe folgende Aktionen aus:
   a) Streiche alle Zahlen durch, die Vielfache von p sind.
   b) Setze p gleich der nächsten nicht durchgestrichenen Zahl.

Behauptung: Am Ende enthält das Sieb alle Primzahlen zwischen 2 und n.

4. Zahlentheorie

4.3 Primzahlen

- Das Sieb des Eratosthenes ist nicht effizient für große Zahlen.
- Es gibt effizientere Verfahren zur Primzahl**bestimmung**.
- Es sind keine effizienteren Verfahren zur **allgemeinen** Primfaktor**zerlegung** bekannt.
- Kryptographische Verfahren verwenden Produkte riesiger Primzahlen
  und halten ihre Zerlegung geheim.
- Sicher sind nur Faktoren mit mehr als 2000 bits (ab 2023: 3000)

Anzahl von Primzahlen: Relevant für die Suche nach sicheren Faktoren

1) Es gibt unendlich viele Primzahlen.

2) Die Primzahlen sind im Durchschnitt fast gleich verteilt:
   Jede ln (n) – te Zahl bis n ist im Durchschnitt eine Primzahl.

4. Zahlentheorie

4.3 Primzahlen

Hauptsatz der elementaren Zahlentheorie:
Existenz und Eindeutigkeit der Primzahlzerlegung

Jede natürliche Zahl n > 1 lässt sich als Produkt von Primzahlpotenzen darstellen:

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$$

Die Primzahlen dieser Darstellung und die Exponenten (d.h. die Häufigkeit ihres Auftretens) sind eindeutig, d.h. die Darstellung als Produkt von Primzahlpotenzen ist bis auf die Reihenfolge eindeutig.

4. Zahlentheorie

4.3 Primzahlen

Anwendungen des Hauptsatzes

Charakterisierung und Bestimmung vom ggT und kgV:

Seien $m = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_s^{m_s}$ und $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$

$$ggT(m,n) = p_1^{\min\{m_1,n_1\}} \cdot p_2^{\min\{m_2,n_2\}} \cdot \ldots \cdot p_s^{\min\{m_s,n_s\}}$$

$$kgV(m,n) = p_1^{\max\{m_1,n_1\}} \cdot p_2^{\max\{m_2,n_2\}} \cdot \ldots \cdot p_s^{\max\{m_s,n_s\}}$$

Daraus ergibt sich die Schulmethode zur Bestimmung von ggT und kgV über die Primzahlzerlegung.

Aus Folie DM4-5:

Beweis des Zusammenhangs zwischen ggT und kgV

Charakterisierung von teilerfremden Zahlen

Beweis der Teilbarkeitsregel für teilerfremde Zahlen

4. Zahlentheorie

4.4 Modulare Arithmetik

Definition einer Restklasse modulo n

Sei $a \in \mathbb{Z}$:

Die Menge $[a]_n := \{b \in \mathbb{Z}: b \bmod n = a \bmod n\}$ heißt *Restklasse* von a modulo n

Eigenschaften von Restklassen:

Die Definition von solchen Restklassen induziert eine Äquivalenzrelation auf $\mathbb{Z}$.

Die Restklassen sind die Äquivalenzklassen bzgl. dieser Äquivalenzrelation.

Mit $\mathbb{Z}_n$ wird die Menge der Restklassen modulo n bezeichnet.

$\mathbb{Z}_n = \{ [0]_n , [1]_n , ... , [n-1]_n \}$ ($\mathbb{Z}_n$ besteht also aus genau n Elementen)

4. Zahlentheorie

4.4 Modulare Arithmetik

Rechnen mit Restklassen

Addition: $[a]_n + [b]_n := [a+b]_n$

Multiplikation: $[a]_n \cdot [b]_n := [a \cdot b]_n$

Satz: Addition und Multiplikation sind wohldefiniert.

Definition von neutralen und inversen Elementen bzgl. Verknüpfungen:

Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Funktion f: M x M $\rightarrow$ M mit f (a,b) = a $\circ$ b

e heißt *neutrales Element* bzgl. einer Verknüpfung $\circ$, wenn $\forall m \in M$: $e \circ m = m \circ e = m$

m^{-1} heißt *inverses Element* von m bzgl. einer Verknüpfung $\circ$, wenn $m^{-1} \circ m = m \circ m^{-1} = e$

Anm.: Bei nichtkommutativen Verknüpfungen unterscheidet man zwischen links- und rechtsneutralen Elementen sowie zwischen links- und rechtsinversen Elementen.

4. Zahlentheorie

4.4 Modulare Arithmetik

Neutrale und inverse Elemente von Restklassen

$[0]_n$ ist das neutrale Element der Addition: $\forall a \in \mathbb{Z}: [0]_n + [a]_n = [a]_n + [0]_n = [a]_n$

$[n-a]_n$ ist das inverse Element von $[a]_n$ der Addition: $\forall a \in \mathbb{Z}: [n-a]_n + [a]_n = [a]_n + [n-a]_n = [0]_n$

$[1]_n$ ist das neutrale Element der Multiplikation: $\forall a \in \mathbb{Z}: [1]_n \cdot [a]_n = [a]_n \cdot [1]_n = [a]_n$

Ein inverses Element von $[a]_n$ der Multiplikation existiert nicht immer!

Satz: Ein inverses Element von $[a]_n$ der Multiplikation existiert genau dann, wenn a und n teilerfremd sind.

Korollar: Ein inverses Element von $[a]_n$ der Multiplikation existiert für alle $a \neq 0$, wenn n eine Primzahl ist.

4. Zahlentheorie

4.4 Modulare Arithmetik

Beispiele für das Rechnen in Restklassen:

$\mathbb{Z}_2$

$\oplus$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\mathbb{Z}_5$

$\oplus$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

$\odot$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

$\mathbb{Z}_6$

$\oplus$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

$\odot$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kap. 5: Algebraische Strukturen

Referenzen zum Nacharbeiten:

Iwanowski / Lang 5
Steger 5
Biggs 20, 22, 23
Kurzweil (deutschsprachige Vertiefung, insb. für Endliche Körper)
Hachenberger 10 (Vertiefung für Polynome)

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Definition der Struktur einer Gruppe:

Sei G eine nichtleere Menge und $\oplus$ eine Verknüpfung zwischen den Elementen von G.
Dann heißt die Struktur (G, $\oplus$) eine **abelsche Gruppe**, wenn folgende Eigenschaften erfüllt sind:

1) $\forall\ a,b \in G: a \oplus b \in G$ — ***innere Verknüpfung***

2) $\forall\ a,b,c \in G: (a \oplus b) \oplus c = a \oplus (b \oplus c)$ — ***Assoziativgesetz***

3) $\exists\ e \in G\ \forall\ a \in G: e \oplus a = a \oplus e = a$ — ***Neutrales Element***

4) $\forall\ a \in G\ \exists\ a^{-1} \in G: a^{-1} \oplus a = a \oplus a^{-1} = e$ — ***Inverses Element***

5) $\forall\ a,b \in G: a \oplus b = b \oplus a$ — ***Kommutativgesetz***

nur Eigenschaft 1):	Gruppoid
nur Eigenschaft 1), 2):	Halbgruppe
nur Eigenschaft 1), 2), 3), 4):	Gruppe

Vorbilder: $(\mathbb{Z},+)$ für eine unendliche Gruppe $(\mathbb{Z}_n,+)$ für eine endliche Gruppe

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für oder gegen unendliche Gruppen bzw. Unterstrukturen:

1) $(\mathbb{N},+)$
2) $(\mathbb{Z},+)$
3) $(\mathbb{Z},\cdot)$
4) $(\mathbb{Q},+)$
5) $(\mathbb{Q},\cdot)$
6) $(\mathbb{Q} \setminus \{0\},\cdot)$
7) $(\mathbb{Q}^+,\cdot)$
8) $(\mathbb{R} \setminus \{0\},\cdot)$
9) $(\mathbb{R} \setminus \{0\},+)$
10) $(\{f: \mathbb{R}\to\mathbb{R}\},+)$
11) $(\{f: \mathbb{R}\to\mathbb{R}\},\cdot)$
12) $(\{f: \mathbb{R} \setminus \{0\} \to\mathbb{R} \setminus \{0\}\},\cdot)$
13) $(\{f: \mathbb{R}^+ \to\mathbb{R}^+\},\cdot)$
14) $(\{f: \mathbb{R} \to\mathbb{R}\},\circ)$
15) $(\{f: \mathbb{R} \to\mathbb{R}$, f bijektiv$\},\circ)$
16) $(\{f: \mathbb{R} \to\mathbb{R}$, f differenzierbar$\},\circ)$
17) $(\{f: \mathbb{R} \to\mathbb{R}$, f bijektiv und differenzierbar$\},\circ)$
18) $(\{f: \mathbb{R} \to\mathbb{R}$, f linear$\},\circ)$
19) $(\{f: \mathbb{R} \to\mathbb{R}$, f linear$\},+)$
20) $(\{f: \mathbb{R} \to\mathbb{R}$, f Polynomfunktion$\},+)$

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

1) $(\mathbb{Z}_n,+)$ *(zyklische Gruppe mit additiver Verknüpfung)*

2) $(\mathbb{Z}_n,\cdot)$

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

4) $(\mathbb{Z}_n^*,\cdot)$ *(multiplikative Gruppe der zu n teilerfremden Restklassen,* ***prime Restklassengruppe mod n****))*

$$\mathbb{Z}_n^* = \{ [a]_n : ggT(a,n) = 1\}$$

$(\mathbb{Z}_8^*, \odot)$:

$\odot$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

$(\mathbb{Z}_{10}^*, \odot)$:

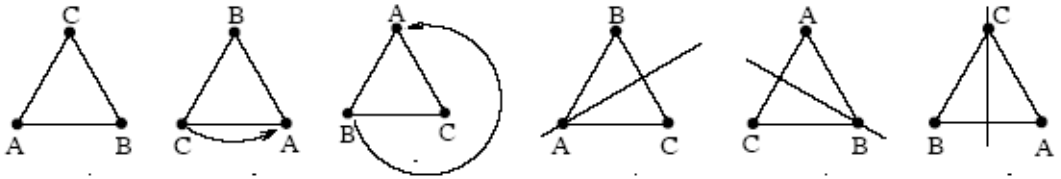
$\odot$	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_{10}$
$[1]_{10}$	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_{10}$
$[3]_{10}$	$[3]_{10}$	$[9]_{10}$	$[1]_{10}$	$[7]_{10}$
$[7]_{10}$	$[7]_{10}$	$[1]_{10}$	$[9]_{10}$	$[3]_{10}$
$[9]_{10}$	$[9]_{10}$	$[7]_{10}$	$[3]_{10}$	$[1]_{10}$

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

5) Symmetriegruppe eines gleichseitigen Dreiecks



$(S_3, \circ)$:

$\circ$	ρ_0	ρ_1	ρ_2	σ_l	σ_r	σ_o
ρ_0	ρ_0	ρ_1	ρ_2	σ_l	σ_r	σ_o
ρ_1	ρ_1	ρ_2	ρ_0	σ_o	σ_l	σ_r
ρ_2	ρ_2	ρ_0	ρ_1	σ_r	σ_o	σ_l
σ_l	σ_l	σ_r	σ_o	ρ_0	ρ_1	ρ_2
σ_r	σ_r	σ_o	σ_l	ρ_2	ρ_0	ρ_1
σ_o	σ_o	σ_l	σ_r	ρ_1	ρ_2	ρ_0

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

6) ($\{x, \frac{1}{x}, 1-x, \frac{x-1}{x}, \frac{1}{1-x}, \frac{x}{x-1}\}$,$\circ$) (Hintereinanderschaltung der Funktionen)

$(\mathbb{Q}_6, \circ)$:

$\circ$	x	$\frac{1}{x}$	$1-x$	$\frac{x-1}{x}$	$\frac{1}{1-x}$	$\frac{x}{x-1}$
x	x	$\frac{1}{x}$	$1-x$	$\frac{x-1}{x}$	$\frac{1}{1-x}$	$\frac{x}{x-1}$
$\frac{1}{x}$	$\frac{1}{x}$	x	$\frac{1}{1-x}$	$\frac{x}{x-1}$	$1-x$	$\frac{x-1}{x}$
$1-x$	$1-x$	$\frac{x-1}{x}$	x	$\frac{1}{x}$	$\frac{x}{x-1}$	$\frac{1}{1-x}$
$\frac{x-1}{x}$	$\frac{x-1}{x}$	$1-x$	$\frac{x}{x-1}$	$\frac{1}{1-x}$	x	$\frac{1}{x}$
$\frac{1}{1-x}$	$\frac{1}{1-x}$	$\frac{x}{x-1}$	$\frac{1}{x}$	x	$\frac{x-1}{x}$	$1-x$
$\frac{x}{x-1}$	$\frac{x}{x-1}$	$\frac{1}{1-x}$	$\frac{x-1}{x}$	$1-x$	$\frac{1}{x}$	x

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

7) $(\mathbb{Z}_n \times \mathbb{Z}_n, +)$ *(2-dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*

$\oplus_2$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

$\mathbb{Z}_3^2$:

$\oplus_3$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$	$(2,1)$	$(2,2)$	$(2,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$	$(2,2)$	$(2,0)$	$(2,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(2,1)$	$(2,2)$	$(2,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(2,2)$	$(2,0)$	$(2,1)$	$(0,2)$	$(0,0)$	$(0,1)$
$(2,0)$	$(2,0)$	$(2,1)$	$(2,2)$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(2,1)$	$(2,1)$	$(2,2)$	$(2,0)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(2,2)$	$(2,2)$	$(2,0)$	$(2,1)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Beispiele für endliche Gruppen bzw. Halbgruppen:

8) $((\mathbb{Z}_n)^r,+)$ *(r-dimensionale zyklische Gruppe mit koordinatenweise additiver Verknüpfung)*

$\mathbb{Z}_2^3$:

$\oplus_2$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,0)$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,1)$	$(0,0,1)$	$(0,0,0)$	$(0,1,1)$	$(0,1,0)$	$(1,0,1)$	$(1,0,0)$	$(1,1,1)$	$(1,1,0)$
$(0,1,0)$	$(0,1,0)$	$(0,1,1)$	$(0,0,0)$	$(0,0,1)$	$(1,1,0)$	$(1,1,1)$	$(1,0,0)$	$(1,0,1)$
$(0,1,1)$	$(0,1,1)$	$(0,1,0)$	$(0,0,1)$	$(0,0,0)$	$(1,1,1)$	$(1,1,0)$	$(1,0,1)$	$(1,0,0)$
$(1,0,0)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$
$(1,0,1)$	$(1,0,1)$	$(1,0,0)$	$(1,1,1)$	$(1,1,0)$	$(0,0,1)$	$(0,0,0)$	$(0,1,1)$	$(0,1,0)$
$(1,1,0)$	$(1,1,0)$	$(1,1,1)$	$(1,0,0)$	$(1,0,1)$	$(0,1,0)$	$(0,1,1)$	$(0,0,0)$	$(0,0,1)$
$(1,1,1)$	$(1,1,1)$	$(1,1,0)$	$(1,0,1)$	$(1,0,0)$	$(0,1,1)$	$(0,1,0)$	$(0,0,1)$	$(0,0,0)$

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Wann gelten zwei Gruppen als gleich?

Definition: Zwei Gruppen $(G,\oplus)$ und $(H,\odot)$ gelten als gleich (isomorph), wenn es zwischen ihnen eine bijektive Abbildung $I: G \to H$ gibt, welche die Verküpfungsstruktur erhält:

$$\forall\, a,b \in G: I(a \oplus b) = I(a) \odot I(b)$$

$$\forall\, a,b \in H: I^{-1}(a \odot b) = I^{-1}(a) \oplus I^{-1}(b)$$

I wird ***Isomorphismus*** genannt.

Charakteristische Größen endlicher Gruppen:

Ordnung eines Elements: Für $a \in G$ und $m,m' \in \mathbb{N}$ sei $o(a) = m \;:\Leftrightarrow\; (a^m = e \wedge (a^{m'} = e \Rightarrow m' \geq m))$

Ordnung einer Gruppe: maximale Ordnung ihrer Elemente

Erzeugnis eines Elements $a \in G$: $\{a^1, a^2, ..., a^{o(a)}\}$ (bildet eine Untergruppe)

Definition: Gruppen, die durch ***ein*** Element erzeugt werden, heißen ***zyklisch***. **Bsp.:** $(\mathbb{Z}_n,+)$

Erzeugnis zweier Elemente $a,b \in G$: $\{c \in G \mid c = a^i \oplus b^j, i=1, ..., o(a), j=1, ..., o(b))\}$
(bildet eine Untergruppe)

Analog: Erzeugnis mehrerer Elemente

5. Algebraische Strukturen für Zahlenmengen

5.1 Gruppen

Charakteristische Invarianten endlicher Gruppen:

Satz: Jede endliche Gruppe wird durch endlich viele Elemente erzeugt.

Bemerkung: Auch unendliche Gruppen können durch endlich viele Elemente erzeugt werden (aber niemals durch ein einzelnes).

Satz: Jeder Isomorphismus bildet Elemente aufeinander ab, die dieselbe Ordnung haben.

Satz: Erzeugende Elemente werden auf erzeugende Elemente abgebildet.

Korollar: Isomorphe Gruppen enthalten für jede Ordnungszahl dieselbe Anzahl von Elementen mit dieser Ordnung.

Korollar: Isomorphe Gruppen werden durch dieselbe Zahl von Elementen erzeugt:
Die Abbildung der erzeugenden Elemente legt den Rest der Abbildung fest.

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Definition der Struktur eines Körpers:

Sei K eine nichtleere Menge und $\oplus$, $\odot$ Verknüpfungen zwischen den Elementen von K.
Dann heißt die Struktur (K, $\oplus$, $\odot$) ein **Körper**, wenn folgende Eigenschaften erfüllt sind:

1) (K, $\oplus$) ist abelsche Gruppe mit neutralem Element e_0

2) (K, $\odot$) ist Halbgruppe

3) $\forall\ a,b,c \in K: (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$
$c \odot (a \oplus b) = (c \odot a) \oplus (c \odot b)$ ***Distributivgesetze***

4) $\exists\ e_1 \in K\ \forall\ a \in K: e_1 \odot a = a \odot e_1 = a$ ***Neutrales Element***

5) $\forall\ a \in K \setminus \{e_0\}\ \exists\ a^{-1} \in K \setminus \{e_0\}: a^{-1} \odot a = a \odot a^{-1} = e_1$ ***Inverses Element***

6) $\forall\ a,b \in K: a \odot b = b \odot a$ ***Kommutativgesetz***

nur Eigenschaft 1), 2), 3) (bei Lang auch 4), 6)): Ring
nur Eigenschaft 1), 2), 3), 4), 6) + Nullteilerfreiheit: Integritätsbereich
nur Eigenschaft 1), 2), 3), 4), 5): Schiefkörper

Vorbilder: $(\mathbb{Q},+,\cdot)$ für einen unendlichen Körper $(\mathbb{Z}_2,+,\cdot)$ für einen endlichen Körper

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Beispiele von unendlichen Körpern, Ringen, etc.:

1) $(\mathbb{Z},+,\cdot)$
2) $(\mathbb{Q},+,\cdot)$
3) $(\mathbb{R} \setminus \{0\},+,\cdot)$
4) $(\{f: \mathbb{R}\to\mathbb{R}\},+,\cdot)$
5) $(\{f: \mathbb{R}\to\mathbb{R}$, f bijektiv$\},+,\circ)$
6) $(\{f: \mathbb{R}\to\mathbb{R}$, f bijektiv$\},\circ,+)$
7) $(\{f: \mathbb{R}\to\mathbb{R}$, f linear$\},+,\cdot)$
8) $(\{f: \mathbb{R}\to\mathbb{R}$, f Polynomfunktion$\},+,\cdot)$

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p,+,\cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r,+,\cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Satz (Galois, 1811-1832): ***Das sind alle!***

Endliche Körper gibt es nur mit p^r Elementen (p Primzahl, r natürliche Zahl).
Jeder endliche Körper ist bis auf Isomorphie gleich zu den oben genannten.
Der Körper mit q Elementen wird GF (q) genannt (GF = Galoisfeld)

Wie sieht die multiplikative Verknüpfung für r > 1 aus ?

Satz:

Die multiplikative Gruppe des Körpers $((\mathbb{Z}_p)^r,+,\cdot)$ ist isomorph zu $(\mathbb{Z}_{p^r-1},+)$.

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p,+,\cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r,+,\cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Bsp.: $(\mathbb{Z}_2)^3$ Additionsgruppe

$\mathbb{Z}_2^3$:

$\oplus_2$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,0)$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,1)$	$(0,0,1)$	$(0,0,0)$	$(0,1,1)$	$(0,1,0)$	$(1,0,1)$	$(1,0,0)$	$(1,1,1)$	$(1,1,0)$
$(0,1,0)$	$(0,1,0)$	$(0,1,1)$	$(0,0,0)$	$(0,0,1)$	$(1,1,0)$	$(1,1,1)$	$(1,0,0)$	$(1,0,1)$
$(0,1,1)$	$(0,1,1)$	$(0,1,0)$	$(0,0,1)$	$(0,0,0)$	$(1,1,1)$	$(1,1,0)$	$(1,0,1)$	$(1,0,0)$
$(1,0,0)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$
$(1,0,1)$	$(1,0,1)$	$(1,0,0)$	$(1,1,1)$	$(1,1,0)$	$(0,0,1)$	$(0,0,0)$	$(0,1,1)$	$(0,1,0)$
$(1,1,0)$	$(1,1,0)$	$(1,1,1)$	$(1,0,0)$	$(1,0,1)$	$(0,1,0)$	$(0,1,1)$	$(0,0,0)$	$(0,0,1)$
$(1,1,1)$	$(1,1,1)$	$(1,1,0)$	$(1,0,1)$	$(1,0,0)$	$(0,1,1)$	$(0,1,0)$	$(0,0,1)$	$(0,0,0)$

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p,+,\cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r,+,\cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Bsp.: $(\mathbb{Z}_2)^3$ Versuch mit einer zyklischen Gruppe für die Multiplikation

$\mathbb{Z}_2^3 \setminus \{(0,0,0)\}$: **(falscher Versuch)**

$\odot$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,1)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,1,0)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$	$(0,0,1)$
$(0,1,1)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$	$(0,0,1)$	$(0,1,0)$
$(1,0,0)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$
$(1,0,1)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$
$(1,1,0)$	$(1,1,0)$	$(1,1,1)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$
$(1,1,1)$	$(1,1,1)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	(1, 1, 0)

Leider ist das Distributivgesetz verletzt! ☹

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p,+,\cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r,+,\cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Bsp.: $(\mathbb{Z}_2)^3$ Erfolgreicher Versuch einer zyklischen Gruppe für die Multiplikation

$\odot_2^g$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$
$(0,0,1)$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,1,0)$	$(0,0,0)$	$(0,1,0)$	$(1,0,0)$	$(1,1,0)$	$(0,1,1)$	$(0,0,1)$	$(1,1,1)$	$(1,0,1)$
$(0,1,1)$	$(0,0,0)$	$(0,1,1)$	$(1,1,0)$	$(1,0,1)$	$(1,1,1)$	$(1,0,0)$	$(0,0,1)$	$(0,1,0)$
$(1,0,0)$	$(0,0,0)$	$(1,0,0)$	$(0,1,1)$	$(1,1,1)$	$(1,1,0)$	$(0,1,0)$	$(1,0,1)$	$(0,0,1)$
$(1,0,1)$	$(0,0,0)$	$(1,0,1)$	$(0,0,1)$	$(1,0,0)$	$(0,1,0)$	$(1,1,1)$	$(0,1,1)$	$(1,1,0)$
$(1,1,0)$	$(0,0,0)$	$(1,1,0)$	$(1,1,1)$	$(0,0,1)$	$(1,0,1)$	$(0,1,1)$	$(0,1,0)$	$(1,0,0)$
$(1,1,1)$	$(0,0,0)$	$(1,1,1)$	$(1,0,1)$	$(0,1,0)$	$(0,0,1)$	$(1,1,0)$	$(1,0,0)$	$(0,1,1)$

Wieso ist diese Gruppe zyklisch?

➔ Finde ein Element a der Ordnung 7 und sortiere die Elemente um in a, a^2, a^3, a^4, a^5, a^6, a^7=1

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Endliche Körper:

1) $(\mathbb{Z}_p,+,\cdot)$ für beliebige Primzahl p

2) $((\mathbb{Z}_p)^r,+,\cdot)$ für beliebige Primzahl p und beliebige natürliche Zahl r

Bsp.: $(\mathbb{Z}_2)^3$ Erfolgreicher Versuch einer zyklischen Gruppe für die Multiplikation

$\odot_2^3$	(0,0,0)	(0,1,0)	(1,0,0)	(0,1,1)	(1,1,0)	(1,1,1)	(1,0,1)	(0,0,1)
(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)
(0,1,0)	(0,0,0)	(1,0,0)	(0,1,1)	(1,1,0)	(1,1,1)	(1,0,1)	(0,0,1)	(0,1,0)
(1,0,0)	(0,0,0)	(0,1,1)	(1,1,0)	(1,1,1)	(1,0,1)	(0,0,1)	(0,1,0)	(1,0,0)
(0,1,1)	(0,0,0)	(1,1,0)	(1,1,1)	(1,0,1)	(0,0,1)	(0,1,0)	(1,0,0)	(0,1,1)
(1,1,0)	(0,0,0)	(1,1,1)	(1,0,1)	(0,0,1)	(0,1,0)	(1,0,0)	(0,1,1)	(1,1,0)
(1,1,1)	(0,0,0)	(1,0,1)	(0,0,1)	(0,1,0)	(1,0,0)	(0,1,1)	(1,1,0)	(1,1,1)
(1,0,1)	(0,0,0)	(0,0,1)	(0,1,0)	(1,0,0)	(0,1,1)	(1,1,0)	(1,1,1)	(1,0,1)
(0,0,1)	(0,0,0)	(0,1,0)	(1,0,0)	(0,1,1)	(1,1,0)	(1,1,1)	(1,0,1)	(0,0,1)

Wie kamen wir eigentlich auf diese Gruppe?

➔ Konstruktionsanleitung mit Hilfe von Polynomen

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Definition Polynom für einen beliebigen Körper K:

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

Hierbei steht x für eine Variable mit Definitionsbereich K, a_i für eine beliebige Konstante aus K und x^i bedeutet die i-fache Hintereinanderschaltung der multiplikativen Verknüpfung angewendet auf das Körperelement x.
Ein Polynom ist durch die Angabe des Tupels $(a_n,a_{n-1},...,a_1,a_0)$ eindeutig charakterisiert.

Das größte n mit $a_n \neq 0$ wird als *Grad des Polynoms* bezeichnet.
Die Menge der Polynome über einem Körper K wird mit K[x] bezeichnet.

Satz:

(K[x],+,·) bildet einen Ring (sogar einen Integritätsbereich).

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Weitere Definitionen:

Eine ***Nullstelle*** zu einem gegebenen Polynom ist ein Wert des Körpers K, dessen Einsetzung in das Polynom den Wert 0 ergibt.

Ein ***Polynom*** f[x] über einem Körper K heißt **reduzibel**, wenn es zwei Polynome g[x], h[x] in K[x] gibt mit f[x] = g[x]·h[x] (übliche Polynommultiplikation) und g[x], h[x] $\notin$ {1, f[x]}.
Wenn es keine solche Zerlegungsmöglichkeit gibt, heißt f[x] **irreduzibel**.

Satz: f[x] mit Grad > 1 ist irreduzibel $\Rightarrow$ f[x] hat keine Nullstelle .

Für Polynome f[x] mit Grad ≤ 3 gilt sogar: f[x] ist irreduzibel $\Leftrightarrow$ f[x] hat keine Nullstelle.

Polynomdivision mit Rest:

Seien f[x], g[x] Polynome.
Dann gibt es Polynome q[x], r[x] mit Grad (r[x]) < Grad (g[x]):

$$f[x] = q[x] \cdot g[x] + r[x]$$

Die Polynome q[x], r[x] werden analog zum schriftlichen Divisionsverfahren von Zahlen gebildet. (Euklidischer Algorithmus).
Analog zur Definition bei Zahlen wird das Restpolynom r[x] auch f[x] mod g[x] genannt.

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Konstruktionsanleitung für GF (q) mit $q = p^r$ (p Primzahl, r natürliche Zahl):

1) Bestimme die Additions- und Multiplikationstabellen von GF (p):
   Dieser *Primkörper* ist isomorph zum Restklassenkörper $(\mathbb{Z}_p,+,\cdot)$.

2) Identifiziere die Elemente aus GF (q) mit den p^r verschiedenen Polynomen über $(\mathbb{Z}_p,+,\cdot)$ mit Grad < r

3) Bilde die Additionstabelle wie bei Polynomen üblich.
   (Anmerkung: Die entstehende Gruppe ist isomorph zu $((\mathbb{Z}_p)^r,+)$)

4) Wähle ein irreduzibles Polynom g[x] über GF (p) mit Grad = r.
   Bilde die Multiplikationstabelle wie bei Polynomen üblich,
   aber *rechne modulo g[x]*, um jeweils Polynome mit Grad < r zu erzeugen.
   (Anmerkung: Die entstehende Gruppe ist isomorph zu $(\mathbb{Z}_{q-1},+)$)

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Beispiel: GF (8) $8 = 2^3$ (p =2, r=3)

Der Primkörper ist also GF(2)

Elemente: {0, 1 , x , x+1 , x^2 , x^2+1, x^2+x, x^2+x+1}

Alle Polynome mit Grad < 3

0, 1 , 2 , 3 , 4 , 5 , 6 , 7

Irreduzibles Polynom: x^3+x+1

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

5. Algebraische Strukturen für Zahlenmengen

5.2 Körper

Beispiel: GF (9) $9 = 3^2$ (p =3, r=2)

Der Primkörper ist also GF(3)

Elemente: {0, 1 , 2 , x , x+1 , x+2 , 2x , 2x+1, 2x+2}

Alle Polynome mit Grad < 2

0, 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8

Irreduzibles Polynom: x^2+1

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

·	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	2	5	8	1	4	7
4	0	4	8	5	6	1	7	2	3
5	0	5	7	8	1	3	4	6	2
6	0	6	3	1	7	4	2	8	5
7	0	7	5	4	2	6	8	3	1
8	0	8	4	7	3	2	5	1	6

Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kap.6: Kombinatorik

Referenzen zum Nacharbeiten:

Iwanowski / Lang 6
Beutelspacher 4 (außer Fixpunkte von Permutationen)
Meinel 8
Steger 1.1 – 1.3 (mit Bezug zur Schulnotation)

6. Kombinatorik

Die Kombinatorik beschäftigt sich mit der Anzahl der Elemente endlicher Strukturen.

6.1 Zählformeln für endliche Mengen

Bezeichnung der Anzahl der Elemente einer endlichen Menge M: |M|, #M

Zusammenhang zwischen den Elementzahlen von Schnittmengen, Vereinigungsmengen und den Einzelmengen:

Siebformel

$$\#(M_1 \cup M_2 \cup \ldots \cup M_k) = \#M_1 + \ldots + \#M_k - \#(M_1 \cap M_2) - \#(M_1 \cap M_3) - \ldots - \#(M_{k-1} \cap M_k) + \#(M_1 \cap M_2 \cap M_3) + \ldots + \#(M_{k-2} \cap M_{k-1} \cap M_k) - \ldots + (-1)^{k-1} \#(M_1 \cap M_2 \cap \ldots \cap M_k)$$

$$\#\left(\bigcup_{i=1}^{k} M_i\right) = \sum_{i=1}^{k} \#M_i - \sum_{\substack{i_1,i_2=1 \\ i_1<i_2}}^{k} \#(M_{i_1} \cap M_{i_2}) + \ldots + (-1)^{l-1} \sum_{\substack{i_1,i_2,\ldots,i_l=1 \\ i_1<i_2<\ldots<i_l}}^{k} \#\left(\bigcap_{j=1}^{l} M_{i_j}\right) + \ldots + (-1)^{k-1} \#\left(\bigcap_{i=1}^{k} M_i\right)$$

6. Kombinatorik

Die Kombinatorik beschäftigt sich mit der Anzahl der Elemente endlicher Strukturen.

6.1 Zählformeln für endliche Mengen

Zusammenhang zwischen den Elementzahlen von Mengen und ihrem Kreuzprodukt:

$$\#(M_1 \times M_2 \times \ldots \times M_k) = \#M_1 \cdot \ldots \cdot \#M_k$$

Anzahl der k-Tupel einer n-elementigen Menge: n^k

Anzahl der möglichen Anordnungen einer n-elementigen Menge: $n!$

(Anzahl der Permutationen)

6. Kombinatorik

Die Kombinatorik beschäftigt sich mit der Anzahl der Elemente endlicher Strukturen.

6.1 Zählformeln für endliche Mengen

Zusammenhang zwischen der Elementzahl einer Menge und der Anzahl ihrer Teilmengen:

$$\#P(M) = 2^{\#M}$$

Zusammenhang zwischen der Elementzahl n einer Menge und der Anzahl ihrer k-elementigen Teilmengen (1 ≤ k ≤ n):

$$\binom{n}{k} := \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \frac{n!}{k! \cdot (n-k)!}$$

(Binomialkoeffizient)

6. Kombinatorik

Die Kombinatorik beschäftigt sich mit der Anzahl der Elemente endlicher Strukturen.

6.1 Zählformeln für endliche Mengen

Zusammenhang zwischen Binomialkoeffizient und binomischer Formel:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot x^{n-i} \cdot y^i$$

Zusammenhang zwischen den Binomialkoeffizienten:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Pascalsches Dreieck: Rekursive Berechnung der Binomialkoeffizienten

Bilde für n = 0, 1, 2, ... nacheinander die Reihe der Binomialkoeffizienten $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$:

Verwende für jedes n die Regel $\binom{n}{0} = \binom{n}{n} = 1$

und berechne die $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ aus den $\binom{n-1}{1}, \binom{n-1}{2}, \ldots, \binom{n-1}{n-1}$ nach der rekursiven Formel

6. Kombinatorik

6.2 Permutationen

Eine n-Permutation ist eine bijektive Abbildung *f* von einer n-elementigen Menge in sich selbst:

$$f : \{1,\ldots,n\} \to \{1,...,n\} \qquad i = j \Leftrightarrow f(i) = f(j)$$

Darstellungsweise von Permutationen:

Permutationstabelle $\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ **Bsp.:** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

Anordnung $f(1)\ \ f(2)\ \ \ldots\ \ f(n)$ $7\ \ 6\ \ 5\ \ 4\ \ 1\ \ 2\ \ 3$

Zyklendarstellung (1 7 3 5) (2 6) (4) = (1 7 3 5) (2 6)

Die Zerlegung in Zyklen ist nicht eindeutig, nur die in *disjunkte* Zyklen maximaler Länge, wobei die zyklische Umstellung eines Zyklus als gleich angesehen wird.

Ein Zyklus der Länge 2 heißt *Transposition*

6. Kombinatorik

6.2 Permutationen

Hintereinanderschaltung (Komposition) von Permutationen:

$$(1\ 7\ 3\ 5)\ (2\ 6) \circ (1\ 3\ 5)\ (2\ 4\ 7\ 6) = (1\ 5\ 7\ 2\ 4\ 3)$$

- Die Komposition wird von *rechts nach links* ausgeführt.
- Das Operationssymbol ◦ kann in der Zyklendarstellung weggelassen werden,
  da die Zerlegung in disjunkte Zyklen auch als Komposition aufgefasst werden kann.

6. Kombinatorik

6.2 Permutationen

Zerlegung von Permutationen in Transpositionen:

Jede Permutation kann in eine Komposition von Transpositionen zerlegt werden:

$$(a_1 \dots a_n) = (a_1\, a_n)\,(a_1\, a_{n-1}) \dots (a_1\, a_2)$$

$$(1\ 7\ 3\ 5)\ (2\ 6) = (1\ 5)\ (1\ 3)\ (1\ 7)\ (2\ 6)$$

- Diese Zerlegung ist nicht eindeutig, ebenfalls nicht die Anzahl von Transpositionen.
  Es gilt aber immer, dass Zerlegungen für dieselbe Permutation entweder *alle* eine gerade Anzahl oder *alle* eine ungerade Anzahl von Transpositionen haben.

- Gemäß ihrer Zerlegungseigenschaft in Transpositionen
  bezeichnet man eine *Permutation* als *gerade* oder *ungerade*.

6. Kombinatorik

6.2 Permutationen

Die Permutationsgruppe S_n:

- Die Menge aller n-Permutationen bildet mit der Komposition als Verknüpfung eine Gruppe, die **symmetrische Gruppe S_n**.

- Die symmetrische Gruppe ist nicht abelsch,
  d.h. das Kommutativgesetz gilt nicht.

- Die Menge der geraden Permutationen bildet eine Untergruppe von S_n.
  Sie heißt die **alternierende Gruppe A_n**.

Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kap. 7: Graphentheorie

Referenzen zum Nacharbeiten:

Iwanowski / Lang 7
Beutelspacher 8.1-8.5
Meinel 11
Steger 2
zur Vertiefung: Aigner 6, 7 (7.4: Algorithmus von Dijkstra)
Matousek 3, 4, 5 (3.5: Algorithmus für Eulerwege)

7. Graphentheorie

7.1 Terminologie und Repräsentation

Definition:

Ein Graph (V,E) ist ein Gebilde aus Ecken (Knoten, *vertices*) und Kanten (*edges*): Eine Kante verbindet immer 2 Ecken. Diese Ecken sind die *Endpunkte* der Kante.

Darstellung in der Ebene:

- Die Ecken werden als Punkte in der Ebene markiert.
- Die Kanten sind Kurvensegmente (in der Regel Strecken), welche zwischen ihren Endpunkten verlaufen.
- Die Darstellung eines Graphen ist nicht eindeutig.

Isomorphie oder: Wann gelten 2 Graphen als gleich ?

2 Graphen gelten als gleich (äquivalent, isomorph), wenn sie aus gleich vielen Ecken und Kanten bestehen und eine bijektive Abbildung besteht, so dass die zugeordneten Ecken durch die zugeordneten Kanten miteinander verbunden sind.

7. Graphentheorie

7.1 Terminologie und Repräsentation

Weitere Begriffe:

- Kanten können gerichtet oder ungerichtet sein.
  Gerichtete Kanten werden auch ***Bögen*** (*arcs*) genannt.
  Graphen mit ausschließlich ungerichteten Kanten heißen ***ungerichtete Graphen***,
  Graphen mit gerichteten Kanten heißen ***Digraphen*** (*directed Graphs*).
- adjazente (benachbarte) Ecken
- inzidente (anliegende) Ecken und Kanten
- Schlingen, Mehrfachkanten
- Grad (Valenz) einer Ecke
- Zusammenhang, Zusammenhangskomponenten, isolierte Ecken

Einfache *(schlichte)* ***Graphen*** *haben keine Schlingen oder Mehrfachkanten.*

7. Graphentheorie

7.1 Terminologie und Repräsentation

Darstellung von Graphen im Computer:

- **Adjazenzmatrix:**
  An Position (i,j) steht eine 1, wenn die Ecken i und j durch eine Kante verbunden sind, sonst 0.

- **Adjazenzliste:**
  In Zeile i stehen die Nummern aller Ecken, die durch eine Kante mit Ecke i verbunden sind.

- **Inzidenzmatrix:**
  An Position (i,j) steht eine 1, wenn die Kante i als Endpunkt die Ecke j hat, sonst 0.
  In den Zeilen dürfen auch die Ecken und in den Spalten die Kanten stehen.

7. Graphentheorie

7.2 Wege in Graphen

Eulerwege

Definition *Eulerweg (Eulerzug)*:

Weg, der alle Kanten im Graphen genau einmal durchläuft

Definition *Eulerkreis*:

Geschlossener Eulerweg (gleiche Anfangs- und Endecke)

Definition *Eulerscher Graph*:

Graph mit einem Eulerkreis

Satz: Ein Graph ist eulersch $\Leftrightarrow$ G ist zusammenhängend
und jede Ecke hat gerade Valenz

7. Graphentheorie

7.2 Wege in Graphen

Eulerwege

Algorithmus zum Auffinden eines Eulerkreises
in einem zusammenhängenden Eulerschen Graphen:

- Beginne mit einer beliebigen Ecke v_0 und dem leeren Weg $W_0 = (v_0)$.
- Wiederhole:
  Erweitere den Weg $W_i = (v_0, e_1 , v_1 , ..., v_{i-1} , e_i , v_i)$
  zu einem Weg $W_{i+1} = (v_0, e_1 , v_1 , ..., v_{i-1} , e_i , v_i, e_{i+1} , v_{i+1})$ um eine Kante e_{i+1},
  die an der letzten Ecke v_i von W_i beginnt,
  sodass der Restgraph R_{i+1}, der aus G entsteht, indem alle Kanten aus W_{i+1}
  und alle daraufhin isolierten Ecken aus G entfernt werden,
  zusammenhängend ist und weiterhin die Ecke v_0 enthält.
  (d.h. die Wegnahme von e_{i+1} darf die Ecke v_0 nicht isolieren
  und muss die noch nicht gewählten Kanten zusammenhängend lassen)
  bis das nicht mehr möglich ist.

Satz: Der vom Algorithmus erzeugte Weg W_k enthält alle Kanten von G,
d.h. W_k ist ein Eulerkreis.

Frage: Wie prüft man nach, ob ein Graph zusammenhängend ist ?

7. Graphentheorie

7.2 Wege in Graphen

Eulerwege

Algorithmus zum Auffinden eines Eulerweges in einem zusammenhängenden Graphen mit 2 Ecken ungerader Valenz:

- Die Ecken ungerader Valenz seien v_a und v_e.
  Beginne mit der Ecke v_a und dem leeren Weg $W_0 = (v_a)$. (Nur der Beginn bei v_e wäre auch noch möglich)
- Wiederhole:
  Erweitere den Weg $W_i = (v_a, e_1 , v_1 , ..., v_{i-1} , e_i , v_i)$
  zu einem Weg $W_{i+1} = (v_a, e_1 , v_1 , ..., v_{i-1} , e_i , v_i, e_{i+1} , v_{i+1})$ um eine Kante e_{i+1},
  die an der letzten Ecke v_i von W_i beginnt,
  sodass der Restgraph R_{i+1}, der aus G entsteht, indem alle Kanten aus W_{i+1}
  und alle daraufhin isolierten Ecken aus G entfernt werden,
  zusammenhängend ist und weiterhin die Ecke v_e enthält.
  (d.h. die Wegnahme von e_{i+1} darf die Ecke v_e nicht isolieren
  und muss die noch nicht gewählten Kanten zusammenhängend lassen)
  bis das nicht mehr möglich ist.

7. Graphentheorie

7.2 Wege in Graphen

Hamiltonwege

Definition *Hamiltonweg*:

Weg, der alle Ecken im Graphen genau einmal durchläuft

Definition *Hamiltonkreis*:

Geschlossener Hamiltonweg (gleiche Anfangs- und Endecke)

Definition *Hamiltonscher Graph*:

Graph mit einem Hamiltonkreis

Problem: Es ist kein effizienter Algorithmus zum Auffinden eines Hamiltonkreises bekannt.

7. Graphentheorie

7.2 Wege in Graphen

Bewertete Graphen

Definition *Bewerteter (gewichteter, weighted) Graph*:

Graph, dessen Kanten mit Gewichten bewertet sind (den Kantenlängen)

Anmerkung: Bewertete Graphen können auch gerichtet sein.

Darstellung eines bewerteten Graphen im Computer:

- **Adjazenzmatrix:**
  An Position (i,j) steht die Kantenlänge, wenn die Ecken i und j durch eine Kante verbunden sind, sonst ∞.

- **Adjazenzliste:**
  In Zeile i stehen die Paare (Eckennummer, Kantenlänge) aller Ecken, die durch eine Kante mit Ecke i verbunden sind.

7. Graphentheorie

7.2 Wege in Graphen

Algorithmus von Dijkstra (Kürzeste Wegeberechnung)

Voraussetzung: Alle Kantenlängen müssen nichtnegativ sein.

Ziel: Es soll der Weg mit der minimalen Kantenlänge von A nach B gefunden werden.

Algorithmus:

- In der Menge **`Berechnet`** sei nur die Ecke A. Markiere A mit Weglänge 0.
  In der Menge **`Vorläufig`** sind alle anderen Ecken des Graphen.
  Markiere die Nachbarn N von A mit der Länge der Kante von A nach N
  und alle anderen Ecken mit Weglänge ∞.
- Wiederhole:
  Wähle die Ecke V aus **`Vorläufig`** mit der kleinsten Markierung
  und verschiebe sie in die Menge **`Berechnet`**.
  Betrachte alle Nachbarn N von V aus **`Vorläufig`**:
  Ersetze die Markierung von N durch das Minimum seiner bisherigen Markierung
  und der Summe der Markierung von V plus der Länge der Kante von V zu N.
  bis V = B

7. Graphentheorie

7.2 Wege in Graphen

Algorithmus von Dijkstra (Kürzeste Wegeberechnung)

Satz: Die Markierungen aller Ecken V der Menge **`Berechnet`** entsprechen der Länge des kürzesten Wegs von A nach V.

Erweiterung zur *Ausgabe* des kürzesten Wegs:

- Wiederhole:
  Wähle die Ecke V aus **`Vorläufig`** mit der kleinsten Markierung
  und verschiebe sie in die Menge **`Berechnet`**.
  Betrachte alle Nachbarn N von V aus **`Vorläufig`**:
  Ersetze die Markierung von N durch das Minimum seiner bisherigen Markierung und der Summe der Markierung von V plus der Länge der Kante von V zu N.
  Falls die Markierung aktualisiert werden muss, mache V zum **Vorgänger** von N.
  bis V = B
- Sammle nacheinander alle Vorgänger von B bis A auf
  und gib den Weg in umgekehrter Reihenfolge wieder aus.

Satz: Der Algorithmus von Dijkstra berechnet nicht nur den kürzesten Weg von A nach B, sondern auch alle kürzesten Wege von A zu allen anderen Ecken, die näher an A sind als B.

7. Graphentheorie

7.3 Bäume

Definition *Baum*:

Ein Baum ist ein zusammenhängender Graph ohne Kreise.

Definition *Wald*:

Ein Wald ist ein Graph ohne Kreise (nicht notwendig zusammenhängend)

Satz: Folgende Aussagen sind äquivalent:

- G ist ein Baum.
- G ist ein Graph ohne Kreise mit maximal vielen Kanten
  (d.h. beim Hinzufügen einer beliebigen Kante entsteht immer ein Kreis).
- G ist ein zusammenhängender Graph mit n-1 Kanten
  (wobei n die Eckenzahl des Graphen ist).
- G ist ein kreisfreier Graph mit n-1 Kanten
  (wobei n die Eckenzahl des Graphen ist).

7. Graphentheorie

7.3 Bäume

Definition *Aufspannender Baum (Gerüst)*:

Ein Aufspannender Baum (Gerüst) eines Graphen ist ein Teilgraph,
der selbst ein Baum ist und alle Ecken des ursprünglichen Graphen enthält.

Konstruktion eines aufspannenden Baums für einen beliebigen Graphen G:

- Beginne mit dem leeren Wald W, bestehend aus keiner Kante.
- Wiederhole für alle Kanten e_1, e_2, ..., e_m des Graphen G (Reihenfolge beliebig):
  Untersuche, ob e_i zu W hinzugefügt werden kann,
  sodass W weiterhin kreisfrei bleibt:
  Falls ja, füge e_i zu W hinzu.
  bis W aus n-1 Kanten besteht (n sei die Anzahl der Ecken von G).

Satz: Der so konstruierte Wald W ist ein aufspannender Baum für G.

7. Graphentheorie

7.3 Bäume

Definition *Minimaler Aufspannender Baum*:

Ein Minimaler Aufspannender Baum eines gewichteten Graphen ist ein aufspannender Baum, dessen Gesamtkantenlänge minimal ist.

Algorithmus von Kruskal:

Konstruktion eines minimalen aufspannenden Baums für ein beliebiges G:

- Beginne mit dem leeren Wald W, bestehend aus keiner Kante.
- Wiederhole für alle Kanten e_1, e_2, ..., e_m des Graphen G (Reihenfolge sortiert):
  Untersuche, ob e_i zu W hinzugefügt werden kann,
  sodass W weiterhin kreisfrei bleibt:
  Falls ja, füge e_i zu W hinzu.
  bis W aus n-1 Kanten besteht (n sei die Anzahl der Ecken von G).

Satz: Der so konstruierte Wald W ist ein minimaler aufspannender Baum für G.

7. Graphentheorie

7.3 Bäume

Definition *Wurzelbaum*:

- Ein *Wurzelbaum* ist ein Baum, in dem ein Knoten als Wurzel ausgezeichnet ist.
- Das *Niveau (Suchtiefe) eines Knotens* ist die Länge des Weges zur Wurzel.
- Die *Tiefe (Höhe) eines Wurzelbaums* ist das maximale Niveau seiner Knoten.
- Die Nachbarn eines Knoten, die auf einem größerem Niveau liegen als dieser, heißen *Kinder* dieses Knoten.
- Der (eindeutige) Nachbarn eines Knoten, der auf einem niedrigeren Niveau liegt als dieser, heißt *Elternteil* dieses Knoten.
- Ein *Blatt* ist ein Knoten ohne Kinder.

Wurzelbäume mit maximaler Kinderzahl:

- Ein binärer *Wurzelbaum* ist ein Wurzelbaum, in dem alle Knoten maximal 2 Kinder haben.
- Ein ternärer *Wurzelbaum* ist ein Wurzelbaum, in dem alle Knoten maximal 3 Kinder haben.
- Ein d-ärer *Wurzelbaum* ist ein Wurzelbaum, in dem alle Knoten maximal d Kinder haben.

Satz: Ein d-ärer Wurzelbaum mit n Blättern hat mindestens Tiefe $\log_d n$

7. Graphentheorie

7.4 Planare Graphen

Definition *Planarer Graph*:

Graph, der in der Ebene so dargestellt werden *kann*,
dass sich seine Kanten nicht überkreuzen.

(Beutelspacher nennt das plättbaren Graphen.
Planare Graphen sind bei ihm Graphen, die mit dieser Eigenschaft dargestellt *sind*.)

Definition *Gebiet (Land)*:

Ein Gebiet eines planaren Graphen zu einer *gegebenen kreuzungsfreien Darstellung in der Ebene* ist eine maximale Fläche in der Ebene,
in der je zwei Punkte durch eine Kurve verbunden werden können,
die keine Kante des Graphen schneidet.

Ein Gebiet wird häufig durch die Angabe der Begrenzungskanten charakterisiert („Nadeln“ werden mitgezählt).
Diese Charakterisierung ist nicht immer eindeutig, d.h. manche Gebiete haben dieselben Begrenzungskanten.

7. Graphentheorie

7.4 Planare Graphen

Satz: Die Charakterisierung aller Gebiete durch die Angabe der Begrenzungskanten hängt von der Darstellung des Graphen ab.

Satz: Die Anzahl der Gebiete hängt *nicht* von der Darstellung des Graphen ab:

$$n - m + g = 2$$

Eulersche Polyederformel für zusammenhängende Graphen

$$n - m + g = 1 + z$$

Eulersche Polyederformel für Graphen mit z Zusammenhangskomponenten

7. Graphentheorie

7.4 Planare Graphen

Wie erkennt man an der Struktur, dass ein Graph planar ist ?

Def.: Der ***vollständige Graph*** K_n ist der Graph mit n Ecken, die paarweise miteinander durch eine Kante verbunden sind.

Def.: Der ***vollständige bipartite Graph*** $K_{n,m}$ ist der Graph mit zwei Mengen aus n bzw. m Ecken, sodass jede Ecke der einen Menge mit jeder Ecke der anderen Menge durch eine Kante verbunden ist.

Satz: K_n ist planar genau dann, wenn $n \leq 4$.

Satz: $K_{n,m}$ ist planar genau dann, wenn $\min\{n,m\} \leq 2$.

Satz von Kuratowski:

Ein Graph ist planar genau dann, wenn er keine Unterteilung von K_5 oder $K_{3,3}$ enthält.

Def: Eine Unterteilung eines Graphen entsteht durch Einfügen von zusätzlichen Ecken in bestehende Kanten.

7. Graphentheorie

7.5 Färbungen

Def.: Eine *zulässige Färbung eines Graphen* ist die Zuweisung von Zahlen aus einer endlichen Menge (den „Farben“) an die Ecken des Graphen derart, dass zwei verschiedene benachbarte Ecken nie die gleiche Farbe haben.

Def.: Die chromatische Zahl $\chi(G)$ ist die minimale Anzahl von Farben, die notwendig sind, um G zulässig zu färben.

4-Farben-Satz:

Für jeden planaren Graphen gilt: $\chi(G) \leq 4$ (*Four colors suffice!*)

ca. 1850:	Vermutung durch britischen Mathematikstudenten Francis Guthrie
1879:	„Beweis“ durch Alfred Kempe
1890:	Finden des Fehlers im „Beweis“ von Kempe durch Percy Heawood
20. Jahrhundert:	4-Farben-Vermutung als Anstoß vieler neuer Entwicklungen in der Graphentheorie
ca. 1965:	Vorbereitung eines Computerbeweises durch H. Heesch, kein Geld für Computer
1976:	Computerbeweis durch K. Apel und W. Haken aufbauend auf Ideen von Heesch

7. Graphentheorie

7.5 Färbungen

Was hat unsere Definition von χ(G) mit Landkarten zu tun ?

Def.: Zu einem planaren Graphen G mit kreuzungsfreier Darstellung
wird der *duale Graph D* definiert als folgender Graph:
i) Ersetze jedes Gebiet von G in D durch eine Ecke
ii) Verbinde zwei Ecken in D durch eine Kante genau dann,
wenn die zugehörigen Gebiete in G durch eine Kante benachbart sind.
Hierbei wird für jede Kante einer Gebietsgrenze in G eine eigene Kante zwischen den zugehörigen Ecken in D gezogen (was unter Umständen Mehrfachkanten erzeugt).

Satz:
i) Der duale Graph zu einem planaren Graphen ist wieder planar und immer zusammenhängend.
ii) Wenn der Graph zusammenhängend ist, gilt:
Der duale Graph eines dualen Graphen ist wieder der Graph selbst.
Aus i) und ii) folgt:
Jeder planare Graph kann auch als dualer Graph aufgefasst werden. Damit ist jede Eckenfärbung eines planaren Graphen G auch die Landkartenfärbung eines anderen planaren Graphen und umgekehrt.

4-Farben-Satz:

Für jede Landkarte gilt: Sie kann mit 4 Farben immer so gefärbt werden, dass zwei durch eine eindimensionale Grenze benachbarte Länder niemals die gleiche Farbe haben.

7. Graphentheorie

7.5 Färbungen

Einige Schranken für die (ecken-) chromatische Zahl:

Definition: Ein bipartiter Graph ist ein Graph mit zwei Eckenmengen M und N, sodass die Kanten nur eine Ecke von M mit einer Ecke von N verbinden, aber es gibt keine Kanten zwischen den Ecken von M oder zwischen den Ecken von N. Jeder bipartite Graph ist also ein Subgraph von einem $K_{m,n}$ (dem vollständigen bipartiten Graph zwischen m bzw. n Ecken).

Satz: Für jeden bipartiten Graphen G gilt: $\chi(G) = 2$.

Korollar: Die Umkehrung des 4-Farben-Satzes gilt *nicht*:
Wenn $\chi(G) \leq 4$, dann könnte G trotzdem nicht planar sein.

Satz: Wenn G einen K_n als Teilgraph enthält, dann gilt: $\chi(G) \geq n$.

Achtung: Auch hier gilt *nicht* die Umkehrung:
Wenn $\chi(G) \geq n$, muss G nicht K_n als Teilgraph enthalten.

Beispiele:

i) Ein ungerader Kreis braucht immer 3 Farben, auch wenn er nicht K_3 enthält.

ii) Ein Graph mit einer Ecke, deren Nachbarn einen ungeraden Kreis bilden, braucht immer 4 Farben, auch wenn er nicht K_4 enthält.