Grundlagen der Mathematik

Mitschrift von Thomas Battermann

1. Semester

Inhaltsverzeichnis

1 Logik **1**
- 1.1 Formeln . . . 1
- 1.2 Äquivalenz von Formeln . . . 3
  - 1.2.1 Rechengesetze: . . . 3
- 1.3 Normalformen . . . 5
- 1.4 Die Länge der Normalformen . . . 6

2 Mengen **8**
- 2.1 Definition von Mengen . . . 8
- 2.2 Notation von Mengen . . . 8
- 2.3 Teilmengen . . . 8
- 2.4 Operationen auf Mengen . . . 10
- 2.5 Rechenregeln . . . 10
- 2.6 Kreuzprodukte . . . 11

3 Relationen **13**
- 3.1 Relationen . . . 13
- 3.2 Zusammengesetzte Relationen . . . 15
- 3.3 Die Klassifikation von Relationen . . . 17
  - 3.3.1 Transitive Hülle . . . 18
  - 3.3.2 Äquivalenzrelationen, Partitionen, Äquivalenzklassen . . . 19

4 Funktionen **22**
- 4.1 Permutation . . . 24

5 Vollständige Induktion **26**
- 5.1 Einführung des Beweisverfahrens . . . 26
  - 5.1.1 Die Türme von Hanoi . . . 28
- 5.2 Anwendung: Analyse von Algorithmen . . . 29
- 5.3 Anwendungen in der Graphentheorie . . . 30
  - 5.3.1 Färbung von Graphen . . . 33

6 Kombinatorik **35**

7 Zahlentheorie **39**
- 7.1 Teilbarkeit . . . 39
- 7.2 Primzahlen . . . 43
- 7.3 Kongruenzen . . . 45

8 Algebra **50**
8.1 Gruppen 50

9 Exkurs: Polynome **54**

1 Logik

- Grundlage (Mathematischer und anderer Beweise)
- interessante Problemstellungen in der Informatik:
  Besitzt eine logische Formel eine Lösung?
- Kontrollstrukturen in Computerprogrammen arbeiten nach den Gesetzen der Logik

1.1 Formeln

Aussagen sind Sätze, die wahr oder falsch sind.
Beispiele:

- „3 ist eine Primzahl“ ist eine (wahre) Aussage
- „4 ist eine Primzahl“ ist eine (falsche) Aussage
- „Wieviel Uhr ist es?“ ist keine Aussage, sondern eine Frage
- „Sagen sie mir bitte wieviel Uhr es ist.“ ist eine Aufforderung, keine Aussage

Formeln entstehen durch Verknüpfung einzelner Aussagen (oder Formeln).
Beispiele: Seien A und B Aussagen.
Dann sind

- nicht A
- A oder B
- entweder A oder B
- wenn A, dann B

Formeln.

Die Verknüpfungen nicht, oder usw. heißen Junktoren.

Formeln nehmen (wie die Aussage) einen der Wahrheitswerte wahr oder falsch an; dieser hängt ab von den Wahrheitswerten enthaltenen Aussagen.
Diese abhängigkeiten stellen wir in einer Wahrheitstabelle dar, die für jede Kombination der Aussagen den zugehörigen Wahrheitswert der Formel enthält.

Abkürzungen: $0\widehat{=}$ falsch
$1\widehat{=}$ wahr

Negation (nicht $A =: \neg A =: \overline{A}$

A	$\overline{A}$
0	1
1	0

Konjunktion (A und $B =: A \wedge B =: A \cdot B$)

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Disjunktion (A oder $B =: A \vee B =: A + B$)

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Exklusive Disjunktion (entweder A oder $B =: A \oplus B$)

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Implikation (wenn A, dann $B =: A \leftarrow B$)

A	B	$A \rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

A: Vorraussetzung
B: Folgerung

Equivalenz (A genau dann, wenn $B =: A \leftrightarrow B$)

A	B	$A \leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Formeln können zu komplexeren Formeln verknüpft werden.
Beispiel: $(A \oplus B) \rightarrow (C \vee B)$

Eine Formel heißt erfüllbar, wenn es eine Belegung der enthaltenen Aussagen gibt, so dass eine Formel wahr wird.
Eine Formel, die nicht erfüllbar ist, heißt unerfüllbar.
Eine Formel, die bei jeder Belegung wahr wird, heißt gültig oder tautologisch.

Beispiel:

- $A \vee B$ ist erfüllbar.
- $A \wedge \overline{A}$ ist unerfüllbar.
- $A \vee \overline{A}$ ist tautologisch.
- Sei F eine Formel.
  F ist genau dann tautologisch, wenn $\overline{F}$ unerfüllbar ist.

1.2 Äquivalenz von Formeln

Zwei Formeln F und G heißen äquivalent, wenn F und G bei jeder Variablenbelegung denselben Wahrheitswert annehmen (d. h. die Wahrheitstabellen sind identisch).
$F \equiv G, \quad F \Leftrightarrow G$
(F,G heißen gleich, wenn ihre Definitionen Zeichen für Zeichen übereinstimmen, $F = G$)

Beispiel:
$F := A \wedge B, \quad G := B \wedge A$
$\Rightarrow F \equiv G, \quad F \neq G$

in Analogie zu $\Leftrightarrow$:
$F \Rightarrow G$

(G wird bei jeder wahr, bei der auch F wahr ist.)
Beispiel:
$A \wedge B \Rightarrow A$

1.2.1 Rechengesetze:

- Kommutativgesetze
  Vertauschungsgesetze

$$A \vee B \equiv B \vee A$$
$$A \wedge B \equiv B \wedge A$$
$$A \oplus B \equiv B \oplus$$
$$A \leftrightarrow B \equiv B \leftrightarrow A$$

- Assoziativgesetze
  (Klammergesetze)

$$A \vee (B \vee C) \equiv (A \vee B) \vee C$$
$$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$$
$$A \oplus (B \oplus C) \equiv (A \oplus B) \wedge C$$
$$A \leftrightarrow (B \leftrightarrow C) \equiv (A \leftrightarrow B) \leftrightarrow C$$

- Distributivgesetze
  (Ausklammern)

  vgl. mit Arithmetik:
  $a \cdot (b + c) = a \cdot b + a \cdot c$
  i. a. $a + (b \cdot c) \neq (a + b)(a + c)$

  In der Logik:

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$
$$A \wedge (B \oplus C) \equiv (A \wedge B) \oplus (A \wedge C)$$

- doppelte Negation

  $\overline{\overline{A}} = A$

- deMorgansche Gesetze
  $\neg(A \wedge B) \equiv \overline{A} \vee \overline{B}$
  $\neg(A \vee B) \equiv \overline{A} \wedge \overline{B}$

- weitere Negation-Gesetze
  $\overline{A \oplus B} \equiv A \leftrightarrow B \equiv \overline{A} \leftrightarrow \overline{B}$
  $\overline{A \leftrightarrow B} \equiv A \oplus B \equiv \overline{A} \oplus \overline{B}$

A	B	$A \oplus B$	$\overline{a\oplus}$	$A \leftrightarrow B$
0	0	0	1	1
0	1	1	0	0
1	0	1	0	0
1	1	0	1	1

- Absorptionsgesetze

$$(A \wedge B) \vee A \equiv A$$
$$(A \vee B) \wedge A \equiv A$$

- Idempotenzgesetze
  $A \wedge A \equiv A \equiv A \vee A$

- ausgeschlossenes Drittes

$$A \wedge \overline{A} \equiv 0$$
$$A \vee \overline{A} \equiv 1$$

- Gesetze für 0 und 1

$$A \wedge 1 \equiv A \qquad A \vee 1 \equiv 1$$
$$A \wedge 0 \equiv 0 \qquad A \vee 0 \equiv A$$
$$A \oplus 0 \equiv A \qquad A \oplus 1 \equiv \overline{A}$$

- Kontraposition
  $A \to B \equiv \overline{B} \to \overline{A}$
  (verwendet man z. B. beim Widerspruchsbeweis)

- auch noch wichtig

$A \to B \equiv \overline{A} \vee B$
$\overline{C} \vee D \equiv C \to D$

A	B	$A \to B$	$\overline{A} \vee B$
0	0	1	
0	1	1	
1	0	0	
1	1	1	

Beispiel:
Beweis der Kontrapositionsgesetzes

$$A \to B \underset{12}{\equiv} \overline{A} \vee B \underset{1}{\equiv} B \vee \overline{A} \underset{4}{\equiv} \overline{\overline{B}} \vee \overline{A} \underset{12}{\equiv} \overline{B} \to \overline{A}$$

A	B	$\overline{A}$	$\overline{B}$	$\overline{B} \to \overline{A}$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	0
1	1	0	0	1

1.3 Normalformen

Konstruktion einer zu F Äquivalenten Formel:

Idee: Suche eine Formel , die genau bei den 1-Zeilen wahr wird.

A	B	C	F	
0	0	0	0	
0	0	1	1	$\overline{A} \wedge \overline{B} \wedge C$
0	1	0	1	$\overline{A} \wedge B \wedge \overline{C}$
0	1	1	0	
1	0	0	1	$A \wedge \overline{B} \wedge \overline{C}$
1	0	1	0	
1	1	0	1	$A \wedge B \wedge \overline{C}$
1	1	1	0	

$F' := \overline{A}\overline{B}C \vee \overline{A}B\overline{C} \vee A\overline{B}\overline{C} \vee AB\overline{C}$

Die entstandene Formel ist also eine Disjunktion von Konjunktionen von Variablen der negierten Variablen.
(Variablen und negierte Variablen bezeichnet man als Literale, Konjunktionen von Literalen als (Und-)Klauseln)
Solche Formeln heißen disjunktive Normalformen (DNF).

A	B	C	F
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

2. Idee: Suche eine Formel für F'', die genau bei den 0-Zeilen in der Wahrheitstabelle falsch wird.

$$\begin{aligned} F'' &= \neg(\overline{A}\overline{B}\overline{C}) \wedge \neg(\overline{A}BC) \wedge \neg(A\overline{B}C) \wedge \neg(ABC) \qquad (*) \\ &= (A \vee B \vee C) \wedge \left(A \vee \overline{B} \vee \overline{C}\right) \wedge \left(\overline{A} \vee B \vee \overline{C}\right) \wedge \left(\overline{A} \vee \overline{B} \vee \overline{C}\right) \end{aligned}$$

Eine solche Konjunktion von (Oder-)Klauseln heißt Konjunktive Normalform (KNF).
An der Formel $(*)$ sieht man, daß es zu jeder Formel eine äquivalente Formel gibt, die nur die Junktoren $\wedge, \neg$ enthält.
Junktorenmenge mit dieser Eigenschaft nennt man Basen.

Beispiel: Auch $\{\vee, \neg\}$ ist eine Basis.
Es gibt zwei Basen aus nur einem Junktor:

- NAND (A NAND $B = \neg(A \wedge B)$)

- NOR (weder-noch),
  A NOR $B = \overline{A} \wedge \overline{B}$

  Beweisidee:
  $\{\vee, \neg\}$ ist eine Basis;
  $A \vee B \equiv \overline{\overline{A \vee B}} \equiv \overline{\overline{A} \wedge \overline{B}} \equiv \neg(A \text{ NOR } B)$
  $\neg A \equiv \overline{A} \wedge \overline{A} \equiv A \text{ NOR } A \equiv (A \text{ NOR } B) \text{ NOR } (A \text{ NOR } B)$

Beispiel: Logik-Rätsel Banküberfall

a) Es kommen nur drei Personen, Herbert, Klaus und Fritz, in Frage.
   $G_a = H \vee K \vee F$

b) Wenn Herbert schuldig und Klaus unschuldig ist, dann ist Fritz schuldig.
   $G_b = (H \wedge \overline{K}) \to F$

c) Fritz „arbeitet“ niemals alleine.
   $G_c = F \to (H \vee K)$

d) Herbert arbeitet nie mit Fritz zusammen.
   $G_d = H \to \overline{F} (= F \to \overline{H})$

H	K	F	G_a	G_b	G_c	G_d	$G_a \wedge G_b \wedge G_c \wedge G_d$
0	0	0	0	1	1	1	0
0	0	1	1	1	0	1	0
0	1	0	1	1	1	1	1
0	1	1	1	1	1	1	1
1	0	0	1	0	1	1	0
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	1	1	0	0

Antwort: Klaus war auf jeden Fall beteiligt.

DNF: $\overline{H}F\overline{K} \vee \overline{H}KF \vee HK\overline{F}$
KNF: $(H \vee K \vee F) \wedge (H \vee K \vee \overline{F}) \wedge (\overline{H} \vee K \vee F) \wedge (\overline{H} \vee K \vee \overline{F}) \wedge (\overline{H} \vee \overline{K} \vee \overline{F})$

1.4 Die Länge der Normalformen

Mit dem Verfahren aus 1.3 erhält man Normalformen, bei denen alle Klauseln jede Variable (negiert oder nicht negiert) enthalten.
Solche Normalformen bezeichnet man als vollständige oder kanonische DNF, bzw. KNF.

Wahrheitstabelle, kanonische DNF und kanonische KNF sind eineindeutige Dartsellung äquivalenter Formeln.
Diese Darstellungen besitzen i. a. unterschiedliche Länge. Bei n Variablen und k erfüllende Belegungen enthält

- die Wahrheitstabelle 2^n Zeilen
- die kanonische DNF k Klauseln
- die kanonische KNF $2^n - k$ Klauseln.

Häufig kann man die Normalformen verkürzen.

Beispiel von vorhin:

$$
\begin{aligned}
\text{DNF:} \quad & \overline{H}F\overline{K} \vee \overline{H}KF \vee HK\overline{F} \\
& \equiv \overline{H}F\overline{K} \vee \overline{H}KF \vee \overline{H}KF \vee HK\overline{F} \\
& \equiv \overline{H}K \underbrace{(\overline{F} \vee F)}_{\equiv 1} \vee \underbrace{(\overline{H} \vee H)}_{\equiv 1} K\overline{F} \\
& \equiv \overline{H}K \vee K\overline{F} && \text{(verkürzte DNF)} \\
& \equiv K(\overline{H} \vee \overline{F}) && \text{(verkürzte KNF)}
\end{aligned}
$$

Bem.: In manchen Fällen kann die kanonische DNF (oder KNF) nicht mehr verkürzt werden.
Beispiel:
$F_n := (A_1 \oplus A_2) \wedge (A_3 \oplus A_4) \wedge ... \wedge (A_{n-1} plus A_n)$
n gerade.
Kann nicht gekürzt werden.
Beweis durch Widerspruch:
Sei $\hat{F}_n$ die kanonische DNF von F_n, $\tilde{F}_n$ eine verkürzte DNF von F_n
$\Rightarrow \tilde{F}_n$ enthält eine Klausel K, die nicht alle Variablen enthält. Sei A_j in K nicht enthalten.

Wähle $A_1, ..., A_n$ so, dass K den Wert 1 annimmt.
($\Rightarrow \hat{F}_n, F_n, \tilde{F}_n$ sind wahr.)

Ändere den Wert von A_j
Der Wert von K (und $\tilde{F}_n$) ändert sich nicht, aber der Wert von F_n wird 0.
$\rightarrow$ Widerspruch!
$\rightarrow \tilde{F}_n$ gibt es nicht.

2 Mengen

2.1 Definition von Mengen

Wir definieren hier eine Menge als Zusammenfassung wohldefinierter, unterscheidbarer Objekte. Ein Objekt x heißt Element der Menge M ($x \in M$), wenn x in M enthalten ist.. (anderfalls $x \notin M$)

Anmerkung: Diese „naive“ Definition von Mengen kann zu Widersprüchen führen. Keine Widersprüche treten auf, wenn man nur Teilmengen einer zuvor Definierten Grundmenge betrachtet.

Zwei Mengen M, N sind gleich, wenn sie dieselben Elemente enthalten:
$M = N \Leftrightarrow$ Für alle Objekte x gilt: $x \in M$ genau dann, wenn $x \in N$

Bem.: Insbesondere sind keine Konzepte wie die Häufigkeit der Elemente in einer Menge oder die Reihenfolge der Elemente in einer Menge definiert.
z. B.:

$$\begin{aligned} \{1,2,3\} &= \{3,2,1\} \\ &= \{1,2,2,3,3,3\} \\ |\{1,2,3\}| &= 3 \end{aligned}$$

Die Anzahl der verschiedenen Elemente einer Menge M heißt die Mächtigkeit von M (Abk.: $|M|$)

2.2 Notation von Mengen

- Aufzählung (bei endlich vielen Elementen).
  $T_{10} = \{1, 2, 5, 10\}$ (Menge der Teiler von 10)
- Aufzählung mit Auslassungszeichen:
  $\{1, 2, ..., n\} =: [n]$ (alle natürlichen Zahlen von 1 bis n)
- Bei unendlichen Mengen:

$$\begin{aligned} \mathbb{N} :=& \{0,1,2,...\} && \text{(Menge der natürlichen Zahlen)} \\ & \{1,3,5,7,...\} && \text{(ungerade natürliche Zahlen)} \\ Q =& \{0,2,4,9,16\} && \text{(Quadratzahlen)} \end{aligned}$$

- ganz allgemein: Angabe einer Eigenschaft:

$$\begin{aligned} Q &= \{x \in \mathbb{N} \mid x \text{ ist Quadratzahl}\} \\ &= \{x \in \mathbb{N} \mid \text{ es gibt } y \in \mathbb{N} : y^2 = x\} \\ &= \{x \in \mathbb{N} \mid \sqrt{(x)} \in \mathbb{N}\} \\ \mathbb{Q} &= \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ und } b \neq 0 \right\} \qquad \text{(Menge der Natürlichen Zahlen)} \end{aligned}$$

2.3 Teilmengen

Enthält M alle Elemte der Menge N, dann heißt, dann heißt N Teilmenge von M ($N \subseteq N$)
$N \subseteq M$

und M Obermenge von N.
Wenn M ein Element enthält, das nicht in N vorkommt $N \subseteq, aber N \neq M$, dann heißt N echte Teilmenge von M ($N \subset M, N \subsetneq M$).

Jede Menge hat zwei triviale Teilmengen:

$$M \subseteq M$$
$$\emptyset \subseteq M$$

Die Teilmengenbeziehung nennt man auch Inklusion.
Die Inklusion hat folgende Eigenschaften:

1. Reflexivität:
   $M \subseteq M$ für jede Menge M
2. Transivität:
   $A \subseteq B$ und $B \subseteq C$
   $\Rightarrow A \subseteq C$
3. Antisymmetrie:
   $A \subseteq B \quad \wedge \quad B \subseteq A \Leftrightarrow A = B$

Beispiel:

$$A := \{2 \cdot x \mid x \in \mathbb{Z}\}$$
$$B := \{y + z \mid y + z \in \mathbb{Z}, y \text{ und } z \text{ ungerade }\}$$
$$A \stackrel{?}{=} B$$
$$A \stackrel{!}{=} B$$
Sei $2x \in A, x \in \mathbb{Z}$
$$\Rightarrow 2x = \underbrace{(2x+1)}_{=y}\underbrace{-1}_{=z} \in B$$
$$\Rightarrow A \subseteq B$$
$B \subseteq A$:
Sei $y + z \in B$ y,z ungerade
$y = 2n + 1$ für ein $n \in \mathbb{Z}$
$z = 2n + 1$
$\Rightarrow y + 2 = 2(n + m + 1)$ ist gerade
$\Rightarrow y + z \in A, B \subseteq A$

Antisymmetrie:
$\Rightarrow A = B$

Die Potenzmenge $\mathcal{P}(M)$ einer Menge M ist die Menge aller Teilmegen von M.

Bsp.:
$\mathcal{P}(T_q) = \mathcal{P}(\{1, 3, 9\})$
$= \{\emptyset, \{1\}, \{3\}, \{9\}, \{1, 3\}, \{1, 9\}, \{3, 9\}, \{1, 3, 9\}\}$
$|\mathcal{P}(M)| = 2^{|M|}$

2.4 Operationen auf Mengen

Es seien A, B zwei beliebige Mengen.

- Vereinigungsmenge:
  $A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$
- Schnittmenge:
  $A \cap B := \{x \mid x \in A \text{ und } c \in B\}$
- Differenzmenge:
  $A - B := A \backslash B := \{x \mid x \in A \text{ und } x \notin B\}$
- Symmetrische Differenz:
  $A \triangle B := (A \backslash B) \vee (B \backslash A)$
  $= \{x \mid \text{entweder } x \in A \text{ oder } x \in B\}$

2.5 Rechenregeln

(Folgen direkt aus den Regeln für logische Formeln.)

$A \cup B = \{x \mid x \in A \text{ oder } x \in B\} \underset{(1)}{=} \{x \mid x \in B \text{ oder } x \in A\} = B \cup A$

(1) Kummutativgesetz für $\wedge$

1. Kommutativgesetz $(*)$
   $A \cup B = B \cup A$
   $A \cap B = B \cup A$
   $A \triangle B = B \triangle A$
2. Assoziotivgesetze $(*)$
   $A \cup (B \cup C) = (A \cup B) \cup C$
   $A \cap (B \cap C) = (A \cap C) \cap C$
   $A \triangle (B \triangle C) = (A \triangle C) \triangle C$
3. Distributivgesetze $(*)$
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$
4. Doppeltes Komplement
   $\overline{\overline{A}} = A$
5. de Morgansche Gesetze
   $\overline{A \cup B} = \overline{A} \cap \overline{B}$
   $\overline{A \cap B} = \overline{A} \cup \overline{B}$
6. weiteres Gesetz mit Komplement
   $A \triangle B = \overline{A} \triangle \overline{b}$
7. Verschmelzungsgesetze $(*)$
   $A \cap (A \cup B) = A$
   $A \cup (A \cap B) = A$

8. Idempotenzgesetze
   $A \cup A = A$
   $A \cap A = A$

9. Existenz des komplementären Elements $(*)$
   $A \cup \overline{A} = M$
   $A \cap \overline{A} = \emptyset$

10. Gesetze für $M, \emptyset$

$$A \cup M = M \qquad A \cup \overbrace{\emptyset}^{1} = A$$
$$A \cap \underbrace{M}_{2} = A \qquad A \cap \emptyset = \emptyset$$

    (1) neutrales Element bzgl. $\cup$
    (2) neutrales Element bzgl. $\cap$

11. Kontraposition
    $A \backslash B = \overline{B} \backslash \overline{A}$

12. weitere
    $A \backslash B = A \cap \overline{B} = \overline{\overline{A} \cup B}$

Def.: Sei M eine beliebige Menge, $A \subseteq M$.
Dann heißt
$\overline{A} = M \backslash A = \{x \mid x \in M \text{ und } x \notin A\}$
das Komplement von A bzgl. M.

2.6 Kreuzprodukte

Bei vielen Anwendungen hat man mit geordneten Paaren von Objekten zu tun.

Beispiel: kartesische Koordinaten in der Ebene.

Mengen sind ungeeignet zur Darstellung geordneter Paare.
$(\{1, \sqrt{3}\} = \{\sqrt{3}, 1\})$

Definition:
Seien A und B beliebige Mengen.
Die Menge:
$A \times B := \{(a, b) \mid a \in A \text{ und } b \in B\}$

der geordneten Paare mit erster Komponente in A und zweiter Komponente in B heißt das Kreuzprodukt (oder kartesische Produkt) von A und B.

Abkürzung: $A \times A =: A^2$

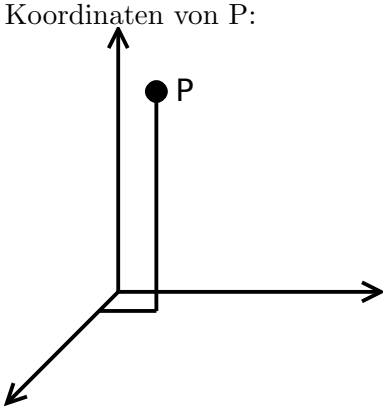
Beispiel:

- Koordinatenmenge der Eben:
  $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
- Seien $[x_{min}; x_{max}] \subset \mathbb{R}, [y_{min}; y_{max}] \subset \mathbb{R}$ (mit $x_{min} < x_{max}, y_{min} < y_{max}$) zwei Intervalle.
  $[x_{min}, x_{max}] \times [y_{min}, y_{max}]$

- Polarkoordinaten (in der Ebene)
  $(r, \phi) \in \mathbb{R}_0^+ \times [0, 2\pi)$
  $= \{r', \phi' \mid 0 \leq r', 0 \leq \phi' < 2\pi\}$

Allgemeiner:
Für beliebige Mengen $A_1, ...A_n$ bezeichnet das n-fache Kreuzprodukt
$A_1 \times ... \times A_n := \{(a_1, a_2, ..., a_n) \mid a_i \in A_i \text{ für } i = 1, ..., n\}$
die Menge aller n-Tupel mit i-ter Komponente in A_i.

Beispiel: kartesische Koordinaten in 3D:
Koordinaten von P:



$(x_P, Y_P, Z_P) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}$
$(1, \sqrt{3}, 5)$

Beispiel: Zylinderkoordinaten
$(r_P, \phi_P, Z_P) \in \mathbb{R}_0^+ \times [0, 2\pi) \times \mathbb{R}$

$(r, \phi, Z) \in [0, R] \times [0, 2\pi) \times [0, Z], \quad R, Z \in \mathbb{R}^+$

Beispiel:

$$\mathbb{B} := \{0, 1\} \widehat{=} 1 \text{ Bit}$$
$$\mathbb{B}^8 = \underbrace{\mathbb{B} \times ... \times \mathbb{B}}_{\text{8-mal}} \widehat{=} 1 \text{ Byte} = 8 \text{ Bit}$$

$\mathbb{B}^n \widehat{=}$ Menge aller Bitstrings von Länge n.

$\underbrace{\{\}}_{\text{Leeres Wort}} \cup \mathbb{B} \cup \mathbb{B}^2 \cup \mathbb{B}^3 \cup ... =: \bigcup_{i=0}^{\infty} \mathbb{B}^i$
$= B^*$
(B^* enthält alle Bitstrings von endlicher Länge)

Mit einem Bit lassen sich zwei Zahlen darstellen, mit einem Byte $\left|\mathbb{B}^8\right| = 2^8 = 256$.

Allgemein gilt:
Wenn $A_1, ...A_n$ endliche Mengen sind, ist $|A_1 \times ... \times A_n| = |A_1| \cdot ... \cdot |A_n|$

3 Relationen

3.1 Relationen

Das Kreuzprodukt $A \times B$ enthält alle Kombinationen von Elementen aus A mit Elementen aus der Menge B. Häufig ist man nur an einer Teilmenge dieser Kombinationen interessiert.

Beispiel: Kategorisierung von Objekten, etwa:

- Bücher: Autor, Vertrag, Genre, Themengebiet
- Online-Shop:
  Artikel nach Produkttyp, Hersteller, Preisklasse, Sonderangebote

Artikel:	Produkttyp:			
T	Bügeleisen	Fernseher	DVD-Player	...
1023	X			
0815		X	X	
923	X			

T $\subseteq$ Menge aller Artikel $\times$ Menge aller Produkttypen

Definition: Seien A, B zwei Mengen, $R \subseteq A \times B$
Dann heißt R eine Relation zwischen A und B. Falls $A = B$, d. h. $R \subseteq A^2$, dann heißt R auch Relation auf A
$(A^2 = A \times A)$

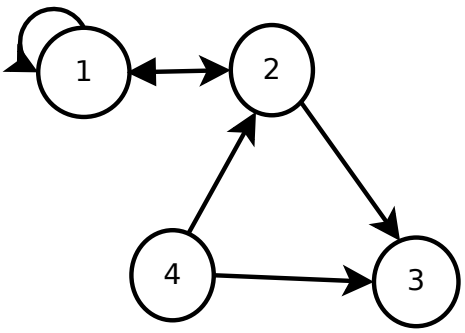
Beispiel:
$T = \{(1023,\ \text{Bügeleisen}), (0815,\ \text{Fernseher}), (0815,\ \text{DVD-Player}), ...\}$
Schreibweise: statt $(a, b) \in \mathbb{R}$ schreibt man häufig $a\mathbb{R}b$

Allgemeiner:
Jede Teilmenge $\mathbb{R} \leq A_1 \times ... \times A_n$ eines n-fachen Kreuzprodukts heißt n-stellige Relation.

Beispiel: Vater-Mutter-Kind-Relation:
$(x, y, z) \in B \Leftrightarrow$ x ist Vater von z und y ist Mutter von z.

Beispiel Online-Shop:
$T' \subseteq$ Menge der Artikel $\times$ Menge der Produkttypen $\times$ Menge der Preisklassen $\times$ Menge der Hersteller.

Besodners häufig hat man es mit binären Relationen R auf eine endliche Menge A zu tun; solche Relationen ann man auch durch einen Graphen darstellen:



Graph $G = (V, E)$
V: Menge der Knoten („Punkte“, vertices)

E: Menge der Kanten („Pfeile“, edges)
$R = E \subseteq V \times V = A \times A$

alternative Darstellung von Graphen:
(z. B. Algorithmen)

Adjazenzmatrix:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Der Eintrag M_{ij} in Zeile i, Spalte j von M ist 1, wenn es im Graphen eine Kante vom Knoten i zum Knoten j gibt, sonst 0.

Die Adjazenzmatrix läßt sich also mit $|V|^2$ vielen Bits abspeichern.

Definition:
Sei $R \subseteq A \times B$ eine binäre Relation.
$D(R) := \{a \in A \mid$ es gibt ein $b \in B$ mit $aRb\}$
(Definitionsbereich von R)
$W(R) := \{b \in B \mid$ es gibt ein $a \in A$ mit $aRb\}$
(Definitionsbereich von R)

Obiges Beispiel:
$D(R) = \{1, 2, 5\}$
(Zeile 3 ist eine Nullzeile in M)
$W(R) = \{1, 2, 3\}$
(Spalte 4 in M ist eine Nullspalte)

Einschub: Quantoren
Sei $F(x)$ eine Formel, die von einer Variablen x abhängt.
Wir führen zwei Quantoren, den Allquantor $\forall$ und den Existenzquantor $\exists$ ein:
$\forall x : F(x))$ bedeutet „für alle x gilt F(x)“
$\exists x : F(x)$ bedeutet „es gibt ein x, so dass F(x) gilt“

Für eine Formel $G(x_1, ..., x_n)$ definiert man analog:
$Q_1 x_1 : Q_2 x_2 : ... : Q_n x_n : G(x_1, ...x_n)$
wobei die Q_i jeweils ein Allquantor oder ein Existenzquantor sind.
Beispiel: „Es gibt jemanden, der alles versteht.“
entspricht: $\exists x : \forall y : x$ versteht y.
Die Reihenfolge der Quantoren ist wichtig:
$\forall y : \exists x : x$ versteht y
„Jede Sache wird von jemandem verstanden.“

Negation quantisierter Formeln:
$\neg\forall x : F(x)$ („nicht für alle x gilt $F(x)$)
$\equiv \exists x : \neg F(x)$ („es gibt ein x, so dass $F(x)$ nicht gilt.“)
$\neg\exists x : F(x)$ („es gibt kein x, so dass $F(x)$ gilt“)
$\equiv \forall x : \neg F(x)$ („für alle x gilt $F(x)$ nicht“)

Beispiel:
„Niemand versteht alles“
$\neg\exists x : \forall y : x$ versteht y
$\equiv \forall x : \neg(\forall y : x$ versteht $y)$ („Jeder versteht nicht alles.“)
$\equiv \forall x : \exists y : \neg(x$ versteht $y)$ („Für jedes x gibt es etwas, was x nicht versteht“)

3.2 Zusammengesetzte Relationen

Seien R, S zwei Relationen ($R \subseteq A \times B, S \subseteq B \times C$)

- Die Umkehrrelation $R^{-1} \subseteq B \times A$ ist definiert als
  $R^{-1} = \{(a,b) \mid (a,b) \in R\}$
  - Rollen der Zeilen und Spalten vertauscht
  - für die Matrixeinträge gilt:
    $(A_{R^{-1}})_{ij} = (A_R)_{ji}$ für $i,j = a, ..., e$
  - $A_{R^{-1}}$ ist also die Transponierte von $(A_R)^T$ von A_R
  - $A_{R^{-1}}$ geht durch Spiegelung an der Hauptdiagonalen aus A_R hervor
  - $(A_{(R^{-1})^{-1}})_{ij} = (A_{R^{-1}})_{ji}$
    $\Rightarrow (A_{(R^{-1})^{-1}}) = (A_R)_{ij}$
- Die Verkettungsrelation $S \circ R \subseteq A \times C$ (S nach R)
  ist $S \circ R := \{(a,c) \in A \times C \mid \exists v \in B : aRb \wedge bSc\}$

Beispiel: Online-Shop:
„Heute 20% Rabatt auf Tiernahrung und Fernseher."

S	„-20%"	„-10%"	„±0%
Tiernahrung	X		
Fernseher	X		
Bügeleisen			X

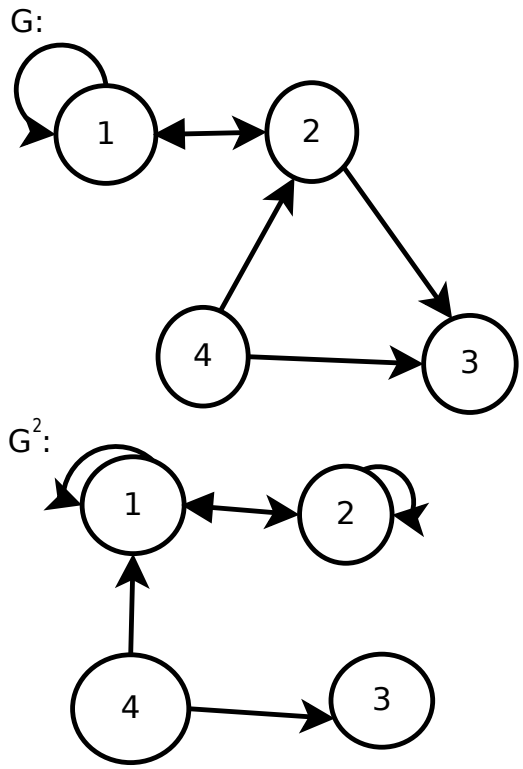
Frage: „Wieviel Rabatt gibt es auf Artikel 0815?"
Lösung:
Betrachte $S \circ T$
wir finden: (0815, Fernseher) $\in T$,
(0815, DVD-Player) $\in T$,
(Fernseher,„-20%) $\in S$
$\Rightarrow$ (0815, „-20%") $\in S \circ T$
(wähle b=Fernseher in der Definition von $S \circ T$

Beispiel für die Umkehrrelation:

- Kleiner-gleich-Relation auf $\mathbb{R}$:
  $y \leqslant^{-1} x \Leftrightarrow x \leqslant y \Leftrightarrow y \geqslant x$
  $(y,x) \in \leqslant^{-1} \quad (x,y) \in \leqslant \quad (y,x) \in \geqslant$
  $\Rightarrow$ Die Umkehrrelation von $\leqslant$ ist $\geqslant$.

am Beispiel von Graphen:

- Umkehrrelation:
  Es ändert sich lediglich die Richtung der Pfeile.
- Verkettungsrelation:
  $G^2 = G \circ G := (V, E \circ E)$
  wenn $G = (V, E)$



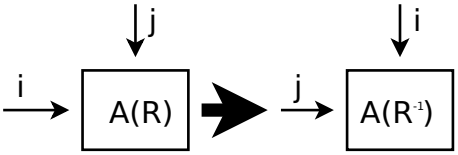
Eigenschaften von Umkehr- und Verkettungsrelationen

Einschub: Umkehrrelation

$R \subseteq A \times B, C \subseteq B \times C, R \subseteq B \times A$
$b(R^{-1})a \Leftrightarrow aRb$
$b \in B, a \in A$

Bsp.:
$x \leq y \Leftrightarrow y \geq x$
$\leq^{-1} \Leftrightarrow \geq$

Adjezenzmatrix von $\mathbb{R}$:



Einschub Verkettungsrelation:

$S \circ R \subseteq A \times C, \quad a \in A \quad c \in C$
$a(A \circ R)c \Leftrightarrow \exists b \in B : aRb \wedge bSc$

Eigenschaften:

- $(R^{-1})^{-1} = R \subseteq A \times B : a \in A, b \in B$ beliebig gewählt.
  $a(R^{-1})^{-1}b \Leftrightarrow b(R^{-1})a \Leftrightarrow aRb$
- $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$
  Beweis: siehe Übungsaufgabe

3.3 Die Klassifikation von Relationen

Eine Relation $R \subseteq A \times A$ kann folgende Eigenschaften besitzen:

- Reflexivität: $\forall a \in A : aRa\,(R)$
- Symmetrie: $\forall a, b \in A : aRb \leftrightarrow bRa\,(S)$
- Antisymmetrie: $\forall a, b \in A : aRb \wedge bRa \rightarrow a = b\,(AS)$
- Transitivität: $\forall a, b, c \in A : aRb \wedge bRc \rightarrow aRc\,(TR)$
- Totalität: $\forall a, b \in A : aRb \vee bRa\,(TO)$

Von besonderer Bedeutung sind folgende Kombinationen dieser Eigenschaften:

1. R ist eine Äquivalenzrelation, wenn R die Eigenschaften $(R), (S), (TR)$ besitzt.
2. R ist eine Halbordnung, wenn R die Eigenschaften der $(R), (AS), (TR)$ besitzt.
3. Eine Halbordnung, für die zusätzlich (TO) gilt, heißt totale Ordnung.

Bsp.:

- Die Äquivalenz aussagen logischer Formeln ($\equiv$) ist ein Bsp für eine Äquivalenzrelation
- Definiere $\cong$ als Relation auf $\mathbb{Z}$ als:
  $a \cong b :\Leftrightarrow a, b$ sind beide gerade oder beide Ungerade
  $a \cong a$ (R)
  $a \cong b \wedge b \cong c \rightarrow a \cong c\,(TR)$
  $\Rightarrow \cong$ ist eine Äquivalenzrelation
- Die Kleiner-Gleich-Relation $\leq$ auf $\mathbb{R}$ ist eine totale Ordnung:

$$x \leq x \qquad (R)$$
$$x \leq y \wedge y \leq x \rightarrow x = y \qquad (AS)$$
$$x \leq y \wedge y \leq z \rightarrow y \leq z \qquad (TR)$$

Es gilt auch immer:

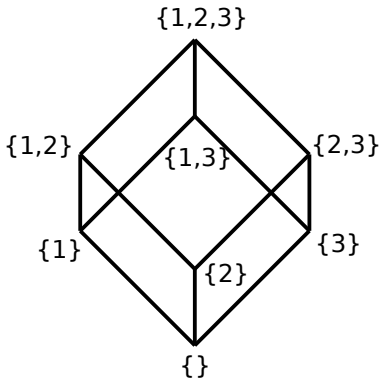
$$x \leq y \vee y \leq x \qquad (TO)$$

- Eine Halbordnung, die keine totale Ordnung ist:
  Die Inklusion als Relation auf $\mathcal{P}(M)$ für eine Menge.
  Seien $A, B, C \in \mathcal{P}(M)$ (d. h. $A \subseteq M, B \subseteq M, C \subseteq M$)

$$\Rightarrow A \subseteq A \qquad (R)$$
$$\Rightarrow A \subseteq B \wedge B \subseteq A \rightarrow A = B \qquad (AS)$$
$$\Rightarrow A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C \qquad (TR)$$

Wenn $|M| \geq 2$, dann gibt es $x \in M, y \in M$ mit $x \neq y$
$\Rightarrow \{x\} \not\subseteq \{y\} \quad \{y\} \not\subseteq \{x\}$
$\Rightarrow$ Die Inklusion ist nicht total, wenn M als 2 Elemente.

Darstellung einer Halbordnung auf einer endlichen Menge Hasse-Diagramm (am Bsp. einer Inklusion auf $\{1, 2, 3\}$)

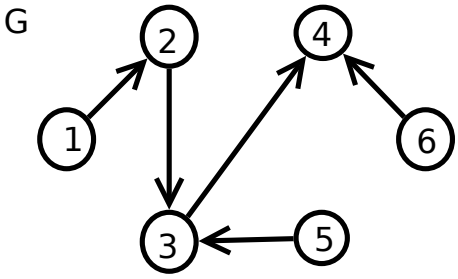


neue Klasse

- zum Hinzufügen in eine Menge: Äquivalenzrelation!
- zum Hinzufügen in eine sortierte Datenstruktur Totale Ordnung

3.3.1 Transitive Hülle

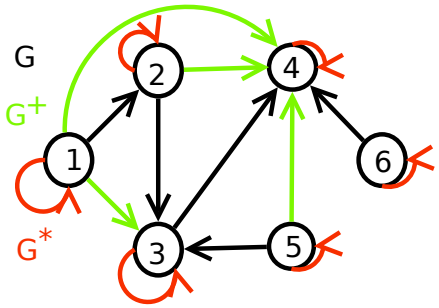
Transitivität: $aRb \wedge bRc \rightarrow aRc$
Veranschaulichung an deinem Graphen
$G := (V, E)$:



Fragestellung:
Welche Knoten sind von eine gegebenen Knoten aus erreichbar?
$G^+ := \bigcup_{i=1}^{\infty} G^i = G^1 \cup G^2 \cup G^3 \cup ...$

transitive Hülle von G:
Relation R:
$R^+ := \bigcup_{i=1}^{\infty} R^i = R^1 \cup R^2 \cup R^3 \cup ...$
R^+ ist die kleinste transitive Relation die R enthält.

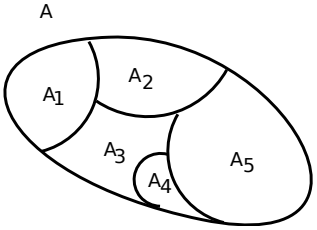
reflexiv-transitive Hülle einer Relation R:
$R^* := R^0 \cup R^+ = \bigcup_{i \in \mathbb{N}} R^i$
(Falls R Relation auf der Menge M ist:
$R^0 := \{(x, x) \mid x \in M\}$)
R^* ist die kleinste Relation, die R enthält und (R) sowie (TR) erfüllt.



Falls R bereits transitiv ist:
$R^+ = R$
(Falls R bereits reflexiv und Transitiv ist:
$R^* = R$

3.3.2 Äquivalenzrelationen, Partitionen, Äquivalenzklassen

Gegeben sei eine beliebige Menge A.

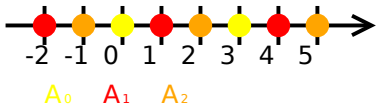


Unterteile A in dijunkte Teilmengen A_i (für alle $i \neq j : A_i \cap A_j = \emptyset$)
$\bigcup_i A_i = A$
Die Teilmengen A_i bilden also eine Partition von A.

Dann ist die Relation R:
$aRb \Leftrightarrow \exists i : a \in A_i \wedge b \in A_i$
eine Äquivalenzrelation auf A.

Beispiele:

- Unterteile $\mathbb{Z}$ in Teilmengen
  $A_i = \{x \in \mathbb{Z} \mid x \text{ hat Rest } i \text{ bei Division durch } n\}$ mit $n \in \mathbb{N}, n > 0$.



  Äquivalenzrelation:
  $x \equiv y(mod n)$
  (Sprechweise: „x ist kongruent zu y modulo n“) $x \equiv y(mod n)$ genau dann, wenn $\underbrace{x \bmod n}_{=\text{ Divisionsrest}} =$
  $y \bmod n$

- Rundung reeller Zahlen ($A = \mathbb{R}$):
  $A_i := \{x \in \mathbb{R} \mid x \in (i - \frac{1}{2}, i + \frac{1}{2}]\}$
  x und y sind also äquivalent genau dann, wenn x und y auf dieselbe ganze Zahl gerundet werden.

umgekehrt:
Es sei R eine Äquivalenzrelation auf einer Menge M. Für $x \in M$ ist

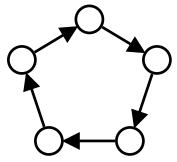
$[x]_R := \{y \in M \mid xRy\}$
die Äquivalenzklasse von x bzgl. R.

Der „Quotient“
$M/R := \{[x]_R \mid x \in M\}$

Behauptung:
Die Äquivalenzklassen von R bilder eine Partition von M.
Beweis:

- Die Äquivalenzklassen überdecken M:
  Sei $x \in M$ beliebig.
  Dann ist $x \in [x]_R$, denn:
  xRx (folgt aus (R))
  $\Rightarrow \bigcup_{x \in M} [x]_R = M$
- Verschiedene Äquivalenzklassen sind disjunkt:
  Sei $[x]_R \neq [y]_R$,
  Annahme: $[x]_R \cap [y]_R \neq \emptyset$
  Dann gibt es ein $c \in [x]_R \cap [y]_R$.
  Wähle $z \in [x]_R$, zeige: $z \in [y]_R$:
  $xRz \wedge xRc \underset{(S)}{\Rightarrow} cRx \wedge xRz \underset{(TR)}{\Rightarrow} cRz, yRc \underset{(TR)}{\Rightarrow} yRz \Leftrightarrow z \in [y]_R$
  also: $[x]_R \subseteq [y]_R, [y]_R \subseteq [x]_R \rightarrow [x]_R = [y]_R$ Widerspruch!!

Sei G der Graph einer reflexiv-transitiven Relation R.
R ist eine Halbordnung $\leftrightarrow$ G enthält keine Kreise.



(G enthält einen Kreis $\Leftrightarrow$ R ist keine Halbordnung.

$\overset{\text{Beweis}}{\Leftarrow}$ (R),(TR) gelten laut Voraussetzung.
$\rightarrow$ (AS) ist Verletzt.

$\Rightarrow \exists x, y : xRy \wedge yRx$

in G: 

$\Rightarrow$ Sei ein Kreis in G.

$\Rightarrow x_1Rx_2, x_2Rx_3, ..., x_{n-1}Rx_n, x_nRx_1$
$\Rightarrow x_1Rx_n, x_nRx_1$
$x_1 \neq x_n \rightarrow$ (AS) ist verletzt.

Einbettung einer Halbordnung in eine totale Ordnung.

Algorithmus:

1. Wähle ein minimales x (d. h. $\neg\exists y : y \leq x$)
   (im zugehörigen Graphen führt also keine Kante zu x.)

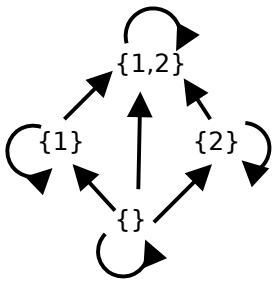
2. Setze $x_1 := x$, entferne x aus dem Graphen, ebenso alle Kanten von x.

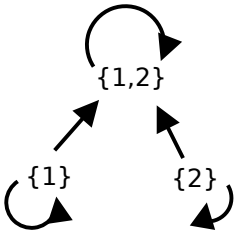
3. Fahre bei 1. fort und wähle nacheinander $x_1, x_2, ..., x_n$ bis der Graph leer ist.

$\Rightarrow$ Definiere:
$x_1 \leq x_2 \leq ... \leq x_n$

Beispiel:
$\subseteq$ auf der Menge $\mathcal{P}(\{1,2\})$

$x_1 := \{\}$
$x_2 := \{2\}$
$x_3 := \{1\}$
$x_4 := \{1,2\}$



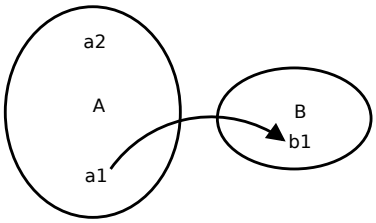


$\Rightarrow$Gefundene totale Ordnung.
$\{\} \leq \{2\} \leq \{1\} \leq \{1,2\}$

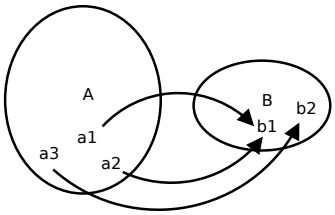
4 Funktionen

Sei R eine Relation zwischen A und B. R heißt eindeutig, wenn es zu jedem $a \in A$ höchstens ein $b \in B$ gibt, so dass aRb. Eine eindeutige Relation $R \subseteq A \times B$ heißt Funktion oder Abbildung, wenn $D(R) = A$

Veranschaulichung:



eindeutige Relation



Funktion

Schreibweise:
$f\colon A \to B$ „d ist eine Funktion von A nach B“
$f\colon a \to b$ oder $f(a) = b$
„f bildet a auf b ab.“
„Der Funktionswert von f an der Stelle a ist b.“
(„a und b stehen in Relation bzgl. f.“)

Frage: „Wann ist die Umkehrrelation von f wieder eine Funktion?“

- f^{-1} muss eindeutig sein, d. h.
  $\forall b \in B : \exists$ höchstens ein $a \in A : f(a) = b$ oder gleichbedeutend:
  $\forall a_1, a_2 \in A$ mit $a_1 \neq a_2$
  $\Rightarrow f(a_1) \neq f(a_2)$
  Funktionen mit dieser Eigenschaft heißen injektiv.

- Es muss gelten:
  $D(f^{-1}) = B$.
  $D(f^{-1}) = W(F)$
  $f\colon Y \to X$
  $\forall y \in Y \exists x \in X : f(x) = y$
  Funktionen mit dieser Eigenschaft heißen surjektiv.

Also f^{-1} ist eine Funktion (von B nach A), wenn f injektiv und surjektiv ist. (Dann heißt f bijektiv.)

Beispiele:

a) $f(x) := 2x$ ist surjektiv auf $\mathbb{Q}$, aber nicht auf $\mathbb{Z}$ und injektiv auf $\mathbb{Q}$ und auf $\mathbb{Z}$.

b) $f(x) := x^2$ ist nicht surjektiv auf $\mathbb{N}$, ist injektiv auf $\mathbb{N}$

Definition: Zwei Mengen A,B heißen gleichmächtig, wenn es eine bijektion zwischen A und B gibt.
Bem.: Eine Menge A ist endlich, wenn es ein $n \in \mathbb{N}$ gibt mit
$A \sim [n]$.
(Dann hat A die Mächtigkeit n.)

A ist unendlich, wenn A nicht endlich ist.
Definition:
A heißt abzählbar unendlich, wenn $A \sim \mathbb{N}$.
A heißt überabzählbar unendlich, wenn A unendlich, aber nicht abzählbar unendlich ist.

Beispiele:

- $\mathbb{N}\backslash\{0\}$
  Bijektion$f\colon \mathbb{N} \to \mathbb{N}\backslash\{0\}, f(x) := x+1$
  f ist injektiv: seien $x, y \in \mathbb{N}, x \neq y$
  $f(x) = x+1, f(y) = y+1$
  $x \neq y$
  $x+1 \neq y+1$
  also: $f(x) \neq f(y)$
  f ist surjektiv:
  Sei $z \in \mathbb{N}\backslash\{0\}$ beliebig:
  Wähle $x := z-1 \in \mathbb{N}$
  $\to f(x) = z$
  d. h. $W(f) = \mathbb{N}\backslash\{0\}$.

- $\mathbb{Z}$ ist auch abzählbar unendlich:
  Nummerierung:
  5310246
  Bijetkion: $f\colon \mathbb{N} \to \mathbb{Z}, f(x) := (-1)^x \lceil \frac{x}{2} \rceil$

- $\mathbb{Q}$ ist abzählbar:
  $\mathbb{Q} \sim \mathbb{Z}^2 \sim \mathbb{N}^2$

- allgemeiner:
  Es seien $A_n, n \in \mathbb{N}$, abzählbar unendliche Mengen. Dann ist auch
  $\bigcup\limits_{n\in\mathbb{N}} A_n$ abzählbar.

  Konstruiere eine Bijektion
  $f\colon \mathbb{N} \to \bigcup\limits_{n\in\mathbb{N}} A_n$
  a_n ist abzählbar unendlich
  $\to$ es gibt eine Bijektion
  $g_n\colon \mathbb{N} \to A_N$

  Definiere f:

  $$f(0) := g_0(0) \qquad f(4) := g_1(1)$$
  $$f(1) := g_0(1) \qquad f(5) := g_2(0)$$
  $$f(2) := g_1(0) \qquad f(6) := g_0(3)$$
  $$f(3) := g_0(2)$$

  Falls einer der $g_i(j)$ schon vorher in dieser Liste auftaucht, wird es übersprungen.

- $\mathbb{R}$ ist überabzählbar unendlich

Widerspruchsbeweis mit Diagonalargument:
Annahme: $\mathbb{R}$ ist abzählbar unendlich (offensichtlich: $\mathbb{R}$ ist nicht endlich)
$\rightarrow$ es gibt eine Bijektion
$r: \mathbb{N} \rightarrow \mathbb{R}$
Wir zeigen: $\exists c \in \mathbb{R} : c \notin W(r)$
Konstruiere c:
Es sei $R_i(n)$ die i-te Nachkommastelle von $r(n)$;
setze $c := c_0, c_1 c_2 c_3 c_4 ...$ (c = Dezimalziffer)
wobei $c_0 \neq r_0(0), c_1 \neq r_1(1), c_2 \neq r_2(2)$
allgemein: $c_n \neq r_n(n)$
$\Rightarrow c \neq r(0), c \neq r(1), c \neq r(2)$
$\forall n \in \mathbb{N} : c \neq r(n)$
weil c und $r(n)$ sich in der n-ten Nachkommastelle underscheiden.
$\Rightarrow c \notin W(r)$ aber $c \in \mathbb{R}$
$\Rightarrow$ r ist keine Bijektion
$\rightarrow \mathbb{R} \not\sim \mathbb{N}$

- ähnlich:
  $\mathcal{P}(\mathbb{N}) \not\sim \mathbb{N}$ (s. Übungsaufgabe)

4.1 Permutation

Zufallsexperiment:
n Kugeln mit Nummern $1, ..., n$;
ziehe Kugeln ohne zurücklegen, beachte die Reihenfolge:

n	1	2	3	4	5
$f(n)$	2	3	5	4	1

(mögliches Ergebnis für $n = 5$)

$\rightarrow f$ ist eine Bijektion.
Eine Bijektion auf einer endlichen Menge heißt Permutation.
Die Menge aller Permutationen auf $[n] =: S_n$

Algorithmus zum Erzeugen aller Permutationen auf $[n]$:

- Interpretiere die Permutationen als Zahlen
- generiere alle Permutationen „der Größe nach“ geordnet

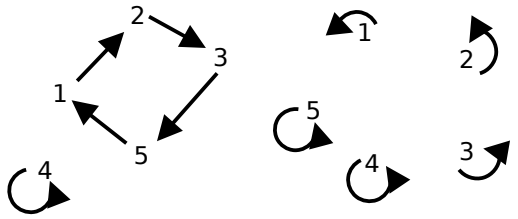
  1. 12345 (id = „Identität“)

  nächst größere Zahl (von 23541 aus):
  $a := 2\underbrace{3}_{j}541$
  $b := 24135$

Graphen zu Permutationen

n	1	2	3	4	5
$\sigma(n)$	2	3	5	4	1

n	1	2	3	4	5
$id(n)$	1	2	3	4	5



Allgemein gilt: Jeder Knoten besitzt genau einen Nachfolger und genau einen Vorgänger.
$\rightarrow$ Der Graph besteht aus unzusammenhängenden Kreisen, d. h. jeder Knoten ist in genau einem Kreis enthalten.

Zyklenschreibweise:
$(1\,2\,3\,5)(4)$
Letzteres wird oft weggelassen.

$\sigma := (1\,2\,3\,5)(4)$
$\tau := (1\,2\,4)(3\,5)$

$\sigma \circ \sigma = (1\,3)(2\,5)(5)$
$\sigma \circ \tau = (1\,3)(2\,4)(5)$

$\sigma^{-1} = (5\,3\,2\,1)(4) = (1\,5\,3\,2)(4)$

$\sigma^{-1} \circ \sigma = (1)(2)(3)(4)(5) = \mathrm{id}$

5 Vollständige Induktion

5.1 Einführung des Beweisverfahrens

$1 + 2 + ... + 100 = ?$

1	2	...	50	
+100	99	...	51	
101+	101+	...+	101	$= 50 \cdot 101 = \frac{100 \cdot (100+1)}{2}$

allgemeiner Beweis mit vollständiger Induktion: $\sum_{k=1}^{n} k \stackrel{!}{=} \frac{n \cdot (n+1)}{2}$

Induktionsanfang: $n = 1$

$\sum_{k=1}^{1} k = 1 = \frac{1 \cdot 2}{2}$ ✓

Induktionsschritt:

Zeige die Behauptung „für n+1“, unter der Vorraussetzung, dass sie „für n“ gilt.

$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1)$

$\sum_{k=1}^{n+1} k \stackrel{!}{=} \frac{(n+1)(n+2)}{2}$

$\underset{\text{Induktionsvorraussetung}}{=} \frac{n \cdot (n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$

Allgemeine Struktur eines Beweises mit vollständiger Induktion:
Wir möchten alle Aussagen $A_i, i \in \mathbb{N}$, beweisen. Das funktioniert (u. U.) mit diesen zwei Schritten:

1. Induktionsanfang:
   Beweise A_0

2. Induktionsschritt:
   Beweise A_{n+1} (für beliebiges $N \in \mathbb{N}$
   unter der sog. Induktionsvorraussetzung, dass A_n gilt.

   $A_0 \wedge (A_0 \to A_1) \wedge (A_1 \to A_2) \wedge (A_2 \to A_3)$
   $\Rightarrow A_0 \wedge A_1$

Geometrische Reihe

wenn der Summationsindex im Exponenten steht:

$\sum_{i=0}^{n} q^i, \text{ mit } q \in \mathbb{R}$

$q \sum_{i=0}^{n} q^i = \sum_{i=0}^{n} q^{i+1} = \sum_{j=1}^{n+1} q^j = \sum_{i=0}^{n} + q^{n+1} - 1$

$$(q-1) \sum_{i=0}^{n} q^i = q^{n+1} - 1 \qquad |: (q-1) \text{ falls } q \neq 1$$

$$\sum_{i=0}^{n} q^i = \frac{q^{n+1} - 1}{1 - q}$$

$$\sum_{i=0}^{n} q^i = \frac{1 - q^{n+1}}{1 - q}$$

Bemerkung:

Für $q \in \mathbb{Z}$ ist also $1 - q^{n+1}$ teilbar duch $1 - q$.

Beispiel:

- $12^{17} - 1$ ist teilbar duch 11.
- $2^{24} - 1 = (2^3)^8 - 1 = 8^8 - 1$ ist durch 7 teilbar.

$q = 1$:
$\sum_{i=0} nq^i = \sum_{i=0}^{n} = n + 1.$

alternativ: Beweis mit vollständiger Induktion (für $q \neq 0$)
IA: $n = 0$,
$\sum_{i=0}^{0} q^i = 1 = \frac{1-q^{0+1}}{1-q}$

IS: $\sum_{i=0} n + 1q^i = \sum_{i=0}^{n} q^i + q^{n+1}$
$\underset{\text{I.V.}}{=} \frac{1-q^{n+1}}{1-q} + \frac{q^{n+1}-q^{n+2}}{1-q}$

$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$
kleine Verallgemeinerung:
$\sum_{k=0}^{n} p^{n-k} \cdot q^k = \sum_{k=0}^{n} \frac{p^n}{p^k} \cdot q^k$
$= \frac{pn+1-q^{n+1}}{p-q}$

Folgerung falls $p, q \in \mathbb{Z}$, ist
$p^{n+1} - q^{n+1}$ teilbar durch p-q.
z.B. $12^100 - 5^100$ ist teilbar duch 7.

Einschub: Summen und Produkte

1. Definition (rekursiv):
   $\sum_{k=1}^{0} a_k := 0$ „leere Summe“
   $\prod_{k=1} 0a_k := 1$ „leeres Produkt“

   $\sum_{k=1} n + 1a_k := \sum_{k=1} na_k + a_{n+1}$
   $\prod_{k=1} n + 1a_k := a_{n+1} \prod_{k=1} na_k$
2. Präzendent der Operatoren
   $\sum_{k=1}^{n} a_k = \left(\sum_{k=1}^{n} a_k\right) + b$
   $\sum_{k=1}^{n} a_k \cdot b = \sum_{k=1}^{n} (a_k \cdot b)$
   $\prod_{k=1}^{n} a_k + b = \left(\prod_{k=1}^{n} a_k\right) + b$
   $\prod_{k=1}^{n} a_k \cdot b = \left(\prod_{k=1}^{n} a_k\right) \cdot b$

   $\sum$ bindet geringfügig stärker als „+“ und „-“
   $\prod$ bindet geringfügig stärker als „$\cdot$“

3. konstante Faktoren
$\sum_{k=1}^{n} a_k \cdot c = c \cdot \sum_{k=1}^{n} a_k$
$a_1 \cdot c + a_2 \cdot c + ... = c \cdot (a_1 + a_2 + ...)$
$\prod_{k=1}^{n} (a_k \cdot c) = c^n \cdot \prod_{k=1}^{n} a_k$

4. Aufspaltung
$\sum_{k=1}^{n} a_k = \sum_{k=1}^{l} a_k + \sum_{k=l+1}^{n} a_k$
mit $l \in \{1, ..., n\}$
$\prod_{k=1}^{n} a_k = \prod_{k=1}^{l} a_k \cdot \prod_{k=l+1}^{n} a_k$
$\sum_{k=1}^{n} (a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k$
$\prod_{k=1}^{n} (a_k + b_k) = \prod_{k=1}^{n} a_k \cdot \prod_{k=1}^{n} b_k$

5. Umnummerierung
$\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} a_{\sigma(k)}$
$\prod_{k=1}^{n} a_k = \prod_{k=1}^{n} a_{\sigma(k)}$
mit einer Permutation $\sigma \in S_n$

6. Mehrfachsummen/-produkte
$\sum_{k=1}^{m} \sum_{l=1}^{n} a_{kl} = \sum_{l=1}^{n} \sum_{j=1}^{m} a_{kl}$
$\prod_{k=1}^{m} \prod_{l=1}^{n} a_{kl} = \prod_{l=1}^{n} \prod_{j=1}^{m} a_{kl}$

5.1.1 Die Türme von Hanoi

Aufgabe: Bringe n Scheiben von A nach C, so dass jederzeit keine Scheibe auf einer kleineren Scheibe liegt.

Lösung: Bringe $n-1$ Scheiben von A nach B; lege anschließend Scheibe n von A nach B. Bringe zuletzt die $n-1$ Scheiben von B nach C.

Die minimale Anzahl an Operationen um das Problem zu lösen, sei T_n

$T_n = T_{n-1} + 1 + T_{n-1} = 2T_{n-1} + 1$
$T_1 = 1$

n	1	2	3	4	5
T_n	1	3	7	15	31

$T_n \stackrel{?}{=} 2^n - 1$ Beweis

Beweis von $2^n - 1$

IA: n = 1
$T_1 = 1 = 2^1 - 1$

IS

$$\begin{aligned} T_{n+1} &= 2 \cdot T_n + 1 \\ &\underset{\text{IV}}{=} 2 \cdot (2^n - 1) + 1 \\ &= 2^{n+1} - 1 \qquad \text{q.e.d.} \end{aligned}$$

Wenn sie für n gilt, sollte sie auch für $n+1$ gelten, ziel der Vollständigen Induktion.

5.2 Anwendung: Analyse von Algorithmen

Dec2Bin(n)

1. k = 0
2. while $n > 0$ do
3. b[k] = n mod 2
4. n = $\lfloor n/n \rfloor$
5. k = k + 1
6. return b

Bei erreichen von Zeile 2 gilt jedesmal die Invariante
$m = 2^k \cdot n + \sum_{j=0}^{k-1} b[j] \cdot 2^j \quad (*)$

Bei verlassen der Schleife (n=0) ist $m = \sum_{j=0}^{k-1} b[j] \cdot 2^j$.
Also enthält b die Binärziffern von m.

Beweis von $(*)$ mit vollständiger Induktion:

IA: (vor dem ersten Schleifendurchlauf)
$m = nmk = 0 \Rightarrow 2^k \cdot n + \sum_{j=0}^{k-1} b[j] \cdot 2^j = n + 0 = m$

IS: $(*)$ gelte vor einem Schleifendurchlauf (I.V.)
Nach dem Durchlauf:
$k' = k + 1, n' = \lfloor n/2 \rfloor$
$2^{k+1} \lfloor n/2 \rfloor + \sum_{j=0}^{k} b[j] \cdot 2^j$
$\underset{\text{i.V.}}{=} 2^{k+1} \cdot \lfloor n/2 \rfloor + (m - 2^k \cdot n) + \underbrace{b[k]}_{n \mod 2} \cdot 2^k$
$= m + 2^k(2 \cdot \lfloor n/2 \rfloor + n \mod 2 - n)$

Der Wert der Klammer is 0:
$n = c \cdot \lfloor n/c \rfloor + n \mod c$ für beliebiges $c \in \mathbb{N}, c > 0$

denn der Devisionsrest ist definiert als $n \mod c := n - c \cdot \lfloor n/c \rfloor$
$\rightarrow 2^{k'} \cdot n' + \sum_{j=0}^{k'-1} b[j] \cdot 2^j = m$ q.e.d

Laufzeitabschätzung:
Es sei T(n) die Anzahl der Schleifendurchläufe bei Eingabe n.
$T(1) = 1$
$T(n) = 1 + T(\lfloor n/2 \rfloor)$
Das ist eine Rekursionsgleichung ähnlich wie bei Aufgabe 5.4
$\Rightarrow T(n) = \lfloor \log_2 n \rfloor + 1$

Schnelle Exponentation

berechne $a^n = \underbrace{a \cdot ... \cdot a}_{\text{n-mal}}$ -¿ Aufwand O(n).

mit einem Aufwand von O(log n)

In Zeile 3 gilt die Invariante:
$d = a^{(b_{k-1}...b_{i+1})_2}$
am Ende: $i = -1, d = a^{b_{k-1}...b_0} = a^n$

IA: (vor dem ersten Durchlauf)
$1 = d, i = k - 1$
$\Rightarrow a^{(b_{k-1}...b_{i+1})_2}$
$= a^{()_z} = a^0 =^= d$ q.e.d

IS: Werte nach dem schleifen Durchlauf:
$i' = i - 1$
Fall 1: $b_i = 0$
$d' = d \cdot d = [a^{(b_{k-1}...b_{i+1})_2}]^2$
$= a^{(b_{k-1}...b_{i+1})_2 + (b_{k-1}...b_{i+1})_2} = a^{(b_{k-1}...b_{i+1}0)_2}$
$= a^{(b_{k-1}...b_i)_2}$
$= a^{(b_{k-1}...b_{i'+1})_2}$

a^n
Invariante in Zeile 3:
$d = a^{(b_{m-1}...b_{i+1})_2}$
Fall 2: $b_i = 1$
nach der Ausführung des Schleifendurchlaufs:
$i' = i - 1$
$d' = d^2 \cdot a \underset{\text{i.V.}}{=} a^{2 \cdot (b_{k-1}...b_{i+1})_2 + 1}$
$= a^{(b_{k-1}...b_{i+1}1)_2}$
$= a^{(b_{k-1}...b_{i'+1})_2}$
q.e.d.

5.3 Anwendungen in der Graphentheorie

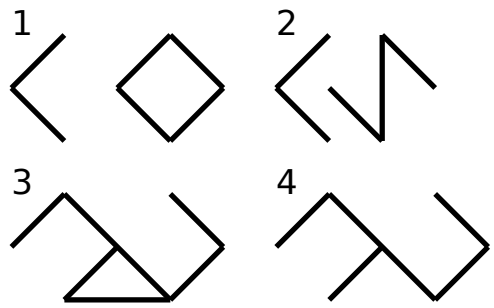
In diesem Abschnitt ist stets $G = (V, E)$ ein ungerichteter Graph ohne Schleifen, über der Knotenmenge $V := [n]$ mit $|E| =: e$ vielen Kanten. Bei Ungerichteten Graphen:
$E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$

Def.: Der Grad (degree, engl.) deg(v) eines Knotens ist die Anzahl der Kanten, die bei v beginnen.

Def.: Ein Baum ist ein zusammenhängender, azyklischer Graph. (G heißt zusammenhängend, wenn man von einem jedem Knoten in G zu jedem anderen Knoten gelangen kann. Zusammenhangskomponenten: größte zusammenhängende Teilgraphen.)

Ein Wald ist ein azyklischer Graph. (d. h. die Zusammenhangskomponenten eines solchen Graphen sind Bäume)

Die Knoten vom Grad 1 (oder 0) eines Baumes heißen Blätter, alle anderen Knoten sind innere Knoten.



1. nicht azyklisch, nicht zusammenhängend
2. azyklisch, nicht zusammenhängend, ein Wald aus zwei Bäumen.
3. enthält einen Kreis, weder Baum noch Wald.
4. Ein Baum: azyklisch und zusammenhängend.

Beh.: Jeder Baum hat Blätter.
Beweis: Starte bei einem beliebigen Knoten, gehe entlang beliebiger Kanten, ohne bereits besuchte Knoten nochmals zu besuchen. Da $|V|$ endlich ist, endet dieser Vorgang nach spätestens n Schritten.✓

Satz: Jeder Baum hat $e = n - 1$ viele Kanten.

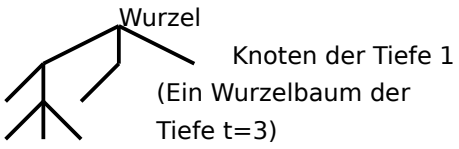
Beweis mit Vollständiger Induktion übder n:
IA: $n = 1 \to e = 0$ ✓
IS: G' habe $n+1$ Knoten. Sei v ein Blatt von G'. es sei G der Teilgraph von G', den man durch Entfernen von v (und der Kante v) erhält.
$\Rightarrow$ G hat n Knoten
$\overset{\text{i.V.}}{\Rightarrow}$ G hat $n-1$ Kanten
$\Rightarrow$ G' hat $(n-1)+1 = n$ Kanten ✓

Folgerung: Hat G n oder mehr Kanten, dann enthält G einen Kreis.

Def.: Ein Wurzelbaum ist ein Baum mit einem ausgezeichneten Knoten, der sog. Wurzel.

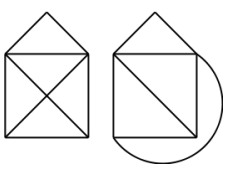
Def.: Die Tiefe eines Knotens in einem Wurzelbaum ist sein Abstand zur Wurzel.
Die Tiefe eines Wurzelbaumes ist die größte Tiefe eines Knotens in diesem Baum.

Bsp.:

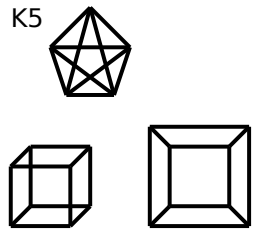


Def.: Ein Binärbaum ist ein Wurzelbaum, in dem jeder Knoten Grad ≤ 3 hat, die Wurzel hat Grad 2.

Satz: Ein Binärbaum der Tiefe t hat höchstens 2^t viele Blätter.



Def.: Ein Graph ist planar, wenn man ihn so in der Ebene zeichnen kann, dass sich keine Kanten überschneiden.



Bem.: Jeder planare Graph unterteilt die Ebene in disjunkte Gebiete.

Eulersche Polyederformel:

$$n + \underbrace{g}_{\text{anzahl der Gebiete}} = e + 2$$

Gilt für zusammenhängende planare Graphen.

Beweis mit vollständiger Induktion über g:

IA: Es sei G ein zusammenhängender planarer Graph mit nur einem Gebiet.
Jeder planare Graph mit min. einem Kreis hat min. ein inneres Gebiet.
$\rightarrow$ G kann keinen Kreis enthalten, G ist also ein Baum. $\Rightarrow e = n - 1$,
$n + g = n + 1 = e + 2$ ✓

IS: Es sei G' ein zusammenhängender, planarer Graph mit $g + 1$ Gebieten, n' Knoten und e' Kanten.
z.z. $n' + (g + 1) \overset{!}{=} e' + 2$
G' enthält min ein inneres Gebiet, also auch einen Kreis. Wähle eine Kante auf dem Kreis, entferne diese.
$\Rightarrow$ Es entsteht der zusammenhängende, planare Graph G mit g Gebieten. $\underset{\text{I.V.}}{\Rightarrow}$ für G gilt:
$n + g = e + 2$,
$n' = n, e' = e + 1$
$\Rightarrow$ für G' gilt: $n' + (g + 1) = (n + g) + 1 = e + 3 = e' + 2$ q.e.d.

gesucht: Zusammenhang zwischen e und n (oder Schranke für e)

- edes innere Gebiet ist von mindestens drei Kanten umgeben.
- Jede Kante trennt höchstens zwei Gebiete.

Zähle paare von Gebieten und Kanten: $M := \{(\gamma, \kappa \mid \gamma \text{ ein inneres Gebiet, } \kappa \text{ eine Kante, die J begrenzt}\}$

$$\begin{aligned} g \cdot 3 \leq |M| \leq 2 \cdot e \Rightarrow g \leq \frac{2}{3}e \Leftrightarrow g + n \leq \frac{2}{3}e + n & \\ n + \frac{2}{3} \cdot e \geq n + g \underset{\text{Euler}}{=} e + 3 & \quad | - \frac{2}{3} \cdot e \\ n \geq \frac{1}{3}e + 2 & \quad | - 2 \\ n - 2 \geq \frac{1}{3}e & \quad | \cdot 3 \\ 3n - 6 \geq e & \end{aligned}$$

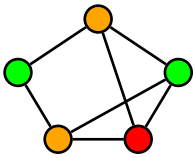
gilt für alle zusammenhängenden planaren Graphen.

5.3.1 Färbung von Graphen

Eine Färbung von G ist eine Zuordnung von Knoten auf Farben, sodass benachbarte Kanten unterschiedliche Farben besitzen.

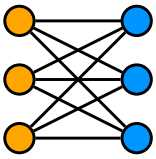
Bem.: Als „Farben“ können können die Elemente beliebiger endlicher Mengen dienen.

Bsp.:



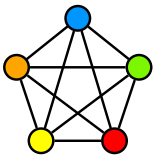
3-färbbar (d. h. es gibt eine Färbung mit 3 Farben)

K3,3



2-Färbbar
$\chi(K_{3,3}) = 2$

K5



5-Färbbar
$\chi(K_5) = 5$

Die minimale Anzahl an Farben einer Färbung von G heißt chromatische Zahl $\chi(G)$ von G.

Vier-Farben-Satz

Jede politische Landkarte kann mit vier Farben so gefärbt werden, dass benachbarte Länder verschiedene Farbe besitzen.

Beweis des Vier-Farben-Satzes 1971 von Appel und Haken. (Reduktion auf ca. 2000 einzelne Graphen, Untersuchung derselben in ca. 1200 Rechnerstunden).

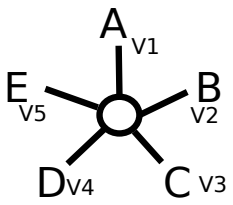
Fünf-Farben-Satz (Heowood)

Jeder planare Graph ist 5-färbbar

Beweis: Induktion über n:
IA: n = 1,2,3,4,5 ✓
IS: n ¿ 5
(Graph G' mit n+1 Kanten)
$\Rightarrow$ Es gibt einen Knoten mit $deg(v) \leq 5$
G' ist planarer Graph.

Konstruiere Teilgraph G um G' durch entfernen von V.
$\Rightarrow$ G hat n Knoten und ist planar
$\Rightarrow$ G ist 5-färbbar

I.V. Falls die Nachbarn von V weniger als 5 verschiedene Farben besitzen, kann V mit der fünften Farbe gefüllt werden. Sonst (d. h. die Nachbarn haben fünf versch. Farben)
Beweisidee:



Farben $= \{A, B, C, D, E\}$
Fall 1: Es gibt keinen „A-C, weg V_1 nach $V_3 \Rightarrow$ Vertausche die Farben A und C inder Umgebung von $V_3 \rightarrow$ Färbe V mit C.

Fall 2(sonst): Es gibt keinen „B-D“ Weg von V_2 nach V_4 Verfahre analog zu Fall 1.

6 Kombinatorik

Zufallsexperiment:

- Gegeben ist eine Urne mit n Kugeln, die von 1 bis n durchnummeriert sind.
- Ziehe k Kugeln, wieviele mögliche Ergebnisse gibt es?

mögliche Modi:

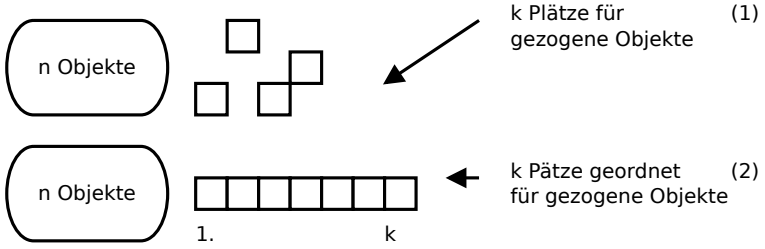
- mit zurücklegen oder ohne zurücklegen
- die Reihenfolge der gezogenen Kugeln wird beachtet, oder nicht.

Bsp.: Ziehe zwei Zahlen aus $\{1, 2, 3\}$.

1. geordnet, mit zurücklegen
   ziehe k Zahlen aus $[n]$
   Menge möglicher Ergebnisse: $[n]^k$
   Anzahl: $\left|[n]^k\right| = |[n]|^k = n^k$
   Bsp.: Mögliche Zustände eines Bytes:
   $|\{0,1\}|^8 = 2^8 = 256$ Bsp.: Anzahl der Wörter mit fünf Buchstaben über dem Alphabet $C := \{a, ..., z\}$:
   $|\{a, ..., z\}^5| = |C|^5 = 26^5$

2. geordnet, ohne zurücklegen Anzahl insgesamt:
   $n \cdot (n-1) \cdot (n-2) \cdot (n-k+1) = \prod_{j=0} k - 1(n-j)$
   $n^{\underline{k}} = \underbrace{n \cdot (n-1)...(n-k+1)}_{\text{k Faktoren}}$
   „fallende Faktorielle“ Zusammenhang mit der Fakultät:
   $n^{\underline{k}} = n!$
   $n^{\underline{n}} = \frac{n(n-1)...1}{(n-k)(n-k-1)...1}$
   $= \frac{n!}{(n-k)!}$
   Bsp.: $5^{\underline{3}} = 5 \cdot 4 \cdot 3 = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = \frac{5!}{3!} = 60$

3. ungeordnet, ohne zurücklegen



   Jedes Ergebnis im Fall (1) entspricht $k!$ Ergebnissen im Fall (2), nämlich allen $k!$ Permutationen dieser k Objekte.
   Anzahl möglicher Ergebnisse im Fall (1)
   = Anzahl möglicher Ergebnisse im Fall (2) $\cdot \frac{1}{k!}$
   $= \frac{n^{\underline{k}}}{k!} = \frac{n!}{(n-k)!\cdot n!} =: \binom{n}{k}$
   Binomialkoeffizient, „k aus n“ Bsp.: von oben: „Zwei aus Drei“ $\binom{2}{3} = \frac{3!}{1!\cdot 2!} = \frac{3\cdot 2\cdot 1}{1\cdot 2\cdot 1} = 3$ ✓
   Bsp. Lotto:
   $\binom{49}{6} = \frac{49!}{43!\cdot 6!} = \frac{49\cdot 48\cdot 47\cdot 46\cdot 45\cdot 44}{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1} = 13.983.816$ mögliche Ergebnisse
   $\Rightarrow$ Warhscheinlichkeit für sechs richtige $\approx \frac{1}{14.000.000}$

Wahrscheinlichkeit für drei Richtige:
Anzahl günstiger Ergebnisse:
$\binom{6}{3} \cdot \binom{43}{3}$

Wahrscheinlichkeit für genau drei Richtige:
$\frac{\binom{6}{3} \cdot \binom{43}{3}}{\binom{49}{6}} = \frac{6!^2 \cdot 43!^2}{3!^3 \cdot 40! \cdot 49!} = \frac{8815}{499422}$

Bem.: $\binom{n}{k}$ ist die Anzahl der Möglichkeiten, eine k-elementige Teilmenge aus einer n-elementigen Menge zu wählen.

Bsp.: Wieviele Bitstrings der Länge 8 mit fünf Einsen (und drei Nullen) gibt es?
Menge der Indizes = $\{0, 1, ..., 7\}$
Ergebnis = Anzahl fünfelementiger Teilmengen von $\{0, 1, ..., 7\}$
$= \binom{8}{5} = \binom{8}{8-5} = \binom{8}{3} = 56$
$\binom{8}{5} = \frac{n!}{k! \cdot (n-k)!} = \frac{n!}{(n-k)! \cdot (n-(n-)k)!} = \binom{n}{n-k}$

4. ungeordnet, mit zurücklegen
   mit $x_i \in \mathbb{N}, \sum_{i=1}^{n} = k$ (Gesamtzahl gezogener Objekte)
   Bsp.: 5 Objekte, ziehe 8

Objekt	Anzahl
1	3
2	0
3	1
4	2
5	2

$\Rightarrow$ | 1 | 1 | 1 | 3 | 4 | 4 | 5 | 5 |

   Anzahl der Ergebnisse = $\binom{k+n-1}{n-1} = \binom{k+n-1}{n}$

Zusatz: Ziehen aus einer Menge von Objekten, die nicht alle verschieden sind, am Beispiel des Algorithmus Permutations.

Eingabe: l Ziffern mit Häufigkeiten $n_9, ..., n_l$ mit $\sum_{i=1}^{l} n_i = n$.
Gesucht: Anzahl der der Zahlen, die sich aus diesen Ziffern bilden lassen.
Das entspricht dem Fall „geordnet, ohne zurücklegen“.
Nehme zunächst an, dass alle Ziffern unterscheidbar sind. Zähle diese Möglichkeiten und vergesse anschließend die Idendität gleicher Ziffern.
Anzahl der Möglichkeiten im Zwischenschritt:
$n^{\underline{n}} = n!$
Bsp.: alle Ziffern $1, 1, 2, ..., n-1$ (nur die 1 kommt doppelt vor)
Zwischenschritt:

- ersetze $1, 1$ durch $1a, 1b$
- zu jeder Kombination X der Ziffern gibt es genau eine Kombination X', bei der lediglich $1a$ und $1b$ vertauscht sind.
- Vergisst man die Identität von $1a, 1b$ dann führen X und X' auf dieselbe Kombination des ursprünglichen Problems

$\Rightarrow$ Anzahl der möglichkeiten im Ursprünglichen Problem $= \frac{1}{2} \cdot n!$

Im allgemeinen Fall:
Ziffern i mit Häufigkeit n_i können beliebig untereinander ausgetauscht werden $\rightarrow n_i!$ Permutationen

$\Rightarrow$ Endergebnis: $\frac{n!}{n_1!n_2!...n_l!} = \frac{n!}{\prod_{i=1}^{l} n_i!}$

Bsp.: Aufgabe 7.1
$1, 1, 3, 3, 3$
$\Rightarrow \frac{5!}{2!3!} = \frac{5\cdot 4}{2\cdot 1} = 10$ ✓

Bsp.: John hat 4 Büchsen Gulaschsuppe, 2 Dosen Ravioli und eine Fertigpizza. Wieviele Wochenspeisepläne sind möglich?
$\rightarrow$ Ziehen ohne zurücklegen, geordnet, mit ununterscheidbaren Objekten.

Bei Unterscheidbaren Mahlzeiten:
Anzahl Speisepläne $= 7^{\underline{7}} = 7!$
bei Unterscheidbaren Mahlzeiten:
Anzahl der Speisepläne $= \frac{7!}{4!2!1!} = 7 \cdot 3 \cdot 5$
$= 105$

einige Eigenschaften der Binomialkoeffizienten
fall $n, j \in \mathbb{N}, n \geq k$: $\binom{n}{k} := \frac{n!}{k!(n-k)!}$
allgemeiner:
$\alpha \in \mathbb{R}, k \in \mathbb{N}$
$\binom{\alpha}{k} := \prod_{j=1}^{k} \frac{\alpha+1-j}{j} = \frac{\alpha\cdot(\alpha-1)\cdot...\cdot(\alpha+1-k)}{k\cdot(k-1)\cdot...\cdot 1}$

im Folgenden ist jeweils $\alpha \in \mathbb{R}; k, n \in \mathbb{N}$

1. $\binom{n}{k} = 0$ falls $0 \leq n < k$
   z. B. $\binom{3}{5} = \frac{3\cdot 2\cdot 1\cdot 0\cdot(-1)}{5\cdot 4\cdot 3\cdot 2\cdot 1} = 0$
2. $\binom{n}{k} = \binom{n}{n-k}$ (Symmetrie)
3. $\binom{\alpha}{k} = \frac{\alpha\cdot...\cdot(\alpha+1-k)}{k...1}$
   $= \frac{\alpha+1-k}{k} \frac{\alpha...(\alpha+2-k)}{(k-1)...1}$
   $= \frac{\alpha+1-k}{k} \cdot \binom{\alpha}{k-1}$
4. $\binom{\alpha}{k} = \frac{\alpha}{k} \cdot \frac{(\alpha-1)...(\alpha+1-k)}{(k-1)...1}$
   $= \frac{\alpha}{k}\binom{\alpha-1}{k-1}$
5. Summenformel:
   $\binom{\alpha}{k} + \binom{\alpha}{k-1} \underset{3.}{=} \frac{\alpha+1-k}{k}\binom{\alpha}{k-1} + \binom{\alpha}{k-1}$
   $= \frac{\alpha+1}{k}\binom{\alpha}{k-1} \underbrace{-\frac{k}{k}\binom{\alpha}{k-1} + \binom{\alpha}{k-1}}_{=0}$
   $\underset{4.}{=} \binom{\alpha+1}{k}$

   $\rightarrow$ Pascalsches Dreieck

Binomealtheorem
$(a+b)^2 = a^2 + 2ab + b^2$
$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
$(a+b)^n = (a+b)(a+b)...(a+b)$

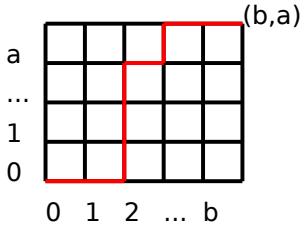
Ausmultiplizieren von $(a+b)^n$ liefert eine Summe von Termen der Form
$x_1x_2...x_n$ mit $x_i = a$ oder $x_i = b$;

jede Kombination kommt einmal vor.
$\Rightarrow$ Der Wert von $x_1x_2...x_n$ hängt nur von der Anzahl der enthaltenen a's und b's ab.
$(a+b)^n = \sum_{k=0}^{n} a^{n-k}b^k$

Folgerung:
$(1+x)^n = \sum_{k=0}^{n} 1^{n-k}x^k$
$= \sum_{k=0}^{n} \binom{n}{k} \cdot x^k$
$\Rightarrow \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k}1^k = (1+1)^n = 2^n$
$\sum_{k=0}^{n} (-1)^k\binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k = (1+(-1))^n = 0$

Monotone Gitterwege

Gegeben sein ein Rechtwinkliges Gitter.



Gesucht: Anzahl der kürzesten Wege von (0,0) nach (b,a); die Länge der kürzesten Wege ist $l = a + b$.
Die Anzahl kürzester Wege sei$w(a,l)$

falls $a = 0 : w(0,l) = 1$
falls $b = 0 : w(a,a) = 1$
falls $a > 0, b > 0$

$w(a,l) = w(a,l-1) + w(a-1,l-1)$
Beh.:
$w(a,l) \overset{!}{=} \binom{l}{a} \underset{\text{symmetrie}}{=} \binom{l}{b}$

Beweis mit vollständiger Induktion, Induktionsschritt:
$w(a,l-1) + w(a-1,l-1)$
$\underset{\text{I.V.}}{=} \binom{l-1}{a} + \binom{l-1}{a-1}$
$= \binom{l}{a}$ ✓

7 Zahlentheorie

7.1 Teilbarkeit

Def.: Es seien $m, n \in \mathbb{Z}$.

1. $m|n :\Leftrightarrow m$ ist Teiler n.
   $:\Leftrightarrow \exists t \in \mathbb{Z} : m \cdot t = n$.
2. $T_m := \{k \mid k \in \mathbb{Z}, k > 0, k|m\}$
   ist die Menge aller positiven Teiler von m
3. $T_{m,n} := T_m \cap T_n$
   ist die Menge der gemeinsamen (positiven) Teiler von m und n.
   Bsp.:
   - $3|12$, denn $3 \cdot 4 = 12$
   - $5 \not| 12$
   - $T_{12} = \{1, 2, 3, 4, 6, 12\}$
     $T_{18} = \{1, 2, 3, 6, 9, 18\}$
   - $\forall m \in \mathbb{Z} : 1|m$, denn $1 \cdot m = m$
     $m|m$
   - $\forall m \in Z : m|0$, denn $0 \cdot m = 0$
     $\rightarrow T_0 = \{t \in \mathbb{Z} \mid t > 0\}$
     $T_{0,n} = T_0 \cap T_n = T_n$

Def.: Divisionsrest
Es seien $m, n \in \mathbb{Z}, m > 0$.
Der Rest bei Division n durch m ist $n \mod m := n - \lfloor \frac{n}{m} \rfloor m$.
($\lfloor x \rfloor$ bedeutet Abrunden, also:
$\lfloor x \rfloor$ ist die größte ganze Zahl y mit $y \leq x$;
$\lceil x \rceil$ ist die kleinste Zahl $z \in \mathbb{Z}$ mit $z \geq x$)

Bez.: $n \mod m$ „n modulo m“
Bsp.:

- $7 \mod 3 = 7 - \lfloor \frac{7}{3} \rfloor \cdot 3 = 7 - \lfloor 2 + \frac{1}{3} \rfloor \cdot 3 = 7 - 2 \cdot 3 = 1$
- $-7 \mod 3 = -7 - \lfloor -2 - \frac{1}{3} \rfloor \cdot 3$
  $= -7 - (-3) \cdot 3 = -7 + 9 = 2$

Folgerung:

- falls $m|n, t \cdot m = n$
  $n \mod m = n - \lfloor \frac{n}{m} \rfloor \cdot m$
  $= n - m\lfloor t \rfloor m = n - t \cdot m = 0$
- $r := n \mod m \in \{0, ...m - 1\}$:

  1. $r \geq 0$: $\lfloor \frac{n}{m} \rfloor \leq \frac{n}{m} \rightarrow r = \lfloor \frac{n}{m} \rfloor m \overset{m>0}{\geq} n - \frac{n}{m} \cdot m = 0$

2. $r < m$:
   Setze $t := \lfloor \frac{n}{m} \rfloor$
   $r = n - t \cdot m \quad | + tm - r$
   $t \cdot m = n - r \quad | : m$
   $t = \frac{n-r}{m}$

   Annahme: $r \geq m$

$$\Rightarrow t + 1 = \frac{n-r}{m} + \frac{n}{m}$$
$$= \frac{n - (\overset{\geq 0}{r - m})}{m} \leq \frac{n}{m}$$

   also $t + 1 \in \mathbb{Z}, t + 1 \leq \frac{n}{m}$
   $\Rightarrow t$ ist nicht die größte ganze Zahl $\leq \frac{n}{m}$, widerspruc zu $t := \lfloor \frac{n}{m} \rfloor$.
   $\Rightarrow r < m$

- Falls $n = t \cdot m + r$ mit $r \in \{0, ..., m-1\}$, dann gilt $t = \lfloor \frac{n}{m} \rfloor, r = n \mod m$. (ohne Beweis)

Def.: Es seien $m, n \in \mathbb{Z}, (m, n) \neq (0, 0)$.
Dann ist ggT(m,n) der größte gemeinsame Teiler von m und n, d. h. ggT(m,n) = max. $T_{m,n}$

kgV(m,n) :=$min\{k \in \mathbb{N} \mid k > 0, m|kundn|k\}$ ist das kleinste gemeinsame Vielfache von m und n.
Bsp.:
ggT(12,18) = max($T_{12} \cap T_{18}$) = max($\{1, 2, 3, 5\}$) = 6
kgV(12,18) = 36($12 \cdot 3 = 35, 18 \cdot 2 = 36$)

Beh.: Für alle $a \in \mathbb{Z}$ ist $T_{min} = T_{m,n-a \cdot m}$

1. $T_{m,n} \leq T_{m,n-m \cdot a}$
   Es sei $x \in T_{m,n}$;
   $t, s \in \mathbb{Z}$ mit $t \cdot x = m, s \cdot x = n$.
   $x|m$ ✓
   $x|n - a \cdot m$:
   $(s - a \cdot t) \cdot x = n - a \cdot m$
   $\Rightarrow x \in T_{m,n-a \cdot m}$,
   d. h. $T_{m,n} \leq T_{m,n-a \cdot m}$

2. $T_{m,n} \geq T_{m,n-a \cdot m}$
   Es sei $x \in T_{m,n-a \cdot m}$,
   $t, s \in \mathbb{Z}$ mit $x \cdot t =, x \cdot s = n - a \cdot m$
   $x \in T_{m,n}$:
   $x|m$ ✓
   $x|n : (s + a \cdot t) \cdot x = n$
   $\rightarrow T_{m,n} \supseteq T_{m,n-a \cdot m}$,
   $T_{m,n} = T_{m,n-a \cdot m}$

   Folgerung: $T_{m,n} = T_{m,n-\lfloor \frac{n}{m} \rfloor \cdot m}$
   $= T_{m,n \mod m}$,
   $ggT(m, n) = maxT_{m,n}$
   $= maxT_{m,n \mod m}$
   $= maxT_{n \mod m,m}$
   $ggT(n \mod m, m)$

Anwendung: Euklidscher Algorithmus zur Bestimmung des ggT.

- rekursive Formulierung:
  Eingabe: $m, n \in \mathbb{Z}, m, n \geq 0, (m, n) \neq (0, 0)$
  EUKLID(m,n)
  if $m = 0$ then return n
  else return EUKLID($n \mod m, m$)
  Bsp.: ggT(18,12)
  $= ggt(\underbrace{12 \mod 18}_{=12}, 18)$
  $= ggt(\underbrace{18 \mod 12}_{=6}, 12)$
  $= ggt(\underbrace{12 \mod 6}_{=0}, 6)$
  $= 6$

- iterative Formulierung:
  EUKLID1(m,n)
  while $m \neq 0$
  tmp := m
  m := n mod m
  n := tmp
  return n

Beh.: Für alle Zahlen $m, n \in \mathbb{Z}, (m, n) \neq (0, 0), 0 \leq m \leq n \leq 2^c$ (für ein $c \in \mathbb{N}$) sei $R(m, n)$ die Anzahl rekursiver Aufrufe bei der Berechnung EUKLID(n mod m,m)
Dann ist $R(m, n) \leq 2 \cdot c + 1$.
Beweis mit vollständiger Induktion über c:
IA: $c = 0$

$\Rightarrow n = 1, m \in 0, 1.$

1. $ggT(0, 1) = 1$
   $\rightarrow R(0, 1) = 0$

2. $ggt(1, 1) = ggT(0, 1) = 1$
   $\rightarrow R(1, 1) = 1 \leq 2 \cdot 0 + 1$ ✓

IS: $0 \leq m \leq n \leq 2^{c+1}$
z.z. $R(m, n) \leq (2(c + 1) + 1)$ $ggT(m, n) = ggT(n \mod m, m)$
$= ggT(\underbrace{m \mod (n \mod m)}_{=:m'}, \underbrace{n \mod m}_{=:n'})$
$\Rightarrow m' < m$;
$n' \leq \frac{n}{2} \leq 2^c$
Fall 1: $2m > n$:
$n < 2m \rightarrow n \mod m = n - m < n - \frac{n}{2} = \frac{n}{2}$
Fall 2: $2m < n$:
$\Rightarrow n \mod m \leq m - 1 < m \leq \frac{n}{2}$

Also: Nach den ersten zwei rekursiven Aufrufen gilt: $0 \leq m' \leq n' \leq \frac{n}{2} \leq 2^c$.
Wegen Induktionsvorraussetzung gilt also

$$\begin{aligned} R(m', n') &\leq 2 \cdot c + 1 \\ \Rightarrow R(m, n) &\leq 2 + R(m', n') \\ &\leq 2 \cdot (c + 1) + 1. \quad \checkmark \end{aligned}$$

Die Laufzeit von Euklid(m,n) ist also $\leq 2 \cdot \lceil \log_2 max\{m,n\} \rceil + 2$

Der erweiterte Euklidsche Algorithmus
Beh.: $\exists x, y \in \mathbb{Z} : ggT(m,n) = x \cdot m + y \cdot n$
Beweis:
Fall 1: $m = 0 \Rightarrow ggT(m,n) = ggT(0,n) = n = 0 \cdot m + 1 \cdot n$, d. h. wähle $x := 0, y := 1$.
Fall 2: $m > 0 \Rightarrow ggT(m,n) = ggT(n \mod m, m)$

Beweis mit volständiger Induktion:
IA: $m = 0$ ✓(s. o.)
IS: IV: $\forall m' < m : \exists x, y \in \mathbb{Z} : ggT(m',n) = x \cdot m' + y \cdot n$.
z. z.: Dann gilt:
$\exists x', y' \in \mathbb{Z} : x' \cdot m + y' \cdot n = ggT(m,n)$

$$ggT(m,n) = ggT(\underbrace{n \mod m}_{=:m', m' < m}, m)$$
$$\overset{IV.}{=} x \cdot m' + y \cdot m$$
$$= x \cdot (n - \lfloor \tfrac{n}{m} \rfloor \cdot m) + y \cdot m$$
$$= \underbrace{(y - x \cdot \lfloor \frac{n}{m} \rfloor)}_{=x'} \cdot m + \underbrace{x}_{=y'} \cdot m \checkmark$$

erweiterter Euklidscher Algorithmus:
Eingabe (wie zuvor), $m, n \in \mathbb{N}, (m,n) \neq (0,0)$
Ausgabe: $d, x, y)$ mit $d = ggT(m,n) = x \cdot m + y \cdot n$
ExtendedEuklid(m,n)
  if m = 0 then return (n,0,1)
  else
    (d,x,y):= ExtendedEuklid(n mod m, m)
    return (d, $y - x\lfloor \frac{n}{m} \rfloor, x$)

Bsp. (für die Ausführung des erweiterten Euklidischen Algorithmus).

$ggT(48,27) = x \cdot 48 + y \cot 27$
$m_0 = 48, n_0 = 27;$
$m_{i+1} = n_i, n_{i+1} = m_i \mod n_i = m_i - \lfloor \frac{m_i}{n_i} \rfloor \cdot n_i$
$x_{i-1}, y_{i-1} = ?$
$ggT(m_{i+1}, n_{i+1}) = x_{i+1}m_{i+1} + y_{i+1}n_{i+1}$
$= y_{i+1}m_i + (x_{i+1} - \lfloor \frac{m_i}{n_i} \rfloor y_{i+1})n_i$
$= ggT(m_0, n_0)$

i	n_i	m_i	y_i	x_i
0	48	27	4	$-3 - \lfloor \frac{48}{27} \rfloor \cdot 4 = -7$
1	27	21	-3	$1 - \lfloor \frac{27}{21} \rfloor \cdot (-3) = 4$
2	21	6	1	$0 - \lfloor \frac{21}{6} \rfloor \cdot 1 = -3$
3	6	3	0	$1 - \lfloor \frac{6}{3} \rfloor \cdot 0 = -1$
4	3	0	1	0

$4 \cdot 48 - 7 \cdot 27 = 160 + 32 - 140 - 40 = 3 = ggT(48,27)$

Den ggT braucht man z.B. zum Vollständigen lürzen von Brüchen.

Anwendungsbeispiel für den erweiterten Euklidischen Algorithmus:
geg. zwei Meßlatten der Längen
  $l_1 = 48$cm , $l_2 = 27$cm
Damit kann man die Länge l = 3cm (ggt(48,27)=3) vermessen:

$\underset{=4}{x} \cdot 48 + \underset{=-7}{y} \cdot 27 = 3$
$\rightarrow 4 \cdot l_1$ abmessen, $7 \cdot l_2$ abziehen.

7.2 Primzahlen

Jede ganze Zahl n hat min. die trivialen Teiler 1 und n.
Def.: $p \in \mathbb{N}$ heißt Primzahl, wenn p genau zwei positive Teiler besitzt (1 und p).

Die kleinsten Primzahlen sind:
$2, 3, 5, 7, 11, 13, 17, 19$

Beh.: Jede natürliche Zahl ≥ 1 kann als Produkt von Primzahlen geschrieben werden.

Beweis mit vollst. Induktion:
alternative Formulierung der Beh.:
Alle positiven natürlichen Zahlen $\leq n$ lassen sich als Primzahlprodukt schreiben. ($n \geq 1$ beliebig)

IA: $n = 1 \rightarrow 1$ ist der Wert des leeren Produkts. ✓
IS: IV.: alle Zahlen $\leq n$ sind Primzahlprodukte
zu zeigen: alle Zahlen $\leq n+1$ sind Primzahlprodukte
Es genügt, zu zeigen: $n+1$ ist Primzahlprodukt
Fall 1:
$\rightarrow$ n+1 ist Primzahlprodukt mit nur einem Faktor. Fall 2:
$n+1$ ist keine Primzahl,
$n+1 = k \cdot l$ mit $1 < k, l < n+1$
$\overset{\text{IV.}}{\Rightarrow} k$ und l sind Primzahlprodukte
$\Rightarrow n+1 = k \cdot l$ ist auch Primzahlprodukt. □

Die Darstellung einer Zahl $n \in \mathbb{N}$ als Primzahlprodukt $n = p_1 p_2 \dots p_k$ heißt auch Primfaktorzerlegung von n (PFZ), die p_i sind Primfaktoren von n.

Satz: Die Primfaktorzerlegung
$n = p_1 p_2 \dots p_k, \quad p_1 \leq p_2 \leq \dots \leq p_k$

Beweis:
IA: n = 1 (leeres Produkt) ist eindeutig ✓
IS: n+1 habe zwei verschiedene PFZ, $n+1 = p_1 \dots p_r = q_1 \dots q_s$ mit $p_1 \leq \dots \leq p_r, q_1 \leq \dots \leq q_s$
1. Fall: $p_1 = q_1 \Rightarrow \frac{n+1}{p_1} = p_2 \dots p_r = q_2 \dots q_s = \frac{n+1}{q_1}$
IV: $\rightarrow$ PFZ von $\frac{n+1}{p_1} \leq n$ ist eindeutig
$\Rightarrow r = s, p_i = q_i$
$\Rightarrow$ Die PFZen von $p_1, \dots, p_r$ und $q_1, \dots, q_r$ sind gar nicht verschieden, Widerspruch.

2. Fall: $p_1 < q_1$
$p_1 | n+1 = q_1 \dots q_s$
$p_1 | p_1 q_2 \dots q_s$
$\Rightarrow p_1 | (q_1 - p_1) q_2 \dots q_s$
$q_2, \dots, q_s$ sind nicht durch p_1 teilbar, denn $q_2, \dots, q_s \geq q_1 > p_1$.
$\curvearrowright p_1 | q_1 - p_1 \curvearrowright p_1 | q_1$, aber $p_1 < q_i \Rightarrow$ Widerspruch.

3. Fall: $p_1 > q_1$: analofg zu Fall 2.

$\Rightarrow$ PFZ von $n+1$ ist eindeutig. □

Häufig faßt man gleiche Primfaktoren zu Potenzen zusammen:

$n = \sum_{i=1}^{n} p_i^{e_i}$ mit $p_1 < p_2 < \cdots < p_k$
Ist $p_i \not| n$, muss natürlich $e_i = 0$ sein.

Es ist nützlich, alle Primzahlen in das Produkt aufzunehmen:
$n = \prod_{i=1}^{\infty} p_i^{e_i}$
Wir können jede Zahl $n \in \mathbb{N}, n > 0$ durch die unendliche folge $e_1, e_2, e_3, \dots$ von Exponenten in der PFZ darstellen.

Definiere die Hilfsfunktion
$P(n) := (e_1, e_2, e_3, \dots$
(„P liefert die PFZ einer beliebigen Zahl“)

P ist eine Bijektion, da die PFZ eineindeutig ist.
Rechenregeln für P:
(Es seien $P(m) = (m_1, m_2, m_3, \dots)$
und $P(n) = (n_1, n_2, n_3, \dots))$

- $P(m \cdot n) = ?$
  $m \cdot n = (\prod_{i=1}^{\infty} p_i^{m_i})(\prod_{i=1}^{\infty} p_i^{n_i})$
  $= \prod_{i=1}^{\infty} p_i^{m_i+n_i}$
  $\Rightarrow P(m \cdot n) = (m_1 + n_1, m_2 + n_2, m_3 + n_3, \dots)$
- falls $n|m : P(\frac{m}{n}) = (m_1 - n_1, m_2 - n_2, m_3 - n_3)$ (analog)
- $P(ggT(m,n)) = ?$
  $ggT(m,n) = ggT(\prod_{i=1}^{\infty} p_i^{m_i}, \prod_{i=1}^{\infty} p_i^{n_i})$
  $= \prod_{i=1} \infty p_i^{min(m_i,n_i)} \curvearrowright P(ggT(m,n)) = (min(m_1,n_1), min(m_2,n_2), min(m_3,n_3), \dots)$
- $P(kgV(m,n)) = (max(m_1,n_1), max(m_2,n_2), max(m_3,n_3), \dots)$
- $P(ggT(m,n) \cdot kgV(m,n)) = (min(m_1,n_1)+max(m_1,n_1), min(m_2,n_2)+max(m_2,n_2), min(m_3,n_3)+max(m_3,n_3), \dots)$
  $= (m_1 + n_1, m_2 + n_2, \dots)$
  $= P(m,n)$

P ist injektiv $\Rightarrow ggT(m,n) \cdot kgV(m,n) = m \cdot n$
$kgV(m,n) = \frac{m \cdot n}{ggT(m,n)}$
(Kann mit Euklid berechnet werden.)

Anwendung der PFZ:
$\sqrt{2}$ ist irrational (d. h. nicht rational, d. h. kein Bruch)
Annahme: $\exists \frac{a}{b} \in \mathbb{Q} : \left(\frac{a}{b}\right)^2 = 2$
$\Rightarrow \underbrace{a^2}_{\text{gerade..}} = \underbrace{2b^2}_{\text{ungerade..}}$
.. Anzahl an Zweiern in der PFZ
aber PFZ ist eindeutig
$\Rightarrow a^2 \neq 2b^2$
$\rightarrow$ Widerspruch, $\sqrt{2} \notin \mathbb{Q}$

Def.: Zwei Zahlen $m, n \in \mathbb{N}; m, n > 0$ mit $ggT(m,n) = 1$ heißen teilerfremd. (Abk.: $m \perp n$)

Bsp.: Ein Bruch $\frac{a}{b}$ ist vollständig gekürzt, wenn $a \perp b$.
$\frac{16}{9}$ ist vollständig gekürzt, $16 \perp 9$.

Frage: Warum gibt es unendlich viele Primzahlen?
Annahme: Es gibt nur k verschiedene Primzahlen $p_1, \ldots, p_k$
Konstruiere eine weitere Prizahl $P := p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$

- p ist nicht teilbar durch $p_1, p_2, \ldots, p_k$
- also: Die PFZ von p enthält keine der Primzahlen $p_1, \cdot, p_k$, also muss sie aus „neuen" Primzahlen bestehen.

$\Rightarrow$ Widerspruch. $\square$

Primzahlsatz:
$\pi(n) := |\{p \leq n \mid p \text{ ist Primzahl }\}|$
(Anzahl Primzahlen $\leq n$)
$\pi(n) \underset{\text{asymptotisch äquivalent}}{\sim} \frac{n}{\log n} \left(\pi(n) \cdot \frac{\log n}{n} \underset{n\to\infty}{\longrightarrow} 1\right)$

7.3 Kongruenzen

Es seien $a, b, m \in \mathbb{Z}, m > 0$.
$a \equiv b(\mod m) :\Leftrightarrow a \mod m = b \mod m \Leftrightarrow m|(a-b)$
„a ist kongruent zu b modulo m"

Wir haben bereits gesehen (Aufgabe 3.5 zur Vorlesung) dass $\equiv$ (mod m) eine Äquivalenzrelation ist. Diese hat m verschiedene Äquivalenzklassen:
$[0]_{\equiv \mod m} = \{t \cdot m + 0 \mid t \in \mathbb{Z}\}$
$[1]_{\equiv \mod m} = \{t \cdot m + 1 \mid t \in \mathbb{Z}\}$
...
$[m-1]_{\equiv \mod m} = \{t \cdot m + (m-1) \mid t \in \mathbb{Z}\}$

zum Rechnen mit Resten:
$(a+b) \mod m = (a + (b \mod m)) \mod m$:
$a + (b \mod m) = a + b - \lfloor \frac{b}{m} \rfloor m$
$\curvearrowright (a + (b \mod m)) \mod m$
$= (a + b - \lfloor \frac{b}{m} \rfloor m) - \lfloor \frac{a+b-\lfloor \frac{b}{m} \rfloor m}{m} \rfloor m$
$= a + b - \lfloor \frac{b}{m} \rfloor m - (-\lfloor \frac{b}{m} + \lfloor \frac{a+b}{m} \rfloor) m$
$= a + b - (\lfloor \frac{a+b}{m} \rfloor) m$
$= (a+b) \mod m$

$\Rightarrow (a+b) \mod m = (a + (b \mod m)) \mod m$
$= ((a \mod m) + (b \mod m)) \mod m$
vertausche Rollen von a und b

- analog: $(a-b) \mod m = ((a \mod m) - (b \mod m)) \mod m$
- $(a \cdot b) \mod m = (\underbrace{a + \cdots + a}_{\text{b-mal}}) \mod m$
  $= (\underbrace{(a \mod m) + \cdots + (a \mod m)}_{\text{b-mal}}) \mod m$

$= ((a \mod m) \cdot b) \mod m$
$= ((a \mod m) \cdot (b \mod m)) \mod m$

Bsp.: $(3.8\dot{1}0^9 + 378956743) \mod 5$
$= ((3.8\dot{1}0^9 \mod 5) + (378956743 \mod 5)) \mod 5$
$= (0 + 3) \mod 5 = 3$

Rechenregeln für Kongruenzen
Es seien $a \equiv b(\mod m), c \equiv d(\mod m)$
$\Rightarrow (a + c) \equiv b + d(\mod m)$
$(a - c) \equiv b - d(\mod m)$
$(a \cdot c) \equiv b \cdot d(\mod m)$
Beweis:
$a \pm c \equiv a \pm d(\mod m)$
$\Leftrightarrow m| \underbrace{(a \pm b) - (c \pm d)}_{=(a-b)\pm(c-d)}$
$m|(a - b), m|(c - d)$
$\Rightarrow m|\,[(a - b) \pm (c - d)]$ ✓

$a \cdot c \equiv b \cdot d(\mod m)$
$\Leftrightarrow m| \underbrace{a \cdot c - b \cdot d}$
$= a \cdot c - b \cdot c + b \cdot c - b \cdot d$
$= \underbrace{(a - b)}_{\text{Vielfache von m}} \cdot c + b \cdot \underbrace{(c - d)}$ □

Inverse modulo m
Wann gibt es $x \in \mathbb{Z}$ mit
$a \cdot x \equiv 1(\mod m)$?

- falls ggT(a,m) = 1:
  erweiterter Euklidischer Algorithmus liefert $x, y \in \mathbb{Z}$ mit
  $a \cdot x + m \cdot y = ggT(a, m) = 1$
  $\Rightarrow \underbrace{a \cdot x = m \cdot y}_{\equiv 1} = a \cdot x(\mod m)$
  $\Rightarrow x$ aus dem erw. Eukl. Alg. ist genau das Inverse von a.
  Bez.: $x = a^{-1}$ oder $x = a^{-1}_{\mod m}$
- falls $d := ggt(a, m) > 1$:
  $(a \cdot x) \mod m = \underbrace{a \cdot x - \left\lfloor \frac{a \cdot x}{m} \right\rfloor m}_{\text{teilbar durch d}}$
  $\Rightarrow d|(a \cdot x) \mod m$,
  aber $d \not| 1$
  $\Rightarrow (a \cdot x) \mod m \neq 1 \mod m$
  $\Leftrightarrow a \cdot x \not\equiv 1(\mod m)$
  Also hat a kein Inverses modulo m.

Man kann zeigen:
Falls $a \perp m$, dann gibt es ein eindeutiges Inverses $a^{-1}_{\mod m} \in \mathbb{Z}_m := \{0, 1, \ldots, m - 1\}$

Menge der Zahlen mit Inversen modulo m:
$\mathbb{Z}_m^x := \{a \in \mathbb{Z}_m \mid a \perp m\}$

Bsp.:
$\mathbb{Z}_2^x = \{1\}, Z_3^x = \{1, 2\}$

$(1^{-1} = 1, 2^{-1} = 2 : 2 \cdot 2 \mod 3 = 1)$
$\mathbb{Z}_4^x = \{1, 3\}, \mathbb{Z}_5^x = \{1, 2, 3, 4\}$
$\mathbb{Z}_6^x = \{1, 4, 5\}$

Damit lassen sich lineare Kongruenzen lösen:
$a \cdot x \equiv b(\mod m)$
mit $a \in \mathbb{Z}_m^x, b \in \mathbb{Z}_m$
$x := a^{-1} \cdot b \mod m$
$\rightarrow a \cdot x = a(a^{-1} \cdot b) \mod m$
$\equiv \underbrace{(a \cdot a^{-1})}_{\equiv 1} \cdot b \equiv b(\mod m)$
Diese Lösung für x ist eindeutig in $\mathbb{Z}_m$.

„Wie groß ist $\mathbb{Z}_m^x$?“
Def.: $\phi(m) := |\mathbb{Z}_m^x|$

Eulersche Phi-Funktion
Wir wissen:

- falls p Primzahl ist: $\phi(p) = |\{1, ..., p-1\}| = p - 1$.
- für Primzahlpotenzen gilt:
  $\phi(p^k) = |\mathbb{Z}_{p^k} \backslash \{0, p, 2 \cdot p, 3 \cdot p, ..., p^k - p\}|$
  größtes Vielfaches von $p \leq p^k$ ist p^k; ... $p < p^k$ ist $p^k - p$
  $\curvearrowright \phi(p^k) = |\mathbb{Z}_{p^k}| - |\{0, p, 2p, ..., p^k - p\}|$
  $= p^k - \frac{p^k}{p} = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$
  Bsp.:
  $|\mathbb{Z}_{125}^x| = \phi(125)$
  $= \phi(5^3) = 5^3(1 - \frac{1}{5}) = 100$
- allgemeiner Fall: $m = \prod_{i=1}^{k} p_i^{m_i} \leftarrow$ Primfaktorzerlegung
  $\phi(m) = \phi\left(\prod_{i=1}^{k} p_i^{m_i}\right) = ?$
  Zusammenhang zwischen
  $\mathbb{Z}^x_{p_1^{m_k} ... p_k^{m_k}}$ und $\mathbb{Z}_{p_1^{m_k}}, ..., \mathbb{Z}^x_{p_k^{m_k}}$?

Chinesischer Restsatz
Gibt es eine Lösung x des Systems von Kongruenzen?
$c_1 \cdot x \equiv d_1(\mod m)$
$c_2 \cdot x \equiv d_2(\mod n)$
(Hierbei seien $c_1 \in \mathbb{Z}_m^x, c_2 \in \mathbb{Z}_n^x, d_1, d_2 \in \mathbb{Z}$)
Multipliziere mit c_1^{-1}, c_2^{-1}
$x \equiv c_1^{-1} d_1(\mod m)$
$x \equiv c_2^{-1} d_2(\mod m)$
setze:
$a := c_1^{-1} \cdot d_1 \in \mathbb{Z}_m,$
$b := c_2^{-1} \cdot d_2$
Ansatz: $x = y \cdot m + z \cdot n$ mit $y, z \in \mathbb{Z}$
$\rightarrow x \mod m = z \cdot n \mod m \overset{!}{\equiv} a$
$x \mod n = y \cdot m \mod n \overset{!}{\equiv} b$
löse also $z \cdot n \equiv a(\mod m)$ nach z
auf, $y \cdot m \equiv b(\mod n)$ nach y.

Falls $m \perp n$:
$z = a \cdot n^{-1}_{\bmod m}, y = b \cdot m^{-1}_{\bmod n}$
$\Rightarrow x = b \cdot m^{-1}_{\bmod n} \cdot m + a \cdot n^{-1}_{\bmod m} \cdot n$
Man kann zeigen: x ist eindeutig bis auf Vielfache von $m \cdot n$.
Zu jedem Paar $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ gibt es eine eindeutige Lösung $x \in \mathbb{Z}_{m \cdot n}$.
Definiere die Funktion $\psi : \mathbb{Z}_{m \cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n$;
$\psi(x) := (x \mod m, x \mod n)$.
ψ ist also bijektiv.
$\curvearrowright |\mathbb{Z}_{m \cdot n}| = |\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n|$

Eigenschaften vo ψ:

- ψ ist bijektiv
- $\psi(1) = (1, 1)$
  $\psi(0) = (0, 0)$
- $\psi((x + y) \mod (m \cdot n)) = \psi(x) + \psi(y)$,
  wobei $(a, b) + (c, d) := (a + c \mod m, b + d \mod n)$
- $\psi(x \cdot y) \mod (m \cdot n) = \psi(x) \cdot \psi(y)$, mit $(a, b)(c, d) = ((a \cdot c) \mod m, (b \cdot d) \mod n)$

$(x \cdot y) \mod (m \mod n) = x \cdot y - \left\lfloor \frac{x \cdot y}{m \cdot n} \right\rfloor \cdot m \cdot n$
$\curvearrowright (x \cdot y) \mod (m \mod n) \equiv x\dot{y}(\mod m)$
$(x \cdot y) \mod (m \mod n) \equiv x \cdot y(\mod n)$
$\Rightarrow \psi((x \cdot y) \mod (m \cdot n)) = ((x \cdot y) \mod m, (x \cdot y) \mod n)$
$= ((x \mod m)(y \mod m) \mod m, (x \mod n)(y \mod n) \mod n)$
$= \psi(x) \cdot \psi(x)$

Eingaben $\in \mathbb{Z}_{m \cdot n}$	$\xrightarrow[\psi]{}$	Eingabe $\in \mathbb{Z}_m \times \mathbb{Z}_n$
Richtung in $\mathbb{Z}_{m \cdot n} \downarrow$		$\downarrow$Richtung in $\mathbb{Z}_m \times \mathbb{Z}_n$
Ergebnis in $\mathbb{Z}_{m \cdot n}$	$\xleftarrow[\psi^{-1}]{}$	Ergebnis in $\mathbb{Z}_m \times \mathbb{Z}_n$

$(x \cdot y) \mod (m \cdot n) = 1$
$\Leftrightarrow \psi(x) \cdot \psi(y) = \psi((x \cdot y) \mod (m \cdot n)) = (1, 1)$
Also: $(x_1, x_2) := \psi(x), (y_1, y_2) := \psi(y)$
$\Rightarrow x_1\dot{y}_1 \mod m = 1$,
$x_2\dot{y}_2 \mod m = 1$
also: $x_1 \in \mathbb{Z}^x_m$
$x_x \in \mathbb{Z}^x_n$.

ψ ist also auch eine Bijektion zwischen $\mathbb{Z}^x_{m \cdot n}$ und $\mathbb{Z}^x_m \times \mathbb{Z}^x_n$.
$\Rightarrow |\mathbb{Z}^x_{m \cdot n}| = |\mathbb{Z}^x_m \times \mathbb{Z}^x_n| = |\mathbb{Z}^x_m| \cdot |\mathbb{Z}^x_n|$
Konsequenz für $\phi\left(\prod_{i=1}^{k} p_i^{m_i}\right)$:
$p_i^{m_i} \perp p_j^{m_j}$ für $i \neq j$
$\curvearrowright |\mathbb{Z}^x_{p_1^{m_1} \ldots p_k^{m_k}}| = |\mathbb{Z}^x_{p_1^{m_1}}| \ldots |\mathbb{Z}^x_{p_k^{m_k}}|$
$= p_1^{m_1}\left(1 - \frac{1}{p_1}\right) \ldots p_k^{m_k}\left(1 - \frac{1}{p_k}\right)$
$m \prod_{p|m} \left(1 - \frac{1}{p}\right)$

Bsp.: $\phi(100) = |\mathbb{Z}_{100}^x|$

$= \phi(2^2 \cdot 5^2) = 100 \cdot \underbrace{(1 - \frac{1}{2})}_{=\frac{1}{2}} \cdot \underbrace{(1 - \frac{1}{5})}_{=\frac{4}{5}}$

$= 40$

$\phi(2) = 2 \cdot \left(1 - \frac{1}{2}\right) = 1$
$\phi(3) = 3 \cdot \left(1 - \frac{1}{3}\right) = 2$
$\phi(4) = 4 \cdot \left(1 - \frac{1}{2}\right) = 2$
$\phi(5) = 5 \cdot \left(1 - \frac{1}{5}\right) = 4$
$\phi(6) = 6 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2$

8 Algebra

algebraische Strukturen, Beispiele:

Gruppe:	$(S_n, \circ), (\mathbb{Z}_m^x, \cdot), (\mathbb{Z}, +)$
Ring:	$(\mathbb{Z}, +, \cdot), \mathbb{Z}, +, \cdot)$
Körper	$\mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$ (p Primzahl)
Vektorräume	$\mathbb{R}^3$

8.1 Gruppen

Def.: Gegeben seien eine Menge G und eine binäre Operation $*$: $G \times G \mapsto G$.
(G,$*$) heißt Gruppe, falls folgende Axiome gelten:

(G1) $\forall a, b, c \in G : (a * b) * c = a * (b * c)$ (assoziativgesetz)
(G2) $\exists e \in G : \forall a \in G : a * e = a$ (neutrales Element)
(G3) $\forall a \in G : \exists a^{-1} \in G : a \cdot a^{-1} = e$ (Inverses)

(G,$*$) heißt Abelsche oder kommutative Gruppe, wenn zusätzlich gilt:
(G4) $\forall a, b \in G : a * b = b * a$.

Bem.: Wenn die Verknüpfung $*$ aus dem Kontext hervorgeht, bezeichnet man auch G als Gruppe.

Beispiele:

1. $(\mathbb{Z}, +)$ ist eine Kommutative Gruppe:
   (G1) $(a + b) + c = a + (b + c)$ ✓
   (G2) $a + 0 = a$ ✓
   (G3) $a^{-1} := -a; a + (-a) = 0$ ✓
   (G4) $a + b = b + a$ ✓

2. $(\mathbb{Z}_m^x, \cdot)$
   (G1) $((a \cdot b) \mod m \cdot c) \mod m = (a \cdot ((b \cdot c) \mod m)) \mod m$ ✓
   (G2) $a \cdot 1 \mod m = a$ ✓
   (G3) $\exists a^{-1} \in \mathbb{Z}_m^x : a \cdot a^{-1} \mod m = 1$ ✓
   (G4) $(a \cdot b) \mod m = (b \cdot a) \mod m$ ✓
   $\rightsquigarrow$ $(\mathbb{Z}_m^x, \cdot)$ ist eine kommutative Gruppe

3. aber: $(\mathbb{Z}_m, \cdot)$ ist keine Gruppe, weil z. B. $0 \in \mathbb{Z}_m$ kein Inverses besitzt.

4. $(S_n, \circ)$ ist eine Gruppe, aber nicht Kommutativ:
   (G1) ✓
   (G2) $id : x \mapsto x, \sigma \circ id = \sigma$ ✓
   (G3) $\exists \sigma^{-1} \in S_n : \sigma \circ \sigma^{-1} = id$ ✓
   (G4) $(12) \circ (23) = (123) \neq (23) \circ (12) = (132)$

Es gilt stets:

1. $a^{-1} * a = e$
2. $e * a = a^{-1}$
3. $(a^{-1})^{-1} = a$
4. $(a * b)^{-1} = b^{-1} * a^{-1}$

Eindeutigkeit des Inversen

$\curvearrowright (a*b)^{-1} = b^{-1} * a^{-1} \square$

Die Gleichungen
$a * x = b, \quad y * a = b$
besitzen die eindeutigen Lösungen:
$x = a^{-1} * b, \quad y = b * a^{-1}$.
(Es sei $a * x = b = a * x'$)
$\Rightarrow x = a^{-1} * (a * x) = a^{-1} * (a * x') = x'$
Die Eindeutigkeit von y folgt analog.
Folgerung: Das neutrale Element und die inversen Elemente sind Eindeutig

Untergruppen

Def.: $(G, *), (U, *)$ seien Gruppen, $U \subseteq G$ Dann heißt U Untergruppe von G
(Schreibweise: $U \leq G$)

Bsp.:
$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$

- Es sei G eine endliche Gruppe, $a \in G$.
  $< a >:= \{a^0, a, a^2, a^3, ...\}$
  ($a^n = \underbrace{a * ... * a}_{\text{n-mal a}}$)
  $a^0 = e < a >$ heißt die von a erzeugte Gruppe.
  $< a >$ ist die kleinste Untergruppe von G, die a enthält.
  Beispiel: $G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$
  $\curvearrowright < 2 >= \{1, 2, 2^2 = 4, 2^3 \equiv 1(\mod 7)\} = \{1, 2, 4\}$,
  $< 2 > \leq \mathbb{Z}_7^*$
  Bem.: Jede Gruppe G hat zwei triviale Untergruppen, $G \leq G$ und $\{e\} \leq G$. Alle anderen Untergruppen von G sind nichttrivial.

Satz von Lagrange
Es seien $U \leq G$ Gruppen , G endlich. Dann ist $|U| \,\big|\, |G|$,

Def.: Für $x \in G$ definiert man die Nebenklasse von U in G,
$x * U := \{x * a \mid a \in U\}$
Bsp.: $(Z_6, +) \geq < 3 >= \{0, 3\}$
Nebenklassen von $< 3 >$ in $\mathbb{Z}_6$:
$0 + < 3 >= \{0 + 0, 0 + 3\} = \{0, 3\} = 3 + < 3 >$
$1 + < 3 >= \{1 + 0, 1 + 3\} = \{1, 4\} = 4 + < 3 >$
$2 + < 3 >= \{2 + 0, 2 + 3\} = \{2, 5\} = 5 + < 3 >$

Die Nebenklassen von U in Gbilden eine Partition von G:

1. Überdeckung: $\bigcup\limits_{x \in G} (x * U) \overset{!}{=} G$
   Es sei $x \in G$ beliebig gewählt.
   $\Rightarrow x \in x * U$, denn $x = x * e \in x * U$
   $\curvearrowright G \subseteq \bigcup\limits_{c \in G} (x * U)$ ✓
2. Disjunktheit:
   Es sei $z \in (x * U) \wedge (y * U) \neq \emptyset$
   zu zeigen: $x * U = y * U$
   (wir zeigen: $x * U \subseteq y * U; x * U \supseteq y * U$ folgt analog)

Es sei $a \in x * U, a = x * a_x$ mit $a_x \in U$.
$z = x * z_x = y * z_y$, wobei $x_z, z_y \in U$.
$a = x * a_x = (x * z_x) * z_x^{-1} * a_x$
$= (x * \underbrace{z_y) * z_x^{-1} * a_x}_{\in U}$
$\Rightarrow a \in y + U$. $\square$

3. Alle Nebenklassen $x * I$ sind gleichmächtig.
(Beweisidee: Finde eine Bijektion zwischen $x * U$ und $e * U, |e * U| = |U|$)

Beweis des Satzes von Lagrange

Wähle $M \subseteq G$, so dass:
$G = \biguplus_{x \in M} (x * U)$ d. h. $x_1 * U \neq x_2 * U$, für $x_1 \neq x_2$
$|G| = \sum_{x \in M} |x * U| = \sum_{x \in M} |U| = |M| \cdot |U|$
$\rightarrow |U| \cdot |G|$ $\square$

Es sei G eine endliche Gruppe, $a \in G$.
Betrachte $< a >:= \{a^0, a^1, a^2, ...\}$
G ist endlich. $\Rightarrow \exists s, t \in \mathbb{N} : a^s = a^t, s < t$.
$\Rightarrow a^{t-s} = e$
D. h. $\exists n > 0 : a^n = e$ $(n = t - s)$

Def.: Die Ordnung von a, $ord(a)$ ist die kleinste Zahl $n > 0$, so dass $a^n = e$.
$\Rightarrow < a >= \{a^1, a^2, a^3, ..., a^{ord(a)} = e\}$
also: $| < a > | = ord(a)$

Folgerung:
$< a > \leq G \overset{\text{Lagrange}}{\Rightarrow} |G| = m \cdot | < a > |$,
$a^{|G|} = \left(a^{|<a>|}\right)^m = \underbrace{\left(a^{ord(a)}\right)^m}_{=e} = e$.

Beispiele:

- Satz von Fermat
Es sei p eine Primzahl, $a \in \{1, ..., p-1\}$.
$\Rightarrow a^{p-1} = a^{|\mathbb{Z}_p^x|} \equiv 1(\mod p)$.

- Satz von Euler:
Es sei $n > 1; |\mathbb{Z}_n^x| = \phi(n), a \in \mathbb{Z}_n^x$
$\rightarrow a^{\phi(n)} = a^{|\mathbb{Z}_n^x|} \equiv 1(\mod n)$

Beispiel:
$7^{243} \mod 300 = ?$
$|\mathbb{Z}_{300}^x| = \phi(300) = \phi(2^2 \cdot 3 \cdot 5^2)$
$= 300 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5})$
$= 300 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 10 \cdot 2 \cdot 4 = 80$
$\overset{\text{Euler}}{\underset{7 \perp 300}{\rightarrow}} 7^{80} \equiv 1(\mod 300)$,
$7^{243} = \underbrace{(7^{80})^3}_{\equiv 1} \cdot 7^3 \equiv 7^3 \equiv 343(\mod 300) \equiv 43(\mod 300)$

n zusammengesetz, keine Camichael-Zahl:
$U := \{a \in \mathbb{Z}_n^x \mid a^{n-1} \equiv 1(\mod n)\} \neq \mathbb{Z}_n^x$

Falls $U \leq \mathbb{Z}_n^x$:
$|u||\mathbb{Z}_n^x| \to |\mathbb{Z}_n^x| = m \cdot |U|$
$\to |U| \leq \frac{1}{2}|\mathbb{Z}_n^x|$

Ist $U \leq \mathbb{Z}_n^x$?
$\mathbb{Z}_n^x$ ist endlich $\Rightarrow$ Prüfe (G0) !
Wähle $a, b \in U$ beliebig.
$\Rightarrow (ab)^{n-1} = \underbrace{a^{n-1}}_{\equiv 1} \cdot \underbrace{b^{n-1}}_{\equiv 1} \equiv 1(\mod n)$
$\Rightarrow ab \in I$, also: $U \leq G = \mathbb{Z}_n^x$

RSA-Public-Key-Kryptosystem

geheime Nachricht: $m \in \mathbb{Z}_n$
verschlüsselte Nachricht: $c \in \mathbb{Z}_n$

Schlüsselkonstruktion:

1. Primzahlen $p \neq q, n := p \cdot q$
   $\phi(n) = n(1 - \frac{1}{p})(1 - \frac{1}{q}) = (p-1)(q-1)$
2. geheimer Schlüssel:
   Zufallszahl d (für „decryption“)
   $\in \mathbb{Z}_{\phi(n)}^x$
3. öffentlicher Schlüssel:
   $(\underbrace{d^{-1}_{\mod \phi(n)}}_{mitEuklid}, n)$
   „encryption“ := e

Protokoll:

A		B
		m
	$\to c := m^e(\mod n)$	
	$\swarrow$	
berechtet		
$c^d \mod n = m$		

1. Fall:

$m \perp n, m \in \mathbb{Z}_n^x$
$\Rightarrow c^d \equiv (m^e)^d \equiv m^{e \cdot d}(\mod n)$
$m^{\mathbb{Z}_n^x} = m^{\phi(n)} \equiv 1(\mod n)$
$\to c^d \equiv m^{e \cdot d} \equiv m^{(e \cdot d) \mod \phi(n)} \equiv m^1(\mod n)$

2. Fall:
$ggT(m, n) > 1$, entweder $ggT(m, n) = p$ oder $ggT(m, n) = q$
hier: $ggT(m, n) = p$

Chinesischer Restsatz:
Der Lösung von $x \equiv m^{e \cdot d}(\mod n)$ (t)
entspricht genau einer Lösung von
$x \equiv m^{e \cdot d}(\mod p)(*)$

$x \equiv m^{e \cdot d}(\mod q)(*)$
Wir zeigen, dass $x = m$ die von $(*)$ ist, und deshalb auch von (t)

$p|m \Rightarrow m \equiv 0(\mod p)$
$\curvearrowright m^{e \cdot d} \equiv 0^{e \cdot d} = 0(\mod p)$
$\Rightarrow m \equiv m^{e \cdot d}(\mod p);$
$m \perp q; ed = 1(\mod (p-1)(q-1))$
$\rightarrow \exists k \in \mathbb{Z} : ed = 1 + k \cdot (p-1)(q-1)$
modulo $|\mathbb{Z}_q^x| = \phi(q) = q - 1$: $ed = 1 + [k(p-1)] \cdot (q-1)$
$\Rightarrow ed \equiv 1(\mod (q-1))$
$m^{ed} \equiv m^{ed \mod q-1} \equiv m^1(\mod q)$
also: m ist die eindeutige Lösung $\in \mathbb{Z}_n$ von $(*)$.

$\rightarrow$ Entschlüsselung liefert tatsächlich m.

Entschlüsselung ist möglich, wenn $\phi(n)$ bekannt ist. Warum ist $\phi(n)$ schwierig zu bestimmen?
Primfaktor $\overset{\text{leicht}}{\rightarrow} \phi(n)$
Primfaktor $\underset{\text{leicht?}}{\leftarrow} \phi(n)$
$\phi(n) = (p-1)(q-1)$
$\Rightarrow$ betrachte:
$f(x) = x^2 - (n - \phi(n) + 1)x + n = x^2 - (pq - [pq - p - q + 1] + 1)x + n$
$= x^2 - (n - \phi(n) + 1)x + n = x^2 - (p+q)x + pq$
$= (x-p)(x-q)$
f(x) hat genau die Nullstellen p und q, $\phi(n)$ zu berechnen ist also ebenso schwierig wie die PFZ zu bestimmen.

9 Exkurs: Polynome

Polynom: $p(x) := \sum_{i=0}^{n} a_i \cdot x^i$ mit $a_0, ..., a_n \in \mathbb{R}$
Der Grad von p ist n, falls $a_n \neq 0$.
Abkürzung: $n = grad(p)$

Aufwand zur Berechnung von $p(x_0)$:
$p(x_0) = a_n \cdot x_0^n + a_{n-1} \cdot x_0^{n-1} + ... + a_1 \cdot x_0^1 + a_0$
$\Rightarrow$ Aufwand: n Additionen, $2n - 1$ Multiplikationen.
effizienter: Horner-Schema

$$\begin{aligned} p(x_0) &= \underbrace{a_n \cdot x_0^n + a_{n-1} \cdot x_0^{n-1}} + a_{n-2} \cdot x_0^{n-2} + ... + a_0 \\ &= \underbrace{(a_n \cdot x_0 + a_{n-1}) \cdot x_0^{n-1} + a_{n-2} \cdot x_0^{n-2}} + ... + a_0 \\ &= \underbrace{((a_n \cdot x_0 + a_{n-1}) \cdot x_0 + a_{n-2}) x_0^{n-2} + ... + a_0} \\ &= ((...(a_n \cdot x_0 + a_{n-1})x_0 + ...) + a_1)x_0 + a_0 \end{aligned}$$

$\Rightarrow$ Aufwand: n Additionen, n Multiplikationen

Rechnen mit Polynomen:
es seien $a(x) := \sum_{i=0}^{m} a_i \cdot x^i, b(x) = \sum_{i=0}^{n} n_i \cdot x^i$
zwei Polynome, $a_m \neq 0 \neq b_n (m \geq n)$

- Summe: $a(x) + b(x) = \sum_{i=0}^{m}(a_i + b_i)x^i$
  $(b_{n+1}, ...b_m := 0$
- DIfferenz: analog
- Produkt: $a(x) \cdot b(x) = (\sum_{i=0}^{m} a_i \cdot x^i)(\sum_{i=0}^{n} b_i \cdot x^i)$
  $= \sum_{i=0}^{m+n} c_i \cdot x^i$ mit $c_i = \sum_{j=0}^{m} a_j b_i - j$
  $b_i := 0$ für $i < 0$
- Division?
  Satz: Es seien $a(x), b(x)$ Polynome, $b \neq 0$. Dann existieren Polynome $q(x)$ und $r(x)$, so dass gilt:
  $a(x) = q(x) \cdot b(x) + r(x)$
  wobei $r = 0$ oder $grad(r) < grad(b)$.
  Beweis: ohne.

Bsp.: $p(x) := 3x^3 + 4x^2 - 5x + 1$
$\Rightarrow ((3x + 4)x - 5)x + 1$
$p(2) = ((3 \cdot 2 + 4) \cdot 2 - 5) \cdot 2 + 1$
$= (10 \cdot 2 - 5) \cdot 2 + 1 = 15 \cdot 2 + 1 = 31$

$\frac{(3x^3+4x^2-5x+1)}{x^2-x+1} = 3x + 7 (= q(x))$ Rest $-x - 6 (= r(x))$

Häufig interessiert man sich für die Nullstellen eines Polynoms.
Bsp.:

$$p(x) := 2x^2 - 4x + 1 \stackrel{!}{=} 0$$
$$\Leftrightarrow x^2 - 2x + \frac{1}{2} \stackrel{!}{=} 0$$
$$\curvearrowright x_{1/2} = +1 \pm \sqrt{1^2 - \frac{1}{2}}$$
$$= 1 \pm \sqrt{\frac{1}{2}}$$

Wieviele Nullstellen kann ein Polynom $p \neq 0$ vom Grad n besitzen?
Höchstens n Nullstellen!

Beweis: mit vollständiger Induktion nach n
I.A. $n = 0 : p(x) = a_0 \neq 0$
$\curvearrowright$ Keine Nullstellen ✓

I.S. Es sei $grad(p) = n + 1$:

1. Fall: p hat keine Nullstelle $\rightarrow$ ✓

2. Fall: p besitzt eine Nullstelle x_0.
   Es sei $p(x) = q(x)(x - x_0) + r(x)$ mit $r \neq 0 \vee grad(r) < grad(x - x_0) = 0$
   $\curvearrowright grad(r) = 0$
   x_0 ist Nullstelle von $p \rightsquigarrow$
   $p(x_0) = q(x_0) \underbrace{(x_0 - x_0)}_{=0} + r(x_0) \stackrel{!}{=} 0$

$\Rightarrow r(x_0) = 0 \vee grad(r) = 0 \Rightarrow r = a_0 \neq 0$
$\Rightarrow r = 0,$
$p(x) = q(x)(x - x_0)$, wobei $grad(q) = grad(p) - 1 = n$
Alle weiteren Nullstellen von p sind Nullstellen von q; Induktionsvorraussetzung:
q hat höchstens n Nullstellen.
$\Rightarrow p$ hat höchstens $n + 1$ Nullstellen $\square$