

Grundlagen und Diskrete Mathematik

Inhaltsverzeichnis

1	Grundbegriffe und elementare Logik	3
1.1	Aussagen, Prädikate und Quantoren	4
1.2	Grundlegende Beweistechniken	13
2	Syntax und Semantik am Beispiel der formalen Aussagenlogik	17
2.1	Syntax der Aussagenlogik	19
2.2	Semantik der Aussagenlogik	21
3	Mengen	34
3.1	Der Mengenbegriff und grundlegende Definitionen	35
3.2	Grössenvergleiche von unendlichen Mengen	47
4	Relationen	56
4.1	Grundlagen	57
4.2	Äquivalenzrelationen	62
4.3	Ordnungsrelationen	69
5	Rekursive Strukturen und die natürlichen Zahlen	75
5.1	Die grundlegende Struktur der natürlichen Zahlen	76
5.2	Vom Induktionsbeweis zum rekursiven Algorithmus	82
5.3	Rekursive Definitionen	86
6	Elementare Zahlentheorie	91
6.1	Teilbarkeit und Euklidischer Algorithmus	93
6.2	Primzahlen	101
6.3	Modulare Arithmetik	104
6.3.1	Chinesischer Restsatz	109

1 Grundbegriffe und elementare Logik

Prolog

Am Anfang aller Logik steht...

Wenn “Doken” stets “derig” sind und wenn es “Raken” gibt die auch “Doken” sind, dann gibt es derige Raken und alle underigen Raken sind keine Doken.

...die Erkenntnis, dass gewisse Argumente unabhängig von deren Inhalt aber aufgrund ihrer Struktur als eindeutig schlüssig/korrekt identifizierbar sind. Dieses Kapitel gibt Ihnen eine informelle Einführung in die Prädikatenlogik.

Beispiele für Anwendungen in der Informatik

- Grundlage für die Entwicklung einer soliden “Theorie der Informatik”.
- Künstliche Intelligenz, Wissensrepräsentation, Expertensysteme.
- Allgegenwärtig in der Programmierung (z.B. “if ... then ... else...”-Befehle).
- Formale Verifikation der Korrektheit von Programmen.

Lernziele

Sie kennen die Konzepte von

- Aussagen und Prädikaten.
- universeller und existenzieller Quantifikation.

Sie verstehen wie

- durch Implikation, Äquivalenz, Negation, Konjunktion und Disjunktion neue Aussagen und Prädikate aus bereits bestehenden gewonnen werden.
- durch Quantifikation von Prädikaten neue Aussagen und Prädikate gewonnen werden.

Sie sind in der Lage

- natürlichsprachliche (mathematische) Aussagen in der Sprache der Prädikatenlogik zu formalisieren.

- mittels Fallunterscheidung, Widerspruchsargumenten und Kontraposition einfache mathematische Tatsachen zu beweisen.

Sie bewerten

- einfache Beweise und Argumente bezüglich ihrer Korrektheit und Stringenz.

Literatur und Links

Ergänzende Literatur:

- [3] Kapitel 1.2 bis 1.4.
- [2] Kapitel 2.
- [1] Kapitel 2.

Weiterführende Literatur:

- [5] ganzes Buch.

Nützliche Links:

- http://de.wikipedia.org/wiki/Pr%C3%A4dikatenlogik_erster_Stufe
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Logik
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Logik:_Anwendung
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Logik:_Quantor
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Beweis

1.1 Aussagen, Prädikate und Quantoren

Wir werden im folgenden Abschnitt auf pragmatische Art und Weise die grundlegenden Konzepte der Logik und Mathematik kennenlernen. Um nicht nur langweilige Beispiele machen zu können, werden wir in diesem Kapitel auf gewisse mathematische Begriffe wie z.B. “natürliche Zahlen” ($0, 1, 2, \dots$) oder “Primzahlen” ($2, 3, 5, 7, 11, \dots$) zurückgreifen, ohne diese vorher sauber eingeführt zu haben. Die Anschauung, welche Sie von der Schule mitbringen, sollte aber ausreichen um die Beispiele zu verstehen.

Definition 1. Unter einer *Aussage* wollen wir ein “sprachliches Gebilde” verstehen, welchem zumindest im Prinzip ein Wahrheitswert “wahr” oder “falsch” zugeordnet werden kann.

Beispiel 1. Einige Beispiele für Aussagen mit ihren Wahrheitswerten:

- a) “Esel haben lange Ohren.” (wahr)
- b) “Jede natürliche Zahl ist entweder durch 2 oder durch 3 teilbar.” (falsch)
- c) “Es gibt unendlich viele natürliche Zahlen.” (wahr)
- d) “ $3 + 4 = 106$ ” (falsch)

Bemerkung 1. Wir sagen, dass eine Variable frei¹ in einem Ausdruck $A(x)$ vorkommt, falls diese weder für einen noch für eine Menge von konkreten Werten steht, sondern einen reinen “Platzhalter” darstellt. Beispiele in denen die Variable x frei vorkommt sind: “ $x < 3$ ” oder “ x ist ein Tisch”. Im Gegensatz dazu kommt x in “alle x die durch 4 teilbar sind, sind gerade” nicht frei vor weil in dieser Aussage die Gesamtheit (Menge) aller möglichen Belegungen von x betrachtet wird. Ein Prädikat ist nun im wesentlichen eine Aussage, die freie Variablen enthält:

Definition 2. Es sei n eine natürliche Zahl. Ein sprachliches Gebilde, in dem n viele Variablen (frei) vorkommen und das bei Belegung aller (freien) Variablen in eine Aussage übergeht, nennen wir ein *n -stelliges Prädikat*.

Bemerkung 2. Ist $A(x)$ ein Prädikat und ist Ob ein (mathematisches) Objekt so, dass $A(Ob)$ eine wahre Aussage ist, dann sagen wir, dass das Prädikat (manchmal auch die Eigenschaft) A auf Ob zutrifft. Das Prädikat $x > 100$ trifft zum Beispiel auf die Zahl (Objekt) 232 zu, weil $232 > 100$ eine wahre Aussage ist.

Bemerkung 3. Aussagen sind 0-stellige Prädikate.

Beispiel 2. Einige Beispiele für Prädikate:

- a) $U(p) :=$ ² “Die Person p hat Übergewicht.”
- b) $T(x) :=$ “Die Natürliche Zahl x ist durch 21 teilbar.”
- c) $P(r) :=$ “ $r > 0$ ”
- d) $Q(x, y) :=$ “Wenn $x < y$ ist, dann gilt $x^2 + 14x - 15 = 0$ ”

Die Aussagen

$T(42)$	$P(7)$	$Q(17, 17)$
$T(357)$	$P(1)$	$Q(1, 17)$

sind alle wahr. Deshalb können wir, entsprechend der vorhergehenden Bemerkung, z.B. “ T trifft auf 42” zu oder auch “7 hat die Eigenschaft P ” sagen.

¹Mehr dazu erfahren Sie im Abschnitt über Quantoren.

²Die Zeichenfolge “ $:=$ ” steht für “ist definiert als” oder “ist per Definition gleich”.

Junktoren

Aus gegebenen Aussagen lassen sich durch Verknüpfung neue komplexere Aussagen gewinnen. Betrachten wir zum Beispiel die Aussagen

$A := \text{“78 ist keine Primzahl”}$

und

$B := \text{“15 ist keine Primzahl”},$

so können wir eine neue Aussage, nennen wir sie C , betrachten. C soll ausdrücken, dass sowohl A als auch B wahr ist, d.h.

$C := \text{“78 ist keine Primzahl und 15 ist keine Primzahl”}$

oder etwas anders formuliert (aber mit gleichem Wahrheitswert)

$C := \text{“weder die 15 noch die 78 ist eine Primzahl”}.$

Wir werden nun einige abkürzende Schreibweisen einführen um bequem über solche zusammengesetzten Aussagen sprechen zu können.

Definition 3. Es seien A und B beliebige Prädikate. Wir führen folgende abkürzende Schreibweisen ein:

- $\neg A$ (gesprochen: Nicht A) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn A falsch ist.
- $A \wedge B$ (gesprochen: A und B) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn sowohl A als auch B wahr sind.
- $A \vee B$ (gesprochen: A oder B) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn A wahr ist oder B wahr ist (oder beide wahr sind).
- $A \Rightarrow B$ (gesprochen: A impliziert B) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn $\neg A \vee B$ wahr ist.
- $A \Leftrightarrow B$ (gesprochen: A äquivalent B) ist das Prädikat, welches (für jede Belegung) genau dann wahr ist, wenn $A \Rightarrow B$ und $B \Rightarrow A$ wahr sind.

Die Zeichen $\neg, \Rightarrow, \wedge$ und \vee nennen wir *Junktoren*.

Bemerkung 4. Das Prädikat $A \Rightarrow B$ besagt, dass in jedem Fall in dem A wahr ist auch B wahr sein muss. Die Äquivalenz zweier Prädikate besagt also, dass diese stets denselben Wahrheitswert haben. Umgangssprachlich wird oft vorausgesetzt, dass zwischen den

Prädikaten A und B ein “inhaltlicher Zusammenhang” bestehen muss, damit $A \Rightarrow B$ gelten kann. Dies ist in der mathematischen Logik nicht der Fall. Die Aussagen

Es gibt Einhörner \Rightarrow 8 ist eine Primzahl

und

Spinat ist grün \Rightarrow 2 ist eine Primzahl

sind beispielsweise beide (mathematisch gesehen) war.

Beispiel 3. Gegeben sind die Aussagen A und B :

A := “Alle Hasen haben lange Ohren.”

B := “Es gibt Hasen mit kurzen Beinen.”

Es gilt:

- a) $\neg A$ entspricht “Es gibt mindestens einen Hasen, der keine langen Ohren hat.”
- b) $A \wedge \neg B$ entspricht “Alle Hasen haben lange Ohren und keine kurzen Beine.”
- c) $A \Rightarrow B$ entspricht “Wenn alle Hasen lange Ohren haben, dann gibt es Hasen mit kurzen Beinen.”

Übung 1. Negieren Sie umgangssprachlich folgende Aussagen (so präzise wie möglich).

- a) Alle Autos haben vier Räder.
- b) Zwillinge haben stets die identische Haarfarbe.
- c) Es gibt flugunfähige Vögel.
- d) Alle Dinosaurier sind ausgestorben.

Lösung.

- a) Es gibt Autos, die nicht vier Räder haben.
- b) Es gibt mindestens ein Zwillingspaar mit verschiedenen Haarfarben.
- c) Alle Vögel können fliegen.
- d) Mindestens ein Dinosaurier lebt noch.

Wir werden nun einige Umformungsregeln betrachten, die unterschiedlich zusammengesetzte Aussagen, rein aufgrund ihrer logischen Struktur, als äquivalent deklarieren. Wir werden diese Regeln als evident betrachten und sie ohne Beweis übernehmen. Diese Regeln werden es uns erlauben mit Aussagen und Prädikaten zu “rechnen”.

Bemerkung 5 (Junktorenregeln). Seien A, B und C beliebige Aussagen. Es gelten folgende Äquivalenzen

- Regel der doppelten Negation:

$$\neg\neg A \Leftrightarrow A$$

- Kommutativität:

$$A \wedge B \Leftrightarrow B \wedge A \quad \text{und} \quad A \vee B \Leftrightarrow B \vee A$$

- Assoziativität:

$$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$$

$$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$$

- Distributivität:

$$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$$

$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$$

- Regeln von De Morgan:

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$$

$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$$

Beispiel 4 (Kontraposition). Wir können die eben aufgestellten Rechenregeln dazu verwenden um wiederum neue Tatsachen abzuleiten. Unter anderem folgt daraus das sogenannte Prinzip der *Kontraposition*. Dieses Prinzip besagt, dass $A \Rightarrow B$ äquivalent ist zu $\neg B \Rightarrow \neg A$. Wollen wir dies nun mit unseren Rechenregeln nachvollziehen, so beginnen wir mit $A \Rightarrow B$ und wenden nacheinander verschiedene Regeln an um schlussendlich $\neg B \Rightarrow \neg A$ zu erhalten:

$$\begin{array}{ll} A \Rightarrow B & \\ \Leftrightarrow \neg A \vee B & \text{(Definition von } A \Rightarrow B) \\ \Leftrightarrow \neg\neg(\neg A \vee B) & \text{(Doppelte Negation)} \\ \Leftrightarrow \neg(\neg\neg A \wedge \neg B) & \text{(De Morgan)} \\ \Leftrightarrow \neg(A \wedge \neg B) & \text{(Doppelte Negation)} \\ \Leftrightarrow \neg(\neg B \wedge A) & \text{(Kommutativität)} \\ \Leftrightarrow \neg\neg B \vee \neg A & \text{(De Morgan)} \\ \Leftrightarrow \neg B \Rightarrow \neg A & \text{(Definition von } \neg B \Rightarrow \neg A) \end{array}$$

Quantoren

Quantoren sind Symbole anhand derer wir aus Prädikaten neue Prädikate oder Aussagen gewinnen können. Wir betrachten das Beispiel des Prädikates

$$A(x) := \text{“}x \text{ ist eine Primzahl und } x \text{ ist ein Teiler von } 24\text{”}$$

und die Aussage

$$B := \text{“es gibt eine Primzahl welche ein Teiler von } 24 \text{ ist”}$$

mit anderen Worten,

$$B := \text{“es existiert ein } x \text{ mit } A(x)\text{”}.$$

Wir sagen, dass B aus $A(x)$ durch existenzielle Quantifizierung über x entsteht.

Andererseits können wir aus dem Prädikat $A(x)$ aber auch die (offensichtlich falsche) Aussage

$$C := \text{“alle Zahlen sind Primzahlen und ein Teiler von } 24\text{”}$$

konstruieren. Diese ist gleichbedeutend mit

$$C := \text{“alle Zahlen } x \text{ erfüllen } A(x)\text{”}.$$

Wir sagen, dass C aus $A(x)$ durch universelle Quantifizierung entsteht³.

Definition 4. Es sei M eine Menge von Objekten. Ist $A(x)$ ein Prädikat, dann bedeutet

- $\forall x A(x)$ (gesprochen: Für alle x gilt $A(x)$), dass A auf jedes (mathematische) Objekt zutrifft.
- $\forall x \in M A(x)$ (gesprochen: Für alle x aus M gilt $A(x)$), dass A auf jedes Objekt aus M zutrifft.
- $\exists x A(x)$ (gesprochen: Es gibt ein x mit $A(x)$), dass es (mindestens) ein Objekt O gibt, auf welches A zutrifft.
- $\exists x \in M A(x)$ (gesprochen: Es gibt ein x aus M mit $A(x)$), dass es (mindestens) ein Objekt aus M gibt, auf welches A zutrifft.

Die Symbole \forall und \exists heissen *Allquantor* und *Existenzquantor*.

Bemerkung 6. Prädikate von der Form $\forall x \forall y A(x, y)$ und $\exists x \exists y A(x, y)$ kürzen wir mit $\forall x, y A(x, y)$ und $\exists x, y A(x, y)$ ab.

³Obwohl in den Aussagen B und C formal die Variable x vorkommt, steht sie nicht als Platzhalter für ein einzusetzendes Objekt, sondern “läuft” über die Gesamtheit aller möglichen Objekte. Wir sagen, dass die Variable nicht frei sondern durch einen Quantor gebunden ist.

Bemerkung 7. Ein n -stelliges Prädikat wird durch Quantifizierung stets zu einem neuen $n - 1$ stelligen Prädikat.

Beispiel 5. Einige quantifizierte Aussagen mit ihren Wahrheitswerten:

- a) Es sei S die Menge aller Schweine und $R(x)$ das Prädikat “ x ist rosa”. Es gilt

$$“\exists x \in S R(x)” \Leftrightarrow “\text{es gibt rosarote Schweine}”.$$

Diese Aussage ist offensichtlich wahr. Wenn wir nun die Allquantifizierung betrachten, so erhalten wir

$$“\forall x \in S R(x)” \Leftrightarrow “\text{alle Schweine sind rosa}”.$$

Dies ist eine falsche Aussage, da etwa Wildschweine einerseits Elemente von S sind aber andererseits R nicht erfüllen, da sie nicht rosa sind.

- b) Wir wollen nun die Aussage

$$A := “\text{alle Informatiker können programmieren}”$$

mit Quantoren ausdrücken. Wir definieren dazu zuerst das Prädikat

$$B(x) := “x \text{ kann programmieren}”.$$

Wir haben nun zwei mögliche Vorgehensweisen. Einerseits können wir die Menge I aller Informatiker betrachten und kommen dann mittels der Aussage

$$\forall x \in I B(x)$$

zum Ziel. Andererseits können wir auch A umformulieren als “alles was ein Informatiker ist kann programmieren” und erhalten die gewünschte Aussage mit uneingeschränkter Quantifikation

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

Diesen Zusammenhang zwischen eingeschränkter und uneingeschränkter Quantifikation werden wir in der nächsten Bemerkung noch allgemein formulieren.

Übung 2. Es seien $P(x)$ ein einstelliges und $Q(y, z)$ ein zweistelliges Prädikat. Formulieren Sie:

- a) Es gibt genau ein x mit $P(x)$.
- b) Es gibt mindestens zwei Dinge mit der Eigenschaft P .
- c) Es gibt höchstens ein x mit $P(x)$.
- d) Wenn $P(x)$ und $P(y)$ gilt, dann gilt stets auch $Q(x, y)$.
- e) Für kein x gilt $Q(x, x)$.

Lösung. a) $\exists x (P(x)) \wedge \forall y, z (P(y) \wedge P(z) \Rightarrow y = z)$
b) $\exists x, y (P(x) \wedge P(y) \wedge x \neq y)$
c) $\neg \exists x, y (P(x) \wedge P(y) \wedge x \neq y)$
d) $\forall x, y (P(x) \wedge P(y) \Rightarrow Q(x, y))$
e) $\forall x \neg Q(x, x)$

Ähnlich wie mit den durch Junktoren zusammengesetzten Aussagen, stellen wir nun auch “Rechenregeln” zum Umgang mit Quantoren zusammen.

Bemerkung 8 (Quantorenregeln). Ist $A(x)$ ein Prädikat und K eine Menge, welche mindestens ein Element enthält, so gelten folgende Äquivalenzen:

a) Vertauschungsregel für unbeschränkte Quantoren

$$\forall x A(x) \Leftrightarrow \neg \exists x \neg A(x)$$

b) Vertauschungsregel für beschränkte Quantoren

$$\forall x \in K A(x) \Leftrightarrow \neg \exists x \in K \neg A(x)$$

c) Beschränkter und unbeschränkter Allquantor

$$\forall x \in K A(x) \Leftrightarrow \forall x (x \in K \Rightarrow A(x))$$

d) Beschränkter und unbeschränkter Existenzquantor

$$\exists x \in K A(x) \Leftrightarrow \exists x (x \in K \wedge A(x))$$

Beispiel 6. Mit den Rechenregeln für Quantoren und den Rechenregeln für Junktoren können wir wieder neue Tatsachen (=Wahrheitswerte neuer Aussagen) herleiten. Als Beispiel betrachten wir das Duale zur Vertauschungsregel für unbeschränkte Quantoren, nämlich:

$$\exists x A(x) \Leftrightarrow \neg \forall x \neg A(x)$$

Wir beginnen also mit $\exists x A(x)$ und erhalten durch Anwenden der Rechenregeln $\neg \forall x \neg A(x)$.

$$\begin{aligned} & \exists x A(x) \\ \Leftrightarrow & \neg \neg \exists x A(x) && \text{(Doppelte Negation)} \\ \Leftrightarrow & \neg (\neg \exists x A(x)) \\ \Leftrightarrow & \neg (\neg \exists x \neg (\neg A(x))) && \text{(Doppelte Negation)} \\ \Leftrightarrow & \neg (\forall x \neg A(x)) && \text{(Vertauschungsregel)} \end{aligned}$$

Warnung. Wir haben keine Distributionsregel mit Quantoren und Junktoren. Die Äquivalenzen

$$\forall x A(x) \vee \forall x B(x) \Leftrightarrow \forall x (A(x) \vee B(x))$$

und

$$\exists x A(x) \wedge \exists x B(x) \Leftrightarrow \exists x (A(x) \wedge B(x))$$

gelten im Allgemeinen **nicht**. Wir betrachten dazu als Gegenbeispiel die Aussagen

$$A(x) := \text{“}x \text{ ist eine gerade natürliche Zahl“}$$

und

$$B(x) := \text{“}x \text{ ist eine ungerade natürliche Zahl“}.$$

Die Aussage

$$\exists x A(x) \wedge \exists x B(x)$$

besagt also in diesem Fall, dass es mindestens eine gerade natürliche Zahl gibt und dass es ebenfalls mindestens eine ungerade natürliche Zahl gibt. Diese Aussage ist offensichtlich wahr. Die Aussage

$$\exists x (A(x) \wedge B(x))$$

besagt nun aber, dass es eine natürliche Zahl gibt, welche “gleichzeitig” gerade und ungerade ist, was offensichtlich falsch ist. Die beiden Aussagen sind also nicht äquivalent.

Übung 3. Geben Sie Prädikate $P(x)$ und $Q(x)$ an, so dass $\forall x P(x) \vee \forall x Q(x)$ falsch ist aber $\forall x (Q(x) \vee P(x))$ wahr ist.

Lösung. Zum Beispiel (im Kontext von allen Menschen)

$$P(x) := \text{“}x \text{ ist eine Frau“}$$

und

$$Q(x) := \text{“}x \text{ ist ein Mann“}.$$

Die Aussage $\forall x P(x) \vee \forall x Q(x)$ bedeutet, dass jeder Mensch eine Frau ist oder jeder Mensch ein Mann ist, diese Aussage ist falsch. Die Aussage $\forall x (P(x) \vee Q(x))$ ist hingegen die wahre Behauptung, dass jeder Mensch entweder ein Mann oder eine Frau ist.

Übung 4. Gruppieren Sie folgende Aussagen so, dass in jeder Gruppe alle Aussagen äquivalent sind und keine äquivalenten Aussagen in verschiedenen Gruppen sind.

1. $\forall x (P(x) \Rightarrow Q(x))$
2. $\exists x (P(x) \Leftrightarrow Q(x))$

3. $\forall x (Q(x) \Rightarrow P(x))$
4. $\forall x (\neg P(x) \Rightarrow \neg Q(x))$
5. $\forall x (\neg Q(x) \Rightarrow \neg P(x))$
6. $\neg \exists x (\neg \neg Q(x) \wedge \neg P(x))$
7. $\neg \exists x (P(x) \wedge \neg Q(x))$
8. $\exists x (P(x) \wedge Q(x)) \vee \exists x (\neg P(x) \wedge \neg Q(x))$
9. $\forall x \exists y (P(x) \wedge P(y))$

Lösung. Die Aussagen 1., 5., 7. und 3., 4., 6. und 2., 8. sind jeweils untereinander äquivalent. Es gibt keine weiteren Äquivalenzen.

1.2 Grundlegende Beweistechniken

Wir wollen im Folgenden einige der elementarsten Standardbeweistechniken besprechen. Natürlich sollen diese Techniken in etwas komplexeren Beweisen auch beliebig kombiniert werden dürfen. Wir könnten beispielsweise zum Beweis einer Äquivalenz die eine Richtung durch Kontraposition und die andere Richtung direkt oder durch Widerspruch beweisen.

Direkter Beweis einer Implikation

Problemstellung: Es gilt eine Aussage $A \Rightarrow B$ zu beweisen.

Lösungsstrategie: Wir geben, basierend auf der Annahme, dass A wahr ist, *zwingende* Argumente für die Richtigkeit von B .

Beispiel: Wir zeigen, wenn x und y gerade (natürliche) Zahlen sind, dann ist auch $x \cdot y$ gerade.

Beweis. Wir nehmen an x, y seien (irgendwelche) gerade natürliche Zahlen (Voraussetzung). Da x, y gerade sind, gibt es natürliche Zahlen n_x und n_y so, dass

$$x = 2 \cdot n_x \qquad y = 2 \cdot n_y$$

gilt. Für das Produkt $x \cdot y$ gilt folglich

$$x \cdot y = (2 \cdot n_x) \cdot (2 \cdot n_y) = 2 \cdot (n_x \cdot 2 \cdot n_y)$$

und ist somit dass $x \cdot y$ ein vielfaches von 2 also gerade ist. □

Beweis durch Widerspruch

Problemstellung: Es gilt eine Aussage A zu beweisen.

Lösungsstrategie: Nehmen Sie an, die Aussage A wäre falsch und benützen Sie diese Annahme um einen Widerspruch herzuleiten. Leiten Sie also unter der Annahme der Falschheit von A eine Aussage her von der bereits bekannt ist, dass sie falsch ist oder im Widerspruch zur Annahme steht.

Beispiel: $A :=$ "Es gibt keine grösste natürliche Zahl"

Beweis. Wir nehmen an, dass es eine grösste natürliche Zahl gibt, wir nennen sie m . Wir wissen, dass für jede natürliche Zahl n gilt, dass einerseits $n + 1$ ebenfalls eine natürliche Zahl ist und dass andererseits $n < n + 1$ erfüllt ist. Wir wenden dies auf die natürliche Zahl m an und erhalten damit eine grössere natürliche Zahl (nämlich $m + 1$). Dies steht jedoch im Widerspruch zu unserer ursprünglichen Annahme, dass m die grösste natürliche Zahl sei. \square

Beweis durch (Gegen-) Beispiel

Problemstellung: Es gilt zu zeigen, dass eine bestimmte Eigenschaft nicht auf alle Objekte (aus einem Kontext) zutrifft.

Lösungsstrategie: Geben Sie konkret ein Objekt an, welches die erwähnte Eigenschaft nicht besitzt.

Beispiel: "Nicht jede natürliche Zahl ist eine Quadratzahl⁴."

Beweis. Weil die Funktion $f(x) = x^2$ monoton ist (später mehr dazu) und weil $1 \cdot 1 < 2 < 2 \cdot 2$ gilt, kann die Zahl 2 nicht als Quadrat von einer natürlichen Zahl geschrieben werden. Somit ist 2 das (oder ein) gesuchte Gegenbeispiel. \square

Beweis durch Kontraposition

Problemstellung: Es gilt eine Aussage von der Form $A \Rightarrow B$ zu beweisen.

Lösungsstrategie: Beweisen Sie die Kontraposition $\neg B \Rightarrow \neg A$.

Beispiel: "Für jede natürliche Zahl n gilt: $(n^2 + 1 = 1) \Rightarrow (n = 0)$ "

Beweis. Ist $n \neq 0$ so folgt, dass auch $n^2 \neq 0$ gilt. Dies impliziert, dass für jede weitere natürliche Zahl m die Ungleichung $n^2 + m \neq m$ erfüllt ist. Insbesondere gilt daher, dass (der Fall $m = 1$) $n^2 + 1 \neq 1$ gilt. \square

⁴Von der Form x^2 für eine geeignete natürliche Zahl x .

Beweis einer Äquivalenz

Problemstellung: Es gilt eine Aussage von der Form $A \Leftrightarrow B$ zu beweisen.

Lösungsstrategie: Beweisen Sie $B \Rightarrow A$ sowie $A \Rightarrow B$.

Beispiel 1: “Für jede natürliche Zahl n gilt: $(n^2 + 1 = 1) \Leftrightarrow (n = 0)$ ”

Beweis. Wir haben in den vorhergehenden Beispielen bereits $A \Rightarrow B$ bewiesen, wir müssen also nur noch $B \Rightarrow A$ beweisen. Wir nehmen also B an, es gelte also $n = 0$. Daraus folgt $n^2 = n \cdot n = 0 \cdot 0 = 0$ und somit $n^2 + 1 = 0 + 1 = 1$. \square

Beispiel 2: “Für jede natürliche Zahl n gilt: $(n \text{ ist gerade}) \Leftrightarrow (n^2 \text{ ist gerade})$.”

Beweis. Wir beweisen zuerst $(n \text{ ist gerade}) \Rightarrow (n^2 \text{ ist gerade})$. Wir nehmen also an, dass n eine gerade natürliche Zahl ist. Daraus folgt, dass es eine weitere natürliche Zahl k mit $n = 2 \cdot k$ gibt. Es folgt, dass

$$n^2 = n \cdot n = 2 \cdot k \cdot 2 \cdot k = 2 \cdot (k \cdot 2 \cdot k)$$

offenbar gerade ist.

Nun wollen wir noch die “Rückrichtung” $(n^2 \text{ ist gerade}) \Leftarrow (n \text{ ist gerade})$ beweisen. Wir wollen diese Richtung durch Kontraposition beweisen und nehmen also an, dass n ungerade sei. Es folgt, dass es eine natürliche Zahl k gibt mit $2 \cdot k - 1 = n$. Also ist $n^2 = (2 \cdot k - 1)(2 \cdot k - 1) = 4k^2 - 4k + 1 = 4(\underbrace{k^2 - k}_{\text{gerade}}) + 1$ ungerade. \square

Übung 5. Beweisen Sie: Jeder Geldbetrag von mindestens 4 Cents lässt sich allein mit Zwei- und Fünfcentstücken bezahlen.

Hinweis: Machen Sie eine Fallunterscheidung ob der zu bezahlende Betrag gerade oder ungerade ist.

Lösung. Zuerst bemerken wir, dass jeder gerade Betrag mit Zweicentstücken bezahlt werden kann. Ist der gegebene Betrag, sagen wir x cent, ungerade, so muss er mindestens fünf Cent entsprechen, es gilt also $x \geq 5$. Weil x ungerade ist, ist $x - 5$ gerade. Wie wir bereits festgestellt haben können wir diesen geraden Betrag mit lauter Zweicentstücken bezahlen. Der gesamte Betrag kann also mit einem Fünfcentstück und Zweicentstücken bezahlt werden.

Übung 6. Beweisen Sie, dass man $\sqrt{2}$ nicht als (gekürzten) Bruch schreiben kann.

Hinweis: Wenden Sie ein Widerspruchsargument an.

Lösung. Wir nehmen an, dass $\sqrt{2}$ als gekürzter Bruch dargestellt werden kann und leiten daraus einen Widerspruch her. Es seien a, b teilerfremde ganze Zahlen mit

$$\frac{a}{b} = \sqrt{2}.$$

Es folgt:

$$2 = \sqrt{2}^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$$

und somit

$$a^2 = 2b^2.$$

Die Zahl a^2 muss also gerade sein. Daraus folgt, dass auch a selbst gerade ist. Weil a gerade ist, gibt es eine ganze Zahl c mit der Eigenschaft

$$a = 2c.$$

Daraus folgt

$$2b^2 = a^2 = (2c)^2 = 4c^2$$

und damit

$$b^2 = 2c^2.$$

Anhand der letzten Gleichung sehen wir, dass b^2 und somit auch b gerade sein muss, dies widerspricht aber der Annahme, dass die Zahlen a und b teilerfremd seien.

2 Syntax und Semantik am Beispiel der formalen Aussagenlogik

Prolog

Wir betrachten Wörter die aus den Zeichen z, P, G gebildet werden können, also zum Beispiel $zzzPPGPGP$, zzz oder $zzPzzzGzzzzz$. Da uns aber nicht alle diese Wörter interessieren, schränken wir uns auf “zulässige” Wörter ein, die wir folgendermassen definieren: Ein Wort ist zulässig, wenn

- genau ein G und ein P darin vorkommen und das P vor dem G vorkommt.

Zulässige Wörter (wir nennen diese jetzt auch zPG -Wörter) sind also von der Form

$$\dots P \dots G \dots$$

wobei “ \dots ” für jeweils eine beliebige (nicht notwendigerweise von Null verschiedener) Anzahl z steht. Beispiele von zulässigen Wörtern sind $zzzPzzGzzzzz$, PzG oder $PzGz$. Die Regeln, die wir eingeführt haben um zulässige von unzulässigen Wörtern zu unterscheiden, sind Teil der *Syntax* unserer zPG -Sprache. Obwohl wir jetzt eine primitive “Grammatik” für unsere Sprache haben, bleibt völlig unklar was wir mit dieser Sprache aussagen wollen – was die Bedeutung oder *Semantik* von zPG -Wörtern ist. Wie können wir also zulässige Wörter interpretieren? Haben Sie eine Idee? Schauen wir was passiert, wenn wir zPG -Wörter wie Aussagen als Wahrheitswerte “wahr” oder “falsch” interpretieren. Wir betrachten die (partielle) Zuordnung

zPG-Wort		Wahrheitswert
$zzzPzGzzz$	\longleftrightarrow	falsch
PG	\longleftrightarrow	wahr
$zPzGzz$	\longleftrightarrow	wahr
$PzzGz$	\longleftrightarrow	falsch

Haben Sie eine Idee, wie wir diese Zuordnung von zPG -Wörtern zu Wahrheitswerten vervollständigen können? Nehmen Sie sich einen Moment Zeit darüber nachzudenken, bevor Sie weiter lesen. Wenn wir an elementare Arithmetik denken, so könnten¹ wir in einem zPG -Wort zum Beispiel die Symbole P, G als $+$ und $=$ und Blöcke von der Form $z \dots z$ als unärcodierte natürliche Zahlen interpretieren. Unter dieser Interpretation ergibt sich das folgende Bild:

¹Das heisst nicht, dass es keine anderen “sinnvollen” Interpretationen von zPG -Wörtern gibt, wir haben uns hier willkürlich festgelegt.

zPG-Wort		Wahrheitswert
zzzPzGzzz	\longleftrightarrow	$3 + 1 = 3$ (falsch)
PG	\longleftrightarrow	$0 + 0 = 0$ (wahr)
zPzGzz	\longleftrightarrow	$1 + 1 = 2$ (wahr)
PzzGz	\longleftrightarrow	$0 + 2 = 1$ (falsch)

Nun erweitern wir unsere zPG-Sprache (die Menge aller zPG-Wörter) zu einem “formalen System”, indem wir rein syntaktische Regeln angeben “die zPG-Reduktion”, um aus zPG-Wörtern neue zPG-Wörter zu generieren.

- Ist das zu reduzierende Wort von der Form $z \dots Pz \dots Gzz \dots$, dann reduzieren wir nach $\dots P \dots G \dots$.
- Ist das zu reduzierende Wort von der Form $Pz \dots Gz \dots$, dann reduzieren wir nach $P \dots G \dots$.
- Ist das zu reduzierende Wort von der Form $z \dots PGz \dots$, dann reduzieren wir nach $\dots PG \dots$.
- Trifft keiner der oben genannten Fälle zu, dann ist das Wort vollständig reduziert.

Was passiert, wenn wir ein “wahres” zPG-Wort reduzieren? Was passiert, wenn wir ein zPG-Wort reduzieren, das nicht “wahr” ist?

Die wahren zPG-Wörter sind genau diejenigen, deren vollständig reduzierte Form das Wort PG ist.

Wir können also sagen, dass eine Reduktion eines zPG-Wortes nach PG einem formalen “Beweis” im zPG-System vom ursprünglichen Wort entspricht. Eine vollständige Reduktion, die in einem Wort endet, welches von PG verschieden ist, ist in diesem Sinne eine “formale Verwerfung” vom Ursprungswort. Insbesondere haben wir einen syntaktischen Kalkül (Reduktion terminiert immer), der von einem zPG-Wort entscheidet, ob dieses wahr ist. Man sagt in diesem Fall, dass das System *entscheidbar* und vollständig (bzgl. der gegebenen Semantik) ist. Dies ist eine starke Eigenschaft, die für kompliziertere Systeme im Allgemeinen nicht gilt.

Noch ein paar Beispiele für die syntaktische und die semantische Ebene:

Syntax		Semantik
Partitur	\longleftrightarrow	Musik (Schallwellen)
Java Code	\longleftrightarrow	Verhalten eines Computers
Terme einer math. Theorie	\longleftrightarrow	Math. Objekte
Aussagenlogische Formeln	\longleftrightarrow	Boolesche Funktionen
Peano Axiome	\longleftrightarrow	Die Struktur $(\mathbb{N}, +, \cdot)$
Feynman-Diagramm	\longleftrightarrow	Wechselwirkungen

Beispiele für Anwendungen in der Informatik

- Künstliche Intelligenz, Wissensrepräsentation und Expertensysteme
- Theoretische Informatik ($P = NP$ -Frage, SAT, ...)
- Regeltechnik und Simulation, Beispiel: http://www.bmwgroup.com/d/0_0_www_bmwgroup_com/forschung_entwicklung/science_club/veroeffentlichte_artikel/2003/news200316.html

Lernziele

Sie kennen die

- Syntax der Aussagenlogik.
- Semantik der Aussagenlogik.

Sie verstehen

- wie die Begriffe Syntax und Semantik zusammenhängen.
- was der Wahrheitswert einer aussagenlogischen Formel ist.

Sie sind in der Lage

- von aussagenlogischen Formeln zu entscheiden, ob diese allgemeingültig, erfüllbar oder unerfüllbar sind.
- Wahrheitstabellen auch für kompliziertere Formeln aufzuschreiben und daraus Schlüsse über den Wahrheitswert der Formel zu ziehen.
- Aussagenlogische Formeln in verschiedene Normalformen zu überführen.

Literatur und Links

Wie im ersten Kapitel.

2.1 Syntax der Aussagenlogik

Definition 5. Die *Sprache der Aussagenlogik* (auch Zeichenvorrat genannt) besteht aus:

- Atomare Formeln $p, q, p_1, p_2, q_1, q_2, \dots$
- Klammern $(,)$
- Junktoren $\neg, \wedge, \vee, \rightarrow$

Notation. Wir schreiben $\mathbb{A} := \{p, q, p_1, q_1, \dots\}$ für die Menge der atomaren Formeln.

Nachdem wir nun die Zeichen festgelegt haben, aus welchen die “Wörter der Aussagenlogik” zusammengesetzt sind, werden wir in der nächsten Definition, die für uns interessanten Wörter festlegen. Wir definieren, also im Sinn vom einführenden Beispiel, die “zulässigen Wörter” (genannt Formeln) der Aussagenlogik.

Definition 6. Die *Formeln* der Aussagenlogik sind wie folgt gegeben:

- Alle atomaren Formeln sind Formeln.
- Sind P und Q schon Formeln, dann auch: $(P \wedge Q)$, $(P \vee Q)$, $(P \rightarrow Q)$ und $\neg P$.

Notation. Wir schreiben \mathbb{F} für die Menge aller aussagenlogischen Formeln.

Bemerkung 9. Wir können die Aussagenlogischen Formeln auch durch die folgende Grammatik (vgl. Vorlesung theoretische Informatik) beschreiben:

- Variablen: F
- Terminalsymbole: $(,), \wedge, \vee, \rightarrow, p, q, p_1, q_1, \dots$
- Produktionen:

$$\begin{array}{lll} F \mapsto (F \wedge F) & F \mapsto (F \vee F) & F \mapsto q \mid q_1 \mid \dots \\ F \mapsto (F \rightarrow F) & F \mapsto \neg F & F \mapsto p \mid p_1 \mid \dots \end{array}$$

Bemerkung 10. Ist eine Formel von einem Klammernpaar umgeben, dann lassen wir die äussersten Klammern zugunsten einer besseren Lesbarkeit weg. Wir schreiben beispielsweise $(p \vee q) \wedge p_2$ anstelle von $((p \vee q) \wedge p_2)$.

Beispiel 7. Einige aussagenlogische Formeln:

$$p \vee (p \rightarrow \neg(q \wedge p)) \quad p \wedge \neg p \quad p \rightarrow (q \rightarrow p) \quad \neg(p \vee \neg q)$$

Einige Zeichenreihen, die *keine* aussagenlogische Formeln sind:

$$\neg \rightarrow p \quad \forall x p(x) \quad \text{“es regnet”}$$

2.2 Semantik der Aussagenlogik

Wir wollen jeder aussagenlogischen Formel nun eine Bedeutung zuordnen. Am bequemsten wäre es, wenn wir jeder Formel direkt einen der Wahrheitswert 1 (wahr) oder 0 (falsch) zuordnen könnten. Bei einigen Formeln gelingt dies tatsächlich ohne Probleme; $\neg p \vee p$ beispielsweise ist immer wahr, egal ob p selbst wahr oder falsch ist. Für andere Formeln ist das aber weniger klar; der Wahrheitswert der Formel $p_1 \vee p_4$ hängt von den Wahrheitswerten der Formeln p_1 und p_4 ab. Wir haben also folgendes Problem:

- Bevor wir die Wahrheitswerte von komplizierten Formeln bestimmen/definieren können, müssen wir die Wahrheitswerte der atomaren Formeln schon bestimmt haben.
- Die Zuordnung von Wahrheitswerten zu atomaren Formeln ist völlig willkürlich; es gibt keinen Grund, dass beispielsweise die Formel p_1 "weniger wahr" als die Formel p_4 sein soll.

Wir stellen also fest, dass wir einer aussagenlogischen Formel nur einen Wahrheitswert *bezüglich* einer Belegung der atomaren Formeln mit Wahrheitswerten geben können. Zum Beispiel, wenn wir die Variablen p_1 und p_4 beide mit dem Wahrheitswert 0 belegen, dann hat die Formel $p_1 \vee p_4$ *unter dieser Belegung* ebenfalls den Wahrheitswert 0.

Definition 7. Eine *Belegung* ist eine Zuordnung von atomaren Formeln zu Wahrheitswerten, d.h. eine Funktion $B : \mathbb{A} \rightarrow \{0, 1\}$.

Nun werden wir sehen, wie man ausgehend von einer Belegung jeder aussagenlogischen Formel einen Wahrheitswert zuordnen kann. Bevor wir uns der formalen Definition widmen, skizzieren wir unser Vorgehen exemplarisch an der Formel $(p \vee q) \wedge \neg p$. Nehmen wir an, dass B eine Belegung mit $B(p) = 1$ und $B(q) = 0$ sei. Wir wollen nun den Wahrheitswert von $(p \vee q) \wedge \neg p$ sinnvoll definieren. Wegen $B(p) = 1$ sollte die Formel $\neg p$ den Wahrheitswert 0 haben, und die Formel $p \vee q$ den Wert 1 erhalten. Zusammenfassend sehen wir, dass die Formel $\underbrace{(p \vee q)}_X \wedge \underbrace{\neg p}_Y$ von der Form $X \wedge Y$ ist wobei X den Wahrheitswert 1 und Y den Wahrheitswert 0 hat. Es ist daher sinnvoll den Wahrheitswert von $(p \vee q) \wedge \neg p$ auf 0 zu setzen.

Nun zur formalen Definition

Definition 8. Es sei eine Belegung B gegeben. Die Funktion \hat{B} ist die Funktion, die jeder aussagenlogischen Formel ihren Wahrheitswert bezüglich der Belegung B zuordnet, d.h. die Funktion $\hat{B} : \mathbb{F} \rightarrow \{0, 1\}$ ist gegeben durch:

- Für beliebige atomare Formeln x gilt $\hat{B}(x) = B(x)$.

- Für beliebige Formeln F und G gilt

$$\hat{B}(F \wedge G) = \begin{cases} 1 & \text{falls } \hat{B}(F) = 1 \text{ und } \hat{B}(G) = 1 \\ 0 & \text{sonst.} \end{cases}$$

- Für beliebige Formeln F und G gilt

$$\hat{B}(F \vee G) = \begin{cases} 1 & \text{falls } \hat{B}(F) = 1 \text{ oder } \hat{B}(G) = 1 \\ 0 & \text{sonst.} \end{cases}$$

- Für beliebige Formeln F gilt

$$\hat{B}(\neg F) = \begin{cases} 1 & \text{falls } \hat{B}(F) = 0 \\ 0 & \text{sonst.} \end{cases}$$

- Für beliebige Formeln F und G gilt $\hat{B}(F \rightarrow G) = \hat{B}(\neg F \vee G)$.

Bemerkung 11. Wenn wir auf grundlegende Operationen zurückgreifen, dann können wir die obige Definition etwas knapper formulieren. Eine Möglichkeit wäre etwa die entsprechenden Klauseln in der Definition durch die Zuordnungen

- $\hat{B}(F \wedge G) = \min(\hat{B}(F), \hat{B}(G))$
- $\hat{B}(F \vee G) = \max(\hat{B}(F), \hat{B}(G))$
- $\hat{B}(\neg F) = 1 - \hat{B}(F)$

zu ersetzen. Mithilfe dieser Darstellung können wir, wenn eine Belegung B gegeben ist, den Wahrheitswert einer beliebigen aussagenlogischen Formel unter der Belegung B “berechnen”.

Beispiel 8. Es sei eine Belegung B gegeben, die $B(p_n) = 1$ genau dann erfüllt, wenn n

eine gerade Zahl ist. Wir berechnen den Wahrheitswert von $(p_4 \rightarrow (p_5 \rightarrow p_6)) \vee p_{13}$.

$$\begin{aligned}
\hat{B}((p_4 \rightarrow (p_5 \rightarrow p_6)) \vee p_{13}) &= \max(\hat{B}(p_4 \rightarrow (p_5 \rightarrow p_6)), \underbrace{\hat{B}(p_{13})}_{=0}) \\
&= \hat{B}(p_4 \rightarrow (p_5 \rightarrow p_6)) \\
&= \hat{B}(\neg p_4 \vee (p_5 \rightarrow p_6)) \\
&= \max(\hat{B}(\neg p_4), \hat{B}(p_5 \rightarrow p_6)) \\
&= \max(1 - \underbrace{\hat{B}(p_4)}_{=1}, \hat{B}(\neg p_5 \vee p_6)) \\
&= \hat{B}(\neg p_5 \vee p_6) \\
&= \max(\hat{B}(\neg p_5), \underbrace{\hat{B}(p_6)}_{=1}) \\
&= 1
\end{aligned}$$

Übung 7. Es sei $B : \mathbb{A} \rightarrow \{0, 1\}$ eine Belegung, die genau diejenigen atomaren Formeln p_i wahr macht, bei denen i eine Primzahl ist. Bestimmen Sie \hat{B} von folgenden Formeln:

- a) $p_3 \rightarrow p_2$
- b) $(p_8 \rightarrow p_5) \wedge p_{13}$
- c) $p_1 \vee ((p_2 \rightarrow p_7) \wedge p_8)$

Lösung. a)

$$\hat{B}(p_3 \rightarrow p_2) = \hat{B}(\neg p_3 \vee p_2) = \max(\hat{B}(\neg p_3), \underbrace{\hat{B}(p_2)}_{=1}) = 1$$

b)

$$\begin{aligned}
\hat{B}((p_8 \rightarrow p_5) \wedge p_{13}) &= \min(\hat{B}(p_8 \rightarrow p_5), \underbrace{\hat{B}(p_{13})}_{=1}) = \hat{B}(p_8 \rightarrow p_5) \\
&= \hat{B}(\neg p_8 \vee p_5) = \max(\hat{B}(\neg p_8), \underbrace{\hat{B}(p_5)}_{=1}) = 1
\end{aligned}$$

c)

$$\begin{aligned}
\hat{B}(p_1 \vee ((p_2 \rightarrow p_7) \wedge p_8)) &= \max(\underbrace{\hat{B}(p_1)}_{=0}, \hat{B}((p_2 \rightarrow p_7) \wedge p_8)) \\
&= \hat{B}((p_2 \rightarrow p_7) \wedge p_8) \\
&= \min(\hat{B}(p_2 \rightarrow p_7), \underbrace{\hat{B}(p_8)}_{=0}) = 0
\end{aligned}$$

Definition 9. Eine aussagenlogische Formel A heisst

- *gültig* oder *wahr* unter einer Belegung B , falls $\widehat{B}(A) = 1$.
- *allgemeingültig*, wenn sie unter jeder Belegung gültig ist.
- *erfüllbar*, wenn es mindestens eine Belegung gibt, unter der A wahr ist.
- *unerfüllbar*, wenn sie nicht erfüllbar ist.

Beispiel 9. Einige allgemeingültige Formeln:

$$p \vee \neg p \qquad p \rightarrow (q \rightarrow p) \qquad F \rightarrow F \qquad .$$

Einige erfüllbare nicht allgemeingültige Formeln:

$$p_1 \vee (p_2 \vee p_3) \qquad p_3 \qquad p \rightarrow q$$

Einige unerfüllbare Formeln:

$$(p_1 \rightarrow \neg p_1) \wedge (\neg p_1 \rightarrow p_1) \qquad \neg p_3 \wedge p_3 \qquad \neg(F \rightarrow F)$$

Welche der Formeln

$$(p_1 \rightarrow (p_2 \vee p_1)) \vee (\neg p_1 \vee (p_2 \wedge p_1)) \qquad \neg p_3 \wedge p_3 \qquad \neg(F \rightarrow \neg F)$$

sind allgemeingültig, welche erfüllbar und welche unerfüllbar?

Bemerkung 12. Eines der grössten ungelösten Probleme der (theoretischen) Informatik ist die Frage, ob es einen “effizienten” Algorithmus gibt, der von jeder aussagenlogischen Formel entscheidet ob sie erfüllbar ist oder nicht. Diese Problemstellung wird mit **SAT** (von engl. **satisfiability**) bezeichnet. Die Relevanz dieser Frage kommt daher, dass sich das $P \stackrel{?}{=} NP$ Problem (die Frage ob zwei der wichtigsten Komplexitätsklassen übereinstimmen) darauf reduzieren lässt.

Übung 8. Zeigen sie: Eine aussagenlogische Formel F ist genau dann allgemeingültig, wenn $\neg F$ unerfüllbar ist.

Lösung. Es sei F eine beliebige aussagenlogische Formel. Wir müssen folgende Behauptungen beweisen:

- Ist F allgemeingültig, dann ist $\neg F$ nicht erfüllbar.
- $\neg F$ nicht erfüllbar, dann ist F allgemeingültig.

Für die erste Behauptung nehmen wir an, dass F allgemeingültig sei. Aus der Allgemeingültigkeit von F folgt $\hat{B}(F) = 1$ für jede Belegung B . Somit gilt $\hat{B}(\neg F) = 1 - \hat{B}(F) = 0$ für jede Belegung B , also ist die Formel $\neg F$ unerfüllbar.

Für die zweite Behauptung nehmen wir nun an, dass die Formel $\neg F$ nicht erfüllbar sei. Weil $\neg F$ unerfüllbar ist, gilt $1 - \hat{B}(F) = 0$ für jede Belegung B . Daraus folgt $\hat{B}(F) = 1$ für jede Belegung B und somit, dass F allgemeingültig ist.

Übung 9. Ist die Behauptung korrekt, dass jede Formel genau dann erfüllbar ist, wenn ihre Negation nicht erfüllbar ist? Begründen Sie Ihre Antwort.

Lösung. Die Behauptung ist falsch. Ein Gegenbeispiel zu der Aussage ist die (atomare) Formel p , sie ist erfüllbar und die Negation $\neg p$ ist ebenfalls erfüllbar.

Übung 10. Geben Sie zwei erfüllbare Formeln F und G an, so dass die Formel $F \wedge G$ nicht erfüllbar ist.

Lösung. Die Formeln $F := p$ und $G := \neg p$ sind beide erfüllbar, die Formel $p \wedge \neg p$ ist jedoch unerfüllbar.

Definition 10. Es seien F und G beliebige aussagenlogische Formeln. Wir sagen

- F ist eine *Konsequenz* von G , falls F unter jeder Belegung wahr ist unter der G wahr ist. D.h. wenn für jede Belegung B die Abschätzung $\hat{B}(G) \leq \hat{B}(F)$ gilt.
- F und G sind *logisch äquivalent*, wenn G und F unter jeder Belegung denselben Wahrheitswert annehmen.

Sind F und G äquivalente Formeln, dann schreiben wir $F \equiv G$.

Bemerkung 13. Zwei aussagenlogische Formeln sind genau dann äquivalent, wenn beide Formeln von der jeweils anderen eine Konsequenz sind.

Wir können nun, ähnlich wie wir dies im ersten Kapitel informell für die Prädikatenlogik getan haben (als Konsequenz davon!), einige grundlegende logische Äquivalenzen nachweisen.

Bemerkung 14. Ein “Lemma” ist ein “Hilfssatz”, d.h. eine Aussage, die für sich selbst genommen nicht unbedingt interessant sein muss, deren Nutzen aber darin besteht, den Beweis einer anderen Aussage zu vereinfachen. In gewissem Sinn dienen Lemmata auch dazu die Mathematik zu “modularisieren”; anstelle eines einzigen grossen Beweises für eine wichtige Aussage zu schreiben, kann man sich mit Lemmata an die grossen Sätze gewissermassen “herantasten”.

Lemma 1. *Für alle natürlichen Zahlen $x, y, z \in \{0, 1\}$ gelten folgende Identitäten*

$$i) \quad 1 - \min(x, y) = \max(1 - x, 1 - y)$$

$$ii) \quad 1 - \max(x, y) = \min(1 - x, 1 - y)$$

$$iii) \quad 1 - (1 - x) = x$$

$$iv) \quad \min(x, \max(y, z)) = \max(\min(x, y), \min(x, z))$$

$$v) \quad \max(x, \min(y, z)) = \min(\max(x, y), \max(x, z))$$

$$vi) \quad \min(x, \min(y, z)) = \min(\min(x, y), z)$$

$$vii) \quad \max(x, \max(y, z)) = \max(\max(x, y), z)$$

Beweis. Alle Aussagen lassen sich sofort anhand einer Fallunterscheidung verifizieren. Wir präsentieren beispielhaft die Fallunterscheidung von *i*).

- Falls $x = y = 0$:

$$1 - \min(x, y) = 1 - 0 = 1 = \max(1, 1) = \max(1 - x, 1 - y)$$

- Falls $x = 0$ und $y = 1$:

$$1 - \min(x, y) = 1 - 0 = 1 = \max(1, 0) = \max(1 - x, 1 - y)$$

- Falls $x = 1$ und $y = 0$:

$$1 - \min(x, y) = 1 - 0 = 1 = \max(0, 1) = \max(1 - x, 1 - y)$$

- Falls $x = y = 1$:

$$1 - \min(x, y) = 1 - 1 = 0 = \max(0, 0) = \max(1 - x, 1 - y) \quad \square$$

Bemerkung 15. Mit einem *Satz* bezeichnet man in der Mathematik eine zur Theoriebildung wichtige oder in der Anwendung nützliche Erkenntnis, die durch einen Beweis belegt wird.

Satz 1. *Sind F, G und H beliebige aussagenlogische Formeln, dann gelten folgende Äquivalenzen:*

- Gesetz der doppelten Negation: $\neg\neg F \equiv F$
- Absorption: $F \wedge F \equiv F$ und $F \vee F \equiv F$
- Kommutativität: $F \wedge G \equiv G \wedge F$ und $F \vee G \equiv G \vee F$
- Assoziativität: $F \wedge (G \wedge H) \equiv (F \wedge G) \wedge H$
- Assoziativität: $F \vee (G \vee H) \equiv (F \vee G) \vee H$
- Distributivität: $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
- Distributivität: $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
- De Morgan: $\neg(F \wedge G) \equiv \neg F \vee \neg G$
- De Morgan: $\neg(F \vee G) \equiv \neg F \wedge \neg G$
- Kontraposition: $F \rightarrow G \equiv \neg G \rightarrow \neg F$

Beweis. Wir müssen für jede der behaupteten Äquivalenzen nachweisen, dass die genannten Formeln unter jeder Belegung denselben Wahrheitswert haben. Wenn wir also von einer beliebigen Belegung B ausgehen, dann müssen wir, um eine Äquivalenz von der Form $X \equiv Y$ nachzuweisen, bloss zeigen, dass $\widehat{B}(X) = \widehat{B}(Y)$ gilt.

- Doppelte Negation: Aus Lemma 1 ii) erhalten wir

$$\widehat{B}(\neg\neg F) = 1 - \widehat{B}(\neg F) = 1 - (1 - \widehat{B}(F)) = \widehat{B}(F).$$

- Absorption: Dies folgt sofort aus der Tatsache, dass für alle $x \in \{0, 1\}$ die Identitäten $\min(x, x) = x$ und $\max(x, x) = x$ gelten.
- Kommutativität: Dies folgt sofort aus der Tatsache, dass für alle $x, y \in \{0, 1\}$ die Identitäten $\min(x, y) = \min(y, x)$ und $\max(x, y) = \max(y, x)$ gelten.
- Assoziativität: Aus Lemma 1 vi) erhalten wir

$$\begin{aligned} \widehat{B}(F \wedge (G \wedge H)) &= \min(\widehat{B}(F), \min(\widehat{B}(G), \widehat{B}(H))) \\ &= \min(\min(\widehat{B}(F), \widehat{B}(G)), \widehat{B}(H)) \\ &= \widehat{B}((F \wedge G) \wedge H). \end{aligned}$$

Im Fall der Formel $F \vee (G \vee H)$ argumentieren wir analog mit vii) aus dem Lemma.

- Distributivität: Mit dem Teil iv) von Lemma 1 erhalten wir

$$\begin{aligned} \widehat{B}(F \wedge (G \vee H)) &= \min(\widehat{B}(F), \max(\widehat{B}(G), \widehat{B}(H))) \\ &= \max(\min(\widehat{B}(F), \widehat{B}(G)), \min(\widehat{B}(F), \widehat{B}(H))) \\ &= \widehat{B}((F \wedge G) \vee (F \wedge H)) \end{aligned}$$

- Distributivität: Für die Formel $F \vee (G \wedge H)$ argumentieren wir analog mit Lemma 1 Teil v).
- De Morgan: Aus dem Teil i) von Lemma 1 folgt:

$$\begin{aligned}\widehat{B}(\neg(F \wedge G)) &= 1 - \widehat{B}(F \wedge G) \\ &= 1 - \min(\widehat{B}(F), \widehat{B}(G)) \\ &= \max(1 - \widehat{B}(F), 1 - \widehat{B}(G)) \\ &= \widehat{B}(\neg F \vee \neg G)\end{aligned}$$

- De Morgan: Für die Äquivalenz $\neg(F \vee G) \equiv \neg F \wedge \neg G$, argumentieren wir analog mit Teil ii) von Lemma 1.
- Kontraposition: Dies folgt aus den bereits bewiesenen Äquivalenzen

$$\neg G \rightarrow \neg F \equiv \neg\neg G \vee \neg F \equiv G \vee \neg F \equiv \neg F \vee G \equiv F \rightarrow G \quad \square$$

Bemerkung 16. Mit *Theorem* bezeichnet man in der Mathematik besonders wichtige Sätze.

Das nächste Theorem schlägt eine wichtige Brücke zwischen Syntax und Semantik der Aussagenlogik, indem es die logische Konsequenz (Semantik) in Beziehung zur Implikation (Syntax) setzt. Man kann das Theorem dahingehend interpretieren, dass die Implikation \rightarrow eine adäquate Formalisierung des Folgerungsbegriffes \Rightarrow vom ersten Kapitel darstellt.

Theorem 1 (Folgerungstheorem). *Sind F und G aussagenlogische Formeln, dann gelten:*

- i) *G ist genau dann eine Konsequenz von F , wenn die Formel $F \rightarrow G$ allgemeingültig ist.*
- ii) *F und G sind genau dann logisch äquivalent, wenn die Formel $F \rightarrow G \wedge G \rightarrow F$ allgemeingültig ist.*

Beweis. Wir beobachten zuerst, dass

$$\widehat{B}(F \rightarrow G) = 1 \Leftrightarrow \widehat{B}(F) \leq \widehat{B}(G) \quad (2.1)$$

für jede Belegung B gilt. Um dies einzusehen, betrachten wir die Äquivalenzen

$$\begin{aligned}\widehat{B}(F \rightarrow G) = 1 &\Leftrightarrow \widehat{B}(\neg F \vee G) = 1 \\ &\Leftrightarrow \max(\widehat{B}(\neg F), \widehat{B}(G)) = 1 \\ &\Leftrightarrow \widehat{B}(\neg F) = 1 \text{ oder } \widehat{B}(G) = 1 \\ &\Leftrightarrow \widehat{B}(F) = 0 \text{ oder } \widehat{B}(G) = 1 \\ &\Leftrightarrow \widehat{B}(F) \leq \widehat{B}(G).\end{aligned}$$

- i) Dies folgt nun direkt aus der Definition von Konsequenz und aus (2.1).

- ii) Dies folgt nun aus dem ersten Teil. \square

Normalformen

Bemerkung 17. Ausdrücke von der Form $F_1 \vee \dots \vee F_n$ oder $F_1 \wedge \dots \wedge F_n$ stehen stellvertretend für alle möglichen Formeln die durch Kammersetzung aus ihnen gebildet werden können. Für den Wahrheitswert der Formeln ist die genaue Klammerung, wegen der Assoziativität unwichtig.

Definition 11. *Literale* sind atomare Formeln oder negierte atomare Formeln.

Beispiel 10. Beispiele für Literale: p , $\neg q$, $\neg p_{34}$.

Definition 12. Eine aussagenlogische Formel ist:

- In *Negations Normalform*(NNF), wenn alle Negationen in Literalen vorkommen und wenn keine Implikationen (\rightarrow) vorkommen.
- In *disjunktiver Normalform*(DNF), wenn sie von der Form

$$(L_{1,1} \wedge L_{1,2} \wedge \dots) \vee (L_{2,1} \wedge L_{2,2} \wedge \dots) \vee (L_{3,1} \wedge L_{3,2} \wedge \dots) \dots$$

mit Literalen $L_{i,j}$ ist.

- In *konjunktiver Normalform*(KNF), wenn sie von der Form

$$(L_{1,1} \vee L_{1,2} \vee \dots) \wedge (L_{2,1} \vee L_{2,2} \vee \dots) \wedge (L_{3,1} \vee L_{3,2} \vee \dots) \dots$$

mit Literalen $L_{i,j}$ ist.

Beispiel 11. Die Formel

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

ist in keiner der oben eingeführten Normalformen. Die Formel

$$(\neg p \vee q) \wedge ((p \wedge p_1) \vee (p_2 \wedge p_3))$$

ist in *NNF* aber weder in *DNF* noch in *KNF*. Die Formel

$$p \vee q$$

ist in *NNF*, *KNF* und *DNF*.

Satz 2. Für jede aussagenlogische Formel gibt es äquivalente Formeln in *NNF*, *KNF* und *DNF*.

Beweis.

- *NNF*: Wir gehen folgendermassen vor, um aus einer Formel eine äquivalente Formel in *NNF* zu konstruieren.
 1. Implikationen eliminieren durch Anwenden der Regel $F \rightarrow G \equiv \neg F \vee G$.
 2. Negationen, die nicht zu einem Literal gehören werden sukzessive durch Anwenden der De Morganschen Regeln und der Regel über doppelte Negation eliminiert.
- *KNF/DNF*: Jede Formel in *NNF* kann durch sukzessives Anwenden der Distributivgesetze wahlweise in *KNF* oder *DNF* gebracht werden. Da wir bereits wissen, dass jede Formel in *NNF* gebracht werden kann, ist die Behauptung somit bewiesen. \square

Beispiel 12. Wir bringen die Formel

$$(\neg p \rightarrow q) \rightarrow ((p \wedge p_1) \vee (p_2 \wedge p_3))$$

in *DNF*. Wir eliminieren zuerst alle Implikationen und doppelten Negationen:

$$\begin{aligned} (\neg p \rightarrow q) \rightarrow ((p \wedge p_1) \vee (p_2 \wedge p_3)) &\equiv \neg(\neg p \rightarrow q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \\ &\equiv \neg(\neg \neg p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \\ &\equiv \neg(p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)). \end{aligned}$$

Als Nächstes eliminieren wir alle Negationen, die nicht in Literalen vorkommen:

$$\neg(p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \equiv (\neg p \wedge \neg q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)).$$

Die Formel, die wir erhalten haben, ist sowohl in *NNF* als auch in *DNF*. Wir konstruieren nun noch eine zur Formel

$$(p \wedge p_1) \vee (p_2 \wedge p_3)$$

äquivalente Formel in *KNF*. Wir wenden sukzessive die Distributivgesetze an:

$$\begin{aligned} (p \wedge p_1) \vee (p_2 \wedge p_3) &\equiv ((p \wedge p_1) \vee p_2) \wedge ((p \wedge p_1) \vee p_3) \\ &\equiv ((p \wedge p_1) \vee p_2) \wedge ((p \vee p_3) \wedge (p_1 \vee p_3)) \\ &\equiv ((p \vee p_2) \wedge (p_1 \vee p_2)) \wedge ((p \vee p_3) \wedge (p_1 \vee p_3)). \end{aligned}$$

Übung 11. Bringen Sie die Formel

$$(p_1 \rightarrow p_3) \vee (p_1 \wedge p_2)$$

in *KNF* und in *DNF*.

Lösung.

$$\begin{aligned}
 (p_1 \rightarrow p_3) \vee (p_1 \wedge p_2) &\equiv \underbrace{(\neg p_1 \vee p_3) \vee (p_1 \wedge p_2)}_{DNF} \\
 &\equiv \underbrace{((\neg p_1 \vee p_3) \vee p_1) \wedge ((\neg p_1 \vee p_3) \vee p_2)}_{KNF}
 \end{aligned}$$

Wahrheitstabellen

Einen alternativen Zugang zur Semantik der Aussagenlogik bieten sogenannte Wahrheitstabellen. Sie werden dazu genutzt um alle für jeweils eine bestimmte Formel relevanten Teile einer möglichen Belegungen tabellarisch darzustellen.

Definition 13. In einer *Wahrheitstabelle einer Formel F* entspricht jede Spalte einer Teilformel von F und jede Zeile einer Belegung. Am Kreuzungspunkt von einer Zeile und einer Spalte wird jeweils der Wahrheitswert der durch die Spalte gegebenen Formel unter der durch die Zeile gegebenen Belegung eingetragen. Man spricht von einer vollständigen Wahrheitstabelle, wenn alle Teilformeln durch Spalten und alle Belegungen der atomaren Teilformeln durch Zeilen repräsentiert sind.

Beispiel 13. Die Teilformeln von der Formel $p_0 \rightarrow (q \vee p_1)$ sind: $p_0, p_1, q, (q \vee p_1)$ und $p_0 \rightarrow (q \vee p_1)$. Eine vollständige Wahrheitstabelle von $p_0 \rightarrow (q \vee p_1)$ ist also:

p_0	q	p_1	$q \vee p_1$	$p_0 \rightarrow (q \vee p_1)$
0	0	0	0	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Bemerkung 18. Man kann Wahrheitstabellen auch zur Darstellung von logischen Operatoren² benutzen. Beispielhaft geben wir die Wahrheitstabellen für die Operatoren (Junktoren) $\vee, \wedge, \rightarrow, \neg$ an.

²Funktionen, die aus aussagenlogischen Formeln neue aussagenlogische Formeln generieren.

F	G	$F \wedge G$	F	G	$F \vee G$	F	G	$F \rightarrow G$	F	$\neg F$
0	0	0	0	0	0	0	0	1	0	1
0	1	0	0	1	1	0	1	1	1	0
1	0	0	1	0	1	1	0	0		
1	1	1	1	1	1	1	1	1		

In der folgenden Bemerkung wollen wir noch kurz darauf eingehen, wie man die semantischen Konzepte von Allgemeingültigkeit, Erfüllbarkeit, Konsequenz und Äquivalenz anhand von Wahrheitstabellen verstehen kann. Wir gehen dabei von der Annahme aus, dass die zur untersuchenden Formel gehörende Spalte, die letzte Spalte der Wahrheitstabelle ist.

Bemerkung 19. Eine aussagenlogische Formel F ist

- genau dann allgemeingültig, wenn in der letzten Spalte der Wahrheitstabelle von F alle Einträge 1 sind.
- genau dann erfüllbar, wenn in der letzten Spalte der Wahrheitstabelle von F nicht alle Einträge 0 sind.
- genau dann unerfüllbar, wenn in der letzten Spalte der Wahrheitstabelle keine 1 steht.

Als Folgerung daraus und mit Theorem 1, erhalten wir, für beliebige zwei aussagenlogische Formeln F und G , dass:

- F und G sind äquivalent, wenn in der letzten Spalte der Wahrheitstabelle von der Formel $F \rightarrow G \wedge G \rightarrow F$ alle Einträge 1 sind.
- G ist eine Konsequenz von F , wenn in der letzten Spalte der Wahrheitstabelle von der Formel $F \rightarrow G$ alle Einträge 1 sind.

Beispiel 14. Wir können nun die Äquivalenz der Formeln $p \rightarrow q$ und $\neg q \rightarrow \neg p$ anhand ihrer Wahrheitstabellen nachvollziehen.

p	q	$p \rightarrow q$	p	q	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$
0	0	1	0	0	1	1	1
0	1	1	0	1	0	1	1
1	0	0	1	0	1	0	0
1	1	1	1	1	0	0	1

Übung 12. Zeigen Sie mit der Methode der Wahrheitstabellen, dass die Formeln $p \rightarrow q$ und $q \rightarrow p$ nicht äquivalent sind.

Lösung.

p	q	$p \rightarrow q$	$q \rightarrow p$
0	0	1	1
0	1	1	0
1	0	0	1
1	1	1	1

3 Mengen

Prolog

Der Zweck der Mengenlehre besteht darin, mehrere mathematische Objekte zusammenzufassen und diese Zusammenfassung als neues eigenständiges mathematisches Objekt zu verstehen. Der Prozess der Mengenbildung und das Konzept einer Menge sind fundamental für den gesamten Aufbau der Mathematik aber keineswegs unproblematisch. Die Probleme, die ein allzu naiver Umgang mit Mengenexistenzannahmen verursachen können, zeigten sich eindrücklich im Zusammenhang mit der sogenannten “Grundlagenkrise der Mathematik”¹. Ein Auslöser der Grundlagenkrise war die sogenannte “Russelsche Antinomie”. Die Russelsche Antinomie zeigt, dass man nicht beliebige Dinge anhand einer Eigenschaft zu einer Menge zusammenfassen kann. Die Antinomie entsteht wie folgt: Wir nehmen an, dass zu jeder Eigenschaft E die Menge aller Dinge mit der Eigenschaft E

$$\{x \mid x \text{ hat die Eigenschaft } E(x)\}$$

existiert. Wir erhalten eine paradoxe Menge R , wenn wir als Eigenschaft E das Prädikat $x \notin x$ wählen. Nach unserer Annahme müsste es nun die Menge

$$R = \{x \mid x \notin x\}$$

aller Mengen, die sich nicht selbst als Element enthalten, geben. Wir können uns nun fragen, ob R ein Element von sich selbst ist. . . Versuchen Sie diese Frage zu beantworten.

Relevanz für die Informatik

Die Bedeutung der Mengenlehre kommt nicht in erster Linie von etwaigen direkten Anwendungen, sondern von ihrer Stellung innerhalb der Mathematik. Mengen sind der *primitive Datentyp* der (modernen) Mathematik. Dies hat unter anderem folgende Konsequenzen:

- Die Mengenlehre bildet (zusammen mit der Prädikatenlogik) die Sprache der Mathematik.
- Alle mathematischen Objekte sind Mengen, insbesondere sind auch alle in der theoretischen Informatik behandelten Strukturen (berechenbare Funktionen, Turing Maschinen, . . .) Mengen.

¹Phase der Verunsicherung der mathematischen Öffentlichkeit zu Beginn des 20. Jahrhunderts.

Lernziele

Sie kennen die

- grundlegenden mengentheoretischen Operationen (Vereinigung, Schnitt, Komplement, Potenzmenge).
- Zahlenmengen \mathbb{N} , \mathbb{Z} , \mathbb{Q} und \mathbb{R} .
- verschiedenen Darstellungsformen für Mengen.

Sie verstehen

- wie man Mengen in ihrer Mächtigkeit vergleicht.
- den Unterschied zwischen einer abzählbaren und einer überabzählbaren Menge.

Sie sind in der Lage

- Argumente für die Abzählbarkeit von \mathbb{Z} , \mathbb{Q} und ähnlichen Mengen anzugeben.
- zu beweisen, dass \mathbb{R} und ähnliche Mengen überabzählbar sind.

Literatur und Links

Ergänzende Literatur:

- [3] Kapitel 2 ohne 2.4 und 2.5.
- [4] Kapitel 1 Teil 1.

Nützliche Links:

- [http://de.wikipedia.org/wiki/Menge_\(Mathematik\)](http://de.wikipedia.org/wiki/Menge_(Mathematik))
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Mengenlehre

3.1 Der Mengenbegriff und grundlegende Definitionen

Wenn, wie vorher angedeutet, jedes mathematische Objekt eine Menge ist, wie definiert man dann was eine Menge ist? Dies ist in der Tat ein wenig problematisch. Dieser Umstand wird in der Literatur auf zwei unterschiedliche Arten angegangen:

- Auf eine Definition verzichten und dafür wichtige Eigenschaften von Mengen festhalten.
- Eine anschauliche “Definition” zu verwenden, die zwar den Standards einer mathematischen Definition nicht genügt, aber trotzdem wichtige Eigenschaften von Mengen festhält.

Wir werden unseren Mengenbegriff dadurch aufbauen, dass wir einige *definierende Eigenschaften* und Schreibweisen für Mengen einführen. Die wichtigste Schreibweise im Umgang mit Mengen ist die Notation, die ausdrückt ob etwas zu einer Menge gehört oder nicht.

Notation. Ist X eine Menge und y ein *Element* von X , dann schreiben wir $y \in X$. Ist y kein Element von X , dann schreiben wir $y \notin X$.

Die erste *definierende Eigenschaft* von Mengen ist die Tatsache, dass jede Menge durch ihre Elemente vollständig beschrieben ist.

Definition 14 (Definierende Eigenschaft). Zwei Mengen sind genau dann gleich, wenn sie die selben Elemente enthalten: Es gilt für alle Mengen X und Y die Äquivalenz

$$X = Y \Leftrightarrow \forall z (z \in X \Leftrightarrow z \in Y).$$

Da Mengen bereits durch Angabe ihrer Elemente bestimmt werden, können wir jede (endliche) Menge durch Auflisten ihrer Elemente festlegen.

Definition 15 (Explizite Schreibweise). Sind mathematische Objekte x_1, \dots, x_n gegeben, dann schreiben wir

$$\{x_1, \dots, x_n\}$$

für die Menge die als Elemente genau x_1, \dots, x_n hat.

Beispiel 15.

- Die Menge $\{2, 34, 77\}$ enthält die drei Elemente 2, 34 und 77.
- Die Menge $\{ \}$ heisst *leere Menge*. Die leere Menge ist die einzige Menge, die gar keine Elemente besitzt, sie wird mit \emptyset bezeichnet.

Bemerkung 20. Wenn keine Missverständnisse zu befürchten sind, so beschreibt man Mengen auch durch “angedeutende” Aufzählung ihrer Elemente. Die Menge \mathbb{N} der *natürlichen Zahlen* wird beispielsweise durch

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

beschrieben. Die Menge der *ganzen Zahlen* wird durch

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

beschrieben.

Bemerkung 21. Die Tatsache, dass Mengen durch ihre Elemente eindeutig beschrieben werden hat zur Folge, dass Mengen sehr “unstrukturierte Datentypen” sind, d.h. Mengen haben keine “innere Ordnung”. Es gelten unter anderem:

- Für beliebige z, x_1, \dots, x_n

$$z \in \{x_1, \dots, x_n\} \Leftrightarrow z = x_1 \vee \dots \vee z = x_n$$

- Für alle x

$$\{x\} = \{x, x\} = \{x, x, x\} = \dots$$

- Für alle x, y

$$\{x, y\} = \{y, x\}.$$

Definition 16 (Teilmengen). Wir schreiben $X \subset Y$ und sagen X ist eine *Teilmenge* von Y , wenn jedes Element von X auch ein Element von Y ist:

$$X \subset Y : \Leftrightarrow \forall x (x \in X \Rightarrow x \in Y).$$

Wir schreiben $X \subsetneq Y$ und sagen X ist eine *echte Teilmenge* von Y , falls X eine von Y verschiedene Teilmenge von Y ist:

$$X \subsetneq Y : \Leftrightarrow X \subset Y \wedge X \neq Y.$$

Beispiel 16.

- Die Menge aller Hühner ist eine (echte) Teilmenge der Menge aller Vögel, weil alle Hühner Vögel sind (und weil es Vögel gibt die keine Hühner sind).
- Die Menge aller Primzahlen ist eine (echte) Teilmenge von \mathbb{N} .
- Die Menge aller Primzahlen ist *keine* Teilmenge aller ungeraden Zahlen, weil die Zahl 2 eine Primzahl aber keine ungerade Zahl ist.

Bemerkung 22. Zwei Mengen X und Y sind gleich, wenn $X \subset Y$ und $Y \subset X$ gilt.

Mengenbildung

Wir führen im Folgenden einige Operationen und Schreibweisen ein, mithilfe derer wir neue Mengen (aus bereits vorhandenen) generieren können. Wir erhalten beispielsweise die Menge aller Primzahlen aus der Menge der natürlichen Zahlen, indem wir

$$\{p \in \mathbb{N} \mid p \text{ hat genau 2 Teiler}\}$$

schreiben.

Definition 17 (Prädikative Schreibweise). Ist X eine Menge und ist E eine Eigenschaft (Prädikat), dann bezeichnen wir mit

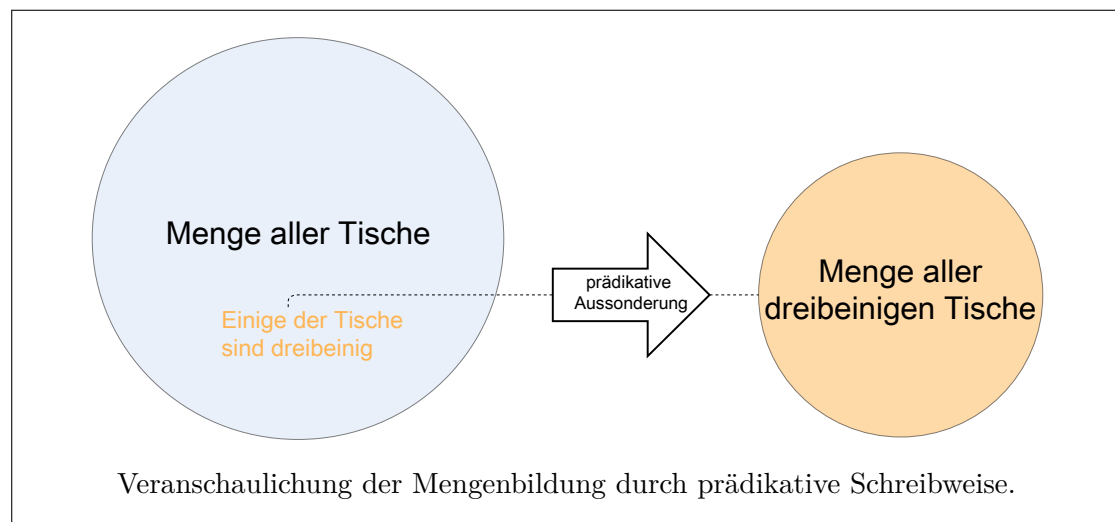
$$\{z \in X \mid E(z)\}$$

oder mit

$$\{z \mid z \in X \wedge E(z)\}$$

die Menge aller Elemente z von X mit der Eigenschaft $E(z)$.

Beispiel 17. Wenn man aus der Menge aller Tische die Dinge mit der Eigenschaft “drei Beine zu haben” aussondert (und zusammenfasst), dann erhält man die Menge aller dreibeinigen Tische.



Beispiel 18. Die Menge aller geraden natürlichen Zahlen erhält man auch durch die prädikative Schreibweise,

- $\{n \in \mathbb{N} \mid n \text{ ist gerade}\}$
- $\{n \in \mathbb{N} \mid \exists z \in \mathbb{N} (n = 2 \cdot z)\}$

Definition 18 (Ersetzungsschreibweise). Ist F eine Funktion und ist $E(x)$ eine Eigenschaft (Prädikat), dann beinhaltet die Menge

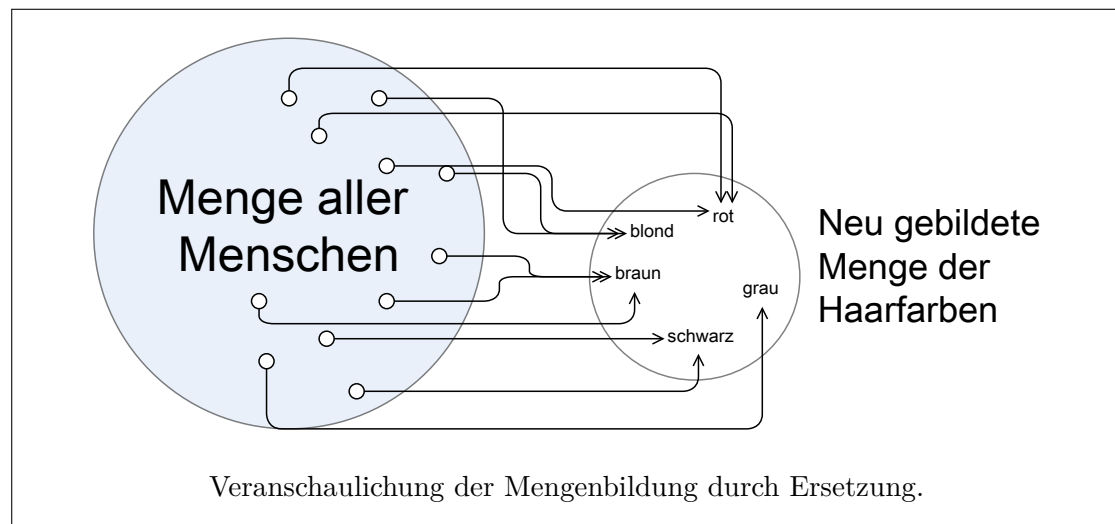
$$\{F(x) \mid E(x)\}$$

alle Funktionswerte $F(x)$, die man dadurch erhalten kann, dass man ein Element x mit der Eigenschaft $E(x)$ in F einsetzt:

$$\{F(x) \mid E(x)\} := \{y \mid \exists x (y = F(x) \wedge E(x))\}.$$

Beispiel 19. Wenn F die Funktion ist, die jeder Person ihre Haarfarbe zuordnet, dann erhalten wir die Menge H aller Haarfarben aus der Menge M aller Menschen durch

$$H = \{F(x) \mid x \in M\}.$$



Beispiel 20. Die Menge der geraden natürlichen Zahlen lässt sich nun mithilfe der Funktion $F(x) = 2 \cdot x$ als

$$\{F(x) \mid x \in \mathbb{N}\} = \{2x \mid x \in \mathbb{N}\}$$

schreiben.

Definition 19. Sind X und Y Mengen, dann ist

$$X \cup Y := \{x \mid x \in X \vee x \in Y\}$$

die *Vereinigung* von X mit Y . Die *Schnittmenge* von X und Y ist durch

$$X \cap Y := \{x \in X \mid x \in Y\} = \{x \in Y \mid x \in X\} = \{x \mid x \in X \wedge x \in Y\}$$

gegeben. Ist I eine Menge so, dass für alle Elemente $i \in I$ auch A_i eine Menge ist, dann wird

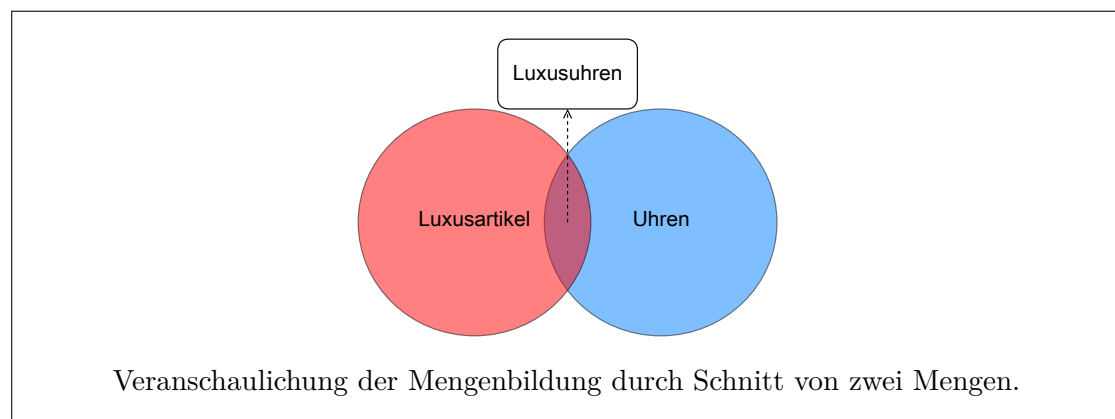
$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I (x \in A_i)\}.$$

die Vereinigung von $\{A_i \mid i \in I\}$ genannt. Analog dazu, ist die *Schnittmenge* durch

$$\bigcap_{i \in I} A_i := \{x \mid \forall i \in I (x \in A_i)\}$$

gegeben, falls $I \neq \emptyset$ ist.

Beispiel 21. Die Schnittmenge der Menge der Luxusgüter mit der Menge aller Uhren beinhaltet genau die Luxusuhren.



Übung 13. Beschreiben Sie folgende Mengen:

- a) $\{0, 2, 4, \dots\} \cap \{p \in \mathbb{N} \mid p \text{ ist eine Primzahl}\}$
- b) $\mathbb{N} \cap \{\mathbb{N}\}$
- c) $\mathbb{N} \cup \{\mathbb{N}\}$

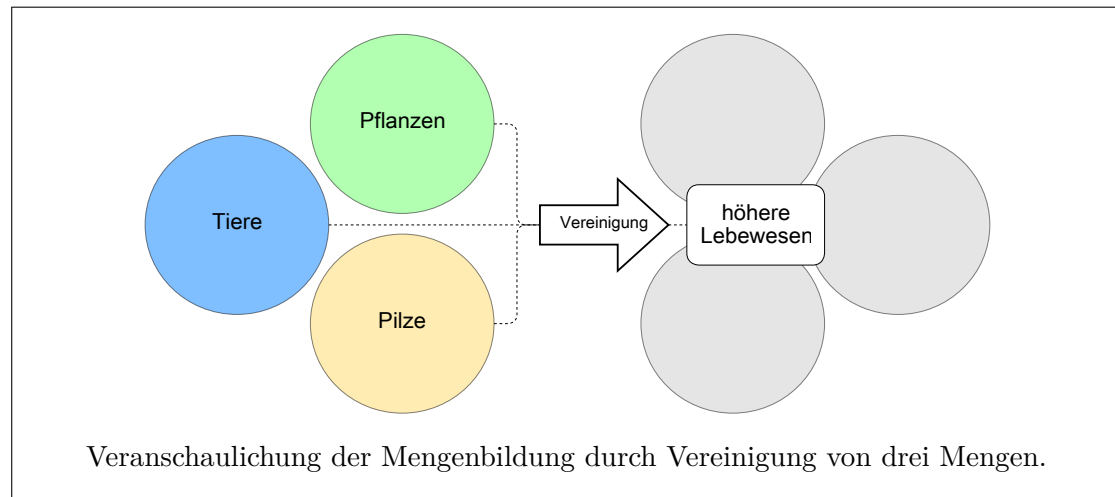
Lösung.

- a) $\{2\}$
- b) \emptyset
- c) $\{\mathbb{N}, 0, 1, 2, \dots\}$

Beispiel 22. Wenn A_1 die Menge aller Tiere, A_2 die Menge aller Pflanzen und A_3 die Menge aller Pilze ist, dann ist

$$\bigcup_{i \in \{1,2,3\}} A_i = A_1 \cup A_2 \cup A_3$$

die Menge aller höheren Lebewesen (Mehrzeller).



Beispiel 23. a) $\mathbb{N} = \{n \in \mathbb{N} \mid n \text{ ist gerade}\} \cup \{n \in \mathbb{N} \mid n \text{ ist ungerade}\}$

b) $\emptyset = \{n \in \mathbb{N} \mid n \text{ ist gerade}\} \cap \{n \in \mathbb{N} \mid n \text{ ist ungerade}\}$

c) Sind X_a und X_b beliebige Mengen, dann gilt:

$$X_a \cup X_b = \bigcup_{i \in \{a,b\}} X_i.$$

d) Ist für jede natürliche Zahl n die Menge X_n als $\{0, \dots, n\}$ gegeben, dann gilt

$$\bigcup_{n \in \mathbb{N}} X_n = \mathbb{N}$$

und

$$\bigcap_{n \in \mathbb{N}} X_n = \{0\}.$$

Definition 20. Zwei Mengen X und Y heißen *disjunkt*, falls sie keine gemeinsamen Elemente haben, d.h. falls $X \cap Y = \emptyset$ gilt. Wir sagen eine Menge $\{X_i \mid i \in I\}$ von Mengen bestehe aus *paarweise disjunkten* Mengen, wenn folgendes gilt:

$$\forall i, j \in I (i \neq j \Rightarrow A_i \cap A_j = \emptyset).$$

Bemerkung 23. Für Mengen $\{X_i \mid i \in I\}$, hat die Annahme

$$\bigcap_{i \in I} X_i = \emptyset$$

nicht notwendigerweise zur Folge, dass die X_i 's paarweise disjunkt sind. Die Mengen

$$\{x \in \mathbb{N} \mid x < 24\}$$

$$\{x \in \mathbb{N} \mid 22 < x\}$$

$$\{x \mid x \text{ ist durch } 6 \text{ teilbar}\}$$

sind *nicht* paarweise disjunkt, die Schnittmenge ist jedoch leer.

Definition 21. Sind X und Y beliebige Mengen, so definieren wir als

$$X \setminus Y := \{x \in X \mid x \notin Y\}$$

die Menge aller Elemente von X , die nicht zu Y gehören.

Beispiel 24. Die Menge der ungeraden Zahlen können wir als

$$\mathbb{N} \setminus \{2x \mid x \in \mathbb{N}\}$$

schreiben.

Übung 14. Beschreiben Sie folgende Mengen.

- a) $\mathbb{N} \setminus \{x \in \mathbb{N} \mid x \text{ ist gerade}\}$
- b) $\{x \in \mathbb{N} \mid x \text{ ist gerade}\} \setminus \{3x \mid x \in \mathbb{N}\}$
- c) $\mathbb{N} \setminus (\mathbb{N} \setminus \mathbb{Z})$

Lösung.

- a) $\{x \in \mathbb{N} \mid x \text{ ist ungerade}\}$
- b) Die Menge aller geraden und nicht durch 3 teilbaren natürlichen Zahlen.
- c) \mathbb{N}

Satz 3 (Rechenregeln). *Es gelten für beliebige Mengen A, B und C folgende Identitäten:*

a) *Kommutativität der Vereinigung und des Schnittes:*

$$A \cup B = B \cup A \text{ und } A \cap B = B \cap A.$$

b) *Assoziativgesetze von Schnitt und Vereinigung:*

$$A \cap (B \cap C) = (A \cap B) \cap C \text{ und } A \cup (B \cup C) = (A \cup B) \cup C$$

c) *Distributivgesetze von \cap mit \cup :*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ und } A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

d) *Idempotenzgesetz:*

$$A \cap A = A \text{ und } A \cup A = A$$

e) *Regeln von De Morgan:*

$$(C \setminus A) \cap (C \setminus B) = C \setminus (A \cup B) \text{ und } (C \setminus A) \cup (C \setminus B) = C \setminus (A \cap B)$$

f) *Charakterisierung der Teilmengenbeziehung:*

$$A \subset B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$$

Beweis. Übung

□

Übung 15. Zeigen Sie für beliebige Mengen A und B :

a) $A \setminus (A \setminus B) = A \cap B$

b) $(A \setminus B) \setminus B = A \setminus B$

Lösung.

a) Es sei x beliebig, es gilt:

$$\begin{aligned} x \in A \setminus (A \setminus B) &\Leftrightarrow x \in A \wedge (x \notin A \setminus B) \\ &\Leftrightarrow x \in A \wedge \neg(x \in A \wedge x \notin B) \\ &\Leftrightarrow x \in A \wedge (x \notin A \vee x \in B) \\ &\Leftrightarrow (x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B) \\ &\Leftrightarrow x \in A \wedge x \in B \\ &\Leftrightarrow x \in A \cap B \end{aligned}$$

b) Es sei x beliebig, es gilt:

$$\begin{aligned} x \in (A \setminus B) \setminus B &\Leftrightarrow x \notin B \wedge (x \in A \setminus B) \\ &\Leftrightarrow x \notin B \wedge (x \in A \wedge x \notin B) \\ &\Leftrightarrow x \in A \wedge x \notin B \\ &\Leftrightarrow x \in A \setminus B \end{aligned}$$

Definition 22. Ist A eine beliebige Menge, dann bezeichnen wir mit

$$\mathcal{P}(A) := \{x \mid x \subset A\}$$

die *Potenzmenge* von A , die genau die Teilmengen von A als Elemente enthält.

Beispiel 25. a) $\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$

b) $\mathcal{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$

Übung 16. Beschreiben Sie in aufzählender Form:

a) $\mathcal{P}(\{3, 4\})$

b) $\mathcal{P}(\{a, \{c\}\})$

c) $\mathcal{P}(\{\{\{x\}\}\})$

Lösung.

a) $\{\{\}, \{3\}, \{4\}, \{3, 4\}\}$

b) $\{\{\}, \{a\}, \{\{c\}\}, \{a, \{c\}\}\}$

c) $\{\{\}, \{\{\{x\}\}\}\}$

Übung 17. Geben Sie Mengen A und B an, mit

$$\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B).$$

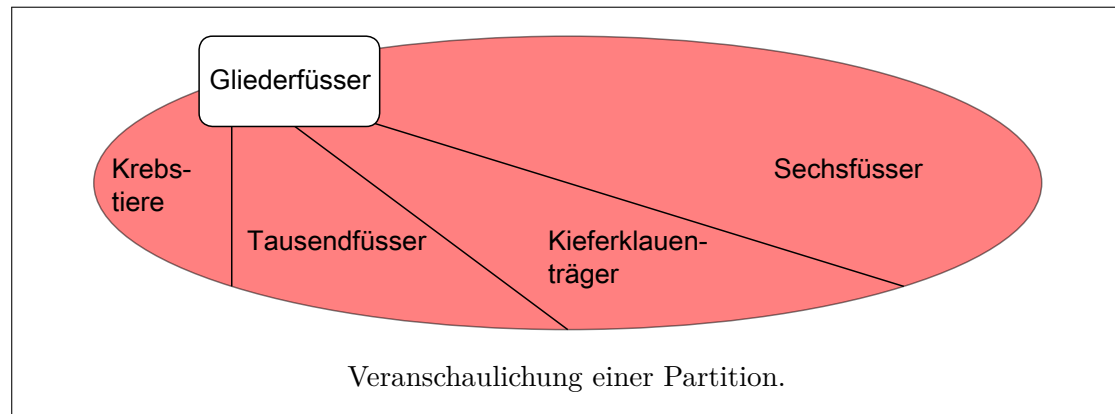
Lösung. z.B. $A = \{1, 2\}$ und $B = \{2, 3\}$

Definition 23 (Partitionen). Eine *Partition* $P = \{P_i \mid i \in I\}$ einer Menge A , ist eine Menge von Teilmengen von A , die folgende beiden Voraussetzungen erfüllt:

- Die Elemente von P sind nichtleer und paarweise disjunkt.
- $\bigcup_{i \in I} P_i = A$

Die Elemente einer Partition werden *Blöcke* der Partition genannt.

Beispiel 26. Die Partition (Unterteilung) der Gliederfüßer in Tausendfüßer, Krebstiere, Kieferklauenträger und Sechsfüßer.



Beispiel 27. Die Menge aller geraden natürlichen Zahlen und die Menge aller ungeraden natürlichen Zahlen bilden zusammen eine Partition der natürlichen Zahlen. Genauer, falls G die Menge der geraden natürlichen Zahlen und U die Menge der ungeraden natürlichen Zahlen ist, dann ist die Menge $\{G, U\}$ eine Partition von \mathbb{N} mit zwei Blöcken.

Übung 18.

- Geben Sie eine Partition von \mathbb{N} in unendlich viele Blöcke an.
- Geben Sie eine Partition von \mathbb{N} an, deren Blöcke alle unendlich gross sind.
- Geben Sie eine Menge X an, so dass

$$\{X, \{n \in \mathbb{N} \mid n > 15\}\}$$

eine Partition von \mathbb{N} ist.

Lösung.

- Z.B. $\{\{0\}, \{1\}, \dots\}$ also $\{P_i \mid i \in \mathbb{N}\}$ mit $P_i = \{i\}$.
- z.B. $\{P_1, P_2\}$ mit $P_1 = \{x \in \mathbb{N} \mid x \text{ ist gerade}\}$ und $P_2 = \{x \in \mathbb{N} \mid x \text{ ist ungerade}\}$.
- $X = \{x \in \mathbb{N} \mid x \leq 15\}$.

Definition 24 (Tupel). Ein n -Tupel ist ein Term von der Form

$$(x_1, \dots, x_n).$$

Für beliebige Tupel gilt per Definition:

$$(x_1, \dots, x_n) = (y_1, \dots, y_k) :\Leftrightarrow n = k \wedge x_1 = y_1 \wedge \dots \wedge y_n = x_n.$$

2-Tupel nennen wir *Paare* und 3-Tupel *Tripel*.

Bemerkung 24. Tupel sind die mathematische Entsprechung zu Listen und Arrays in der Informatik.

Definition 25. Es seien A_1, \dots, A_n Mengen und $n \in \mathbb{N}$ mit $n > 0$. Das *kartesische Produkt* von A_1, \dots, A_n , ist die Menge aller n -Tupel mit Einträgen aus den Mengen A_1, \dots, A_n :

$$\prod_{i=1}^n A_i = \{(a_1, \dots, a_n) \mid a_1 \in A_1 \wedge \dots \wedge a_n \in A_n\}.$$

Bemerkung 25. Für das kartesische Produkt von A_1, \dots, A_n schreiben wir auch $A_1 \times A_2 \times \dots \times A_n$. Insbesondere schreiben wir $X \times Y$ für das kartesische Produkt von zwei Mengen X und Y , konkret heisst das:

$$X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}.$$

Beispiel 29. Die Menge der rationalen Zahlen

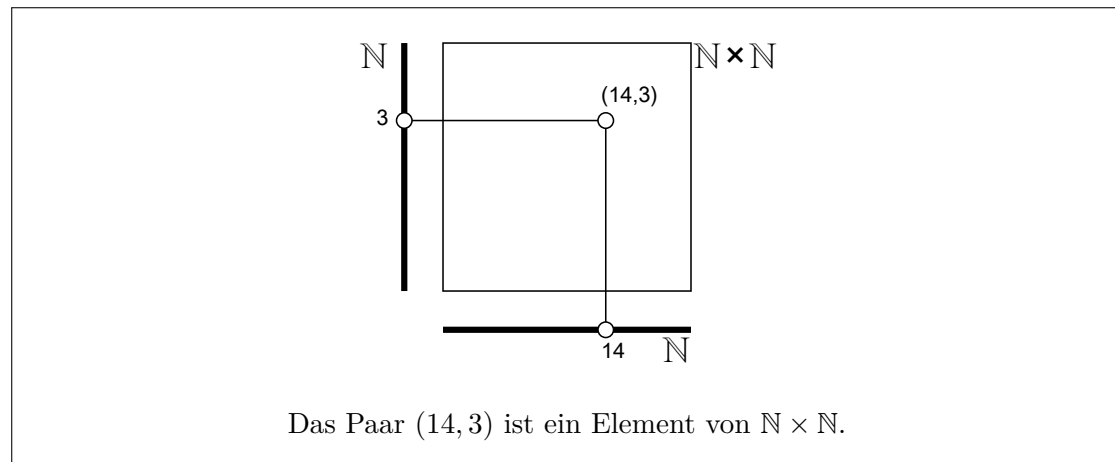
$$\mathbb{Q} := \left\{ \frac{x}{y} \mid x \in \mathbb{Z} \wedge y \in \mathbb{N} \setminus \{0\} \right\}$$

kann man als das Kartesische Produkt

$$\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$$

interpretieren.

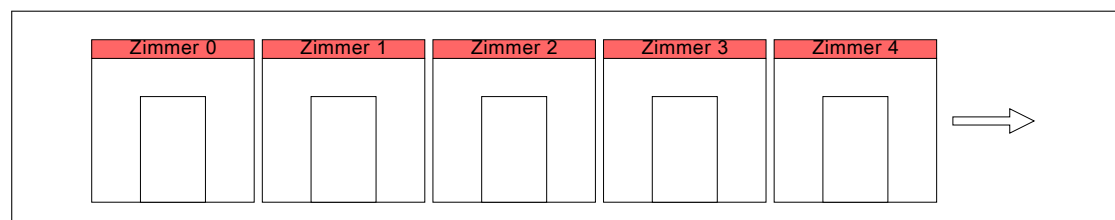
Beispiel 28. Das Kartesische Produkt der Menge \mathbb{N} mit sich selbst enthält alle möglichen Paare von natürlichen Zahlen.



3.2 Größenvergleiche von unendlichen Mengen

Bevor wir uns mit unendlichen Mengen befassen, sollten wir uns darüber im Klaren sein, dass unser “gesunder Menschenverstand” ein gefährlicher Begleiter auf diesem Weg sein kann. Um zu sehen wie heikel die Vermischung von alltäglichen Konzepten mit der Vorstellung des Unendlichen sind, betrachten wir ein Hotel mit unendlich vielen Zimmern – das sogenannte Hilbert Hotel.

Beispiel 30 (Hilbert’s Hotel). Hilbert’s Hotel hat unendlich viele Zimmer, für jede natürliche Zahl eines.



Im Rahmen eines Ferienjobs haben Sie eine Stelle als Concierge in Hilbert’s Hotel angenommen². An Ihrem ersten Arbeitstag haben Sie die Nachtschicht. Herr Hilbert, der Hotelbesitzer, hat sich bereits zu seinem wohlverdienten Feierabend verabschiedet, als unvermittelt ein älterer Herr (ä.H.) die Lobby betritt.

ä.H.: Ich bräuchte ein Zimmer in Ihrem Hotel.

Sie: Es tut mir leid, wir sind voll belegt. Ich könnte Ihnen aber das Hotel “Cantors Paradise” empfehlen. Es ist hier ganz in der Nähe, hier steht die Adresse.

²Sie verdienen schliesslich für jedes Zimmer einen Franken pro Arbeitstag.

Sie überreichen dem ä.H. eine Visitenkarte vom "Cantors Paradise".

ä.H.: Mein lieber Concierge, laut Werbebroschüre hat Ihr Hotel unendlich viele Zimmer. Wie soll denn das bitte ausgebucht sein?

Sie: Naja, wir haben im Moment unendlich viele Gäste – in jedem Zimmer einen.

ä.H.: Das lass ich mal Ihr Problem sein! Mir genügt es, dass hier schwarz auf weiss steht, dass man angeblich keine Reservation zu tätigen braucht, um in diesem Hotel unterzukommen. Zudem werben Sie, mit Bezugnahme auf die Unendlichkeit Ihres Hotels, damit, dass jedem Gast und zu jeder Zeit ein Zimmer garantiert werden kann!

Der ä.H. kramt genervt seine Werbebroschüre hervor und zeigt sichtlich irritiert auf die entsprechende Seite.

Sie: Hmm, ich werde sehen, ob sich da vielleicht doch was machen lässt. Bitte gedulden Sie sich einen Moment.

Der ä.H. lässt sich auf die grosse Couch fallen, die in der Eingangshalle steht. Sie, nicht ohne ein ziemlich ungutes Gefühl dabei zu haben, wählen Hilberts private Telefonnummer.

Hi.: Hilbert am Apparat.

Sie: Entschuldigen Sie die späte Störung Herr Hilbert. Es ist mir unendlich unangenehm, aber ich habe hier im Hotel ein Problem.

Hi. Worum geht es denn?

Sie: Ich habe einen Gast, der trotz Vollbelegung auf ein Zimmer besteht. Und er kann sich erst noch auf unsere eigene Broschüre stützen, in der ja steht, dass wir nie ausgebucht seien, selbst dann nicht, wenn wir mal voll sein sollten!

Hi.: Ach ja, ich hatte vergessen Sie darauf aufmerksam zu machen. Alle unsere Gäste haben sich beim Bezug ihres Zimmers, im Kleingedruckten, damit einverstanden erklärt, dass wir sie im Notfall ein einziges Mal umplazieren können. Nutzen Sie diese Klausel um unserem Gast ein Zimmer frei zu machen. Noch etwas, machen Sie das Zimmer so frei, dass sie weitere Gäste, die vielleicht später noch kommen, ebenfalls noch unterbringen könnten und bedenken Sie stets, dass jeder Gast höchstens einmal umplaziert werden darf.

Sie beenden das Gespräch und wenden sich dem ungeduldig wartenden ä.H. zu.

Sie: Sehr geehrter Herr, wir haben ein Zimmer für Sie gefunden, sie müssen sich bloss zwei Minuten gedulden, dann können Sie einziehen.

ä.H.: Sehen Sie, geht doch!

Wie bringen Sie den ä.H. unter? Bringen Sie weitere Gäste unter? Was machen Sie, wenn ein voller Limesbus (ein Bus mit unendlich vielen Sitzplätzen) ankommt? Wie lange dauert es bis der ganze Limesbus untergebracht wird?

Definition 26.

- Eine Menge X heisst *endlich*, wenn es eine natürliche Zahl n und eine Darstellung der Form $X = \{x_1, x_2, \dots, x_n\}$ gibt.
- Nicht endliche Mengen nennen wir *unendlich*.
- Eine Menge X heisst *abzählbar*, wenn eine surjektive Abbildung $F : \mathbb{N} \rightarrow X$ existiert oder wenn $X = \emptyset$ gilt.
- Die Menge X heisst *abzählbar unendlich*, wenn X abzählbar und unendlich ist.
- Eine *überabzählbare* Menge ist eine Menge, die nicht abzählbar ist.

Bemerkung 26. Ähnlich wie im Fall von endlichen Mengen, ist jede abzählbare Menge X von der Form

$$X = \{a_0, a_1, a_2, \dots\} = \{a_i \mid i \in \mathbb{N}\}.$$

Den Zusammenhang zu Definition 26 liefert hier die Funktion $F : \mathbb{N} \rightarrow X$, die durch $F(i) = a_i$ gegeben ist.

Bemerkung 27. Abzählbare Mengen kann man sich auch als die Mengen vorstellen, deren Elemente von den natürlichen Zahlen durchnummeriert (Wiederholungen erlaubt) werden können. Die Elemente einer abzählbaren Menge lassen sich also in eine Liste schreiben, die für jede natürliche Zahl eine Spalte hat.

\mathbb{N}	X
0	x
1	y
2	z
\vdots	\vdots

Beispiel 31. Die Menge aller geraden natürlichen Zahlen ist abzählbar.

Beweis. Ist G die Menge der geraden Zahlen, dann folgt die Behauptung aus der Tatsache, dass die Funktion

$$F : \mathbb{N} \rightarrow G \quad \text{mit} \quad F(n) = 2n$$

jede gerade natürliche Zahl trifft (und somit surjektiv ist). □

Dass die Menge der geraden natürlichen Zahlen auch anschaulich abzählbar ist, kann man sich etwa mit folgender Auflistung vergegenwärtigen:

\mathbb{N}	G
0	0
1	2
2	4
\vdots	\vdots

Beispiel 32. Die Menge \mathbb{Z} der ganzen Zahlen ist abzählbar.

Beweis. Wir müssen eine Funktion $F : \mathbb{N} \rightarrow \mathbb{Z}$ angeben, die jedes Element von \mathbb{Z} trifft. Dies gelingt uns wie folgt:

$$F(n) = \begin{cases} -\frac{n}{2} & \text{falls } n \text{ gerade} \\ \frac{n+1}{2} & \text{falls } n \text{ ungerade.} \end{cases}$$

□

Anschaulich ergibt sich durch die Funktion F folgende Auflistung der ganzen Zahlen:

\mathbb{N}	\mathbb{Z}
0	0
1	1
2	-1
3	2
4	-2
5	3
\vdots	\vdots

Beispiel 33. Die Menge aller *endlichen* Sequenzen der Buchstaben a, b ist abzählbar unendlich. Eine mögliche Auflistung der endlichen Sequenzen ist etwa durch

\mathbb{N}	X
0	a
1	b
2	aa
3	ab
4	ba
5	bb
6	aaa
7	aab
8	aba
9	abb
\vdots	\vdots

gegeben.

Beispiel 34. Die Menge aller Java, C, C#, C++, Fortran... Programme ist abzählbar.

Beweis. Wenn jedes Programm mit seinem Bytecode identifiziert wird, dann entspricht jedes Programm einer endlichen 0, 1-Folge. Diese können, gleich wie endliche a, b -Sequenzen, abgezählt werden. \square

Satz 4. *Jede endliche Menge ist abzählbar.*

Beweis. Ist X eine endliche Menge, dann können wir X als $\{x_1, \dots, x_n\}$ mit einer natürlichen Zahl n schreiben. Da die leere Menge per Definition abzählbar ist, können wir annehmen, dass X mindestens ein Element x_1 besitzt. Wir definieren nun die Funktion $F : \mathbb{N} \rightarrow X$ mit

$$F(i) = \begin{cases} x_i & \text{falls } 0 < i \leq n \\ x_1 & \text{sonst.} \end{cases}$$

Da F offensichtlich jedes Element von $X = \{x_1 \dots x_n\}$ trifft, ist F surjektiv. Somit ist X abzählbar. \square

Satz 5. *Jede Teilmenge einer abzählbaren Menge ist abzählbar.*

Beweis. Es sei $X \subset Y$ und Y sei eine abzählbare Menge. Da Y abzählbar ist, gibt es eine surjektive Funktion $F : \mathbb{N} \rightarrow Y$. Wenn $X = \emptyset$ gilt, dann ist X per Definition abzählbar und wir sind fertig. Ist $X \neq \emptyset$, dann gibt es ein Element $a \in X$. Wir können nun wie folgt eine Abbildung $G : \mathbb{N} \rightarrow Y$ angeben.

$$G(x) = \begin{cases} F(x) & \text{falls } F(x) \in X \\ a & \text{sonst.} \end{cases}$$

Da $X \subset Y$ gilt und weil jedes Element von Y von der Funktion F getroffen wird, wird auch jedes Element von Y von G getroffen. Somit ist $G : \mathbb{N} \rightarrow Y$ surjektiv und Y ist also surjektiv. \square

Satz 6. *Ist X eine abzählbare Menge und gibt es eine surjektive Funktion $F : X \rightarrow Y$, dann ist auch Y abzählbar.*

Beweis. Sollte X die leere Menge sein, dann ist auch Y leer und somit abzählbar. Ist X nichtleer, dann folgt aus der Abzählbarkeit von X , dass es eine surjektive Abbildung $G : \mathbb{N} \rightarrow X$ gibt. Wir können nun die Funktion $H : \mathbb{N} \rightarrow Y$ durch Komposition der Funktionen F und G bilden, d.h. wir definieren

$$H : \mathbb{N} \rightarrow Y \quad \text{mit} \quad H(n) = F(G(n)).$$

Wir müssen nun noch zeigen, dass wir mit der Funktion H jedes Element von Y treffen. Wir nehmen dazu ein beliebiges Element y von Y und zeigen, dass es eine natürliche Zahl n gibt mit $H(n) = y$. Es sei also $y \in Y$ beliebig. Da die Funktion $F : X \rightarrow Y$ surjektiv ist, muss es ein $x \in X$ geben so, dass $F(x) = y$ gilt. Weil aber auch die Funktion $G : \mathbb{N} \rightarrow X$ surjektiv ist, muss es ebenfalls eine natürliche Zahl n geben, mit

gibt. Da für jede natürliche Zahl i die Menge A_i abzählbar ist, gibt es für jede natürliche Zahl i auch eine surjektive Funktion $F_i : \mathbb{N} \rightarrow A_i$. Wir können die Vereinigungsmenge der A_i 's also wie folgt schreiben:

$$\begin{aligned} \bigcup_{i \in \mathbb{N}} A_i &= \{F_i(j) \mid i, j \in \mathbb{N}\} \\ &= \{F_i(j) \mid (i, j) \in \mathbb{N} \times \mathbb{N}\}. \end{aligned}$$

Daraus folgt, dass die Funktion

$$H : \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_{i \in \mathbb{N}} A_i \quad \text{mit} \quad H(i, j) = F_i(j),$$

die gesuchte surjektive Funktion ist. □

Folgerung. Die Menge $\mathbb{Z} \times \mathbb{Z}$ ist abzählbar.

Beweis. Wir wissen bereits, dass die Menge $\mathbb{N} \times \mathbb{N}$ abzählbar ist. Daraus folgt, dass auch die Mengen

$$\begin{aligned} X &= \mathbb{N} \times \{-n \mid n \in \mathbb{N}\} \\ Y &= \{-n \mid n \in \mathbb{N}\} \times \mathbb{N} \\ Z &= \{-n \mid n \in \mathbb{N}\} \times \{-n \mid n \in \mathbb{N}\} \end{aligned}$$

abzählbar sind. Aus Satz 8 folgt also, dass die Menge

$$\mathbb{Z} \times \mathbb{Z} = (\mathbb{N} \times \mathbb{N}) \cup X \cup Y \cup Z$$

abzählbar ist. □

Folgerung. Die Menge $\mathbb{Q} = \{\frac{x}{y} \mid x, y \in \mathbb{Z}\}$ der rationalen Zahlen (Brüche) ist abzählbar.

Beweis. Da die Funktion

$$F : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Q} \quad \text{mit} \quad F(x, y) = \frac{x}{y}$$

surjektiv ist, folgt die Behauptung aus Satz 6. □

Übung 19. Ist die Menge aller endlichen Teilmengen von \mathbb{N} abzählbar? Begründen Sie Ihre Antwort.

Lösung. Wir können jede endliche Menge von natürlichen Zahlen via der Charakteristischen Funktion (vgl. Vorlesung) mit einer endlichen Binärsequenz identifizieren. Durch hinzufügen einer führenden 1 zu jeder endlichen Binärsequenz entspricht jede dieser Sequenzen einer natürlichen Zahl in Binärdarstellung. Daraus folgt die Behauptung.

Theorem 2 (Zweites Diagonalargument). *Die Menge aller unendlichen Binärsequenzen (Sequenzen aus Nullen und Einsen) ist überabzählbar.*

Beweis. Beweis durch Widerspruch. Wäre die Menge aller unendlichen Binärsequenzen abzählbar, dann gäbe es eine Liste von der Form³

\mathbb{N}	Binärsequenzen
0	$s_0 = 01101011 \dots$
1	$s_1 = 10010110 \dots$
2	$s_2 = 00101001 \dots$
\vdots	\vdots

in der alle unendlichen Binärsequenzen vorkommen. Wir konstruieren nun, ausgehend von dieser Liste, eine Binärsequenz b , die nicht in der Liste enthalten sein kann. Wir definieren b wie folgt:

$$\begin{aligned}
 0\text{-tes Glied} &= b(0) = 1 - s_0(0) \\
 1\text{-tes Glied} &= b(1) = 1 - s_1(1) \\
 2\text{-tes Glied} &= b(2) = 1 - s_2(2) \\
 &\vdots \\
 n\text{-tes Glied} &= b(n) = 1 - s_n(n) \\
 &\vdots
 \end{aligned}$$

Die Folge $b = 110\dots$ kann nicht in der Liste vorkommen, weil sie sich von jedem Element in der Liste in mindestens einem Glied unterscheidet (von der n -ten Sequenz unterscheidet sich b im n -ten Glied). Dies steht im Widerspruch zu unserer Annahme, dass in der Liste alle unendlichen Binärsequenzen vorkommen. \square

Folgerung. *Das Intervall $(0, 1) = \{r \in \mathbb{R} \mid 0 < r < 1\}$ ist überabzählbar. Insbesondere ist die Menge \mathbb{R} der reellen Zahlen überabzählbar.*

Beweis. Die reellen Zahlen (in Binärdarstellung) im Intervall $(0, 1)$ sind von der Form $0, \dots$ wobei \dots für eine unendliche Binärsequenz steht. Daher steht das Intervall $(0, 1)$ mit der Menge aller unendlichen Binärsequenzen in eins-zu-eins Korrespondenz. Die Behauptung folgt daher aus Theorem 2. \square

Folgerung. *Die Potenzmenge von \mathbb{N} ist überabzählbar.*

Beweis. Jede Teilmenge A von \mathbb{N} kann wie folgt durch eine Binärsequenz χ_A beschrieben werden:

$$\chi_A(n) = \begin{cases} 1 & \text{falls } n \in A \\ 0 & \text{falls } n \notin A. \end{cases}$$

³Natürlich ist die angedeutete Liste Beispielhaft und dient nur der Veranschaulichung unserer Konstruktion der Sequenz b . Die Sequenz s_0 , beispielsweise, könnte auch mit dem Präfix 00000100 oder irgend einer anderen Folge von Nullen und Einsen beginnen.

Daher folgt die Behauptung aus Theorem 2. □

Folgerung. *Die Menge aller Funktionen $F : \mathbb{N} \rightarrow \mathbb{N}$ ist überabzählbar.*

Beweis. Die Menge der Binärsequenzen entspricht der Menge der Funktionen $F : \mathbb{N} \rightarrow \{0, 1\}$. Daher folgt die Behauptung aus Theorem 2. □

Folgerung. *Es gibt Funktionen $F : \mathbb{N} \rightarrow \mathbb{N}$, die von keinem Java, C, C++, Fortran... Programm berechenbar sind. Solche Funktionen heissen unberechenbar.*

Übung 20. Zeigen Sie, dass die Menge

$$U = \{1, 11, 111, 1111, \dots\}$$

aller endlichen Sequenzen von Einsen abzählbar ist. Ist die Menge aller unendlichen⁴ Sequenzen von Einsen auch abzählbar?

Lösung. Wir müssen zeigen, dass eine surjektive Abbildung $F : \mathbb{N} \rightarrow \{1, 11, \dots\}$ existiert. Da dies z.B. für die Funktion

$$F(n) = \underbrace{11 \dots 1}_{n \text{ viele}}$$

erfüllt ist, gilt die Behauptung. Die Menge aller (abzählbar) unendlichen 1-Sequenzen besteht aus nur einem Element und ist somit natürlich abzählbar.

⁴Streng genommen müsste man hier nach der Menge der “abzählbar langen” Sequenzen von Einsen fragen.

4 Relationen

Relevanz für die Informatik

Beziehungen werden in der Mathematik mit Relationen modelliert. Als Modell für ein derart fundamentales Konzept sind Relationen sowohl in der Mathematik als auch in der Informatik nahezu allgegenwärtig. Einige Beispiele von Relationen in der Informatik:

- Relationale Datenbanken
- E-R-Diagramme
- Zustandsklassen von endlichen Automaten
- Input-Output Relation
- Funktionen
- \vdots

Lernziele

Sie kennen

- Äquivalenzrelationen und Äquivalenzklassen sowie ihre grundlegenden Eigenschaften.
- Ordnungsrelationen (in den verschiedenen Variationen) und ihre grundlegenden Eigenschaften.

Sie verstehen

- den Zusammenhang von Äquivalenzrelationen und Partitionen.
- die Problematik der “Wohldefiniertheit” von Funktionen auf Faktormengen.

Sie sind in der Lage

- (endliche) Ordnungsrelationen als Hasse Diagramme zu skizzieren.
- eine Ordnungsrelation aus einem Hasse Diagramm abzulesen.

Literatur und Links

Ergänzende Literatur:

- [3] Kapitel 4.1 bis 4.3.
- [4] Kapitel 1.4 und 1.5.

Nützliche Links:

- http://de.wikipedia.org/wiki/Relation_%28Mathematik%29
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Relation
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Relation:_Bin%C3%A4re_Relation
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Relation:_%C3%84quivalenzrelation
- http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Relation:_Ordnungsrelation

4.1 Grundlagen

Relationen beschreiben Beziehungen zwischen (mathematischen) Objekten. Es soll die ganze Bandbreite an möglichen Beziehungen modelliert werden können. Folgend, vier völlig verschiedene Relationen.

Beispiel 35. Wir definieren die Relationen R_1 , R_2 , R_3 und T durch folgende Zuordnungen:

- Zwei Geraden stehen in Relation R_1 zu einander, wenn sie parallel sind. Dies ist eine (binäre) Relation auf der Menge aller Geraden.
- Zwei Punkte auf der Erdoberfläche stehen zueinander in Relation R_2 , wenn der erste Punkt zu Fuss (und ohne weitere Hilfsmittel) vom zweiten Punkt aus erreichbar ist.
- Eine Person P steht in Relation R_3 zu Person Q , wenn P in Q verliebt ist.
- Eine natürliche Zahl x steht in Relation T zu einer natürlichen Zahl y , falls x ein Teiler von y ist.

Wie können wir den Relationsbegriff fassen, damit wir möglichst keinen Einschränkungen unterliegen, wenn wir beliebige (auch beliebig exotische) Beziehungen als Relationen modellieren/auffassen wollen? Wie können wir also die Definition einer Relation möglichst weitläufig fassen?

Definition 27. Eine n -Stellige *Relation* R auf den Mengen A_1, \dots, A_n ist eine Menge von n -Tupeln aus $A_1 \times \dots \times A_n$. Mit anderen Worten, die Relationen auf A_1, \dots, A_n sind genau die Teilmengen

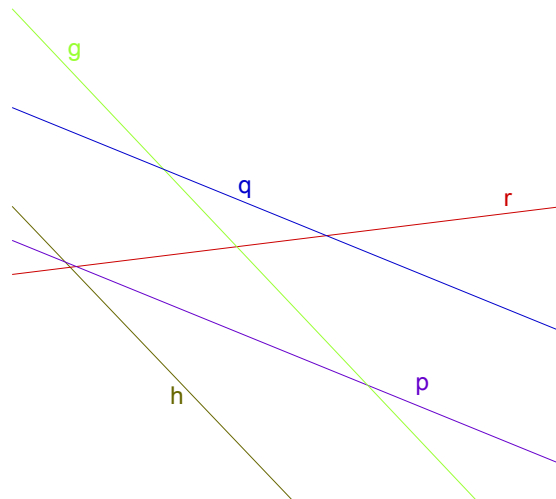
$$R \subset \prod_{i=1}^n A_i.$$

Ist R eine n -stellige Relation und gilt $(x_1, \dots, x_n) \in R$, dann sagen wir, dass die Elemente x_1, \dots, x_n zueinander in Relation R stehen. Eine 2-stellige Relation $R \subset X \times Y$ heisst auch eine *binäre Relation* auf den Mengen X und Y .

Notation. Ist R eine binäre Relation und sind x, y Elemente mit $(x, y) \in R$ (d.h. x steht in Relation R zu y), dann schreiben wir auch xRy .

Wir werden uns im Folgenden auf binäre Relationen beschränken.

Beispiel 36. Wir betrachten die Relation R_1 von Beispiel 35 auf der Menge $\{g, h, p, q, r\}$. Die Geraden g, h, p, q, r sind wie im folgenden Bild gegeben:



Offenbar gelten folgende Beziehungen:

- Die Gerade g steht in Relation R_1 zu folgenden Geraden: g, h .
- Die Gerade h steht in Relation R_1 zu folgenden Geraden: g, h .
- Die Gerade p steht in Relation R_1 zu folgenden Geraden: p, q .
- Die Gerade q steht in Relation R_1 zu folgenden Geraden: p, q .
- Die Gerade r steht mit keiner anderen Geraden in Relation R_1 .

Als Menge geschrieben, nimmt die Relation¹ R_1 also folgende Gestalt an:

$$R_1 = \{(g, g), (g, h), (h, h), (h, g), (p, p), (p, q), (q, q), (q, p), (r, r)\}.$$

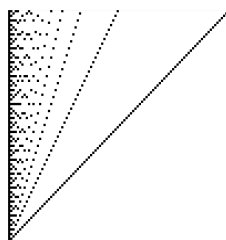
Bildlich lässt sich die Relation als Tabelle darstellen:

r	\times	\times	\times	\times	\checkmark
q	\times	\times	\checkmark	\checkmark	\times
p	\times	\times	\checkmark	\checkmark	\times
h	\checkmark	\checkmark	\times	\times	\times
g	\checkmark	\checkmark	\times	\times	\times
	g	h	p	q	r

Aus der Tabelle erhält man sofort den Graph der Relation:

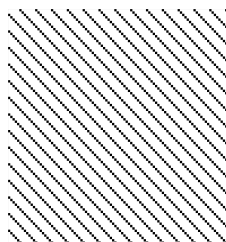
r					■
q			■	■	
p			■	■	
h	■	■			
g	■	■			
	g	h	p	q	r

Beispiel 37. Eine schematische Darstellung vom Graph der Teilbarkeitsrelation (die Relation T von Beispiel 35) auf der Menge $\{n \in \mathbb{N} \mid 1 < n < 100\}$.



Der Graph der Relation

$$R = \{(x, y) \mid x, y \in \mathbb{N} \wedge x, y < 100 \wedge x + y \text{ ist ein Vielfaches von } 7\}$$



¹Streng genommen sprechen wir hier von der Einschränkung von R_1 auf die Menge $\{g, h, p, r, r\}$.

Definition 28. Eine binäre Relation R auf einer Menge X heisst:

- *Reflexiv*, wenn für alle $x \in X$

$$xRx$$

gilt.

- *Symmetrisch*, wenn für alle $x, y \in X$

$$xRy \Rightarrow yRx$$

gilt.

- *Antisymmetrisch*, wenn für alle $x, y \in X$

$$xRy \wedge yRx \Rightarrow x = y$$

gilt.

- *Transitiv*, wenn für alle $x, y, z \in X$

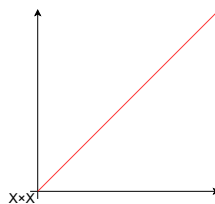
$$xRy \wedge yRz \Rightarrow xRz$$

gilt.

Bemerkung 28. Die Relation $R \subset X \times X$ ist genau dann reflexiv, wenn die Diagonale

$$\Delta_X := \{(x, x) \mid x \in X\}$$

eine Teilmenge von R ist. Graphisch heisst das, dass die Diagonale (rot markiert) in R enthalten ist.



Die Relation R ist symmetrisch, wenn ihr Graph symmetrisch bezüglich der Geraden Δ_X ist.

Beispiel 38. Wir betrachten nochmals die Verliebtheitsrelation aus Beispiel 35:

$$pLq :\Leftrightarrow \text{Person } p \text{ liebt Person } q.$$

Die Verliebtheitsrelation hat unter anderem folgende Eigenschaften:

- L ist nicht reflexiv, da nicht alle Menschen “selbstverliebt” sind.
- L ist (leider²) nicht symmetrisch, da Liebe nicht immer auf Gegenseitigkeit beruht.
- L ist nicht Antisymmetrisch, da es durchaus “echte” Liebespaare (aus zwei Partnern bestehend) gibt.
- L ist nicht transitiv, da die Meisten Leute den angebeteten der eigenen angebeteten nicht lieben (ganz im Gegenteil!).

Übung 21. Geben sie binäre Relationen (auf der Menge aller Menschen) mit folgenden Eigenschaften an:

- a) Transitiv und nicht antisymmetrisch.
- b) Transitiv, reflexiv und antisymmetrisch.
- c) Nicht reflexiv, nicht transitiv.

Lösung. Zum Beispiel:

- a) $pJq :\Leftrightarrow$ Person p ist jünger als Person q .
- b) $pWq :\Leftrightarrow$ Person p hat denselben Wohnort wie Person q .
- c) $pGq :\Leftrightarrow$ Person p ist vom anderen Geschlecht als Person q .

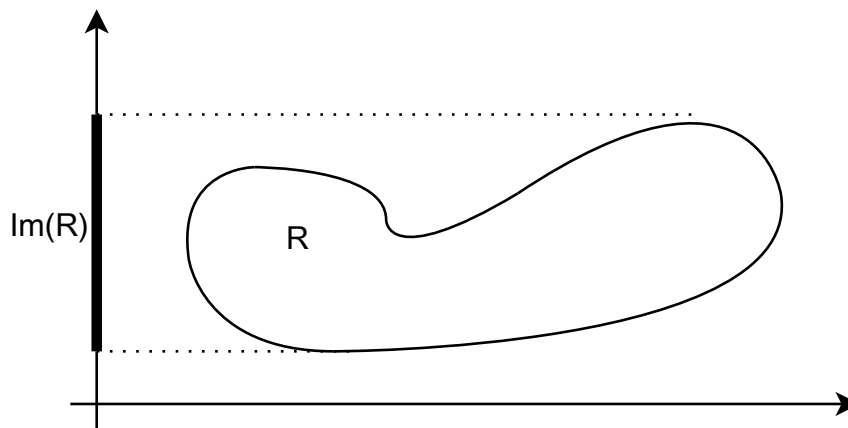
Definition 29. Ist $R \subset X \times Y$ eine Relation, dann ist das *Bild* von R definiert als:

$$Im(R) = \{y \in Y \mid \exists x \in X (xRy)\}.$$

Beispiel 39. Das Bild der “Verliebtheitsrelation” (R_3 aus Beispiel 35 oder L vom vorherigen Beispiel) ist genau die Menge aller Menschen, die von mindestens jemandem geliebt werden.

Beispiel 40. Veranschaulichung der Bildmenge einer Relation R .

²Andererseits gäbe es wohl keine Literatur oder gar Kunst wenn diese Relation tatsächlich symmetrisch wäre.



Bemerkung 29. Jede Funktion $F : X \rightarrow Y$ kann man als Menge von Paaren

$$\{(x, y) \in X \times Y \mid y = F(x)\}$$

und somit als Relation auf $X \times Y$ ansehen. In diesem Kontext stimmen die Bildmenge

$$\{F(x) \mid x \in X\}$$

von F (als Funktion gesehen) und das Bild $Im(F)$ von F (als Relation gesehen) überein.

4.2 Äquivalenzrelationen

Äquivalenzrelationen sind in einem gewissen Sinn (konkret im Sinn von Satz 12) verallgemeinerte Gleichheitsrelationen. Sie werden dazu verwendet, (im Sinn der Relation) ähnliche Objekte miteinander zu identifizieren und als “gleich” zu behandeln.

Definition 30. *Äquivalenzrelationen* sind reflexive, symmetrische und transitive Relationen.

Beispiel 41. Auf jeder Menge X ist die Gleichheitsrelation $\Delta_X = \{(x, x) \mid x \in X\}$ eine Äquivalenzrelation. Weil jede Äquivalenzrelation reflexiv ist, ist die Gleichheitsrelation auf jeder Menge die “kleinste” Äquivalenzrelation. Am anderen Ende des Spektrums steht die Relation $X \times X$, sie ist die grösste Äquivalenzrelation auf der Menge X .

Beispiel 42. Von den Relationen R_1, R_2, R_3 und T aus Beispiel 35, sind R_1, R_2 Äquivalenzrelationen.

- Die Relation R_3 ist keine Äquivalenzrelation weil sie nicht reflexiv (nicht jeder liebt sich selbst), nicht symmetrisch (es gibt unglücklich Verliebte) und nicht transitiv ist. Man beachte, dass jeder einzelne der genannten Gründe genügt, damit R_3 keine Äquivalenzrelation ist.

- Die Relation T ist zwar reflexiv und transitiv, aber nicht symmetrisch und daher auch keine Äquivalenzrelation.

Definition 31. Es sei R eine Äquivalenzrelation auf einer Menge X und $x \in X$. Die *Äquivalenzklasse* $[x]_R$ von x bezüglich R ist die Menge aller Elemente von X , die zu x in Relation R stehen:

$$[x]_R := \{y \in X \mid xRy\}$$

Jedes Element einer Äquivalenzklasse nennen wir einen *Repräsentanten* der entsprechenden Äquivalenzklasse. Die *Faktormenge* X/R von X modulo R ist die Menge aller Äquivalenzklassen:

$$X/R := \{[x]_R \mid x \in X\}$$

Beispiel 43. Wir betrachten die Relation \equiv_5 auf der Menge \mathbb{Z} , die wie folgt gegeben ist:

$$x \equiv_5 y :\Leftrightarrow (x - y) \text{ ist ein Vielfaches von } 5.$$

Als Java Code könnte man die Relation auch wie folgt darstellen:

```
static boolean Rel(int x, int y){
    if (y<0) return Rel(x,y+5);
    if (x<0) return Rel(x+5,y);
    return x % 5 == y % 5;
}
```

Wir überzeugen uns nun davon, dass diese Relation eine Äquivalenzrelation ist.

- **Reflexivität:** Es gilt für jede ganze Zahl z

$$0 \cdot 5 = 0 = (z - z).$$

Also ist $(z - z)$ ein Vielfaches von 5, somit gilt $z \equiv_5 z$.

- **Symmetrie:** Gilt $x \equiv_5 y$, dann gibt es eine ganze Zahl z mit $5z = (x - y)$. Also ist auch

$$(y - x) = -(x - y) = -5z = 5 \cdot (-z)$$

ein Vielfaches von 5, d.h. es gilt $y \equiv_5 x$.

- **Transitivität:** Gilt $x \equiv_5 y$ und $y \equiv_5 z$, dann gibt es ganze Zahlen r, s mit $5r = x - y$ und $5s = y - z$. Insgesamt erhalten wir, dass

$$x - z = (x - y) + (y - z) = 5r + 5s = 5(r + s)$$

ein Vielfaches von 5 ist und somit, dass $x \equiv_5 z$ gilt.

4.2. ÄQUIVALENZRELATIONEN

Wir betrachten nun die Äquivalenzklassen modulo der Relation \equiv_5 (diese heissen Restklassen modulo 5).

$$\begin{aligned}[0]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 0 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid z \text{ ist ein Vielfaches von } 5\} \\ &= \{5z \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[1]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 1 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 1\} \\ &= \{5z + 1 \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[2]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 2 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 2\} \\ &= \{5z + 2 \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[3]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 3 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 3\} \\ &= \{5z + 3 \mid z \in \mathbb{Z}\}\end{aligned}$$

$$\begin{aligned}[4]_{\equiv_5} &= \{x \in \mathbb{Z} \mid 4 \equiv_5 y\} \\ &= \{z \in \mathbb{Z} \mid \text{Bei Division durch } 5 \text{ lässt } z \text{ den Rest } 4\} \\ &= \{5z + 4 \mid z \in \mathbb{Z}\}\end{aligned}$$

Die Faktormenge der Relation \equiv_5 ist also durch

$$\mathbb{Z}/_{\equiv_5} = \{[0]_{\equiv_5}, [1]_{\equiv_5}, [2]_{\equiv_5}, [3]_{\equiv_5}, [4]_{\equiv_5}\}$$

gegeben.

Lemma 2. *Ist \sim eine Äquivalenzrelation auf einer Menge X und gilt $x, y \in X$ mit $x \sim y$, dann gilt $[x]_{\sim} = [y]_{\sim}$. Mit anderen Worten, äquivalente Elemente repräsentieren stets dieselbe Äquivalenzklasse.*

Beweis. Seien X, \sim, x, y wie in der Behauptung. Um zu zeigen, dass $[x]_{\sim} = [y]_{\sim}$ gilt, genügt es nachzuweisen, dass $x \sim z \Leftrightarrow y \sim z$ für beliebige $z \in X$ gilt. Wir nehmen $x \sim y$ an, dann gilt

$$y \sim z \Rightarrow x \sim y \wedge y \sim z \xrightarrow{\text{Transitivität}} x \sim z$$

und

$$x \sim z \Rightarrow x \sim y \wedge x \sim z \xrightarrow{\text{Symmetrie}} y \sim x \wedge x \sim z \xrightarrow{\text{Transitivität}} y \sim z,$$

wie gewünscht. □

Folgerung. Ist \sim eine Äquivalenzrelation auf X und sind $x, y \in X$ mit $x \in [y]_\sim$, dann gilt $[x]_\sim = [y]_\sim$. Mit anderen Worten, jedes Element einer Äquivalenzklasse ist auch ein Repräsentant dieser Äquivalenzklasse.

Beweis. Es seien X, \sim, x und y wie in der Behauptung. Aus $x \in [y]_\sim$ folgt $y \sim x$. Die Behauptung folgt nun aus Lemma 2. \square

Satz 9. Ist \sim eine Äquivalenzrelation auf X und sind $x, y \in X$ mit $[x]_\sim \neq [y]_\sim$, dann gilt $[x]_\sim \cap [y]_\sim = \emptyset$. Mit anderen Worten, verschiedene Äquivalenzklassen sind immer disjunkt.

Beweis. Es seien X, \sim, x und y wie in der Behauptung. Wir zeigen die Kontraposition, d.h.

$$[x]_\sim \cap [y]_\sim \neq \emptyset \Rightarrow [x]_\sim = [y]_\sim.$$

Es gelte also $[x]_\sim \cap [y]_\sim \neq \emptyset$, es gibt daher ein $z \in [x]_\sim \cap [y]_\sim$. Daraus folgt, dass $x \sim z \wedge y \sim z$ gilt und wegen der Transitivität und der Symmetrie von \sim folgt sofort $x \sim y$. Die Behauptung folgt nun aus Lemma 2. \square

Satz 10. Ist \sim eine Äquivalenzrelation auf einer Menge X , dann ist die Faktormenge X/\sim eine Partition von X .

Beweis. Es sei \sim eine beliebige Äquivalenzrelation auf einer Menge X . Wir müssen folgende Punkte verifizieren:

- a) Die Äquivalenzklassen sind alle nichtleer.
- b) Die Äquivalenzklassen paarweise disjunkt.
- c) Es gilt

$$\bigcup_{x \in X} [x]_\sim = X.$$

Der erste Punkt folgt aus der Definition von der Faktormenge (die Äquivalenzklassen sind via ihrer Repräsentanten definiert). Die Tatsache, dass die Äquivalenzklassen paarweise disjunkt sind, ist genau die Aussage von Satz 9. Wir brauchen also bloss noch den letzten Punkt zu verifizieren. Dies folgt, da für jedes $z \in X$, wegen der Transitivität von \sim , $z \sim z$ und somit

$$z \in [z]_\sim \subset \bigcup_{x \in X} [x]_\sim$$

gilt. \square

Bemerkung 30. Das Konzept von Äquivalenzklassen (und deren Zusammenhang mit Partitionen) werden Sie in der theoretischen Informatik in Form von sogenannten “Zustandsklassen” wiederfinden, diese werden dort gebraucht, um zu zeigen, dass es Sprachen gibt, die nicht mit “endlichen Zustandsautomaten” erkannt werden können.

Übung 22. Gegeben Sei die Äquivalenzrelation

$$pRq :\Leftrightarrow p \text{ hat am gleichen Tag Geburtstag wie } q.$$

Kommentieren Sie folgende Aussagen mit wahr, falsch oder unklar (unter der Annahme $\text{Ray } R \text{ Greg}$):

- a) Ray ist älter als Greg oder Greg ist älter als Ray.
- b) Ray und Greg sind gleich alt.
- c) Ray ist verwandt mit Greg.
- d) Der Altersunterschied von Ray und Greg in Jahren ist ganzzahlig.

Lösung. d) ist wahr, die restlichen Aussagen sind aufgrund der Annahmen nicht entscheidbar.

Übung 23. Wie viele Äquivalenzklassen hat die Relation R von Übung 22?

Lösung. 366 (Auch in Schaltjahren haben an jedem Tag Leute Geburtstag.)

Wir haben in Satz 10 gesehen, dass jede Äquivalenzrelation auf einer Menge eine Partition auf eben dieser Menge induziert. Als Nächstes sehen wir, dass auch die Umkehrung gilt; jede Partition induziert eine Äquivalenzrelation, deren Faktormenge genau der ursprünglichen Partition entspricht. Insgesamt sehen wir, dass eine eins-zu-eins Korrespondenz zwischen allen möglichen Partitionen und allen möglichen Äquivalenzrelationen auf einer gegebenen Menge existiert.

Satz 11. Ist $P = \{A_i \mid i \in I\}$ eine Partition von der Menge X , dann ist die Relation \sim , gegeben durch

$$x \sim y :\Leftrightarrow \exists i \in I (x \in A_i \wedge y \in A_i),$$

eine Äquivalenzrelation auf X . Zusätzlich gilt

$$X/\sim = P.$$

Beweis. Zuerst zeigen wir, dass die Relation \sim unter den gegebenen Umständen eine Äquivalenzrelation ist.

- **Reflexivität:** Sei $x \in X$ beliebig. Wir müssen zeigen, dass $x \sim x$ gilt. Da $P = \{A_i \mid i \in I\}$ eine Partition von X ist, gibt es ein $i \in I$ mit $x \in A_i$, daraus folgt sofort $x \sim x$.

- **Symmetrie:** Es gelte $x \sim y$. Wir müssen $y \sim x$ zeigen. Aus $x \sim y$ folgt, dass es ein $i \in I$ mit $x \in A_i \wedge y \in A_i$ gibt, dies ist offensichtlich äquivalent zu $y \sim x$.
- **Transitivität:** Es gelte $x \sim y \wedge y \sim z$. Wir müssen $x \sim z$ zeigen. Aus $x \sim y \wedge y \sim z$ folgt, dass es $i, j \in I$ gibt so, dass $x, y \in A_i$ und $y, z \in A_j$ gilt. Da $P = \{A_i \mid i \in I\}$ eine Partition ist, kann y nicht in zwei verschiedenen Blöcken enthalten sein, es gilt daher $i = j$ und somit $x \sim z$.

Dass die Äquivalenzklassen von \sim genau den Blöcken von P entsprechen ist sofort klar, wenn man beachtet, dass zwei Elemente genau dann äquivalent sind, wenn sie im selben Block von P liegen. \square

Am Anfang dieses Abschnittes haben wir Äquivalenzrelationen als verallgemeinerte Gleichheitsrelationen beschrieben, dies können wir im folgenden Satz präzisieren.

Satz 12. *Für jede Relation \sim auf einer Menge X sind folgende beiden Aussagen äquivalent.*

1. *Die Relation \sim ist eine Äquivalenzrelation.*
2. *Es gibt eine Menge Y und eine Funktion $F : X \rightarrow Y$ so, dass für alle $x, y \in X$*

$$x \sim y \Leftrightarrow F(x) = F(y)$$

gilt.

Beweis. Wenn \sim eine Äquivalenzrelation auf der Menge X ist, dann erfüllt die Abbildung

$$F : X \rightarrow \mathcal{P}(X) \quad \text{mit} \quad F(x) = [x]_{\sim}$$

alle geforderten Eigenschaften. Ist umgekehrt eine Funktion $F : X \rightarrow Y$ wie in der Behauptung gegeben, dann gilt für die Relation \sim Folgendes:

- **Reflexivität** gilt, da für jedes Element $x \in X$ trivialerweise $F(x) = F(x)$ gilt.
- **Symmetrie** folgt, da für beliebige Elemente $x, y \in X$

$$x \sim y \Rightarrow F(x) = F(y) \Rightarrow F(y) = F(x) \Rightarrow y \sim x$$

gilt.

- **Transitivität** folgt, da für beliebige Elemente $x, y, z \in X$

$$x \sim y \wedge y \sim z \Rightarrow F(x) = F(y) \wedge F(y) = F(z) \Rightarrow F(x) = F(z) \Rightarrow x \sim z$$

gilt.

\square

Beispiel 44. Es sei \sim_{14} die folgendermassen auf der Menge $Fun(\mathbb{R}) = \{F \mid F : \mathbb{R} \rightarrow \mathbb{R}\}$ gegebene Relation:

$$F \sim G :\Leftrightarrow F(14) = G(14).$$

Wir betrachten die Funktion

$$Eval_{14} : Fun(\mathbb{R}) \rightarrow \mathbb{R} \quad \text{mit} \quad Eval_{14}(F) = F(14).$$

Offenbar gilt

$$F \sim_{14} G \Leftrightarrow Eval_{14}(F) = Eval_{14}(G).$$

Anhand von Satz 12 sehen wir also sofort, dass es sich bei \sim_{14} um eine Äquivalenzrelation handelt.

Bemerkung 31 (Wohldefiniertheitsproblem). Wir betrachten die Relation \simeq , die wie folgt auf der Menge \mathbb{N} gegeben ist.

$$n \simeq m \Leftrightarrow n, m \text{ haben die gleichen Primteiler.}$$

Nun definieren wir eine Funktion

$$F : \mathbb{N}/\simeq \rightarrow \mathbb{N} \quad F([x]_{\simeq}) := x + 102.$$

Es soll zum Beispiel $F([7]_{\simeq}) = 109$ gelten. Sehen Sie ein Problem bei unserem Vorgehen? Ist $F([49]_{\simeq}) = 151$? Es gilt doch $7 \simeq 49$ und somit auch $[7]_{\simeq} = [49]_{\simeq}$. Sollte dann nicht auch $F([7]_{\simeq}) = F([49]_{\simeq})$ gelten? Natürlich schon! Das Problem, das wir hier haben, nennt man ein *Wohldefiniertheitsproblem*. Es entsteht, wenn man Funktionswerte von Äquivalenzklassen mit Bezugnahme auf deren Repräsentanten definiert, ohne sicherzustellen, dass der Funktionswert nicht von der Wahl der Repräsentanten abhängt.

Sind eine Äquivalenzrelation \sim auf einer Menge X und eine Funktion $F : X \rightarrow Y$ gegeben, so erhält man nur dann durch die Zuordnung

$$\tilde{F}([x]_{\sim}) := F(x)$$

eine wohldefinierte Funktion

$$\tilde{F} : X/\sim \rightarrow Y,$$

wenn die Funktion F mit der Relation \sim verträglich ist. Das heisst, wenn

$$x \sim y \Rightarrow F(x) = F(y)$$

gilt.

Beispiel 45. Ein Beispiel (vgl. 43) für eine wohldefinierte Abbildung

$$F : \mathbb{Z}/\equiv_5 \rightarrow \mathbb{Z}/\equiv_5$$

erhalten wir z.B. durch die Zuordnung

$$F([x]_{\equiv_5}) := [2x + 3]_{\equiv_5}.$$

Um zu sehen, dass diese Funktion tatsächlich wohldefiniert ist, betrachten wir:

$$\begin{aligned}
 x \equiv_5 y &\Rightarrow (x - y) \text{ ist Vielfaches von } 5 \\
 &\Rightarrow \exists z \in \mathbb{Z} (5z = x - y) \\
 &\Rightarrow \exists z \in \mathbb{Z} ((2x + 3) - (2y + 3) = 2x - 2y = 2(x - y) = 5(2z)) \\
 &\Rightarrow (2x + 3) - (2y + 3) \text{ ist ein Vielfaches von } 5 \\
 &\Rightarrow [2x + 3]_{\equiv_5} = [2y + 3]_{\equiv_5}
 \end{aligned}$$

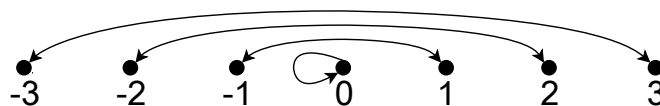
4.3 Ordnungsrelationen

Bemerkung 32. Eine binäre Relation R auf einer Menge M kann schematisch als gerichteter Graph dargestellt werden. Dazu werden diejenigen Punkte x, y aus M , für die xRy gilt, mit einem Pfeil verbunden.

Beispiel 46. Auf der Menge $\{-3, -2, -1, 0, 1, 2, 3\}$ sei die Relation R durch

$$xRy :\Leftrightarrow x + y = 0$$

gegeben. Der gerichtete Graph von R ist



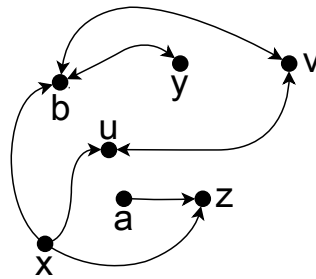
Definition 32. Es sei R eine binäre Relation auf der Menge M .

- Zwei Elemente $x, y \in M$ heißen *R-unvergleichbar*, falls weder xRy noch yRx gilt.
- Ein Element $x \in X$ einer Teilmenge $X \subset M$ von M heisst *R-minimal in X*, falls es kein anderes Element $y \in X$ mit yRx gibt.
- Ein Element $x \in X$ einer Teilmenge $X \subset M$ von M heisst *R-maximal in X*, falls es kein anderes Element $y \in X$ mit xRy gibt.

Wenn keine Missverständnisse zu befürchten sind, dann schreiben wir anstelle von *R-minimal*, *R-maximal* und *R-unvergleichbar* auch einfach *minimal*, *maximal* und *unvergleichbar*.

Bemerkung 33. Es sei X eine Teilmenge von M und R eine binäre Relation auf M . Die *R-minimalen* Elemente von X entsprechen den Punkten im gerichteten Graph, bei denen keine Pfeile enden, die ihren Ursprung in X haben. Die *maximalen* Elemente entsprechen den Punkten, von denen alle ausgehenden Pfeile aus der Menge X "hinauszeigen". Zwei Elemente $x, y \in M$ sind *R-unvergleichlich*, wenn es keinen Pfeil zwischen x und y gibt.

Übung 24. Die Relation R sei auf der Menge $M = \{a, b, u, v, x, y, z\}$ durch ihren gerichteten Graphen gegeben.



Geben Sie alle minimalen und maximalen Elemente von M an.

Lösung.

- Die minimalen Elemente von M sind a und x .
- Das einzige maximale Element von M ist z .

Definition 33. Es sei R eine binäre Relation auf der Menge M .

- R ist eine *Präordnung* auf M , wenn R reflexiv und transitiv ist.
- R ist eine *Halbordnung* auf M , wenn R reflexiv, antisymmetrisch und transitiv ist.
- R ist eine *totale Ordnung* auf M , wenn R eine Halbordnung ist und keine R -unvergleichbaren Elemente existieren.
- R ist eine *Wohlordnung* auf M , wenn R eine totale Ordnung auf M ist so, dass jede Teilmenge $X \neq \emptyset$ von M (mindestens) ein R -minimales Element enthält.

Beispiel 47.

- Die Relation \leq auf der Menge \mathbb{R} ist eine totale Ordnung, die aber keine Wohlordnung ist (die Menge $\{x \in \mathbb{R} \mid 0 < x < 1\}$ hat kein kleinstes Element). Auf der Menge \mathbb{N} ist \leq eine Wohlordnung³. Auf der Menge \mathbb{Z} ist die Relation \leq keine Wohlordnung. Wieso?
- Ist A eine Menge von Mengen, dann ist die Teilmengenrelation \subset eine Halbordnung.
- Die Teilerrelation T auf der Menge \mathbb{Z} ist eine Halbordnung aber keine totale Ordnung. Die Elemente 7 und 5 sind T -unvergleichlich.

³Ein Beweis dazu kommt im nächsten Kapitel.

Bemerkung 34. Sind zwei Mengen A und B sowie zwei Halbordnungen $<_A$ auf A und $<_B$ auf B gegeben, dann nennt man die Relation

$$(x, y) \prec (u, v) :\Leftrightarrow x <_A u \vee (x = u \wedge y <_B v)$$

die *lexikographische Ordnung* auf $A \times B$. Sind $<_A$ und $<_B$ totale Ordnungen, dann ist auch die lexikographische Ordnung \prec eine totale Ordnung auf $A \times B$.

Bemerkung 35. Wohlordnungen spielen eine wichtige Rolle im Zusammenhang mit rekursiven Strukturen. Die Tatsache, dass eine Wohlordnung keine unendlichen absteigenden Ketten zulässt, stellt sicher, dass Rekursionen entlang dieser Ordnung immer “terminieren”. Wir werden uns im nächsten Kapitel genauer mit dieser Beziehung auseinandersetzen. Der nächste Satz gibt aber einen ersten Hinweis auf diesen Zusammenhang.

Satz 13. *Ist \preceq eine Wohlordnung auf einer Menge M , dann gibt es keine unendlich absteigende Folge*

$$a_0 \succeq a_1 \succeq \cdots \succeq a_n \succeq a_{n+1} \succeq \cdots$$

von verschiedenen Elementen aus M .

Beweis. Gibt es eine absteigende Folge a_0, a_1, \dots wie in der Behauptung, dann ist die Menge

$$\{a_i \mid i \in \mathbb{N}\}$$

eine Teilmenge von M , die kein \preceq -minimales Element besitzt. Die Relation \preceq kann also in diesem Fall keine Wohlordnung sein. Die Behauptung folgt durch Kontraposition. \square

Beispiel 48. Die im Folgenden definierte Präordnung spielt eine wichtige Rolle in der sogenannten \mathcal{O} -Notation zur Beschreibung des Laufzeitverhaltens von Programmen. Die Relation \leq^* ist auf der Menge $\{f \mid f : \mathbb{N} \rightarrow \mathbb{N}\}$ wie folgt gegeben:

$$f \leq^* g :\Leftrightarrow K(g, f) \text{ ist endlich}$$

wobei

$$K(g, f) = \{x \in \mathbb{N} \mid g(x) < f(x)\}.$$

Die Relation $f \leq^* g$ besagt informell, dass die Funktion f nicht schneller als die Funktion g wächst. Die Relation \leq^* ist eine Präordnung aber keine Halbordnung und auch nicht total. Es gibt darüber hinaus unendlich absteigende Folgen von Funktionen bezüglich der Relation \leq^* .

Übung 25. Geben Sie zwei \leq^* unvergleichbare Funktionen f und g an.

Lösung. Zum Beispiel

$$f(n) = \begin{cases} 1 & \text{falls } n \text{ gerade} \\ 0 & \text{sonst} \end{cases}$$

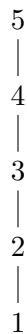
und

$$g(n) = \begin{cases} 0 & \text{falls } n \text{ ungerade} \\ 1 & \text{sonst} \end{cases}$$

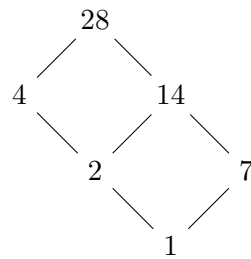
Definition 34. Es sei \preceq eine Halbordnung auf einer Menge M . Das *Hasse-Diagramm* von R erhalten wir wie folgt aus einem gerichteten Graphen von R .

- Die Richtung eines Pfeiles $a \rightarrow b$ für Elemente $a, b \in M$ wird dadurch zum Ausdruck gebracht, dass sich der Knoten b oberhalb von a befindet.
- Pfeile zwischen zwei Punkten a, b werden gelöscht, wenn es einen weiteren Punkt c mit $a \preceq c \preceq b$ gibt.
- Pfeile, die von einem Punkt auf denselben Punkt zeigen (Schleifen), werden weggelassen.

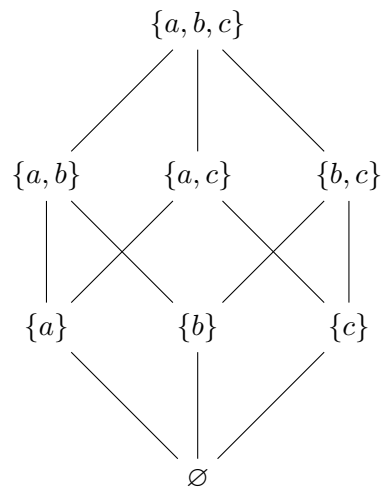
Beispiel 49. Eine Darstellung als Hasse-Diagramm von der Relation \leq auf der Menge $\{1, \dots, 5\}$.



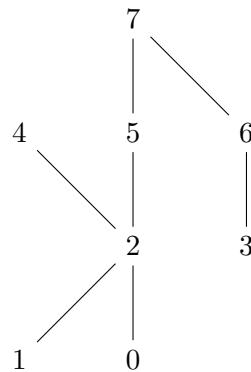
Beispiel 50. Eine Darstellung der Teilbarkeitsrelation auf der Menge Teilmengen von 28 ($\{1, 2, 4, 7, 14, 28\}$).



Beispiel 51. Die Teilmengenrelation \subset auf der Menge $\mathcal{P}(\{a, b, c\})$, als Hasse-Diagramm dargestellt.



Übung 26. Das Hasse-Diagramm einer Halbordnung auf der Menge $\{0, \dots, 7\}$ ist wie folgt gegeben.

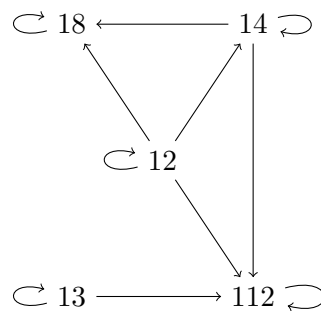


- Geben Sie alle maximalen und alle minimalen Elemente von der Menge $\{0, \dots, 7\}$ an.
- Geben Sie drei paarweise unvergleichbare Elemente an.

Lösung. - Minimale Elemente: 0, 1, 3

- Maximale Elemente: 4, 7
- Drei paarweise unvergleichbare Elemente: Z.B. 1, 0, 3 oder 4, 5, 6 usw.

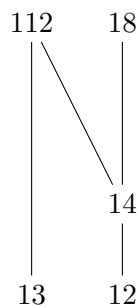
Übung 27. Der gerichtete Graph einer Halbordnung auf der Menge $\{12, 13, 14, 18, 112\}$ ist wie folgt gegeben.



- a) Zeichnen Sie ein Hasse-Diagramm für diese Halbordnung.
- b) Geben Sie die Relation als Menge an.

Lösung.

a)



- b) $\{(13, 13), (13, 112), (12, 12), (12, 112), (12, 14), (12, 18), (14, 14), (14, 112), (14, 18), (18, 18), (112, 112)\}$

5 Rekursive Strukturen und die natürlichen Zahlen

Relevanz für die Informatik

- Rekursion ist ein wichtiges Sprachelement von höheren Programmiersprachen (absolut zentral für funktionale Sprachen).
- Induktion kann verwendet werden um die Korrektheit von rekursiven Programmen zu beweisen.
- Rekursion und Induktion sind von fundamentaler Bedeutung für die theoretische Informatik (rekursive Funktionen, verallgemeinerter Rekursionsbegriff)
- Informatik ist voll von “induktiven Definitionen” (Syntax und Semantik von Programmiersprachen, primitiv rekursive Funktionen uvm.).

Lernziele

Sie kennen die

- Peano Axiome und verstehen deren Bedeutung.
- Die Begriffe von Induktion und Rekursion

Sie verstehen

- wie Induktion und Rekursion zusammenhängen.
- wie man rekursiv eine Funktion definieren kann und wie diese Definitionsweise zu rechtfertigen ist.
- wie sich die arithmetischen Operationen rekursiv aus der Nachfolgerabbildung definieren lassen.
- wie die üblichen Rechenregeln für natürliche Zahlen aus den Peano Axiomen folgen.

Sie sind in der Lage

- Induktionsbeweise zu führen.
- Algorithmen und Problemlösungsstrategien durch Rekursion zu beschreiben.
- Probleme zu erkennen, die sich effektiv durch Rekursion lösen lassen.

Literatur und Links

- Aufgaben mit Lösungen zu Induktion:
<http://www.emath.de/Referate/induktion-aufgaben-loesungen.pdf>
- Erklärungen zu Induktion:
http://de.wikibooks.org/wiki/Mathe_f%C3%BCr_Nicht-Freaks:_Vollst%C3%A4ndige_Induktion
- Wikipedia Einträge zu Induktion und Rekursion:
http://de.wikipedia.org/wiki/Vollst%C3%A4ndige_Induktion
<http://de.wikipedia.org/wiki/Rekursion>

5.1 Die grundlegende Struktur der natürlichen Zahlen

Wir haben die Menge \mathbb{N} bereits kennen und als Grundlage für viele Beispiele auch schätzen gelernt. In diesem Kapitel möchten wir diese Menge etwas genauer verstehen, wir wollen ihre innere Struktur (Ordnung und Operationen) untersuchen. Ausgangspunkt für unsere Betrachtungen ist die Anschauung der natürlichen Zahlen als eine auf dem “Zahlenstrahl” angeordnete, diskrete Menge:

$$0 \xrightarrow{+1} 1 \xrightarrow{+1} 2 \xrightarrow{+1} 3 \xrightarrow{+1} \dots$$

Von dieser Anschauung geleitet, listen wir nun einige Grundtatsachen über die Struktur \mathbb{N} auf. Diese Grundannahmen werden als *Peano Axiome* bezeichnet.

- Die Zahl 0 ist eine natürliche Zahl. Jede natürliche Zahl k hat genau einen Nachfolger $k + 1$. Der Nachfolger jeder natürlichen Zahl ist wiederum eine natürliche Zahl.
- Die Zahl 0 ist die einzige natürliche Zahl, die kein Nachfolger ist:

$$\forall n \in \mathbb{N} \underbrace{(\forall k \in \mathbb{N} (n \neq k + 1))}_{n \text{ ist kein Nachfolger}} \Leftrightarrow n = 0).$$

- Jede natürliche Zahl ist Nachfolger von höchstens einer natürlichen Zahl:

$$\forall n, m \in \mathbb{N} (n + 1 = m + 1 \Rightarrow n = m).$$

- *Das Prinzip der (vollständigen) Induktion:* Es sei $A(n)$ eine Eigenschaft (ein Prädikat) von natürlichen Zahlen. Aus den beiden Voraussetzungen

Induktionsverankerung (I.V.): $A(0)$

Induktionsschritt (I.S.): $\forall n \in \mathbb{N} (A(n) \Rightarrow A(n + 1))$,

folgt die Gültigkeit von $\forall n \in \mathbb{N} (A(n))$.

Bemerkung 36. Der Induktionsschritt ist stets von der Form

$$\forall n \in \mathbb{N} \left(\underbrace{A(n)}_{\text{Induktionsannahme}} \Rightarrow A(n+1) \right)$$

für ein Prädikat A . Der Teil $A(n)$ wird dabei *Induktionsannahme* genannt, weil er beim Nachweis von $A(n+1)$ als Annahme verwendet werden darf.

Bemerkung 37. Das Prinzip der vollständigen Induktion ist ein mächtiges Mittel um viele verschiedene Behauptungen über natürliche Zahlen beweisen zu können. Will man eine Aussage von der Form

$$\text{Jede natürliche Zahl } n \text{ erfüllt } E(n)$$

für ein Prädikat E beweisen, dann muss man, wenn man die Eigenschaft E nicht für alle natürlichen Zahlen *simultan* beweisen kann, im Prinzip unendlich viele Schritte bewältigen:

1. Schritt: Zeige $E(0)$.
2. Schritt: Zeige $E(1)$.
3. Schritt: Zeige $E(2)$.
- ⋮

Die Stärke des Induktionsargumentes liegt nun darin, all diese unendlich vielen Schritte auf zwei Schritte zu reduzieren:

1. Schritt (I.V.): Zeige $E(0)$.
2. Schritt (I.S.): Zeige, dass die Eigenschaft E unter Nachfolgern erhalten bleibt. Intuitiv könnte man sagen, dass die Eigenschaft E von jeder natürlichen Zahl auf die nächste “vererbt” wird.

Beispiel 52. Wir betrachten die Eigenschaft $A(n)$, die besagt, dass die Summe aller natürlichen Zahlen bis n halb so gross wie die Zahl $n(n+1)$ ist:

$$0 + 1 + \dots + n = \frac{n(n+1)}{2}.$$

Wir beweisen nun per Induktion nach n , dass die Eigenschaft $A(n)$ für jede natürliche Zahl n zutrifft.

Beweis. Wir zeigen zuerst die Induktionsverankerung:

- **Verankerung** ($n = 0$): $A(0)$ gilt, weil

$$0 = \frac{0 \cdot 1}{2}$$

offensichtlich korrekt ist.

- **Schritt** ($n \rightarrow n + 1$): Für den Induktionsschritt müssen wir zeigen, dass für jede natürliche Zahl n mit der Eigenschaft $A(n)$ auch $A(n + 1)$ gilt. Wir nehmen dazu an, dass n eine beliebige solche natürliche Zahl sei und betrachten

$$\begin{aligned} 0 + 1 + \cdots + n + (n + 1) &= (0 + 1 + \cdots + n) + (n + 1) \\ &\stackrel{A(n)}{=} \frac{n(n + 1)}{2} + (n + 1) \\ &= \frac{n(n + 1) + 2(n + 1)}{2} \\ &= \frac{(n + 1)(n + 2)}{2}. \end{aligned}$$

Daraus folgt der Induktionsschritt.

□

Beispiel 53. Wir benützen ein Induktionsargument um zu beweisen, dass alle natürlichen Zahlen $n > 1$ für beliebige reelle Zahlen $r > -1$ die folgende Eigenschaft haben:

$$(1 + r)^n > 1 + nr.$$

Beweis.

- **Verankerung** ($n = 2$): Die Verankerung gilt, wegen

$$(1 + r)^2 = 1 + 2r + r^2 > 1 + 2r.$$

- **Schritt** ($n \rightarrow n + 1$): Wir nehmen nun an, dass die Aussage für n gilt (I.A.) und zeigen sie für $n + 1$:

$$\begin{aligned} (1 + r)^{n+1} &= (1 + r)^n(1 + r) \\ &\stackrel{I.A.}{>} (1 + nr)(1 + r) \\ &= 1 + nr + r + \underbrace{nr^2}_{\text{positiv}} \\ &> 1 + (n + 1)r. \end{aligned}$$

□

Definition 35. Ist X eine endliche Menge, dann bezeichnen wir mit $|X|$ die Anzahl Elemente von X .

Beispiel 54. Für jede endliche Menge X gilt

$$|\mathcal{P}(X)| = 2^{|X|}.$$

Beweis. Wir führen den Beweis durch Induktion nach der Anzahl Elemente der Menge X .

- **Verankerung** ($|X| = 0$): Die einzige Menge mit 0 Elementen ist die leere Menge, es gilt also wie gewünscht

$$|\mathcal{P}(X)| = |\mathcal{P}(\emptyset)| = |\{\emptyset\}| = 1 = 2^0 = 2^{|X|}.$$

- **Schritt:** Es sei nun X eine $n + 1$ elementige Menge. Aufgrund der Induktionsannahme können wir davon ausgehen, dass für alle Mengen Y mit n Elementen die Gleichung

$$|\mathcal{P}(Y)| = 2^{|Y|}$$

erfüllt ist. Da $X \neq \emptyset$ gilt, können wir ein $x \in X$ auswählen. Wir unterteilen die Potenzmenge von X in zwei disjunkte, gleich grosse Teile A und B :

$$\begin{aligned} A &= \{Y \subset X \mid x \notin Y\} \\ B &= \{Y \subset X \mid x \in Y\}. \end{aligned}$$

Es gilt:

$$\begin{aligned} |\mathcal{P}(X)| &= |A \cup B| = |A| + |B| \\ &= |A| + |A| = 2|A| = 2|\mathcal{P}(X \setminus \{x\})| \\ &\stackrel{I.A.}{=} 2 \cdot 2^n = 2^{n+1}. \end{aligned} \quad \square$$

Satz 14 (Vollständige Induktion mit Mengen). *Für jede Menge X von natürlichen Zahlen gilt: Wenn X die Bedingungen*

- *Induktionsverankerung:* $0 \in X$
- *Induktionsschritt:* $\forall n (n \in X \Rightarrow n + 1 \in X)$

erfüllt, dann ist bereits $X = \mathbb{N}$.

Beweis. Ist $E(n)$ das Prädikat $n \in X$, dann folgt mit vollständiger Induktion sofort $\forall n (E(n))$ und somit $\mathbb{N} = X$. \square

Definition 36. Die Ordnung \leq auf den natürlichen Zahlen ist durch

$$x \leq y :\Leftrightarrow \exists k \in \mathbb{N} (x + k = y)$$

gegeben. Wir schreiben weiter

$$x < y :\Leftrightarrow x \leq y \wedge x \neq y.$$

Bemerkung 38. Wird die Zahlengerade der natürlichen Zahlen vertikal aufgezeichnet, dann ist sie ein Hasse-Diagramm für die Ordnung \leq auf \mathbb{N} .



Satz 15. Jede nichtleere Menge von natürlichen Zahlen hat ein minimales Element.

Beweis. Wir zeigen, dass jede Menge von natürlichen Zahlen, die kein minimales Element enthält, leer ist. Dazu wählen wir eine beliebige Menge $X \subset \mathbb{N}$ ohne minimales Element. Um zu zeigen, dass die Menge X leer ist, genügt es zu zeigen, dass die Menge

$$Y = \{n \in \mathbb{N} \mid \forall x \in X (n < x)\}$$

aller natürlichen Zahlen, die “unterhalb” von X liegen, bereits alle natürlichen Zahlen enthält. Wir zeigen $Y = \mathbb{N}$ mithilfe von Satz 14.

- **Verankerung:** Es gilt $0 \in Y$, weil sonst 0 das minimale Element von X wäre, was unserer Wahl von X widerspricht.
- **Induktionsschritt:** Ist $n \in Y$, dann gilt für alle Elemente x von X die Ungleichung $n < x$. Es gilt daher $n + 1 \leq x$ für alle Elemente x von X . Da $n + 1$ kein minimales Element von X sein kann, gilt daher $n + 1 \in Y$.

Aus Satz 14 folgt nun, dass $Y = \mathbb{N}$ und somit wie gewünscht $X = \emptyset$ ist. □

Satz 16. Es gibt keine unendlich absteigende Folge

$$a_0 > a_1 > \dots > a_n > a_{n+1} > \dots$$

von natürlichen Zahlen.

Beweis. Gäbe es eine absteigende Folge

$$a_0 > a_1 > \dots > a_n > a_{n+1} > \dots,$$

dann hätte die Menge

$$\{a_0, a_1, \dots, a_n, a_{n+1}, \dots\}$$

kein minimales Element. Dies widerspricht Satz 15. □

Aus den eben bewiesenen Sätzen können wir neue Beweismethoden herleiten:

Bemerkung 39 (Der kleinste Verbrecher). Die Beweismethode des “kleinsten Verbrechers” geht wie folgt: Will man zeigen, dass alle natürlichen Zahlen eine Eigenschaft E haben, dann geht man davon aus, dass wenn dies nicht der Fall wäre, es eine kleinste natürliche Zahl n_0 (der kleinste Verbrecher) gäbe, die *nicht* die Eigenschaft E hat. Führt man diese Annahme zu einem Widerspruch, so hat man die ursprüngliche Behauptung bewiesen. Obwohl die Methode des “kleinsten Verbrechers” also nichts anderes als die Kombination eines Widerspruchsargumentes mit Satz 15 ist, handelt es sich doch um eine sehr “anwenderfreundliche” und einprägsame Beschreibung dieser Argumentationsfolge.

Beispiel 55. Wir benützen die Methode des “kleinsten Verbrechers” um zu beweisen, dass jede natürliche Zahl, die mindestens zwei Teiler hat, mindestens einen Primfaktor besitzt (von einer Primzahl geteilt wird).

Beweis. Es sei n_0 die kleinste natürliche Zahl mit mindestens zwei Teilern, die keine Primfaktoren besitzt (der “kleinste Verbrecher”). Da n_0 keine Primfaktoren hat, ist n_0 selbst auch keine Primzahl und es gilt $n_0 \neq 0$. Es folgt somit, dass ein Teiler $1 < x < n_0$ von n_0 existieren muss. Da $1 < x$ gilt, hat x mindestens zwei Teiler (1 und x) und somit, wegen $x < n_0$, einen Primfaktor p . Da die Teilbarkeitsrelation transitiv ist, muss p aber auch ein Primfaktor von n_0 sein. Dies ist der gesuchte Widerspruch. \square

Übung 28. Beweisen Sie mit der Methode des “kleinsten Verbrechers”. Jede (natürliche) von der Form $(n^2 + n)$ ist gerade.

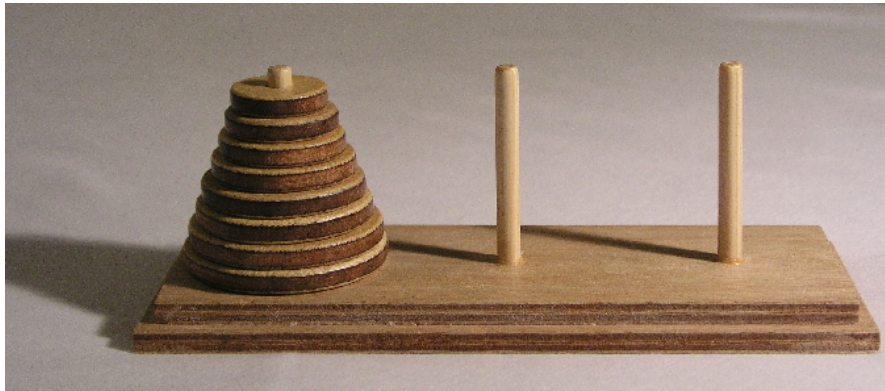
Lösung. Wir nehmen an, dass es ungerade natürliche Zahlen von der Form $n^2 + n$ gibt. Die Zahl $n^2 + n$ sei die kleinste solche Zahl (der kleinste Verbrecher). Weil n nicht Null sein kann (sonst wäre $n^2 + n$ gerade), muss es ein $k \in \mathbb{N}$ mit $n = k + 1$ geben. Weil $k < n$ gilt, muss $k^2 + k$ aber gerade sein. Daraus folgt

$$\begin{aligned} n^2 + n &= (k + 1)^2 + (k + 1) = k^2 + 2k + 1 + k + 1 \\ &= \underbrace{k^2 + k}_{\text{gerade}} + \underbrace{2k + 2}_{\text{gerade}} \end{aligned}$$

und somit, dass $n^2 + n$ gerade ist (im Widerspruch zur Annahme).

5.2 Vom Induktionsbeweis zum rekursiven Algorithmus

Beispiel 56 (Türme von Hanoi).



“Die Türme von Hanoi”¹ ist ein Geduldspiel. Das Spiel besteht aus drei gleich großen Stäben A, B und C, auf die mehrere gelochte Scheiben gelegt werden, alle verschieden groß. Zu Beginn liegen alle Scheiben auf Stab A, der Größe nach geordnet, mit der größten Scheibe unten und der kleinsten oben. Ziel des Spiels ist es, den kompletten Scheiben-Stapel von A nach C zu versetzen. Bei jedem Zug darf die oberste Scheibe eines beliebigen Stabes auf einen der beiden anderen Stäbe gelegt werden, vorausgesetzt, dort liegt nicht schon eine kleinere Scheibe. Folglich sind zu jedem Zeitpunkt des Spieles die Scheiben auf jedem Feld der Größe nach geordnet.

Wir wollen beweisen, dass “die Türme von Hanoi” mit beliebig vielen Scheiben erfolgreich gespielt werden können.

Beweis. Wir benutzen ein Induktionsargument (n sei die Anzahl Scheiben):

- **Verankerung** $n = 0$: Dieser Fall ist trivial, da es keine Scheiben zu bewegen gibt.
- **Induktionsschritt** $n \rightarrow n + 1$: Wir betrachten das Spiel mit $n + 1$ Scheiben. Nach Induktionsvoraussetzung gibt es eine Lösungsstrategie für das Spiel mit nur n Scheiben. Diese Strategie können wir offensichtlich dazu verwenden, um alle bis auf die grösste Scheibe auf den Stab B zu verschieben. Nun können wir die grösste Scheibe auf den Stab C verschieben um anschliessend nochmal die Strategie für das Spiel mit n Scheiben anzuwenden und alle kleineren Scheiben auf den Stab C zu bewegen. Das Spiel ist somit auch für $n + 1$ Scheiben lösbar. \square

Bemerkung 40. Der Beweis, dass die Türme von Hanoi für beliebige n gelöst werden können, ist mehr als nur eine Argumentationskette, die dazu geeignet ist jemanden davon zu überzeugen, dass es tatsächlich *irgendwie möglich sein muss* das Spiel zu gewinnen. Es steckt viel mehr in diesem Beweis; der Beweis gibt einen konkreten Algorithmus

¹Beschreibung und Bild von Wikipedia.

(rekursiv) vor, wie das Spiel erfolgreich gespielt werden kann. Wir betrachten eine Implementierung dieser Lösungsstrategie in der Sprache F#. Sie können das untenstehende Skript (und beliebige andere F# Skripte) unter <http://www.tryfsharp.org/> ausführen.

```
//x-viele Scheiben von A nach B verschieben:  
//Falls x=0, dann ist nichts zu tun.  
//Sonst, zuerst die oberen (x-1) Scheiben von A nach C  
//verschieben,  
//dann die grösste Scheibe von A nach B verschieben  
//und schliesslich alle anderen Scheiben von C nach B  
//verschieben  
  
let rec AB x =  
    if x=0 then " "  
    else (AC (x-1))+ "▯AB▯" +(CB (x-1))  
  
and AC x =  
    if x=0 then " "  
    else (AB (x-1))+ "▯AC▯" +(BC (x-1))  
  
and BC x =  
    if x=0 then " "  
    else (BA (x-1))+ "▯BC▯" +(AC (x-1))  
  
and BA x =  
    if x=0 then " "  
    else (BC (x-1))+ "▯BA▯" +(CA (x-1))  
  
and CB x =  
    if x=0 then " "  
    else (CA (x-1))+ "▯CB▯" +(AB (x-1))  
  
and CA x =  
    if x=0 then " "  
    else (CB (x-1))+ "▯CA▯" +(BA (x-1))  
  
let solve x = AC x
```

Die sechs Funktionen zu einer zusammengefasst:

```
//bewegen von n Scheiben von x nach y via Umweg z
let rec hanoi x y z n =
  if n=0 then ""
  else (hanoi x z y (n-1))+ "□"+x+y+(hanoi z y x (n-1))

let solve = hanoi "A" "C" "B"
```

Der selbe Algorithmus in Java:

```
public class HanoiSolver{

    public String solve(int size){
        return AC(size);
    }

    private String AB(int x){
        if (x==0) return "";
        return AC(x-1)+"□AB□"+CB(x-1);
    }

    private String AC(int x){
        if (x==0) return "";
        return AB(x-1)+"□AC□"+BC(x-1);
    }

    private String BC(int x){
        if (x==0) return "";
        return BA(x-1)+"□BC□"+AC(x-1);
    }

    private String BA(int x){
        if (x==0) return "";
        return BC(x-1)+"□BA□"+CA(x-1);
    }

    private String CB(int x){
        if (x==0) return "";
        return CA(x-1)+"□CB□"+AB(x-1);
    }
}
```

```
private String CA(int x){
    if (x==0) return "";
    return CB(x-1)+"␣CA␣"+BA(x-1);
}

}
```

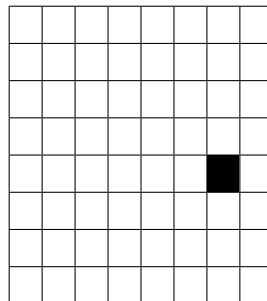
und die kurze Fassung:


```
public class HanoiSolverCompact{

    public String solve(int size){
        return hanoi("A","C","B",size);
    }

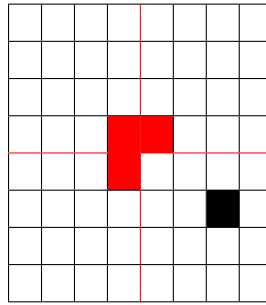
    private String hanoi(String x,String y,String z,int n){
        if(n==0) return "";
        return hanoi(x,z,y,n-1)+"␣"+x+y+hanoi(z,y,x,n-1);
    }
}
```

Beispiel 57. Ist es immer möglich ein “gelochtes $n \times n$ -Quadrat”



mit Flächen von der Form  “passgenau” zu überdecken? Ja, wenn n eine Zweierpotenz ist. Wir können diese Behauptung durch Induktion wie folgt beweisen: Wir nehmen an, dass das “gelochte Quadrat” eine Seitenlänge von 2^n hat.

- Verankerung ($n = 0$): Wenn $n = 0$, dann besteht das gelochte Quadrat nur aus einem Loch. Wir können das Quadrat (ohne etwas zu tun) überdecken.
- Hat das Quadrat die Seitenlänge 2^{n+1} , dann zerlegen wir es in vier gleich grosse Quadranten, die alle die Seitenlänge 2^n haben. Wir platzieren eine der Flächen wie unten angedeutet (rot).



Nun sind alle Quadranten ein “gelochtes Quadrat” der Seitenlänge 2^n . Wir können also nach Induktionsvoraussetzung alle Quadranten passgenau belegen.

Übung 29. Implementieren Sie (ausgehend vom Beispiel 57) in einer Programmiersprache Ihrer Wahl, einen Algorithmus zur Überdeckung von “gelochten Quadraten”, die eine Zweierpotenz als Seitenlänge haben.

5.3 Rekursive Definitionen

Rekursive Definitionen bezeichnen die mathematisch einwandfreie Art, ein Objekt durch Bezugnahme (Selbstreferenz) auf das zu definierende Objekt selbst zu definieren.

Beispiel 58. Ein Palindrom ist ein Wort, das rückwärts und vorwärts gelesen gleich lautet. Beispiele von Palindromen sind *xyx*, *acaca*, *arbbra*, *b*, *a*, \dots . Obwohl es uns anschaulich klar ist, welche Wörter Palindrome sind und welche nicht, ist unsere Beschreibung keine mathematisch präzise Definition. Dies wird insbesondere dann offensichtlich, wenn wir ein Programm schreiben müssen (ohne “String-umkehrende” Operatoren benützen zu dürfen), das von einem gegebenen Wort (String) entscheidet ob dieses ein Palindrom ist oder nicht. Wie können wir also Palindrome definieren (eindeutig beschreiben), ohne auf unsere Vorstellung von rückwärts und vorwärts lesen angewiesen zu sein? Durch Rekursion:

Ein Wort w ist ein Palindrom, wenn mindestens eine der beiden folgenden Bedingungen erfüllt ist:

- Das Wort w besteht aus einem oder gar keinem Buchstaben (Länge von $w < 2$).
- Es gibt einen Buchstaben (Zeichen, char) x und ein Palindrom u so, dass $w = xux$ gilt.

Selbstreferenz

Obwohl diese Definition, durch die in ihr vorhandenen Selbstreferenz, ein wenig “obskur” erscheinen mag, können wir sie direkt in ein Computerprogramm übersetzen.

In Java:

```
boolean palindrome(String w){
    if (w.length() < 2) return true;
    int last = w.length() - 1;
    char a = w.charAt(0);
    char b = w.charAt(last);
    if (a == b) return palindrome(w.substring(1, last - 1));
    return false;
}
```

In F#:

```
let rec pal s =
    let l = String.length s
    (l < 2) || (s.[0] = s.[l-1] && pal s.[1..(l-2)])
```

Theorem 3 (Rekursive Definitionen). *Ist M eine beliebige Menge und $G : M \times \mathbb{N} \rightarrow M$ sowie $c \in M$, dann gibt es eine eindeutig bestimmte Funktion $F : \mathbb{N} \rightarrow M$, welche die Gleichungen (Rekursionsgleichungen)*

$$\begin{aligned} F(0) &= c \\ F(k+1) &= G(\underbrace{F(k)}_{\text{Selbstbezug}}, k) \end{aligned}$$

erfüllt.

Beweisidee. Die Behauptung besteht aus einer Eindeutigkeitsaussage und einer Existenzaussage:

- Die Funktion $F : \mathbb{N} \rightarrow M$ ist durch die Rekursionsgleichungen eindeutig bestimmt. Das heisst, dass es keine andere Funktion gibt, die den Rekursionsgleichungen von F genügt.
- Es gibt überhaupt eine Funktion, die den Rekursionsgleichungen genügt.

Wir beweisen zuerst die Eindeutigkeitsbedingung. Wir nehmen an, dass F und H zwei Funktionen sind, die beide die oben genannten Rekursionsgleichungen erfüllen und zeigen, dass daraus $F = H$ folgt. Es genügt mit Induktion zu zeigen, dass für jede natürliche Zahl $n \in \mathbb{N}$ die Gleichung $F(n) = H(n)$ gilt (weil dann $H = F$ gilt).

- Verankerung ($n = 0$): Aufgrund von

$$F(0) = c = H(0)$$

ist die Induktionsverankerung erfüllt.

- Schritt $(n \rightarrow n+1)$: Wir nehmen an, dass $F(n) = H(n)$ gilt und müssen $F(n+1) = H(n+1)$ beweisen. Dies folgt sofort aus

$$F(n+1) = G(F(n), n) \stackrel{IA}{=} G(H(n), n) = H(n+1).$$

Nun kommen wir zur Existenzaussage. Anstelle eines formalen Beweises, wollen wir uns an dieser Stelle bloss anschaulich davon überzeugen, dass eine Funktion F immer existiert. Wir geben einen iterativen Algorithmus an, der die gesuchte Funktion realisiert.

```
input(n)
lst=[c] // Eine Liste mit einzigem Eintrag c
for i = 0..(n-1) do
    x = G(lst[i], i)
    lst.add(x) // Den aktuellen Funktionswert zur Liste
                // (aller Funktionswerte) hinzufuegen.
return lst[n]
```

□

Beispiel 59. Die üblichen arithmetischen Grundoperationen können alle relativ kompakt als rekursive Definitionen geschrieben werden:

- Die Addition von natürlichen Zahlen:

$$\begin{aligned}x + 0 &= x \\ x + (n+1) &= (x + n) + 1\end{aligned}$$

- Die Multiplikation von natürlichen Zahlen:

$$\begin{aligned}x \cdot 0 &= 0 \\ x \cdot (n+1) &= (x \cdot n) + x\end{aligned}$$

- Die Exponentiation von natürlichen Zahlen:

$$\begin{aligned}x^0 &= 1 \\ x^{n+1} &= x \cdot x^n\end{aligned}$$

- Die Fakultätsfunktion:

$$\begin{aligned}0! &= 1 \\ (n+1)! &= n! \cdot (n+1)\end{aligned}$$

- Endliche Summen:

$$\sum_{i=1}^0 a_i = 0$$
$$\sum_{i=1}^{n+1} a_i = \left(\sum_{i=0}^n a_i \right) + a_{n+1}$$

- Endliche Produkte:

$$\prod_{i=1}^0 a_i = 1$$
$$\prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^n a_i \right) \cdot a_{n+1}$$

Die üblichen Rechenregeln für natürliche Zahlen lassen sich aufgrund dieser rekursiven Definitionen mit Induktion (und genügend Geduld) beweisen. Wir beschränken uns beispielhaft auf den Beweis von Satz 19.

Übung 30. Implementieren Sie alle Funktionen von Beispiel 59 in der Programmiersprache Ihrer Wahl (natürlich ohne Verwendung der vorimplementierten Grundoperationen). Halten Sie sich so präzise wie möglich an die mathematische Definition.

Lösung. Vgl. OLAT “rekursive Operationen”

Satz 17. Für alle natürlichen Zahlen n, m, k gelten folgende Rechenregeln für deren Addition:

- a) *Neutrales Element:* $0 + n = n$
- b) *Kommutativität:* $n + m = m + n$
- c) *Assoziativität:* $(n + m) + k = n + (m + k)$
- d) *Kürzbarkeit:* $n + k = m + k \Rightarrow n = m$

Bemerkung 41. Wegen der Assoziativität der Addition, können wir Klammern in endlichen Summen von natürlichen Zahlen weglassen.

Satz 18 (Rechenregeln für die Multiplikation). Für alle $n, m, k \in \mathbb{N}$ gelten folgende Identitäten²:

²Wir vereinbaren hier, dass die Multiplikation “stärker bindet” als die Addition. Ein Ausdruck von der Form $nm + k$ wird also als $(nm) + k$ interpretiert.

- a) *Absorbtion*: $0 \cdot n = 0$
- b) *Neutrales Element*: $1 \cdot n = n$
- c) *Kommutativität*: $n \cdot m = m \cdot n$
- d) *Assoziativität*: $n \cdot (m \cdot k) = (n \cdot m) \cdot k$
- e) *Distributivität*: $n \cdot (m + k) = nm + nk$

Übung 31. Nachdem wir die Addition rekursiv definiert haben, lassen sich alle diese Tatsachen durch Induktion beweisen. Weil die einzelnen Beweise nicht sonderlich spannend sind werden sie der Leserschaft als Übung überlassen.

Satz 19 (Rechenregeln für Partialsummen). *Sind $(a_i)_{i \in \mathbb{N}}$ und $(b_i)_{i \in \mathbb{N}}$ beliebige Folgen und ist $c \in \mathbb{N}$, dann gilt für jedes $n \in \mathbb{N}$:*

$$\sum_{i=1}^n (ca_i + cb_i) = c \left(\sum_{i=1}^n a_i + \sum_{i=1}^n b_i \right)$$

Beweis. Induktion nach n .

- Verankerung ($n = 0$): Die Verankerung gilt aufgrund von

$$\sum_{i=1}^0 (ca_i + cb_i) = 0 = c(0 + 0) = c \left(\sum_{i=1}^0 a_i + \sum_{i=1}^0 b_i \right).$$

- Schritt ($n \rightarrow n + 1$):

$$\begin{aligned} \sum_{i=1}^{n+1} (ca_i + cb_i) &= \left(\sum_{i=1}^n (ca_i + cb_i) \right) + (ca_{n+1} + cb_{n+1}) \\ &= \left(\sum_{i=1}^n (ca_i + cb_i) \right) + c(a_{n+1} + b_{n+1}) \\ &\stackrel{IA}{=} c \left(\sum_{i=1}^n a_i + \sum_{i=1}^n b_i \right) + c(a_{n+1} + b_{n+1}) \\ &= c \left(\sum_{i=1}^n a_i + \sum_{i=1}^n b_i + a_{n+1} + b_{n+1} \right) \\ &= c \left(\sum_{i=1}^n a_i + a_{n+1} + \sum_{i=1}^n b_i + b_{n+1} \right) \\ &= c \left(\sum_{i=1}^{n+1} a_i + \sum_{i=1}^{n+1} b_i \right) \end{aligned}$$

□

6 Elementare Zahlentheorie

Lernziele

Sie kennen die

- Grundlagen der Teilbarkeitslehre.
- den Begriff der Primzahl.
- das kgV und den ggT und wie diese mithilfe des euklidischen Algorithmus berechnet werden.
- das Lemma von Bézout.
- den chinesischen Restsatz.
- den kleinen Fermatschen Satz.

Sie verstehen

- wieso und wie ganze Zahlen in ihre Primfaktoren zerlegt werden können.
- die modulare Arithmetik.
- den Zusammenhang vom chinesischen Restsatz und der Lösbarkeit von simultanen Kongruenzen.

Sie sind in der Lage

- die Stellenwertsysteme ineinander umzurechnen.
- Systeme simultaner Kongruenzen aufzulösen.

Literatur und Links

- Euklidischer Algorithmus:
http://de.wikipedia.org/wiki/Euklidischer_Algorithmus

Analog zu unserem Vorgehen mit den natürlichen Zahlen wollen wir auch die *ganzen Zahlen* informell einführen. Wir definieren

$$\mathbb{Z} := \{.., -2, -1, 0, 1, 2, \dots\}.$$

Die Motivation die Menge \mathbb{N} zur Menge \mathbb{Z} erweitern zu wollen fusst auf der Tatsache, dass für feste natürliche Zahlen k, k' im Allgemeinen die Gleichung

$$k + x = k'$$

keine Lösung in \mathbb{N} besitzt. Es ist in der Tat so, dass bei der Konstruktion von \mathbb{Z} aus \mathbb{N} (was wir nicht tun werden) die Menge \mathbb{Z} im Prinzip als die Menge aller Lösungen von solchen Gleichungen eingeführt wird.

Wir wollen es als gegeben erachten, dass die Multiplikation und die Addition derart von \mathbb{N} auf \mathbb{Z} fortgesetzt werden können, dass folgende Rechenregeln bestehen:

Bemerkung 42 (Rechenregeln auf \mathbb{Z}). Für alle $r, s, z \in \mathbb{Z}$ gelten folgende Gleichungen.

$-1 \cdot z = -z$	
$-(-z) = z$	
$-z + z = 0$	Inverse Elemente bezüglich +
$0 \cdot z = 0$	Absorbtion
$1 \cdot z = z$	Neutrales Element bezüglich \cdot
$0 + z = z$	Neutrales Element bezüglich +
$r(sz) = (rs)z$	Assoziativität von \cdot
$r + (s + z) = (r + s) + z$	Assoziativität von +
$rs = sr$	Kommutativität von \cdot
$r + s = s + r$	Kommutativität von +
$r(s + z) = rs + sz$	Distributivität
$rx = ry \Rightarrow x = y \vee r = 0$	Kürzbarkeit

Definition 37. Wir definieren die *Subtraktion*

$$- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

durch

$$x - y := x + (-y),$$

die *Betragsfunktion*

$$|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}$$

durch

$$|z| = \begin{cases} z & \text{falls } z \in \mathbb{N} \\ -1 \cdot z & \text{sonst} \end{cases}$$

und die Relation \leq durch

$$x \leq y :\Leftrightarrow \exists n \in \mathbb{N} (x + n = y).$$

6.1 Teilbarkeit und Euklidischer Algorithmus

Definition 38. Sind $x, y \in \mathbb{Z}$ ganze Zahlen, so sagen wir, dass x ein Teiler von y ist, falls es ein $k \in \mathbb{Z}$ gibt mit $xk = y$. Wir schreiben in diesem Fall $x|y$. Es gilt also

$$x|y :\Leftrightarrow \exists k \in \mathbb{Z} (y = xk).$$

Mit $T(y)$ bezeichnen wir die Menge aller natürlichen Zahlen, welche Teiler von y sind, also $T(y) = \{x \in \mathbb{N} \mid x|y\}$.

Beispiel 60.

- a) Die Zahl 1 ist ein Teiler jeder ganzen Zahl z , da $1 \cdot z = z$.
- b) $T(0) = \mathbb{N}$.

Bemerkung 43. Die Teilbarkeitsrelation ist reflexiv und transitiv auf der Menge \mathbb{Z} , auf der Menge \mathbb{N} ist die Teilbarkeitsrelation sogar eine Halbordnung (wieso nicht auf der Menge \mathbb{Z} ?).

Beweis. Wir zeigen, dass die Teilbarkeitsrelation reflexiv, transitiv und für natürliche Zahlen auch antisymmetrisch ist.

- Reflexivität: Dies gilt, da jede ganze Zahl sich selbst teilt.
- Transitivität: Seien x, y, z ganze Zahlen. Aus $x|y$ und $y|z$ folgt, dass es ganze Zahlen k_1, k_2 gibt mit $x \cdot k_1 = y$ und $y \cdot k_2 = z$. Es folgt

$$x \cdot (k_1 \cdot k_2) = (x \cdot k_1) \cdot k_2 = y \cdot k_2 = z.$$

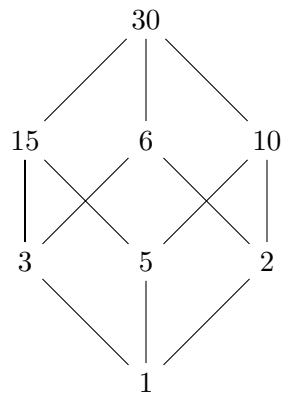
Somit gibt es also eine natürliche Zahl k (nämlich $k = k_1 \cdot k_2$) mit $k \cdot x = z$, also gilt $x|z$ wie gewünscht. \square

- Antisymmetrie auf \mathbb{N} : Wir müssen zeigen, dass für natürliche Zahlen x und y aus $x|y$ und $y|x$ folgt, dass $x = y$ gilt. Es gelte also $xk = y$ und $x = yr$ für ganze Zahlen k, r . Es folgt

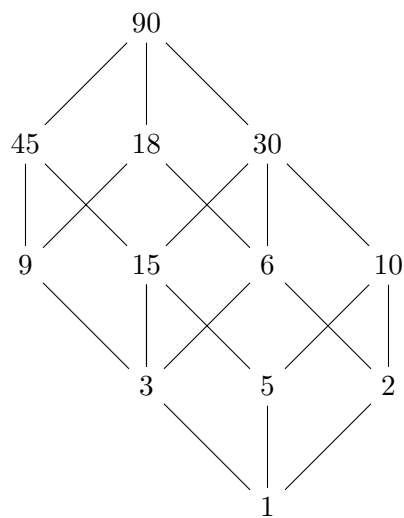
$$x = yr = (xk)r = x(kr)$$

und deswegen, dass $kr = 1$ und somit $k = r = 1$, was $x = y$ bedeutet.

Beispiel 61. Das Hasse-Diagramm der Teilbarkeitsrelation auf der Menge $T(30)$:



Das Hasse-Diagramm der Teilbarkeitsrelation auf der Menge $T(90)$:



Bemerkung 44. Sind $x, y \in \mathbb{Z}$ und gilt $x \cdot y = 1$ so gilt $|x| = |y| = 1$.

Satz 20 (Teilen mit Rest). *Sind $n, m \in \mathbb{N} \setminus \{0\}$, dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{N}$, so dass Folgendes gilt:*

- a) $m = kn + r$
- b) $r < n$

Wir sagen in diesem Zusammenhang, dass die Zahl r den Rest von der (ganzzahligen) Division von m durch n ist.

Beweis. Seien $n, m \in \mathbb{N} \setminus \{0\}$ beliebig. Die Menge

$$M := \{k \in \mathbb{N} \mid kn \leq m\}$$

ist endlich (da $n \geq 1$), somit gibt es ein maximales Element $k_0 \in M$. Wir definieren $r := m - k_0 n$. Da $k_0 \in M$ gilt, ist $r \in \mathbb{N}$. Es gilt

$$k_0 n + r = k_0 n + (m - k_0 n) = m.$$

Falls $r \geq n$ wäre, dann würde

$$m - (k_0 + 1)n = m - (k_0n + n) = r - n \geq 0$$

und somit $k_0 + 1 \in M$ gelten, was im Widerspruch zur Maximilität von k_0 in M steht. Wir müssen nun noch die Eindeutigkeit zeigen. Es genügt zu zeigen, dass für $r, r' < n$

$$(kn + r = k'n + r') \Rightarrow (k = k')$$

gilt. Wir machen einen Beweis durch Widerspruch und nehmen also $k \neq k'$ an. Aus Symmetriegründen können wir $k < k'$ und somit $k' = k + p$ mit $p > 0$ annehmen. Es gilt also

$$kn + r = k'n + r' = (k + p)n + r' = kn + pn + r'$$

und somit

$$r = pn + r' \geq n,$$

ein Widerspruch. □

Übung 32. Schreiben Sie in der Programmiersprache Ihrer Wahl eine Funktion, die zwei positive ganze Zahlen mit Rest teilt (natürlich ohne die Verwendung des Modulo Operators).

Lösung. z.B. in F#:

```
let div x y = printfn "%i : %i = %i Rest %i x y" (x/y) (x-(x/y)*y)
```

Definition 39. Seien $n, m \in \mathbb{Z}$. Wir definieren das *kleinste gemeinsame Vielfache* von n und m als

$$kgV(n, m) := \min\{k \in \mathbb{N} \mid n|k \wedge m|k\}.$$

Ist $n \neq 0$ oder $m \neq 0$, dann definieren wir den *grössten gemeinsamen Teiler* von n und m als

$$ggT(n, m) := \max\{k \in \mathbb{N} \mid k|n \wedge k|m\}.$$

Lemma 3. Sind $x, y, z \in \mathbb{Z}$, dann sind folgende Aussagen äquivalent:

1. $x|y \wedge x|z$
2. $x|y \wedge x|(y - z)$

Beweis. 1. \Rightarrow 2.: Wenn $x|y \wedge x|z$, dann gibt es ganze Zahlen $k, k' \in \mathbb{Z}$, so dass $y = kx$ und $z = k'x$. Es gilt also $y - z = kx - k'x = (k - k')x$.

2. \Rightarrow 1.: Es seien $k, k' \in \mathbb{Z}$, so dass $y = kx$ und $y - z = k'x$. Durch einsetzen erhält man $kx - z = k'x$ und somit $z = kx - k'x = x(k - k')$. \square

Satz 21 (Euklidischer Algorithmus). Für $n, m \in \mathbb{N}$ mit $0 < n < m$ gilt

$$\text{ggT}(n, m) = \text{ggT}(n, m - n) = \text{ggT}(m, m - n).$$

Beweis. Aus Lemma 3 folgt für $n, m \in \mathbb{N}$ mit $n < m$

$$\{k \in \mathbb{N} \mid k|n \wedge k|m\} = \{k \in \mathbb{N} \mid k|n \wedge k|(m - n)\}.$$

Daraus folgt weiter

$$\text{ggT}(n, m) = \max\{k \in \mathbb{N} \mid k|n \wedge k|m\} = \max\{k \in \mathbb{N} \mid k|n \wedge k|(m - n)\} = \text{ggT}(n, m - n).$$

Die Gleichung

$$\text{ggT}(n, m) = \text{ggT}(m, m - n)$$

folgt analog aus Lemma 3. \square

Bemerkung 45 (Euklidischer Algorithmus). Aus dem eben bewiesenen Satz 21 erhalten wir direkt einen rekursiven Algorithmus zur Berechnung des ggT . Beispielhaft geht man dabei wie folgt vor:

$$\begin{aligned} \text{ggT}(45, 25) &\stackrel{\text{Satz 21}}{=} \text{ggT}(25, 20) \\ &\stackrel{\text{Satz 21}}{=} \text{ggT}(20, 5) \\ &\stackrel{\text{Satz 21}}{=} \text{ggT}(5, 15) \\ &\stackrel{\text{Satz 21}}{=} \text{ggT}(5, 10) \\ &\stackrel{\text{Satz 21}}{=} \text{ggT}(5, 5) = 5. \end{aligned}$$

Dieses Vorgehen lässt sich direkt in Programme umsetzen.

In F#:

```
let rec ggT n m =  
    if n = m then n  
    elif n < m then ggT n (m - n)  
    else ggT m (n - m)
```

und als Java Methode:


```
int ggT(int n, int m){
    if (n == m) return n;
    if (n < m) return ggT(n, m - n);
    return ggT(m, n - m);
}
```

Betrachten wir nochmals den Satz 21, dann sehen wir, dass wir mehrere Schritte zu einem einzigen Schritt zusammenfassen können. Bei $x > y$ wird nämlich, zum berechnen von $ggT(y, x)$ sooft x von y subtrahiert, bis das Resultat kleiner oder gleich y ist. Man kann all diese Subtraktionen also durch eine einzige Division mit Rest ersetzen. Die beispielhafte Berechnung von $ggT(45, 25)$ können wir nun als 2 Divisionen mit Rest darstellen:

$$\begin{aligned} 45 &= 1 \cdot 25 + 20 \\ 25 &= 1 \cdot 20 + \underbrace{5}_{ggT(45, 25)} . \end{aligned}$$

Zusammenfassend stellen wir fest, dass

$$ggT(y, x) = ggT(y, R(x, y))$$

mit

$$R(x, y) = \text{der Rest der Division von } x \text{ durch } y$$

gilt. Die Funktion $R(x, y)$ steht in vielen Programmiersprachen als “modulo Funktion” zur Verfügung und wird im Quellcode oft durch das Prozentzeichen % aufgerufen. Dies eröffnet die Möglichkeit den euklidischen Algorithmus kompakter zu notieren:

In F#:

```
let rec ggT n m =
    if n = 0 then m
    elif n < m then ggT (m % n) n
    else ggT (n % m) m
```

In Java:

```
int ggT(int n, int m){
    if (n == 0) return m;
    if (n < m) return ggT(m % n, n);
    return ggT(n % m, m);
}
```

Übung 33. Benutzen Sie den euklidischen Algorithmus um $ggT(27, 96)$ auszurechnen (notieren Sie die Zwischenresultate).

Lösung.

$$\begin{aligned}
 ggT(27, 96) &= ggT(96 \% 27, 27) \\
 &= ggT(15, 27) = ggT(27 \% 15, 15) \\
 &= ggT(12, 15) = ggT(15 \% 12, 12) \\
 &= ggT(3, 12) = ggT(12 \% 3, 3) \\
 &= ggT(0, 3) = 3
 \end{aligned}$$

Definition 40. Zwei ganze Zahlen x, y heissen *teilerfremd*, wenn $ggT(x, y) = 1$ gilt.

Theorem 4 (Lemma von Bézout). Sind $x, y \in \mathbb{Z}$ mit $x, y \neq 0$, dann gibt es ganze Zahlen a, b so dass

$$ggT(x, y) = ax + by$$

gilt.

Beweis. Wir beweisen das Theorem exemplarisch für den Fall, dass $ggT(m, n) = 1$ gilt. Ohne Einschränkung sei $m > n$. Sind x, y beliebige ganze Zahlen, dann bezeichnen wir

$$R(x, y) := \begin{cases} \text{Der Rest von der ganzzahligen Division von } x \text{ durch } y & \text{falls } x, y > 0 \\ 0 & \text{sonst.} \end{cases}$$

Wir definieren rekursiv eine absteigende Folge $(r_i)_{i \in \mathbb{N}}$ von natürlichen Zahlen wie folgt:

$$r_i = \begin{cases} m & \text{falls } i = 0 \\ n & \text{falls } i = 1 \\ R(r_{i-2}, r_{i-1}) & \text{sonst.} \end{cases}$$

Da es keine echt absteigende Folge von natürlichen Zahlen gibt, muss die Folge der $(r_i)_{i \in \mathbb{N}}$ stationär werden. Es folgt also aus der Definition der Folge $(r_i)_{i \in \mathbb{N}}$, dass es ein $p \in \mathbb{N}$ gibt, so dass $r_p \neq 0$ und für alle $p' > p$ gilt $r_{p'} = 0$. Es sei $(\lambda_i)_{i \in \mathbb{N}}$ die durch $(r_i)_{i \in \mathbb{N}}$ eindeutig bestimmte Folge natürlicher Zahlen mit der Eigenschaft (*):

$$\begin{aligned}
 r_0 &= \lambda_0 \cdot r_1 + r_2 \\
 r_1 &= \lambda_1 \cdot r_2 + r_3 \\
 &\vdots \\
 r_{p-2} &= \lambda_{p-2} \cdot r_{p-1} + r_p
 \end{aligned}$$

Behauptung: $r_p = 1$

Beweis: Wir zeigen, dass r_p ein Teiler von allen r_i mit $i \leq p$ ist. Weil $r_0 = m, r_1 = n$ teilerfremd sind, gilt dann $r_p = 1$. Wir beweisen mit (der allgemeinen Version von) Induktion für alle $k \in \mathbb{N}$, dass entweder $r_p | r_{p-k}$ oder $k > p$ gilt. Falls $k > p$ ist, dann sind wir fertig. Wir können also ohne Einschränkung der Allgemeinheit annehmen, dass $k \leq p$ gilt. Nach Induktionsannahme ist nun r_p ein Teiler von $r_{p-(k-1)}$ und von $r_{p-(k-2)}$, es gibt also ganze Zahlen x, y mit $x \cdot r_p = r_{p-(k-1)}$ und $y \cdot r_p = r_{p-(k-2)}$. Insgesamt haben wir dann

$$r_{p-k} = \lambda_{p-k} \cdot r_{p-k+1} + r_{p-k+2} = \lambda x r_p + y r_p = r_p(\lambda x + y)$$

und somit wie gewünscht, dass r_p ein Teiler von r_{p-k} ist.

Wir können nun das Gleichungssystem (*) als

$$\begin{aligned} r_0 &= \lambda_0 \cdot r_1 + r_2 \\ r_1 &= \lambda_1 \cdot r_2 + r_3 \\ &\vdots \\ r_{p-2} &= \lambda_{p-2} \cdot r_{p-1} + 1 \end{aligned}$$

schreiben. Dies ist jedoch mit

$$\begin{aligned} 1 &= r_{p-2} - \lambda_{p-2} r_{p-1} \\ r_{p-1} &= r_{p-3} - \lambda_{p-3} r_{p-2} \\ &\vdots \\ r_{p-i} &= r_{p-i-2} - \lambda_{p-i-2} r_{p-i-1} \\ &\vdots \\ \underbrace{r_{p-p+2}}_{r_2} &= \underbrace{r_{p-p}}_m - \lambda_0 \underbrace{r_{p-p+1}}_n \end{aligned}$$

äquivalent. Indem wir nun sukzessiv (von unten beginnend) in jeder Zeile des Gleichungssystem die r_i 's auf der rechten Seite durch eine Summe von Vielfachen von n und m ersetzen, erhalten wir zuoberst im Gleichungssystem für geeignete s, δ_i, γ_i eine Gleichung von der gewünschten Gestalt

$$1 = \sum_{i=1}^s \delta_i n - \gamma_i m = \sum_{i=1}^s \delta_i n - \sum_{i=1}^s \gamma_i m = n \sum_{i=1}^s \delta_i - m \sum_{i=1}^s \gamma_i. \quad \square$$

Beispiel 62. Wir wollen ganze Zahlen a und b finden, die die Gleichung

$$a \cdot 504 + b \cdot 29 = \text{ggT}(504, 29) = 1$$

erfüllen.

- Schritt 1: Sukzessives Teilen mit Rest.

$$\begin{aligned}504 &= 17 \cdot 29 + 11 \\29 &= 2 \cdot 11 + 7 \\11 &= 1 \cdot 7 + 4 \\7 &= 1 \cdot 4 + 3 \\4 &= 1 \cdot 3 + \underbrace{1}_{\text{ggT}(504,29)}.\end{aligned}$$

- Schritt 2: "Rückwärts einsetzen".

$$\begin{aligned}1 &= 4 - 3 \\&= (11 - 7) - (7 - 4) \\&= ((504 - 17 \cdot 29) - (29 - 2 \cdot 11)) - ((29 - 2 \cdot 11) - (11 - 7)) \\&= ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29))) \\&\quad - ((29 - 2 \cdot (504 - 17 \cdot 29)) - ((504 - 17 \cdot 29) - (29 - 2 \cdot 11))) \\&= ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29))) - ((29 - 2 \cdot (504 - 17 \cdot 29)) \\&\quad - ((504 - 17 \cdot 29) - (29 - 2 \cdot (504 - 17 \cdot 29)))).\end{aligned}$$

- Schritt 3: Zusammenfassen (Zählen der Vorkommen von 504 und 29).

$$\begin{aligned}a &= 1 + 2 + 2 + 1 + 2 = 8 \\b &= -17 - 1 - (2 \cdot 17) - 1 - (2 \cdot 17) - 17 - 1 - (2 \cdot 17) = -139\end{aligned}$$

- Test:

$$8 \cdot 504 - 139 \cdot 29 = 1.$$

Übung 34. Finden Sie ganze Zahlen a und b , die folgende Gleichung erfüllen:

$$a \cdot 3215 + b \cdot 123 = 1.$$

Lösung. Sukzessives Teilen mit Rest ergibt:

$$\begin{aligned}3215 &= 26 \cdot 123 + 17 \\123 &= 7 \cdot 17 + 4 \\17 &= 4 \cdot 4 + 1.\end{aligned}$$

Wir erhalten somit:

$$\begin{aligned}1 &= 17 - 4 \cdot 4 \\&= (3215 - 26 \cdot 123) - 4 \cdot (123 - 7 \cdot 17) \\&= (3215 - 26 \cdot 123) - 4 \cdot (123 - 7 \cdot (3215 - 26 \cdot 123)) \\&= 29 \cdot 3215 - 758 \cdot 123.\end{aligned}$$

Also gilt $a = 29$ und $b = -758$.

6.2 Primzahlen

Primzahlen sind natürliche Zahlen, die genau zwei natürliche Zahlen als Teiler haben. Eine dazu äquivalente Formulierung ist, dass eine Primzahl also eine von 1 verschiedene natürliche Zahl ist, die (in \mathbb{N}) nur durch sich selbst und durch 1 teilbar ist. Die ersten 25 Primzahlen sind:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Definition 41. Eine natürliche Zahl $p \in \mathbb{N}$ ist eine *Primzahl*, wenn $|T(p)| = 2$ gilt. Die Menge aller Primzahlen bezeichnen wir mit \mathbb{P} .

Bemerkung 46. Ist p eine Primzahl, dann gilt $T(p) = \{1, p\}$.

Beweis. Für jede Zahl $n \in \mathbb{N}$ gilt offensichtlich $n \in T(n)$ und $1 \in T(n)$. Bei Primzahlen kommt dazu, dass (wegen $|T(n)| = 2$) keine weiteren Teiler existieren. \square

Bemerkung 47. Betrachtet man die Teilbarkeitsrelation auf der Menge $\mathbb{N} \setminus \{1\}$, dann sind die Primzahlen genau die minimalen Elemente dieser Halbordnung.

Primzahlen haben die Eigenschaft, dass sie mit jedem Produkt auch mindestens einen der Faktoren teilen. Umgekehrt ist auch jede von 1 verschiedene natürliche Zahl mit dieser Eigenschaft eine Primzahl. Diese Tatsache wird als Lemma von Euklid bezeichnet.

Satz 22 (Lemma von Euklid). *Folgende Aussagen sind für $p \in \mathbb{N}$ mit $p \neq 1$ äquivalent:*

1. $\forall n, m \in \mathbb{N} (p|nm \Rightarrow p|n \vee p|m)$
2. $p \in \mathbb{P}$

Beweis. $1 \Rightarrow 2$: Wir müssen zeigen, dass eine natürliche Zahl p mit der Eigenschaft wie in 1. bereits eine Primzahl ist. Wir nehmen an, dass p die in 1. postulierte Eigenschaft

besitzt und dass $x \in \mathbb{N}$ ein Teiler von p ist. Wir müssen zeigen, dass $x = 1$ oder $x = p$ gilt. Da x ein Teiler von p ist, gibt es eine natürliche Zahl y mit $xy = p$, insbesondere gilt also $p|xy$. Wegen 1. gilt also $p|x$ oder $p|y$, daraus folgt $p = x$ oder $p = y$ (Antisymmetrie der Teilbarkeit auf \mathbb{N}). Es folgt wie gewünscht, dass $x = 1$ oder $x = p$ gilt.

$2 \Rightarrow 1$: Wir nehmen an, dass p eine Primzahl sei und müssen für beliebige natürliche Zahlen n, m

$$p|(nm) \Rightarrow (p|n) \vee (p|m)$$

zeigen. Wir tun dies, indem wir aus $p|(nm)$ und $\neg(p|n)$ folgern, dass $p|m$ gelten muss. Weil $|T(p)| = 2$ gilt und da p kein Teiler von n ist, sind n und p teilerfremd. Nach Theorem 4 (Lemma von Bézout) gibt es also ganze Zahlen k, r mit

$$1 = pk + nr.$$

Andererseits folgt aus $p|nm$, dass es eine natürliche Zahl t mit

$$nm = pt$$

gibt. Insgesamt gilt also

$$\begin{aligned} m &= m \cdot 1 = m(pk + nr) \\ &= mpk + mnr \\ &= mpk + ptr \\ &= p(mk + tr). \end{aligned}$$

Somit ist also wie gewünscht, p ein Teiler von m . □

Satz 23. *Jede ganze Zahl z mit $z \notin \{-1, 1\}$ besitzt einen Primfaktor (einen Teiler, der eine Primzahl ist). Formal können wir dies als*

$$\forall z \in \mathbb{Z} (z \notin \{-1, 1\} \Rightarrow T(z) \cap \mathbb{P} \neq \emptyset).$$

ausdrücken.

Beweis. Sei $z \in \mathbb{Z}$ mit $z \notin \{-1, 1\}$. Die Menge $M := \{n \in \mathbb{N} \mid n > 1 \wedge n|z\}$ ist nicht leer, da sie mindestens $|z|$ als Element enthält. Nach dem Minimumsprinzip besitzt M also ein kleinstes Element $m = \min(M)$. Wir zeigen durch Widerspruch, dass m eine Primzahl ist. Wenn wir annehmen, dass m keine Primzahl ist, dann gibt es einen Teiler $t \in \mathbb{N}$ von m mit $1 < t < m$ (da $|T(m)| \geq 3$). Aus der Transitivität der Teilbarkeitsrelation folgt aus $t|m$ und $m|z$, dass $t|z$ gilt. Insgesamt ist also $t < m$ und $t \in M$, was im Widerspruch zur Minimalität von m in M steht. □

Theorem 5. *Es gibt unendlich viele Primzahlen.*

Beweis. Wir machen einen Widerspruchsbeweis. Wir nehmen an, dass es nur endlich viele Primzahlen $\mathbb{P} = \{p_1, \dots, p_n\}$ gibt. Nach Satz 23 gibt es eine Primzahl p_i so, dass

$$p_i \mid \left(\prod_{j=1}^n p_j \right) + 1.$$

Es gibt also eine natürliche Zahl k so, dass

$$p_i \cdot k = \left(\prod_{j=1}^n p_j \right) + 1$$

gilt. Daraus folgt

$$\begin{aligned} 1 &= p_i \cdot k - \left(\prod_{j=1}^n p_j \right) = p_i \cdot k - (p_1 \cdot \dots \cdot p_i \cdot \dots \cdot p_n) \\ &= p_i \cdot k - p_i \underbrace{(p_1 \cdot \dots \cdot p_{i-1} \cdot p_{i+1} \cdot \dots \cdot p_n)}_{:=p} \\ &= p_i(k - p). \end{aligned}$$

Es folgt also, dass p_i ein Teiler von 1 ist, das steht aber im Widerspruch zu $p_i \in \mathbb{P}$. \square

Theorem 6. *Jede natürliche Zahl grösser als 1 ist das Produkt von endlich vielen Primzahlen.*

Beweis. Wir machen einen Beweis durch Widerspruch. Angenommen es gibt natürliche Zahlen, die sich nicht als Produkt von Primzahlen schreiben lassen, dann ist die Menge

$$M := \{n \in \mathbb{N} \setminus \{0, 1\} \mid n \text{ ist nicht das Produkt von endlich vielen Primzahlen}\}$$

nicht leer. Nach dem Minimumsprinzip gibt es also ein kleinstes Element $m = \min(M)$. Nach Satz 23 gibt es eine Primzahl p mit $p|m$. Da m selbst keine Primzahl ist, gibt es also eine natürliche Zahl k mit $1 < k < m$ und $pk = m$. Da $k < m$ gilt, muss es, wegen der Minimalität von m in M , eine Darstellung von k als Produkt von Primzahlen geben. Es gibt also eine natürliche Zahl $n > 0$ und Primzahlen p_1, \dots, p_n so, dass

$$k = \prod_{i=1}^n p_i = p_1 \cdot p_2 \cdot \dots \cdot p_n.$$

Daraus folgt aber, dass

$$m = pk = p \cdot \prod_{i=1}^n p_i = p \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n$$

ebenfalls das Produkt von endlich vielen Primzahlen ist, ein Widerspruch zu $m \in M$. \square

Theorem 7 (Primfaktorzerlegung). *Es sei p_i jeweils die i -te Primzahl. Für jede natürliche Zahl $n > 1$ gibt es eine eindeutig bestimmte, endliche Folge a_1, \dots, a_k von natürlichen Zahlen mit $a_k \neq 0$, so dass*

$$n = \prod_{i=1}^k p_i^{a_i}$$

gilt.

Beweis. Die Existenzaussage folgt sofort aus Theorem 6. Die Eindeutigkeitsaussage folgt indessen aus Satz 22. \square

Übung 35. Implementieren Sie in der Programmiersprache Ihrer Wahl einen Algorithmus, der jede gegebene natürliche Zahl ($1 >$) in ihre Primfaktoren zerlegt.

Lösung. z.B. in F#:

```
let rec pf x = function
  | b when b>x -> []
  | b when x%b=0 -> b::(pf (x/b) b)
  | b -> pf x (b+1)
```

6.3 Modulare Arithmetik

In der modularen Arithmetik geht es darum mit Restklassen, annähernd so wie mit Zahlen, zu rechnen. Die Anwendungen der modularen Arithmetik durchdringen viele Teilgebiete der Informatik:

- Modulare Arithmetik wird oft verwendet um Prüfsummen nachzurechnen. Im Kontext von IBAN Nummern werden zum Beispiel Eingabefehler durch Summation modulo 97 erkannt.
- In der Kryptographie findet die modulare Arithmetik direkte Anwendung im *RSA*-Kryptosystem.
- In der Computeralgebra verwendet man modulare Arithmetik für effiziente Algorithmen. Zum Beispiel zur Faktorisierung von Polynomen.
- Modulare Arithmetik wird oft im Kontext von Operationen auf zyklischen Datenstrukturen verwendet (z.B. Bitweise Operationen). Die *XOR*-Operation kann man z.B. durch die Summe der Bits modulo 2 berechnen.

Die Grundlage der modularen Arithmetik ist die “kongruent modulo”-Relation.

Definition 42. Es sei $n \in \mathbb{N}$ beliebig. Wir definieren eine Relation \equiv_n auf \mathbb{Z} wie folgt:

$$r \equiv_n s :\Leftrightarrow n|(r - s).$$

Gilt für $r, s \in \mathbb{Z}$ die Relation $r \equiv_n s$, dann sagen wir, dass r gleich s modulo n ist und schreiben $r = s \pmod{n}$.

Bemerkung 48. Die Relation \equiv_n ist für jede natürliche Zahl n eine Äquivalenzrelation auf \mathbb{Z} .

Bemerkung 49. Es sei $n \in \mathbb{N}$ beliebig. Für je zwei ganze Zahlen x und y gilt $x \equiv_n y$ genau dann, wenn x und y den selben Rest bei Division durch n lassen.

Folgerung. Es sei $n \in \mathbb{N}$ beliebig. Jede ganze Zahl z steht mit genau einer natürlichen Zahl aus $\{0, \dots, n-1\}$ in der Relation \equiv_n .

Definition 43. Es sei $n \in \mathbb{N}$ beliebig. Für jede ganze Zahl z bezeichnen wir mit

$$[z]_n := \{x \in \mathbb{Z} \mid x \equiv_n z\}$$

die Äquivalenzklasse von z bezüglich der Relation \equiv_n und nennen diese auch die *Restklasse* von z . Abkürzend bezeichnen wir $[z]_n$ auch mit \bar{k} , wenn $k \in \{0, \dots, n-1\}$ und $z \equiv_n k$ gilt.

Folgerung. Es sei $n \in \mathbb{N}$ beliebig. Es gilt

$$[z]_n = \{z + yn \mid y \in \mathbb{Z}\} = \{\dots, z - 3n, z - 2n, z - n, z, z + n, z + 2n, z + 3n, \dots\}.$$

Damit wir mit Restklassen sinnvoll rechnen können, müssen wir uns davon überzeugen, dass die Rechenoperationen unabhängig von der Wahl von Repräsentanten sind.

Bemerkung 50. Es sei $n \in \mathbb{N}$ beliebig. Für ganze Zahlen x, x' und y, y' gelten¹:

$$\text{a) } [x] = [x'] \wedge [y] = [y'] \Rightarrow [x + y] = [x' + y']$$

$$\text{b) } [x] = [x'] \wedge [y] = [y'] \Rightarrow [xy] = [x'y']$$

Beweis. a) Aus $[x] = [x']$ und $[y] = [y']$ folgt, dass $x - x'$ und $y - y'$ Vielfache von n sind. Es folgt also, dass

$$(x + y) - (x' + y') = x - x' + (y - y')$$

auch ein Vielfaches von n ist und somit, dass $[x + y] = [x' + y']$ gilt.

b) Wir zeigen zuerst, dass unter der Voraussetzung $x \equiv_n x'$ für alle $z \in \mathbb{Z}$ die Gleichung

$$[xz + x] = [x'z + x']$$

gilt. Diese folgt aber aus

$$\begin{aligned} (xz + x) - (x'z + x') &= xz - x'z + x - x' = z(x - x') + (x - x') \\ &= (z + 1) \underbrace{(x - x')}_{\text{ist Vielfaches von } n}. \end{aligned}$$

¹Wenn die natürliche Zahl n aus dem Kontext klar ersichtlich ist, so lassen wir diese in der Notation $[x]_n$ auch manchmal weg.

Daraus folgt für $[x] = [x']$ und $[y] = [y']$:

$$\begin{aligned}
 [xy] &= [x(y-1) + x] \\
 &= [x'(y-1) + x'] \\
 &= [x'y] = [yx'] \\
 &= [y(x'-1) + y] \\
 &= [y'(x'-1) + y'] \\
 &= [x'y'].
 \end{aligned}$$

□

Definition 44. Es sei $n \in \mathbb{N}$ beliebig. Die Menge aller Restklassen von \mathbb{Z} modulo n bezeichnen wir mit

$$\mathbb{Z}/n = \{[z]_n \mid z \in \mathbb{Z}\} = \{\bar{k} \mid 0 \leq k < n-1 \wedge z \equiv_n k\} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

Wir definieren zwei Verknüpfungen $\cdot : (\mathbb{Z}/n)^2 \rightarrow \mathbb{Z}/n$ und $+: (\mathbb{Z}/n)^2 \rightarrow \mathbb{Z}/n$ durch die Zuordnungen

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

und

$$[x]_n \cdot [y]_n := [xy]_n.$$

Beispiel 63. Die Verknüpfungstabelle der Addition in $\mathbb{Z}/6$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Die Verknüpfungstabelle der Multiplikation in $\mathbb{Z}/6$:

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Bemerkung 51. Wir betrachten die Gleichung

$$\bar{3} + x = \bar{2}$$

in $\mathbb{Z}/5$. Setzen wir

$$x = \bar{2} - \bar{3} = \overline{2-3} = \overline{-1} = \bar{4},$$

dann haben wir eine Lösung für die obige Gleichung:

$$\bar{3} + x = \bar{3} + \bar{4} = \overline{3+4} = \bar{7} = \bar{2}.$$

Dass dieses Vorgehen für jeden Modulo und jede Gleichung zielführend ist, folgt sofort aus

$$\overline{a + (b - a)} = \bar{b}.$$

Beispiel 64 (Rechnen mit Uhrzeiten). Rechnen mit Uhrzeiten (volle Stunden einer Analoguhr) entspricht mit Restklassen Modulo 12 zu rechnen.

- Es ist 9 Uhr. Wie lange dauert es, bis es das nächste mal 2 Uhr ist? Wir müssen die Gleichung

$$\bar{9} + x = \bar{2}$$

lösen. Wie vorher gesehen, erhalten wir die Lösung durch

$$x = \bar{2} + \overline{-9} = \overline{2-9} = \overline{-7} = \bar{5}.$$

Es geht also noch 5 Stunden bis 2 Uhr.

Beispiel 65 (Rechnen mit Wochentagen).

- Es ist Montag. Welcher Wochentag ist in 2454 Tagen? Wir bezeichnen die Wochentage mit Elementen von $\mathbb{Z}/7$: Mo.= $\bar{0}$, Di.= $\bar{1}$, ... Der Wochentag in 2454 Tagen ist also

$$\bar{0} + \overline{2454} = \overline{2454} = \bar{4}$$

ein Freitag.

Bemerkung 52. Wir betrachten die Gleichung

$$\bar{2} \cdot x = \bar{3}$$

in $\mathbb{Z}/5$. Diese Gleichung besitzt als Lösung $x = \bar{4}$, weil

$$\bar{2} \cdot \bar{4} = \overline{2 \cdot 4} = \bar{8} = \bar{3}$$

gilt. Betrachten wir die selbe Gleichung aber über $\mathbb{Z}/4$, dann sehen wir, dass diese Gleichung keine Lösung hat, weil:

$$\bar{2} \cdot \bar{0} = \bar{0} \neq \bar{3}$$

$$\bar{2} \cdot \bar{1} = \bar{2} \neq \bar{3}$$

$$\bar{2} \cdot \bar{2} = \bar{0} \neq \bar{3}$$

$$\bar{2} \cdot \bar{3} = \bar{2} \neq \bar{3}.$$

Woran liegt dies? Das Problem ist, dass $\bar{2}$ in $\mathbb{Z}/2$ nicht “invertierbar” ist, “ $\frac{1}{2}$ ” existiert in $\mathbb{Z}/4$ nicht. In $\mathbb{Z}/5$ hingegen ist $\bar{2}$ sehr wohl invertierbar, weil $\bar{2} \cdot \bar{3} = \bar{1}$ gilt (“ $\frac{1}{2}$ ” ist $\bar{3}$ in $\mathbb{Z}/5$).

Im nächsten Satz sehen wir, dass in \mathbb{Z}/n genau dann alle Gleichungen von der Form

$$ax = b$$

(für beliebige aber feste $a, b \in \mathbb{Z}/n$ mit $a \neq 0$) eine Lösung besitzen, wenn n eine Primzahl ist.

Theorem 8. *Es sei $n \in \mathbb{N} \setminus \{1\}$ beliebig. Folgende Aussagen sind äquivalent:*

1. *n ist eine Primzahl.*
2. *Für jedes $\bar{k} \in \mathbb{Z}/n$ mit $\bar{k} \neq \bar{0}$ gibt es genau ein $r \in \{0, \dots, n-1\}$ mit $\bar{k} \cdot \bar{r} = \bar{1}$.*

Die zweite Aussage besagt, dass man in \mathbb{Z}/n Gleichungen von der Form $ax = b$ stets nach x auflösen kann. Sind $\bar{k}, \bar{r} \in \mathbb{Z}/n$ mit $\bar{k} \cdot \bar{r} = \bar{1}$, so sagen wir \bar{r} sei invers (bezüglich der Multiplikation) zu \bar{k} und schreiben auch $(\bar{k})^{-1}$ für \bar{r} .

Beweis. Wir beweisen zuerst $1. \Rightarrow 2.$ und dann $2. \Rightarrow 1.$

$1. \Rightarrow 2.$: Es sei n eine Primzahl und $\bar{k} \neq \bar{0}$. Ohne Einschränkung sei $0 < k < n$. Weil n eine Primzahl ist, sind n und k teilerfremd. Daraus folgt, dass es ganze Zahlen a und b gibt mit

$$ak + bn = 1.$$

Es gilt also

$$\bar{1} = \overline{ak + bn} = \overline{ak} + \underbrace{\overline{bn}}_{=\bar{0}} = \overline{ak} = \bar{a} \cdot \bar{k}.$$

Die gesuchte Zahl r erhalten wir somit durch den Rest der Division von a durch n ($r = a \% n$).

$2. \Rightarrow 1.$: Es sei $n \in \mathbb{N} \setminus \mathbb{P}$. Da wir ohne Einschränkung $n \notin \{0, 1\}$ annehmen können², gibt es natürliche Zahlen $1 < r, s < n$ mit $n \mid rs$. Wenn nun die Aussage 2. für n gelten würde, dann hätten wir

$$\bar{1} = \bar{r}(\bar{r})^{-1}\bar{s}(\bar{s})^{-1} = \underbrace{(\bar{r} \cdot \bar{s})}_{=\bar{0}}(\bar{r})^{-1}(\bar{s})^{-1} = \bar{0},$$

ein Widerspruch. □

Übung 36. Es sei $n \in \mathbb{N}$ beliebig, dann heisst $\bar{k} \in \mathbb{Z}/n$ invertierbar falls es zu \bar{k} inverse Elemente in \mathbb{Z}/n gibt.

- a) Geben Sie alle invertierbaren Elemente von \mathbb{Z}/n für $n = 1, 3, 4, 5$ an.
- b) Lösen Sie $\bar{3}x = \bar{4}$ in $\mathbb{Z}/7$.
- c) Geben Sie das bezüglich \cdot zu 3 inverse Element in $\mathbb{Z}/11$ an.

²Für $n = 0$ entspricht $(\mathbb{Z}/n, \cdot)$ der Struktur (\mathbb{Z}, \cdot) , für $n = 1$ der Struktur $(\{\bar{0}\}, \cdot)$

6.3.1 Chinesischer Restsatz

Der Chinesische Restsatz besagt, dass bei paarweise teilerfremden Zahlen $n_1, \dots, n_k \in \mathbb{N}_{>1}$ und beliebigen ganzen Zahlen y_1, \dots, y_k , Gleichungssysteme von der Form³

$$\begin{aligned}x &\equiv_{n_1} y_1 \\x &\equiv_{n_2} y_2 \\&\vdots \\x &\equiv_{n_k} y_k\end{aligned}$$

eindeutig in $\mathbb{Z}/(n_1, \dots, n_k)$ lösbar⁴ sind.

Satz 24 (Chinesischer Restsatz). *Es seien $n_1, \dots, n_k \in \mathbb{N}_{>1}$ paarweise teilerfremd und weiter $y_1, \dots, y_k \in \mathbb{Z}$ beliebig. Es gibt genau eine natürliche Zahl $x < \prod_{i=1}^k n_i$ so, dass die Lösungsmenge des Systems*

$$\begin{aligned}x &\equiv_{n_1} y_1 \\x &\equiv_{n_2} y_2 \\&\vdots \\x &\equiv_{n_k} y_k\end{aligned}$$

der Menge $[x]_{\prod_{i=1}^k n_i}$ entspricht.

Beweis. Vgl. Algorithmus. □

Beispiel 66. Wir betrachten folgendes System simultaner Kongruenzen:

$$\begin{aligned}x &\equiv_2 0 \\x &\equiv_3 2 \\x &\equiv_5 3\end{aligned}$$

Wir sehen, dass 8 das System löst und wissen daher, wegen dem chinesischen Restsatz, dass die Lösungsmenge gerade

$$[8]_{30} = \{8 + 30z \mid z \in \mathbb{Z}\} = \{\dots, -22, 8, 38, \dots\}$$

entspricht.

³Solche Gleichungssysteme heißen simultane Kongruenzen.

⁴Damit meinen wir, dass die Lösungsmenge des Gleichungssystems genau ein Element (Äquivalenzklasse) von $\mathbb{Z}/(n_1, \dots, n_k)$ ist.

Übung 37. Lösen Sie das System

$$x \equiv_4 3$$

$$x \equiv_5 2$$

$$x \equiv_9 1$$

Bemerkung 53. Aus dem chinesischen Restsatz folgt, dass wir, um ein System simultaner Kongruenzen zu lösen, bloss eine Lösung davon kennen müssen. Durch sukzessive Substitution genügt es also jeweils eine Lösung von einem System mit zwei Gleichungen zu finden um beliebige Systeme lösen zu können. Wie Sie in der letzten Aufgabe eventuell geahnt haben, kann dies aber immer noch ziemlich mühsam sein, daher wollen wir dieses Teilproblem algorithmisch lösen.

Algorithmus (Lösen simultaner Kongruenzen). Wir wollen ein System simultaner Kongruenzen mit zwei Gleichungen lösen, etwa

$$x \equiv_{n_1} y_1$$

$$x \equiv_{n_2} y_2$$

mit n_1 und n_2 teilerfremd. Wir gehen schrittweise wie folgt vor:

- a) Durch sukzessives Teilen mit Rest (wie im Beweis von Satz 4) erhalten wir ganze Zahlen a, b mit $an_1 + bn_2 = 1$.
- b) Wir setzen $x := y_1bn_2 + y_2an_1$.

Korrektheit des Algorithmus: Wir müssen lediglich überprüfen, dass $x := y_1bn_2 + y_2an_1$ das System löst, wenn $an_1 + bn_2 = 1$ ist. Es gilt

$$[1]_{n_1} = [an_1 + bn_2]_{n_1} = [bn_2]_{n_1}$$

und damit

$$[y_1]_{n_1} = [y_1]_{n_1} \cdot [bn_2]_{n_1} = [y_1bn_2]_{n_1} = [y_1bn_2]_{n_1} = [y_1bn_2]_{n_1} + \underbrace{[y_2an_1]_{n_1}}_{=[0]} = [y_1bn_2 + y_2an_1]_{n_1}$$

Also gilt $x = y_1 \bmod n_1$. Andererseits gilt auch

$$[1]_{n_2} = [an_1 + bn_2]_{n_2} = [an_1]_{n_2}$$

und deshalb

$$[y_2]_{n_2} = [y_2an_1]_{n_2} = [y_1bn_2]_{n_2} + [y_2an_1]_{n_2} = [y_1bn_2 + y_2an_1]_{n_2}.$$

□

Beispiel 67. Wir lösen das System

$$x \equiv_7 3$$

$$x \equiv_5 2$$

$$x \equiv_9 6$$

Wir lösen zuerst das Teilsystem

$$x \equiv_7 3$$

$$x \equiv_5 2$$

Wir teilen sukzessive mit Rest und erhalten

$$7 = 1 \cdot 5 + 2 \tag{6.1}$$

$$5 = 2 \cdot 2 + 1 \tag{6.2}$$

und somit

$$\begin{aligned} 1 &\stackrel{(4.2)}{=} 5 - 2 \cdot 2 \\ &\stackrel{(4.1)}{=} 5 - 2(7 - 5) \\ &= 5 - 2 \cdot 7 + 2 \cdot 5 \\ &= \mathbf{3} \cdot 5 + \mathbf{(-2)} \cdot 7 \end{aligned}$$

Wir haben also als Lösung

$$x = 3 \cdot 3 \cdot 5 + 2 \cdot (-2) \cdot 7 = 17$$

und als Lösungsmenge $[17]_{35}$. Wir müssen nun noch das System

$$x \equiv_{35} 17$$

$$x \equiv_9 6$$

lösen. Wir teilen sukzessive mit Rest:

$$35 = 3 \cdot 9 + 8$$

$$9 = 1 \cdot 8 + 1.$$

Wir erhalten damit:

$$\begin{aligned} 1 &= 9 - 8 \\ &= 9 - (35 - 3 \cdot 9) \\ &= \mathbf{4} \cdot 9 + \mathbf{(-1)} \cdot 35. \end{aligned}$$

Eine Lösung ergibt sich erneut durch

$$x := 17 \cdot 4 \cdot 9 + 6 \cdot (-1) \cdot 35 = 402.$$

Die Lösungsmenge des ganzen Systems ist also $[402]_{35 \cdot 9} = [87]_{315}$.

Der nächste Satz ist der sogenannte “kleine (Satz von) Fermat”. Er findet Verwendung bei (probabilistischen) Primzahltests und bildet die Grundlage des “Shor-Algorithmus”, einem quanten-Algorithmus zur Faktorisierung von ganzen Zahlen.

Zuerst ein Lemma.

Lemma 4. *Ist $a \in \mathbb{Z}/n$ mit $n > 0$ invertierbar, dann ist die Funktion*

$$\begin{aligned} f : \mathbb{Z}/p &\rightarrow \mathbb{Z}/p \\ f(x) &= \bar{a} \cdot x \end{aligned}$$

surjektiv.

Beweis. Da die Menge \mathbb{Z}/n endlich ist, genügt es zu zeigen, dass für alle x und y die Implikation

$$f(x) = f(y) \Rightarrow x = y$$

gilt. Sei b das Inverse von a (es gilt also $ab = ba = \bar{1}$). Es gilt nun wie gewünscht:

$$\begin{aligned} f(x) &= f(y) \\ \Rightarrow ax &= ay \\ \Rightarrow bax &= bay \\ \Rightarrow x &= y. \end{aligned}$$

□

Satz 25 (Kleiner Fermat). *Ist $p \in \mathbb{P}$ und a kein Vielfaches von p , dann gilt*

$$a^{p-1} \equiv_p 1.$$

Beweis. Da $a \in \mathbb{Z}$ kein Vielfaches von p ist, sind a und p teilerfremd, a ist somit invertierbar in \mathbb{Z}/p (wir dürfen in \mathbb{Z}/p somit “durch a teilen”). Wir betrachten die Funktion

$$\begin{aligned} f : \mathbb{Z}/p &\rightarrow \mathbb{Z}/p \\ f(x) &= \bar{a} \cdot x \end{aligned}$$

Weil a eine Einheit ist, wissen wir aus Lemma 4, dass die Funktion f surjektiv ist. Es gilt also

$$f(\bar{1}) \cdot \dots \cdot f(\overline{p-1}) = \bar{1} \cdot \dots \cdot \overline{p-1}.$$

und somit

$$\bar{a}\bar{1} \cdot \dots \cdot \overline{ap-1} = \bar{1} \cdot \dots \cdot \overline{p-1}$$

also

$$\bar{a}^{p-1}\bar{1} \cdot \dots \cdot \overline{p-1} = \bar{1} \cdot \dots \cdot \overline{p-1}.$$

Da alle Zahlen $2, \dots, p-1$ zu p teilerfremd sind, erhalten wir daraus

$$\bar{a}^{p-1} = \bar{1}.$$

□

Literaturverzeichnis

- [1] Rod Haggarty. *Diskrete Mathematik für Informatiker*. Pearson Studium, 2007.
- [2] Peter Hartmann. *Mathematik für Informatiker – ein praxisbezogenes Lehrbuch*. Mathematik/Informatik. Vieweg, 3 edition, 2004.
- [3] Ulrich Knauer. *Diskrete Strukturen – kurz gefasst*. Spektrum–Hochschultaschenbuch. Spektrum Akademischer Verlag, 2011.
- [4] Bodo Pareigis. *Lineare Algebra für Informatiker*. Springer, 2000.
- [5] H. D. Ebbinghaus / J. Flum / W. Thomas. *Einführung in die mathematische Logik*. Hochschultaschenbuch. Spektrum Akademischer Verlag, 5 edition, 2007.