Formale Grundlagen und Methoden

Bachelorstudium Lehramt

Elmar Eder

21. Februar 2021

Inhalt I

Abschnitt 1

Logik

Unterabschnitt 1

Informelle Einführung

Logik

- Sprache zum Formulieren logischer Aussagen
- Begriff der Wahrheit
- Logisches Schließen (Beweisen)

Aussagen

Definition

Eine Aussage ist ein deutscher Satz, der entweder wahr oder falsch ist.

Beispiele

- Der Amazonas ist ein Fluss in Südamerika.
  (wahr)
- Die Zahl 5 ist gerade.
  (falsch)
- Jede gerade Zahl, die größer als 2 ist, ist die Summe zweier Primzahlen. (Goldbach'sche Vermutung)
  (nicht bekannt, ob wahr oder falsch)

Wahrheitswerte

Definition

Die Symbole w und f heißen Wahrheitswerte.

w	wahr
f	falsch

Jede Aussage hat entweder den Wahrheitswert w oder den Wahrheitswert f.

Verum und Falsum

Definition

- $\top$ (verum) bezeichnet eine Aussage, die immer wahr ist.
- $\bot$ (falsum) bezeichnet eine Aussage, die immer falsch ist.

Der Wahrheitswert von $\top$ ist w.
Der Wahrheitswert von $\bot$ ist f.

$\bot$ stellt Widerspruch dar.

Verknüpfung von Aussagen

Aus Aussagen lassen sich neue komplexere Aussagen bilden mit aussagenlogischen Verknüpfungen

Verknüpfungen werden mit Symbolen bezeichnet: Junktoren

Verknüpfung	Junktor	
nicht	$\neg$	
und	$\wedge$	
oder	$\vee$	
wenn . . . , dann . . .	$\Rightarrow$	(oder $\rightarrow$)
genau dann, wenn	$\Leftrightarrow$	(oder $\leftrightarrow$)

Verknüpfung von Aussagen

Beispiele

Sei A die Aussage „2 ist ungerade“ und sei B die Aussage „3 ist eine Primzahl“. Dann ist

$\neg A$	die Aussage „2 ist nicht ungerade“,
$A \wedge B$	die Aussage „2 ist ungerade und 3 ist eine Primzahl“,
$A \vee B$	die Aussage „2 ist ungerade oder 3 ist eine Primzahl“,
$A \Rightarrow B$	die Aussage „Wenn 2 ungerade ist, dann ist 3 eine Primzahl“,
$A \Leftrightarrow B$	die Aussage „2 ist genau dann ungerade, wenn 3 eine Primzahl ist“.

Welche dieser Aussagen sind wahr, welche falsch?

Verknüpfungen von Aussagen

Definition

Sind A und B Aussagen, so heißt

$\neg A$	die Negation von A
$A \wedge B$	die Konjunktion von A und B
$A \vee B$	die Disjunktion (oder Adjunktion) von A und B
$A \Rightarrow B$	die Implikation von B aus A
$A \Leftrightarrow B$	die Äquivalenz von A und B.

Auch Konjunktionen und Disjunktionen von mehr als zwei Aussagen sind möglich, z.B. $A \wedge B \wedge C$.

Klammerung

Bei einem Ausdruck wie $A \wedge B \vee C$ ist nicht ersichtlich welche der folgenden beiden Aussagen gemeint ist:

- Die Konjunktion von A und $B \vee C$
- Die Disjunktion von $A \wedge B$ und C.

Um solche Mehrdeutigkeiten zu vermeiden, ist ggf. zu klammern:

Beispiel

- $A \wedge (B \vee C)$
- $(A \wedge B) \vee C$.

Klammerung

Vereinbarung

- $\neg$ bindet stärker als $\wedge$ und $\vee$
- $\wedge$ und $\vee$ binden stärker als $\Rightarrow$ und $\Leftrightarrow$.

Beispiel

$\neg A \wedge B \Rightarrow C \vee D$ bedeutet dasselbe wie $((\neg A) \wedge B) \Rightarrow (C \vee D)$.

Ketten von Implikationen und Äquivalenzen

Bei Ketten von Implikationen und Äquivalenzen ist die Terminologie leider nicht einheitlich.

In der Mathematik

ist $A_1 \Rightarrow A_2 \Rightarrow \ldots \Rightarrow A_n$ eine Abkürzung für
$(A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_3) \wedge (A_3 \Rightarrow A_4) \wedge \cdots \wedge (A_{n-1} \Rightarrow A_n)$.

In der formalen Logik

steht $A_1 \to A_2 \to \ldots \to A_n$ für
$A_1 \to (A_2 \to (A_3 \to (\ldots (A_{n-1} \to A_n) \ldots)))$.

In der Mathematik

ist $A_1 \Leftrightarrow A_2 \Leftrightarrow \ldots \Leftrightarrow A_n$ eine Abkürzung für
$(A_1 \Leftrightarrow A_2) \wedge (A_2 \Leftrightarrow A_3) \wedge (A_3 \Leftrightarrow A_4) \wedge \cdots \wedge (A_{n-1} \Leftrightarrow A_n)$.

Wahrheitswerttafeln

Der Wahrheitswert einer zusammengesetzten Aussage errechnet sich aus den Wahrheitswerten der Teilaussagen aufgrund der folgenden Wahrheitswerttafeln.

A	$\neg A$
w	f
f	w

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	f	w	w	f
f	f	f	f	w	w

Prädikate

Prädikate sind Eigenschaften oder Relationen, die auf jeweils eine feste Anzahl von Gegenständen aus einer gegebenen Menge von Gegenständen (Individuenbereich) bezogen werden können.

Beispiele (für Prädikate, die sich auf natürliche Zahlen beziehen)

- $P(x)$ bedeute „x ist eine Primzahl“. Dann ist P ein einstelliges Prädikat. $P(4)$ bedeutet „4 ist eine Primzahl“ und ist falsch.
- $Q(x, y)$ bedeute „$x < y$“. Dann ist Q ein zweistelliges Prädikat.
- $R(x, y, z)$ bedeute „x hat den Rest y modulo z“.
  Dann ist R ein dreistelliges Prädikat.
  $R(9, 1, 4)$ ist wahr, weil $9 \mod 4 = 1$.

Prädikate

Für ein n-stelliges Prädikat P und Gegenstände $a_1, \ldots, a_n$ muss $P(a_1, \ldots, a_n)$ entweder wahr oder falsch sein.

Notation

Für $P(a_1, \ldots, a_n)$ schreiben wir gelegentlich einfach $Pa_1 \ldots a_n$.

Extensionalität

Definition

Zwei n-stellige Prädikate P und Q heißen einander extensional gleich, wenn für alle Gegenstände $a_1, \ldots, a_n$ gilt

$$P(a_1, \ldots, a_n) \iff Q(a_1, \ldots, a_n) \,.$$

In der Logik werden extensional gleiche Prädikate meist als identisch betrachtet.

Variablen und Aussageformen

Der Satz

x ist der Vater von y.

ist keine Aussage, da die Zeichen x und y keine feste Bedeutung haben und daher an sich nicht feststeht, ob dieser Satz wahr oder falsch ist.

Definition

x und y heißen Variablen.

Definition

Ein Satz, der Variablen enthalten darf und bei Ersetzung der Variablen durch Bezeichnungen von Gegenständen in eine Aussage übergeht, heißt eine Aussageform.

Komprehension

Eine Aussageform F, die höchstens die Variablen $x_1, \ldots, x_n$ enthält, definiert ein n-stelliges Prädikat P durch

$$P(x_1, \ldots, x_n) \iff F \ .$$

Beispiel

Die Aussageform „x ist Vater von y“ definiert das Prädikat P durch

$$P(x, y) \iff x \text{ ist Vater von } y \ .$$

Quantifizierung

Ist F eine Aussageform und ist x eine Variable, so können daraus die folgenden neuen Aussageformen gebildet werden:

$\forall x\, F$ *Dies bedeutet „Für alle x gilt F“.*

$\exists x\, F$ *Dies bedeutet „Es gibt ein x so, dass F gilt“.*

Beispiel

$\forall x\,(x^2 > y)$ ist eine Aussageform über dem Individuenbereich der reellen Zahlen. Sie ist wahr für negative Werte von y und falsch sonst.

Komplexe Aussagenformen

Mit Hilfe der Junktoren und Quantoren können aus einfachen Aussageformen komplexere Aussagenformen aufgebaut werden.

Beispiel

$$\forall x_0 \forall \epsilon(\epsilon > 0 \Rightarrow \exists \delta(\delta > 0 \wedge \forall x(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon)))$$

drückt aus, dass die Funktion f stetig ist.

Eingeschränkte Quantifizierung

In der Mathematik und im täglichen Leben schränkt man Quantifizierungen oft auf einen Teilbereich des Individuenbereichs ein.

Beispiel

1. Für alle ϵ, die größer als 0 sind, gilt $P(\epsilon)$.
2. Es gibt ein δ, das größer als 0 ist, sodass $Q(\delta)$ gilt.

Schreibweise

1. $\forall \epsilon > 0 \colon P(\epsilon)$
2. $\exists \delta > 0 \colon Q(\delta)$

Schreibweise (mit vergrößertem $\wedge$- bzw. $\vee$-Zeichen)

1. $\bigwedge_{\epsilon > 0} P(\epsilon)$
2. $\bigvee_{\delta > 0} Q(\delta)$

Eingeschränkte Quantifizierung

Kein neues sprachliches Ausdrucksmittel, sondern nur Schreibersparnis:

$$\bigwedge_{\epsilon>0} P(\epsilon) \quad \text{ist Abkürzung für} \quad \forall\epsilon(\epsilon > 0 \Rightarrow P(\epsilon))$$

$$\bigvee_{\delta>0} Q(\delta) \quad \text{ist Abkürzung für} \quad \exists\delta(\delta > 0 \wedge Q(\delta))$$

Z.B. ist

$$\bigwedge_{x_0} \bigwedge_{\epsilon>0} \bigvee_{\delta>0} \bigwedge_{x} (|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon)$$

eine Abkürzung für die Stetigkeitsaussage

$$\forall x_0 \forall\epsilon(\epsilon > 0 \Rightarrow \exists\delta(\delta > 0 \wedge \forall x(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon)))$$

Noch kürzer: $$\bigwedge_{x_0} \bigwedge_{\epsilon>0} \bigvee_{\delta>0} \bigwedge_{\substack{x \\ |x-x_0|<\delta}} |f(x) - f(x_0)| < \epsilon$$

Beweise

Um nachzuweisen, dass eine Aussage wahr ist oder dass eine Aussageform gültig, d.h. für alle Werte der Variablen wahr ist, verwendet man

Das Prinzip des logischen Schließens

Axiome sind Aussagen oder Aussageformen, die als wahr oder gültig angenommen werden.

Schlussregeln sind Regeln, mit denen aus bereits als wahr oder gültig nachgewiesenen Aussagen oder Aussageformen neue Aussagen oder Aussageformen als wahr oder gültig nachgewiesen werden.

Beweise

Axiome werden einfach so hingeschrieben.
Schlussregeln werden folgendermaßen geschrieben.

$$\frac{A_1 \quad \ldots \quad A_n}{B}$$

bedeutet: Wenn Aussagen oder Aussagenformen $A_1, \ldots, A_n$ bereits bewiesen sind, dann kann man auf die Gültigkeit von B schließen.
$A_1, \ldots, A_n$ heißen die Prämissen des Schlusses, und B heißt die Konklusion des Schlusses.

Der indirekte Beweis

Um A zu beweisen, nimmt man $\neg A$ an und leitet daraus einen Widerspruch ab.

Beweis mit Fallunterscheidung

Aus $A_1 \vee \cdots \vee A_n$ und $A_1 \Rightarrow B, \ldots, A_n \Rightarrow B$ schließt man auf B.

Gleichheit

In der Logik mit Gleichheit wird ein zweistelliges Prädikat, das Gleichheitsprädikat $=$ gesondert behandelt. Es wird in Infixschreibweise geschrieben und genügt den folgenden Axiomen:

Gleichheitsaxiome

- $x = x$
- $x = y \Rightarrow (Fx \Rightarrow Fy)$

Logik höherer Stufe

In der Logik erster Stufe

- dürfen Prädikate nur auf Objekte angewendet werden.
- darf nur über Objekte quantifiziert werden.

In der Logik zweiter Stufe darf auch über Prädikate quantifiziert werden.

Beispiel (Das Axiom der vollständigen Induktion)

$$\forall P\Big(P(0) \land \forall x\big(P(x) \Rightarrow P(f(x))\big) \Rightarrow \forall x\, P(x)\Big)$$

In Logiken höherer Stufen gibt es auch Prädikatenprädikaten, usw.

Der Beweis durch vollständige Induktion

Satz

Für alle $n \in \mathbb{N}$ gilt $P(n)$.

Beweis durch vollständige Induktion nach n

- Induktionsanfang $P(0)$
  Beweis: ...
- Induktionsvoraussetzung $P(n)$
- Induktionsbehauptung $P(n')$
  Beweis: ... (darf Induktionsvoraussetzung benutzen)

Nach dem Prinzip der vollständigen Induktion gilt daher $P(n)$ für alle $n \in \mathbb{N}$. □

Der Beweis durch vollständige Induktion (Beispiel)

Satz

Für alle $n \in \mathbb{N}$ *gilt* $\sum_{i=0}^{n} 1 = n + 1$.

Beweis durch vollständige Induktion nach n

- Induktionsanfang $\sum_{i=0}^{0} 1 = 0 + 1$
  Beweis: $\sum_{i=0}^{0} 1 = 1$ und $0 + 1 = 1$.
- Induktionsvoraussetzung $\sum_{i=0}^{n} 1 = n + 1$
- Induktionsbehauptung $\sum_{i=0}^{n'} 1 = n' + 1$
  Beweis: $\sum_{i=0}^{n'} 1 = \sum_{i=0}^{n} 1 + 1 \overset{\text{I.V.}}{=} n' + 1$

Nach dem Prinzip der vollständigen Induktion gilt daher $\sum_{i=0}^{n} 1 = n + 1$ für alle $n \in \mathbb{N}$. □

Definition

Einführung eines neuen Zeichens oder einer neuen Notation als Abkürzung für ein Objekt, eine Funktion, ein Prädikat, usw.

Explizite Definition

1. $a := t$
2. $f(x_1, \ldots, x_n) := t$ mit Komprehension
3. $P(x_1, \ldots, x_n) :\Leftrightarrow F$ mit Komprehension

Beispiele

1. $a := \int_{x=0}^{c} f(x)\mathrm{d}x$
2. $f(x, y) := axy + bx + cy + d$
3. $P(x) :\Leftrightarrow x$ ist Primzahl

Definition

Implizite Definition

Definiere X durch eine Aussageform, die für genau ein X erfüllt ist.

Beispiele

- $a \in \mathbb{R}$ sei definiert durch
  $a^2 = 2 \wedge a > 0$.
- $f : \mathbb{R} \to \mathbb{R}$ sei definiert durch
  $f(x)^3 = x$.
- $\arctan : \mathbb{R} \to \mathbb{R}$ sei definiert durch
  $\forall x(\arctan'(x) = \frac{1}{1+x^2}) \wedge \arctan(0) = 0$.
- Das einstellige Prädikat P auf $\mathbb{N}$ sei definiert durch
  $P(0) \wedge \neg P(1) \wedge \forall x(P(x) \Leftrightarrow P(x+2))$.

Definition

Implizite nicht-eindeutige Definition

Definiere X durch eine Aussageform, die für mindestens ein X erfüllt ist.

Beispiele

1. Sei a eine Wurzel von $1 + i$, d.h. $a^2 = 1 + i$.
2. Für jede komplexe Zahl x sei $f(x)$ eine komplexe Zahl mit $f(x)^2 = x$.

Eine Definition wie 2. erfordert im Allgemeinen die Annahme des Auswahlaxioms der Mengenlehre.

Unterabschnitt 2

Aussagenlogik

Grundzeichen

- Aussagensymbole P, Q, R, ...
- Junktoren
  - $\neg$ nicht
  - $\wedge$ und
  - $\vee$ oder
- Runde Klammern (,)

Formeln

Definition

Formeln sind spezielle Zeichenreihen aus Grundzeichen, und zwar

1. Jedes Aussagensymbol ist eine Formel
2. Wenn F eine Formel ist, dann ist auch $\neg F$ eine Formel.
3. Wenn F und G Formeln sind, dann sind auch $(F \wedge G)$ und $(F \vee G)$ Formeln.

Interpretationen

Definition

Die Zeichen w und f heißen Wahrheitswerte. Sie stehen für „wahr“ bzw. „falsch“.

Definition

Eine Interpretation ist eine Abbildung von der Menge der Aussagensymbole in die Menge der Wahrheitswerte.

Der Wahrheitswert einer Formel bei einer Interpretation

Definition

Der Wahrheitswert F^I einer Formel F bei einer Interpretation I ist induktiv definiert durch

1. $P^I := I(P)$ für jedes Aussagensymbol P.
2. $(\neg F)^I := \begin{cases} \text{w}, & \text{wenn } F^I = \text{f} \\ \text{f} & \text{sonst} \end{cases}$
3. $(F \wedge G)^I := \begin{cases} \text{w}, & \text{wenn } F^I = \text{w} \text{ und } G^I = \text{w} \\ \text{f} & \text{sonst} \end{cases}$
4. $(F \vee G)^I := \begin{cases} \text{w}, & \text{wenn } F^I = \text{w} \text{ oder } G^I = \text{w} \\ \text{f} & \text{sonst} \end{cases}$

Einige Begriffe der Semantik

Definition

Ein Modell einer Formel F ist eine Interpretation I so, dass $F^I = \mathrm{w}$ ist.

Definition

- Eine Formel F heißt allgemeingültig, wenn für jede Interpretation I gilt $F^I = \mathrm{w}$.
- Eine Formel F heißt erfüllbar, wenn es eine Interpretation I gibt mit $F^I = \mathrm{w}$.
- Andernfalls heißt sie unerfüllbar.

Einige Begriffe der Semantik

Definition

- G folgt semantisch aus F, in Zeichen $F \models G$, wenn jedes Modell von F auch Modell von G ist.
- F und G heißen semantisch äquivalent, in Zeichen $F \sim G$, wenn $F^I = G^I$ ist für alle Interpretationen I.

$\sim$ ist eine Äquivalenzrelation auf der Menge der Formeln.

Einige Begriffe der Semantik

Definition

Sei S eine Menge von Formeln und G eine Formel.

- I heißt Modell von S, wenn I Modell jeder Formel $F \in S$ ist.
- G folgt semantisch aus S, in Zeichen $S \models G$, wenn jedes Modell von S ein Modell von G ist.
- S heißt erfüllbar, wenn S ein Modell hat.
- Andernfalls heißt S unerfüllbar.

Einige semantische Äquivalenzen

$F \wedge G \sim G \wedge F$	Kommutativität von $\wedge$
$F \vee G \sim G \vee F$	Kommutativität von $\vee$
$\neg\neg F \sim F$	
$(F \wedge G) \wedge H \sim F \wedge (G \wedge H)$	Assoziativität von $\wedge$
$(F \vee G) \vee H \sim F \vee (G \vee H)$	Assoziativität von $\vee$
$F \wedge (G \vee H) \sim (F \wedge G) \vee (F \wedge H)$	Distributivgesetz
$F \vee (G \wedge H) \sim (F \vee G) \wedge (F \vee H)$	Distributivgesetz
$F \wedge F \sim F$	
$F \vee F \sim F$	
$\neg(F \wedge G) \sim \neg F \vee \neg G$	DeMorgan'sche Regel
$\neg(F \vee G) \sim \neg F \wedge \neg G$	DeMorgan'sche Regel

Eigenschaften semantischer Begriffe

Satz

Sei F eine Formel. Dann gilt:

- *F ist allgemeingültig $\iff$ $\neg F$ ist unerfüllbar.*
- *F ist unerfüllbar $\iff$ $\neg F$ ist allgemeingültig.*

Satz

Sei S eine Formelmenge und F eine Formel. Dann gilt:

$$S \models F \iff S \cup \{\neg F\} \text{ ist unerfüllbar.}$$

Unterabschnitt 3

Prädikatenlogik

Sprache der Prädikatenlogik erster Stufe

Grundzeichen

- Variable
- Konstanten
- Funktionszeichen
- Prädikatszeichen
- Junktoren $\neg$, $\wedge$, $\vee$
- Quantoren $\forall$, $\exists$
- Runde Klammern (,) und Komma ,

Sprache der Prädikatenlogik erster Stufe

Terme

- Variable
- Konstanten
- $f(t_1, \ldots, t_n)$

Formeln

- $P(t_1, \ldots, t_n)$
- $\neg F$, $F \wedge G$, $F \vee G$
- $\forall x\, F$, $\exists x\, F$

Semantik der Prädikatenlogik erster Stufe

Interpretation I gegeben durch

- Individuenbereich (engl. domain) D (nichtleere Menge)
- Funktion ordnet jeder/jedem
  - Konstanten a ein $a^I \in D$
  - n-stelligen Funktionszeichen f eine Funktion $f^I : D^n \to D$
  - n-stelligen Prädikatszeichen P eine Relation $P^I \subseteq D^n$

  zu.

Variablenbelegung V ordnet jeder Variablen x ein $x^V \in D$ zu.

Semantik der Prädikatenlogik erster Stufe

Wert t^{IV} eines Terms t bei I und V

- $x^{IV} := x^V$, wenn x Variable
- $a^{IV} := a^I$, wenn a Konstante
- $f(t_1, \ldots, t_n)^{IV} := f^I(t_1^{IV}, \ldots, t_n^{IV})$

$$V_\xi^x(y) := \begin{cases} \xi, & \text{wenn } y \equiv x \\ V(y) & \text{sonst} \end{cases}$$

Semantik der Prädikatenlogik erster Stufe

Wahrheitswert F^{IV} einer Formel F bei I und V

- $P(t_1, \ldots, t_n)^{IV} := \begin{cases} \text{w}, & \text{wenn } (t_1^{IV}, \ldots, t_n^{IV}) \in P^I \\ \text{f} & \text{sonst} \end{cases}$
- $(\neg F)^{IV} := \begin{cases} \text{w}, & \text{wenn } F^{IV} = \text{f} \\ \text{f} & \text{sonst} \end{cases}$
- $(F \wedge G)^{IV} := \begin{cases} \text{w}, & \text{wenn } F^{IV} = \text{w} \text{ und } G^{IV} = \text{w} \\ \text{f} & \text{sonst} \end{cases}$
- $(F \vee G)^{IV} := \begin{cases} \text{w}, & \text{wenn } F^{IV} = \text{w} \text{ oder } G^{IV} = \text{w} \\ \text{f} & \text{sonst} \end{cases}$
- $(\forall x\, F)^{IV} := \begin{cases} \text{w}, & \text{wenn } F^{IV^x_\xi} = \text{w} \text{ für alle } \xi \in D \\ \text{f} & \text{sonst} \end{cases}$
- $(\exists x\, F)^{IV} := \begin{cases} \text{w}, & \text{wenn } F^{IV^x_\xi} = \text{w} \text{ für mindestens ein } \xi \in D \\ \text{f} & \text{sonst} \end{cases}$

Semantik der Prädikatenlogik erster Stufe

Eine Formel heißt geschlossen, wenn

- jede Variable durch einen Quantor gebunden ist.

Dann ist F^{IV} unabhängig von V und wir schreiben einfach F^I.

Eine geschlossene Formel F heißt

- allgemeingültig, wenn $F^I = \mathrm{w}$ für alle I.
- erfüllbar, wenn $F^I = \mathrm{w}$ für mindestens ein I.

Abschnitt 2

Mengenlehre

Der Mengenbegriff

Definition

Eine Menge ist eine Zusammenfassung von wohlunterscheidbaren Dingen.

Definition

Diese Dinge heißen die Elemente der Menge.

Notation

$x \in A$ *Das Ding* x *ist Element der Menge* A.

Das Extensionalitätsprinzip

Extensionalitätsprinzip

Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente haben:

$$A = B \iff \forall x(x \in A \Leftrightarrow x \in B)$$

Folgerung

- *Eine Menge kann ein Element nur einmal enthalten.*
- *Eine Menge gibt keine Reihenfolge der Elemente vor.*

Weitere Notationen

Notationen

$x \notin A$	$\neg\, x \in A$
$\{x_1, \ldots, x_n\}$	die Menge mit den Elementen $x_1, \ldots, x_n$.
$\emptyset$	die leere Menge $\{\}$.
$\{x \mid P(x)\}$	die Menge, deren Elemente diejenigen Dinge x sind, für die $P(x)$ gilt. Komprehension

Es gilt:

$$\{x_1, \ldots, x_n\} = \{x \mid x = x_1 \vee \cdots \vee x = x_n\}$$
$$\emptyset = \{x \mid \bot\}$$

Teilmengen

Definition

Eine Menge A heißt Teilmenge einer Menge B, in Zeichen $A \subseteq B$, wenn gilt

$$\forall x(x \in A \Rightarrow x \in B) \ .$$

Eigenschaften von $\subseteq$

Für alle Mengen A, B, C gilt

- $A \subseteq A$
- Wenn $A \subseteq B$ und $B \subseteq A$, dann $A = B$
- Wenn $A \subseteq B$ und $B \subseteq C$, dann $A \subseteq C$.

Potenzmenge

Definition

Die Menge der Teilmengen einer Menge A heißt Potenzmenge von A. Sie wird mit $\mathcal{P}(A)$ oder 2^A bezeichnet.

Wenn eine Menge genau n Elemente enthält, dann enthält ihre Potenzmenge genau 2^n Elemente.

Operationen auf Mengen

Operationen auf Mengen

$$A \cap B := \{x \mid x \in A \wedge x \in B\} \qquad \text{Durchschnitt}$$
$$A \cup B := \{x \mid x \in A \vee x \in B\} \qquad \text{Vereinigung}$$
$$A \setminus B := \{x \mid x \in A \wedge x \notin B\} \qquad \text{Differenz}$$

Komplement

- Gegeben ein Universum (eine Menge) U.
- Betrachte nur Mengen $A \subseteq U$.
- $\overline{A} := U \setminus A$ Komplement

Mengendiagramme

siehe Tafelfotos vom 8.11.2018

Operationen auf Mengen

Operationen auf Mengen von Mengen

$$\bigcap A := \{x \mid \bigwedge_{X \in A} x \in X\} \qquad \text{Durchschnitt}$$

$$\bigcup A := \{x \mid \bigvee_{X \in A} x \in X\} \qquad \text{Vereinigung}$$

Paare

Definition

- Ein Paar ist eine Zusammenfassung (a, b) von zwei Dingen a und b.
- Diese Dinge heißen Komponenten des Paares.

Gegensatz zu Mengen

- Ein Paar kann ein Ding zweimal enthalten: (a, a)
- Es kommt auf die Reihenfolge an: Im Allgemeinen ist $(a, b) \neq (b, a)$.

Tupel

Definition

Ein n-Tupel ist eine Zusammenfasung $(a_1, \ldots, a_n)$ von n Dingen $a_1, \ldots, a_n$.

Ein Paar ist also ein 2-Tupel.

Definition

Das kartesische Produkt von Mengen $A_1, \ldots, A_n$ ist definiert als

$$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) \mid a_1 \in A_1 \wedge \cdots \wedge a_n \in A_n\}$$

$A^n := A \times \cdots \times A \qquad (n\ A\text{'s}).$

Relationen

Definition

- Eine n-stellige Relation ist eine Teilmenge eines kartesischen Produkts $A_1 \times \cdots \times A_n$.
- Eine n-stellige Relation auf einer Menge A ist eine Teilmenge von A^n.

Definition

- Wenn $(a_1, \ldots, a_n) \in R$, dann sagen wir, $a_1, \ldots, a_n$ stehen in Relation R zueinander.
- Wir schreiben dann auch $R(a_1, \ldots, a_n)$
- Für $n = 2$ auch $a_1 R a_2$ z.B. $a = b$, $a < b$

Prädikate

Definition

In der Logik ist

- ein Individuenbereich eine nichtleere Menge D.
- ein n-stelliges Prädikat auf D eine n-stellige Relation auf D.

Funktionen

Definition

Eine Funktion f ist eine Zuordnung:

- Jedem Element x einer Menge A wird ein und nur ein Element einer Menge B zugeordnet.
- Man schreibt dann $f : A \to B$.
- Das dem x zugeordnete Element der Menge B bezeichnet man mit $f(x)$.

Extensionalitätsprinzip

Seien $f : A \to B$ und $g : A \to B$ zwei Funktionen mit

$$\bigwedge_{x \in A} f(x) = g(x)$$

Dann gilt $f = g$.

Funktionen

Eindeutige Spezifikation einer Funktion

Um eine Funktion $f : A \to B$ mit dem Extensionalitätsprinzip eindeutig zu definieren, braucht man folgende Angaben:

- die Mengen A und B
- das Element $f(x)$ für jedes $x \in A$

Beispiel

1. $f : \mathbb{R} \to \mathbb{R}$
2. $f(x) = x^2$ für alle $x \in \mathbb{R}$

Wenn A und B klar sind, schreiben wir für f auch z.B. $x \mapsto x^2$ oder $\lambda x.x^2$

Funktionen

Definition

Der Graph von $f : A \to B$ ist die Menge $\{(x, f(x)) \mid x \in A\}$.

Funktionen

In der Mengenlehre wird meist eine Funktion mit ihrem Graphen gleichgesetzt. Dann gilt die

Definition

Eine Funktion oder Abbildung ist eine Menge f von Paaren, sodass gilt

$$\forall x \forall y_1 \forall y_2 \left((x, y_1) \in f \wedge (x, y_2) \in f \Rightarrow y_1 = y_2 \right) .$$

Funktionen

Definition

Unter einer *n*-stelligen Funktion auf einer Menge D verstehen wir eine Funktion $f : D^n \to D$.

Definition

- Der Definitionsbereich einer Funktion $f : A \to B$ ist die Menge A, also $\{x \mid \exists y\ (x, y) \in f\}$.
- Der Wertebereich oder Bildbereich von f ist die Menge aller Werte $f(x)$, also $\{y \mid \exists x\ (x, y) \in f\}$

Injektive und surjektive Funktionen

Definition

- Eine Funktion $f : A \to B$ heißt injektiv oder eine Injektion, wenn

$$\bigwedge_{x_1, x_2 \in A} (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

- Eine Funktion $f : A \to B$ heißt surjektiv oder eine Surjektion, wenn

$$\bigwedge_{y \in B} \bigvee_{x \in A} f(x) = y.$$

- Eine Funktion $f : A \to B$ heißt bijektiv oder eine Bijektion, wenn f injektiv und surjektiv ist.

Mächtigkeit von Mengen

Definition

- Eine Menge A heißt höchstens gleichmächtig zu einer Menge B, wenn es eine injektive Abbildung $f : A \to B$ gibt. Wir schreiben dann $|A| \leq |B|$.
- Zwei Mengen A und B heißen gleichmächtig, wenn es eine bijektive Abbildung $f : A \to B$ gibt. Wir schreiben dann $|A| = |B|$.

Satz

- *„höchstens gleichmächtig zu“ ist eine Quasiordnung (reflexive transitive Relation) auf der Klasse der Mengen.*
- *„gleichmächtig“ ist eine Äquivalenzrelation auf der Klasse der Mengen.*

Mächtigkeit von Mengen

Satz (Cantor, Bernstein, Schröder)

Wenn $|A| \leq |B|$ *und* $|B| \leq |A|$, *dann* $|A| = |B|$.

Satz

Eine Menge A *ist genau dann höchstens gleichmächtig wie eine Menge* B, *wenn* $A = \emptyset$ *ist oder es eine surjektive Abbildung* $f : B \to A$ *gibt.*

Definition

Wenn $|A| \leq |B|$, aber nicht $|A| = |B|$ ist, schreibt man $|A| < |B|$ und sagt B ist mächtiger als A.

Endliche Mengen

Definition

Eine Menge heißt endlich, wenn sie gleichmächtig zu einer der Mengen $\{x \in \mathbb{N} \mid x < n\}$ mit $n \in \mathbb{N}$ ist.

Eine Menge ist genau dann endlich, wenn sie nicht gleichmächtig zu einer echten Teilmenge ist. (wenn sie Dedekind-endlich ist)

Eigenschaften von endlichen Mengen

- Die leere Menge ist endlich
- Jede Teilmenge einer endlichen Menge ist endlich
- Die Vereinigung zweier oder endlich vieler endlicher Mengen ist endlich.
- Der Durchschnitt zweier oder endlich vieler, aber mindestens einer, endlicher Mengen ist endlich.
- Die Differenz zweier endlicher Mengen ist endlich.
- Die Potenzmenge einer endlichen Menge ist endlich.
- Das kartesische Produkt zweier oder endlich vieler endlicher Mengen ist endlich.

Abzählbare Mengen

Definition

Eine Menge A heißt abzählbar, wenn A höchstens gleichmächtig zu $\mathbb{N}$ ist.

Beispiel

Jede endliche Menge ist abzählbar.

Satz

Eine Menge A ist genau dann abzählbar,
wenn A leer ist oder eine surjektive Abbildung $\theta\colon \mathbb{N} \to A$ existiert.

Abzählbare Mengen

Beispiel (Die Menge $\mathbb{N}$ der natürlichen Zahlen ist abzählbar)

Surjektive Abzählungsfunktion $\theta\colon \mathbb{N} \to \mathbb{N}$:

$$\theta(n) := n.$$

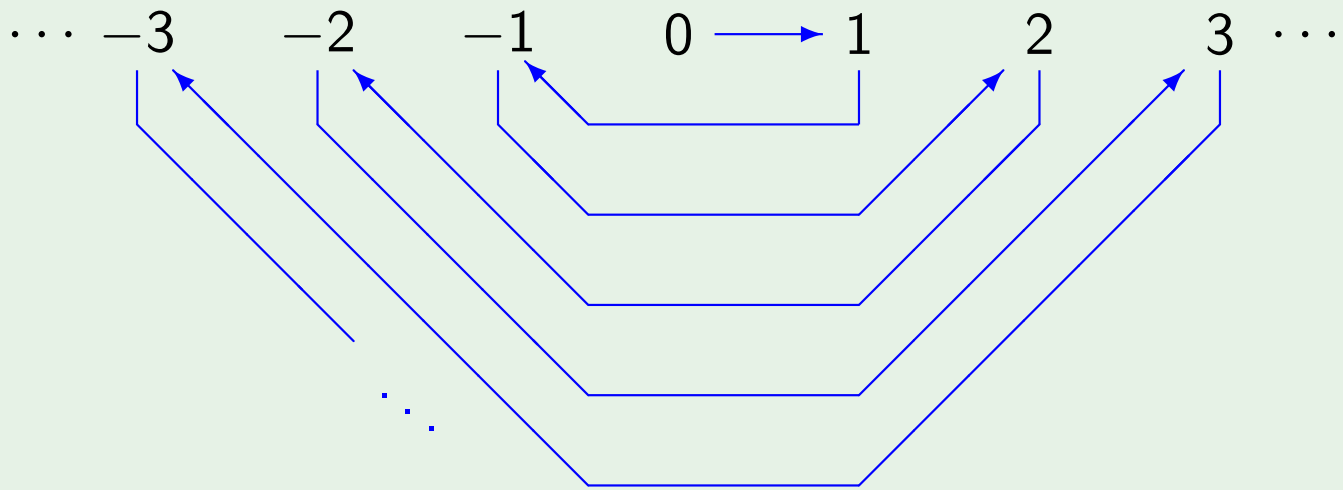
$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow \cdots$$

Abzählbare Mengen

Beispiel (Die Menge $\mathbb{Z}$ der ganzen Zahlen ist abzählbar)

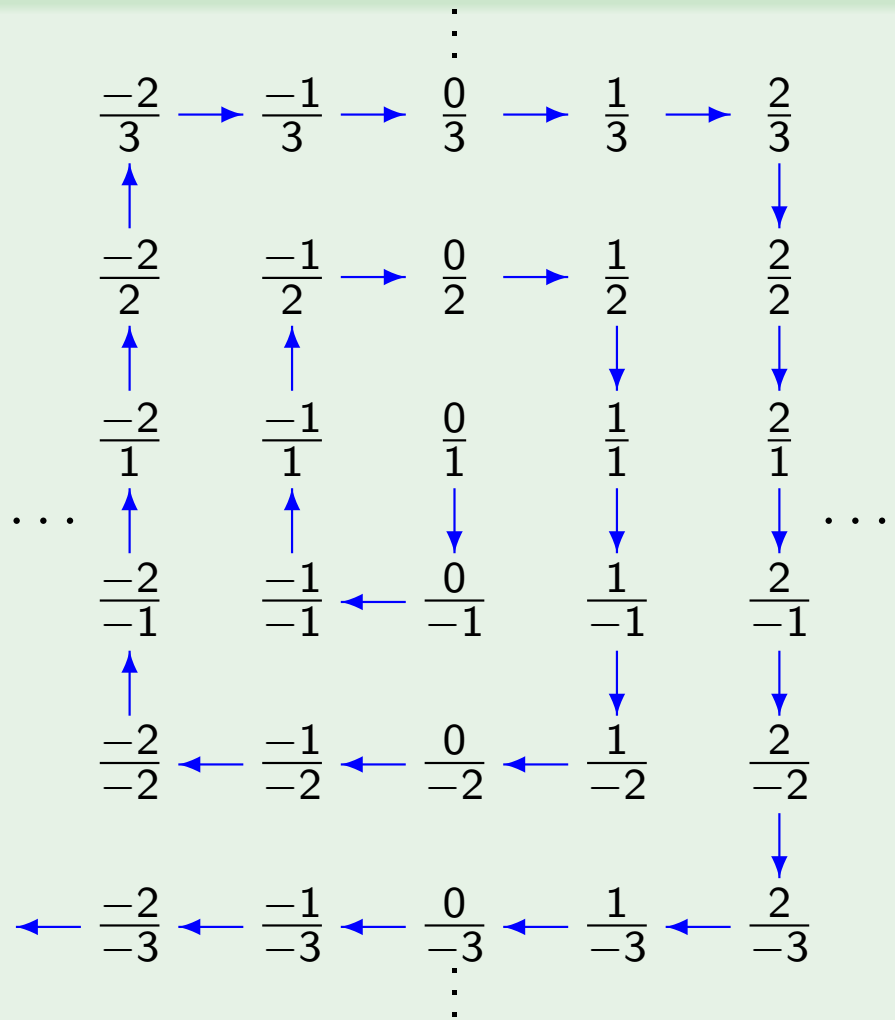
Surjektive Abzählungsfunktion $\theta\colon \mathbb{N} \to \mathbb{Z}$:

$$\theta(2n) := -n$$
$$\theta(2n+1) := n+1.$$



Abzählbare Mengen

Beispiel (Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar)



Abzählbare Mengen

Satz

- *Jede Teilmenge einer abzählbaren Menge ist abzählbar.*
- *Die Vereinigung zweier abzählbaren Mengen ist abzählbar.*
- *Die Vereinigung einer abzählbaren Menge von abzählbaren Mengen ist abzählbar.*
- *Das kartesische Produkt $A_1 \times \cdots \times A_n$ von endlich vielen abzählbaren Mengen $A_1, \ldots, A_n$ ist abzählbar.*

Das Cantor'sche Diagonalverfahren

Satz (Cantor)

Die Menge $\mathbb{R}$ der reellen Zahlen ist nicht abzählbar.

Das Cantor'sche Diagonalverfahren

Beweis mit dem Cantor'schen Diagonalverfahren, indirekt

- Angenommen, $\mathbb{R}$ wäre abzählbar.
- Dann wäre auch die Teilmenge $[0, 1)$ abzählbar.
- Abzählung
$$\begin{aligned} &0, a_{11}\, a_{12}\, a_{13} \ldots \\ &0, a_{21}\, a_{22}\, a_{23} \ldots \\ &0, a_{31}\, a_{32}\, a_{33} \ldots \\ &\quad\vdots \end{aligned}$$
- Diagonale $a_{11}\, a_{22}\, a_{33} \ldots$

  abgeändert zu $0, b_1\, b_2\, b_3 \ldots$ $\qquad b_k := \begin{cases} 3, & \text{falls } a_{kk} = 6 \\ 6 & \text{sonst} \end{cases}$
- Dieser Dezimalbruch kommt in der Abzählung nicht vor.
- Zahl aus $[0, 1)$. Kommt in Abzählung nicht vor. Widerspruch

Das Cantor'sche Diagonalverfahren

Beispiel

- Abzählung

$$
\begin{aligned}
&0,\textcolor{red}{6}589732\ldots\\
&0,1\textcolor{red}{0}92845\ldots\\
&0,32\textcolor{red}{1}1691\ldots\\
&0,244\textcolor{red}{8}123\ldots\\
&0,567\textcolor{red}{7}980\ldots\\
&0,448276\textcolor{red}{1}\ldots\\
&0,500179\textcolor{red}{9}\ldots\\
&\qquad\vdots
\end{aligned}
$$

- Diagonale $\textcolor{red}{6018969\ldots}$
  abgeändert zu $\textcolor{blue}{0,3666636\ldots}$

Das Cantor'sche Diagonalverfahren

Satz

Die Menge $\mathbb{N}^{\mathbb{N}}$ der Funktionen $f : \mathbb{N} \to \mathbb{N}$ ist nicht abzählbar.

Das Cantor'sche Diagonalverfahren

Beweis mit dem Cantor'schen Diagonalverfahren, indirekt

- Angenommen, $\mathbb{N}^{\mathbb{N}}$ wäre abzählbar.
- Dann gäbe es eine Abzählung $f_0, f_1, f_2, \ldots$ von $\mathbb{N}^{\mathbb{N}}$.
-

$$\begin{array}{cccc} f_0(0) & f_0(1) & f_0(2) & \\ f_1(0) & f_1(1) & f_1(2) & \ldots \\ f_2(0) & f_2(1) & f_2(2) & \\ & \vdots & & \ddots \end{array}$$

- Veränderte Diagonale $\qquad f(k) := f_k(k) + 1$

$$f_0(0) + 1 \quad f_1(1) + 1 \quad f_2(2) + 1 \quad \ldots$$

Das Cantor'sche Diagonalverfahren

Beweis (Fortsetzung)

- Die Funktion f ist keine der Funktionen f_n der Abzählung, da sonst
$$f(n) = f_n(n) + 1 = f(n) + 1.$$
- Widerspruch zur Annahme, dass $f_0, f_1, f_2, \ldots$ eine Abzählung von $\mathbb{N}^{\mathbb{N}}$ ist. □

Mengen von Mengen

Mengen dürfen auch selbst Elemente von Mengen sein:

$$\{\emptyset\}$$
$$\{\{\emptyset\}\}$$
$$\{\emptyset, \{\emptyset\}\}$$

sind Mengen.

Mengen von Mengen

In der Mengenlehre kommt man mit dem Mengenbildungsbegriff allein aus um praktisch alle mathematischen Begriffe zu definieren. Z.B. die natürlichen Zahlen:

$$
\begin{aligned}
0 &:= \emptyset \\
1 &:= \{0\} \\
2 &:= \{0, 1\} \\
3 &:= \{0, 1, 2\} \\
&\vdots \\
\omega = \mathbb{N} &= \{0, 1, 2, \dots\}
\end{aligned}
$$

Auch Paare definiert man in der Mengenlehre als Mengen:
$(a, b) := \{\{a\}, \{a, b\}\}$.

Satz von Cantor

Satz (Cantor)

Für jede Menge A gilt $|A| < |\mathcal{P}(A)|$.

Beweis.

indirekt und mit dem Cantor'schen Diagonalverfahren:

- Andernfalls gäbe es eine Surjektion $f : A \to \mathcal{P}(A)$.
- Sei $B := \{x \in A \mid x \notin f(x)\}$. (1)
- Dann ist $B \in \mathcal{P}(A)$.
- Da f surjektiv ist, gäbe es ein $a \in A$ mit $f(a) = B$. (2)
- $a \in B \overset{(1)}{\iff} a \notin f(a) \overset{(2)}{\iff} a \notin B$. Widerspruch

□

Eine Antinomie der Mengenlehre

Sei $A := \{x \mid x \notin x\}$.

$$A \in A \Leftrightarrow A \notin A$$

Widerspruch

Man darf nicht erlauben, dass eine Menge sich selbst enthält.

Ausweg

Unterscheidung zwischen **Klassen** und **Mengen**

- Eine Klasse ist eine Zusammenfassung von Mengen.
- Eine Menge ist eine „kleine“ Klasse.

Nur Mengen sind zugelassen als Elemente von Klassen oder von Mengen.

Die Axiome der Mengenlehre

Extensionalitätsaxiom

$\forall x(x \in A \Leftrightarrow x \in B) \Rightarrow A = B$

Komprehensionsaxiom

$a \in \{x \mid Fx\} \Leftrightarrow Fa \wedge a$ ist Menge

Paarmengenaxiom

Für alle Mengen A und B ist auch $\{A, B\}$ eine Menge.

Die Axiome der Mengenlehre

Vereinigungsmengenaxiom

Für jede Menge A ist auch $\bigcup A$ eine Menge.

Unendlichkeitsaxiom

Es gibt eine Menge N so, dass $\emptyset \in N$ und für jedes $n \in N$ auch $n' \in N$.

Ersetzungsaxiom

Wenn f eine Funktion ist, deren Definitionsbereich eine Menge ist, dann ist auch ihr Bildbereich eine Menge.

Die Axiome der Mengenlehre

Fundierungsaxiom

$\forall x(x \neq \emptyset \Rightarrow \exists y(y \in x \wedge x \cap y = \emptyset))$

Potenzmengenaxiom

Die Potenzmenge einer Menge ist eine Menge.

Auswahlaxiom

Für jede Menge x gibt es eine Menge y, die eine Funktion ist, derart, dass für jede Menge z, die eine nichtleere Teilmenge von x ist, gilt: $y(z) \in z$.

Abschnitt 3

Zahlen

Unterabschnitt 1

Natürliche Zahlen

Die natürlichen Zahlen

- Die Zahlen $0, 1, 2, \ldots$ (in Mengenlehre, Logik und Informatik)
  In der Mathematik oft $1, 2, 3, \ldots$
- Nachfolger einer Zahl n oft mit n' bezeichnet. $n' = n + 1$
- Menge der natürlichen Zahlen $\mathbb{N}$

Peano-Axiome

1. 0 ist eine natürliche Zahl
2. Wenn n eine natürliche Zahl ist, dann ist auch n' eine natürliche Zahl.
3. Für jede natürliche Zahl n ist $n' \neq 0$.
4. Wenn m und n natürliche Zahlen sind und $m' = n'$ ist, dann ist $m = n$.
5. Für jedes einstellige Prädikat P auf der Menge der natürlichen Zahlen gilt:
   Wenn $P(0)$ gilt und für jedes n mit $P(n)$ auch $P(n')$ gilt, dann gilt $P(n)$ für alle natürlichen Zahlen n.

Nachfolgerfunktion

Die Nachfolgerfunktion $n \mapsto n' : \mathbb{N} \to \mathbb{N}$ ist

- nicht surjektiv (wegen Axiom 3)
- aber injektiv (wegen Axiom 4)

Die Nachfolgerfunktion ist eine Bijektion von $\mathbb{N}$ auf eine echte Teilmenge von $\mathbb{N}$, also nicht Dedekind-endlich.

Vollständige Induktion

Beweis von $P(n)$ durch vollständige Induktion nach n

- Beweise $P(0)$
- Beweise $P(n) \Rightarrow P(n')$ für alle $n \in \mathbb{N}$
- Dann gilt $P(n)$ für alle $n \in \mathbb{N}$.

Definiton von $f : \mathbb{N} \to A$ durch vollständige Induktion

- Definiere $f(0)$
- Definiere $f(n')$ unter Bezugnahme auf $f(n)$
- Damit ist $f(n)$ definiert für alle $n \in \mathbb{N}$.

Vollständige Induktion

Beispiel (Fakultätsfunktion)

Die Rekusionsgleichungen:

$$f(0) := 1$$
$$f(n') := f(n) \cdot n'$$

oder mit der Notation $n!$ für n Fakultät:

$$0! := 1$$
$$n'! := n! \cdot n'$$

Vollständige Induktion

Auch Funktionen $f : \mathbb{N}^k \to A$.

Beispiel (Definition von $a + b$ durch vollständige Induktion nach b)

$$a + 0 := a$$
$$a + b' := (a + b)'$$

Beispiel (Definition von $a \cdot b$ durch vollständige Induktion nach b)

$$a \cdot 0 := 0$$
$$a \cdot b' := a \cdot b + a$$

Vollständige Induktion

Beispiel (Definition von a^b durch vollständige Induktion nach b)

$$a^0 := 1$$
$$a^{b'} := a^b \cdot a$$

Wohlordnung der Menge der natürlichen Zahlen

Die Menge der natürlichen Zahlen ist wohlgeordnet, d.h.

Wohlordnung der Menge der natürlichen Zahlen

Jede nichtleere Menge von natürlichen Zahlen hat ein kleinstes Element.

Diese Eigenschaft der Menge der natürlichen Zahlen ist (unter gewissen weiteren Annahmen) äquivalent zum Prinzip der vollständigen Induktion.

Binomialkoeffizienten

Definition

Der Binomialkoeffizient n über k, in Zeichen $\binom{n}{k}$ für zwei natürliche Zahlen n und k mit $k \leq n$ ist definiert durch

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

Das Monoid $(\mathbb{N}, +)$

$+$ ist eine assoziative Verknüpfung auf $\mathbb{N}$:

$$(a + b) + c = a + (b + c)$$

und 0 ist neutrales Element:

$$0 + a = a + 0 = a$$

$(\mathbb{N} \setminus \{0\}, +)$ ist eine Halbgruppe:
Menge $\mathbb{N} \setminus \{0\}$ mit assoziativer Verknüpfung $+$

Unterabschnitt 2

Ganze Zahlen

Die ganzen Zahlen

Die Zahlen $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$

- die negativen ganzen Zahlen $-n$ mit $n \in \mathbb{N} \setminus \{0\}$
- die Null 0
- die positiven ganzen Zahlen $n \in \mathbb{N} \setminus \{0\}$

$\mathbb{Z}$ Menge der ganzen Zahlen
Operationen auf $\mathbb{Z}$: $+$, $-$, $\cdot$

Die Gruppe $(\mathbb{Z}, +)$

Das Paar $(\mathbb{Z}, +)$ ist eine Gruppe:

- $\mathbb{Z}$ ist Menge und $+$ eine innere zweistellige Verknüpfung darauf.
- Assoziativität
$$(a + b) + c = a + (b + c)$$
- Es gibt ein neutrales Element $0 \in \mathbb{Z}$:
$$a + 0 = 0 + a = a$$
- Zu jedem $a \in \mathbb{Z}$ gibt es ein inverses Element $-a$:
$$a + (-a) = (-a) + a = 0$$

$(\mathbb{Z}, +)$ ist eine Abelsche oder kommutative Gruppe: Zusätzlich

- Kommutativgesetz
$$a + b = b + a$$

Verknüpfungen

Definition

Eine innere zweistellige Verknüpfung (oder einfach Verknüpfung) auf einer Menge M ist eine Abbildung $*\colon M \times M \to M$.

Notation

- *Man schreibt $*(a, b)$ überlicherweise in Infixschreibweise: $a * b$.*
- *Wenn die Verknüpfung als $\cdot$ geschrieben wird (zum Beispiel Multiplikation von Zahlen), lässt man sie oft auch ganz weg und schreibt einfach ab.*

Verknüpfungen

Beispiele (für Verknüpfungen)

- Addition $+$ und Multiplikation $\cdot$ auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$.
- Subtraktion $-$ auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$
  (nicht auf $\mathbb{N}$, da z.B. $1 \in \mathbb{N} \wedge 2 \in \mathbb{N} \wedge 1 - 2 \notin \mathbb{N}$).
- Division $/$ auf $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ oder $\mathbb{C} \setminus \{0\}$
  (nicht auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$, da $a/0$ undefiniert ist;
  nicht auf $\mathbb{N} \setminus \{0\}$ oder $\mathbb{Z} \setminus \{0\}$, da z.B. $1/2 \notin \mathbb{N}$ und $1/2 \notin \mathbb{Z}$).
- Konkatenation $\cdot$ von Wörtern auf der Menge Σ^* der Wörter über einem Alphabet Σ.
- Zweistellige aussagenlogische Verknüpfungen $\wedge$, $\vee$, $\Rightarrow$, $\ldots$ auf der Menge $\{w, f\}$ der Wahrheitswerte.
- Zweistellige aussagenlogische Verknüpfungen $\wedge$, $\vee$, $\Rightarrow$, $\ldots$ auf der Menge der Formeln.

Verknüpfungen

Beispiele (für Verknüpfungen)

- Komposition $\circ$ auf der Menge der bijektiven Funktionen $\pi\colon A \to A$ auf einer Menge A, auch Permutationen von A genannt.
  Die Komposition ist definiert durch $(\pi \circ \rho)(x) = \pi(\rho(x))$.
  Die Menge der Permutationen auf $\{1, \ldots, n\}$ wird mit S_n bezeichnet.
  Die Komposition $\circ$ auf S_n ist eine Verknüpfung auf S_n.
  Eine übliche Notation für ein $\pi \in S_n$ ist $\begin{pmatrix} 1 & \ldots & n \\ \pi(1) & \ldots & \pi(n) \end{pmatrix}$. Zum Beispiel $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}(1) = 1$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}(2) = 3$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}(3) = 2$ und $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.
- Multiplikation modulo 6 $\otimes : A \to A$ auf $A = \{0, 1, 2, 3, 4, 5\}$ definiert durch $x \otimes y = xy \bmod 6$.

Verknüpfungstafel

Eine Verknüpfung auf einer endlichen Menge kann durch eine Verknüpfungstafel dargestellt werden.

Beispiele

- Aussagenlogische Verknüpfungen $\wedge$, $\vee$ und $\Rightarrow$ auf der Menge $\{w, f\}$ der Wahrheitswerte:

$\wedge$	w	f
w	w	f
f	f	f

$\vee$	w	f
w	w	w
f	w	f

$\Rightarrow$	w	f
w	w	f
f	w	w

- Multiplikation $\cdot$ auf der Menge $\{-1, 0, 1\}$:

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

Verknüpfungstafel

Beispiel (Komposition $\circ$ auf $S_3 = \{e, p, q, r, s, t\}$, Permutationen)

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $p = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $q = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,
$s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $t = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Allgemein $\pi = \begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix}$.

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	s	t	q	r
q	q	r	e	p	t	s
r	r	q	t	s	e	p
s	s	t	p	e	r	q
t	t	s	r	q	p	e

Verknüpfungstafel

Beispiel (Multiplikation modulo 6)

Sei $A = \{0, 1, 2, 3, 4, 5\}$ die Menge aller Reste modulo 6 und sei $\otimes : A \to A$ auf A definiert durch $x \otimes y = xy \bmod 6$.

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Verknüpfungen

Definition

- $*$ heißt assoziativ, wenn $(a * b) * c = a * (b * c)$ für alle $a, b, c \in M$.
- $*$ heißt kommutativ, wenn $a * b = b * a$ für alle $a, b \in M$.
- Ein Element $e \in M$ heißt neutrales Element bezüglich $*$, wenn $a * e = e * a = a$ für alle $a \in M$.

Eindeutigkeit des neutralen Elements

Eine Verknüpfung hat höchstens 1 neutrales Element.

Beweis.

Wenn e und e' neutrale Elemente sind, dann gilt $e = e * e' = e'$. □

Verknüpfungen

Definition

Sei $*$ eine Verknüpfung mit neutralem Element e.
Ein Element $b \in M$ heißt Inverses eines Elements $a \in M$ bezüglich $*$, wenn $a * b = b * a = e$.

Eindeutigkeit des Inversen bezüglich einer assoziativen Verknüpfung

Bezüglich einer assoziativen Verknüpfung mit neutralem Element hat jedes Element a höchstens 1 Inverses.

Beweis.

Angenommen, b und c seien Inverse von a bezüglich $*$.
Dann gilt $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. □

Verknüpfungen

Beispiele

- Addition $+$, Multiplikation $\cdot$ und Substraktion $-$ ganzer oder reeller Zahlen sind Verknüpfungen auf $\mathbb{Z}$ bzw. auf $\mathbb{R}$.
  Addition und Multiplikation sind assoziativ und kommutativ.
- Division $/$ reeller Zahlen ist keine Verknüpfung auf $\mathbb{R}$, weil z.B. $1/0$ undefiniert ist, aber es ist eine Verknüpfung auf $\mathbb{R} \setminus \{0\}$.
- Konkatenation $\cdot$ von Wörtern über einem Alphabet Σ ist eine assoziative Verknüpfung auf Σ^*. Wenn Σ nur aus einem Zeichen besteht, $\Sigma = \{a\}$, dann ist $\cdot$ auch kommutativ, z.B.
  $aa \cdot aaa = aaaaa = aaa \cdot aa$. Wenn aber Σ mindestens zwei verschiedene Zeichen a und b enthält, dann ist $\cdot$ nicht kommutativ, weil $a \cdot b = ab$ und $b \cdot a = ba$, also $a \cdot b \neq b \cdot a$.

Algebraische Strukturen mit einer Veknüpfung

Definition (Magma)

Ein Magma ist ein Paar $(M, *)$ mit den Eigenschaften

- M ist Menge und $*$ eine innere zweistellige Verknüpfung darauf.

Algebraische Strukturen mit einer Veknüpfung

Definition (Halbgruppe)

Eine Halbgruppe ist ein Paar $(H, *)$ mit den Eigenschaften

- H ist Menge und $*$ eine innere zweistellige Verknüpfung darauf.
- Assoziativität $(a * b) * c = a * (b * c)$

Algebraische Strukturen mit einer Veknüpfung

Definition (Monoid)

Ein Monoid ist ein Paar $(M, *)$ mit den Eigenschaften

- M ist Menge und $*$ eine innere zweistellige Verknüpfung darauf.
- Assoziativität $(a * b) * c = a * (b * c)$
- Es gibt ein neutrales Element $e \in M$:
  $a * e = e * a = a$

Algebraische Strukturen mit einer Veknüpfung

Definition (Gruppe)

Eine Gruppe ist ein Paar $(G, *)$ mit den Eigenschaften

- G ist Menge und $*$ eine innere zweistellige Verknüpfung darauf.
- Assoziativität $(a * b) * c = a * (b * c)$
- Es gibt ein neutrales Element $e \in G$:
  $a * e = e * a = a$
- Zu jedem $a \in G$ ein gibt es ein inverses Element a^{-1}:
  $a * a^{-1} = a^{-1} * a = e$

Algebraische Strukturen mit einer Veknüpfung

Definition (Gruppe)

Eine Gruppe ist ein Paar $(G, *)$ mit den Eigenschaften

- G ist Menge und $*$ eine innere zweistellige Verknüpfung darauf.
- Assoziativität $(a * b) * c = a * (b * c)$
- Es gibt ein neutrales Element $e \in G$:
  $a * e = e * a = a$
- Zu jedem $a \in G$ ein gibt es ein inverses Element a^{-1}:
  $a * a^{-1} = a^{-1} * a = e$

Abelsche oder kommutative Gruppe: Zusätzlich

- Kommutativgesetz $a * b = b * a$

Algebraische Strukturen mit einer Veknüpfung

Beispiele

- $(\mathbb{N}, -)$ ist kein Magma, weil $2 \in \mathbb{N} \wedge 3 \in \mathbb{N} \wedge 2 - 3 \notin \mathbb{N}$, also $-$ keine innere Verknüpfung auf $\mathbb{N}$ ist.
- $(\mathbb{Z}, -)$ ist ein Magma, weil $x \in \mathbb{Z} \wedge y \in \mathbb{Z} \Rightarrow x - y \in \mathbb{Z}$.
  $(\mathbb{Z}, -)$ ist keine Halbgruppe, weil $(2 - 3) - 4 \neq 2 - (3 - 4)$.
- $(\mathbb{N} \setminus \{0\}, +)$ ist eine Halbgruppe, aber kein Monoid.
- $(\mathbb{N}, +)$ ist ein Monoid mit neutralem Element 0, aber keine Gruppe, weil die 1 kein Inverses hat.
- $(\mathbb{N}, \cdot)$ und $(\mathbb{Z}, \cdot)$ sind Monoide mit neutralem Element 1, aber keine Gruppen, weil die 0 und die 2 keine Inverse haben.
- Für ein Alphabet Σ ist $(\Sigma^*, \cdot)$ ein Monoid mit neutralem Element ϵ, aber keine Gruppe, weil für $a \in \Sigma$ das Wort a kein Inverses hat.
  Die Konkatenation $\cdot$ ist kommutativ genau dann, wenn $|\Sigma| = 1$.

Algebraische Strukturen mit einer Veknüpfung

Beispiele

- $(\mathbb{Z}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen mit neutralem Element 0. Das Inverse einer Zahl a ist die Zahl $-a$.
- $(\mathbb{R}, \cdot)$ ist ein Monoid mit neutralem Element 1, aber keine Gruppe, weil die 0 kein Inverses hat.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1. Das Inverse einer Zahl a ist der reziproke Wert (Kehrwert) $1/a$ von a.

Die Einheitengruppe eines Monoids

Definition

Sei $(M, *)$ ein Monoid mit dem Einselement e.

- Eine Einheit von $(M, *)$ ist ein Element $a \in M$, zu dem ein $b \in M$ existiert mit $a * b = b * a = e$.

Einheitengruppe

- Die Menge $M^\times$ der Einheiten von $(M, *)$ bildet mit der Verknüpfung $*$ eine Gruppe $(M^\times, *)$, die Einheitengruppe von $(M, *)$.

$\mathbb{Z}$ mit den Verknüpfungen $+$ und $\cdot$

- $(\mathbb{Z}, +)$ ist eine abelsche Gruppe mit neutralem Element 0 und zu a inversem Element $-a$.
- $(\mathbb{Z}, \cdot)$ ist eine kommutative Halbgruppe mit neutralem Element 1, aber keine Gruppe.

Der Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen

Definition (Ring)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zweistelligen Operationen $+$ und $\cdot$ darauf mit

- $(R, +)$ ist abelsche Gruppe
- $(R, \cdot)$ ist Halbgruppe
- Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

kommutativ, wenn $\cdot$ kommutativ
Einselement: neutrales Element bezüglich $\cdot$

Statt $a \cdot b$ wird oft einfach ab geschrieben.
$(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement 1.

Ideale

Definition (Ideal in einem Ring)

- Ein Ideal in einem Ring $(R, +, \cdot)$ ist eine Teilmenge I von R mit
  - $0 \in I$
  - Wenn $x, y \in I$, dann $x - y \in I$.
  - Wenn $x \in I$ und $r \in R$, dann $rx \in I$ und $xr \in I$.

Für ein Ideal I gilt:
Wenn $x, y \in I$, dann $x + y \in I$.

Ideale

Definition (Das von einer Menge erzeugte Ideal)

- Das von einer Teilmenge A von R erzeugte Ideal (A) oder $\langle A \rangle$ ist das kleinste Ideal I mit $A \subseteq I$.
- Das von $a_1, \ldots, a_n$ erzeugte Ideal ist das von $\{a_1, \ldots, a_n\}$ erzeugte Ideal.
- Ein von nur einem Ringelement erzeugtes Ideal $(a) := (\{a\})$ heißt Hauptideal.

In kommutativen Ringen mit Einselement gilt

$$(A) = \{a_1 r_1 + \cdots + a_n r_n \mid a_1, \ldots a_n \in A,\ r_1, \ldots, r_n \in R\}.$$

Im Ring $(\mathbb{Z}, +, \cdot)$ ist jedes Ideal ein Hauptideal $(a) = a\mathbb{Z} := \{az \mid z \in \mathbb{Z}\}$ mit einer ganzen Zahl a.

[hier ohne Beweis; der setzt ggT und Lemma von Bézout voraus]

Unterabschnitt 3

Weitere Zahlenklassen

Der Körper $(\mathbb{Q}, +, \cdot)$ der rationalen Zahlen

Rationale Zahlen: $\frac{a}{b}$ (auch a/b geschrieben) mit $a, b \in \mathbb{Z}$, $b \neq 0$
$\mathbb{Q}$ Menge der rationalen Zahlen
Operationen auf $\mathbb{Q}$: $+$, $-$, $\cdot$, $/$ (a/b nur für $b \neq 0$)

Definition (Körper)

Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$ mit Einselement mit

- Sei 0 das neutrale Element von $(K, +)$.
- $(K \setminus \{0\}, \cdot)$ ist Gruppe.

$(\mathbb{Q}, +, \cdot)$ ist ein Körper mit Nullelement 0 und Einselement 1.

Der Körper $(\mathbb{R}, +, \cdot)$ der reellen Zahlen

- Alle rationalen Zahlen und alle Zahlen dazwischen
- Es gibt reelle Zahlen, die nicht rational sind, z.B. $\sqrt{2}$, e
- Jede Cauchy-Folge hat einen Limes
- $\mathbb{R}$ Menge der reellen Zahlen

Die Wurzel $\sqrt{a}$ einer reellen Zahl ist eine reelle Zahl, wenn $a > 0$ ist.

Der Körper $(\mathbb{C}, +, \cdot)$ der komplexen Zahlen

- Die imaginäre Einheit $i = \sqrt{-1}$
- Komplexe Zahlen: $a + bi$ mit $a, b \in \mathbb{R}$
- $\mathbb{C}$ Menge der komplexen Zahlen
- Jede komplexe Zahl hat ein oder zwei Quadratwurzeln.
- Jedes Polynom über $\mathbb{C}$ lässt sich in Linearfaktoren zerlegen.
- Jedes nichtkonstante Polynom über $\mathbb{C}$ hat Nullstellen.

Unterabschnitt 4

Teilbarkeit im Ring $(\mathbb{Z}, +, \cdot)$ der ganzen Zahlen

Teiler

Definition

$t \in \mathbb{Z}$ heißt Teiler von $a \in \mathbb{Z}$ (in Zeichen $t|a$), wenn es eine ganze Zahl s gibt mit $a = ts$. Man sagt dann,

- a sei durch t teilbar, oder
- a sei ein Vielfaches von t.

Für ganze Zahlen t, a, b gilt:

- Wenn $t|a$ und $t|b$, dann $t|a + b$ und $t|a - b$.
- Wenn $t|a$, dann $t|ab$.

Die Vielfachen von t bilden also ein Ideal (ein Hauptideal).

Division mit Rest

Satz (Division mit Rest)

Für zwei ganze Zahlen a und $b \neq 0$ gibt es eindeutig bestimmte ganze Zahlen q und r mit $a = b \cdot q + r$ und $0 \leq r < |b|$.

q heißt Ganzzahlquotient
r heißt Rest
bei der Division von a durch b.

Wir schreiben auch $a : b = q$ Rest r.

Wenn $b > 0$, dann $q = a$ div b und $r = a$ mod b.

Division mit Rest

Beispiel

Die Division $100 : 7$ ergibt den Ganzzahlquotient 14 und den Rest 2, weil $100 = 7 \cdot 14 + 2$ und $0 \leq 2 < |7|$.

$100 \operatorname{div} 7 = 14 \quad$ und $\quad 100 \bmod 7 = 2.$

Wir schreiben auch

$$100 : 7 = 14 \text{ Rest } 2$$

Restgleichheit

Definition

a_1 heißt restgleich oder kongruent zu a_2 modulo b,

$$a_1 \equiv a_2 \pmod{b},$$

wenn a_1 und a_2 bei der Division durch b den gleichen Rest haben.
Äquivalent: $a_1 = a_2 + k \cdot b$ mit $k \in \mathbb{Z}$.

Beispiel

$100 \equiv 2 \pmod{7}$, aber auch $100 \equiv 9 \pmod{7}$ (Rest jeweils 2)

Rechnen modulo n

Lemma

Seien a_1, a_2, b_1, b_2 und n ganze Zahlen mit $n > 0$ so, dass

- $a_1 \equiv a_2 \pmod{n}$
- $b_1 \equiv b_2 \pmod{n}$.

Dann gilt

- $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$
- $a_1 - b_1 \equiv a_2 - b_2 \pmod{n}$
- $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$.

Rechnen modulo n

- Es soll der Rest modulo n des Wertes eines mit $+$, $-$ und $\cdot$ aus ganzen Zahlen gebildeten Ausdrucks bestimmt werden.
- Dazu führe alle Operationen modulo n aus und wende das Lemma an!
- Das kann viel Rechenarbeit ersparen, da die Zahlen nicht so groß werden.

Beispiel (Berechne $(9581 \cdot 7963 \cdot 18924 \cdot 7627) \bmod 1000$)

- Ohne Lemma (zeitaufwändige Multiplikationen nötig): $9581 \cdot 7963 \cdot 18924 \cdot 7627 = 76293503 \cdot 18924 \cdot 7627 = 1443778250772 \cdot 7627 = 11011696718638044$. Der Rest modulo 1000 ist 44.
- Mit Lemma (Multiplikationen nur von Zahlen < 1000 nötig): $9581 \cdot 7963 \cdot 18924 \cdot 7627 \equiv 581 \cdot 963 \cdot 924 \cdot 627 = 559503 \cdot 924 \cdot 627 \equiv 503 \cdot 924 \cdot 627 = 464772 \cdot 627 \equiv 772 \cdot 627 = 484044 \equiv 44 \pmod{1000}$.

Rechnen modulo n

Lemma

Seien a, b, n und k ganze Zahlen mit $n > 0$ und $k \geq 0$ so, dass

- $a \equiv b \pmod{n}$.

Dann gilt

- $a^k \equiv b^k \pmod{n}$.

Berechnung von a^k mod n

a^k kann man auch für große k effizient auf Multiplikation zurückführen:

- Quadrieren $a^2 = a \cdot a$ erfordert eine Multiplikation.
- Gerader Exponent: $a^{2k} = (a^k)^2$
- Ungerader Exponent: $a^{2k+1} = a \cdot a^k$.

Zum Berechnen von a^k mod n
bildet man in jedem Schritt den Rest modulo n.

Rechnen modulo n

Beispiele (3^{64} mod 7 ohne/mit Lemma sowie 7^{23} mod 143)

- $3^{64} = (((((3^2)^2)^2)^2)^2)^2 = ((((9^2)^2)^2)^2)^2 = (((81^2)^2)^2)^2 = ((6561^2)^2)^2 = (43046721^2)^2 = 1853020188851841^2 = 3433683820292512484657849089281.$
- $3^{64} = (((((3^2)^2)^2)^2)^2)^2 = ((((9^2)^2)^2)^2)^2 \equiv ((((2^2)^2)^2)^2)^2 = (((4^2)^2)^2)^2 = ((16^2)^2)^2 \equiv ((2^2)^2)^2 = (4^2)^2 = 16^2 \equiv 2^2 = 4 \pmod 7$
- Ähnlich: $7^{23} \equiv 7 \cdot (7 \cdot (7 \cdot (7^2)^2)^2)^2 \equiv 2 \pmod{143}$.

Komplexität der Berechnung von a^k mod n

- Wenn k eine r-stellige Zahl ist, dann braucht man weniger als $8r$ Multiplikationsschritte.
- Das ist mit einem Computer leicht machbar auch für Zahlen n und k mit jeweils mehreren hundert oder tausend Ziffern.

Größter gemeinsamer Teiler

Definition

Ein gemeinsamer Teiler von Zahlen $a_1, \ldots, a_k \in \mathbb{Z}$ ist eine Zahl $t \in \mathbb{Z}$ mit $t|a_1 \wedge \cdots \wedge t|a_k$.

Definition

Der größte gemeinsame Teiler (ggT) zweier ganzer Zahlen a und b ist diejenige ganze Zahl $\mathrm{ggT}(a, b) = t \geq 0$, für die gilt

- t ist gemeinsamer Teiler von a und b.
- Jeder gemeinsame Teiler von a und b ist Teiler von t.

Wenn a und b nicht beide gleich Null sind, ist dies tatsächlich der bezüglich $\leq$ größte gemeinsame Teiler von a und b.

Definition

Zwei ganze Zahlen a und b sind teilerfremd, wenn es keine ganze Zahl x außer 1 und -1 gibt mit $x|a \wedge x|b$.

a und b sind teilerfremd genau dann, wenn $\mathrm{ggT}(a, b) = 1$.

Definition

Ganze Zahlen $a_1, \ldots, a_n$ sind paarweise teilerfremd, wenn für alle $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt: a_i und a_j sind teilerfremd.

Der euklidische Algorithmus: Berechnung von ggT(a, b)

$$\text{ggT}(38, 8) = \text{ggT}(8, 6) = \text{ggT}(6, 2) = \text{ggT}(2, 0) = 2.$$

$$\begin{aligned} 38 : 8 &= 4 \text{ Rest } 6 \\ 8 : 6 &= 1 \text{ Rest } 2 \\ 6 : 2 &= 3 \text{ Rest } 0 \end{aligned}$$

Der euklidische Algorithmus: Berechnung von ggT(a, b)

Bei der Division von c durch d mit Ganzzahlquotient q und Rest r gilt

- $c = d \cdot q + r$ mit $0 \leq r < |d|$
- $\text{ggT}(c, d) = \text{ggT}(d, r)$ mit $r := c \bmod d$, wenn $d > 0$.

Wiederholte Anwendung dieser Gleichung. Z.B.

$$\text{ggT}(38, 8) = \text{ggT}(8, 6) = \text{ggT}(6, 2) = \text{ggT}(2, 0) = 2.$$

$$\begin{array}{r|l} c = & d \cdot q + r \\ \hline 38 = & 8 \cdot 4 + 6 \\ 8 = & 6 \cdot 1 + 2 \\ 6 = & 2 \cdot 3 + 0 \end{array}$$

Effizienz des euklidischen Algorithmus

Rechenzeit des euklidischen Algorithmus zur Berechnung von ggT(a, b) mit dem Computer für zwei Zahlen a und b mit mehreren tausend Stellen:

- Der euklidische Algorithmus ersetzt in jedem Schritt das Zahlenpaar (a, b) durch das Zahlenpaar $(b, a \bmod b)$.
- Für $a \geq b$ gilt $a \bmod b \leq a/2$.
- Daher werden a und b nach 2 Schritten zumindest halbiert.
- Wenn $a < 2^k$ und $b < 2^k$, dann ist also nach höchstens $2k$ Schritten die Zahl 0 erreicht.
- Wenn a und b höchstens n-stellig sind, dann terminiert der Algorithmus also nach höchstens $2k \leq 8n$ (sogar $5n$) Schritten.
- Jeder Schritt erfordert die Berechnung von $a \bmod b$, was mit dem Computer auch für große Zahlen schnell geht.
- Mit dem Computer lässt sich der ggT daher schnell berechnen.

Das Lemma von Bézout

a und b und alle berechneten Reste im euklidischen Algorithmus sind in dem von a und b erzeugten Ideal

$$\{ax + by \mid x, y \in \mathbb{Z}\}.$$

Das gilt auch für den letzten berechneten Rest vor der 0, also für $\mathrm{ggT}(a, b)$.

Satz (Lemma von Bézout)

Zu $a, b \in \mathbb{Z}$ gibt es $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = ax + by$.

Der erweiterte euklidische Algorithmus

Zu $a, b \in \mathbb{N}$ finde $\mathrm{ggT}(a, b)$ und $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = ax + by$.

- $\mathrm{ggT}(c, d) = \mathrm{ggT}(d, r)$ mit $r := c \bmod d$
- $c = au + bv \wedge d = aw + bz \Rightarrow r = a(u - qw) + b(v - qz)$

Wiederholte Anwendung dieser Gleichung bzw. Implikation liefert $\mathrm{ggT}(a, b)$ und die Lösung (x, y) der diophantischen Gleichung $\mathrm{ggT}(a, b) = ax + by$ im Lemma von Bézout.

Beispiel ($\mathrm{ggT}(38, 8)$ und Lösung für $\mathrm{ggT}(38, 8) = 38x + 8y$)

$c = d \cdot q + r,$	$c = a \cdot u + b \cdot v,$	$d = a \cdot w + b \cdot z$
$38 = 8 \cdot 4 + 6,$	$38 = 38 \cdot 1 + 8 \cdot 0,$	$8 = 38 \cdot 0 + 8 \cdot 1$
$8 = 6 \cdot 1 + 2,$	$8 = 38 \cdot 0 + 8 \cdot 1,$	$6 = 38 \cdot 1 + 8 \cdot (-4)$
$6 = 2 \cdot 3 + 0,$	$6 = 38 \cdot 1 + 8 \cdot (-4),$	$2 = 38 \cdot (-1) + 8 \cdot 5$

$\mathrm{ggT}(38, 8) = 2 = 38 \cdot (-1) + 8 \cdot 5$, also $x = -1$ und $y = 5$.

Der erweiterte euklidische Algorithmus

Beispiel (ggT(38, 8) und Lösung für ggT(38, 8) = 38x + 8y)

$$
\begin{aligned}
38 &= 38 \cdot 1 + 8 \cdot 0 \\
8 &= 38 \cdot 0 + 8 \cdot 1 \qquad 38 : 8 = 4 \text{ Rest } 6 \qquad 6 = 38 - 8 \cdot 4 \\
6 &= 38 \cdot 1 + 8 \cdot (-4) \qquad 8 : 6 = 1 \text{ Rest } 2 \qquad 2 = 8 - 6 \cdot 1 \\
2 &= 38 \cdot (-1) + 8 \cdot 5 \qquad 6 : 2 = 3 \text{ Rest } 0
\end{aligned}
$$

$\text{ggT}(38, 8) = 2 = 38 \cdot (-1) + 8 \cdot 5$, also $x = -1$ und $y = 5$.

Multiplikatives Inverses modulo n

Definition

Seien a und n zwei ganze Zahlen mit $n > 0$. Eine ganze Zahl x mit $0 \leq x < n$ heißt multiplikatives Inverses von a modulo n, wenn gilt $a \cdot x \equiv 1 \pmod{n}$.

Beispiele

- Die Zahl 13 ist multiplikatives Inverses von 7 modulo 15, weil $7 \cdot 13 = 91 \equiv 1 \pmod{15}$.
- Es gibt kein multiplikatives Inverses der Zahl 5 modulo 15, weil jedes Vielfache $5 \cdot x$ der 5 den Rest 0, 5 oder 10 modulo 15 hat, also niemals den Rest 1.

Wann hat a ein multiplikatives Inverses modulo n?

Lemma (Existenz und Eindeutigkeit)

Seien a und n teilerfremd. Dann hat a genau 1 multiplikatives Inverses modulo n.

Beweis.

- **Existenz**: Nach dem Lemma von Bézout gibt es x und y mit $a \cdot x + n \cdot y = 1$. Also $a \cdot x \equiv 1 \pmod{n}$. Sei $u := x \bmod n$. Dann ist $a \cdot u \equiv 1 \pmod{n}$. Also ist u multiplikatives Inverses von a modulo n.
- **Eindeutigkeit**: Sei auch $a \cdot v \equiv 1 \pmod{n}$. Dann gilt $u = u \cdot 1 \equiv u \cdot (a \cdot v) = (u \cdot a) \cdot v = (a \cdot u) \cdot v \equiv 1 \cdot v = v \pmod{n}$.

(s. Eindeutigkeit des Inversen bzgl. einer assoziativen Verknüpfung) □

Berechnung des Inversen

- Berechne x und y mit dem erweiterten euklidischen Algorthmus.
- Dann ist das Inverse von a modulo n die Zahl $x \bmod n$.

Wann hat a kein multiplikatives Inverses modulo n?

Lemma (Nichtexistenz)

Seien a und n nicht teilerfremd. Dann hat a kein multiplikatives Inverses modulo n.

Beweis.

- Angenommen, x wäre multiplikatives Inverses von a modulo n.
- Dann $a \cdot x \equiv 1 \pmod{n}$.
- Folglich gibt es eine ganze Zahl y mit $a \cdot x + n \cdot y = 1$.
- $\mathrm{ggT}(a, n)$ ist Teiler von a und von n und daher auch von $a \cdot x + n \cdot y$, also von 1.
- Es folgt $\mathrm{ggT}(a, n) = 1$ im Widerspruch zur Voraussetzung.

Kleinstes gemeinsames Vielfaches

Definition

Das kleinste gemeinsame Vielfache $\mathrm{kgV}(a, b)$ zweier von 0 verschiedener ganzer Zahlen a und b ist die kleinste positive ganze Zahl c, die Vielfaches von a und von b ist.

Satz

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = |a \cdot b|$$

Beispiel

$\mathrm{ggT}(4, 6) = 2, \quad \mathrm{kgV}(4, 6) = 12, \quad 2 \cdot 12 = 4 \cdot 6$
Berechnung des kgV:

$$\mathrm{kgV}(4, 6) = \frac{4 \cdot 6}{\mathrm{ggT}(4, 6)} = \frac{4 \cdot 6}{2} = 12$$

Kleinstes gemeinsames Vielfaches

- Kleinstes gemeinsames Vielfaches von mehreren Zahlen:
  Beispiel: $\text{kgV}(4, 5, 6) = 60$
- Anwendung:
  Berechnung der Summe oder Differenz von Brüchen.
  Berechne kgV der Nenner als neuen gemeinsamen Nenner.
  Bringe Brüche durch Erweitern auf diesen Nenner.
  Beispiel:

$$\frac{3}{4} + \frac{2}{5} - \frac{5}{6} = \frac{45}{60} + \frac{24}{60} - \frac{50}{60} = \frac{45 + 24 - 50}{60} = \frac{19}{60}$$

Simultane Kongruenzen

Zu teilerfremden Zahlen (hier 5 und 7) löse Kongruenzen

Beispiel

$$x \equiv 4 \pmod 5$$
$$x \equiv 6 \pmod 7$$

Lösung

- *Löse* $5u + 7v = 1$ *mit dem erweiterten euklidischen Algorithmus:*
- $u = 3$, $v = -2$. *Es ist* $5u = 15$, $7v = -14$.
- $7v \equiv 1 \pmod 5$, $5u \equiv 0 \pmod 5$
- $7v \equiv 0 \pmod 7$, $5u \equiv 1 \pmod 7$
- *Eine Lösung:* $x = 4 \cdot 7v + 6 \cdot 5u = -56 + 90 = 34$.
- *Alle Lösungen:* $x = 34 + 5 \cdot 7 \cdot z$ *mit* $z \in \mathbb{Z}$. *Also* $x \equiv 34 \pmod{35}$.

Mehrere simultane Kongruenzen

Beispiel

5, 7, 11 sind paarweise teilerfremd. Löse die simultanen Kongruenzen

$$x \equiv 4 \pmod 5$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 9 \pmod{11}$$

Lösung

- *Löse die ersten zwei Kongruenzen:* $x \equiv 34 \pmod{35}$.
- *Löse auf gleiche Weise diese und die restliche Kongruenz*

$$x \equiv 34 \pmod{35}$$
$$x \equiv 9 \pmod{11}$$

Lösungen: $x \equiv 174 \pmod{385}$

Chinesischer Restsatz (simultane Kongruenzen)

Satz

Seien $n_1, \ldots, n_k$ paarweise teilerfremde positive ganze Zahlen und $a_1, \ldots, a_k$ ganze Zahlen. Dann gibt es genau eine ganze Zahl x mit $0 \leq x < n_1 \cdots n_k$ und

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Konstruktion dieser Zahl x:

- Für $k = 2$ finde mit dem erweiterten euklidischen Algorithmus u und v mit $n_1 u + n_2 v = 1$. Dann wähle $x = (a_1 n_2 v + a_2 n_1 u) \bmod (n_1 n_2)$.
- Für $k + 1$ löse die ersten k Kongruenzen. Lösung y. Dann löse $x \equiv y \pmod{n_1 \cdots n_k}$ und $x \equiv a_{k+1} \pmod{n_{k+1}}$.

Simultane Kongruenzen

Seien $n_1, \ldots, n_k$ paarweise teilerfremde positive ganze Zahlen und $a_1, \ldots, a_k$ ganze Zahlen.
Wenn x eine Lösung der simultanen Kongruenzen

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

ist, dann sind alle Lösungen gegeben durch $x + n_1 \cdots n_k \cdot z$ mit $z \in \mathbb{Z}$.

Primzahlen

Definition

Eine natürliche Zahl $n > 1$ heißt Primzahl, wenn sie außer 1 und sich selbst keine Teiler hat.

Das Lemma von Euklid

Lemma (Euklid)

Sei p eine Primzahl und seien a und b ganze Zahlen mit $p|ab$.
Dann gilt $p|a$ oder $p|b$.

Beweis:

Fall 1: p ist Teiler von a. Dann gilt die Behauptung.

Fall 2: p ist nicht Teiler von a. Dann sind p und a teilerfremd. Daher gibt es nach dem Lemma von Bézout ganze Zahlen x und y mit $px + ay = 1$. Also $pxb + aby = b$. Nun gilt:

- $p|pxb$.
- Nach Voraussetzung $p|ab$, also $p|aby$.
- Daher $p|pxb + aby$, also $p|b$.

Primfaktorzerlegung

Satz (Primfaktorzerlegung)

Jede natürliche Zahl > 1 lässt sich eindeutig (bis auf die Reihenfolge der Faktoren) als Produkt von Primzahlen schreiben.

Beweis.

der Existenz indirekt (durch Widerspruch):

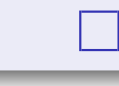
- Annahme, es gäbe eine Zahl > 1 ohne Zerlegung.
- Dann gibt es eine kleinste solche Zahl a.
- Dann ist a keine Primzahl, also zusammengesetzt:
- $a = b \cdot c$ mit $1 < b < a$ und $1 < c < a$.
- Also gibt es Primzahlzerlegungen für b und für c, also auch für a.

Primfaktorzerlegung

Beweis.

der Eindeutigkeit indirekt (durch Widerspruch):

1. Annahme, es gäbe eine Zahl > 1 mit zwei Zerlegungen.
2. Dann gibt es eine kleinste solche Zahl a.
3. Zerlegungen $a = p_1 \cdots p_k$ und $a = q_1 \cdots q_l$.
4. Nach dem Lemma von Euklid ist p_1 Teiler eines der q_i.
5. Da q_i Primzahl ist, ist $p_1 = q_i$.
6. Dann sind $p_2 \cdots p_k$ und $q_1 \cdots q_{i-1} q_{i+1} \cdots q_l$ zwei verschiedene Zerlegungen von a/p_1.
7. a/p_1 wäre also eine Zahl mit zwei Zerlegungen, und $a/p_1 < a$.
8. Widerspruch zu (2).



Komplexität der Primfaktorzerlegung

- Für eine kleine Zahl n ist die Primfaktorzerlegung leicht zu finden: Man sucht eine Primzahl $p \leq \sqrt{n}$, die ein Teiler von n ist und zerlegt n/p weiter, wenn es eine solche Primzahl p gibt. Wenn es aber keine solche Primzahl p gibt, dann ist n selbst eine Primzahl.
- Für große Zahlen n ist $\sqrt{n}$ auch groß (z.B. n 100-stellig und $\sqrt{n}$ 50-stellig) und die Suche nicht praktisch durchführbar (würde mehr Zeit erfordern als das Alter des Weltalls).
- Es ist kein effizienter Algorithmus für die Primfaktorzerlegung einer großen Zahl n bekannt. Auch für Zahlen n, die das Produkt $p \cdot q$ zweier Primzahlen p und q sind, kennt man keinen effizienten Algorithmus zur Berechnung dieser Primzahlen p und q.

Sätze über Primzahlen

Satz (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis.

indirekt:

1. Angenommen es gäbe nur endliche viele Primzahlen.
2. Dann gibt es eine größte Primzahl n.
3. Die Zahl $n! + 1$ ist durch eine Primzahl p teilbar.
4. p ist keine der Zahlen von 1 bis n.
5. Also ist $p > n$.
6. Widerspruch zu (2).

Äquivalenzrelationen

Definition

Eine Äquivalenzrelation auf einer Menge A ist eine zweistellige Relation $\sim$ auf A, sodass für alle $x, y, z \in A$ gilt:

- $x \sim x$ (Reflexivität)
- Wenn $x \sim y$, dann $y \sim x$ (Symmetrie)
- Wenn $x \sim y$ und $y \sim z$, dann $x \sim z$ (Transitivität)

Beispiel (Kongruenz modulo n)

- Seien $a, b, n \in \mathbb{Z}$.
- a und b heißen *kongruent modulo* n wenn $n|(a - b)$.
- Wir schreiben dann $a \equiv b \pmod{n}$ oder $a \equiv_n b$.
- $\equiv_n$ ist eine Äquivalenzrelation auf $\mathbb{Z}$.

Partitionen

Definition

Eine Partition einer Menge M ist eine Menge P von paarweise disjunkten nichtleeren Teilmengen von M, deren Vereinigung die Menge M ist.

Beispiel

$\{\{a, b\}, \{c\}, \{d, e, f\}\}$ ist eine Partition der Menge $\{a, b, c, d, e, f\}$.

Beispiel

- Sei $n \in \mathbb{Z}$.
- Für $a \in \mathbb{Z}$ heißt $\{b \in \mathbb{Z} \mid b \equiv_n a\}$ Restklasse von a modulo n.
- Die Restklassen modulo n bilden eine Partition von $\mathbb{Z}$.
- Wenn $n > 0$, dann gibt es genau n Restklassen modulo n.

Äquivalenzklassen

Definition

Sei $\sim$ eine Äquivalenzrelation auf A.

- Für $x \in A$ heißt $[x]_\sim := \{y \in A \mid y \sim x\}$ die Äquivalenzklasse von x bezüglich $\sim$.

Beispiel

Menge $A = \{a, b, c, d, e, f\}$.

- $\sim$ definiert durch
  $x \sim y \iff x, y \in \{a, b\} \vee x, y \in \{c\} \vee x, y \in \{d, e, f\}$.
- Äquivalenzklassen: $\{a, b\}$, $\{c\}$ und $\{d, e, f\}$.

Beispiel

Die Restklassen modulo n sind die Äquivalenzklassen bezüglich $\equiv_n$.

Äquivalenzklassen

Partition in Äquivalenzklassen

Jede Äquivalenzrelation $\sim$ auf einer Menge A definiert eine Partition P von A und umgekehrt:

- $P :=$ Menge der Äquivalenzklassen bezüglich $\sim$.
- $x \sim y :\iff x$ und y liegen in derselben Menge $B \in P$.

Beispiel

Menge $A = \{a, b, c, d, e, f\}$.

- $\sim$ definiert durch
  $x \sim y \iff x, y \in \{a, b\} \vee x, y \in \{c\} \vee x, y \in \{d, e, f\}$.
- $P := \{\{a, b\}, \{c\}, \{d, e, f\}\}$.

Beispiel

Äquivalenzrelation $\equiv_n$ auf $\mathbb{Z}$ und Partition von $\mathbb{Z}$ in Restklassen modulo n.

Äquivalenzklassen

Definition

Sei $\sim$ eine Äquivalenzrelation auf A.

- Faktor- oder Quotientenmenge von $\sim$ auf A: Menge $A/\sim := \{[x]_\sim \mid x \in A\}$ der Äquivalenzklassen.
- $|A/\sim|$ heißt Index von $\sim$.

Gruppen

Definition

- Sei $(G, *)$ eine Gruppe.
- Sei $U \subseteq G$ so, dass $(U, *)$ selbst eine Gruppe ist.
- Dann heißt $(U, *)$ eine Untergruppe von $(G, *)$.

Oft sagt man einfach: U ist Untergruppe von $(G, *)$.

Definition

- Sei $(G, *)$ eine Gruppe.
- Sei $A \subseteq G$.
- Die von A erzeugte Gruppe ist die kleinste Untergruppe $(U, *)$ von G mit $A \subseteq U$.
- Für $a \in G$ ist die von a erzeugte Gruppe die von $\{a\}$ erzeugte Gruppe.

Die von $a \in G$ erzeugte Gruppe ist $\{a^n \mid n \in \mathbb{Z}\}$.

Gruppen

Definition

- Die Ordnung einer Gruppe $(G, *)$ ist $|G|$.
- Die Ordnung eines Elements $a \in G$ ist die Ordnung der von a erzeugten Untergruppe.

Die Ordnung von a ist die kleinste positive ganze Zahl n mit $a^n = e$ oder unendlich, wenn es kein solches n gibt.

Gruppen

Definition

Sei $(G, *)$ eine Gruppe, $(U, *)$ eine Untergruppe und $a \in G$. Dann heißt

- die Menge $a * U := \{a * x \mid x \in U\}$ eine *Linksnebenklasse* von U.
- die Menge $U * a := \{x * a \mid x \in U\}$ eine *Rechtsnebenklasse* von U.
- Wenn $*$ kommutativ ist, sind beide Begriffe dasselbe und wir sprechen einfach von einer *Nebenklasse*.

- $a \sim_{\text{links}} b \iff a^{-1} * b \in U$ definiert eine Äquivalenzrelation auf G. Äquivalenzklassen sind die Linksnebenklassen: $[a]_{\sim_{\text{links}}} = a * U$.
- $a \sim_{\text{rechts}} b \iff b * a^{-1} \in U$ definiert eine Äquivalenzrelation auf G. Äquivalenzklassen sind die Rechtsnebenklassen: $[a]_{\sim_{\text{rechts}}} = U * a$.

Gruppen

Äquivalenzrelation $a \sim_{\text{links}} b$ genau dann, wenn $a * U = b * U$.
Äquivalenzklassen sind die Linksnebenklassen von U.
Die haben alle die Mächtigkeit $|U|$.

Sei G eine Gruppe und U eine Untergruppe von G.
Dann ist die Anzahl der Linksnebenklassen gleich der Anzahl der Rechtsnebenklassen von U in G.
Sie wird als Index $[G : U]$ von U in G bezeichnet.

Satz von Lagrange: $|G| = [G : U] \cdot |U|$.

Folgerung:
Die Ordnung eines Elements einer Gruppe ist stets ein Teiler der Ordnung der Gruppe.

Einheitengruppe eines Rings mit Einselement

Für einen Ring $(R, +, \cdot)$ mit Einselement definiert man die Begriffe „Einheit“ und „Einheitengruppe“ als die entsprechenden Begriffe für den Modul $(R, \cdot)$:

Definition

Sei $(R, +, \cdot)$ ein Ring mit Einselement e.

- Eine Einheit von $(R, +, \cdot)$ ist ein Element $a \in R$, zu dem ein $b \in R$ existiert mit $a \cdot b = b \cdot a = e$.
- Die Einheitengruppe ist die Menge der Einheiten mit der Multiplikation $\cdot$ des Rings.

Restklassen

Definition

- Eine Restklasse modulo n ist eine Nebenklasse $a + n\mathbb{Z}$ der additiven Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen.
  Wenn n klar ist, schreibt man auch $[a]$ oder $\overline{a}$.
- Menge der Restklassen modulo n ist $\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$.

Die Restklassen modulo n bilden einen Ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

- $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z}$.
- $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := (a \cdot b) + n\mathbb{Z}$.
- Einselement $1 + n\mathbb{Z}$

In Kurzschreibweise:

- $[a] + [b] := [a + b]$
- $[a] \cdot [b] := [a \cdot b]$
- Einselement $[1]$

Die Einheitengruppe des Restklassenrings $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

Satz

Im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ ist $[a]$ genau dann eine Einheit, wenn a und n teilerfremd sind.

Beweis.

- Sei $[a]$ eine Einheit. Dann gibt es ein $x \in \mathbb{Z}$ mit $[a] \cdot [x] = [1]$, also $ax \equiv 1 \pmod{n}$. Also $\mathrm{ggT}(a, n) = 1$.
- Sei $\mathrm{ggT}(a, n) = 1$. Dann gibt es nach dem Lemma von Bézout ganze Zahlen x und y mit $ax + ny = \mathrm{ggT}(a, n) = 1$. Also $ax \equiv 1 \pmod{n}$ und somit $[a] \cdot [x] = [1]$. Also ist $[a]$ eine Einheit. □

Konstruktion des Inversen einer Einheit im Restklassenring

Aus dem Beweis des Satzes ist ersichtlich, wie man das Inverse $[a]^{-1} = [x]$ einer Einheit $[a]$ des Restklassenrings $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ berechnet:

- Mit dem erweiterten euklidischen Algorithmus finde ganze Zahlen x und y mit $ax + ny = \mathrm{ggT}(a, n) = 1$ (Lemma von Bézout).
- Dann ist $[x]$ das gesuchte Inverse $[a]^{-1}$ von $[a]$ in der Einheitengruppe des Restklassenrings $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Man nennt x auch multiplikatives Inverses von a bezüglich des Moduls n.

Da der erweiterte euklidische Algorithmus ebenso wie der einfache euklidische Algorithmus effizient ist, geht diese Berechnung auch für große Zahlen schnell.

Rechnen mit ganzen Zahlen modulo n oder im Restklassenring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$?

- Das kommt im wesentlichen auf das gleiche hinaus.
- Beim Rechnen mit Zahlen modulo n bildet man nach jeder Operation den Rest des Ergebnisses modulo n. Ausnahme: Bei a^k darf man nur von a, nicht aber von k den Rest modulo n bilden.[1] Von Zahlen im Exponenten darf man nicht den Rest modulo n bilden.
- Einige Resultate und auch Notationen aus der Algebra (Ringtheorie und Gruppentheorie) lassen sich im Restklassenring leichter verstehen und unmittelbarer anwenden.

[1] Wenn $\mathrm{ggT}(a, n) = 1$, darf man von k den Rest modulo $\phi(n)$ bilden (nächste Folie).

Eulersche ϕ-Funktion und Satz von Euler-Fermat

Definition

Für eine positive ganze Zahl n ist $\phi(n)$ definiert als die Anzahl der zu n teilerfremden Zahlen von 0 bis $n-1$.

- $\phi(n)$ ist die Anzahl der zu n teilerfremden Reste modulo n.
- Für $n > 1$ ist $\phi(n)$ die Ordnung der Einheitengruppe des Restklassenrings $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Satz (Euler, Fermat)

Für zwei teilerfremde positive ganze Zahlen a und n gilt

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Beweis mit dem Satz von Lagrange in der Einheitengruppe.

Eigenschaften der eulerschen ϕ-Funktion

Satz

Für teilerfremde positive ganze Zahlen m und n ist $\phi(mn) = \phi(m)\phi(n)$.

Beweis.

Nach dem chinesischen Restsatz gibt es
zu jedem der $\phi(m)$ zu m teilerfremden Reste a modulo m und
zu jedem der $\phi(n)$ zu n teilerfremden Reste b modulo n
genau eine ganze Zahl x mit $0 \leq x < mn$ und
$x \equiv a \pmod{m} \wedge x \equiv b \pmod{n}$.
Diese $\phi(m)\phi(n)$ Zahlen x sind genau die $\phi(mn)$ zu mn teilerfremden Reste modulo mn. □

Eigenschaften der eulerschen ϕ-Funktion

- Für jede Primzahl p gilt $\phi(p) = p - 1$.
- Für zwei verschiedene Primzahlen p und q gilt $\phi(pq) = (p - 1)(q - 1)$.

Der kleine fermatsche Satz

Sei $a \in \mathbb{Z}$ und p eine Primzahl. Dann gilt
$a^p \equiv a \pmod{p}$
$a^{p-1} \equiv 1 \pmod{p}$, wenn $p \nmid a$.

Zum Beweis für $p \nmid a$: Restklasse $[a] := a + p\mathbb{Z}$.

- $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Körper mit p Elementen.
- $(\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}, \cdot)$ ist also eine Gruppe der Ordnung $p - 1$.
- Definiere n als die Ordnung der von $[a]$ erzeugte Untergruppe $\{[a]^z \mid z \in \mathbb{Z}\} = \{[a]^0, \ldots, [a]^{n-1}\}$. Dabei ist $[a]^n = [1]$. Nach dem Satz von Lagrange ist n ein Teiler von $p - 1$, also $p - 1 = ns$ mit $s \in \mathbb{Z}$.
- Also $[a]^{p-1} = [a]^{ns} = ([a]^n)^s = [1]^s = [1]$ und damit $a^{p-1} \equiv 1 \pmod{p}$.

Ist aber ein Spezialfall des Satzes von Euler und Fermat.

Abschnitt 4

RSA-Kryptosystem

Asymmetrische kryptographische Verfahren

- zum Verschlüsseln und Signieren von Nachrichten
- Privater Schlüssel (geheim)
- Öffentlicher Schlüssel (für jeden erhältlich)
- Sender und Empfänger haben verschiedene Schlüssel (asymmetrisch).
- Geheimnachricht:
  - Sender verschlüsselt mit öffentlichem Schlüssel des Empfängers.
  - Geheimtext kann nur mit privatem Schlüssel des Empfängers gelesen werden.
- Signierte Nachricht, Authentifikation:
  - Sender verschlüsselt mit eigenem privatem Schlüssel.
  - Nachricht kann von jedermann mit dem öffentlichen Schlüssel des Senders entschlüsselt werden,
  - aber nicht ohne Kenntnis des privaten Schlüssels des Senders gefälscht werden.

Einwegfunktionen

- Einwegfunktion: Funktion $f : A \to B$, die leicht zu berechnen ist, aber deren Umkehrfunktion schwer zu berechnen ist.
- Beispiel: $f(p, q) := p \cdot q$ für Primzahlen p und q ist leicht zu berechnen. Umkehrfunktion: Zerlegung einer Zahl in ein Produkt zweier Primzahlen ist nach heutigem Wissen extrem zeitaufwändig.
- Falltürfunktion: Einwegfunktion, deren Umkehrfunktion
  - mit Zusatzinformation leicht zu berechnen,
  - aber ohne diese Zusatzinformation schwer zu berechnen ist.
- In der Kryptographie:
  - Falltürfunktion
    - mit öffentlichem Schlüssel leicht zu berechnen
  - Umkehrfunktion
    - mit privatem Schlüssel leicht zu berechnen
    - ohne privaten Schlüssel schwer zu berechnen

RSA-Kryptosystem

- asymmetrisches kryptographisches Verfahren
- von Rivest, Shamir, Adleman (MIT)

Erzeugung der Schlüssel

- Wähle zufällig zwei Primzahlen p und q mit $p \neq q$.
- Berechne den RSA-Modul $N = p \cdot q$.
- Berechne $M := \phi(N) = (p-1) \cdot (q-1)$.
- Wähle geeigneten Verschlüsselungsexponent (encryption exponent) e: zu M teilerfremde natürliche Zahl mit $1 < e < M$. $\quad \mathrm{ggT}(e, M) = 1$.
- Berechne das multiplikative Inverse d von e modulo M, d.h. $e \cdot d \equiv 1 \pmod{M}$. Dafür löse die Gleichung $e \cdot d + M \cdot y = 1$ mit dem erweiterten euklidischen Algorithmus.
- d ist der Entschlüsselungsexponent (decryption exponent).
- Öffentlicher Schlüssel (encryption key): Zahlenpaar (e, N).
- Privater Schlüssel (decryption key): Zahlenpaar (d, N).

Falltürfunktion

- Nachricht (message) kodiert als natürliche Zahl $m < N$.
- Mit öffentlichem Schlüssel erzeuge Chiffrat (Geheimtext) $f(m) = c$:

$$c = m^e \bmod N$$

- c ist leicht zu berechnen, da e und N öffentlich sind.
- Umkehrfunktion: $f^{-1}(c) = m$. Berechnung mit privatem Schlüssel:

$$m = c^d \bmod N$$

- m ist schwer zu berechnen, wenn man d nicht kennt.
- m ist leicht zu berechnen, wenn man d kennt.

RSA Beispiel (aus Wikipedia)

- Zufällig gewählte Primzahlen $p = 11$ und $q = 13$.
- Berechne den RSA-Modul $N = 11 \cdot 13 = 143$.
- Berechne $M := \phi(N) = (11 - 1) \cdot (13 - 1) = 120$.
- Wähle einen zu 120 teilerfremden Verschlüsselungsexponent $e = 23$.
- Berechne das multiplikative Inverse d von 23 modulo 120:
  Mit dem erweiterten euklidischen Algorithmus löse die Gleichung $23 \cdot d + 120 \cdot y = 1$. Lösung $d = 47$ und $y = -9$.
- Öffentlicher Schlüssel $(e, N) = (23, 143)$.
- Privater Schlüssel $(d, N) = (47, 143)$.

Verschlüsselung von $m = 7$ zu $c = 2$ und Entschlüsselung von 2 zu 7:

- $7^{23} \equiv 7 \cdot (7 \cdot (7 \cdot (7^2)^2)^2)^2 \equiv 2 \pmod{143}$.
- $2^{47} \equiv 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2^2)^2)^2)^2)^2 \equiv 7 \pmod{143}$.
- Dabei in jedem Schritt Rest modulo 143 bilden, damit die Zahlen nicht zu groß werden!

Rechnung in der Einheitengruppe des Rings $(\mathbb{Z}/N\mathbb{Z}, +, \cdot)$

$N = p \cdot q$. Alle Restklassen sind modulo N.
$G = \{[m] \mid m \text{ teilerfremd zu } N\}$.
Einheitengruppe $(G, \cdot)$ des Restklassenrings $(\mathbb{Z}/N\mathbb{Z}, +, \cdot)$.

- $[m]^{\phi(N)} = [1]$ (Satz von Euler-Fermat).
- Berechne $M = \phi(N) = (p-1) \cdot (q-1)$ aus p und q.
- Wähle eine Zahl e mit $1 < e < M$ und $\mathrm{ggT}(e, M) = 1$.
- Finde d mit $e \cdot d = \phi(N) \cdot k + 1$ für ein $k \in \mathbb{Z}$.
- Verschlüsselung einer Nachricht $[m]$ zu $[c] = [m]^e$.
- Entschlüsselung eines Chiffrats $[c]$ zu $[m] = [c]^d$, weil $([m]^e)^d = [m]^{e \cdot d} = [m]^{\phi(N) \cdot k + 1} = ([m]^{\phi(n)})^k \cdot [m] = [1]^k \cdot [m] = [m]$.

Signieren von Nachrichten

Alle Restklassen sind modulo N:

- Signieren einer Nachricht mit dem eigenen privaten Schlüssel (d, N): $[c] = [m]^d$.
- Prüfen einer signierten Nachricht auf Echtheit mit dem öffentlichen Schlüssel (e, N) des Senders: $[m] = [c]^e$.

Abschnitt 5

Kombinatorik

Permutation

Anordnung von n Objekten in einer Reihenfolge (Vertauschung)

Permutation ohne Wiederholung

- Alle Objekte sind verschieden (voneinander unterscheidbar).
- Es gibt $n!$ Permutationen ohne Wiederholung:
  - n mögliche Objekte für Platz 1
  - $n-1$ mögliche Objekte für Platz 2
  - $n-2$ mögliche Objekte für Platz 3
  - ...
  - 1 mögliches Objekt für Platz n
  - Insgesamt $n \cdot (n-1) \cdot \ldots \cdot 1 = n!$ Möglichkeiten

Permutation mit Wiederholung

Permutation mit Wiederholung

- Es gibt r verschiedene Arten von Objekten. Objekte einer Art sind zueinander identisch (nicht voneinander unterscheidbar).
- Es gibt k_1 Objekte der ersten Art, k_2 Objekte der zweiten Art, u.s.w., wobei $n = k_1 + \cdots + k_r$.
- Es gibt $\binom{n}{k_1,\ldots,k_r}$ Permutationen mit Wiederholung. Multinomialkoeffizient

$$\binom{n}{k_1, \ldots, k_r} := \frac{n!}{k_1! \cdots k_r!}$$

  - Ordne Objekte an: $n!$ mögliche Vertauschungen.
  - Davon liefern jeweils $k_1!k_2! \ldots k_r!$ das gleiche Resultat (unterscheiden sich nur in den Reihenfolgen von Objekten der jeweils gleichen Art).

Variation (geordnete Stichprobe)

k-malige Auswahl jeweils eines Objekts aus einer Menge A von n gegebenen Objekten, wobei die Reihenfolge eine Rolle spielt.
k-Tupel $(x_1, \ldots, x_k) \in A^k$

Variation ohne Wiederholung

- Alle k Objekte der Auswahl müssen verschieden sein.
- $x_i \neq x_j$ für $i \neq j$.
- Es gibt $\binom{n}{k} \cdot k! = \frac{n!}{(n-k)!}$ Variationen ohne Wiederholung:
  - Permutiere alle Objekte aus A. $n!$ mögliche Permutationen
  - Wähle nacheinander die ersten k Objekte aus.
  - Jeweils $(n-k)!$ Permutationen liefern das gleiche Resultat (unterscheiden sich nur in der Reihenfolge der nicht ausgewählten Objekte).
- Im Urnenmodell: Ziehung von Kugeln ohne Zurücklegen

Variation mit Wiederholung

Variation mit Wiederholung

- Objekte können mehrmals gewählt werden.
- Keine weitere Einschränkung für die x_i.
- Es gibt n^k Variationen mit Wiederholung:
  - Für das 1. Objekt n Möglichkeiten
  - Für das 2. Objekt n Möglichkeiten
  - ...
  - Für das k. Objekt n Möglichkeiten
- Im Urnenmodell: Ziehung von Kugeln mit Zurücklegen

Multimengen

- Eine Menge enthält jedes ihrer Elemente nur einmal.
- Eine Multimenge (englisch multiset, bag) darf Elemente mehrfach enthalten. Reihenfolge spielt keine Rolle.
- Notation: $\{x_1, \ldots, x_k\}_b$. Das b (für „bag“) wird oft weggelassen.

Definition (Multimengen)

- Sei A eine Menge.
- Eine Multimenge über A ist eine Abbildung $M\colon A \to \mathbb{N}$.
- Für $x \in A$ gibt $M(x)$ an, wie oft x in M vorkommt.
- M ist k-elementig, wenn $\sum_{x \in A} M(x) = k$ ist.

Beispiel

- Sei $A = \{a, b, c, d, e\}$ und $M = \{a, a, c, c, c, d\}_b$.
- Dann ist $M = \{c, d, a, c, a, c\}_b$ und M ist 6-elementig.
- $M(a) = 2$, $M(b) = 0$, $M(c) = 3$, $M(d) = 1$, $M(e) = 0$.

Kombination (ungeordnete Stichprobe)

k-malige Auswahl jeweils eines Objekts aus einer Menge $A = \{x_1, \ldots, x_n\}$ von n gegebenen Objekten, wobei die Reihenfolge keine Rolle spielt.

Kombination ohne Wiederholung

- Alle k Objekte müssen verschieden sein.
- Auswahl ist k-elementige Teilmenge $\{x_{i_1}, \ldots, x_{i_k}\}$ von A.
- Es gibt $\binom{n}{k}$ Kombinationen ohne Wiederholung:
  - Wähle Variation $(x_{i_1}, \ldots, x_{i_k})$ ohne Wiederholung.
  - Es gibt $\frac{n!}{(n-k)!}$ mögliche Variationen ohne Wiederholung.
  - Jeweils $k!$ Variationen liefern die gleiche Kombination (unterscheiden sich nur durch die Reihenfolge der ausgewählten Objekte).
  - Anzahl der Kombinationen ohne Wiederholung: $\frac{n!}{k!(n-k)!} = \binom{n}{k}$.
- Im Urnenmodell: Ziehung von Kugeln ohne Zurücklegen

Kombination mit Wiederholung

Kombination mit Wiederholung

- Objekte können mehrmals gewählt werden.
- Auswahl ist k-elementige Multimenge $\{x_{i_1}, \ldots, x_{i_k}\}_b$ über A.
- Es gibt $\left(\binom{n}{k}\right) = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}$ Kombinationen mit Wiederholung:
  - Kodiere Multimenge $M = \{x_1, \ldots, x_1, x_2, \ldots, x_2, \ldots, x_n \ldots x_n\}_b$ als Wort $x \ldots x|x \ldots x| \ldots |x \ldots x = x^{M(1)}|x^{M(2)}| \ldots |x^{M(n)}$ über dem Alphabet $\{x, |\}$. Beispiel: $A = \{x_1, \ldots, x_5\}$. Multimenge $\{x_1, x_1, x_3, x_3, x_3, x_4\}_b$ wird kodiert als Wort $xx||xxx|x|$.
  - $n-1$ mal der $|$, k mal das x.
  - Von den $n-1+k$ Positionen im Wort sind k für das x zu wählen.
  - Dafür gibt es $\binom{n-1+k}{k}$ Möglichkeiten.
- Im Urnenmodell: Ziehung von Kugeln mit Zurücklegen

Kombinationen und monoton steigende Zahlenfolgen

Definition

Eine endliche Zahlenfolge $(i_1, \ldots, i_k)$ heißt

- monoton steigend, wenn $i_r \leq i_s$ für $r < s$
- streng monoton steigend, wenn $i_r < i_s$ für $r < s$.

Folgen und Kombinationen

Für eine n-elementige Menge $A = \{x_1, \ldots, x_n\}$ gibt es eine Bijektion

- $(i_1, \ldots, i_k) \mapsto \{x_{i_1}, \ldots, x_{i_k}\}$ von der Menge der streng monoton steigenden Folgen von Zahlen aus $\{1, \ldots, n\}$ in die Menge der Kombinationen ohne Wiederholung
- $(i_1, \ldots, i_k) \mapsto \{x_{i_1}, \ldots, x_{i_k}\}_b$ von der Menge der monoton steigenden Folgen von Zahlen aus $\{1, \ldots, n\}$ in die Menge der Kombinationen mit Wiederholung.

Kombinationen und monoton steigende Zahlenfolgen

Für die k-elementigen Folgen von Zahlen aus $\{1, \ldots, n\}$ gilt:

Folgerung

- *Die Anzahl der streng monoton steigenden Folgen ist gleich der Anzahl $\binom{n}{k}$ der Kombinationen ohne Wiederholung.*
- *Die Anzahl der monoton steigenden Folgen ist gleich der Anzahl der Kombinationen mit Wiederholung.*

Monoton steigende und streng monoton steigende Folgen

- Bijektion $(i_1, \ldots, i_k) \mapsto (i_1, i_2 + 1, i_3 + 2, \ldots, i_k + k - 1)$ von der Menge der monoton steigenden Folgen von Zahlen aus $\{1, \ldots, n\}$ in die Menge der streng monoton steigenden Folgen von Zahlen aus $\{1, \ldots, n + k - 1\}$.
- Daher gibt es genau $\binom{n+k-1}{k}$ monoton steigende Folgen und damit $\binom{n+k-1}{k}$ Kombinationen mit Wiederholung. (alternative Herleitung)

Das Prinzip von Inklusion und Exklusion

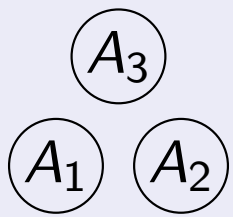
Das Problem

- Gegeben endlich viele endliche Mengen $A_1, \ldots, A_n$.
- Die Mächtigkeiten dieser Mengen und aller ihrer Durchschnitte seien bekannt.
- Berechne die Mächtigkeit $|A_1 \cup \cdots \cup A_n|$.

Lösung, wenn die Mengen disjunkt sind ($A_i \cap A_j = \emptyset$)

Inkludiere die Elemente aller Mengen A_i:

$$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|.$$

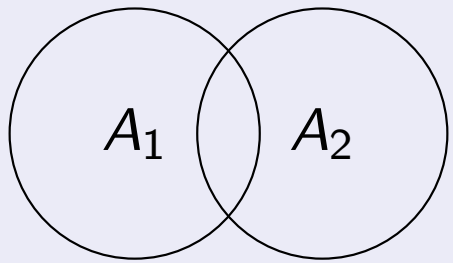


Das Prinzip von Inklusion und Exklusion

Zwei nicht notwendig disjunkte Mengen

Ausdruck für $|A_1 \cup A_2|$:

- Inklusion: $|A_1| + |A_2|$
- zählt die Elemente von $A_1 \cap A_2$ doppelt.
- Muss korrigiert werden (Exklusion): $|A_1| + |A_2| - |A_1 \cap A_2|$.

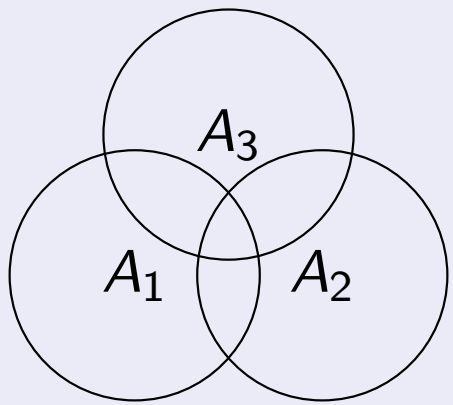


Das Prinzip von Inklusion und Exklusion

Drei Mengen

Ausdruck für $|A_1 \cup A_2 \cup A_3|$:

- Inklusion: $|A_1| + |A_2| + |A_3|$
- zählt die Elemente von $A_i \cap A_j$ doppelt.
- Exklusion: $|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3|$.
- zählt Elemente von $A_1 \cap A_2 \cap A_3$ nur $3 - 3 = 0$ statt 1 mal.
- Inklusion:
  $|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$.



Das Prinzip von Inklusion und Exklusion

$$|A_1 \cup \cdots \cup A_n| = \sum_{\substack{M \subseteq \{A_1,\ldots,A_n\} \\ M \neq \emptyset}} -(-1)^{|M|} \cdot |\bigcap M|.$$

Für $j = |M|$ ist $\bigcap M$ ein Durchschnitt von j A_i's.

Beweisidee:

- Sei S der Summenausdruck auf der rechten Seite.
- Betrachte ein $x \in A_1 \cup \cdots \cup A_n$.
- Sei $M_0 := \{A \mid A \in \{A_1, \ldots, A_n\} \wedge x \in A\}$ und $k := |M_0|$. x ist in k A_i's.
- Für $1 \leq j \leq k$ gibt es $\binom{k}{j}$ Mengen M mit $M \subseteq M_0 \wedge |M| = j$.
  x ist in $\binom{k}{j}$ Durchschnitten von j A_i's.
- $\bigcap M$ inkludiert/exkludiert x in S , wenn j ungerade/gerade.
- Für jedes j wird x genau $\binom{k}{j}$ mal inkludiert/exkludiert.
- x wird insgesamt $-\sum_{j=1}^{k} \binom{k}{j}(-1)^j$ mal, also 1 mal gezählt. Denn
- $-\sum_{j=1}^{k} \binom{k}{j}(-1)^j = 1 - \sum_{j=0}^{k} \binom{k}{j}(-1)^j = 1 - (1-1)^k = 1$ nach dem binomischen Lehrsatz.

Fixpunktfreie Permutationen

Definition

- Ein Fixpunkt einer Permutation ist ein Objekt, das bei ihr seine Position nicht ändert.
- Eine Permutation, die keine Fixpunkte hat, heißt fixpunktfrei.

Beispiel

Die Permutation, die $(1, 2, 3, 4, 5)$ vertauscht zu $(3, 2, 5, 4, 1)$, wird geschrieben als

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}.$$

Sie hat die Fixpunkte 2 und 4, erkennbar daran, dass dort oben und unten die gleiche Zahl steht.

Fixpunktfreie Permutationen

Satz

Für n verschiedene Objekte $x_1, \ldots, x_n$ gibt es genau $n! \cdot \sum_{r=0}^{n} \frac{(-1)^r}{r!}$ fixpunktfreie Permutationen.

Beweis:

- Für $i = 1, \ldots, n$ sei A_i die Menge der Permutationen mit Fixpunkt x_i.
- Für r verschiedene Objekte $x_{i_1}, \ldots, x_{i_r}$ ist $A_{i_1} \cap \cdots \cap A_{i_r}$ die Menge der Permutationen mit Fixpunkten $x_{i_1}, \ldots, x_{i_r}$.
- Also $|A_{i_1} \cap \cdots \cap A_{i_r}| = (n-r)!$.
- Für die Wahl der Menge $\{x_{i_1}, \ldots, x_{i_r}\}$ gibt es $\binom{n}{r}$ Möglichkeiten.
- Nach dem Prinzip von Inklusion und Exklusion ist daher $|A_1 \cup \cdots \cup A_n| = -\sum_{r=1}^{n}(-1)^r \binom{n}{r}(n-r)! = -\sum_{r=1}^{n}(-1)^r \frac{n!}{r!}$.
- Also gibt es $n! - (-\sum_{r=1}^{n}(-1)^r \frac{n!}{r!}) = n! \cdot \sum_{r=0}^{n} \frac{(-1)^r}{r!}$ fixpunktfreie Permutationen. Für große n fast exakt $\frac{n!}{e}$ fixpunktfreie Permutationen.
  Beispiel Wichteln: Wahrscheinlichkeit $\frac{1}{e}$, dass niemand sein eigenes Geschenk erhält.