Logik und Diskrete Strukturen

0. Einführung

Wir werden uns im wesentlichen mit

- Mengen, Relationen und Funktionen
- Logik und
- Beweise

beschäftigen. Dabei interessieren wir uns u.a. für folgende Fragen:

- Was sind Mengen?
- Was kann man mit Mengen machen?
- Wie beschreibt man Mengen?
- Wie entscheidet man, ob ein gegebenes Objekt in einer gegebenen Menge enthalten ist?
- Wie operiert man auf Mengen?
- Was ist ein Beweis?
- Welche allgemeine Beweistechniken sollte man kennen?
- Wie führt man einen Beweis?

Als erstes größere Anwendungsproblem werden wir uns mit der lexikalischen Analyse in einem Compiler beschäftigen. Dabei werden wir ausführlich die Theorie der endlichen Automaten kennenlernen.

Literatur

- Harry R. Lewis, Christos H. Papadimitriou
  Elements of the Theory of Computation,
  Prentice Hall 1981.
- Stasys Jukna, Crashkurs Mathematik für
  Informatiker, Teubner 2008.
- Christos H. Papadimitriou, Computational
  Complexity, Addison-Wesley 1994.
- Jürgen Dassow, Logik für Informatiker,
  Vieweg + Teubner 2005.
- Norbert Blum, Einführung in formale
  Sprachen, Berechenbarkeit, Informations-
  und Lerntheorie, Oldenbourg 2007.

Inhalt

1. Mengen, Relationen und Funktionen
   - 1.1 "Wenn ... dann ..." und verwandtes
   - 1.2 Mengen
   - 1.3 Relationen und Funktionen
   - 1.4 Spezielle Typen von binären Relationen
   - 1.5 Abschlusseigenschaften
   - 1.6 Endliche und unendliche Mengen
   - 1.7 Drei grundlegende Beweistechniken
     - 1.7.1 Die vollständige Induktion
     - 1.7.2 Das Schubfachprinzip
     - 1.7.3 Die Diagonalisierung
2. Modulare Arithmetik
   - 2.1 Teilbarkeit und Division mit Rest
   - 2.2 Teilerfremde Zahlen
   - 2.3 Rechnen modulo n
   - 2.4 Der Euklid'sche Algorithmus
   - 2.5 Primzahlen
   - 2.6 Der chinesische Restsatz
3. Algebraische Strukturen
   - 3.1 Gruppen
   - 3.2 Homomorphe Abbildungen
   - 3.3 Ringe und Körper
4. Einführung in die Logik
   - 4.1 Die Aussagenlogik

4.1.1 Aussagenlogische Ausdrücke
4.1.2 Erfüllbarkeit und Gültigkeit
4.2 Die Prädikatenlogik
4.2.1 Die Syntax der Prädikatenlogik
4.2.2 Strukturen und Modelle
4.2.3 Gültige Ausdrücke
4.2.4 Axiome und Beweise

5. Automatentheorie und formale Sprachen
5.1 Die lexikalische Analyse
5.1.1 Reguläre Mengen, reguläre Ausdrücke und endliche Automaten
5.1.2 Minimierung endlicher Automaten

1. Mengen, Relationen und Funktionen

1.1 "Wenn ... dann ..." und verwandtes

In der Mathematik beschäftigt man sich u.a. mit wahren und falschen Aussagen und mit den Beziehungen zwischen Aussagen. Hierbei verwendet man häufig die deutsche Sprache, jedoch auf eine präzisere Art und Weise als im Alltag.

Beispiel 1.1

"Das Wort "Kaffeetasse" enthält mehr "e" als "s"."

oder

"Das Wort "Kaffeetasse" enthält mindestens soviele "e" wie "s"."

oder

"Das Wort "Kaffeetasse" enthält mindestens soviele "x" wie "y"."

◆

Alle drei Aussagen sind offensichtlich wahr. Dabei beschreibt die erste Aussage die Situation präziser als die zweite, was allerdings keinen Einfluss auf den Wahrheitswert der zweiten Aussage hat. Da das Wort "Kaffeetasse" weder ein "x" noch ein "y" enthält, ist auch die

dritte Aussage wahr, auch wenn diese nicht sinnvoll zu sein scheint.

Mittels Bindewörter können zwei Aussagen zu einer einzigen Aussage kombiniert werden. Dabei ergibt sich der Wahrheitswert der kombinierten Aussage aus den Wahrheitswerten der einzelnen Aussagen. Wir werden nun einige häufig verwendeten Kombinationen diskutieren. Seien hierbei p und q zwei Aussagen.

a) p und q bzw. p oder q

p und q ist { wahr falls p wahr und q wahr
falsch sonst

p oder q ist { wahr falls mindestens eine der Aussagen p und q wahr
falsch sonst

b) wenn p dann q

wenn p dann q ist { wahr falls p falsch oder q wahr ist.
falsch sonst

D.h., wenn wir Fallunterscheidung bzgl. dem Wahrheitswert von p machen, dann ergibt sich:

1. Fall p wahr

Damit "wenn p dann q" wahr ist, muss auch die Aussage q wahr sein.

2. Fall p falsch

Dann ist "wenn p dann q", unabhängig vom Wahrheitswert von q, wahr.

Bemerkung:
Der Wahrheitswert von "wenn p dann q" hängt nur von den Wahrheitswerten von p bzw. q ab. Es besteht keine Notwendigkeit zu überprüfen, ob die Verknüpfung von p mit q "sinnvoll" ist oder nicht.

Häufig werden Aussagen über Klassen von Objekten gemacht. Hierzu verwendet man Symbole, die für ein beliebiges Objekt der betrachteten Klasse stehen. Bezeichne z.B. x ein beliebiges Wort der deutschen Sprache

Beispiel 1.2

"Wenn x mehr "e" als "s" hat, dann enthält x mindestens ein "e"."

Beh.: Die Aussage des Beispiels 1.2 ist wahr.

Bew.:

Wir unterscheiden zwei Fälle:

1) x enthält nicht mehr "e" als "s".

Dann impliziert obiger 2. Fall, dass die Aussage wahr ist.

2) x enthält mehr "e" als "s".

x kann nicht weniger als null s enthalten. Also muss x mindestens nächste Zahl größer als null viele e enthalten. Also enthält x mindestens ein e. D.h., die Aussage ist wahr.

■

Falls der wenn-Teil einer "wenn... dann..."-Aussage unter keinem Umstand wahr sein kann, dann ist die "wenn... dann..." - Aussage nichtssagend wahr.

Beispiel 1.3

Seien a_1 und a_2 zwei Buchstaben und $n(a_1)$ und $n(a_2)$ zwei Zahlen.

"Wenn x $n(a_1)$ Buchstaben a_1, $n(a_2)$ Buchstaben a_2 enthält und $n(a_1) < n(a_2)$ dann ent-

hält x mindestens $n(a_1) + n(a_2)$ Buchstaben."

Beh.: Die Aussage des Beispiels 1.3 ist wahr.

Bew.:

Wir müssen nur den Fall, dass die wenn-Aussage wahr ist, näher untersuchen.

Falls a_1 und a_2 derselbe Buchstabe sind, dann gilt $n(a_1) = n(a_2)$ und die wenn-Aussage ist falsch.

Falls a_1 und a_2 verschiedene Buchstaben sind, dann enthält x $n(a_1)$ Buchstaben a_1 und $n(a_2)$ Buchstaben a_2, insgesamt also mindestens $n(a_1) + n(a_2)$ Buchstaben. ∎

Wir können "wenn p dann q" auch folgendermaßen interpretieren:

Falls diese Aussage wahr ist, dann ist es unmöglich, dass gleichzeitig p wahr und q falsch sind.

D.h., um zu beweisen, dass "wenn p dann q" wahr ist, können wir annehmen, dass q falsch und p wahr sind und dies zu einem Widerspruch führen.

Beispiel 1.4

"Wenn $x^2 = 0$ dann $x = 0$."

Beh.: Die Aussage des Beispiels 1.4 ist wahr.

Bew.:

Annahme: $x^2 = 0$ aber $x \neq 0$

Dann gilt entweder $x > 0$ oder $x < 0$. Aber

wenn $x > 0$ dann $x^2 > 0$ und

wenn $x < 0$ dann $x^2 > 0$.

In beiden Fällen gilt $x^2 > 0$. Dies ist ein Widerspruch zur Annahme, dass $x^2 = 0$.

Die Aussage

"p allein wenn q"

meint dasselbe wie

"wenn p dann q."

Beispiel 1.5

Seien x und y ganze Zahlen. Dann meint

"x + y ist ungerade allein wenn eine der Zahlen x und y ungerade sind"

dasselbe wie

" wenn $x+y$ ungerade ist, dann ist eine der Zahlen x und y ungerade",

was eine wahre Aussage ist.

◊

Auch

" q wenn p "

meint dasselbe wie

" wenn p dann q".

Beispiel 1.5 (Fortführung)

Obige Aussage kann auch folgendermaßen geschrieben werden:

"x oder y ist ungerade wenn $x+y$ ungerade".

◊

Häufig kombiniert man die Aussagen

" p allein wenn q" (d.h. "wenn p dann q")

und

" p wenn q" (d.h. "wenn q dann p")

zu folgender Aussage

" p genau dann wenn q"

Damit diese Aussage wahr ist müssen entweder p und q wahr oder p und q falsch sein.

D.h., p und q sind in exakt denselben Situationen wahr.

Zum Beweis, dass eine "p genau dann wenn q"-Aussage wahr ist, teilt man diese auf und beweist beide Teile seperat.

Beispiel 1.5 (Fortführung)

"x+y ist ungerade genau dann wenn exakt eine der Zahlen x und y ungerade ist."

Beh.: Die letzte Aussage des Beispiels 1.5 ist wahr.

Bew.:

Wir zerlegen obige Behauptung wie folgt:

a) Wenn exakt eine der Zahlen x und y ungerade ist, dann ist x+y ungerade.

b) Wenn x+y ungerade ist, dann ist exakt eine der Zahlen x und y ungerade.

Bew. von a):

Exakt eine der Zahlen ist ungerade impliziert, dass wir beide Zahlen wie folgt schreiben können: $2n$ und $2n+1$.

Es gilt $2m + 2n + 1 = 2(m+n) + 1$ ist ungerade.

Bew. von b):

Annahme: $x + y$ ist ungerade aber entweder beide oder keine der Zahlen ist ungerade.

Beide Fälle in der Annahme können wir direkt zum Widerspruch führen. ∎

1.2 Mengen

Eine Menge ist eine Zusammenfassung von Objekten. Zum Beispiel ist die Zusammenfassung der vier Buchstaben a, b, c und d einer Menge, die wir L nennen können. Wir schreiben dann

$$L := \{a, b, c, d\}$$

(Mengenklammer; Aufzählung aller Objekte in L)

Lies: "L wird definiert als"

Die Objekte in L heißen Elemente der Menge L.

Zum Beispiel ist b ein Element der Menge L (in Symbolen: $b \in L$). Manchmal sagen wir hierfür b ist in L oder auch L enthält b. Andererseits ist z kein Element der Menge L (in Symbolen: $z \notin L$)

Die Elemente einer Menge müssen nicht mein-ander in irgendeine Beziehung stehen. So ist zum Beispiel

$$\{5, \text{Apfel}, \text{rot}, \{\text{blau}, 3\}\}$$

eine Menge mit vier Elementen, wovon ein Element selbst eine Menge ist.

In Mengen unterscheiden wir nicht Wiederholungen von Elementen. D.h., die Mengen $\{3,7,5,3\}$ und $\{3,7,5\}$ sind identisch. Auch ist die Reihenfolge der Elemente in Mengen unwesentlich. So bezeichnen $\{3,7,5\}$, $\{5,3,7\}$ und $\{7,5,3\}$ dieselbe Menge. Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente enthalten.

Es gibt eine Menge, die keine Elemente enthält, die sogenannte <u>leere Menge</u> (in Symbolen $\emptyset$). Jede andere Menge ist <u>nichtleer</u>.

Bisher haben wir eine Menge durch die Aufzählung ihre Elemente spezifiziert. Dies ist bei Mengen, die unendlich viele Elemente enthalten, nicht möglich. Derartige Menge heißen <u>unendlich</u>. Zum Beispiel ist $\mathbb{N}$, die Menge der natürlichen Zahlen, unendlich. Zwar können wir $\mathbb{N}$ durch

$$\mathbb{N} := \{1, 2, 3, \ldots\}$$

unter Verwendung von drei Punkten und unserer Intuition, wie die Aufzählung fortzusetzen ist, spezifizieren, jedoch gibt es viele unendliche Mengen, wo dies nicht möglich ist. (Hierzu später mehr). Eine Menge, die nicht unendlich ist, ist endlich.

Eine weitere Möglichkeit für die Spezifikation einer Menge ist die Bezugnahme auf andere Mengen und auf Eigenschaften, die die Elemente der Menge haben oder nicht haben.

Beispiel 1.6:

Seien $I := \{1, 3, 9\}$ und $G := \{3, 9\}$. Dann kann G als die Menge derjenigen Elemente der Menge I, die größer als 2 sind, beschrieben werden. Wir schreiben dann

$$G := \{x \mid x \in I \text{ und } x \text{ größer als } 2\}.$$

Im allgemeinen können wir, falls eine Menge A definiert ist und P eine Eigenschaft ist, die Elemente von A haben oder nicht haben, eine neue Menge B definieren durch

$$B := \{x \mid x \in A \text{ und } x \text{ hat Eigenschaft } P\}.$$

So kann z.B. die Menge der ungeraden natürlichen Zahlen spezifiziert werden durch

$$U := \{x \mid x \in \mathbb{N} \text{ und } x \text{ ist nicht teilbar durch } 2\}.$$

Eine Menge A ist eine Teilmenge einer Menge B, falls jedes Element von A auch ein Element von B ist. Wir schreiben dann

$$A \subseteq B.$$

Wir sagen dann auch, dass A in B enthalten ist.

Beispiel 1.6 (Fortführung)

Es gilt

$$G \subseteq \mathbb{I} \quad \text{und auch} \quad \mathbb{U} \subseteq \mathbb{N}.$$

◇

Bemerkung:
Gemäß unserer Definition ist jede Menge Teilmenge von sich selbst.

Falls A Teilmenge von B und $A \neq B$, dann sagen wir, dass A eine echte Teilmenge von B ist. Wir schreiben dann

$$A \subsetneq B.$$

Bemerkung:

Die leere Menge $\emptyset$ ist eine Teilmenge von jeder Menge.

Um zu beweisen, dass zwei Mengen A und B gleich sind, genügt es $A \subseteq B$ und $B \subseteq A$ zu be-

weisen. Jedes Element von A ist dann auch ein Element von B und umgekehrt. D.h., A und B haben dieselben Elemente und somit gilt gemäß Definition

$$A = B.$$

Mittels verschiedenen Mengenoperationen können wir zwei Mengen zur Bildung einer dritten Menge kombinieren:

Die Vereinigung zweier Mengen A und B ist diejenige Menge, deren Elemente in mindestens einer der Mengen A und B enthalten sind. Wir verwenden das Symbol $\cup$ um die Vereinigung zu bezeichnen. Wir erhalten somit

$$A \cup B := \{x \mid x \in A \text{ oder } x \in B\}.$$

Beispiel 1.6 (Fortführung):

$$\{1,3,9\} \cup \{3,5,7\} = \{1,3,9,5,7\}$$

◇

Der Durchschnitt zweier Mengen A und B ist diejenige Menge, deren Elemente in beiden Mengen A und B enthalten sind. Das Symbol $\cap$ bezeichnet den Durchschnitt. Somit erhalten wir

$$A \cap B := \{x \mid x \in A \text{ und } x \in B\}.$$

Beispiel 1.6 (Fortführung)

$$\{1,3,9\} \cap \{3,5,7\} = \{3\}$$

$$\mathbb{U} \cap \mathbb{N} = \mathbb{U}$$

◊

Die **Differenz** zweier Mengen A und B (in Zeichen $A \setminus B$) ist die Menge derjenigen Elemente von A, die nicht Elemente von B sind. D.h.,

$$A \setminus B := \{x \mid x \in A \text{ und } x \notin B\}.$$

Beispiel 1.6 (Fortführung)

$$\{1,3,9\} \setminus \{3,5,7\} = \{1,9\}$$

◊

Die **symmetrische Differenz** $A \oplus B$ zweier Mengen A und B ist definiert durch

$$A \oplus B := A \setminus B \cup B \setminus A.$$

Beispiel 1.6 (Fortführung)

$$\{1,3,9\} \oplus \{3,5,7\} = \{1,9,5,7\}$$

◆

Einige Eigenschaften der Mengenoperationen können leicht aus deren Definitionen gefolgert werden. Seien A, B und C Mengen. Dann gelten folgende Regeln:

Idempotenz: $A \cup A = A$
$A \cap A = A$

Kommutativität: $A \cup B = B \cup A$
$A \cap B = B \cap A$

Assoziativität: $(A \cup B) \cup C = A \cup (B \cup C)$
$(A \cap B) \cap C = A \cap (B \cap C)$

Distributivität: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Absorbtion: $A \cap (A \cup B) = A$
$A \cup (A \cap B) = A$

De Morgan'sche Regeln: $A \setminus (B \cup C) = A \setminus B \cap A \setminus C$
$A \setminus (B \cap C) = A \setminus B \cup A \setminus C$

Wir beweisen die erste der De Morgan'schen Regeln.
Seien

$$L := A \setminus (B \cup C) \text{ und } R := A \setminus B \cap A \setminus C.$$

Zu zeigen ist $L = R$. Hierzu beweisen wir zunächst $L \subseteq R$ und dann $R \subseteq L$.

$L \subseteq R$:

Betrachte $x \in L$ beliebig. Dann gilt

$$x \in A \text{ aber } x \notin B \text{ und } x \notin C.$$

Also gilt $x \in A \setminus B$ und auch $x \in A \setminus C$.

Also ist x auch ein Element von R. Da x ein beliebiges Element von L ist, folgt somit $L \subseteq R$.

$R \subseteq L$:

Betrachte $x \in R$ beliebig. Dann gilt

$$x \in A \setminus B \quad \text{und} \quad x \in A \setminus C.$$

Somit gilt

$$x \in A \quad \text{aber} \quad x \notin B \cup C.$$

Demnach folgt $x \in L$. Da x ein beliebiges Element von R ist, folgt somit $R \subseteq L$. ∎

Übung:

Beweisen Sie eines der beiden Distributivitätsgesetze.

Zwei Mengen A und B heißen disjunkt, wenn sie kein gemeinsames Element besitzen. D.h., $A \cap B = \emptyset$.

Man kann auch den Durchschnitt oder die Vereinigung von mehr als zwei Mengen bilden. Sei S eine Kollektion von Mengen. Dann schreiben wir

$$\bigcup S := \{ x \mid x \in P \text{ für eine Menge } P \in S \}$$

und

$$\bigcap S := \{ x \mid x \in P \text{ für alle Mengen } P \in S \}.$$

Zum Beispiel gilt für

$$S = \{ \{a,b\}, \{b,c\}, \{b,d\} \}$$

$$\bigcup S = \{a,b,c,d\} \text{ und } \bigcap S = \{b\}.$$

Die Kollektion aller Teilmengen einer Menge A ist selbst eine Menge. Wir nennen diese Menge Potenzmenge von A und bezeichnen diese mit 2^A.

Beispiel 1.7

Sei $A = \{a,b,c\}$. Dann gilt

$$2^A := \{ \emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\} \}.$$

◊

Eine Partition Π einer nichtleeren Menge A ist eine Teilmenge von 2^A, so dass

i) $\emptyset \notin \Pi$

ii) Für jedes $x \in A$ existiert genau eine Menge $B \in \Pi$ mit $x \in B$.

Dies bedeutet insbesondere, dass die Elemente

von Π paarweise disjunkt sind und dass $\bigcup \Pi = A$.

1.3 Relationen und Funktionen

In der Mathematik interessiert man sich nicht nur für Aussagen über Objekte sondern auch für Beziehungen zwischen Objekten. Wir nennen solche Beziehung auch Relation.

Beispiel 1.8

a) "kleiner als" ist eine Relation zwischen Zahlen. Diese gilt zwischen 3 und 8; nicht jedoch zwischen 8 und 3 oder zwischen 3 und 3.

b) "verheiratet" ist eine Relation zwischen Menschen. ◊

Obige Beschreibung der Relationen "kleiner als" und "verheiratet" ist noch informell. ⇝

Frage:
Wie definieren wir formal eine Relation?

Man könnte zwei Objekte, die zueinander in Relation stehen, zu einem Paar gruppieren. Da z.B. 3 kleiner ist als 8 aber 8 nicht kleiner ist als 3, müssen wir zwischen den beiden Teilen eines Paares unterscheiden können. Dies führt zur Definition von so genannten geordneten Paaren.

(a,b) bezeichnet das geordnete Paar der Objekte a und b. Dabei heißen a und b Komponenten des geordneten Paares (a,b).

Beachte

Das geordnete Paar (a,b) ist aufgrund seiner Ordnung verschieden zur Menge $\{a,b\}$.
Es gilt

$$(a,b) \neq (b,a) \text{ aber } \{a,b\} = \{b,a\}.$$

Des weiteren fordern wir nicht, dass die beiden Komponenten eines geordneten Paares verschieden sein müssen. So ist z.B. $(3,3)$ ein gültiges geordnetes Paar. Zwei geordnete Paare (a,b) und (c,d) sind nur dann gleich wenn $a=c$ und $b=d$.

Das kartesische Produkt $A \times B$ zweier Mengen A und B ist die Menge aller geordneten Paare (a,b) mit $a \in A$ und $b \in B$. D.h.,

$$A \times B := \{(a,b) \mid a \in A \text{ und } b \in B\}.$$

Eine binäre Relation (oder auch zweistellige Relation) auf zwei Mengen A und B ist eine Teilmenge von $A \times B$.

Beispiel 1.8 (Fortführung)

a) Die Teilmenge

$$\{(i,j) \mid i,j \in \mathbb{N} \text{ und } i < j\}$$

von $\mathbb{N} \times \mathbb{N}$ definiert die "kleiner als" Relation auf $\mathbb{N}$ und $\mathbb{N}$.

b) Wenn Jutta mit Peter und Gabi mit Klaus und sonst keine der Frauen aus

$$M_1 := \{\text{Ulrike, Jutta, Petra, Gabi}\}$$

mit einem der Männer aus

$$M_2 := \{\text{Peter, Klaus, Wolfgang}\}$$

verheiratet ist, dann definiert

$$\{(\text{Gabi, Klaus}), (\text{Jutta, Peter})\}$$

die Relation "verheiratet" auf M_1 und M_2.

■

Man kann auch mehr als zwei Objekte zueinander in Beziehung setzen. Z.B. könnte man aus einer Menge von Arbeitern Teams der Größe fünf bilden.

↝

Sei $n \in \mathbb{N}$. Seien $a_1, a_2, \dots, a_n$ n Objekte, die nicht notwendigerweise verschieden sein müssen. Dann ist $(a_1, a_2, \dots, a_n)$ ein <u>geordnetes n-Tupel</u>.

a_i, $1 \leq i \leq n$ ist die <u>i-te Komponente</u> von $(a_1, a_2, \dots, a_n)$. Sei $(b_1, b_2, \dots, b_m)$, $m \in \mathbb{N}$ ein geordneter m-Tupel. Dann gilt

$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_m)$ genau dann, wenn $n = n$ und $a_i = b_i$ für $1 \leq i \leq n$.

Seien $A_1, A_2, \dots, A_n$ beliebige nichtleere Mengen. Dann ist das n-fache kartesische Produkt $A_1 \times A_2 \times \dots \times A_n$ die Menge aller geordneten n-Tupel $(a_1, a_2, \dots, a_n)$ mit $a_i \in A_i$ für $1 \leq i \leq n$. D.h.,

$$A_1 \times A_2 \times \dots \times A_n := \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ für } 1 \leq i \leq n\}.$$

Falls $A_1 = A_2 = \dots = A_n = A$, dann schreiben wir für $A \times A \times \dots \times A$ auch kürzer A^n.

Eine n-stellige Relation auf den Mengen $A_1, A_2, \dots, A_n$ ist eine Teilmenge von $A_1 \times A_2 \times \dots \times A_n$.

Eine binäre Relation $f \subseteq A \times B$ mit

für jedes $a \in A$ existiert genau ein $b \in B$, so dass $(a, b) \in f$

heißt Funktion oder Abbildung von A nach B. A ist der Definitionsbereich und B der Bild- oder Wertebereich der Funktion f. Eine Funktion ordnet somit jedem Element a des Definitionsbereiches auf eindeutiger Weise ein Element $f(a)$ des Bildbereiches zu. Wir schreiben

$$f: A \to B$$

um eine Funktion f von A nach B zu bezeichnen.

Für $A' \subseteq A$ heißt

$$f(A') := \{ f(a) \mid a \in A' \}$$

das Bild von A' unter f. Für $B' \subseteq B$ heißt

$$f^{-1}(B') := \{ a \in A \mid f(a) \in B' \}$$

das Urbild von B' unter f. Für $b \in B$ schreibt man $f^{-1}(b)$ anstatt $f^{-1}(\{b\})$. D.h.,

$$f^{-1}(b) := \{ a \in A \mid f(a) = b \}.$$

Eine Funktion $f: A \to B$ heißt

- injektiv, falls für $a, a' \in A$ mit $a \neq a'$ stets $f(a) \neq f(a')$,
- surjektiv, falls für jedes $b \in B$ ein $a \in A$ mit $f(a) = b$ existiert und
- bijektiv, falls f injektiv und surjektiv ist.

Eine Abbildung $f: A \to B$ heißt Bijektion zwischen A und B, falls f bijektiv ist.

Beispiel 1.9

Die Funktion $f: \mathbb{N} \to \mathbb{N}$ mit $f(x) = x^2$ ist injektiv. Wegen $-1 \neq 1$ aber $(-1)^2 = 1^2$ ist die Funktion $g: \mathbb{Z} \to \mathbb{Z}$ mit $g(x) = x^2$ nicht injektiv. Beide Funktionen sind nicht surjektiv, da $\sqrt{2}$ kein Element von $\mathbb{Z}$ ist.

Für jede binäre Relation $R \subseteq A \times B$ ist die inverse Relation $R^{-1} \subseteq B \times A$ definiert durch

$(b,a) \in R^{-1}$ genau dann, wenn $(a,b) \in R$.

Zur Definition einer inversen Funktion (oder auch Umkehrfunktion) einer Funktion $f: A \to B$ benötigen wir, dass f injektiv ist, da ansonsten die inverse Relation f^{-1} keine Funktion mehr ist.

Die Hintereinanderausführung (oder auch Komposition) $R \circ Q$ zweier binären Relationen Q und R ist definiert durch

$$R \circ Q := \{ (a,b) \mid \text{es existiert ein } c \text{ mit } (a,c) \in Q \text{ und } (c,b) \in R \}.$$

Die Hintereinanderausführung ($g \circ f$) zweier Funktionen $f: A \to B$ und $g: B' \to C$, $B' \subseteq B$ ist eine Funktion $h: A \to C$, wobei

$$h(a) = g(f(a)) \text{ für alle } a \in A.$$

1.4 Spezielle Typen von binären Relationen

Ziel:

Beschreibung von Eigenschaften "gut strukturierter" binären Relationen.

Wir betrachten nur binäre Relationen auf eine Menge und dieselbe Menge. D.h., eine Relation $R \subseteq A \times A$ für eine Menge A.

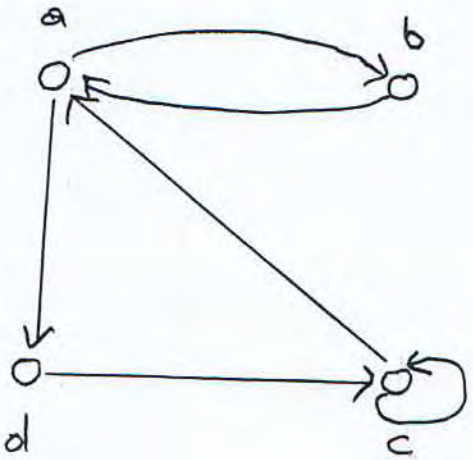
Falls A endlich ist, dann kann R auf folgende Art und Weise durch einen gerichteten Graphen repräsentiert werden. Jedes Element von A wird durch einen kleinen Kreis, einen sogenannten Knoten, repräsentiert. Wir zeichnen genau dann einen Pfeil, eine sogenannte gerichtete Kante von a nach b, wenn $(a,b) \in R$.

Beispiel 1.10

Betrachte

$$R = \{(a,b), (b,a), (a,d), (d,c), (c,c), (c,a)\}.$$

Folgender gerichtete Graph repräsentiert R:



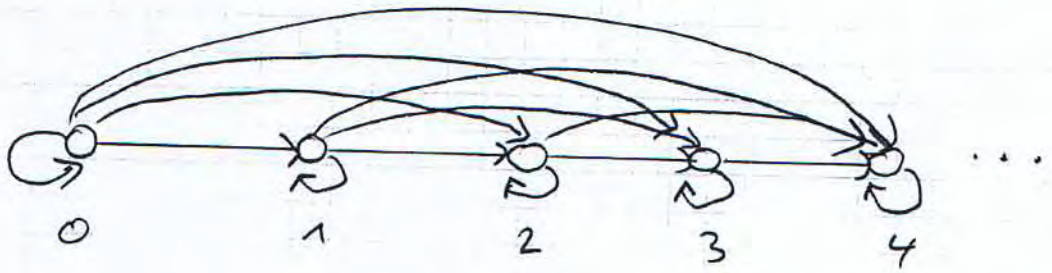
◊

Eine Relation $R \subseteq A \times A$ heißt reflexiv, falls $(a,a) \in R$ für alle $a \in A$.

Bemerkung:
Der gerichtete Graph, der eine reflexive Relation repräsentiert besitzt für jeden Knoten eine Selbstschleife.

Beispiel 1.11

Betrachte die "kleiner gleich"-Relation $\{(i,j) \mid i,j \in \mathbb{N}_0, i \leq j\}$. Wir erhalten folgenden Graphen



Eine Relation $R \subseteq A \times A$ heißt Symmetrisch, falls $(b,a) \in R$ wenn $(a,b) \in R$.

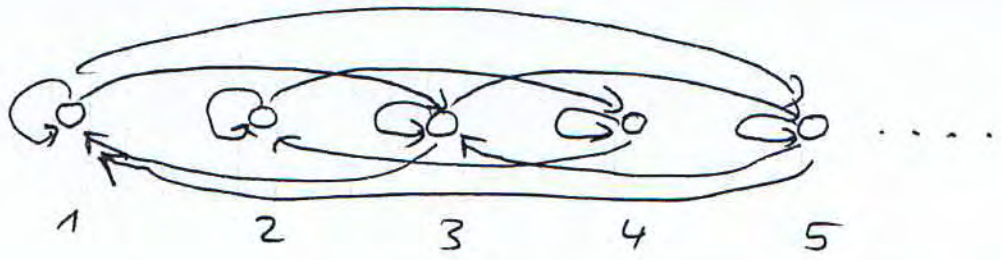
Bemerkung:
Der gerichtete Graph, der eine symmetrische Relation repräsentiert enthält zwischen zwei Knoten Pfeile in beide Richtungen oder keinen Pfeil.

Beispiel 1.12

Betrachte

$\{(i,j) \mid i,j \in \mathbb{N}$ i und j gerade oder i und j ungerade$\}$

Wir erhalten folgenden Graphen:

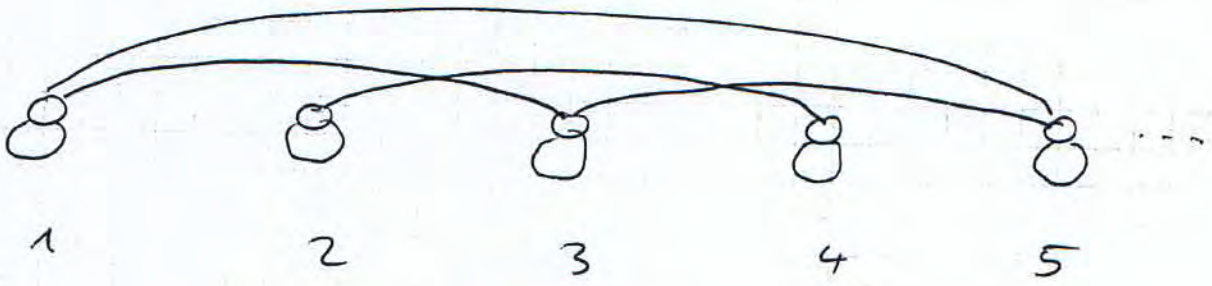


◊

Symmetrische Relationen können durch ungerichtete Graphen repräsentiert werden.

Beispiel 1.12 (Fortführung)

Wir erhalten folgenden ungerichteten Graphen:



◆

Eine Relation $R \subseteq A \times A$ heißt antisymmetrisch falls $(a,b) \in R$ und $a \neq b$, dann $(b,a) \notin R$.

Beispiel 1.13

Sei A die Menge aller Personen. Dann ist

$\{(a,b) \mid a,b \in A$ und a ist Vater von $b\}$

antisymmetrisch.

Die Relation

$$\{(a,b) \mid a,b \in A \text{ und } a \text{ ist Bruder von } b\}$$

ist weder symmetrisch noch antisymmetrisch.

◊

Eine Relation $R \subseteq A \times A$ heißt <u>transitiv</u> falls $(a,b) \in R$ und $(b,c) \in R$ dann $(a,c) \in R$.

<u>Beispiel 1.13</u> (Fortführung)

Die Relation

$$\{(a,b) \mid a,b \in A \text{ und } a \text{ ist ein Vorfahr von } b\}$$

ist transitiv.

◆

<u>Bemerkung</u>:

In Graphen, der eine transitive Relation repräsentiert, ist die Transitivität äquivalent zur Eigenschaft:

Wenn eine Folge von Pfeilen von einem Knoten a zu einem Knoten z existiert, dann existiert auch ein Pfeil von a nach z.

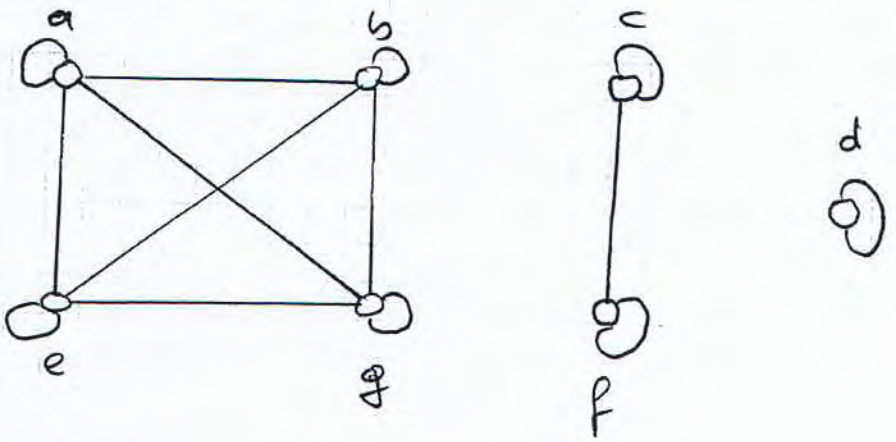
Eine Relation, die reflexiv, symmetrisch und transitiv ist, heißt <u>Äquivalenzrelation</u>.

Bemerkung:
Die Repräsentation einer Äquivalenzrelation durch einen ungerichteten Graphen besteht aus einer Anzahl von Komponenten, für die gilt:

i) In jeder Komponente ist jedes Paar von Knoten durch eine Kante miteinander verbunden.
ii) Zwei Knoten in verschiedenen Komponenten sind nicht miteinander verbunden.

Beispiel 1.14

Folgender Graph repräsentiert eine Äquivalenzrelation:



Die Komponenten einer Äquivalenzrelation heißen Äquivalenzklassen. Wir schreiben $[a]_R$ für diejenige Äquivalenzklasse bzgl der Äquivalenzrelation R, die a enthält. Falls R fest ist, dann schreiben wir kürzer $[a]$. D.h.,

$$[a] = \{b \mid (a,b) \in R\}.$$

Schreibweisen:

$\forall x \ldots$	bedeutet	"für alle $x \ldots$"
$\exists x \ldots$	bedeutet	"es existiert ein x mit..."
$G \Rightarrow H$	bedeutet	"wenn G, dann H"
		"aus G folgt H"
$G \Leftrightarrow H$	bedeutet	$G \Rightarrow H$ und $H \Rightarrow G$.

Satz 1.1
Sei R eine Äquivalenzrelation auf einer Menge A. Dann bilden die Äquivalenzklassen von R eine Partition von A.

Beweis:

Sei $$\Pi = \{ [a] \mid a \in A \}.$$

Ziel: Beweis, dass Π eine Partition von A ist.

Hierzu müssen wir zeigen, dass

i) jede Äquivalenzklasse in Π nichtleer,
ii) die Äquivalenzklassen in Π paarweise disjunkt und
iii) A gleich der Vereinigung der Äquivalenzklassen in Π

sind.

Reflexivität von $R \Rightarrow a \in [a] \ \forall a \in A$.
$\Rightarrow$ i)

Annahme:

Es existieren zwei verschiedene Äquivalenzklassen $[a]$ und $[b]$ mit $[a] \cap [b] \neq \emptyset$

Dann existiert ein $c \in A$ mit $c \in [a] \cap [b]$.

$\Rightarrow$

$(a,c) \in R$ und $(c,b) \in R$.

Transitivität von R $\Rightarrow$ $(a,b) \in R$

Symmetrie von R $\Rightarrow$ $(b,a) \in R$.

Betrachte $d \in [a]$ beliebig. Dann gilt

$(d,a) \in R$

Transitivität von R $\Rightarrow$ $(d,b) \in R$

$\Rightarrow$

$d \in [b]$

Also gilt $[a] \subseteq [b]$.

Genauso zeigt man $[b] \subseteq [a]$.

Also gilt $[a] = [b]$, was ein Widerspruch zur Annahme $[a] \neq [b]$ ist.

$\Rightarrow$ ii)

Wegen $\bigcup \Pi = \bigcup_{a \in A} [a]$ und $a \in [a]$ $\forall a \in A$ gilt iii) offensichtlich.

$\square$

Gegeben eine Äquivalenzrelation R auf einer Menge A können wir die zu R korrespondierende Partition Π von A konstruieren.

Umgekehrt können wir die zu einer gegebenen Partition Π einer Menge A korrespondierende Äquivalenzrelation R wie folgt definieren:

$$R := \{ (a,b) \mid a,b \in A \text{ und } a,b \text{ sind in derselben Menge der Partition } \Pi \}.$$

Beachte, dass in der Definition von R die Elemente a und b nicht verschieden sein müssen.

Eine Relation, die reflexiv, antisymmetrisch und transitiv ist, heißt <u>partielle Ordnung</u>.

<u>Beispiel 1.15:</u>

<u>Vereinbarung</u>: Jede Person ist Vorfahr von sich selbst.

Dann ist folgende Relation R eine partielle Ordnung:

$$R := \{ (a,b) \mid a,b \text{ Personen und } a \text{ ist ein Vorfahr von } b \}$$

◊

Eine partielle Ordnung $R \subseteq A \times A$ heißt <u>totale Ordnung</u>, falls $\forall\, a,b \in A,\ a \neq b$

entweder $(a,b) \in R$ oder $(b,a) \in R$.

Beispiel 1.15 (Fortführung)

Obige Relation R ist nicht total, da Geschwister nicht miteinander in Relation stehen.

$\leq$ definiert eine totale Ordnung auf Zahlen. ◆

Eine Kette in einer binären Relation R ist eine Folge $(a_1, a_2, \ldots, a_n)$ für ein $n \geq 1$, so dass $n=1$ oder $(a_i, a_{i+1}) \in R$ für $1 \leq i < n$. Wir sagen dann, dass $(a_1, a_2, \ldots, a_n)$ eine Kette von a_1 nach a_n ist. Die Kette $(a_1, a_2, \ldots, a_n)$ ist ein einfacher Kreis, falls $n=1$ oder $a_i \neq a_j$ für $1 \leq i < j \leq n$ und $(a_n, a_1) \in R$. Ein einfacher Kreis $(a_1, a_2, \ldots, a_n)$ ist trivial, falls $n=1$. Andernfalls ist ein einfacher Kreis nichttrivial.

Satz 1.2

Eine Relation R ist genau dann eine partielle Ordnung, wenn sie reflexiv und transitiv ist und keine nichttriviale Kreise besitzt.

Beweis:

„$\Rightarrow$“

Annahme: R ist eine partielle Ordnung.

Definition von partielle Ordnung $\Rightarrow$

R ist reflexiv und transitiv.

Zu zeigen: R besitzt keine nichttriviale Kreise.

Annahme:

R hat nichttrivialen Kreis $(a_1, a_2, \dots, a_n)$, $n \geq 2$.

$\Rightarrow$

$(a_n, a_1) \in R$

Transitivität von R $\Rightarrow$ $(a_1, a_n) \in R$.

Dies ist ein Widerspruch zur Antisymmetrie der partiellen Ordnung

$\Rightarrow$

R besitzt keine nichttriviale Kreise.

„$\Leftarrow$"

Annahme:

R ist reflexiv, transitiv und besitzt keine nichttriviale Kreise.

Zu zeigen: R ist antisymmetrisch.

Annahme: R ist nicht antisymmetrisch

$\Rightarrow$

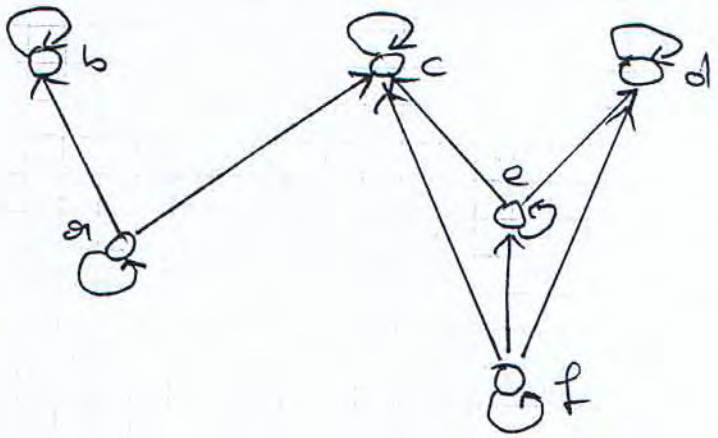
$\exists\, a, b$ mit $a \neq b$ und $(a,b), (b,a) \in R$

Dann ist (a,b) ein nichttrivialer Kreis, was gemäß Annahme nicht sein kann.

$\Rightarrow$ R ist antisymmetrisch.

Sei $R \subseteq A \times A$ eine partielle Ordnung. Ein Element $a \in A$ heißt <u>minimales Element bezüglich R</u>, falls $(b, a) \in R \Rightarrow b = a$. Falls die partielle Ordnung fest ist, dann heißt a auch <u>minimales Element von A</u>.

<u>Beispiel 1.20</u>



a und f sind die minimale Elemente.

<u>Bemerkung</u>

- Jede endliche partielle Ordnung besitzt mindestens ein minimales Element. (überzeugen Sie sich).
- Eine unendliche partielle Ordnung kann ein minimales Element besitzen oder nicht. (überzeugen Sie sich).

Beispiel 1.21

Sei S eine beliebige Kollektion von Mengen. Die Relation R_S sei wie folgt definiert:

$$R_S := \{ (A,B) \mid A,B \in S \text{ und } A \subseteq B \}.$$

R_S definiert eine partielle Ordnung auf S.

- Betrachte

$$S := \left\{ \{ x \mid x \in \mathbb{R} \text{ und } 0 \leq x \leq \tfrac{1}{n} \} \mid n \in \mathbb{N} \right\}$$

Dann besitzt R_S kein minimales Element.

- Betrachte

$$S := \{ \{a\}, \{b\}, \{a,b\} \}.$$

Dann besitzt R_S zwei minimale Elemente.

◆

Infixnotation:

Manchmal schreiben wir $a R b$ anstatt $(a,b) \in R$.

Für Gleichheit verwenden wir immer die Infix-notation. Wir schreiben

$$a = b \text{ anstatt } (a,b) \in =.$$

1.5 Abschlusseigenschaften

Die Summe zweier natürlichen Zahlen ist stets wieder eine natürliche Zahl. Daher sagen wir, dass die Menge $\mathbb{N}$ der natürlichen Zahlen unter der Operation Addition abgeschlossen ist. Die Differenz zweier natürlichen Zahlen kann eine negative Zahl ergeben. Da negative Zahlen keine natürliche Zahlen sind, ist somit $\mathbb{N}$ nicht unter der Operation Subtraktion abgeschlossen.

Frage:
Welche Zahlen müssen wir zu $\mathbb{N}$ hinzunehmen um eine unter Subtraktion abgeschlossene Menge, die $\mathbb{N}$ enthält, zu erhalten?

Wenn wir zu $\mathbb{N}$ die Null und die negative Zahlen hinzunehmen, dann erhalten wir die Menge $\mathbb{Z}$ der ganzen Zahlen. Diese ist unter der Subtraktion abgeschlossen. Wenn wir aus $\mathbb{Z}$ die Null oder eine negative Zahl entfernen, dann ist die resultierende Menge nicht mehr unter der Subtraktion abgeschlossen. Somit ist $\mathbb{Z}$ die kleinste Menge, die $\mathbb{N}$ enthält und unter Subtraktion abgeschlossen ist.

Weiterhin ist die Menge $\mathbb{Z}$ genau diejenige Menge von Zahlen, die man aus $\mathbb{N}$ mittels wiederholten Subtraktionen erhalten kann.

Daher heißt $\mathbb{Z}$ auch der Abschluss von $\mathbb{N}$ unter Subtraktion.

Ziel:
Entwicklung von allgemeinen Eigenschaften von Abschlüssen.

Hierm definieren wir zunächst allgemein, wann eine Menge abgeschlossen ist. Seien D eine Menge, $n \geq 0$ und $R \subseteq D^{n+1}$ eine $(n+1)$-stellige Relation auf D. Eine Teilmenge B von D heißt abgeschlossen unter R, falls

$$b_1, b_2, \ldots, b_n \in B \text{ und } (b_1, b_2, \ldots, b_{n+1}) \in R$$
$$\Rightarrow \quad b_{n+1} \in B.$$

Jede Eigenschaft der Form "B ist abgeschlossen unter den Relationen $R_1, R_2, \ldots, R_m$" heißt Abschlusseigenschaft von B.

Beispiel 1.22

Seien $D = 2^{\mathbb{N}}$, $n = 2$ und $R \subseteq D^3$ definiert durch

$$(S, T, U) \in R \iff U = S \cap T.$$

B ist abgeschlossen unter R bedeutet dann, dass der Durchschnitt zweier beliebigen Mengen in B wieder in B liegt.

Folgende Teilmenge $\mathcal{B}$ von D ist abgeschlossen unter R:

$$\mathcal{B} := \{\{x \in \mathbb{N} \mid a \leq x \leq b\} \mid a, b \in \mathbb{N}\}.$$

Beachte, dass $a > b$

$$\{x \in \mathbb{N} \mid a \leq x \leq b\} = \emptyset$$

impliziert.

Beispiel 1.23

Da Relationen selbst Mengen sind, können wir sagen, dass eine Relation unter einer oder mehreren anderen Relationen abgeschlossen ist.

Seien D eine Menge und $Q \subseteq (D \times D)^3$ eine dreistellige Relation auf D^2 definiert durch

$$Q := \{((a,b),(b,c),(a,c)) \mid a, b, c \in D\}.$$

Dann ist eine Relation $R \subseteq D \times D$ genau dann transitiv, wenn R unter Q abgeschlossen ist. Somit kann die Transitivität einer Relation als eine Abschlusseigenschaft aufgefasst werden.

Auch die Reflexivität von R kann als eine Abschlusseigenschaft aufgefasst werden. Hierzu definieren wir folgende einstellige Relation auf D^2:

$Q' := \{((a,a)) \mid a \in D\}$.

$R \subseteq D \times D$ ist genau dann reflexiv, wenn R unter Q' abgeschlossen ist.

◆

Beispiel 1.24

Seien D eine Menge, $n \geq 0$ und $f: D^n \to D$ eine Funktion. $B \subseteq D$ heißt abgeschlossen unter f, falls $f(b_1, b_2, \ldots, b_n) \in B$ für alle $b_1, b_2, \ldots, b_n \in B$.

Wenn wir $f: D^n \to D$ als eine Relation $R \subseteq D^{n+1}$ auffassen, dann kann "abgeschlossen unter f" als "abgeschlossen unter R" interpretiert werden.

◆

Ausgehend von einer Menge A betrachtet man häufig "die kleinste" Menge B, die A enthält und eine Eigenschaft P besitzt. Damit die Menge B wohldefiniert ist, muss "die kleinste" eine eindeutige Bedeutung besitzen. Üblicherweise bedeutet "die kleinste" nicht "die kleinste Größe haben", sondern "die minimale bezüglich der partiellen Ordnung bei Mengeninklusion".

Da eine Menge von Mengen verschiedene minimale Elemente oder keines besitzen kann, hängt die Wohldefiniertheit von B von der Art der Eigenschaft P und der Menge A ab.

Beispiel 1.25

Betrachte $A := \{a\}$ und

$P :=$ " besitzt entweder b oder c als Element ".

Dann ist B nicht wohldefiniert, da sowohl $\{a,b\}$ als auch $\{a,c\}$ minimale Mengen mit A als Teilmenge und mit Eigenschaft P sind.

Folgender Satz zeigt, dass für eine Abschlusseigenschaft P die Menge B immer wohldefiniert ist.

Satz 1.3

Sei P eine Abschlusseigenschaft, die durch Relationen auf einer Menge D definiert ist und sei $A \subseteq D$. Dann existiert eine eindeutige minimale Menge B mit $A \subseteq B$, die die Eigenschaft P besitzt.

Beweis:

Sei P definiert als Abschluss unter den Relationen $R_1, R_2, \dots, R_m$, wobei $R_i \subseteq D^{n_i+1}$ für ein $n_i \in \mathbb{N}_0$, $1 \leq i \leq m$.

Sei S die Menge <u>aller</u> Mengen, die unter $R_1, R_2, \dots, R_m$ abgeschlossen sind und A als Teilmenge haben.

Da D selbst unter jedem R_i abgeschlossen ist und $A \subseteq D$ gilt

$$S \neq \emptyset.$$

Betrachte

$$B := \bigcap S.$$

<u>Beh.</u>: B ist das eindeutige minimale Element von S.

<u>Bew d. Beh.</u>:

Zunächst beweisen wir, dass $B \in S$.

- Es gilt $A \subseteq B$, da $A \subseteq C \quad \forall C \in S$.
- Betrachte $i \in \{1, 2, \dots, m\}$ beliebig aber fest. Seien
$$b_1, b_2, \dots, b_{n_i} \in B \text{ und } (b_1, b_2, \dots, b_{n_i+1}) \in R_i$$

Dann gilt

$$b_1, b_2, \dots, b_{n_i} \in C \quad \forall C \in S.$$

Da jedes $C \in S$ abgeschlossen ist unter R_i gilt

$$b_{u_i+1} \in C \quad \forall\, C \in S$$

$$\Rightarrow$$

$$b_{u_i+1} \in B$$

Also ist B abgeschlossen unter R_i.
Insgesamt haben wir gezeigt, dass $B \in S$.

Betrachte B' beliebig mit

$A \subseteq B'$ und B' ist abgeschlossen unter R_i, $1 \leq i \leq m$.

Dann gilt $B' \in S$. $\Rightarrow$ $B \subseteq B'$.
Also ist B minimal und auch das einzige minimale Element von S.

■

Das im Beweis von Satz 1.3 konstruierte B heißt <u>Abschluss von A unter den Relationen $R_1, R_2, \ldots, R_m$</u>.

Eine wichtige Anwendung des Satzes 1.3 ist der <u>reflexive, transitive Abschluss</u> R^* einer binären Relation $R \subseteq A \times A$. R^* ist der Abschluss von R unter den Relationen

$$Q := \{((a,b),(b,c),(a,c)) \mid a,b,c \in A\}$$

$$Q' := \{((a,a)) \mid a \in A\}.$$

Beispiel 1.26

Betrachte

$$R := \{(a,b) \mid \exists \text{ Straße zwischen } a \text{ und } b\}.$$

Dann ist

$$R^* = \{(a,b) \mid b \text{ ist von } a \text{ über Straßen erreichbar}\}.$$

Die Definition von R^* gemäß Satz 1.3 gibt uns eine Sicht "von oben". R^* ist minimal unter einer Klasse von Relationen mit ähnlichen Eigenschaften. Folgender Satz charakterisiert R^* "von unten":

Satz 1.4

Der reflexive, transitive Abschluss R^* einer zweistelligen Relation R ist gleich

$$R \cup \{(a,b) \mid \exists \text{ Kette in } R \text{ von } a \text{ nach } b\}.$$

Bemerkung:

Obiger Satz sagt aus, welche geordnete Paare zu R hinzugenommen werden müssen, um R^* zu erhalten.

Beweis:

Sei $\bar{R} := R \cup \{(a,b) \mid \exists \text{ Kette von } a \text{ nach } b \text{ in } R\}$

Zu zeigen: $R^* = \bar{R}$

Hierzu beweisen wir zunächst $R^* \subseteq \bar{R}$ und dann $R^* \supseteq \bar{R}$.

„$\subseteq$"

Betrachte $(a,b) \in R^*$ beliebig aber fest.
Zu zeigen: $(a,b) \in \bar{R}$.

Falls $(a,b) \in R$, dann gilt offensichtlich $(a,b) \in \bar{R}$.
Gemäß der Definition einer Kette existiert in jeder Relation R die Kette von a nach a.
$\Rightarrow$
$(a,a) \in \bar{R}$ $\forall a \in A$. Somit haben wir $(a,b) \in \bar{R}$ für den Fall $a = b$ bewiesen.

Annahme: $(a,b) \notin R$ und $a \neq b$.

$(a,b) \in R^* \Rightarrow$

(a,b) ist im Abschluss von R unter der Relation Q.

$\Rightarrow \exists\, c \in A$ mit $(a,c), (c,b) \in R^*$
D.h., wir haben nun die Folge

$(a,c), (c,b)$

Falls $(a,c) \in R$, dann terminiert unsere

Betrachtung bezüglich (a,c). Falls $(a,c) \notin R$, dann setzen wir die Betrachtung von (a,c) rekursiv fort und ersetzen in obiger Folge (a,c) durch die aus (a,c) konstruierte Folge.

Genauso verfahren wir mit (c,b).

Insgesamt erhalten wir eine Folge

$$(a,c_1), (c_1,c_2), \ldots, (c_{k-1}, c_k), (c_k, b)$$

mit $k \geq 1$ und jedes Paar in obiger Folge ist in R enthalten.

$\Rightarrow$

Wir haben die Kette $(a, c_1, c_2, \ldots, c_k, b)$ von a nach b in R konstruiert.

$\Rightarrow$

$(a,b) \in \overline{R}$.

„$\supseteq$"

Übung

■

Mitunter verwendet man in der Literatur

„reflexive, transitive Hülle" Synonym für „reflexiven, transitiven Abschluss".

Falls man nicht die Reflexivität verlangt, dann spricht man vom <u>transitiven Abschluss</u> R^+.

1.6 Endliche und unendliche Mengen

Zwei Mengen A und B sind gleichmächtig (in Zeichen: $|A| = |B|$), falls eine bijektive Abbildung $f: A \to B$ existiert.

Bemerkung:

a) Falls A eine endliche Menge ist, dann bedeutet $|A| = |B|$, dass B auch eine endliche Menge ist und B genausoviele Elemente enthält wie A.

b) Wenn $f: A \to B$ eine bijektive Abbildung ist, dann existiert eine bijektive Abbildung $f^{-1}: B \to A$. Also ist die Relation "gleichmächtig" symmetrisch.

Frage:
Sind die Mengen der Vielfachen von 1001 $A := \{1001, 2002, 3003, \dots\}$ und die Menge $\mathbb{N}$ gleichmächtig?

Zur Beantwortung dieser Frage genügt es, entweder eine Bijektion $f: A \to \mathbb{N}$ anzugeben oder zu beweisen, dass solche nicht existiert.

$f: A \to \mathbb{N}$ mit $f(i \cdot 1001) := i$ ist eine bijektive Abbildung. (Überzeugen Sie sich).

Wenn A eine endliche Menge ist, dann ist die Kardinalität von A gleich der Elementanzahl von A. Es gibt unendliche Mengen, die nicht gleichmächtig sind (das werden wir noch beweisen). Dies wirft folgende Frage auf:

Frage:
Wie definiert man die Kardinalität von unendlichen Mengen?

Die Beantwortung dieser Frage geht über die Vorlesung hinaus. Jedoch werden wir zwischen zwei Arten von unendlichen Mengen unterscheiden.

Eine Menge A heißt abzählbar, wenn es eine injektive Abbildung $f: A \to \mathbb{N}_0$ gibt. Falls keine solche Injektion existiert, dann heißt A überabzählbar.

Bemerkung:
Abzählbare Mengen sind endlich oder gleichmächtig zu $\mathbb{N}_0$.

Übung:
Zeigen Sie, dass die Relation "gleichmächtig" eine Äquivalenzrelation ist.

Falls eine Menge A abzählbar und nicht endlich ist, dann sagen wir auch, dass A

abzählbar unendlich ist.

Übung:
Beweisen Sie, dass die Menge aller abzählbar unendlichen Mengen exakt diejenigen Mengen, die zu $\mathbb{N}$ gleichmächtig sind, enthält.

Ist $f: A \to \mathbb{N}_0$ injektiv, dann ist f auch auf jeder Teilmenge $S \subseteq A$ injektiv. Also ist jede Teilmenge einer abzählbaren Menge abzählbar.

Satz 1.5
Sei A eine abzählbar unendliche Menge. Dann sind A und $\mathbb{N}$ gleichmächtig.

Beweis:
Wir haben zu zeigen, dass eine bijektive Abbildung $f: A \to \mathbb{N}$ existiert.

A abzählbar unendlich $\Rightarrow$

$\exists$ injektive Abbildung $g: A \to \mathbb{N}_0$.

D.h., für $a, a' \in A$ mit $a \neq a'$ gilt $g(a) \neq g(a')$
Sei

$$g(A) := \{n \in \mathbb{N}_0 \mid \exists\, a \in A \text{ mit } g(a) = n\}.$$

Da A abzählbar unendlich ist $g(A)$ unendlich.

Annahme:

Die Zahlen in $g(A)$ sind aufsteigend sortiert und in dieser Reihenfolge mit 1 beginnend durchnummeriert.

Bezeichne $g(A,i)$ die i-te Zahl in dieser Liste. Wir definieren dann für $a \in A$

$$f(a) := i \text{ , wobei } g(a) = g(A,i)$$

Da g injektiv ist, ist auch f injektiv. Da für jedes $j \in \mathbb{N}$ auch ein $a' \in A$ mit $f(a') = j$ existiert, ist f auch surjektiv.

$\Rightarrow$

f ist bijektiv.

∎

Somit existiert für jede abzählbar unendliche Menge eine Bijektion $f: A \to \mathbb{N}$. Dies erleichtert uns nachfolgend die Arbeit.

Satz 1.6

Die Vereinigung von endlich vielen abzählbaren Mengen ist abzählbar.

Beweis:

Seien

$A_1, A_2, \ldots, A_t$ abzählbare Mengen.

Falls A_i, $i \in \{1,2,\ldots,t\}$ abzählbar unendlich ist,

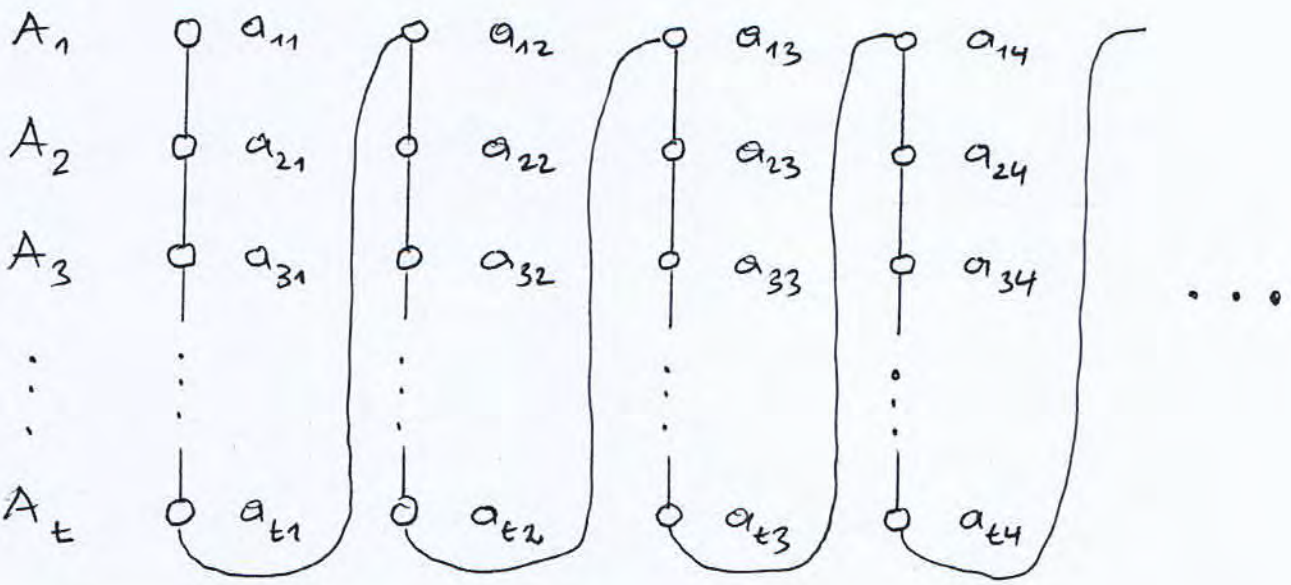
dann existiert eine Bijektion $f: A_i \to \mathbb{N}$.
Falls A_i endlich ist und n Elemente enthält, dann existiert eine Bijektion $f: A_i \to \{1, 2, \dots, n\}$. Dasjenige $a \in A_i$ mit $f(a) = j$ ist das j-te Element von A_i.

Nachfolgend bezeichnet a_{ij} das j-te Element der Menge A_i.

Ziel:
Konstruktion einer Injektion $g: \bigcup_{i=1}^{t} A_i \to \mathbb{N}$.

Idee:

Betrachte zunächst das erste Element von A_1, dann das erste Element von A_2, usw.
Nach dem ersten Element von A_t, betrachte das zweite Element von A_1, dann das zweite Element von A_2, u.s.w. D.h., wir betrachten die Elemente von $A_1, A_2, \dots, A_t$ in der nachfolgend skizzierten Reihenfolge:



Wir starten mit

$$j := 1,$$

betrachten in obiger Reihenfolge das erste Element a_{11}, definieren

$$g(a_{11}) := j;$$
$$j := j+1$$

und betrachten das nächste Element.

Sei a_{akt} das aktuell betrachtete Element. Dann wird wie folgt verfahren:

Falls $g(a_{akt})$ nicht definiert, dann

$$g(a_{akt}) := j;$$
$$j := j+1;$$

Betrachte das nächste Element.

Andernfalls betrachte das nächste Element.

Falls die Mengen $A_1, A_2, \ldots, A_t$ nicht paarweise disjunkt sind, dann kommt es vor, dass für ein aktuell betrachtetes Element a_{akt} der Wert $g(a_{akt})$ bereits definiert ist.

Aus der Konstruktion ergibt sich direkt, dass die Abbildung $g: \bigcup_{i=1}^{t} A_i \longrightarrow \mathbb{N}$ injektiv ist.

■

Satz 1.7

$\mathbb{N} \times \mathbb{N}$ ist abzählbar.

Beweis:

$\mathbb{N} \times \mathbb{N}$ kann betrachtet werden als die Vereinigung von abzählbar unendlich vielen paarweise disjunkten Mengen

$$\{1\} \times \mathbb{N}, \{2\} \times \mathbb{N}, \{3\} \times \mathbb{N}, \ldots$$

Ziel:
Konstruktion einer Injektion $g: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Die Besuchsreihenfolge aus dem Beweis von Satz 1.6 kann hier nicht verwendet werden, da niemals das zweite Element einer Menge besucht werden würde.

Idee:

1. In der ersten Runde besuchen wir das erste Element der ersten Menge: $(1,1)$.
2. In der zweiten Runde besuchen wir das nächste Element der ersten Menge $(1,2)$ und dann das erste Element der zweite Menge: $(2,1)$.
3. In der dritten Runde besuchen wir das nächste nicht besuchte Element der ersten Menge, $(1,3)$ dann das nächste nicht besuchte Element der zweite Menge, $(2,2)$ und dann das erste Element der dritten Menge: $(3,1)$.

⋮

4. In der n-ten Runde besuchen wir das n-te Element der ersten Menge, $(1,n)$, dann das $(n-1)$-te Element der zweiten Menge, $(2,n-1)$, ..., und das erste Element der n-ten Menge.

Unter Verwendung obiger Besuchsreihenfolge können wir endlich zum Beweis von Satz 1.6 den Beweis zuende führen. ∎

Übung:

a) Arbeiten Sie den Beweis von Satz 1.7 aus.

b) Zeigen Sie, dass die Vereinigung von abzählbar vielen abzählbaren Mengen wieder abzählbar ist.

1.7. Drei grundlegende Beweistechniken

Wir werden drei grundlegende Beweistechniken, die in Beweisen immer wieder ihre Anwendung finden, kennenlernen. Diese sind:

die vollständige Induktion, das Schubfachprinzip und die Diagonalisierung.

1.7.1 Die vollständige Induktion

Die Grundidee der vollständigen Induktion beruht auf dem axiomatischen Aufbau der natürlichen Zahlen nach Peano: Man kann jede natürliche Zahl dadurch erhalten, dass man mit eins beginnend wiederholt eins addiert. D.h., wir können die Menge $\mathbb{N}$ der natürlichen Zahlen wie folgt induktiv definieren:

Sei A eine Menge von natürlichen Zahlen, so dass

i) $1 \in A$ und
ii) für jede natürliche Zahl n impliziert $n \in A$ auch $n+1 \in A$.

Dann gilt $A = \mathbb{N}$.

Obiges Prinzip kann man zum Beweis, dass eine Eigenschaft P für alle $n \in \mathbb{N}$ wahr ist, verwenden. Hierzu wendet man obiges Prinzip auf die Menge

$$A := \{ n \in \mathbb{N} \mid P \text{ ist wahr für } n \}$$

auf folgende Art und Weise an:

1) Induktionsanfang: Zeige $1 \in A$.

2) Induktionsvoraussetzung:
Nehmen wir an, dass $n \in A$, d.h., die Eigenschaft P gilt für n.

3) Induktionsschritt $n \rightsquigarrow n+1$:

Unter Verwendung der Induktionsvoraussetzung beweise, dass die Eigenschaft P auch für $n+1$ gilt.

Dann impliziert das Induktionsprinzip, dass $A = \mathbb{N}$, d.h., die Eigenschaft P gilt für jede natürliche Zahl. n heißt Induktionsvariable oder Induktionsparameter.

Beispiel 1.27

Beh.: Für $n \geq 1$ gilt: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Bew.:

$n = 1$:

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}. \quad \checkmark$$

Annahme:
Die Behauptung gilt für ein $n \geq 1$.
D.h., $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

$n \rightsquigarrow n+1$:

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n+1) \underset{\text{Ind.Vor.}}{=} \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2},$$

■

Beispiel 1.28

Beh.:
Für jede endliche Menge A gilt
$$|2^A| = 2^{|A|}$$

Bew.:
Wir beweisen die Behauptung mittels vollständiger Induktion über die Elementanzahl $|A|$ von A.

$|A| = 0$:

Dann ist $A = \emptyset$. Wegen $2^A = \{\emptyset\}$ gilt
$$|2^A| = |\{\emptyset\}| = 1.$$
Ferner gilt
$$2^{|A|} = 2^0 = 1. \quad \checkmark$$

Annahme:

$n \geq 0$ und $\forall A$ mit $|A| = n$ gilt
$$|2^A| = 2^{|A|}$$

$n \rightsquigarrow n+1$:

Sei A eine beliebige Menge mit $|A| = n+1$. Wegen $n \geq 0$ enthält A mindestens ein Element a. Sei
$$B := A \setminus \{a\}.$$
Dann gilt $|B| = n$.

Induktionsvoraussetzung $\Rightarrow$

$$|2^B| = 2^{|B|} = 2^n.$$

Betrachte 2^A. Zerlege 2^A wie folgt:

$$A_1 := \{ C \in 2^A \mid a \notin C \}$$

$$A_2 := \{ D \in 2^A \mid a \in D \}$$

A_1 und A_2 sind paarweise disjunkt und $2^A = A_1 \cup A_2$.

$\Rightarrow$

$$|2^A| = |A_1| + |A_2|$$

Wegen $A_1 = 2^B$ gilt

$$|A_1| = 2^n.$$

A_2 kann wie folgt geschrieben werden:

$$A_2 = \{ C \cup \{a\} \mid C \in 2^B \}.$$

Also gilt

$$|A_2| = |2^B| = 2^n.$$

Insgesamt gilt also

$$|2^A| = 2^n + 2^n = 2^{n+1} = 2^{|A|}.$$

■

Wir haben unseren Induktionsanfang für $|A| = 0$ und nicht für $|A| = 1$ bewiesen. Dennoch ist obiger Beweis korrekt.

Im obigen Beweis haben wir der Induktionsvariablen n folgendermaßen, in Abhängigkeit von der Anzahl der Elementen, Mengen zugeordnet:

$1 \;\hat{=}\;$ Menge mit null Elementen.
$2 \;\hat{=}\;$ Mengen mit einem Element
$3 \;\hat{=}\;$ Mengen mit zwei Elementen
$\vdots$
$n \;\hat{=}\;$ Mengen mit $n-1$ Elementen.

Dann haben wir vollständige Induktion über den Induktionsparameter durchgeführt.

Beispiel 1.29

Beh.:
Die Summe der ersten n, $n \geq 1$ ungeraden Zahlen ist gleich n^2.

Bew.:
n gibt uns hier die Anzahl der ersten ungeraden Zahlen, die aufaddiert werden, an.

$n = 1$:

$$1 = 1^2 \qquad \checkmark$$

Annahme:
Sei $n \geq 1$ und $\sum_{i=0}^{n-1} 2i + 1 = n^2$.

$n \rightsquigarrow n+1$:

$$\sum_{i=0}^{n} (2i+1) = \sum_{i=0}^{n-1} (2i+1) + 2n + 1$$

$$= n^2 + 2n + 1$$

$$= (n+1)^2$$

■

Nicht immer ist es im Induktionsschritt einfach, allein von n auf $n+1$ zu schließen. Betrachtet man den Induktionsschritt genauer, dann sieht man, dass sogar die Gültigkeit der Aussage für alle $\ell \leq n$ vorausgesetzt werden kann. Tut man dies, dann spricht man von der verallgemeinerten vollständigen Induktion.

Beispiel 1.30

Beh.:
Sei $n \geq 2$ eine natürliche Zahl. Dann ist n das Produkt von Primzahlen.

Erinnerung:
$p \in \mathbb{N}$ ist genau dann eine Primzahl, wenn $p \geq 2$ und p nur durch 1 und durch p teilbar ist.

Beweis:

$n = 2$:

2 ist triviales Produkt von sich selbst. Da 2 eine Primzahl ist, folgt somit die Behauptung

Annahme:

Sei $n \geq 2$. Seien alle Zahlen $2 \leq e \leq n$ Produkt von Primzahlen.

$n \rightsquigarrow n+1$:

1. Fall: $n+1$ ist Primzahl.

Dann erfüllt das triviale Produkt, das nur aus dem Faktor $n+1$ besteht, die Behauptung.

2. Fall: $n+1$ ist keine Primzahl.

Dann existieren $2 \leq a, b < n+1$ mit

$$n+1 = a \cdot b$$

Induktionsvoraussetzung $\Rightarrow$

$$a = p_1 \cdot p_2 \cdots p_r \quad \text{und} \quad b = q_1 \cdot q_2 \cdots q_s,$$

wobei die Faktoren in beiden Produkten nicht notwendigerweise verschiedene Primzahlen sind.

$\Rightarrow$

$$n+1 = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

erfüllt die Behauptung.

□

Beispiel 1.31

Beh.:
Jeder Geldbetrag von mindestens 4 Cents kann mit Zwei- und Fünfcentsstücken bezahlt werden.

Bew.:
Hier müssen wir aufgrund des Induktionsschrittes beim Induktionsanfang etwas aufpassen.

$4 \leq n \leq 6$:

Es gilt: $4 = 2+2$ und $6 = 2+2+2$ ✓

Annahme
$n \geq 6$ und jeder Betrag $4 \leq e \leq n$ kann mit Zwei- und Fünfcentsstücken bezahlt werden.

$n \rightsquigarrow n+1$:

Der Betrag $(n+1)-2$ liegt zwischen vier und n und kann somit gemäß Induktionsvoraussetzung mit Zwei- und Fünfcentsstücken bezahlt werden. Fügen wir ein weiteres Zweicentsstück hinzu, dann erhalten wir den Betrag $n+1$.

∎

1.7.2 Das Schubfachprinzip

Schubfachprinzip:
Seien A und B nichtleere endliche Mengen mit $|A| > |B|$. Dann gibt es keine injektive Funktion $f: A \to B$.

Hiervon müssen wir uns überzeugen. Wir interpretieren B als einen Schrank mit $|B|$ Schubfächer und f als eine Methode, die Elemente von A in die Schubfächer des Schrankes platzieren. Wir betrachten die Elemente von A in einer beliebigen, aber festen Ordnung und legen jeweils Betrachtung das Element a in das Schubfach $f(a)$. Falls in dem Fach $f(a)$ bereits ein Element liegt, dann ist f nicht injektiv. Spätestens bei Betrachtung des $(|B|+1)$-ten Elements a (welches wegen $|A| > |B|$ existiert) muss sich in Fach $f(a)$ bereits ein Element befinden. Also kann f nicht injektiv sein.

Beim Beweis des folgenden einfachen Satzes verwenden wir das Schubfachprinzip.

Satz 1.8

Sei R eine binäre Relation auf einer endlichen Menge A. Falls in R eine Kette der Länge $|A|+1$ existiert, dann gibt es in R einen Kreis.

Beweis:

Seien $n := |A|+1$ und $(a_1, a_2, \ldots, a_n)$ eine Kette in R. Betrachte die Funktion

$$f: \{1,2,\ldots,n\} \to A \text{ mit } f(i) = a_i \; \forall i.$$

Schubfachprinzip $\Rightarrow$ f ist nicht injektiv.

Also existieren $1 \leq i < j \leq n$ mit $f(i) = f(j)$.

Betrachte $k > 0$ minimal, so dass $f(m) = f(m+k)$ für ein m, $1 \leq m < n$.

Dann ist $(a_m, a_{m+1}, \ldots, a_{m+k-1})$ ein einfacher Kreis.

■

1.7.3 Die Diagonalisierung

Sei R eine binäre Relation auf einer Menge A. Die Diagonalmenge D der Relation R ist definiert durch

$$D := \{a \mid a \in A \text{ und } (a,a) \notin R\}.$$

Für jedes $a \in A$ sei R_a definiert durch

$$R_a := \{ b \mid b \in A \text{ und } (a,b) \in R \}.$$

Dann gilt $D \neq R_a \quad \forall\, a \in A$.

Dies ist der Fall, da $\forall\, a \in A$ gilt:

$$a \in R_a \iff a \notin D.$$

Wir verwenden obiges Diagonalisierungsprinzip beim Beweis des folgenden Satzes.

Satz 1.9
Die Menge $2^{\mathbb{N}}$ ist überabzählbar.

Beweis:

Annahme: $2^{\mathbb{N}}$ ist aufzählbar unendlich.

$\Rightarrow$

$\exists$ Bijektion $f: \mathbb{N} \to 2^{\mathbb{N}}$.

$\Rightarrow$

$2^{\mathbb{N}}$ kann aufgezählt werden durch

$$S_1, S_2, S_3, \ldots,$$

wobei $S_i = f(i)$ für $i \in \mathbb{N}$.

Betrachte folgende Menge

$$D := \{ n \in \mathbb{N} \mid n \notin S_n \}.$$

Da D eine Menge von natürlichen Zahlen ist, gilt $D \in 2^{\mathbb{N}}$.

$\Rightarrow$

$\exists\, k \in \mathbb{N}$ mit $S_k = D$.

Frage: Gilt $k \in S_k$?

Annahme: $k \in S_k$

Definition von $D \Rightarrow k \notin D$.

Wegen $D = S_k$ impliziert dies $k \notin S_k$

Widerspruch

Annahme: $k \notin S_k$

Definition von $D \Rightarrow k \in D$

Wegen $D = S_k$ impliziert dies $k \in S_k$

Widerspruch

Somit führt die Annahme, dass $2^{\mathbb{N}}$ auf-zählbar unendlich ist, in jedem Fall zum Widerspruch

$\Rightarrow$ Diese Annahme ist falsch

$\Rightarrow$ $2^{\mathbb{N}}$ ist überabzählbar.

∎

2. Modulare Arithmetik

Arithmetik bezeichnet allgemein das Rechnen mit natürlichen und ganzen Zahlen und die Untersuchung der Konsequenzen, die sich daraus ergeben, dass die Division in den ganzen Zahlen nur eingeschränkt möglich ist.

Unter modulare Arithmetik versteht man das Rechnen mit natürlichen Zahlen, wobei dies zyklisch in einem begrenzten Bereich geschieht. Diese geht auf Gauß zurück.

Eine alltägliche Anwendung der modularen Arithmetik ist die Uhr, die den Tag in zwei Abschnitte von jeweils zwölf Stunden aufteilt. Es ist acht Uhr. Wie spät war es vor zehn Stunden? Wie spät wird es in fünf Stunden sein? Jeder kann diese Fragen beantworten. D.h., zyklisches addieren und subtrahieren ist einfach. Die Frage, wie man zyklisch multipliziert bzw dividiert, ist wesentlich schwerer zu beantworten. Dies ist die wichtigste Frage der modularen Arithmetik, die wir nachfolgend beantworten werden.

2.1 Teilbarkeit und Division mit Rest

Seien $a, b \in \mathbb{Z}$. Dann teilt a die Zahl b, falls es ein $k \in \mathbb{Z}$ mit $b = k \cdot a$ gibt. Wir schreiben dafür $a \mid b$. Falls a die Zahl b nicht teilt, dann schreiben wir $a \nmid b$.

Sprechweisen

$a \mid b$: a teilt b, a ist Teiler von b, b ist Vielfaches von a, a ist durch b teilbar.

Unmittelbar aus der Definition ergeben sich die Teilbarkeitsregeln in folgender Übungsaufgabe:

Übung:
Beweisen Sie folgende Teilbarkeitsregeln:

a) $a \mid b \Rightarrow a \mid bc$ für alle $c \in \mathbb{Z}$.
b) ($a \mid b$ und $b \mid c$) $\Rightarrow a \mid c$ (Transitivität)
c) ($a \mid b$ und $a \mid c$) $\Rightarrow a \mid (sb + tc)$ für alle $s, t \in \mathbb{Z}$.
d) ($a \mid (b+c)$ und $a \mid b$) $\Rightarrow a \mid c$.
e) Falls $c \neq 0$, dann gilt $a \mid b \Leftrightarrow ac \mid bc$.
f) ($a \mid b$ und $b \mid a$) $\Rightarrow a = \pm b$.
g) Für $a, b \in \mathbb{N}$ gilt: $a \mid b \Rightarrow a \leq b$.

Die Zahl 0 ist durch alle Zahlen teilbar. Keine Zahl $b \neq 0$ ist durch 0 teilbar. Die Zahlen $+1, -1, b$ und $-b$ heißen triviale Teiler von b.

Eine natürliche Zahl $p \geq 2$, die nur durch 1 und sich selbst teilbar ist, heißt Primzahl.

Satz 2.1 (Division mit Rest)

Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$, so dass

$$a = q \cdot b + r \quad \text{und} \quad 0 \leq r < |b|.$$

Beweis:

Sei S die Menge aller Zahlen ≥ 0 der Form

$$a - xb \quad \text{mit} \quad x \in \mathbb{Z}.$$

$b \neq 0 \Rightarrow S \neq \emptyset$ (überzeugen Sie sich)

Sei

$$r = a - qb$$

das minimale Element in S. Es gilt

$$a = q \cdot b + r$$

Ziel: Beweis, dass $r < |b|$.

Annahme: $r \geq |b|$.

Dann gilt $0 \leq r - |b| < r$

$\Rightarrow$

$$\begin{aligned} r - |b| &= (a - q \cdot b) - |b| \\ &= a - (q \pm 1)\, b \qquad \in S \end{aligned}$$

Dies ist ein Widerspruch dazu, dass r das minimale Element von S ist.

$\Rightarrow$ Annahme ist falsch und somit $r < |b|$.

Dies beweist die Existenz von q und r.
Es verbleibt noch der Beweis der Eindeutigkeit von q und r.

Seien

$$a = qb + r \quad \text{und} \quad a = q'b + r'$$

mit $0 \leq r, r' < |b|$.

Dann gilt

$$r = a - qb \quad \text{und} \quad r' = a - q'b$$

$\Rightarrow$

$$(*) \qquad r - r' = b(q' - q)$$

D.h., $r - r'$ ist ein Vielfaches von b.

Ferner gilt

$$(**) \qquad |r - r'| < |b| \quad \text{(überzeugen Sie sich)}$$

(*) und (**) $\Rightarrow$ $r = r'$

$\Rightarrow$

$$q = q'$$

Die (eindeutig bestimmte) Zahl r heißt <u>Rest von a modulo b</u>. Wir schreiben hierfür

$$r = a \bmod b.$$

Zwei Zahlen a und b, die den selben Rest modulo $n \in \mathbb{N}$ besitzen, heißen kongruent modulo n. Wir schreiben dann

$$a \equiv b \mod n.$$

Bemerkung:

- $a \equiv 0 \mod n$ bedeutet, dass a durch n teilbar ist.
- "$a \equiv b \mod n$" und "$a = b \mod n$" unterscheiden sich.

  $a \equiv b \mod n$ besagt, dass die Reste $a \mod n$ und $b \mod n$ gleich sind.
  $a = b \mod n$ besagt, dass a der Rest von b modulo n ist. Dies impliziert insbesondere $0 \leq a < n$.

Folgende Eigenschaft der Kongruenzen werden wir des Öfteren verwenden, ohne dies explizit zu erwähnen.

Lemma 2.1

Seien $a, b \in \mathbb{Z}$. Dann gilt $a \equiv b \mod n$ genau dann, wenn $a-b$ durch n teilbar ist.

Beweis:

"$\Rightarrow$" Seien

$$a = q_1 n + r \quad \text{und}$$
$$b = q_2 n + r,$$

wobei $0 \leq r < n$.

Dann gilt

$$a - b = q_1 n + r - (q_2 n + r)$$
$$= (q_1 - q_2) n .$$

$$\Rightarrow \quad n \mid (a-b)$$

$\subset =$ " Seien

$$a = q_1 n + r_1 \text{ und}$$
$$b = q_2 n + r_2 ,$$

wobei $0 \leq r_1, r_2 < n$.

$$n \mid (a-b) \Rightarrow n \mid \big((q_1 - q_2) n + (r_1 - r_2)\big)$$

Wegen $|r_1 - r_2| < n$ ist dies nur möglich, wenn $r_1 = r_2$ (Teil d obiger Übungsaufgabe)

$$\Rightarrow \quad a \equiv b \bmod n .$$

∎

Übung:

Seien $d \in \mathbb{N}_0$, $x \equiv y \bmod n$ und $a \equiv b \bmod n$.
Dann gilt:

a) $x + a \equiv y + b \bmod n$.
b) $x - a \equiv y - b \bmod n$.
c) $xa \equiv yb \bmod n$.
d) $x^d \equiv y^d \bmod n$.

Übung:

Beweisen Sie, dass $\equiv$ eine Äquivalenzrelation ist.

2.2 Teilerfremde Zahlen

Seien $a, b \in \mathbb{Z}$ (nicht beide Null). Der größte gemeinsame Teiler $ggT(a,b)$ von a und b ist die größte ganze Zahl $d \geq 1$, die beide Zahlen teilt. a und b heißen teilerfremd oder relativ prim, falls $ggT(a,b) = 1$.

$ax + by$ mit $x, y \in \mathbb{Z}$ heißt Linearkombination von a und b. Falls $ax + by \geq 1$, dann ist die Linearkombination $ax + by$ positiv.

Satz 2.2

Seien $a, b \in \mathbb{Z}$. Dann ist $ggT(a,b)$ die kleinste positive Linearkombination von a und b.

Beweis:

Seien

$$d = ggT(a,b) \quad \text{und}$$

t die kleinste Zahl in $A := \{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}$

Es gilt $A \neq \emptyset$ (überzeugen Sie sich.)

Teil c) der Übungsaufgabe auf S. 71 $\Rightarrow$

$$d \mid t \quad \text{(Beachte } d \mid a \text{ und } d \mid b\text{)}.$$

Teil g, der Übungsaufgabe auf S. 71 $\Rightarrow$

$$d \leq t.$$

Wir zeigen nun $t \mid a$ und $t \mid b$, d.h., t ist ein gemeinsamer Teiler von a und b.

Da d der größte gemeinsame Teiler von a und b ist, folgt aus $d \leq t$, dass $d = t$, womit dann der Satz bewiesen ist.

Wir beweisen nun $t \mid a$ indirekt.

Annahme: $t \nmid a$

Satz 2.1 $\Rightarrow$

$\exists\, q, r \in \mathbb{Z}$, so dass $a = q \cdot t + r$, wobei $0 < r < t$.

Also gilt:

$$r = a - q \cdot t = a - q(ax_0 + by_0)$$
$$= a(1 - qx_0) + b(-qy_0)$$
$$\in A$$

Dies ist ein Widerspruch dazu, dass t die kleinste Zahl in A ist.

$\Rightarrow$

Annahme ist falsch

$\Rightarrow$ $t \mid a$.

$t \mid b$ zeigt man genauso.

Im Allgemeinen gilt nicht

$$n \mid a \cdot b \Rightarrow n \mid a \text{ oder } n \mid b.$$

So gilt zum Beispiel

$$4 \mid 2 \cdot 6 \quad \text{aber} \quad 4 \nmid 2 \quad \text{und} \quad 4 \nmid 6.$$

Im obigen Beispiel sind keine der beiden Zahlen $a = 2$ und $b = 6$ teilerfremd zu $n = 4$.
Der folgende Euklid'sche Hilfssatz zeigt, dass dies so sein muss.

Satz 2.3 (Euklid'scher Hilfssatz)

$$\left(n \mid a \cdot b \text{ und } ggT(a,n) = 1 \right) \Rightarrow n \mid b.$$

Beweis:

Satz 2.2 $\Rightarrow$

$1 = ggT(a,n)$ kann als Linearkombination

$$1 = nx + ay$$

dargestellt werden. Dann gilt auch

$$b = bnx + bay.$$

Da die Zahl n beide Summanden bnx und bay teilt, teilt n auch ihre Summe b.
(beweisen Sie dies formal.)

■

Korollar 2.1

$$ggT(n,a) = ggT(n,b) = 1 \Rightarrow ggT(n, a \cdot b) = 1.$$

Beweis: (indirekt)

Annahme: $ggT(n, a \cdot b) = z \geq 2$.

$z \mid n$, $z \mid a \cdot b$ und $ggT(n,a) \Rightarrow z \nmid a$

Satz 2.3 $\Rightarrow$ $z \mid b$

Dies ist ein Widerspruch zu $ggT(n,b) = 1$.

$\Rightarrow$

Unsere Annahme ist falsch, d.h., $ggT(n, a \cdot b) = 1$. ∎

Sei $n > 0$ eine natürliche Zahl.

Satz 2.1 $\Rightarrow$

Teilt man eine ganze Zahl durch n, dann erhält man einen eindeutigen Rest aus $\{0, 1, 2, \ldots, n-1\}$.

Fasst man die Zahlen in $\mathbb{Z}$, die denselben Rest ergeben, zusammen, dann erhält man eine Partition von $\mathbb{Z}$ in n disjunkte Teilmengen

$$n\mathbb{Z},\ n\mathbb{Z}+1,\ n\mathbb{Z}+2,\ \ldots,\ n\mathbb{Z}+(n-1),$$

wobei für $r = 0, 1, 2, \ldots, n-1$

$$n\mathbb{Z} + r := \{a \cdot n + r \mid a \in \mathbb{Z}\}.$$

Wählt man aus jeder dieser Teilmengen eine beliebige Zahl, dann erhält man eine Repräsentantenmenge. Eine <u>Repräsentantenmenge</u> modulo n ist eine Teilmenge $R \subseteq \mathbb{Z}$ mit $|R| = n$ und die Zahlen in R sind paarweise nicht kongruent modulo n.

$\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ ist somit eine Repräsentantenmenge modulo n.

In $\mathbb{Z}$ kann man für $a \neq 0$ die Gleichung

$$x \cdot a = y \cdot a$$

mit a kürzen, d.h., beide Seiten der Gleichung werden durch a dividiert. Man erhält dann

$$x = y.$$

In $\mathbb{Z}_n$ ist dies nicht ohne weiteres möglich.

<u>Beispiel 2.1</u>

Es gilt

$$2 \cdot 3 \equiv 4 \cdot 3 \mod 6,$$

aber nicht

$$2 \equiv 4 \mod 6.$$

Beobachtung: $ggT(3,6) = 3 > 1$.

Frage:

Kann $xa \equiv ya \mod n$ durch a gekürzt werden, falls $ggT(a,n) = 1$?

Lemma 2.2 (Kürzungsregel).

Falls $ggT(a,n) = 1$ und $ax \equiv ay \mod n$, dann gilt auch $x \equiv y \mod n$.

Beweis:

$$(ax \equiv ay \mod n) \Rightarrow$$

$$n \mid ax - ay \quad \text{(rechnen Sie nach!)}$$

Also gilt auch $n \mid (x-y)a$.

$ggT(n,a) = 1$ und Satz 2.3 $\Rightarrow$

$$n \mid (x-y)$$

D.h., $x \equiv y \mod n$.

∎

Seien $a \in \mathbb{Z}$ und $R \subseteq \mathbb{Z}$ eine Repräsentantenmenge modulo n. Die Menge

$$aR = \{ ax \mod n \mid x \in R \}$$

ist nicht notwendigerweise eine Repräsentantenmenge

menge modulo n.

Beispiel 2.2

$n = 4$, $a = 2$ und $R = \{0,1,2,3\}$.

Es gilt: $2R = \{ 2 \cdot x \bmod 4 \mid x \in R \}$
$= \{0, 2\}$

$\Rightarrow$ $2R$ ist keine Repräsentantenmenge modulo 4.

Beobachtung: $ggT(2,4) = 2 > 1$.

Frage:

Falls $ggT(a,n) = 1$. Gilt dann

R Repräsentantenmenge modulo n
$\Rightarrow$ aR " " " ?

Lemma 2.3

Seien R ein Repräsentantenmenge modulo n und $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$. Dann ist auch aR eine Repräsentantenmenge modulo n.

Beweis:

Es ist zu zeigen, dass $|aR| = n$.

D.h., für $x, y \in R$, $x \neq y$ haben ax und ay modulo n verschiedene Reste.

Annahme:
$\exists\, x, y \in R,\ x \neq y$ mit $ax \equiv ay \bmod n$.

Dann gilt wegen $ggT(a,n) = 1$ und Lemma 2.2

$$x \equiv y \bmod n.$$

Dann sind gemäß Definition von R x und y gleich, Widerspruch

$\Rightarrow$ Annahme ist falsch, d.h. $|aR| = n$.

In $\mathbb{Z}$ ist die Gleichung $ax = b$, $a, b \in \mathbb{Z}$ eindeutig lösbar. Beispiel 2.2 zeigt, dass dies für die Gleichung $ax \equiv b \bmod n$ nicht der Fall sein muss.

~~Frage~~:
Falls $ggT(a,n) = 1$, ist dann $ax \equiv b \bmod n$ in $\mathbb{Z}$ eindeutig lösbar?

Satz 2.4
Seien $a, n \in \mathbb{N}$ und $ggT(a,n) = 1$. Dann ist $ax \equiv b \bmod n$ in $\mathbb{Z}$ lösbar und die Lösung ist modulo n eindeutig.

Beweis:

Sei R eine Repräsentantenmenge modulo n.
Dann gibt es ein eindeutiges Element in R,
das zu b kongruent modulo n ist.

Lemma 2.3 $\Rightarrow$

aR ist eine Repräsentantenmenge modulo n.

Dann gibt es ein eindeutiges Element $ax_0 \in aR$,
$x_0 \in R$, das zu b kongruent modulo n ist. D.h.,

$$ax_0 \equiv b \mod n.$$

$\Rightarrow$

x_0 ist die modulo n eindeutige Lösung von
$ax \equiv b \mod n$.

∎

2.3 Rechnen modulo n

Ziel: Rechnen in der Menge $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

Addition und Multiplikation sind einfach.
Für $a, b \in \mathbb{Z}_n$ berechne $a+b$ bzw $a \cdot b$
in $\mathbb{Z}$ und bilde die Reste modulo n.

Die beiden anderen Operationen $a-b$ und
a/b werden in allen algebraischen Strukturen
mit Hilfe der Addition bzw. Multiplikation
definiert.

$b - a := b + y$, wobei y die Lösung von $x + a = 0$ ist und

$b / a := b \cdot z$, wobei z die Lösung von $x \cdot a = 1$ ist.

Die Zahlen y bzw z heißen die <u>additive</u> bzw. <u>multiplikative Inverse</u> von a und werden mit

$y = -a$ bzw. $z = a^{-1}$ bezeichnet.

Dies bedeutet, dass obige Operationen nur dann definiert sind, wenn die korrespondierenden Inverse existieren.

<u>Beispiel 2.3</u>

Wir möchten $2 - 3$ in $\mathbb{Z}_7$ berechnen. Das additive Inverse -3 von $a = 3 \bmod 7$ ist 4, da

$$4 < 7 \quad \text{und} \quad 3 + 4 = 0 \bmod 7.$$

$\Rightarrow$

$$2 - 3 = 2 + (-3) = 2 + 4 = 6 \quad \text{in } \mathbb{Z}_7.$$

◊

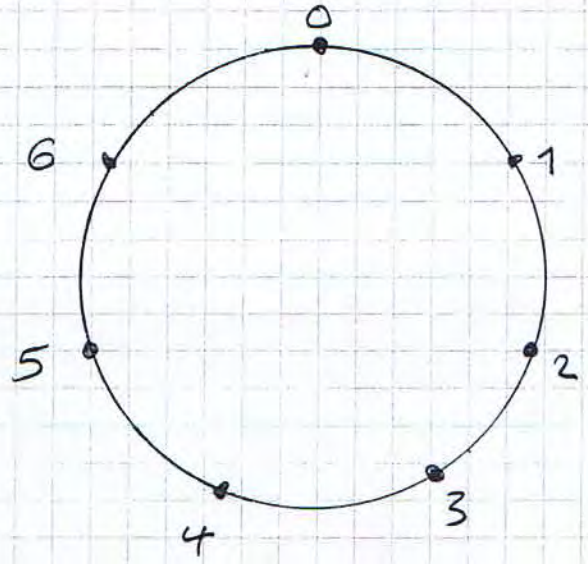
Wegen

$$a + (n - a) = n = 0 \bmod n$$

gilt $-a = n - a$.

Anschauung:

Man kann sich die Menge $\mathbb{Z}_n$ als einen Kreis, auf dem mit gleichem Abstand die n Punkte $0, 1, 2, \ldots, n-1$ markiert sind



$\mathbb{Z}_7$

Zur Berechnung von $a+b$ startet man im Punkt a und geht b Punkte vorwärts. In $\mathbb{Z}_7$ ist dann $3+6 = 2$.

Zur Berechnung von $a-b$ startet man in Punkt a und geht b Punkte rückwärts. In $\mathbb{Z}_7$ erhält man dann $2-3 = 6$.

Zur Berechnung von $a \cdot b \bmod n$ startet man in 0 und geht $a \cdot b$ Punkte vorwärts. In $\mathbb{Z}_7$ erhält man dann $3 \cdot 4 = 5$.

Die Division mod n ist etwas komplizierter. Um durch $a \in \mathbb{Z}_n$ modulo n dividieren zu können, muss in $\mathbb{Z}_n$ das multiplikative Inverse a^{-1} von a mit $a \cdot a^{-1} \equiv 1 \bmod n$ existieren. Existiert

dieses, dann ist Division durch a gleich der Multiplikation mit a^{-1}.

Da in $\mathbb{Z}_n$ die Gleichung $x \cdot 0 = 1$ keine Lösung besitzt, hat 0 kein multiplikatives Inverses. Somit gilt für alle $n \in \mathbb{N}$, dass in $\mathbb{Z}_n$ nicht durch Null dividiert werden kann.

Frage:
Wann besitzt $a \in \mathbb{Z}_n \setminus \{0\}$ ein multiplikatives Inverses?

Satz 2.5
Für eine ganze Zahl a existiert ihr multiplikatives Inverses modulo n genau dann, wenn a relativ prim zu n ist.

Beweis:

„$\subseteq$“

Annahme: $ggT(a,n) = 1$

Satz 2.4 $\Rightarrow$

$ax \equiv 1 \mod n$ hat genau eine Lösung in $\mathbb{Z}_n$.

Definition $\Rightarrow$ Diese Lösung ist das multiplikative Inverse modulo n der Zahl $a \in \mathbb{Z}_n \setminus \{0\}$.

„⇒“

Annahme:

Für ein $a \in \mathbb{Z}_n \setminus \{0\}$ existiert kein multiplikatives Inverses a^{-1} und $ggT(a,n) = d \geq 2$.

Lemma 2.1 $\Rightarrow$ $n \mid ax - 1$

Da $d \mid n$ gilt somit auch $d \mid ax - 1$

Da $d \mid a$ muss 1 auch durch d teilbar sein, was wegen $d \geq 2$ nicht möglich ist.

$\Rightarrow$: Annahme ist falsch. Also gilt Existenz des multiplikativen Inversen a^{-1}

$\Rightarrow$ $ggT(a,n) = 1$.

2.4 Der Euklid'sche Algorithmus

Ziel:

Entwicklung eines Algorithmus, der für gegebene ganze Zahlen a und b den $ggT(a,b)$ berechnet.

Der Algorithmus basiert auf den folgenden einfachen Beobachtungen:

1) $b \mid a \Rightarrow ggT(a,b) = b$.

2) $a = b \cdot t + r \Rightarrow ggT(a,b) = ggT(b,r)$

Übung:
Beweisen Sie die beiden obigen Beobachtungen.

↝

Algorithmus EUKLID
Eingabe: $a, b \in \mathbb{Z}$ mit $a \geq b > 0$.
Ausgabe: $ggT(a,b)$
Methode:

(1) while $b \neq 0$
do
$r := a \bmod b$;
$a := b$;
$b := r$
od;
(2) Ausgabe $:= a$.

Beispiel 2.4

Ziel: Berechnung von $ggT(315, 126)$

$315 = 2 \cdot 126 + 63$
$126 = 2 \cdot 63$

↝ $ggT(315, 126) = 63$ ♦

Frage:
Wie viele Schleifendurchläufe führt der Algorithmus EUKLID höchstens aus?

Satz 2.6

Der Algorithmus EUKLID terminiert nach höchstens $2\lceil \log b \rceil$ Schleifendurchläufe.

Beweis:

Im ersten Durchlauf wird die größere Zahl a durch den Rest r ersetzt.

Wegen $a = t \cdot b + r$, wobei $t \geq 1$ und $b > r$ gilt:

$$r < \frac{a}{2}.$$

D.h., die größere Zahl wird durch eine Zahl, die weniger als halb so groß ist, ersetzt.

Danach ist die andere Zahl b die größere Zahl.

Dies wird solange wiederholt, bis der Rest 0 ist. Da in jedem 2. Durchlauf die zu b korrespondierende Zahl zumindest halbiert wird, ist dies nach

$$\leq 2 \cdot \lceil \log b \rceil$$

Durchläufen der Fall. ∎

Übung

Versuchen Sie für eine Konstante $c < 2$ zu beweisen, dass der Algorithmus EUKLID $\leq c \cdot \log b$ Schleifendurchläufe durchführt. Was ist das kleinste c, für das Sie solchen Beweis hinbekommen?

Frage:
Wie berechnet man für gegebenes $a \in \mathbb{Z}_n \setminus \{0\}$ das multiplicative Inverse a^{-1} modulo n, falls dieses existiert?

1. Idee:

Probiere für alle Zahlen $x = 1, 2, 3, \ldots, n-1$, ob

$$n \mid ax - 1.$$

Ist dies für x der Fall, dann gilt $x = a^{-1}$.

Dieses triviale Verfahren ist sehr aufwändig, so dass dieses für großes n nicht anwendbar ist.

↝

2. Idee
Verwende den Euklid'schen Algorithmus, so dass a^{-1} wesentlich effizienter berechnet wird.

Durchführung:
Wir wenden den Euklid'schen Algorithmus an, um $ggT(a,n) = d$ und gleichzeitig die Linearkombination $d = ax + ny$ zu berechnen.

Wegen

$$ny \equiv 0 \bmod n$$

gilt

$d = 1 \Rightarrow ax \equiv 1 \bmod n$

Also ist im Fall $ggT(a,n) = 1$

$x \bmod n$

das gesuchte multiplikative Inverse.

Frage:

Wir erhalten wir zusätzlich zum $ggT(a,n)$ auch dessen Darstellung als Linearkombination von a und n?

Beobachtung:

- Zunächst berechnet der Euklid'sche Algorithmus

$$n = q_0 a + r_0$$
$$\Leftrightarrow \quad r_0 = n - q_0 a \quad ,$$

was den Rest r_0 als Linearkombination von n und a darstellt.

- Im nächsten Schritt berechnet der Algorithmus

$$a = q_1 \cdot r_0 + r_1$$
$$\Leftrightarrow \quad r_1 = a - q_1 r_0$$

Wir ersetzen nun r_0 durch $n - q_0 a$ und erhalten dann

$$r_1 = a - q_1 (n - q_0 a)$$

$$\Leftrightarrow \quad r_1 = -q_1 n + (1 + q_0 q_1) \cdot a \,,$$

was den Rest r_1 als Linearkombination von n und a darstellt.

u. s. w.

Übung:
Erweitern Sie den Algorithmus EUKLID, so dass dieser auch die Linearkombination des $ggT(a,b)$ der Eingaben a und b ausgibt.

2.5 Primzahlen

Eine wichtige Eigenschaft der Primzahlen ist die Tatsache, dass sich alle Zahlen in $\mathbb{Z} \setminus \{-1, 0, 1\}$ bis auf die Anordnung eindeutig als Produkte von Primzahlen darstellen lassen.

Satz 2.7 (Fundamentalsatz der Arithmetik)

Jede Zahl $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ lässt sich bis auf die Reihenfolge der Faktoren auf genau eine Weise als Produkt von Primzahlen schreiben. D.h., es gibt eine eindeutige Menge von Primzahlen $p_1, p_2, \ldots, p_k$ und positive natürliche Zahlen $s_1, s_2, \ldots, s_k$ mit

$$a = \pm\, p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}.$$

Beweis:

Wir haben bereits im Beispiel 1.30 bewiesen, dass a eine derartige Primzahlzerlegung hat. Somit verbleibt noch der Beweis der Eindeutigkeit der Zerlegung.

Annahme:

a besitzt zwei verschiedene Primzahlzerlegungen.

Wenn wir die Primzahlen, die in beiden Zerlegungen vorkommen, in beiden wegdividieren, dann erhalten wir eine Gleichung der Form

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t ,$$

wobei

a) die Faktoren p_i und q_j Primzahlen sind,

b) auf jeder Seite der Gleichung Primzahlen mehrfach vorkommen können, jedoch

c) keine Primzahl auf der rechten Seite auch auf der linken Seite vorkommt und umgekehrt.

Da $p_1 \mid p_1 p_2 \cdots p_s$ gilt wegen

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

auch

$$p_1 \mid q_1 q_2 \cdots q_t .$$

Satz 2.3 $\Rightarrow$

p_1 ist Teiler von mindestens einem q_j.

Da p_1 und q_j Primzahlen sind, impliziert dies $p_1 = q_j$, Widerspruch.

$\Rightarrow$

Annahme ist falsch, d.h., die Primzahlzerlegung ist eindeutig.

∎

Da die Primzahlzerlegungen teilerfremder Zahlen keine gemeinsamen Primzahlen enthalten, folgt aus Satz 2.7 direkt folgendes Lemma:

Lemma 2.4

Ist eine ganze Zahl x durch a und b teilbar und sind a und b teilerfremd, dann ist x auch durch das Produkt $a \cdot b$ teilbar.

2.6 Der chinesische Restsatz

Beispiel 2.5

"Wie alt bist Du" wird Daisy von Donald gefragt. "So was fragt man eine Dame doch nicht" antwortet diese. "Aber wenn Du mein Alter durch drei teilst, bleibt der Rest zwei!" "Und wenn man Dein Alter durch fünf teilt?" "Dann bleibt wieder der Rest zwei. Und jetzt sage ich Dir auch

noch, dass bei der Division durch sieben der Rest fünf bleibt. Nun müsstest Du aber wissen, wie alt ich bin."

$\rightsquigarrow$

Mathematische Formulierung:

Man finde eine Zahl, die bei Division durch 3, 5, 7 die Reste 2, 2, 5 lässt.

$\Rightarrow$

Zu lösen ist folgendes modulare Gleichungssystem:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 5 \mod 7 \end{aligned}$$

◊

Eine allgemeine Lösungsmethode für derartige Probleme gibt uns der Beweis des folgenden Satzes:

Satz 2.8 (chinesischer Restsatz)

Seien $m_1, m_2, \ldots, m_r$ paarweise teilerfremde natürliche Zahlen und $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. Dann haben die Kongruenzen

$$x \equiv a_i \mod m_i \,, \quad i = 1, 2, \ldots, r$$

gemeinsame Lösungen. Je zwei Lösungen sind einander modulo $\prod_{i=1}^{r} m_i$ kongruent.

Beweis:

Sei $m = \prod_{i=1}^{r} m_i$.

Da die m_i, $1 \le i \le r$ paarweise teilerfremd sind, gilt

$$ggT\left(\frac{m}{m_j}, m_j\right) = 1 \quad \text{für } 1 \le j \le r.$$

Satz 2.5 $\Rightarrow$

$\exists$ ganze Zahlen b_j (das multiplikative Inverse von $\frac{m}{m_j}$ modulo m_j) mit

$$\frac{m}{m_j} \cdot b_j \equiv 1 \mod m_j.$$

Wegen $m_i \mid \frac{m}{m_j}$ für $i \neq j$ ist $\frac{m}{m_j} \cdot b_j$ ein Vielfaches von m_i. Also gilt dann

$$\frac{m}{m_j} \cdot b_j \equiv 0 \mod m_i.$$

Wir setzen

$$x_0 := \sum_{j=1}^{r} \frac{m}{m_j} \cdot b_j \cdot a_j.$$

Dann gilt für $1 \le i \le r$

$$x_0 \equiv \sum_{j=1}^{r} \frac{m}{m_j} \cdot b_j \cdot a_j \equiv \frac{m}{m_i} b_i a_i \equiv a_i \mod m_i.$$

$\Rightarrow$ x_0 ist eine gemeinsame Lösung der gegebenen Kongruenzen.

Es ist noch zu zeigen, dass jede andere gemeinsame Lösung der Kongruenzen modulo m zu x_0 kongruent ist.

Sei hierzu x_1 auch eine gemeinsame Lösung der Kongruenzen.

Ziel:
Charakterisierung von x_1 in Abhängigkeit von x_0.

Es gilt:

$$x_0 \equiv x_1 \mod m_i \quad \text{für } 1 \leq i \leq r.$$

Also impliziert Lemma 2.1

$$m_i \mid x_0 - x_1 \quad \text{für } 1 \leq i \leq r$$

Da m_i, $1 \leq i \leq r$ paarweise teilerfremd sind, folgt aus Lemma 2.4

$$m \mid x_0 - x_1$$

Also impliziert wiederum Lemma 2.1

$$x_0 \equiv x_1 \mod m,$$

womit der Satz bewiesen ist.

□

Beispiel 2.5 (Fortführung)

Wie alt ist nun Daisy? Um dies herauszubekommen müssen wir das modulare Gleichungssystem

$$x \equiv 2 \mod 3$$
$$x \equiv 2 \mod 5$$
$$x \equiv 5 \mod 7$$

lösen. Hierzu wenden wir den chinesischen Restsatz an und erhalten

$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7$$

Diese sind offensichtlich paarweise teilerfremd.

$$m = 3 \cdot 5 \cdot 7 = 105$$

$$\frac{m}{m_1} = 35 \equiv 2 \mod 3 \qquad b_1 = 2^{-1} \mod 3 = 2$$

$$\frac{m}{m_2} = 21 \equiv 1 \mod 5 \qquad b_2 = 1^{-1} \mod 5 = 1$$

$$\frac{m}{m_3} = 15 \equiv 1 \mod 7 \qquad b_3 = 1^{-1} \mod 7 = 1$$

$\rightsquigarrow$

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 5$$
$$= 257$$
$$\equiv 47 \mod 105$$

$\Rightarrow$

Daisy ist 47 Jahre alt.

3. Algebraische Strukturen

In der Schule haben wir bereits gelernt mit Zahlen zu rechnen. Implizit wenden wir dabei Regeln an, die uns das Rechnen erleichtern. Können wir derartige Regeln nur beim Rechnen mit rationalen Zahlen anwenden oder können diese auch bei anderen Mengen, die ähnliche Eigenschaften besitzen, anwenden?

Obige Frage zeigt, wozu Algebra gut ist. Hat man einmal die Anwendbarkeit von Regeln für eine abstrakte algebraische Struktur, die bestimmte Eigenschaften besitzt, bewiesen, dann sind diese auch in allen konkreten Strukturen, für die diese Eigenschaften zutreffen, anwendbar.

Ziel:
Kennenlernen einiger wichtigen algebraischen Strukturen.

3.1 Gruppen

Eine Verknüpfung $\circ$ auf einer Menge M ist eine Abbildung

$$\circ : M \times M \longrightarrow M,$$

die jedem Paar (x,y) von Elementen aus M ein eindeutiges Element $\circ(x,y)$ aus M zuordnet. Wir schreiben auch $x \circ y$ anstatt $\circ(x,y)$.

$\circ$ heißt <u>assoziativ</u>, falls $(x \circ y) \circ z = x \circ (y \circ z)$ für alle $x, y, z \in M$ und <u>kommutativ</u>, falls $x \circ y = y \circ x$ für alle $x, y \in M$.

<u>Beispiel 3.1</u>

Die Addition, Subtraktion und Multiplikation sind Verknüpfungen auf $\mathbb{Q}$. Die Addition und die Multiplikation sind kommutativ und assoziativ. Die Subtraktion ist weder kommutativ noch assoziativ. Da $\frac{x}{0}$ für ein $x \in \mathbb{Q}$ nicht definiert ist, ist die Division keine Verknüpfung auf $\mathbb{Q}$.

◊

Sei M eine Menge und $\circ$ eine Verknüpfung auf M. Falls $\circ$ assoziativ ist, dann heißt die Struktur $(M, \circ)$ <u>Halbgruppe</u>. Ist die Verknüpfung $\circ$ zusätzlich kommutativ, dann heißt $(M, \circ)$ <u>kommutative Halbgruppe</u>.

<u>Beispiel 3.1</u> (Fortführung)

$(\mathbb{Q}, +)$ und $(\mathbb{Q}, \cdot)$ sind kommutative Halbgruppen. $(\mathbb{Q}, -)$ ist keine Halbgruppe.

◊

Ein Element $e \in M$ heißt <u>neutrales Element</u>, falls für alle $x \in M$ gilt

$$e \circ x = x \circ e = x.$$

Sei $(M, \circ)$ eine Halbgruppe und $e \in M$ ein neutrales Element in $(M, \circ)$. Dann heißt die Struktur $(M, \circ, e)$ Monoid.

Übung:
Beweisen Sie, dass eine Halbgruppe $(M, \circ)$ höchstens ein neutrales Element besitzen kann.

Beispiel 3.1 (Fortführung)

$(\mathbb{Q}, +, 0)$ und $(\mathbb{Q}, \cdot, 1)$ sind Monoide.

◇

Besitzt eine Halbgruppe $(M, \circ)$ ein neutrales Element, dann ist folgende Frage sinnvoll:

Existiert für jedes $x \in M$ ein $y \in M$, so dass

$$x \circ y = e \quad ?$$

Sei $(M, \circ, e)$ ein Monoid. Dann heißt $y \in M$ mit $x \circ y = y \circ x = e$ inverses Element oder einfach Inverses von x.

Beispiel 3.1 (Fortführung)

In $(\mathbb{Q}, +)$ ist $-x$ Inverses von x. In $(\mathbb{Q}, \cdot)$ ist $\frac{1}{x}$ Inverses von x.

◇

Ein Monoid $(G, \circ, e)$, in dem jedes Element ein Inverses hat, heißt **Gruppe**.

$\rightsquigarrow$

Sei G eine Menge und $\circ$ eine Verknüpfung auf G. Dann ist $(G, \circ)$ eine **Gruppe**, falls die folgenden drei Eigenschaften erfüllt sind:

1) Es existiert ein neutrales Element $e \in G$.
2) Jedes Element $x \in G$ hat ein Inverses $x^{-1} \in G$.
3) Die Verknüpfung $\circ$ ist assoziativ.

Die Eigenschaften 1-3 heißen **Gruppenaxiome**.

Ist die Verknüpfung $\circ$ auch kommutativ, dann heißt die Gruppe $(G, \circ)$ **kommutative** oder **abelsche** Gruppe.

(Niels Henrik Abel 1802 – 1829).

Beispiel 3.1 (Fortführung)

$(\mathbb{Q}, +)$ und $(\mathbb{Q}, \cdot)$ sind abelsche Gruppen.

Sei $(G, \circ, e)$ eine Gruppe. Die Gleichung $x \circ a = b$ heißt eindeutig lösbar in $(G, \circ, e)$, falls $\forall\, a, b \in G$ genau ein $x \in G$ mit $x \circ a = b$ existiert.

Die Definition von Gruppen ist ein erster Schritt zur Abstraktion von konkreten Mengen und Verknüpfungen.

Frage:
Welche Eigenschaften gelten allgemein in Gruppen?

Satz 3.1 (Gruppeneigenschaften)

Sei $(G, \circ, e)$ eine Gruppe. Dann gilt:

1) Jedes Element $x \in G$ besitzt genau ein Inverses $x^{-1} \in G$.
2) Für alle $x \in G$ gilt $(x^{-1})^{-1} = x$.
3) Für alle $x, y \in G$ gilt $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.
4) Kürzungsregel: Für alle $x, y, z \in G$ gilt
   $(x \circ y = x \circ z \Rightarrow y = z)$ und
   $(y \circ x = z \circ x \Rightarrow y = z)$
5) Eindeutige Lösbarkeit von Gleichungen:
   Für alle $a, b \in G$ existiert genau ein $x \in G$ mit $a \circ x = b$ und genau ein $y \in G$ mit $y \circ a = b$.

Beweis:

1) Annahme: $\exists x \in G$, das zwei verschiedene Inverse y und y' besitzt (d.h., $y \neq y'$).

$\Rightarrow$

$$y = y \circ e = y \circ (x \circ y') = (y \circ x) \circ y'$$
$$= e \circ y' = y' \quad \text{Widerspruch!}$$

2) Sei $y := x^{-1}$. Dann gilt

$$x = x \circ e = x \circ (y \circ y^{-1}) = (x \circ y) \circ y^{-1}$$
$$= e \circ y^{-1} = y^{-1} = (x^{-1})^{-1}$$

3) Es gilt

$$(x \circ y) \circ y^{-1} \circ x^{-1} = x \circ (y \circ y^{-1}) \circ x^{-1}$$
$$= x \circ e \circ x^{-1}$$
$$= x \circ x^{-1}$$
$$= e$$

und

$$y^{-1} \circ x^{-1} \circ (x \circ y) = y^{-1} \circ (x^{-1} \circ x) \circ y$$
$$= y^{-1} \circ e \circ y$$
$$= y^{-1} \circ y$$
$$= e$$

Also ist $y^{-1} \circ x^{-1}$ das Inverse $(x \circ y)^{-1}$ von $x \circ y$.

4) Es gilt

$$y = e \circ y = (x^{-1} \circ x) \circ y = x^{-1} \circ (x \circ y)$$
$$= x^{-1} \circ (x \circ z) = (x^{-1} \circ x) \circ z = e \circ z = z$$

Die zweite Kürzungsregel zeigt man analog

5) Die Elemente $x := a^{-1} \circ b$ und $y := b \circ a^{-1}$ leisten das Gewünschte. Ihre Eindeutigkeit folgt aus den Kürzungsregeln.

∎

Übung:

a) Beweisen Sie die zweite Kürzungsregel.

b) Beweisen Sie die Eindeutigkeit der Elemente $x := a^{-1} \circ b$ und $y := b \circ a^{-1}$ als Lösungen der Gleichungen $a \circ x = b$ und $y \circ a = b$.

Übung:

Bezeichne S_n die Menge aller bijektiven Abbildungen $f: \{1,2,\dots,n\} \longrightarrow \{1,2,\dots,n\}$, d.h., die Menge aller Permutationen von $1,2,\dots,n$. Als Verknüpfung $\circ$ der Permutationen nehmen wir ihre Hintereinanderausführung, d.h., $f \circ g(x) = f(g(x))$. Bezeichne e die identische Permutation, d.h., $e(x) = x$. Zeigen Sie, dass $(S_n, \circ, e)$ eine Gruppe ist. Ist diese Gruppe kommutativ? Beweisen Sie Ihre Antwort.

Beispiel 3.2

Betrachten wir $\mathbb{Z}_n = \{0,1,\dots,n-1\}$ mit den Operationen Addition $+$ modulo n und Multiplikation $\cdot$ modulo n.

- $(\mathbb{Z}_n, +)$ ist eine kommutative Gruppe mit neutralem Element 0 und Inversen $a^{-1} = n-a$ von a.

- $(\mathbb{Z}_n, \cdot)$ ist keine Gruppe, da z.B. 0 kein Inverses besitzt.
- $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ ist für $n = 2$ und $n = 3$ eine kommutative Gruppe. $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ ist keine Gruppe, da $\{1,2,3\}$ nicht bezüglich $\cdot$ abgeschlossen ist. Es gilt

$$2 \cdot 2 \bmod 4 = 0 \notin \mathbb{Z}_4 \setminus \{0\}.$$

Zudem besitzt 2 kein Inverses.

- $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ ist eine Gruppe. (überzeugen Sie sich.) ◆

Sei $\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n \mid a \neq 0 \bmod ggT(a,n) = 1\}$.

Satz 2.5 $\Rightarrow$

$\mathbb{Z}_n^\times$ ist die Menge der Elemente in $\mathbb{Z}_n$, die ein multiplikatives Inverses besitzen.

Satz 3.2

Sei $n > 1$ eine natürliche Zahl und bezeichne $\cdot$ die Multiplikation modulo n. Dann ist $(\mathbb{Z}_n^\times, \cdot)$ eine kommutative Gruppe.

Beweis:

Korollar 2.1 $\Rightarrow$

$\mathbb{Z}_n^\times$ ist unter $\cdot$ abgeschlossen.

Wegen $a \cdot b \bmod n = b \cdot a \bmod n$ ist die Multiplikation modulo n kommutativ.

$1 \in \mathbb{Z}_n^\times$ ist ein neutrales Element in $(\mathbb{Z}_n^\times, \cdot)$.

Satz 2.5 $\Rightarrow$

Jedes Element $a \in \mathbb{Z}_n^\times$ besitzt ein multiplikatives Inverses a^{-1} in $\mathbb{Z}_n$:

Falls $ggT(a^{-1}, n) = 1$, dann liegt a^{-1} auch in $\mathbb{Z}_n^\times$.

Sei
$$d := ggT(a^{-1}, n)$$

Es gilt
$$a \cdot a^{-1} = 1 + kn$$

Wegen $d \mid a^{-1}$ und $d \mid n$ gilt auch $d \mid 1$.

$\Rightarrow$
$$d = 1$$

Also ist in der Tat a^{-1} auch in $\mathbb{Z}_n^\times$. ∎

Sei $(G, \circ, e)$ eine Gruppe. $H \subseteq G$ heißt <u>Untergruppe</u> von G, falls $e \in H$ und $(H, \circ, e)$ eine Gruppe ist. Eine Untergruppe $H \subseteq G$ heißt <u>trivial</u>, falls $H = \{e\}$ oder $H = G$.

<u>Ziel:</u> Bestimmung aller Untergruppen von $(\mathbb{Z}, +, 0)$.

Für $m \in \mathbb{N}$ sei

$$m\mathbb{Z} := \{ m \cdot x \mid x \in \mathbb{Z} \}$$

die Menge aller durch m teilbaren Zahlen in $\mathbb{Z}$.

Satz 3.3

Sei $H \subseteq \mathbb{Z}$ und $(H, +, 0)$ eine nichttriviale Untergruppe von $(\mathbb{Z}, +, 0)$. Dann gilt $H = m\mathbb{Z}$ für ein $m \in \mathbb{N}$.

Beweis:

$(H, +, 0)$ nichttrivial $\Rightarrow$ $H \neq \{0\}$.

$\Rightarrow$

H enthält mindestens ein Paar $-a, a$

Sei $m \in H$ die kleinste positive Zahl in H (d.h., $-m, m \in H$).

Beh.: $H = m\mathbb{Z}$

Bew. d. Beh.:

"$m\mathbb{Z} \subseteq H$":

Offensichtlich gilt $0 \in H$. Eine beliebige Zahl $x \in m\mathbb{Z} \setminus \{0\}$ hat die Form

$$x = \pm q m \quad \text{für ein } q \in \mathbb{N}.$$

$q \cdot m$ erhält man durch q-maliges Addieren von m, $-qm$ durch q-maliges Addieren von $-m$.

H abgeschlossen unter Addition $\Rightarrow$ $x \in H$.

"$\underline{H \subseteq m\mathbb{Z}}$"

Betrachte $x \in H \setminus \{0\}$ beliebig.

z.z. $m \mid x$.

Satz 2.1 $\Rightarrow$

$$x = qm + r \quad \text{für ein } 0 \leq r < m$$

$$\Leftrightarrow \quad r = x - qm$$

Wegen $x, -m \in H$ und H abgeschlossen unter $+$ gilt

$$r \in H$$

Wahl von m $\Rightarrow$ $r = 0$

$\Rightarrow$ $m \mid x$ ∎

Übung

Sei $m \in \mathbb{N}$. Zeigen Sie, dass $(m\mathbb{Z}, +, 0)$ eine Untergruppe von $(\mathbb{Z}, +, 0)$ ist.

(110a)

Seien $(G, \circ, e)$ eine Gruppe, $H \subseteq G$ eine Untergruppe von G und $a \in G$. Dann heißt

$$a \circ H := \{a \circ x \mid x \in H\}$$

$\underline{\text{Linksklasse}}$ von a bezüglich der Untergruppe H und

Übung:
Seien $(G, \circ, e)$ eine Gruppe und $H \subseteq G$. Dann ist $(H, \circ)$ genau dann eine Gruppe, wenn gilt

(1) $a, b \in H \Rightarrow a \circ b \in H \quad \forall\, a, b \in G$,
(2) $e \in H$ und
(3) $a \in H \Rightarrow a^{-1} \in H$.

Übung
Seien $(G, \circ, e)$ eine Gruppe und $H \subseteq G$. Dann ist $(H, \circ)$ genau dann eine Untergruppe von G, wenn $H \neq \emptyset$ und $\forall\, a, b \in G: a, b \in H \Rightarrow a b^{-1} \in H$.

$$H \circ a := \{ x \circ a \mid x \in H \}$$

Rechtsklasse von a bezüglich der Untergruppe H.

Beispiel 3.3

Betrachten wir die Untergruppe

$$H := 5\mathbb{Z} = \{ 5 \cdot x \mid x \in \mathbb{Z} \}$$

der Gruppe $(\mathbb{Z}, +, 0)$.

Die Linksklassen $2 + H$ und $7 + H$ sind gleich, da

$$7 + 5x = 2 + 5(x+1).$$

Es gibt genau fünf voneinander verschiedenen Linksklassen bezüglich H, nämlich die Restklassen modulo 5.

Satz 3.4

Sei $(H, \circ, e)$ eine Untergruppe der Gruppe $(G, \circ, e)$. Dann gehört jedes Element $x \in G$ zu genau einer Linksklasse bezüglich H.

Beweis:

Wegen $e \in H$ gehört jedes $x \in G$ zur Linksklasse $x \circ H$.

z.z. $\nexists x \in G$ mit x ist Element von zwei verschiedenen Linksklassen.

Annahme: $a \circ H \cap b \circ H \neq \emptyset$

2.2. $a \circ H = b \circ H$

"$a \circ H \subseteq b \circ H$"

Annahme $\Rightarrow \exists v, w \in H: \; a \circ w = b \circ v$

$\Rightarrow \quad a = b \circ v \circ w^{-1}$

$\Rightarrow \quad a \circ u = b \circ \underbrace{v \circ w^{-1} \circ u}_{\in H} \qquad \forall u \in H$

Also gilt $\forall u \in H: \; a \circ u \in b \circ H$

$\Rightarrow \quad a \circ H \subseteq b \circ H$

"$b \circ H \subseteq a \circ H$"

analog (Übung)

∎

Übung:

Sei $(G, \circ, e)$ eine Gruppe und $H \subseteq G$ eine Untergruppe von G. $a, b \in G$ heißen äquivalent $a \sim b$, wenn $a^{-1} b \in H$.

a) Zeigen Sie, dass $\sim$ eine Äquivalenzrelation ist.
b) Zeigen Sie, dass die Äquivalenzklassen der Relation $\sim$ genau die Linksklassen bezüglich H sind.
c) Beweisen Sie, dass $a \circ H$ und H gleichmächtig sind.

In einer Gruppe $(G,\circ,e)$ definieren wir für ein Element $a \in G$ induktiv

$$a^0 := e \,, \quad a^1 := a \,,$$
$$a^k := a \circ a^{(k-1)} \quad \text{für } k > 1$$
$$a^{-k} := (a^{-1})^k$$

Seien $(G,\circ,e)$ eine Gruppe und $H \subseteq G$ eine Untergruppe. Die Anzahl der verschiedenen Linksklassen bezüglich H heißt <u>Index von H in G</u> (in Zeichen: $[G:H]$ oder einfach und H, falls die zugrunde liegende Gruppe G klar ist).

Die Anzahl der Elemente einer Gruppe $(G,\circ,e)$ heißt <u>Ordnung</u> $\operatorname{ord} G$ der Gruppe G. Falls es für $a \in G$ eine natürliche Zahl m mit $a^m = e$ gibt, dann heißt die kleinste solche Zahl m die <u>Ordnung</u> $\operatorname{ord} a$ von a (in G). Gibt es ein derartiges m nicht, dann ist die Ordnung von a (in G) unendlich.

<u>Satz 3.5</u>

Seien $(H',\circ,e)$ und $(H'',\circ,e)$ Untergruppen der Gruppe $(G,\circ,e)$ mit $H'' \subseteq H'$. Dann gilt

$$[G:H''] = [G:H'] \cdot [H':H''].$$

<u>Beweis:</u>

Wir stellen G als Vereinigung der Links-klassen bezüglich H' dar, etwa:

$$G = \bigcup_{i \in I} a_i H' , \qquad (*)$$

wobei die Elemente $a_i \in G$ derart gewählt sind, dass die Linksklassen paarweise verschieden sind.

$\Rightarrow$

$a_i H'$, $i \in I$ sind paarweise disjunkt und

$$|I| = [G : H'] .$$

Sei

$$H' = \bigcup_{j \in J} b_j H'' , \qquad (**)$$

wobei die Elemente $b_j \in H'$ derart gewählt sind, dass die Linksklassen paarweise verschieden sind.

$\Rightarrow$

$b_j H''$, $j \in J$ sind paarweise disjunkt und

$$|J| = [H' : H''] .$$

Durch Einsetzung von $(**)$ in $(*)$ erhalten wir

$$G = \bigcup_{i \in I} a_i \left(\bigcup_{j \in J} b_j H'' \right)$$

$$= \bigcup_{i \in I} \bigcup_{j \in J} a_i b_j H'' .$$

Übung:
Beweisen Sie, dass die Mengen

$$a_i b_j H'' \quad , \quad i \in I, j \in J$$

paarweise disjunkt sind.

$\Rightarrow$

$$[G : H''] = |I| \cdot |J|$$

$$= [G : H'] \cdot [H' : H'']$$

Der folgende Satz von Lagrange ist eine einfache Folgerung aus Satz 3.5

Satz 3.6 (Satz von Lagrange)
Sei $(G, \circ, e)$ eine Gruppe und $(H, \circ, e)$ eine Untergruppe von G. Dann gilt

$$\operatorname{ord} G = \operatorname{ord} H \cdot \operatorname{ind} H.$$

Beweis:

Sei $E := \{e\}$ triviale Untergruppe von G und auch von H. Dann gilt

$$\operatorname{ord} G = [G : E] \quad \text{und}$$
$$\operatorname{ord} H = [H : E].$$

Satz 3.5 $\Rightarrow$

$$[G:E] = [G:H] \cdot [H:E]$$

" " "

ord G und H ord H

Satz 3.7

Seien $(G, \circ, e)$ eine endliche Gruppe, d.h. ord $G < \infty$, und $a \in G$. Dann ist $H_a := \{a^0, a^1, \dots\}$ eine Untergruppe von G.

Beweis

Da es nur endlich viele Gruppenelemente gibt, muss mindestens ein Glied in der Folge $a^0, a^1, a^2, \dots$ mehrfach vorkommen

Betrachte i minimal, so dass a^i mehrfach vorkommt und sei $j > i$ minimal, so dass $a^i = a^j$.

Es gilt

$$\begin{aligned} e &= a^i \circ (a^i)^{-1} \\ &= a^i \circ (a^{-1})^i \\ &= a^j \circ (a^{-1})^i \\ &= a^{j-i} \end{aligned}$$

Zunächst zeigen wir, dass $i = 0$ sein muss.

Annahme: $i > 0$

$\Rightarrow \quad j - i \geq 1$

Falls $j - i > i$, dann erhalten wir einen Widerspruch zur Wahl von j.

Falls $j - i < i$, dann wäre dies ein Widerspruch zur Wahl von i.

$\Rightarrow \quad j - i = i \quad \Leftrightarrow \quad j = 2i$

Dann gilt aber auch

$$e = a^0 = a^i$$

was wiederum der Wahl von i widerspricht

Also ist unsere Annahme falsch, d.h., es gilt

$$i = 0.$$

Also gilt

$$H_a = \{a^0, a^1, \ldots, a^m\},$$

wobei $m = \operatorname{ord} a$.

Übung:

Beweisen Sie, dass $H_a = \{a^0, a^1, \ldots, a^{\operatorname{ord} a}\}$ eine Untergruppe von G ist.

∎

Eine Gruppe $(G,\circ,e)$ heißt <u>zyklisch</u>, wenn $a \in G$ mit $H_a = G$ existiert. Dann heißt das Element a <u>erzeugendes Element</u> von G.

<u>Beispiel 3.4</u>

Betrachten wir die Gruppe

$$(\mathbb{Z}_5, +, 0), \quad \mathbb{Z}_5 = \{0,1,2,3,4\}.$$

Dann ist jedes $a \in \mathbb{Z}_5 \setminus \{0\}$ ein erzeugendes Element dieser Gruppe:

erzeugendes Element				
1	$\overbrace{1}^{1}$	$\overbrace{1+1}^{2}$	$\overbrace{1+1+1}^{3}$	$\overbrace{1+1+1+1}^{4}$
2	$\overbrace{2}^{2}$	$\overbrace{2+2}^{4}$	$\overbrace{2+2+2}^{1}$	$\overbrace{2+2+2+2}^{3}$
3	$\overbrace{3}^{3}$	$\overbrace{3+3}^{1}$	$\overbrace{3+3+3}^{4}$	$\overbrace{3+3+3+3}^{2}$
4	$\overbrace{4}^{4}$	$\overbrace{4+4}^{3}$	$\overbrace{4+4+4}^{2}$	$\overbrace{4+4+4+4}^{1}$

◆

Im Beweis des Satzes 3.7 haben wir implizit den kleinen Fermat'schen Satz bewiesen.

<u>Satz 3.8</u> (kleiner Satz von Fermat)
Seien $(G,\circ,e)$ eine endliche Gruppe und $a \in G$. Dann gilt $a^{\operatorname{ord} G} = e$.

Beweis:

Übung

Satz 3.9

Jede endliche Gruppe $(G, \circ, e)$ mit $\operatorname{ord} G$ ist eine Primzahl ist zyklisch.

Beweis:

Sei $\operatorname{ord} G = p \geq 2$. Betrachte $a \in G \setminus \{e\}$ beliebig. Dann gilt

H_a ist eine zyklische Untergruppe von G.

Satz von Lagrange $\Rightarrow$

$\operatorname{ord} H_a \mid \operatorname{ord} G = p$

p Primzahl $\Rightarrow$ $\operatorname{ord} H_a = 1$ oder $\operatorname{ord} H_a = p$.

$a \neq e \Rightarrow \operatorname{ord} H_a > 1$

Also gilt $\operatorname{ord} H_a = p$.

Wegen $H_a \subseteq G$ und $|H_a| = |G|$ folgt

$H_a = G$

3.2 Homomorphe Abbildungen

Seien zwei algebraische Strukturen $(G, \circ)$ und $(H, *)$ gegeben.

Frage: Was haben diese Strukturen gemeinsam?

Dies bedeutet, dass man die strukturellen Eigenschaften der Verknüpfungen $\circ$ und $*$ miteinander vergleichen will.

Eine Abbildung $f: G \to H$ heißt homomorph - oder ein Homomorphismus -, wenn für alle $x, y \in G$ gilt:

$$f(x \circ y) = f(x) * f(y).$$

Falls ein Homomorphismus auch bijektiv ist, dann heißt dieser Isomorphismus. Existiert für zwei Strukturen $(G, \circ)$ und $(H, *)$ ein Isomorphismus, dann sind diese Strukturen isomorph. Dies bedeutet dann, dass diese Strukturen bis auf Umbenennung der Elemente gleich sind.

Ein Homomorphismus $f: G \to G$ von G in sich selbst heißt Endomorphismus. Ein Endomorphismus, der auch ein Isomorphismus ist, heißt Automorphismus.

Beispiel 3.5

Die Abbildung $f: (\mathbb{R}\times\mathbb{R}, +) \to (\mathbb{R}, +)$ mit $f(x_1, x_2) = 2x_1 + x_2$ ist ein Homomorphismus, da $\forall\, (x_1, x_2), (y_1, y_2) \in \mathbb{R}\times\mathbb{R}$ gilt:

$$\begin{aligned} f((x_1, x_2) + (y_1, y_2)) &= f(x_1 + y_1, x_2 + y_2) \\ &= 2(x_1 + y_1) + (x_2 + y_2) \\ &= (2x_1 + x_2) + (2y_1 + y_2) \\ &= f(x_1, x_2) + f(y_1, y_2) \end{aligned}$$

Die Abbildung f ist aber kein Isomorphismus, da diese nicht injektiv ist. Es gilt z.B.

$$f(1, -2) = 0 = f(0, 0).$$

Satz 3.10

Seien $(G, \circ, e_G)$, $(H, *, e_H)$ Gruppen und $f: G \to H$ ein Homomorphismus. Dann gilt

a) $f(e_G) = e_H$.

b) $\forall\, x \in G$ gilt: $f(x^{-1}) = (f(x))^{-1}$

Beweis:

a) Kürzungsregeln $\Rightarrow$
In einer Gruppe ist das neutrale Element das einzige Element x mit $x = x \circ x$.

$\Rightarrow$

$$f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$$

impliziert $f(e_G) = e_H$.

b) Sei nun $x \in G$. Es gilt

$$e_H = f(e_G) = f(x \circ x^{-1}) = f(x) * f(x^{-1})$$

Also ist $f(x^{-1})$ das Inverse $(f(x))^{-1}$ zu $f(x)$, womit b) bewiesen ist.

■

Der Satz von Cayley charakterisiert exakt, wann zwei zyklische Gruppen isomorph sind.

Satz 3.11 (Satz von Cayley)

Zwei zyklische Gruppen sind genau dann isomorph, wenn sie dieselbe Ordnung haben.

Beweis:

„$\Rightarrow$"

Eine Abbildung von einer endlichen Menge in eine andere kann nur dann bijektiv sein, wenn beide Mengen dieselbe Anzahl von Elementen haben.

„$\Leftarrow$"

Seien $(G, \circ)$ und $(H, *)$ zwei zyklische Gruppen mit erzeugenden Elementen $g \in G$

und $h \in H$. Ferner sei $\operatorname{ord} G = \operatorname{ord} H$.

Betrachte die Abbildung

$$f: G \to H, \text{ wobei}$$

$$f(g^k) := h^k \quad \text{für} \quad k = 0, 1, 2, \ldots$$

Übung:

Beweisen Sie, dass die Abbildung f bijektiv ist.

Für alle $x, y \in G$ existieren $i, j \in \mathbb{N}$ mit

$$x = g^i \quad \text{und} \quad y = g^j.$$

Es gilt:

$$\begin{aligned} f(x \circ y) &= f(g^i \circ g^j) \\ &= f(g^{i+j}) \\ &= h^{i+j} \\ &= h^i * h^j \\ &= f(g^i) * f(g^j) \\ &= f(x) * f(y), \end{aligned}$$

womit der Satz bewiesen ist. ∎

Da für jede natürliche Zahl m $(\mathbb{Z}_m, +, 0)$ eine zyklische Gruppe mit erzeugendem Element 1 ist, gilt:

Korollar 3.1

Bis auf Isomorphie sind $(\mathbb{Z}_m, +, 0)$ die einzigen

3.3 Ringe und Körper

Bisher haben wir nur algebraische Strukturen mit einer Verknüpfung wie z.B. "Multiplikation" oder "Addition" betrachtet. Uns interessieren selbstverständlich auch Strukturen, in denen man sowohl addieren / subtrahieren als auch multiplizieren / dividieren kann.

Eine Struktur $(R, +, \cdot, 0, 1)$ heißt <u>Ring</u>, falls die folgenden drei Eigenschaften erfüllt sind:

1) $(R, +, 0)$ ist eine kommutative Gruppe.
2) $(R \setminus \{0\}, \cdot, 1)$ ist ein Monoid.
3) Es gelten die <u>Distributivgesetze</u>. D.h., $\forall\, x, y, z \in R$ gilt

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

und

$$(x + y) \cdot z = (x \cdot z) + (y \cdot z).$$

<u>Beispiel 3.6</u>

$(\mathbb{Z}, +, \cdot, 0, 1)$ und auch $(\mathbb{Z}_m, +, \cdot, 0, 1)$, $m \geq 2$ sind Ringe.

◊

In Ringen kann man somit addieren, subtrahieren und multiplizieren. Nur dividieren kann man nicht ohne weiteres. Dies kann man auch in

sogenannten Körpern.

Eine Struktur $(\mathbb{F}, +, \cdot, 0, 1)$ heißt <u>Körper</u>, falls folgendes gilt:

1) $(\mathbb{F}, +, 0)$ und $(\mathbb{F}\setminus\{0\}, \cdot, 1)$ sind kommutative Gruppen.
2) Es gelten die Distributivgesetze.

Jeder Körper $\mathbb{F}$ besitzt somit zwei neutrale Elemente 0 und 1. Zudem besitzt jedes Element $x \in \mathbb{F}\setminus\{0\}$ zwei Inverse; das additive Inverse $-x$ und das multiplikative Inverse x^{-1}.

<u>Satz 3.12</u> (Körpereigenschaften)

Sei $(\mathbb{F}, +, \cdot, 0, 1)$ ein Körper. Dann gilt $\forall x, y \in \mathbb{F}$:

a) $0 \cdot x = 0$
b) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$
c) $(-x)^{-1} = -x^{-1}$ für $x \neq 0$
d) $x \cdot y = 0 \Rightarrow x = 0$ oder $y = 0$.

<u>Beweis</u>:

a) Es gilt

$$0 \cdot x = (0+0)x = 0x + 0x$$

Da in einer Gruppe $(\mathbb{F}, +, 0)$ das neutrale Element 0 das einzige Element x mit

$x + x = x$ ist, folgt somit $0 \cdot x = 0$.

b) Es gilt:

$$(-x) \cdot y + x \cdot y \underset{DG}{=} (-x + x)\, y$$
$$= 0 \cdot y$$
$$\underset{a)}{=} 0$$

$\Rightarrow$

$(-x) \cdot y$ ist das additive Inverse $-(x \cdot y)$ von $x \cdot y$.

Genauso zeigt man, dass $x \cdot (-y)$ das additive Inverse $-(x \cdot y)$ von $x \cdot y$ ist.

c) Es gilt:

$$(-x^{-1}) \cdot (-x) = x^{-1} \cdot (-(-x))$$
$$\underset{b)}{=} x^{-1} \cdot x$$
$$\underset{S.3.1}{=} 1$$

$\Rightarrow$

$-x^{-1}$ ist das multiplikative Inverse $(-x)^{-1}$ von $-x$.

d) Annahme: $x \cdot y = 0$ und $x \neq 0$

$\Rightarrow$

$$0 \underset{a)}{=} x^{-1} \cdot x \cdot y \underset{AG}{=} (x^{-1} \cdot x)\, y = y$$

Die bekanntesten Körper sind
- der Körper $\mathbb{Q}$ der rationalen Zahlen und
- der Körper $\mathbb{R}$ der reellen Zahlen.

Beide Körper enthalten unendlich viele Elemente.

Frage:
Gibt es Körper, die nur endlich viele Elemente enthalten?

Satz 3.13
Sei p eine Primzahl. Dann ist $(\mathbb{Z}_p, +, \cdot, 0, 1)$ ein Körper.

Beweis: Übung ∎

Somit gibt es für jede Primzahl p einen Körper, der genau p Elemente enthält.

4. Einführung in die Logik

Wir haben uns zu Beginn der Vorlesung informell mit Aussagen und einige Dinge, die man mit solchen tun kann, beschäftigt. Dies war notwendig damit wir die Grundlagen legen und erste Beweise führen konnten. Wir hatten nicht definiert, was wir genau unter einer Aussage verstehen sondern uns auf unsere Intuition verlassen.

Eine Aussage ist ein sprachliches Gebilde, für das genau einer der Wahrheitswerte wahr oder falsch zutrifft. Gemäß dieser Definition gelten für Aussagen folgende grundlegende Prinzipien:

Prinzip der Zweiwertigkeit:
Jede Aussage ist wahr oder falsch.

Prinzip vom ausgeschlossenen Widerspruch:
Es gibt keine Aussage, die sowohl wahr als auch falsch ist.

Beispiel 4.1

"Die Sonne kreist um die Erde."
"Fünf ist eine Primzahl."
"Es gibt unendlich viele Primzahlzwillinge"

(Primzahlen, deren Differenz 2 ist)

sind Aussagen. Die erste ist falsch, die zweite ist wahr und der Wahrheitswert der dritten Aussage ist unbekannt.

"Heute ist schönes Wetter."
"x ist eine Primzahl."

sind keine Aussagen. Aufgrund des subjektiven Begriffes "schön" kann der Wahrheitswert des ersten Satzes nicht angegeben werden. Der Wahrheitswert des zweiten Satzes hängt von dem

Wert ab, den x annimmt.

Folgender Satz ist weder wahr noch falsch und somit keine Aussage.

"Dieser Satz ist falsch."

Angenommen, der Satz wäre wahr, dann müsste er falsch sein. Wenn wir davon ausgehen, dass der Satz falsch ist, dann müsste er wahr sein. (Paradoxon von Bertrand Russell).

Setzen wir mehrere Aussagen zu einer Aussage zusammen, dann hängt der Wahrheitswert der zusammengesetzten Aussage nur von den Wahrheitswerten der einzelnen Aussagen und nicht von etwaigen Sinnzusammenhängen der Zusammensetzung ab.

Beispiel 4.2

"Wenn es eine ganze Zahl y mit $x = y + 1$ für alle ganze Zahlen x gibt, dann gilt $w = z$ für alle ganze Zahlen w und z."

Wie wir bereits wissen, ist obige Aussage wahr, auch wenn diese trivial ist und völlig unsinnig aussieht.

Ziel:

Untersuchung, wie sich der Wahrheitswert von zusammengesetzten Aussagen aus den Wahrheitswerten der einzelnen Aussagen ergibt.

Zunächst werden wir uns in der sogenannten Aussagenlogik mit Aussagen, die sich aus elementaren Aussagen mit Hilfe der einfachen logischen Operationen "und", "oder" und "nicht" zusammensetzen lassen, beschäftigen. In der Aussagenlogik können eine Vielzahl von interessanten Aussagen nicht formuliert werden. Hierzu benötigt man zusätzlich sogenannte Prädikate und Quantoren. Fügt man diese zu den Operationen der Aussagenlogik hinzu, dann erhält man die sogenannte Prädikatenlogik. Mit dieser werden wir uns im Anschluss an die Aussagenlogik beschäftigen.

4.1 Die Aussagenlogik

4.1.1 Aussagenlogische Ausdrücke

Zunächst werden wir definieren, was wir unter einem aussagenlogischen Ausdruck verstehen.

Sei $X := \{x_1, x_2, \dots\}$ eine abzählbar unendliche Menge von Boole'schen Variablen. Dies sind Variablen, die die beiden Werte wahr und falsch annehmen können. Wir kombinieren Boole'sche Variablen

unter Verwendung der Boole'schen Operationen $\wedge$ (logisches und), $\vee$ (logisches oder) und $\neg$ (logisches nicht).

Ein aussagenlogischer Ausdruck ist

i) eine Boole'sche Variable $x_i \in X$ oder
ii) ein Ausdruck der Form $\neg \phi_1$, wobei ϕ_1 ein Boole'scher Ausdruck ist, oder
iii) ein Ausdruck der Form $(\phi_1 \wedge \phi_2)$, wobei ϕ_1 und ϕ_2 Boole'sche Ausdrücke sind, oder
iv) ein Ausdruck der Form $(\phi_1 \vee \phi_2)$, wobei ϕ_1 und ϕ_2 Boole'sche Ausdrücke sind.

Dies sind alle aussagenlogische Ausdrücke.

$\neg \phi_1$ heißt Negation von ϕ_1. Der Ausdruck $(\phi_1 \wedge \phi_2)$ ist die Konjunktion von ϕ_1 und ϕ_2. $(\phi_1 \vee \phi_2)$ ist die Disjunktion von ϕ_1 und ϕ_2. Ein Ausdruck der Form x_i oder $\neg x_i$ heißt Literal.

Was wir definiert haben ist die Syntax von aussagenlogischen Ausdrücken. Was einem Ausdruck Leben gibt ist seine Semantik. Die Semantik von aussagelogischen Ausdrücken ist relativ einfach. In Abhängigkeit der Wahrheitswerte der enthaltenen Variablen kann ein Ausdruck wahr oder falsch sein.

Wir haben aussagenlogische Ausdrücke induktiv definiert. Beginnend mit Variablen setzen wir diese unter Verwendung von Boole'schen Operationen zu komplizierteren Ausdrücken zusammen. Demzufolge werden unsere Definitionen von Eigenschaften von aussagelogischen Ausdrücken denselben induktiven Pfad der ursprünglichen Definition folgen. Auch werden wir bei unseren Beweisen <u>Induktion über die Struktur der Ausdrücke</u> verwenden.

Eine <u>Belegung</u> $\mathcal{B}$ ist eine Abbildung

$$\mathcal{B} : X' \longrightarrow \{\text{wahr}, \text{falsch}\},$$

die einer endlichen Menge $X' \subset X$ von Variablen jeweils einen Wahrheitswert zuordnet.

Sei ϕ ein aussagelogischer Ausdruck. Dann definieren wir wir wie folgt die Menge $X(\phi)$ von Boole'schen Variablen, die in ϕ vorkommt:

i) Falls $\phi = x_i \in X$, dann ist $X(\phi) := \{x_i\}$.
ii) Falls $\phi = \neg \phi_1$, dann $X(\phi) := X(\phi_1)$.
iii) Falls $\phi = (\phi_1 \wedge \phi_2)$ oder $\phi = (\phi_1 \vee \phi_2)$, dann $X(\phi) := X(\phi_1) \cup X(\phi_2)$.

Sei $\mathcal{B} : X' \to \{\text{wahr}, \text{falsch}\}$ eine Belegung mit $X(\phi) \subseteq X'$. Dann heißt $\mathcal{B}$ <u>geeignet für</u> ϕ. Wir definieren nun induktiv, wann eine für ϕ geeignete Belegung $\mathcal{B}$ den Ausdruck ϕ <u>erfüllt</u>.

Wir schreiben dann $\mathcal{B} \models \phi$. Falls $\mathcal{B}$ den Ausdruck ϕ nicht erfüllt, dann schreiben wir $\mathcal{B} \not\models \phi$.

i) Falls $\phi = x_i \in X'$, dann

$\mathcal{B} \models \phi$, falls $\mathcal{B}(x_i) =$ wahr.

ii) Falls $\phi = \neg \phi_1$, dann

$\mathcal{B} \models \phi$, falls $\mathcal{B} \not\models \phi_1$.

iii) Falls $\phi = (\phi_1 \wedge \phi_2)$, dann

$\mathcal{B} \models \phi$, falls sowohl $\mathcal{B} \models \phi_1$, als auch $\mathcal{B} \models \phi_2$.

iv) Falls $\phi = (\phi_1 \vee \phi_2)$, dann

$\mathcal{B} \models \phi$, falls $\mathcal{B} \models \phi_1$ oder $\mathcal{B} \models \phi_2$.

Beispiel 4.3

Betrachte $\phi := ((\neg x_1 \vee x_2) \wedge x_3)$ und die geeignete Belegung $\mathcal{B}$ mit

$\mathcal{B}(x_1) = \mathcal{B}(x_3) =$ wahr und $\mathcal{B}(x_2) =$ falsch.

Frage: Erfüllt $\mathcal{B}$ den Ausdruck ϕ?

Es gilt:

$\mathcal{B} \models x_1 \Rightarrow \mathcal{B} \not\models \neg x_1$ und $\mathcal{B} \not\models x_2$

$\Rightarrow \mathcal{B} \not\models (\neg x_1 \vee x_2) \Rightarrow \mathcal{B} \not\models \phi$

Wir verwenden zwei weitere Boole'sche Operationen:

$(\phi_1 \to \phi_2)$ für $(\neg\phi_1 \vee \phi_2)$

$(\phi_1 \leftrightarrow \phi_2)$ für $(\phi_1 \to \phi_2) \wedge (\phi_2 \to \phi_1)$

Zwei Ausdrücke ϕ_1 und ϕ_2 heißen äquivalent, falls für jede Belegung $\mathcal{B}$ mit $\mathcal{B}$ ist für ϕ_1 und für ϕ_2 geeignet, gilt:

$$\mathcal{B} \models \phi_1 \iff \mathcal{B} \models \phi_2.$$

Wir schreiben dann $\phi_1 \equiv \phi_2$.

Übung:
Beweisen Sie, dass die Relation $\equiv$ eine Äquivalenzrelation ist.

Lemma 4.1
Seien ϕ_1, ϕ_2 und ϕ_3 beliebige aussagenlogische Ausdrücke. Dann gilt

Idempotenz: $(\phi_1 \vee \phi_1) \equiv \phi_1$
$(\phi_1 \wedge \phi_1) \equiv \phi_1$

Kommutativität: $(\phi_1 \vee \phi_2) \equiv (\phi_2 \vee \phi_1)$
$(\phi_1 \wedge \phi_2) \equiv (\phi_2 \wedge \phi_1)$
$(\phi_1 \leftrightarrow \phi_2) \equiv (\phi_2 \leftrightarrow \phi_1)$

Assoziativität: $((\phi_1 \vee \phi_2) \vee \phi_3) \equiv (\phi_1 \vee (\phi_2 \vee \phi_3))$
$((\phi_1 \wedge \phi_2) \wedge \phi_3) \equiv (\phi_1 \wedge (\phi_2 \wedge \phi_3))$

Absorbtion: $(\phi_1 \vee (\phi_1 \wedge \phi_2)) \equiv \phi_1$
$(\phi_1 \wedge (\phi_1 \vee \phi_2)) \equiv \phi_1$

Distributivität: $(\phi_1 \wedge (\phi_2 \vee \phi_3)) \equiv ((\phi_1 \wedge \phi_2) \vee (\phi_1 \wedge \phi_3))$
$(\phi_1 \vee (\phi_2 \wedge \phi_3)) \equiv ((\phi_1 \vee \phi_2) \wedge (\phi_1 \vee \phi_3))$

Doppelte Negation: $\neg\neg\phi_1 \equiv \phi_1$

DeMorgan $\neg(\phi_1 \vee \phi_2) \equiv (\neg\phi_1 \wedge \neg\phi_2)$
$\neg(\phi_1 \wedge \phi_2) \equiv (\neg\phi_1 \vee \neg\phi_2)$

Beweis: Übung ■

Lemma 4.1 ermöglicht uns die Vereinfachung der Notation zur Repräsentation von aussagelogischen Ausdrücken. So vermeiden wir Klammern, wenn diese binäre Operationen ($\wedge$ oder $\vee$) derselben Art separieren.

Beispiel 4.4

Anstatt
$$(((x_1 \vee \neg x_3) \vee x_2) \vee (x_4 \vee (x_2 \vee x_5)))$$
schreiben wir
$$(x_1 \vee \neg x_3 \vee x_2 \vee x_4 \vee x_2 \vee x_5)$$

◊

Dies bedeutet, dass wir "lange" Disjunktionen und Konjunktionen erlauben. Mittels Verwendung der Kommunität und Idempotenz können

wir dafür sorgen, dass lange Disjunktionen und lange Konjunktionen nur verschiedene Ausdrücke enthalten.

Beispiel 4.4 (Fortführung)

Anstatt

$$(x_1 \vee \neg x_3 \vee x_2 \vee x_4 \vee x_2 \vee x_5)$$

schreiben wir

$$(x_1 \vee \neg x_3 \vee x_2 \vee x_4 \vee x_5).$$

◆

Des Weiteren verwenden wir folgende Schreibweisen:

$\bigwedge_{i=1}^{n} \phi_i$ steht für $(\phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_n)$.

$\bigvee_{i=1}^{n} \phi_i$ steht für $(\phi_1 \vee \phi_2 \vee \dots \vee \phi_n)$.

Als nächstes werden wir zeigen, dass jeder aussagelogischer Ausdruck ϕ in einen äquivalenten Ausdruck, der eine spezielle Form hat, transformiert werden kann.

Ein aussagelogischer Ausdruck ϕ ist in konjunktiver Normalform (KNF), falls

$$\phi = \bigwedge_{i=1}^{n} C_i,$$

wobei $n \geq 1$ und jedes C_i ist die Disjunktion von einem oder mehreren Literalen.

Φ ist in <u>disjunktiver Normalform</u> (DNF), falls

$$\Phi = \bigvee_{i=1}^{n} D_i ,$$

wobei $n \geq 1$ und jedes D_j ist die Konjunktion von einem oder mehreren Literalen. Die D_j's heißen <u>Implikanten</u> des Ausdruckes in DNF.

<u>Satz 4.1</u>

Jeder aussagenlogischer Ausdruck Φ ist äquivalent zu einem Ausdruck in KNF und zu einem Ausdruck in DNF.

<u>Beweis:</u>

Wir beweisen den Satz mittels Induktion über die Struktur von Φ.

<u>$\Phi = x_j \in X$:</u>

Φ ist eine einzelne Variable. Dann folgt aus der Definition von KNF und von DNF, dass Φ sowohl in KNF als auch in DNF bereits ist.

<u>Annahme:</u>

Φ_1 und Φ_2 sind aussagelogische Ausdrücke, zu den äquivalente Ausdrücke Φ_1' und Φ_2' in KNF sowie äquivalente Ausdrücke Φ_1'' und Φ_2'' in DNF existieren

Wir beweisen nun nacheinander, dass dann auch äquivalente Ausdrücke in KNF bzw DNF für

$\neg \phi_1$, $\phi_1 \vee \phi_2$ und $\phi_1 \wedge \phi_2$ existieren.

$\underline{\phi = \neg \phi_1}$:

Seien

$$\phi_1' := \bigwedge_{i=1}^{n} C_i \quad \text{und} \quad \phi_1'' := \bigvee_{i=1}^{m} D_i.$$

Dann gilt:

$$\neg \phi_1 \equiv \neg \phi_1' = \neg \left(\bigwedge_{i=1}^{n} C_i \right)$$

$$\underset{\text{DeM.}}{=} \bigvee_{i=1}^{n} \neg C_i$$

$$\underset{\text{DeM}}{=} \bigvee_{i=1}^{n} \tilde{D}_i,$$

wobei $\tilde{D}_i$ mittels Anwendung von DeMorgan auf $\neg C_i$ entsteht.

$\Rightarrow$

$\tilde{D}_i$ ist die Konjunktion der negierten Literalen in C_i.

$\Rightarrow \bigvee_{i=1}^{n} \tilde{D}_i$ ist in DNF.

Analog konstruiert man aus $\neg \phi''$ einen zu $\neg \phi_1$ äquivalenten Ausdruck in KNF.
Übung.

$\underline{\phi = (\phi_1 \vee \phi_2)}$:

Da $\phi_1'' \vee \phi_2''$ bereits in DNF ist, ist die Konstruktion des zu ϕ äquivalenten Ausdrucks

in DNF trivial.

Für die Konstruktion des zu Φ äquivalenten Ausdrucks in KNF betrachten wir $(\Phi_1' \vee \Phi_2')$.

Seien

$$\Phi_1' := \left(\bigwedge_{i=1}^{n} C_{1i}\right) \text{ und } \Phi_2' := \left(\bigwedge_{j=1}^{m} C_{2j}\right)$$

Dann gilt

$$(\Phi_1' \vee \Phi_2') = \left(\bigwedge_{i=1}^{n} C_{1i} \vee \bigwedge_{j=1}^{m} C_{2j}\right)$$

$$\overset{\text{Dis}}{=} \left(\bigwedge_{j=1}^{m} \left(\left(\bigwedge_{i=1}^{n} C_{1i}\right) \vee C_{2j}\right)\right)$$

$$\overset{\text{Dis}}{=} \left(\bigwedge_{j=1}^{m} \left(\bigwedge_{i=1}^{n} (C_{1i} \vee C_{2j})\right)\right)$$

$$= \bigwedge_{j=1}^{m} \bigwedge_{i=1}^{n} (C_{1i} \vee C_{2j})$$

↑ KNF ✓

$\underline{\Phi = (\Phi_1 \wedge \Phi_2)}$: analog (Übung)

■

Übung:

Vervollständigen Sie den Beweis von Satz 4.1.

4.1.2 Erfüllbarkeit und Gültigkeit

Ein aussagelogischer Ausdruck ϕ heißt erfüllbar, falls eine für ϕ geeignete Belegung $\mathcal{B}$ mit $\mathcal{B} \models \phi$ existiert. Andernfalls heißt ϕ nicht erfüllbar oder unerfüllbar. Ein Ausdruck ϕ heißt gültig oder eine Tautologie, falls $\mathcal{B} \models \phi$ für alle für ϕ geeignete Belegungen $\mathcal{B}$. Wir schreiben dann auch $\models \phi$. Falls ein Ausdruck ϕ unerfüllbar ist, dann gilt $\mathcal{B} \not\models \phi$ und somit $\mathcal{B} \models \neg\phi$ für alle für ϕ geeignete Belegungen $\mathcal{B}$. Also gilt

Lemma 4.2
Ein aussagelogischer Ausdruck ϕ ist genau dann unerfüllbar, wenn seine Negation $\neg\phi$ gültig ist.

Sei ϕ ein aussagelogischer Ausdruck und

$$X_n := \{x_1, x_2, \ldots, x_n\}$$

die Menge der Variablen, von denen ϕ abhängt.

Frage:
Wie können wir testen, ob ϕ erfüllbar ist oder nicht?

Idee:
Bestimme für jede Belegung von X_n den Wahrheitswert, den diese Belegung für Φ induziert.

Jede Variable $x_i \in X_n$ kann den Wert wahr oder den Wert falsch annehmen.
$\Rightarrow$
Es existieren 2^n verschiedene Belegungen von X_n.

Insbesondere, wenn Φ unerfüllbar ist, würde jede der 2^n Belegungen überprüft werden.
$\Rightarrow$
Bereits für relativ kleine n verbietet sich diese Vorgehensweise.

Ziel:
Entwicklung einer Methode, die in der Praxis "häufig schneller" feststellt, dass ein gegebener Ausdruck Φ nicht erfüllbar ist.

Zunächst benötigen wir einige Bezeichnungen.

Eine Klausel K ist eine endliche, möglicherweise leere Menge von Literalen. Jede Disjunktion C von Literalen korrespondiert zur Klausel

$$K_C := \{ y \mid y \text{ ist Literal in } C \}.$$

Umgekehrt korrespondiert jede nichtleere Klausel K zur folgenden Disjunktion C_K von Literalen:

$$C_K := \bigvee_{y \in K} y.$$

Wir schreiben $\square$ für die leere Klausel, die zu keinem Ausdruck korrespondiert.

Jede endliche nichtleere Menge $\mathcal{K} := \{K_1, K_2, \dots, K_s\}$ von Klauseln mit $\square \notin \mathcal{K}$ korrespondiert zum folgenden Ausdruck $\Phi_{\mathcal{K}}$ in konjunktiver Normalform.

$$\Phi_{\mathcal{K}} := \bigwedge_{i=1}^{s} C_{K_i}.$$

$\mathcal{K}$ heißt auch eine Klauselmenge.

Zu einem Ausdruck

$$\Phi = \bigwedge_{i=1}^{t} C_i$$

korrespondiert die Klauselmenge

$$\mathcal{K}_\Phi := \{K_{C_1}, K_{C_2}, \dots, K_{C_t}\}.$$

Seien K_1, K_2 und D Klauseln. Die Klausel D heißt genau dann Resolvente von K_1 und K_2, wenn es ein Literal y gibt mit

i) $y \in K_1$, $\neg y \in K_2$ und
ii) $D = (K_1 \setminus \{y\}) \cup (K_2 \setminus \{\neg y\})$.

Wir sagen, zwei Klauselmengen $\mathcal{K}_1$ und $\mathcal{K}_2$ sind äquivalent wenn die korrespondierenden Ausdrücke $\Phi_{\mathcal{K}_1}$ und $\Phi_{\mathcal{K}_2}$ äquivalent sind. Eine Klauselmenge $\mathcal{K}$ heißt genau dann erfüllbar, wenn $\Phi_{\mathcal{K}}$ erfüllbar ist.

Lemma 4.3 (Resolutionsregel)

Seien $\mathcal{K}$ eine Klauselmenge, $K_1, K_2 \in \mathcal{K}$ und D eine Resolvente von K_1 und K_2. Dann sind $\mathcal{K}$ und $\mathcal{K}' := \mathcal{K} \cup D$ äquivalent.

Beweis:

Sei $\mathcal{B}$ eine für $\Phi_{\mathcal{K}}$ geeignete Belegung. Offensichtlich gilt:

$$\mathcal{B} \models \Phi_{\mathcal{K}'} \Rightarrow \mathcal{B} \models \Phi_{\mathcal{K}}.$$

Annahme:

$$\mathcal{B} \models \Phi_{\mathcal{K}} \text{ und } D = (K_1 \setminus \{y\}) \cup (K_2 \setminus \{\neg y\})$$

zu zeigen: $\mathcal{B} \models \Phi_D$

Da $\mathcal{B}$ nicht gleichzeitig y und $\neg y$ erfüllen kann muss $\mathcal{B}$ mindestens ein Literal in $(K_1 \setminus \{y\}) \cup (K_2 \setminus \{\neg y\})$ erfüllen. Also gilt

$$\mathcal{B} \models \Phi_D.$$

∎

Die Resolutionsregel besagt, dass das Hinzufügen der Resolventen zweier Klauseln der betrachteten Klauselmenge zu einer äquivalenten Klauselmenge führt.

...

Übung:

Zeigen Sie, dass die Klauseln, mittels denen die Resolvente gebildet wurde, nicht aus der Klausel-

menge entfernt werden dürfen, da dann die resultierende Klauselmenge nicht mehr äquivalent zur ursprünglichen Klauselmenge sein muss.

Sei $\mathcal{K}$ eine Klauselmenge. Die Operation R ist dann definiert durch:

$$R(\mathcal{K}) := \mathcal{K} \cup \{D \mid D \text{ ist eine Resolvente in } \mathcal{K}\}.$$

D.h., R fügt zu $\mathcal{K}$ alle Resolventen von Klauseln aus $\mathcal{K}$ hinzu. Aus obiger Resolutionsregel folgt, dass $\mathcal{K}$ und $R(\mathcal{K})$ äquivalent sind.

Seien nun

$$R^0(\mathcal{K}) := \mathcal{K}$$
$$R^{i+1}(\mathcal{K}) := R(R^i(\mathcal{K})) \quad \text{für } i \geq 0$$
$$R^*(\mathcal{K}) := \bigcup_{i \geq 0} R^i(\mathcal{K}).$$

D.h., $R^*(\mathcal{K})$ ist der Abschluss von $\mathcal{K}$ unter der Operation R.

Bemerkung:
Falls $\mathcal{K}$ endlich ist, dann können von $\mathcal{K}$ ausgehend nur endlich viele unterschiedliche Klauseln konstruiert werden. Also existiert ein $n \geq 0$, so dass $R^{n+1}(\mathcal{K}) = R^n(\mathcal{K})$, womit $R^*(\mathcal{K}) = R^n(\mathcal{K})$.

Satz 4.2 (Resolutionssatz)

Eine Klauselmenge $\mathcal{K}$ ist genau dann unerfüllbar, wenn $\square \in R^*(\mathcal{K})$.

Beweis:

„$\Leftarrow$"

Annahme: $\square \in R^*(\mathcal{K})$

Wegen $\square \notin \mathcal{K}$ existiert ein $k \geq 1$ mit

i) $\square \notin R^{(k-1)}(\mathcal{K})$ und
ii) $\square \in R^k(\mathcal{K})$.

$\Rightarrow$ $\square$ ist Resolvente zweier Klauseln K_1 und K_2 aus $R^{(k-1)}(\mathcal{K})$.

$\Rightarrow$ $\exists$ Literal y mit

$K_1 = y$ und $K_2 = \neg y$

$\Rightarrow$

Der zu $R^{(k-1)}(\mathcal{K})$ korrespondierende Ausdruck ist nicht erfüllbar.

$\Rightarrow$ $\mathcal{K}$ ist unerfüllbar.

„$\Rightarrow$"

Annahme: $\mathcal{K}$ ist unerfüllbar.

Zu zeigen: $\square \in R^*(\mathcal{K})$.

Wir beweisen dies durch vollständige Induktion über die Anzahl n von unterschiedlichen Variablen in K.

$n = 1$:

Sei x_1 diejenige Variable, die in K vorkommt. Dann sind

$$K_1 := \{x_1\}, \quad K_2 := \{\neg x_1\}, \quad K_3 = \{x_1, \neg x_1\}$$

die einzigen möglichen nichtleeren Klauseln in K.

Da ϕ_K unerfüllbar, muss K die Klauseln K_1 und K_2 enthalten. Da $\square$ die Resolvente von K_1 und K_2 ist, enthält $R^*(K)$ die leere Klausel $\square$.

Annahme:

$n \geq 1$ und die Behauptung ist wahr für Klauselmengen, die n unterschiedliche Variablen enthalten.

$n \rightsquigarrow n+1$:

Sei K eine Menge von nichtleeren Klauseln, in denen die Variablen $x_1, x_2, \ldots, x_{n+1}$ vorkommen, so dass ϕ_K unerfüllbar ist.

Wir konstruieren zwei Klauselmengen K^+ und K^-, in denen x_{n+1} nicht vorkommt, durch:

Wir erhalten K^+ aus K, indem wir alle Klauseln, die das Literal x_{n+1} enthalten,

aus $\mathcal{K}$ entfernen und in jeder verbleibenden Klausel gegebenenfalls das Literal $\neg x_{n+1}$ streichen. D.h.,

$$\mathcal{K}^+ := \{ \mathcal{K} \setminus \{\neg x_{n+1}\} \mid K \in \mathcal{K},\ x_{n+1} \notin K \}.$$

Analog erhalten wir $\mathcal{K}^-$:

$$\mathcal{K}^- := \{ \mathcal{K} \setminus \{x_{n+1}\} \mid K \in \mathcal{K},\ \neg x_{n+1} \notin K \}.$$

Beh.: $\mathcal{K}^+$ und $\mathcal{K}^-$ sind unerfüllbar.

Bew. d. Beh.:

Annahme: $\Phi_{\mathcal{K}^+}$ ist erfüllbar.

Dann existiert eine Belegung $\mathcal{B}$ der Variablen $x_1, x_2, \dots, x_n$, die $\Phi_{\mathcal{K}^+}$ erfüllt. Wir erweitern die Belegung $\mathcal{B}$ zu einer Belegung $\mathcal{B}'$ der Variablen $x_1, x_2, \dots, x_n, x_{n+1}$, indem wir der Variablen x_{n+1} den Wert wahr zuweisen. Dann erfüllt $\mathcal{B}'$ jede Klausel, die wir aus $\mathcal{K}$ entfernt haben

$\Rightarrow$

$$\mathcal{B}' \models \Phi_{\mathcal{K}} \qquad \text{Widerspruch.}$$

Also war unsere Annahme falsch. D.h., $\Phi_{\mathcal{K}^+}$ ist unerfüllbar.

Genauso beweist man, dass $\Phi_{\mathcal{K}^-}$ unerfüllbar ist.

□

Induktionsvoraussetzung $\Rightarrow$

$\square \in R^*(\mathcal{K}^+)$ und $\square \in R^*(\mathcal{K}^-)$.

$\Rightarrow$

Es existiert eine Folge $C_1, C_2, \ldots, C_m$ von Klauseln, so dass

i) $C_m = \square$ und

ii) für $1 \leq i \leq m$ gilt $C_i \in \mathcal{K}^+$ oder es existieren $j, k < i$ mit C_i ist Resolvente von C_j und C_k.

Einige der Klauseln in obiger Folge können aus Klauseln in $\mathcal{K}$ durch Streichen von $\neg x_{n+1}$ entstanden sein.

Ist dies nicht der Fall, dann gilt:

$C_1, C_2, \ldots, C_m \in R^*(\mathcal{K})$,

also $\square \in R^*(\mathcal{K})$.

Andernfalls erhalten wir durch Wiedereinfügen der gestrichenen Literalen $\neg x_{n+1}$ eine Folge von Klauseln $C_1', C_2', \ldots, C_m'$, welche zeigt, dass

$\{\neg x_{n+1}\} \in R^*(\mathcal{K})$.

Analog impliziert $\square \in R^*(\mathcal{K}^-)$, dass

$\square \in R^*(\mathcal{K})$ oder $\{x_{n+1}\} \in R^*(\mathcal{K})$.

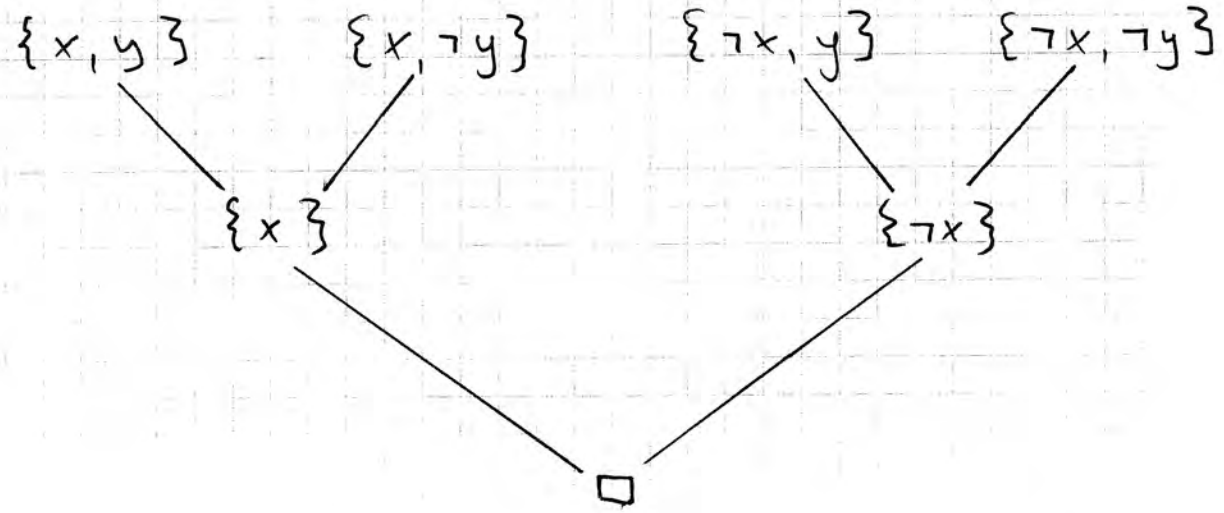
Obiger Algorithmus berechnet alle möglichen Resolventen.

Frage: Ist dies notwendig?

Beobachtung:
Jede Klausel in $R^{\mathcal{K}}(\exists \mathcal{K}_{\varphi'})$ hat einen "Stammbaum", der die Entstehung der Klausel widerspiegelt.

Beispiel 4.5

Betrachte $\mathcal{K} := \{\{x,y\}, \{x,\neg y\}, \{\neg x, y\}, \{\neg x, \neg y\}\}$
Folgender Baum zeigt die Unerfüllbarkeit von $\mathcal{K}$:



Die Klausel $\{y\}$, die Resolvente von $\{x,y\}, \{\neg x, y\}$ ist, wird nicht konstruiert.

■

Idee:
Anstatt alle möglichen Resolventen zu bilden genügt es, nur solche zu bilden, die zur Konstruktion der leeren Klausel benötigt werden.

Obige Idee legt folgende Definition nahe:

Eine <u>Deduktion</u> aus einer Klauselmenge $\mathcal{K}$ ist eine Folge $C_1, C_2, \ldots, C_m$ von Klauseln, so dass jeder C_i entweder eine Klausel in $\mathcal{K}$ oder eine Resolvente zweier Klauseln C_j und C_k für ein $j, k < i$ ist. Obige Deduktion ist dann eine Deduktion von C_m, der letzten Klausel in obiger Folge.

Der Resolutionssatz könnte wie folgt umformuliert werden:

Eine Menge von Klauseln ist genau dann unerfüllbar, wenn es eine Deduktion der leeren Klausel aus ihr gibt.

Diese Formulierung des Resolutionssatzes ist die Basis für viele Computerprogramme, die für aussagenlogischen Ausdrücke entscheiden, ob diese erfüllbar sind.

<u>Beispiel 4.6</u>:

Betrachte $\mathcal{K} := \{\{x, y, \neg z\}, \{\neg x\}, \{x, y, z\}, \{x, \neg y\}\}$
Eine mögliche Deduktion von $\square$ aus $\mathcal{K}$ ist die folgende:

$K_1 = \{x, y, \neg z\}$ (Klausel aus $\mathcal{K}$)
$K_2 = \{x, y, z\}$ (Klausel aus $\mathcal{K}$)

Da $\square$ Resolvente der Klauseln $\{x_{n+1}\}, \{\neg x_{n+1}\}$ ist, impliziert $\{x_{n+1}\}, \{\neg x_{n+1}\} \in R^*(\mathcal{K})$ auch

$$\square \in R^*(\mathcal{K}).$$

■

Der Resolutionssatz kann nun verwendet werden um die Erfüllbarkeit einer aussagenlogischen Ausdruckes zu testen. Dies leistet folgender Algorithmus:

Algorithmus RESOLUTION

Eingabe: aussagenlogischer Ausdruck ϕ

Ausgabe: { erfüllbar falls ϕ erfüllbar
{ unerfüllbar sonst.

Methode:

(1) Transformiere ϕ in einen Ausdruck ϕ' in KNF.

(2) Bilde die zu ϕ' korrespondierende Klauselmenge $\mathcal{K}_{\phi'}$.

(3) Konstruiere die Folge

$$R(\mathcal{K}_{\phi'}), R^2(\mathcal{K}_{\phi'}), \ldots$$

bis $R^k(\mathcal{K}_{\phi'}) = R^{k+1}(\mathcal{K}_{\phi'})$ für ein k.

(4) Falls $\square \in R^k(\mathcal{K}_{\phi'})$, dann

Ausgabe := unerfüllbar.

Andernfalls

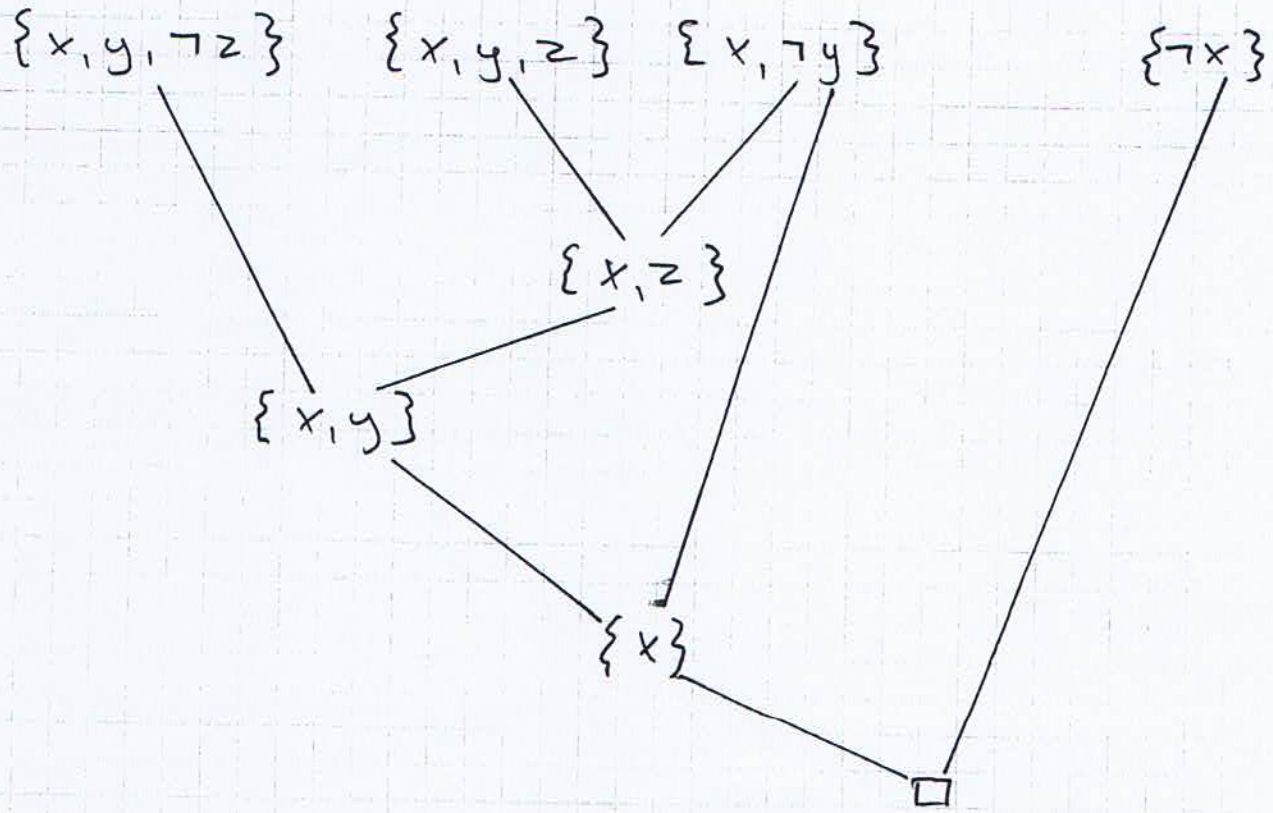
Ausgabe := erfüllbar.

$K_3 = \{x, \neg y\}$ (Klausel aus $\mathcal{K}$)
$K_4 = \{x, z\}$ (Resolvente von K_2, K_3)
$K_5 = \{x, y\}$ (Resolvente von K_1, K_4)
$K_6 = \{x\}$ (Resolvente von K_3, K_5)
$K_7 = \{\neg x\}$ (Klausel aus $\mathcal{K}$)
$K_8 = \square$ (Resolvente von K_6, K_7)

In obiger Deduktion wird die Klausel $\{x, \neg y\}$ zweimal verwendet. Es gibt eine kürzere Möglichkeit, aus $\mathcal{K}$ die leere Klausel $\square$ herzuleiten.

Übung:
Geben Sie eine kürzere Deduktion von $\square$ aus $\mathcal{K}$ an.

Folgender Graph veranschaulicht obige Deduktion:



4.2 Die Prädikatenlogik

In der Aussagenlogik können ausschließlich Aussagen, die aus Booleschen Variablen und den aussagelogischen Verknüpfungen $\wedge, \vee, \neg$ bestehen, gebildet werden. Aussagen der Form

"Es gibt eine ganze Zahl x, die eine Primzahl ist."

oder

"Alle ganze Zahlen sind Primzahlen"

sind in der Aussagelogik nicht möglich.

Ziel:
Entwicklung einer Logik, in der auch komplexere mathematische Sachverhalte ausdrückbar sind.

Diese Logik heißt Prädikatenlogik oder auch Logik erster Stufe.

4.2.1 Die Syntax der Prädikatenlogik

Ein Vokabular (oder auch Signatur genannt) $\Sigma := (\Phi, \Pi, \tau)$ besteht aus

- einer abzählbaren Menge Φ von Funktionssymbolen,
- einer abzählbaren Menge Π von Relationssymbolen und

- einer Abbildung $r : \Phi \cup \Pi \to \mathbb{N}_0$, der sogenannten Stelligkeitsfunktion.

Dabei sind Φ und Π disjunkt. r ordnet jedem Symbol aus $\Phi \cup \Pi$ seine Stelligkeit zu. $f \in \Phi$ mit $r(f) = k$ heißt k-stelliges Funktionssymbol und $R \in \Pi$ mit $r(R) = k$ heißt k-stelliges Relationssymbol. Nullstellige Funktionssymbole heißen Konstanten. Relationssymbole sind niemals nullstellig. Bei uns wird Π stets die binäre Gleichheitsrelation $=$ enthalten.

$V := \{x, y, z, \ldots\}$ bezeichnet eine feste, aufzählbare Menge von Variablen, die Werte aus dem zugrundeliegenden Universum annehmen können.

Wir definieren induktiv Terme über dem Vokabular Σ durch:

i) Jede Variable in V ist ein Term.
ii) Falls $f \in \Phi$ ein k-stelliges Funktionssymbol und $t_1, t_2, \ldots, t_k$ Terme sind, dann ist $f(t_1, t_2, \ldots, t_k)$ ein Term.

Bemerkung
Gemäß obiger Definition ist eine Konstante c ein Term. Wenn $k = 0$ und lasse in $c()$ die Klammern weg.

Ziel:
Definition von Ausdrücke über dem Vokabular Σ.

Seien $R \in \Pi$ ein k-stelliges Relationssymbol und $t_1, t_2, \ldots, t_k$ Terme. Dann ist $R(t_1, t_2, \ldots, t_k)$ ein atomarer Ausdruck. Wir definieren nun prädikatenlogische Ausdrücke induktiv durch:

i) Jeder atomarer Ausdruck ist ein prädikatenlogischer Ausdruck.
ii) Seien ϕ und ψ prädikatenlogische Ausdrücke. Dann sind $\neg\phi$, $(\phi \vee \psi)$ und $(\phi \wedge \psi)$ prädikatenlogische Ausdrücke.
iii) Seien ϕ ein prädikatenlogisches Ausdruck, $x \in V$ eine Variable und $\forall$ ein Zeichen mit der Bedeutung "für alle". Dann ist $(\forall x \phi)$ ein prädikatenlogisches Ausdruck.
iv) Dies sind alle prädikatenlogische Ausdrücke.

Schreibweisen:

- Genauso wie in der Aussagenlogik verwenden wir auch in der Prädikatenlogik die Schreibweisen $\rightarrow$ und $\leftrightarrow$
- Wir schreiben $(\exists x \phi)$ für $\neg(\forall x \neg\phi)$.
  Die Symbole $\forall$ und $\exists$ heißen Quantoren.
  $\forall$ ist der Allquantor, $\exists$ ist der Existenzquantor.
- Wenn dadurch keine Mehrdeutigkeit entsteht, lassen wir, wie in der Aussagenlogik, Klammern weg.

Will man konkrete Sachverhalte mit Hilfe der Prädikatenlogik ausdrücken, dann wählt man das zugrundeliegende Vokabular dementsprechend. Wir werden dies anhand von zwei Beispielen demonstrieren.

Beispiel 4.7

Zahlentheorie: Betrachte das Vokabular $\Sigma_N := (\Phi_N, \Pi_N, \tau_N)$, wobei

- $\Phi_N := \{0, \sigma, +, \times, \uparrow\}$

  0 ist eine Konstante und σ eine unäre Funktion (Nachfolgerfunktion). $+$ (Addition), $\times$ (Multiplikation) und $\uparrow$ (Exponentiation) sind binäre Funktionen.

- $\Pi_N := \{=, <\}$

  Beide Relationen $=$ und $<$ sind binär.

Ein Ausdruck über Σ_N ist z.B.:

$$\forall x < (+(x, \sigma(\sigma(0))), \sigma(\uparrow(x, \sigma(\sigma(0))))).$$

Üblicherweise werden derartige Ausdrücke vereinfacht, damit diese leichter zu lesen sind:

i) Verwendung von Infixnotation für Funktionen und Relationen. So schreibt man $(x \times 0)$ anstatt $\times(x,0)$ oder auch $(y<y)$ anstatt

$<(y,y)$. Auch schreibt man 2 anstatt $\sigma(\sigma(0))$. Dies tut man für jede feste Anzahl der Anwendungen von σ auf 0:

5155 steht für $\underbrace{\sigma(\sigma(\sigma(\ldots(\sigma(0)\ldots))}_{5155 \text{ Anwendungen.}}$

Wenden wir diese Vereinfachungen auf obigen Ausdruck an, dann erhalten wir

$$\forall x((x+2) < \sigma((x \uparrow 2))).$$

Ein anderer Ausdruck über Σ_N ist z.B.:

$$((2 \times 3) + 3) = ((2 \uparrow 3) + 1).$$

Obige Ausdrücke sind bis jetzt Zeichenfolgen ohne irgendeine mathematische Bedeutung.

◊

Beispiel 4.8

Graphentheorie: Betrachte das Vokabular $\Sigma_G := (\Phi_G, \Pi_G, r_G)$, wobei

- $\Phi_G = \emptyset$, d.h., Σ_G enthält kein Funktionssymbol
- $\Pi_G = \{=, G\}$
  Beide Relationen $=$ und G sind binär.

Typische Ausdrücke über Σ_G sind z.B.:

$G(x,x)$

$\exists x(\forall y\, G(y,x))$

$\forall x(\forall y(G(x,y) \to G(y,x)))$

$\forall x(\forall y(\exists z(G(x,z) \wedge G(z,y)) \to G(x,y)))$.

◊

Eine Variable kann mehrmals innerhalb des Textes eines Ausdruckes erscheinen. Zum Beispiel erscheint x in $(\forall x(x+y>0)) \wedge (x>0)$ dreimal. Jedoch interpretiert man das x direkt nach $\forall$ als Teil des "Pakets" $\forall x$.

Ein Erscheinen einer Variablen x im Text eines Ausdruckes ϕ, das nicht direkt auf einen Quantor folgt, heißt ein <u>Vorkommen</u> von x in ϕ. Vorkommen einer Variablen kann <u>frei</u> oder <u>gebunden</u> sein. Intuitiv ist im obigen Ausdruck das Vorkommen von x in $x+y>0$ nicht frei, da es sich auf den Quantor $\forall x$ bezieht. Jedoch ist das zweite Vorkommen in $x>0$ frei. Demzufolge definieren wir:

Falls $\forall x \phi$ ein Ausdruck ist, dann heißt jedes Vorkommen von x in ϕ <u>gebunden</u>. Alle Vorkommen, die nicht gebunden sind, heißen <u>frei</u>.

Eine Variable, die ein freies Vorkommen in einem Ausdruck ϕ hat, ist eine <u>freie Variable</u> von ϕ (auch wenn dieselbe Variable andere gebundene Vorkommen in ϕ hat).

Ein Ausdruck ohne freie Variablen heißt Satz. Obiger Ausdruck ist kein Satz, da dieser zwei freie Variablen enthält. Dahingegen ist

$$\forall x(\forall y(\forall z(G(x,z) \wedge G(z,y)) \rightarrow G(x,y)))$$

ein Satz.

4.2.2 Strukturen und Modelle

Der Wahrheitswert eines prädikatenlogischen Ausdruckes ergibt sich aus den Werten seiner Bestandteile. Jedoch können in prädikatenlogischen Ausdrücken Variablen, Funktionen und Relationen komplexere Werte als wahr oder falsch annehmen. Das zu Belegungen analoge mathematische Objekt heißt Struktur.

Sei Σ ein festes Vokabular. Eine für Σ geeignete Struktur ist ein Paar $M := (U, \mu)$, wobei U eine beliebige aber nichtleere Menge, das sogenannte Universum von M, ist.
$\mu: V \cup \Phi \cup \Pi \rightarrow U$ ist eine Abbildung, die

- jeder Variablen $x \in V$ ein Element $x^M \in U$,
- jeder k-stelligen Funktion $f \in \Phi$ eine k-stellige Funktion $f^M: U^k \rightarrow U$ und
- jeder k-stelligen Relation $R \in \Pi$ eine k-stellige Relation $R^M \subseteq U^k$

zuordnet. Dabei wird der Gleichheitsrelation $=$ stets die Relation $=^M := \{(u,u) \mid u \in U\}$ zugeordnet.

Bemerkung:
Falls $c \in \Phi$ eine Konstante ist, dann impliziert obige Definition, dass c^M ein Element von U ist.

Ziel:
Definition der Semantik t^M eines Terms t in der Struktur M.

Wir definieren die Semantik von t induktiv.

i) Falls t eine Variable oder Konstante ist, dann ist t^M explizit durch M definiert.

ii) Falls $t = f(t_1, t_2, \dots, t_k)$ für eine k-stellige Funktion f, dann ist t^M definiert durch

$$f^M(t_1^M, t_2^M, \dots, t_k^M),$$

was ein Element des Universums U ist.

Sei ϕ ein Ausdruck über dem Vokabular Σ und M eine für Σ geeignete Struktur.

Ziel:
Definition, wann M den Ausdruck ϕ erfüllt (in Zeichen: $M \models \phi$).

Falls ϕ ein atomarer Ausdruck ist, d.h., $\phi = R(t_1, t_2, \dots, t_k)$, $R \in \Pi$ und $t_1, t_2, \dots, t_k$ sind Terme, dann erfüllt M den Ausdruck ϕ, falls $(t_1^M, t_2^M, \dots, t_k^M) \in R^M$.

Für nichtatomare Ausdrücke ϕ definieren wir die Erfüllbarkeit induktiv über den Aufbau von ϕ:

i) Falls $\phi = \neg\psi$, dann $M \models \phi$ falls $M \not\models \psi$.

ii) Falls $\phi = \psi_1 \vee \psi_2$, dann

$M \models \phi$ falls $M \models \psi_1$ oder $M \models \psi_2$.

iii) Falls $\phi = \psi_1 \wedge \psi_2$, dann

$M \models \phi$ falls $M \models \psi_1$ und $M \models \psi_2$.

$M_{x=u}$ bezeichnet diejenige Struktur, die wir aus M durch $x^{M_{x=u}} := u$ erhalten.

iv) Falls $\phi = \forall x \psi$, dann

$M \models \phi$ falls $M_{x=u} \models \psi$ für alle $u \in U$.

Folgendes Lemma zeigt, dass die Erfüllbarkeit eines Ausdruckes durch eine Struktur nicht von den Werten, die diese den nicht freien Variablen zuweist, abhängt.

Lemma 4.4

Seien ϕ ein Ausdruck über Σ und M und M' zwei für Σ geeignete Strukturen. Falls M und M' sich nur in Werten, die diese Variablen, die in ϕ nicht frei sind, zuweisen, unterscheiden, dann gilt genau dann $M \models \phi$ wenn $M' \models \phi$.

Beweis: (mittels Induktion über den Aufbau des Ausdruckes).

ϕ ist ein atomarer Ausdruck:

Dann sind alle Variablen in ϕ frei.

$\Rightarrow$ $M = M'$

Also gilt die Behauptung trivialerweise.

Annahme:
Die Behauptung gilt für die Ausdrücke ψ, ψ_1 und ψ_2.

$\phi = \neg\psi$:

Die freien Variablen in ϕ sind exakt dieselben wie in ψ. Also gilt

$M \models \phi \Leftrightarrow M \not\models \psi \Leftrightarrow M' \not\models \psi \Leftrightarrow M' \models \phi$.

$\phi = \psi_1 \wedge \psi_2$:

Die freien Variablen in ϕ ist die Vereinigung der freien Variablen in ψ_1 und in ψ_2.

Wenn M und M' sich nur bezüglich Werten, den diese nicht freien Variablen in ϕ zuweisen, unterscheiden, dann gilt dies auch bezüglich ψ_1 und ψ_2.

Induktionsannahme $\Rightarrow$

$M \models \psi_i \Leftrightarrow M' \models \psi_i$ für $i = 1, 2$

$\Rightarrow$

$M \models \phi \Leftrightarrow (M \models \psi_1$ und $M \models \psi_2)$
$\Leftrightarrow (M' \models \psi_1$ und $M' \models \psi_2)$
$\Leftrightarrow M' \models \phi.$

$\phi = \psi_1 \vee \psi_2$:

analog Übung

$\phi = \forall x \psi$:

Bis auf x sind die freien Variablen in ϕ exakt die freien Variablen in ψ. Die Variable x ist in ϕ gebunden. In ψ kann x frei sein oder nicht.

Definition $\Rightarrow$

$M \models \phi \Leftrightarrow M_{x=u} \models \psi$ für alle $u \in U$.

Induktionsannahme $\Rightarrow$

[$(M_{x=u} \models \psi$ für alle $u \in U)$
$\Leftrightarrow ((M_{x=u})' \models \psi$ für alle $u \in U)$ für alle Strukturen $(M_{x=u})'$, die sich nur bzgl. nichtfreie Variablen von ψ anders verhalten als $M_{x=u}$.]

In letzten Ausdruck variieren Werte der in ψ nichtfreien Variablen und Werte von x
$\Rightarrow$
Es variieren Werte der in ϕ nichtfreien Variablen
$\Rightarrow$

[$M \models \varnothing \iff$
$M' \models \phi$ für alle M', die sich von M nur bezüglich in ϕ nichtfreie Variablen unterscheiden.]

Beispiel 4.7 (Fortführung):

Ziel:
Definition einer für $\Sigma_N = (\Phi_N, \Pi_N, r_N)$ geeigneten Struktur $\mathcal{N} = (U, \mu)$.

- $U := \mathbb{N}_0$
- $\mu(0) = 0^{\mathcal{N}} := 0 \quad (\in \mathbb{N}_0)$
- $\mu(\sigma) := \sigma^{\mathcal{N}} : \mathbb{N}_0 \to \mathbb{N}_0$, wobei $\sigma^{\mathcal{N}}(n) := n+1$.
- $\mu(+)$ Addition
- $\mu(\times)$ Multiplikation
- $\mu(\uparrow)$ Exponentiation

- Für zwei Zahlen m und n gilt $m <^{\mathcal{N}} n$, falls m kleiner als n ist.
- μ bildet jede Variable auf die Zahl 0 ab.

Beh. 1.: $\mathcal{N} \models \forall x\,(x < x+1)$

Bew.:
Zum Beweis der Beh. 1 müssen wir unser Wissen bezüglich Eigenschaften von natürlichen Zahlen verwenden.

2.2. Für alle $n \in \mathbb{N}_0$ gilt $\mathcal{N}_{x=n} \models x < x+1$

D.h., wir müssen beweisen, dass für alle $n \in \mathbb{N}_0$

$$n <^{\mathcal{N}} n +^{\mathcal{N}} 1^{\mathcal{N}}.$$

Dies bedeutet $n < n+1$, was bekanntlich für jede ganze Zahl n gilt.

■

Beh. 2: $\mathcal{N} \not\models \forall x \exists y (x = y + y)$

Bew.:

Es gilt

$$\mathcal{N}_{x=1} \not\models \exists y (x = y + y)$$

oder äquivalent

$$\mathcal{N}_{x=1} \models \forall y \neg (x = y + y)$$

D.h., $1 \neq n + n$ für alle Zahlen $n \in \mathbb{N}_0$, was bekanntlich gilt.

■

◊

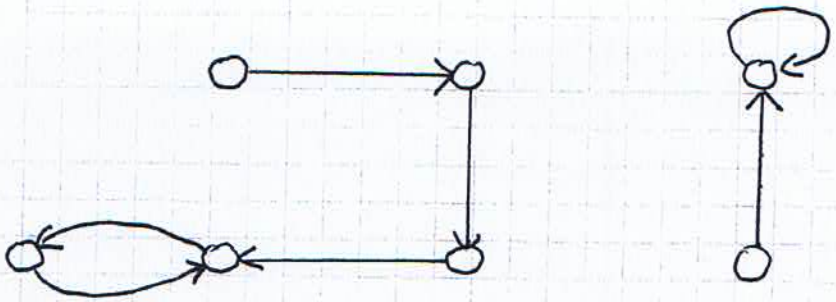
Beispiel 4.8 (Fortführung)

Es gibt eine interessante Dualität zwischen Sätze und Strukturen. Eine Struktur erfüllt einen Satz oder erfüllt diesen nicht. Andererseits kann ein Satz als Beschreibung derjenigen Menge von Strukturen, die diesen erfüllen, angesehen werden. Wir illustrieren dies anhand der Vokabulars $\Sigma_G := (\Phi_G, \Pi_G, \Gamma_G)$.

Jede für Σ_G geeignete Struktur ist ein Graph. Wir betrachten nur endliche Graphen. Betrachte folgenden Satz:

$$\phi_1 := (\forall x \exists y\, G(x,y) \wedge \forall x \forall y \forall z ((G(x,y) \wedge G(x,z)) \rightarrow y = z))$$

Folgende für Σ_G geeignete Struktur Γ erfüllt ϕ_1:



Das Universum von Γ ist die Menge der sieben Knoten des Graphen im obigen Bild. Ferner gilt

$G^\Gamma(x,y)$, falls eine Kante von x nach y im obigen Graphen existiert.

Mittels Überprüfung überzeugt man sich, dass

$$\Gamma \models \phi_1.$$

<u>Frage</u>: Welche andere Graphen erfüllen ϕ_1?

<u>Übung</u>:
Zeigen Sie, dass genau diejenigen Graphen, deren Knoten alle den Ausgangsgrad eins haben, ϕ_1 erfüllen.

Somit erfüllen genau diejenigen Graphen, die eine <u>totale Funktion</u> repräsentieren ϕ_1 mit Def.-Bereich = Bildbereich.

Betrachte folgende Sätze:

$$\Phi_2 := \forall x(\forall y(G(x,y) \rightarrow G(y,x)))$$

$$\Phi_3 := \forall x(\forall y(\forall z((G(x,z) \wedge G(z,y)) \rightarrow G(x,y))))$$

Φ_2 erfüllen genau die Symmetrische und Φ_3 genau die transitive Graphen. ◆

Lemma 4.4 besagt, dass die Tatsache, ob eine Struktur einen Ausdruck erfüllt oder nicht, nicht von denjenigen Werten abhängt, die die Struktur gebundenen oder im Ausdruck nicht vorkommenden Variablen zuordnet.

Wir sagen, dass eine Struktur für einen Ausdruck geeignet ist, wenn diese Struktur für alle im Ausdruck vorkommenden Funktionen, Relationen und freien Variablen definiert ist.

Eine für einen Ausdruck ϕ geeignete Struktur Γ heißt genau dann Modell für ϕ, wenn $\Gamma \models \phi$.

4.2.3 Gültige Ausdrücke

Ein Ausdruck ϕ heißt genau dann erfüllbar, wenn es ein Modell für ϕ gibt. ϕ heißt genau dann gültig, wenn jede für ϕ geeignete Struktur ein Modell für ϕ ist. Wenn ϕ gültig ist, dann schreiben wir $\models \phi$.

Lemma 4.5

Ein Ausdruck ist genau dann unerfüllbar, wenn seine Negation gültig ist.

Beweis:

Übung

Frage: Was macht einen Ausdruck gültig?

Intuitiv ist ein Ausdruck aus grundlegenden Gründen, die etwas mit allgemeinen Eigenschaften von Funktionen, Gleichheit, Quantoren u.s.w. zu tun haben, gültig.

Ziel:
Herausarbeiten von solchen Basisgründen.

a) **Aussagelogische Gültigkeit**

Betrachten wir folgenden Ausdruck:

$$\phi := \forall x\, P(x) \;\vee\; \neg \forall x\, P(x).$$

ϕ hat die Form $\psi \vee \neg\psi$, wobei $\psi = \forall x\, P(x)$.

Wenn wir ψ als Boolesche Variable interpretieren, dann ist $\psi \vee \neg\psi$ eine Tautologie in der Aussagenlogik.

$\Rightarrow$

ϕ ist in der Prädikatenlogik ein gültiger Ausdruck

Der Ausdruck

$$(G(x,y) \wedge G(y,x)) \rightarrow (G(y,x) \wedge G(x,y))$$

ist gültig, da $\wedge$ kommutativ ist.

Obige prädikatenlogische Ausdrücke sind aus aussagelogischen Gründen gültig. Wir möchten diese Sichtweise verallgemeinern. Hierzu definieren wir für einen Ausdruck ϕ die Menge seiner Stammteilausdrücke $S(\phi)$:

i) ϕ atomarer Ausdruck oder $\phi = \forall x \psi$.
Dann besitzt ϕ genau einen Stammteilausdruck, nämlich sich selbst.

ii) $\phi = \neg \psi$.
Dann gilt $S(\phi) := S(\psi)$.

iii) $\phi = \psi_1 \vee \psi_2$ oder $\phi = \psi_1 \wedge \psi_2$.
Dann gilt $S(\phi) := S(\psi_1) \cup S(\psi_2)$.

Beispiel 4.9:

Betrachte

$$\phi := \forall x\, G(x,y) \wedge \exists x\, G(x,y) \wedge (G(z,x) \vee \forall x\, G(x,y))$$

Zunächst expandieren wir

$$\exists x\, G(x,y) \text{ zu } \neg \forall x \neg G(x,y)$$

und erhalten dann

$$S(\phi) = \{ \forall x G(x,y),\ \forall x \neg G(x,y),\ G(z,x) \}$$

◊

Jeder prädikatenlogischer Ausdruck ϕ kann als aussagelogischer Ausdruck mit Stammteilausdrücke anstatt Boolesche Variablen interpretiert werden. Wir nennen dies die <u>aussagelogische Form</u> von ϕ.

<u>Beispiel 4.9</u> (Fortführung):

Die aussagenlogische Form von ϕ ist

$$x_1 \wedge (\neg x_2) \wedge (x_3 \vee x_1),$$

wobei $x_1 = \forall x G(x,y)$, $x_2 = \forall x \neg G(x,y)$ und $x_3 = G(z,x)$.

<u>Lemma 4.6</u>

Wenn die aussagelogische Form eines prädikatenlogischen Ausdruckes ϕ eine Tautologie ist, dann ist ϕ gültig.

<u>Beweis</u>:

Sei M eine beliebige für ϕ geeignete Struktur. Jeder Stammteilausdruck von ϕ wird von M erfüllt oder nicht erfüllt. Dies definiert eine Belegung der Stammteilausdrücke von ϕ. Da

die aussagenlogische Form von ϕ eine Tautologie ist, muss dies ϕ erfüllen.

Mit Hilfe der Aussagenlogik können nicht nur neue gültige Ausdrücke identifiziert sondern auch bekannte gültige Ausdrücke zu neuen kombiniert werden.

Wenn ϕ und ψ gültig sind, dann folgt ebenso die Gültigkeit von $\phi \wedge \psi$. Wenn ϕ und $\phi \to \psi$ gültig sind, dann ist auch ψ gültig.

Lemma 4.7 (Modus Ponens):
Wenn ϕ und $\phi \to \psi$ gültig sind, dann ist auch ψ gültig.

b) Gleichheit

Ein Ausdruck kann auch aufgrund der Eigenschaften der Gleichheit gültig sein. So ist z.B. $x+1 = x+1$ gültig. Betrachte

$$\phi := x = 1 \to 1 + 1 = x + 1.$$

Dieser Ausdruck ist unabhängig von der Semantik von 1 und + gültig. Wenn $x = 1$, dann führt jede Funktion, angewandt auf die Argumente $x, 1$ und auf $1, 1$ zum selben Resultat.

Dasselbe gilt für den Ausdruck

$$x = y \to (G(x,x) \to G(y,x)).$$

Falls $x = y$, dann impliziert $G(x,x)$ unabhängig von der Bedeutung von G auch $G(y,x)$.

Insgesamt gilt folgendes Lemma:

Lemma 4.8

Seien $t_1, t_2, \ldots, t_k, t_1', t_2', \ldots, t_k'$ Terme. Dann ist jeder der folgenden Ausdrücken gültig:

i) $t_1 = t_1$,

ii) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \ldots \wedge t_k = t_k') \Rightarrow$
$f(t_1, t_2, \ldots, t_k) = f(t_1', t_2', \ldots, t_k')$ und

iii) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \ldots \wedge t_k = t_k') \rightarrow$
$\left(R(t_1, t_2, \ldots, t_k) \rightarrow R(t_1', t_2', \ldots, t_k')\right)$.

c) Quantoren

Des Weiteren kann ein Ausdruck aufgrund der Bedeutung der Quantoren gültig sein. So ist z.B. der Ausdruck

$$G(x,1) \rightarrow \exists z\, G(x,z)$$

gültig. In jeder geeigneten Struktur impliziert im Falle, dass $G(x,1)$ gilt, dass es ein z gibt, so dass $G(x,z)$ gilt; nämlich $z = 1$.

Auch ist $\forall x\, G(x,y) \rightarrow G(z,y)$ gültig.

Sein ϕ ein Ausdruck, x eine Variable und t ein Term. Die Substitution von x durch t in ϕ $\phi[x := t]$ ist derjenige Ausdruck, den wir aus ϕ nach Ersetzung von allen freien Vorkommen der Variablen x durch den Term t erhalten.

Beispiel 4.10

Seien

$$\phi := (x = 1) \to \exists x (x = y) \quad \text{und} \quad t = y + 1.$$

Dann erhalten wir

$$\phi[x := t] = (y + 1 = 1) \to \exists x (x = y) \quad \text{und}$$

$$\phi[y := t] = (x = 1) \to \exists x (x = y + 1).$$

◊

Es gibt ein Problem mit obiger Definition falls t eine Variable, die an einer Position in der x vorkommt gebunden ist, enthält.

Beispiel 4.10 (Fortführung)

Betrachte folgende Modifikation von ϕ:

$$\phi' := (x = 1) \to \exists y (x = y)$$

Dann gilt:

$$\phi'[x := t] = (y + 1 = 1) \to \exists y (y + 1 = y),$$

was nicht unser Verständnis der Addition entspricht. ◆

t ist genau dann für x in ϕ substituierbar, wenn es in t keine Variable y gibt, für die gilt: Es gibt einen Teilausdruck von ϕ der Form $\forall y\, \psi$ oder $\exists y\, \psi$, in dem die Variable x frei vorkommt.

Wir werden die Notation $\phi[x := t]$ nur dann verwenden, wenn t für x in ϕ substituierbar ist. Dies bedeutet, dass die Verwendung dieser Notation diese Annahme implizit enthält.

Lemma 4.9

Jeder Ausdruck der Form $\forall x\, \phi \to \phi[x := t]$ ist gültig.

Lemma 4.10

Falls ϕ gültig ist, dann ist auch $\forall x\, \phi$ gültig.

Lemma 4.11

Falls x nicht frei in ϕ vorkommt, dann ist der Ausdruck $\phi \to \forall x\, \phi$ gültig.

Lemma 4.12

Für alle ϕ und ψ ist der Ausdruck

$$(\forall x\, (\phi \to \psi)) \to ((\forall x\, \phi) \to (\forall x\, \psi))$$

gültig.

Übung:

Beweisen Sie die Lemmata 4.9 – 4.12.

d) Die Pränexnormalform

Mit Hilfe der Gültigkeit können wir Ausdrücke vereinfachen. Falls $\phi \leftrightarrow \psi$ gültig ist, dann können wir in einem Ausdruck den Teilausdruck ϕ durch ψ ersetzen. Die sorgfältige Anwendung von solchen Ersetzungen führt zu einfacheren Ausdrücke. Falls $\phi \leftrightarrow \psi$ gültig ist, dann schreiben wir $\phi \equiv \psi$, d.h. ϕ und ψ sind äquivalent.

Lemma 4.13

Seien ϕ und ψ beliebige prädikatenlogische Ausdrücke. Dann gilt:

i) $\forall x(\phi \wedge \psi) \equiv (\forall x \phi \wedge \forall x \psi)$.

ii) Falls x nicht frei in ψ vorkommt, dann $\forall x(\phi \wedge \psi) \equiv (\forall x \phi \wedge \psi)$.

iii) Falls x nicht frei in ψ vorkommt, dann $\forall x(\phi \vee \psi) \equiv (\forall x \phi \vee \psi)$.

iv) Falls y nicht in ϕ vorkommt, dann $\forall x \phi \equiv \forall y \phi[x := y]$.

v) $\neg \forall x \phi \equiv \exists x \neg \phi$ und $\neg \exists x \phi \equiv \forall x \neg \phi$.

Beweis:

Übung

■

Ein prädikatenlogischer Ausdruck ist in Pränex-normalform, falls er aus einer Folge von Quantoren gefolgt von einem Ausdruck ohne Quantoren besteht.

Ziel:
Umformung eines beliebigen prädikatenlogischen Ausdruckes in einen äquivalenten Ausdruck in Pränexnormalform.

Beispiel 4.11

$$(\forall x\,(G(x,x) \wedge (\forall y\, G(x,y) \vee \exists y \neg G(y,y))) \wedge G(x,0))$$

$\rightsquigarrow$ Le 4.13 iv)

$$(\forall x\,(G(x,x) \wedge (\forall y\, G(x,y) \vee \exists z \neg G(z,z))) \wedge G(w,0))$$

$\rightsquigarrow$ 2x Le 4.13 ii)

$$\forall x\,((G(x,x) \wedge (\forall y\, G(x,y) \vee \exists z \neg G(z,z))) \wedge G(w,0))$$

$\rightsquigarrow$ Le 4.13 iii)

$$\forall x\,((G(x,x) \wedge \forall y\,(G(x,y) \vee \exists z \neg G(z,z))) \wedge G(w,0))$$

$\rightsquigarrow$ 2x Le 4.13 iv)

$$\forall x \forall y\,((G(x,x) \wedge (G(x,y) \vee \exists z \neg G(z,z))) \wedge G(w,0))$$

Le 4.13 v)

$$\forall x \forall y \, ((G(x,x) \wedge (G(x,y) \vee \neg \forall z \, G(z,z))) \wedge G(w,0))$$

De Morgan

$$\forall x \forall y \, ((G(x,x) \wedge \neg (\neg G(x,y) \wedge \forall z \, G(z,z))) \wedge G(w,0))$$

Le 4.13 ii)

$$\forall x \forall y \, ((G(x,x) \wedge \neg \forall z (\neg G(x,y) \wedge G(z,z))) \wedge G(w,0))$$

De Morgan

$$\forall x \forall y \, (\neg (\neg G(x,x) \vee \forall z (\neg G(x,y) \wedge G(z,z))) \wedge G(w,0))$$

Le. 4.13 iii)

$$\forall x \forall y \, (\neg \forall z (\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \wedge G(w,0))$$

De Morgan

$$\forall x \forall y \neg (\forall z (\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \vee \neg G(w,0))$$

Le 4.13 ii)

$$\forall x \forall y \neg \forall z ((\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \vee \neg G(w,0))$$

Le 4.13 v)

$$\forall x \forall y \exists z \neg ((\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \vee \neg G(w,0))$$

Der letzte Ausdruck ist in Pränexnormalform.

Allgemein gilt folgendes Satz:

Satz 4.3

Jeder prädikatenlogischer Ausdruck kann in einen äquivalenten Ausdruck in Pränexnormalform transformiert werden.

Beweis:

Wir beweisen den Satz mittels Induktion über den Aufbau des Ausdruckes.

ϕ atomarer Ausdruck

Dann enthält ϕ keinen Quantor und ist somit bereits in Pränexnormalform

Annahme:

Zu ψ, ψ_1 und ψ_2 existieren äquivalente Ausdrücke in Pränexnormalform.

$\phi = \neg\psi$

Sei $Q_1 x_1 Q_2 x_2 \dots Q_n x_n \varphi$ ein zu ψ äquivalenter Ausdruck in Pränexnormalform, wobei φ keinen Quantor enthält. Mittels wiederholter Anwendung des Lemmas 4.13 v) erhalten wir (wobei $\bar{\forall} := \exists$ und $\bar{\exists} := \forall$):

$$\begin{aligned}
\phi = \neg\psi &\equiv \neg Q_1 x_1 Q_2 x_2 \dots Q_n x_n \varphi \\
&\equiv \bar{Q}_1 x_1 \neg Q_2 x_2 \dots Q_n x_n \varphi \\
&\vdots \\
&\equiv \bar{Q}_1 x_1 \bar{Q}_2 x_2 \dots \bar{Q}_n x_n \neg\varphi .
\end{aligned}$$

Der letzte Ausdruck ist in Pränexnormalform.

$\Phi = \varphi_1 \circ \varphi_2$, wobei $\circ \in \{\wedge, \vee\}$:

Betrachte zu φ_1 und zu φ_2 äquivalente Ausdrücke in Pränexnormalform. Mittels wiederholter Anwendung des Lemmas 4.13 iv) erreichen wir, dass keine freie Variable in einem der beiden Ausdrücken gebunden vorkommt und dass die gebundenen Variablen in beiden Ausdrücken paarweise disjunkt sind.
Seien

$$Q_1' y_1 Q_2' y_2 \cdots Q_k' y_k \varphi_1 \quad \text{und}$$
$$Q_1'' z_1 Q_2'' z_2 \cdots Q_\ell'' z_\ell \varphi_2$$

die resultierenden Ausdrücke in Pränexnormalform. Betrachte

$$\Phi = \varphi_1 \circ \varphi_2 \equiv Q_1' y_1 \cdots Q_k' y_k \varphi_1 \circ Q_1'' z_1 \cdots Q_\ell'' z_\ell \varphi_2$$

Wiederholte Anwendung Anwendung von

$$\begin{cases} \text{Lemma 4.13 ii)} & \text{falls } \circ = \wedge \\ \text{Lemma 4.13 iii)} & \text{falls } \circ = \vee \end{cases}$$

ergibt dann

$$\Phi \equiv Q_1' y_1 Q_2' y_2 \cdots Q_k' y_k Q_1'' z_1 Q_2'' z_2 \cdots Q_\ell'' z_\ell (\varphi_1 \circ \varphi_2).$$

Die rechte Seite ist in Pränexnormalform.

$\Phi = \forall x \psi$:

Sei $Q_1 x_1 Q_2 x_2 \dots Q_n x_n \varphi$ ein zu ψ äquivalenter Ausdruck in Pränexnormalform. Dann gilt:

$$\Phi = \forall x \psi \equiv \forall x Q_1 x_1 Q_2 x_2 \dots Q_n x_n \varphi .$$

Die rechte Seite ist in Pränexnormalform.

∎

4.2.4 Axiome und Beweise

Bisher haben wir die Syntax und die Semantik eines Systems, in dem wir mathematische Aussagen formulieren können, definiert. Was noch fehlt ist eine systematische Methode, mittels der wir beweisen können, dass eine Aussage wahr ist. Zunächst müssen wir definieren, was wir darunter verstehen, dass eine Aussage wahr ist. In der Prädikatenlogik können wir "Wahrheit" und Gültigkeit identifizieren. Dies bedeutet, dass wir dann eine systematische Methode benötigen, mittels der wir die Gültigkeit von Ausdrücken beweisen können. Hierzu konstruieren wir ein Beweissystem, das auf den Basisgründen für die Gültigkeit und den Lemmata 4.7 - 4.12 aufbaut. Dieses wird auf Ausdrücken über einem festen Vokabular Σ anwendbar sein.

Unser Beweissystem baut auf einer aufzählbar unendlichen Menge von logischen Axiomen auf. Diese sind unsere elementare gültige Ausdrücke.

Basisaxiome:

AX 0: Alle Ausdrücke, deren aussagelogische Form eine Tautologie ist.

AX 1: Alle Ausdrücke, die eine der folgenden Formen haben ($t \in \mathbb{N}$):

a) $t = t$.

b) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \dots \wedge t_t = t_t') \rightarrow f(t_1, t_2, \dots, t_t) = f(t_1', t_2', \dots, t_t')$

c) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \dots \wedge t_t = t_t') \rightarrow (R(t_1, t_2, \dots, t_t) \rightarrow R(t_1', t_2', \dots, t_t'))$.

AX 2: Alle Ausdrücke der Form
$$\forall x \phi \rightarrow \phi[x := t].$$

AX 3: Alle Ausdrücke der Form
$$\phi \rightarrow \forall x \phi,$$
wobei x nicht frei in ϕ vorkommt.

AX 4: Alle Ausdrücke der Form
$$(\forall x(\phi \rightarrow \psi)) \rightarrow (\forall x \phi \rightarrow \forall x \psi).$$

AX 5: Alle Ausdrücke der Form $\forall x \phi$, wobei ϕ ein elementarer gültiger Ausdruck ist.

Unter Verwendung von Modus ponens (Lemma 4.7) kann unser Beweissystem neue (nicht =

elementare) gültige Ausdrücke generieren. Betrachten wir eine endliche Folge

$$S = \phi_1, \phi_2, \ldots, \phi_n$$

von prädikatenlogischen Ausdrücken, wobei für jeden Ausdruck ϕ_i, $1 \leq i \leq n$ in dieser Folge gilt:

a) $\phi_i \in \Omega$, wobei Ω die Menge der elementare gültigen Ausdrücke ist

oder

b) es existieren unter $\phi_1, \phi_2, \ldots, \phi_{i-1}$ zwei Ausdrücke der Form ψ bzw. $\psi \rightarrow \phi_i$ (Anwendung von Modus ponens)

Dann ist S ein <u>Beweis</u> (oder auch <u>Ableitung</u>) des Ausdrucken ϕ_n. Der Ausdruck ϕ_n heißt dann <u>Satz der Prädikatenlogik</u> und wir schreiben $\vdash \phi_n$.

<u>Bemerkung:</u>

Wenn $\vdash \phi$, dann ist der Ausdruck ϕ gültig. Wenn $\models \phi$, dann ist der Ausdruck ϕ auch gültig. Jedoch muss nicht notwendigerweise ϕ aus den Axiomen ableitbar sein; d.h., es muss nicht notwendigerweise $\vdash \phi$ gelten.

Beispiel 4.12

- Die Reflexivität $x = x$ der Gleichheit ist ein Axiom.

- Die Symmetrie $x = y \to y = x$ der Gleichheit ist ein Satz der Prädikatenlogik. Diesen werden wir nun beweisen.

Betrachten wir folgende Folge von Ausdrücken:

$$S = \phi_1, \phi_2, \phi_3, \phi_4, \phi_5,$$

wobei

$$\phi_1 := (x = y \wedge x = x) \to (x = x \to y = x)$$
$$\phi_2 := (x = x)$$
$$\phi_3 := x = x \to (((x = y \wedge x = x) \to (x = x \to y = x)) \to (x = y \to y = x))$$
$$\phi_4 := ((x = y \wedge x = x) \to (x = x \to y = x)) \to (x = y \to y = x)$$
$$\phi_5 := (x = y \to y = x)$$

Wir werden nun zeigen, dass S ein Beweis des Ausdruckes $x = y \to y = x$ ist.

ϕ_1 ist ein Axiom der Gruppe AX1c), wobei

$k = 2$, R ist die Gleichheit, $t_1 = t_2 = t_2' = x$ und $t_1' = y$.

ϕ_2 ist ein Axiom der Gruppe AX1a).

ϕ_3 ist ein Axiom der Gruppe AX0
(überzeugen Sie sich).

ϕ_4 erhalten wir aus ϕ_2 und ϕ_3 mittels Modus ponens.

ϕ_5 erhalten wir aus ϕ_1 und ϕ_4 mittels Modus ponens.

Insgesamt haben wir $\vdash x = y \to y = x$ gezeigt. ∎

Sei Δ eine Menge von Ausdrücke und $\phi \notin \Delta$ ein weiterer Ausdruck. ϕ ist genau dann eine gültige Konsequenz von Δ, wenn jede Struktur, die jeden Ausdruck in Δ erfüllt, auch ϕ erfüllt. Wir schreiben dann $\Delta \models \phi$.

Ziel:
Verallgemeinerung des obigen Beweissystems.

Sei Δ eine Menge von Ausdrücken. Sei

$$S := \phi_1, \phi_2, \dots, \phi_n$$

eine Folge von Ausdrücken, wobei für jeden Ausdruck ϕ_i, $1 \le i \le n$ in dieser Folge gilt:

a) $\phi_i \in \sigma$ oder
b) $\phi_i \in \Delta$ oder
c) es existieren unter $\phi_1, \phi_2, \dots, \phi_{i-1}$ zwei Ausdrücke der Form ψ bzw. $\psi \to \phi_i$
(Anwendung von Modus ponens)

Dann ist S ein Beweis (oder Ableitung) des Ausdruckes ϕ_n aus Δ. Der Ausdruck ϕ_n heißt dann Δ-Satz der Prädikatenlogik und wir schreiben $\Delta \vdash \phi_n$.

Bemerkung:
Beachte auch hier den Unterschied von $\Delta \vdash \phi$ und $\Delta \models \phi$.

Im obigen erweiterten Beweissystem heißen die Ausdrücke in Δ nichtlogische Axiome des Beweissystems.

Ziel:
Herausarbeiten von drei Standardbeweismethoden der Mathematik.

Satz 4.4 (Deduktionstechnik)

Nehmen wir an, dass $\Delta \cup \{\phi\} \vdash \psi$. Dann gilt $\Delta \vdash \phi \to \psi$.

Beweis:
Betrachten wir einen Beweis $S = \phi_1, \phi_2, \ldots, \phi_n$ von ψ aus $\Delta \cup \{\phi\}$. D.h., $\phi_n = \psi$.

Idee:
Beweise mittels Induktion über i, dass

$$\phi \to \phi_i \text{ aus } \Delta \text{ für } i = 1, 2, \ldots, n.$$

Hieraus folgt dann wegen $\phi_n = \psi$ die Behauptung.

Durchführung:

$i = 1$:

Da $S = \phi_1, \phi_2, \ldots, \phi_n$ ein Beweis von ψ aus $\Delta \cup \{\phi\}$ ist, gilt $\phi_1 \in \Gamma \cup \Delta \cup \{\phi\}$.

Falls $\phi_1 = \phi$, dann ist $\phi \to \phi$ ein Axiom aus der Gruppe AX0 und somit ein Beweis für $\phi \to \phi_1$.

Falls $\phi_1 \in \Gamma \cup \Delta$, dann ist

$$\phi_1, \phi_1 \to (\phi \to \phi_1), \phi \to \phi_1$$

ein Beweis für $\phi \to \phi_1$ aus Δ, da

a) $\phi_1 \in \Gamma \cup \Delta$ gemäß Annahme,
b) $\phi_1 \to (\phi \to \phi_1)$ Axiom aus AX0 und
c) $\phi \to \phi_1$ aus den vorangegangenen Ausdrücken mittels Modus ponens entsteht.

Annahme:

$1 \leq i < n$ und $\phi \to \phi_j$ für $1 \leq j \leq i$.

$i \rightsquigarrow i+1$:

Der Beweis für $\phi \to \phi_{i+1}$ enthält alle Beweise der Ausdrücke $\phi \to \phi_j$, $1 \leq j \leq i$ erweitert um einige neue Ausdrücke, die von ϕ_{i+1} abhängen. Bezüglich ϕ_{i+1} sind drei Fälle möglich:

1) $\phi_{i+1} = \phi$

Dann fügen wir $\phi \to \phi$, was ein Axiom aus AX0 ist, dem Beweis hinzu.

2) $\phi_{i+1} \in \Gamma \cup \Delta$

Dann erweitern wir den Beweis mit

$$\phi_{i+1},\ \phi_{i+1} \to (\phi \to \phi_{i+1}),\ \phi \to \phi_{i+1}$$

Dies ist ein Beweis für $\phi \to \phi_{i+1}$ aus Δ (Begründung s.o.).

3) ϕ_{i+1} erhält man in S aus einem ϕ_j und $\phi_j \to \phi_{i+1}$ mittels Modus ponens, wobei $j \leq i$.

Dann enthält unser Beweis bereits

$$\phi \to \phi_j \quad \text{und} \quad \phi \to (\phi_j \to \phi_{i+1}).$$

Wir erweitern unseren Beweis um die Ausdrücke

$$(\phi \to \phi_j) \to (((\phi \to (\phi_j \to \phi_{i+1})) \to (\phi \to \phi_{i+1})),$$
$$(\phi \to (\phi_j \to \phi_{i+1})) \to (\phi \to \phi_{i+1}) \quad \text{und}$$
$$\phi \to \phi_{i+1}$$

Der erste Ausdruck ist ein Axiom der Gruppe AX0. Die beiden anderen Ausdrücke entstehen mittels Modus ponens. (Überzeugen Sie sich).

■

Bemerkung:
Nur im 3. Fall benötigen wir die Induktionsvoraus =

Setzung.

Als nächstes betrachten wir den Widerspruchsbeweis. D.h., um ϕ zu beweisen nehmen wir $\neg\phi$ an und führen diese Annahme zu einem Widerspruch.

Formal kann ein Widerspruch durch einen Ausdruck

$$\psi \wedge \neg\psi ,$$

wobei ψ ein beliebiger Ausdruck ist, definiert werden.

Falls es einen Beweis von $\psi \wedge \neg\psi$ aus Δ gibt, dann gilt $\Delta \vdash \phi$ für alle Ausdrücke ϕ.

Übung:
Zeigen Sie, dass $\Delta \vdash \psi \wedge \neg\psi$ auch $\Delta \vdash \phi$ für jeden Ausdruck ϕ impliziert.

Falls $\Delta \vdash \phi$ für alle Ausdrücke ϕ, dann heißt Δ inkonsistent. Falls kein Widerspruch aus Δ bewiesen werden kann, dann heißt Δ konsistent.

Satz 4.5 (Widerspruchsbeweis)

Falls $\Delta \cup \{\neg\phi\}$ inkonsistent ist, dann gilt $\Delta \vdash \phi$.

Beweis:

Annahme: $\Delta \cup \{\neg\phi\}$ ist inkonsistent.

Dann gilt

$$\Delta \cup \{\neg\phi\} \vdash \phi$$

Satz 4.4 $\Rightarrow$

$$\Delta \vdash \neg\phi \to \phi$$

Wir erweitern den Beweis von $\neg\phi \to \phi$ aus Δ durch Hinzufügen der Folge

$$(\neg\phi \to \phi) \to \phi,\ \phi$$

Der erste Ausdruck ist ein Axiom der Gruppe AX0. Den zweiten Ausdruck erhalten wir mittels Modus ponens aus $\neg\phi \to \phi$ und dem ersten Ausdruck.

■

Häufig nimmt man aus einer Menge ein beliebiges, aber festes Element und beweist für dieses eine Eigenschaft. Da dieses Element aus der Menge beliebig gewählt worden ist, schließt man nun daraus, dass jedes Element der Menge diese Eigenschaft besitzt. Diese Vorgehensweise heißt gerechtfertigte Verallgemeinerung.

Satz 4.6 (gerechtfertigte Verallgemeinerung)

Nehmen wir an, dass $\Delta \vdash \phi$ und x in keinem Ausdruck in Δ frei vorkommt. Dann gilt $\Delta \vdash \forall x\, \phi$.

Beweis:

Betrachten wir einen Beweis

$$S := \phi_1, \phi_2, \dots, \phi_n$$

von ϕ aus Δ (d.h., $\phi_n = \phi$).

Idee:

Beweise mittels Induktion über i, dass

$$\Delta \vdash \forall x \phi_i \quad \text{für } i = 1, 2, \dots, n.$$

Hieraus folgt dann wegen $\phi_n = \phi$ die Behauptung.

Durchführung:

$i = 1$:

Es gilt $\phi_1 \in \Omega \cup \Delta$.

1) $\phi_1 \in \Omega$

Dann ist auch $\forall x \phi_1 \in \Omega$.

2) $\phi_1 \in \Delta$

Dann ist ϕ_1 ein nichtlogisches Axiom. Gemäß Voraussetzung kommt x nicht frei in ϕ_1 vor.

$\Rightarrow$ (Ax 3)

Die Folge $\phi_1, \phi_1 \to \forall x \phi_1, \forall x \phi_1$ ist ein Beweis für $\forall x \phi_1$ aus Δ.

Annahme:

$1 \leq i < n$ und $\Delta \vdash \forall x \phi_j$ für $1 \leq j \leq i$.

$i \rightsquigarrow i+1$:

Der Beweis für $\forall x \phi_{i+1}$ enthält alle Beweise für die Ausdrücke $\forall x \phi_j$, $1 \leq j \leq i$, erweitert um einige neue Ausdrücke, die von ϕ_{i+1} abhängen. Bezüglich ϕ_{i+1} sind drei Fälle möglich:

1) $\phi_{i+1} \in \Gamma$.

Dann gilt auch $\forall x \phi_{i+1} \in \Gamma$ und wir fügen $\forall x \phi_{i+1}$ dem Beweis hinzu.

2) $\phi_{i+1} \in \Delta$.

Dann ist ϕ_{i+1} ein nichtlogisches Axiom. Gemäß Voraussetzung kommt x nicht frei in ϕ_{i+1} vor.

Wir erweiten unseren Beweis um die Ausdrücke

$$\phi_{i+1},\ (\phi_{i+1} \to \forall x \phi_{i+1}) \overset{AX3}{\downarrow},\ \forall x \phi_{i+1}$$

3) ϕ_{i+1} erhält man in S aus einem ϕ_j und $\phi_j \to \phi_{i+1}$ mittels Modus ponens, wobei $j \leq i$.

Induktionsannahme $\Rightarrow$

Unser Beweis enthält bereits

$\forall x \phi_j$ und $\forall x (\phi_j \to \phi_{i+1})$

Wir erweitern unseren Beweis um die Ausdrücke

$(\forall x (\phi_j \to \phi_{i+1})) \to (\forall x \phi_j \to \forall x \phi_{i+1})$ $\in AX4$

$\forall x \phi_j \to \forall x \phi_{i+1}$ Modus ponens

$\forall x \phi_{i+1}$ Modus ponens.

∎

Beispiel 4.13

a) Beh.: $\vdash \forall x \forall y \phi \to \forall y \forall x \phi$.

Bew.:

Sei $\phi_1 := \forall x \forall y \phi$.

Für die Anwendung der Deduktionstechnik nehmen wir an, dass die Voraussetzung des gewünschten Ausdrucks erfüllt ist. D.h., wir setzen

$\Delta := \{\phi_1\}$.

Wir erweitern die bisherige Folge ϕ_1 durch

$\phi_2 := \forall x \forall y \phi \to \forall y \phi \quad \in AX2$, da

$\forall x \forall y \phi \to \forall y \phi [x \leftarrow x] \in AX2$

$\phi_3 := \forall y \phi \to \phi \quad \in AX2$

$\phi_4 := \forall y \phi$ Modus ponens

$\phi_5 := \phi$ Modus ponens

$\phi_6 := \forall x \phi$ gerechtfertigte Verallgemeinerung
(Beachte, dass x nicht in ϕ_1 frei vorkommt)

$\phi_7 := \forall y \forall x \phi$ gerechtfertigte Verallgemeinerung

Also haben wir gezeigt:

$$\{\forall x \forall y \phi\} \vdash \forall y \forall x \phi$$

$$\Rightarrow \quad \vdash \forall x \forall y \phi \to \forall y \forall x \phi.$$

Satz 4.4

b) Beh.: $\vdash \forall x \phi \to \exists x \phi$

Bew.: Setze $\phi_1 := \forall x \phi$ und $\Delta := \{\phi_1\}$.

Wir erweitern die Folge ϕ_1 durch

$\phi_2 := (\forall x \phi) \to \phi \qquad \in AX2$

$\phi_3 := \phi$ Modus ponens

$\phi_4 := \forall x \neg\phi \to \neg\phi \qquad \in AX2$

$\phi_5 := \big(\forall x \neg\phi \to \neg\phi\big) \to (\phi \to \exists x \phi) \quad \in AX0$
(Beachte, dass $\exists$ eine Abkürzung ist.)

$\phi_6 := \phi \to \exists x \phi$ Modus ponens

$\phi_7 := \exists x \phi$ Modus ponens

c) Beh.: Seien ϕ und ψ zwei Ausdrücke, die bis auf folgenden Unterschied identisch sind:
ϕ hat genau an denjenigen Positionen freie Vorkommen von x in denen ψ freie Vor-Kommen von y hat. Dann gilt

$$\vdash \forall x \phi \to \forall y \psi .$$

Bew.:

Setze $\phi_1 := \forall x \phi$ und $\Delta := \{\phi_1\}$.
Wir erweitern die Folge ϕ_1 durch:

$\phi_2 := \forall x \phi \to \psi$ $\quad \in AX2$, da $\psi = \phi[x \leftarrow y]$.
$\phi_3 := \psi$ $\quad$ Modus ponens
$\phi_4 := \forall y \psi$ $\quad$ gerechtfertigte Verallgemeinerung (Beachte: y ist nicht frei in $\forall x \phi$.

■

◆

Der nächste Satz zeigt, dass unser Beweissystem nur gültige Konsequenzen beweist.

Satz 4.7

Wenn $\Delta \vdash \phi$, dann $\Delta \models \phi$.

Beweis: ... Übung

■

Die umgekehrte Richtung ist der berühmte Gödel'sche Vollständigkeitssatz der Prädikatenlogik.

Satz 4.8 (ohne Beweis)

Wenn $\Delta \models \phi$, dann $\Delta \vdash \phi$.