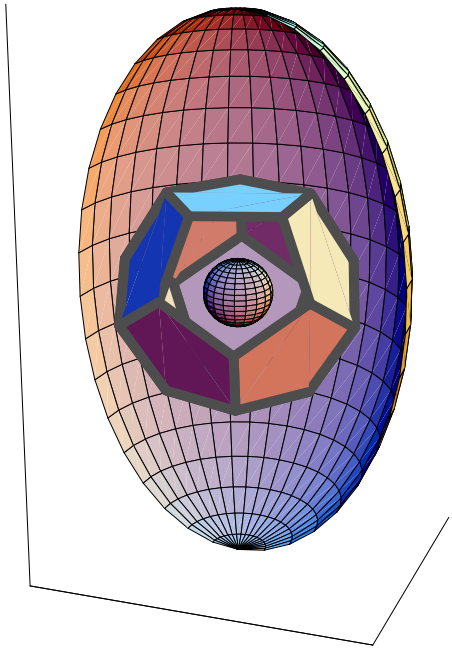
Script ◇ Math ◇ Ing
◇ Diskrete und angewandte Mathematik ◇
◇ Mathématiques discrètes et appliquées ◇
◇ kurz & bündig ◇ concis



von

Rolf Wirz

Ingenieurschule Biel // Neu: Berner FH, HTA-Biel // BFH, HTI–HSB

Scripta bilingua

Mit nach den NeXT–Crash von 1999 restaurierten Teilen, Ausgabe vom 18. September 2007, N.V. 1.7 / d (f)

WIR/NeXT/1993/1996/1999/2005/2006/2007/LaTex/KursDiskr.tex

Ehemals Teil 2, 3, 4 und 6 des Repetitoriums und Textbuchs zur Begleitung und Ergänzung des Unterrichts.
Geplante Anzahl Teile, Reihenfolge, Gliederung: Im Jahre 1993 noch offen. (Wurde laufend ergänzt und neu gegliedert.)
Produziert mit LaTeX auf NeXT-Computer, restauriert mit PCTeX unter Win98/XP.
Einige Graphiken sind auch mit *Mathematica* entstanden.

1999 hat der Autor einen Computer–Crash erlebt. Infolge des dadurch provozierten Systemwechsels haben einige Graphiken gelitten. Sie werden neu erstellt, sobald die Zeit dafür vorhanden ist.

Lasst niemanden meine Werke Lesen, der nicht Mathematiker ist...

Leonardo da Vinci

Können wir uns dem Göttlichen auf keinem anderen Wege als durch Symbole nähern, so werden wir uns am passendsten der mathematischen Symbole bedienen, denn diese besitzen unzerstörbare Gewissheit. Das Wissen vom Göttlichen ist für einen mathematisch ganz Ungebildeten unerreichbar.

Nikolaus von Cues alias Cusanus (1401 – 1464)

Aktuelle Adresse des Autors (2007):

Rolf W. Wirz-Depierre
Prof. für Math.
Berner Fachhochschule (BFH), Dep. AHB und TI
Pestalozzistrasse 20
Büro B112 CH–3400 Burgdorf/BE
Tel. ++41 (0)34 426 42 30 / intern 230
Mail: Siehe http://rowicus.ch/Wir/indexTotalF.html unter „Koordinaten von R.W.“
(Alt: Ingenieurschule Biel (HTL), Ing'schule des Kt. Bern, Fachhochschule ab 1997) // BFH HTA Biel // BFH HT/

Inhaltsverzeichnis • Table des matières

Kapitel • Chapitre 1

Vorwort zum Teil Aussagenlogik oder Junktorenlogik

Liebe Leserin, lieber Leser,

Wir haben uns vorgenommen, die streng aufgebaute Mathematik so zu studieren, dass wir sie zusammenhängend verstehen und somit auch als Werkzeug fachmännisch verwenden können. Dem reifen Studenten ist sicher im bisherigen Leben längst klar geworden, dass auf keinem Arbeitsgebiet etwas erreicht werden kann ohne gute Kenntnisse und Fertigkeiten in der Anwendung von Werkzeugen. Das ist hier nicht anders. Das wichtigste Werkzeug der Mathematik ist nun die *Logik*. Ohne Logik bleibt da ein Verständnis schwierig. Denn Mathematik gilt ja weithin auch als die Wissenschaft vom Beweisen, als Gebiet der sicheren, der bewiesenen Resultate und der exakten Formulierungen, die keine Missverständnisse mehr zulassen sollten. Und die Werkzeuge für das Beweisen oder das exakte Formulieren, das Definieren, für das Herleiten, ist die Logik. Vor allem eben die aus mathematischer Sicht noch sehr einfache 2–wertige Aussagenlogik. Mit dieser beginnen wir und schaffen uns so eine feste Grundlage für eine niveaugerechte Einarbeitung in weitere Gebiete: Erst in Mengenlehre, dann darauf aufbauend in das Gebiet der Relationen. Hier lässt sich dann befriedigend der sehr zentrale Begriff der mathematischen Abbildung und der mathematischen Funktion abstützen, auf den man dann weite Teile der nachfolgenden Mathematik aufbauen kann. Z.B. später in der Differential– und Integralrechnung macht man ja eigentlich nichts anderes, als Funktionen untersuchen. Mit Hilfe von Funktionen lassen sich in der Praxis viele Probleme elegant lösen. Auch andere Gebiete wie z.B. die Boolsche Algebra — oder dann speziell die Schaltalgebra — stützen sich direkt auf die Logik. Das Fundament „Logik“ muss stark sein, damit das darauf gebaute Gebäude hält. Versuchen wir also, die nötige Seriosität in die Sache zu legen. Und vergessen wir dabei nie den Ratschlag: „Nach einem Hammerschlag sitzt ein Nagel selten. Lass Dich nicht entmutigen; arbeite mit Beharrlichkeit und dem Gedanken, dass Deine Fähigkeiten sich mehr und mehr entwickeln.“ Doch vergessen wir dabei ob diesem strengen Stoff auch das Lachen nicht. Es bringt dem heiss gewordenen, vielleicht „dampfenden“, müden Kopf frische Energie und Kühle.

Im Herbst 1994/99 Der Autor

Der Geist, der Schärfe, aber nicht Weite hat, bleibt an jedem Punkt stecken und kommt nicht von der Stelle . . . Ein Geist, der nur Logik ist, gleicht einem Messer, das nichts ist als Klinge. Die Hand wird blutig beim Gebrauch. . . .

Tagore

Kapitel • Chapitre 2

Vorkenntnisse: Aufgabe, Herkunft der 2–wertigen Aussagenlogik

2.1 Wozu bei uns Logik in der Mathematik?

In den unteren Schulen hauptsächlich technischer Richtung hört man heute öfters das Wort „Logik“, vielleicht im Zusammenhang mit elektrischen Schaltungen. Das ist jedoch eine sehr spezielle Sicht, die den Umfang des hier Angesprochenen kaum erahnen lässt. Was versteht man dann sonst unter „Logik“ in den exakten Wissenschaften, in der Mathematik?
Unter *Logik* fasst man heute einen Wissenschaftszweig zusammen, den viele Wissenschaften als Teil für sich reklamieren: So etwa Philosophie, Theologie, Sprachwissenschaften, Jurisprudenz, Mathematik. Es gibt somit nicht nur eine einzige Logik. Juristische Logik hat vielleicht nicht viel zu tun mit Kants „transzendentaler Logik“ , die in die Philosophie gehört. Und dies wiederum ist nicht zu verwechseln mit der mathematischen Logik, von der dieser Teil handeln soll.
Mathematische Logik ist *formale Logik*. Das bedeutet, dass das hauptsächliche Interesse nicht der Botschaft, nicht dem Inhalt, nicht dem intentionalen Inhalt einer sprachlichen Konstruktion gilt, sondern der Form. Vereinfacht gesagt: Das Interesse gilt mehr der grammatikalischen Konstruktionsart. Zudem können wir hier nur auf einen *sehr winzigen Teil* der mathematischen Logik eingehen: Auf 2–wertige Aussagenlogik, mit einem kleinen Ausblick auf das an Umfang unvergleichlich grössere Gebiet der mathematischen Prädikatenlogik. Alles andere muss ungesagt bleiben.
Man mag sich jetzt fragen, welche Aufgaben der formalen Logik der Mathematik dann zukommen. Drei Aufgabenkreise lassen sich sofort unterscheiden: Erstens ist Logik ein eigenständiges Gebiet mit ureigenen Fragestellungen, die ins Gebiet der Erkenntnistheorie gehören. Zweitens ist Logik aber auch sehr verwandt mit anderen mathematischen Gebieten, etwa der Verbandstheorie, somit der Boolschen Algebra — und darauf aufbauend der Schaltalgebra oder auch der Mengenlehre. Logik ist hier das Fundament. Drittens aber hat jede Wissenschaft ihre Sprache, so auch die Mathematik. Mathematik bedient sich zur Formulierung ihrer Sachverhalte und zum Aufbau ihrer Regeln der Sprache der Logik. Logik wird also hier als Sprache benützt.
Merken wir uns also:

Die Sprache der Mathematik ist die formale Logik.

2.2 Wie und wann hat sich die Logik entwickelt? – Wie alt ist sie?

Der Titel zeigt Fragen nach der Geschichte. Blättern wir in dieser kurz zurück. Erste Ansätze der später von Kant[1] so bezeichneten „formalen Logik“ finden sich bei Aristoteles[2]. Inspiriert durch Platon[3] hat sich dieser daran gemacht, über Wahrsein und Falschsein von Aussagen nachzudenken. Er hat erkannt, dass man unter Benutzung gewisser Operationsregeln aus als wahr betrachteten Axiomen neue Aussagen abgeleitet werden kann, die man wegen den Regeln wieder als wahr betrachten muss. Die hier auftauchenden einfachen Schlussregeln nennt man *Syllogismen*. Abgesehen von Ansätzen etwa bei Leibnitz[4], der vielleicht als erster eine künstliche Sprache zu benutzen versuchte, oder bei Lambert[5] schlief die formale mathematische Logik mehr oder weniger einen Dornröschenschlaf bis ins 19. Jahrhundert. Mit den Arbeiten von De Morgan[6] und Boole[7] begann dann die formale Logik aufzublühen. Und um die Wende zum 20. Jahrhundert stellen wir plötzlich eine eigentliche, fast explosionsartig ansteigende Forschungstätigkeit und Wissensvermehrung fest, vor allem verknüpft mit den Namen Schröder[8], Peano[9], Peirce[10], Frege[11], Whitehead[12], Russel[13], Hilbert[14] und später Ramsey[15], Turing[16], Gödel[17], Skolem[18], Tarski[19] und andere. Vor allem durch die von Gödel ab 1931 puplizierten Vollständigkeits– resp. Unvollständigkeitssätze erfolgte ein Durchbruch zu einer ganz anderen Weltanschauung. Analog zur Endlichkeit der materiellen Welt hat man auch Grenzen der Welt des exakten Denkens gefunden und weiss nun auch hier, wohin man nie gelangen kann.
Bei all dem vielen jetzt Gesagten ist wichtig mitzunehmen, dass die nun folgende formale Logik nicht eine uralte Sache ist, sondern eher ein Kind der neueren Zeit.

2.3 Zum Gegenstand

2.3.1 Was ist Logik?

In der philosophischen Logik befasste man sich früher mit den „Naturgesetzen“ der Vernunft, mit der Kunst des Denkens resp. des richtigen Denkens. In dieser Logik werden die Fragen behandelt, was denn die zwingend erscheinenden Regeln des vernünftigen Schliessens überhaupt sind, wieso diese Regeln so sind, was die Zusammenhänge zwischen Ursache und Wirkung sind. Die heutige philosophische Logik befasst sich eher mit denjenigen Schlüssen, die alleine aufgrund der (sprachlichen) Form zu wahren Aussagen führen, also mit symbolischer oder formaler Logik. Auch die mathematische Logik ist formale Logik. Sie handelt von Aussagen in einer „exakt“ gefassten Sprache *(Aussagenlogik)*, oder auch, etwas unscharf gesprochen, von unterteilbaren Aussagen *(Prädikatenlogik)*. Dabei interessieren hauptsächlich Fragen wie:

[1] Kant: Deutscher Philosoph, 1724 – 1804
[2] Aristoteles: Schüler Platons, 384 – 322 v. Chr.
[3] Platon: griech. Philosoph 427 – 347 v. Chr.
[4] Leibnitz: Deutscher Mathematiker und Philosoph 1646 – 1716
[5] Lambert: Deutscher Mathematiker 1728 – 1777
[6] De Morgan: Englischer Mathematiker 1808 – 1871
[7] Boole: Englischer Mathematiker 1815 – 1864
[8] Schröder: Deutscher Mathematiker 1841 – 1902
[9] Peano: Italienischer Mathematiker 1858 – 1932
[10] Peirce: Amerikanischer Mathematiker 1839 – 1941
[11] Frege: Deutscher Mathematiker 1848 – 1925
[12] Whitehead: Englischer Mathematiker 1861 – 1947
[13] Russel: Englischer Mathematiker 1847 – 1970
[14] Hilbert: Deutscher Mathematiker 1862 – 1943
[15] Ramsey: Englischer Mathematiker 1904 – 1930
[16] Turing: Englischer Mathematiker 1912 – 1954
[17] Gödel: Österreichischer Mathematiker geb. 1906
[18] Skolem: Norwegischer Mathematiker 1887 – 1963
[19] Tarski: Polnischer Mathematiker, 20. Jhdt.

- ⊘ Vollständigkeit einer formal gefassten Sprache, Beweisbarkeit: Sind alle wahren Aussagen auch in der Sprache herleitbar?
- ⊘ Entscheidbarkeit eines Problems: Existiert ein Entscheidungsweg? Was für sprachliche Konstruktionen sind herleitbar?
- ⊘ Definierbarkeit: Ist die Sprache genügend umfangreich oder lässt sich etwas, über das man „reden möchte“ vielleicht gar nicht definieren?
- ⊘ Sicherheit: Ist eine Menge von Regeln (ein Axiomensystem) — und daher die darauf aufgebaute Theorie — auch widerspruchsfrei?
- ⊘ Machbarkeit: Wie ist die Theorie nun aufzubauen?
- ⊘ Darstellbarkeitsproblem: Wie wenig braucht man an sprachlichen Werkzeugen, um etwas damit wiedergeben zu können?
- ⊘ Sprachnievau: Wie kompliziert muss eine Sprache sein, um etwas Gewolltes ausdrücken zu können?
- ⊘ Form: Wann hängt der Wahrheitsgehalt einer Aussage alleine von der Form ab und nicht vom Inhalt?
- ⊘ Inhalt: Wie hängen Inhalt und Form zusammen?
- ⊘ U.s.w.

2.3.2 Wie weit wir gehen

Und das alles muss man dann können? — Oh nein, das eben nicht. Wir werden hier die Sprache der Logik nur soweit entwickeln, als es für das Folgende und für die Allgemeinbildung von relevantem Wert ist. Das bedeutet, dass wir schwierigkeitsmässig das alte „Aristotelische Niveau“ kaum verlassen werden. Wir werden nicht in die moderne mathematische Logik, in die sogenannte *Methodologie der exakten Wissenschaften* resp. in die *höheren Prädikatenlogiken* (oder *Stufenlogik*) vordringen. Da fehlen Zeit, Vorbildung und Notwendigkeit. Wir werden hier den Weg einer *nicht-strengen*, einer sogenannt *„naiven“ Behandlung* verfolgen. Das wird genügen.

2.4 Welche Literatur ist empfehlenswert?

Die Literatur über formale Logik ist äusserst umfangreich. Doch die meisten Bücher sind nicht für Ingenieurstudenten geschrieben. Solche Bücher erscheinen dann vom Sprachniveau her dem Laien als unleserlich, unverständlich, unbrauchbar. In englischer und deutscher Sprache existiert eine ausgedehnte Literatur. Als niveaugerecht können folgende Werke gelten: Mendelson, SCHAUM (Bibl.: mendelson), Lipschutz, SCHAUM, Bibl.: lipschutz). Oder auch spezielle Bücher für obere Mittelschulen, herausgegeben von Schulbuchverlagen (Bibl.: jehle, deller). Leider ist es so, dass das Kapitel „Logik“ in mathematischen Fachbüchern für Ingenieure meistens fehlt.
Hinweise für Fortgeschrittene: Weiterführende Literatur findet sich u.a. in Bibl.: asser, church, hermes, hilbert, shoen, tarski, vandalen.
Was die französischsprachige Literatur betrifft, sind die Studenten gebeten, beim Autor mündlich zu fragen.

2.5 Übungen

Übungen zum Teil 2 finden sich auch in den Übungsblättern, z.B. *DIYMU*. (Vgl. Bibl.: wirz [20]

[20] Übungsbuch *DIYMU*: „An Stelle einer Einleitung“, Bibl.: wirz.

Kapitel • Chapitre 3

Junktorenlogik oder Aussagenlogik

3.1 Aussagen, Aussagenvariablen und Belegungen

3.1.1 Aussagen

Wir wollen uns fragen, was wir unter dem Begriff *Aussage* verstehen sollen. Damit wir über *Aussagen* reden können, müssen wir davon zuerst eine Vorstellung entwickeln. Da wir bis anhin noch keine einfachen Begriffe definiert haben, auf denen wir aufbauen könnten, lassen wir uns von folgender Idee leiten („Begriffserklärung“ Pseudodefinition, noch nicht streng):

Begriffserklärung 1 (Aussage) *: Eine* **Aussage** *ist ein sprachliches Grundgebilde, das eine „Wahrheit“ oder „Unwahrheit“ mitteilt.*

Dabei haben wir vorher nicht definiert, was *„wahr“* oder „nicht wahr“ (resp. *„falsch“*) bedeuten soll. Wir nehmen an, dass jeder selbst so vernünftig ist, dass er beurteilen kann, wann etwas Einsichtiges wahr ist oder nicht[1]. Was „vernünftig“ ist, soll unter für vernünftig gehaltenen Menschen einfach durch ausdiskutieren demokratisch entschieden werden. Eine andere Möglichkeit, durch Vernunft zur „Wahrheit“ zu gelangen, bleibt dem Menschen nicht. Weiter nehmen wir auch an, dass wir genügend wissen, was ein „sprachliches Gebilde“ ist. Aussagen sind also hier *Grundgebilde* — ähnlich dem Punkt in der Geometrie, der ja auch nicht näher definiert werden kann. Das stört heute niemanden mehr ernsthaft.

Spezielle, von ihrer Natur her klare Aussagen finden wir in den *mathematischen Aussagen* oder (falls wichtig) *mathematischen Sätzen*, die man als wahr erachtet, sofern man die Voraussetzungen dazu akzeptiert. Einfache mathematische Aussagen sind z.B. in Gleichungen oder Ungleichungen mit Zahlen. *Aus diesem Grunde werden wir in den folgenden Beispielen hauptsächlich mathematische Aussagen verwenden.*

Beispiele:

$a :\equiv$ “$2+2=4$”	(wahre mathematische Aussage[1])
$b :\equiv$ “$2+2=5$”	(falsche mathematische Aussage)
$c :\equiv$ “$2+2+5$”	(keine Aussage)
$d :\equiv$ “Wohin gehst Du?”	(keine Aussage)
$e :\equiv$ “Komm bitte mit!”	(keine Aussage)
$f :\equiv$ “Die Birke ist ein Baum!”	(wahre Aussage)
$g :\equiv$ “1.1111 ist keine Zahl”	(falsche mathematische Aussage)

[1] Das Problem der Natur der Wahrheit als „Problem der Erkenntnis“ gilt als ein Grundproblem der Philosophie überhaupt. Die Philosophie kennt im wesentlichen drei Grundprobleme: Das Problem des *Sein*, das Problem der *Erkenntnis* und das *Moralproblem*.

$h :\equiv$ "Bei geöffnetem Schalter fliesst Strom." (falsche Aussage)

Bemerkung 1 (zu den verwendeten Symbolen): Hier sind a, b, c, d und e Namen für die Aussagen. Das Zeichen „$:\equiv$“ bedeutet „definiert als äquivalent“. „$\equiv$“ alleine meint äquivalent, dies um Verwechslungen mit dem Gleichheitszeichen in mathematischen Aussagen (z.B. in $2 + 2 = 4$) zu vermeiden.

Bemerkung 2 (zur zweiwertigen Logik):
In der *zweiwertigen Logik* betrachtet man nur Aussagen, die entweder *wahr* oder *falsch* sind und *keine meitere Möglichkeit* für den Wahrheitsgehalt offen lassen. In der Sprache des täglichen Lebens stellt diese Situation aber eher eine Ausnahme dar, die man gerne in die Mathematik abschiebt. Z.B. ein Gegenstand ist nicht etwa „hell“ oder „nicht hell“ (womit man dann gelegentlich „dunkel“ meint). Sondern er hat eine gewisse Helligkeit. Ebenso mit schwarz und weiss. Dazwischen liegen viele, viele Graustufen. Oder denken wir an das „liebe“ Haustier Katze, die ab und zu sehr böse sein kann, wenn sie einen kratzt —. Auch der gute Haushund, der keineswegs Begeisterung erweckt, wenn er dann eben doch zubeisst... Das Gegenteil der Aussage „Der Hund ist *gut*“ ist dann nicht etwa die Aussage „Der Hund ist *schlecht*“. Ebenso auch nicht die Aussage „Der Hund ist *nicht gut*“ (absolut gesehen). Eher trifft als Gegenteil die Aussage zu: „Der Hund ist *manchmal nicht gut*“. Denn der Hund zeigt sich uns einmal als gut, ein andermal erfahren wir ihn als bösen Hund, ein weiteres Mal als gut und schlecht zugleich, und ein viertes Mal als weder gut noch schlecht noch sonst etwas, denn er ist seit Tagen nicht mehr nach Hause gekommen, ist einfach nicht da, nicht erfahrbar.
Die Begriffe „wahr“ und „falsch“ reichen hier nicht mehr aus. Es braucht differenzierte Zwischenstufen, die sich ähnlich den Farben nicht in eine eindimensionale Skala einordnen lassen müssen. So kommen wir zu einer *mehrwertigen Logik*. Nimmt man noch den Wahrheitswert *unbestimmt* dazu, so kommt man zur *dreiwertigen Logik*[2]. Der Satz „In zweihundert Jahren ist die Schweiz ein Königreich!“ ist wohl nicht heute schon entscheidbar, bleibt also vorerst für uns absolut unbestimmt, da wir es noch nicht wissen. „Variabel“ ist die Aussage aber nicht, denn wir können an der Realität er Zukunft nichts ändern oder ersetzen. Was wir ändern können ist nur unsere Vorstellung von der Zukunft. Auch wenn wir jetzt ein Orakel befragen: Was wirklich eintritt, wird erst eine spätere Generation mit absoluter Bestimmtheit wissen. Heute bleibt uns der Wahrheitswert unzugänglich — und wir können ihn vielleicht noch durch unser Handeln beeinflussen, doch nur in die später einmal feststehende Richtung. Denn es gibt nur eine Vergangenheit und auch nur eine Zukunft.
Ein anderes, vielleicht eindrücklicheres Beispiel: Auf einem Kreuzfahrtschiff mit hundert wohlbetuchten Passagieren bedroht ein plötzlich aufgetauchter, sichtlich verarmter, verlumpter, hungernder „blinder“ Passagier eine Gruppe von Leuten mit einer Waffe. Man sieht ihm an, dass er keinen Moment zögern wird, seinen Forderungen nach Essbarem Nachdruck zu verleihen — vielleicht bleibt ihm keine Wahl, so zu handeln. Der ebenfalls bewaffnete Kapitän entdeckt die Sache und schiesst sofort, der blinde Passagier fällt tot aufs Deck. — Ist das Vorgehen des Kapitäns nun gut oder nicht gut? — Hier kommen wir zur kaum je lösbaren Moralfrage. Jedes Urteil für oder gegen Deine Meinung kann schnell als Ideologie identifiziert werden. Mit nur „wahr“ oder „falsch“ kommt man hier nicht weiter. Ähnliche Fragen tauchen auf bei Nationalhelden, die die eigenen Idole — oder auch die verhassten Idole der Feinde sein können, bei Märtyrern, bei Geliebten, bei Vorbildern und so fort. Zu allgemein gestellte Fragen lassen keine zu spezielle Antwort zu. Mehrwertige Logik werden wir hier aber nicht weiter behandeln.
Was die Aussagen betrifft, so sei erwähnt, dass wir unser Interesse hier hauptsächlich auf *mathematische Aussagen* richten wollen. Andere Aussagen wie *„Der Strom fliesst, da der Schalter geschlossen ist.“* spielen später in der *Schaltalgebra* (spezielle Boolsche Algebra) eine Rolle.

3.1.2 Aussagenvariablen

Beispiel: Wir betrachten die Gleichung $''x = y''$. Setzt man für die Variablen x die Zahl 1 und für y auch 1, so geht die Gleichung über in die Aussage $a :\equiv'' 1 = 1''$. Diese Aussage akzeptieren wir natürlich als wahr. Setzen wir hingegen $x = 2$ und $y = 3$, so geht die Gleichung über in die Aussage $b :\equiv'' 2 = 3''$.

[1] Sofern einer die Arithmetik mit Zahlen akzeptiert.
[2] Z.B. Logik von Lukasiewicz und Post sowie intuitionistische Logik.

Diese Aussage bedeutet für unser Sprachverständnis eine Zahlengleichung, die falsch ist. Der Gleichung $A :\equiv'' \; x = y''$ jedoch kommt weder der Wahrheitsgehalt *falsch noch wahr* zu. Aus A kann durch einsetzen von Werten für x und y eine Aussage werden, doch A selbst ist vorläufig eine *neutrale Stelle*, ein *Stellvertreter* oder *Platzhalter* für eine Aussage, so etwa wie bei einem Computer ein Speicherplatz, der ein Zeichen aufnehmen kann, selbst aber noch kein Zeichen, sondern eben nur ein Leerplatz ist. Daher legen wir fest:

Begriffserklärung 2 (Aussagenvariable) *: Ein orthographisches Zeichen, das nach Ersetzung durch ein sprachliches Gebilde in eine Aussage übergeht, nennen wir* **Aussagenvariable**.

Anmerkung:

Symbole 1 (für Aussagen und Aussagenvariablen) *: Um jederzeit die Unterscheidung zwischen Aussagen und Aussagenvariablen zu gewährleisten, verwenden wir für Aussagen* **Kleinbuchstaben** *(z.B. a, b, c . . .) und für Aussagenvariablen* **Grossbuchstaben** *(z.B. A, B, C . . .).*

Z.B. kann so dann für die Variable A (oder den Leerplatz A) eine bestimmte Aussage a gesetzt werden, welche wahr oder falsch sein kann. In der *zweiwertigen Logik* hat man hier immer zwei Möglichkeiten. A kann in eine *wahre* oder eine *falsche* Aussage übergehen.

Schematisch:

Tabelle 10. 0: Aussagenvariable, Aussagen und Wahrheitswerte

Aussagenvariable A	zugeordneter Wahrheitswert	
	Variante 1	Variante 2
Ersetzt durch *wahre* Aussage a_1	w	1
Ersetzt durch *falsche* Aussage a_2	f	0

Begriffserklärung 3 (Wahrheitswerte) *: Die verwendeten Abkürzungen w, f resp.* 1, 0 *heissen* **Wahrheitswerte**. *Sie stehen für „wahr“ oder „falsch“.*

Falls wir uns auf ein eindeutiges Verfahren zu Feststellung des Wahrheitswertes einer Aussage festlegen können (z.B. durch *interpersonale Verifikation*, Erzielung eines Konsenses in einem Gremium vernünftiger Menschen mit gleicher Sprache), so können wir definieren:

Definition 3.1 (Wahrheitswerte einer Aussage a) *: Der* **Wahrheitsert** $t(a)$ *einer Aussage a ist festgelegt durch*

$$t(a) := \begin{cases} 0 & , \quad falls\ a\ als\ falsch\ erkannt\ wird. \\ 1 & , \quad falls\ a\ als\ wahr\ erkannt\ wird. \end{cases}$$

(*Anmerkung:* „t“ in $t(A)$ bedeutet *„truth“*[3] . $t(a)$ ist auch eine *Funktion* auf dem Definitionsbereich „Menge der Aussagen“ in den Wertebereich $\{0, 1\}$.)
In der Aussagenlogik interessiert man sich nicht primär für den *Inhalt* einer Aussage, sondern nur für ihre *Form*. Bezüglich der Form haben wir hier bisher nur *nicht weiter zerlegbare Aussagen,* d.h. *elementare* oder *atomare* Aussagen getroffen. Im Gegensatz dazu gibt es auch *zusammengesetzte* Aussagen. Elementare Aussagen haben keine besondere Form. Sie lassen sich nicht sinnvoll in Teilaussagen zerlegen, die wieder entweder wahr oder falsch sind. Die einzige Eigenschaft, die sie noch haben, ist die, dass sie selbst jeweils entweder wahr oder falsch sind. Ein Beispiel dazu: „Die Tanne ist ein Baum.“ Diese Aussage lässt sich nicht weiter in Teilaussagen zerlegen. Für das weitere Studium der Sache dürfen wir daher vom Inhalt einer Aussage abstrahieren und nur noch ihren Wahrheitswert betrachten, denn das genügt hier.

[3] engl. „Wahrheit“

Definition 3.2 (Elementaraussage) *: **Elementaraussagen** sind Aussagen, die sich nicht weiter in Teilaussagen zerlegen lassen.*

Wie wir jetzt wissen, lassen sich Aussagenvariablen ersetzen durch Aussagen, denen jeweils entweder der Wahrheitswert 1 oder 0 zukommt. Einer Aussage ist also ein Wahrheitswert *zugeordnet*. Betrachten wir an Stelle einer Aussagenvariablen (Leerstelle) nun nicht bloss eine Aussage a, sondern auch deren zugeordneter Wahrheitswert $t(a)$, so ordnen wir in diesem Fall auch der Aussagenvariablen durch die Aussage einen Wahrheitswert zu. Wir sagen, wir *besetzen* oder *belegen* die Aussagenvariable mit einem Wahrheitswert.

Definition 3.3 (Belegung) *: Die Zuordnung eines Wahrheitswerts* 0 *oder* 1 *zu einer Aussagenvariablen A heisst „**Belegung** von A mit Wahrheitswerten“ .*

Durch eine Belegung einer Aussagenvariablen mit Wahrheitswerten wird daher die Variable stillschweigend durch eine Aussage etwa der Form „diese Stelle ist mit 0 besetzt“oder „die Stelle ist mit 1 besetzt“ersetzt. Die Aussagenvariable geht so in eine *abstrakte Aussage* über, denn abgesehen vom eingesetzten Wahrheitswert, spielen für unsere Zwecke Inhalt und Form der neuen Aussage keine Rolle. Auch Inhalt und Form der ursprünglichen Aussagen a_i brauchen nicht bekannt zu sein. In der *formalen Logik* interessieren wir uns daher einzig für die Belegungen und die Verknüpfungen der Aussagenvariablen (vgl. nächstes Kapitel), aber nicht für die Inhalte der Aussagen.

Tabelle 10. 1: Belegung einer Aussagenvariablen mit Wahrheitswerten

Aussagenvariable	A	Bedeutung	Zugeordnete Aussage
Belegungen	1	Wert „wahr“	Aussage a_1, mit beliebigem wahren Inhalt
	0	Wert „falsch“	Aussage a_2, mit beliebigem falschen Inhalt

Kapitel • Chapitre 4

Aussagen über Aussagen: Zusammengesetzte Aussagen

4.1 Die Negation

Zur Gewinnung der Negation einer Aussage treffen wir die nachstehende Vereinbarung. Einer Aussage a_1 sei eine neue Aussage a_2 wie folgt zugeordnet: a_1 ist genau dann wahr wenn a_2 falsch ist.

Beispiele: (1) $a_1 :\equiv$ "Es regnet." (3) $b_1 :\equiv$ "$3 = 5$"
(2) $a_2 :\equiv$ "Es regnet nicht." (4) $b_2 :\equiv$ "$3 \neq 5$"

Die Aussagen a_2 (bzw. b_2) empfinden wir mit unserem natürlichen Sprachgefühl als das *Gegenteil* von a_1 (bzw. b_1). Daher wird niemand opponieren, wenn wir definieren:

Definition 4.1 (Negation, „¬“) *: Eine der Aussage a_1 zugeordnete Aussage a_2, die genau dann wahr ist, wenn a_1 falsch ist, heisst „***Negation** *$\neg a_1$“ von a_1.*

Diese Definition lässt sich auch mittels einer Tabelle mit *Aussagenvariablen* wiedergeben, in der eine vollständige Sammlung aller möglichen Belegungen mit Wahrheitswerten aufgeführt ist, wobei jede Belegung einen Aussagentyp repräsentiert. Eine solche Tabelle nennen wir *Wahrheitstabelle*. Da wir den Begriff *Wahrheitstabelle* hiermit zwar zweckdienlich und verständlich, aber eben nur exemplarisch und nicht vollständig lückenlos umschrieben haben, können wir hier nicht von einer exakten *mathematischen Definition* des Begriffes sprechen. Für unsere Zwecke wird aber die so gegebene Begriffserklärung ausreichen.

Begriffserklärung 4 (Wahrheitstabelle) *: Eine Tabelle aller möglichen Belegungen von Aussagenvariablen mit Wahrheitswerten nennen wir* **Wahrheitstabelle**.

Die Negation lässt sich demnach durch folgende Tabelle definieren:

Tabelle 10.0: Wahrheitstabelle zur Definition von ¬

A	$\neg A$
0	1
1	0

Die Aussage $\neg A$ ist jetzt formal zusammengesetzt, nämlich aus den Zeichen ¬ und A. Das Zeichen ¬ bezeichnen wir als *logisches Zeichen*.

Achtung: Die Aussage $a_3 :\equiv$ "Die Sonne scheint" ist nicht etwa die Negation von $a_1 :\equiv$ "Es regnet". Es kann ja regnen, wenn auch die Sonne scheint. Man denke an die wunderbaren Regenbogen. Also aufgepasst! Hüte Dich davor, innere Beziehungen in Aussagen hineinzuinterpretieren, in die sie nicht hineingehören.

Bemerkung: In der Logik verwenden wir das Zeichen $\neg$ (z.B. bei $\neg A$, nicht aber bei $\bar{A}$), um Verwechslungen mit der Mengenlehre (Komplementmenge), der Schaltalgebra, oder mit komplexen Zahlen (konjugiert–komplexe Zahl) vorzubeugen. Denn in mathematischen Definitionen verwenden wir die logischen Symbole als schon bekannte Sprachelemente (Metasprache), um mathematische Symbole zu definieren. Diese Schreibweise hat technisch den Vorteil, dass sie *eindimensional* ist. Sie könnte von einer Maschine ab einer Spur eingelesen werden. Das spielt auch beim Studium der Beziehungen zwischen Logik und Maschinen eine grosse Rolle.

4.2 Die Konjunktion („und"-Verknüpfung)

Jetzt und später in den folgenden Unterkapiteln wollen wir logische Verknüpfungen betrachten, die aus einem logischen Zeichen (hier auch *Junktor* genannt) und zwei Aussagenvariablen bestehen. Um diese Verknüpfungen vernünftig definieren zu können, folgen wir einerseits dem Sprachgefühl. Andererseits wollen wir aber nicht den Verdacht aufkommen lassen, hier sei absolute Willkür am Werk. Dann würden wir ja die Mathematik auf Zufallsprodukte stützen. Um die Definitionen akzeptabel zu machen, vertraut man „vernünftigen Empfindungen" bei der Abwicklung eines *philosophischen Dialogs* über das Thema, das gerade in Frage steht. Ein Befürworter *(Proponent)* und ein Gegner *(Opponent)* sollen die Sache ausmachen und alle Möglichkeiten „vernünftig" ausdiskutieren. Falls ein Vorschlag suspekt erscheint, frägt man sich, ob das Gegenteil (das Komplement) etwa besser wäre. Kommt es dann so heraus, dass der Gegner einem nicht vom Gegenteil eines gemachten Vorschlags zu überzeugen vermag, so nimmt man den Vorschlag an. Denn im Rahmen der 2-wertigen Logik gibt es ja ausser *wahr* und *falsch* keine dritte Möglichkeit.
So gesehen lässt sich gegen die folgende Zuordnung der Wahrheitswerte zur Gesamtaussage wohl wenig einwenden:

Beispiele aus dem gewöhnlichen Zahlenrechnen:

$a :\equiv$ "$2+2=4$" und "$3\cdot 3=9$"	(wahre Aussage)
$b :\equiv$ "$2+2=5$" und "$3\cdot 3=9$"	(falsche Aussage)
$c :\equiv$ "$2+2=4$" und "$3\cdot 3=6$"	(falsche Aussage)
$d :\equiv$ "$2+2=5$" und "$3\cdot 3=6$"	(falsche Aussage)

Hier erzeugen wir also mittels „und" aus zwei Teilaussagen eine neue Gesamtaussage, die wieder entweder wahr oder falsch ist. (Z.B. aus der Aussage $a_1 :\equiv$ "$2+2=4$" und der Aussage $a_2 :\equiv$ "$3\cdot 3=9$" entsteht die neue Aussage a.) Symbolisch geschrieben haben wir folgende Zuordnung:

$$(a_1,\, a_2) \mapsto a :\equiv a_1 \wedge a_2.$$

„$\wedge$ " ist also das Zeichen für „und ". Daher können wir „$\wedge$" durch die folgende Wahrheitstabelle definieren:

Definition 4.2 (Konjunktion, „$\wedge$") *:*

Tabelle 10.1: Definition der Konjunktion

Var	A	B	$A \wedge B$
$t(Var)$	0	0	0
	0	1	0
	1	0	0
	1	1	1

Die Aussage $a :\equiv a_1 \wedge a_2$ ist somit nur dann wahr, wenn a_1 sowohl als auch a_2 wahr sind. Sonst ist a falsch!
Bemerkung: In der *Schaltalgebra* verwendet man für „und“ häufig den Malpunkt (z.B. $a_1 \cdot a_2$ statt $a_1 \wedge a_2$). Das kann aber in der Logik zu *Verwirrungen* führen. **Beispiel:**

$$(a_1 \wedge a_2) :\equiv \underbrace{(3 \cdot 3 = 9}_{a_1} \wedge \underbrace{6 + 5 = 11)}_{a_2} \not\equiv (3 \cdot 3 = \underbrace{9 \cdot 6 + 5}_{59} = 11)$$

4.3 Die Adjunktion, Disjunktion („oder“-Verknüpfung)

Wir studieren wieder einige Aussagen aus dem Bereiche der Mathematik. Diese haben nicht den Nachteil von Aussagen der Umgangssprache, welche aus Gewohnheitsgründen nur schwerlich in der blossen abstrakten Reduktion auf ihre Wahrheitswerte betrachtet werden können. Wer bringt es schon leicht fertig, eine Aussage wie "Napoleon ist gestorben oder Peter hat einen langen Bart" unabhängig von ihrem spezifischen Inhalt zu betrachten? Manch einer frägt sich doch sofort, was denn Napoleon mit Peters Bart zu tun hat — und schüttelt den Kopf. Doch auf eine etwaige inhaltliche Beziehung der Teilaussagen kommt es ja eben jetzt gar nicht an! Gerade davon wollen wir abstrahieren.

Beispiele: Die Wahrheitswerte folgender zusammengesetzter Gesamtaussagen lassen sich sofort wie angegeben akzeptieren. Ansonst müsste man ja das Gegenteil akzeptieren können, was weit weniger dem natürlichen Empfinden entspricht. Ein Drittes ist ausgeschlossen, denn wir behandeln *2-wertige Logik:*

$a :\equiv$ “$2+2=4$” oder “$3 \cdot 3 = 9$”	(wahre Aussage)
$b :\equiv$ “$2+2=5$” oder “$3 \cdot 3 = 9$”	(wahre Aussage)
$c :\equiv$ “$2+2=4$” oder “$3 \cdot 3 = 6$”	(wahre Aussage)
$d :\equiv$ “$2+2=5$” oder “$3 \cdot 3 = 6$”	(falsche Aussage)

Eine durch *„oder“* verknüpfte Gesamtaussage können wir als *wahr* akzeptieren, soblad eine Teilaussage als wahr erkannt ist. Mit „oder“ meinen wir, dass nur eines wahr zu sein braucht.
Symbolisch schreiben wir:

$$(a_1, a_2) \mapsto a :\equiv a_1 \vee a_2.$$

Das Zeichen „$\vee$“, das jetzt für „oder“ steht, symbolisiert den Anfangsbuchstaben des lateinischen Wortes „vel“[1]. „$\wedge$“ ist das auf den Kopf gestellte „$\vee$“. Die folgende Definition können wir jetzt als sinnvoll akzeptieren:

Definition 4.3 (Adjunktion, „$\vee$“) *:*

Tabelle 10.2: Definition der Adjunktion

Var	A	B	$A \vee B$
$t(Var)$	0	0	0
	0	1	1
	1	0	1
	1	1	1

Bemerkung zur Aufstellung der Tabelle: Es erscheint als praktisch, die Reihenfolge der Wahrheitswerte von A und B so zu wählen, dass diese gerade eine *Abzählung der Dualzahlen* darstellen. Die Zeilen unter den Eingangsvariablen kann man dann als Dualzahlen lesen. Bei vier Eingangsvariablen hätte man zuerst 0000, dann 0001, dann 0010, dann 0011, dann 0100, dann 0101 etc. .

[1] lat. „vel“ bedeutet „oder“.

4.4 Die Exklusion („entweder – oder“–Verknüpfung)

Mit „Exklusion“ meinen wir das *ausschliessende oder*. Wenn man hört: „Die Erde ist entweder ein Planet — oder sie ist kein Planet“, so hat im allgemeinen niemand etwas dagegen einzuwenden. Doch auch hier wieder aufgepasst! Lassen wir uns nicht vom Inhalt verführen. Wir wollen ja nicht Teilaussagen betrachten, bei denen neben dem Wahrheitswert noch die inhaltliche Struktur eine Rolle spielt.

Eine Aussage $a :\equiv a_1$ „entweder – oder “ a_2 schreiben wir symbolisch wie folgt:

$$(a_1,\, a_2) \mapsto a :\equiv a_1 \dot{\vee} a_2.$$

Wir definieren nun das „entweder – oder“ durch die unten aufgeführte Wahrheitstabelle. Dabei beachte man, dass im Zweifelsfalle der Wahrheitswert zu akzeptieren ist, falls niemand etwas dagegen einwenden kann:

Definition 4.4 (Exklusion, „$\dot{\vee}$“) *:*

Tabelle 10.3: Definition der Exklusion

Var	A	B	$A \dot{\vee} B$
$t(Var)$	0	0	0
	0	1	1
	1	0	1
	1	1	0

Diese Definition steht im Einklang mit dem üblichen logischen Denken. Dem kann schwerlich widersprochen werden.

4.5 Die Subjunktion unabhängiger Aussagen

Dieses Unterkapitel handelt von *wenn–dann–Aussagen*. „Wenn die Badewanne voll ist, so (d.h. dann) läuft das Badewannewasser über“ ist ein umgangssprachliches Beispiel einer solchen Aussage. — Doch gerade solche umgangssprachliche Beispiele nützen uns vorerst in der mathematischen Logik nicht viel, da zwischen den einzelnen Satzteilen eine inhaltliche Beziehung besteht und nicht nur eine rein formale. (Das Badewannewasser erfordert die Badewanne.) Inhaltlich verknüpfte wenn–dann–Aussagen wollen wir hier vorerst *nicht* speziell betrachten.
Uns geht es mehr um die Zusammensetzung unabhängig alleine für sich bestehender Aussagen zu neuen Aussagen. Anders gesagt: Wir wollen neue Aussagen erzeugen, indem wir die schon vorhandenen Aussagen zu neuen Aussagen mittels logischer Zeichen verknüpfen. Und die logischen Zeichen leiten wir aus gammatikalischen Konjunktionen[2] ab. Im Beispiel hat das überlaufende Badewannewasser zwingend mit der Badewanne zu tun: Die Aussagen sind nicht inhaltlich unabhängig. Der Wahrheitswert der zweiten Aussage wird so durch den Inhalt der ersten Aussage wesentlich mitbestimmt. Andererseits mag es manch einem komisch zu Mute sein, wenn wir versuchen, durch „wenn–dann“ unabhängige alltagssprachliche Aussagen zu verknüpfen. Beispiel: „Wenn (falls) der Mond Ohren hat, dann gelingt es meinem Onkel, 40 Meter hoch zu hüpfen“. So eine Aussageverknüpfung wird jeder wohl rasch als *Unsinn* abtun, da sie vom alltäglichen Sprachgebrauch her als ungewohnt erscheint. Natürlich sind hier die einzelnen Aussagen unabhängig. Doch was soll das Gerede von „ob der Mond Ohren hat“? — Auf die physikalische Realität bezogen, handelt es sich hier um eine falsche Aussage. Doch immerhin um eine Aussage. Auf einer Kinderzeichnung kann das sogar vorhanden und somit wahr sein. — Wie soll man daher den Wahrheitswert einer zusammengesetzten Aussage beurteilen, wenn man mit dem für uns unwesentlichen Inhalt schon enorme Mühe hat? Solche Konstruktionen sind ja in der Umgangssprache unüblich und ungewohnt. Vielfach erkennen wir daher in umgagssprachlichen Aussagen den zweiten Teil

[2] Konjunktion: Das ist eine der 10 Wortarten.

als Spezialisierung des ersten Teils, d.h. wir finden eine innere Abhängigkeit. Anders in der Welt der Märchen: „Schneewittchen ist alt geworden. Daher wurde es dann vom Wolf gefressen.“ Wie will man dagegen argumentieren?
Wie soll man aber mit voneinander unabhängigen mathematischen Aussagen umgehen? Eine Methode bietet der folgende Ansatz: Falls wir eine Aussage komisch finden, sie also nicht gleich akzeptieren oder verwerfen können, so fragen wir uns, ob denn die Aussage falsch, also das Gegenteil wahr sein muss. Einen dritten Wahrheitswert gibt es nicht in der zweiwertigen Logik. Falls man die Wahrheit des Gegenteils nicht stützen kann, d.h. sie verwerfen muss, so akzeptieren wir die Aussage.
Nehmen wir z.B. eine Gleichung. Hier handelt es sich um eine eigenständige Aussage, die wahr oder falsch sein kann. Solche Gleichungen sind inhaltlich nicht verknüpft, da keine für das Bestehen der anderen gebraucht wird. So erhalten wir mit Gleichungen als Teilaussagen:

$a :\equiv$ Wenn gilt “$2+2=4$”, dann gilt “$3\cdot 3=9$”.	(wahre Aussage)
$b :\equiv$ Wenn gilt “$2+2=5$”, dann gilt “$3\cdot 3=9$”	(wahre Aussage)
$c :\equiv$ Wenn gilt “$2+2=4$”, dann gilt “$3\cdot 3=6$”	(falsche Aussage)
$d :\equiv$ Wenn gilt “$2+2=5$”, dann gilt “$3\cdot 3=6$”	(wahre Aussage)

Man kann nichts dagegen einwenden, wenn jemand aus einer falschen Aussage etwas Wahres oder auch etwas Falsches folgert. Das kommt immer gut, denn der Fall, wo es schlecht kommen könnte, existiert gar nicht. Unter der Voraussetzung einer falschen Gleichung können wir eine wahre oder eine falsche Gleichung, d.h. irgend etwas folgern. Denn der Fall, in dem man die Voraussetzung antrifft und akzeptiert, tritt nie ein. Wir können daher hier auch nie eine falsche Folgerung durchführen. Daher müssen wir *wahr* akzeptieren.
Aus etwas Wahrem können wir natürlich etwas Wahres folgern. Doch aus etwas Wahrem dürfen wir nichts Falsches ableiten, das hiesse ja Fehler machen. Man soll doch in der Logik aus Wahrheiten nicht Unsinn gewinnen können.
Daher dürfen wir die „wenn–dann–Verknüpfung“, symbolisch gekennzeichnet durch das Zeichen „$\Rightarrow$“, wie folgt definieren:

Definition 4.5 (Subjunktion, „$\Rightarrow$“) *:*

Tabelle 10.4: Definition der Subjunktion

Var	A	B	$A \Rightarrow B$
$t(Var)$	0	0	1
	0	1	1
	1	0	0
	1	1	1

Bemerkung zu den Pfeilen: In der Mathematik verwenden wir noch andere Pfeilarten: Z.B mit $A \mapsto B$ meinen wir eine *Abbildung* von A nach B. Mit $x \to x_0$ drücken wir das „strebt gegen“ resp. „konvergiert gegen“ aus (beim Bilden von Grenzwerten) etc.. Statt $A \Rightarrow B$ schreiben wir auch $B \Leftarrow A$.

Sprechweisen: $A \Rightarrow B$ lesen wir als „falls A gilt, so gilt auch B“. Oder auch als „wenn A dann B“. Oder „wenn A so gilt auch B“ etc.. Die Ausdrücke *„Implikation“* , *„impliziert“* , *„ist notwendig“* oder *„ist hinreichend“* findet man meist nur im Zusammenhang mit wahren Subjunktionen. (Doch haben in der Mathematik, die ja seit Aristoteles immer als „international“ akzeptiert war, zum Glück die Autoren noch die Freiheit, den für sie gerade sinnvollen Wortschatz selbst aufzubauen. Die Konsequenz ist, dass leider dann nicht alle exakt die selbe Sprache verwenden, wodurch aber selten jemand behindert wird. Es spielt keine Rolle, denn gute Mathematiker liefern ja ihr verwendetes Sprachgebäude gerade mit, und andere gute Mathematiker verstehen zu lesen.)

4.6 Die Bijunktion unabhängiger Aussagen

Unter „Bijunktion“ verstehen wir die *genau–dann–wenn–Verknüpfung*. Folgende Beispiele mögen die Situation bezüglich der Wahrheitswerte klären. Man beachte, dass wir wiederum inhaltlich unabhängige Aussagen verwenden, da nur die Wahrheitswerte und die logische genau–dann–wenn–Verknüpfung wesentlich sind, nicht etwaige inhaltliche Zusammenhänge.

$a :\equiv$ “$2+2=4$” genau dann wenn “$3\cdot 3=9$”.	(wahre Aussage)
$b :\equiv$ “$2+2=5$” genau dann wenn “$3\cdot 3=9$”	(falsche Aussage)
$c :\equiv$ “$2+2=4$” genau dann wenn “$3\cdot 3=6$”	(falsche Aussage)
$d :\equiv$ “$2+2=5$” genau dann wenn “$3\cdot 3=6$”	(wahre Aussage)

Dass die letzte Zeile, d.h. „falsch genau dann wenn falsch“, als richtig gewertet wird, dagegen können wir nichts einwenden, denn verwerfen darf man diese Richtigkeit ja wohl kaum. Also muss man sie akzeptieren. Symbolisch verwenden wir für „genau dann wenn“ das Zeichen „$\Leftrightarrow$“. Die logische Verknüpfung definieren wir wie folgt:

Definition 4.6 (Bijunktion, „$\Leftrightarrow$“) *:*

Tabelle 10.5: Definition der Bijunktion

Var	A	B	$A \Leftrightarrow B$
$t(Var)$	0	0	1
	0	1	0
	1	0	0
	1	1	1

Bemerkung: Es ist nun sinnvoll, den eingeführten logischen Verknüpfungszeichen Namen zu geben. Daher führen wir folgende Sprechweisen ein:

Begriffserklärung 5 (Junktoren) *:*
Logische Verknüpfungszeichen wie $\neg$, $\wedge$, $\vee$, $\dot{\vee}$, $\Rightarrow$, $\Leftrightarrow$ *nennen wir* **Junktoren**.

Und weiter:

Begriffserklärung 6 (Logische Funktion) *: Durch einen Junktor wird einer Belegung der verknüpften Aussagenvariablen mit Wahrheitswerten ein neuer Wahrheitswert, der Wahrheitswert der Verknüpfung, zugeordnet. Eine solche Zuordnung nennen wir* **logische** *oder* **binäre Funktion**.

4.7 Klammerungen

Wir betrachten zwei zusammengesetzte Aussagen $R \equiv A \wedge B$ und $S \equiv B \vee C$. Man kann nun vermuten, dass der Ausdruck $Z \equiv: A \wedge B \vee C$ nicht mehr eindeutig ist. Z könnte bedeuten:

$$Z \equiv R \vee C \equiv (A \wedge B) \vee C.$$

Jedoch auch:

$$Z \equiv A \wedge S \equiv A \wedge (B \vee C).$$

Wir stellen daher folgendes Problem:

Problem 4.1 *Hat eine zusammengesetzte Aussage bei verschiedenen Klammerungen immer dieselben Wahrheitswerte?*

Ein Vergleich bei zwei speziell gewählten Belegungen für obige Ausdrücke zeigt die Nichteindeutigkeit auf:

$(A$	$\wedge$	$B)$	$\vee$	C	A	$\wedge$	$(B$	$\vee$	$C)$
0		1		1	0		1		1
$\searrow$		$\swarrow$		$\downarrow$	$\downarrow$		$\searrow$		$\swarrow$
	0			1	0			1	
	$\searrow$			$\swarrow$	$\searrow$			$\swarrow$	
			1			0			$(\neq)$

Resultat: $(A \wedge B) \vee C$ hat also nicht bei jeder möglichen Belegung den gleichen Wahrheitswert wie $A \wedge (B \vee C)$. Daher gilt der Satz:

Satz 4.1 (Klammerungen) *: Bei zusammengesetzten Aussagen mit mehreren Junktoren sind Klammerungen im allgemeinen notwendig.*

Klammern können daher nur weggelassen werden, wenn dadurch die Eindeutigkeit nicht verlorengeht. Das gleiche Problem kennt man ja schon von der Arithmetik mit Zahlen. Wie heisst es da nicht schon wieder? — „Punkt vor Strich!“— Wäre es daher nicht auch geschickt, hier ebenfalls derartige Prioritätsregeln einzuführen? Um das zu tun, legen wir fest:

Definition 4.7 (Prioritätsregeln) *: Wir vereinbaren:*

$\neg$	bindet stärker als	$\wedge$.
$\wedge$	bindet stärker als	$\vee$.
$\vee$	bindet stärker als	$\Rightarrow$.
$\Rightarrow$	bindet stärker als	$\Leftrightarrow$.

Man wird sofort bemerken, dass in dieser Definition $\dot{\vee}$ fehlt. Das macht nichts. Auch die weiter im Text folgenden neu definierten Junktoren lassen wir hier aus, um die Sache jetzt nicht zu überladen. Wir werden uns gegebenenfalls mit Klammern behelfen. Die obige Definition wird ausreichen.
Nun kann man sich aber noch eine zweite Frage stellen: Wie ist es, falls in einem Zusammengesetzten Ausdruck nur ein einziger Junktor, dafür aber mehrmals, vorkommt? Also fragen wir:

Problem 4.2 *Hat eine zusammengesetzte Aussage wie z.B. $A \Rightarrow B \Rightarrow C$ bei verschiedenen Klammerungen immer dieselben Wahrheitswerte?*

Wie oben können wir die Frage verneinen, falls wir eine Belegung finden, bei der bei den verschiedenen Klammerungen verschiedene Wahrheitswerte herauskommen.
Beispiel:

$(A$	$\Rightarrow$	$B)$	$\Rightarrow$	C	A	$\Rightarrow$	$(B$	$\Rightarrow$	$C)$
0		1		0	0		1		0
$\searrow$		$\swarrow$		$\downarrow$	$\downarrow$		$\searrow$		$\swarrow$
	1			0	0			0	
	$\searrow$			$\swarrow$	$\searrow$			$\swarrow$	
			0			1			$(\neq)$

Daher könne wir festhalten:

Satz 4.2 (Klammerungen bei nur mehrfachem Junktor) *: Bei zusammengesetzten aussagenlogischen Ausdrücken mit einem einzigen, aber mehrfach vorkommenden Junktor sind Klammerungen im allgemeinen auch notwendig.*

Mittels Wahrheitstabellen kann man dagegen folgenden Sachverhalt nachprüfen:

Satz 4.3 (Klammerungen mit nur $\wedge$, $\vee$ oder $\Leftrightarrow$) *: Bei zusammengesetzten Aussagen mit einem einzigen Junktor $\wedge$, $\vee$ oder $\Leftrightarrow$, sind Klammern nicht notwendig.*

Das heisst: $A \wedge B \wedge C$, $A \vee B \vee C$ oder $A \Leftrightarrow B \Leftrightarrow C$ sind eindeutig bestimmte Ausdrücke. Wie wir auch die Klammern setzen, die Wahrheitswerte am Schluss sind dieselben.
Um im Folgenden dennoch die Schreibweise etwas mehr vereinfachen zu können, vereinbaren wir die *Linksassoziativität*. In einem von links her geklammerten Ausdruck lassen wir einfach die Klammern weg.
Beispiel:

$$((A \Rightarrow B) \Rightarrow C) \Rightarrow D \quad \equiv: \quad A \Rightarrow B \Rightarrow C \Rightarrow D$$

Definition 4.8 (Linksassoziativität) *: Fehlen in einem nicht eindeutigen aussagenlogischen Ausdruck die Klammern, so gilt der Ausdruck als von links her geklammert.*

Beispiele:

1. $(\neg A) \vee (B \wedge C) \equiv \neg A \vee B \wedge C$
2. $(\neg A) \wedge (B \vee C) \equiv \neg A \wedge (B \vee C)$

Die letzte Klammer im Beispiel 2 muss bleiben!

4.8 Aussageformen

4.8.1 Definition des Begriffs „Aussageform“

Seien X_1, X_2, X_3 etc. Aussagenvariablen. Wir wollen nun den Begriff *Aussageform* wie folgt *rekursiv* erklären:

Definition 4.9 (Aussageform) *: Ein Ausdruck*[3] *P heisst* **Aussageform***, falls gilt:*

1: $P \equiv X_i$, $(i = 1, 2, 3, \ldots)$
2: $P \equiv P(X_1, X_2, \ldots) \equiv$ *sinnvolle Verknüpfung von endlich vielen Aussagenvariablen durch Junktoren, wobei auch Klammern stehen können.*

Mit „sinnvolle Verknüpfung“ meinen wir hier, dass jede Klammer beidseitig geschlossen ist, dass zweistellige Junktoren immer zwischen Ausdrücken stehen, die schon als Aussageform erkannt sind und dass „$\neg$“ immer vor einer (als solche erkannten) Aussageform steht. Dabei kann natürlich statt X_i auch X, Y, Z etc. vorkommen. Das sind nur Namen.

Beispiele: X, Y, $\neg X$, $X_1 \wedge X_2$, $\neg X \vee \neg X$, $(X \vee (Y \wedge \neg Z) \Rightarrow (X \Rightarrow \neg Z))$ etc. .

Mit Hilfe von *Wahrheitswerttabellen* machen wir uns eine Übersicht über alle Belegungen der Variablen einer Aussageform mit Wahrheitswerten. So können wir auf übersichtliche Art die Gesamtwarheitswerte zu jeder Belegung ermitteln. Das damit verbundene Problem wollen wir formulieren:

Problem 4.3 (Wahrheitswerttabelle) *: Wie gelangt man zu einer Übersicht über sämtliche Wahrheitswerte einer Aussageform mittels einer Wahrheitswerttabelle? Wie stellt man eine solche Tabelle auf?*

Dazu ein Beispiel: Wir verschaffen uns die Übersicht über die Wahrheitswerte von $\neg(X \wedge \neg Y) \Rightarrow Z$:

Tabelle 10.6: Wahheitswerte von $\neg(X \wedge \neg Y) \Rightarrow Z$

[3] P bedeutet „Polynom“

X	Y	Z	$\neg Y$	$X \wedge \neg Y$	$\neg(X \wedge \neg Y)$	$\neg(X \wedge \neg Y) \Rightarrow Z$
0	0	0	1	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	1	0
0	1	1	0	0	1	1
1	0	0	1	1	0	1
1	0	1	1	1	0	1
1	1	0	0	0	1	0
1	1	1	0	0	1	1

In der letzten Kolonne sehen wir die *Gesamtwahrheitswerte*. Man kann nun einsehen, dass durch eine Belegung der Aussagenvariablen X, Y und Z mit Wahrheitswerten die Aussageform $\neg(X \wedge \neg Y) \Rightarrow Z$ zu einer Aussage wird der Art „Form wird wahr“ (Wert 1) oder „Form wird falsch“ (Wert 0). Generell können wir folgende Feststellung machen:

Feststellung: Ein Gesamtwahrheitswert einer Aussageform bei einer gegebenen Belegung führt immer zur *neuen Aussage*: *„. . . Form besitzt Wahrheitswert . . . “* .
Weiter zeigt die Wahrheitstabelle auch die durch die Aussageform gegebene *Belegungsfunktion* (auch Wahrheitsfunktion, binäre Funktion), d.h. die Zuordnung: {Mögliche Belegungen} $\mapsto$ { 0, 1 }.
Übungen dazu befinden sich im Übungsbuch *DIYMU* Kap. 2 Bibl.: wirz.

4.8.2 Aussageform mit genau zwei Aussagenvariablen

Aussageformen mit genau zwei Aussagenvariablen bestehen aus einem zweistelligen Junktor, der zwei Teile verknüpft, die ihrerseits wieder spezielle Aussageformen sind. Ein solcher Teil ist entweder eine Aussagenvariable — oder eine Aussagenvariable verbunden mit einem einstelligen Junktor, z.B. mit $\neg$. (Später, wenn die Begrifflichkeit eingeführt sein wird, werden wir von einer „Funktion mit einem Argument“ reden.) Man sieht sofort, dass es *genau* 4 *einstellige Junktoren* geben kann: (1) $\neg$, (2) *identisch wahr* resp. w (der Junktor, der jeder Variablen immer den Wert „wahr“ resp 1 zuweist), (3) *identisch falsch* resp. f (der Junktor, der jeder Variablen immer den Wert „falsch“ resp 0 zuweist) und (4) *neutral* resp. n, der Junktor, der die Variable so lässt wie er ist. Dazu die Tabelle:

Tabelle 10.7: Mögliche einstellige Junktoren

X	*neutral* X	$\neg X$	w	f
0	0	1	1	0
1	1	0	1	0

Andere Kombinationsmöglichkeiten für die Wahrheitswerte hat man nicht. Darauf aufbauend können wir uns jetzt die wichtige Frage stellen: Wieviele Möglichkeiten gibt es bei einer Verknüpfung von zwei Aussagenvariablen? Man hat daher das Problem:

Problem 4.4 (Belegungsfunktionen) *: Mache Dir eine Übersicht über sämtliche Belegungsfunktionen einer Aussageform, die nur* 2 *Aussagenvariablen enthält.*

Wir erstellen dazu wieder eine Tabelle, wobei eine mögliche Gesamtverknüpfung vorerst einfach f_i heisst. Die Anzahl der möglichen Funktionen ergibt sich aus der möglichen Anzahl geordneter 4-er Gruppen mit den Elementen 0 und 1. Das ist auch die Anzahl der Dualzahlen von 0000 bis 1111, d.h. im 10-er System die Anzahl der Zahlen von 0 bis $2^4 - 1$ (d.h.bis 15). Das gibt 16 Möglichkeiten. Um sie alle darzustellen, wählen wir wieder eine ans Dualsystem angelehnte Abzählungsmethode:

Tabelle 10.8: Mögliche zweistellige Junktoren

X_1	X_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
		f	$\wedge$					$\dot{\vee}$	$\vee$	$\downarrow$	$\Leftrightarrow$				$\Rightarrow$	$\mid$	w

Man erkennt sofort: f_0 ist die *identisch falsche Verknüpfung*. Was wir auch für Belegungen nehmen, das Resultat ist immer falsch. Entsprechend ist f_{15} die *identisch wahre Verknüpfung*. f_1 erkennen wir als „$\wedge$“. f_2 hat noch keinen Namen. Man kann f_2 als $\neg(X_1 \Rightarrow X_2)$ interpretieren oder auch als $X_1 \wedge \neg X_2$. f_8 und f_{14} sind noch wichtige Verknüpfungen, die Namen tragen:

Definition 4.10 (Nicodsche Verknüpfung, Scheffer–Strich, W und F) *:*
f_0 *heisst* **identisch falsche** *Verknüpfung F,* f_{15} *heisst* **identisch wahre** *Verknüpfung W.* f_8 *heisst* **Nicodsche** *Verknüpfung* ($\downarrow$) *und* f_{14} *ist der Scheffer–Strich* ($|$) *.*

Bemerkung: In der *Schaltalgebra* entspricht die Nicodsche Verknüpfung dem NOR und der Scheffer–Strich dem $NAND$. Den Scheffer–Strich $|$ schreibt man auch in der Form $\uparrow$.

4.8.3 Doppelte Verneinung und Regeln von De Morgan

„Nicht *nicht die Wahrheit sagen*“ bedeutet von unserem jetztigen Wissensstand aus gesehen „klar die Wahrheit sagen“. Wir begegnen hier der *doppelten Verneinung* („nicht ... nicht ...“). Mittels der Wahrheitstafel kann man in der Aussagenlogik belegen, dass diese doppelte Verneinung eine „Be-ja-ung“ ist. Es gilt der Satz:

Satz 4.4 (Doppelte Verneinung) *:* $A \equiv \neg\neg A.$

Beweis: Den Beweis führen wir mittels der Wahrheitstafel. Falls die Wahheitswerte zeilenweise übereinstimmen, ist die Sache bewiesen. Wir sehen sofort, dass die erste und die dritte Kolonne übereinstimmen, der Satz also *wahr* ist:

Tabelle 10.8: Doppelte Verneinung

A	$\neg A$	$\neg\neg A$
0	1	0
1	0	1

Untersucht man nun verneinte $\wedge$– sowie $\vee$–Verknüpfungen, so stösst man auf die Regeln von *De Morgan*:

Tabelle 10.9: De Morgan

A	B	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$\neg(\neg A \wedge \neg B)$	$A \vee B$
0	0	1	1	1	0	0
0	1	1	0	0	1	1
1	0	0	1	0	1	1
1	1	0	0	0	1	1

Aus den letzten beiden Kolonnen und wegen der doppelten Verneinung ersieht man:

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

Ebenso beweist man:

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

Nehmen wir statt A neu $\neg X_1$ und statt B neu $\neg X_2$, so dürfen wir wegen der doppelten Verneinung schreiben:

Satz 4.5 (De Morgan) *:*

1. $\neg(X_1 \wedge X_2) \equiv \neg X_1 \vee \neg X_2,$
2. $\neg(X_1 \vee X_2) \equiv \neg X_1 \wedge \neg X_2.$

4.8.4 Aussageform mit mehreren Aussagenvariablen und unbekannten Junktoren

Betrachtet man die obige Tabelle 10 , so kann man sich z.B. fragen, ob und wie etwa f_{11} durch andere Junktoren ausdrückbar sei. Dass so etwas immer möglich ist, lässt sich in einem *Hilfssatz* so ausdrücken:

Lemma 4.1 (Reduktion auf gebräuchliche Junktoren) *: Jede Aussageform lässt sich durch eine Wahrheitsfunktion $f(X_1, X_2, \ldots)$ (d.h. durch eine* **Ersatzform***) darstellen, die nur durch die wenigen Junktoren $\neg$, $\wedge$ sowie $\vee$ vorkommen.*

Zum Beweis: Das können wir einsehen, indem wir die Methode aufzeigen, mit der die Ersatzform gewonnen werden kann. Da zur Anwendung der Methode keine Einschränkungen bestehen, funktioniert das immer. Wir zeigen das am Beispiel von f_{11}:

Tabelle 10.11: Untersuchung von f_{11}

X_1	X_2	$f(X_1, X_2) = f_{11}$	$\neg X_1$	$\neg X_2$	$\neg X_1 \wedge \neg X_2$	$X_1 \wedge \neg X_2$	$X_1 \wedge X_2$	$(\neg X_1 \wedge \neg X_2) \vee (X_1 \wedge \neg X_2) \vee (X_1 \wedge X_2)$
0	0	1	1	1	1	0	0	1
0	1	0	1	0	0	0	0	0
1	0	1	0	1	0	1	0	1
1	1	1	0	0	0	0	1	1

$f(X_1, X_2) = f_{11}$ ist nur wahr, wenn die Belegungen der Zeile 1 — oder die der Zeile 3 resp. 4 vorhanden ist. Sonst ist f_{11} falsch, denn in der letzten Kolonne muss eine 1 stehen. Die Belegung der Zeile 1 ist aber vorhanden, wenn X_1 den Wert 0 und X_2 den Wert 0 hat, d.h. wenn $\neg X_1$ den Wert 1 und $\neg X_2$ auch den Wert 1 hat. Die Belegung der Zeile 3 ist entsprechend vorhanden, wenn X_1 den Wert 1 und X_2 den Wert 0 hat, d.h. wenn $\neg X_2$ den Wert 1 annimmt. Ebenso ist die Belegung der Zeile 4 vorhanden, wenn X_1 den Wert 1 und X_2 auch den Wert 1 hat. D.h. $f(X_1, X_2) = f_{11}$ ist wahr, wenn $\neg X_1$ den Wert 1 und $\neg X_2$ auch den Wert 1 hat — oder wenn X_1 den Wert 1 und $\neg X_2$ gleichzeitig auch den Wert 1 — oder wenn X_1 den Wert 1 und X_2 auch den Wert 1 hat. Sonst ist $f(X_1, X_2) = f_{11}$ falsch. Exakt dieselben Wahrheitswerte entstehen aber, wenn man $\neg X_1 \wedge \neg X_2$ (nur wahr im Falle der Zeile 1) mit $X_1 \wedge \neg X_2$ (nur wahr im Falle der Zeile 3) und mit $X_1 \wedge X_2$ (nur wahr im Falle der Zeile 4) durch $\vee$ verknüpft (vgl. letzte Spalte). So sieht man ein, dass gilt:

$$f(X_1, X_2) = f_{11} \equiv (\neg X_1 \wedge \neg X_2) \vee (X_1 \wedge \neg X_2) \vee (X_1 \wedge X_2).$$

Im letzten Ausdruck kommen tatsächlich nur die Junktoren $\neg$, $\wedge$ sowie $\vee$ vor. Dieser Ausdruck ist aber etwa nicht eindeutig! Denn man kann auch wie folgt argumentieren:
$f(X_1, X_2) = f_{11}$ ist falsch, d.h. $\neg f(X_1, X_2) = \neg f_{11}$ wahr, genau wenn die Belegung der Zeile 2 vorhanden ist. Dies ist dann der Fall, wenn X_1 den Wert 0 und X_2 den Wert 1 haben, d.h. wenn $\neg X_1$ den Wert 1 und X_2 auch den Wert 1 hat. Dies ist genau dann so, wenn $\neg X_1 \wedge X_2$ wahr ist. Wie wir später beweisen, ist das genau dann der Fall, wenn $\neg(\neg X_1 \wedge X_2)$ falsch ist. $\neg(\neg X_1 \wedge X_2)$ und $f(X_1, X_2) = f_{11}$ sind also übereinstimmend falsch. Somit ist:

$$f(X_1, X_2) = f_{11} \equiv \neg(\neg X_1 \wedge X_2) \equiv X_1 \vee \neg X_2.$$

Die letzte Umformung geschieht nach den *Regeln von De Morgan*, die wir später beweisen werden. Wir halten fest:

Korollar 4.1 (Eindeutigkeit der Darstellung mit gebräuchlichen Junktoren) *Die Darstellung eines Ausdrucks mit Hilfe der Junktoren $\neg$, $\wedge$ sowie $\vee$ ist nicht eindeutig.*

Daher können wir die folgende Methode zur Konstruktion einer Ersatzform mit nur den Junktoren $\neg$, $\wedge$ sowie $\vee$ benützen:

Methode 4.1 (Konstruktion einer Ersatzform) *: Wir nehmen all jene Zeilen, in denen die anvisierte Aussageform den Wahrheitswert* 1 *hat und erstellen eine* $\wedge$*–Verknüpfung für jede Zeile. Für die Aussagenvariablen* X_i*, bei denen vorne der Wahrheitswert* 1 *steht, schreiben wir* X_i*, für die andern* $\neg X_i$*. Die so erhaltenen Ausdrücke für die Zeilen verknüpfen wir mit* $\vee$*.*

Nochmals ein Beispiel: Gegeben sei $g(X_1, X_2, X_3)$ durch die folgende Tabelle. Konstruiere eine Ersatzform mit $\neg$ $\wedge$ und $\vee$!

Tabelle 10.12: Ersatzform für $g(X_1, X_2, X_3)$

X_1	X_2	X_3	$g(X_1, X_2, X_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Nach der oben angegebenen Methode lesen wir ab:

$$g(X_1, X_2, X_3) \equiv \underbrace{(\neg X_1 \wedge \neg X_2 \wedge \neg X_3)}_{\text{Aus der 1. Zeile}} \vee \underbrace{(\neg X_1 \wedge X_2 \wedge X_3)}_{\text{Aus der 2. Zeile}} \vee (X_1 \wedge \neg X_2 \wedge X_3) \vee (X_1 \wedge X_2 \wedge X_3).$$

4.9 Verknüpfungsbasen

In 10.8.4 haben wir gesehen, dass wir eine beliebige Aussageform darstellen können ohne andere Junktoren als $\neg$, $\wedge$ sowie $\vee$ zu gebrauchen. Eine solche Menge von Junktoren (wie oben $\{\neg, \wedge, \vee\}$) nennen wir *Verknüpfungsbasis*. Allgemein definieren wir:

Definition 4.11 (Verknüpfungsbasis) *: Eine Menge von Junktoren, die ausreicht, um jede Wahrheitsfunktion als Aussageform darzustellen, heisst* **Verknüpfungsbasis**.

Aus 10.8.3 wissen wir, dass gilt:

1. $X_1 \vee X_2 \equiv \neg(\neg X_1 \wedge \neg X_2)$,
2. $X_1 \wedge X_2 \equiv \neg(\neg X_1 \vee \neg X_2)$.

Daher dürfen wir $\vee$ ersetzen durch $\neg$, $\wedge$ und Klammern. Ebenso dürfen wir den Junktor $\wedge$ austauschen durch die Junktoren $\neg$, $\vee$ sowie Klammern. Also sind $\{\neg, \wedge\}$ sowie $\{\neg, \vee\}$ Verknüpfungsbasen. Man kann mittels Wahrheitstabellen nachprüfen, dass folgender Satz gilt:

Satz 4.6 (Subjunktionsersatz) *: Es gilt:*

$$X_1 \Rightarrow X_2 \equiv \neg(X_1 \wedge \neg X_2) \equiv \neg X_1 \vee X_2.$$

Wegen der doppelten Verneinung kann man somit immer $\{\neg, \wedge\}$ und $\{\neg, \vee\}$ ersetzen durch $\{\neg, \Rightarrow\}$. D.h. es gilt der Satz:

Satz 4.7 (Verknüpfungsbasen) *:* $\{\neg, \wedge\}$*,* $\{\neg, \vee\}$ *und* $\{\neg, \Rightarrow\}$ *sind Verknüpfungsbasen.*

Es mag erstaunen, dass so wenige Junktoren genügen, um alle Aussageformen darzustellen. Doch man kann die Sache noch weitertreiben. Wir definieren:

Definition 4.12 (Elementare Verknüpfungsbasis) *: Ein Junktor bildet eine* **elementare Verknüpfungsbasis***, falls man durch ihn alleine mit Hilfe von Klammern alle Aussageformen mit endlich vielen Aussagenvariablen darstellen kann.*

Interessanterweise gilt der Satz:

Satz 4.8 (Darstellbarkeit durch elementare Verknüpfungsbasen) *: $\{\uparrow\}$ und $\{\downarrow\}$ (der Scheffer–Strich und der Nicodsche Junktor) sind die einzigen elementaren Verknüpfungsbasen.*

Zum Beweis: Dass $\{\uparrow\}$ und $\{\downarrow\}$ elementare Verknüpfungsbasen sind, geht aus folgendem Hilfssatz hervor, den man leicht durch Nachprüfung über die Wahrheitstafeln beweist:

Lemma 4.2 (Darstellbarkeit durch $\{\uparrow\}$ und $\{\downarrow\}$) *:*

$$\begin{array}{rcl@{\qquad}rcl} \neg A & \equiv & A \uparrow A & \neg A & \equiv & A \downarrow A \\ A \vee B & \equiv & A \uparrow A \uparrow (B \uparrow B) & A \wedge B & \equiv & A \downarrow A \downarrow (B \downarrow B) \end{array}$$

Die andere Aussage, nämlich die, dass es keine weiteren elementare Verknüpfungsbasen gibt, kann man nachprüfen, indem man zeigt, dass $\{\uparrow\}$ und $\{\downarrow\}$ durch keinen einzigen dritten Junktor alleine dargestellt werden können. Das zu zeigen ist eine längere Sache.

4.10 Tautologien, Kontradiktionen, Äquivalenzen, Implikationen

In diesem Unterkapitel wollen wir einige *spezielle Aussageformen* studieren. Wir beginnen mit der *Tautologie.*

4.10.1 Tautologien

Wir definieren:

Definition 4.13 (Tautologie) *: Eine Aussageform, die bei jeder Belegung wahr ist, heisst* **Tautologie** *(auch identisch wahre oder allgemeingültige Aussageform).*

Beispiele:

Tabelle 10.13: Folgende Aussageformen sind Tautologien:

1.1	$A \Rightarrow A$	1.2	$A \Rightarrow \neg\neg A$
2.1	$A \vee \neg A$	2.2	$\neg(A \wedge \neg A)$
3.1	$A \vee B \Leftrightarrow B \vee A$	3.2	$A \wedge B \Leftrightarrow B \wedge A$
4.1	$\neg(A \vee B) \Leftrightarrow \neg B \wedge \neg A$	4.2	$\neg(A \wedge B) \Leftrightarrow \neg B \vee \neg A$
5.1	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	5.2	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
6.1	$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$	6.2	$A \Leftrightarrow \neg(\neg A)$

Die Nachprüfung geschieht mittels Wahrheitstabelle. Z.B. für 1.1 wie folgt:

A	A	$A \Rightarrow A$
0	0	1
1	1	1

q. e. d.

Definition 4.14 (Kontradiktion) *: Eine Aussageform, die bei jeder Belegung falsch ist, heisst* **Kontradiktion** *(auch identisch falsche Aussage oder Widerspruch).*

Beispiele: Folgende Aussageformen sind Kontradiktionen:

$$A \wedge \neg A \text{ sowie } (A \vee B) \wedge \neg A \wedge \neg B \text{ etc. .}$$

Nachprüfung für das erste Beilspiel:

A	A	$A \Rightarrow A$	$\neg(A \Rightarrow A)$	
0	0	1	0	
1	1	1	0	*q. e. d.*

Eine Tautologie ist immer wahr, eine Kontradiktion ist (ebenso wie „¬ eine Tautologie“) immer falsch. Daher gilt trivialerweise der Satz:

Satz 4.9 (Beziehung zwischen Tautologie und Kontradiktion) *: $P(X_1, X_2, \ldots)$ ist Tautologie genau dann wenn $\neg P(X_1, X_2, \ldots)$ Kontradiktion ist.*

Bei einer Tautologie $P(X_1, X_2, \ldots)$ spielt die Belegung keine Rolle. Man kann irgendwelche Wahrheitswerte für die X_i einsetzen, die Aussageform bleibt wahr. Ersetzt man dann die Aussagenvariablen X_i durch neue Aussageformen $P_i(X_1, X_2, \ldots)$ und belegt diese mit Wahrheitswerten, so hat man als Resultate der Belegungen der neuen Aussageformen P_i einfach eine andere Belegung der ursprünglichen Aussageform P, die ja eine Tautologie ist. Das ändert aber nichts an der Tautologie, denn diese ist ja immer wahr. Man kann daher den folgenden Satz notieren:

Satz 4.10 (Ersetzung der Aussagenvariablen in einer Tautologie) *:*

Voraussetzung: Sei $P(X_1, X_2, \ldots)$ eine Tautologie sowie P_1, P_2, P_3 beliebige Aussageformen $(P_i \equiv P_i(X_1, X_2, \ldots)$.
Behauptung: $P(P_1, P_2, \ldots)$ ist wieder eine Tautologie.

Beispiel: $(A \vee B) \Leftrightarrow (B \vee A)$ ist Tautologie. Somit ist
$((\underbrace{\neg A \wedge B}) \vee B) \Leftrightarrow (B \vee (\underbrace{\neg A \wedge B}))$ auch Tautologie.

Hier ist A ersetzt worden durch $(\underbrace{\neg A \wedge B})$. Der neue Ausdruck bleibt eine Tautologie.

4.10.2 Äquivalenzen

Definition 4.15 (Äquivalenz) *: Zwei Aussageformen $P(X_1, \ldots, X_n)$ und $Q(X_1, \ldots, X_n)$ heissen* **äquivalent***, falls $P(X_1, \ldots, X_n) \Leftrightarrow Q(X_1, \ldots, X_n)$ eine Tautologie ist.*

Sind $P(X_1, \ldots, X_n)$ und $Q(X_1, \ldots, X_n)$ äquivalent, so schreiben wir $P(X_1, \ldots, X_n) \equiv Q(X_1, \ldots, X_n)$. $P(X_1, \ldots, X_n) \equiv Q(X_1, \ldots, X_n)$ bedeutet also, dass $P(X_1, \ldots, X_n) \Leftrightarrow Q(X_1, \ldots, X_n)$ immer wahr ist. Das heisst, dass $P(X_1, \ldots, X_n)$ genau dann wahr (oder falsch) ist, wenn $Q(X_1, \ldots, X_n)$ wahr (oder falsch) ist.

4.10.3 Implikation

Definition 4.16 (Implikation) *: Die Aussageformen $P(X_1, \ldots, X_n)$* **impliziert** *die Aussageform $Q(X_1, \ldots, X_n)$, falls $P(X_1, \ldots, X_n) \Rightarrow Q(X_1, \ldots, X_n)$ eine Tautologie ist.*

Beispiele: 1) $A \Rightarrow A$ 3) $A \wedge B \Rightarrow A$
2) $A \Rightarrow A \vee B$ 3) $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

In einer Implikation $P \Rightarrow Q$ lassen sich die Aussageformen A und B nicht beliebig mit ¬ versehen und vertauschen. Trotzdem haben aber solche Verwandlungen in der Praxis eine Bedeutung. Man hat daher zur Vereinfachung des Sprachgebrauchs folgende Namen eingeführt:

Definition 4.17 (Konversion, Inversion, Kontraposition) *: Gegeben sei $P \Rightarrow Q$. Der Ausdruck $Q \Rightarrow P$ heisst* **Konversion** *von $P \Rightarrow Q$. Der Ausdruck $\neg P \Rightarrow \neg Q$ heisst* **Inversion** *von $P \Rightarrow Q$. $\neg Q \Rightarrow \neg P$ heisst* **Kontraposition** *oder auch* **Transposition** *von $P \Rightarrow Q$.*

Es gilt der wichtige Satz, der in der mathematischen Beweistechnik häufig Verwendung findet:

Satz 4.11 (Indirekter Beweis) *:*

$$\neg Q \Rightarrow \neg P \qquad \equiv \qquad P \Rightarrow Q$$

Diese Äquivalenz kann man rasch mit Hilfe einer Wahrheitstabelle verifizieren. (Dies zu tun ist eine gute Übung ....) Wichtig für die mathematischen Beweistechnik ist nun, dass man statt $P \Rightarrow Q$ zu beweisen, genauso gut $\neg Q \Rightarrow \neg P$ verifizieren kann. Das kann Vereinfachungen bringen.

4.10.4 Wichtige Äquivalenzen

Die folgenden Gesetze spielen bei logischen Umformungen und beim Beweisen eine wichtige Rolle. Man verifiziert sie am einfachsten mit Hilfe von Wahrheitstabellen. *Hinweis: Man mache das zur Übung selbst...*

(1)	Gesetz der doppelten Negation	$\neg\neg A$	$\equiv$	A
(2)	Idempotenz	$A \vee A$	$\equiv$	A
		$A \wedge A$	$\equiv$	A
(3)	Assoziativität	$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$
		$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$
(4)	Kommutativität	$A \vee B$	$\equiv$	$B \vee A$
		$A \wedge B$	$\equiv$	$B \wedge A$
(5)	Distributivität	$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$
		$A \wedge (B \vee C)$	$\equiv$	$A \wedge B) \vee (A \wedge C)$
(6)	Neutrales Element	$A \vee F$	$\equiv$	A
		$A \wedge W$	$\equiv$	A
(7)	Erzwungene Adjunktion	$A \vee W$	$\equiv$	W
	Erzwungene Konjunktion	$A \wedge F$	$\equiv$	F
(8)	Komplementarität:			
	Ausgeschlossenes Drittes	$A \vee \neg A$	$\equiv$	W
	Gesetz vom Widerspruch	$A \wedge \neg A$	$\equiv$	F
(9)	Dualität	$\neg W$	$\equiv$	F
		$\neg F$	$\equiv$	W
(10)	De Morgan	$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$
		$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$
(11)	Absorptionsgesetze	$A \vee (A \wedge B)$	$\equiv$	A
		$A \wedge (A \vee B)$	$\equiv$	A
		$(A \wedge B) \vee \neg B$	$\equiv$	$A \vee \neg B$
		$(A \vee B) \wedge \neg B$	$\equiv$	$A \wedge \neg B$
(12)	Kontraposition	$A \Rightarrow B$	$\equiv$	$\neg B \Rightarrow \neg A$
(13)	Dualisierung der Kontraposition	$A \Leftrightarrow W$	$\equiv$	$\neg A \Leftrightarrow F$
(14)	Subjunktionsersatz	$A \Rightarrow B$	$\equiv$	$\neg A \vee B$
		$A \Rightarrow B$	$\equiv$	$\neg(A \wedge \neg B)$
(15)	Bijunktionsersatz	$A \Leftrightarrow B$	$\equiv$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
(16)	Ex falso quodlibet	$F \Rightarrow A$	$\equiv$	W
(17)	Ex quodlibet verum	$A \Rightarrow \mathrm{W}$	$\equiv$	W
(18)	Abschwächung der Konjunktion	$(A \wedge B) \Rightarrow A$	$\equiv$	W
(19)	Abschwächung der Adjunktion	$A \Rightarrow (A \vee B)$	$\equiv$	W
(20)	Gesetz vom negiertem Vorderglied	$\neg A \Rightarrow (A \Rightarrow B)$	$\equiv$	W
(21)	Gesetz vom Hinterglied	$B \Rightarrow (A \Rightarrow B)$	$\equiv$	W
(22)	Konjunktion impliziert Disjunktion	$(A \vee B) \Rightarrow (A \vee B)$	$\equiv$	W
(23)	Modus ponens	$(A \wedge (A \Rightarrow B)) \Rightarrow B)$	$\equiv$	W
(24)	Modus tollens	$(\neg B \wedge (A \Rightarrow B)) \Rightarrow \neg A)$	$\equiv$	W
(25)	Transitivitätsgesetz	$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$	$\equiv$	W
(26)	Gesetz der Fallunterscheidung	$((A \vee B) \wedge ((A \Rightarrow C)) \wedge (B \Rightarrow C)) \Rightarrow C$	$\equiv$	W

4.11 Logisches Schliessen

Hier wollen wir durch einen kurzen Exkurs etwas Einblick ins *logische Schliessen* oder *logische Beweisen* gewinnen.
Seien $P_1, P_2, \ldots, P_n$ und Q Aussageformen. Häufig tritt nun folgendes Problem auf:

Problem 4.5 (Logischer Schluss) *: Es gilt festzustellen, ob sich Q aus $P_1, P_2, \ldots, P_n$ herleiten lässt. Symbolisch schreiben wir: $P_1, P_2, \ldots, P_n \vdash Q$.*

Um das Problem besser behandeln zu können, führen wir die folgende Sprechweise ein:

Begriffserklärung 7 (Prämissen, Konklusion) *: Im eben erwähnten Problem heissen $P_1, P_2, \ldots, P_n$ die* **Prämissen** *(Voraussetzungen), Q heisst die* **Konklusion** *(Folgerung) und $P_1, P_2, \ldots, P_n \vdash Q$ heisst* **logischer Schluss**.

Eine logische Folgerung oder ein logischer Schluss kann in der zweiwertigen Logik wiederum wahr oder falsch sein. Falsche Schlüsse sind ein Ärgernis, das es zu vermeiden gilt. Uns interessieren vor allem die wahren Schlüsse. daher definieren wir:

Definition 4.18 (Korrekter logischer Schluss) *: $P_1, P_2, \ldots, P_n \vdash Q$ heisst* **korrekter logischer Schluss**, *falls $(P_1 \wedge P_2 \wedge \ldots \wedge P_n \Rightarrow Q)$ eine Tautologie ist.*

In einem korrekten logische Schluss impliziert also die Konjunktion der Prämissen die Konklusion.

Beispiel: Wir wollen zeigen, dass $A, A \Rightarrow B \vdash B$ gilt, d.h. $A, A \Rightarrow B \vdash B$ ist ein korrekter logischer Schluss. Wir müssen also zeigen, dass $(A \wedge A \Rightarrow B) \Rightarrow B$ eine Tautologie ist. Wir machen das anhand einer Tabelle:

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	$(A \wedge A \Rightarrow B) \Rightarrow B$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

$(A \wedge A \Rightarrow B) \Rightarrow B$ ist also in jedem möglichen Fall wahr. Der untersuchte Ausdruck ist demnach eine Tautologie. Vielleicht haben Sie es gemerkt — es ist der modus ponens.
Die Bedeutung des modus ponens (Abtrennungsregel) liegt in folgender Konsequenz: Man kann, um eine Aussage B als wahr zu erweisen, auch eine beliebige andere Aussage A sowie die Subjunktion $A \Rightarrow B$ als wahr erweisen. Solchen Situationen begegnet man in „mathematischen Sätzen“. Denn ein solcher Satz hat meistens folgende abstrakte Struktur:

Satz:	**Voraussetzung:**	Aussage $a_1 \wedge a_2 \wedge \ldots \wedge a_n$	Kürzer:	**Satz:**	**Vor:**	$a_1 \wedge a_2 \wedge \ldots \wedge a_n$
	Behauptung:	Aussage b			**Beh.:**	b

Man behauptet also, dass — falls die Voraussetzung wahr ist, die Behauptung auch wahr ist (d.h. nie falsch sein kann). Falls die Voraussetzung aber falsch ist, interessiert sich für die Behauptung niemand ernsthaft. D.h. sie kann wahr oder falsch sein, es macht unter einer falschen, also nie eintreffenden Voraussetzung nichts aus. Daher muss man zum Beweis des Satzes die Subjunktion $a \Rightarrow b$ als wahr erweisen. Diese Subjunktion erscheint hier nicht in der Bedeutung einer Aussageform, sondern ist für den Leser des mathematischen Satzes eine Aussage. Man muss daher bei einem Beweis nur den Fall „$a_1 \wedge a_2 \wedge \ldots \wedge a_n$ wahr und b wahr“ als wahr erweisen. Es gilt also hier, korrekt logisch von $a_1 \wedge a_2 \wedge \ldots \wedge a_n$ auf b zu schliessen.
Wir machen uns diesen Sachverhalt an folgendem Beispiel klar:

Satz 4.12 (Paradigma aus der Geometrie) [4]*:*
Vor.: *Für die Geraden g_i gilt: $g_1 \| g_2$ (Aussage a_1) und $g_1 \perp g_3$ (Aussage a_2).*
Beh.: *Es gilt dann auch $g_2 \perp g_3$ (Aussage b).*

Weitere logische Schlüsse:	(1)	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$\vdash$	$(A \Rightarrow C)$
	(2)	$(A \Rightarrow \neg B) \wedge B$	$\vdash$	$\neg A$
Trugschlüsse:	(1)	$(A \Rightarrow B) \wedge B$	$\vdash$	A
	(2)	$(A \Rightarrow B) \wedge \neg A$	$\vdash$	$\neg B$

[4] Ein Paradigma ist ein Lehrbeispiel

Trugschlüsse haben ihren Grund oft darin, dass man sich von der „ungenauen und oberflächlichen Umgangssprache“ leiten lässt. Achtung: Trugschlüsse führen zu Irrtümern!
Hinweis: Die Nachprüfung, wann obige Trugschlüsse falsch sind, ist eine gute Übung.

4.12 Die polnische Notation

4.12.1 Herkunft und Sinn

Anfänglich im Zusammenhang mit theoretischen Untersuchungen ist die Frage aktuell geworden, ob es nicht eine eindimensionale Schreib- und Lesemöglichkeit gibt, in der man *ohne Klammern auskommt*. Mit Hilfe einer solchen eindimensionalen Schreib- und Lesemöglichkeit sollen sich Aussageformen z.B. auch von einer Maschine schreiben oder lesen lassen können. Eine solche Maschine schreibt oder liest immer nur ein Zeichen. Dann geht sie in immer gleicher Richtung zum nächsten Zeichen über, hat jedoch keine Möglichkeit, den Schreib- oder Lesekopf wieder zurückzubewegen. Eine solche Maschine soll sich nicht noch zusätzlich eine Stelle merken müssen, an der eine Klammer aufgegangen ist, die es dann später wieder zu schliessen gilt. Dieses Prinzip ist natürlich im Zusammenhang mit dem Bau von Computern heute wichtig. Ein Beispiel einer solchen abstrakten Maschine ist die *Turingmaschine*, benannt nach dem Engländer Turing (erste Hälfte des 20. Jahrhunderts). Der Pole J. Lukasiewicz hat eine solche Schreibweise vorgeschlagen, die auch funktioniert: Die *polnische Notation*. Damit werden Klammern überflüssig. Es zeigt sich aber rasch, dass Klammern für den Menschen vor allem zum Lesen unentbehrlich sind, denn sonst kann es äusserst mühsam werden, die Übersicht rasch zu gewinnen. Der Mensch hat ein dreidimensionales Sehvermögen. Er funktioniert nicht eindimensional wie eine der eben beschriebenen Maschinen. Allerdings wenden heute noch gewisse Hersteller (vor allem von Taschenrechnern) das Prinzip der polnischen klammerlosen Schreibweise unter diversen Umständen in abgewandelter Form an. (Bekannt ist z.B. die *umgekehrte polnische Notation* bei HP.)

4.12.2 Regeln zur polnischen Notation

Nachstehend ist die Sache am Beispiel der häufigsten Junktoren erläutert. Das damit erklärte Prinzip lässt sich mühelos auf die andern Junktoren übertragen.
Beispiele:

$$\begin{array}{rcl} \neg A & \equiv & \neg A \\ A \wedge B & \equiv & \wedge AB \\ A \vee B & \equiv & \vee AB \\ A \Rightarrow B & \equiv & \Rightarrow AB \\ A \Leftrightarrow B & \equiv & \Leftrightarrow AB \end{array}$$

Man erkennt daraus folgende Vorgehensweise:

Methode 4.2 (Polnische Notation) *: Ein Junktor, der bei normaler Notation zwischen zwei Aussagen oder Aussageformen steht, wird bei der Polnischen Notation voran geschrieben.*

Beispiele:

$$\begin{array}{rcl} ((\neg A) \wedge (B \vee A)) & \equiv & \wedge\neg A \vee BA \\ A \Rightarrow ((\neg B) \Leftrightarrow (A \vee C)) & \equiv & \Rightarrow A \Leftrightarrow \neg B \vee AC \\ (A \vee B) \Rightarrow ((\neg C) \vee ((\neg B) \wedge C)) & \equiv & \Rightarrow \vee AB \vee \neg C \wedge \neg BC \end{array}$$

Da das Prinzip des Voranstellens des Junktors nicht vom Junktor abhängt, gilt es auch für den Scheffer-Strich und auch für die Nicodsche Verknüpfung. Diese beiden Junktoren bilden aber die einzigen *elementaren Verknüpfungsbasen,* d.h. jede Aussageform lässt sich alleine mit ihnen schrieben. Mit Hilfe der polnischen Notation ist es möglich, die Klammern zu vermeiden. Daher können wir folgern:

Satz 4.13 (Elementarste Darstellung einer Aussageform resp. einer Aussage) *: Jede Aussageform resp. jede Aussage lässt sich alleine mit $\uparrow$ und Aussagenvariablen resp. elementaren Aussagen schreiben. Ebenso lässt sich jede Aussageform resp. jede Aussage alleine mit $\downarrow$ und Aussagenvariablen resp. elementaren Aussagen schreiben.*

Als Konsequenz ergibt sich daher, dass neben den Aussagenvariablen und Elementaraussagen nur ein einziger Junktor nötig ist, um jeden Ausdruck der Aussagenlogik schreiben zu können.

4.13 Logikzeitung

Die Logikzeitung

Reklameteil: Ja–Parole für mehr Logik im Magen!

Partei für Inweltschutz Wetterbericht: Erst Sturm u. Drang, dann Föhn im Badezimmer

---

Letzte Nachrichten auf der folgenden Seite!

Die Logikzeitung

Das Paradoxon der unerwarteten Hinrichtung

(Gekürzt nach einer Erzählung von Martin Gartener)

Inserat: Zu empfehlen:
M. Gartener, Logik unterm Galgen

Gartener schreibt unter anderem: "Das Urteil wurde an einem Samstag gesprochen. 'Die Hinrichtung wird mittags an einem der sieben Tage der nächsten Woche stattfinden', sagte der Richter zu dem Gefangenen. 'Aber Sie werden nicht wissen, an welchem Tage, bis Sie am Morgen des Hinrichtungstages Bescheid bekommen.'

Der Richter war als Mann bekannt, der immer sein Wort hielt. Der Verurteilte ging, vom Anwalt begleitet, in seine Zelle zurück. Als die beiden allein waren, lächelte der Anwalt und meinte:' Merken Sie nichts? Das Urteil des Richters kann unmöglich vollstreckt werden.'

'Das verstehe ich nicht', sagte der Gefangene.

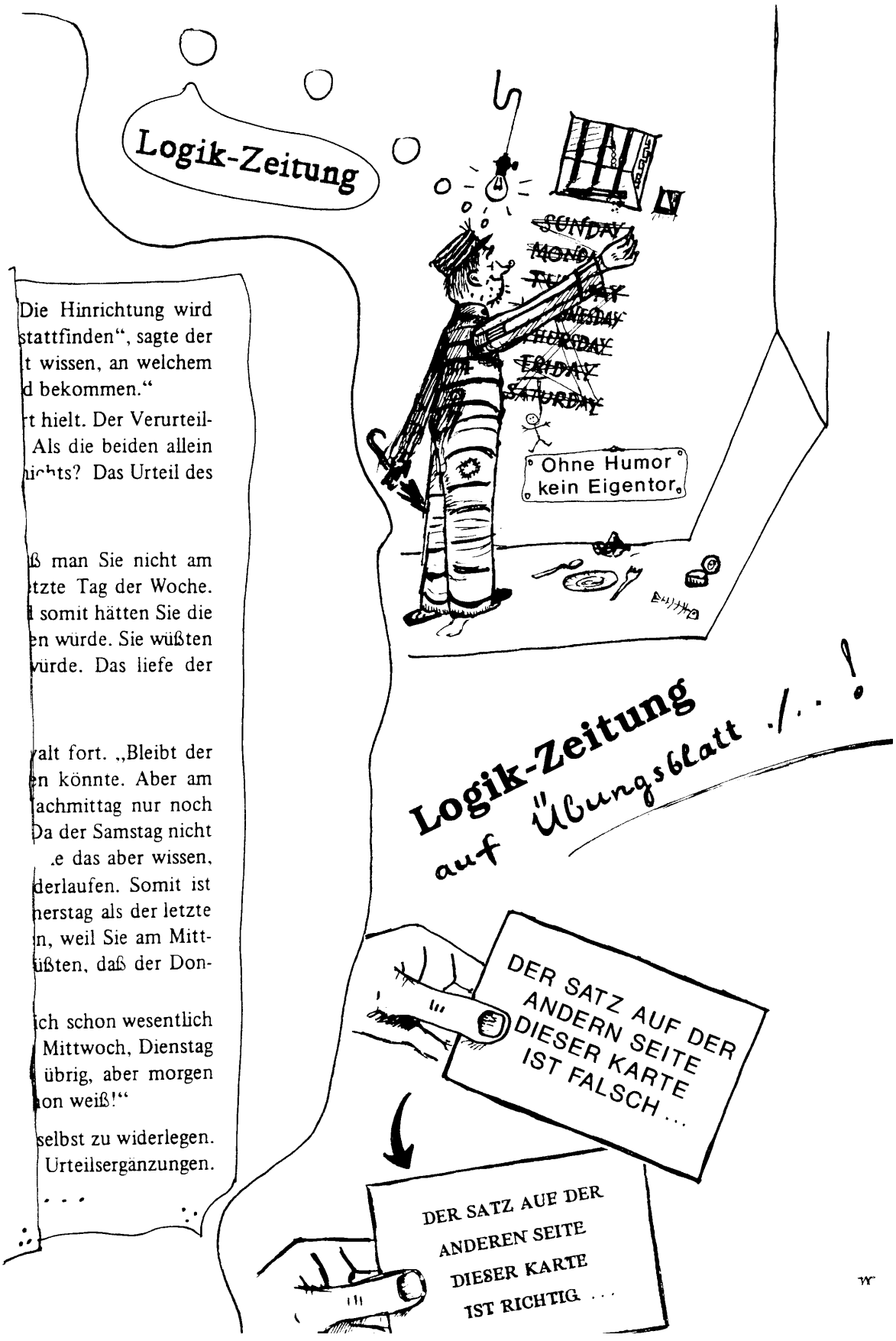
'Ich erkläre es Ihnen. Es ist ganz offensichtlich, dass man Sie nicht am nächsten Samstag hinrichten kann. Samstag ist der letzte Tag der Woche. Am Freitag nachmittag wären Sie noch am Leben und somit hätten Sie die absolute Gewissheit, dass man Sie am Samstag hinrichten würde. Sie wüßten es, bevor es ihnen am Samstag morgen mitgeteilt würde. Das liefe der Anordnung des Richters zuwider.'
'Stimmt', sagte der Gefangene.

'Samstag ist damit also ausgeschlossen', fuhr der Anwalt fort. 'Bleibt der Freitag als letzter Tag, an dem man Sie hinrichten könnte. Aber am Freitag ist dies nicht möglich, weil am Donnerstag nachmittag nur noch zwei Tage übrigbleiben, nämlich Freitag und Samstag. Da der Samstag nicht in Frage kommt, müsste es am Freitag geschehen. Da Sie das aber wissen, würde es ebenfalls der Anordnung des Richters zuwiderlaufen. Somit ist auch der Freitag ausgeschlossen. Damit bleibt der Donnerstag als der letzte mögliche Tag. Aber Donnerstag ist auch ausgeschlossen, weil Sie am Mittwoch nachmittag noch am Leben wären und damit wüssten, dass der Donnerstag der Tag der Hinrichtung sein müsste.'

'Jetzt verstehe ich', sagte der Verurteilte und fühlte sich schon wesentlich wohler. 'Auf diese Art und Weise kann ich auch Mittwoch, Dienstag und Montag streichen. Dann bleibt nur noch morgen übrig, aber morgen kann ich nicht hingerichtet werden, weil ich es heute schon weiss!'

Kurz und gut, die Anordnung des Richters scheint sich selbst zu widerlegen. Es gibt keinen logischen Widerspruch in den beiden Urteilsergänzungen. Trotzdem kann offenbar das Urteil nicht ausgeführt werden - oder doch? Um dies zu klären, kehren wir zu dem Verurteilten in die Zelle zurück. Er ist durch die scheinbar unanfechtbare Logik überzeugt, dass er nicht hingerichtet werden kann, ohne dass dadurch die Bedingungen des Urteilsspruchs verletzt würden. Zu seiner grössten überraschung kam jedoch am Donnerstag morgen der Henker. Es ist klar, dass er ihn nicht erwartet hatte. Was noch mehr überrascht: Nun ist der Urteilsspruch des Richters völlig korrekt. Das Urteil kann vollstreckt werden, genau wie es der Richter verkündet hatte." Lässt dieser Beigeschmack der Logik, die von der Welt negiert wird, das Paradoxon nicht recht faszinierend erscheinen?

Aufruf an alle intelligenten Studenten!
Dipl. Ing. ABC kann seit der Lektüre des Paradoxons von der unerwarteten Hinrichtung seinen Verstand nicht mehr finden. Er soll sich hinter der Lösung versteckt haben. Wo ist sie? Erbete Mitteilung an Red.. Die Red.


Logik-Zeitung
Die Hinrichtung wird
stattfinden", sagte der
t wissen, an welchem
d bekommen."
t hielt. Der Verurteil-
Als die beiden allein
ichts? Das Urteil des
ß man Sie nicht am
tzte Tag der Woche.
somit hätten Sie die
n würde. Sie wüßten
ürde. Das liefe der
alt fort. „Bleibt der
n könnte. Aber am
achmittag nur noch
Da der Samstag nicht
.e das aber wissen,
derlaufen. Somit ist
herstag als der letzte
n, weil Sie am Mitt-
ßten, daß der Don-
ich schon wesentlich
Mittwoch, Dienstag
übrig, aber morgen
on weiß!"
selbst zu widerlegen.
Urteilsergänzungen.
SUNDAY
MONDAY
TUESDAY
WEDNESDAY
THURSDAY
FRIDAY
SATURDAY
Ohne Humor
kein Eigentor
Logik-Zeitung
auf Übungsblatt ./. . !
DER SATZ AUF DER
ANDERN SEITE
DIESER KARTE
IST FALSCH . . .
DER SATZ AUF DER
ANDEREN SEITE
DIESER KARTE
IST RICHTIG . . .

Kapitel • Chapitre 5

Aussagenlogische Normalformen

5.1 Gegenstand, praktische Anwendung

Im letzten Kapitel haben wir folgendes Problem studiert: Gegeben war eine Aussageform. Gesucht waren dann alle möglichen Belegungen für diese Aussageform. Man musste also die Wahrheitstabelle finden. Dabei haben wir gesehen, dass äusserlich verschieden erscheinende Aussageformen dieselbe Wahrheitstabelle haben können.
In der Praxis hat man aber häufig das umgekehrte Problem: Gegeben ist eine Wahrheitstabelle. Dazu soll man eine Aussageform finden, die zur gegebenen Wahrheitstabelle gehört. *Aussagenlogische Normalformen* sind spezielle zusammengesetzte Aussagenformen, mit denen man die Lösung eines sochen Problems sehr rasch finden kann. Das ist in der Praxis wichtig.
Normalformen sind manchmal auch anderswo hilfreich: Um zwei Aussageformen zu vergleichen, kann man die Wahrheitstafel heranziehen. Es gibt aber noch einen andern Weg. Man sucht zu beiden gegebenen Aussageformen je einen ganz gewissen Typ einer standardisierten Normalform, die *kanonische Normalform* (auch *vollständige* Normalform). Stimmen die beiden kanonischen Normalformen bis auf die Reihenfolge der Terme überein, so sind die beiden gegebenen Aussageformen äquivalent.
Man unterscheidet zwei verschiedene Typen von aussagenlogischen Normalformen:

1. *Konjuktive Normalformen*
2. *Alternative Normalformen*

Statt *alternative Normalform* sind auch die Ausdrücke *alternierende Normalform, disjunktive Normalform* oder *adjunktive Normalform* gebräuchlich.

5.2 Definitionen

Da die Logik als eigenständige Disziplin eine noch relativ junge Wissenschaft ist, hat sich in der mathematischen Literatur bezüglich Logik noch kein einheitlicher Sprachgebrauch durchgesetzt. Das nachstehende Konzept folgt der bei Asser (Bibl.: asser) eingeschlagenen Richtung.

Seien H_1, H_2, …, H_n, …, H_{n+m} paarweise verschiedene Aussagenvariablen. ($n \geq 0$, $m \geq 0$, $m+n \geq 1$.)
Damit bauen wir die Definition von *Normalformen* wie folgt auf:

Definition 5.1 (Einfache Terme, Konjunktions- und Adjunktionsterme) *:*

1. *Ein* **einfacher Term** *ist eine Aussagenvariable oder die Negation einer Aussagenvariablen (Negationsterm).*

2. *Ein* **Konjunktionsterm** *ist eine Konjuktion von einfachen Termen.*
   Konjuktionsterm $:= H_1 \wedge H_2 \wedge \ldots \wedge H_n \wedge \neg H_{n+1} \wedge \ldots \wedge \neg H_{n+m} = \bigwedge_{i=1}^{n} H_i \wedge \bigwedge_{j=n+1}^{n+m} \neg H_j$.

3. *Ein* **Adjunktionsterm** *ist eine Adjunktion von einfachen Termen.*
   Adjunktionsterm $:= H_1 \vee H_2 \vee \ldots \vee H_n \vee H_{n+1} \vee \ldots \vee \neg H_{n+m} = \bigvee_{i=1}^{n} H_i \vee \bigvee_{j=n+1}^{n+m} \neg H_j$.

4. *Wir verabreden noch, dass ein Konjunktionsterm zu einem „Konjunktionsterm mit nur einem einzigen Glied" entartet sein darf. Dasselbe gilt für den Adjunktionsterm.*

Definition 5.2 (Enthaltensein von Konjunktions- und Adjunktionstermen) *:*

1. *T_0, T_1, T_2 seien Konjunktionsterme. „T_1 ist in T_2* **enthalten***" bedeutet: Es gibt (symbolisch $\exists$) einen Term T_0 mit $T_1 \wedge T_0 \equiv T_2$.*

2. *R_0, R_1, R_2 seien jetzt Alternativterme. „R_1 ist in R_2* **enthalten***" bedeutet: $\exists_{R_0}$ mit $R_1 \wedge R_0 \equiv R_2$.*

Definition 5.3 (Konjunktive und alternative Normalform) *:*

1. *Seien $A_1, \ldots, A_k$ Alternativterme. Dann heisst*
   $K \equiv A_1 \wedge A_2 \wedge \ldots \wedge A_k \equiv \bigwedge_{i=1}^{k} A_i$ **konjunktive Normalform** *(kNF).*

2. *Seien $K_1, \ldots, K_k$ Konjunktionsterme. Dann heisst*
   $A \equiv K_1 \vee K_2 \vee \ldots \vee K_k \equiv \bigvee_{i=1}^{k} K_i$ **alternative Normalform** *(aNF).*

Bemerkungen:

1. Es gibt Autoren, die zusätzlich verlangen, dass bei einer kNF keiner der Alternativterme K_i in einem andern Alternativterm enthalten ist[5]. Ebenso für die Konjunktionsterme einer aNF[5]. Falls ein Alternativterm einer kNF in einem andern solchen Term enthalten ist, kann man den längern der beiden Terme weglassen. (Es gilt ja $(A_1 \vee A_2) \wedge A_1 \equiv A_1$). Ebenso bei einer aNF, wenn ein Konjunktionsterm in einem andern enthalten ist: Man kann dann den kürzern der beiden weglassen.

2. Wie schon bei den Adjunktions– und Konjunktionstermen verabreden wir auch hier, dass eine aNF zu einer „aNF mit nur einem einzigen Konjunktionsterm" entartet sein darf. Dasselbe gilt für die kNF. Daher ist ein einfacher Term insbesondere auch eine aNF sowie auch eine kNF.

Beispiele:

1. $A \wedge B$ ist enthalten in $A \wedge B \wedge \neg C$, aber nicht in $A \wedge \neg B$

2. A ist aNF wie auch kNF (entarteter Fall).

3. $A \wedge \neg B \wedge C$ ist kNF (bestehend aus drei einfachen Termen) oder auch aNF (bestehend aus einem einzigen Konjunktionsterm).

4. $(A \wedge \neg B \wedge C) \vee B$ ist aNF.

5. $(A \wedge B \wedge \neg C) \vee (\neg A \wedge C)$ ist aNF.

6. $X \vee (A \wedge B(\vee C(\wedge D)))$ ist keine Normalform.

7. $A \vee (B \wedge C) \wedge (\neg C \vee D)$ ist ebenfalls keine Normalform.

[5] Z.B. bei Mendelson (Bibl.: mendelson) wird das Enthaltensein verlangt, hingegen z.B. bei Asser (Bibl.: asser) nicht. Beide Wege sind möglich.

5.3 Das Existenzproblem

Es gilt der folgende Satz über die Existenz einer äquivalenten kNF resp. aNF:

Satz 5.1 (Existenzsatz) *: Zu jeder Aussageform existiert eine äquivalente kNF sowie eine aNF.*

Bemerkung zum Beweis:

1. $\{\neg, \vee, \wedge\}$ ist Verknüpfungsbasis. Daher kann man die andern Junktoren $(\Rightarrow, \Leftrightarrow, \ldots)$ dadurch zum Verschwinden bringen, dass man Terme mit $\Rightarrow, \Leftrightarrow, \ldots$ einer nach dem andern durch mögliche äquivalente Terme mit $\neg, \vee, \wedge$ ersetzt.
2. Man wendet die Regeln von De Morgan an: $\neg(A \wedge B) \equiv \neg A \vee \neg B, \neg(A \vee B) \equiv \neg A \wedge \neg B$. Damit kann man Klammern wegschaffen und den Junktor $\neg$ vor die Variablen bringen.
3. Weiter kann man Klammern mit Hilfe des Distributivgesetzes in die gewünschte Position „verschieben“ (z.B. mit $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$).

So gelingt es, unerwünschte Junktoren zu entfernen und $\neg, \vee, \wedge$ sowie die Klammern an den „richtigen Ort“ zu verschieben.

Beispiele:

1. Mit Hilfe der Wahrheitstafel verifiziert man sofort:

2. $$A \Leftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$$

$$\begin{aligned} X: \quad &\equiv (A \wedge \neg B) \Leftrightarrow (B \vee A) \\ &\equiv ((A \wedge \neg B) \wedge (B \vee A))) \vee (\neg(A \wedge \neg B) \wedge \neg(B \vee A)) \\ &\equiv ((A \wedge \neg B \wedge B) \vee (A \wedge \neg B \wedge A)) \vee ((\neg A \vee \neg\neg B) \wedge (\neg B \wedge \neg A)) \\ &\equiv f \vee (A \wedge \neg B) \vee (\lfloor(\neg A \vee B) \wedge \neg A\rfloor \wedge \neg B) \\ &\equiv (A \wedge \neg B) \vee (\lfloor(\neg A \wedge \neg A) \vee (B \wedge \neg A)\rfloor \wedge \neg B) \\ &\equiv (A \wedge \neg B) \vee (\neg A \vee (B \wedge \neg A) \wedge \neg B) \\ &\equiv (A \wedge \neg B) \vee (\neg A \wedge \neg B). \end{aligned}$$

Der letzte Ausdruck ist schon eine aNF. Darin lässt sich aber $\neg B$ ausklammern und man erhält:

$$X \equiv \neg B \vee (A \wedge \neg A) \equiv \neg B.$$

$\neg B$ ist eine aNF wie auch eine kNF.

5.4 Das Eindeutigkeitsproblem

Eben haben wir gesehen, dass die Aussageform $X :\equiv (A \wedge \neg B) \Leftrightarrow (B \vee A)$ äquivalent ist zu den beiden aNF $(A \wedge \neg B) \vee (\neg A \wedge \neg B)$ und $\neg B$. Die Darstellung einer Aussageform durch eine aNF ist also nicht eindeutig. Das gleiche gilt natürlich für die kNF. (Beispiel: $(A \vee \neg B) \wedge (\neg A \vee \neg B) \equiv \neg B \wedge (A \vee \neg A) \equiv \neg B$..)
Es ist nun naheliegend, eine spezielle kNF oder aNF zu suchen, die *bis auf die Reihenfolge der Terme* **eindeutig** ist. Das erreichen wir durch *Ergänzung der fehlenden Variablen* in den einzelnen Adjunktions– resp. Konjunktionstermen. Wir können so Aussageformen erzeugen, in denen in jedem Adjunktions– oder Konjunktionsterm jede Variable genau einmal vorkommt. Das geschieht so:
Es fehle z.B. im Term T_i die Variable X_k.

1. Sei zuerst T_i ein Konjunktionsterm einer aNF. Dann erweitern wir T_i wie folgt:

$$T_i \equiv T_i \wedge w \equiv T_i \wedge (X_k \vee \neg X_k) \equiv (T_i \wedge X_k) \vee (T_i \wedge \neg X_k) \equiv T_{i_1} \vee T_{i_2}$$

Der Term T_i der aNF ist damit ersetzt worden durch eine Adjunktion von zwei erweiterten Konjunktionstermen, in denen jeweils T_i, aber auch X_k resp. $\neg X_k$ vorkommen. Das Resultat ist wieder eine aNF.

2. Sei jetzt R_j ein Adjunktionsterm einer kNF. Dann erweitern wir R_j wie folgt:

$$R_j \equiv R_j \vee f \equiv R_j \vee (X_k \wedge \neg X_k) \equiv (R_j \vee X_k) \wedge (R_j \vee \neg X_k) \equiv R_{j_1} \vee R_{j_2}$$

Der Term R_j der kNF ist damit ersetzt worden durch eine Konjunktion von zwei erweiterten Adjunktionstermen, in denen jeweils R_j, aber auch X_k resp. $\neg X_k$ vorkommen. Das Resultat ist wieder eine kNF.

Da $A \wedge A \equiv A$ sowie $A \vee A \equiv A$ ist, können mehrfach vorkommende Terme gestrichen werden. Man kann also jede aNF resp. jede kNF in eine solche aNF resp. kNF verwandeln, in der jede anfangs vorkommende Variable in jedem Term genau einmal vorkommt und keine Terme mehrfach vorkommen. Da die Anzahl Variablen dann in jedem Term gleich gross ist, ist dann auch kein Term in einem andern enthalten. Wir definieren nun:

Definition 5.4 (Kanonische Normalform) *:*
Eine aNF resp. kNF, in der in jedem Term jede Variable genau einmal vorkommt, heisst **kanonische Normalform**.

Die entstehenden kanonischen Normalformen kann man nach den Kommutativgesetzen für $\wedge$ und $\vee$ sogar nach folgenden Prinzipien eindeutig ordenen:

1. Ordne alle Terme nach aufsteigenden Variablennummern.

2. Ersetze in den Adjunktions– resp. Konjunktionsermen T_i die einfachen Terme durch die Ziffern 0 oder 1 nach folgender Regel: Falls der einfache Term eine Variable X_i ist, so ersetze diese durch 0. Falls aber der einfache Term eine negierte Variable $\neg X_i$ ist, so ersetze diese durch 1. Wenn man im so entstandenen Ausdruck die Junktoren weglässt, so erhält man statt dem Term T_i eine Dualzahl. Jeder Term T_i entspricht dann genau einer Dualzahl. Jetzt kann man demnach die Terme entsprechend der aufsteigenden Grösse der Dualzahlen ordnen.

So erhält man *geordnete kanonische Normalformen*. Für diese gilt ersichtlicherweise der Satz:

Satz 5.2 (Eindeutigkeitssatz) *: Zu jeder Aussageform existiert genau eine äquivalente geordnete kanonische aNF sowie kNF.*

5.5 Das Darstellungsproblem

Für gegebene Aussageformen lassen sich die kanonischen Formen sehr einfach aus der Wahrheitstabelle *ablesen*. In der Praxis ist sogar oft die Aussageform gar nicht bekannt, sondern nur die Wahrheitstabelle. Das damit gegebene Problem heisst *Darstellungsproblem*. Die sofort ablesbaren kanonischen Formen sind dann Aussageformen, die der gegebene Wahrheitstabelle genügen. Allerdings erhält man so meistens nicht die einfachsten oder kürzesten aller möglichen Aussageformen, die in Betracht kommen. Das Auffinden einer möglichst einfachen Form nennt man das *Vereinfachungsproblem*.
Wir wollen das Darstellungsproblem anhand eines Beispiels studieren. (Für das Vereinfachungsproblem muss auf den Teil *Boolsche Algebra* verwiesen werden. Eine Methode zur Vereinfachung bei gewissen vorgeschriebenen Junktoren ist z.B. die *Karnaugh-Methode*, in der mit Mengendiagrammen gearbeitet wird.)

Beispiel: Gegeben sei die Aussageform $X \equiv (A \vee B) \Leftrightarrow \neg C$. Gesucht ist die äquivalente aNF. Zuerst stellen wir uns die zugehörige Wahrheitstabelle auf:

Zeilennummer	A	B	C	$X \equiv (A \vee B) \Leftrightarrow \neg C$
1	0	0	0	0
2	0	0	1	1
3	0	1	0	1
4	0	1	1	0
5	1	0	0	1
6	1	0	1	0
7	1	1	0	1
8	1	1	1	0

X ist genau dann wahr, wenn wir eine der Belegungen haben, die gegeben ist durch die Zeilen 2, 3, 5 oder 7 der Wahrheitstabelle. Zeile 2 z.B. trifft zu, wenn A den Wahrheitswert 0 und B den Wahrheitswert 0 und C den Wahrheitswert 1 hat. D.h. wenn $\neg A$ den Wahrheitswert 1 und $\neg B$ den Wahrheitswert 1 und C den Wahrheitswert 1 hat. Das ist genau dann der Fall, wenn die Form $(\neg A \wedge \neg B \wedge C)$ den Wahrheitswert 1 hat. (Bei allen andern Belegungen hat die letzte Aussageform den Wahrheitswert 0.) Somit trifft Zeile 2 zu, wenn $(\neg A \wedge \neg B \wedge C)$ wahr ist. Genau so trifft Zeile 3 zu, wenn $(\neg A \wedge B \wedge \neg C)$ wahr ist. Zeile 5 trifft zu, wenn $(A \wedge \neg B \wedge \neg C)$ wahr ist und Zeile 7, wenn $(A \wedge B \wedge \neg C)$ wahr ist. X ist wahr, wenn wir eine Belegung haben, die gegeben ist durch die wahre Zeile 2 oder die wahre Zeile 3 oder die wahre Zeile 5 oder die wahre Zeile 7. (Bei den andern Belegungen ist X falsch.) D.h. X ist genau dann wahr, wenn $(\neg A \wedge \neg B \wedge C)$ oder $(\neg A \wedge B \wedge \neg C)$ oder $(A \wedge \neg B \wedge \neg C)$ oder $(A \wedge B \wedge \neg C)$ wahr ist. Also ist X genau dann wahr, wenn $(\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C)$ wahr ist. Bei den restlichen Belegungen der Variablen A, B und C ist X nicht wahr. Daher gilt:

$$X \equiv (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C).$$

Wir haben somit X *ersetzt durch eine kanonische aNF,* denn die gewonnenen Konjunktionsterme sind mit $\vee$ verknüpft. Durch den Ablesevorgang ist diese so gewonnene Form sogar geordnet.
Man kann sich daher folgendes Vorgehen merken: Streiche diejenigen Zeilen der Wahrheitstabelle, in denen hinten eine 0 steht. In den übrigbleibenden Zeilen ersetze man die Wahrheitswerte 1 durch die zur jeweiligen Kolonne gehörige Aussagenvariable, die Wahrheitswerte 0 durch die Negation der zur jeweiligen Kolonne gehörigen Aussagenvariablen und verknüpfe diese durch $\wedge$. So erhält man für jede bleibende Zeile einen Konjunktionsterm. Diese Terme verknüpfe man durch $\vee$.
Falls man dasselbe Verfahren auf diejenigen Zeilen anwendet, in denen hinten der Wahrheitswert 0 steht, so erhält man die aNF: $Y \equiv (\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge C)$. Diese aNF Y ist genau dann *falsch*, wenn X wahr ist. Daher ist $\neg Y$ genau dann wahr, wenn X wahr ist. Es gilt also $\neg Y \equiv X$. Für $\neg Y$ gilt aber nach den De Morganschen Regeln die Äquivalenz $\neg((\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge C)) \equiv (A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C)$. Das ist aber die geordnete kanonische kNF.
Die geordnete kanonische kNF erhält man also aus der Wahrheitstabelle, wenn man das oben beschriebene Verfahren auf diejenigen Zeilen anwendet, in denen hinten eine 0 steht und vor die erhaltene aNF den Junktor $\neg$ setzt. Nach den De Morganschen Regeln erhält man daraus die gesuchte kNF.

Kapitel • Chapitre 6

Grenzen der Aussagenlogik, Quantoren und Ausblick

6.1 Grenzen der Aussagenlogik

In 9.1.1 haben wir den Begriff *„Aussage“* als *sprachliches Gebilde* verstanden, das eine *Wahrheit* oder eine *Unwahrheit* ausdrückt. Sprachliche Gebilde, mit denen man Wahrheiten oder Unwahrheiten ausdrücken kann, nennt man aber in der Grammatik *Sätze*. Beispiele:

1. Der Satz „Hans ist nicht hier“ ist jetzt entweder wahr oder falsch. Weitere Sätze:
2. „Hans füttert das Pferd.“
3. „Jetzt scheint draussen die Sonne.“
4. „Heute ist die Sonne im Osten zweimal aufgegangen.“
5. „Unser FC hat am letzten Samstag wieder einmal nicht gewonnen.“
6. „Eins und eins ist zwei.“
7. „$1 + 1 = 2$.“
8. „Auf der Rechnung der Firma Abschneider ist eins und eins gleich drei.“
9. „Aus $a = 6$ folgt $2a = 12$.“

Im Vergleich dazu sind die sprachlichen Gebilde „Hurra!“, „Ha ha ha!“, „Wie komm ich am schnellsten zum Park?“, „Komm her!“, „Hau ab!“ keine Aussagen. Es handelt sich um Exklamationen oder Interrogationen (Ausrufe, Fragen). Ebenso ist das Gebilde „X fährt Auto“ unbestimmt, also keine Aussage.
Historisch finden wir die Wurzeln der logischen Aussage bei Aristoteles. Statt von Aussagen redet man daher auch von *Aristotelischen Aussagen*. Wie man leicht nachprüft, sind solche Aussagen einfache Sätze, bestehend aus Subjekt, Prädikat und Objekt. Dabei kann das Subjekt oder das Objekt noch durch ein Attribut erweitert sein oder das Prädikat durch ein Adverbiale. Daneben finden wir solche einfache Sätze als Teile von zusammengesetzten Sätzen, von Satzverbindungen und Satzgefügen. Details dazu finden sich in jedem einschlägigen Schulbuch unter dem Titel „Satzlehre“. Es würde den Rahmen der mathematischen Logik sprengen, die Grundbegriffe der Grammatik hier auch nochmals aufzuarbeiten. Sie seien vorausgesetzt.
Betrachten wir den folgenden Satz: „Hans füttert das Pferd.“

$$\overbrace{\text{Hans}}^{\text{Subjekt}} \quad \underbrace{\overbrace{\text{füttert}}^{\text{Prädikat}} \quad \overbrace{\text{das Pferd.}}^{\text{Objekt}}}_{\text{Prädikativer Ausdruck}}$$

Das ist eine Aussage.

Betrachten wir dagegen den Satz: „X füttert das Pferd“, so kann man nicht mehr entscheiden, ob das jetzt wahr oder falsch ist. Ein Teil des Satzes ist hier variabel und unabhängig: Für X kann man ja irgend ein Subjekt einsetzen. Setzt man für X „Hans“ ein, so ist der nun entstehende Satz in unserem Kontext wahr. Setzt man aber für X „Die Dampflokomotive“ ein, so ist der dann entstehende Satz ganz sicher falsch. Da X für das Subjekt steht, nennt man X *„freie Subjektvariable“*.

Ähnlich gelagert liegt die Sache bei „Aus $x = 5$ folgt $2x = 10$“, resp. bei „$(x = 5) \Rightarrow (x = 10)$“. $(x = 5)$ ist selbst eine Aussagenvariable, denn darin steckt die Variable x. Der Ausdruck wird zu einer Aussage, wenn man für x einen Wert einsetzt. Setzt man für x den Wert 5, so entsteht eine wahre Aussage. Setzt man hingegen für x den Wert 6, so entsteht eine falsche Aussage. Die Aussagenvariable $X \equiv (x = 5)$ wird demnach im Ausdruck $(x = 5) \Rightarrow (x = 10)$ zu einer Subjektvariablen, denn sie steht an der Stelle des Subjekts. $\Rightarrow$ hat die Bedeutung des Prädikats, $(x = 10)$ die Bedeutung einer *Objektvariablen*. Durch Einsetzung einer Zahl für x ensteht dann aus $(x = 5) \Rightarrow (x = 10)$ eine zusammengesetzte Aussage, die aus Zahlengleichungen als Teilaussagen besteht. Lässt man hingegen x stehen, so ist $(x = 5) \Rightarrow (x = 10)$ ebenfalls eine Aussage, die aber nicht in Teilaussagen aufspaltbar ist, sondern nur in zwei Aussagenvariablen und in einen Junktor. Hingegen ist die Zahlenvariable x selbst keine Aussage, sondern nur Teil einer Aussagenvariablen.
Bei den jetzt besprochenen Beispielen fällt aber auf, dass eine Aussage eine *innere Struktur* haben kann. So sind z.B. Subjekt, Prädikat und Objekt Teile einer Aussage, die aber einzeln manipuliert werden können, selbst aber noch keine Aussagen sind. Die Aussagenlogik alleine liefert keine Handhabe für eine solche Manipulation. Man stösst so hier an die Grenzen der Aussagenlogik: Mit Aussagenlogik alleine ist noch längst nicht alles getan!

6.2 Quantoren

Wir betrachten als Beispiel folgende drei Aussagen:

(1) A ≡ Alle Fische leben im Wasser. Symbolisch: (Alle ⟩ Fisch ⟩ Prädikat(Wasser))
(2) B ≡ Die Forelle ist ein Fisch. – (Forelle ⟩ Prädikat(Fisch))
(3) C ≡ Die Forelle lebt im Wasser. – (Forelle ⟩ Prädikat(Wasser))

Offenbar ist (3) aus Teilen von (1) und (2) durch Neukombination entstanden. Der prädikative Ausdruck von (2) ist mit dem Subjekt von (1) zu (3) kombiniert worden. Für die Kombination von solchen Teilen von Aussagen zu einer neuen Aussage bietet aber die Aussagenlogik keine Regeln. $A \wedge B \vdash C$ kann also nicht mit den Regeln der Aussagenlogik hergeleitet werden, da hier die innere Struktur einer Aussage wesentlich ist. Die Theorie, die diesem Problem gerecht wird, nennen wir *Prädikatenlogik*. Man unterscheidet da sogar *verschiedene Stufen von Prädikatenlogiken (Stufenlogik)*.
In der Prädikatenlogik studiert man nicht nur Aussagen und Aussagenvariablen, sondern auch *Subjekte*, *Subjektvariablen*, *Prädikate*, *Prädikatenvariablen* und auch *Quantoren*. Quantoren sind logische Zeichen oder Wörter, die eine *Quantität* ausdrücken, im Gegensatz zu Aussagen oder Aussagenvariablen, die eine *Qualität* wiedergeben. Da Quantoren eine sehr kompakte Schreibweise mathematischer Aussagen erlauben, werden sie in der Hochschulmathematik sehr häufig verwendet. Das gilt in der Folge natürlich auch für die Ingenieurmathematik von Hochschulniveau!
Für uns sind zwei Quantoren wichtig: der *Allquantor* und der *Existenzquantor*. Zeichen und Bedeutung finden sich in der folgenden Tabelle zusammengestellt:

Name	Symbol	Weiteres Symbol	Bedeutung
Allquantor	$\forall$	$\bigwedge$	Für alle
Existenzquantor	$\exists$	$\bigvee$	Es gibt

Die folgenden Beispiele mögen zur weiteren Erklärung dienen. Sei $M := \{1, 2, 3, 4\}$

1. $\forall_{x \in M} : x < 5$ bedeutet: $(1 < 5) \wedge (2 < 5) \wedge (3 < 5) \wedge (4 < 5)$.
2. $\exists_{x \in M} : x = 3$ bedeutet: $(1 = 3) \vee (2 = 3) \vee (3 = 3) \vee (4 = 3)$.

Da im ersten Beispiel alle Zahlen aus M kleiner 5 sind und im zweiten Beispiel eine Zahl aus M existiert, die die Gleichung $x = 3$ erfüllt (es gilt ja $3 = 3$), haben wir in beiden Fällen wahre Aussagen. x ist hier in beiden Beispielen eine an den Quantor gebundene Subjektvariable. (*Gebundene* Subjektvariable.)

6.3 Ausblick: Weitere Resultate der Logik

Ohne Beweis wollen wir hier noch einige Resultate besprechen, die praktisch bedeutsam sind. Die Beweise dazu sind relativ sehr lang und setzen eine gehörige Portion Übung im mathematisch–logischen Denken voraus.

Satz 6.1 (Vollständigkeitssatz) *: Die Aussagenlogik ist vollständig.*

Vollständig bedeutet hier, dass jeder wahre Satz der Aussagenlogik auch in endlich vielen Schritten (d.h. in einer *Beweiskette*) herleitbar ist. Dies kann man also beweisen. „Q ist wahr“ bedeutet also, dass es einen Beweis (d.h. einen korrekten logischen Schluss) $w \vdash Q$ gibt.
Achtung! Für die höhere Prädikatenlogik gilt dieser Satz nicht mehr! Das bedeutet, dass in der höheren Prädikatenlogik wahre Sätze existieren, zu denen es keine endliche Beweiskette mehr gibt, die in derselben Stufe der Prädikatenlogik formulierbar ist. Man kann also beweisen, dass es Sätze gibt, die im gegebenen Rahmen nicht beweisbar sind, dass also die Menge der wahren Sätze grösser ist als die Menge der herleitbaren Sätze. Das zeigen die Resultate von Gödel aus den Dreissigerjahren des zwanzigsten Jahrhunderts. Turing und andere sind ebenfalls auf diesem Gebiet zu Resultaten gelangt, die Auswirkungen auf das Problem der Berechenbarkeit haben.
Weiter gilt der folgende Satz:

Satz 6.2 (Widerspruchsfreiheit der Aussagenlogik) *: Die Aussagenlogik ist widerspruchsfrei.*

Das bedeutet, dass in der Aussagenlogik kein Widerspruch entstehen kann, dass also z.B. $P \wedge \neg P$ nicht herleitbar ist, egal um welche Aussage oder Aussageform P es sich handelt. Mit andern Worten: $w \nvdash P \wedge \neg P$ oder auch $w \nvdash f$.
Wie wir später im Beispiel der *Schaltalgebra* sehen werden, genügt die Aussagenlogik vollständig für die Maschinenverarbeitung (Bit–Maschinen, von Neumann-Maschinen). Denn alle Programme werden ja mit Schaltungen der gegebenen Hardware abgearbeitet. Und die Schaltungen genügen den Regeln der Schaltalgebra. D.h.: Was mit den klassischen Computern machbar ist, liegt alles im Rahmen der Aussagenlogik. Andererseits lassen sich Probleme, deren Formulierung nicht auf die Aussagenlogik zurückführbar sind, die also wirklich der Prädikatenlogik bedürfen (wie etwa Quantifizierungen über unendlichen Mengen), mit dem klassischen Computer nicht behandeln. Ebenso solche, die von rein Qualitativem handeln, sich vom Gegenstand her nicht auf Quantifizierbares reduzieren lassen[1]. Darunter fallen Probleme der philosophisch–humanwissenschaftlichen Disziplinen. Prädikatenlogik lässt sich eben nicht vollkommen auf Maschinen zurückführen und damit auf Schaltalgebra und auf Aussagenlogik, auch wenn die Intelligenz dieser Maschinen noch so künstlich ist. Sonst käme man ja mit der Aussagenlogik alleine aus. Ein Grundproblem ist wohl, dass eine endliche Maschine mit endlichen Algorithmen nicht über unendlichen Mengen abstrahieren kann wie ein Mensch, der einen nicht abbrechenden Prozess wieder als aktuales Objekt begreifen und damit arbeiten kann. Der Mensch hat die Fähigkeit der gezielten, erfolgbringenden Abstraktion, der Bildung neuer, genialer Begriffe aus einem Akt des Wollens heraus. Die Maschine hingegen kann nicht wollen, sie kann nur befolgen, ist immer Sklave eines Programms. Ein anderes Grundproblem entsteht nun auch aus der Einsicht heraus, dass Qualitäten und ihre Beziehungen sich nicht immer auf Quantitäten und deren Beziehungen reduzieren lassen...

[1] Die Strömung, in der diese Reduktion in völliger Ignoranz der Ergebnisse der Logik trotzdem versucht wird, nennt man *Reduktionismus*

Chapitre 7

Préface à la logique propositionnelle

Chère lectrice, cher lecteur,

Nous nous sommes proposé d'étudier ainsi les mathématiques strictement composées afin de les comprendre d'une façon cohérente et de pouvoir les employer en tant qu'outil professionnel. L'étudiant mûr aura compris depuis longtemps que dans la vie l'on ne peut rien atteindre en aucun champ d'activité sans de bonnes connaissances et sans habilités dans l'application des outils. Cela n'est pas différent pour les mathématiques. L'outil le plus important des mathématiques est donc la logique. Sans la logique la compréhension reste difficile. Car les mathématiques sont considérées comme la science basée sur les preuves, comme domaine de la certitude, des résultats attestés et des formules exactes, qui n'admettent aucun malentendu. Et l'outil, pour le fait de prouver ou le fait de formuler exactement, le fait de définir, pour le fait de déduire, c'est la logique. En particulier c'est justement la logique à deux valeurs de vérité qui est encore très simple, du point de vue mathématiques. Nous commençons par celle-là. ça nous donne une base solide pour une mise au courant dans des domaines plus vastes, conformément au niveau: D'abord dans la théorie des ensembles, après, basé sur cela, dans le domaine des rapports. Alors ici nous pouvons appuyer de façon satisfaisante l'idée très centrale de l'application mathématique et de la fonction mathématique, sur laquelle on construit une grande partie des mathématiques consécutives. P.ex. plus tard dans le calcul différentiel– et intégral, on ne fait proprement rien d'autre que d'examiner des fonctions. En pratique on peut facilement résoudre des problèmes à l'aide de fonctions. D'autres régions aussi, par exemple l'algèbre de Boole — ou alors spécialement l'algèbre des circuits électriques — s'appuient directement sur la logique. Le fondement "logique" doit être solide afin que le bâtiment qu'on construit tienne. Essayons ainsi de nous y appliquer avec rigeur. Et n'oublions jamais le conseil: Un clou n'est rarement bien placé après un coup de marteau. Ne te laisse décourager; travaille avec persévérance et avec la pensée que tes facultés se développent de plus en plus. Mais n'oublions pas de rire à cause de cette matière difficile.ça porte de l'énergie et de la fraîcheur à la tête chaude, fumante et fatiguée.

Automne 1994/99 L'auteur

> *L'esprit qui n'est que l'acuité, mais pas étendue, hésite à chaque point et n'avance pas ... Un esprit, qui est seulement de la logique, ressemble à un couteau qui n'est que lame. La main devient sanglante à l'emploi. ...*
>
> *Tagore*

Chapitre 8

Idée, origine de la logique propositionnelle bivalente

8.1 Pourquoi insistons–nous sur la logique dans les mathématiques?

Dans les écoles inférieures d'orientation principalement technique, on entend aujourd'hui assez souvent le terme de "logique " , peut-être dans le contexte des couplages électriques. C'est cependant une vue très spéciale qui ne laisse pas deviner l'ampleur de la matière à laquelle on fait allusion ici. Qu'est-ce qu'on comprend alors par "logique" dans les sciences exactes, dans les mathématiques?

Le terme de *logique* comprend aujourd'hui un domaine scientifique qui est réclamé par beaucoup de sciences comme partie d'elles–mêmes: Entre autres la philosophie, la théologie, la linguistique, la jurisprudence, les mathématiques. Il n'y a par conséquent pas de logique unique. La logique juridique n'a peut–être pas beaucoup à faire avec "la logique transcendentale" de Kant, qui appartient à la philosophie. Et ceci de nouveau, n'est pas à confondre avec la logique mathématique, que cette partie va traiter. La logique mathématique est une *logique formelle*. ça signifie que l'intérêt principal ne va ni au message, ni au contenu, ni au contenu intentionnel d'une construction linguistique, mais à la forme. Plus simplement: L'intérêt est pour la construction grammaticale. En outre nous pouvons nous consacrer ici seulement à une *partie très restreinte* de la logique mathématique: A la logique bivalente (à deux valeurs de vérité), avec une petite perspective dans le domaine incomparablement plus grand de la logique mathématique des prédicats. Tout le reste ne sera pas considéré.
On peut se demander maintenant quels sont les devoirs de la logique formelle des mathématiques. On discerne dès l'abord trois domaines de devoirs: Premièrement la logique est un domaine indépendant où se situent les questions inhérentes, qui appartiennent à la théorie de la connaissance. Deuxièmement la logique est aussi très apparentée aux autres domaines mathématiques, tels que la théorie des treillis, par conséquent l'algèbre de Boole — et basé sur cela l'algèbre des circuits ou bien la théorie des ensembles. La logique est le fondement ici. Troisièmement chaque science a son langage, ainsi donc aussi les mathématiques. Les mathématiques se servent, pour formuler les exposés et pour la construction des règles, du langage de la logique. Ici, la logique est donc utilisée comme le langage. *Retenons donc:*

Le langage des mathématiques est la logique formelle.

8.2 Comment et quand est-ce que la logique s'est formée? — Quel âge a–t–elle?

Le titre fait allusion à l'histoire. Faisons un saut en arrière. On peut trouver les premiers commencements de la "logique" formelle, plus tard nommée ainsi par Kant [1], chez Aristote [2]. Inspiré par Platon [3], Aristote c'est mis à raisonner sur la vérité et la fausseté d'ennoncés. Il a reconnu qu'on peut dériver des axiomes considérés comme vrais, par l'usage de règles d'opération, certaines propositions nouvelles qu'on doit considérer comme vraies à cause des règles. On appelle ces règles de déduction des *syllogismes*. Hormis quelques tentatives de Leibnitz [4], qui a essayé d'utiliser peut-être le premier une langue artificielle, ou de Lambert [5], la logique mathématique et formelle a dormi plus ou moins un sommeil de Belle au bois dormant jusque au 19ème siècle. Par les travaux de De Morgan [6] et Boole [7], la logique formelle a commencé à fleurir. Et au tournant du vingtième siècle nous constatons soudainement un début frénétique de la recherche, et une augmentation explosive du savoir, en particulier liés aux noms de Schröder [8], de Peano [9], de Peirce [10], de Frege [11], de Whitehead [12], de Russel [13], de Hilbert [14] et de Ramsey [15], de Turing [16], de Gödel [17], de Skolem [18], de Tarski [19] et d'autres. En particulier par les théorèmes de complétude et d'incomplétude, publiés par Gödel en 1931, a pu naître une conception du monde tout à fait différente. Analogiquement aux limites du monde matériel on a trouvé aussi des limites au monde de la pensée exacte et maintenant on sait donc où on ne pourra jamais parvenir.
A part tout ce qu'on vient de dire, il est important de retenir que la logique formelle qui se développe maintenant, n'est pas une chose ancienne mais plutôt récente.

8.3 Quant à l'objet

8.3.1 La logique, qu'est–ce que c'est?

Dans la logique philosophique on s'occupait autrefois des "lois de la nature" de la raison, de l'art de penser resp. de la pensée correcte. Dans cette logique, on traite les questions concernant les règles de la déduction raisonnable qui apparaissent contraignantes, les raisons pourquoi ces règles sont ainsi et les rapports entre la cause et l'effet. La logique philosophique actuelle s'occupe plutôt des déductions qui mènent à des propositions justes seulement à cause de la forme ou pour des raisons linguistiques, donc à l'aide de la logique symbolique ou formelle. La logique mathématique aussi est logique formelle. Elle traite des propositions formulées dans une langue "exacte", *logique propositionnelle,* ou bien, exprimé de façon peu floue, de propositions qu'on peut subdiviser, *logique des prédicats*. Principalement on s'intéresse à des questions telles que les suivantes:

1. Kant: philosophe allemand, 1724–1804
2. Aristote: Elève de Platon, 384–322 V. Chr.
3. Platon: Philosophe grec, 427–347 av.J.Chr.
4. Leibnitz: mathématicien et philosophe allemand 1646–1716
5. Lambert: mathématicien allemand 1728–1777
6. De Morgan: mathématicien anglais 1808–1871
7. Boole: mathématiciens anglais 1815–1864
8. Schröder: mathématicien allemand 1841 – 1902
9. Peano: mathématicien italien 1858 – 1932
10. Peirce: mathématicien américain 1839 – 1941
11. Frege: mathématicien allemand 1848 – 1925
12. Whitehead: mathématicien anglais 1861 – 1947
13. Russel: mathématicien anglais 1847 – 1970
14. Hilbert: mathématicien allemand 1862 – 1943
15. Ramsey: mathématicien anglais 1904 – 1930
16. Turing: mathématicien anglais 1912 – 1954
17. Gödel: mathématicien austrichien, né en 1906
18. Skolem: mathématicien norvégien 1887 – 1963
19. Tarski: mathématicien polonais, 20ème siècle

- L'intégralité d'une langue composée formellement, possibilité de prover : Est-ce que toutes les propositions vraies sont aussi deduisibles dans la langue elle-même?
- Possibilité de décision concernant un problème: Est-ce qu'un chemin de décision existe? Quelles constructions linguistiques sont déduisibles?
- Possibilité de définir : Est–ce que la langue est suffisamment riche (ample) ou est–ce que quelque chose dont on "voudrait parler" ne peut pas du tout être défini?
- La sécurité: Un ensemble de règles (un système d'axiomes) est–il exempt de contradictions — et par conséquent la théorie basée sur cela —?
- La faisabilité: Comment la théorie est-elle à construire maintenant?
- Problème de la représentation: Quel est le minimum d'outils linguistiques qu'on nécessite pour pouvoir rendre quelque chose?
- Niveau de la langue: Combien doit–elle être une langue compliquée pour pouvoir exprimer quelque chose qu'on veut exprimer?
- La forme: Quand est–ce que le niveau de vérité d'une proposition dépend seulement de la forme et non du contenu?
- Le contenu: Comment est–ce que le contenu et la forme sont liés?
- Etc.

8.3.2 Où est-ce qu'on va s'arrêter?

Et on doit alors savoir tout cela? — Oh non, justement pas. Ici nous développerons le langage de la logique seulement autant qu'il est essentiel et de valeur pour ce qui suit et pour la formation commune. Ça signifie que nous allons à peine quitter le vieux "niveau aristotélien" . Nous n'avancerons pas dans la logique mathématique moderne, dans la *méthodologie des sciences exactes* resp. dans la *logique des prédicats de niveau élevé* (ou dans la *logique graduée*). Là le temps, la formation et la nécessité manquent. Nous poursuivons ici le chemin *non–sévère*, dit *"naïf"*. Ça suffira.

8.4 Littérature conseillée

La littérature sur la logique formelle est extrêmement étendue. Mais la plupart des livres ne sont pas écrits pour l'étudiant ingénieur. De tels livres paraissent à l'amateur, quant au niveau de la langue, illisibles, incompréhensibles, inutilisables. Une littérature étendue existe en anglais et en allemand. Les oeuvres suivantes, que l'auteur connaît, peuvent être considérées comme conformes au niveau: Mendelson, SCHAUM (Bibl.: mendelson), Lipschutz, SCHAUM (Bibl.: lipschutz). Ou bien aussi des livres spéciaux pour les collèges supérieurs, (éditions scolaires)(Bibl.: jehle , deller). Malheureusement on constante que le chapitre "logique" manque d'ordinaire dans les livres techniques mathématiques pour les ingénieurs. Indications pour les avancés: La littérature de niveau plus élevé se trouve entre autres dans Bibl.: asser, church, hermes, hilbert, shoen, tarski, vandalen. En ce qui concerne la littérature en langue française, les étudiants sont priés de s'adresser à l'auteur.

8.5 Exercices

Les exercices pour la partie deux se trouvent aussi sur les feuilles d'excercices *DIYMU*. (Voir Bibl.: wirz [20]

20. Livre d'exercice *DIYMU*: "En guise d'introduction" (Bibl.: wirz).

Chapitre 9

Logique propositionnelle

9.1 Propositions, variables propositionnelles et valuations

9.1.1 Propositions

Nous allons nous demander ce que signifie la notion de *proposition*. Afin que nous puissions parler de *propositions*, nous devons en développer d'abord une idée. Comme nous n'avons encore défini aucune notion simple sur laquelle nous pourrions nous baser, nous allons suivre l'idée ci–dessous(" idée de notion" pseudo – définition, pas encore stricte:

Explication de la notion 1 (Proposition) *: Une* **proposition** *est une création linguistique, qui exprime une "vérité" ou une "fausseté".*

Jusqu'à maintenant nous n'avons pas défini ce que *" vrai "* ou " pas vrai " (resp. *" faux "*) devrait signifier. Nous supposons que chacun est si raisonnable qu'il peut apprécier quand quelque chose est compréhensiblement vrai ou non[1]. Ce qui doit être considéré comme "raisonnable" peut être décidé par des personnes retenues raisonnables au moyen d'une discussion démocratique.

L'homme n'a pas d'autre possibilité pour parvenir à la " vérité " par la raison. En outre nous supposons aussi que nous savons suffisamment ce qu'est une " création linguistique ". Ici les propositions sont donc des *créations de la raison* –, semblablement au point dans la géométrie, qui ne peut non plus être défini plus précisément. Aujourd'hui cela ne dérange plus personne sérieusement.

Nous trouvons des propositions spécialement claires du point de vue de leur nature dans le *propositions mathématiques* ou (si cela est important) dans les *théorèmes mathématiques* qu'on estime vrais, si on accepte les conditions de l'hypothèse. Par exemple les équations ou les inéquations avec des nombres sont des propositions mathématiques simples. *Pour cette raison nous appliquerons principalement dans les exemples suivants des propositions mathématiques.*

Exemples:

$a :\equiv$ "$2+2=4$"	(proposition math. vraie[2])
$b :\equiv$ "$2+2=5$"	(proposition math. fausse)
$c :\equiv$ "$2+2+5$"	(pas de proposition)
$d :\equiv$ "Est-ce que tu vas dormir?"	(pas de proposition)
$e :\equiv$ "Viens, s.t.p.!"	(pas de proposition)
$f :\equiv$ "Le bouleau est un arbre!"	(pas de proposition)

1. Le problème de la nature de la vérité comme "problème de la connaissance" est de toute façon un problème fondamental de la philosophie. La philosophie connaît trois problèmes de fond: Le problème de l'*être* , le problème de la *reconnaissance* et le *problème de la morale*.

2. Si on accepte l'arithmétique avec les nombres.

$g :\equiv$ "1.1111 n'est pas un nombre" (proposition math. fausse)
$h :\equiv$ "Si l'interrupteur est ouvert, le courrant passe." (proposition fausse)

Remarque 1 (quant aux symboles utilisés): Ici a, b, c, d et e sont des noms pour les propositions. Le signe ":≡" signifie "définit comme équivalent". "≡" seul signifie équivalent. Nous utilisons ce signe pour éviter des confusions avec le signe d'égalité dans les propositions mathématiques (p.ex. dans $2 + 3 = 5$).

Remarque 2 (quant à la logique bivalente):
Dans la *logique bivalente* on considère seulement des propositions qui sont *vraies* ou *fausses* et qui ne laissent ouverte *aucune autre possibilité* pour la valeur de vérité. Dans la langue quotidienne, cette situation représente plutôt une exception qu'on aime repousser dans les mathématiques. P.ex. un objet n'est pas "clair" ou "non clair" (à l'occasion on pourrait dire "sombre".) L'objet possède une certaine clarté. La même chose vaut pour noir et blanc. Entre les deux extrêmes il y a beaucoup, beaucoup de nuances de gris. Prenons comme autre exemple le chat, "cher" animal domestique , mais qui peut être très méchant quand il nous griffe. Et aussi le bon chien de maison, qui n'éveille pas du tout d'enthousiasme, quand il mord au moment où on ne s'y attend pas ... Le contraire de la déclaration (ici *proposition*) "le chien est *bon*" n'est donc pas la déclaration "le chien est *mauvais*" ou "le chien n'est *pas bon*", mais: "Le chien n'est *parfois pas bon*". Car le chien se montre une fois bon, une autre fois nous le subissons comme chien mauvais, une fois plutôt comme bon et mauvais en même temps, et une quatrième fois ni bon ni mauvais ni autre chose, car il n'est plus rentré à la maison depuis quelques jours, il n'est simplement pas pas présent.
Ici les notions de "vrai" et de "faux" ne suffisent plus. On a besoin de degrés intermédiaires variés, qu'on ne peut pas ranger dans une échelle graduée unidimensionnelle, semblablement aux couleurs. Ainsi nous arrivons à une *logique polyvalente* . Si on introduit encore la valeur de vérité *indéterminée*, on parvient donc à une *logique trivalente*[2]. On ne peut pas encore décider si la phrase "Dans deux cent ans la Suisse sera un royaume!" exprime une vérité, elle reste donc d'abord absolument indéterminée pour nous, parce que nous ne le savons pas encore. Mais la déclaration n'est pas "variable", car nous ne pouvons rien changer ou remplacer à la réalité de l'avenir. Ce que nous pouvons changer, c'est seulement notre idée de l'avenir. Même si nous interrogeons maintenant un oracle. Seule une génération postérieure connaîtra avec sûreté absolue la réalité. Aujourd'hui la vérité nous reste inaccessible — peut–être nous pouvons l'influencer encore par nos actions, mais seulement dans la direction qui existerait une fois fixement. Car il y a seulement un passé et aussi seulement un avenir.
Un autre exemple peut-être plus frappant: Pendant une croisière un groupe de passagers aisés et menacés par un passager clandestin armé soudainement émergé, évidemment appauvri, en chiffons et qui a faim. On voit tout de suite qu'il n'hésitera pas à se servir de son arme pour demander de la nouriture –, peut–être il ne lui reste aucun choix d'agir ainsi. Le capitaine aussi armé découvre la chose et tire tout de suite, le passager clandestin tombe mort sur le pont, abatu. — Est–ce que la façon d'agir du capitaine est bonne ou mauvaise? — Voici un problème de morale qui ne pourra jamais être résolu. Ici on n'avance pas avec "vrai" ou "faux" seulement. Chaque jugement pour ou contre ton opinion peut être identifié comme idéologie. Des questions pareilles émergent quand il s'agit de héros nationaux (qui peuvent être les propres idoles — ou bien les idoles odieuses des ennemis) de martyrs, de petits amis, de gens admirés et autres. Mais ici nous cesserons de considérer la logique polyvalente.

En ce qui concerne les propositions (déclarations), il faut mentionner qu'ici nous voulons diriger notre intérêt principal vers les *propositions (déclarations) mathématiques*. Plus tard d'autres déclarations telles que *"le courant passe parce que l'interrupteur est fermé. "* jouent un rôle dans l'*algèbre des circuits électriques* (spécialement l'algèbre de Boolsche).

9.1.2 Variables propositionnelles

Exemple: Nous considérons l'équation "$x = y$" .

2. P.ex. logique de Lukasiewicz et Post ainsi que la logique intuitioniste.

Si on remplace les variables x et y par 1, l'équation se transforme en proposition (déclaration) $a :\equiv'' 1 = 1''$. Nous acceptons naturellement cette proposition (déclaration) comme vraie. Mettons par contre $x = 2$ et $y = 3$, ainsi l'équation se transforme en proposition (déclaration) $b :\equiv'' 2 = 3''$. Cette proposition représente selon notre compréhension une équation numérique fausse. Cependant à l'équation $A :\equiv'' x = y''$ n'est liée aucune valeur de vérité *ni vrai, ni faux*. A peut être transformé en proposition (déclaration) par l'introduction des valeurs pour x et y. Mais A elle–même est provisoirement une *place neutre*, un *remplaçant* ou un *support de place* pour une proposition (déclaration), par exemple comme à un ordinateur une place dans la mémoire qui peut prendre un symbole, mais qui n'est elle–même pas un symbole, mais justement et simplement une place vide. Par conséquent nous déterminons:

Explication de la notion 2 (Variable propositionnelle) *: Nous appelons un signe orthographique qui se transforme après le remplacement par une création linguistique en une proposition (déclaration)* **variable propositionnelle**.

Remarque:
Symbole 1 (pour propositions et variables propositionnelles) *Pour garantir en tout temps la distinction entre propositions (déclarations) et variables propositionnelles, nous appliquons pour les propositions des lettres* **minuscules**, *par exemple* a, b, $c\ldots$, *et pour les variables propositionnelles des* **majuscules**, *par exemple* A, B, $C\ldots$.
P.ex. on peut donc mettre pour la variable A ou la place vide A une proposition (déclaration) déterminée a, qui peut être vraie ou fausse. Dans la *logique bivalente* on a ici toujours deux possibilités. A peut passer à une proposition *vraie* ou à une proposition *fausse*.

Schématiquement:

Tableau 10. 0: Variable propositionnelle, propositions et valeurs de vérité

Variable propositionnelle A	valeur de vérité liée	
	Variante 1	Variante 2
Remplacé par proposition *vraie* a_1	w	1
Remplacé par proposition *fausse* a_2	f	0

Explication de la notion 3 (Valeurs de vérité) *: Les abréviations utilisées telles que* w, f *resp.* 1, 0 *s'appellent* **valeurs de vérité**. *Elles signifient "vrai" ou "faux".*

Si nous pouvons nous engager à déterminer une méthode claire à la constatation de la valeur de vérité d'une proposition (par exemple par *vérification interpersonale*, obtention d'un accord dans une commission de gens raisonnables avec la même langue), ainsi nous pouvons définir:

Définition 9.1 (Valeurs de vérité d'une proposition a) *:*
La **valeur de vérité** $t(a)$ *d'une proposition* a *est définie par*

$$t(a) := \begin{cases} 0 & , \quad si\ a\ est\ reconnu\ comme\ faux. \\ 1 & , \quad si\ a\ est\ reconnu\ comme\ vrai. \end{cases}$$

(*Remarque:* "t" dans $t(A)$ signifie *"truth"*[3] . $t(a)$ est aussi une *fonction* dans le domaine de définition "ensemble de propositions" dans le domaine de valeurs {0,1}.)

Dans la logique propositionnelle, on ne s'intéresse pas en premier lieu au *contenu* d'une proposition mais plustôt à la *forme*. Concernant la forme, jusqu'ici nous avons rencontré seulement *des propositions non démontables,* c.–à.–d. *élémentaires* ou *atomiques*. Par contre il existe aussi des propositions *composées*. Les propositions élémentaires n'ont pas de forme particulière. Elles ne se laissent pas décomposer en propositions partielles sensées, qui sont à leur tour encore vraies ou fausses. La qualité unique, qu'elles

3. anglais "vérité"

ont encore, est d'être vraies ou fausses elles-mêmes. Quant à cela un exemple: "Le sapin est un arbre." Cette proposition ne peut plus être décomposée en propositions partielles plus petites. Pour les études ultérieures, par conséquent, nous pouvons ignorer le contenu d'une proposition et regarder seulement encore sa valeur de vérité, car celle–ci suffit ici.

Définition 9.2 (Proposition élémentaire) *:* **Propositions élémentaires** *sont des propositions qui ne sont pas décomposables en des propositions partielles.*

Comme nous savons maintenant, les variables propositionnelles se laissent remplacer par des propositions auxquelles sont appliquées chaque fois les valeurs de vérité 1ou 0. A une proposition est donc *adjointe* une valeur de vérité. Considérons maintenant à la place d'une variable propositionnelle (comprise comme espace libre) non seulement une proposition a, mais aussi sa valeur de vérité adjointe $t(a)$, alors nous attribuons dans ce cas une valeur de vérité à la variable propositionnelle par la proposition. Nous disons que nous *occupons* ou *recouvrons* la variable propositionnelle par une valeur de vérité resp. nous mettons la valeur de vérité comme *poids* ou comme *valuation* à la variable.

Définition 9.3 (Poids) *: Si on applique une valeur de vérité* 0 *ou* 1 *à une variable propositionnelle A, on dit: "***poids** *des valeurs de vérité" sur A ("valuation" de A).*

Par l'application d'un poids des valeurs de vérité sur une variable propositionnelle, la variable est par conséquent tacitement remplacée par une proposition de la forme "cette place est occupée par 0" ou "la place est occupée par 1". La variable propositionnelle est transformée ainsi en une *proposition abstraite*, car à part la valeur de vérité qu'on y a placée, le contenu et la forme de la nouvelle proposition ne jouent pas de rôle pour notre intention. Le contenu et la forme des propositions originales a_i ne doivent pas nécessairement être connus. Dans la *logique formelle* nous nous intéressons par conséquent uniquement aux poids et aux liaisons des variables propositionnelles (voir chapitre prochain), mais au le contenu des propositions.

Tableau 10. 1: Valeurs de vérité comme poids à une variable propositionnelle

Variable propositionnelle	A	Signification	proposition adjointe
Poids	1	valeur "vrai"	proposition a_1, avec contenu vrai quelconque
	0	valeur "faux"	proposition a_2, avec contenu faux quelconque

Chapitre 10

Propositions sur des propositions: Propositions composées

10.1 La négation

Pour obtenir la négation d'une proposition, nous acceptons la convention suivante. A une proposition a_1 est liée une nouvelle proposition a_2 comme il suit: a_1 est exactement vrai quand a_2 est faux.

Exemples: (1) $a_1 :\equiv$ "Il pleut." (3) $b_1 :\equiv$ "$3 = 5$"
(2) $a_2 :\equiv$ "Il ne pleut pas." (4) $b_2 :\equiv$ "$3 \neq 5$"

D'après notre sentiment naturel de la langue nous considérons les proposition a_2 (resp. b_2) comme le *contraire* de a_1 (resp. b_1). Par conséquent personne ne s'opposera si nous définissons:

Définition 10.1 (Négation, "¬") *: Une proposition a_2 adjointe à la proposition a_1 qui est exactement vraie quand a_1 est fausse, s'appelle "***négation** $\neg a_1$*" de a_1.*

On peut rendre cette définition aussi par un tableau avec des *variables propositionnelles*, dans lequel on donne une collection complète de tous les poids possibles de valeurs de vérité. Chaque poids représente un type de proposition. Nous appelons un tel tableau *tableau de vérité*. Comme nous avons ainsi décrit la notion de *tableau de vérité* de façon utile et compréhensible, mais seulement exemplairement et non pas de façon complète sans lacunes, nous ne pouvons pas parler ici d'une *définition mathématique* exacte d'une notion. Mais l'explication donnée de la notion suffira pour notre intention.

Explication de la notion 4 (Tableau de vérité) *: Nous appelons un tableau de tous les poids possibles de variables de propositions avec les valeurs de vérité* **tableau de vérité**.

On peut définir donc la négation par le tableau suivant:

Tableau 10.0: Tableau de vérité pour la définition de ¬

A	$\neg A$
0	1
1	0

La proposition $\neg A$ est maintenant formellement composée, c'est à dire par les signes ¬ et A. Nous qualifions le signe ¬ comme *signe logique* .

Attention: La proposition $a_3 :\equiv$ "Le soleil brille" n'est pas la négation de $a_1 :\equiv$ "il pleut". Il peut pleuvoir même quand le soleil brille. Pensons aux arcs–en–ciel merveilleux. Alors attention! Méfie–toi

d'introduire, en interprétant les propositions, des relations internes qui n'ont effectivement rien à faire avec la chose.

Remarque: Dans la logique, nous appliquons le signe $\neg$ (par exemple dans $\neg A$, mais non dans $\bar{A}$), pour éviter des confusions avec la théorie des ensembles (ensemble complémentaire), l'algèbre des circuits électriques, ou avec les nombres complexes (nombre complexe conjugué). Car dans les définitions mathématiques, nous employons les symboles logiques comme éléments de langue déjà connus (méta–langage) pour définir des symboles mathématiques. Cette orthographe a techniquement l'avantage qu'elle est *unidimensionnelle*. Elle pourrait être lue par une machine dans une trace. Ça joue aussi un grand rôle pour les études des relations entre la logique et des machines.

10.2 La conjonction (liaison "et")

Ici et dans les sous–chapitres suivants, nous aimerons considérer des liaisons logiques, qui consistent en un signe logique (aussi appelée *symbole logique*), et deux variables propositionnelles. Pour pouvoir définir ces liaisons de façon raisonnable, nous suivons d'une part le sentiment de la langue. D'autre part nous ne voulons inspirer le soupçon qu'ici il règne l'arbitraire absolu. Alors nous baserions les mathématiques sur des produits du hasard. Pour rendre plus acceptables les définitions, on a confiance en des "sentiments raisonnables" pendant un *dialogue philosophique* sur le thème momentanément en question. Un préconiseur *(proponent)* et un antagoniste *(opposant)* devraientt discuter à fond le sujet en question, toutes les possibilités "raisonnables" incluses. Si une proposition paraît suspecte on se demande, si le contraire (le complément) vaudrait peut–être mieux. S'il arrive que l'antagoniste ne peut pas nous convaincre du contraire d'une proposition faite, tous les deux acceptent la proposition. Car dans le cadre de la logique bivalente, en dehors de *vrai* et de *faux*, il n'existe aucune troisième possibilité.

D'après ce qu'on vient de dire on ne peut probablement rien objecter au classement suivant des valeurs de vérité appliquées à la proposition composée ou totale:

Exemples du calcul commun avec des nombres:

$a :\equiv$ "$2+2=4$" et "$3\cdot 3=9$"	(proposition vraie)
$b :\equiv$ "$2+2=5$" et "$3\cdot 3=9$"	(proposition fausse)
$c :\equiv$ "$2+2=4$" et "$3\cdot 3=6$"	(proposition fausse)
$d :\equiv$ "$2+2=5$" et "$3\cdot 3=6$"	(proposition fausse)

Ici, nous produisons donc, de deux propositions partielles, au moyen de "et" une nouvelle proposition totale, qui est soit vraie soit fausse. (P. ex. de la propositions $a_1 :\equiv$ " $2+2=4$" et de la proposition $a_2 :\equiv$" $3\cdot 3=9$" il résulte la nouvelle proposition a.) Ecrit symboliquement nous avons le classement suivant:

$$(a_1, a_2) \mapsto a :\equiv a_1 \wedge a_2.$$

"$\wedge$" est donc le symbole pour " et ". Par conséquent nous pouvons définir "$\wedge$" par le tableau de vérité suivant:

Définition 10.2 (Conjonction, "$\wedge$") *:*

Tableau 10.1: Définition de la conjonction

Var	A	B	$A \wedge B$
$t(Var)$	0	0	0
	0	1	0
	1	0	0
	1	1	1

La proposition $a :\equiv de \wedge a_1 a_2$ n'est par conséquent vraie que si a_1 aussi bien que a_2 sont vraies. Sinon a est faux!
Remarque: Dans *l'algèbre des circuits électriques* on applique souvent le point de multiplication à la place de "et" (p.ex. $a_1 \cdot a_2$ au lieu de $a_1 \wedge a_2$). Mais dans la logique pure ceci peut causer des *confusions*.
Exemple:

$$(a_1 \wedge a_2) :\equiv \underbrace{(3 \cdot 3 = 9}_{a_1} \wedge \underbrace{6 + 5 = 11)}_{a_2} \not\equiv (3 \cdot 3 = \underbrace{9 \cdot 6 + 5}_{59} = 11)$$

10.3 Adjonction, disjonction (liaison "ou")

Nous étudions encore quelques propositions mathématiques. Celles-ci n'ont pas le désavantage de propositions du langage familier qu'on ne peut pas bien considérer uniquement dans leur réduction abstraite et simple quant à leurs valeurs de vérité, pour des raisons d'habitude. Qui arrive facilement à considérer une proposition comme "Napoléon est mort ou Pierre a une barbe longue" indépendamment de l'intention spécifique? Plus d'un se demandera tout de suite ce que Napoléon a à faire avec la barbe de Pierre — et secouera la tête. Mais une éventuelle relation entre le contenu des deux propositions partielles n'est d'aucun intérêt maintenant! C'est ce que nous voulons finalement ignorer.

Exemples: Nous pouvons accepter tout de suite les valeurs de vérité des propositions composées totales qui suivent ci–dessous. Si non on devrait accepter le contraire, ce qui correspond beaucoup moins au sentiment naturel. Une troisième proposition est impossible, car nous traitons la logique bivalente:

$a :\equiv$ "$2 + 2 = 4$" ou "$3 \cdot 3 = 9$"	(proposition vraie)
$b :\equiv$ "$2 + 2 = 5$" ou "$3 \cdot 3 = 9$"	(proposition vraie)
$c :\equiv$ "$2 + 2 = 4$" ou "$3 \cdot 3 = 6$"	(proposition vraie)
$d :\equiv$ "$2 + 2 = 5$" ou "$3 \cdot 3 = 6$"	(proposition fausse)

Nous pouvons accepter une proposition totale liée par *"ou"* comme *vraie*, dès qu'une proposition partielle est reconnue pour vraie. Lorsque "ou" relie deux propositions, il suffit qu'une soit vraie.

Nous écrivons symboliquement:

$$(a_1, a_2) \mapsto a :\equiv a_1 \vee a_2.$$

Le signe "$\vee$", qui signifie maintenant "ou", symbolise la lettre initiale du mot latin "vel" [1]. "$\wedge$" est le "$\vee$" renversé. Maintenant nous pouvons accepter la définition suivante comme raisonnable:

Définition 10.3 (Adjunktion, "$\vee$") *:*

Tableau 10.2: Définition de l'adjonction

Var	A	B	$A \vee B$
$t(Var)$	0	0	0
	0	1	1
	1	0	1
	1	1	1

Remarque quant à la composition du tableau: Il apparaît pratique de choisir l'ordre des valeurs de vérité de A et de B de façon que elles-ci représentent exactement une *énumération des nombres binaires*. Alors on peut lire les lignes sous les variables au début comme nombres binaires. Lors de quatre variables au début, on aurait d'abord 0000, puis 0001, puis 0010, puis 0011, puis 0100, puis 0101 etc. .

1. lat vel. " vel" signifie "ou".

10.4 L' exclusion (liaison "soit – soit / ou – ou")

"Exclusion" signifie ici *ou exclusif*. Si on entend: "La terre est soit une planète — soit elle n'est pas une planète", généralment personne n'a rien à objecter à cela. Mais soyons attentifs maintenant! Ne nous laissons pas séduire par le contenu. Nous ne voulons pas considérer des propositions partielles où, à part la valeur de vérité, la structure du contenu joue un rôle.

Nous écrivons une proposition $a :\equiv a_1$ "soit – ou soit" a_2 comme il suit:

$$(a_1, a_2) \mapsto a :\equiv a_1 \dot{\vee} a_2.$$

Maintenant nous définissons "soit ou – ou" par le tableau de vérité ci–dessous. Retenons qu'en cas de doute la valeur de vérité est à accepter, si personne n'a rien à objecter:

Définition 10.4 (Exclusion, "$\dot{\vee}$") *:*

Tableau 10.3: Définition de l'exclusion

Var	A	B	$A \dot{\vee} B$
$t(Var)$	0	0	0
	0	1	1
	1	0	1
	1	1	0

Cette définition est en accord avec la façon usuelle de raisonner logiquement. Il est difficile d'y contredire.

10.5 La subjonction de propositions indépendantes

Dans ce sous–chapitre il s'agit de propositions du type *si–alors*. "Si la baignoire est pleine, alors l'eau commence à déborder" est un exemple familier d'une telle proposition. – Mais exactement de tels exemples familiers ne nous servent à rien dans la logique mathématique parce qu'entre les parties de la phrase il existe une relation du contenu et non une relation purement formelle. (L'eau de la baignoire exige la baignoire.) Ici nous ne voulons *pas* examiner spécialement les propositions "si–alors" liées quant au contenu.

Il s'agit plutôt de composer des propositions par des propositions qui existent indépendamment les unes des autres. Dit différemment: Nous voulons produire de nouvelles propositions en liant les propositions disponibles par des symboles logiques et en produisant de cette manière de nouvelles propositions. Et nous dérivons les signes (symboles) logiques de conjonctions gammaticales[2]. Dans l'exemple l'eau débordant de la baignoire a à faire nécessairement avec la baignoire: Quant au contenu les propositions ne sont pas indépendantes. La valeur de vérité de la deuxième proposition est ainsi influencée substantiellement par le contenu de la première proposition. D'autre part plus d'un trouvera bizarre si nous essayons de lier des propositions quotidiennes et indépendantes par "si–alors". Exemple: "Si la lune a des oreilles, mon oncle réussit à faire un saut de 40 mètres". Chacun ressentira propablement une telle liaison de propositions comme un *non–sens*, parce que contraire à l'usage quotidien. Ici naturellement les propositions partielles sont indépendantes. Mais pourquoi dire: "Si la lune a des oreilles"? — Si l'on respecte la réalité physique, il s'agit ici d'une proposition fausse. Mais toutefois d'une proposition. Mais sur un dessin d'enfant, on peut même découvrir une chose pareille et par conséquent là c'est vrai. — Comment devrait–on juger par conséquent la valeur de vérité d'une proposition composée, si déjà le contenu non essentiel nous cause énormément de peine? De telles constructions sont inhabituelles et inaccoutumées dans le langage familier. Souvent nous reconnaissons la deuxième partie de propositions de la langue parlée comme la spécialisation de la première partie, c.–à.–d. nous constatons une liaison interne. Par contre dans le monde des contes:"Blanche-Neige est devenue vieille. Par conséquent elle a été mangé par le loup." Comment

2. Conjonction: C'est une des 10 espèces de mots.

est-ce qu'on veut argumenter contre cela?
Comment traiter des propositions mathématiques dont une est indépendante de l'autre? La disposition suivante offre une méthode: Si nous trouvons une proposition drôle et ne pouvons pas tout de suite l'accepter ou la repousser, nous nous demandons si la proposition est donc fausse, et pensons ainsi que le contraire doit donc être vrai. Il y n'a pas de troisième valeur de vérité dans la logique bivalente. Si on ne peut pas accepter la vérité du contraire, c.–à.–d. si on doit la repousser, nous acceptons la proposition.

Prenons par exemple une équation. Ici, il s'agit d'une proposition indépendante, qui peut être vraie ou fausse. De telles équations ne sont pas liées en ce qui concerne le contenu, parce qu'aucune n'est utilisée pour garantir l'existence de l'autre. Ainsi nous obtenons p.ex. des propositions composées de deux équations:

$a :\equiv$ S'il vaut "$2+2=4$", il vaut aussi "$3\cdot 3=9$".	(proposition vraie)
$b :\equiv$ S'il vaut "$2+2=5$", il vaut aussi "$3\cdot 3=9$"	(proposition vraie)
$c :\equiv$ S'il vaut "$2+2=4$", il vaut aussi "$3\cdot 3=6$"	(proposition fausse)
$d :\equiv$ S'il vaut "$2+2=5$", il vaut aussi "$3\cdot 3=6$"	(proposition vraie)

On ne peut rien objecter si quelqu'un conclut quelque chose de vrai ou bien quelque chose de faux d'une proposition fausse. Cela va toujours bien, car le cas, où cela pourrait aller mal, n'existe pas du tout. Sous la condition d'une équation fausse, nous pouvons déduire un équation vraie ou une équation fausse, c.–à.–d. conclure n'importe quoi. Car le cas, dans lequel on trouve et accepte la condition, n'existe pas. Par conséquent ici nous ne pouvons jamais effectuer une conclusion fausse. Par conséquent nous devons accepter *vrai*.
De quelque chose de vrai, nous pouvons naturellement conclure quelque chose de vrai. Mais de quelque chose de vrai nous ne devons jamais déduire quelque chose de faux, ça voudrait dire faire des fautes. Partant de vérités, il ne faut pas pouvoir déduire du non–sens .
Par conséquent nous pouvons définir la liaison "si–alors", marquée symboliquement par le signe " $\Rightarrow$", comme il suit:

Définition 10.5 (Subjonction, "$\Rightarrow$") *:*

Tableau 10.4: Définition de la subjonction

Var	A	B	$A \Rightarrow B$
$t(Var)$	0	0	1
	0	1	1
	1	0	0
	1	1	1

Remarque concernant les flèches: Dans les mathématiques, nous appliquons encore d'autres sortes de flèches: P.ex. $A \mapsto B$ signifie une *application* de A à B. $x \to x_0$ signifie "converger" resp. "raprocher" (constituer une valeur limite) etc.. Au lieu de $A \Rightarrow B$ nous écrivons aussi $B \Leftarrow A$.

Façons d'exprimer: Nous lisons $A \Rightarrow B$ comme "si A vaut, il suit que B vaut aussi". Ou bien comme "si A donc B". Ou "si A est vrai, B est aussi vrai" etc.. Généralement on trouve les expressions *"implication"*, *"implique"*, *"est nécessaire"* ou *"est suffisant"* seulement dans le contexte des subjonctions vraies. (Mais dans les mathématiques, qui depuis Aristote ont toujours été acceptées comme "internationales", les auteurs ont encore la liberté de constituer un lexique raisonnable et adapté à la situation en question. La conséquence en est malheureusement que tous n'appliquent pas exactement la même langue, ce qui crée rarement des inconvénients. Cela ne joue aucun rôle, car les bons mathématiciens livrent leur langue technique directement avec la théorie, et d'autres bons mathématiciens réussissent à les comprendre.)

10.6 La bijonction de propositions indépendantes

Sous "bijonction" on entend les *liaisons précisément (exactement)–quand–alors–si*. Les exemples suivants peuvent clarifier la situation concernant les valeurs de vérité. Considérons que nous utilisons de nouveau des propositions indépendantes en ce qui concerne le contenu, parce que seulement les valeurs de vérité et la liaison logique "précisément–quand–alors–si" sont importants et non pas la relation qu'on a éventuellement quant au contenu.

$a :\equiv$ "$2+2=4$" exactement si "$3\cdot 3=9$".	(proposition vraie)
$b :\equiv$ "$2+2=5$" exactement si "$3\cdot 3=9$"	(proposition fausse)
$c :\equiv$ "$2+2=4$" exactement si "$3\cdot 3=6$"	(proposition fausse)
$d :\equiv$ "$2+2=5$" exactement si "$3\cdot 3=6$"	(proposition vraie)

Si on juge correcte la dernière ligne, c.–à.–d. "incorrect quand 'exactement si' faux", nous ne pouvons rien objecter à cela. Car on ne peut repousser cette exactitude. Ainsi on doit l'accepter. Symboliquement nous utilisons pour "exactement si alors" le signe " $\Leftrightarrow$". Nous définissons la liaison logique comme il suit:

Définition 10.6 (Bijonction, "$\Leftrightarrow$") *:*

Tableau 10.5: Définition de la Bijonction

Var	A	B	$A \Leftrightarrow B$
$t(Var)$	0	0	1
	0	1	0
	1	0	0
	1	1	1

Remarque: Maintenant il paraît raisonnable de donner des noms aux symboles ou aux signes introduits, qui signifient une certaine liaison. Par conséquent nous employons les notions suivantes:

Explication de la notion 5 (Symboles logiques) *:*
Nous appelons les symboles ou signes de liaison $\neg$, $\wedge$, $\vee$, $\dot{\vee}$, $\Rightarrow$, $\Leftrightarrow$ *des* **symboles logiques**.

Et en outre:
Explication de la notion 6 (Fonctions logiques) *: Par les symboles logiques on applique une nouvelle valeur de vérité à un poids (valeurs de vérité) des variables propositionnelles ainsi liées, c'est la valeur de vérité de la liaison (connection). Une telle application s'appelle* **fonction logique** *ou* **binaire**.

10.7 Parenthèses

Nous considérons deux propositions composées $R \equiv A \wedge B$ et $S \equiv B \vee C$. Maintenant on peut supposer que l'expression $Z \equiv$: $A \wedge B \vee C$ n'est plus univoque. Z pourrait signifier:

$$Z \equiv R \vee C \equiv (A \wedge B) \vee C.$$

Mais il pourrait aussi signifier:

$$Z \equiv A \wedge S \equiv A \wedge (B \vee C).$$

C'est pourquoi nous posons maintenant le problème suivant:

Problème 10.1 *Est-ce qu'une proposition composée a toujours les mêmes valeurs de vérité, même si on déplace les parenthèses?*

Une comparaison à deux poids spécialement choisis pour les expressions susdites montre l'inévidence:

$(A$	$\wedge$	$B)$	$\vee$	C	A	$\wedge$	$(B$	$\vee$	$C)$
0		1		1	0		1		1
$\searrow$		$\swarrow$		$\downarrow$	$\downarrow$		$\searrow$		$\swarrow$
	0			1	0			1	
	$\searrow$			$\swarrow$	$\searrow$			$\swarrow$	
			1			0			$(\neq)$

Résultat: $(A \wedge B) \vee C$ n'a donc pas pour tous les poids possibles la même valeur de vérité comme $A \wedge (B \vee C)$. C'est pourquoi le théorème suivant est valable:

Théorème 10.1 (Parenthèses) *: Pour des propositions composées à plusieurs symboles logiques les parenthèses sont généralement nécessaires.*

Les parenthèses peuvent être donc omises seulement si l'évidence (univocité) ne se perd pas par cela. On connaît déjà le même problème de l'arithmétique avec les nombres. Rappelons–nous la règle là? – "Le point devant le trait!"— Par conséquent ne vaudrait–il pas la peine d'introduire aussi des règles de priorité? Pour faire cela nous définissons:

Définition 10.7 (Règles de priorité) *: Nous déclarons:*

$$\begin{array}{ccc} \neg & \text{lie plus fortement que} & \wedge\,. \\ \wedge & \text{lie plus fortement que} & \vee\,. \\ \vee & \text{lie plus fortement que} & \Rightarrow\,. \\ \Rightarrow & \text{lie plus fortement que} & \Leftrightarrow\,. \end{array}$$

On remarque tout de suite que $\dot{\vee}$ manque dans cette définition. Ça ne fait rien. Nous omettons aussi les symboles logiques définis plus bas dans le texte pour ne pas surcharger la chose maintenant. Dans le cas échéant nous nous débrouillerons avec des parenthèses. La définition susdite suffira donc.
Maintenant on peut se poser encore une deuxième question: Que faire s'il y a dans une expression composée seulement un signe logique unique, mais plusieurs fois le même? Ainsi on peut se demander:

Problème 10.2 *Est-ce qu'une proposition composée telle que p.ex. $A \Rightarrow B \Rightarrow C$ a toujours des valeurs de vérité égales même quand les parenthèses sont rangées de façons différentes?*

Comme en haut nous pouvons nier la question si nous trouvons un poids où on obtient des valeurs de vérité différentes si on pose les parenthèses différemment.
Exemple:

$(A$	$\Rightarrow$	$B)$	$\Rightarrow$	C	A	$\Rightarrow$	$(B$	$\Rightarrow$	$C)$
0		1		0	0		1		0
$\searrow$		$\swarrow$		$\downarrow$	$\downarrow$		$\searrow$		$\swarrow$
	1			0	0			0	
	$\searrow$			$\swarrow$	$\searrow$			$\swarrow$	
			0			1			$(\neq)$

Nous pouvons donc noter:

Théorème 10.2 (Parenthèses pour des symboles logiques différents) *: Généralement les parenthèses sont nécessaires dans les expressions de logique propositionnelle où un symbole logique unique apparaît à plusieurs positions dans l'expression.*

Par contre on peut contrôler la situation suivante à l'aide de tableaux de vérité:

Théorème 10.3 (Parenthèses et uniquement $\wedge$, $\vee$ ou $\Leftrightarrow$) *: Quant aux propositions composées par un seul symbole logique $\wedge$, $\vee$ or $\Leftrightarrow$, les parenthèses ne sont pas nécessaires.*

ça veut dire: $A \wedge B \wedge C$, $A \vee B \vee C$ ou $A \Leftrightarrow B \Leftrightarrow C$ sont des expressions clairement déterminées. N'importe comme nous posons les parenthèses, les valeurs de vérité sont les mêmes à la fin.
Pour pouvoir pourtant simplifier en peu de plus l'orthographe dans ce qui suit, nous convenons l'*associativité de gauche*. Dans une expression cramponnée de gauche nous omettons simplement les parenthèses.
Exemple:

$$((A \Rightarrow B) \Rightarrow C) \Rightarrow D \quad :\equiv \quad A \Rightarrow B \Rightarrow C \Rightarrow D$$

Définition 10.8 (Associativité de gauche) *: Si dans une expression de logique propositionnelle non–univoque il manque les parenthèses, on dit que les parenthèses sont mises en commençant à gauche.*

Exemple:

1. $(\neg A) \vee (B \wedge C) \equiv \neg A \vee B \wedge C$
2. $(\neg A) \wedge (B \vee C) \equiv \neg A \wedge (B \vee C)$

La dernière parenthèse dans l'exemple 2 doit rester!

10.8 Formes propositionnelles

10.8.1 Définition de la notion "Forme propositionnelle"

Soient X_1, X_2, X_3 etc. des variables propositionnelles. Nous voulons maintenant expliquer la notion de *forme propositionnelle de façon récursive* comme il suit:

Définition 10.9 (Forme propositionnelle) *: Une expression*[1] *P s'appelle* **forme propositionnelle**, *s'il vaut:*

1: $P \equiv X_i, (i = 1,2,3,\ldots)$
2: $P \equiv P(X_1,X_2,\ldots) \equiv$ *liaison appropriée d'un nombre fini de variables propositionnelles par des symboles logiques et, il peut y avoir aussi des parenthèses.*

Ici nous entendons par "liaison raisonnable" que chaque parenthèse est fermée des deux côtés, que les symboles logiques sont toujours placés entre des expressions qui sont déjà reconnues comme formes propositionnelles, et que "¬" apparaît toujours devant une forme propositionnelle reconnue de telle manière. Quant à cela naturellement au lieu de X_i on peut aussi rencontrer X, Y, Zetc., car il s'agit seulement de noms.

Exemple: $X, Y, \neg X, X_1 \wedge X_2, \neg X \vee \neg X, (X \vee (Y \wedge \neg Z) \Rightarrow (X \Rightarrow \neg Z))$ etc. .

A l'aide de *tableaux de valeurs de vérité* nous nous faisons un aperçu de tous les poids des variables d'une forme propositionnelle. Ainsi nous pouvons trouver de façon claire la valeur de vérité totale pour chaque poids. Nous formulons le problème conjoint:

Problème 10.3 (Tableau de valeurs de vérité) *: Comment est-ce qu'on réussit à se faire un aperçu de toutes les valeurs de vérité d'une forme propositionnelle au moyen d'un tableau de valeurs de vérité? Comment est-ce qu'on établit un tel tableau?*

Voici un exemple: Nous nous faisons un aperçu des valeurs de vérité de $\neg(X \wedge \neg Y) \Rightarrow Z$:

Tabelle 10.6: Valeurs de vérité de $\neg(X \wedge \neg Y) \Rightarrow Z$

1. P signifie "polynôme"

X	Y	Z	$\neg Y$	$X \wedge \neg Y$	$\neg(X \wedge \neg Y)$	$\neg(X \wedge \neg Y) \Rightarrow Z$
0	0	0	1	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	1	0
0	1	1	0	0	1	1
1	0	0	1	1	0	1
1	0	1	1	1	0	1
1	1	0	0	0	1	0
1	1	1	0	0	1	1

Dans la dernière colonne, nous voyons les *valeurs de vérité totales*. On peut maintenant facilement reconnaître que par un poids des variables propositionnelles X, Y et Z, par des valeurs de vérité, la forme propositionnelle $\neg$,$X \wedge \neg Y$, $\Rightarrow Z$ devient une proposition de forme "forme devient vraie" (valeur 1) ou "forme devient fausse" (valeur 0). Généralement on peut constater:

Constatation: Une valeur de vérité totale d'une forme propositionnelle à un poids donné mène toujours à une *nouvelle proposition*: *"... la forme possède la valeur de vérité ..."*.
En outre le tableau de vérité montre aussi la *fonction de poids* donnée par la forme propositionnelle (aussi fonction de vérité, fonction binaire) c.–à.–d. le classement (application):

$$\{\text{Poids possibles }\} \mapsto \{0, 1\}.$$

Exercices concernant ce sujet p.ex. voir livre d'exercices *DIYMU* Kap. 2 (Bibl.: wirz).

10.8.2 Forme propositionnelle à exactement deux variables propositionnelles

Les formes propositionnelles à exactement deux variables propositionnelles consistent en un symbole logique à deux places qui lie deux parties qui à leur tour sont des formes propositionnelles spéciales. Une telle partie est ou une variable propositionnelle — ou une variable propositionnelle reliée par un symbole logique à une place, par exemple $\neg$. (Plus tard, quand les notions seront introduites, nous dirons "fonction à un argument".) On voit tout de suite qu'il existe *exactement* 4 *symboles logiques à une place*: (1) $\neg$, (2) *identiquement vrai* resp. w (le symbole logique qui assigne toujours à chaque variable la valeur "vrai" resp. 1), (3) *identiquement faux* resp. f (le symbole logique qui assigne toujours à chaque variable la valeur "faux" resp. 0) et (4) *neutre* resp. n (le symbole logique, qui laisse la variable comme elle est. Le tableau correspondant:

Tableau 10.7: Symboles logiques possibles à une place

X	*neutral* X	$\neg X$	w	f
0	0	1	1	0
1	1	0	1	0

On n'a pas d'autres possibilités de combinaison pour les valeurs de vérité. S'appuyant sur ce fait nous pouvons poser maintenant la question importante: Combien de possibilités est-ce qu'il y a pour établir une liaison entre deux variables propositionnelles? On a donc le problème suivant:

Problème 10.4 (Fonctions de poids) *: Fais–toi un aperçu de toutes les fonctions de poids d'une forme propositionnelle qui contient seulement* 2 *variables propositionnelles.*

Quant à cela nous faisons encore un tableau. D'abord nous appelons une liaison totale possible simplement f_i. Le nombre de fonctions possibles résulte du nombre possible de groupes à 4 aux éléments 0 et 1. Ceci est aussi le nombre des nombres binaires de 0000 jusqu'à 1111, c.–à.–d. dans le système décimal le nombre des nombres entiers de 0 jusqu'à $2^4 - 1$ (c.–à.–d. jusqu'à 15). Ça donne 16 possibilités. Pour les représenter toutes, nous choisissons une méthode d'énumération appuyée au système binaire:

Tableau 10.8: Symboles logiques possibles à deux places

X_1	X_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
		f	$\wedge$					$\dot{\vee}$	$\vee$	$\downarrow$	$\Leftrightarrow$				$\Rightarrow$	$\mid$	w

On reconnaît tout de suite: f_0 est la *liaison identiquement fausse*. N'importe quels poids nous prenons, le résultat est toujours faux. Conformément à cela, f_{15} est la *liaison identiquement vraie*. Nous reconnaissons f_1 comme "$\wedge$". f_2 n'a pas encore de nom. On peut interpréter f_2 comme $\neg(X_1 \Rightarrow X_2)$ ou bien comme $X_1 \wedge \neg X_2$. Aussi f_8 et f_{14} sont des liaisons importantes qui portent des noms:

Définition 10.10 (Liaison de Nicod, trait de Scheffer, W et F) *:*
f_0 *s'appelle liaison* **identiquement fausse** F, f_{15} *s'appelle* **identiquement vraie** W. f_8 *s'appelle liaison de* **Nicod** ($\downarrow$) *et* f_{14} *est le trait de Scheffer* ($\mid$) .

Remarque: Dans *l'algèbre des circuits* la liaison de Nicod correspond au NOR et le trait de Scheffer au $NAND$. Le trait de Scheffer "$\mid$" s'écrit aussi de cette façon "$\uparrow$".

10.8.3 Négation double, règles de De Morgan

"Ne pas *ne pas dire la vérité*" signifie, du point de vu de notre savoir actuel "dire clairement la vérité". Nous rencontrons ici *la négation double* ("ne pas ... ne pas ..." . Dans la logique propositionnelle on peut prouver par le moyen du tableau de vérité que cette négation double est une "affirmation". Il vaut le théorème:

Théorème 10.4 (Négation double) *:* $A \equiv \neg\neg A$.

Preuve: Nous prouvons la chose au moyen du tableau de vérité. Si les valeurs de vérité concordent ligne par ligne, la chose est attestée. Nous voyons tout de suite que la première et la troisième colonne concordent, le théorème ainsi est *vrai*:

Tableau 10.8: Négation double

A	$\neg A$	$\neg\neg A$
0	1	0
1	0	1

Maintenant si on examine des liaisons $\wedge$ – ainsi que $\vee$ niées, on trouve les règles de *De Morgan*:

Tableau 10.9: De Morgan

A	B	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$\neg(\neg A \wedge \neg B)$	$A \vee B$
0	0	1	1	1	0	0
0	1	1	0	0	1	1
1	0	0	1	0	1	1
1	1	0	0	0	1	1

Des deux dernières colonnes et à cause de la négation double on voit:

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

On prouve également:

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

Si nous prenons au lieu de A donc $\neg X_1$ et au lieu de B donc $\neg X_2$, nous pouvons écrire à cause de la négation double:

Théorème 10.5 (De Morgan) *:*

1. $\neg(X_1 \wedge X_2) \equiv \neg X_1 \vee \neg X_2$,
2. $\neg(X_1 \vee X_2) \equiv \neg X_1 \wedge \neg X_2$.

10.8.4 Formes prop. à plusieurs var. prop. et des symboles logiques inconnus

On regarde le tableau 10 ci–dessus, on doit p.ex. se demander, si et comment f_{11} pourrait être exprimé par d'autres symboles logiques. Qu'une chose pareille est toujours possible, cela se laisse exprimer par le *lemme* suivant:

Lemme 10.1 (Réduction aux symboles logiques habituels) *: Chaque forme propositionnelle est représentable par une fonction de vérité $f(X_1,X_2,\ldots)$, c.–à.–d. par une* **forme remplaçante** *dans laquelle il n'apparaît que les trois symboles logiques $\neg$, $\wedge$ ainsi que $\vee$.*

Quant à la preuve: Nous pouvons accepter le théorème après avoir montré la méthode par laquelle on obtient la forme remplaçnte par déduction. Comme il n'existe aucune limite à l'application de cette méthode, ça doit fonctionner dans tous les cas. Nous le montrons par l'exemple de f_{11}:

Tableau 10.11: Examen de f_{11}

X_1	X_2	$f(X_1,X_2)=f_{11}$	$\neg X_1$	$\neg X_2$	$\neg X_1 \wedge \neg X_2$	$X_1 \wedge \neg X_2$	$X_1 \wedge X_2$	$(\neg X_1 \wedge \neg X_2) \vee (X_1 \wedge \neg X_2) \vee (X_1 \wedge X_2)$
0	0	1	1	1	1	0	0	1
0	1	0	1	0	0	0	0	0
1	0	1	0	1	0	1	0	1
1	1	1	0	0	0	0	1	1

$f(X_1,X_2)=f_{11}$ est seulement vrai, si on a le cas des poids de la ligne 1 — ou ceux de la ligne 3 resp. 4. Sinon f_{11} est faux, car dans la dernière colonne, il faut avoir la valeur 1. Mais le poids de la ligne 1 apparaît, si X_1 possède la valeur 0 et X_2 aussi la valeur 0, c.–à.–d. si $\neg X_1$ possède la valeur 1 et $\neg X_2$ aussi la valeur 1. Correspondamment on a le poids de la ligne 3 si X_1 possède la valeur 1 et X_2 la valeur 0, c.–à.–d. si $\neg X_2$ possède la valeur 1. Egalement on obtient le poids de la ligne 4, si X_1 a la valeur 1 et X_2 aussi la valeur 1. C.–à.–d. $f(X_1,X_2)=f_{11}$ est vrai, si $\neg X_1$ possède la valeur 1 et $\neg X_2$ a aussi la valeur 1 — ou si X_1 possède la valeur 1 et $\neg X_2$ simultanément aussi la valeur 1 — ou si X_1 possède la valeur 1 et X_2 aussi la valeur 1. Sinon $f(X_1,X_2)=f_{11}$ est faux. On obtient exactement les mêmes valeurs de vérité, si on fait la liaison par $\vee$ ("ou") entre $\neg X_1 \wedge \neg X_2$ (vrai seulement dans le cas de la ligne 1), $X_1 \wedge \neg X_2$ (vrai seulement dans le cas de la ligne 3) et $X_1 \wedge X_2$ (vrai seulement dans le cas de la ligne 4), (voir dernière colonne). Par conséquent on voit qu'il vaut:

$$f(X_1,X_2)=f_{11} \equiv (\neg X_1 \wedge \neg X_2) \vee (X_1 \wedge \neg X_2) \vee (X_1 \wedge X_2).$$

Dans la dernière expression, on a seulement les symboles logiques $\neg$, $\wedge$ et $\vee$.
Cette expression n'est pas univoque! Car on peut argumenter aussi comme il suit:

$f(X_1,X_2)=f_{11}$ est faux, c.–à.–d. $\neg f(X_1,X_2)=\neg f_{11}$ est vrai, exactement quand on a le poids de la ligne. C'est donc le cas, si X_1 a la valeur 0 et X_2 la valeur 1, c.–à.–d. si $\neg X_1$ a la valeur 1 et X_2 a aussi la valeur 1. C'est alors exactement le cas, si $\neg X_1 \wedge X_2$ est vrai. Comme nous allons prouver plus tard, c'est exactement le cas, si $\neg(\neg X_1 \wedge X_2)$ est faux. $\neg(\neg X_1 \wedge X_2)$ et $f(X_1,X_2)=f_{11}$ sont donc faux en conformité. Par conséquent on obtient:

$$f(X_1,X_2)=f_{11} \equiv \neg(\neg X_1 \wedge X_2) \equiv X_1 \vee \neg X_2.$$

On obtient la dernière transformation d'après les *règles de De Morgan*, que nous prouverons plus tard. Nous retenons donc:

Corollaire 10.1 (Non–univocité de la représentation à l'aide de symboles logiques habituels) *La représentation d'une expression à l'aide des symboles logiques $\neg$, $\wedge$ ainsi que $\vee$ n'est pas univoque.*

Par conséquent nous pouvons utiliser la méthode suivante pour la construction d'une forme de remplacement qui ne possède que les symboles logiques $\neg$, $\wedge$ ainsi que $\vee$:

Méthode 10.1 (Construction d'une forme de remplacement) *: Nous prenons toutes les lignes dans lesquelles la forme propositionnelle envisagée a la valeur de vérité* 1 *et établissons une liaison* $\wedge$ *pour chacune de ces lignes. Pour les variables propositionnelles* X_i*, qui ont devant la valeur de vérité* 1*, nous écrivons* X_i*. Par contre pour les autres nous écrivons* $\neg X_i$*. Nous lions les expressions, ainsi obtenues pour les lignes, par* $\vee$*.*

Encore un exemple: Soit donné $g(X_1,X_2,X_3)$ par le tableau suivant. Construire une forme de remplacement par $\neg$ $\wedge$ et $\vee$!

Tableau 10.12: Forme de remplacement de $g(X_1,X_2,X_3)$

X_1	X_2	X_3	$g(X_1,X_2,X_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

D'après la méthode indiquée en haut nous pouvons lire:

$$g(X_1,X_2,X_3) \equiv \underbrace{(\neg X_1 \wedge \neg X_2 \wedge \neg X_3)}_{\text{De la ligne 1}} \vee \underbrace{(\neg X_1 \wedge X_2 \wedge X_3)}_{\text{De la ligne 2}} \vee (X_1 \wedge \neg X_2 \wedge X_3) \vee (X_1 \wedge X_2 \wedge X_3).$$

10.9 Bases d'opérations logiques (de compositions)

Nous avons vu dans 10.8.4 que nous pouvons représenter une forme propositionnelle quelconque sans utiliser d'autres symboles logiques que $\neg$, $\wedge$ ainsi que $\vee$. Un tel ensemble de symboles logiques (comme en haut $\{\neg, \wedge, \vee\}$) s'appelle *base de compositions*. Généralement nous définissons:

Définition 10.11 (Base de compositions) *: Un ensemble de symboles logiques qui suffisent de représenter chaque fonction de vérité comme forme propositionnelle s'appelle* **base de compositions**.

Par 10.8.3 nous savons qu'il vaut:

1. $X_1 \vee X_2 \equiv \neg(\neg X_1 \wedge \neg X_2)$,
2. $X_1 \wedge X_2 \equiv \neg(\neg X_1 \vee \neg X_2)$.

Par conséquent nous pouvons remplacer $\vee$ par $\neg$, $\wedge$ et des parenthèses. Egalement nous pouvons échanger le symbole logique $\wedge$ par les symboles logiques $\neg$, $\vee$ ainsi que des parenthèses. Donc $\{\neg, \wedge\}$ ainsi que $\{\neg, \vee\}$ sont des bases de compositions. On peut vérifier au moyen de tableaux de vérité que le théorème suivant vaut:

Théorème 10.6 (Remplacement de la subjonction) *: Il vaut:*

$$X_1 \Rightarrow X_2 \equiv \neg(X_1 \wedge \neg X_2) \equiv \neg X_1 \vee X_2.$$

A cause de la négation double, on peut par conséquent toujours remplacer $\{\neg, \wedge\}$ et $\{\neg, \vee\}$ par $\{\neg, \Rightarrow\}$. C.–à..-d. il vaut le théorème:

Théorème 10.7 (Bases de compositions) *:* $\{\neg, \wedge\}$, $\{\neg, \vee\}$ *et* $\{\neg, \Rightarrow\}$ *sont des bases de compositions.*

On peut être étonné de voir que si peu de symboles logiques suffisent pour représenter toutes les formes propositionnelles. Mais on peut encore aller plus loin. Nous définissons:

Définition 10.12 (Bases de compositions élémentaires) *: Un symbole logique forme une* **base de compositions élémentaire***, si on peut représenter toutes les formes propositionnelles à un nombre fini de variables propositionnelles par ce symbole seul et à l'aide de parenthèses.*

Il est intéressant que le théorème suivant vaut:

Théorème 10.8 (Représentation par des bases de liaisons élémentaires) *:* $\{\uparrow\}$ *et* $\{\downarrow\}$ *(le trait de Scheffer et la liaison de Nicod) sont les bases de compositions élémentaires uniques.*

Quant à la preuve: Le lemme suivant montre que $\{\uparrow\}$ et $\{\downarrow\}$ sont des bases de compositions élémentaires. (On prouve cela facilement par une vérification à l'aide de tableaux de vérité):

Lemme 10.2 (Possibilité de représentation par {↑} und {↓}) *:*

$$\begin{array}{rcl@{\qquad}rcl} \neg A & \equiv & A \uparrow A & \neg A & \equiv & A \downarrow A \\ A \vee B & \equiv & A \uparrow A \uparrow (B \uparrow B) & A \wedge B & \equiv & A \downarrow A \downarrow (B \downarrow B) \end{array}$$

On peut démontrer qu'il n'y a pas d'autres bases de compositions élémentaires en plus. Quant à cela il faut montrer que ni $\{\uparrow\}$ ni $\{\downarrow\}$ ne peuvent être représentés par aucun troisième symbole logique. Démontrer cela prendrait trop de temps.

10.10 Tautologies, contradictions, équivalences, implications

Dans ce sous–chapitre, nous voulons étudier quelques *formes propositionnelles spéciales*. Nous commençons par la *tautologie*.

10.10.1 Tautologies

Nous définissons

Définition 10.13 (Tautologie) *: Une forme propositionnelle, qui est vraie à chaque poids, s'appelle* **tautologie** *(ou forme propositionnelle identiquement vraie ou généralement valable).*

Exemples:

Tableau 10.13: Les formes propositionnelles suivantes sont des tautologies:

1.1	$A \Rightarrow A$	1.2	$A \Rightarrow \neg\neg A$
2.1	$A \vee \neg A$	2.2	$\neg(A \wedge \neg A)$
3.1	$A \vee B \Leftrightarrow B \vee A$	3.2	$A \wedge B \Leftrightarrow B \wedge A$
4.1	$\neg(A \vee B) \Leftrightarrow \neg B \wedge \neg A$	4.2	$\neg(A \wedge B) \Leftrightarrow \neg B \vee \neg A$
5.1	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	5.2	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
6.1	$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$	6.2	$A \Leftrightarrow \neg(\neg A)$

On vérifie cette chose par le moyen du tableau de vérité. P.ex. pour 1.1 comme suit:

A	A	$A \Rightarrow A$	
0	0	1	
1	1	1	*q. e. d.*

Définition 10.14 (Contradiction) *: Une forme propositionnelle, qui est fausse à chaque poids, s'appelle* **contradiction***, ou bien proposition identiquement fausse.*

Exemples: Les formes propositionnelles suivantes sont des contradictions:

$$A \wedge \neg A \text{ sowie } (A \vee B) \wedge \neg A \wedge \neg B \text{ etc. .}$$

Vérification pour le premier exemple:

A	A	$A \Rightarrow A$	$\neg(A \Rightarrow A)$
0	0	1	0
1	1	1	0

q. e. d.

Une tautologie est toujours vraie, une contradiction est toujours fausse (également comme "$\neg$ une tautologie"). Par conséquent le théorème suivant vaut (c'est trivial):

Théorème 10.9 (Rapport entre tautologie et contradiction) *: $P(X_1,X_2,\ldots)$ est tautologie exactement quand $\neg P(X_1,X_2,\ldots)$ est contradiction.*

Lors d'une tautologie $P(X_1(X_2,\ldots)$ le poids ne joue pas un rôle. On peut placer n'importe quelles valeurs de vérité pour les X_i, la forme propositionnelle reste vraie. Si on remplace donc les variables propositionnelles X_i par de nouvelles formes propositionnelles $P_i(X_1,X_2,\ldots)$ et y applique comme poids des valeurs de vérité, on a comme résultats des poids des nouvelles formes propositionnelles P_i simplement un autre poids de la forme propositionnelle P d'origine qui est, comme on sait, une tautologie. Cela ne change en rien la tautologie, car celle-ci est toujours vraie. Par conséquent on peut donc noter le théorème suivant:

Théorème 10.10 (Remplacement d'une variable propositionnelle d'une tautologie) *:*

Hyp.: Soit $P(X_1,X_2,\ldots)$ tautologie ainsi que P_1,P_2,P_3 d. formes prop. quelc.
$(P_i \equiv P_i(X_1,X_2,\ldots)$.
Th.: $P(P_1,P_2,\ldots)$ est de nouveau tautologie.

Exemple: $(A \vee B) \Leftrightarrow (B \vee A)$ est tautologie. Donc
$((\underbrace{\neg A \wedge B}) \vee B) \Leftrightarrow (B \vee (\underbrace{\neg A \wedge B}))$ est aussi tautologie.

Ici A a été remplacé par $(\underbrace{\neg A \wedge B})$. La nouvelle expression reste une tautologie.

10.10.2 Equivalences

Définition 10.15 (Equivalence) *: Deux formes propositionnelles $P(X_1,\ldots,X_n)$ et $Q(X_1,\ldots,X_n)$ s'appellent* **équivalentes***, si $P(X_1,\ldots,X_n) \Leftrightarrow Q(X_1,\ldots,X_n)$ est une tautologie.*

Si $P(X_1,\ldots,X_n)$ und $Q(X_1,\ldots,X_n)$ sont équivalentes, nous écrivons $P(X_1,\ldots,X_n) \equiv Q(X_1,\ldots,X_n)$. $P(X_1,\ldots,X_n) \equiv Q(X_1,\ldots,X_n)$ signifie donc que $P(X_1,\ldots,X_n) \Leftrightarrow Q(X_1,\ldots,X_n)$ sont toujours vrais. Ça veut dire que $P(X_1,\ldots,X_n)$ est vrai (ou faux) exactement quand $Q(X_1,\ldots,X_n)$ est vrai (ou faux).

10.10.3 Implication

Définition 10.16 (Implication) *: La forme propositionnelle $P(X_1,\ldots,X_n)$***implique** *la forme propositionnelle $Q(X_1,\ldots,X_n)$, si $P(X_1,\ldots,X_n) \Rightarrow Q(X_1,\ldots,X_n)$ est une tautologie.*

Exemples: 1) $A \Rightarrow A$ 3) $A \wedge B \Rightarrow A$
2) $A \Rightarrow A \vee B$ 3) $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

Dans une implication $P \Rightarrow Q$ on ne peut ni échanger les formes propositionnelles A et B de façon quelconque ni y ajouter des $\neg$ comme on veut. Mais quand même de tels changements ont une signification pratique. Pour simplifier l'usage de la langue on a introduit par conséquent les noms suivants:

Définition 10.17 (Conversion, inversion, contraposition) *: Soit donné $P \Rightarrow Q$.*
L'expression $Q \Rightarrow P$ s'appelle **conversion** *de $P \Rightarrow Q$. L'expression $\neg P \Rightarrow \neg Q$ s'appelle* **inversion** *de $P \Rightarrow Q$. $\neg Q \Rightarrow \neg P$ s'appelle* **contraposition** *ou bien* **transposition** *de $P \Rightarrow Q$.*

Le théorème important, fréquemment utilisé dans la technique mathématique de la preuve, vaut:

Théorème 10.11 (Preuve indirecte) *:*

$$\neg Q \Rightarrow \neg P \qquad \equiv \qquad P \Rightarrow Q$$

On peut rapidement vérifier cette équivalence à l'aide d'un tableau de vérité. (C'est un bon exercice de le faire ....) Pour la technique mathématique de la preuve il est important de pouvoir vérifier $\neg Q \Rightarrow \neg P$ au lieu de prouver $P \Rightarrow Q$. Ça peut apporter des simplifications.

10.10.4 Equivalences importantes

Les lois suivantes jouent un rôle important lors de transformations logiques et quand il s'agit de prouver. On les vérifie le plus simplement à l'aide de tableaux de vérité. *Indication: On fait l'exercice soi–même ...*

(1)	Lois de la négation double	$\neg\neg A$	$\equiv$	A
(2)	Idempotence	$A \vee A$	$\equiv$	A
		$A \wedge A$	$\equiv$	A
(3)	Associativité	$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$
		$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$
(4)	Commutativité	$A \vee B$	$\equiv$	$B \vee A$
		$A \wedge B$	$\equiv$	$B \wedge A$
(5)	Distributivité	$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$
		$A \wedge (B \vee C)$	$\equiv$	$A \wedge B) \vee (A \wedge C)$
(6)	Elément neutre	$A \vee F$	$\equiv$	A
		$A \wedge W$	$\equiv$	A
(7)	Adjonction forcée	$A \vee W$	$\equiv$	W
	Conjonction forcée	$A \wedge F$	$\equiv$	F
(8)	Complementarité:			
	Troisième exclu	$A \vee \neg A$	$\equiv$	W
	Lois de la contradiction	$A \wedge \neg A$	$\equiv$	F
(9)	Dualité	$\neg W$	$\equiv$	F
		$\neg F$	$\equiv$	W
(10)	De Morgan	$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$
		$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$
(11)	Lois de l'absorption	$A \vee (A \wedge B)$	$\equiv$	A
		$A \wedge (A \vee B)$	$\equiv$	A
		$(A \wedge B) \vee \neg B$	$\equiv$	$A \vee \neg B$
		$(A \vee B) \wedge \neg B$	$\equiv$	$A \wedge \neg B$
(12)	Contraposition	$A \Rightarrow B$	$\equiv$	$\neg B \Rightarrow \neg A$
(13)	Dualiser la contraposition	$A \Leftrightarrow W$	$\equiv$	$\neg A \Leftrightarrow F$
(14)	Remplacer la subjonction	$A \Rightarrow B$	$\equiv$	$\neg A \vee B$
		$A \Rightarrow B$	$\equiv$	$\neg(A \wedge B)$
(15)	Remplacer la bijonction	$A \Leftrightarrow B$	$\equiv$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
(16)	Ex falso quodlibet	$F \Rightarrow A$	$\equiv$	W
(17)	Ex quodlibet verum	$A \Rightarrow \mathrm{W}$	$\equiv$	W
(18)	Conjonction affaiblie	$(A \wedge B) \Rightarrow A$	$\equiv$	W
(19)	Adjonction affaiblie	$A \Rightarrow (A \vee B)$	$\equiv$	W
(20)	Première partie niée	$\neg A \Rightarrow (A \Rightarrow B)$	$\equiv$	W
(21)	Dernière partie niée	$B \Rightarrow (A \Rightarrow B)$	$\equiv$	W
(22)	Conjonction implique disjonction	$(A \vee B) \Rightarrow (A \vee B)$	$\equiv$	W
(23)	Modus ponens	$(A \wedge (A \Rightarrow B)) \Rightarrow B)$	$\equiv$	W
(24)	Modus tollens	$(\neg B \wedge (A \Rightarrow B)) \Rightarrow \neg A)$	$\equiv$	W
(25)	lois de la transitivité	$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$	$\equiv$	W
(26)	Distinction des cas	$((A \vee B) \wedge ((A \Rightarrow C)) \wedge (B \Rightarrow C)) \Rightarrow C$	$\equiv$	W

10.11 Conclusions logiques

Ici, nous voulons gagner une vue partielle dans la *nature des conclusions logiques* ou des *preuves logiques* par une courte digression.
Soyent P_1,P_2,...,P_n et Q des formes propositionnelles. Souvent le problème suivant apparaît:

Problème 10.5 (Conclusions logiques) *:*
Il est essentiel de savoir, si Q est déduisible de P_1,P_2,...,P_n.

Nous écrivons de façon symbolique: $P_1,P_2,\ldots,P_n \vdash Q$.

Pour pouvoir mieux traiter le problème, nous introduisons le langage suivant:

Explication de la notion 7 (Prémisses, conclusion) *: Dans le problème qu'on vient de mentionner,* $P_1,P_2,\ldots,P_n$ *s'appellent les* **prémisses** *(hypothèses),* Q *s'appelle la* **conclusion** *(thèse) et* $P_1,P_2,\ldots,P_n \vdash Q$ *s'appelle* **déduction logique**.

Dans la logique bivalente, une conclusion logique ou une déduction logique peuvent de nouveau être vraies ou fausses. Les conclusions fausses sont une contrariété qu'il faut éviter. Les conclusions vraies nous intéressent particulièrement. Par conséquent nous définissons:

Définition 10.18 (Déduction logique correcte) *:* $P_1,P_2,\ldots,P_n \vdash Q$ *s'appelle* **déduction (conclusion) logique correcte**, *si* $(P_1 \wedge P_2 \wedge \ldots \wedge P_n \Rightarrow Q)$ *est une tautologie.*

Ainsi dans une déduction logique et correcte, la conjonction des prémisses implique la conclusion.

Exemple: Nous voulons montrer que $A,A \Rightarrow B \vdash B$ est vrai, c.–à.–d. $A,A \Rightarrow B \vdash B$ est une déduction logique correcte. Nous devons enfin montrer que $(A \wedge A \Rightarrow B) \Rightarrow B$ est une tautologie. Faisons–le à l'appui d'un tableau:

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	$(A \wedge A \Rightarrow B) \Rightarrow B$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

$(A \wedge A \Rightarrow B) \Rightarrow B$ est donc vrai dans tous les cas possibles. L'expression examinée est donc une tautologie. Peut-être vous l'avez retenu – c'est le modus ponens.
La signification du modus ponens (règle de séparation) se trouve dans la conséquence suivante: Pour montrer qu'une proposition B est vraie, on peut aussi montrer qu'une autre proposition A quelconque ainsi que la subjonction $A \Rightarrow B$ sont vraies. On rencontre des telles situations dans un "théorème mathématique" . Car un tel théorème a souvent la structure abstraite suivante:

Théor.:	**Hypothèse:**	Propos. $a_1 \wedge a_2 \wedge \ldots \wedge a_n$	Bref:	**Thé.:**	**Hyp.:**	$a_1 \wedge a_2 \wedge \ldots \wedge a_n$
	Thèse:	Propos. b			**Thè.:**	b

On affirme donc que — si la condition (hypothèse) est vraie, l'affirmation (thèse) aussi est vraie (c.–à.–d. elle ne peut jamais être fausse). Si la condition par contre est fausse, personne ne s'intéresse sérieusement à l'affirmation. C.-.à.–d. elle peut être vraie ou fausse, une hypothèse fausse, qui n'arrive jamais, n'importe pas. Par conséquent pour prouver le théorème on doit prouver la subjonction $a \Rightarrow b$ comme vraie. Ici cette subjonction n'apparaît pas dans la signification d'une forme propositionnelle. Pour le lecteur du théorème mathématique elle est plutot une proposition ou bien une déclaration. Par conséquent dans le cas d'une preuve on doit seulement démontrer que le cas "$a_1 \wedge a_2 \wedge \ldots \wedge a_n$ vrai et b vrai" est vrai. Ici il faut donc déduire b de $a_1 \wedge a_2 \wedge \ldots \wedge a_n$ de la façon de la logique correcte.
Nous nous rendons compte de ce fait par l'exemple suivant:

Théorème 10.12 (Paradigme de la géométrie) [3]*:*
Hyp.: *Pour les droites* g_i *il vaut:* $g_1 \| g_2$ *(proposition* a_1*) et* $g_1 \perp g_3$ *(proposition* a_2*).*
Thè.: *Il vaut toujours encore* $g_2 \perp g_3$ *(proposition* b*).*

3. Un paradigme est un exemple dont on apprend.

D'autres déductions logiques:	(1)	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$\vdash$	$(A \Rightarrow C)$
	(2)	$(A \Rightarrow \neg B) \wedge B$	$\vdash$	$\neg A$
Paralogismes:	(1)	$(A \Rightarrow B) \wedge B$	$\vdash$	A
	(2)	$(A \Rightarrow B) \wedge \neg A$	$\vdash$	$\neg B$

Les paralogismes naissent quand on se laisse tromper par le "langage familier inexact et superficiel". Attention: Les paralogismes mènent à des fautes!
Indication: Contrôler si les paralogismes susdits sont faux, c'est un bon exercice.

10.12 La notation polonaise

10.12.1 Origine et sens

Au début, dans le contexte des examens théoriques, la question suivante est devenue actuelle: Est–ce qu'il existe une écriture unidimensionnelle ainsi qu'une façon de lire unidimensionelle – sans l'exigence *de parenthèses*? A l'aide d'une telle écriture et possibilité de lire unidimensionnelles on devrait pouvoir écrire et lire des formes propositionnelles p.ex. aussi par une machine. Une telle machine écrit ou lit seulement un signe à la fois. Après elle passe toujours dans la même direction au signe prochain, mais elle n'a cependant aucune possibilité de rétrograder le dispositif qui lit ou qui écrit. Une telle machine ne devrait pas retenir encore parallèlement une place à laquelle une parenthèse a été ouverte, qu'il faudra refermer plus tard. Ce principe est naturellement important aujourd'hui dans le contexte de la construction d'ordinateurs. Un exemple d'une telle machine abstraite est la *machine de Turing*, nommée d'après l'Anglais Turing (première moitié du 20ème siècle). Le Polonais J. Lukasiewicz a proposé une telle orthographe qui fonctionne: La *notation polonaise*. A l'aide de cette notation les parenthèses sont superflues.
Mais on reconnaît rapidement, que les parenthèses sont indispensables pour l'homme en particulier pour lire, autrement il est extrêmement difficile d'obtenir une vue d'ensemble précise. L'homme a une vue tridimensionnelle. Il ne fonctionne pas de façon unidimensionnelle comme une de ces machines qu'on vient de décrire.
En effet certains producteurs (en particulier de calculatrices) utilisent encore aujourd'hui le principe de l'orthographe polonaise sans parenthèses dans des circonstances diverses en forme modifiée. (Nous connaissons par exemple *la notation polonaise inverse* chez HP.)

10.12.2 Règles quant à la notation polonaise

Cette chose est expliquée ci–dessus par des exemples avec les symboles logiques les plus fréquents. Le principe ainsi expliqué peut être adapté sans peine aux autres symboles logiques.
Exemples:

$$\begin{array}{rcl} \neg A & \equiv & \neg A \\ A \wedge B & \equiv & \wedge AB \\ A \vee B & \equiv & \vee AB \\ A \Rightarrow B & \equiv & \Rightarrow AB \\ A \Leftrightarrow B & \equiv & \Leftrightarrow AB \end{array}$$

On en reconnaît le procédé suivant:

Méthode 10.2 (Notation polonaise) *: Un symbole logique, qui dans la notation normale est placé entre deux propositions ou formes propositionnelles, est écrit en tête dans la notation polonaise.*

Exemples:

$$\begin{array}{rcl} ((\neg A) \wedge (B \vee A)) & \equiv & \wedge \neg A \vee BA \\ A \Rightarrow ((\neg B) \Leftrightarrow (A \vee C)) & \equiv & \Rightarrow A \Leftrightarrow \neg B \vee AC \\ (A \vee B) \Rightarrow ((\neg C) \vee ((\neg B) \wedge C)) & \equiv & \Rightarrow \vee AB \vee \neg C \wedge \neg BC \end{array}$$

Comme le principe de placer en tête le symbole logique ne dépend pas du symbole logique, il vaut aussi pour le trait de Scheffer et aussi pour la liaison de Nicod. Ces deux symboles logiques forment les *bases de*

compositions élémentaires uniques, c.–à.–d. chaque forme propositionnelle peut s'écrire seulement avec un de ces symboles. A l'aide de la notation polonaise, il est possible d'éviter les parenthèses. Par conséquent nous pouvons conclure:

Théorème 10.13 (Représentat. la plus élémentaire d'une forme propos. resp. d'une prop.) *:*
Chaque forme propositionnelle resp. chaque proposition peut s'écrire seulement à l'aide de $\uparrow$ *et des variables propositionnelles resp. des propositions élémentaires. Egalement chaque forme propositionnelle resp. chaque proposition peut s'écrire seulement avec* $\downarrow$ *et des variables propositionnelles resp. des propositions élémentaires.*

La conséquence est que, à part les variables propositionnelles et les propositions élémentaires, un seul symbole logique suffit pour pouvoir écrire chaque expression de la logique propositionnelle.

Chapitre 11

Formes normales de la logique propositionnelle

11.1 Sujet, application pratique

Dans le dernier chapitre, nous avons étudié le problème suivant: Il était donné une forme propositionnelle. Pour cette forme propositionnelle, il fallait trouver tous les poids possibles. On devait donc trouver le tableau de vérité. Nous avons vu que des formes propositionnelles extérieurement différentes peuvent avoir le même tableau de vérité.
Mais dans la pratique, on a souvent le problème inverse: Soit donné un tableau de vérité. On devrait trouver une forme propositionnelle qui va avec ce tableau de vérité donné. *Des formes normales de la logique propositionnelle* sont des formes propositionnelles spéciales et composées, à l'aide desquelles on peut très vite trouver la solution d'un tel problème. C'est important pour la pratique.
Parfois on utilise les formes normales aussi ailleurs: Pour comparer deux formes propositionnelles, on peut recourir au tableau de vérité. Mais il y a encore une méthode. Pour les deux formes propositionnelles données (à comparer), on cherche un certain type de forme normale standardisé, la *forme normale canonique* , aussi *forme normale complète* . Si les deux formes normales canoniques sont identiques, horsmis l'ordre des termes, les deux formes propositionnelles données sont donc équivalentes.
On distingue deux types différents de formes normales de la logique propositionnelle:

1. *Forme normale conjonctive*
2. *Forme normale alternative*

Au lieu de la notion *forme normale alternative* on utilise aussi les notions de *forme normale alternante, forme normale disjonctive* ou *forme normale adjonctive.*

11.2 Définitions

Comme la logique, en tant que discipline indépendante, est une science relativement jeune, aucun usage unitaire ne s'est encore imposé dans la littérature mathématique concernant la logique. Le projet suivant suit la direction proposée par Asser (Bibl.: asser).

Soyent H_1, H_2, ..., H_n, ..., H_{n+m} des variables propositionnelles différentes en paires. ($n \geq 0$, $m \geq 0$, $m + n \geq 1$.) Sur cette base nous construisons la définition de *forme normale* comme il suit:

Définition 11.1 (Termes simples, Termes de conjonction et d'adjonction) *:*

1. *Un* **terme simple** *est une variable propositionnelle ou bien la négation d'une variable propositionnelle (terme de négation).*

2. *Un* **terme de conjonction** *est une conjonction de termes simples.*
   Terme de conjonction $:= H_1 \wedge H_2 \wedge \ldots \wedge H_n \wedge \neg H_{n+1} \wedge \ldots \wedge \neg H_{n+m} = \bigwedge_{i=1}^{n} H_i \wedge \bigwedge_{j=n+1}^{n+m} \neg H_j$.
3. *Un* **terme d'adjonction** *est une adjonction de termes simples.*
   Terme d'adjonction $:= H_1 \vee H_2 \vee \ldots \vee H_n \vee H_{n+1} \vee \ldots \vee \neg H_{n+m} = \bigvee_{i=1}^{n} H_i \vee \bigvee_{j=n+1}^{n+m} \neg H_j$.
4. *En plus nous convenons qu'un terme de conjonction peut être dégénéré comme "terme de conjonction consistant en un élément unique". La même chose vaut pour le terme d'adjonction.*

Définition 11.2 (D. termes d. conj. et d'adj. qui cont. d'autres termes d. même genre) *:*

1. *Soyent* T_0, T_1, T_2 *des termes de conjonction. "*T_1 *est* **contenu dans** T_2*" signifie: Il existe (symbolquement* $\exists$*) un terme* T_0 *tel que* $T_1 \wedge T_0 \equiv T_2$.
2. *Soyent* R_0, R_1, R_2 *des termes adjonctifs (alternatifs). "*R_1 *est* **contenu dans** R_2 *signifie:* $\exists_{R_0}$ *tel que* $R_1 \wedge R_0 \equiv R_2$.

Définition 11.3 (Formes normales conjonctives et alternatives) *:*

1. *Soyent* $A_1, \ldots, A_k$ *des termes alternatifs. Ça signifie:*
   $K \equiv A_1 \wedge A_2 \wedge \ldots \wedge A_k \equiv \bigwedge_{i=1}^{k} A_i$ **forme normale conjonctive** *(kNF).*
2. *Soyent* $K_1, \ldots, K_k$ *des termes conjonctifs. Ça signifie:*
   $A \equiv K_1 \vee K_2 \vee \ldots \vee K_k \equiv \bigvee_{i=1}^{k} K_i$ **forme normale adjonctive** *(aNF).*

Remarques:

1. Il y a des auteurs qui imposent en plus qu'à une kNF aucun des termes alternatifs K_i soit contenu dans un autre terme alternatif[5]. Egalement pour les termes de conjonction d'une aNF[5]. Au cas où un terme alternatif d'une kNF est contenu dans un autre tel terme, on peut omettre le plus long des deux termes. (Il vaut $(A_1 \vee A_2) \wedge A_1 \equiv A_1$). Egalement à une aNF, si un terme de conjonction est contenu dans un autre: On en peut omettre le plus court.
2. Comme on a convenu déjà à l'occasion des termes d'adjonciton et de conjonction nous convenons aussi ici qu'une aNF peut être dégénérée à une "aNF à un seul terme de conjonction unique". Le même vaut pour le kNF. Par conséquent un terme simple est surtout aussi une aNF ainsi qu'une kNF.

Exemples:

1. $A \wedge B$ est contenu dans $A \wedge B \wedge \neg C$, mais non dans $A \wedge \neg B$
2. A est aNF ainsi que kNF (cas dégénéré).
3. $A \wedge \neg B \wedge C$ est kNF (consistant en trois termes simples) ou aussi aNF (consistant en un seul terme de conjonciton).
4. $(A \wedge \neg B \wedge C) \vee B$ est aNF.
5. $(A \wedge B \wedge \neg C) \vee (\neg A \wedge C)$ est aNF.
6. $X \vee (A \wedge B(\vee C(\wedge D)))$ n'est pas une forme normale.
7. $A \vee (B \wedge C) \wedge (\neg C \vee D)$ n'est non plus une forme normale.

11.3 Le problème de l'existence

Quant à l'existence d'une kNF ou d' une aNF équivalente il vaut le théorème suivant:

Théorème 11.1 (Théorème d'existence) *: Pour chaque forme propositionnelle quelconque il existe une kNF ainsi qu'une aNF équivalente.*

5. P.ex. à Mendelson 8Bibl.: mendelson) l'auteur impose ceci, mais par contre p.ex. à Asser (Bibl.: asser) l'auteur ne l'impose pas. Les deux chemins sont possibles.

Remarque quant à la preuve:

1. $\{\neg, \vee, \wedge\}$ est une base de composition. Par conséquent on peut faire disparaître les autres symboles logiques ($\Rightarrow$, $\Leftrightarrow$, ...) en remplaçant des termes qui contiennent $\Rightarrow$, $\Leftrightarrow$, ... un après l'autre par des termes équivalents et possibles $\neg, \vee, \wedge$.
2. On utilise les règles de De Morgan: $\neg(A \wedge B) \equiv \neg A \vee \neg B, \neg(A \vee B) \equiv \neg A \wedge \neg B$. Comme ça on peut supprimer des parenthèses et transporter le symbole logique $\neg$ devant les variables.
3. En plus on peut "déplacer" des parenthèses à l'aide de la loi distributive dans la position voulue (p.ex. en utilisant $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.)

Ainsi on réussit à faire disparaître des symboles logiques indésirables et de déplacer $\neg, \vee, \wedge$ ainsi que les parenthèses à la "place correcte".

Exemples:

1. A l'aide du tableau de vérité, on vérifie tout de suite:

2. $$A \Leftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$$

$$\begin{array}{rcl} X: & \equiv & (A \wedge \neg B) \Leftrightarrow (B \vee A) \\ & \equiv & ((A \wedge \neg B) \wedge (B \vee A))) \vee (\neg(A \wedge \neg B) \wedge \neg(B \vee A)) \\ & \equiv & ((A \wedge \neg B \wedge B) \vee (A \wedge \neg B \wedge A)) \vee ((\neg A \vee \neg\neg B) \wedge (\neg B \wedge \neg A)) \\ & \equiv & f \vee (A \wedge \neg B) \vee (\lfloor(\neg A \vee B) \wedge \neg A\rfloor \wedge \neg B) \\ & \equiv & (A \wedge \neg B) \vee (\lfloor(\neg A \wedge \neg A) \vee (B \wedge \neg A)\rfloor \wedge \neg B) \\ & \equiv & (A \wedge \neg B) \vee (\neg A \vee (B \wedge \neg A) \wedge \neg B) \\ & \equiv & (A \wedge \neg B) \vee (\neg A \wedge \neg B). \end{array}$$

La dernière expression est bien une aNF. On peut y placer $\neg B$ devant les parenthèses et reçoit donc:

$$X \equiv \neg B \vee (A \wedge \neg A) \equiv \neg B.$$

$\neg B$ est une aNF ainsi qu'une kNF.

11.4 Le problème de l'univocité

Justement nous avons vu que la forme propositionnelle $X :\equiv (A \wedge \neg B) \Leftrightarrow (B \vee A)$ est équivalente aux deux aNF $(A \wedge \neg B) \vee (\neg A \wedge \neg B)$ et $\neg B$. La représentation d'une forme propositionnelle par une aNF n'est pas claire (non univoque). La même chose vaut naturellement pour la kNF.
(Exemple: $(A \vee \neg B) \wedge (\neg A \vee \neg B) \equiv \neg B \wedge (A \vee \neg A) \equiv \neg B$.)
Il est maintenant concevable de chercher une kNF ou une aNF spéciale qui est **univoque** *jusqu'à l'ordre des termes*. Nous atteignons cela *en complétant les variables manquantes* dans chaque terme d'adjonction ou de conjonction. Nous pouvons produire ainsi des formes propositionnelles, dans lesquelles dans chaque terme d'adjonction ou de conjonction chaque variable apparaît exactement une fois. Ça se passe ainsi:
Soit p.ex. qu'il manque la variable X_k dans le terme de T_i.

1. Soit T_i d'abord un terme de conjonction d'une aNF. Alors nous élargissons T_i de la façon suivante:

$$T_i \equiv T_i \wedge w \equiv T_i \wedge (X_k \vee \neg X_k) \equiv (T_i \wedge X_k) \vee (T_i \wedge \neg X_k) \equiv T_{i_1} \vee T_{i_2}$$

Le terme T_i de l'aNF a été ainsi remplacé par une adjonction de deux termes de conjonction élargis, dans lesquels chaque fois il apparaît T_i, mais aussi X_k resp. $\neg X_k$. Le résultat est de nouveau une aNF.

2. Soit maintenant R_j un terme d'adjonction d'une kNF. Alors nous élargissons R_j de la façon suivante:

$$R_j \equiv R_j \vee f \equiv R_j \vee (X_k \wedge \neg X_k) \equiv (R_j \vee X_k) \wedge (R_j \vee \neg X_k) \equiv R_{j_1} \vee R_{j_2}$$

   Le terme R_j de la kNF a ainsi été remplacé par une conjonction de deux termes d'adjonction élargis, dans lesquels nous trouvons les R_j, mais aussi les X_k resp. les $\neg X_k$. Le résultat est de nouveau une kNF.

Comme $A \wedge A \equiv A$ ainsi que $A \vee A \equiv A$, on peut tracer les termes qui apparaissent plusieurs fois. On peut ainsi transformer chaque aNF resp. chaque kNF en une aNF resp. kNF, dans laquelle on trouve chaque variable dans chaque terme exactement une fois, ça veut dire dans aucun terme une telle variable est représentée plusieurs fois. Comme le nombre de variables est donc égal dans chaque terme, aucun terme n'est donc contenu dans un autre. Nous définissons maintenant:

Définition 11.4 (Forme normale canonique) *:*
Une aNF resp. une kNF dans laquelle dans chaque terme chaque variable apparaît exactement une seule fois, s'appelle **forme normale canonique**.

On peut même ranger de façon univoque les formes normales canoniques par les lois commutatives pour $\wedge$ et $\vee$ d'après les principes suivants:

1. Range tous les termes selon les numéros de variables ascendants.
2. Remplace dans les termes d'adjonction resp. de conjonction $T_i$les termes simples par les chiffres 0 ou 1 d'après la règle suivante: Si le terme simple est une variable X_i, remplaçons–la par 0. Mais soit le cas que le terme simple est une variable niée $\neg X_i$, alors remplacçons–la par 1. Si on omet les symboles logiques dans l'expression ainsi obtenue, on obtient au lieu du terme T_i un nombre binaire. Ainsi chaque terme T_i correspond à exactement un nombre binaire. Maintenant on peut ordonner donc les termes selon la grandeur ascendante des nombres binaires.

Ainsi on obtient des *formes normales canoniquess ordonnées.* Pour celles-ci vaut évidemment le théorème suivant:

Satz 11.1 (Théorème d'univocité) *: Pour chaque forme propositionnelle il existe exactement une aNF ainsi qu'exactement une kNF canonique ordonnée.*

11.5 Le problème de représentation

En ce qui concerne les formes propositionnelles données, on peut *lire* leurs formes canoniques de façon très simple dans le tableau de vérité. En pratique souvent la forme propositionnelle n'est pas du tout connue, mais seulement le tableau de vérité. Le problème ainsi donné s'appelle *problème de représentation.* Les formes canoniques qu'on peut tout de suite lire sont des formes propositionnelles qui satisfont au tableau de vérité donné. En effet d'ordinaire on n'obtient pas les plus simples ou le plus brèves de toutes les formes propositionnelles possibles en considération. Trouver une forme aussi simple que possible, c'est le *problème de simplification.*
Nous voulons étudier le problème de représentation à l'appui d'un exemple. (Quant au problème de simplification il faut consulter l'*algèbre de Boole.*
P.ex. la *méthode de Karnaugh* est une méthode de simplification, qu'on peut utiliser pour certains symboles logiques, qui utilise les diagrammes d'Euler (pour des ensembles).)

Exemple: Soit donnée la forme propositionnelle $X \equiv (A \vee B) \Leftrightarrow \neg C$. On cherche l'aNF équivalente. D'abord nous établissons le tableau de vérité appartenant:

No. de la ligne	A	B	C	$X \equiv (A \vee B) \Leftrightarrow \neg C$
1	0	0	0	0
2	0	0	1	1
3	0	1	0	1
4	0	1	1	0
5	1	0	0	1
6	1	0	1	0
7	1	1	0	1
8	1	1	1	0

X est vrai exactement si nous avons un des poids qui est donné par les lignes 2, 3, 5 ou 7 du tableau de vérité. La ligne 2 par exemple s'applique, si A a la valeur de vérité 0 et B a la valeur de vérité 0 et C a la valeur de vérité 1. C.–à.–d. si $\neg A$ a la valeur de vérité 1 et $\neg B$ a la valeur de vérité 1 et C a la valeur de vérité 1. C'est le cas exactement si la forme $(\neg A \wedge \neg B \wedge C)$ a la valeur de vérité 1. (Pour tous les autres poids, la dernière forme propositionnelle a la valeur de vérité 0.) Par conséquent la ligne 2 est appliquable si $(\neg A \wedge \neg B \wedge C)$ est vrai. Ainsi la ligne 3 $(\neg A \wedge B \wedge \neg C)$ est vrai. La ligne 5 s'applique, si $(A \wedge \neg B \wedge \neg C)$ est vrai et la ligne 7 s'applique, si $(A \wedge B \wedge \neg C)$ est vrai. X est vrai, si nous avons un poids qui est donné par la ligne 2, la ligne 3, la 5 ou la ligne 7 qui sont des lignes vraies. (Pour les autres poids, X est faux.) C.–à.–d. X est vrai exactement si $(\neg A \wedge \neg B \wedge C)$ ou $(\neg A \wedge B \wedge \neg C)$ ou $(A \wedge \neg B \wedge \neg C)$ ou $(A \wedge B \wedge \neg C)$ sont vrais. X est donc vrai exactement si $(\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C)$ est vrai. Pour les autres poids des variables A, B et C, X n'est pas vrai. Par conséquent on obtient:

$$X \equiv (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C).$$

Par conséquent nous avons *remplacé X par une aNF canonique,* car les termes de conjonction obtenus sont liés par $\vee$. Par la méthode d'obtenir la forme, celle–là est même ordonnée.
On peut donc retenir le procédé suivant: D'abord tracer les lignes du tableau de vérité, qui se terminent par 0. Dans les lignes qui restent, on remplace les valeurs de vérité 1 par la variable propositionnelle due à la colonne en question et les valeurs de vérité 0 par la négation de la variable propositionnelle due à cette colonne. Ensuite on lie ces termes simples obtenus par $\wedge$. Ainsi on obtient pour chaque ligne non–raturée un terme de conjonction. Après on lie ces termes de conjonction par $\vee$. Si on applique la même méthode aux lignes qui ont dans la dernière colonne la valeur de vérité 0, on obtient ainsi l'aNF: $Y \equiv (\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge C)$. Cette aNF Y est *fausse* exactement si X est vrai. Par conséquent $\neg Y$ est vrai exactement si X est vrai. Ainsi il vaut $\neg Y \equiv X$. Mais pour $\neg Y$ d'après les règles de De Morgan vaut l'équivalence $\neg((\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge C)) \equiv (A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C)$. Ceci est par contre la kNF canonique régulière.
On obtient ainsi la kNF canonique et ordonnée du tableau de vérité, si on applique la méthode décrite en haut aux lignes qui se terminent par 0 et si on place devant l'aNF ainsi obtenue le symbole logique $\neg$. D'après les règles de De Morgan, on obtient enfin la kNF qu'on cherche.

11.6 Journal de la logique

Le journal de la logique

Dernières nouvelles à la page suivante!

Journal de la logique

Le paradoxe de l'exécution inattendue

(Abrégé d'après Martin Gartener)

Petite annonce : A recommander:
M. Gartener, Logique sous le gibet

Entre autres Gartener écrit: "Le jugement a été prononcé un samedi. 'L'exécution aura lieu à midi un des sept jours de la semaine prochaine', dit le juge au prisonnier. 'Mais vous ne saurez pas quel jour, jusqu'à ce qu'on vous préviendra le matin du jour de l'exécution.!

Le juge était connu comme personne qui tenait sa parole. L'accusé retourna accompagné par son avocat dans sa cellule. Quand les deux furent seuls, l'avocat souria et dit: 'Vous ne remarquez rien? Il est impossible que le jugement sout exécuté.'

'Je ne comprend pas cela', dit le prisonnier.

'Je vous l'explique. Il est tout à fait évident qu'on ne vous exécutera pas samedi prochain. Samedi est le dernier jour de la semaine. Vendredi après–midi vous seriez envore en vie et ainsi vous auriez la certitude absolue qu'on vous exécuterait samedi. Vous le sauriez avant qu'on vous le dise samedi matin. Cela contredirait l'arrêt du juge.' 'C'est vrai', dit le prisonnier.

'Samedi est donc exclu', continue l'avocat. 'Reste le vendredi comme dernier jour, où on pourrait vous exécuter. Mais vendredi ce n'est pas possible, parce que jeudi après–midi il ne reste plus que deux jours: à savoir vendredi et samedi. Comme le samedi n'entre pas en considération, ça devrait être le vendredi. Mais comme vous savez, cela serait aussi contraire à l'arrêt du juge. Ainsi le vendredi est aussi exclu et le jeudi est le dernier jour possible. Mais le jeudi est aussi exclu, parce que vous seriez encore en vie le mercredi après–midi et vous sauriez donc que le jeudi devrait être le jour de l'exécution!

'Maintenant je comprends', dit le condamné et se sentait déjà bien mieux. 'De cette façon je peux aussi tracer mardi et lundi. Il ne reste donc plus que demain, mais demain je ne peux pas être exécuté, parce que je le sais déjà aujourd'hui!'

Bref, l'arrêt du juge semble se contredire lui–même. Il n'y a pas de contradiction logique dans les deux conditions ajoutées au jugement. Malgré cela le jugement ne peut pas être exécuté évidemment — ou quand même? Pour éclaircir cela retournons dans la cellule chez le condamné. Il est convaincu, par une logique apparemment incontestable, qu'il ne pourra pas être exécuté sans que les conditions du jugement en soient blessées. A sa plus grande surprise, le bourreau arriva le jeudi matin. Il est clair qu'il ne s'y attendait pas. Ce qui surprend davantage: Le jugemant du juge est complètement correct. Le jugement peut être exécuté, exactement comme le juge l'avait déclaré." Est–ce que cet arrière–goût de la logique, qui est nié par le monde, ne fait pas apparaître le paradoxe d'une façon fascinante?

Appel à tous les étudiants intélligents!
Depuis la lecture de ce paradoxe de l'exécution inattendue, ing. dipl. ABC ne trouve plus la raison. On prétend que celle–ci s'est cachée derière la solution. C'est comment, la solution? Comminuquer à la réd., s.v.p.. La réd.

Chapitre 12

Limites de la logique propositionnelle, quantificateurs et perspectives

12.1 Limites de la logique propositionnelle

Dans 9.1.1 nous avons compris la notion de *"proposition"* comme *création linguistique*, qui exprime une *vérité* ou un *mensonge*. Mais dans la grammaire, on appelle des créations linguistiques qui expriment des vérités ou des mensonges des *phrases*. Exemples:

1. La phrase "Jean n'est pas ici" est en ce moment ou vraie ou fausse. Voilà d'autres phrases:
2. "Jean nourrit le cheval."
3. "Maintenant le soleil brille dehors."
4. "Aujourd'hui le soleil s'est levé deux fois à l'est."
5. "De nouveau notre CF n'a pas gagné le samedi dernier."
6. "Un et un est deux. "
7. "$1 + 1 = 2$."
8. "Dans la facture de l'entreprise Coupe–gorge un plus un font trois."
9. "De $a = 6$ on déduit $2\,a = 12$."

Par contre des créations linguistiques comme "hourra!", "Hi hi hi!", "Comment est-ce que j'arrive au parc le plus vite?", "Viens!", "Disparais!" ne sont pas des propositions. Il s'agit d'exclamations ou d'interrogations (questions). Egalement la création "X conduit la voiture" est indéterminée, n'est donc pas une proposition.
Historiquement nous trouvons les racines de la proposition logique chez Aristote . Par conséquent nous les appelons *propositions d'Aristote* au lieu de parler simplement de propositions. Comme on peut facilement se rendre compte, des telles propositions sont des phrases simples , consistant en un sujet, un prédicat (verbe) et un objet. En plus, le sujet ou l'objet peuvent être élargis par un attribut ou le prédicat par une expression adverbiale. Nous trouvons aussi des telles phrases simples comme parties de phrases composées, de liaisons de phrases et de phrases complexes . Nous trouvons des détails dans chaque livre scolaire spécialisé en ce sujet sous le titre "syntaxe". Cela dépasserait le cadre de la logique mathématique de répéter les notions de base de la grammaire ici. Qu'elles soyent supposées.
Regardons la phrase suivante: "Jean nourrit le cheval."

Sujet	verbe	Objet	
Jean	nourrit	le cheval.	Ceci est une proposition.
	Expression prédicative		

Si nous considérons par contre la phrase: "X nourrit le cheval", nous ne pouvons plus décider si ceci est maintenant vrai ou faux. Ici, une partie de la phrase est variable et indépendante: Pour X on peut mettre n'importe quel sujet. Si on remplace X par "Jean", la phrase ainsi obtenue est vraie dans notre contexte. Mais si on remplace X par "la locomotive à vapeur", la phrase ainsi obtenue est sûrement fausse. Comme X tient la place du sujet, on appelle X *"variable libre de sujet"* .

On trouve une situation semblable à "De $x = 5$ on déduit $2x = 10$", resp. à " $(x = 5) \Rightarrow (x = 10)$". $(x = 5)$ pris pour soi est une variable propositionnelle, car dans l'expression il se trouve la variable x. L'expression change en proposition, si on remplace x par une valeur. Si on met pour x la valeur 5, on obtient une proposition vraie. Si on met par contre pour x la valeur 6, on obtient une proposition fausse. La variable propositionnelle $X \equiv (x = 5)$ change donc dans l'expression $(x = 5) \Rightarrow (x = 10)$ en une variable de sujet, car elle appartient maintenant à la place du sujet. $\Rightarrow$ a la signification du verbe (du prédicat), $(x = 10)$ la signification d'une *variable d'objet*. Par l'introcuction d'un nombre à la place de x on obtient au lieu de $(x = 5) \Rightarrow (x = 10)$ une proposition composée, qui consiste en équations de nombres comme propositions partielles. Si par contre on ne touche pas le x, l'expression $(x = 5) \Rightarrow (x = 10)$ est aussi une proposition, mais qui n'est pas décomposable en des propositions partielles. On peut seulement la décomposer en deux variables propositionnelles et un symbole logique. Par contre la variable de nombres x, considérée toute seule, n'est pas une proposition; ici elle est seulement une partie d'une variable propositionnelle.
Quant aux exemples qu'on vient de discuter, on remarque qu'une proposition peut avoir une *structure interne*. Ainsi le sujet, le verbe (prédicat) et l'objet sont des parties d'une proposition qui peuvent être manipulées chacune individuellement, mais qui ne sont pas des propositions.
La logique propositionnelle seule ne fournit pas de règles pour une telle manipulation. On arrive ici ainsi aux limites de la logique propositionnelle: Avec la logique propositionnelle seule on ne peut jamais traiter tous les problèmes de la logique!

12.2 Quantificateurs

Considérons comme exemples les trois propositions suivantes:

(1)	A	$\equiv$	Tous les poissons vivent dans l'eau.	Symbol.:	(Tous $\rangle$	poisson $\rangle$	prédicat(eau))
(2)	B	$\equiv$	La truite est un poisson.	–	(	Truite $\rangle$	prédicat(poisson))
(3)	C	$\equiv$	La truite vit dans l'eau.	–	(	Truite $\rangle$	prédicat(eau))

Il apparaît que (3) est né de parties de (1) et (2) par une nouvelle combinaison de parties. L'expression prédicative de (2) a été combinée avec le sujet de (1) pour obtenir (3). Pour la combinaison de telles parties de propositions à une nouvelle proposition, la logique propositionnelle n'offre pas de règles. $A \wedge B \vdash C$ ne peut donc pas être déduit par les règles de la logique propositionnelle, parce qu'ici la structure interne de la proposition est essentielle. Nous appelons la théorie qui rend compte de ce problème *la logique des prédicats*. On distingue même *différents niveaux de logique des prédicats (la logique des niveaux)* .
Dans la logique des prédicats on n'étudie pas seulement des propositions et des variables propositionnelles mais aussi des *sujets*, des *variables de sujets*, des *prédicats*, *des variables de prédicats* et aussi des *quantificateurs*. Les quantificateurs sont des signes logiques ou des mots qui expriment une *quantité*, contrairement à des propositions ou des variables propositionnelles, qui rendent une *qualité*. Comme les quantificateurs permettent une orthographe très compacte de propositions mathématiques, ils sont très souvent appliqués dans les mathématiques universitaires. Ça vaut en suite évidemment aussi pour les mathématiques d'ingénieur d'un niveau de haute école!

Deux quantificateurs sont importants pour nous: Le *quantificateur universel* et le *quantificateur d'existence*. On trouve les signes et les significations assortis dans le tableau suivant:

Nom	Symbole	Autre symbole	Signification
Quantificateur universel	$\forall$	$\bigwedge$	Pour tous
Quantificateur d'existence	$\exists$	$\bigvee$	Il existe

Les exemples suivants peuvent servir à une explication plus vaste. Soit $M := \{1,2,3,4\}$

1. $\forall_{x \in M} : x < 5$ signifie: $(1 < 5) \wedge (2 < 5) \wedge (3 < 5) \wedge (4 < 5)$.
2. $\exists_{x \in M} : x = 3$ signifie: $(1 = 3) \vee (2 = 3) \vee (3 = 3) \vee (4 = 3)$.

Comme dans le premier exemple tous les nombres de M sont plus petite que 5 et dans le deuxième exemple il existe un nombre de M qui satisfait l'équation $x = 3$ (il vaut $3 = 3$), nous avons des propositions vraies dans les deux cas. Ici x est une variable de sujet reliée au quantificateur dans les deux exemples. (Variable de sujet *liée*.)

12.3 Perspective: D'autres résultats de la logique

Nous voulons discuter encore quelques résultats qui ont une certaine importance en pratique, sans les prouver ici. Les preuves à cela sont relativement longues et demandent une portion d'expérience dans le raisonnement mathématique et logique.

Théorème 12.1 (Théorème d'intégralité) *: La logique propositionnelle est complète.*

Complète signifie ici que dans la logique propositionnelle chaque proposition vraie peut être déduite en un nombre fini d'étapes, c.–à.–d. à l'aide d'une chaîne *d'étapes de preuves* . On peut donc prouver ceci. "Q est vrai" signifie donc qu'il existe une preuve (c.-à.–d. une déduction logique et correcte) $w \vdash Q$.
Attention! Dans la logique des prédicats de niveau supérieur ce théorème ne vaut plus! ça signifie qu'il existe dans la logique des prédicats des propositions vraies (théorèmes), pour lesquelles il n'y a plus aucune chaîne d'étapes de preuves finie qui peut être exprimée à l'aide d'expressions du même niveau de la logique des prédicats. On peut donc prouver qu'il y a des théorèmes qui ne sont plus prouvables dans le cadre donné. C'est à dire que la quantité de théorèmes vrais est ainsi plus grande que la quantité de théorèmes déduisibles. Ce sont surtout les résultats de Gödel des années trente du vingtième siècle qui montrent ceci. Turing et d'autres ont aussi établi dans ce domaine des résultats qui influencent les effets quant au problème de la prévisibilité.
En plus vaut le théorème suivant:

Théorème 12.2 (Liberté de contradictions de la logique propositionnelle) *: La logique propositionnelle est exempte de contradictions.*

ça signifie qu'aucune contradiction ne peut naître dans la logique propositionnelle, que donc par exemple $P \wedge \neg P$ n'est pas déduisible, n'importe de quelle proposition ou forme propositionnelle P il s'agit. En d'autres mots: $w \nvdash P \wedge \neg P$ ou bien $w \nvdash f$.
Comme nous verrons postérieurement p.ex. dans *l'algèbre des circuits*, la logique propositionnelle suffit complètement pour le traitement par des machines (bit–machines, machines de von Neumann). Car tous les programmes tournent à l'aide de couplages du hardware donné. Et les couplages satisfont aux règles de l'algèbre des circuits électriques. C.–à.–d.: Ce qu'on peut faire sur les ordinateurs classiques est tout dans le cadre de la logique propositionnelle. D'autre part les problèmes dont la formulation n'est pas attribuable à la logique propositionnelle, qui ont vraiment besoin de la logique des prédicats, ne se laissent pas traiter à l'aide d'ordinateurs classiques (comme p.ex. des quantifications sur des ensembles infinis d'ordre supérieur). Egalement les problèmes où il s'agit purement du qualitatif, de choses qui de part leurs qualités ne se laissent pas réduire à des quantités[1]. Cela cerne des problèmes des disciplines de la philosophie et de la science humaine. Il est justement implossible d'attribuer la logique des prédicats parfaitement aux machines et y compris par cela à l'algèbre des circuits électriques et à la logique propositionnelle, même si l'intelligence de ces machines est aussi artificielle qu'on aimerait. Sinon la logique propositionnelle suffirait pour toutes nos intentions. Un problème fondamental est bien qu'une machine finie aux algorithmes finis ne peut pas abstraire parmi les quantités ou ensembles infinis tel que l'homme, qui arrive à comprendre

1. Le mouvement qui essaye de faire cette réduction quand même, dans l'ignorance entière des résultats de la logique, s'appelle *réductionnisme*

un processus infini comme objet actuel et peut donc travailler avec la notion qu'il en construit. L'homme a l'aptitude de l'abstraction dirigée vers le succès, il peut formuler des notions nouvelles, géniales, par un acte de la volonté. La machine par contre ne peut pas vouloir, elle peut seulement observer des directives (instructions), elle est toujours l'esclave d'un programme. Un autre problème fondamental naît maintenant aussi de la connaissance que les qualités et leurs relations ne se laissent pas toujours réduire à des quantités et leurs relations...

Kapitel • Chapitre 13

Vorwort zu Mengen, Relationen, Funktionen

Liebe Leserin, lieber Leser,

Dieser Text ist in Skriptform abgefasst. Das bedeutet, dass er in äusserst knapper Fassung nur das wesentliche Skelett des zu lernenden Stoffes wiedergibt. Für weitere und ausführliche Erklärungen, Beispiele, viele Beweise und ergänzende Ausführungen ergeht daher an den Studenten der Rat, ein oder mehrere Lehrbücher beizuziehen. Studieren bedeutet ja zu einem wesentlichen Teil, sein Wissen selbständig mit Hilfe der Literatur zu erweitern, streckenweise sogar selbständig zu erarbeiten, zu festigen und anzuwenden. Ein Skript ist dabei nur ein Wegweiser und nie ein Lehrbuchersatz. Welche Lehrbücher jemand verwenden will, ist jedem freigestellt, denn die Neigungen und Lerngewohnheiten der Menschen sind genau so verschieden wie ihre Lieblingsessen, ihre Trinkgewohnheiten und ihr Lustgefühl beim Sport. In Teil 1, vom Autor (Bibl.: wirz) findet sich eine grosse Literaturliste. Speziell für den in diesem Teil dargestellten Stoff sei auf Ayres, Algebra (Bibl.: ayres) verwiesen. Übungen finden sich in *DIYMU* , vom Autor (Bibl.: wirz1). Nun also los! Profitieren wir davon, dass die ins Ziel genommene Mathematik schon erfunden ist und nur noch verstanden und gelernt werden muss.

Im Sommer 1996 Der Autor

Man lernt nichts kennen als was man liebt, und je tiefer und vollständiger die Kenntnis werden soll, desto stärker, kräftiger und lebendiger muss die Liebe sein ...

Goethe an Jacobi

• *On n'apprend rien à connaître qu ce qu'on aime, et le plus profondément et complètement le connaissances devrait devenir, d'autant l'amour doit être plus fortement, solidement et vitalement ...*

Goethe à Jacobi

Kapitel • Chapitre 14

Einführung in die elementare Mengenlehre (Repetition)

14.1 Zu den Grundlagen

14.1.1 Einleitung

Zuerst werden wir hier kurz die sicher von der Schule her bekannte elementare Mengenlehre repetieren und die hier verwendete Begriffs– und Symbolsprache vorstellen. Mit Hilfe des Begriffs der *Produktemenge* können wir dann den Begriff *Relation* erarbeiten und damit sauber die Begriffe *Abbildung* und *Funktion* samt den speziellen gebräuchlichen Ausprägungen allgemein und abstrakt einführen. Damit ist dann die Grundlage geschaffen für Dinge wie Funktionen, die den $\mathbf{R}^n$ in den $\mathbf{R}^m$ abbilden — oder z.B. für das Verständnis des Assoziativitätsgesetzes für allgemeine Abbildungen.

14.1.2 Zum Mengenbegriff

Wir wählen hier einen naïven Zugang zur Mengenlehre, gehen somit nicht streng axiomatisch vor. Es ist uns nicht um Cantors Theorie der *transfiniten Kardinalzahlen* gelegen. (Georg Cantor hat sich u.a. aus theologischen Erwägungen mit dem Problem des Unendlichen beschäftigt. Daraus ist die mathematische Mengenlehre geworden, in der es um „unendliche oder transfinite Zahlen“ geht. Man muss dort diverse Stufen oder Typen von “unendlich” unterscheiden, mit denen man wie mit Zahlen rechnen kann. Das nützt man in der Non–Standard–Analysis aus.)

Begriffserklärung 8 (Menge als Grundgebilde) *:*
Eine **Menge** *ist für uns ein von unserer Spracherfahrung her bekanntes Grundgebilde.*

Andere, nicht weiter definierte Grundgebilde kennen wir aus der Geometrie (z.B. der Punkt). Es wird hier nicht gesagt, was eine Menge exakt ist. Wir definieren die Menge vorerst nicht exakt, denn der Begriff ist genügend bekannt. Anschaulich denken wir bei der Menge an eine Zusammenfassung gewisser Individuen nach gewissen Zusammenfassungsregeln. Folgende intuitive Beschreibung einer Menge stammt von Cantor:

Begriffserklärung 9 (Cantor) *: Eine* **Menge** *ist eine wohldefinierte Ansammlung oder Auflistung von Objekten des Denkens. Diese Objekte heissen* **Elemente** *der Menge.*

Wir legen später fest, wann und wie eine Menge gegeben ist oder welche Beziehungen sie erfüllt (Klassifikation von Eigenschaften). Das genügt für unseren Bedarf.

Symbole 2 (Mengen, Elemente) *:*

1. *Mengen: M, A, B, C ... (Grossbuchstaben)*

2. *Elemente: a, b, c, e, p, q ... (Kleinbuchstaben)*

Die nun folgende *Grundrelation* wollen wir als *Axiom*[1] akzeptieren:

Axiom 14.1 (Enthaltensein) *: Ein Element kann zu einer Menge gehören — oder nicht. Symbolisch:* $p \in M$ *(p ist Element von M) oder* $\neg(p \in M)$*, d.h.* $p \notin M$ *(p ist nicht Element von M)*

Das Axiom postuliert also für das Enthaltensein die zweiwertige Logik. Mehrdeutigkeit ist hier ausgeschlossen.

14.1.3 Zu den Möglichkeiten, eine bestimmte Menge anzugeben

Man kennt *zwei* Möglichkeiten, eine Menge anzugeben:

1. Durch *Aufzählen (Auflisten)* der Elemente, z.B. $A = \{1, 2, 3, 4, 5, 6\}$ (abbrechend) oder $\mathbf{N} = \{1, 2, 3, 4, \ldots\}$ (nicht abbrechend).
2. Durch *Angabe einer charakterisierenden Eigenschaft*, z.B. $B = \{x \in \mathbf{N} \mid x < 6\}$

In B ist $\mathbf{N}$ die *Grundmenge* (*Fundamentalmenge*, Universalmenge, die den Bezugsrahmen festlegt. $(x < 6)$ ist die definierende Eigenschaft.

Von der Schule bekannte **Beispiele** sind: Lösungsmengen von Gleichungen, Punktmengen aus der Geometrie. (Z.B. eine Gerade kann analytisch aufgefasst werden als unendliche Punktmenge, im Gegensatz zur Geraden als Grundgebilde der Geometrie, also als Ding an sich.) Für uns wichtige Mengen sind die in der *Analysis* verwendeten *Intervalle*, z.B. das *offene Intervall* $(a,\ b)$ (vgl. Seite 99.) Gemäss den Gepflogenheiten in der Mathematik treffen wir die folgende Vereinbarung:

Vereinbarung 1 (Wiederholte Elemente) *: Es sei eine Menge durch Aufzählung gegeben. Kommt ein Element dann mehrmals vor, so darf man die Duplikate streichen.*

Beispiel: $\{1, 2, 3, 2, 4, 3, 1, 5, 2\} = \{1, 2, 3, 4, 5\}$

Vereinbarung 2 (Anordnung der Elemente) *: Bei einer Menge spielt die Anordnung der aufgezählten Elemente keine Rolle.*

14.1.4 Gleichheit von Menge

Definition 14.1 (Gleichheit von Menge) *: Zwei Mengen heissen* **gleich***, wenn sie dieselben Elemente enthalten. In logischen Symbolen:*

$$A = B :\Longleftrightarrow [\forall_{x \in A}(x \in A) \Rightarrow (x \in B) \wedge \forall_{y \in B}(y \in B) \Rightarrow (y \in A)]$$

ist wahr.

14.1.5 Leere Menge

Definition 14.2 (Leere Menge) *: Eine Menge, die kein Element enthält, heisst* **leere Menge** *oder* **Nullmenge***.*

Symbole 3 (Leere Menge) *:* $\{\}$ *oder* $\emptyset$*.*

Beispiel: $\{x \mid x \neq x\} = \{\}$.

Noch eine witzige Geschichte. Sie soll sich im Ausland zugetragen haben. An der Bushaltstelle 1 stiegen 5 Studenten in einen leeren Bus. An der nächsten Haltstelle stiegen dann 6 Studenten aus. (Das ist kein Druckfehler...) An der nächsten Haltstelle stieg dann wieder einer ein. Dann war der Bus leer! — Warum ist die „Passagiermenge“ hier keine Menge?

[1] Irgendwo muss man auch in der Mathematik einmal beginnen. Ein **Axiom** ist eine grundlegende mathematische Aussage, d.h. ein Satz, der am Beginn steht. Es soll somit keine andern noch grundlegendere Sätze geben, aus denen ein Axiom hergeleitet werden kann.

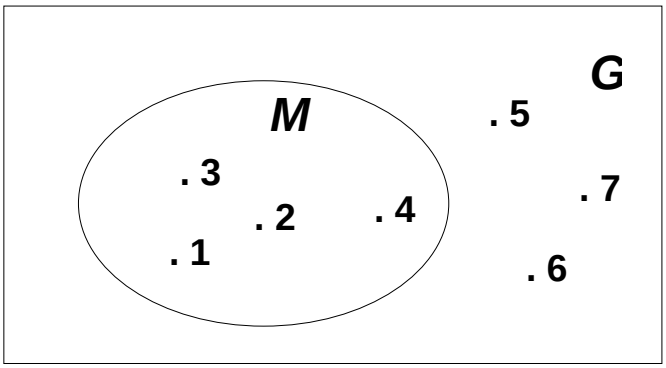
14.1.6 Antinomien

Antinomien sind widersprüchliche Mengenbildungen. Leider können solche in der naïven Mengenlehre entstehen. Doch im Schulalltag stellt das erfahrungsgemäss keine grosse Behinderung dar. Wir wollen dennoch kurz darauf eingehen.
Da wir die Grundbegriffe „Menge“ und „Element“ unterscheiden, gilt für eine Menge allgemein $M \notin M$, d.h. es ist $\neg(M \in M)$. Man bilde nun $R = \{M \mid M \in R \Leftrightarrow M \notin R\}$. Das ist *Russels* [2] Menge aller Mengen, die sich nicht selbst enthalten. Da die Menge R durch die Angabe der Eigenschaft ihrer Elemente gegeben ist, ist R eine Menge. Für Mengen gilt aber $M \notin M$, d.h speziell für R gilt $R \notin R$. Also gehört auch R zu den Elementen von R, denn die Eigenschaft $R \notin R$ ist ja erfüllt. “R gehört zu R” bedeutet aber, dass $R \in R$ gilt, im Widerspruch zur Feststellung $R \notin R$. Man hat also den Widerspruch, dass $R \notin R \Leftrightarrow R \in R$ wahr sei, was aber der Widerspruchsfreiheit der Aussagenlogik widerspricht.
Heute kann man die Mengenlehre axiomatisch widerspruchsfrei aufbauen. Die Konstruktion erweist sich allerdings als sehr komplex. Die interessierten Studenten sind auf die Fachliteratur verwiesen (vgl. Bibl.: schmidt, potter).

14.1.7 Graphische Darstellung von Mengen

Zur Darstellung von Mengen verwenden wir *Euler–Diagramme*, früher auch als *Venn–Diagramme*[3] bezeichnet. Beispiel:

Abbildung 14.1: Euler–(Venn)–Diagramm



In 14.1 ist G die Grundmenge und M die betrachtete Menge. Z.B. gilt $1 \in M$ und $6 \notin M$.

14.1.8 Endliche Mengen, Mächtigkeit

Definition 14.3 (Endliche Menge) *: Eine Menge heisst* **endlich**, *falls man ihre Elemente abschliessend aufzählen kann:* $M = \{e_1, e_2, e_3, \ldots, e_n\}$ *mit* $n \in \mathbf{N}$. *Andernfalls heisst* M *unendlich.*

Die Menge aller Fliegen der Erde ist wohl endlich, obwohl niemand die momentane Anzahl Fliegen exakt kennt. Bekannte unendliche Mengen sind die Zahlenmengen $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Q}^+$, $\mathbf{R}$, $\mathbf{C}$ (natürliche, ganze, rationale, positive rationale, reelle, komplexe Zahlen).

Definition 14.4 (Mächtigkeit) *: Sei die Menge* M *endlich. Die Anzahl der Elemente von nennen wir die* **Mächtigkeit** $|M|$ *von* M.

[2] B. Russel, Mathematiker und Philosoph. Er übte Kritik an Cantors Mengenlehre.
[3] Man hat ende 20 Jhdt. entdeckt, dass Euler vor Venn solche Diagramme auch schon verwendet hat.

Bei unendlichen Mengen ist die Sache komplizierter. Zwar reden wir da von unendlicher Mächtigkeit ($|M| = \infty$), doch zeigt eben gerade die höhere Mengenlehre, dass man verschiedene Stufen von unendlich unterscheiden muss, um Widersprüche zu vermeiden. So kann man z.B. zeigen, dass gilt: $|N| = |Q| < |R|$. Dass man unendliche Bereiche als Dinge an sich begreifen und unterscheiden kann, siehen wir schon in der Geometrie. Wie erwähnt ist eine Gerade eine einerseits unendliche Punktmenge. Andererseits aber auch ein Ding an sich, z.B. ein blosses Element der Mengen aller Geraden, die eine Ebene bilden. Eine Ebene kann somit einerseits als Punktmenge, andererseits als Geradenmenge oder Figurenmenge – und drittens als Ding an sich verstanden werden.

14.1.9 Mengenbeziehungen: Definitionen

Teilmengen

Definition 14.5 (Teilmenge) *: A heisst* **Teilmenge** *von B ($A \subseteq B$) resp. B heisst* **Obermenge** *von A ($B \supseteq A$) wenn jedes Element von A auch in B enthalten ist: $\forall_{x \in A}\, x \in B$.*
Falls gilt: $(A \subseteq B) \wedge \exists_{x \in B} : x \notin A$, so heisst A echte Teilmenge von B.

Symbole 4 *Teilmengen]: Wir schreiben dann $A \subset B$ resp. $B \supset A$.*

Beispiel: In Abb. 14.1 ist $M \subset G$.

Satz 14.1 (Zu Teilmengen) *:*

1. $A \subset B \Leftrightarrow |A| < |B|$
2. $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C} \ldots$

Korollar 14.1 (Triviale Folgerungen) *: Folgende Beziehungen sind wahr:*

1. $(A = B) \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$
2. $A \subseteq B$ *(Reflexivität)*
3. $(A \subseteq B \wedge B \subseteq C) \Rightarrow (A \subseteq C)$ *(Transitivität)*
4. $\forall_A : \{\} \subseteq A$ *(Die leere Menge ist Teilmenge jeder Menge.)*

Klassen von Mengen, Potenzmengen

Wie wir vorhin gesehen haben, kann man eine Gerade g der Euklidschen Geometrie als Grundgebilde, d.h. als Ding an sich auffassen. Andererseits ist dieselbe Gerade auch als unendliche Punktmenge γ denkbar. Weiter lässt sich eine Ebene Φ als unendliche Menge von Geraden deuten, die zusammen Φ ausmachen. Φ ist so gesehen eine unendliche Menge von Geraden γ_i, von denen wiederum jede aus unendlich vielen Punkten besteht. Φ ist somit eine unendliche Menge von unendlichen Mengen. Mengen von Mengen sind in gewissem Sinne „höhere Mengen“. Daher ist es üblich, für Mengen von Mengen ein andere Bezeichnung zu gebrauchen:

Begriffserklärung 10 (Klasse) *: Eine Menge von Mengen nennen wir* **Mengenfamilie** *oder* **Mengenklasse** *(kurz auch* **Klasse***. Statt „Teilmengen“ sagen wir „Teilklassen“.*

Beispiel: $\{\{2,3\},\{2\},\{4,5\}\}$ ist eine solche Mengenklasse. Teilklassen sind $\{\{2,3\},\{2\}\}, \{\{2\}\}$ etc. .

Definition 14.6 (Potenzmenge) *: Die* **Potenzmenge** $\wp(M)$ *einer Menge M ist die Menge oder Klasse aller Teilmengen von M.*

Beispiel: Sei $M = \{a, b\}$. Dann ist $\wp(M) = \{\{\}, \{a\}, \{b\}, \{a, b\}\}$.
Mit Hilfe der Kombinatorik ist es möglich, den folgenden allgemeinen Satz zu beweisen:

Satz 14.2 (Mächtigkeit der Potenzmenge) *:*

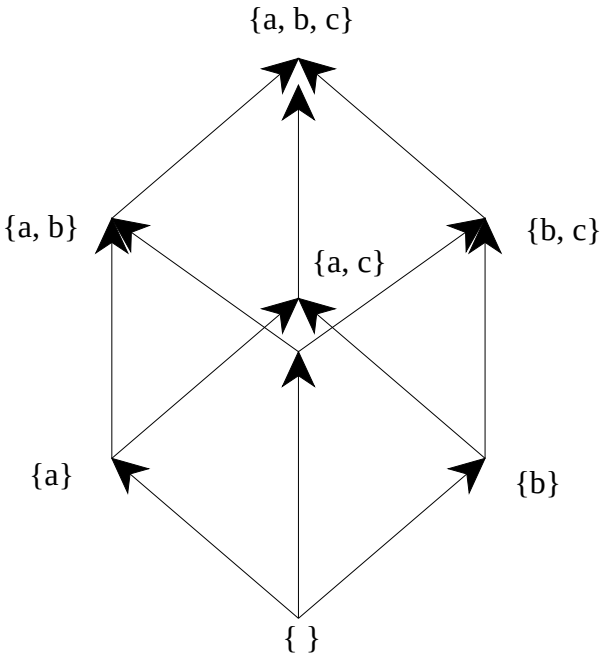
$$|M| = n \;\Rightarrow\; |\wp(M)| = 2^n = 2^{|M|}$$

Hasse-Diagramme

Hasse-Diagramme[4] dienen dazu, eine graphische Übersicht über alle Elemente einer Potenzmenge zu geben.

Beispiel: Sei $M = \{a, b, c\}$ (vgl. Abb. 14.2). M hat 8 Teilmengen. Das Zeichen $\subset$ ist im Diagramm durch einen Pfeil ersetzt. Das Diagramm hat dann 12 Pfeile.

Abbildung 14.2: Hasse–Diagramm



Mengenverknüpfungen

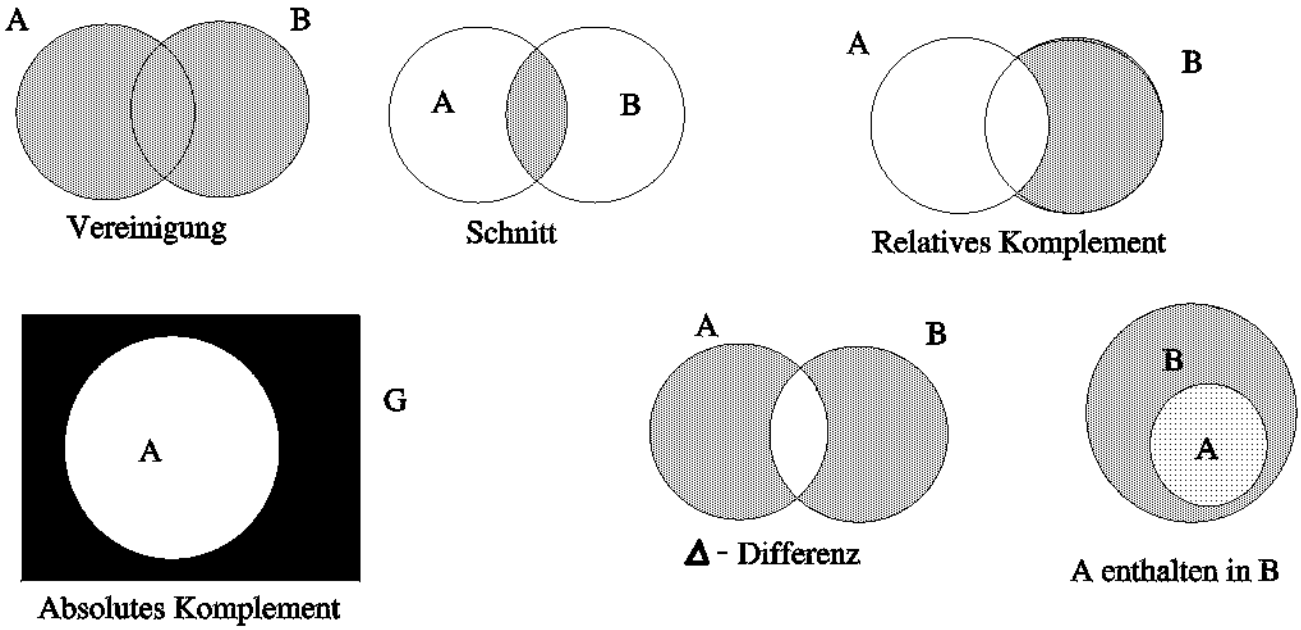
Mengenverknüpfungen sind sicher jedermann aus der Schule bekannt. Hier seien nur die abstrakten Definitionen wiedergegeben ((vgl. Abb. 14.3)):

Definition 14.7 (Mengenverknüpfungen) *: Sei G = Grundmenge.*

- **Vereinigungsmenge** *von A und B:* $A \cup B = \{x \in G | \, x \in A \vee x \in B\}$
- **Schnittmenge** *von A und B:* $A \cap B = \{x \in G | \, x \in A \wedge x \in B\}$
- *A und B heissen* **disjunkt**, *falls gilt:* $A \cap B = \{\}$
- **Differenz** *(relatives Kompliment) von A und B:* $A \setminus B = \{x \in A | \, x \notin B\}$
- **Komplement** *(absolutes Komplement) von A:* $\bar{A} = A^c = \{x \in G | \, x \notin A\}$
- **Symmetrische Differenz** *von A und B:* $A \triangle B = (A \setminus B) \cup (B \setminus A)$

[4] Helmut Hasse war ein Mathematiker (Zahlentheoretiker) aus unserer Elterngeneration. Er lebte in Hamburg.

Abbildung 14.3: Mengen–Verknüpfungen



14.1.10 Gesetze der Mengenalgebra

Satz 14.3 (Mengenalgebra) : *Sei G die Grundmenge, A, B, C seien Mengen. Folgende Gesetze gelten:*

(1)	Idempotenz	$A \cup A$	$=$	A		$A \cap A$	$=$	A
(2)	Assoziativität	$(A \cup B) \cup C$	$=$	$A \cup (B \cup C)$		$(A \cap B) \cap C$	$=$	$A \cap (B \cap C)$
(3)	Kommutativität	$A \cup B$	$=$	$B \cup A$		$A \cap B$	$=$	$B \cap A$
(4)	Distributivität	$A \cup (B \cap C)$	$=$	$(A \cup B) \cap (A \cup C))$		$A \cap (B \cup C)$	$=$	$(A \cap B) \cup (A \cap C)$
(5)	Identitäten	$A \cup \{\}$	$=$	A		$A \cap G$	$=$	A
		$A \cup G$	$=$	G		$A \cap \{\}$	$=$	$\{\}$
(6)	Komplementgesetze	$A \cup \bar{A}$	$=$	G		$A \cap \bar{A}$	$=$	$\{\}$
		$\bar{G}$	$=$	$\{\}$		$\overline{\{\}}$	$=$	G
		$\overline{(\bar{A})}$	$=$	A				
(7)	De Morgan	$\overline{(A \cup B)}$	$=$	$\bar{A} \cap \bar{B}$		$\overline{(A \cap B)}$	$=$	$\bar{A} \cup \bar{B}$

Als **Beispiel** zeigen wir die *Kommutativität*: smallskip
Beweis: $A \cup B = \{x \in G | x \in A \vee x \in B\} = \{x \in G | x \in B \vee x \in A\} = B \cup A$. Dabei haben wir uns auf das Kommutativgesetz der Aussagenlogik abgestützt.

Satz 14.4 (Zur Mächtigkeit) : *Folgende Gesetze gelten:*

(1)	$A \cap B$	$=$	$\{\}$	$\Rightarrow$	$\lvert A \cup B \rvert$	$=$	$\lvert A \rvert + \lvert B \rvert$
(2)	$A \cap B$	$\neq$	$\{\}$	$\Rightarrow$	$\lvert A \cup B \rvert$	$=$	$\lvert A \rvert + \lvert B \rvert - \lvert A \cap B \rvert$

Vom letzten Bild aus Abb. 14.3 kann man ablesen:

Satz 14.5 (Zum Enthaltensein) *: Es gilt:*

$$\begin{array}{lll} A \subseteq B & \Longleftrightarrow & A \cap B = A \\ & \Longleftrightarrow & A \cup B = B \\ & \Longleftrightarrow & \bar{B} \subseteq \bar{A} \\ & \Longleftrightarrow & A \cap \bar{B} = \{\} \\ & \Longrightarrow & \bar{A} \cup B = G \end{array}$$

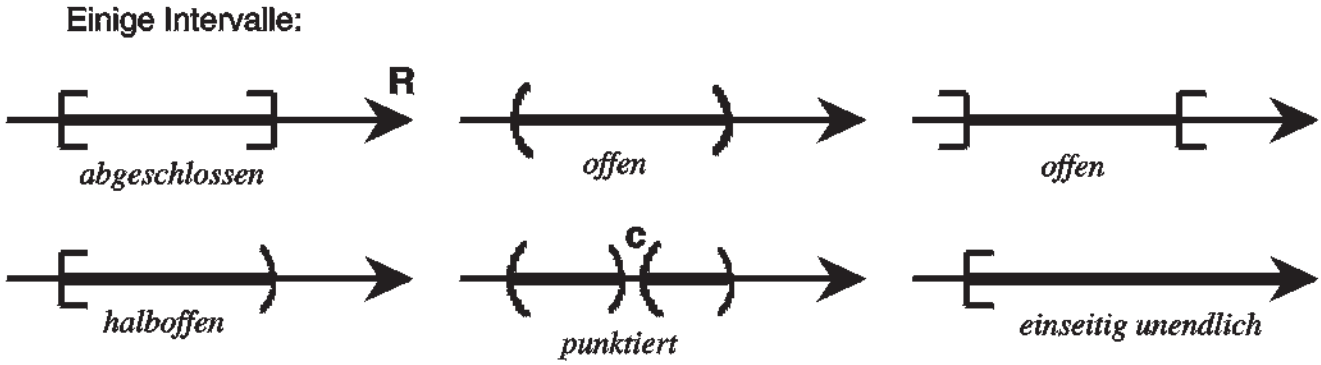
Hinweis: Zur Übung überlege man sich die Beweise einiger der obigen Aussagen.

14.1.11 Eine Anwendung in der Analysis: Intervalle

Intervalle sind spezielle Mengen. Es handelt sich dabei um Teilmengen der reellen Zahlen. In der Analysis trifft man solche Intervalle häufig als *Lösungsmengen* von Ungleichungen oder als *Definitionsbereiche* oder *Wertebereiche* von Funktionen.

Beispiele von Intervalltypen:

Abbildung 14.4: Intervalle



Definition 14.8 (Intervalle) *(vgl. Abb. 14.4):*

1. **Offenes Intervall**[5]*:* $I = (a,\ b) := \{x \in \mathbf{R} |\, a < x < b\}$.
2. **Abgeschlossenes Intervall***:* $\bar{I} = [a,\ b] := \{x \in \mathbf{R} |\, a \leq x \leq b\}$.
3. **Halboffene Intervalle***:* $I = (a,\ b] := \{x \in \mathbf{R} |\, a < x \leq b\}$, $\bar{I} = [a,\ b) := \{x \in \mathbf{R} |\, a \leq x < b\}$.
4. **punktiertes Intervall***:* $I(c) := \{x \in \mathbf{R} |\, x \in (a,b) \wedge x \neq c\}$. *Punktierte Intervalle heissen auch* **Umgebungen**
5. *Das* **beidseitig unendliche Intervall** *isr gleich* $\mathbf{R}$*:* $\mathbf{R} := \{x \in |\, -\infty < x < \infty\}$. [6]
6. **Einseitig unendliche Intervalle***:* $(a,\ \infty) := \{x \in \mathbf{R} | a < x\}$, $[a,\ \infty) := \{x \in \mathbf{R} | a \leq x\}$, $(\infty,\ b) := \{x \in \mathbf{R} | x < b\}$, $(\infty,\ b] := \{x \in \mathbf{R} | x \leq b\}$.

14.2 Produktmengen

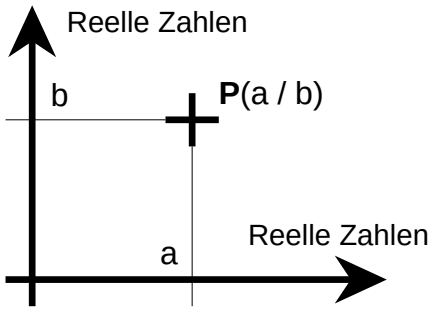
14.2.1 Definitionen: Geordnete Paare und Produktmengen

Mit dem Zahlenstrahl, d.h. durch die Punkte auf einem geometrischen Strahl, stellen wir bekanntlich die Menge der reellen Zahlen dar. Welche entsprechende Menge aber stellen wir durch die Punkte $\mathbf{P}$ der Ebene

[5] Das offene Intervall wird manchmal auch als $]a, b[$ geschrieben.

[6] ∞ ist keine reelle Zahl. Man kann die reellen Zahlen aber um ∞ erweitern. Das bedingt aber weitere Kenntnisse.

Abbildung 14.5: Ein Punkt einer Ebene



(vgl. Abb. 14.5) dar? Im Folgenden wollen wir diese Menge konstruieren. Wir werden sie *Produktmenge* $\mathbf{R} \times \mathbf{R}$ nennen. Dabei ist es wesentlich, dass man das erste Element a (1. Koordinate) in der Reihenfolge vom 2. Element b unterscheiden kann. Dazu brauchen wir den Begriff des *geordneten Paares*.
Sei allgemein $a \in A$ und $b \in B$. Ein *geordnetes Paar* (a, b) besteht aus zwei Elementen, wobei a als das erste und b als das zweite ausgezeichnet ist. Um die Reihenfolge der Elemente mit Hilfe der bisher erarbeiteten Grundlagen (Mengenlehre, Logik) exakt festzulegen, brauchen wir einen Trick. Mit einer Menge alleine kommen wir nicht weiter, denn die Reihenfolge der Elemente wird bei der Mengenbildung ja nicht berücksichtigt. In einer Menge geben wir an, welches das 1. Element ist (durch Angabe einer Menge mit einem Element) und welche beiden Elemente das Paar bilden (durch Angabe einer Menge mit zwei Elementen). Ausser der Mengenbildung haben wir dann dabei weiter nichts benutzt. Das geht so:

Definition 14.9 (Geordnetes Paar) *:* $(a, b) \; = \; \{\{a\}, \{a, b\} =\}$ **geordnetes Paar**.

Ein geordnetes Paar ist demnach eine Menge von Mengen, d.h. eine Klasse.
Man kann einfach folgenden Satz beweisen (Übung):

Satz 14.6 (Gleichheit geordneter Paare) *:*

$$(a, b) \; = \; (c, d) \iff (a = c \; \wedge \; b = d)$$

Beispiele: $(1, 2) \neq (2, 1)$, $(3, 3) \neq \{3, 3\} \; = \; \{3\}$, $(5, 6) \; = \; (10, 12)$.

Nun können wir die *Produktmenge* als Menge von geordneten Paaren definieren. Seien dazu A und B zwei gegebene Mengen:

Definition 14.10 (Produktmenge) *:* **Produktmenge** $A \times B \; = \{(a, b) \mid a \in A \wedge b \in B\}$

Es ist daher:

$$A \times B \; = \{(a, b) \mid a \in A \wedge b \in B\} \; = \; \{\{\{a\}, \{a, b\}\} \mid a \in A \wedge b \in B\}.$$

$A \times B$ ist eine Menge von Mengen von Mengen, d.h. eine Familie von Klassen von Mengen. Das ist etwas Neues, wie wir es bisher noch nie angetroffen haben, eine neue *Qualität* also! Wir benützen weiter folgende Abkürzung:

Begriffserklärung 11 (Zum Mengenprodukt) *: Statt $A \times A$ schreiben wir kurz A^2.*

Beispiele: Sei $A = \{1, 2\}$ und $B = \{a, b, c\}$.

$$\begin{array}{rcl} A^2 & = & \{\{1, 1\}, \{1, 2\}, \{2, 1\}, \{2, 2\}\} \\ A \times B & = & \{\{1, a\}, \{1, b\}, \{1, c\}, \{2, a\}, \{2, b\}, \{2, c\}\} \end{array}$$

Bemerkung: Aus diesen Beispielen sieht man: Für $A \neq B$ ist $A \times B \neq B \times A$.

Trivialerweise gilt:

Satz 14.7 (Mächtigkeit des Mengenprodukts) *:*

$$|A \times B| \;=\; |A| \;\cdot |B|$$

14.2.2 Verallgemeinerung auf mehrere Faktoren

Jetzt können wir induktiv[7] geordnete *n–Tupel* und Produktmengen *mit mehreren Faktoren* definieren. Da $M \;=\; A \times B$ definiert und auch eine Menge ist, wird es möglich, $A \times B \times C$ wie folgt zu definieren: $A \times B \times C \;:=\; M \times C \;=\; (A \times B) \times C$. Allgemein legen wir fest:

Definition 14.11 (geordnete n–Tupel) *:*

$$(a_1, a_2, \ldots, a_n) \;:= \{\{(a_1, a_2, \ldots, a_{n-1})\}, \{(a_1, a_2, \ldots, a_{n-1}), a_n\}\}$$

Definition 14.12 (Produktmengen mit mehreren Faktoren) *:*

$$A_1 \times A_2 \times \ldots \times A_n \;:=\; (A_1 \times A_2 \times \ldots \times A_{n-1}) \times A_n$$

Natürlich gilt wieder:

Satz 14.8 (Gleichheit geordneter Paare) *:*

$$(a_1, a_2, \ldots, a_n) \;=\; (b_1, b_2, \ldots, b_n) \iff (a_1 = b_1 \;\wedge\; a_2 = b_2 \wedge \ldots \wedge a_n = b_n)$$

14.2.3 Wahrheitsmengen

Sei P eine Aussageform und $M \;=\; \{0, 1\}$ (Menge der Wahrheitswerte). Wir definieren die *Wahrheitsmenge* $\tau(P)$[8]. wie folgt:

Definition 14.13 (Wahrheitsmenge) *:*

$$\tau(P) \;:=\; \{(x_1, x_2, \ldots, x_n) \in M^n = \{0, 1\}^n \mid P \;\; \textit{ist wahr für die Belegung} \;\; (x_1, x_2, \ldots, x_n)\}$$

Beispiel: $\tau((X \Rightarrow Y) \wedge (Y \Rightarrow Z)) \;=\; \{(1, 1, 1), (0, 1, 1), (0, 0, 1), (0, 0, 0)\}$. (Man prüfe das nach!)

[7] Nach dem Prinzip der vollständigen Induktion.
[8] τ steht für *„truth“*

Satz 14.9 (Über Wahrheitsmengen) *:*

1. $\tau(P_1 \wedge P_2) \;=\; \tau(P_1) \cap \tau(P_2)$
2. $\tau(P_1 \vee P_2) \;=\; \tau(P_1) \cup \tau(P_2)$
3. $\tau(\neg P) \;=\; \overline{\tau(P)}$
4. $(P \vdash Q) \iff (\tau(P) \subseteq \tau(Q))$ *ist Tautologie.*
5. *Im letzten Fall ist auch* $(P \implies Q)$ *Tautologie.*

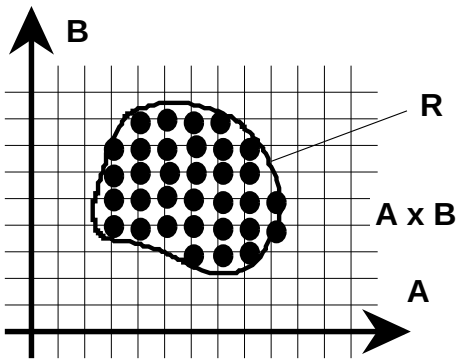
Kapitel • Chapitre 15

Relationen, Abblidungen und Funktionen

15.1 Der Begriff „Relation“

15.1.1 Definitionen

Abbildung 15.1: Relationsmenge



Definition 15.1 (Relationsmenge) *: Eine Teilmenge $\mathcal{R} \subseteq A \times B$ heisst zweistellige* **Relationsmenge** *oder kurz* **Relation** *von A nach B.*

(Vgl. dazu Abb. 15.1.) Ist $(a, b) \in \mathcal{R} \subseteq A \times B$ so schreiben wir *symbolisch:*

Symbole 5 (Relation) *:* $a \smile b \ :\Longleftrightarrow \ (a, b) \in \mathcal{R} \subseteq A \times B$.

„$\smile$ “ ist ein frei erfundenes Symbol, das keine weitere konkrete Bedeutung hat. Falls wir konkrete bekannte Relationen betrachten, so ersetzen wir es durch das jeweile übliche Relationssymbol.

Sprechweise: Falls $a \smile b$ gilt, so sagen wir *„a steht in Relation zu b“.*

Es gilt somit $\mathcal{R} = \{(a, b) \mid a \smile b \text{ resp. } (a, b) \in \mathcal{R}\}$. $A \times B$ zerfällt daher in zwei Teilmengen: $A \times B = \mathcal{R} \cup \bar{\mathcal{R}}$. $\mathcal{R}$ ist die Menge der geordneten Paare, die zueinander in Relation stehen, $\bar{\mathcal{R}}$ die Menge

der geordneten Paare, die zueinander nicht in Relation stehen. Sind A und B endlich, so lässt sich die Relation wie in Abb 15.1 graphisch darstellen.

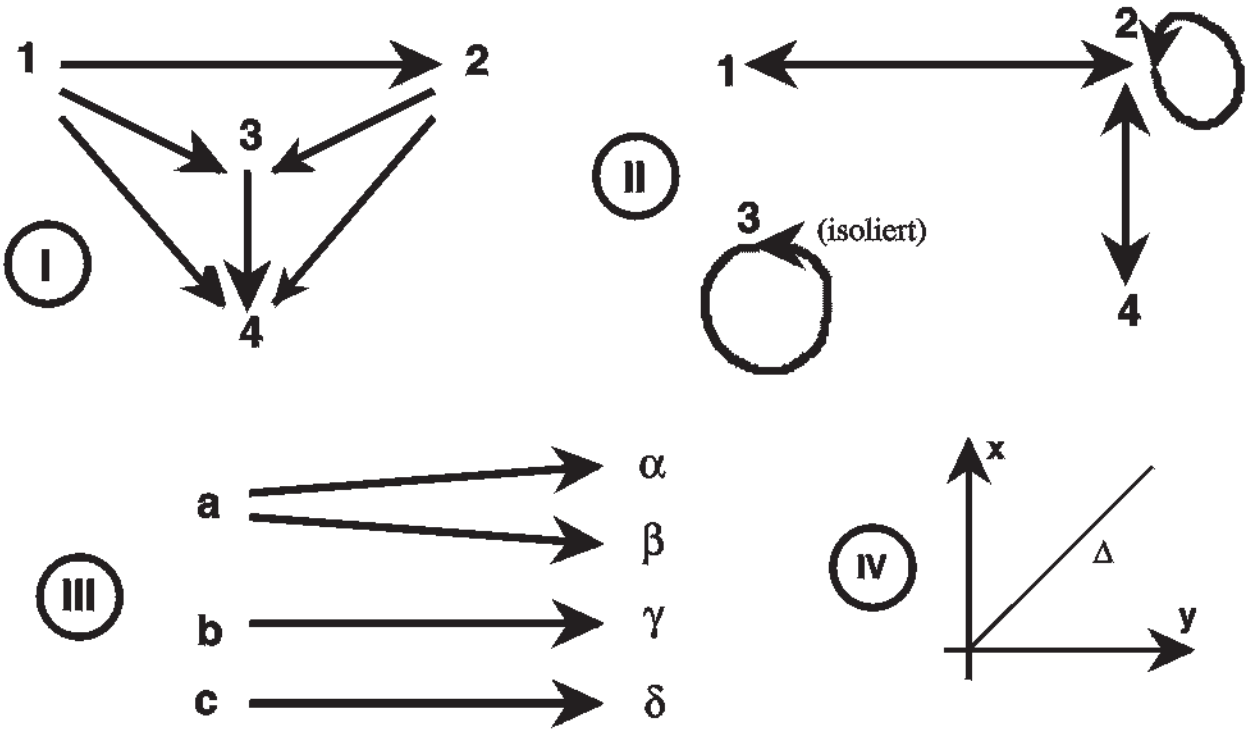
Beispiele:

1. $A \times B = \mathbf{R} \times \mathbf{R}$. $a \smile b :\Longleftrightarrow a < b$. Somit ist $\mathcal{R} = \{(a, b) \mid a < b\}$.
2. $A \times B = \Gamma \times \Gamma$, $\Gamma = \{\text{Geraden einer Ebene}\}$. $\mathcal{R} = \{(g_1, g_2) \in \{\Gamma \times \Gamma\} \mid g_1 \perp g_2\}$. DAnnn ist: $a \smile b :\Longleftrightarrow g_1 \perp g_2$. ($\perp$ bedeutet „senkrecht stehen“.)

15.1.2 Darstellung durch Pfeildiagramme

Endliche Relationsmengen lassen sich übersichtlich durch *Pfeildiagramme* darstellen. Der Begriff ist selbsterklärend, wie die folgenden Beispiele zeigen:

Abbildung 15.2: Pfeildiagramme



Beispiele (vgl. Abb. 15.2):

1. $\mathcal{R} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\} \subseteq \{1, 2, 3, 4\} \times \{1, 2, 3, 4\}\}$ (Bild I)
2. $\mathcal{R} = \{\{1, 2\}, \{2, 2\}, \{2, 4\}, \{2, 1\}, \{3, 3\}, \{4, 2\} \subseteq \{1, 2, 3, 4\} \times \{1, 2, 3, 4\}\}$ (Bild II)
3. $\mathcal{R} = \{\{a, \alpha\}, \{a, \beta\}, \{b, \gamma\}, \{c, \delta\} \subseteq \{a, b, c\} \times \{\alpha, \beta, \gamma\}\}$ (Bild III)

Die Zahl 3 in Bild II ist ein *isoliertes Element*: 3 ist nur in Relation zu sich selbst.

15.2 Spezielle Relationen in $A \times A$ oder $A \times B$

15.2.1 Diagonalrelation (Identitätsrelation)

Definition 15.2 (Diagonalrelation) *:*

$$\triangle_A \ := \ \mathcal{R} = \{(a_1, a_2) \in A \times A \mid a_1 = a_2\} = \{(a_1, a_2) \mid a \in A\}$$

Die Diagonalrelation besteht somit ausschliesslich aus isolierten Elementen, die nur in Relation zu sich selbst stehen. Falls $A = \mathbf{R}$ ist (Bild IV, Abb. Abb. 15.2), so ist das Bild der Relationsmenge darstellbar als die Winkelhalbierende des I. Quadranten (bei einer Darstellung in einem kartesischen Koordinatensystem). Daher der Name *Diagonalrelation.* $\Delta = \{(x, y) \in \mathbf{R}^2 \mid x = y\}$

15.2.2 Inverse Relation

Sei eine Relation $\mathcal{R} = \{(a, b) \mid a \smile b\}$ gegeben.

Definition 15.3 (Inverse Relation) *:* $\mathcal{R}^{-1} = \{(b, a) \mid a \smile b$ *resp.* $(a, b) \in \mathcal{R}\}$ *heisst* **inverse Relation** *zu* $\mathcal{R}$*.*

Beispiele:

1. $\mathcal{R} = \{\{a, 1\}, \{a, 2\}, \{c, 0\}\}$. Dann ist $\mathcal{R}^{-1} = \{\{1, a\}, \{2, a\}, \{0, c\}\}$.
2. $\mathcal{R} = \{$(Mann, Frau) $\mid$ Mann verheiratet mit Frau$\}$.
   $\mathcal{R}^{-1} = \{$(Frau, Mann) $\mid$ Mann verheiratet mit Frau$\}$.

Trivialerweise ist fogender Sachverhalt richtig:

Satz 15.1 (Zur inversen Relation) *:*

1. $\Delta^{-1} = \Delta$
2. $|\mathcal{R}^{-1}| = |\mathcal{R}|$. *(Die Mächtigkeit der Inversen ändert nicht.)*

15.2.3 Reflexive Relation

Sei $\mathcal{R} \subseteq A^2$.

Definition 15.4 (Reflexive Relation) *:* $\mathcal{R}$ *heisst* **reflexiv** $:\Longleftrightarrow \ \forall_{a \in A} : \ (a, a) \in \mathcal{R}$*.*

Jedes Element ist also mit sich selbst in Relation. (Vgl. Abb. 15.3.) Daher gilt die einfache Folgerung:

Satz 15.2 (Zur reflexiven Relation) *: Sei* $\mathcal{R}$ *reflexiv. Dann ist:*

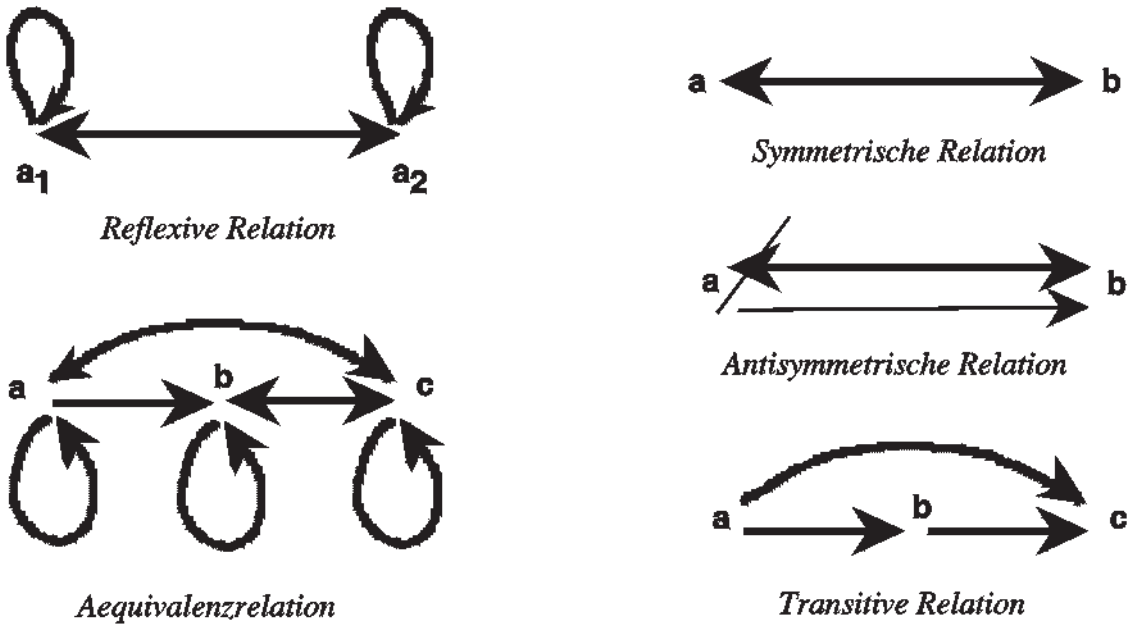
1. $A^2 \subseteq \mathcal{R}$
2. $\Delta_A \subseteq \mathcal{R}$

Beispiele dazu:

1. Für geometrische Dreiecke: Sei $Dreieck_1 \smile Dreieck_2 :\Longleftrightarrow Dreieck_1 \sim Dreieck_2$ ($\sim$ bedeutet hier „ähnlich“). $\sim$ ist natürlich reflexiv, da jedes Dreieck zu sich selbst ähnlich ist.
2. Ebenso ist es mit der Kongruenz von Dreiecken.
3. Ebenso für $\perp$ bei Geraden einer Ebene: $g_1 \perp g_2 \Longrightarrow g_2 \perp g_1$.
4. Für reelle Zahlen a, b: $a \smile b :\Longleftrightarrow \ a < b$. Daraus folgt aber $b \not< a$. Diese Relation ist nicht reflexiv. (Sie ist *antireflexiv.*)

Definition 15.5 (Antieflexive Relation) *:* $\mathcal{R}$ *heisst* **antireflexiv** $:\Longleftrightarrow \ \forall_{a \in A} : \ (a, a) \notin \mathcal{R}$*.*

Abbildung 15.3: Diverse Relationen



15.2.4 Symmetrische Relation

Definition 15.6 (Symmetrische Relation) *:*
Eine Relation $\mathcal{R}$ *heisst* **symmetrisch**, *falls gilt:* $a \smile b \Longrightarrow b \smile a$.

Reflexive Relationen sind somit umkehrbar (vgl. Abb. 15.3). Alle Pfeile sind Doppelpfeile.

Beispiele:

1. Die Ähnlichkeitsrelation bei geometrischen Dreiecken.
2. Kongruenzrelation bei geometrischen Dreiecken.
3. Die Diagonalrelation.
4. $(a < b) \not\Longrightarrow (a < b)$. Diese Relation ist *antisymmetrisch*. (Vgl. Abb. 15.3.)

Definition 15.7 (Antisymmetrische Relation) *:*
Eine Relation $\mathcal{R}$ *heisst* **antisymmetrisch**, *falls gilt:* $a \smile b \Longrightarrow b \not\smile a$.

15.2.5 Transitive Relation

Definition 15.8 (Transitive Relation) *:*
Eine Relation $\mathcal{R}$ *heisst* **transitiv**, *falls gilt:* $:\Longleftrightarrow \ ((a \smile b) \wedge (b \smile c) \Longrightarrow a \smile c)$.

(Zur Transitiven Relation vgl. auch Abb. 15.3.)

Beispiele:

1. Die Ähnlichkeitsrelation bei geometrischen Dreiecken ist transitiv.

2. Ebenso die Kongruenzrelation bei geometrischen Dreiecken.
3. Die Gleichheitsrelation bei Zahlen: $a = b \wedge b = c \Longrightarrow a = c$.
4. Die $<$–Relation bei Zahlen: $a < b \wedge b < c \Longrightarrow a < c$.
5. Die $\perp$–Relation bei Geraden einer Ebene ist nicht transitiv: $g_1 \perp g_2 \wedge g_2 \perp g_3 \Longrightarrow g_1 \not\perp g_3$.

15.2.6 Äquivalenzrelation

Definition der Äquivalenzrelation

Sei $\mathcal{R} \subseteq A^2$. Dann definieren wir (vgl. dazu auch Abb. 15.3.) :

Definition 15.9 (Äquivalenzrelation) *:*
Eine Relation $\mathcal{R}$ heisst **Äquivalenzrelation***, falls $\mathcal{R}$ reflexiv, symmetrisch und transitiv ist.*

Symbole 6 (Relation) *: Für die Äquivalenzrelation benützen wir das Symbol „$\sim$“.*

Beispiele: Wegen den bisher betrachteten Beispielen wissen wir, dass folgende Relationen Äquivalenzrelationen sind: Ähnlichkeit geometrischer Figuren, Kongruenz geometrischer Figuren, Parallelität von Geraden, Ebenen oder Pfeilen, Gleichheit von Zahlen, Zugehörigkeit von Pfeilen zu einem geometrischen Vektor.

Von den Vektoren her ist uns bekannt, dass „die Menge aller zu einem gegebenen Pfeil gleich langen, parallelen und gleichgerichteten Pfeile im Raum“einen *geometrischen Vektor* bilden. Durch die Kriterien „gleich lang, parallel und gleichgerichtet“ wird nun auf dem Mengenprodukt *(Menge aller Pfeile)* $\times$ *(Menge aller Pfeile)* ($A =$ *Menge aller Pfeile*) eindeutig eine Teilmenge ausgesondert, d.h. eine Relation definiert:

$$Pfeil_1 \backsim Pfeil_2 \Longleftrightarrow \textit{beide Pfleile gehören zum selben Vektor.}$$

Man sieht sofort ein, dass diese Relation reflexiv, symmetrisch und transitiv ist, also eine Äquivalenzrelation stiftet. Die geordneten Paare der Relation bilden eine Mengenklasse. Bei den Elementen von A, die zu einer Äquivalenzrelation gehören, spricht man daher von einer *Äquivalenzklasse.*

Definition 15.10 (Äquivalenklasse) *:*
$[a] := \{x \in A \mid x \sim a\}$ *heisst* **Äquivalenklasse** *mit dem Repräsentanten a.*

$[a]$ ist somit die „Menge aller zu a äquivalenten Elemente von A“. Es gilt natürlich $[a] \subseteq A$.

Das Beispiel der Restklassen

Ein wichtiges **Beispiel** einer Äquivalenzrelation ist durch die *Restklassen* in den ganzen Zahlen Z gegeben. Restklassen sind also Äquivalenklassen.
Seien $a, b, c \in \mathbf{Z}$. Wir definieren zuerst die *Kongruenz* in $\mathbf{Z}$:

Definition 15.11 (Kongruenz „modulo“) *: a heisst* **kongruent** *zu b* **modulo** *c genau dann, wenn a und b bei der Division durch c denselben Divisionsrest haben.*

Symbole 7 (Kongruenz „modulo“) *: Für a* **kongruent** *b* **modulo** *c schreiben wir kürzer:*

$$a \equiv b \mod c \quad \textit{oder} \quad a \equiv b(c)$$

Beispiele:

$$17 \equiv 12 \equiv 7 \equiv 2 \equiv -3 \equiv -8 \mod 5.$$

Arithmetisch kann man die Kongruenz auch wie folgt definieren:

Definition 15.12 (Andere Erklärung der Kongruenz) *:*

$$a \equiv b \mod c :\Longleftrightarrow \exists_{k\in\mathbf{Z}} : \ a = c \cdot k + b$$

Die durch die Kongruenz modulo einer ganzen Zahl gegebene Äquivalenzrelation teilt $\mathbf{Z}$ in disjunkte Teilmengen auf, nämlich die Äquivalenzklassen. Diese nennen wir jetzt *Restklassen*.

Definition 15.13 (Restklassen) *: Eine Restklasse in* $\mathbf{Z}$ *ist eine durch die Kongruenzrelation modulo einer Zahl gegebene Ähnlichkeitsklasse.*

Als **Beispiel** wollen wir die Restklasen modulo 3 betrachten. Das sind diejenigen Teilmengen von $\mathbf{Z}$, deren Elemente bei der Division durch 3 jeweils denselben Rest lassen. Wir haben somit:

Nullklasse:	$[0]_3 = \{x \in \mathbf{Z} \mid x \equiv 0 \mod 3\} = \{0, \pm 3, \pm 6, \ldots\}$
Einsklasse:	$[1]_3 = \{x \in \mathbf{Z} \mid x \equiv 1 \mod 3\} = \{1, 4, 7, \ldots, -2, -5, -8, \ldots\}$
Zweiklasse:	$[2]_3 = \{x \in \mathbf{Z} \mid x \equiv 2 \mod 3\} = \{2, 5, 8, \ldots, -1, -4, -7, \ldots\}$

Man sieht sofort, dass gilt:

$$[0]_3 \cup [1]_3 \cup [2]_3 = \mathbf{Z}, \qquad [0]_3 \cup [1]_3 = \{\} \qquad \text{etc..}$$

15.2.7 Die strenge Ordnungsrelation

Für zwei verschiedene reelle Zahlen a und b gilt: Entweder ist $a < b$ oder es ist $b < a$. Dadurch ist auf $\mathbf{R}^2$ eine *strenge Ordnungsrelation* gegeben. Exakt definiert man die strenge Ordnungsrelation wie folgt:

Definition 15.14 (Strenge Ordnungsrelation) *:*
Eine Relation, die antireflexiv, antisymmetrisch und transitiv ist, heisst **strenge Ordnungsrelation**.

Beispiele:

1. Sei $\mathbf{N}_n = \{1, 2, 3, \ldots, n\}$ und $M = \{\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3, \ldots\}$. Dann ist durch $\mathbf{N}_1 \subset \mathbf{N}_2 \subset \mathbf{N}_3 \subset \mathbf{N}_4 \subset \ldots$ eine strenge Ordnungsrelation auf M gegeben.
2. In jeder nummerierten Menge kann man die Elemente nach ihren Nummern ordnen. Damit hat man eine strenge Ordnungsrelation.

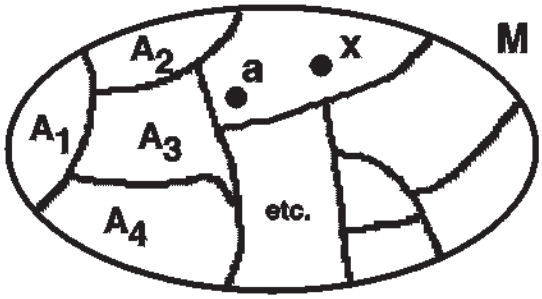
15.2.8 Partitionen und Quotientenmengen

Mit Hilfe des Mengenprodukts ist es möglich, auf abstrakte Art und Weise aus alten Mengen neue, grössere zu bilden. Eine weitere Möglichkeit zur Bildung neuer Mengen erschliesst sich durch die *Quotiontenmengen*. (Vgl. auch Lipschutz (Bibl.: lipschutz1 und lipschutz2).)
Um diese Möglichkeit zu studieren, wollen wir zuerst den Begriff *Partition* erklären. Zu diesem Zweck betrachten wir eine Menge M und denken uns diese aufgeteilt in paarweise disjunkte Teilmengen $A_1, A_2, A_3, \ldots$. Dabei schränken wir uns für unsere Zwecke auf den einfachen Fall ein, wo die Anzahl dieser Teilmengen abzählbar[1] ist. Für eine solche Aufteilung in Teilmengen verwenden wir den Begriff *Partition*. Exakt:

Definition 15.15 (Partition) *:*
$P_M = \{A_1, A_2, A_3, \ldots\}$ *heisst* **Partition** *von* $M :\Longleftrightarrow \ (M = A_1 \cup A_2 \cup A_3 \cup \ldots) \wedge (\forall_{i\neq j} : A_i \cap A_j = \{\})$.

[1] Später wird gezeigt, dass nicht alle Mengen abzählbar sind. Ein Beispiel ist die Menge der reellen Zahlen.

Abbildung 15.4: Partitionen



Beispiel: Wir betrachten $M = \{a, b, c, d\}$. Dann ist durch $P_M = \{\{a\}, \{b, c\}, \{d\}\}$ eine Partition gegeben. Man merkt sofort, dass die Anzahl aller möglichen Partitionen von M mit der Mächtigkeit $|M|$ sehr rasch anwächst.

Sei nun auf M eine Partition $P_M = \{A_1, A_2, A_3, \ldots\}$ gegeben. In einer beliebigen Teilmenge A_i wählen irgend ein Element a_i aus und halten es fest. Durch $x \sim a_i \;:\Longleftrightarrow\; (a_i \in A_i \wedge x \in A_i)$ ist damit eine Relation gegeben, denn wir haben damit geordnete Paare in M^2. Wegen der gemeinsamen Zugehörigkeit der Elemente x und a_i zu A_i ist diese Relation reflexiv, symmetrisch und transitiv. Es handelt sich also um eine Äquivalenzrelation.
Wenn andererseits auf M eine Äquivalenzrelation gegeben ist, so können wir irgend ein Element $a_1 \in M$ auswählen und damit die Menge A_1 aller zu a_1 äquivalenten Elemente bilden. Dann streichen wir die Elemente von A_1 aus M weg, wählen in der Restmenge ein Element a_2 und verfahren ebenso. Das führt zur Streichung der Menge A_2 aller zu a_2 äquivalenten Elemente. So fahren wir weiter. Die Mengen A_i sind nach Konstruktion disjunkt. Da mit jedem Element a_i eine Menge A_i gebildet werden kann, schöpft das Verfahren die ganze Menge M aus. Damit wissen wir:

Satz 15.3 (Äquivalenzrelation und Partition) *:*
Eine Äquivalenzrelation erzeugt auf M eine Partition und umgekehrt.

Ein anschauliches **Beispiel** liefert die Volksschule. Jeder Schüler einer solchen Schule genört zu genau einer Klasse. Die Schüler einer Klasse sind äquivalent bezüglich Notengebung, denn sie haben dieselben Lehrkräfte, also dieselben Bedingungen. Man hat somit eine Äquivalenzrelation. Und die Schule ist eindeutig in disjunkte Klassen aufgeteilt.
Da es nicht mehr disjunkte Teilmengen als Elemente geben kann, gilt:

Satz 15.4 (Mächtigkeit einer Partition) *:*

$$|M| \geq |P_M|$$

Sei jetzt auf M eine Äquivalenzrelation $\mathcal{R} \subseteq M^2$ gegeben. Damit existiert eine Partition P_M. Wir definieren:

Definition 15.16 (Quotientenmenge) *: Die Partition P_M heisst* **Quotientenmenge nach $\mathcal{R}$**. *Symbolisch: $P_M = M/\mathcal{R}$*

Beispiele:

1. Kongruenz modulo 3 in $\mathbf{Z}$: $P_M = \{[0]_3, [1]_3, [2]_3\}$.
2. Bei der Relation „gleich lang und gleich gerichtet“ bei geometrischen Pfeilen ist $P_M = \{geometrischeVektoren\}$.
3. Bei der Ähnlichkeitsrelation mit geometrischen Figuren ist P_M die Menge der geometrischen Formen.

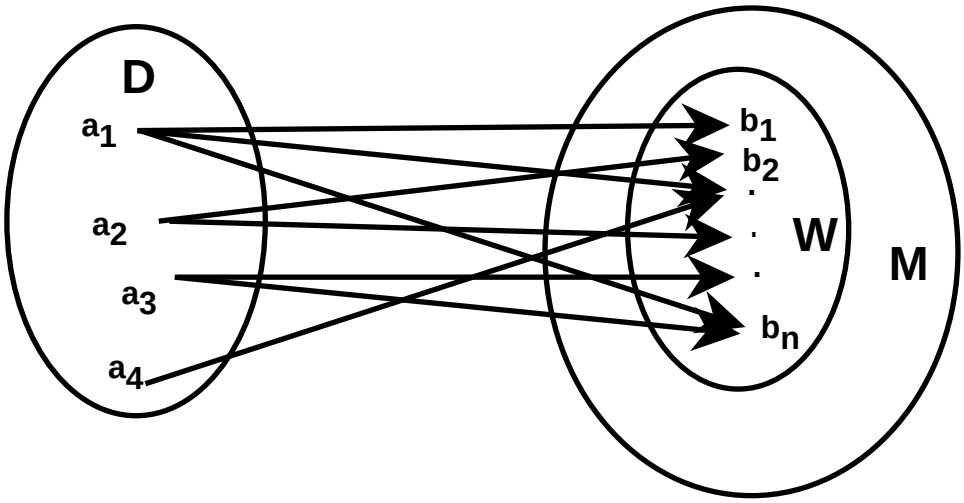
15.3 Abbildungen und Funktionen

15.3.1 Definitionen

Abbildungen

Definition 15.17 (Linkstotale Relation) *:*
Eine Relation $\mathcal{R} \subseteq D \times M$ *heisst* **linkstotal** $:\Longleftrightarrow\ \forall_{a\in D}\exists_{b\in M}\ (a,b) \in \mathcal{R}$

Abbildung 15.5: Linkstotale Relation



Zu jedem $a \in D$ muss es also mindestens ein b geben (es können auch mehrere sein), so dass das geordnete Paar (a, b) zur Relationsmenge $\mathcal{R}$ gehört. Jedes a hat also ein Bild. Dabei ist W die Menge der Elemente b, die in der Relationsmenge jeweils in den geordneten Paaren an zweiter Stelle vorkommen. Nicht alle Elemente aus dem Vorrat M müssen vorkommen. W kann eine Teilmenge von M sein. D auf der linken Seite in Abb. 15.5 wird also total ausgeschöpft: „linkstotal“ also.
Es gilt daher: $W = \{b_i \in M \mid \exists_{a_k\in D} :\ (a_k, b_i) \in \mathcal{R}\}$.
In der mathematischen Fachsprache sind im Zusammenhang mit Abbildungen mehrere Begriffe geläufig. Die wichtigsten sind nachstehend zusammengestellt:

Definition 15.18 (Abbildung, Definitionsbereich, Wertebereich) *: Eine linkstotale Relation nennen wir* **Abbildung** $\mathcal{A}$*. Die Menge* D *(in der letzten Definition) heisst* **Definitionsbereich**, **Urbildbereich** *oder* **Argumentenbereich**. W *heisst* **Wertebereich** *(wenn es sich um Zahlen handelt),* **Bildbereich** *oder* **Zielbereich**. M *heisst* **Wertevorrat** *oder* **Bildvorrat**. *Ein Element aus dem Definitionbereich heisst* **Urbild** *oder* **Argument**. *Ein Element aus dem Bildbereich heisst* **Bild**, **Wert** *(wenn es sich um Zahlen handelt) oder* **Ziel**. *Eine Variable über dem Urbildbereich nennen wir auch* **unabhängige Variable**, *eine Variable über dem Bildbereich* **abhängige Variable**.

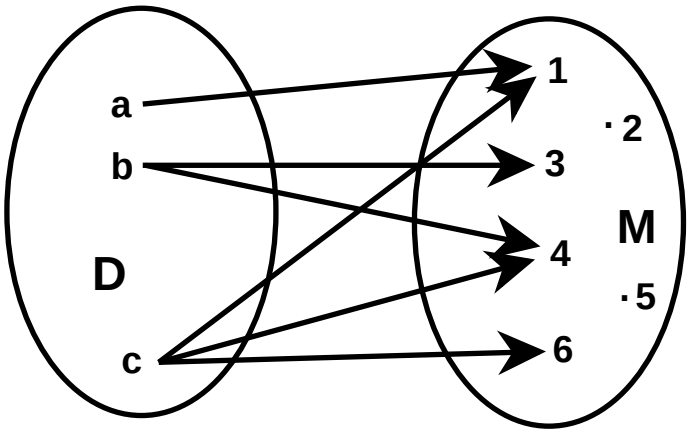
Durch eine linkstotale Relation (Abbildung) wird also einem *Urbild* immer ein *Bild zugeordnet*. Man spricht daher auch von einer *Zuordnung*. Die anvisierte Vorratsmenge M muss dabei aber nicht voll ausgenützt werden.

Symbole 8 (Abbildung) *: Bei einer Abbildung schreiben wir statt* $(a, b) \in \mathcal{R}$ *kurz* $a \longmapsto b$.

Beispiele:

1. In Abb.15.6 ist die Abbildung $\mathcal{R} = \{(a, 1), (b, 3), (b, 4), (c, 1), (c, 4), (c, 6)\} \subset D \times M$ gezeigt.

Abbildung 15.6: Relationsmenge und Abbildung



2. Durch die Zuordnung $x \longmapsto x^2$ wird z.B. eine Abbildung definiert mit $D = \mathbf{R}$ und $M = \mathbf{R}$. Dann ist $W = \mathbf{R}_0^+$ (positive reelle Zahlen oder null). M kann aber auch auf $\mathbf{R}_0^+$ reduziert werden.

Die Umkehrabbildungen

Wenn man die Elemente eines geordnetes Paares vertauscht, so entsteht ein neues geordnetes Paar: Die Menge der vertauschten Paare bilden auf natürliche Weise wiederum eine Relation. Wir nennen sie die *Umkehrabbildung*.

Definition 15.19 (Umkehrabbildung) *: Eine Abbildung $\mathcal{A}$ sei durch eine gegebene Relation $\mathcal{R}$ definiert: $\mathcal{A} = \mathcal{R} = \{(a,b) | a \in D \wedge b \in W \subseteq D \times W$. Dann heisst die Menge $\mathcal{A}^{-1} = \{(b,a) |\ a \in D \wedge b \in W\}$* **Umkehrabbildung** *zu $\mathcal{A}$.*

Es gilt daher: $\mathcal{A}^{-1} \subseteq W \times M$.

Funktionen

In der Praxis macht der Fall, wo einem Urbild mehrere Bilder zugeordnet werden können, vielfach keinen Sinn. Zu einer Auswahl von Messwerten von Strom und Spannung (Urbilder) möchte man einen eindeutigen Widerstand (Bild, Wert) berechnen können und nicht mehrere gleichzeitig geltende verschiedene Resultate akzeptieren. Für den Fall, wo die Bilder eindeutig sind, führen wir daher den Begriff *Funktion* ein. Dazu definieren wir die *Rechtseindeutigkeit* (vgl Abb. 15.7:

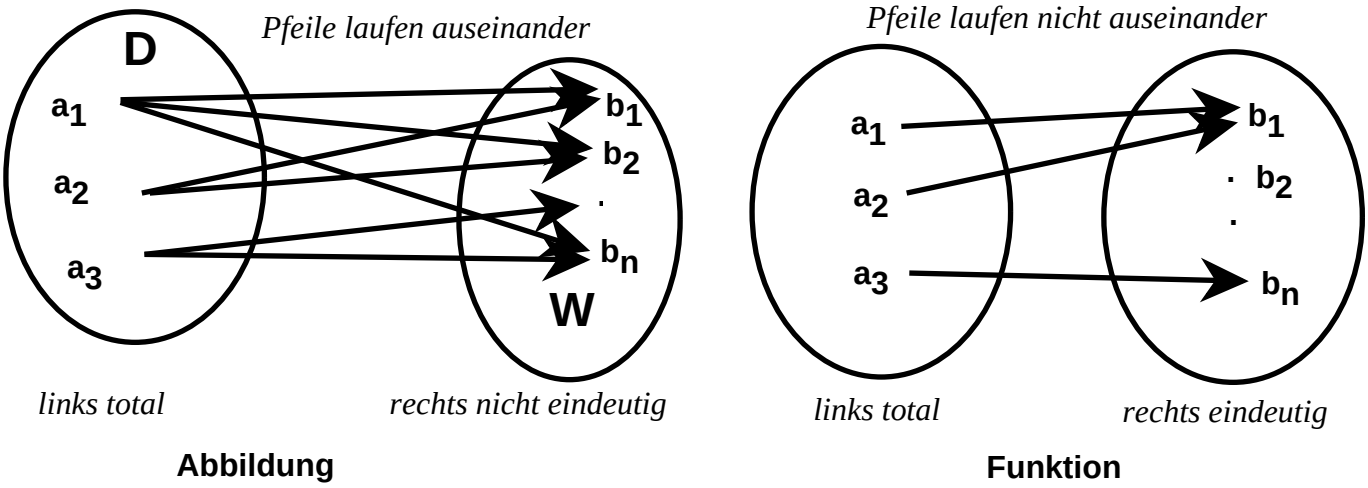
Definition 15.20 (Rechtseindeutigkeit) *:*
Gilt für eine Abbildung $(x \longmapsto y \wedge x \longmapsto z) \Longrightarrow y = z$, so nennen wir die Abbildung **rechtseindeutig**.

Definition 15.21 (Funktion) *: Eine rechtseindeutige Abbildung heisst* **Funktion**.

Bei einer Funktion laufen also von einem Urbild nie zwei oder mehrere Pfeile weg. Ein Urbild hat immer nur ein einziges Bild. Sei bei einer Funktion die Relationsmenge $\mathcal{R} = \mathcal{F}$. Dann könne wir sagen: Zu jedem $a \in D$ gibt es *genau ein* $b \in W$, sodass $(a,b) \in \mathcal{F}$ gilt. Symbolisch:

$$\forall_{a \in D}\ \dot{\exists}_{b_i n W} : (a,b) \in \mathcal{F} \qquad \dot{\exists} \text{ heisst „es gibt } \textit{genau} \text{ ein“} \ldots$$

Abbildung 15.7: Relationsmenge und Funktion



Diese Aussage ist normalerweise nicht umkehrbar, denn $\forall$ und $\exists$ dürfen nicht einfach vertauscht werden. Die Umkehrabbildung $\mathcal{F}^{-1}$ braucht daher nicht wieder eine Funktion zu sein.
Statt $(a,b) \in \mathcal{F}$ resp. $a \longmapsto b$ benützen wir künftig auch folgende symbolische Schreibweise:

Symbole 9 (Funktion) *:* $f : a \longmapsto b = f(a)$, $a \overset{f}{\longmapsto} b = f(a)$ *oder kurz* $b = f(a)$ *für die Elemente und* $f : D \longmapsto W = f(D)$ *für die Bereiche. Statt* D *resp.* W *schreiben wir auch* D_f *resp.* W_f*.*

Zur Sprechweise: Wir sagen nun: *„f ist die Funktions– oder Zuordnungsvorschrift*, durch die dem Urbild a das Bild b zugeordnet wird.“Für die Bildmenge gilt dann natürlich $W = f(D) = \{f(a)|a \in D\}$. Statt D resp. W schreiben wir dann auch D_f resp. W_f.
In der mathematischen Alltagssprache ist es üblich, statt von der Funktionsvorschrift kürzer nur von der *Funktion* zu reden, was uns wenig stören wird. Achtung jedoch, was die Gleichheit von Funktionen betrifft: Die Definition des Funktionsbegriffes hat zur Konsequenz, dass *zwei Funktionen genau dann gleich* sind, wenn ihre Relationsmengen gleich sind.

Beispiele:

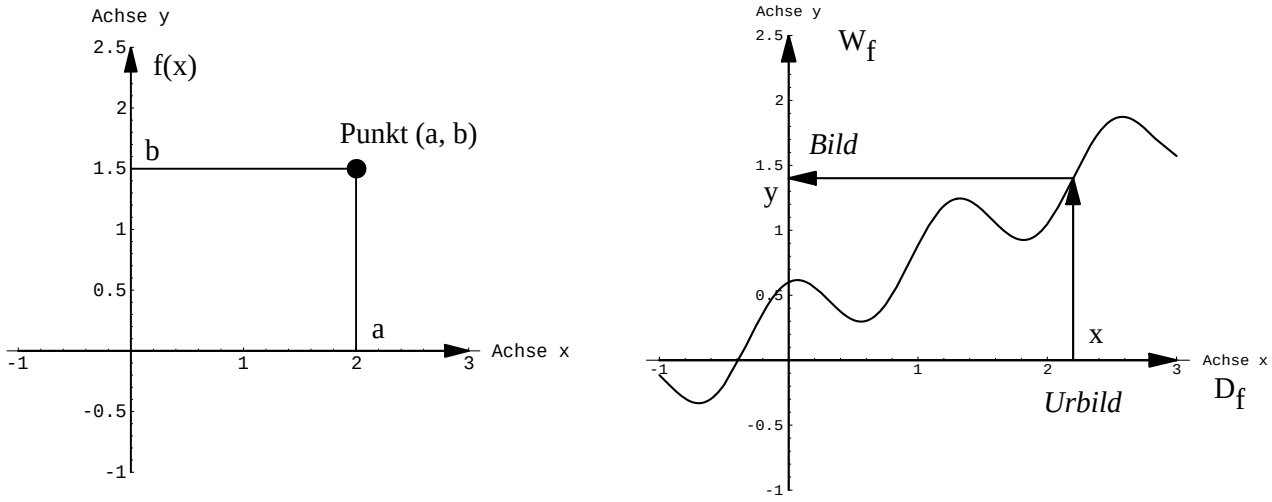
1. $f : x \longmapsto y = f(x) = x^2$, $D_f = \mathbf{R}$, $W_f = \mathbf{R}_\mathbf{0}^+$
2. $f : x \longmapsto y = f(x) = \frac{1}{x}$, $D_f = \dot{\mathbf{R}}$[2], $W_f = \dot{\mathbf{R}}$
3. $f : x \longmapsto y = f(x) = 7$, $D_f = \mathbf{R}$, $W_f = \{7\}$
4. $f : x \longmapsto y = f(x) = [x]$ (Gauss–Klammer–Funktion) [3], $D_f = \mathbf{R}$, $W_f = \mathbf{Z}$
5. $f : x \longmapsto y = f(x) = \begin{cases} x & : \quad x \in \mathbf{Q} \\ 5 & : \quad x \notin \mathbf{Q} \end{cases}$, $D_f = \mathbf{R}$, $W_f = \mathbf{Q}$
6. $f : x \longmapsto y = f(x) = \begin{cases} 0 & : \quad x \in \mathbf{Q} \\ 1 & : \quad x \notin \mathbf{Q} \end{cases}$ (Kamm–Funktion)[4], $D_f = \mathbf{R}$, $W_f = \{0,1\}$

[2] $\dot{\mathbf{R}} = \mathbf{R} \setminus \{0\}$
[3] $[x] = n$ für $x \in [n, n+1\}, n \in \mathbf{Z}$
[4] unendlich dichter Kamm

7. f : geometrischer Pfeil $\overrightarrow{PP'} \longmapsto$ Vektor mit dem Repräsentanten $\overrightarrow{PP'}$, D_f = Menge der Pfeile, W_f = Menge der Vektoren

8. $f : P = (x_1, x_2, x_3, x_4) \longmapsto \begin{pmatrix} \sin(x_1 \cdot x_2) \\ \cos(x_1 + x_3) \\ \tan(x_4) \end{pmatrix}$, $D_f = \mathbf{R}^4$, $W_f = \ldots$

Abbildung 15.8: Diagramme 1 (Graphen)



15.3.2 Funktionsgraphen

Wir betrachten eine gegebene Funktion $f : D_f \longmapsto W_f$. Dabei setzen wir voraus, dass D_f und W_f *geordnete Mengen*[5] sind (Fall 1), was z.B. bei $\mathbf{R}$ zutrifft. Das bedeutet, dass D_f und W_f jeweils mittels einer skalierten Linie, z.B. durch einen Zahlenstrahl oder durch eine Koordinatenachse bildlich dargestellt werden kann. Abweichend davon wollen wir für D_f auch Produktmengen $A \times B$ mit geordneten Mengen A und B zulassen. D_f ist dann eine Menge von geordneten Paaren, die sich als Punkte einer Fläche, z.B. einer Ebene, darstellen lassen (Fall 2). In beiden Fälle ist es möglich, die geordneten Paare (a, b) der Funktionsmenge (Relationsmenge) $\mathcal{F} = \{(a, b) | a = f(b)$ resp. $a \in D_f \wedge b \; in W_f\}$ in einem ebenen oder räumlichen Koordinatensystem[6] darzustellen. Wir vereinbaren unter den obigen Voraussetzungen:

Definition 15.22 (Funktionsgraph) *:*
Die Menge der geometrischen Punkte (a, b) *nennen wir* **Graphen** *der Funktion* f*.*

Zur bildlichen Darstellung des Graphen verwendet man meistens kartesische Koordinatensysteme. Im Falle 1 ist dann $a = x \in \mathbf{R}$ und $b = y \in \mathbf{R}$. (Vgl. Abb. 15.8.) Da ein Graph oft aus unendlich vielen Punkten besteht, ist es jeweils unmöglich, alle Punkte numerisch zu berechnen. Man behilft sich daher mit einer vernünftigen Auswahl, mit einer *Wertetabelle*.

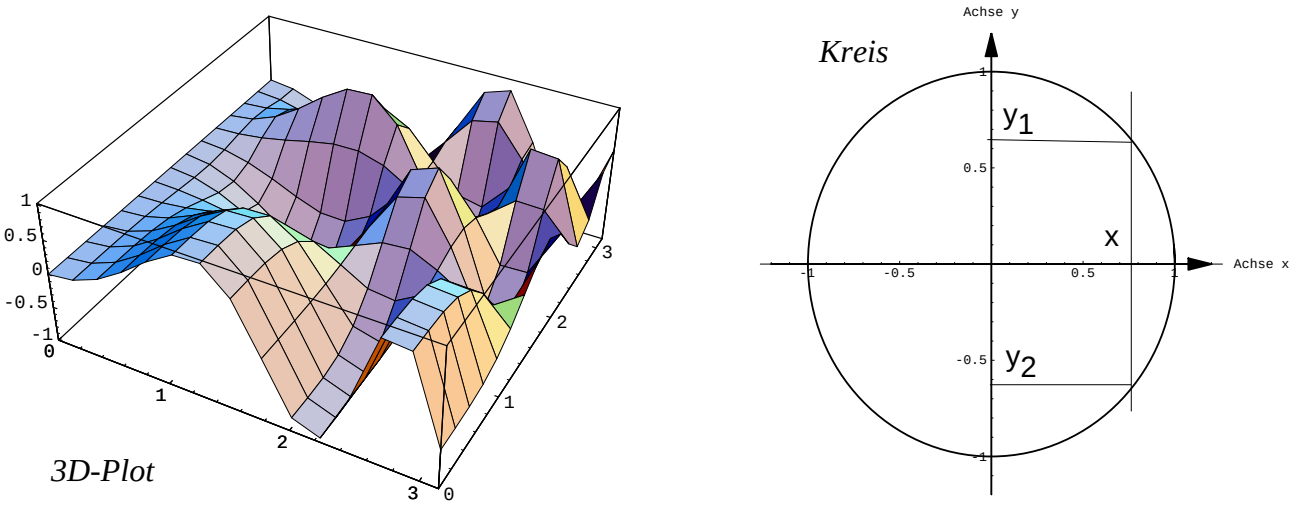
Im Falle 2, wo a schon als Punkt einer Ebene interpretiert werden kann, ist $a = (x,\ y) \in \mathbf{R}^2$ und $b = z \in \mathbf{R}$. (Vgl. Abb. 15.9.)

Beispiele bekannter Funktionen:

1. $f(x) = c = 3$: Konstante Funktion

[5] für zwei verschiedene Elemente ist eine strenge Ordnungsrelation erklärt
[6] Vgl. Mathematikkurs für Ingenieure, Teil 1 (Bibl.: wirz)

Abbildung 15.9: Diagramme 2 (Graphen)



2. $f(x) = ax + b$: Lineare Funktion
3. $f(x) = ax^2 + bx + c$: Quadratische Funktion
4. $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$: Polynomfunktion
5. $y = f(x)$ mit $D_f =$ *diskrete Menge*[7]: Diskrete Funktion
6. $f(x) = \sin(x)$: Trigonometrische Funktion etc.
7. Hingegen stellt der Kreis in Abb. 15.9 keine Funktion dar, da einem Wert x jeweils zwei Werte y_1 und y_2 zugeordnet werden.

In Abb Abb. 15.10 sind die Graphen der Funktionen $f(x) = x^2$ (kartesische Koordinaten) und $r(\phi) = 1.8(\phi + 0.5\sin(0.4\phi^2))/13$ (Polarkoordinaten) wiedergegeben.

15.3.3 Zusammengesetzte (hintereinandergeschaltete) Funktionen

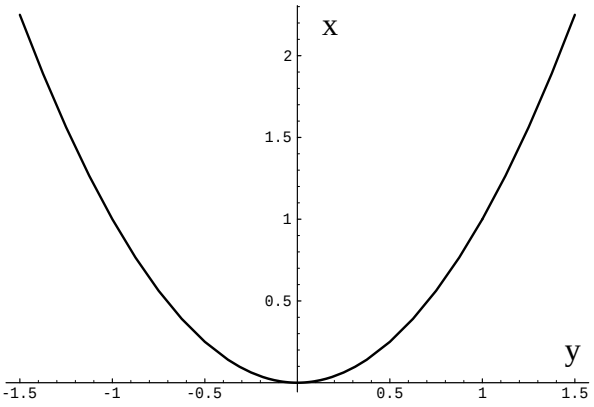
Wir betrachten eine Funktion f auf ihrem Definitionsbereich $A = D_f$. Der Wertebereich W_f von f sei eine Teilmenge der Menge B, auf der eine zweite Funktion g definiert ist: $B = D_g$. Der Wertegereich W_g von g ist umfasst daher den Wertebereich C der *Restriktion*[8] von g auf W_f. (Vgl. Abb.15.11.)
Wir können daher folgendes festhalten: Sei $c = g(b) \in W_g$ und $b = f(a) \in W_f$. Falls $W_f \subset D_g$ gilt, kann man auch $c = g(b) = g(f(a))$ bilden. Man hat daher eine neue, *zusammengesetzte Funktion* φ konstruiert, die a direkt in c (resp. die Menge A in die Menge C) abbildet:

$$\varphi : A \longmapsto C \quad \text{oder} \quad c = \varphi(a) = g(f(a)) \; \textit{oder}$$

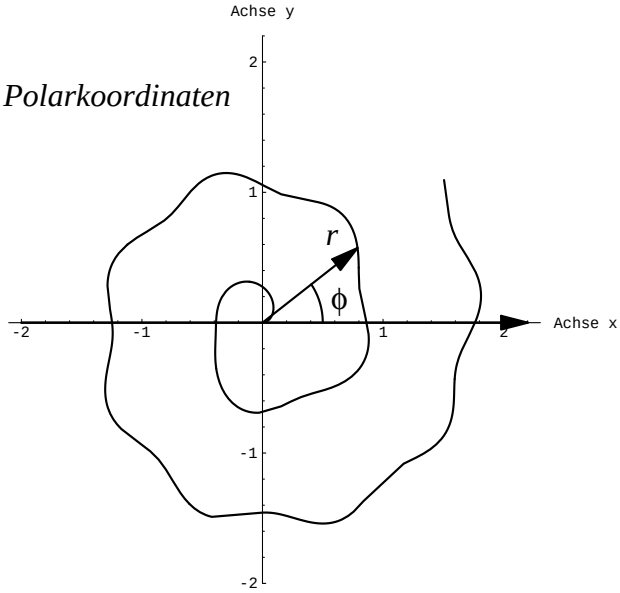
$$\underbrace{a \overset{f}{\longmapsto} b \overset{g}{\longmapsto} c}_{\overset{\varphi}{\longmapsto}}$$

[7] abzählbare Menge von isolierten Punkten
[8] Einschränkung

Abbildung 15.10: Diagramme 3 (Graphen)



Kartesisches Koordinatensystem



Da f und g linkstotal und rechtseindeutig sind, muss das auch für φ gelten, denn beim Zusammensetzen tritt weder rechts eine Mehrdeutigkeit auf noch wird links ein Element ausgelassen. Nun können wir die Operation $\circ$ (nacheinanderaudführen von Funktionen, auch *Verknüpfen*) definieren:

Definition 15.23 (Operation $\circ$) *:*

$$\varphi(a) = g(f(a)) := (g \circ f)(a) \quad \textit{resp.} \quad \varphi := g \circ f.$$

Beispiel: Sei $f(1) = c, \quad f(2) = a, \quad f(3) = a, \quad g(a) = \gamma, \quad g(b) = \beta, \quad g(c) = \alpha$. Dann ist $\varphi(1) = \alpha, \quad \varphi(2) = \gamma \quad$ und $\quad \varphi(3) = \gamma$.

Beim folgenden Satz ist es nicht nötig, Funktionen zu verlangen. Der Sachverhalt gilt allgemein für Abbildungen:

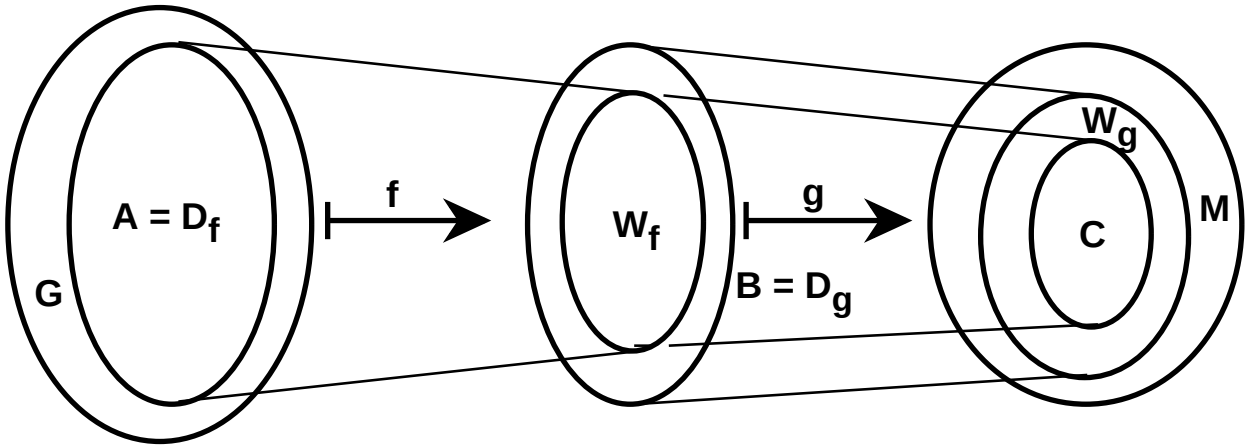
Satz 15.5 (Assoziativität von Abbildungen) *:*
Vor.: *$\varphi_1 = h \circ g$ und $\varphi_2 = g \circ f$ seien definierte Abbildungen. Weiter seien die Ausdrücke $(\varphi_1 \circ f)(x)$ und $(h \circ \varphi_2)(x)$ für ein bestimmtes $x \in D_f$ bildbar.*
Beh.: *Es gilt das Assoziativgesetz: $(h \circ g) \circ f = h \circ (g \circ f)$.*

Beweis: $x \in D_f$ sei ein beliebiges Element, das die Voraussetzung erfüllt. Dann gilt:

$$((h \circ g) \circ f)(x) = (\varphi_1 \circ f)(x) = \varphi_1(f(x)) = (h \circ g)(f(x)) = h(g(f(x))) \quad \text{und}$$
$$(h \circ (g \circ f))(x) = (h \circ \varphi_2)(x) = h(\varphi_2(x)) = h((g \circ f)(x)) = h(g(f(x))) \quad \text{und somit}$$
$$((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x) \forall_x, \quad \text{also} \quad (h \circ g) \circ f) = (h \circ (g \circ f)) \quad \text{q.e.d.}$$

Daher darf man beim Zusammensetzen von Abbildungen die Klammern weglassen.
Achtung: Zwar gilt für das Hintereinanderausführen resp. Verknüpfen von Funktionen das Assoziativitätsgesetz, ein Kommutativitätsgesetz gilt aber nicht! Allgemein ist $f \circ g \neq g \circ f$.
Z.B. ist $\sin(\sqrt{-\pi}) \neq \sqrt{\sin(-\pi)} = 0$

Abbildung 15.11: Hintereinandergeschaltete Funktionen



15.3.4 Funktionstypen, Umkehrfunktionen

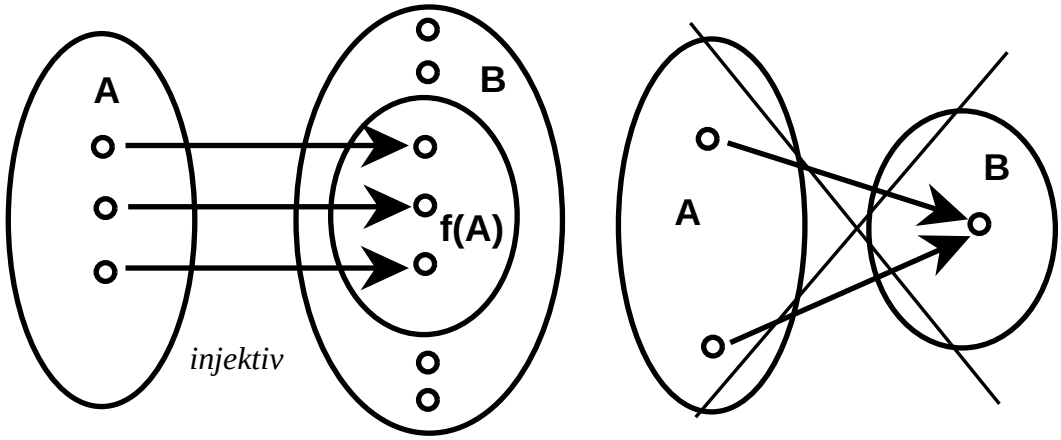
Injektiv, surjektiv, bijektiv

Um das Problem der Umkehrbarkeit von Funktionen studieren zu können, müssen wir erst einige Begriffe einführen, mit denen wir die Funktionen klassifizieren können.

Definition 15.24 (Injektivität) *: Eine Funktion f heisst* **injektiv**, *falls gilt:* $f(a) = f(b) \Longrightarrow a = b$.

In der Kontraposition heisst das: $a \neq b \Longrightarrow f(a) \neq f(b)$. Eine Veranschaulichung zeigt Abb. 15.12.

Abbildung 15.12: Injektiv

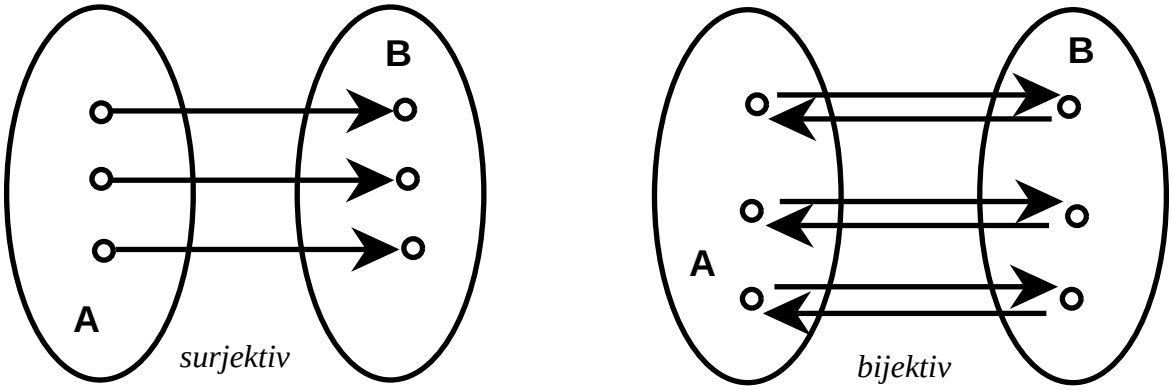


Definition 15.25 (Surjektivität) *: Eine Funktion f heisst* **surjektiv**, *falls gilt:* $f(A) = B$.

Im surjektiven Fall wird also der gesammte Wertevorrat ausgenützt. Jedes Element des Wertevorrats kommt auch als Bild vor. (Vgl Abb. 15.13.)

Definition 15.26 (Bijektivität) *: Eine Funktion f heisst* **bijektiv**, *wenn sie injektiv und surjektiv zugleich ist.*

Abbildung 15.13: Bijektiv



Im surjektiven Fall wird der gesammte Wertevorrat ausgenützt und jedes Bild genau einmal angenommen. (Vgl Abb. 15.13.) Wie in Abb. 15.13 denken wir uns nun Urbilder und Bilder durch abstrakte Pfeile verbunden. Da nun bei einer Funktion jedes Bild geanu ein Urbild hat (Rechtseindeutigkeit) und in einer richtigen „abstrakten graphischen Darstellung“ bei jedem Element des Wertevorrates genau ein Pfeil endet, kommt jedes Element des Urbild– und des Bildbereiches genau an einem Anfangs– oder Endpunkt eines gedachten Pfeiles vor. Kehrt man jetzt sämtliche Pfeile um, so vertauschen sich Bilder und Urbilder. Die Umkehrabbildung ist daher wieder eine bijektive Funktion (linkstotal, rechtseindeutig, injektiv, surjektiv). Man spricht hier von einer *ein–eindeutigen Zuordnung* der Elemente. Daher gilt der Satz:

Satz 15.6 (Existenz der Umkehrfunktion) *:*
Vor.: *Sei* $f : A \longmapsto B$ *bijektiv.*
Beh.:

1. f^{-1} *ist wieder eine Funktion:* $f^{-1} : B \longmapsto A.$
2. f^{-1} *ist auch bijektiv.*

Definition 15.27 (Umkehrfunktion) *: Ist* f^{-1} *wieder eine Funktion, so heisst sie* **Umkehrfunktion**.

Beispiel: Die erste Figur in Abb. 15.10 zeigt den Graphen von $f(x) = x^2$. Auf $D_f = \mathbf{R}_0^+$ (nicht–negative reelle Zahlen) ist f ersichtlicherweise bijektiv. Wir kennen die Umkehrfunktion: $f^{-1}(x) = +\sqrt{x}$. Auf $D_f = \mathbf{R}$ jedoch ist f^{-1} nicht umkehrbar, da jedes Bild ausser 0 zwei Urbilder hat: Z.B. $(-1)^2 = 1^2 = 1$.
Wenn $b = f(a)$ (d.h. $a \overset{f}{\longmapsto} b$) ist, so ist $f^{-1}(b) = a$, (d.h. $b \overset{f^{-1}}{\longmapsto} a$). Somit wird $f^{-1}(f(a)) = a$, $f(f^{-1}(b)) = b$ und weiter: $f(f^{-1}(f(a))) = f(a)$, $f^{-1}(f(f^{-1}(b))) = f^{-1}(b)$ etc.. Daher gilt:

Satz 15.7 (Identische Abbildung) *:*
Vor.: *Sei* $f : A \longmapsto B$ *bijektiv,* $a \in A$.
Beh.:

1. $(f^{-1} \circ f)(a) = a$, *d.h.* $(f^{-1} \circ f) = \triangle_{D_f}$
2. $(f \circ f^{-1})(b) = b$, *d.h.* $(f^{-1} \circ f) = \triangle_{W_f}$
3. $(f^{-1)^{-1}} = f$

$\triangle_{D_f}$ ist die Diagonalrelation oder *identische Abbildung* auf D_f, $\triangle_{W_f}$ ist die Diagonalrelation oder *identische Abbildung*[9] auf W_f. Für diese identischen Abbildungen gilt trivialerweise:

Satz 15.8 (Identische Abbildung) *:*
Vor.: *Sei f eine beliebige Funktion*
Beh.: $\triangle_{W_f} \circ f = f = f \circ \triangle_{D_f}$

Falls eine andere Funktion g ebenfalls D_f in W_f abbildet ($D_f \overset{g}{\longmapsto} W_f$), so kann man die identische Abbildung auch mit g verknüpfen:

Satz 15.9 (Identische Abbildung) *:*
Vor.: *Sei g eine Funktion mit $D_f \overset{g}{\longmapsto} W_f$.*
Beh.: $\triangle_{W_f} \circ g = g = g \circ \triangle_{D_f}$

Wenn umgekehrt die beiden möglichen Verknüpfungen zweier Funktionen immer die identische Abbildung ergeben, so kann man auf die Existenz der Umkehrfunktionen, d. h. auf die Bijektivität schliessen:

Satz 15.10 (Existenz der Umkehrfunktionen) *:*
Vor.: *Seien f und g beliebige Funktion mit $D_f \overset{f}{\longmapsto} W_f$ und $W_f \overset{g}{\longmapsto} D_f$.* .
Dazu gelte: $g \circ f = \triangle_A$ und $f \circ g = \triangle_B$
Beh.:

1. *f^{-1} und g^{-1} existieren, d.h. f und g sind bijektiv.*
2. *$f^{-1} = g$ und $g^{-1} = f$.*

Der Beweis dieses Satzes sei dem Leser überlassen. Hinweis: Man zeige zuerst, dass g eine Umkehrabbildung von f ist, was einfach geht. Dann muss man zwei Probleme lösen: Erstens ist zu zeigen, dass f injektiv ist. Am besten zeigt man das indirekt. Anschliessend ist zu zeigen, dass f surjektiv ist. Das geht ebenfalls indirekt. Dann hat man die Bijektivität von f. da der Satz symmetrisch in f und g ist, gilt das Bewiesene auch für g. Da $g \circ f = \triangle_A$ ist, folgt aus der Bijektivität $f^{-1} = g$.

Bemerkung: Im Fall wo für bijektive Funktion f_1, f_2 und f_3 gilt $D_{f_1} = W_{f_1} = D_{f_2} = \ldots = W_{f_3} = M$, sind die Gruppenaxiome erfüllt:

1. $(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$ (Assoziativirät)
2. $\triangle_M \circ f_i = f_i \circ \triangle_M$ (neutrales Element)
3. $f_i \circ f_i^{-1} = f_i^{-1} \circ f_i = \triangle_M$ (inverses Element)

Eine Gruppe ist eine algebraische Struktur[10]. Gruppen trifft man überall in der Mathematik[11] Der Gruppenbegriff hat seine Wichtigkeit daher, weil eine Gruppe diejenige Struktur ist, in der man Gleichungen lösen kann.

[9] *auch neutrale Abbildung*
[10] Algebraische Struktur: Menge, auf der Operationen erklärt sind
[11] Bei den Zahlen, Vektoren, bei geometrischen Operationen, bei den Matrizen etc..

15.4 Anhang aus dem Algebrascript

15.4.1 Spezielle Relationen

Die nachfolgenden Relationen sind durch die angegebenen logischen Aussagen definiert, die als wahr angenommen werden:
• *Les relations suivantes sont définies par les propositions logiques données qui sont considérées comme propositions vraies:*

⊘ **Identitäts– oder Diagonalrelation:** • **Relation diagonale:** $\mathcal{R} = \triangle_A = \{(a,a) \mid a \in A\}$

⊘ **Inverse Relation:** • **Relation inverse:** $\mathcal{R}^{-1} = \{(b,a) \mid (a,b) \in \mathcal{R}\} \rightsquigarrow |\mathcal{R}^{-1}| = |\mathcal{R}|$

⊘ **Reflexive Relation:** • **Relation réflexive:**
$\triangle_A \subseteq \mathcal{R}$, $\mathcal{R}$ reflexiv • *réflexive* $\Leftrightarrow \forall_{a\in A} : (a,a) \in \mathcal{R} \subseteq A^2$

⊘ **Antireflexive Relation:** • **Relation antiréflexive:** $\forall_{a\in A} : (a,a) \notin \mathcal{R}$

⊘ **Symmetrische Relation:** • **Relation symétrique:** $\forall_{(a,b)\in\mathcal{R}} : (a,b) \in \mathcal{R} \Rightarrow (b,a) \in \mathcal{R}$

⊘ **Streng antisymmetrische Relation:** • **Relation antisymétrique stricte:**
$\forall_{(a,b)\in\mathcal{R}} : (a,b) \in \mathcal{R} \Rightarrow (b,a) \notin \mathcal{R}$

⊘ **Milde antisymmetrische Relation:** • **Relation antisymétrique non stricte:**
$\forall_{(a,b)\in\mathcal{R}} : (a,b) \in \mathcal{R} \ \wedge \ (b,a) \in \mathcal{R} \Rightarrow a = b$

⊘ **Asymmetrische Relation:** • **Relation asymétrique:** $\forall_{(a,b)\in\mathcal{R}} : (a,b) \in \mathcal{R} \ \dot\vee \ (b,a) \in \mathcal{R}$

⊘ **Transitive Relation:** • **Relation transitive:** $\forall_{(a,b)\in\mathcal{R}} : ((a,b) \in \mathcal{R} \wedge (b,c) \in \mathcal{R}) \Rightarrow (a,c) \in \mathcal{R}$

⊘ **Äquivalenzrelation:** • **Relation d'équivalence:**
Reflexiv, symmetrisch und transitiv. • *Réflexive, symétrique et transitive.*

$\rightsquigarrow$ Führt zu Klasseneinteilung: **Äquivalenzklassen**
• *Mène à un classement, une classification:* **classes d' équivalence**.

⊘ **Totale Relation:** • **Relation totale:** $\forall_{(a,b)\in\mathcal{R}} : ((a,b) \in \mathcal{R} \ \vee \ (b,a) \in \mathcal{R})$

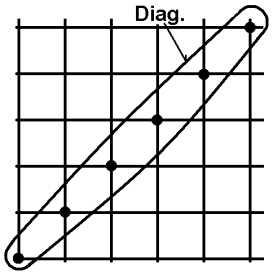
⊘ **Teilordnungsrelation:** • **Relation d'ordre partielle:**
Reflexiv, antisymmetrisch und transitiv. • *Réflexive, antisymétrique et transitive.*

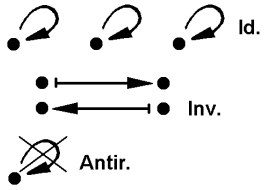
⊘ **Ordnungsrelation (mild):** • **Relation d'ordre (non stricte):**
Reflexiv, antisymmetrisch, transitiv und total. • *Réflexive, antisymétrique, transitive et totale.*

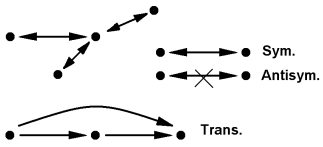
⊘ **Strikte Halbordnung:** • **Relation d'ordre partielle de façon stricte:**
Asymmetrisch und transitiv. • *Asymétrique et transitive.*

⊘ **Strenge Ordnungsrelation:** • **Relation d'ordre stricte:**
Antireflexiv, streng antisymmetrisch und transitiv. • *Antiréflexive, strictement antisymétrique et transitive.*

⊘ **Lexikographische Ordnung:** • **Relation d'ordre lexicographique:**
Nach dem Ordnungsprinzip des Alphabeths. • *D'après le principe de l'alphabet.*







Man sieht sofort: • *On voit tout de suite:*

Satz: • **Théorème:** **Vor.:** • **Hyp.:**

$\mathcal{R}$ streng antisymmetrisch und total
• $\mathcal{R}$ *strictement antisymétrique et totale*

Beh.: • **Thè.:**

$\mathcal{R}$ asymmetrisch • $\mathcal{R}$ *asymétrique*

Satz: • **Théorème:** **Vor.:** • **Hyp.:**

$\mathcal{R}$ Teilordnung auf M
• $\mathcal{R}$ *relation d'ordre partielle sur* M
$SR = \{(x, y) \in M \times M \mid ((x, y) \in \mathcal{R}) \ \wedge \ (x \neq y)\}$

Beh.: • **Thè.:**

SR ist strikte Teilordnung (Halbordnung)
• SR *est relation d'ordre partielle de façon stricte*

Beweis: • **Preuve:**

$\mathcal{R}$ Teilordnung • $\mathcal{R}$ *ordre partiel* $\rightsquigarrow$ SR antisymmetrisch • SR *antisymétrique*

Problem: SR strikt? D.h. SR asymmetrisch, transitiv? • *Problème:* SR *stricte? Ç.v.d.* SR *asymétrique, transitive?*

Nach Definition von SR: • *D'après la définition de* SR*:*

$SR = \{(x, y) \in M \times M \mid ((x, y) \in \mathcal{R}) \ \wedge \ (x \neq y)\} \rightsquigarrow \ ((x, y) \in SR \ \wedge \ (y, z) \in SR) \ \Rightarrow \ ((x \neq y) \ \wedge \ (y \neq z))$

$\rightsquigarrow$ Problem: • *Problème:* $(x \neq z)$? $(\rightsquigarrow \ (x, z) \in SR$?)

Sei • *Soit* $x = z \rightsquigarrow \ (SR \ni (x, y) = (z, y)) \ \wedge \ (SR \ni (y, z) = (y, x))$
$\Rightarrow \ ((x, y) \in SR \subseteq \mathcal{R}^2 \ \wedge \ (y, x) \in SR \subseteq \mathcal{R}^2) \ \Rightarrow \ x = y \ \Rightarrow \ y = x = z \ \Rightarrow \ ((x, y) \notin SR \ \wedge \ (y, z) \notin SR)$
$\rightsquigarrow$ Widerspruch! • *Contradiction!* ☺

15.5 Übungen

Übungen finden sich in *DIYMU* (Bibl.: wirz1) sowie in der klassischen Schulbuchliteratur für Berufsschulen und die Gymnasialstufe. Achtung: Die Nummerierung der Kapitel im *DIYMU* ist unabhängig!

Kapitel • Chapitre 16

Vorwort zur Einführung in die Boolsche Algebra

Liebe Leserin, lieber Leser,

Das Thema *Boolsche Algebra* gehört zu den klassischen Wissensgebieten für Elektroingenieure und Informatiker. Für einigen Elektroberufe ist es auch ein wesentlicher Bestandteil der Berufsbildung.
Hier soll das Theme jedoch nicht nur vom praktischen Standpunkt der Schaltalgebra her beleuchtet werden. Es geht uns vielmehr darum, das Gebiet vom Hintergrund der Mathematik her zu betrachten, um damit diejenigen theoretischen Kenntnisse zu vermitteln, die an einer Hochschule zu verlangen sind. Dabei geht es nicht so sehr ums Detail. Wichtiger sind die Zusammenhänge und der Überblick. Nur so kann ein Verständnis dafür wachsen, dass z.B. die Schaltalgebra nur ein Spezialfall unter vielen einer Boolschen Algebra ist.
Dieser Text ist in Skriptform abgefasst. Das bedeutet, dass er in äusserst knapper Fassung nur das wesentliche Skelett des zu lernenden Stoffes wiedergibt. Für weitere und ausführliche Erklärungen, Beispiele, exakte Beweise und ausgeschmücktere Ausführungen ergeht daher an den Studenten der Rat, ein oder mehrere Lehrbücher beizuziehen. Studieren bedeutet zu einem wesentlichen Teil, sein Wissen selbständig mit Hilfe der Literatur zu erweitern, streckenweise sogar selbständig zu erarbeiten, zu festigen und anzuwenden. Ein Skript ist dabei nur ein Wegweiser – und nie ein Lehrbuchersatz. Welche Lehrbücher jemand verwenden will, bleibt seinem eigenen Gutdünken überlassen . Das Thema Boolsche Algebra findet sich in vielen Unterrichtswerken dargestellt. Beispiele enthalten Deller (Bibl.: deller), Mendelson (Bibl.: mendelson), Dörfler, Peschek (Bibl.: dorflerPeschek), Brenner, Lesky, Band 1 (Bibl.: brennerlesky) .

Im Sommer 1996 Der Autor

Du gleichst dem Geist, den du begreifst . . .

Der Erdgeist in Goethes Faust

Kapitel • Chapitre 17

Einführung in die Boolsche Algebra

17.1 Einleitung

17.1.1 Ein Vergleich zwischen Aussagenlogik und Mengenalgebra

Beim Aufbau der Mengenlehre[1] ist offenbar geworden, dass in der Mengenalgebra Gesetze gelten, zu denen es in der Ausagenlogik entsprechende Gesetze gibt. Z.B. ist das Kommutativitätsgesetz bei der Bildung der Schnittmenge ($A \cap B = B \cap A$) auf das Kommutativgesetz für den Junktor $\wedge$ in der Aussagenlogik abgestützt worden $X \wedge Y \equiv Y \wedge X$. Offenbar gibt es formale Gemeinsamkeiten und ebenso Unterschiede zwischen der Aussagenlogik und der Mengenalgebra. In der Folgenden Tabelle stellen wir jeweils entsprechende Objekte aus den beiden Theorien gegenüber. Das bietet eine Grundlage, bezüglich der die beiden Seiten verglichen werden können.

Aussagenlogik	Mengenlehre
Sprachelemente und syntaktisches Vokabular	Elemente
Aussagen	Mengen
Aussagenvariablen	Mengenvariablen
Zuordnung Variable $\mapsto$ Wahrheitswert	Zuordnung Menge $\mapsto$ Mächtigkeit
Junktoren $\neg, \wedge, \vee \ldots$	Operationen $^{-}, \cup, \cap \ldots$
Gesetze: Kommutativität	Duale Gesetze: Kommutativität
Distributivität	Distributivität
$\vdots$	$\vdots$

Offenbar gibt es zwischen den Begriffen links und denen rechts eine Entsprechung. Diejenigen Leser, die schon etwas Schaltalgebra kennen, wissen, dass man genauso diese der Aussagenlogik oder der Mengenalgebra gegenüberstellen kann. Damit taucht die Frage auf, ob es hinter der Aussagenlogik, der Mengenalgebra und andern solchen Disziplinen nicht eine gemeinsame *abstrakte algebraische Struktur*[2] (oder *Verknüpfungsgebilde*) gibt. Eine solche gibt es tatsächlich. Um den Rahmen für das Studium einer solchen Struktur zu schaffen, bedarf es aber etwas Vorarbeit. Dazu müssen wir uns vorerst über das Wesen und den abstrakten Aufbau der Mathematik unterhalten.

17.1.2 Aufbaumethodik und Problemkreise

Aufbaumethodik, mathematische Struktur

In einem wesentlichen Teil der Mathematik richtet man heute das Interesse auf die oben erwähnten *mathematischen Strukturen*. Solche Strukturen sind grundlegend, denn die Sätze, die in ihnen gelten,

[1] Vgl. Teil 3

[2] Eine algebraische Struktur ist eine Menge, auf der Operationen definiert sind.

gelten dann auch in allen speziellen Interpretationen solcher Strukturen. Man braucht die Beweise dann nur einmal abstrakt zu führen, was Aufwand spart. Ein einfachstes Beispiel dazu: Wenn man einmal weiss, dass $2 + 2 = 4$ ist, so muss man ihm nicht mehr beweisen, dass $2\,\mathrm{kg} + 2\,\mathrm{kg} = 4\,\mathrm{kg}$ oder $2\,\mathrm{m} + \mathrm{m}2 = 4\,\mathrm{m}$ ist. Der Beweis für den abstrakten Fall genügt. Die Interpretation von 2 spielt keine Rolle.
Ein anderes Beispiel: In Teil 3 haben wir den Begriff *Äquivalenzrelation* kennengelernt. Wir wissen: Sobald man eine Äquivalenzrelation hat, kann man Äquivalenzklassen bilden. Ob man eine Relation zwischen geometrischen Pfeilen oder zwischen ganzen Zahlen betrachtet, ist egal. Beide Male entstehen Äquivalenzklassen: Einmal z.B. Vektoren, das andere Mal z.B. Restklassen.
In der Mathematik studiert man nun viel allgemeiner *mathematische Systeme*, die man mit Hilfe der Regeln der Logik aufbaut. Diese bestehen aus folgenden Komponenten:

Mathematische Systeme:

- *Grundbegriffe* und dazwischen *Grundrelationen*.
- *Axiome:* Axiome sind grundlegende Sätze (Aussagen), die für den Aufbau der Theorie als wahr angenommen werden. Die Theorie ist dann nur richtig, wenn die Axiome erfüllt sind. Z.B. das in der Euklidschen Geometrie gültige Parallelenaxiom ist in einer Nichteuklidschen Geometrie, z.B. in der Kugelgeometrie oder in der hyperbolischen Geometrie ungültig. Vgl. z.B. Grosses Handbuch der Mathematik (Bibl.: gellert).
- *Ein Deduktionsgerüst* oder Ableitungsgerüst. Ein solches Gerüst besteht aus Definitionsverfahren (Regeln, die beim Definieren zu befolgen sind), logischen Schlussregeln (vgl. z.B. Aussagenlogik) und Beweismethoden.
- Die *Theorie*, d.h. die Menge der abgeleiteten Sätze.

Die mathematische Aufbaumethode führt also von akzeptierten Grundgebilden, Regeln, Axiomen und gesicherten Begriffe mittels der Logik zur Theorie. Ein mathematisches System lässt meist spezielle Interpretationen zu. Eine solche Interpretation nennen wir *Modell des Systems*.
Z.B. sind die ganzen Zahlen mit der Addition ein spezielles Modelle einer kommutativen Gruppe[3]. Ebenso die Drehungen von geometrischen Figuren einer Ebene um einen Punkt P. Später werden wir auch zeigen, dass gewisse Teile der Aussagenlogik, der Mengenalgebra und die Schaltalgebra spezielle Modelle einer gewissen *Boolschen Algebra* sind.

Problemkreise in einem mathematischen System

Wegen den gemachten Erfahrungen beschäftigt sich die Mathematik immer wieder mit den nachfolgend beschriebenen wichtigen Problemkreisen:

Problemkreise in einem mathematischen System:

1. Die *Widerspruchsfreiheit* des Axiomensystems: Man würde es nicht akzeptieren, wenn eine falsche Aussage hergeleitet, d.h. bewiesen werden könnte. In der Mathematik will man sicher sein, dass die hergeleiteten Aussagen stimmen. Die Wiederspruchsfreiheit muss also bewiesen werden.
2. Die *Vollständigkeit* eines Axiomensystems bezüzglich einem gegebenen Modell: Lässt sich jeder vermutete Satz aus dem Axiomensystem deduzieren?.
3. Die *Unabhängigkeit der Axiome*: Folgt nicht schon ein Axiom aus den andern Axiomen? Aus ästethischen und ökonomischen Gründen möchte man unnötigen Ballast abwerfen.
4. Die *Ableitung der Theorie*: Wie finde ich die wesendlichen, erkenntnisbringenden Sätze?

Diese Probleme zu lösen, ist Aufgabe der Mathematiker. Die Anwendung der gefundenen und so gesicherten Theorie geht auch den Ingenieur und den Naturwissenschaftler etwas an. Wenn wir im Folgenden nun ein Axiomensystem betrachten, können wir davon ausgehen, dass die Mathematiker dazu obige Probleme $1 - 3$ gelöst haben.

[3] Der Gruppenbegriff ist in Teil 3 erklärt worden.

17.2 Verbände oder Gitter

Ein *Verband* ist eine spezielle algebraische Struktur. Um ihn zu definieren, führen wir die folgenden Symbole ein:

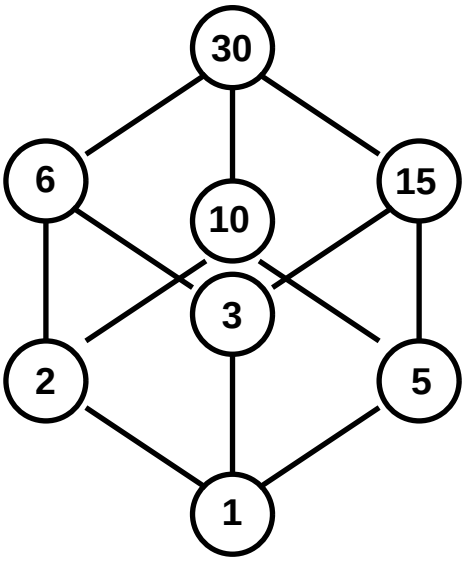
Symbole 10 (Verbandsoperationen) *: $\sqcup$ und $\sqcap$ seien irgendwelche zweistelligen Verknüpfungen.*

(Beispiele von zweistelligen Verknüpfungen sind $\cup$, $\cap$, $+$, $-$, $\wedge$, $\vee$, $\times$ etc.)
Sei Weiter $\mathcal{V}$ eine gegebene Menge.

Definition 17.1 (Verband) *:*
$(\mathcal{V}, \sqcap, \sqcup)$ *heisst genau dann* **Verband**, *wenn für alle* $a, b, c \in \mathcal{V}$ *die folgenden* **Axiome** *erfüllt sind:*

(1)	*Kommutativgesetze*	$a \sqcap b$	$=$	$b \sqcap a$	*und dual dazu:*	$a \sqcup b$	$=$	$b \sqcup a$
(2)	*Assoziativgesetze*	$(a \sqcap b) \sqcap c$	$=$	$a \sqcap (b \sqcap c)$	*und dual dazu:*	$(a \sqcup b) \sqcup c$	$=$	$a \sqcup (b \sqcup c)$
(3)	*Absorptionsgesetze*	$a \sqcap (a \sqcup b)$	$=$	a	*und dual dazu:*	$a \sqcup (a \sqcap b)$	$=$	a

Abbildung 17.1: Hasse–Diagramm



Hasse-Diagramm zur Relation "a ist Teiler von 30"

Beispiele:

1. $(\mathcal{V}, \sqcap, \sqcup) = (\wp(M), \cap, \cup)$. (Mengenlehre: Potenzmenge)
2. $(\mathcal{V}, \sqcap, \sqcup) = \{w, f\}, \wedge, \vee)$. (Verknüpfung wahrer oder falscher Aussagen)
3. $(\mathcal{V}, \sqcap, \sqcup) = (V_k, \mathrm{ggT}, \mathrm{kgV})$. (Dabei ist $V_k = \{n \in \mathbf{N} \mid n|k, k \in \mathbf{N}\}$)[4] und $(a \sqcap b) = \mathrm{ggT}(a, b), (a \sqcup b) = \mathrm{kgV}(a, b)$.[5] Dieser Verband heisst *Teilerverband.*
4. Der Untergruppenverband: Sei $\mathcal{V} = \{$Untergruppen einer Gruppe G und $\sqcap$ das Zeichen für die Bildung einer gemeinsamen Untergruppe, $\sqcup$ dasjenige für die Bildung einer gemeinsamen Obergruppe.[6]

In Abb. 17.1 kann man für Beispiel 3 rasch nachprüfen, dass die Verbandsaxiome erfüllt sind. Wenn bei einer Zahl weiter unten die Linien von zweien Zahlen weiter oben her zusammenlaufen, so steht unten der ggT der Zahlen weiter oben. Laufen umgekehrt zwei Linien bei einer Zahl weiter oben zusammen, so steht weiter oben das kgV der beiden Zahlen weiter unten.

[4] $n|k$ heisst „n teilt k“.
[5] ggT ist der grösste gemeinsame Teiler, kgV das kleinste gemeinsame Vielfache.
[6] Eine Untergruppe entsteht durch eine Teilmenge der Gruppenelemente, die wiederum Gruppe ist.

17.3 Boolsche Verbände oder Boolsche Algebren

Definition 17.2 (Distributiver Verband) *:*
Ein Verband $(\mathcal{V}, \sqcap, \sqcup)$ *heisst genau dann* **distributiv**, *wenn für alle* $a, b, c \in \mathcal{V}$ *zusätzlich die folgenden Distributivgesetze (***Axiome***) erfüllt sind:*

(4) $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$ *und dual dazu:* $a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$

Beispiele: Man prüft sofort nach, dass es sich in obigen Beispielen 1 bis 3 um distributive Verbände handelt.

Definition 17.3 (Boolscher Verband) *: Ein Verband* $(\mathcal{V}, \sqcap, \sqcup)$ *heisst genau dann* **komplementär** *(***Boolscher**[7] **Verband**, **Boolsche Algebra***), wenn zusätzlich die folgenden* **Axiome** *erfüllt sind:*

(5) a) $\exists_{\text{neutrales Element } \mathbf{e} \text{ für } \sqcap} : \forall_{a \in \mathcal{V}} \quad a \sqcap e = a$ *(e:* **Einselement***).*

b) $\exists_{\text{neutrales Element } \mathbf{n} \text{ für } \sqcup} : \forall_{a \in \mathcal{V}} \quad a \sqcup n = a$ *(n:* **Nullelement***).*

(6) $\forall_{a \in \mathcal{V}} \dot{\exists}_{\text{inverses Element } \bar{\mathbf{a}}}$*:* *a)* $a \sqcap \bar{a} = n$ *b)* $a \sqcup \bar{a} = e$

Das zu a inverse Element $\bar{a}$ *heisst auch* **Komplement** *von a.*

Wegen dem Komplement schreiben wir statt $(\mathcal{V}, \sqcap, \sqcup)$ nun $(\mathcal{V}, \sqcap, \sqcup, \bar{\ })$.

Beispiele:

1. Der Mengenverband $(\wp(M), \cap, \cup, \bar{\ })$ ist ein Boolscher Verband. Wir setzen: $M = e$ und $\{\} = n$. Dann ist:

$$A \cap \bar{A} = \{\} \qquad A \cap M = A$$
$$A \cup \bar{A} = M \qquad A \cup \{\} = A$$

2. Der Teilerverband $(V_k, \text{ggT}, \text{kgV})$ ist ein Boolscher Verband, falls k keine mehrfachen Primfaktoren enthält.

17.4 Schaltalgebra

Bei elektrischen Schaltern unterscheiden wir zwei mögliche Zustände:

- Schalter geschlossen: Strom kann fliessen (**Leitwert**[8] $= L$)
- Schalter offen: Strom kann nicht fliessen (**Leitwert** $= \emptyset$).

Vgl. dazu Abb 17.2, Schalterdarstellung[9]. (Interessant sind nun die Kombinationen von Schaltern, die ebenfalls in Abb 17.2 gezeigt sind.

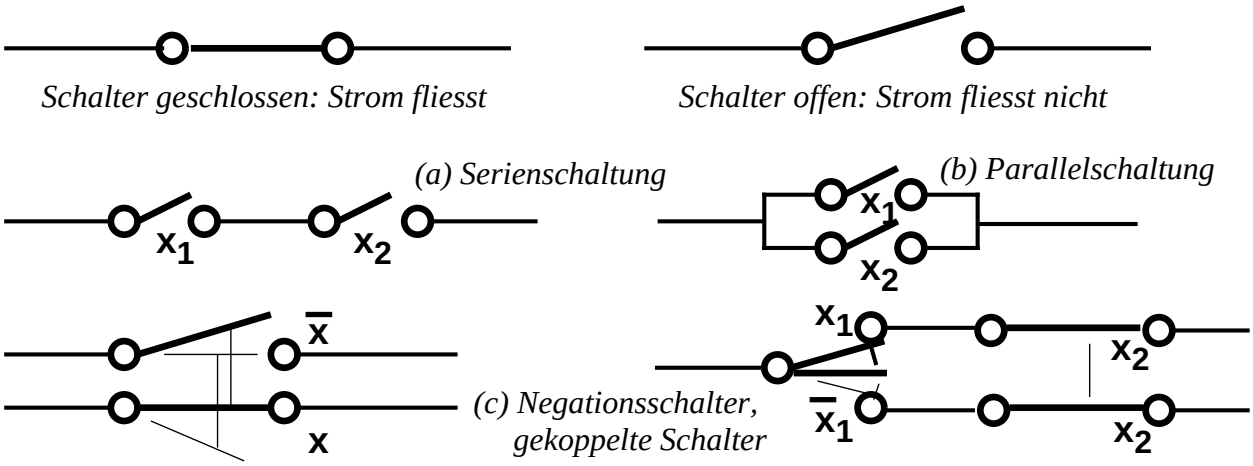
Für den jeweiligen Leitwert eines Schalters benutzen wir die Variable x resp. x_i, und für die Darstellung des Gesamtleitwerts x einer Schaltung durch die Leitwerte x_i der einzelnen Schalter benützen wir die folgende symbolische Schreibweise:

Symbole 11 *:*

Serieschaltung:	$x = x_1 \cdot c_2$
Parallelschaltung:	$x = x_1 + c_2$
Negationsschalter:	$\bar{x} = L$ *genau dann wenn* $x = \emptyset$.
Gekoppelte Schalter:	$x_1 = L$ *genau dann wenn* $x_2 = L$.

[7] Zu Ehren von George Boole (1815 – 1864), der eine solche Struktur bei der Untersuchung der Gesetze der Logik fand.
[8] Vgl. Physik.
[9] Was die in der Elektronik üblichen Gatterdarstellung *(Gates, logische Gatter)* betrifft, sei auf die Fachliteratur in der Elektronik verwiesen.

Abbildung 17.2: Schalter und einfache Kombinationen



Diese Verknüpfpungszeichen benennen wir wie in der Zahlenalgebra resp. der Mengenlehre mit *mal* (Produkt), *plus* (Summe) und *Komplement* (Technik: Negationsschalter, vgl.[10], [11]).
Die Leitwerte der Verknüpfungen definieren wir der physikalischen Realität entsprechend durch folgende zutreffenden Aussagen:

Definition 17.4 (Verknüpfungen von Leitwertvariablen) *:*

1. $x = x_1 \cdot x_2 = L \iff x_1 = L \wedge x_2 = L$
2. $x = x_1 + x_2 = \emptyset \iff x_1 = \emptyset \wedge x_2 = \emptyset$
3. $\bar{x} = L \iff x = \emptyset$

Da die Variablen die beiden Werte $\emptyset$ und L annehmen können, gelten die Verknüpfungen natürlich auch für die Werte. Das Produkt und die Summe folgen somit den gleichen Gesetzen wie sie bei $\wedge$ und $\vee$ in der Aussagenlogik bestehen. Daher haben wir die folgenden Verknüpfungstabellen:

Var	x_1	x_2	$x_1 \cdot x_2$
$t(Var)$	$\emptyset$	$\emptyset$	$\emptyset$
	$\emptyset$	L	$\emptyset$
	L	$\emptyset$	$\emptyset$
	L	L	L

Var	x_1	x_2	$x_1 + x_2$
$t(Var)$	$\emptyset$	$\emptyset$	$\emptyset$
	$\emptyset$	L	L
	L	$\emptyset$	L
	L	L	L

Für das Komplement folgt trivialerweise der Satz:

Satz 17.1 (Komplemente der Leitwerte) *:* $\bar{L} = \emptyset \qquad \bar{\emptyset} = L$

Jetzt sind wir soweit, dass wir die *mathematische Definition der Schaltalgebra* geben können:

Definition 17.5 (Schaltalgebra) *:*
Die algebraische Struktur $(\{\emptyset, L\}, +, \cdot, \bar{\ })$ *heisst* **Schaltalgebra**.

[10] Ein Schalter 1 ist Negationsschalter eines Schalters 2, falls Schalter 1 immer genau dann offen ist, wenn Schalter 2 geschlossen ist.
[11] Ein Schalter 1 ist gekoppelt mit einem Schalters 2, falls Schalter 1 immer genau dann offen ist, wenn Schalter 2 offen ist.

Es gilt der Satz:

Satz 17.2 (Schaltalgebra als Boolscher Verband) *: Die Schaltalgebra ist eine Boolsche Algebra oder ein Boolscher Verband.*

Aus den eben dargelegten Tabellen und dem Satz über die Komplemente der Leitwerte ist ersichtlich, dass formal in der Schaltalgebra dieselben Gesetze gelten wie in der Aussagenlogik bei $\wedge$, $\vee$ und $\neg$. Daher sind die Axiome einer Boolschen Algebra erfüllt: Sie sind von der Aussagenlogik her übertragbar – oder formal genau gleich beweisbar wie dort.

17.5 Der Satz von Stone

Zwei algebraische Strukturen $(\mathcal{V}, \circ, \diamond, \bullet, \ldots)$ und $(\tilde{\mathcal{V}}, \tilde{\circ}, \tilde{\diamond}, \tilde{\bullet}, \ldots)$ nennen wir *isomorph*, wenn sich die Elemente der beiden Mengen $\mathcal{V}, \tilde{\mathcal{V}}$ gegenseitig (d.h. bijektiv) entsprechen und entsprechende Operationen (z.B. $\circ$ und $\tilde{\circ}$ zu sich entsprechenden Resultaten führen. Die bijektive Zuordnung der Elemente wird also durch die Operationen nicht gestört. Die durch die bijektive Zuordnung gegebene Funktion φ nennen wir daher *strukturerhaltend*. Symbolisch schreiben wir für isomorphe Strukturen:

Symbole 12 (Isomorphe algebraische Strukturen) *:*

$$(\mathcal{V}, \circ, \diamond, \bullet, \ldots) \cong (\tilde{\mathcal{V}}, \tilde{\circ}, \tilde{\diamond}, \tilde{\bullet}, \ldots)$$

Formal definieren wir die Isomorphie so:

Definition 17.6 (Isomorphe algebraische Strukturen) *:*
Die algebraische Struktur $(\mathcal{V}, \circ_1, \circ_2, \circ_3, \ldots)$ *heisst* **isomorph** *zur algebraischen Struktur* $(\tilde{\mathcal{V}}, \tilde{\circ}_1, \tilde{\circ}_2, \tilde{\circ}_3, \ldots)$*, falls es eine bijektive Funktion* $\varphi : \mathcal{V} \longmapsto \tilde{\mathcal{V}}$ *gibt, für die bei allen Operationen* $\circ_i$ *gilt:* $\varphi(a \circ_i b) = \varphi(a)\, \tilde{\circ}_i\, \varphi(b)$ *bei beliebigen Elementen* a *und* $b \in \mathcal{V}$*.*

Die Isomorphie stiftet daher eine Relation „auf einer Menge von algebraischen Strukturen S“. (D.h. sie definiert eine Teilmenge von $S \times S$). Trivialerweise gilt der Satz:

Satz 17.3 (Isomorphieklassen) *: Die Isomorphierelation ist eine Äquivalenzrelation.*

Daraus folgt, dass die algebraischen Strukturen in *Isomorphieklassen* (Äquivalenzklassen) zerfallen. Weiter sagen wir:

Definition 17.7 (Endlicher Boolscher Verband) *:*
Ein Boolscher Verband $(\mathcal{V}, \sqcap, \sqcup, \ ^-)$ *heisst* **endlich**, *wenn die Menge* $\mathcal{V}$ *endlich ist.*

Satz 17.4 (von Stone) *: Jeder endliche Boolsche Verband* $(\mathcal{V}, \sqcap, \sqcup, \ ^-)$ *ist isomorph zu einem Mengenverband* $(\wp(M), \cap, \cup, \ ^-)$*.*

Die *Konsequenz dieses Satzes* ist überwältigend: Da sich bei isomorphen algebraischen Strukturen die Elemente und die Resultate der Operationen paarweise entsprechen, braucht man nur einen Vertreter einer Isomorphieklasse zu kennen, damit man weiss, wie sich alle andern Klassenmitglieder bei den Operationen verhalten. Man merke sich:

(Merke!) Wenn man die Mengenverbände $(\wp(M), \cap, \cup, \ ^-)$ kennt, kennt man formal alle endlichen Boolschen Verbände. Speziell ist dann $|\mathcal{V}| = |\wp(M)| = 2^{|M|}$. (Die letzte Gleichung ist in der Kombinatorik bewiesen worden.) Somit wissen wir:

Satz 17.5 (Anzahl Elemente bei einem Boolschen Verband) *: Die Anzahl Elemente der Menge* $\mathcal{V}$ *in einem Boolschen Verband* $(\mathcal{V}, \sqcap, \sqcup, \ ^-)$ *ist immer eine Zweierpotenz.*

Es gibt daher keinen Boolschen Verband mit 3, 5, 6, oder z.B. mit 17 Elementen! Und weiter folgt sofort speziell für die Schaltalgebra:

Korollar 17.1 (Isomorphie der Schaltalgebra) *: Die Schaltalgebra* $(\{\emptyset, L\}, +, \cdot, \bar{\ })$ *ist isomorph zur Mengenalgebra* $(\{\{\{\}\}, \{\}\}, \cup, \cap, \bar{\ })$ [12] *oder zu* $(\{w, f\}, \vee, \wedge, \neg)$ *(Aussagenlogik) oder zum Teilerverband mit* V_k *mit* $k = 2$*.*

Der Beweis des Satzes von Stone ist eine Angelegenheit von mehreren Seiten, da verschiedene Details konsequent durchgeprüft werden müssen. Eine Darstellung findet sich in Boolsche Algebra (Bibl.: deller).

Konsequenz: Wegen der Isomorphie kann man die Schaltalgebra z.B. in die Mengenlehre übersetzen und die dort zur Verfügung stehenden Techniken nutzen. Gewinnbringend wird das bekanntlich bei der Technik mit den *Karnaugh–Diagrammen* angewandt, indem man Schaltausdrücke in die Mengenlehre übersetzt und dort mit Mengendiagrammen arbeitet.

17.6 Algebra mit Boolschen Ausdrücken

17.6.1 Rechengesetze in der Schaltalgebra

Da die Schaltalgebra ein Boolscher Verband ist, können wir die Verbandsaxiome auch in der Sprache der Schaltalgebra schreiben. $\sqcap$ wird dort zu $\cdot$ und $\sqcup$ wird zu $+$. Man kann aber auch von den so erhaltenen Gesetze ausgehen, sie also an den Beginn stellen und damit die Schaltalgebra axiomatisch einführen. Das ergibt das folgende Axiomensystem:

Axiom 17.1 (Verbandsaxiome in der Sprache der Schaltalgebra) *: Für alle* a*,* b *und* $c \in \{\emptyset, L\}$ *gilt:*

(A1)	$a \cdot b$	$=$	$b \cdot a$	*(A1')*	$a + b$	$=$	$b + a$
(A2)	$(a \cdot b) \cdot c$	$=$	$a \cdot (b \cdot c)$	*(A2')*	$(a + b) + c$	$=$	$a + (b + c)$
(A3)	$a \cdot (a + b)$	$=$	a	*(A3')*	$a + (a \cdot b)$	$=$	a
(A4)	$a \cdot (b + c)$	$=$	$(a \cdot b) + (a \cdot c)$	*(A4')*	$a + (b \cdot c)$	$=$	$(a + b) \cdot (a + c)$
(A5)	$a \cdot L$	$=$	a	*(A5')*	$a + \emptyset$	$=$	a
(A6)	$\forall_a \dot{\exists}_{\bar{a}} : a \cdot \bar{a}$	$=$	$\emptyset$	*(A6')*	$\forall_a \dot{\exists}_{\bar{a}} : a + \bar{a}$	$=$	L

Bemerkungen:

- Statt $a \cdot b$ benützen wir wie in der Zahlenalgebra die **Kurzschreibweise** $a\,b$.
- Wegen der Isomorphie zur Aussagenlogik ist das Axiomensystem für Boolsche Algebren widerspruchsfrei, denn die Aussagenlogik ist widerspruchsfrei. Jedoch ist es nicht minimal. (Z.B. lassen sich die Axiome (A2), (A2'),(A3) und (A3') aus den restlichen herleiten.)

Auf der Basis dieser Axiome kann man die folgenden Rechenregeln beweisen:

Satz 17.6 (Rechenregeln für die Schaltalgebra) *:*

(1)	$a\,a$	$=$	a	*(1')*	$a + a$	$=$	a
(2)	a	$=$	$\overline{\overline{a}}$				
(3)	$a\,\emptyset$	$=$	$\emptyset$	*(3')*	$a + L$	$=$	L
(4)	$\bar{\emptyset}$	$=$	L	*(4')*	$\bar{L}$	$=$	$\emptyset$
(5)	$\overline{a\,b}$	$=$	$\bar{a} + \bar{b}$	*(5')*	$\overline{a + b}$	$=$	$\bar{a}\bar{b}$

[12] $\{\{\{\}\}, \{\}\}$ ist ein Beispiel einer Menge mit zwei Elementen.

Beispiele von Beweisen:

Zu (1): $a\,a = a(a+\emptyset) = a$ (mit Hilfe des Absorptionsgesetzes sowie (5')).
Zu (2): Es ist $\bar{a}\cdot\overline{\bar{a}} = \emptyset$ und $\bar{a}\cdot a = a\cdot\bar{a} = \emptyset$ (Kommutativität, (6)). Daraus folgt: $a = \overline{\bar{a}}$, da nach (6) das Inverse eindeutig ist.
Zu (3): $a\cdot\emptyset = \emptyset\cdot a = \emptyset\cdot(a+\emptyset) = \emptyset\cdot(\emptyset+a) = \emptyset$ (Kommutativität, (5'), Absorptionsgesetz).
Zu (4): $\emptyset+\bar{\emptyset} = L$ (nach (6')) und $\emptyset+L = L$ (Kommutativität und (5')). Daraus folgt $\bar{\emptyset} = L$ wieder wegen der Eindeutigkeit des Inversen.
Zu (5): Wegen der Kommutativität, Distributivität, Assoziativität, (3) und (5') ist: $(a+b)\bar{a}\,\bar{b} = a\,\bar{a}\,\bar{b} + b\,\bar{a}\,\bar{b} = \emptyset\,\bar{b} + \emptyset\,\bar{a} = \emptyset+\emptyset = \emptyset$. Wegen der Kommutativität und der Eindeutigkeit des Inversen ist daher $\bar{a}\,\bar{b}$ das Inverse von $(a+b)$, d.h. $\overline{a+b} = \bar{a}\bar{b}$.
Wie man hier ersieht, können die behaupteten Aussagen alleine mit Hilfe der durch die Axiome gegebenen Rechenregeln nachgerechnet werden. Mehr steckt nicht dahinter.

Beispiele von Termumformungen

Nachstehend sind einige Beispiele von Termumformungen gegeben, bei denen nur obige Axiome und Rechenregeln sowie die Resultate schon gerechneter Beispiele verwendet werden. Der Leser möge zur Übung selbst herausfinden, welche Regeln beim jeweiligen Rechenschritt verwendet werden:
Beispiele:

1. $x_1x_2+x_3x_4 = (x_1x_2+x_3)(x_1x_2+x_4) = (x_3+x_1x_2)(x_4+x_1x_2) = (x_3+x_1)(x_3+x_2)(x_4+x_1)(x_4+x_2) = (x_1+x_3)(x_1+x_4)(x_2+x_3)(x_2+x_4)$
2. $x_1x_2 + x_2x_3 + x_3x_1 = x_2(x_1+x_3)x_3x_1 = (x_2+x_3)(x_2+x_1)((x_1+x_3)+x_3)((x_1+x_3)+x_1) = (x_2+x_3)(x_2+x_1)(x_1+x_3)(x_1+x_3) = (x_1+x_2)(x_2+x_3)(x_3+x_1)$
3. $x_1(\bar{x}_1+x_2) + x_2(x_2+x_3) + x_2 = x_1\bar{x}_1 + x_1x_2 + x_2 + x_2 = \emptyset + x_2x_1 + x_2 = x_2x_1 + x_2 = x_2$
4. $x_1 + \bar{x}_1 + x_2 = (x_1\bar{x}_1)(x_1+x_2) = x_1 + x_2$ (*)
5. $(x_1+x_2)(x_1+\bar{x}_2)(\bar{x}_1+x_2)(\bar{x}_1+\bar{x}_2) = (x_1+x_2\bar{x}_2)(\bar{x}_1+x_2\bar{x}_2) = (x_1+\emptyset)(\bar{x}_1+\emptyset) = x_1\bar{x}_1 = \emptyset$
6. $x_1x_2x_3 + x_1 + \bar{x}_2x_3 + x_1x_2x_3\bar{x}_3 = x_1x_3(x_2+\bar{x}_2) + \emptyset = x_1x_3L = x_1x_3$
7. $\overline{x_1+x_2+x_3} = \overline{(x_1+x_2)+x_3} = \overline{(x_1+x_2)}\bar{x}_3 = \bar{x}_1\bar{x}_2\bar{x}_3$
8. $\overline{x_1x_2x_3} = \overline{(x_1x_2)} + \bar{x}_3 = (\bar{x}_1+\bar{x}_2) + \bar{x}_3 = \bar{x}_1 + \bar{x}_2 + \bar{x}_3$
9. $x_1x_2x_3 + \bar{x}_1 + \bar{x}_2 + \bar{x}_3 = x_1x_2x_3 + \overline{x_1x_2x_3} = L$
10. $\overline{x_1x_2 + x_1\bar{x}_2 + \bar{x}_1\bar{x}_2} = \overline{x_1(x_2+\bar{x}_2) + \bar{x}_1\bar{x}_2} = \overline{x_1L + \bar{x}_1\bar{x}_2} = \overline{x_1+\bar{x}_1\bar{x}_2} = \overline{x_1+\bar{x}_2} = \bar{x}_1\overline{\bar{x}_2} = \bar{x}_1x_2$ (unter Benutzung von (*)).

17.6.2 Behandlung von Schaltungen mit Boolscher Algebra

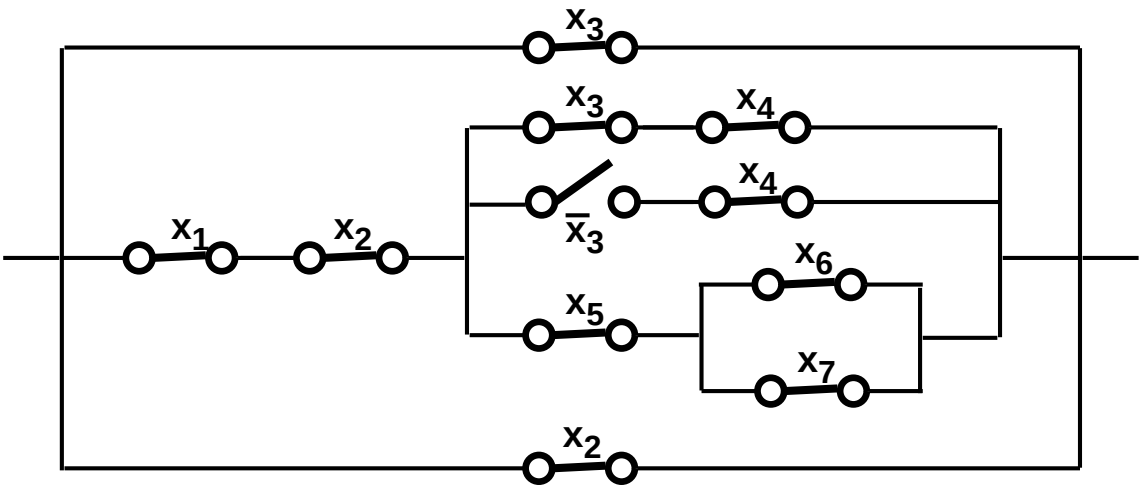
17.6.3 Algebraischer Ausdruck einer Schaltung

Da Summe, Produkt und Komplement in der physikalischen Realität ihre eindeutige Entsprechung haben (Parallelschaltung, Serieschaltung und Negationsschalter), gehört zu einer Schalterdarstellung (resp. zu einer Gatterdarstellung, vgl. Lit.) eindeutig ein algebraischer Ausdruck $f(x_1, x_2, \ldots)$, in dem die Reihenfolge berücksichtigt ist. Ein solcher Ausdruck definiert natürlich dann jeweils eine Funktion mit den unabhängigen Variablen $x_1, x_2, \ldots$.

Beispiele:

1. Schalterdarstellung, Beispiel 1 (vgl. Abb. 17.3):
   $f(x_1, x_2, \ldots, x_7) = x_3 + x_1x_2(x_3x_4 + \bar{x}_3x_4 + (x_5(x_6+x_7))) + x_2$.

Abbildung 17.3: Schalterdarstellung, Beispiel 1



2. Schalterdarstellung, Beispiel 2 (vgl. Abb. 17.4):
   $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3)(\bar{x}_1 + x_2)(x_1x_3 + \bar{x}_1x_2)(\bar{x}_2 + \bar{x}_3)$.

3. Schalterdarstellung, Beispiel 3 (vgl. Abb. 17.5):
   $f(x_1, x_2, \ldots x_5) = x_1(x_2 + x_5(x_4 + \bar{x}_2)) + x_3(x_5x_2 + x_4 + \bar{x}_2)$.

Wie wir bei den Beispielen von Termumformungen gesehen haben (vgl. 17.6.1), ist die Darstellung eines Terms nicht eindeutig, denn man kann einen Term ja umformen. Zu einer Schaltung gibt es daher immer je nach den Umformungsmöglichkeiten des Terms äquivalente[13] Schaltungen, die dasselbe physikalische Resultat ergeben.

Resultat: Zu einer elektrischen Schaltung gehört ein algebraischer Ausdruck und umgekehrt. Der algebraische Ausdruck kann mit Hilfe der Regeln für die Termumformungen äquivalent umgestaltet werden. Die zugehörige neue Schaltung macht dann dasselbe wie die alte.

17.6.4 Das Darstellungsproblem

In der Praxis taucht folgendes Problem auf (vgl. Abb. 17.6):

Problem 17.1 (Darstellungsproblem) *:*

[13] Wir nennen zwei Schaltungen **äquivalent**, wenn sich ihre algebraischen Ausdrücke ineinander umformen lassen.

Abbildung 17.4: Schalterdarstellung, Beispiel 2

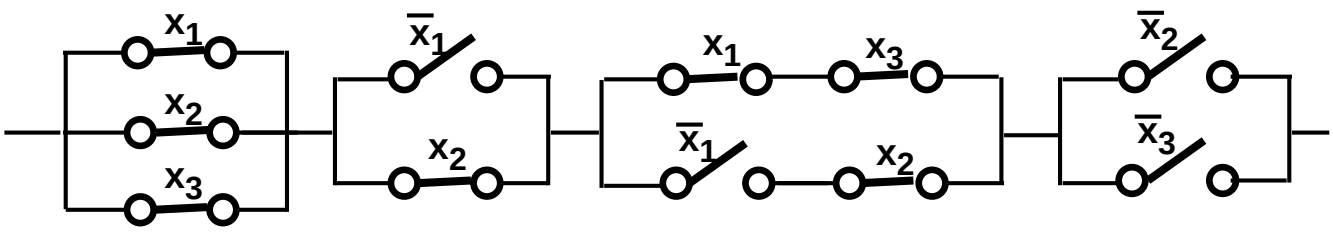
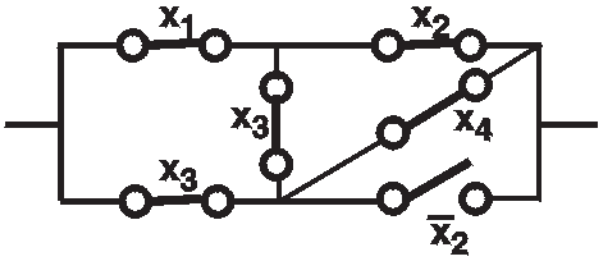


Abbildung 17.5: Schalterdarstellung, Beispiel 3



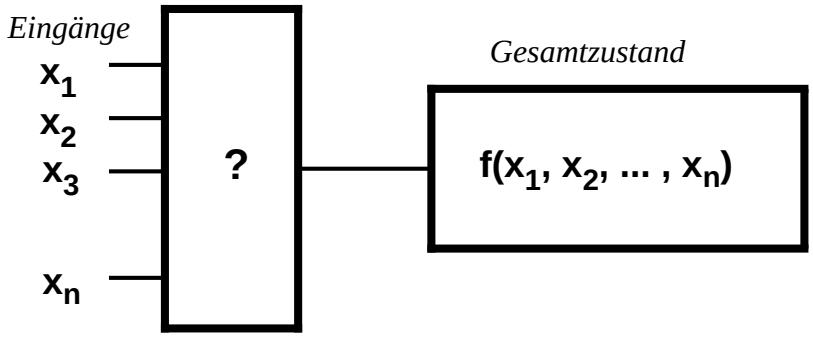
Gegeben: *Zustände von Schaltern (Eingänge sowie Gesamtzustand), z.B. in einer Wertetabelle.*
Gesucht: *Die Schaltung, z.B. in Form eines algebraischen Ausdrucks.*

Beispiel:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
L	L	L	L
L	∅	L	L
L	L	∅	∅
∅	L	L	∅
∅	L	∅	∅
∅	∅	1	frei
L	∅	∅	wählbar
∅	∅	∅	

Um den zugehörigen algebraischen Ausdruck zu finden, können wir die Isomorphie der Schaltalgebra zum entsprechenden Teil der Aussagenlogik ausnützen. Dort haben wir gelernt, zu einer Wertetabelle z.B. die zugehörige *vollständige* oder *kanonische alternative Normalform (ANF)* zu finden. In unserem Beispiel wäre diese ANF $(X_1 \wedge X_2 \wedge X_3) \vee (X_1 \wedge \neg X_2 \wedge X_3)$. Da einige Werte rechts in der Tabelle frei wählbar sind, wählen wir diese Werte so, dass die Länge des entstehenden Ausdrucks möglichst klein wird.

Abbildung 17.6: Schalterdarstellung, Beispiel 3



In die Schaltalgebra übersetzt erhalten wir dann:

$$\begin{aligned} f(x_1, x_2, x_3) &= x_1x_2x_3 + x_1\bar{x}_2x_3 \\ &= x_1x_3(x_2 + \bar{x}_2) \\ &= x_1x_3 \end{aligned}$$

Die Umformung zeigt, dass schliesslich die Schaltung mit Hilfe von nur zwei Schaltern realisiert werden kann. Mit weniger geht es nicht. Andererseits hätte man aber auch mit der *KNF* arbeiten können. Was allgemein besser ist, muss die Praxis zeigen. Wir gelangen so zu folgendem Problem:

17.6.5 Das Minimalisierungsproblem

Problemstellung

Eine verständliche ökonomische Forderung verlangt die Reduzierung der Anzahl Schalter soweit es geht. Schaltungen werden so einfacher, billiger. Für uns entsteht das folgende Problem:

Problem 17.2 (Minimalisierungsproblem) *:*
Gegeben: *Eine Schaltung in Form eines algebraischen Ausdrucks.*
Gesucht: *Die oder eine äquivalente Schaltung mit der minimalen Anzahl Schaltern.*

Es sind mehrere verschiedene Methoden bekannt, die zur Lösung des Problems dienen. In der angegebenen Literatur (z.B. Boolsche Algebra und logische Schaltungen (Bibl.: mendelson)) finden wir:

1. Rechnen mit Hilfe der bekannten Rechengesetze (nicht sehr effizient)
2. *Karnaugh–Methode* (wird weiter unten vorgestellt)
3. Methode von *Quine – Mc Cluskey*
4. *Konsensmethode*

Da die Anzahl Schalter sich algebraisch in der „Länge der Terme“ wiederspiegelt, wird es zum Verständnis der in der Literatur besprochenen Methoden notwendig, diese Termlänge mathematisch irgendwie auszudrücken. Das führ auf den Begriff der *Minimalform.*

Minimalformen

Statt Ausdrücke der Schaltalgebra betrachten wir für den Moment die entsprechenden Ausdrücke der Aussagenlogik, denn für diese haben wir schon früher eine Terminelogie aufgebaut.
Sei somit Φ eine ANF: $\Phi = \Phi_1 \vee \Phi_2 \vee \ldots \vee \Phi_k$, wobei die Φ_i Konjunktionsterme sind.
Sei l_Φ die Anzahl der in Φ vorkommenden verschiedenen Variablen (ohne die Negation $\neg$), d_Φ sei die Anzahl der Adjunktionsglieder.
Wenn wir zwei Terme mit gleichvielen verschiedenen Variablen haben, so nennen wir denjenigen Term den kleineren (kürzeren), der weniger Adjunktionsglieder aufweist. Allgemeiner definieren wir:

Definition 17.8 (kleinerer oder kürzerer Term) *:*
Φ *heisst* **kleiner** *(***kürzer***) als* Ψ *(*$\Phi < \Psi$*) :* $\Longleftrightarrow l_\Phi \leq l_\Psi \wedge d_\Phi \leq d_\Psi$*, wobei mindestens einmal '<' stehen muss.*

Definition 17.9 (Minimalform) *: Die zu* Φ *kleinste mögliche ANF heisst* **adjunktive Minimalform** *(AMF). Entsprechend zur KNF die* **konjunktive Minimalform** *(KMF).*

Bemerkung: Später werden wir in Beispielen sehen, dass eine AMF (KMF) nicht eindeutig zu sein braucht.

Sei nun A eine Aussageform und K ein Konjunktionsterm. Wir sagen:

Definition 17.10 (Primimplikant) *:*
K heisst **Primimplikant** *von A* $\iff$ *1. $K \Rightarrow A$ ist Tautologie. 2. $K_1 \Rightarrow A$ ist für $K_1 < K$ nicht mehr Tautologie.*

Es gilt der folgende Satz:

Satz 17.7 (Über Primimplikanten) *:*
Eine AMF von A ist eine Adjunktion von Primimplikanten von A.

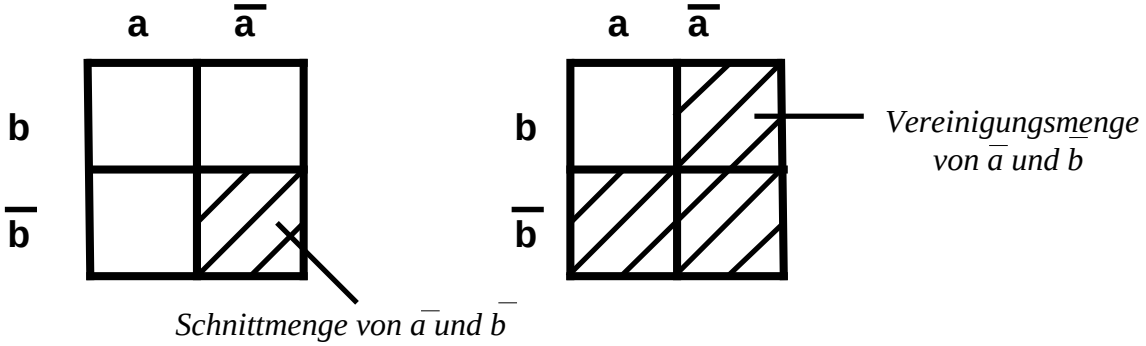
Für den Beweis sei auf die Literatur (z.B. Bibl.: mendelson) verwiesen.

Konsequenz: Das Auffinden der ANF bedeutet algebraisch das Auffinden der Primimplikanten. Das lässt sich methodisch ausbauen und anwenden. Für unsere Belang wollen wir uns aber hier vor allem einer einzigen einfachen Methode zuwenden, die nicht algebraisch funktioniert, sondern sich der Mengendiagramme bedient: die *Karnaugh–Methode*.

17.6.6 Die Karnaugh–Methode

Mit 2 Variablen

Abbildung 17.7: Darstellung von Termen der Schaltalgebra durch Mengendiagramme



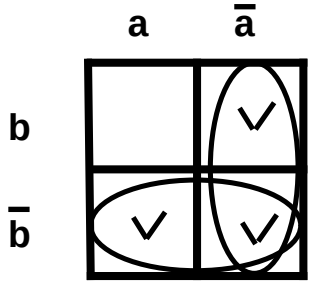
In 17.5 haben wir gesehen, dass die Schaltalgebra $(\{\emptyset, L\}, +, \cdot, \bar{}\,)$ isomorph ist zur Mengenalgebra $(\{\{\{\}\}, \{\}\}, \cup, \cap, \bar{}\,)$ ist – oder auch zu $(\{\{1\}, \{\}\}, \cup, \cap, \bar{}\,)$. Das erlaubt uns, statt $\cdot$ und $+$ neu $\cap$ und $\cup$ zu verwenden und Schnitt– sowie Vereinigungsmengen graphisch zu ermitteln, vgl. Abb17.7.
Beispiel: Statt $a\,\bar{b} + \bar{a}\,b + \bar{a}\,\bar{b}$ studieren wir den entsprechenden Ausdruck $a \cap \bar{b} \cup \bar{a} \cap b \cup \bar{a} \cap \bar{b}$, wobei a und b jetzt als Mengen zu interpretieren sind. Graphisch stellen wir der Einfachheit halber die Schnitt– und Vereinigungsmengen durch Quadrate oder Rechtecke dar (vgl. dazu Abb17.8).

a und $\bar{a}$ werden im Beispiel durch hohe Rechtecke dargestellt, b und $\bar{b}$ liegende Rechtecke. Die Quadrate symbolisieren die Schnittmenten $a \cap \bar{b}$, $\bar{a} \cap b$, $\bar{a} \cap \bar{b}$. Diese Schnittmengen markieren wir je mit einem Haken ($\surd$). Aus der Skizze ist jetzt ersichtlich, dass die Vereinigung dieser Schnittmengen ja gerade gleich $\bar{a} \cup \bar{b}$ ist. Somit gilt:

$$a\,\bar{b} + \bar{a}\,b + \bar{a}\,\bar{b} = \bar{a} + \bar{b}$$

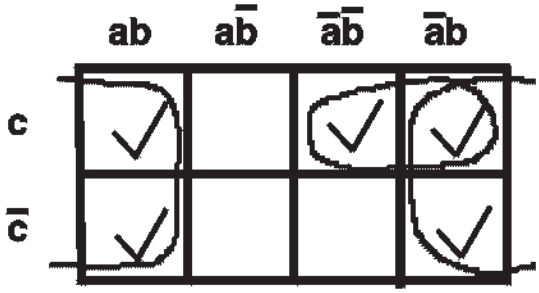
Mengentheoretisch gedeutet ist $\bar{a} + \bar{b}$ die Vereinigung (Symbol $+$) der beiden in der Darstellung umrandeten Vereinigungsmengen.

Abbildung 17.8: Beispiel mit zwei Variablen



Mit 3 Variablen

Abbildung 17.9: Beispiel mit drei Variablen



In Abb17.9 ist das Beispiel $a\,b\,c + \bar{a}\,b\,c + a\,b\,\bar{c} + \bar{a}\,b\,\bar{c} + \bar{a}\,\bar{b}\,c = b + \bar{a}\,c$ dargestellt.

Mit 4 Variablen

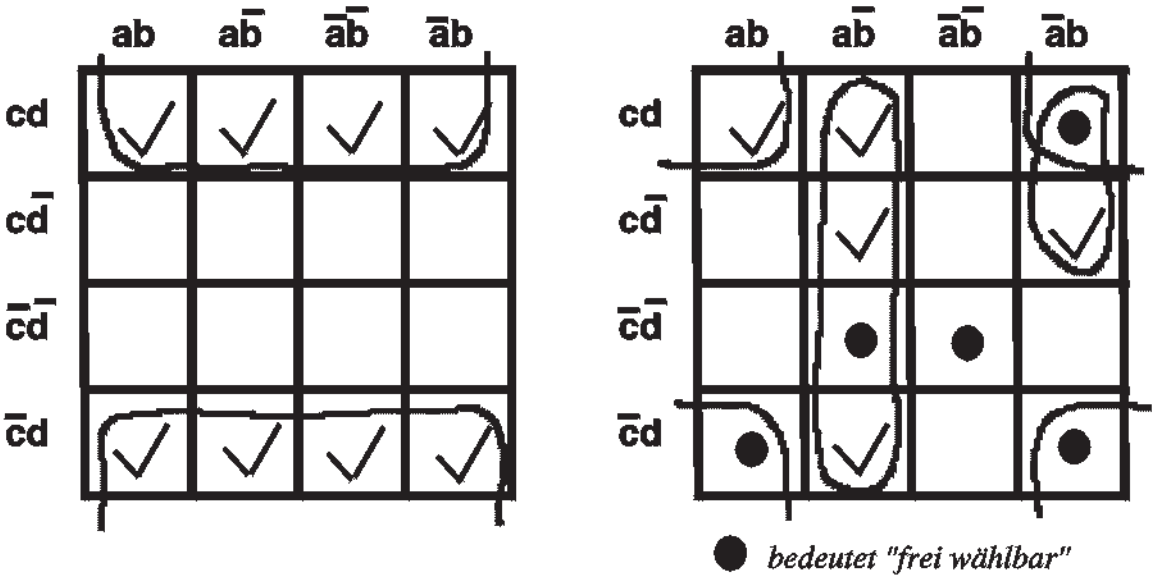
In Abb17.10 links im Bild ist das Beispiel $a\,b\,c\,d + a\,\bar{b}\,c\,d + \bar{a}\,\bar{b}\,c\,d + \bar{a}\,b\,c\,d + a\,b\,\bar{c}\,d + a\,\bar{b}\,\bar{c}\,d + \bar{a}\,\bar{b}\,\bar{c}\,d + \bar{a}\,b\,\bar{c}\,d = d$ dargestellt.
Rechts im Bild steht ein Beispiel, in dem man einige Summanden (alles Produkte) *frei wählen* kann. Sie sind durch einen fetten Punkt markiert. Falls es nützlich erscheint, mag man sie benützen, andernfalls lässt man es bleiben. Das Beispiel hier zeigt $a\,b\,c\,d + a\,\bar{b}\,c\,d + a\,\bar{b}\,c\,\bar{d} + \bar{a}\,b\,c\,\bar{d} + a\,\bar{b}\,\bar{c}\,d$ mit den frei wählbaren Beiträgen $\bar{a}\,b\,c\,d$, $a\,\bar{b}\,\bar{c}\,\bar{d}$, $\bar{a}\,\bar{b}\,\bar{c}\,\bar{d}$, $a\,b\,\bar{c}\,d$, $\bar{a}\,b\,\bar{c}\,d$. Die Minimalformen lauten: $a\,\bar{b} + b\,d + \bar{a}\,b\,c$ (vgl. Abbildung) und $a\,\bar{b} + a\,d + \bar{a}\,b\,c$. Dies ist ein *Beispiel für den Fall*, wo die *Minimalform nicht eindeutig* ist.

Merke: Eine Minimalform braucht nicht eindeutig zu sein.

Mit 5 Variablen

In Abb17.11 finden wir das Beispiel $a\,b\,c\,d\,e + \bar{a}\,\bar{b}\,c\,d\,e + a\,\bar{b}\,c\,\bar{d}\,e + \bar{a}\,\bar{b}\,c\,\bar{d}\,e + \bar{a}\,\bar{b}\,\bar{c}\,\bar{d}\,e + \bar{a}\,b\,\bar{c}\,d\,e + a\,b\,c\,d\,\bar{e} + \bar{a}\,b\,c\,d\,\bar{e} + a\,\bar{b}\,\bar{c}\,\bar{d}\,\bar{e} + \bar{a}\,\bar{b}\,\bar{c}\,\bar{d}\,\bar{e} + a\,b\,\bar{c}\,d\,\bar{e}$. Frei wählbar sind die Beiträge $\bar{a}\,b\,c\,d\,e$, $a\,\bar{b}\,\bar{c}\,\bar{d}\,e$, $a\,b\,\bar{c}\,d\,e$, $a\,\bar{b}\,c\,\bar{d}\,\bar{e}$, $\bar{a}\,\bar{b}\,c\,\bar{d}\,\bar{e}$, $\bar{a}\,b\,\bar{c}\,d\,\bar{e}$. Die Resultate der Vereinfachung sind $b\,d + \bar{b}\,\bar{d} + \bar{a}\,\bar{b}\,c\,e$ und $b\,d + \bar{b}\,\bar{d} + \bar{a}\,c\,d\,e$ (keine Eindeutigkeit).

Abbildung 17.10: Beispiel mit vier Variablen



17.6.7 Bermerkungen zu den andern Methoden

Quine – Mc Cluskey (vgl. Lit. Bibl.: mendelson):
Diese Methode funktioniert ähnlich wie die Karnaugh–Methode. Man arbeitet jedoch mit Tabellen statt mit Diagrammen.

Konsens–Methode (vgl. Lit. Bibl.: mendelson):
Seien Ψ_1 und Ψ_2 Konjunktionsterme und ρ eine Variable, die nicht negiert in Ψ_1 vorkommt, während $\neg\rho$ in Ψ_2 vorkommt. Aus $\Psi_1 \wedge \Psi_2$ bilde man jetzt Φ durch Weglassung von ρ und $\neg\rho$. Man definiert dann:

Definition 17.11 (Konsens) *:*
Der damit entstehende Ausdruck Φ *heisst* **Konsens** *von* Ψ_1 *und* Ψ_2*.*

Man kann dann den folgenden Satz beweisen:

Satz 17.8 (Zum Konsens) *:*

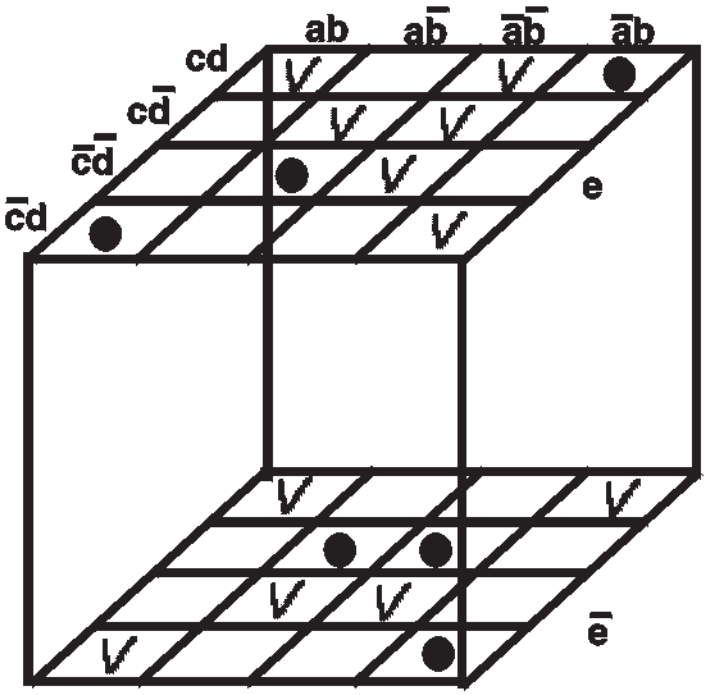
1. $(\Phi \Longrightarrow \Psi_1 \vee \Psi_2)$ *ist Tautologie.*
2. $\Psi_1 \vee \Psi_2 \equiv \Psi_1 \vee \Psi_2 \vee \Phi$*.*

Vorgehen bei der Konsens–Methode:

1. Wir gehen von einer ANF aus. Streiche die Adjunktionsglieder (Konjunktionsterme), die andere enthalten (Oberterme werden hier impliziert).
2. Konsens–Bildung.
3. Repetiere dieses Verfahren, bis ein Stillstand erreicht ist. Das Resultat ist dann eine Adjunktion von Primimplikanten.

Diese Bemerkungen sind nur ein sehr kurzer Ausblick. Eine weiterführende Behandlung der Sache würde unseren Rahmen hier sprengen. Für die Befriedigung eines allfälligen jetzt erwachsenen Erklärungsbedarfs zu diesem Thema sei auf die einschlägige Literatur verwiesen.

Abbildung 17.11: Beispiel mit fünf Variablen



17.7 Übungen

Übungen finden sich in *DIYMU* (Bibl.: wirz1) sowie in der klassischen Schulbuchliteratur für Berufsschulen und die Gymnasialstufe. Achtung: Die Nummerierung der Kapitel im *DIYMU* ist unabhängig!

Kapitel • Chapitre 18

Vorwort zur Kombinatorik — Préface à l'analyse combinatoire

Liebe Leserin, lieber Leser,

Das Thema *Kombinatorik* ist ein klassischer Bestandteil des Mittelschullehrplans (Probleme mit ganzen Zahlen). Auch an Berufsmittelschulen sollte es eigentlich behandelt werden. Doch was, wenn ein Student aus irgendwelchen Gründen gerade diesem Stoff an der Schule nie begegnet ist — oder ihn vergessen hat? Dann heisst es eben nacharbeiten und repetieren. Daher ist dieser Text als *Repetitorium* und als *Ausbau* gedacht.
Die Wichtigkeit der Kombinatorik für den Weg durch die weitere Mathematik ist unbestritten. Sie ist ein Werkzeug zur Lösung von Problemen, die manchmal unverhofft an einem herantreten. Geradezu grundlegend ist das Thema aber für das Wissensgebiet „Wahrscheinlichkeitsrechnung und Statistik".
Dieser Text ist in Skriptform abgefasst. Das bedeutet, dass er in äusserst knapper Fassung nur das wesentliche Skelett des zu lernenden Stoffes wiedergibt. Für weitere, ausführliche Erklärungen, Beispiele, exakte Beweise und ergänzende Ausführungen ergeht daher an den Studenten der Rat, ein oder mehrere Lehrbücher beizuziehen. Studieren bedeutet zu einem wesentlichen Teil, sein Wissen selbständig mit Hilfe der Literatur zu erweitern, streckenweise sogar selbständig zu erarbeiten, zu festigen und anzuwenden. Ein Skript ist dabei nur ein Wegweiser und nie ein Lehrbuchersatz. Welche Lehrbücher jemand verwenden will, ist jedem freigestellt. Das Thema Kombinatorik findet man in praktisch allen Unterrichtswerken für die klassische Gymnasialstufe. Bezüglich der Fachhochschulliteratur sei auf das Beilpiel Brenner, Lesky, Mathematik für Ingenieure und Naturwissenschaftler, Band 1 (Bibl.: brennerlesky) verwiesen.

Im Sommer 1996 Der Autor

Glück hilft manchmal, Arbeit immer ...

Brahmanenweisheit

• *La chance aide parfois, mais le travail aide toujours ...*

• *Sagesse de l'Inde*

• *Chère lectrice, cher lecteur,*

L'analyse combinatoire fait partie du programme du gymnase classique (problèmes concernant les nombres entiers). Dans les écoles qui préparent à la maturité professionelle, il devrait être traité également. Mais quoi, si un étudiant n'a jamais eu contact avec cette matière pour n'importe quelle raison — ou s'il l'a oubliée? Alors il faut l'élaborer ou répéter. Par conséquent ce texte est conçu comme cours de répétition et comme perfectionnement.
L'importance de l'analyse combinatoire est incontestée. Elle est un outil pour la solution de problèmes qui nous surprennent parfois. Elle est la base pour le "calcul des probabilités et la statistique".
Ce texte est écrit en forme de script. Ça signifie qu'il représente une forme très abrégée de la manière à apprendre. Pour des explications plus vastes et détaillées, exemples, preuves exactes et suppléments, on conseille l'étudiant de consulter plusieurs livres de cours. Etudier signifié en grande partie d'élargir soi–même son savoir à l'aide de la littérature et acquérir de la matière, de l'approfondir et de l'utiliser. Pour cela, un script est seulement un indicateur d'itinéraire et ne remplace jamais un livre de cours. Chacun est libre de choisir ses livres de cours. On trouve le sujet de l'analyse combinatoire pratiquement dans toutes les oeuvres de mathématiques pour le gymnase classique. Concernant le niveau des hautes écoles professoinelles le lecteur est renvoyé à des ouvrages tels que Brenner, Lesky, Mathematik für Ingenieure und Naturwissenschaftler, Band 1 (Bibl.: brennerlesky).

Dans l'été 1996 *L'auteur*

Kapitel • Chapitre 19

Kombinatorik — Analyse combinatoire

19.1 Einleitung — Introduction

19.1.1 Problemstellung — Problème

Im Stoffgebiet *Kombinatorik* behandeln wir die 6 Typen der klassischen *Anzahlprobleme*. Dabei geht es um folgende Kategorie von Fragestellungen: Wir fragen nach der *Anzahl* der Möglichkeiten, aus einer endlichen Menge M nach einer gewissen Vorschrift Elemente *auszuwählen*, diese ev. *anzuordnen* oder die Menge *in Klassen einzuteilen.* Dabei können sich Elemente *wiederholen* – oder nicht. Da das Resultat y jeweils eine natürliche Zahl ist, reden wir auch von **Anzahlfunktionen** $M \longmapsto y$.
• *Dans l'analyse combinatiore, nous traitons les 6 types de problèmes des nombres cardinaux classiques. Il s'agit des catégories suivantes de questions: Nous demandons le nombre des possibilités de pouvoir choisir des éléments dans un ensemble fini M d'après une prescription donnée, et eventuellement aussi de les ordonner ou de diviser l'ensemble en classes. Dans certains cas les éléments peuvent être répétés — ou bien non répétés. Comme le résultat y est chaque fois un nombre naturel, nous parlons de* **fonctions dans les nombres cartinaux** $M \longmapsto y$.

19.1.2 Fakultäten — Factorielles

In der Kombinatorik spielt der Begriff *Fakultät* eine grosse Rolle. Man definiert die *Fakultäten induktiv*[1] durch die folgende *Rekursion*:
• *Dans l'analyse combinatiore, la notion des factorielles joue un grand rôle. On définit les factorielles*[2] *par la relation de récurrence suivante:*

Definition • Définition 19.1 (Fakultät: • *Factorielle:*)

$$f(0) = 0! := 1 \qquad \textit{(Verankerung)} \bullet \textit{(Ancrage)}$$
$$f(n) = n! := n \cdot (n-1)! \qquad \textit{(Vererbung)} \bullet \textit{(Hérédité)}$$

Bemerkungen: • *Remarques:*

1. Es gilt dann: • *Il vaut donc:* $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = \prod_{k=1}^{n} k$. (Siehe • *Voir*([3]).)
   Daraus ergibt sich: • *Il vaut donc:* $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$ etc..

[1] Nach dem Schema der vollständigen Induktion, vgl. Thema *natürliche Zahlen, Induktionsaxiom* (eines der Axiome aus dem System von Peano).
[2] D'après le schéma de l'induction complète, voir le sujet des nombres naturels, axiome d'induction, un des axiomes du système de Peano.
[3] $\prod$ steht für *„Produkt"*. • $\prod$ *signifie "produit".*

2. Der Begriff *Rekursion* hat sich heute in der *Informatik* sehr stark verbreitet. Man versteht dort darunter *die Definition einer Funktion oder eines Verfahrens durch sich selbst* (vgl. dazu z.B. Claus, Schwill, Bibl.: clausschwill). Man darf den Begriff *Rekursion* in diesem hier verwendeten einfachen Sinne jedoch nicht verwechseln mit den in der höheren Mathematik gebräuchlichen, etwas schwierigen Begriffen *allgemeine Rekursion*, *primitive Rekursion*, *rekursive Funktion* (in der Zahlentheorie), *rekursive Relation* (in verschiedenem Sinne in Logik und Mengenlehre). Vgl. dazu Fachlexikon a *b c*] (Bibl.: abc), Iyanaga, Kawada (Bibl.: iyanagakawada) und Meschkowski (Bibl.: meschkowski).
• *La notion de récurrence est très répandue aujourd'hui dans l'informatique. On entend par cette notion la définition d'une fonction ou une méthode par elle-même, voir aussi par exemple (Bibl.: Claus, Schwill (Bibl.: clausschwill)). Mais il ne faut pas confondre la notion de la récurrence qui cependant est utilisée ici dans un sens simple avec les notions récurrence commune,récurrence primitive, fonciton de récurrence (dans la théorie des nombres) et relation de récurrence (dans des sens différents dans la logique et la théorie des ensembles) qui sont un peu difficiles et usuelle dans les mathématiques. Voir aussi Fachlexikon* a b c *(Bibl.: abc), Iyanaga, Kawada (Bibl.: iyanagakawada) et Meschkowski (Bibl.: meschkowski)*

Wir halten fest: • *Nous retenons:*

Definition • Définition 19.2 (Rekursion (Informatik) • Récurrence (informatique))
Unter **Rekursion** *verstehen wir hier die Definition einer Funktion oder eines Verfahrens durch sich selbst.*
• *Sous* **récurrence** *nous entendons la définition d'une fonction ou d'une méthode par elle-même.*

Beispiel: • Exemple: Aus der Definition von $n!$ ergibt sich: $f(n) = n \cdot f(n-1)$. Die Funktion an der Stelle n wird also durch die Funktion (also durch sich selbst) an der Stelle $n-1$ definiert. • *De la définition de* $n!$ *on conclut:* $f(n) = n \cdot f(n-1)$. *La fonction à la place* n *est donc définie par la fonction à la place* $n-1$ *(ainsi par elle-même).*
Die Werte $f(n) = n!$ werden sehr rasch sehr gross. z.B. ist: • *Les valeurs* $f(n) = n!$ *augmentent très vite. Par exemple il vaut:*

$$40! = 815915283247897734345611269596115894272000000000 \approx 8.15915\,10^{47}.$$

Ein einfaches Programm auf einem Rechner kann daher schnell Probleme machen. Hier ist eine Formel von *Stirling* hilfreich (ohne Beweis): • *Un programme simple sur un ordinateur peut donc très vite causer des problèmes. Voici une formule de Stirling très utile (sans la preuve):*

Satz • Théorème 19.1 (Formel von Stirling: • Formule de Stirling:)

$$n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$$

e ist hier die Eulersche Zahl: • *Ici* e *est le nombre de Euler:* $e \approx 2.71828182845904523536028747135$ (auf 30 Stellen • *à 30 places*)

19.2 Anordnungsprobleme — Problèmes d'arrangement

19.2.1 Permutationen ohne Wiederholung — Permutations sans répétition

Paradigma — Paradigme (Beispiel eines praktischen Problems) • (Exemple d'un problème pratique)[4]

Problem • Problème 19.1 (Sitzmöglichkeiten: • Possibilités de s'asseoir:)

[4] Ein Paradigma ist ein Lehrbeispiel • *Un paradigme est un exemple démonstratif*

Situation: • **Situation:** *In einem Klassenzimmer befindet sich nichts ausser* 26 *nummerierten Stühlen. Die Nummern gehen von* 1 *bis* 26. *Pulte, Bänke und Tische hat man nach draussen gebracht. Vor der Tür warten 26 Studenten. Zur besseren Unterscheidbarkeit und Benennung erhält auch jeder Student eine verschiedene Nummer von* 1 *bis* 26, *mit der er aufgerufen wird.*

• *Dans une salle de classe il ne se trouve rien à l'exception de 26 chaises numérotées. Les numéros vont de 1 à 26. On vient d'enlever pupitres, bancs et tables. 26 étudiants attendent devant la porte. Pour pouvoir mieux distinguer les étudiants et pour mieux pouvoir les appeler, chaque étudiant reçoit un numéro différent de 1 à 26 avec lequel il est donc appelé.*

Frage: • **Question:** *Auf wieviele Arten kann man die* 26 *Studenten auf die* 26 *Stühle setzen, d.h. wieviele Sitzordnungen gibt es?*

• *De combien de manières différentes est-ce qu'on peut mettre les 26 étudiants sur les 26 chaises, c.-à.-d. combien est–ce que de répartitions des places existent?*

Lösung: • **Solution:**

- Der Student Nr. 1 kommt herein. Er findet 26 freie Stühle vor. Somit hat er für sich 26 Sitzmöglichkeiten.
  • *L'étudiant no. 1 entre. Il trouve 26 chaises libres. Par conséquent il a 26 possibilités de s'asseoir.*

- Der Student Nr. 2 kommt herein, Student Nr. 1 sitzt auf irgend einem Stuhl. Student Nr. 2 findet nur noch 25 freie Stühle vor. Somit hat er für sich nur noch 25 Sitzmöglichkeiten. Diese 25 Sitzmöglichkeiten hat er aber bei jeder Platzierung von Student Nr. 1, welcher sich auf 26 verschiedene Arten platzieren konnte. Zur ersten von Student Nr. 1 benutzten Möglichkeit hat Student Nr. 2 nun 25 Möglichkeiten, zur zweiten Möglichkeit von Student Nr. 1 hat Nr. 2 nun 25 Möglichkeiten, etc., zur letzten Möglichkeit von Student Nr. 1 hat Nr. 2 wiederum 25 Möglichkeiten. Zusammen haben beide also $26 \cdot 25$ Möglichkeiten. Die Anzahlen der Möglichkeiten multiplizieren sich!
  • *L'étudiant no. 2 entre. L'étudiant no. 1 est assis sur une chaise quelconque. L'étudiant Nr. 2 trouve encore 25 chaises libres. Par conséquent il a seulement 25 possibilités de s'asseoir. Mais il a ces 25 possibilités de s'asseoir pour chaque position de l'étudiant no. 1, qui pouvait se placer sur 26 sièges différents. A la première possibilité utilisée par l'étudiant no. 1, l'étudiant no. 2 a maintenant 25 possibilités, pour la deuxième possibilité de l'étudiant no. 1, l'étudiant no. 2 a aussi 25 possibilités, etc, pour la dernière possibilité de l'étudiant no. 1, l'étudiant no. 2 a de nouveau 25 possibilités. En tout les deux ont ainsi* $26 \cdot 25$ *possibilités. Les nombres des possibilités se multiplient!*

- Der Student Nr. 3 kommt herein. Die Studenten Nr. 1 und Nr. 2 sitzen bereits. Student Nr. 3 findet nur noch 24 freie Stühle vor. Somit hat zu jeder der $26 \cdot 25$ Sitzmöglichkeiten der beiden ersten Studenten noch 24 Möglichkeiten. Zusammen haben sie also $26 \cdot 25 \cdot 24$ Möglichkeiten, da sich ja die Anzahlen der Möglichkeiten multiplizieren.
  • *L'étudiant no. 3 entre. Les étudiants no. 1 et no. 2 sont déjà assis. L'étudiant Nr. 3 ne trouve que 24 chaises libres. Il a par conséquent pour chacune des* $26 \cdot 25$ *possibilités des premiers deux étudiants encore 24 possibilités. En tout les trois ont ainsi* $26 \cdot 25 \cdot 24$ *possibilités, parce que les nombres des possibilités se multiplient.*

- So geht es dann weiter. Schliesslich kommt der Student Nr. 25 herein. Er hat bei jeder der Sitzmöglichkeiten der vorher hineingegangenen Studenten noch 2 freie Plätze zur Auswahl. Total haben also die 25 ersten Studenten $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2$ Sitzmöglichkeiten.
  • *Ainsi on avance. Finalement l'étudiant no. 25 entre. Pour chaque façon de se placer des étudiants qui sont déjà là il a encore 2 sièges de libres et par conséquent 2 possibilités de se placer. Totalement les 25 premiers étudiants ont ainsi* $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2$ *possibilités de se placer.*

- Endlich kommt der letzte Student mit der Nummer 26 herein. Er hat bei jeder der Sitzmöglichkeiten der andern Studenten noch einen freien Platz zur Auswahl. Total haben somit die 26 Studenten $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = 26!$ Sitzmöglichkeiten.
  • *Enfin le dernier étudiant, numéro 26, entre. Pour chaque façon de se placer des autres étudiants il ne lui reste qu'une chaise de libre, il n'a donc qu'une seule possibilité de se placer. Totalement les 26 étudiants ont par conséquent* $26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = 26!$ *possibilités de se placer.*

Bemerkung: • **Remarque:** Falls in einer Menge von Individuen jedes Element (Individuum) einen unterscheidbaren Namen trägt, so kann man die Elemente auch den „Namen nach", d.h. alphabetisch ordnen, so wie in einem Lexikon: A... kommt vor B... etc., Aa... vor Ab... etc.. In einem solchen Fall spricht man von einer *lexikographischen Anordnung.*
• *Si dans un ensemble chaque élément (individu) porte un nom distinctif, on peut ranger les éléments "d'après les noms", c.-à.-d. de façon alphabétique, comme dans un lexique: A... vient aevant B... etc, Aa... aevant Ab... etc.. Dans un tel cas on parle d'une disposition lexicographique.*

Zum Nachdenken: • **A réfléchir:**
Falls die Klasse in 10 Sekunden einen Platzwechsel schafft, so braucht sie also $10 \cdot 26!$ Sekunden für alle Platzwechsel. Das sind $\frac{10 \cdot 26!}{60 \cdot 60 \cdot 24 \cdot 365}$ Jahre $= 1.278310^{20}$ Jahre. Vergleich: Das Alter des Universums bei der Urknalltheorie wird gegenwärtig auf ca. 1 bis 2 mal 10^{10} Jahre geschätzt[5]. Um die Sitzordnungen alle ohne Pause zu realisieren, bräuchte es also etwa 10^{10} mal soviel Zeit, wie das Universum alt ist!
• *Si la classe est capable d'exécuter un changement de place en 10 secondes, elle nécessite* $10 \cdot 26!$ *secondes pour tous les changements de place. Ça nous fait* $\frac{10 \cdot 26!}{60 \cdot 60 \cdot 24 \cdot 365}$ *ans* $= 1.278310^{20}$ *ans. Comparaison: L'âge de l'univers d'après la théorie du big bang est actuellement estimée à env. 1 à 2 fois* 10^{10} *ans*[6]*. Pour réaliser toutes les répartitions des places sans pauses, il faudrait donc* 10^{10} *fois l'âge de l'univers!*

Verallgemeinerung des Problems: • **Généralisation du problème:**
Statt mit 26 Studenten kann man das Problem gleich allgemein mit n Studenten lösen. In der Argumentation ist dann 26 durch n, 25 durch $n-1$ etc. zu ersetzen. Man erhält schliesslich so total $(n!)$ Möglichkeiten, n Studenten auf n Plätze zu setzen.
• *Au lieu de résoudre le problème avec 26 étudiants on peut le résoudre généralement avec n étudiants. Dans l'argumentation il faut alors remplacer 26 par n, 25 par* $n-1$ *etc.. Finalement on obtient totalement* $(n!)$ *possibilités de mettre n étudiants sur n places.*

Das abstrakte Problem — Le problème abstrait

Gegeben sei eine Menge $\mathcal{M}_n$ mit n Elementen, welche durchnummeriert sind mit den Nummern von 1 bis n. $\mathcal{M}_n$ entspricht der Menge der Studenten im vorherigen Beispiel. Dadurch hat man eine bijektive Zuordnung der nummerierten Elemente n_k zur Teilmenge der natürlichen Zahlen $\mathbf{N}_n = \{1, 2, 3, \ldots, n\}$. (Damit hat man eine bijektive Funktion). Da die Zuordnung eineindeutig ist, können wir die n_k jeweils gerade durch k ersetzen, ohne das Problem zu verändern: $\mathcal{M} = \mathbf{N}_n = \{1, 2, 3, \ldots, n\}$. Gesucht ist nun die Anzahl der Möglichkeiten, die Menge $\mathbf{N}_n = \{1, 2, 3, \ldots, n\}$ auf sich selbst abzubilden, d.h. im obigen Problem die Menge der Nummern der Studenten $\mathbf{N}_n$ der Menge der Nummern der Stühle $\mathbf{N}_n$ zuzuordnen.
• *Soit donné un ensemble* $\mathcal{M}_n$ *avec n éléments, qui sont énumérotés par les numéros de 1 jusqu'à n.* $\mathcal{M}_n$ *correspond à un ensemble d'étudiants dans l'exemple antérieur. On a ainsi un rapport bijectif des éléments numérotés* n_k *à un sous–ensemble* $\mathbf{N}_n = \{1, 2, 3, \ldots, n\}$ *des nombres naturels. (On a ainsi une fonction bijektive.) Comme le rapport est biunivoque, nous pouvons remplacer les* n_k *chaque fois par k, sans transformer le problème:* $\mathcal{M} = \mathbf{N}_n = \{1, 2, 3, \ldots, n\}$*. Maintenant on cherche le nombre des possibilités d'appliquer l'ensemble* $\mathbf{N}_n = \{1, 2, 3, \ldots, n\}$ *sur lui-même, c.-à.-d. dans le problème susdit appliquer l'ensemble des numéros des étudiants* $\mathbf{N}_n$ *à l'ensemble des numéros des chaises* $\mathbf{N}_n$*.*

[5] Die Fachleute streiten sich allerdings über diesen Wert. Je nach Wissensstand wird er laufend berichtigt.
[6] Les experts se disputent en effet au sujet de cette valeur. Elle est corrigée couramment d'après l'état des connaissances.

Sei $\sigma(k)$ bei einer solchen Zuordnung (im obigen Problem eine Sitzmöglichkeit) das Bild (oben die Stuhlnummer) von k (k entspricht oben der Nummer des Studenten). Dann wird also durch eine solche Zuordnung σ die Menge $\{1, 2, 3, \ldots, n\}$ (oben die Menge der Studenten) der Menge $\{\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n)\}$ (oben die Stühle) zugeordnet. Schreibt man die Bilder $\sigma(k)$ unter die Urbilder k, so erscheint die durch σ ausgesonderte Relationsmenge in folgender Gestalt:
• *Soit $\sigma(k)$ l'image (en haut le numéro des chaises) à une telle application (dans le problème susdit à une possibilité de s'asseoir) de k (en haut k correspond au numéro de l'étudiant. Alors par une telle application, on applique σ (en haut l'ensemble des étudiants) à l'ensemble $\{1, 2, 3, \ldots, n\}$ (en haut les chaises). Si on écrit les images $\sigma(k)$ sous les originaux k, ainsi l'ensemble de relation défini par σ apparaît dans la forme suivante:*

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

Damit ist also eine Teilmenge von $\mathbf{N}_n \times \mathbf{N}_n$ gegeben, für die die Relation „Funktion σ" zutrifft.
• *Ainsi un sous-ensemble de $\mathbf{N}_n \times \mathbf{N}_n$ est donné pour lequel le rapport de "fonction σ" est valable.*
Durch das folgende Schema wird daher eine neue Anordnung $\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n)$ der Elemente $1, 2, 3, \ldots, n$ definiert.
• *Par conséquent, par le schéma suivant, une nouvelle disposition $\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n)$ des éléments $1, 2, 3, \ldots, n$ est définie.*

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

Wir sagen: • *Nous disons:*

Definition • Définition 19.3 (Permutation: • Permutation:)
Die Anordnung $\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n)$ der Elemente aus $\mathbf{N}_n$ heisst **Permutation** *$\mathcal{P}$ der Anordnung $(1, 2, 3, \ldots, n)$ dieser Elemente.*
• *La disposition $\sigma(1), \sigma(2), \sigma(3), \ldots, \sigma(n)$ des éléments de $\mathbf{N}_n$ s'appelle* **permutation** *$\mathcal{P}$ de la disposition $(1, 2, 3, \ldots, n)$ de ces éléments.*

Um eine Permutation zu geben, können wir auch schreiben:
• *Pour donner une permutation, nous pouvons aussi écrire:*

$$P = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

Die Reihenfolge der Spalten kann beliebig sein.
• *Les collonnes se présentent dans un ordre quelconque.*

Beispiel: • Exemple Durch die folgende Anordnung ist eine solche Permutation gegeben: • *Par la disposition suivante, une telle permutation est donnée:*

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

1 wird auf 4, 2 auf 1 u.s.w.. abgebildet. Nun können wir unser Problem mit den Studenten und den Stühlen abstrakt und allgemein stellen:
• *1 est appliqué sur 4, 2 sur 1 etc.. Maintenant nous pouvons poser notre problème avec les étudiants et les chaises de façon abstraite et générale:*

Problem • Problème 19.2
Permutationen ohne Wiederholung: • Permutations sans répétitions:

Frage: *Wieviele Permutationen $\mathcal{P}$ der Nummern $1, 2, \ldots, n$ gibt es?*
• Question: *• Combien de permutations $\mathcal{P}$ des numéros $1, 2, \ldots, n$ existent–ils?*
Oder anders gefragt: Wieviele Anordnungsmöglichkeiten der Zahlen $1, 2, \ldots, n$ in einer Reihe gibt es?
• Autrement: Combien de possibilités de dispositions des nombres $1, 2, \ldots, n$ dans un rang existent–elles?
Oder nochmals anders gefragt: Wieviele bijektive Funktionen $\mathbf{N}_n \longmapsto \mathbf{N}_n$ gibt es?
• Autrement encore: Combien de fonctions bijektives $\mathbf{N}_n \longmapsto \mathbf{N}_n$ existent–elles?

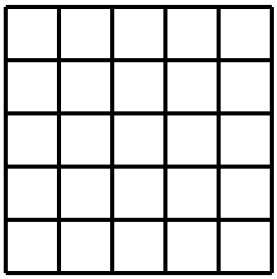
Symbole • Symboles 1 : $P(n)$
Sei $P(n)$ = Anzahl Permutationen der Elemente von M_n der natürlichen Zahlen von 1 bis n.
• Soit $P(n)$ = nombre des permutations des éléments de M_n des nombres naturels de 1 jusqu'à n.

Nun wissen wir: *• Nous savons:*

Satz • Théorème 19.2
Permutationen ohne Wiederholung: • Les permutations sans répétition:

$$P(n) = n!$$

Abbildung 19.1: Teilflächen, verschieden zu färben ... *• Surfaces part., à colorer de manière diff....*



Beispiel: *• Exemple:* Wieviele Möglichkeiten gibt es, die in 19.1 gezeigten Teilflächen mit verschiedenen Farben zu färben? – Bei einer Färbung werden den 25 verschiedenen Flächen 25 verschiedene Farben zugeordnet. Statt Flächen und Farben kann man auch nur die Nummern 1 bis 25 betrachten. Man hat also eine bijektive Abbildung einer Menge $\mathcal{M}_{25}$ oder von $\mathbf{N}_{25}$ auf sich. Es wird also nach $P(25)$ = Anzahl Permutationen von $1, 2, 3, \ldots, 25$ gefragt. Das gibt $25! \approx 1.55112 \cdot 10^{25}$. Wie lange hätte wohl einer, um alle Möglichkeiten auszuprobieren?
• Combien de possibilités est-ce qu'il y a de colorer les différentes surfaces montrées dans 19.1 avec des couleurs différentes? – À une coloration, 25 couleurs différentes sont adjointes aux 25 surfaces différentes. Au lieu de surfaces et couleurs, on peut aussi considérer seulement les numéros de 1 jusqu'à 25. On a ainsi une application bijektive d'un ensemble $\mathcal{M}_{25}$ ou de $\mathcal{M}_{25}$ sur soi–même. On cherche donc $P(25)$ = nombre de permutations de $1, 2, 3, \ldots, 25$. Ça donne $25! \approx 1.55112 \cdot 10^{25}$. Combien de temps est–ce qu'il faudrait probablement pour exécuter toutes les possibilités?

19.2.2 Permutationen mit Wiederholung — Permutations avec répétition

Paradigma — Paradigme

Problem • Problème 19.3
Vertauschungsmöglichkeiten von Briefen: • Possibilités d'échange de lettres:

Situation: *Ein Personalchef hat* 20 *verschiedene Briefe geschrieben. Davon sind* 7 *identische Kopien eines Informationsschreibens an eine Gruppe von Mitarbeitern, die andern* 13 *Briefe sind vertrauliche und persönliche Antworten in Lohnfragenen anderer Mitarbeiter. Die zugehörigen 20 Couverts liegen ebenfalls bereit.*

• Situation: *• Un chef de personnel a écrit 20 lettres différentes. Il y a 7 copies identiques d'une lettre d'information pour un groupe de collaborateurs et 13 lettres concernant des réponses adressées d'autres collaborateurs concernant des questions de salaire. Les 20 enveloppes sont aussi prêtes.*

Frage: *Wieviele Möglichkeiten hat die Sekretärin, die Briefe zu verschicken, sodass für sie Probleme entstehen könnten?*

• Question: *• Combien de possibilités d'envoyer les lettres est-ce que la secrétaire a, de façon que pour elle des problèmes pourraient se poser?*

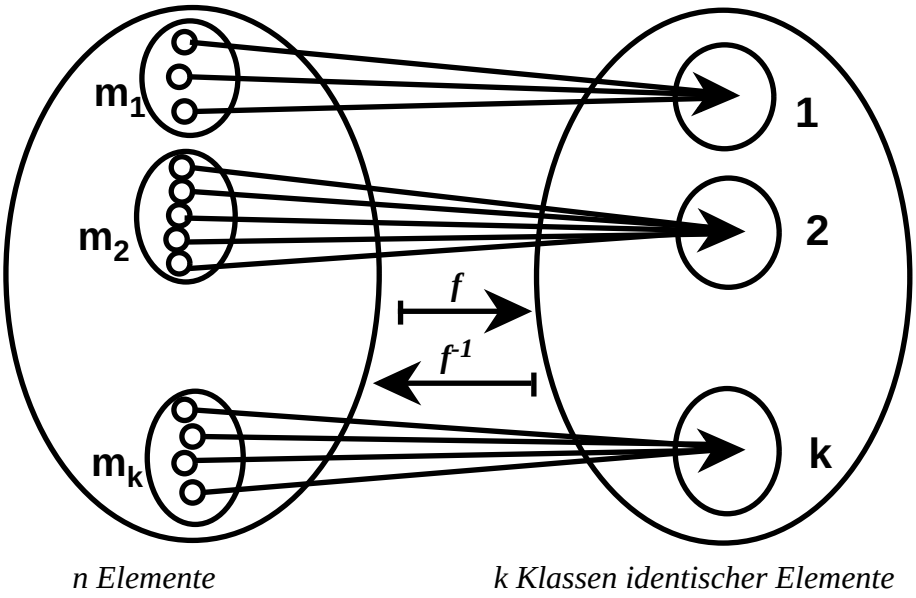
Lösung: **• Solution:** Wenn alle Briefe verschieden wären, so hätte sie 20! Möglichkeiten, die Briefe in Couverts zu stecken. Da nur eine Möglichkeit akzeptiert werden kann, führen dann $(20! - 1)$ Möglichkeiten zu Problemen.
Wenn nun 7 Briefe gleich sind, können diese 7 Briefe unter sich vertauscht werden, ohne dass ein Problem entsteht. Man kann das auf 7! Arten tun. Wenn nun X die Anzahl der Platzierungsmöglichkeiten der 13 verschiedenen Briefe in den 20 Couverts ist, so können zu jeder der X Möglichkeiten der verschiedenen Briefe die restlichen, gleichen Briefe auf $Y = 7!$ Arten unter sich vertauscht werden, ohne dass etwas passiert. Da das bei jeder der X Möglichkeiten der Fall ist, *multiplizieren sich die Anzahlen der Möglichkeiten zur Gesamtzahl der Möglichkeiten.* Andere Vertauschungsmöglichkeiten als die hier vorkommenden hat man nicht. Somit gilt: $20! = X \cdot Y = X \cdot 7!$ und damit $X = \frac{20!}{7!}$.
Die Anzahl unerwünschter Möglichkeiten ist somit $X-1 = \frac{20!}{7!}-1 = 482718652416000-1 \approx 4.82719\,10^{14}$.
• Si toutes les lettres étaient différentes, elle auraient 20! *possibilités de mettre les lettres dans les enveloppes. Comme une seule possibilité peut être acceptée, les* $(20! - 1)$ *autres possibilités causent des problèmes.*
Si 7 lettres sont maintenant les mêmes, ces 7 lettres peuvent être échangées entre elles sans qu'il y ait de problèmes. Cela on peut le faire de 7! *manières différentes. Si maintenant X est le nombre de possibilités de placer les* 13 *lettres différentes dans le* 20 *enveloppes, pour chacune des X possibilités des lettres différentes les lettres identiques qui restent peuvent être échangées entre elles de $Y = 7!$ manières différentes sans qu'il se passe quelque chose d'embêtant. Comme c'est le cas pour chacune des X possibilités, les nombres des possibilités se multiplient au nombre total des possibilités. On n'a pas d'autres possibilités d'échange que celle qui sont mentionnées ici. Par conséquent il vaut:* $20! = X \cdot Y = X \cdot 7!$ *et par conséquent* $X = \frac{20!}{7!}$.
Le nombre de possibilités indésirables est par conséquent $X - 1 = \frac{20!}{7!} - 1 = 482718652416000 - 1 \approx 4.82719\,10^{14}$.

Verallgemeinerung des Problems: **• Généralisation du problème:**
Wir gehen wieder von 20 Briefen aus, 7 davon gleich, die wir zur *Klasse* 1 zusammenfassen. Weiter sei jetzt nochmals ein spezieller Brief da, zu welchem sich noch zwei gleiche finden. Diese 3 seinen in einer *Klasse* 2 zusammengefasst. Dann finden wir nochmals 4 gleiche, die in einer *Klasse* 3 zusammengefasst werden. Sei nun Y_i die Anzahl der Vertauschungsmöglichkeiten der Briefe in der *Klasse* i unter sich und X wie vorhin die Anzahl der Vertauschungsmöglichkeiten der restlichen ungleichen Briefe. Dann gilt aus demselben Grunde wie oben:
• Nous partons encore de 20 lettres dont 7 sont les mêmes qui sont proupées dans une classe 1. *En plus on a une lettre spéciale, pour laquelle on trouve deux autres identiques. Ces 3 soient réunies dans une classe* 2. *Nous trouvons encore 4 identiques qui sont réunies dans une classe* 3. *Soit maintenant Y_i le nombre des possibilités d'échange des lettres entre elles dans la classe i et X comme en haut le nombre des possibilités d'échange des lettres inégales et restantes. Alors il vaut par la même raison comme en haut:*

$$20! = X \cdot Y_1! \cdot Y_2! \cdot Y_3! = X \cdot 7! \cdot 3! \cdot 4!, \quad \text{also} \quad \bullet \ \textit{donc}$$

$$X = \frac{20!}{7! \cdot 3! \cdot 4!}$$

Abbildung 19.2: Anzahl möglicher Umkehrabbildungen f^{-1}? • *Possibilités d'applications inverses* f^{-1}?



• *Esquisse:* *n éléments* $\longmapsto$ *n classes d'éléments identiques*

Das führt uns auf folgendes allgemeinere Problem:
• *Ça nous mène au problème général:*

Gegeben: • **Donné:**
Total n Briefe, n Couverts, davon k Klassen je unter sich gleicher Briefe wie folgt:
• *Totalement* n *lettres,* n *enceloppes dont on a* k *classes de lettres identiques entre elles:*
$Klasse_1$: m_1 gleiche Briefe vom Typ 1 • $Classe_1$*:* m_1 *lettres identiques du type* 1,
$Klasse_2$: m_2 gleiche Briefe vom Typ 2 • $Classe_2$*:* m_1 *lettres identiques du type* 2,
$\vdots$ $\vdots$
$Klasse_k$: m_k gleiche Briefe vom Typ k • $Classe_k$*:* m_k *lettres identiques du type* k

Gesucht: • **Trouver:** Anzahl Möglichkeiten $P_n(m_1, m_2, \ldots, m_k)$, die Briefe in die Couverts zu platzieren.
• *Nombre de possibilités* $P_n(m_1, m_2, \ldots, m_k)$*, de mettre les lettres dans les enveloppes.*

Symbole • Symboles 2 : $P_n(m_1, m_2, \ldots, m_k)$
$P_n(m_1, m_2, \ldots, m_k)$ = Anzahl Möglichkeiten, die eben beschriebenen n Objekte (hier Briefe, wobei k $Klassen$ mit je n_j gleichen Objekten darunter sind) auf n Plätze (hier Couverts) zu platzieren.
• $P_n(m_1, m_2, \ldots, m_k)$ = *nombre de possibilités, de placer les* n *objets qu'on vient de décrire (ici des lettres parmi lesquelles on trouve* k *classes avec* n_j *objets identiques entre eux) sur* n *places (ici des enveloppes).*

Definition • Définition 19.4 (Permutat. m. Wiederholung: • Permut. avec répétitions:)
Gegeben sei eine Menge $\mathcal{M}_n$ mit n Elementen. Darin seinen k $Klassen$ mit je n_i gleichen Elementen (pro $Klasse\, i$) enthalten. Bei der Nummerierung der Elemente erhalten alle Elemente einer Klasse dieselbe

Nummer. Eine Permutation der Elemente von $\mathcal{M}_n$ nennen wir **Permutation mit Wiederholung**.
• *Soit donné un ensemble $\mathcal{M}_n$ avec n éléments. Dans cet ensemble on trouve k classes avec n_i éléments identiques (par classe i). A une énumération des éléments, tous les éléments d'une classe reçoivent le même numéro. Nous appelons une permutation des éléments de $\mathcal{M}_n$* **une permutation avec répétitions**.

Wir wissen jetzt: • *Maintenant nous savons:*

Satz • Théorème 19.3 (Permutationen mit Wiederholung • Permut. avec répétition:) *:*
Anzahl der Permutationen mit Wiederholung: • Nombre de permutations avec répétitionss:

$$P_n(m_1, m_2, \ldots, m_k) = \frac{n!}{m_1! \cdot m_2! \cdot m_k!}$$

Das abstrakte Problem — Le problème abstrait

Gegeben: • Donné: Eine Menge mit n Elementen, z.B. $\mathbf{R}_n = \{1, 2, 3, \ldots, n\}$ sowie eine Menge mit k Elementen, z.B. $\mathbf{R}_k = \{1, 2, 3, \ldots, k\}$, $n \geq k$. Man betrachte dann die möglichen Funktionen $f : \mathbf{R}_n \longmapsto \mathbf{R}_k$ (ein Beispiel ist in Abb. 19.2 dargestellt).
• *Un ensemble avec n éléments, par exemple $\mathbf{R}_n = \{1, 2, 3, \ldots, n\}$ ainsi qu'un ensemble avec k éléments, z.B. $\mathbf{R}_k = \{1, 2, 3, \ldots, k\}$. Puis on considère les fonctions possibles $f : \mathbf{R}_n \longmapsto \mathbf{R}_k$ (un exemple est représenté dans image 19.2).*

Gesucht: • Trouver: Anzahl möglicher Umkehrabbildungen $f^{-1} : \mathbf{R}_k \longmapsto \mathbf{R}_n$. Dabei wird das erste Element (1 rechts im Bild) m_1 mal abgebildet, das zweite Element (2 rechts im Bild) m_1 mal u.s.w..
• *Nombre d'applications inverses possibles $f^{-1} : \mathbf{R}_k \longmapsto \mathbf{R}_n$. Pour cela le premier élément (1 à droite dans l'image) est appliqué m_1 fois, le deuxième élément (2 à droite dans l'image) m_1 fois etc..*

Es werden also die k Klassen gleicher Elemente (gleiche Briefe im Paradigma) auf die n verschiedenen Elemente (Couverts im Paradigma) abgebildet. Die gesuchte Anzahl ist dann $P_n(m_1, m_2, \ldots, m_k)$.
• *Les k classes d'éléments identiques (lettres identiques dans le paradigme) sont ainsi appliquées sur les n éléments différents (enveloppes dans le paradigme). Le nombre qu'on cherche est donc $P_n(m_1, m_2, \ldots, m_k)$.*

Beispiel: • Exemple: Auf wieviele Arten lassen sich in einer Klasse mit 26 Studenten 5 Arbeitsgruppen mit 4, 5, 5, 6 und 6 Studenten bilden? Die Lösung ist:
• *De combien de manières différentes est-ce qu'on peut former dans une classe de 26 étudiants 5 groupes de travail avec 4, 5, 5, 6 et 6 étudiants? La solution est:*

$$P_{26}(4, 5, 5, 6, 6) = \frac{26!}{4! \cdot 5!^2 \cdot 6!^2} = 2251024905729600 \approx 2.25102\,10^{15}$$

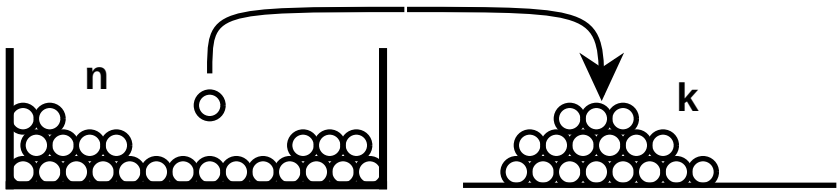
19.3 Auswahlprobleme mit und ohne Anordnung — Problèmes de sélection avec et sans rangement

19.3.1 Die Fragestellungen — Les questions

Kombinationen — Combinaisons

Problem • Problème 19.4 (Auswahlproblem: • Problème de sélection:)

Abbildung 19.3: Auswahlproblem, Kombinationen • *Problème de sélection, combinaisons*



Gegeben: • **Donné:** *Eine Kiste mit n wohlunterscheidbaren Objekten, z.B. verschiedenfarbigen Kugeln. Aus der Kiste werden dann auf eine beliebige Art und Weise k Objekte herausgegriffen und nebenan aufgehäuft. (Vgl. Abb. 19.3.)*
• *Une caisse qui contient n objets bien distincts, par exemple des boules de différents couleurs. Dans la caisse, on choisit k objets de manière quelconque et on les accumule à côté. (Voir fig. 19.3.)*

Frage: • **Question:** *Auf wieviele Arten sind solche Haufenbildungen nebenan möglich?*
• *De combien de manières différentes peut–on former le tas à côté?*

Wohlverstanden spielt bei der Haufenbildung die Anordnung der Objekte resp. der Kugeln keine Rolle. Dieses Problem lässt sich ohne viel Denkaufwand gleich abstrakt stellen. Die Kugeln in der Kiste bilden eine Menge $\mathcal{M}_n$, z.B. $\mathcal{M}_n = \mathbf{N}_n = \{1, 2, 3, \ldots, n\}$. Herausgegriffen wird eine Teilmenge $\mathcal{M}_k \subseteq \mathcal{M}_n$, z.B. $\mathbf{N}_k = \{1, 2, 3, \ldots, k\}$, $k \leq n$. Diese Teilmenge bildet den Haufen nebenan.
• *La disposition des objets ne joue bien entendu aucun rôle à la disposition des objets resp. des boules. Il est possible de poser ce problème tout de suite abstraitement sans beaucoup de dépense de travail de cerveau. Les boules dans la caisse forment un ensemble $\mathcal{M}_n$, par exemple $\mathcal{M}_n = \mathbf{N}_n = \{1, 2, 3, \ldots, n\}$. On choisit un sous-ensemble $\mathcal{M}_k \subseteq \mathcal{M}_n$, z.B. $\mathbf{N}_k = \{1, 2, 3, \ldots, k\}$, $k \leq n$. Ce sous-ensemble forme le tas d'à côté.*

Definition • Définition 19.5
Kombination ohne Wiederholung • Combinaison sans répétition
Eine solche Auswahl von k Elementen aus $\mathcal{M}_n$ heisst **Kombination k–ter Ordnung ohne Wiederholung** *bei n Elementen, kurz: Kombination k–ter Ordnung.*
• *Un tel choix de k éléments dans $\mathcal{M}_n$ s'appelle* **combinaison d'ordre k sans répétition** *pour n éléments, brièvement: Combinaison d'ordre k.*

Symbole • Symboles 3 (Anzahl Kombinationen: • Nombre de combinaisons:)
$C(k, n) =$ *Anzahl Kombinationen k–ter Ordnung bei n Elementen.*
• $C(k, n) =$ *nombre de combinaisons d'ordre k pour n éléments.*

Abstraktes Problem (Kombinationen ohne Wiederholung):
• Problème abstrait (combinaisons sans répétition):

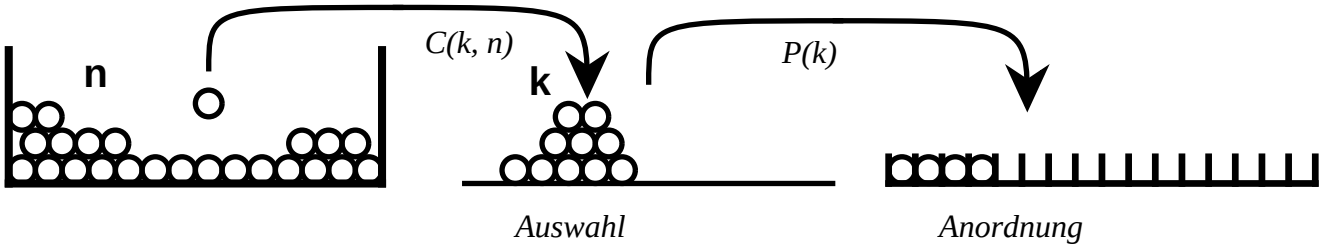
Gegeben: • **Donné:** Eine Menge $\mathcal{M}_n$ mit n Elementen.
• *Un ensemble $\mathcal{M}_n$ à n éléments.*

Frage: • **Question:** $C(k, n) = ?$ D.h. wieviele Teilmengen mit genau k Elementen kann man bilden?
• $C(k, n) = ?$ *C.-à.-d. combien de sous-ensembles peut–on former avec exactement k éléments?*

Variationen — Arrangements

In Abb. 19.4 wird die Auswahl (Kombination) anschliessend noch angeordnet. Zwei solche Kombinationen mit denselben Elementen, aber verschiedener Anordnungen sind jetzt unterscheidbar. Man definiert

Abbildung 19.4: Relationsmenge, Abbildung • *Ensemble de relations et d'applications (choix, disposition)*



daher:
• *Dans la fig. 19.4 le choix (combinaison) est encore arrangé. On peut distinguer deux combinaisons de ce genre avec les mêmes éléments, mais de dispositions différentes. On définit par conséquent:*

Definition • Définition 19.6
Variation ohne Wiederholung: • Arrangement sans répétition:
Werden die aus $\mathcal{M}_n$ ausgewählten Elemente (die Kombination also) noch angeordnet, so spricht man von einer **Variation k–ter Ordnung ohne Wiederholung** *bei n Elementen. Kurz: Variation k–ter Ordnung.*
• *Si les éléments choisis dans $\mathcal{M}_n$ sont encore arrangés, on parle d'un* **arrangement d'ordre k sans répétition** *pour n éléments. Brièvement: Arrangement d'ordre k.*

Symbole • Symboles 4 (Anzahl Variationen: • Nombre d'arrangements:)
$V(k, n) =$ *Anzahl Variationen k–ter Ordnung bei n Elementen.*
• $V(k, n) =$ *nombre d'arrangements d'ordre k pour n éléments.*

Beispiel: • Exemple

Gegeben seien die Elemente a, b und c. Gesucht sind alle Kombinationen und Variationen 2–ter Ordnung.
• *Soient donnés les éléments a, b et c. Trouver toutes les combinaisons et toutes les arrangements d'ordre 2.*

Lösung: • Solution:

Kombinationen • *Combinaisons*:	$a\ b$	$a\ c$	$b\ c$:	3 Stück.	• *3 pièces*
Variationen: • *Arrangements:*	$a\ b$	$a\ c$	$b\ c$		
	$b\ a$	$c\ a$	$c\ b$:	6 Stück.	• *6 pièces*

Wiederholungen — Répétitions

Ersetzt man in der Vorratsmenge $\mathcal{M}_n$ jedes der Elemente e_i durch eine Menge E_i mit gleichen Elementen, die sich nur durch einen *internen Index* unterscheiden (z.B. $E_i = \{e_{i1}, e_{i2}, e_{i3}, \ldots\}$), so wird es möglich, ein Element e_i mehrmals auszuwählen, wobei der interne Index nach der Auswahl wieder weggelassen werden kann[7]. Denselben Effekt erzielen wir, wenn wir nach der Auswahl eines Elementes eine identische Kopie dieses Elementes wieder zurücklegen. Wir stellen uns also vor, dass sich ein Element e_i bei seiner Auswahl dupliziert, sodass trotz Auswahl und Entfernung des Elements die Menge $\mathcal{M}_n$ unverändert bleibt. Ein Element wird also bei der Auswahl und Entfernung aus $\mathcal{M}_n$ sofort wieder in $\mathcal{M}_n$ nachgeliefert, etwa so wie bei einem bestimmten Artikel im Regal eines gut geführten Selbstbedienungsladens, wo die Regale immer sofort wieder aufgefüllt werden. Falls dieses Auffüllen, Duplizieren, Kopieren oder Zurücklegen beliebig oft möglich ist, so sagen wir, die Elemente in $\mathcal{M}_n$ seien *wiederholt auswählbar*. Wir definieren

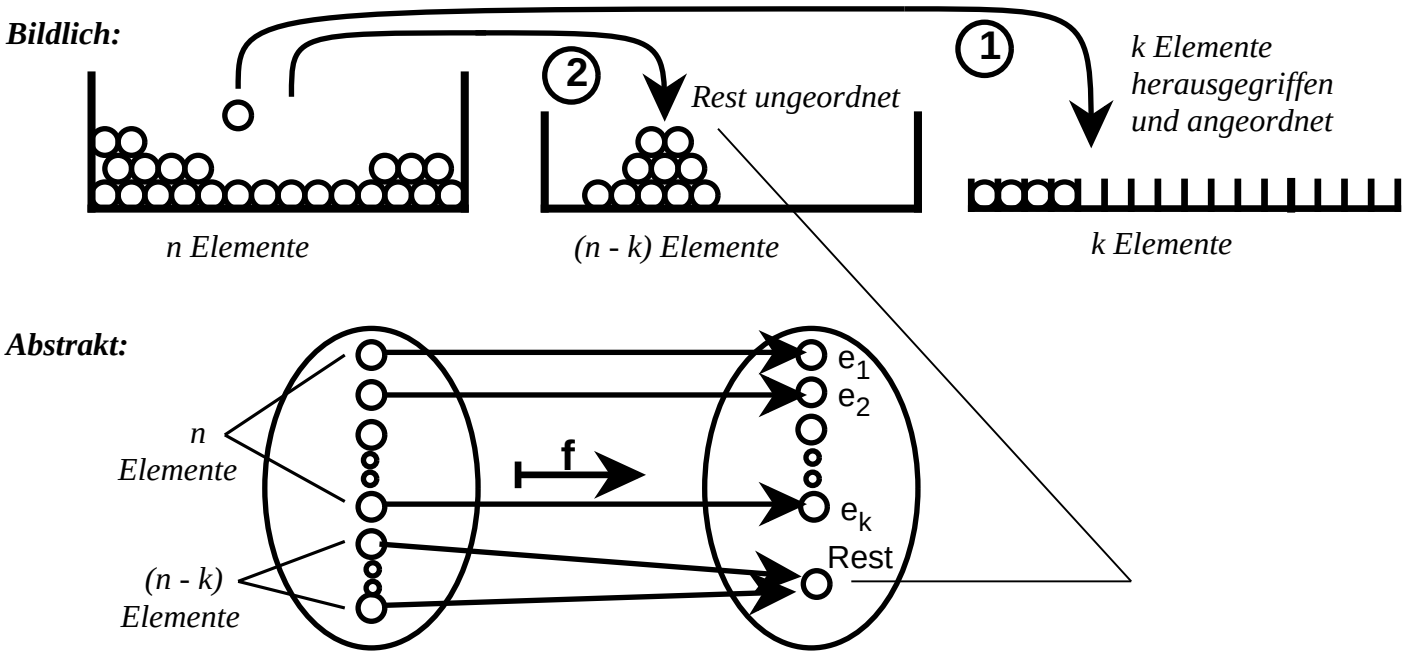
[7] Der interne Index wird nur zur Bildung der „Mengen gleicher Elemente E_i“ gebraucht, die notwendig sind, um eine wiederholte Auswahl desselben Elements möglich zu machen.

nun:
• *Si on remplace dans l'ensemble de réserve $\mathcal{M}_n$ chacun des éléments e_i par un ensemble E_i avec les mêmes éléments, qui ne se distinguent que par un indice interne (par exemple $E_i = \{e_{i1}, e_{i2}, e_{i3}, \ldots\}$), ainsi il devient possible de choisir un élément e_i plusieurs fois. L'indice interne peut être omis après le choix*[8]*. Nous obtenons le même effet si nous mettons en réserve une copie identique de cet élément après le choix de l'élément. Nous nous imaginons donc qu'un élément e_i se duplique lors de son choix, et, que malgré qu'on ait choisi et enlevé l'élément, l'ensemble $\mathcal{M}_n$ reste inchangé. Un élément est donc fourni tout de suite dans $\mathcal{M}_n$ lors qu'on l'a choisi et enlevé de $\mathcal{M}_n$. On peut comparer cela à la situation dans un supermarché où les marchandises sont remplacées sur les étagères au fur et à mesure qu'elles sont vendues. S'il est possible aussi souvent qu'on veut de remplir, copier ou remettre les éléments, nous disons que les éléments dans $\mathcal{M}_n$ sont répétitivement sélectionnables. Nous définissons maintenant:*

Definition • Définition 19.7
Kombination und Variation mit Wiederholung: • Combinaison et arrangement avec répétition:
Sind bei der Bildung einer Kombination oder einer Variation die Elemente aus $\mathcal{M}_n$ wiederholt auswählbar, so spricht man von einer Kombination oder einer Variation **mit Wiederholung**.
• *Si à la formation d'une combinaison ou d'un arrangement les éléments de $\mathcal{M}_n$ sont sélectionnables de façon répétitive, nous parlons d'une combinaison ou d'un arrangement* **avec répétition**.

Wir beginnen nun mit der Variation ohne Wiederholung:
• *Nous commençons maintenant avec l'arrangement sans répétition:*

Abbildung 19.5: Variationen ohne Wiederholung • *Arrangement sans répétition*



• *Arrangement sans répétition: Image — abstrait, éléments, reste.*

[8] L'indice interne n'est utilisé que pour former l'ensemble d'éléments identiques E_i, qui sont nécessaires pour rendre possible un choix répété d'éléments identiques.

19.3.2 Variation ohne Wiederholung — Arrangement sans répétition

Aus n Elementen werden k Elemente herausgegriffen und angeordnet, ohne Wiederholung, so wie in Abb. 19.5 dargestellt. Dort wird z.B. das Element e_1 auf den Platz 1, e_2 auf den Platz 2 u.s.w.. gelegt. Alle $(n-k)$ nicht ausgewählten Elemente, der Rest also, kann man sich anschliessend in eine Kiste nebenan gelegt denken, auf einen Haufen also. Diese anschliessende Operation verändert die Anzahl Auswahl– und Anordnungsmöglichkeiten der ersten k Elemente nicht, denn diese Haufenbildung ist eine einzige, unabhängige Handlung, die nichts weiteres beiträgt. In dieser Restkiste nebenan spielt also die Anordnung der Elemente keine Rolle. Man unterscheidet diese Elemente demnach nicht, es ist egal, wie sie liegen. Daher bilden sie eine Klasse nicht unterschiedener, also gleicher Elemente, die auf nur eine einzige Art angeordnet werden können (da sie als nicht unterscheidbar gelten). Daher hat man folgendes Problem: Man hat n Elemente, k verschiedene und $n-k$ gleiche. Diese Elemente sind anzuordnen. Oder abstrakt: Man sucht die Anzahl der möglichen Umkehrfunktionen f^{-1} (vgl. Abb. 19.5). Das Problem haben wir aber bereits bei den Permutationen mit Wiederholung gelöst: Die Anzahl ist $P_n(n-k) = \frac{n!}{(n-k)!}$
• *Dans n éléments on choisit k éléments qui sont disposés immédiatement, sans répétition d'éléments, à l'instar de fig. 19.5. Là par exemple l'élément e_1 est mis sur la place 1, e_2 sur la place 2 etc.. Ensuite on s'imagine que tous les $(n-k)$ éléments non–choisis, donc le reste, sont mis dans une caisse à part resp. sur un tas. Cette opération ne change pas le nombre de possibilités de choix, le nombre de possibilités de disposition des premiers k éléments , car cette formation de tas est une action unique et indépendante qui ne contribue rien à l'opération. Dans cette caisse de restes à part, la disposition des éléments ne joue pas de rôle. On ne distingue donc pas ces éléments, c'est égal comme ils sont disposés. Par conséquent ils forment une classe d'éléments non–distingués et donc une classe d'éléments égaux qui sont disposés d'une seule manière (parce qu'ils comptent comme non–distinctifs). Par conséquent on a le problème suivant: On a n éléments, k sont distinctifs et $n-k$ sont égaux. Ces éléments sont à arranger. Ou bien abstraitement: On cherche le nombre des fonctions inverses possibles f^{-1} (voir fig. 19.5). Ce problème a été résolu déjà à l'occasion des permutations avec répétition: Le nombre est $P_n(n-k) = \frac{n!}{(n-k)!}$.*

Satz • Théorème 19.4 (Variationen ohne Wiederholung: • Arrangements sans répédition:)

$$V(k,n) = P_n(n-k) = \frac{n!}{(n-k)!}$$

Beispiel: • Exemple:

Auf wieviele Arten kann man 20 verschiedene vorhandene Ferienjobs an 26 verschiedene Studenten verteilen, die alle einen solchen Job haben wollen, wenn diese Jobs nicht in Teiljobs aufteilbar sind?
Es handelt sich um die Auswahl 20 aus 26 mit anschliessender Zuordnung zu unterscheidbaren Studenten, d.h. Anordnung. Die Lösung ist somit:
• *De combien de manières est-ce qu'on peut distribuer 20 jobs de vacances différents et disponibles à 26 étudiants différents qui veulent avoir tous un semblable travail, si ces jobs ne sont pas divisibles dans des job partiels?*
Il s'agit du choix de 20 sur 26 avec un classement des étudiants non distinctifs, c.-à.-d. un arrangement. La solution est par conséquent:

$$V(20,26) = \frac{26!}{(26-20)!} = \frac{26!}{(6)!} = 672152435211009392640000000 \approx 6.72152\,10^{25}$$

Ein Spezialfall: • Un cas spécial: $V(n,n) = P_n(n-n) = P_n(0) = P(n)$
$\rightsquigarrow$ Permutation ohne Wiederholung! • *Permutation sans répétition!*

19.3.3 Kombination ohne Wiederholung — Combinaison sans répétition

Die Formel — La formule

Auf Seite 149 haben wir gesehen, dass sich bei Aussonderung einer Teilmenge gleicher Elemente die Anzahl der Möglichkeiten multiplikativ verhalten. Da war $20! = X \cdot Y = X \cdot 7!$. Die gleiche Situation

finden wir beim Übergang von den Kombinationen zu den Variationen: Eine Variation (k Elemente aus n Elementen) entsteht aus einer Kombination durch Anordnung der k ausgewählten Elemente. Dazu hat man $P(k) = k!$ Möglichkeiten. Es gilt also:
• *A la page 149 nous avons vu qu'à une sélection d'un sous-ensemble de mêmes éléments le nombre des possibilités se comporte de façon multiplikative. On y a trouvé:* $20! = X \cdot Y = X \cdot 7!$. *Nous trouvons la même situation au passage des combinaisons à l'arrangement: Un arrangement (k éléments de n éléments) peut être obtenu d'une combinaison par la disposition des k éléments choisis. On y a* $P(k) = k!$ *possibilités. Il vaut donc:*

Lemma • Lemme 19.1 (Variationen und Kombination: • Arrangements et combinaison:)

$$V(k,n) = C(k,n) \cdot P(k), \text{ also } \tfrac{n!}{(n-k)!} = C(k,n) \cdot k!$$

Daraus folgt: • *Il en suit:*

Satz • Théorème 19.5 (Kombination ohne Wiederholung • Combinaison sans répétition:)

$$C(k,n) = \tfrac{n!}{k! \cdot (n-k)!} = \tfrac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}$$

Das Beispiel Zahlenlotto „6 aus 45“: • L'exemple du jeu de loto "6 de 45":

Auf wieviele Arten kann man 6 verschiedene Zahlen aus den 45 ersten natürlichen Zahlen auswählen? Hier handelt es sich um eine typische Frage nach der Anzahl Kombinationen $C(6, 45)$. Diese ist gleich:
• *De combien de manières différentes est-ce qu'on peut choisir 6 nombres différents dans les 45 premiers nombres naturels? Ici, il s'agit d'une question typique concernant le nombre des combinaisons* $C(6, 45)$. *Celle-ci est égale à:*

$$\frac{45!}{6! \cdot (45-6)!} = \frac{45!}{6! \cdot (39)!} = 8145060 \approx 8.14506\,10^6$$

Binomialkoeffizienten — Coéfficients binomiaux

Multipliziert man das Binom $(a+b)^n = \overbrace{(a+b) \cdot (a+b) \cdot \ldots \cdot (a+b)}^{n \text{ Faktoren}}$ nach den Regeln des Distributivgesetzes aus, so entstehen lauter Summanden der Form $m_k \cdot a^k \cdot b^{n-k}$ mit $0 \leq k \leq n$ und $m, k, n \in \mathbf{N}_0$. Beim Ausmultiplizieren nimmt man der Reihe nach aus jedem Faktor $(a+b)$ einen der Summanden a oder b und multipliziert diese Faktoren zu einem Produkt $a^k \cdot b^{n-k}$. Falls man in jedem Summanden a und nie b nimmt, entsteht $a^n \cdot b^0$. Falls man in j Summanden a und folglich in $n-j$ Summanden b nimmt, entsteht $a^j \cdot b^{(n-j)}$. Dabei gibt es hier verschiedene Möglichkeiten, das a oder das b auszuwählen: Man kann z.B. im ersten Faktor a, im zweiten b, im dritten wieder a wählen etc., man kann aber auch zuerst b, dann a und dann wieder a wählen etc.. m_k ist die Anzahl der Möglichkeiten, a in genau k Faktoren $(a+b)$ und b in genau $n-k$ Faktoren zu wählen. Es ist dann:
• *Si on multiplie le binôme* $(a+b)^n = \overbrace{(a+b) \cdot (a+b) \cdot \ldots \cdot (a+b)}^{n \text{ facteurs}}$ *d'après les règles de la loi distributive, on n'obtient que des termes additionnels de la forme* $m_k \cdot a^k \cdot b^{n-k}$ *avec* $0 \leq k \leq n$ *et* $m, k, n \in \mathbf{N}_0$. *A la multiplication on prend selon le rang de chaque facteur* $(a+b)$ *un des termes additionnels a ou b et on les multiplie en obtenant un produit* $a^k \cdot b^{n-k}$. *Si on prend dans chaque terme additionel a et jamais b, on obtient* $a^n \cdot b^0$. *Si on prend a dans j termes additionnels et b dans* $n-j$ *termes additionnels, on obtient* $a^j \cdot b^{(n-j)}$. *A cette occasion il existe plusieurs possibilités de choisir le a ou le b. Par exemple on peut choisir a dans le premier facteur, b dans le deuxième facteur, de nouveau a dans le troisième facteur etc., mais on peut aussi choisir d'abord b, après a et alors encore une fois a etc... m_k est le nombre des*

possibilités de choisir a dans exactement k facteurs $(a+b)$ et b dans exactement $n-k$ facteurs. Il vaut donc:

$$(a+b)^n = \sum_{k=0}^{n} m_k \cdot a^k \cdot b^{n-k}$$

Wie gross ist nun m_k? — Hier handelt es sich um ein Auswahlproblem: Auf wieviele Arten kann man aus den n Faktoren $(a+b)$ k Faktoren auswählen und dort jeweils den Anteil a (und folglich in den restlichen $n-k$ Faktoren jeweils den Anteil b) nehmen? Diese Frage ist äquivalent mit der einfacheren Frage: Auf wieviele verschiedene Arten kann man aus n Elementen (Faktoren $(a+b)$) jetzt k Elemente auswählen? Die Antwort ist nun einfach: $m_k = C(k,n)$. m_k hat einen Namen:
• *Quelle est maintenant la grandeur de m_k?– Ici, il s'agit d'un problème de choix: De combien de manières différentes est-ce qu'on peut choisir entre les n facteurs $(a+b)$ k facteurs et y prendre la partie a (et par conséquent prendre dans les $n-k$ facteurs restants chaque fois la partie b)? Cette question est équivalente à la question plus simple: De combien de manières différentes est-ce qu'on peut maintenant choisir entre n éléments (facteurs $(a+b)$) k éléments? La réponse est maintenant très simple: $m_k = C(k,n)$. m_k porte un nom:*

Definition • Définition 19.8 (Binomialkoeffizient: • *Coéfficient binomial:*) : m_k *heisst* **Binomialkoeffizient**. • m_k *s'appelle* **Coéfficient binomial**.

Symbole • Symboles 5 (Binomialkoeffizient: • *Coéfficient binomial:*) $m_k := \binom{n}{k}$

Wir wissen jetzt: • *Nous savons maintenant:*

Satz • Théorème 19.6 (Binomischer Lehrsatz • Théorème binomial:)

$$(a+b)^n = \sum_{k=0}^{n} m_k \cdot a^k \cdot b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k}$$

Binomialkoeffizienten kann man bekanntlich im *Pascalschen Dreieck* ablesen:
• *On peut lire les coéfficients binomiaux dans le triangle de Pascal:*

Pascalsches Dreieck: • Triangle de Pascal:

$n=0\ldots$					1					
$n=1\ldots$				1		1				
$n=2\ldots$			1		2		1			
$n=3\ldots$		1		3		3		1		
$n=4\ldots$	1		4		6		4		1	
etc. $\ldots$					$\ldots$					

Die vertikale Position ist n, die horizontale k. Die Numerierung beginnt jeweils mit 0. So liest man z.B. ab: $\binom{4}{1} = 4$ und $\binom{4}{2} = 6$.
• *La position verticale est n, la position horizontale k. Le numérotage commence chaque fois par 0. Ainsi on peut lire par exemple: $c\binom{4}{1} = 4$ und $\binom{4}{2} = 6$.*
Für die Binomialkoeffizienten kann man mit Hilfe von $\binom{n}{k} = C(k,n) = \frac{n!}{k!\cdot(n-k)!} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{1\cdot2\cdot\ldots\cdot k}$ sowie mit dem Prinzip der vollständigen Induktion[9] leicht die folgenden Gesetze beweisen:
• *Pour les coéfficients binomiaux, on peut prouver à l'aide de $\binom{n}{k} = C(k,n) = \frac{n!}{k!\cdot(n-k)!} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{1\cdot2\cdot\ldots\cdot k}$ ainsi qu'avec le principe de l'induction complète[10] facilement les lois suivantes:*

Satz • Théorème 19.7

[9] Vgl. Zahlenlehre
[10] Voir théorie des nombres

Einige Eigenschaften der Binomialkoeffizienten: • **Quelques qualités des coéfficienta binomiaux:**

1)	$\binom{n}{k}$	$=$	$\binom{n}{n-k}$	*2)*	$\binom{n-1}{k-1}+\binom{n-1}{k}$	$=$	$\binom{n}{k}$
3)	2^n	$=$	$\sum_{k=0}^{n}\binom{n}{k}$	*4)*	$\sum_{k=0}^{r}\binom{p}{k}\cdot\binom{q}{r-k}$	$=$	$\binom{p+q}{r}$
5)	$\sum_{s=0}^{n-1}\binom{k+s}{k}$	$=$	$\binom{n+k}{k+1}$	*6)*	$\sum_{k=0}^{p}\binom{p}{k}^2$	$=$	$\binom{2p}{p}$

Z.B. die Formel $2^n=\sum_{k=0}^{n}\binom{n}{k}$ ergibt sich aus $2^n=(1+1)^n=\sum_{k=0}^{n}\binom{n}{k}\cdot 1^k\cdot 1^{n-k}=\sum_{k=0}^{n}\binom{n}{k}$ mit Hilfe des binomischen Lehrsatzes.
• *Par exemple la formule* $2^n=\sum_{k=0}^{n}\binom{n}{k}$ *est obtenue par* $2^n=(1+1)^n=\sum_{k=0}^{n}\binom{n}{k}\cdot 1^k\cdot 1^{n-k}=\sum_{k=0}^{n}\binom{n}{k}$ *à l'aide du théorème binomial.*

19.3.4 Variation mit Wiederholung — Arrangement avec répétition

Die Formel — La formule

Die *Variation mit Wiederholung* ist auf Seite 154 erklärt worden. Die Formel für die Anzahl Variationen mit Wiederholung hingegen müssen wir noch erarbeiten. Dazu verwenden wir folgendes Symbol:
• *L'arrangement avec répétition a été expliqué à la page 154. La formule pour le nombre d'arrangements avec répétition par contre doit encore être élaborée. Pour cela ous utilisons le symbole suivant:*

Symbole • **Symboles 6** : $\bar{V}(k,n)$
$\bar{V}(k,n)$ = *Anzahl Variationen mit Wiederholung bei einer Auswahl von* k *Elementen aus einem Vorrat mit* n *verschiedenen Elementen, die alle wiederholbar sind.*
• $\bar{V}(k,n)$ = *nombre d'arrangements avec répétition pour un choix de* k *éléments dans une réserve avec* n *éléments différents, qui tous peuvent être répétés.*

Herleitung der Formel: • **Déduction de la formule:**
Wir betrachten die k numerierten Plätze, auf denen die auszuwählenden Elemente anzuordnen sind (vgl. Abb. 19.5 oben links im Bild). Da wir jedes der n Elemente im Vorrat auswählen können, hat man n Möglichkeiten, den 1. Platz zu besetzen. Bei der Auswahl für den 2. Platz hat man aber wieder n Elemente im Vorrat zur Auswahl, da wegen der Wiederholbarkeit wieder jedes Element vorhanden ist und gewählt werden kann: Zu jeder der n Möglichkeiten für den 1. Platz hat man n Möglichkeiten für den 2. Platz, total also jetzt $n\cdot n=n^2$ Möglichkeiten. Genauso geht es für den 3. Platz: Zu jeder der n^2 Möglichkeiten für die Plätze 1 und 2 hat man n Möglichkeiten für den 3. Platz, total also jetzt $n^2\cdot n=n^3$ Möglichkeiten. So fährt man fort: Für die Besetzung der ersten 4 Plätze hat man n^4 Möglichkeiten, für die Besetzung der ersten 5 Plätze n^5 Möglichkeiten und schliesslich für die Besetzung der ersten k Plätze hat man n^k Möglichkeiten. Wir haben somit den Satz:
• *Nous considérons les* k *places numérotés sur lesquelles les éléments à choisir sont ordonnés (voir fig. 19.5 en haut à gauche dans l'image). Comme nous pouvons choisir chacun des* n *éléments dans la réserve, on a* n *possibilités d'occuper la 1ère place. Pour la 2ème place on a de nouveau* n *éléments dans la réserve à disposition pour le choix; à cause de la possibilité de répétition chaque élément existe toujours et peut être choisi: Pour chacune des* n *possibilités pour la 1ère place on a* n *possibilités pour la 2ème place, totalement donc* $n\cdot n=n^2$ *possibilités. Également pour la 3ème place: Pour chacun des* n^2 *possibilités pour les places 1 et 2 on a* n *possibilités pour la 3ème place, totalement donc* $n^2\cdot n=n^3$ *possibilités. On continue ainsi: Pour l'occupation des premières 4 places on a* n^4 *possibilités , pour l'occupation des premières 5 places* n^5 *possibilités et finalement pour l'occupation des premières* k *places on a* n^k *possibilités. Par conséquent nous avons le théorème:*

Satz • **Théorème 19.8 (Variationen mit Wiederholung:** • **Arrangement avec répétitions:)**

$$\bar{V}(k,n)=n^k$$

Beispiel: • Exemple:

Auf wieviele Arten können 26 (unterscheidbare) Studenten sich in 12 verschiedene Kurse einschreiben, wenn jeder Kurs 26 Plätze offen hat, also keine Platzbeschränkung besteht?
• *De combien de possibilités différentes est-ce que 26 étudiants (qu'on peut distinguer) peuvent s'inscrire dans 12 cours différents, si chaque cours offre 26 places, c.à.d. s'il n'y a pas de limites aux places?*

Lösung: • Solution:

Der erste Student hat 12 Möglichkeiten, sich in einen Kurs einzuschreiben. Zu jeder dieser Möglichkeiten des ersten Studenten hat der zweite auch 12 Möglichkeiten, sich in einen Kurs einzuschreiben. Beide zusammen haben also 12^2 Möglichkeiten. Für den dritten, vierten etc. Studenten geht das auch so: Jeder hat die 12 Möglichkeiten, und die Möglichkeiten multiplizieren sich. Es handelt sich um eine Variation mit Wiederholung. Total gibt es $\bar{V}(k,n) = \bar{V}(26,12) = 12^{26} = 1144754599728828155521558 1184 \approx 1.14475\,10^{28}$ Möglichkeiten.
• *Le premier étudiant a 12 possibilités de s'inscrire dans un cours. Pour chacune de ces possibilités du premier étudiant le deuxième a aussi 12 possibilités de s'inscrire dans un cours. Les deux ensemble ont* 12^2 *possibilités. Pour le troisième, quatrième etc. étudiant ça fonctionne aussi d'après le même schéma: Chacun a les 12 possibilités, et les possibilités se multiplient. Il s'agit d'un arrangement avec répétitions. Totalement il y a* $\bar{V}(k,n) = \bar{V}(26,12) = 12^{26} = 1144754599728828155521558 1184 \approx 1.14475\,10^{28}$ *possibilités.*

Merke: Aus diesem Beispiel ersieht man, dass $k > n$ sein kann.
• **A retenir:** *Par cet exemple, on voit que k peut être plus grand que n: k > n.*

Anwendung: Die Mächtigkeit der Potenzmenge — Application: Puissance de l'ensemble de parties

Die Potenzmenge ist bekanntlich die Menge aller Teilmengen.
• *L'ensemble de parties est comme chacun sait l'ensemble de tous les sous-ensembles.*

Problem • Problème 19.5
Mächtigkeit der Potenzmenge: • La puissance de l'ensemble de parties
Gegeben: • Donné: *Eine Menge $\mathcal{M}$ mit n Elementen.*
• *Un ensemble $\mathcal{M}$ à n éléments.*
Frage: • Question: *Wieviele Teilmengen hat $\mathcal{M}$?*
• *Combien d'ensembles partiels $\mathcal{M}$ a–t–il?*

Lösung: • Solution:

$\binom{n}{k} = C(k,n)$ ist bekanntlich die Anzahl Teilmengen mit k Elementen, denn hier handelt es sich ja um das typische Auswahlproblem. Nun kann man eine oder mehrere Teilmengen mit 0 (leere Menge), 1, 2, ..., n Elemente wählen. Total hat man also:
• $\binom{n}{k} = C(k,n)$ *est comme chacun sait le sous-ensembles avec k éléments, car ici, il s'agit d'un problème de choix typique. Maintenant on peut choisir un ou plusieurs sous-ensembles avec 0 (quantité vide), 1, 2, ..., n éléments. Totalement on a donc:*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} \cdot 1^k \cdot 1^{n-k} = (1+1)^n = 2^n.$$

Satz • Théorème 19.9 *:*
Mächtigkeit der Potenzmenge: • Puissance de l'ensemble de parties
Die Potenzmenge einer Menge mit n Elementen hat 2^n *Elemente.*
• *L'ensemble de parties d'un ensemble qui contient n éléments possède* 2^n *éléments.*

Eine Menge mit n Elementen hat also genau 2^n Teilmengen.
• *Donc un ensemble avec n éléments contient exactement* 2^n *sous-ensembles.*

19.3.5 Kombination mit Wiederholung — Combinaison avec répétition

Hier sollen aus einer Menge mit n Elementen k Elemente ausgewählt werden, wobei jedes ausgewählte Element bei der Auswahl in der Menge dupliziert wird resp. nachgeliefert wird, so dass die Menge trotz Auswahl immer aus denselben Elementen besteht. Wie gross ist die Anzahl Auswahlmöglichkeiten?
• *Ici il faut choisir k éléments dans un ensemble avec n éléments. Chaque élément choisi se duplique dans l'ensemble de façon que l'ensemble reste toujours le même malgré le choix. Quel est le nombre des options quant au choix?*

Für die Berechnung dieser Anzahl ist es unwesentlich, ob die Menge $\mathcal{M}_n$ aus Kugeln, Losen oder Zahlen etc. besteht, d.h. welcher Natur die Elemente sind. Wir dürfen daher annehmen, es handle sich um die natürlichen Zahlen von 1 bis n: $\mathcal{M}_n = \{1, 2, 3, \ldots, n\}$. Wenn wir jetzt k Elemente (d.h. Zahlen) auswählen, so wollen wir diese immer ihrer Grösse nach aufreihen, statt sie bloss „auf einen Haufen zu legen". Wir reden hier von der *Standardanordnung*. Eine solche Auswahl $\{e_1, e_2, \ldots, e_k\}$ wird also immer in der Anordnung $e_1 \leq e_2 \leq \ldots \leq e_k$ präsentiert. Dadurch wird die Anzahl der Auswahlmöglichkeiten ja nicht verändert.
• *Pour le calcul de ce nombre, il n'est pas essentiel si l'ensemble $\mathcal{M}_n$ consiste en boules, en billets de lotterie ou en nombres, c.-à.-d. quelle est la nature des éléments. Nous pouvons supposer par conséquent qu'il s'agit de nombres naturels de 1 jusqu'à n: $\mathcal{M}_n = \{1, 2, 3, \ldots, n\}$. Si nous choisissons maintenant k éléments (c.-à.-d. des nombres), nous voulons les ranger l'un à côté de l'autre au lieu de les "mettre sur un tas". Nous parlons ici du rangement standard (configuration). Nous presentons donc un tel choix $\{e_1, e_2, \ldots, e_k\}$ toujours dans une disposition $e_1 \leq e_2 \leq \ldots \leq e_k$. Par cela le nombre des options ne change pas.*

Wie ist nun dem Problem der Wiederholungen beizukommen? Die Idee, aus $k \cdot n$ Elementen auszuwählen, führt zu keinem Resultat, da die Elemente einer Auswahlmenge dann auf verschiedene Weise gewonnen werden können, was fälschlicherweise die Anzahl Auswahlmöglichkeiten erhöht. So geht es also nicht. Um der Sache beizukommen, muss man etwas weiter ausholen:
• *Comment résoudre le problème des répétitions? L'idée de choisir parmi $k \cdot n$ éléments ne mène à aucun résultat parce que les éléments d'un ensemble de choix peuvent être obtenus de façon différente ce qui augmente faussement le nombre des possibilités de chois. Donc ça ne va pas de cette manière. Pour venir à bout de la chose on doit aller chercher plus loin:*

Wir führen dazu $k-1$ neue Elemente $J_1, J_2, \ldots, J_{k-1}$ ein und fügen diese der Menge $\mathcal{M}_n$ an. So erhalten wir eine neue Menge $\mathcal{M}_n^{k-1} = \{1, 2, 3, \ldots, n, J_1, J_2, \ldots, J_{k-1}\}$ mit $n + k - 1$ Elementen. Die neu gültige Standardanordnung entspreche der hier gegebenen Aufzählung der Elemente: Die J_i werden hinten den Nummern nach angefügt. Dabei gelte für die Elemente J_i die folgende Interpretation: J_i ist eine Vorschrift oder Funktion, die auf jenen ausgewählten Standardanordnungen operiert, in denen sie selbst allenfalls vorkommt. Die durch J_i gegebene Vorschrift lautet: Ersetze das Symbol J_i in einer ausgewählten Standardanordnung durch das Element e_i derselben Auswahl, nachdem alle J_p mit $p < i$ schon ersetzt sind. Führt man alle diese Ersetzungen durch, so erhält man aus einer *primären Auswahl* die *Endstandardanordnung*. Da k Elemente auszuwählen sind, es aber nur $k-1$ Elemente J_i gibt, kommt in einer Standardauswahl immer mindestens ein Element $e_j \in \mathcal{M}_n$ vor, in unserem Falle eine der gegebenen natürlichen Zahlen $1, 2, 3, \ldots, n$. J_i bewirkt somit immer eine Ersetzung durch ein weiter vorne vorkommendes Element in der Standardanordnung, also eine Duplikation. Da so jedes Element einmal ausgewählt und dann noch durch die J_i maximal $k-1$ mal dupliziert werden kann, besteht die Möglichkeit, dass jedes Element von $\mathcal{M}_n$ dann k mal in der Endstandardanordnung vorkommen kann. Auf diese Art können alle Kombinationen mit Wiederholung gewonnen werden.
• *A cette intention nous introduisons $k-1$ nouveaux éléments $J_1, J_2, \ldots, J_{k-1}$, les incluons dans l'ensemble $\mathcal{M}_n$. Ainsi nous recevons un nouveau ensemble $\mathcal{M}_n^{k-1} = \{1, 2, 3, \ldots, n, J_1, J_2, \ldots, J_{k-1}\}$ à $n+k-1$ éléments. La disposition standard nouvellement valable correspond à l'énumération des éléments donnée ici: Les J_i sont ajoutés derrière d'après les numéros. Pour les éléments J_i l'interprétation suivante est valable: J_i est une prescription ou fonction qui opère sur les dispositions standard choisies,*

dans lesquelles on les trouve elles–mêmes. La prescription donnée par J_i dit: Remplacer le symbole J_i dans une disposition standard choisie par l'élément e_i du même choix après avoir remplacé tous les J_p par $p < i$. Si on effectue tous ces remplacements, on obtient d'un choix primaire la disposition finale standard. Comme il faut choisir k éléments et comme il n'existent que $k-1$ éléments J_i, dans un choix standard on trouve toujours au moins un élément $e_j \in \mathcal{M}_n$, dans notre cas un des nombres naturels $1, 2, 3, \ldots, n$. J_i effectue par conséquent toujours un remplacement par un élément qui es situé plus à l'avant dans la disposition standard, donc une duplicata. Comme chaque élément peut être choisi une fois ainsi et après peut être dupliqué par un J_i au maximum $k-1$ fois, il existe la possibilité que chaque élément de $\mathcal{M}_n$ peut se trouver donc k fois dans la disposition standard finale. De cette façon peuvent être obtenues toutes les combinaisons avec répétition.

Beispiel: • Exemple:

Gegeben sei $\mathcal{M}_7 = \{1, 2, 3, \ldots, 7\}$. Daraus sollen 5 Elemente mit Wiederholung ausgewählt werden. Es ist dann $\mathcal{M}_7^{5-1} = \mathcal{M}_7^4 = \{1, 2, 3, \ldots, 7, J_1, J_2, J_3, J_4\}$.
• *Soit donné $\mathcal{M}_7 = \{1, 2, 3, \ldots, 7\}$. Dans cet ensemble il faut choisir 5 éléments avec répétitions. Il vaut donc: $\mathcal{M}_7^{5-1} = \mathcal{M}_7^4 = \{1, 2, 3, \ldots, 7, J_1, J_2, J_3, J_4\}$.*

Wählt man z.B. $(1, 5, 7, J_1, J_4)$ (in Standardanordnung), so wird wie folgt ersetzt: Zuerst $J_1 \mapsto 1$ (der Index 1 ist kleiner als der Index 4). Das ergibt $(1, 5, 7, 1, J_4)$ in Nicht–Standardanordnung und $(1, 1, 5, 7, J_4)$ in neuer Standardanordnung. Dann wird ersetzt $J_4 \mapsto 7$, was zur Standardanordnung $(1, 1, 5, 7, 7)$ führt.
• *Si on choisit par exemple $(1, 5, 7, J_1, J_4)$ (dans la disposition standard), il faut remplacer comme suit: D'abord $J_1 \mapsto 1$ (l'indice 1 est plus petit que l'indice 4). Ça donne $(1, 5, 7, 1, J_4)$ dans la disposition non–standard et $(1, 1, 5, 7, J_4)$ dans la nouvelle disposition standard. Alors on remplace $J_4 \mapsto 7$ ce qui mène à la disposition standard $(1, 1, 5, 7, 7)$.*

Ähnlich führt die Auswahl $(4, J_1, J_2, J_3, J_4)$ nach allen Ersetzungen zur Standardanordnung $(4, 4, 4, 4, 4)$.
• *Semblablement le choix $(4, J_1, J_2, J_3, J_4)$ mène à la disposition standard $(4, 4, 4, 4, 4)$ après tous les remplacements.*

Bei der Auswahl von 6 Elementen aus $\mathcal{M}_8$ führt die primäre Auswahl $(2, 3, 7, 8, J_2, J_4)$ auf die Endstandardanordnung $(2, 3, 3, 7, 7, 8)$.
• *Au choix de 6 éléments dans $\mathcal{M}_8$ le choix primaire mène à la disposition standard finale $(2, 3, 7, 8, J_2, J_4)$.*

Diese Beispiele machen klar, dass eine primäre Auswahl eindeutig einer Endstandardanordnung entspricht. Die Anzahl der auswählbaren primären Anordnungen ist gleich der Anzahl der Endstandardanordnungen, in welchen alle Elemente bis zu k mal wiederholt vorkommen können. Um $\bar{C}(k, n)$ zu finden, muss man also die Anzahl der primär auswählbaren Standardanordnungen bestimmen. Dort werden k Elemente aus den $n + k - 1$ Elementen $1, 2, 3, \ldots, n, J_1, J_2, \ldots, J_{k-1}$ ausgewählt. Daher ist $\bar{C}(k, n) = C(k, n + k - 1)$. Somit hat man:
• *Ces exemples montrent qu'un choix primaire correspond clairement à une disposition standard finale. Le nombre des dispositions primaires et sélectionnables est égal au nombre des dispositions standard finales, dans lesquelles tous les éléments figurent répétés jusqu' à k fois. Pour trouver $\bar{C}(k, n)$, on doit donc trouver le nombre des dispositions standard primaires sélectionnables. Là, k éléments sont choisis entre $n+k-1$ éléments $1, 2, 3, \ldots, n, J_1, J_2, \ldots, J_{k-1}$. Par conséquent on trouve $\bar{C}(k, n) = C(k, n+k-1)$. On a donc:*

Satz • Théorème 19.10
Kombinationen mit Wiederholung: • Combinaisons avec répétitions:

$$\bar{C}(k,n) = C(k, n+k-1) = \binom{n+k-1}{k}$$

Beispiel: • **Exemple**

Ein Abteilungsleiter hat 19 Ingenieure unter sich, von denen jeder als Projektleiter in Frage kommt. Es stehen 8 neue Projekte an, die wahrscheinlich nacheinander bearbeitet werden müssen. Wieviele Möglichkeiten bieten sich dem Abteilungsleiter, Projektleiter zu bestimmen, wenn auch in Betracht gezogen werden darf, dass im Extremfall derselbe Ingenieur allen 8 Projekten vorsteht?

• *Un chef de rayon dirige 19 ingénieurs desquels chacun est capable d'avoir la responsabilité pour un projet. 8 nouveaux projets sont à faire (en suspens), qui doivent être traités vraisemblablement l'un après l'autre. Combien de possibilités s'offrent au chef de rayon de nommer des responsables pour les projets, si on peut tirer en considération dans le cas extrême, que le même ingénieur assume (dirige) tous les 8 projets?*

Hier handelt es sich um eine Kombination mit Wiederholung. Aus 19 Ingenieuren werden 8 Projektleiter ausgewählt, wobei jeder mehrmals vorkommen darf. Es ist dann:

• *Ici, il s'agit d'une combinaison avec répétitions. Dans un ensemble de 19 ingénieurs, 8 responsables sont choisis de façon que chacun peut être nommé plusieurs fois. Il est donc:*

$$\bar{C}(8,19) = \binom{19+8-1}{8} = \binom{26}{8} = \frac{26!}{8! \cdot (26-8)!} = \frac{26!}{8! \cdot 18!} = 1562275 \approx 1.56228\,10^6.$$

19.4 Übungen — Exercices

Übungen finden sich in *DIYMU*, (Bibl.: wirz1) sowie in der klassischen Schulbuchliteratur für die Gymnasialstufe — oder speziell auch in der Literatur zur Wahrscheinlichkeitsrechnung und Statistik.

• *On trouve des exercices dans DIYMU, (Bibl.: wirz1) ainsi que dans la littérature scolaire classique pour le niveau gymnasial ou spécialement aussi dans les manuels du calcul des probabilités et statistiques.*

Kapitel • Chapitre 20

Kryptologie – Cryptologie

Bemerkung: • Remarque: In diesem Kapitel wird auf Material aus dem Algebra-Skript zurückgegriffen: *http : //rowicus.ch/Wir/Scripts/KAlgGdf.pdf*

• *Ici, il y a pour le moment seulement le texte allemand à disposition. La traduction française manque.*

20.1 Public key, RSA-Verfahren

Das hier besprochene **RSA-Verfahren** ist ein „public key –Chiffrierverfahren“, das durch seine relative Einfachheit besticht. Man benennt es nach den Erfindern Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**dleman.

Zuerst wollen wir den Begriff **„public key –Chiffrierverfahren“** verstehen lernen. Generell hat man beim Chiffrieren die Absicht, eine unterwegs geheim zu haltende Nachricht von einer Stelle oder Person A an eine Stelle oder zu einer Person B zu übermitteln, ohne dass die Nachricht unterwegs von einer dritten Stelle oder Person verstanden werden kann. Ein ursprünglicher Klartext wird dazu chiffriert oder verschlüsselt, dann übermittelt, dann wieder dechiffriert oder entschlüsselt. Danach muss der ursprüngliche Klartext wieder in seiner alten Form vorhanden sein.

Im hier besprochenen Falle dient zur Verschlüsselung und Entschlüsselung ein **kryptologischer Algorithmus**, welcher durch eine offen bekannte mathematische Funktion gegeben ist. Um die Geheimhaltung des chiffrierten Textes „einigermassen sicher“ zu machen, benützt man **Schlüssel**, hier in Form von Zahlenwerten, welche beim Chiffrieren und Dechiffrieren entscheident sind. Alleine den Sendern und Empfängern muss der Schlüssel bekannt sein. Man kann es auch so einrichten, dass es einen **Chiffrierschlüssel** gibt und einen andern, aus dem Chiffrierschlüssel berechenbaren **Dechiffrierschlüssel**. In dieser Situation ist es sogar möglich, den Chiffrierschlüssel **öffentlich** zu machen, wenn die Zeit zur Berechnung des Dechiffrierschlüssels aus dem Chiffrierschlüssel auch mit dem schnellsten Computer alle realen Möglichkeiten übersteigt. Die Idee dazu stammt aus den Jahrn um 1970 (Ellis, Cocks und Williamson) und später 1977 (Diffie-Hellman). Beim RSA–Verfahren benützt man an dieser Stelle die Tatsache, dass allgemein der Rechenaufwand zur exakten Faktorisierung sehr grosser Zahlen extrem gross ist.

20.2 Durchführung des RSA–Verfahrens — Exécution de la méthode RSA

(Vgl. auch: http://de.wikipedia.org/wiki/RSA-Kryptosystem)

20.2.1 Wahl der Primzahlen — Choisir les nombres premiers

Das RSA–Verfahren basiert auf zwei vorerst gewählten grossen Primzahlen p und q, $p \neq q$ mit einer sehr grossen Anzahl von Dezimalziffern. p und q sollten stochastisch unabhängig sein. (Momentan wird je eine Anzahl von über 150 Ziffern empfohlen.) Diese beiden Primzahlen müssen strikte geheim gehalten werden. Mühelos können wir mit Hilfe eines Computers (z.B. mit *Mathematica*) das Produkt $N = p \cdot q$ berechnen. Die Faktorisierung dieses Produktes mit über 300 Ziffern ist ohne Vorwissen mit unrealistisch grossem Aufwand verbunden.

Bsp.: • **Exemple:** $1111\ldots111 * 222222\ldots222$ (je 160 Ziffern) ergibt die Ziffern:
2469135802469135802469135802469135802469135802469135802469135802469135802469135
5802469135802469135802469135802469135802469135802469135802469135802469135802469
9135308641975308641975308641975308641975308641975308641975308641975308641975308
8641975308641975308641975308641975308641975308641975308641975308641975308641975
5308642 mit einer Rechenzeit $t < 0.000001$ Sekunden.

Praktisch kann man diese Primzahlen p und q durch Raten einer Zahl und danach Anwenden eines Primzahltests bestimmen.

20.2.2 Bestimmung der beiden Schlüssel — Callculer des deux clefs

1. Wir berechnen jetzt $\varphi(N) = \varphi(p \cdot q) = (p-1)(q-1)$, wobei φ die Eulersche φ–Funktion bedeutet.
2. Wir wählen dann eine Zahl e (e gross) mit $1 < e < \varphi(N)$, $e \not| \varphi(N)$.
3. Dann berechnen wir mit Hilfe des euklidschen Algorithmus (ev. erweiterteter Algorithmus) eine Zahl d so, dass das Produkt $d \cdot e$ kongruent 1 modulo $\varphi(N)$ ist: $d \cdot e \equiv 1\ (\varphi(N))$. ($d$ ist damit ein „Inverses“ zu e.)
   Vgl. dazu auch: *http://de.wikipedia.org/wiki/Erweiterter_euklidischer_Algorithmus* .
   Natürlich kann man auch d wählen und damit e wie oben berechnen.
4. Der **öffentliche Schlüssel** *(public key)* besteht jetzt aus dem Primzahlprodukt N sowie dem **öffentlichen Exponenten** e.
5. Der **private Schlüssel** *(private key)* besteht aus dem **privaten Exponenten** d. Dieser darf nur dem Anwender bekannt sein.
6. Eine Firma kann nun so für einen gegebenen Kunden zu einem gewählten Paar p und q schliesslich N sowie d und e bestimmen. N und e können ungesichert aufbewahrt werden. e hingegen muss dem Kunden überlassen werden.

Ein oft gezeigtes Beispiel:

Seien $p = 11$ und $q = 13$ die beiden Primzahlen. (Diese sind aus Gründen der praktischen Nachvollziehbarkeit hier klein statt gross gewählt.) Das Produkt wird damit $N = p\,q = 143$. Damit wird $\varphi(N) = (p-1)(q-1) = 10 \cdot 12 = 120$. Nun muss gelten: $ggT'pgdc(e, 120) = 1$. Sei nun z.B. $e = 23$ gewählt. $\rightsquigarrow$ Öffentlicher Schlüssel $(N, e) = (120, 23)$. Nun müssen wir d berechnen: $d \cdot e \equiv 1\ (\varphi(N)) \Rightarrow \exists_k\ d \cdot e + k \cdot \varphi(N) = 1$, $d = \dfrac{1 - k \cdot \varphi(N)}{e} = \dfrac{1 - k \cdot 120}{23}$. Mit $k = -9$ finden wir $d = 47 \in \mathbb{N}$. Bei grossen Zahlen N und e bringt die Ratemethode hier nicht unbedingt Erfolg. Der erweiterte euklidsche Algorithmus führt dann weiter.

Bemerkenswert ist, dass für das weitere Prozedere die beiden Primzahlen p und q nicht mehr gebraucht werden, also vergessen werden können. Sie müssen jedoch auch weiterhin geheim bleiben.

20.2.3 Verschlüsselung (Codierung) — Chiffrement (codage)

Wir gehen hier als Beispiel davon aus, dass es sich bei einer angenommenen geheim zu übermittelnden Nachrichtum um einen Text mit Buchstagen und Zahlen handelt und dass wir jedes verwendete Zeichen im ASCII-Code darstellen können. In diesem Code sind 33 nicht–druckbare sowie die 95 druckbaren Zeichen definiert, beginnend mit dem Leerzeichen, total also 128 Zeichen. Damit genügt für jedes Zeichen eine natürliche Dezimalzahl mit maximal drei Stellen. Sei K ein solches Zeichen einer Nachricht und C seine Verschlüsselung. Um ein Zeichen K zu verschlüsseln, ist jetzt hier die Bedingung $K < 143$ erfüllt.
Die Zahl $K = 7$ verschlüsseln wir daher wie folgt:
$N = 143,\ \ e = 23,\ \ C = K^e\ (mod\ N) = 7^{23}\ (mod\ 143) \equiv (((7^2)^2)^2)^2 * (7^2)^2 * 7^2 * 7\ (mod\ 143) \equiv 2\ (mod\ 143)$
(Sukzessive Berechnung der Restklassen). Schneller ist man mit dem *Mathematica*–Befehl $Mod[7^{23}, 143]$.
Somit ist $C = 2$ zu übermittlen.
Will man hier eine Nachricht in Form einer ASCII–Sequenz übermitteln, die durch eine natüliche Zahl ≥ 143 darstellt werden kann, so kann man die Sequenz in gleichlange Blöcke aufteilen, welche jeder für sich eine Zahl < 143 darstellt. Dann wird eben eine Folge von Teilnachrichten K_i (Teilklartexten) verschlüsselt. Damit erhält man dann eine Folge von chiffrierten Blöcken C_i, welche zu übermitteln sind.

20.2.4 Entschlüsselung (Decodierung) — Décodage (déchiffrement)

Die Decodierung auf der andern Seite funktioniert nach der Formel $K \equiv C^d\ (mod\ N)$. Das ist hier der zentrale theoretische Punkt und daher überprüfungsbedürfdig.

Beweis: • Preuve:

Statt $u \equiv v\ mod\ N$ schreiben wir einfacher und kürzer mit Hilfe der Restklassenschreibweise

$$[u]_N = [v]_N,\ \text{ kurz } [u] = [v].$$

Sei vorerst $[C^d]_N = [K']_N$. $\Rightarrow\ [K']_N = [C^d]_N = [(K^e)^d]_N = [K^{e\cdot d}]_N = [K]_N^{e\cdot d}$.

Es gilt: $N = p \cdot q\ \wedge\ \varphi(N) = \varphi(p \cdot q) = (p-1)(q-1)\ \wedge\ d \cdot e = 1 + m \cdot \varphi(N)$
$\Rightarrow\ [d \cdot e]_{(p-1)(q-1)} = [1]_{(p-1)(q-1)}\ \Rightarrow\ \exists_{u\in\mathbb{Z}} :\ d \cdot e = 1 + u\,(p-1)(q-1)$

Wir unterscheiden nun zwei Fälle:

1. $p|\,K$

   $\rightsquigarrow\ [K]_p = [0]_p\ \Rightarrow\ [K']_p = [K^{e\cdot d}]_p = [0]_p\ \Rightarrow\ [K]_p = [K']_p$

2. $q|\,K$

   $\rightsquigarrow$ Herleitung wie eben gehabt: $\ldots\ \Rightarrow\ [K]_q = [K']_q$

3. $p \not| K,\ \ q \not| K$

   Hier gilt nach dem kleinen Fermatschen Satz: $[K^{p-1}]_p = [1]_p\ \wedge\ [K^{q-1}]_q = [1]_q$

   $\rightsquigarrow\ [K^{e\cdot d}]_p = [K^{1+u\,(p-1)(q-1)}]_p = [K \cdot K^{u\,(p-1)(q-1)}]_p = [K]_p \cdot [(K^{u\,(q-1)})^{(p-1)}]_p = [K]_p \cdot [1]_p = [K]_p$

   $\rightsquigarrow\ [K']_p = [K^{e\cdot d}]_p = [K]_p$

4. Ebenso mit q statt mit p: $[K']_q = [K^{e\cdot d}]_q = [K]_q$
5. $\leadsto\ [K^{e\cdot d} - K]_p = [0]_p\ \wedge\ [K^{e\cdot d} - K]_q = [0]_q\ \Rightarrow\ [K^{e\cdot d} - K]_{p\cdot q} = [K^{e\cdot d}]_{p\cdot q} - [K]_{p\cdot q} = [0]_{p\cdot q}$

$$\leadsto\ K^{e\cdot d} \equiv K\ (mod\ (p \cdot q = N))$$

20.2.5 Das Sicherheitsproblem — Le problème de la sécurité

N ist bei diesem Verfahren bekannt, jedoch p und q nicht. Daher lautet die Frage, was wohl die Chance ist, die beiden Faktoren p und q von N zu finden. Damit könnte man dann via $\varphi(N)$ und dem öffentlichen Schlüssel (N, e) den geheimen Schlüssel d berechnen und damit eine Botschaft dechiffrieren, falls dafür der Geheimtext gegeben ist.

Bekannt ist (Jahr 2006), dass die wachsende Rechenleistung moderner Computer nur eine kurzfristige Sicherheit bedingt. Mit dem schnellen Algorithmus des **quadratischen Siebs** sind bereits Zahlen mit über 100 Stellen faktorisiert worden. Eine weitere Methode der Faktorisierung benutzt **elliptische Kurven**, ist aber für Zahlen mit über ca. 50 Stellen untauglich. Mit der **Methode des Zahlkörpersiebs** ist im Jahre 2005 von Wissenschaftlern der Universität Bonn eine im Rahmen der „RSA Factorization Challenge“ von RSA Laboratories vorgegebene 200-stellige Dezimalzahl in ihre zwei (großen) Primfaktoren zerlegt worden — mit einer Rechenzeit von ca. eineinhalb Jahren. Erreichbar scheint heute die Faktorisierung einer Zahl mit 640 Bits (bzw. 193 Dezimalstellen). Heute üblicher RSA-Schlüssel benutzen dagegen mindestens 300 Dezimalstellen für N.

Vgl. auch $http://de.wikipedia.org/wiki/Elliptische\_Kurve$,
$http://de.wikipedia.org/wiki/Quadratisches\_Sieb$,
$http://de.wikipedia.org/wiki/Zahlkörpersieb$.

20.2.6 Hinweise — Indications

1. Allgemeine Hinweise: Vgl. z.B. $http://de.wikipedia.org/wiki/RSA-Kryptosystem$.
2. Hinweise zur aktuellen Situation sind auch auf dem Internet zu finden, z.B. auf der Home-page von RSA-Laboratories: http://www.rsasecurity.com/
3. Bisher oft empfohlene Sicherheitsparameter waren:
   Allgemein: Zahlen N mit $3 \cdot 256 = 768$ Bits ($\approx 1.5525 \cdot 10^{231}$)
   Firmen: Zahlen N mit $4 \cdot 256 = 1024$ Bits ($\approx 1.79769 \cdot 10^{308}$)
   Hochsicherheit: Zahlen N mit $8 \cdot 256 = 2048$ Bits ($\approx 3.2317 \cdot 10^{616}$).
4. Für das Problem der Angriffe gegen das RSA–Verfahren vgl. die Spezialliteratur.
5. Ein weiteres Problem: Die Erzeugung von Primzahlen. Z.B. stellt sich die Frage: Wieviele Primzahlen mit 308 Dezimalstellen mag es geben: $A(308)$? Zur Abschätzug benutzen wir die Formel der asymptotische Dichte der Primzahlen: $\lim\limits_{x\to\infty} \frac{\pi(x)}{(\frac{x}{ln(x)})} = 1\ \Rightarrow\ \pi(x) \approx \frac{x}{ln(x)}$
   $\Rightarrow\ A(308) \approx \pi(10^{309}) - \pi(10^{309}) \approx \frac{10^{309}}{ln(10^{309})} - \frac{10^{308}}{ln(10^{308})} \approx 1.264479 \cdot 10^{306}$. Vorratsprobleme wird es damit also kaum geben. Zur praktischen Erzeugung von Primzahlen konsultiere man die Spezialliteratur.
6. Das heute sehr aktuelle Problem der digitalen Unterschrift kann hier nur am Rande gestreift werden. Es geht in dieser Sache nicht bloss um die Übermittlung eines geheimen Textes, sondern um die Identifizierung des andern, d.h. um die Verifizierung der Identität. Auch hier konsultiere man die Spezialliteratur.
   Vgl z.B. $http://de.wikipedia.org/wiki/Digitale\_Unterschrift$.

Kapitel • Chapitre 21

Graphentheorie – Théorie des graphes

Bemerkung: • Remarque: Auch in diesem Kapitel wird auf Material aus dem Algebra-Skript zurückgegriffen: *http : //rowicus.ch/Wir/Scripts/KAlgGdf.pdf*

• *Ici, il y a pour le moment seulement le texte allemand à disposition. Momentanément, la traduction française manque encore.*

21.1 Grundlagen

21.1.1 Motivation

Die Graphentheorie behandelt die Information über Verbindungen zwischen gegebenen Punkten, welche man sich als geometrische Punkte denken kann. So entsteht eine mathematische Theorie über die Struktur solcher Verbindungen. Anwendungen ergeben sich vielfältig. Beispiele:

- Eisenbahnnetze zwischen verschiedenen Städten.
- Strassennetze zwischen verschiedenen Orten.
- Rechnernetze, z.B. „Ringstrukturen“, „Hierarchiestrukturen“, „Sternstrukturen“.
- Datenstrukturen, z.B. „Baumstrukturen“.
- Strukturen in Betriebssystemen.
- Computergraphik.

Vgl. auch *http : //de.wikipedia.org/wiki/Graphentheorie*

Historisch war der Ausgangspunkt der Graphentheorie das „Königsberger Brückenproblem“ (Euler, vgl. nebenstehende Skizze; die Punkte stellen öffentliche Plätze dar, die Vergindungslinien dazwischen symbolisieren Brücken zwischen den Plätzen).
Wir sehen hier 4 Plätze, die man über total 7 Brücken erreichen kann. Das Problem ist nun herauszufinden, ob es eine Rundgang gibt, auf dem man an allen Plätzen vorbeikommt und bei dem man jede Brücke nur einmal nehmen muss.
Um dieses Problem lösen zu können ist es ratsam, sich dafür erst ein Begriffssystem sowie etwas Theorie aufzubauen. Dazu gehen wir von von der Realität abstrahierten Figuren wie der nebenstehenden aus, welche wir **Graphen** nennen.

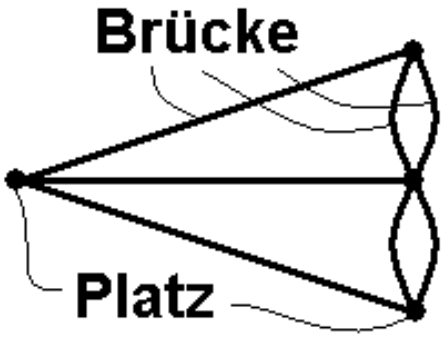


Abb. 1: Brückenproblem, abstrakt

Zurerst müssen wir den neuen Begriff **Graph** mathematisch so exakt zu definieren, dass wir damit vernünftig arbeiten können. Ein Graph wie der eben Angetroffene haben, besteht aus **Ecken** (das waren vorhin die Plätze, welche die Ecken der skizzierten Figur bildeten) und aus **Kanten** (das waren vorhin die Wege über die Brücken, welche in der skizzierten Figur als Linien dargestellt sind). Dabei gehen wir vorläufig von planaren Skizzen aus, in welchen es Punkte und dazwischen vielleicht Verbindungslinien gibt, welche auch gerichtet (Pfeile) sein können. Weitere notwendige Elemente werden wir bei Bedarf definieren.

Bemerkung: Die Struktur dieses Kapitels die in Anlehnung an die empfehlenswerte Literatur von *Manfred Brill* (Bibl.: brill) gewählt worden.

21.1.2 Ungerichtete Graphen, Begriffe, Beispiele, Beziehungen

Sei nun **gegeben**: $E = \{\text{Ecken, Knoten, Punkte oder Endpunkte}\}$,
$K = \{\text{Kanten, Bögen oder Sehnen}\} \subseteq E \times E$. $|E|$ und K seien endlich, wenn nicht anders verlangt.

Für die Ecken schreiben wir hier mit Kleinbuchstaben, z.B. u oder v. Daraus setzen wir die Bezeichnung für die Kanten zusammen: $\{u, v\}$ resp. kurz uv sei die Kante (auch Sehne, Linie oder Strecke) zwischen den Ecken u und v. $\{p_1, p_2\}$ ist damit die Kante zwischen den Ecken p_1 und p_2. Damit gilt: $uv \in K$, $p_1p_2 \in K$, $K =$ Menge der Kanten. Statt p_1p_2 schreiben wir auch kurz $p_{1,2}$.

Bemerkung: In einer Skizze für einen Graphen muss es daher nach dieser Art des Begriffsaufbaus zu einer Kante immer zwei Ecke geben, welche auch zusammenfalle dürfen. Zu zwei Ecken hingegen muss es nicht zwingend Kanten geben. Eine Ecke darf auch isoliert sein.

Definitionen:

Eine Menge derartiger Ecken (Punkte) und Kanten (Sehnen, Verbindungen zwischen den Punkten) nennen wir **Graphen** G: $G = (E, K) = G(E, K)$. Statt Graph sagen wir in diesem Fall auch **ungerichteter Graph**. Speziell:

Ein **einfacher Graph** ist ein Graph ohne besondere Strukturelemente wie Mehrfachkanten (parallele Kanten), orientierte Kanten, Schleifen, Knoten– oder Kantengewichte, Färbungen, Markierungen u.s.w..

Sei nun $E' \subseteq E$, $K' \subseteq K$, sodass (E', K') wieder ein gültiger Graph ist. Dann heisst $G' = G'(E', K')$ **Teilgraph** oder **Untergraph** von $G = G(E, K)$.

Weiter sei $u \in E$. Dann heisst eine Kante uu jetzt **Schlinge**.

Nun seien die Ecken u, v gegeben. Falls es dazu zwei verschiedene Kanten uv und vu gibt, so heissen diese beiden **Kanten parallel**.

Ein **einfacher Grahp** ist ein Graph, in dem es keine Schlingen und parallelen Kanten gibt.

Eine **Ecke** v **inszidiert mit einer Kante** $k = uv = \{u, v\}$, falls $v \in k$ gilt.

Dazu schreiben wir: $K(v) = \{\text{Kanten } k \mid v \text{ inszidiert mit } k\}$.

Falls es eine Kante k gibt mit $uv \in k$, so heissen u und v benachbart. (uv ist also Kante zwischen u und v.)

Ein **Graph** heisst **vollständig**, wenn alle Punkte resp. Ecken paarweise benachbart sind. (Zwischen zwei Punkten gibt es hier immer eine Kante.)

Wir schreiben: K_n = vollständiger Graph mit n Ecken.

$N(v) = \{\text{Nachbarn von } v\}$.
$d(v) :=$ **Grad der Ecke** $v = |N(v)| =$ Anzahl Nachbarn von v.

Die Anzahl der Ecken (Knoten) $n = |E|$ eines Graphen $G(K, E)$ bezeichnet man als die **Ordnung von** $G(K, E)$ bezeichnet.

Eine Ecke v heisst **isoliert** oder **frei**, wenn ihr Grad 0 ist (d.h. wenn sie keine Nachbarn hat).

Ein Graph heisst k–**regulär**, wenn alle Ecken den identischen Grad k haben.

Zwei Graphen $G(K, E)$ und $G'(K', E')$ heissen **isomorph**
$\Leftrightarrow (\exists_{\Phi\ bij.} :\ uv = \{u, v\} \in E\ \Leftrightarrow \{\Phi(u), \Phi(v)\} = \Phi(u)\Phi(v) \in E')$.

Falls nichts anderes vorausgesetzt wird, werden wir in diesem Abschnitt in der Regel einfache Graphen behandeln. Für solche gilt trivialerweise:

Lemma: **Vor.:** $G = (K, E)$, $u, v \in E$ einfach.

Beh.: $uv = \{u, v\} = \{v, u\} = vu$.

Beispiele: (Mit Hilfe von *Mathematica* auf dem Computer erzeugt.)

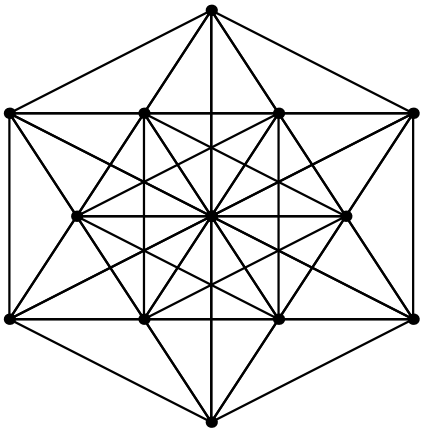


Abb. 2: Graph

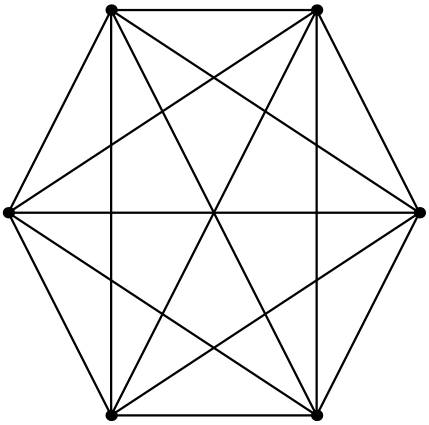


Abb. 3: Vollständiger Graph

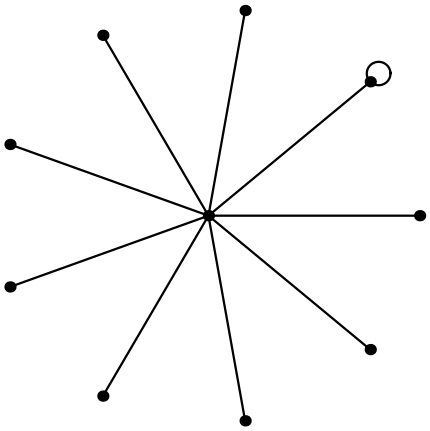


Abb. 4: Graph mit Schlinge

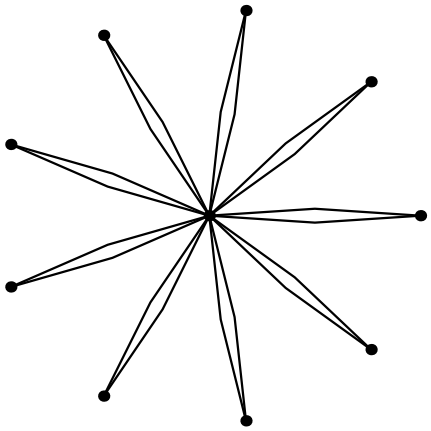


Abb. 5: Parallele Kanten

Abb. 6: Zwei Nachbarn

Abb. 7: Viele Nachbarn von v

Bemerkung: (Zur Darstellung) Um einen Graphen zu zeichnen, können wir die Eckpunkte beliebig auf dem Blatt verteilen. Die Kanten können so krumm gezeichnet werden wie man will. Die Darstellung sollte jedoch lesbar beiben.

$E = \{1, 2, 3, 4, 5, 6, 7\}$
$K = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{2, 5\}, \{4, 6\}\}$

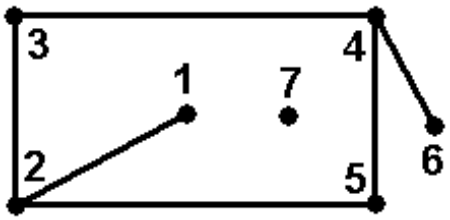


Abb. 8: Isolierter Punkt 7

Teilerrelation in $M = \{1, 2, 3, 4, 5, 6\} \subset \mathbb{N}$

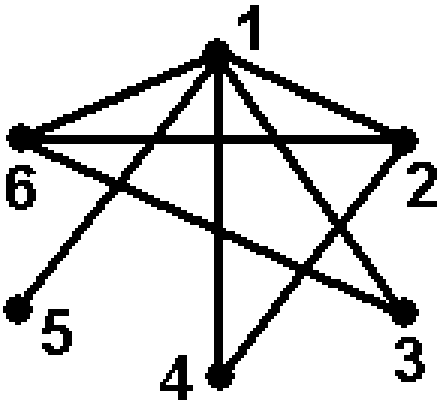


Abb. 9: Teilerrelation in M

Bemerkung: Man sieht sofort, dass durch den Graphen immer eine **Relation** gegeben ist.

Nachstehend die vollständigen Graphen K_1 bis K_6:
(Mit Hilfe von *Mathematica* auf dem Computer erzeugt.)

Abb. 10: Vollständiger Graph K_1

Abb. 11: Vollständiger Graph K_2

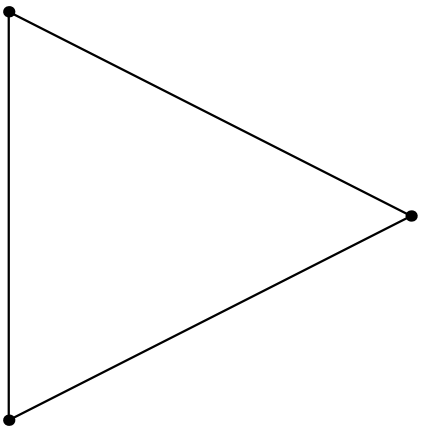


Abb. 12: Vollständiger Graph K_3

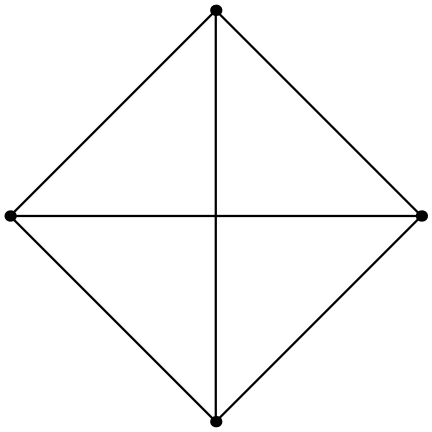


Abb. 13: Vollständiger Graph K_4

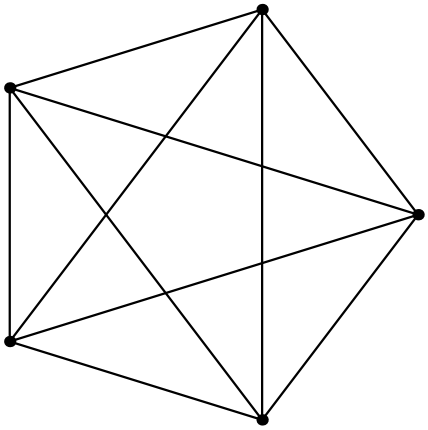


Abb. 14: Vollständiger Graph K_5

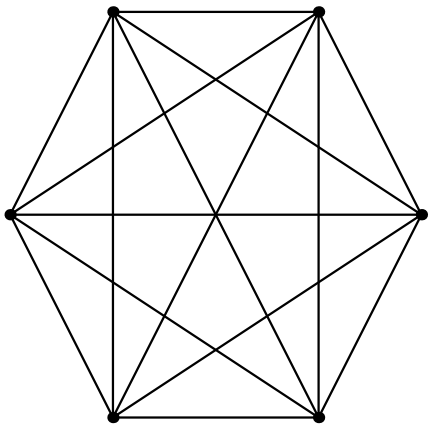


Abb. 15: Vollständiger Graph K_6

Bemerkung: Man sieht sofort ein, dass zwei isomprphe Graphen ohne spezielle Angabe der Bedeutung der Ecken oder Kanten nicht zu unterscheiden sind, da keiner vor dem andern ausgezeichnet ist.

Satz: In einem beliebigen Graphen gilt für die Summe der Grade aller Ecken:

$$\sum_{v \in E} d(v) = 2\,|K|$$

(Der Grad $d(v)$ ist die Mächtigkeit der Nachbarn.)

Beweis:
Schreibt man alle Ecken und dazu jeweils alle Nachbarn mit der zugehörigen Kante in eine Liste, so zählt man im Total jede Kante doppelt. (Denn jede Kante hat auf zwei Seiten einen Eckpunkt, kommt also immer doppelt vor.) Addiert man die Anzahlen der Nachbarn und gleichzeitig auch die gleichgrossen Anzahlen der zweimal gezählten Kanten, so bekommt man obige Formel.

Bsp.: (Vgl. oben das Beispiel mit der Teilerrelation in $M = \{1, 2, 3, 4, 5, 6\} \subset \mathbb{N}$.)
Geht man die Anzahlen der Nachbarn der Reihe nach entsprechend den Zahlen von 1 bis 6 durch, so ergibt sich $\sum_{v \in E} d(v) = 5 + 3 + 2 + 2 + 1 + 3 = 2 \cdot 8 = 16 = 2 \cdot |K|$.

Korollar: Bei einem k–regulären Graphe gilt somit:
$k \cdot E = 2 \cdot |K|$.

Bsp.: Beim vollständigen Graphen K_6 (vgl. oben) gilt: $k \cdot E = 5 \cdot 6 = 30 = 2 \cdot 15 = 2 \cdot |K|$.

Satz: Jeder Graph hat eine gerade Anzahl von Ecken ungeraden Grades.

Beweis:

Sei E_1 = Menge der Ecken ungeraden Grades, E_2 = Menge der Ecken geraden Grades.

$\rightsquigarrow\ E = E_1 \cup E_2,\ E_1 \cap E_2 = \{\ \}$ Dann gilt:

$$\underbrace{2 \cdot |K|}_{\text{gerade}} = \sum_{v \in E} d(v) = \sum_{v \in E_1} d(v) + \underbrace{\sum_{v \in E_2} d(v)}_{\text{gerade}} \ \Rightarrow\ \sum_{v \in E_1} d(v) \text{ gerade.}$$ ☺

21.1.3 Wege, Abstände, Kreise und Brückenproblem

Definitionen:

Ein **Weg** W resp. P_n in einem Graphen $G(E,K)$ ist eine Folge von Ecken $u_1, u_2, \ldots, u_n$ mit $u_i u_{i+1} \in K,\ u_i \neq u_{i+1}$ für $i \neq i+1$. $Anf(P_n) = u_1$ sei dabei der **Anfangspunkt** und $End(P_n) = u_n$ der **Endpunkt** des Weges.

Ein **Pfad** P in einem Graphen $G(E,K)$ ist ein Weg, auf dem alle Knoten (Ecken) in der Folge $u_1, u_2, \ldots, u_n$ voneinander verschieden sind.

Ein **Kreis** oder **Zyklus** C_n in einem Graphen $G(E,K)$ ist eine Folge von Ecken $u_1, u_2, \ldots, u_n$ mit $u_i u_{i+1} \in K,\ u_n u_1 \in K,\ u_i \neq u_{i+1}$ für $i \neq i+1$.

Länge eines Weges $l_n = n - 1 :=$ Anzahl Kanten.

Länge eines Krieses Anzahl Kanten = Anzahl der durchlaufenen Ecken.

Ein **Weg** oder **Kreis** heisst **einfach** $\Leftrightarrow$ Keine Ecke wird doppelt oder mehrmals durchlaufen.

Ein Graph $G(E,K)$ heisst **zusammenhängend**
$\Leftrightarrow\ (\forall_{Paare\ (u,v),\ u,v \in E} \quad \exists_{Weg} :\ u = Anf(P_n), v = End(P_n))$.

Eine **Komponente** eines Graphen ist ein isolierter Untergraph, von dessen Ecken aus es keine Wege zu den Ecken der anderen Komponente(n) gibt.

Eine **Brücke** in einem Graphen ist eine Kante des Graphen, deren Entfernung die Anzahl der Isolierten Untergraphen (Komponenten) erhöht.

Bsp.:

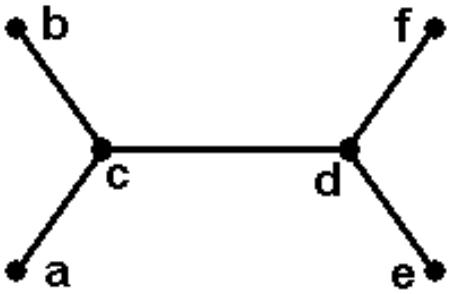


Abb. 16: Brücke in der Mitte

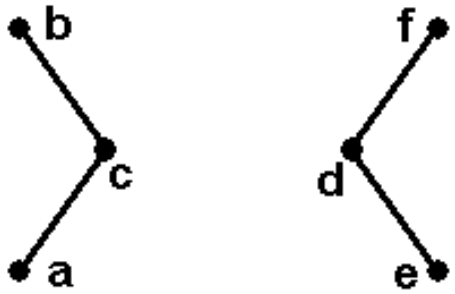


Abb. 17: Nach Entfernung der Brücke

Definition: Der **Abstand** $d(u, v)$ **zweier Eckpunkte** des Graphen $G(E, K)$ ist die Länge des kürzesten Weges W mit $Anf(W) = u$ und $End(W) = v$. Dabei setzt man $d(u, u) = 0$ und $d(u, v) = \infty$, falls zwischen u und v keine Weg existiert.

Bsp.: Im letzten Graphen ist $d(b, e) = 3$.

Definition: Ein Kreis in einem Graphen, der jede Kante des Graphen genau einmal enthält, heisst **Eulerkreis** oder **geschlossener Eulerzug** (auch **Eulertour** oder **Eulersche Linie**). Ein Eulerkreis kann auch eine freie Ecken sein.

Man spricht von einem **offenen Eulerzug** oder **offenen Eulerweg**, wenn die Position von Start- und Endecken nicht verlangt wird. Statt eines Zyklus wird lediglich ein Weg verlangt, der jede Kante des Graphen genau einmal enthält.

Ein zusammenhängenden Graph, der einen Eulerkreis enthält, heisst **Eulergraph**.

Ein Kreis C in einem Graphen der Länge $|E|$, welcher alle Ecken des Graphen exakt einmal besucht und bei dem $Anf(C) = End(C)$ gilt, heisst **Hamiltonkreis**.

Ein Graph, der einen Hamiltonkreis enthält, heisst **Hamiltongraph**.

Konsequenz: Ein Hamiltongraph ist trivialerweise zusammenhängend.

Der folgende Satz beantworter die durch das Königsberger Brückenproblem gestellte Frage. Dabei wird verwendet, dass der im „eulerschen“ Brückenproblem verlangte Weg eben ein „Eulerweg“ ist. Der zu diesem Problem gehörige Graphe ist auf Seite 168 (Figur „Brückenproblem, abstrakt“) dargestellt. Daraus ersieht man, dass darin nur Knoten resp. Ecken mit ungeradem Grad vorkommen. Zudem ist der Graph zusammenhängend.

Satz: Ein zusammenhängender Graph ist genau dann ein Eulergraph, wenn alle Ecken einen geraden Grad haben.

Beweis:
Ein Eulergraph enthält nach Definition einen Kreis, der jede Kante nur einmal enthält. Zum Beweis verifizieren wir die beiden Subjunktionen, welche die behauptete Bijunktion ausmachen:

1. $\Longrightarrow$: Der Graph G sei ein Eulergraph und enthalte daher einen Eulerkreis. Nun entfernen wir den Eulerkreis aus dem Graphen. Damit wird der Grad aller betroffenen Ecken um 2 tiefer, denn in einem reinen Kreisgraphen haben alle Ecken den Grad 2. Da der Eulerkreis alle Kanten des Graphen genau einmal enthält, haben wir nun auch alle Kanten entfernt. Und damit auch alle Knoten. Denn mit fortschreitender Entfernung der Kanten werden in jedem Knoten schrittweise zum Eulerweg

gehörige Kantenpaare entfernt. Führt man die Entfernung auf natürliche Art schrittweise durch, so bleiben am Schluss noch isolierte Knoten vom Grade 0, welche dann auch noch entfernt werden. 0 ist gerade. Der Grad wird also bei diesem Vorgehen schrittweise in jedem Knoten jeweils um 2 reduziert und bleibt am Schluss gerade. Setzt man die Sache wieder rückwärts zusammen, so erhöht man bei jedem Schritt im jeweiligen Knoten den Grad um 2. Das führt also nur zu Knoten mit geradem Grad.

2. $\underline{\Longleftarrow}$: Hier müssen wir von einem zusammenhängenden Graphen G ausgehen, in dem alle Ecken resp. Knoten geraden Grad haben. Darin wählen wir einen Weg maximaler Länge, der jede Kante nur einmal enthält. Da wir hier von endlichen Graphen ausgehen, ist das problemlos möglich. Dieser Weg W sei z.B. durch die Eckpunktfolge $v_0, v_1, \ldots, v_k$ gegeben. Dabei können die Ecken oder Knoten mehrmals durchlaufen werden. Nur für die Kanten besteht die Restriktion des einmaligen Durchlaufs. Da alle diese Eckpunkte geraden Grad haben, ist entweder $v_0 = v_k$ oder v_k wäre nicht Endpunkt. Im letzten Fall wäre der Weg entweder nicht maximal unter der Bedingung, dass v_k trotzdem gerade ist. Oder v_k wäre nicht gerade, was ebenfalls einen Widerspruch bedeutet. Damit ist W ein Kreis und es ergeben sich für W die folgenden Möglichkeiten:

   (a) W ist ein Eulerkreis und damit der Graph ein Eulergraph.

   (b) W bloss ein Kreis, aber nicht ein Eulerkreis. Dann gibt es weitere Ecken u_j in G mit geradem Grad, die in W nicht enthalten sind. Eine solche Kante $u = u_1 \notin W$ muss aber mit Punkten von W verbunden sein (etwa mit v_i, $v_i \in E$), da G zusammenhängend ist.
   $v_0, v_1, \ldots, v_k = v_0$ sei der vorausgesetzte längste Weg.

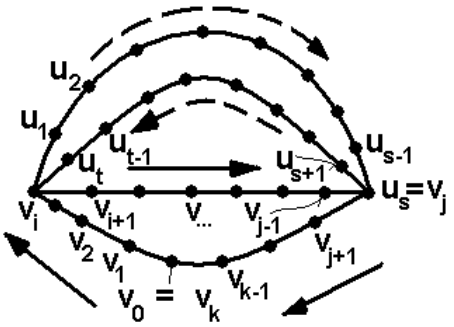


Abb. 18: Erweiterungsweg

Sei also u_1 mit v_i verbunden. Da v_i gerade Grad hat und dieser Knoten im Moment 3 bekannte Nachbarn hat, muss es noch einen vierten Nachbarn geben, etwa $u_t \notin$. Da G endlich und zusammenhängend ist, muss es einen kürzesten Weg W_1 von v_i über u_1 und u_t zurück nach v_i geben. W_1 ist also ein Kreis. Denn sonst gäbe es bei u_t keine Fortsetzung von W_1, und u_t hätte daher Grad 1, im Widerspruch zur Voraussetzung.

Nun könnte es noch sein, dass beim Durchlauf von W_1 eine Kante von $W := W_0$ oder W_1 doppelt durchlaufen wird. Dann müsste sich aber bei einem Punkt u_s der Weg W_1 mit $W = W_0$ vereinigen oder man hätte auf W_1 mindestens eine doppelt durchlaufene Kante mit dem Endpunkt u_s. Dieser Punkt hätte daher wegen der doppelt durchlaufenen Kante einen ungeraden Grad, was wiederum nicht sein kann. W_1 ist daher ein Kreis, der mindestens bei $v_i := u_0$ mit $W = W_0$ zusammenhängt. Dass W_1 noch mehr gemeinsame Punkte mit $W = W_0$ haben kann (z.B. $u_s = v_j$ wie in der Skizze oben gezeigt) spielt bei unserer Argumentation jetzt keine Rolle. Wichtig ist nur, dass die Vereinigung der beiden Wege W_0 und W_1 wieder einen Kreis ergeben, z.B. W_2: $v_0, v_1, v_2 \ldots, v_i, u_1, u_2, \ldots, u_{s-1}, v_j, u_{s+1}, \ldots, u_{t-1}, u_t, v_i, v_{i+1}, \ldots, v_{j-1}, u_s, v_{j+1}, \ldots, v_{k-1}, v_0$.
Damit haben wir aber einen Weg W_2 entdeckt welcher im Widerspruch zur eingangs gemachten Annahme länger ist als der gewählte Weg W_1 maximaler Länge, was nicht sein kann. Die Annahme, dass $W = W_1$ bloss ein Kreis, aber nicht ein Eulerkreis ist, muss daher falsch sein.

Konsequenz: Das Königsberger Brückeproblem besitzt keine Lösung:
Der verlangte Spazierweg existiert nicht.

21.1.4 Gerichtete Graphen (Digraphen)

Nun wollen wir einfache Graphen $G(E, K)$ zu gerichteten Graphen oder Digraphen *(Digraph $\rightsquigarrow$ Directed Graph)* erweitern. Dazu sei jetzt $|K| \in \mathbb{N}$, $K \subseteq E^2 = E \times E$.
$\rightsquigarrow$ $(u, v) \in K \subseteq E \times E$ ist ein geordnetes Paar, $(u, v) \neq uv = \{u, v\}$, $(u, v) \neq (v, u)$.

Definition:

$G = (K, E) := GR(K, E)$ heisst unter diesen Umständen **gerichteter Graph.**

$\vec{k} \in K$ ist dann **gerichtete Kante** (auch „Pfeil"): $\vec{k} = (u, v)$.

$u := k^{-1}$ heisst **Anfangsecke** von $\vec{k}$.

$v := k^{+1}$ heisst **Endecke** von $\vec{k}$.

Statt (u_i, u_j) schreiben wir hier kurz $u_{i,j}$.

Entsprechend der Kombinatorik, wo man den Übergang von der Variation zur Kombination erlebt, hat man hier einen Übergang vom gerichteten zum ungereichteten Graphen. Mehr Information in einem Gebilde auf der einen Seite bedeutet auch mehr Restriktion auf der andern Seite.
Und wie bei den ungereichteten Graphen definieren wir auch hier den **Grad** von Ecken sowie Wege und Kreise u.s.w., wobei es beim gerichteten Graphen oft einer Präzisierung bedarf:

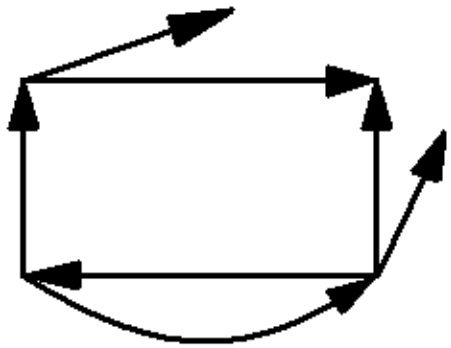


Abb. 19: Gerichteter Graph

Definition:

In Grad (Nachfolgergrad) $:= d^+(v) = |\{\vec{k} \in K \mid k^+ = v\}|$
Out Grad (Vorgängergrad) $:= d^-(v) = |\{\vec{k} \in K \mid k^- = v\}|$.

Gerichteter Weg := Folge verschiedener Ecken $v_1, v_2, v_3, \ldots, v_k$ Gor mit $\vec{k}_i = (v_i, v_{i+1}) \in K \ \forall_i$.
$\rightsquigarrow$ Die einzelnen Kanten $\vec{k}_i = (v_i, v_{i+1})$ sind demnach immer gerichtet nach dem Prinzip „vom Anfangs– zum Endpunkt"!

Länge des gerichteten Weges := Anzahl gerichteter Kanten.

Gerichteter Kreis := Gerichteter Weg mit $v_1 = v_k$.

Ein gerichteter Graph $GR(E, K)$ (Digraph) heisst **azyklisch**, wenn er keinen gerichteten Kreis enthält. (Ein gerichteter Graph kann einen Kreis enthalten, der kein gerichteter Weg ist. Die Pfeile können sich entgegenlaufen.)

In der Kante $\vec{k} = (u, v)$ ist u der **Vorgänger** von v und v der **Nachfolger** von u.

21.1.5 Zur Darstellung von Graphen

Folgende Darstellungsmöglichkeiten von Graphen sind je nach Fall günstig:

1. Graphische Darstellung (Graph).
2. Darstellung durch Aufzählung der Kanten.
3. Darstellung mittels einer Liste: Zu jeder Ecke listet man die Nachbarn resp. seine Nachfolger auf (Adjazenzliste).
4. Darstellung mittels Adjazenzmatrix: Ein Graph mit n Knoten kann durch eine $n \times n$-Matrix repräsentiert werden. Dazu nummeriert man die Knoten von 1 bis n durch und trägt in die Matrix die Beziehungen der Knoten zueinander ein.
5. Darstellung mittels Inzidenzmatrix: Ein Graph mit n Knoten und m Kanten kann auch durch eine Matrix repräsentiert werden. Dazu nummeriert man die Knoten von 1 bis n und die Kanten von 1 bis m durch und trägt in die Matrix die Beziehungen der Knoten zu den Kanten ein.

Natürlich wird es vorkommen, dass die genannten Darstellungsweisen für gereichtete und ungerichtete Graphen verschiedene Charakteristika haben. Wegen den beliebigen Nummerierungsmöglichkeiten von Ecken und Kanten sind die Adjazenzmatrix und die Inzidenzmatrix auch nicht eindeutig.

Sei jetzt vorerste $G(E, K)$ ein ungerichteter Graph mit n Ecken $u_1, \ldots, u_n$ und m Kanten $k_1, \ldots, k_m$

Definition:

Adjazenzmatrix $A = (a_{i,j}) = (n \times n)$–Matrix mit

$$a_{i,j} = \begin{cases} 1 & u_i u_j = k_{i,j} \in K \\ 0 & \text{sonst} \end{cases}$$

Inzidenzmatrix $B = (b_{i,j}) = (n \times m)$–Matrix mit

$$b_{i,j} = \begin{cases} 1 & u_i \in k_j \\ 0 & \text{sonst} \end{cases}$$

Konsequenz:

Eine Adjazenzmatrix informiert also darüber, ob eine jeweilige Kanze zwischen gegebenen Ecken vorhanden ist (Wert 1) oder nicht (Wert 0). Da bei ungerichteten Graphen für die Kanten $v_i v_j = v_j v_j$ gilt, wird die Matrix symmetrisch. Wegen $v_i v_i \notin K$ bei einfachen Graphen, steht bei einer solchen Matrix in der Diagonale immer 0. In der Zeilensummen $S_z(i) = \sum_{j=1}^{n} a_{i,j}$ wird jeweils 1 summiert, wenn die Kante $u_i u_j$ vorhanden ist, d.h. wenn also u_i (i ist hier fix) die Ecke u_j als Nachbar hat. Daher liefert diese Summe den Grad von u_i. Ebenso in den Spaltensummen $S_s(i) = \sum_{j=1}^{n} a_{j,i}$ wird jeweils 1 summiert, wenn die Kante $u_j u_i$ vorhanden ist, d.h. wenn also u_i (i ist hier wieder fix) die Ecke u_j als Nachbar hat. Daher liefert diese Summe wieder den Grad von u_i.

Im Falle von gerichteten Graphen liefert $S_z(i)$ die Anzahl der Nachfolger von u_i und $S_s(i)$ die Anzahl der Vorgänger von u_i.

Während bei einem gerichteten Graphen $GR(E,K)$ die Adjazenzmatrix ganz natürlich gebildet werden kann, muss die Inzidenzmatrix der gerichteten Kanten wegen neu definiert werden:

Definition: Sei $GR(E,K)$ ein gerichteter Graph mit n Ecken $u_1, u_2, \ldots, u_n$ und m gerichteten Kanten $\vec{k}_1, \ldots, \vec{k}_m$.
Inzidenzmatrix $B = (b_{i,j}) = (n \times m)$–Matrix mit

$$b_{i,j} = \begin{cases} 1 & u_i = k_j^+ \\ 0 & u_i \neq k_j^+, k_j^- \\ -1 & u_i = k_j^- \end{cases}$$

Beispiele:

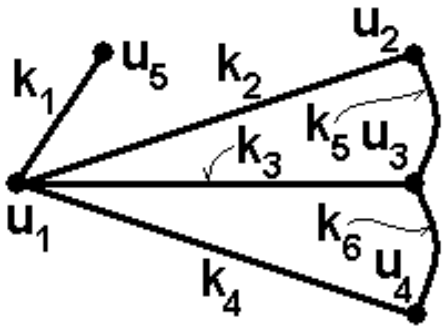


Abb. 20: Ähnlich Brückenproblem

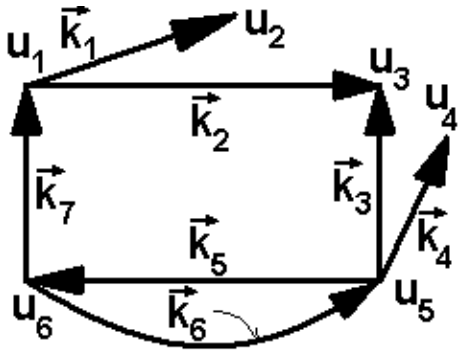


Abb. 21: Gerichteter Graph

In der obigen linken Abbildung (ungerichteter Graph) wird die Adjazenzmatrix:

$$A_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{und die Inzidenzmatrix: } B_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Dabei sind für die Inzidenzmatrix die folgenden Abkürzungen verwendet worden:
$k_1 = u_1u_5 (= k_{1,5})$, $k_2 = u_1u_2$, $k_3 = u_1u_3$, $k_4 = u_1u_3$, $k_5 = u_2u_3$, $k_6 = u_3u_4$.

In der rechten Abbildung dagegen (gerichteter Graph) findet man für die Adjazenzmatrix:

$$A_2 = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{Inzidenzmatrix: } B_2 = \begin{pmatrix} -1 & -1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 \end{pmatrix}$$

Mit dem Computer erzeugte Beispiele von Graphen

Die Folgenden Beispiele sind, wie auch frühere Beispiele mit *Mathematica erzeugt worden.*

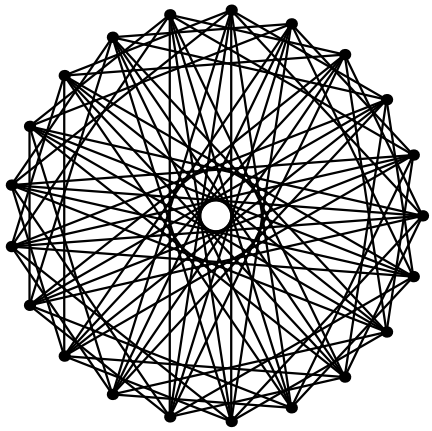


Abb. 22: Zirkulante Graphen

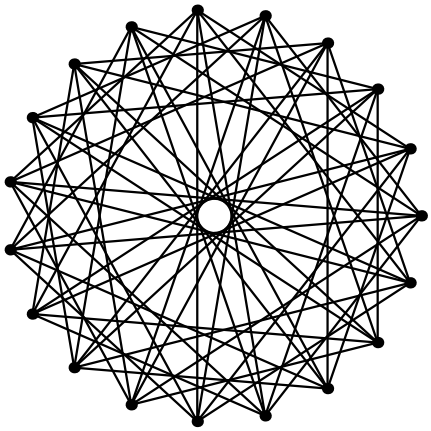


Abb. 23: Zirkulante Graphen

(Ein Graph ist dann zirkulant, wenn in der Folge der Knoten jeweils der i–te Knoten mit dem $i + j$–ten und dem $i - j$–ten adjazent ist. Dabei wird die Indexmenge modulo n genommen, d.h. als Zyklus betrachtet.)
Vgl. dazu $http://mathworld.wolfram.com/CirculantGraph.html$

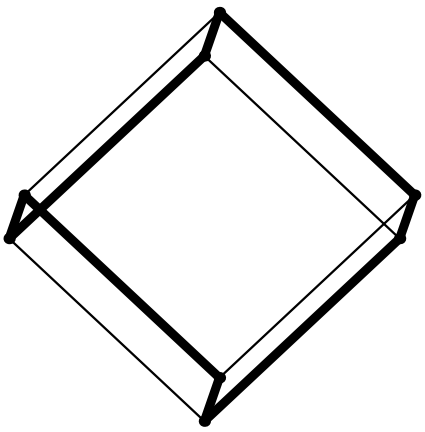


Abb. 24: Hamiltonkreis

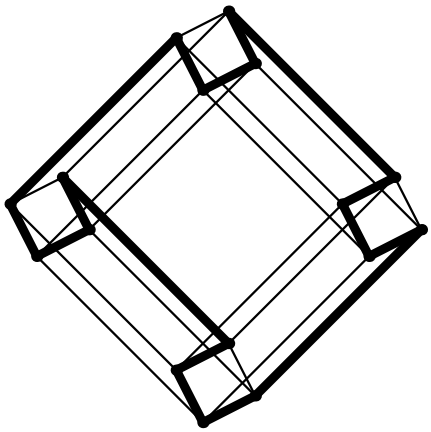


Abb. 25: Hamiltonkreis

21.1.6 Bäume

Definition: **Bäume** sind zusammenhängende Graphen, welche keinen Kreis enthalten.

Ein **Wald** ist ein Graph, dessen Komponenten Bäume sind.

Bemerkung: Bäume sind z.B. wichtig bei Datenstrukturen oder Such– und Sortierverfahren, z.B. „Divide–and–Conquer–Algorithmen“.

Bsp.:

Gegeben: Baum $G(E, K)$:

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

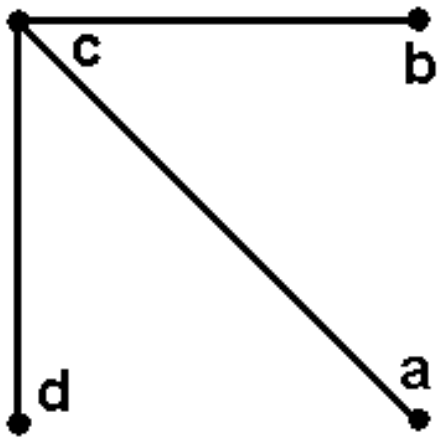


Abb. 26: Baum

Satz: Ein Baum mit $|E| \geq 2$ hat mindestens 2 Ecken mit Grad 1.

Beweis:
Wegen der Endlichkeit von $|E|$ kann man irgendwo einen Weg beginnen und muss dann nach endlich vielen Schritten an ein Ende gelangen, da wegen der Kreisfreiheit keine Kante doppelt oder mehrmals durchlaufen werden kann. Dieses Ende hat Grad 1. Kehrt man von hier in umgekehrter Richtung zum Startpunkt zurück und geht danach, falls dieser Startpunkt nicht schon Grad 1 hat, immer weiter, so muss man wegen der Kreisfreiheit und der Endlichkeit von $|E|$ nach endlich vielen Schritten wiederum zu einem Ende gelangen. Dieses wiederum hat Grad 1.

Die nebenstehende Abbildung zeigt die Verwendung der üblichen Bezeichnungen **Wurzel** und **Blätter** im Fall eines gerichteten Graphen. Im ungerichteten Fall verwendet man diese Bezeichnungen analog. Oft sieht man in solchen Darstellungen aus „technischen Gründen“ die Wurzel oben. Wurzel und Blätter haben Grad 1 (siehe Abbildung).

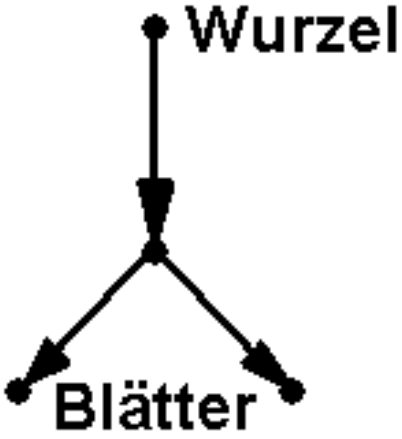


Abb. 27: Wurzel und Blätter

Definition: Ein **Wurzelbaum** ist ein gerichteter Graph $GR = (E, K)$ mit einer Wurzel.

Bemerkung: Aus einem gewöhnlichen Baum kann man leicht einen Wurzelbaum machen, indem man eine Ecke mit Grad 1 als Wurzel definiert und dann den Baum nach der in obiger Skizze verwendeten Art anordnet. So gelangt man zu einer **teilgeordneten, gerichteten Darstellung.** Ein nicht geordneter Graph wird demnach durch dieses Vorgehen geordnet. Diese Darstellungsform wird oft bei Datenstrukturen oder auch bei Stammbäumen verwendet. Statt Wurzel hat man dort den Stammvater, statt die Blätter die Kinder. Als **Kind** bezeichnet man allgemeiner einen direkten Nachfolger eines Knotens (d.h. eines **Vaters**) in einem Baum.

Definition: Ein **binärer Baum** ist ein Baum mit ausgezeichneter Wurzel und höchstens zwei Kindern an jeder Ecke. Der Binärbaum heisst dann **regulär**, wenn ausser der Wurzel mit Grad 2 nur noch Ecken mit Grad 1 und 3 vorkommen. Der Abstand eines Knotens (Ecke) von der Wurzel nennen wir das **Niveau der Ecke**. Das grösste Niveau heisst **Höhe**.

Beispiel eines Binärbaums siehe Skizze nebenan.

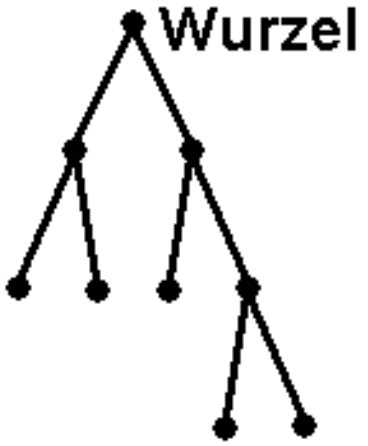


Abb. 28: Binärbaum der Höhe 3

Binärbäume benutzt man zur Auswertung arithmetischer Ausdrücke. Dabei benutzt man entweder die Infix–Notation (Operatoren zwischen die Operanden) oder die Postfix–Notation (Umgekehrte Polnische Notation, kurz UPN, engl. Reverse Polish Notation, RPN), je nach Baumdurchlauf.

Symbol: *ld* bedeutet im Folgenden den logarithmus dualis (2–er Logarithmus).

Dann gilt der Satz:

Satz: 1) Die Anzahl der Ecken in einem Binärbaum auf dem Niveau k ist 2^k.

2) Für die Höhe H eines Binärbaumes mit n Ecken gilt:

$$H \geq ld(n+1) - 1$$

Zum Beweis: Die Formel „Anzahle Ecken auf dem Niveau k gleich 2^k“ ist direkt ablesbar.

Bis zum Niveau 0 (Wurzel) gibt es maximal $n = 1$ Ecken. Damit gilt: $2^{0+1} = 2 \geq 1 + 1 = n + 1$. Bis zum Niveau 1 gibt es maximal $n = 3$ Ecken. (Vgl. obige Skizze.) Dann gilt: $2^{1+1} = 4 = 3 + 1 \geq n + 1$. Bis zum Niveau 2 gibt es maximal $n = 7$ Ecken. Dann gilt: $2^{2+1} = 8 = 7 + 1 \geq n + 1$. Die maximale Anzahl Ecken n bis zum Niveau H berechnet sich zu $n_{Max} = 1 + 2 + 4 + 8 + \ldots + 2^H = \dfrac{2^{H+1} - 1}{2 - 1} = 2^{H+1} - 1$

(geometrische Reihe). Daher ist $2^{H+1} = n_{Max} + 1 \geq n + 1$. Daraus folgt durch Logarithmieren:
$H + 1 \geq ld(n+1)$. ☺

Satz:

Vor.:

Gegeben sei ein regulärer Binärbaum mit n Ecken.

Beh.:

1) Dieser Binärbaum besitzt eine ungerade Anzahl Ecken.

2) Die Anzahl Kanten im Binärbaum ist $|K| = n - 1$.

3) $\frac{n+1}{2}$ = Zahl der Blätter vom Grade 1.

Bemerkung: Trivialerweise hat in einem Binärbaum die Wurzel Grad 2, die Endblätter haben Grad 1 und die Zwischenknoten Grad 3.

Beweis:

1. Die Anzahl der Ecken in einem Binärbaum auf dem Niveau k ist 2^k. Die Summe aller Ecken n berechnet sich demnach zu $n = 2^0 + 2^1 + 2^2 + 2^3 + \ldots + 2^H = 1 + \underbrace{2 + 4 + 8 + \ldots + 2^H}_{\text{gerade}, = 2 \cdot z}$, wobei H die Höhe des Baumes ist. $\rightsquigarrow$ $n = 1 + = 2 \cdot z$ ist ungerade.
2. In der Stammbaumdarstellung (Wurzel oben) gehört zu jeder Ecke eine oben an die Ecke angefügte Kante, ausser bei der Wurzel. Die Anzahl Kanten ist daher gleich die Anzahl Ecken minus 1.
3. Jeder Graph hat eine gerade Anzahl von Ecken ungeraden Grades (Satz von Seite 173). Alle Ecken ausser der Wurzel haben ungeraden Grad (vgl. Bemerkung oben). Damit wird die Summe der Eckengrade:
$$\sum d(v) = \underbrace{2}_{\text{Wurzel}} + 2 \cdot \underbrace{(2 \cdot h + 1)}_{\text{ungerade Zahl}} = \text{gerade Zahl}$$
Sei p die Anzahl der Blätter, so ist die Zahl der innenliegenden Knoten vom Grade 3: $n_i = n - p - 1$. Nun gilt für die Summe der Grade (vgl. Satz Seite 173, $|K|$ = Anzahl Kanten):
$$\sum_{v \in E} d(v) = 2\,|K| = \underbrace{2}_{\text{Wurzel}} + \underbrace{p}_{\text{Blätter}} + 3 \cdot \underbrace{(n - p - 1)}_{\text{Innere}} = 2 + p + 3\,n - 3\,p - 3 = 3\,n - 2\,p - 1$$
Dabei gilt: $|K| = n - 1 \;\Rightarrow\; 2\,|K| = 2\,(n-1) = 2\,n - 2 = 3\,n - 2\,p - 1 \;\Rightarrow\; p = n - 1$

Definition: Ein **In-Tree („Zur–Wurzel–Baum“)** ist ein gerichteter Graph mit einem ausgezeichneten Knoten (genannt **Wurzel**), für den gilt, dass die Wurzel von jedem Knoten aus durch genau einen gerichteten Pfad erreichbar ist.

Ein **Out-Tree („Von–der–Wurzel–Baum“)** ist ein gerichteter Graph mit einem ausgezeichneten Knoten (**Wurzel**), für den gilt, dass jeder Knoten durch genau einen gerichteten Pfad von der Wurzel aus erreichbar ist.

Definition: Als **Ordnung eines Out-Trees** bezeichnet die grösste Anzahl Kinder eines seiner Knoten (maximaler Ausgangsgrad). Alle Knoten mit Ausgangsgrad 0 heissen Blätter.

Bemerkung: Einen ungereichteten Graphen kann man jederzeit durch Einführung von Richtungen in einen gerichteten Graphen verwandlen. Wir nennen hier diesen Prozess **das Richten eines Graphen**.

Bemerkung: Die Ordnung $n = |E|$ eines Graphen darf man nicht mit der Ordnung eines durch richten entstandenen Out-Trees zu verwechseln!

Definition: Ein **Spannbaum** (auch **aufspannender Baum** oder **spannender Baum** (engl. spanning tree)) ist ein Teilgraph eines ungerichteten Graphen $G(E, K)$, welcher ein Baum ist und welcher alle Knoten von $G(E, K)$ enthält.

Konsequenz: Man sieht unmittelbar, dass die Ordnung eines Spannbaums eines Graphen $G(E, K)$ immer $n = |E|$ ist.

Bemerkung: Spannbäume existieren nur in zusammenhängenden Graphen. Anwendung: Das Spannbaumproblem trifft man in der Praxis bei der kürzesten Verdrahtung von Kommunikationsnetzen oder beim Problem des Baus der kürzesten Fahrwege.

Satz: Jeder zusammenhängende Graph enthält einen aufspannenden Baum.

Beweis:

1. Ist der Graph schon ein Baum, so ist der Satz bewiesen: Den Spannbaum erhält man einfach durch Elimination aller überflüssigen Kanten.

2. Ist der Graph kein Baum, so enthält er einen Kreis. Entfernt man eine geeignet gewählte Kante eines Kreises, deren Weglassung den Zusammenhang nicht stört, so entsteht entweder ein Baum — oder der nun entstandene Graph enthält immer noch einen Kreis. Dann ist man entweder fertig wie oben erwähnt — oder die Prozedur ist wiederholbar. Da $G(E, K)$ endlich ist, gelangt man so nach endlich vielen Schritten zu einem Spannbaum.

Satz: Die folgenden Aussagen sind äquivalent:

1. $G(E,K)$ ist ein Baum.
2. $G(E,K)$ ist kreisfrei.
3. Für je zwei beliebige Ecken u und v in $G(E,K)$ gibt es genau einen Weg mit Anfangspunkt u und Endpunkt v.
4. $G(E,K)$ ist zusammenhängend mit $|K| = |E| - 1$ resp. $|E| = |K| + 1$

Beweis:

1. $(1) \Leftrightarrow (2)$ ist identisch mit der Definition des Begriffs „Baum“.

2. $(1,2) \Leftrightarrow (3)$: Da der Graph $G(E,K)$ ein Baum ist, gibt es zwischen u und v immer mindestens einen Weg. Falls es im Baum $G(E,K)$ zwischen u und v zwei Wege gäbe, würde damit in $G(E,K)$ einen Kreis enthalten sein $\rightsquigarrow$ Widerspruch!
   Andererseits folgt aus (3) direkt, dass $G(E,K)$ ein Baum ist.

3. $(1,2,3) \Leftrightarrow (4)$: $G(E,K)$ sei ein Baum $\Rightarrow$ $\exists$ Ecken u, v mit Grad 1. Entfernt man u und auch die Kante uu_1, so bleibt ein kleinerer Baum $G_1(E_1,K_1)$, $|E_1| = |E|-1$, $|K_1| = |K|-1 \Rightarrow |E_1|-|K_1| = |E|-|K|$. Verfährt man bei Bedarf ebenso mit $G_1(E_1,K_1)$ ($\Rightarrow |E_2|-|K_2| = |E|-|K|$) und dann bei Bedaft ebenso mit dem Resultat $G_2(E_2,K_2)$, so gelangt man nach endlich vielen Schritten (Graph endlich!) zu einem Graphen $G_{n-2}(E_{n-2},K_{n-2})$ mit nur noch zwei Ecken und einer Kante. Hier gelten die Beziehungen $1 = 2-1 = |E_{n-2}| - |K_{n-2}| = |E| - |K| \Rightarrow |E| = |K| + 1$ ☺

   Sei nun $G(E,K)$ ein zusammenhängender Graph mit $|E| - |K| = 1$. Jeder solche Graph enthält einen aufspannenden Baum $B(E_B,K_B)$ mit $E_B = E$ und $|K_B| \leq |K| \rightsquigarrow 1 = |E| - |K| = |E_B| - |K| \leq |E_B| - |K_B|$. Für einen Baum (also für $B(E_B,K_B)$) haben wir aber eben gezeigt, dass gilt: $1 = |E_B| - |K_B|$. $\rightsquigarrow$ $1 = |E| - |K| \leq |E_B| - |K_B| = 1 \Rightarrow |K_B| = |K|$. Da alle hier verwendeten Mengen endlich sind, muss $B(E_B,K_B)$ mit $G(E,K)$ identisch sein. ☺

Da nun bei einem Baum $n = |E| = |K| + 1$ gilt, wird für $|K| \geq 1$, also für $n = |E| \geq 2$ nun

$$\sum_{u \in E} d(u) = 2\,|K| = 2\,(n-1) = 2\,n - 2\,n.$$

$\rightsquigarrow$

Satz:

Vor.: Gegeben sei ein Baum mit der Ordnung $n \geq 2$

Beh.:

$$\sum_{u \in E} d(u) = 2\,n - 2\,n$$

Mit dem Computer erzeugte Beispiele von Bäumen

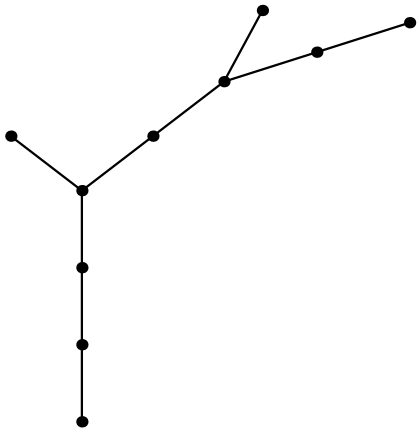


Abb. 29: Baum

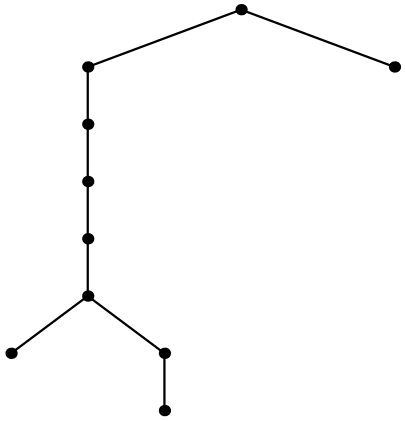


Abb. 30: Baum

21.2 Algorithmen für aufspannende Bäume und minimale Wege

21.2.1 Algorithmus–Begriff und Quicksort

Begriffserklärung

Ein **Algorithmus** ist allgemein eine genau definierte Handlungsvorschrift zur Lösung eines Problems oder einer bestimmten Art von Problemen. Der heute so verstandene Begriff beschränkt sich damit nicht auf die Mathematik. Beispiele für Algorithmen: Genaue Kochrezepte, auch solche mit genauen Teilrezepten, auf die verwiesen wird. Waschmaschinenprogramme, Reparatur- und Bedienungsanleitungen, Hilfen zum Ausfüllen von Formularen, Computerprogramme und eben nicht zuletzt exakte mathematische Vorschriften zur Lösung eines exakt beschriebenen Problems in endlich vielen Schritten. Speziell in der Mathematik:
Ein **mathematischer Algorithmus** ist eine endliche Beschreibung eines endlichen Verfahrens zur Ermittlung gesuchter aus gegebenen Werten.
Ursprünlich stammt der Begriff aus der Mathematik. Das **Wort Algorithmus** wird in verschiedenen Quellen verschieden erklärt. Es entstand als lateinisierte Abwandlung oder Verballhornung des Namens (je nach Quelle anders geschriebenen) von „Muhammad ibn Musa al-Chwarazmi“ , „Alchwãrizimi“ oder „Abu'Abdallah Muhammad ibn Nusa al–Huwarisimi al Magusi“ (* ca. 783; †ca. 850), Bibliothekar des Kalifen Almamun.
Vgl. auch: *http : //de.wikipedia.org/wiki/Algorithmus*

Quicksort

Ein sehr wichtiger und auch sehr leicht verständlicher Algorithmus ist der **Quicksort–Algorithmus**. Er dient zum Sortieren einer endlichen Menge nach einer gegebenen Ordnungsrelation unter den Elementen. Beim diesem Algorithmus wählen wir ein Element aus der zu sortierenden Liste aus (wir nennen es das **Pivotelement**). Damit zerlegen wir die Liste in zwei Teillisten, eine untere und eine obere. Die untere Teilliste enthält alle Elemente kleiner als das Pivotelement. Die obere Teilliste enthält alle Elemente gleich oder gröser dem Pivotelement. Diese beiden Teillisten werden ihrerseits rekursiv nach dem eben beschriebenen Prinzip sortiert. Anschliessend muss das Ergebnis wieder zusammengesetzt werden.
Nachstehend werden wir im Rahmen anderer Algorithmen auf diesen Algorithmus Bezug nehmen.

21.2.2 Problemstellungen für aufspannende Bäume

Problem: Gesucht sind Algorithmen (Rechenvorschriften), welche die folgenden Aufgaben lösen können:

1. Bestimme die Ordnung eines einfachen ungerichteten Graphen.

2. Finde in einem gegebenen zusammenhängenden Graphen einen aufspannenden Baum.

3. Entscheide, ob ein gegebener Graph zusammenhängend ist. (Jeder Knoten muss von einem Algorithmus dazu mindestens einmal besucht werden.)

Ein Algorithmus, welcher diese Aufgaben löst, ist der **Breadth–First–Search–Algorithmus (BFS)**, bekannt auch als **Breitensuche–Algorithmus**.
Vgl. auch *http : //en.wikipedia.org/wiki/Breadth-first_search*

Bemerkung: Wir gehen hier von endlichen Graphen aus, die in irgendwelcher identifizierbaren Form gegeben sind. (Z.B. Adjazenzmatrix oder Inzidenzmatrix). Das bedeutet, dass man sich die Ecken oder Knoten in ein Koordinatensystem eingezeichnet denken kann, analog einem beschriebenen Blatt, auf dem nach der Schreibweise „(1) erst von links nach rechts, (2) dann Zeilensprung (3) gehe wieder zu (1) (Loop!)“. Nach dieser Anweisung kann man die Ecken eines Graphen mit fortlaufenden provisorischen Nummern versehen. $\rightsquigarrow U_1, U_2, \ldots, u_n,\ n = |E| \rightsquigarrow$ Urliste.

Konsequenz: Damit ist das Problem der Bestimmung der Ordnung des Graphen gelöst.

Bevor wir uns daran machen einen Spannbaum zu suchen, wollen wir uns noch vergegenwärtigen, dass der Spannbaum nicht immer eindeutig bestimmt ist. Man sieht das leicht im nebenstehenden vollständigen Graphen K_4, bei dem man jeden der vier verschiedenen Punkte als Wurzel wählen kann und so den Spannbaum bekommt, indem man die überflüssigen Kanten ausputzt. Z.B. ist es möglich, den Spannbaum jeweils in einer Form zu wählen, dass die noch vorhandenen Kanten fächerförmig von der jeweiligen Wurzel ausgehen, was hier zu vier verschiedenen Spannbäumen der Höhe 1 führt. Aber man könnte auch z.B. den Punkt oben als Wurzel wählen und nur die beiden linken Aussenkanten sowie die rechte untere Aussenkanten belassen, womit man dann einem Spannbaum Höhe 3 gewinnt. Für die Höhe gilt trivialerweise die Einschränkung $H < |E| = n$

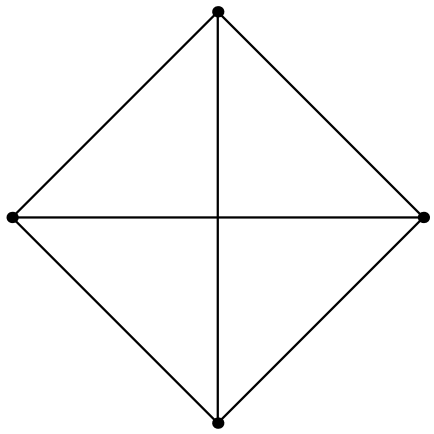


Abb. 31: Vollständiger Graph K_4

Lemma: Der Spannbaum eines einfachen Graphen der Ordnung n ist nicht in jedem Fall eindeutig. Es kann dabei vorkommen, dass es Spannbäume verschiedener Höhe $H < n$ gibt.

Damit ist aber implizit auch schon eine neue Problemstellung formuliert:

Problem: Finde einen Spannbaum minimaler und einen maximaler Höhe.

21.2.3 Breitensuche

Idee: Durchsuche die Ecken eines Graphen $G(E, K)$ der Ordnung $n \in \mathbb{N}$ der **Breite nach**. Dabei sollen die Ecken aufgezählt werden, was gleichbedeutend mit der Erstellung einer Liste ist. Das Nachstehende Beispiel illustriert dabe das Vorgehen:

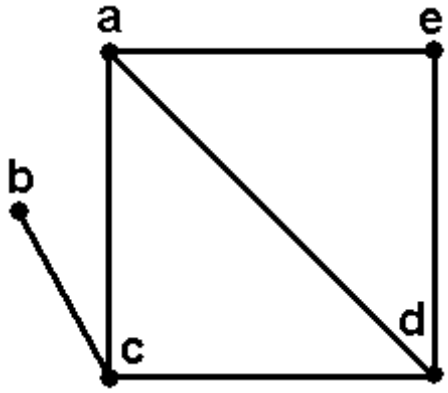


Abb. 32: Graph

1. Starte bei einer gewählten „aktuellen“ Ecke.
2. Erkenne und erzeuge in einer Liste die Nachbarecken c, d, e sowie die Kanten ac, ad, ae.
3. Setze die in der Rangfolge festgestellte Ecke c als als aktuelle Ecke. Gehe gleich vor wie oben unter Ausschluss der schon erzeugten Ecken aus der Liste.
4. Erkenne und erzeuge damit b.
5. Gehe mit d und e gleich vor wie oben mit c, was zu keiner Neuentdeckung führt. Damit ist das Niveau (1) erledigt.
6. Gehe auf Niveau (2) gleich vor mit b, was zu keiner Neuentdeckung führt. Damit ist auch das Niveau (2) erledigt.
7. Ein Niveau (3) existiert nicht: Stop.

Allgemeinere Formulierung:

Wir beachten, dass ein Baumgraph als Stammbaum dargestellt werden kann und dass es günstig ist, in einem solchen zweidimensionalen Gebilde zur raschen Auffindung der Punkte zwei Koordinaten einzuführen: Eine für das Niveau und eine zweite für die Identifikation des Punktes innerhalb aller Punkte auf einem Niveau.

1. Starte bei einer beliebig gewählten „aktuellen“ Ecke v und gebe dieser Ecke die Nummer des Niveaus und eine Laufnummer auf dem Niveau $\rightsquigarrow\ v = v_{0,1}$.
2. Erkenne die Nachbarecken und erzeuge davon eine Liste auf dem Niveau 1: $v_{1,1}, v_{1,2}, \ldots, v_{1,k_1}$ sowie eine Liste der Kanten $v_{0,1}v_{1,1}, v_{0,1}v_{1,2}, \ldots, v_{0,1}v_{1,k_1}$.
3. Verfahre nacheinander gleich mit allen Punkten $v_{1,1}, v_{1,2}, \ldots, v_{1,k_1}$ statt $v_{0,1}$. Besuche aber nur diejenigen Nachbarn, die nicht schon vorher besucht worden sind, was anhand der Identifikation durch die Urliste möglich ist. $\rightsquigarrow\ v_{2,1}, v_{2,2}, \ldots, v_{2,k_2}$
4. Besuche so auf allen Niveaus alle Punkte nach der Rangfolge und unter Ausschluss der schon vorhandenen Punkte und vergebe die notwendigen neuen Nummern.
5. Gehe auf Niveau (j) $1 \geq j \geq n$ gleich vor mit $j-1$, was zu keiner Neuentdeckung führt. Damit ist auch das Niveau (j) erledigt. (Das Niveau j sei das grösste Niveau.)
6. Ein Niveau $(j+1)$ existiert nicht: Stop.
7. Nun sind die Ecken nach dem Schema $E_1 = \{v_{0,1}, v_{1,1}, v_{1,2}, \ldots, v_{1,k_1}, v_{2,1}, v_{2,2}, \ldots, v_{2,k_2}, \ldots, v_{j,k_j}\}$ natürlich sortiert und können fortlaufend nummeriert werden $\rightsquigarrow\ v_{0,1} = u_1, \ldots, v_{j,k_j} = u_m$. Ist $m = |E_1| < n$, so ist der Graph nicht zusammenhängend. Ansonst hat man durch die Identifikation mittles der doppelten Indizes der Punkte den Spannbaum gefunden, da ja nur die für den Algorithmus wesentlichen verbindenden Kanten notiert worden sind. Damit hat man alle Ecken und infolge des Ausschlusses schon besuchter Ecken keine doppelt durchlaufenen Kannten. (Oder: Da die erzeugten Kanten aufsteigend geordnete Nummernpaare haben, kann kein Kreis erzeugt worden sein.)

Satz: Bei einem zusammenhängenden Graphen liefert der Breitenalgorithmus einen Spannbaum.

Das eben beschriebene Verfahren funktioniert also Niveauweise, von der Wurzel bis zu den Blättern. Im Gegensatz dazu kann man sich ein anderes Verfahren denken, bei dem man erst einmal von der Wurzel zu einem Blatt absteigt, z.B. dem am weitesten links liegenden Blatt, und dann wieder aufsteigt bis zur nächsten anzutreffenden Verzweigung und von dort wieder auf einem neuen Pfad absteigt u.s.w.. Das führt zu einem neuen Algorithmus, dem **Depth–First–Search–Algorithmus (DFS)**, bekannt auch als **Tiefensuche–Algorithmus**.

21.2.4 Tiefensuche

Hier sei es dem Leser überlassen, den Algorithmus in Abwandlung des bei er Breitensuche entwickelten Verfahrens selbst zu entwerfen. Bei der Breitensuche war der primäre Index der Punkte der Höhenindex, zu dem jeweils alle Breitenindizes gesucht worden sind. Hier nun muss diese Vorgegensweise umgekehrt werden. Zu einem ersten Breitenindex, gegeben durch das erste aufgefundene Blatt, werden alle notwendigen Höhenindizes notiert. Darauf wird das nächste Blatt resp. den nachsten Knoten vor der Schliessung eines Kreises gesucht und unter Ausschluss schon besuchten Punkte gleich verfahren u.s.w..
Vgl. auch *http://en.wikipedia.org/wiki/Depth_first_search*

21.2.5 Auffinden von Spannbäumen bei bewerteten Graphen

Bewerteten Graphen und gleichwertige unbewertete Graphen

Zuerst wollen wir den Begriff des bewerteten Graphen erklären. Gehen wir vom Beispiel eine Graphen eines Eisenbahnnetzes aus, so wird sofort klar, dass neben den Kanten auch die „Länge der Kanten“, d.h. die Länge der Verbindungen zwischen den Bahnhöfen, wesentlich ist beim Bau eines Netzes kürzester totaler Länge, in dem diese Bahnhöfe erreicht werden können.

Bemerkung: Sind diese Längen alle ganze Zahlen, im einfachsten Falle etwa Vielfache der Länge des kürzesten vorhandenen Abstandes a zwischen zwei Bahnhöfen, so könnte man en Graphen G duch einen etwas komplizierteren, erweiterten Graphen G_e ersetzen, bei welchem auf jeder Strecke (d.h. hier Kante) immer nach dem Abstand a neue Punkte (d.h. hier Bahnhöfe) eingesetzt sind, quasi Zwischenstationen also. Für Schnellzüge mag das belanglos sein, jedoch kann man damit im Graphen die Längen der Kanten weglassen, da ja alle gleich sind. So kann man in G_e einen minimalen Spannbaum suchen. Hier wollen wie diese Idee aber vorerst nicht verwenden und den eingesessenen Theorieaufbau weiter verfolgen.

Ein **bewerteter Graph** ist somit ein Graph, dessen Kanten alle ein Gewicht besitzen (im Beispiel oben die Entfernung der Knoten). Diese Definitione müssen wir jetzt noch so schärfen, dass darauf die heute zur Verfügung stehenden mathematischen Methoden angewendet werden können.

Definition: Gegeben sei ein ungerichteter Graph $G(E, K)$. Dazu existiere nun neu eine Funktion $\omega : K \longmapsto \mathbb{R}$. ω heisst **Kantenbewertung**, $G(E, K, \omega)$ heisst **bewerteter Graph**.

$\rightsquigarrow$ ω ordnet somit jeder Kante $k_i \in K$ eine reelle Zahl $\omega(k_i)$ zu. $\omega(k_i)$ ist der zu k_i gehörige Wert oder die zu k_i gehörige Bewertung.

Bemerkung: Umgekehrt könnte man natürlich in einem nicht bewerteten Graphen mit Kantengewichten $\omega(k_i) \in \mathbb{N}$ jeden abzweigungslosen Pfad ersetzen durch eine bewertete Kante. Man hätte damit einen bewerteten Graphen.

Konsequenz: Für die folgenden Probleme kann ein unbewerteter Graph durch einen bewerteten Graphen ersetzt werden, indem alle Pfade (verzweigungslose Wege) der Länge L_i durch eine Kante mit dem Gewicht L_i ersetzt werden. Umgekehrt kann ein bewerteter Graph mit Kantengewichten $\omega(k_i) = L_i \in \mathbb{N}$ durch einen unbewerteten ersetzt werden, indem man alle Kanten durch einen Pfad ersetzt, dessen Länge gleich dem Gewicht der ersetzten bewerteten Kante ist. Die damit gestiftete Abbildung zwischen der Menge der zusammenhängenden unbewerteten Graphen und der Menge der zusammenhängenden bewerteten Graphen mit **natürlichzahligen Kantengewichten** ist bijektiv.

Bsp.:

Das nebenstehende Beispiel zeigt, dass auch negative Gewichte einbezogen werden.

Wir wollen nun zur Darstellung der Bewertung die Adjaszenzmatrix erweitern.
Statt dem Wert 1 für das Vorhandensein der Kante tragen wir neu das Gewicht der Kante in die Matrix ein. 0 bedeutet nach wie vor „Kante nicht vorhanden“.

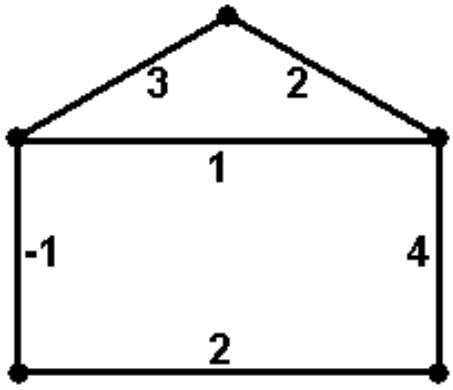


Abb. 33: Bewerteter Graph

21.2.6 Das Problem des minimalen Spannbaums

Problem: Gesucht sind nun wiederum Algorithmen, welche die folgenden Aufgaben lösen können:
Suche einen aufspannenden Baum mit minimaler Kantenbewertung.
($\rightsquigarrow$ Im Falle des vorhin erwähnten Eisenbahnnetzes soll man damit ein Netz minimaler Länge suchen, das alle Knoten verbindet.)

Definition: Gegeben sei ein zusammenhängender und bewerteter Graph $G(E, K, \omega)$. Ein Spannbaum T (Tree) mit minimalem Gewicht $\omega(T) := \sum_{k \in K(T)} \omega(k)$ $\quad (K(T) =$ Kantenmenge des Baums)
heisst **minimal aufspannender Baum**.

$\rightsquigarrow$ **Frage:** Wie ist ein minimaler Spannbaum zu finden? Gesucht ist ein Algorithmus.
Bemerkenswert dabei ist, dass eine sehr grossen Zahl von möglichen Bäume in einem vollständigen Graphen mit paarweise verschiedener Kantengewichtung existieren. Z.B. sind die Pfade, welche alle Punkte besuchen, die Bäume mit der grössten Höhe. Davon gibt es $\frac{1}{2}\,n!$, wenn man die Umkehrbarkeit der Pfade in Betracht zieht. Um eins kürzere Bäume, d.h. solche mit einer Verzweigung, gibt es $\frac{1}{2}\,n!\,(n-2)$

u.s.w.. Man sieht daher sofort, dass die totale Anzahl Möglichkeiten hier mit n überexponentiell ansteigt. Die genaue totale Anzahl der Möglichkeiten $t(n)$ auszurechnen sprengt den hier gesetzten Rahmen. In der Literatur (vgl. *Manfred Brill* (Bibl.: brill) p. 235) wird die exakte Formel $t(n) = n^{n-2}$ angegeben. Damit wird z.B. $t(100) = 100^{98} = (10^2)^{98} = 10^{196}$. Nehmen wir diese Zahl in Sekunden, so ergibt das etwa $2.3\,10^{178}$ mal das Alter des Universums. Es ist daher unvorstellbar, dass alle Spannbäume eines Graphen mit 100 Ecken einmal erzeugt werden können. Umso eindrücklicher ist es, dass man bereits mit einer einfachen, bestechenden Idee einen Algorithmus entwickeln kann, der das Problem löst.

21.2.7 Greedy–Algorithmus

Greedy (englisch) meint „gierig“, d.h. „nimm was du kannst“. Bei diesem Algorithmus ordnen wir erst die Kanten nach absteigendem resp. aufsteigendem Gewicht. Dabei können natürlich zwei verschiedene Kanten dasselbe Gewicht haben. Dazu gibt es Sortieralgorithmen, z.B. „Quicksort“. (Siehe Seite 187.)
Vgl. dazu z.B. *http* : *//de.wikipedia.org/wiki/Quicksort*

Nun gehen wir beim Greedy–Algorithmus wie folgt vor:

1. Beginne als Start mit einem leeren Baum für eine Konstruktion des Spannbaum: $T = \{\}$
2. Nimm eine Kante mit dem kleinsten Gewicht zum Spannbaum hinzu.
   (Die Kante mit dem kleinsten Gewicht nennen wir auch die **kürzeste** Kante).
3. Loop: Gehe an jeder Ecke von T alle Kanten, welche mit der jeweiligen Ecke inzidieren, nach aufsteigendem Gewicht durch. Wähle unter diese Kanten diejenige Kante aus mit dem kleinsten Gewicht (die kürzeste also). Kontrolliere jeweils, ob bei Hinzunahme der nächsten Kante k_j ein Untergraph von $G(E, K, \omega)$ entsteht.
4. Falls die letzte Frage bejaht worden ist und kein Kreis entstanden ist, so erweitere T um k_j.
5. Beende den Loop, wenn alle Ecken des Graphen erreicht sind.
6. Ausgabe des Spannbaums (gewählte Kanten).

Bemerkung: Mit der Greedy–Strategie lassen sich auch andere Probleme lösen. Z.B. das Problem, den Baum mit dem grössten Gewicht aufzufinden. In der Regel ist bei Der Greedy–Strategien nur eine suboptimale Lösung zu erwarten. Betreffend dem Minimierungsproblem der Gewichte haben wir jedoch Glück, wie der Kruskal–Algorithmus zeigt (siehe unten). Vgl. zur optimalen Lösung *http* : *//de.wikipedia.org/wiki/Greedy-Algorithmus* .

Man könnte sich hier auch die Frage stellen, ob es z.B. im Modellfall des Eisenbahnnetz–Graphen möglich ist, neue Ecken in den Graphen einzufügen, welche Schienenverzweigungen darstellen, so dass streckenweise zwei bisherige getrennte Kanten (Schinenstrecken) zusammenfallen und deswegen die Gesamtstrecke noch kürzer wird. Geht man z.B. von einem Reckteckgraphen aus, so könnte man die Kanten, als wären es Gummiseile, nach innen deformieren, bis sich überall je zwei Kanten über die ganze Strecke berühren (d.h. zusammenfallen). Die Lösung des Problems zeigt, dass damit eine noch kürzere Gesamtstrecke erreicht wird als bloss mit Kanten und Diagonalen im Rechteck. Die grosse Frage hier besteht jedoch darin, wie man unter den unendlich vielen möglichen Verzweigungspunkten in der Landschaft die besten auswählen soll (Platzierungsproblem)...
Dieses Problem der kürzesten Verbindungen verlangt nach Methoden der Analysis. Es kann nicht mittels der Graphentheorie gelöst werden.

Statt weiter den allgemeinen Greedy–Algorithmus zu betrachten, ist es nun viel nützlicher, sich zwei Spezialfällen zuzuwenden. Den einen wollen wir dann etwas mehr studieren.

21.2.8 Kruskal–Algorithmus

Zwei Spezialfälle des Greedy–Algorithmus sind die Algorithmen von **Kruskal** und von **Prim**, Vgl. auch:
http : //de.wikipedia.org/wiki/Algorithmus_von_Kruskal
http : //de.wikipedia.org/wiki/Algorithmus_von_Prim

Wir wollen uns hier des beschränkten Raumes wegen nur mit dem Kruskal–Algorithmus beschäftigen. Damit bestimmen wir den aufspannenden Baum wie folgt:

1. Schritt 1: Sortiere die Kanten nach absteigendem resp. aufsteigendem Gewicht, wie beim allgemeinen Greedy–Algorithmus.
2. Schritt 2: Beginne mit einem leeren Baum als Start für eine Konstruktion des Spannbaum: $T = \{\}$
3. Loop, Schritt k: Wähle unter den nicht besuchten Kanten, welche mit den bereits gewählten Ecken inzidieren, die kürzeste aus (resp. eine davon, wenn es mehrere gibt). Falls bei der Hinzunahme der gewählten Kante zu den bereits vorher gewählten ein Kreis entsteht, so verwerfe die Kante (wegstreichen). Sonst füge die Kante zum Graphen hinzu. Streiche so alle inzidierenden Nachbarkanten aus $G(E, K, \omega)$ weg, welche mit den bereits gewählten einen Kreis ergeben.
4. Schritt $k = n$: Falls damit alle Ecken von $G(E, K, \omega)$ besucht worden sind: Stop! Sonst $k < n$: nächster Loopdurchlauf.
5. Ausgabe des Spannbaums resp. der gewählten Kanten.

Betreffend des durch diesen Algorithmus erreichten Optimums resp, Minimums gilt der Satz:

Satz:

Vor.:

$G(E, K, \omega)$ bewerteter zusammenhängender Graph, $n = |E|$.

Beh.:

Der Kruskal–Algorithmus bestimmt einen minimalen Spannbaum.

Beweis:

Sei T_K der durch den Kruskal–Algorithmus gewonnene Spannbaum und T irgend ein anderer Spannbaum von $G(E, K, \omega)$. Wir wollen zeigen:

$$\omega(T_K) = \sum_{k \in T_K} \omega(k) \leq \omega(T) = \sum_{k \in T} \omega(k)$$

Sei dabei T_K gegeben durch die nach aufsteigenden Gewichten geordnete Kantenfolge $k_1, k_2, \ldots, k_{i-1}, k_i, \ldots, k_{n-1}$ und T sei gegeben durch die ebenfalls nach aufsteigenden Gewichten geordnete Kantenfolge $k_1, k_2, \ldots, k_{i-1}, m_i, \ldots, m_{n-1}$. Der Algorithmus erzwingt nun die Beziehnung $\omega(k_i) \leq \omega(m_i)$. Wir bilden die Kantenfolge $k_1, k_2, \ldots, k_{i-1}, k_i, m_i, \ldots, m_{n-1}$. Diese muss einen Kreis enthalten mit einer Kante $m_j,\ j \geq i$ sowie mit der Kante k_i, denn k_i verbindet eine Ecke von T mit einer andern solchen Ecke auf neue Weise, und bis zum Index $j-1$ stimmen die beiden Graphen G und T_K ja überein. Weiter gilt: $\omega(k_i) \leq \omega(m_j),\ j \geq i$. Streichen wir nun die erwähnte Kante m_j aus dem entstandenen Graphen heraus, so entsteht wieder ein Spannbaum T_1 mit $K(T_1) = (K(T) \cup \{k_i\}) \setminus \{m_j\}$. Das Gewicht von $K(T_1)$ wird wegen der bei den Manipulationen benutzten gewichteten Kanten entweder kleiner oder bleibt gleich. Nun können wir dasselbe Verfahren des Kantenaustausches auch auf das paar (T_1, T) anwenden u.s.w.. In endlich vielen Schritten entsteht so aus T über eine Folge $T_1, T_2, \ldots$ schliesslich T_K mit

einem Gewicht, das in allen Teilschritten jeweils kleiner oder gleich dem Gewicht von T geworden resp. geblieben ist. Damit ist die Behauptung des Satzes verifiziert. ☺

21.2.9 Minimale Pfadlänge, Dijkstra–Algorithmus

Zur Problemstellung

Eine andere Frage neben derjenigen nach dem minimal gewichteten Spannbaum ist die folgnde:

Problem: Gegeben sind ein ungerichteter, zusammenhängender, bewerteter Graph $G(E, K, \omega)$ $(n = |E|)$ und darin zwei Ecken u und v. Gesucht ist der kürzeste (minimal gewichtete) Verbindungsweg zwischen u und v. Dabei sei $\omega : \ K \longmapsto \ \mathbb{R}_0^+ = [0, \infty)$ vorausgesetzt (keine negativen Strecken!).

Sei demnach **gegeben**: $G(E, K, \omega), \ \omega : (k_i) \geq 0$. Und sei $P(u, v) = (u, v_1, v_2, \ldots, v_n, v)$ ein Pfad resp. ein Weg von u nach v.

Definition: $L(P) := \sum\limits_{k \in P(u.v)} \omega(k) :=$ **gewichtete Länge** des Weges $P(u, v)$.

Das Auffinden von $Min(L(P))$ wird nun durch den Dijkstra–Algorithmus ermöglicht, welcher nachstehend beschrieben ist:

Dijkstra–Algorithmus

Gegeben sei ein bewerteter, zusammenhängender Graph $G(E, K, \omega, \ |E| = n, \ \omega; \ K \longmapsto \ [0, \infty)$. Weiter seien zwei Ecken $z, v \in E$ gegeben (beliebig, aber fix gehalten).
Der Dijkstra–Algorithmus bestimmt unter diesen Voraussetzungen einen Baum T, welcher einen eindeutigen Weg W von u nach v minimaler Weglänge L enthält. Hier eine Beschreibung, vgl. auch
http : //de.wikipedia.org/wiki/Dijkstra-Algorithmus

1. Schritt 1: Sortiere die Kanten nach absteigendem resp. aufsteigendem Gewicht.
2. Schritt 1: Wähle $u = u_0, \ E_0 = \{u_0\}, \ K_0 = \{\}, \ L(K_0) = 0$. Setze $L(u_0) := 0$.
3. Loop, Schritt i: Sei $E_i = \{u_0, u_1, \ldots, u_i\}, \ K_i = \{k_1, \ldots, k_i\}$.

   Falls $i = n \rightsquigarrow$ Stop!

   Evaluation des Leitparameters $f(k)$:
   $\forall$ *Kanten* $k = vw$ *mit* $v \in E_i, \ w \in E \setminus E_i$: Bestimme $f(k) := L(v) + \omega(k)$.
   Wähle $\tilde{k} = \tilde{v}\tilde{w}$ mit $f(\tilde{k}) = Min(f(k))$.

   Indexverschiebung:
   Setze: $u_{i+1} := \tilde{w}, \ k_{i+1} := \tilde{k}, \ E_{i+1} := E_i \cup \{u_{i+1}\}, \ K_{i+1} := K_i \cup \{k_{i+1}\}, \ L_{i+1} := f(\tilde{k})$

   (Damit sind E_i, K_i und L_i rekursiv definiert.)
   Wiederhole den Loop bis zum Stop (endlich viele Schritte).
4. Ausgabe von E_n, K_n und L_n.

Nun können wir den folgenden Satz beweisen:

Satz: Unter den oben gemachten Voraussetzungen für u und v sowie für die erwähnten zusammenhängenden bewerteten Graphen gilt:

Der Dijkstra–Algorithmus bestimmt einen Spannbaum T derart, dass der darin enthaltene eindeutige Weg von u nach v immer der minimale Weg von u nach v im gewichteten Graphen ist.

Beweis: Da bei diesem Algorithmus alle n Ecken des Graphen besucht werden und wegen $w \in E \setminus E_i$ keine Ecke zweimal besucht werden kann, entsteht durch die bei jedem Schritt gefundene, die neuen Ecke mit den alten Ecken verbindende Kante ein Spannbaum.

Wir führen einen Induktionsbeweis über die Indizes der endlichen Menge der Kanten K_n des Baumes.

Verankerung: Der erste Loopdurchlauf liefert eine Kante $k_1 = u_0u_1$ mit $u = u_0$ fix und $L(u_1) := L_1 := 0$

Vererbung; Voraussetzung:

Sei $T_i(E_i, K_i)$ der bis zum Konstruktionsschritt i konstruierte Baum mit minimaler Gewichtssumme L_j, $j \leq i$, für alle in $G(E, K, \omega)$ möglichen und von u_0 ausgehenden Pfade zu den Punkten u_j in $T_i(E_i, K_i)$.
(L_i entsteht durch Aufsummierung der $\omega(k)$ unter Beachtung der Minimalitätsbedingung
$f(\tilde{k}) = Min(f(k)) = Min(L(v) + \omega(k))$.)

Vererbung; Behauptung und Beweis:

Im folgenden Schritt wird nun die nächste Kante $\tilde{k} = k_{i+1} = \tilde{v}\tilde{w} = u_ju_{i+1}$ und damit der Untergraph $T_{i+1}(E_{i+1}, K_{i+1})$ des Spannbaums $T_n(E_n, K_n)$ konstruiert (j optimal, $j \leq i$). Für u_{i+1} gilt nun ebenfalls die Minimalitätsbedingung $f(\tilde{k}) = f(u_j\tilde{u}_{i+1}) = Min(L(u_j) + \omega(k))$. Damit ist der Weg W_0 von $u = u_0$ nach $\tilde{w} = u_{i+1}$ in $T_{i+1}(E_{i+1}, K_{i+1})$ minimal. Frage: Ist W_0 nur lokal in $T_{i+1}(E_{i+1}, K_{i+1})$ oder auch global in $G(E, K, \omega)$ minimal? Dass die die globale Minimalität zutrifft, zeigen wir jetzt indirekt.

Wir nehmen an, dass es in $G(E, K, \omega)$ einen anderen Weg $H \neq W_0$ von minimaler gewichteter Länge zwischen u_0 und $u_{i+1} = \tilde{w}$ gibt mit $L(H) < L(W_0)$. Dann muss es in der durch den Index gegebenen Rangfolge eine letzte gemeinsame Ecke $h = u_s \in W_0$, $h = u_s \in H$ geben, deren Nachfolger $u_{s+1} \in W_0$ nicht in H liegt und deren Nachfolger $h_{s+1} \in H$ nicht zu W_0 gehört. Sei die Kante $u_sh_{s+1} := k_{h,s}$. Da H von minimaler gewichteter Länge sein muss, sind seine beiden bei $h = u_s$ trennbaren Teilwege H_1 und H_2 ebenfalls minimal. (H_1 ist gegeben durch $u_0, u_1, \ldots, u_s = h$ und H_2 durch $h_s, h_{s+1}, h_{s+2}, \ldots, h_{s+m}, u_{i+1}$.) Ebenso wird durch $h = u_s$ auch W in zwei Teilwege W_1 und W_2 getrennt. ($W_1 = H_1$ ist gegeben durch $u_0, u_1, \ldots, u_s = h$ und W_2 durch $u_s = h_2, u_{s+1}, \ldots, u_i, u_{i+1}$.)
Aus $L(H) < L(W_0)$ und $W_1 = H_1$ folgt nun $L(u_sh_{s+1}) = L(k_{h,s}) \leq L(H_2) < L(W_2)$. Da die Punkte von W_2 durch Minimierung der Abstände von Punken ausserhalb W zu Punkten von W, vermehrt durch den Abstand zu u_0, gewonnen worden sind, müsste damit h_{s+1} unter den Punkten von W_2 anzutreffen sein, was der Annahme widerspricht. $\rightsquigarrow$ $L(H) \geq L(W_0)$ ☺

Vgl. auch *http://de.wikipedia.org/wiki/Dijkstra-Algorithmus*

21.2.10 Das Problem des Handlungsreisenden

Problem und Lösungsstrategien

Problem: Das Problem des Handlungsreisenden (TSP, engl. Traveling Salesman Prolbem) ist ein Optimierungsproblem: Welchen Weg wählt der Handlungsreisenden am besten, damit eine Rundreise möglichst kurz wird, auf der er eine Anzahln in einem Gebiet verstreut wohnender Kunden besuchen muss?

Zur Lösung dieses Problems bietet sich die Graphentheorie an. Der Handlungsreisenden startet beim Knoten A_1, besucht alle Kunden (Knoten A_k) je einmal und kehrt dann wieder zu A_1 zurück. Dabei soll die zurückgelegte Gesamtdistanz minimal sein. Der Handlungsreisende bewegt sich daher auf einem Hamiltonkreis in einem zusammenhängenden, durch die Distanzen bewerteten Grahphen und sollte alle Ecken genau einmal im Graphen besuchen. $\rightsquigarrow$

Definition: Beim **Problem des Handlungsreisenden (TSP)** ist ein vollständiger, zusammenhängender, bewerteter Graph gegeben, d.h. ein K_n mit einer Kantenbewertungsfunktion $\omega : K \longmapsto [0, \infty)$. Gesucht ist ein Hamiltonkreis in K_n mit minimal gewichteter Länge.

Bemerkung: Statt die Distanzen spielen bei der Bewertung oft die Reisekosten pro Kante eine grössere Rolle. Üblicherweise kann man diese Kosten durch eine symmetrische Matrix darstellen.

Lösungsstrategien:

Eine ungünstige Lösungsstrategie wäre, bei n Knoten und damit $\frac{n\,(n-1)}{2}$ Kanten (Anzahl Diagonalen in einem n–Eck inlusive den Aussenkanten) alle Möglichkeiten durchzurechnen und darauf fussend das Minimum zu bestimmen.
In der Praxis verwendet man jedoch oft heuristische, also nicht exakt mathematische Methoden. Damit ist dann auch nicht unbedingt ein absolutes Minimum garantiert, was eine nur suboptimale Lösungen bedeutet.
Z.B. kann man einen minimal aufspannenden Baum verwenden. Denn lässt man in einem Kreis (hier ein Hamiltonkreis) irgend eine Kante weg, so ergibt sich ein Baum. Lässt man aber eine andere Kante weg, so bekommt man einen andern Baum. Unsere Crux ist, dass wir schon einen Algorithmus kennengelernt haben um einen Baum mit minimaler totaler Bewertung zu erzeugen. Wir sollten aber einen Hamiltonkreis und nicht nur einen Baum erzeugen... Und falls wir von einem Baum ausgehen, so stellt sich die Frage, wie man diesen Baum in einen Hamiltonkreis verwandeln könnte: Wo soll man ihn schliessen, wie ihn umwandlen?

MST–Heuristik–Algoritumus

1. Konstruiere im gegebenen zusammenhängenden, bewerteten, vollständigen Graphen einen Baum mit minimaler totaler Bewertung.

2. Verdoppele alle Kanten. Damit entsteht ein Eulergraph T_E.

3. Wähle in T_E einen Eulerkreis $C = \{v_1, v_2, \ldots, v_n\}$.

4. Überspringe bereits durchlaufene Ecken (durch „Kurzschliessen“ der beiden aktuellen, mit der zu überspringenden Ecke inzidierenden Kanten). Dadurch wird der Eulerkreis C_E zu einem Hamiltonkreis C_H.

(„MST“: Engl. Minimal Spanning Tree)

21.2.11 Mit dem Computer erzeugte Beispiele

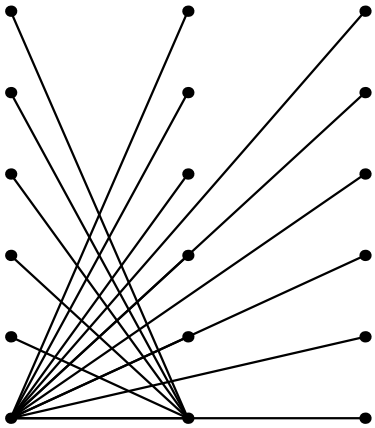


Abb. 34: Minimaler Spannbaum

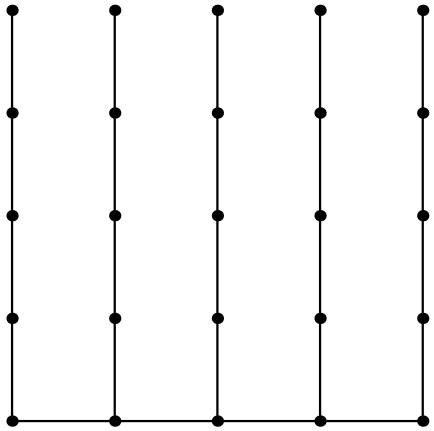


Abb. 35: Spannbaum mit kürzesten Pfaden

Beim rechts gezeigten Graphen ist der Bezugsgraph der Koordinatengittergraph 5×5 gegeben. Darin werden die kürzesten Pfade gezeigt.

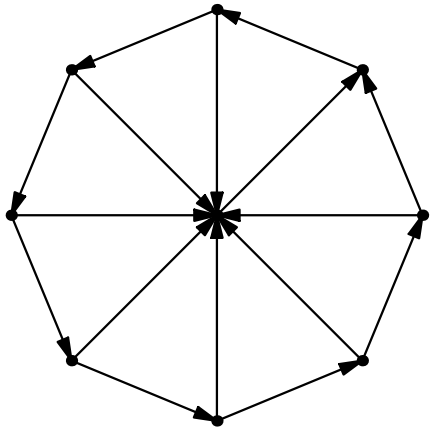


Abb. 36: Rad–Graph

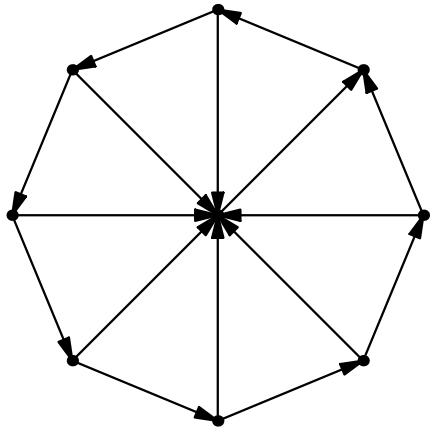


Abb. 37: De Bruijn–Graph

Vgl. dazu *http* : *//mathworld.wolfram.com/CirculantGraph.html*
swie *http* : *//en.wikipedia.org/wiki/De_Bruijn_graph*

Zu diesem Kapitel empfohlene Literatur vgl. (1) *Manfred Brill* (Bibl.: brill),
(2) *Dörfler/Peschek* (Bibl.: doerflerpeschek) sowie (3) Wikipedia (momentan kostenloses Internetlexikon):
http : *//de.wikipedia.org/wiki/Graphentheorie*

21.3 Planare Graphen, Färbungen, Matching

21.3.1 Grundlagen

Definition: Ein Graph heisst genau dann **planar**, wenn es für ihn eine Darstellung in der Ebene ohne Brücken gibt. Also wenn er keine sich kreuzende Kanten hat, sodass die Kreuzungspunkte keine Knoten sind.

Achtung: Die Darstellung eines Graphen ist nicht eindeutig. Oft lassen sich bei einer gewissen Darstellung auftretende Brücken durch Verlagerung der Kanten eliminieren. Jedoch funktioniert das nicht immer. Wir werden unten sehen, dass zwar K_4 planar ist, K_5 jedoch nicht mehr

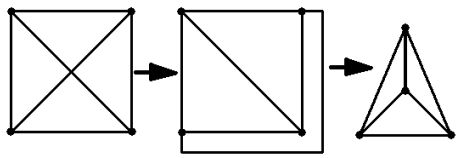


Abb. 38: K_4 verschieden dargestellt

Bsp.: Der vollständige Graph K_4 lässt sich auf verschiedene Weisen darstellen. (Vgl. Skizze nebenan.)
Dass es sich bei diesen Darstellungen um denselben Graphen handelt, ist nicht unbedingt auf den ersten Blick ersichtlich. Die eingeschlossenen Flächenstücke sind bei den verschiedenen Darstellungen nicht immer dieselben. Anzahl und Nachbarn solcher Flächen können verschieden sein oder andere Formen aufweisen. Zudem zeigt die linke Darstellung eine Brücke (oder ein nicht beachteter Knoten in der Mitte).

Zu einem planaren Graphen gehören übrigens eine Anzahl begrenzte, innere Flächenstücke, die **Facetten**, sowie die äussere, unbegrenzte Fläche.

Die folgende Formel **Eulerformel, Polyederformel** wird uns aber zeigen, dass bei einer konstanten Zahl von Ecken (Knoten, ohne Brücken!) und Kanten auch die Gesamtzahl der Flächen immer dieselbe bleibt. Sie ist ein nützliches Hilfsmittel zum Studium von Graphen bezüglich der Anzahl dieser Knoten, Kanten und Flächen. (Diese Formel kann man allgemeiner für topologische Körper eines gegebenen Geschlechts formulieren. Hier sehen wir die Projektion von Körpern in die Ebene.)

Wir betrachten dazu einen Graphen $G(E, K)$ mit $|E|$ = Anzahl der Ecken, $|K|$ = Anzahl der Kanten, $|F|$ = Anzahl der Flächen.

Satz: (Formel von Euler)

Vor.: Gegeben ein planarer, zusammenhängender, einfacher Graph

Beh.: $|E| - |K| + |F| = 2$

Beweis:

1. Sei G ein isolierter Punkt. Dann ist $|E| = 1,\ |K| = 0,\ |F| = 1 \Rightarrow |E| - |K| + |F| = 2$

2. Sei G ein Baum $\rightsquigarrow$ $|F| = 1,\ |K| = |E| - 1 \ \Rightarrow\ |E| - |K| + |F| = 2$

3. Sei G kein Baum. Dann enthält er einen Kreis. Entfernt man darin eine Kante durch aufbrechen eines Kreises so, dass mindestens noch ein Baum bleibt, so verschmeltzen zwei Flächen zu einer. Die Anzahl Flächen und die Anzahl Kanten nimmt somit je um 1 ab. Der Wert von $|E| - |K| + |F|$ ändert dadurch also nicht. In endlich vielen Schritten gelangt man mittels dieses Verfahren zu einem Baum $\rightsquigarrow$ $|E| - |K| + |F| = 2$.

Konsequenz: $|E| - |K| + |F| = 2$ besagt, dass bei gegebenem $|E|$ und $|K|$ auch $|F|$ bestimmt ist. Das bedeutet, dass die Anzal Ecken, Kanten und Flächen nicht von der Darstellung abhängig sein können, falls der Graph planar bleibt. Weiter kann man einen planaren Graphen als Projektion oder Ausbreitung eines elastisch gedachten Körpers auf resp. in eine Ebene auffassen, bei der alle Kanten und Ecken sichtbar bleiben und bei der die vorderste Fläche zur Aussenfläche in der Ebene wird. Daher gilt die Eulerformel so auch für tunnellose Körper im Raum.

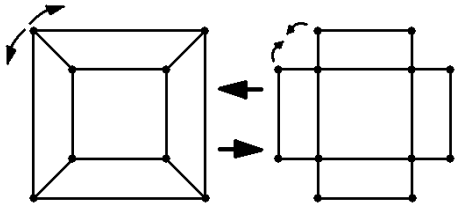


Abb. 39: Verwandlung bei gleichem $|F|$

Eine weitere interessante Beobachtung kann man machen, wenn man (wie in der nebenstehenden Skizze) zwei Aussenecken und Kanten zusammenlegt — oder umgekehrt eine Aussenecke mit der Anschlusskante in je zwei Kanten und Ecken aufspaltet. Bei dieser Operation bleibt $|E| - |K|$ gleich, so dass wegen der Eulerformel auch $|F|$ gleich bleiben muss.

Satz: Für einen planaren, einfachen Graphen mit mindestens 3 Ecken gilt:

$$|K| \leq 3\,|E| - 6$$

Beweis:

1. Im vollständigen Graphen K_2 finden wir $|K| = 1$ und $|E| = 2$. K_2 ist planar.
   Daher wird $|K| = 1 \not\leq 3\,|E| - 6 = 3 \cdot 2 - 6 = 0$. Somit ist $|K| \geq 3$ notwendig.

2. Ist G nicht vollständig, so können wir G durch anfügen von Kanten vollständig machen. Damit wird $|K|$ grösser, d.h. ungünstiger für die Behauptung. Daher beweisen wir die Ungleichung für den Fall des ungünstigeren vollständigen Graphen. Dann ist sie auch für die unvollständigen Graphen bewiesen.

3. G sei also ein planarer, vollständiger Graph mit $|E| \geq 3$. Vollständige Graphen bestehen aus Facetten und einer Aussenfläche. Eine Facette (Innenfläche) ist von mindestens 3 Kanten umgeben, d.h. $|K| \geq 3\,|F|$. Jede Kante gehört zu zwei Flächen, welche die Kante gemeinsam haben. Das gilt auch für die Aussenkanten. Schreibt man also die Flächen in eine Liste und parallel dazu immer auch die begrenzenden Kanten, so kommt jede Kante in der Liste doppelt vor. Addiert man die Anzahl Kanten der Liste, so erhält man daher total $2\,|K|$. Da zu jeder Fläche in der Liste mindestens 3 Kanten gehören, ist daher die Zahl der Kanten in der Liste grösser gleich 3 mal Zahl der Flächen der Liste. $\rightsquigarrow$ $2\,|K| \geq 3\,|F|$. Daher gilt nach der Eulerschen Polyederformel:
   $2\,|K| \geq 3\,|F| = 3\,(2 - |E| + |K|) = 3\,|K| + 6 - 3\,|E| \ \Rightarrow\ 3\,|E| \geq |K| + 6$. ☺

Konsequenz: Bei K_5 ist $|E| = 5,\ |K| = 10$. Damit wird $3\,|E| = 20 \not\geq |K| + 6 = 26$.

Allgemein besitzt der vollständige Graph K_n mit n Knoten $\dfrac{n\,(n-1)}{2} = \dfrac{n^2 - n}{2}$ Kanten (Anzahl Diagonalen in einem n–Eck inlusive den Aussenkanten).

Dann gilt: $3\,|E| = 3\,n \geq \dfrac{n^2-n}{2} + 6 \;\Leftrightarrow 3\,n - \dfrac{n^2-n}{2} - 6 = -\dfrac{1}{2}\,(n-4)(n-3) \geq 0.$
Die letzt Ungleichung ist in $\mathbb{N}$ nur für $n = 3$ und $n = 4$ erfüllbar. (Parabel mit den Nusstellen 3 und 4, nach unten geöffnet.) $\rightsquigarrow$

Korollar: Ein vollständiger Graph ist nur für $|E| \leq 4$ planar.

$\rightsquigarrow$ Vollständige Graphen mit $|E| = n \geq 5$ haben daher in jedem Fall Brücken.

21.3.2 Färbungen, Karthographie

In diesem Abschnitt gehen wir auf Fragestellungen der Kartographie ein. Gegeben sei eine mit n voneinander unterscheidbaren Farben homogen gefärbte Karten. Einer solchen Karte können wir eindeutig einen Graphen zuordnen. Die nachstehende Skizze demonstriert diese **Verwandlung der gefärbten Karte in einen Graphen**. Wie schon früher erwähnt, betrachten wir hier dazu endliche Graphen und andererseits natürlich auch endliche Karten mit endlich vielen gefärbten Teilfächen.

Die erste Figur (links) zeigt eine mit vier Farben gefärbte Karte (red, blue, yellow, green). Die Farbe wird jeweils durch einen Knoten markiert. So gewinnen wir den Farbgraphen der Karte (rechts). Die Kanten haben hier die Bedeutung benachbarter Farben an der Flächengrenze.

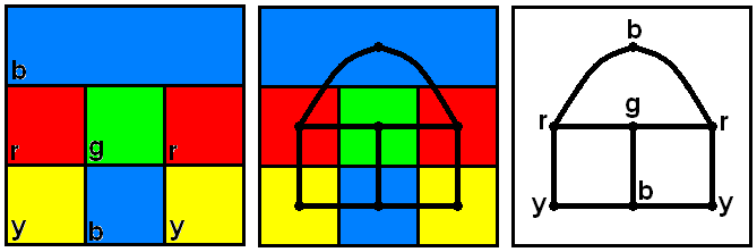


Abb. 40: Farbkarte und Graph

Konsequenz:

Mit dieser Zuordnung $\{\textbf{Karte}\} \longmapsto \{\textbf{planarer Graph}\}$ lassen sich Fragestellungen bezüglich Karten in Graphen–Probleme übersetzen. Denn es existiert offensichtlich zu jeder Karte eine Transformation resp. Abbildung in einen planaren Graphen nach dem gezeigten Muster. Und umgekehrt kann man einen zusammenhängenden, einfachen, planaren Graphen mit zu den Ecken eindeutig zugeordneten Farben immer in eine Karte verwandeln, indem man um jede Ecke derart eine Fläche zeichnet, dass zwischen den Begrenzungen solcher Flächen kein freier Raum bleibt. Dadurch werden die Kanten eindeutig den Grenzen zwischen zwei Flächen zugeordnet. Sei $\{E\}$ die Knotenmenge eines derart zu den Flächen einer Karte zugeordneten Graphen. Damit gilt:

$$\{\text{Flächen}\} \overset{bij.}{\longmapsto} \{E\}$$

Bemerkung: Erwähnenswert ist noch, dass ein Graph nicht einfach sein muss, um dazu eine Karte identifizieren zu können. Schlingen und parallele Kanten ändern an der Flächen nichts, da die Ecken alleine ausreichen, um die Flächen zuordnen zu können. Jedoch stellen die Kanten des Graphen die Grenzen dar.

Parallele Kanten, welche verschiedene Grenzen zwischen Flächen bedeuten, sind in einem planaren Graphen möglich: Wenn es zwischen zwei äusseren Ecken, z.B. einer oberen und einer unteren, aussen herum zwei Kanten gibt, im Beispiel also links und rechts herum. (Vgl. nebenstehende Abbildung.) Hier umschliessen zwei Flächen mit den Farben r und b die restlichen Flächen.

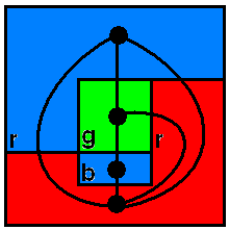


Abb. 41: Farbkarte parallele Kanten.

Problem: Gegeben sei ein gewöhnlicher, zusammenhängender, planarer Graph und dazu die noch ungefärbte Karte. $\rightsquigarrow$ **Frage:** Was ist die minimale Anzahl Farben, mit der sich die Karte einfärben lässt, sodass niemals an einer Grenze zwei gleiche Farben zusammenstossen? — Die Lösung dieses Problem wird durch den **Vierfarbensatz** gegeben.

Definition:

Sei $G(E, K)$ ein einfacher, zusammenhängender, planare Graph und $\mathcal{C}$ = eine endliche Menge von Farben. Eine Funktion $f : E \longmapsto \mathcal{C}$ heisst **Färbung**, wenn gilt: $uv \in K \Rightarrow f(u) \neq f(v)$, d.h. benachbarte Flächen tragen unterschiedlichen Farben.

Die kleinste mögliche Zahl für Färbungen $\chi(G) = Min(|\mathcal{C}|)$ heisst **chromatische Zahl**.

Für endliche Karten ist um 1976 von Kenneth Appel und Wolfgang Haken unter Zuhilfenahme von Coputern der **Vierfarbensatz** bewiesen worden. Vgl. auch *http* : *//de.wikipedia.org/wiki/Wolfgang_Haken* sowie *http* : *//de.wikipedia.org/wiki/Vier-Farben-Satz*.
Der Beweis dieses Satzes ist als erster grösserer Bewies eines mathematischen Satzes bekannt, der von Hand nicht in vernünftiger Zeit hätte geführt werden können. Da beginnt also ein neues Kapitel der Mathematikgeschichte. Der Beweis ist daher hier nicht reproduzierbar. Eine bleibende Frage ist: Wie weit kann man einer Maschine (Computer) vertrauen?

Der vollständige Graph K_4 zeigt, dass 4 Farben notwendig sind (ablesbar). Das Problem ist zu zeigen, dass diese Farben auch in jedem Fall ausreichen. Die Zahl der möglichen Karten ist unbeschränkt, da jede Karte auch erweitert werden kann.

Nun formulieren wir den **Vierfarbensatz**:

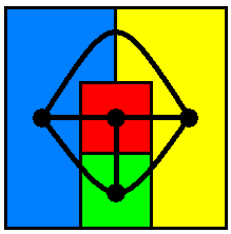


Abb. 42: Farbkarte zum Graphen K_4

Satz:

Vor.:

Gegeben sei ein einfacher, zusammenhängender, planare Graph

Beh.:

Es genügen 4 Farben, um die zum Graphen Karte gehörige Karte im Sinne der obigen Definition zu färben.

Weiter gilt:

Satz: Jeder einfache, zusammenhängende, planare Graph besitzt eine Ecke v, für welche gilt: $d(v) \leq 5$.

Beweis:

Für $|E| = 1$ und $|E| = 2$ ist die Behauptung direkt ersichtlich. Sei daher $|E| \geq 3$. Wir benutzen (vgl. Seite 173): $\sum_{v \in E} d(v) = 2\,|K|$. Wir nehmen nun an: Alle Eckengrade sind ≥ 6. Dann folgt:
$2\,|K| = \sum_{v \in E} d(v) \geq 6\,|E|$. Nun gilt aber $3\,|E| - 6 \geq |K|$ (vgl. Seite **??**.)
$\rightsquigarrow\ 6\,|E| - 12 = 2\,(3\,|E| - 6) \geq 6\,|E| \ \Rightarrow\ -12 \geq 0 \rightsquigarrow$ Widerspruch!

Somit muss die Annahme falsch sein. Es gibt daher mindestens eine Ecke mit Grad ≤ 5.

Statt den Vierfarbensatz nachzuprüfen, können wir hier zeigen:

Satz:

Vor.: G sei ein zusammenhängender, planarer Graph.

Beh.: $\chi(G) \leq 5$

Beweis:

Anhand einer Skizze macht man sich sofort klar: Besitzt der Graph innere Schlingen oder parallele Kanten, so können wir diese weglassen. Den solche Schlingen oder Kanten haben auf die Nachbarschaftsbeziehungen zu andern Flächen keinen Einfluss. Führt eine Schling oder eine parallele Kante zusätzlich um den Graphen herum, so verletzt das die nachträglich verwendete eulersche Polyederformel nicht, denn mit er Hinznahme einer der parallelen Kanten entsteht auch eineneue Fläche. Daher können wir Schlingen und parallele Kanten weglassen, welche keine neuen Flächen erzwingen und uns (abgesehen vom Fall von Seite 201) auf einfache Graphen beschränken.

Nun machen wir eine Induktion über die Anzahl Ecken (endlich viele Schritte). Wir benutzen die eulersche Formel: $|E| + |F| = |K| + 2,\ \ |E| \geq 3$

Verankerung:
Für $|E| = 3$ können wir maximal 3 Farben nehmen. Daher ist hier die Behauptung trivial.

Vererbung; Voraussetzung:
Die Behauptung sei richtig für $n - 1$ Ecken.

Vererbung; Behauptung und Beweis:
G_n habe jetzt n Ecken. Nach dem letzen Satz gibt es eine Ecke mit $d(v) \leq 5$.

Wird diese Ecke v entfernt, so entsteht ein Graph G_{n-1} mit $n-1$ Ecken. G_{n-1} ist ohne Schlingen oder unnötigen parallelen Kanten, zusammenhängend, planar und erfüllt die Beziehung $\chi(G_{n-1}) \leq 5$
Nun betrachten wir die Ecke v. $\rightsquigarrow$ Im Falle, dass v im Graphen weniger als 5 Nachbarn hat, besitzt die zugehörige Fläche in der Karte maximal 4 Nachbarflächen oder Farben. Die 5. Farbe kann also für v verwendet werden. Dann ist $\chi(G_{n-1}) \leq 5$.
$\rightsquigarrow$ Im Falle, dass v im Graphen exakt 5 Nachbarn hat, kann nicht so wie oben geschlossen werden. Es bedarf einer tieferen Betrachtung.

Die Nachbarn von v seien v_1, v_2, v_3, v_4, v_5. Die Zahlen $1, 2, 3, 4, 5$ stehen für 5 verschiedene Farben. Wir nehmen nun an, dass es von v_1 nach v_3 einen alternierenden Weg gibt, auf dem sich die Farben 1 und 3 ständig abwechseln nach dem Prinzip $1, 3, 1, 3, 1, 3, 1, \ldots, 1, 3$. Ebenso soll angenommen werden, dass es von v_2 nach v_4 einen solchen alternierenden Weg gibt mit der Farbsequenz $2, 4, 2, 4, 2, 4, \ldots, 2, 4$. Zwei solche Wege müssen sich aber kreuzen, ohne sich in einer Ecke zu begegnen, denn sie haben keine gemeinsame Ecke mit derselben Farbe. Das bedeutet, dass es in diesem Graphen eine Brücke geben müsste, womit der Graph nicht mehr planar wäre. Dies kann aber nicht sein.

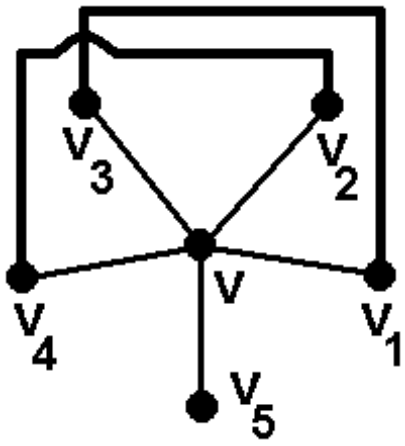


Abb. 43: Knoten um v

Somit kann es keine zwei derartige Wege geben. Angenommen, der alternierende Weg von v_1 nach v_3 existiere nicht. (Andernfalls könnten wir für den Weg von v_2 nach v_4 die Argumentation führen.) Wenn wir nun z.B. in v_3 der Farbe 3 mit der Farbe 1 austauschen und auf allen von dieser Ecke ausgehenden alternierenden Wege mit Farbsequenzen der Art $3, 1, 3, 1, \ldots$ immer die Farbe 1 duch die Farbe 3 und die Farbe 3 durch die Farbe 1 ersetzen, so hat das keinen Einfluss auf den Nachbarpunkt v_1 von v. Durch diesen Prozess wird auch $\chi(\mathcal{C})$ nicht grösser. Nun haben wir es erreicht, dass unter den Nachbarn von v zwei dieselbe Farbe haben, also unter diesen Nachbarn nur noch vier Farben vorkommen. Die fünfte Farbe ist damit frei für v. Damit ist auch für G_n die chromatische Zahl $\chi(\mathcal{C}) \leq 5$. ☺

21.3.3 Bipartite (paare) Graphen

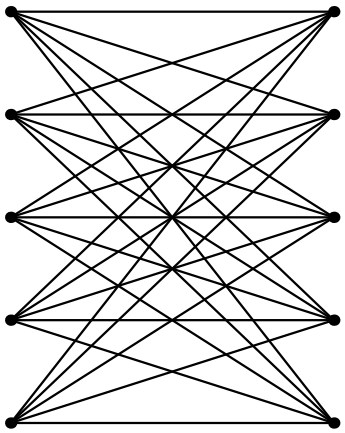


Abb. 44: Bipartiter Graph

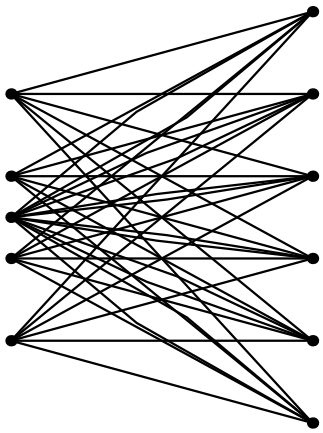


Abb. 45: Bipartiter Graph

Diese Skizzen zeigen vollständige Graphen.

Definition:

$G(E,K)$ heisst **bipartit** oder **paar** $\Leftrightarrow E = S \cup T,\ S \cap T = \{\}$ mit: $\forall_{uv \in K} :\ u \in S\ \wedge\ v \in T$.
(D.h. S und T stiften eine Partition auf E.)

$G(E,K) = K_{m\,n}(E,K)$ mit $|S| = m$ und $|T| = n$ heisst **vollständig bipartit**, wenn $K_{m\,n}$ alle Kanten zwischen S und T enthält.

Nebenstehend ist ein unvollständiger, nicht zuszusammenhängender, bipartiter Graph gezeigt.

Solche Graphen kann man auf verschiedene Weise als Darstellung von Paarbildungen interpretieren. Z.B. Paare die sich über den Besitz oder über einen gegenseitigen Vertrag definieren: (Computer, Mitarbeiter), (Bürger, Bücher), (Frau, Mann), (Hund, Hundehalter) u.s.w..

Nun gilt der folgende Satz für bipartite Graphen:

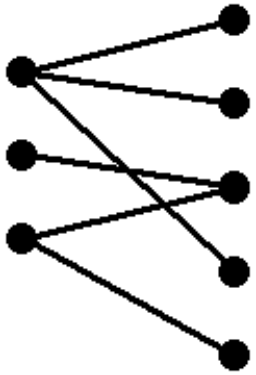


Abb. 46: Unvollst., n. zus'h. bipartit

Satz: $G(E,K)$ bipartit $\Leftrightarrow$ Alle enthaltenen Kreise haben gerade Länge.

Beweis:

1. $\Longrightarrow$: Sei G bipartit $\Rightarrow$ Jeder Kreis mus alternierend sein nach dem Prinzip: $s_1t_1, t_1s_2, s_2, t_2, \ldots, s_jt_j, t_js_1$ (hin und her und hin und her...)
   $\Rightarrow$ Die Länge jedes Kreises ist gerade.

2. $\Longleftarrow$: Sei G ein Graph, der nur Kreise gerader Länge enthält. Sei G zusammenhängend resp. eine zusammenhängende Komponente eines solchen Graphen. Wir betrachten eine Ecke u und konstruieren damit zwei Mengen mit Ecken aus G: Zuerst versorgen wir u in S. Dann schlagen wir, falls es weitere Ecken gibt, alle $v \in E$ zu S, für die die Länge des kürzesten Weges $d(u,v)$ gerade ist. Jene $v \in E$, für die $d(u,v)$ ungerade ist, schlagen wir zu T.
   Nun nehmen wir an, das es in S und T benachbarte Ecken gibt. Z.B. seien $v, w \in T,\ v, w$ benachbart. Dann gilt: $vw \in K$. Da u ein Punkt aus S ist, sind nun $d(u,v)$ und $d(u,w)$ ungerade. Wegen der Annahme $(d(v,w) = 1)$ ist dann die gerade Differenz $|d(u,v) - d(u,w)| \leq 1\ \Rightarrow\ |d(u,v) - d(u,w)| \leq 0\ \Rightarrow\ d(u,v) = d(u,w)$
   Sei nun W_1 ein Weg von u nach v der minimalen Länge (Distanz!) $d(u,v)$ und W_2 ein Weg von u nach w der minimalen Länge (Distanz!) $d(u,w)$ und sei x die letzte gemeinsame Ecke dieser beiden Wege von u aus. Wegen $d(u,v) = d(u,w)$ muss nun auch $d(x,v) = d(x,w)$ gelten. Dann ist der Weg von x über v und w nach x ein Kreis. Seine Läge ergibt sich zu $L_C = d(x,v) + d(v,w) + d(w,x) = d(x,v) + 1 + \underbrace{d(w,x)}_{=d(x,v)} = 2\,d(x,v) + 1\ \Rightarrow$ ungerade $\rightsquigarrow$ Widerspruch!
   $\rightsquigarrow$ in T gibt es keine benachbarten Ecken. Ebenso schliessen wir für S. Somit ist G bipartit.

21.3.4 Matching (Paarung) und Anwendungen

Sei $G(S \cup T, K$ bipartit.

Definition:

Eine Kantenmenge $M \subset K$ heisst **Matching** oder **Paarung** $\Leftrightarrow$ Es gibt in M keine Kanten, welche einzident sind.

Ein Matching heisst **vollständig** $\Leftrightarrow \forall_{u \in E}\ \exists_{k \in M} :\ k, u$ sind inzident.

Im nebenstehenden linken Bild zeigt die erste Figur kein Matching, die zweite Figur zeigt ein Mathcing und die dritte ein vollständiges Matching

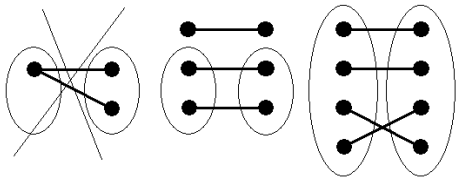


Abb. 47: Diverse Matchings

Eine praktische Problemstellung ist nun die folgende:

Problem: Finde ein möglichst grosses Matching in einem bipartiten Graphen. (Damit sich im Graphen maximal viele unabhängige Eckenpaare identifizieren lassen.)

Zur Behandlung dieser Problemstellung erweitern wir den Begriffsapparat:

Definition:

Gegeben sei der bipartite Graph $G(S \cup T, K)$ mit einem Mastching M. Eine **Ecke** $u \in E$ heisst **frei** bezüglich M, wenn u nicht mit M inzidiert.

Ein Weg W heisst **alternierend** bezüglich M, wenn die Anfangsecken frei sind bezüglich M und jede weitere Ecke mit einer Kante $\in M$ inzidiert.

Um die Vergrösserung eines Matchings verstehen zu lernen, betrachten wir ein Beispiel.

Bsp.:

Sei $S = \{A, B, C, D\},\ T = \{E, F, G, H\}$.
$K = \{\{A, F\}, \{B, F\}, \{B, G\}, \{D, H\}\}$.
$M = \{\{B, F\}, \{D, H\}\}$. Nun ist $\{G, B, F, A\}$ ein alternierender Weg. G und A sind anfangs noch frei.
Damit finden wir ein grösseres Matching $\{\{A, F\}, \{B, G\}, \{D, H\}\}$.

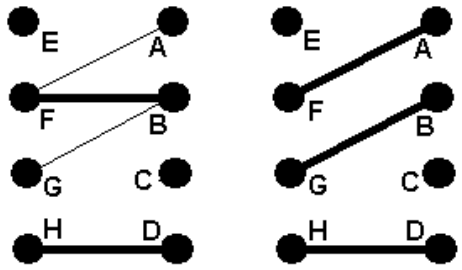


Abb. 48: Vergrösserung eines Matchings

Konsequenz:

Ein Matching ist also vergrösserbar, wenn ein alternierender Weg mit freien Ecken gegeben ist. Das führt uns zu folgendem Rezept zur Lösung des Problems der Matchingvergrösserung:

1. Suche einen alternierender Weg mit freien Ecken.

2. Streiche die enthaltenen Matchingkanten und ersetze diese durch die alternativen Kanten des alternierenden Weges.

Man kann sich hier auch vorstellen, dass wir die Kanten des bestehenden Matchings um ihre Ecken (z.B. diejenigen in S — oder statt die in S diejenigen in T) „umklappt“ oder „die Kanten umschaltet“. Hat das Matching j Kanten, so hat der alternierende Weg $2\,j+1$ Kanten. Lässt man j Kanten aus den Weg weg, so bleiben $j+1$ übrig.

Der folgende Satz ist daher unmittelbar einleuchtend:

Satz: Gegeben sei ein bipartiter Graph $G(S \cup T, K)$ mit einem Mattching M, gebildet durch die Ecken $\{t_1, s_2, t_2, s_3, \ldots, t_{2\,n}, s_{2\,n+1}\}$.
$s_1 t_1 s_2 t_2 \ldots s_{2\,n+1} t_{2\,n+1}$ sei ein alternierender Wer mit freinen Eckpunkten s_1 und $t_{2\,n+1}$.
Bilde nun die folgende Kantenmenge M'
$M' = M \setminus \{t_1 s_1, t_2 s_2, \ldots, t_{2\,n} s_{2\,n+1}\} \cup \{s_1 t_1, s_2 t_2, \ldots, s_{2\,n+1} t_{2\,n+1}\}$

Dann ist M' ein grösseres Matching mit $|M'| = |M| + 1$

Definition: Gegeben sei ein Graph $G(E, K)$.

$C \subset E$ heisst **Eckenüberdeckung**
$\Leftrightarrow \forall_{k \in K}\ \exists_{u \in C}$: k inzidiert mit der Ecke u.

Bsp.: In der nebenstehenden Skizze sind schematisch 4 Besucher gezeigt, die an einem Grill sich mit je einem langen Spiess total 4 Würste holen wollen. Wieviele Besucher können gleichzeitig nach den Würsten stechen ohne sich gegenseitig zu behindern, wenn ein Besucher Vegetarier ist? — Damit es funktioniert, muss ein maximales Matching mit 3 Kanten vorhanden sein. Ein solches gibt es.
Im Graph gibt es zwei Eckenüberdeckungen: Für die Besucher und für die Würste. Bei den Besuchern besteht die Überdeckung aus 3 Elementen, bei den Würsten aus 4. Die minimale Überdeckung hat 3 Ecken.

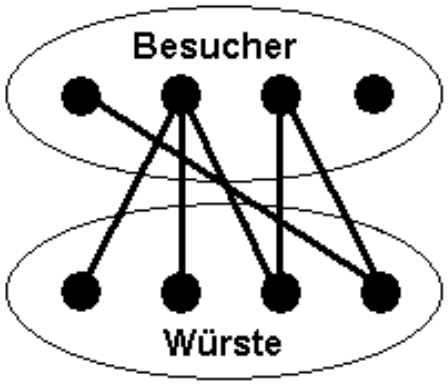


Abb. 49: Grillprolbem

21.3.5 Der Dualitätssatz von König

Satz:

Vor.:

$G(S \cup T, K)$ bipartit.
$|M| := |M_m|$ = maximale Kantenzahl für ein Matching.
$|U| := |E_m|$ = minimale Eckenzahl für eine Eckenüberdeckung.

Beh.:

$$|M_m| = |E_m| \text{ resp. } |M| = |U|.$$

Beweis:

Eigentlich ist dieser Satz unmittelbar einsichtig. Wir führen aber hier trotzdem noch einen kurz gefassten formalen Beweis.

$G(S \cup T, K)$ ist bipartit mit den Partitionen S und T. (Falls G nicht bipartit wäre, dann wäre es noch möglich, einen nicht bipartiten Graphen zu haben, welcher noch freie Ecken besitzt bezüglich M mit inzidierenden Kanten bezüglich $S \times S$ oder $T \times T$. Durch Streichung dieser Ecken zusammen mit ihren Kanten entsteht dann ein bipartiter Graph.)

Sei U = Eckenüberdeckung mit minimale Anzahl Ecken, M = Matching mit maximaler Kantenzahl. Da eine Eckenüberdeckung alle Kanten mindestens einmal trifft, gilt: $|U| \geq |K| \geq |M|$.
Zu zeigen ist: Umgekehrt gilt auch $|U| \leq |M|$. Idee: Konstruiere mit Hilfe von obigem M eine Überdeckung $E_{M,S}$ von U. Wähle zu diesem Zweck zu allen Kanten eine Ecke ($k_i = st \in M,\ \ s \in S,\ \ t \in T$). Wenn in s ein alternierender Weg endet, so wählen wir s. Andernfalls wählen wir t. So entsteht eine Eckenmenge $E_{M,S}$ mit $|E_{M,S}| = |M|$. (Nach Voraussetzung ist M maximal.) Frage: Erhalten wir so eine gewünschte Überdeckung der Ecken? Dann wäre $|U| \leq |E_{M,S}| = |M|$, was wir zeigen wollen.
Nun gehen wir der letzten Frage nach. Zu diesem Zweck sei $k_i = st \in K$ beliebig. Falls $k_i = st \in M$ gilt, so liegt entweder s oder t nach Definition in $E_{M,S}$. Sei daher $\tilde{s}\tilde{t} \notin E_{M,S},\ \ \tilde{s}\tilde{t} \in K$. M ist nun aber das Matching mit der grössten Kantenmenge. Daher müssen wir eine Kante finden können mit entweder $\tilde{s} = s$ oder $\tilde{t} = t$. Denn G ist bipartit und besteht daher aus alternierenden Wegen, aus denen die Mattchinkanten stammen. (Falls die letzte Alternative $\tilde{s}\tilde{t} \notin E_{M,S}$ falsch sein würde, wäre ja $\tilde{s}\tilde{t}$ eine nicht erfasste Matchingkante, im Widerspruch zur Maximalität von M.) Für $t = \tilde{t}$ ist $\tilde{s}\tilde{t}$ ein alternierender Weg und damit $\tilde{t} \in E_{M,S}$. Andernfalls betrachten wir $s = \tilde{s}$. Für $s = \tilde{s} \notin E_{M,S}$ muss dann $\tilde{t} \in E_{M,S}$ gelten nach der Art wie man aus alternierenden Wegen ein Matching bildet. Damit bleibt keine Alternative. $|E_{M,S}|$ muss gleich $|M|$ sein. (Es ist dem Leser überlassen, sich dazu weitere Gedanken zu machen, vgl. auch Lit. „Bibl: brill“.)

21.3.6 Der von Hall

Für den **Heiratssatz** von Hall benötigen wir folgende Definition:

Definition: Sei $N(A) := \{v \in E \mid \exists_{u \in A} : uv \in K\}$ = Menge der Nachbarn v aller Knoten u, welche in A enthalten sind.

Um den nächsten Satz verständlicher zu machen, gehen wir von einer geläufigen Interpretation aus. Sei $S = \{\text{zur Heirat gewillte Damen}\}$ und $T = \{\text{zur Heirat gewillte Herren}\}$. Gleichgeschlechtliche

Heiraten seien bei dieser traditionellen Betrachtung ausgeschlossen. Eine Kante bekommt somit die Bedeutung einer Ehe bzw. eines Ehepaars. Alle Ehepaare bilden ein Matching eines bipartiten Graphen mit $E = S \cup T$, in dem die Kanten zweigeschlechtliche Beziehungen bedeuten. Es leuchtet unmittelbar ein, dass alle Damen nur dann heiraten können, wenn es genügend Herren gibt (und umgekehrt). Das bedeutet, dass es dann für $|S| \leq |T|$ ein Matching mit der gesamten Menge S gibt. Dazu ist notwendig, dass für alle $A \subseteq S$ gelten muss: $|N(A)| \geq |A|$. Die Aussage des Heiratssatzes ist nun, dass die letzte Ungleichung auch eine hinreichende Bedingung ist, dass wir demnach also eine Äquivalenz haben:

Satz: Ein bipartiter Graph $G(S \cup T, K)$ enthält ein Matching von ganz S $\Leftrightarrow \forall_{A \in S} : \ |N(A)| \geq |A|$.

Bemerkung: $|N(A)| \geq |A|$ ist auch bekannt unter dem Namen „Heiratsbedingung“.

Beweis: (Vgl. auch Lit. „Bibl: brill“.)

1. $\underline{\Longrightarrow:}$ Sei G bipartit mit einem Matching von ganz S. Dann gibt es zu jedem $s \in S$ ein $t \in T : \ st \in M$. Zudem gilt: $s_1 \neq s_2 \ \Rightarrow \ t_1 \neq t_2, \ \ s_1t_1, s_2t_2 \in M$. Von jedem $s \in S$ können aber noch weitere Kanten ausgehen. Zudem gilt für alle $i, j : \ s_is_j \notin K$ Daher hat jedes $s \in S$ mindestens einen Nachbarn $t \in T$. Wegen dem Matching für ganz S gilt daher für ein beliebiges $S_j \subseteq S$, das jedes $s_i \in S_j := A$ mindestens einen verschiedenen Nachbarn hat. $\rightsquigarrow \ |N(A)| \geq |A|$

2. $\underline{\Longleftarrow:}$ Sei also $G(S \cup T, K)$ bipartit und $\forall_{A \in S} : \ |N(A)| \geq |A|$. Speziell für $A = \{s_i\}$ ist $|N(\{s_i\})| \geq |\{s_i\}| = 1$. Damit geht von jedem s_i mindestens eine Kante aus. Es gibt daher mindestens ein Matching mit $|M| \geq 1$. Wir müssen jetzt zeigen, dass es damit ein Matching M gibt mit $|S| = |M|$. Wir verfolgen folgendes Konzept: Ist M ein maximales Matching mit $|S| > |M|$ so konstruieren wir mit Hilfe von M einen alternierenden Weg mit freien Ecken in S und damit ein Matching M_1 mit $|M_1| \geq |M|$.
   Sei also $|S| > |M|$. Damit gibt es in S eine Ecke s_i, die mit keiner Kante $k \in M$ inzidiert. Wir numerieren die Ecken nun so, dass $i = 0$ gilt. Wegen $|N(\{s_0\})| \geq |\{s_0\}| = 1$ hat daher s_0 einen Nachbarn $t_1 \in T$ mit $s_0t_1 \notin M$, denn M ist als maximal. Daher muss t_1 eine Ecke einer Kante $s_1t_1 \in M$ sein. Denn andernfalls könnten wir mit s_0t_1 die Menge M vergrössern, diese wäre somit nicht maximal. Nun folgt aus $|N(A)| \geq |A|$ mit $A = \{s_0s_1\}$ sofort $|N(\{s_0, s_1\})| \geq |\{s_0, s_1\}| = 2$. $N(\{s_0, s_1\}$ enthält also mindestens 2 Ecken t_1, t_2. Falls nun t_2 mit keiner Kante des Matchings inzidiert, können wir in M die Kante s_1t_1 durch das Kantenpaar s_0t_1, s_1t_2 ersetzen und das Matching vergrössern. Es war also nicht maximal. Im andern Fall gibt es ein $s_2 \neq s_0, s_1$ mit $s_2t_2 \in M$. Für $\{s_0, s_1, s_2\}$ schliessen wir nun mit der Heiratsbedingung wie vorhin mit $\{s_0, s_1\}$ und erhalten eine Kante t_3 u.s.w.. Nach demselben Muster wie vorhin führt das zu einer letzen Ecke t_j, welche frei sein muss, und wir können wie oben das Matching vergrössern. Dieses Argument benutzen wir, bis M „an die Decke stösst“, d.h. bis $|M| = |S|$ ist. Damit ist die Behauptung bewiesen. ☺

Korollar:

Vor.:

Gegeben: Bipartiter Graph G

Beh.:

Ein Matching $|M|$ ist maximal
$\Leftrightarrow \neg\exists$ alternierender Weg bezüglich M mit freien Ecken.
(D.h. es gibt keinen solchen alternierenden Weg)

21.3.7 Der Ungarische Algorithmus für ein maximales Matching

Das durch obige Sätze gesicherte Wissen können wir nun zu einem Algorithmus „umgiessen“, mittels dem man zu einem gegebenen bipartiten Graphen ein maximales Matching konstruieren kann. Man nennt ihn den **ungarischen Algorithmus**. Gegeben sei ein einfacher, bipartiter Graph $G(S \cup T, K)$.

1. Wir beginnen mit einem beliebigen Matching in G, z.B. $M = \{\}$. Nummeriere alle bezüglich M freien Ecken in S und $T \rightsquigarrow S_f, T_f$.

2. Loop: Wähle ein s_i in S_f. Sei o.B.d.A. $i = 0$. Da der Graph einfach und bipartit ist, gibt es ein $t_j \in T$ mit $s_0 t_j \in K$. Gilt $t_j \in T_f$, so ist $s_0 t_j$ eine neue Matchingkante. M lässt sich durch Hinzunahme dieser Kante vergrössern.
   Andernfalls inzidiert t_j mit einer Kante $k_m \in M$, z.B $k_m = s_m t_j$. Suche nach diesem Muster einen alternierenden Weg bezüglich M. Falls man einen findet, kann man M durch „umklappen “ vergrössern.

3. Im günstigen Fall wird M jetzt vergrössert und die vormals freien Ecken aus S_f, T_f gestrichen.

4. Falls $S_f = \{\}$ ist: Stop und Ausgabe von M.
   Sonst: Ersetze s_i (im ersten Loopdurchlauf s_0) durch das nächste Element $s_{i+1} \in S_f$. Durchlaufe den Loop von neuem.

21.3.8 Der Satz von Kuratowski

Sei K_5 der vollständige Graph mit 5 Ecken und $K_{3,3}$ der vollständige bipartite Graph mit 6 Ecken.
Dann gilt der Satz:

Satz: Ein endlicher Graph ist planar $\Leftrightarrow$
Er enthält keinen Untergraphen (Teilgraphen), der durch Erweiterung von K_5 oder $K_{3,3}$ entstanden ist.

Definition: Dabei verstehen wir unter einer **Graphenerweiterung** das beliebig oft wiederholbare Einfügen von neuen Knoten auf Kanten. Der Graph selbst wird auch als (unechte) Erweiterung seiner selbst verstanden.

Hier endet diese Standardeinführung. Für den Beweis des Satzes von Kuratowski sei auf die Literatur verwiesen.
Vgl. z.B. *http* : *//de.wikipedia.org/wiki/Satz_von_Kuratowski* .

21.3.9 Mit dem Computer erzeugte Beispiele von Graphen

Die folgenden Beispiele sind mit Hilfe von *Mathematica* auf dem Computer erzeugt worden:

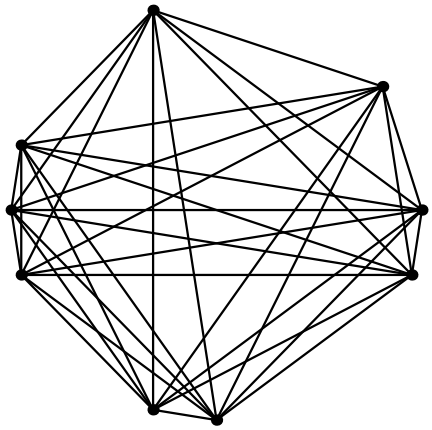


Abb. 50: Maschinenerzeugtes Beispiel

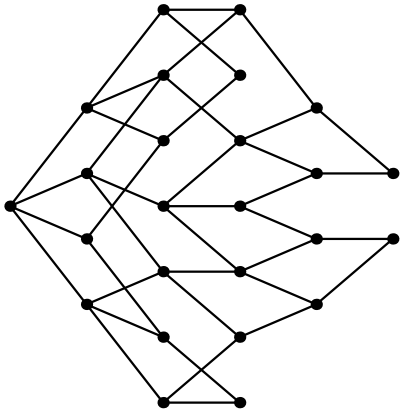


Abb. 51: Maschinenerzeugtes Beispiel

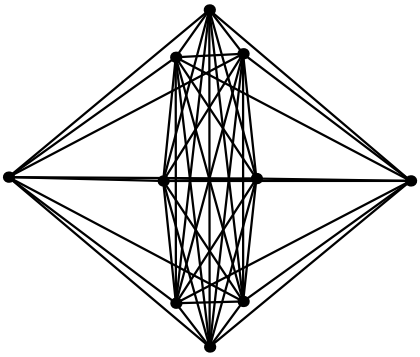


Abb. 52: Maschinenerzeugtes Beispiel

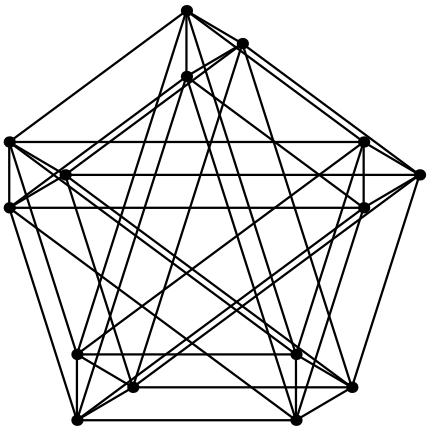


Abb. 53: Maschinenerzeugtes Beispiel

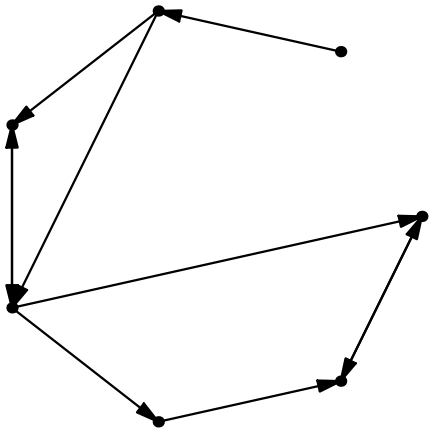


Abb. 54: Maschinenerzeugtes Beispiel

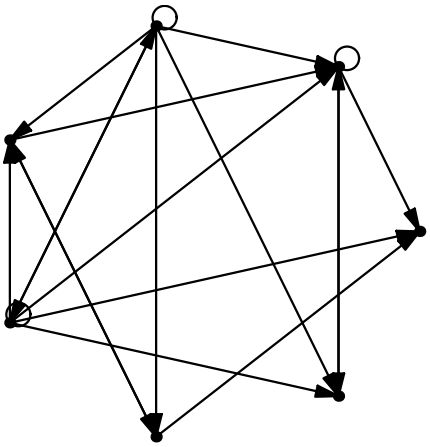


Abb. 55: Maschinenerzeugtes Beispiel

Die letzten beiden Beispiele sind mit dem folgenden *Mathematica*–Code erzeugt worden:
Beispiel links:

```
<<DiscreteMath‘Combinatorica‘;
A=Range[7];B={{1,2},{2,3},{2,4},{3,4},{4,5},{5,6},
{6,7},{7,6},{4,7},{4,3}};
ShowGraph[MakeGraph[A, (MemberQ[B,{#1,#2}])&]];
```

Beispiel rechts:

```
<<DiscreteMath‘Combinatorica‘;
A=Range[7];B=Flatten[Table[Table[{1+Mod[2r+3,s],
1+Mod[5s,2r+3]},{r,10}],{s,1,7}],1];
ShowGraph[MakeGraph[A, (MemberQ[B,{#1,#2}])&]];
```

21.3.10 Literatur

Zu diesen Kapiteln empfohlene Literatur vgl. (1) *Manfred Brill* (Bibl.: brill),
(2) *Dörfler/Peschek* (Bibl.: doerflerpeschek) sowie (3) Wikipedia (momentan kostenloses Internetlexikon):
http : *//de.wikipedia.org/wiki/Graphentheorie*

21.4 Planare Graphen und Polyederkugeln

21.4.1 Ausbreitungsäquivalenz

Ein Polyeder kann man sich aus Gummi denken. Schneidet man ein Loch in eine Fläche, und schneidet man dann diese Fläche, so wie beim nebenstehenden Würfel gezeigt, vom Loch her diagonal auf jede der angrenzenden Ecken zu ein, so kann man das Gummigebilde durch ziehen in die Ebene ausbreiten. Die angeschnittene Fläche soll in der Ebene mit der Aussenfläche des entstehenden Graphen identifiziert werden. Die Schnittkanten werden anschliessend weggelassen.

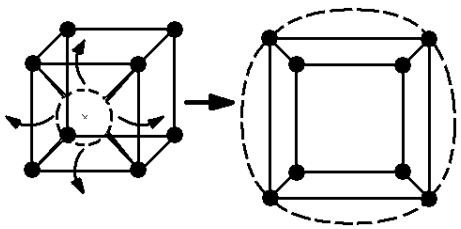


Abb. 56: Ausbreitung eines Würfels

Man sieht sofort, dass bei dieser Transformation in die Ebene keine Ecke, Kante oder Fläche verloren geht. Sogar die eingeschnittene Fläche ist in der Ebene als Aussenfläche wieder vorhanden. Die Polyederflächen gehen bei einer solchen elastischen Dehnung in Flächenstücke in der Ebene über. Die Anzahl Ecken, Kanten und Flächen bleibt demnach bei der **Ausbreitungstransformation** invariant. Da auf der Oberfläche des Polyeders keine Kanten anderswo als in den Ecken miteinander inzidierenden, finden wir ebenso bei den entstehenden Graphen in der Ebene. Jene können daher keine Brücken aufweisen. Sie sind somit einfach und planar. Auch die Rücktransformation existiert nach dem beschriebenen Verfahren bezüglich Ecken–, Kanten– und Flächenzahl eindeutig, denn bei der Ausbreitung haben nie zwei Elemente dasselbe Bild. Dieser Sachverhalt kann schrittweise beschrieben und in einer Induktion über die Anzahl Schritte verifiziert werden. Er ist aber auch unmittelbar evident.

Definition: Eine Transformation wie die eben beschriebene nennen wir **Ausbreitung**, die Rücktransformation nennen wir **Volumeneinschliessung**. Zwei **Polyeder** nennen wir **ausbreitungsäquivalent**, wenn sie durch elastische Dehnung ineinander übergeführt werden können, ohne dass sich die Ecken–, Kanten– und Flächenzahl ändert. Ein **Polyeder** nennen wir **ausbreitungsäquivalent** zu einem einfachen, planaren **Graphen**, wenn sich das Polyeder entsprechend in den Graphen durch Ausbreitung abbilden lässt.

Auch das folgende Lemma ist unmittelbar evident:

Lemma: Die ebenflächig begrenzten räumlichen Polyeder besitzen alle alle einen äquivalenten, einfachen, planaren Graphen.

Die Umkehrung ist nicht richtig, wie man sofort an Trivialbeispielen sieht. Fassen wir z.B. ein beliebiges n–Eck als Graphen mit n Ecken, n Kanten und einer Fläche auf, so ist evident, dass daraus niemals ein volumenumschliessendes Gebilde mit ebenen Flächen werden kann. Man hat hier maximal nur eine ebene n–Eckfläche. Zwar kann man die Aussenfläche eines n–Echs im Raum immer so zurücktransformieren, dass ein Volumen eingeschlossen wird. Doch entweder muss dann die eine der beiden Begrenzungsflächen krumm sein, oder die beiden Begrenzungsflächen fallen zusammen, was ein degeneriertes Volumen (d.h. hier nur eine einzige Fläche) ergibt. Das Resultat einer solchen nicht–degenerierten Rücktransformation nenen wir **Kissen**.
Die Anzahl der Flächen des Polyeders mit der kleinsten Anzahl ebener Flächen ist 4 (Tetraeder).

Ähnlich wie beim n–Eck verhält es sich daher mit Graphen mit zwei oder drei Flächen. Oder mit aneinandergereiten Quadraten wie bei einer Zeile auf einem karierten Blatt Papier. Hier ändert die Sache jedoch, wenn wir (wie vorhin) wieder im Raum **krumme Flächen** zulassen. Z.B. mit einem Kreis und seiner Aussenfläche in der Ebene können wir im Raum ein **Kissen** bilden.

Wenn nun die Ecken–, Kanten– und Flächenanzahl bei der Transformation nicht ändern, so können wir folgern:

Satz: Wird die eulersche Polyederformel für Graphen bewiesen, so gilt sie automatisch auch für die äquivalenten Polyeder und damit für alle Polyeder. Wird sie für Polyeder beweisen, so gilt sie für die äquivalenten Graphen.

21.4.2 Andocken

Das Prinzip

Reguläre Polyeder (platonische Körper), semireguläre Polyeder (archimedische Körper), Prismen, Antiprismen und Johnsonkörper sind besonders interessant, weil man aus ihnen leicht unendlich viele weitere Körper zusammensetzen kann. Im nebenstehenden Beispiel sieht man, wie sich ein Polyeder an ein anderes Polyeder anfügen lässt, wenn die beiden Polyeder ein kongruentes Flächenpaar aufweisen, zu welchem jeder der beiden Körper eine Fläche beisteuert.

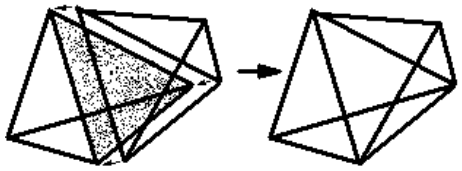


Abb. 57: Andockvorgang

Definition: Die eben gezeigte Zusammensetzungsart nennen wir **andocken**.

Beim Andocken eines Polyeders an ein anderes (durch zusammenfügen zweier Flächen mit je m Ecken) gilt nun wegen der eulerschen Formel $|E_1| - |K_1| + |F_1| = 2$ (beim ersten Polynom) und $|E_2| - |K_2| + |F_2| = 2$ (beim zweiten). $\rightsquigarrow$ $(|E_1| + |E_2|) - m + m - (|K_1| + |K_2|) + |F_1| + |F_2| = 2 + 2 \Rightarrow$ $\underbrace{(|E_1| + |E_2| - m)}_{|E_3|} - \underbrace{(|K_1| + |K_2| - m)}_{|K_3|} + \underbrace{(|F_1| + |F_2| - 2)}_{|F_3|} = 2$ (eulersche Formel erfüllt!).

Folgerung: Beim Andocken zweier Polyeder mit den Ecken–, Kanten– und Flächenzahlen $|E_1|, |K_1|, |F_1|$ sowie $|E_2|, |K_2|, |F_2|$ an einer Fläche mit m Ecken und Kanten entsteht ein Polyeder mit
$|E_3| = |E_1| + |E_2| - m$ Ecken,
$|K_1| + |K_2| - m = |K_3|$ Kanten und
$|F_3| = |F_1| + |F_2| - 2$ Flächen.

Wenn bei einem solchen Andockprozess sich die Polynome durchdrigen, lassen wir die störenden Anteile einfach so weit schrumpfen, bis das Andocken ohne Durchdringung möglich ist. Damit wird die Anzahl der Andockmöglichkeiten grösser. Weil auch Kettenbildungen möglich sind, ist die Anzahl der möglichen Polynome und der dazu äquivalenten Graphen unbegrenzt.

Satz: Die Polyeder sind äquivalent zu einer Teilmenge G_P der einfachen, planaren Graphen mit der Mächtigkeit $|G_P| = \infty$.

Definition: Blasen wir die elastisch gedachten Polyeder derart auf, dass sie Kugelgestalt annehmen, so sprechen wir von **zu den Polyedern äquivalenten Polyederkugeln**.

Polyederkugeln oder Näherungen von solchen, bei denen Flächen in kongruente oder „beinahe kongruente“ Klassen eingeteilt werden können, sind in den Naturwissenschaften und auch z.B. in der Gestaltung (z.B. Architektur) von Interesse.

Korollar: Es gibt unendlich viele verschiedenen Polyederkugeln.

Konsequenzen für die Ecken, Kanten und Flächen

Hier wollen wir uns kurz überlegen, wie ein Andockvorgang die Zahlen $|E|, |K|$ und $|F|$ verändert. Dabei wollen wir auch noch den degenerierten Fall $n = 2$ einschliessen.

Nebenstehend ist links ein Zweieck skizziert. Rechts sieht man, was der in die Fläche übertragene mehrmalige Andockvorgang bewirkt. Es entsteht ein Graph mit 2 Ecken, n Kanten und n Flächen (inklusive der Aussenfläche). Die Eulersche Formel $|E| - |K| + |F| = 2$ ist immer erfüllt. Beim Übergang vom n–ten zum $n + 1$–ten Graphen gilt:

$$|E_{n+1}| = |E_n| = 2, \;\; |K_{n+1}| = |K_n| + 1, \;\; |F_{n+1}| = |F_n| + 1$$

Abb. 58: Zweieck

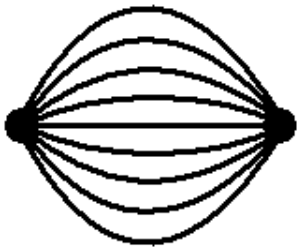


Abb. 59: Andocken von Zweiecken

Um aus den planaren Graphen (hier nicht einfache solche, mit parallelen Kanten) ein räumliches Gebilde erhalten zu können, brauchen wir minimal nur eine Fläche. Damit können wir wegen der Aussenfläche ein Kissen bilden mit mindestens einer krummen Fläche. Im Falle der rechten obigen Skizze mit der Anzahl Kanten $n \geq 2$ mag es z.B. eintreffen, dass das rücktransformierte und dann aufgeblasene Gebilde eine Kugel ist, auf der die vormaligen Kanten mit den Grosskreisen zusammenfallen. Was aber passiert, wenn wir die Forderung stellen, dass nur Polyeder mit äquivalenten ebenen Flächen in Form von regulären n–Ecken zulässig sind? Zwangsläufig müssen wir beim Studium dieser Frage von den kleinsten solchen Gebilden ausgehen, d.h. von den platonischen Körpern. Dazu brauchen wir erst einige Feststellungen:

1. **Andock–Erweiterungen des Tetraeders:**

   Ein Körper mit einer dreieckigen Seitenfläche lässt sich nach einer etwaigen Dehnung durch Andocken eines Tetraeders erweitern (vgl. Bild unten). Diese Andockung hat nach der Ausbreitung

in die Ebene denselben Effekt wie eine Triangulation eines Seitendreiecks. Bei einer solchen Triangulation führen wir im Innern eines Dreiecks einen neuen Punkt ein und verbinden diesen mit den umliegenden drei Ecken. So entstehen drei neue Dreiecke an der Stelle eines alten.

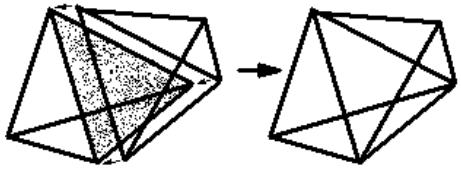


Abb. 60: Andockvorgang

Abb. 61: Triangulation

Für die Anzahlen der Ecken, Kanten und Flächen gilt beim Übergang vom n–ten zum $n+1$–ten Graphen:

$$|E_{n+1}| = |E_n| + 1 = |E_1| + (n-1) = 4 + (n-1),$$
$$|K_{n+1}| = |K_n| + 3 = |K_1| + (n-1)\cdot 3 = 6 + (n-1)\cdot 3 = (n+1)\cdot 3,$$
$$|F_{n+1}| = |F_n| + (3-1) = |F_1| + (n-1)\cdot 2 = 4 + (n-1)\cdot 2 = (n+1)\cdot 2.$$

Daraus lassen sich schon Folgerungen ableiten:

Folgerung:

Dockt man, ausgehend von einem Tetraeder, immer wieder Tetraeder an, so nimmt beim Übergang vom n–ten zum $n+1$–ten Graphen die Anzahl der Ecken um 1 zu, die Anzahl der Kanten ist ein Vielfaches von 3 und die Anzahl der Flächen ist immer gerade.

2. **Andock–Erweiterungen des Hexaeders:**

Nun gehen wir zum Würfel (Hexaeder) über. Der Andockvorgang ist im nebenstehenden Bild gezeigt. Beim Übergang vom n–ten zum $n+1$–ten Graphen nimmt Anzahl der Ecken um 4 zu, die Anzahl der Kanten um 8 und die Anzahl der Flächen um $6-2=4$. Daher gelten die Beziehungen:

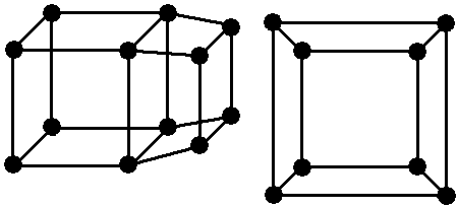


Abb. 62: Andockvorgang

$$|E_{n+1}| = |E_n| + 4 = |E_1| + (n-1)\cdot 4 = 8 + (n-1)\cdot 4 = (n+1)\cdot 4,$$
$$|K_{n+1}| = |K_n| + 8 = |K_1| + (n-1)\cdot 8 = 12 + (n-1)\cdot 8 = 4 + n\cdot 8,$$
$$|F_{n+1}| = |F_n| + 4 = |F_1| + (n-1)\cdot 4 = 6 + (n-1)\cdot 4 = 2 + n\cdot 4.$$

Folgerung:

Dockt man, ausgehend von einem Würfel, immer wieder Würfel an, so ist die Anzahl der Ecken ein Vielfaches von 4, die Anzahl der Kanten ein ungerades Vielfaches von 4 und die Anzahl der Flächen eine ungerades Vielfaches von 2.

Das Oktaeder ist dual zum Hexaeder (Würfel). Ersetzt man daher im Oktaeder „Flächen“ durch “Ecken“, so gewinnt man die Aussagen für den dualen Körper. Ob das auch nach dem Andocken so bleibt? Wir wollen es später untersuchen!

3. **Andock–Erweiterungen des Oktaeders:**

Gegeben sei also ein Oktaeder mit $|E_1| = 6$, $|K_1| = 12$ und $|F_1| = 8$. Beim Andocken (Übergang vom n–ten zum $n+1$–ten Graphen) nimmt die Anzahl der Ecken um $6-3=3$ zu, die Anzahl der Kanten um $12-3=9$ und die Anzahl der Flächen um $8-2=6$. Daher gelten die Beziehungen:

$$|E_{n+1}| = |E_n| + 3 = |E_1| + (n-1)\cdot 3 = 6 + (n-1)\cdot 3 = (n+1)\cdot 3,$$
$$|K_{n+1}| = |K_n| + 9 = |K_1| + (n-1)\cdot 9 = 12 + (n-1)\cdot 9 = 3 + n\cdot 9,$$
$$|F_{n+1}| = |F_n| + 6 = |F_1| + (n-1)\cdot 6 = 8 + (n-1)\cdot 6 = 2 + n\cdot 6.$$

Folgerung:

Dockt man, ausgehend von einem Oktaeder, immer wieder Oktaeder an, so ist die Anzahl der Ecken ein Vielfaches von 3, die Anzahl der Kanten ebenso ein Vielfaches von 3 und die Anzahl der Flächen ist gerade.

Konsequenz: Die Dualität zu den Andock–Erweiterungen des Würfels bleibt bei den Erweiterungen des Oktaeders nicht erhalten.

4. **Andock–Erweiterungen des Dodekaeders:**

Beim Andocken eines Dodekaeders an einen „Klumpen“ schon angedockter Dodekaeder lesen wir die folgenden Beziehung ab:

$|E_1| = 20$, $|K_1| = 30$ und $|F_1| = 12$. Beim Andocken (Übergang vom n–ten zum $n+1$–ten Graphen) nimmt Anzahl der Ecken um $20-5=15$ zu, die Anzahl der Kanten um $30-5=25$ und die Anzahl der Flächen um $12-2=10$. Daher gelten die Beziehungen:

$$|E_{n+1}| = |E_n| + 15 = |E_1| + (n-1)\cdot 15 = 20 + (n-1)\cdot 15 = 5 + n\cdot 15,$$
$$|K_{n+1}| = |K_n| + 25 = |K_1| + (n-1)\cdot 25 = 30 + (n-1)\cdot 25 = 5 + n\cdot 25,$$
$$|F_{n+1}| = |F_n| + 10 = |F_1| + (n-1)\cdot 10 = 12 + (n-1)\cdot 10 = 2 + n\cdot 10.$$

Folgerung:

Dockt man ausgehend von einem Dodekaeder immer wieder Dodekaeder an, so ist die Anzahl der Ecken ein Vielfaches von 5, die Anzahl der Kanten ebenso Vielfaches von 5 und die Anzahl der Flächen ist gerade.

5. **Andock–Erweiterungen des Ikosaeders:**

Beim Andocken eines Ikosaeders an einen „Klumpen“ schon angedockter Ikosaeder lesen wir wegen der Dualität zum Dodekaeder die Beziehung ab:

$|E_1| = 12$, $|K_1| = 30$ und $|F_1| = 20$. Beim Andocken (Übergang vom n–ten zum $n+1$–ten Graphen) nimmt Anzahl der Ecken um $12-3=9$ zu, die Anzahl der Kanten um $30-3=27$ und die Anzahl der Flächen um $20-2=18$. Daher gelten die Beziehungen:

$$|E_{n+1}| = |E_n| + 9 = |E_1| + (n-1)\cdot 9 = 12 + (n-1)\cdot 9 = 3 + n\cdot 9,$$
$$|K_{n+1}| = |K_n| + 27 = |K_1| + (n-1)\cdot 27 = 30 + (n-1)\cdot 27 = 3 + n\cdot 27,$$
$$|F_{n+1}| = |F_n| + 18 = |F_1| + (n-1)\cdot 18 = 20 + (n-1)\cdot 18 = 2 + n\cdot 18.$$

Folgerung:

Dockt man, ausgehend von einem Ikosaeder, immer wieder Ikosaeder an, so ist die Anzahl der Ecken ein Vielfaches von 3, die Anzahl der Kanten ebenso ein Vielfaches von 3 und die Anzahl der Flächen ist gerade.

Hinweis: Wählt man immer den Mittelpunkt einer Kante eines platonischen Körpers als Ecke eines neuen Körpers, so entsteht wieder ein Körper mit regelmässigen n–Ecken als Seitenflächen. Diese Seitenflächen sind jedoch bei einem Körper nicht allgemein kongruent. Das sieht man schon daran, dass es nur 5 platonische Körper gibt und dass die vorkommenden Kantenzahlen 6 und 30 nicht unter den Eckenzahlen der platonischen Körper vertreten sind.

Konsequenz: Durch Andockerweiterungen von platonischen Körpern durch ebensolche Körper kann man nicht immer beliebige Ecken–, Kanten– und Flächenzahlen erreichen. Dockt man z.B. immer wieder Dodekaeder an Dodekaeder an, so entsteht niemals ein Körper mit 97 Ecken, Kanten oder Flächen. (Denn es gilt: $97 \in \mathbb{P}$, 97 ist kein Vielfaches von 5.)

21.4.3 Reguläre Polyederkugeln und ihre Derivate

Definition: Eine Polyederkungel, welche einen äquivalenten platonischen (regulären) Körper besitzt, nennen wir **regulär**. Ist sie zu einem archimedischen Körper äquivalent, so nennen wir sie **semiregulär**.

Platonische Körper bestehen aus lauter gleichseitigen Dreiecken, Quadraten oder gleichseitigen Fünfecken. Mittels andocken können wir damit Klumpen herstellen mit beliebig grosser Ecken–, Kanten oder Flächenzahl. Durch aufblasen entstehen Polyederkugeln mit lauter äquivalenten n–Ecken. Wir wollen jetzt der Frage nachgehen, ob es Polyederkugeln geben kann, deren Flächen aus n–Ecken mit $n > 5$ entstanden sind.

Wir wissen aus der Elementargeometrie, dass man eine Ebene lückenlos in gleichseitige Dreiecke, Quadrate und 6–Ecke aufteilen kann. Mit 5–Ecken geht das nicht. Das liegt an den auftretenden Winkeln: Der Innenwinkel an einer Ecke beim 5–Eck beträgt 144^o. Zwei zusammenstossende 5–Ecke bilden daher an einer Ecke einen Winkel von 288^o, drei 5–Ecke einen Winkel von 432^o. Der volle Winkel von 360^o ist damit nicht erreichbar.

Teilt man eine Ebene in beliebige 6–Ecke auf, so kann an einer Ecke wohl ein Winkel kleiner als 120^o vorkommen (z.B. α oder δ). Dafür sind aber zwangsläufig andere Winkel grösser (in der Skizze β und γ).
In einem Polyeder sind bloss zwei an einer Ecke zusammenstossende Flächen unzulässig. Drei oder mehr zusammenstossende Flächen haben in der Ebene eine Winkelsumme von 360^o, im Raum jedoch wegen dem „einknicken“ eine solche Summe von weniger als 360^o. Andernfalls hätte dort das Polyeder keine Ecke.

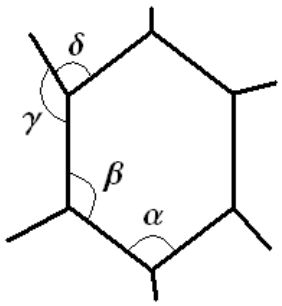


Abb. 63: Winkel beim 6–Eck

Nun besteht die Frage, ob man durch verkleinern der Winkel und vergrössern anderswo in einem n–Eck nicht doch eine Situation erreichen kann, sodass ein unregelmässiges Polyeder aus n-Ecken mit $n \geq 6$ herauskommt.

Es gilt der Satz: Jeder einfache, zusammenhängende, planare Graph besitzt eine Ecke v, für welche gilt: $d(v) \leq 5$. Da in jeder Ecke gleichviele Kanten zusammenkommen, und da wir hier eine reguläre Polyederkugel betrachten, und weil in einer Ecke mindestens drei Kanten zusammenstossen, stehen für die mit einer Ecke inzidierenden Kanten nur noch die Anzahlen 3, 4 und 5 zur Auswahl. Sei m diese Anzahl, so gilt: $|K| = m \cdot |E| \cdot \frac{1}{2}$. Denn jede Kante gehört zu zwei Ecken.
Weiter sei u die Anzahl Kanten einer Fläche. Wir gehen hier nun von der Annahme aus, dass es ein Polyeder gibt, dessen Seitenflächen alle n–Ecke mit $n \geq 6$ sind. Daher muss $u \geq 6$ sein. Da wiederum jede Kante des Polyeders zu zwei Flächen gehört, gilt jetzt: $|K| = u \cdot |F| \cdot \frac{1}{2}$. Somit folgt: $m \cdot |E| = u \cdot |F|$

Setzen wir die nun gewonnenen Beziehungen in den eulerschen Polyedersatz $|E| - |K| + |F| = 2$ ein, so kann man wie folgt schliessen:
$|E| - |K| + |F| = 2 \;\Rightarrow\; |E| - m \cdot |E| \cdot \frac{1}{2} + \frac{m \cdot |E|}{u} = 2 \;\Rightarrow\; 2 \cdot u \cdot |E| - u \cdot m \cdot |E| + 2 \cdot m \cdot |E| = 2 \cdot 2 \cdot u = 4 \cdot u.$
Daher gilt: $|E| \cdot (2 \cdot u - u \cdot m + 2 \cdot m) = 4 \cdot u \;\Rightarrow\; |E| = \frac{Z}{N} = \frac{4 \cdot u}{2 \cdot u - u \cdot m + 2 \cdot m}, \;\; u \geq 6, \;\; m \in \{3, 4, 5\}.$
Der Zähler $Z = 4 \cdot u, \;\; u \geq 6$, ist hier immer positiv. Wie verhält es sich dagegen mit dem Nenner $N = 2 \cdot u - u \cdot m + 2 \cdot m$?

Wir gehen die drei Fälle $m = 3, 4, 5$ nacheinander durch.

1. Der Fall $m = 3$: Hier ist $N = 2 \cdot u - u \cdot 3 + 2 \cdot 3 = -u + 6, \;\; u \geq 6 \;\Rightarrow\; N \leq 0$. Der Nenner ist also entweder 0, was nicht sein kann, oder er ist negativ, was bei einem positiven Zähler zu einer negativen Eckenanzahl führen würde. Dies wiederum kann auch nicht sein. Der Fall $m = 3$ ist daher ausgeschlossen.

2. Der Fall $m = 4$: Hier ist $N = 2 \cdot u - u \cdot 4 + 2 \cdot 4 = -2 \cdot u + 8, \;\; u \geq 6 \;\Rightarrow\; N \leq -2 \cdot 6 + 8 = -12 + 8 = -4$. Damit wäre hier der Nenner wiederum negativ, während der Zähler positiv ist, was wiederum nicht sein kann. Der Fall $m = 4$ ist daher ausgeschlossen.

3. Der Fall $m = 5$: Hier ist $N = 2 \cdot u - u \cdot 5 + 2 \cdot 5 = -3 \cdot u + 10, \;\; u \geq 6 \;\Rightarrow\; N \leq -3 \cdot 6 + 10 = -18 + 10 = -6$. Damit wäre hier der Nenner ebenfalls wiederum negativ, während der Zähler positiv ist, was nicht sein kann. Der Fall $m = 5$ ist daher ausgeschlossen.

Damit haben wir alle Fälle ausgeschlossen, die bei einer reguläre Polyederkugel mit n–Eck–Seitenflächen für $n \geq 6$ noch geblieben sind. Daher gilt der Satz:

Satz: Reguläre Polyederkugel existieren nur für n–Eck–Seitenflächen mit $n \in \{3, 4, 5\}$. Ihre Anzahl ist jeweils unendlich. Entsprechendes gilt für die äquivalenten planaren und einfachen Graphen.

Die letzte Aussage formulieren wir in etwas anderer Art noch als Korollar:

Korollar:

Vor.:

Gegeben sei ein planarer einfacher Graph, dessen Flächen inklusive der Aussenfläche jede von exakt n Kanten eingeschlossene wird.

Beh.:

$n \in \{3, 4, 5\}$.
Für jedes dieser n ist die Anzahl der möglichen Graphen unendlich.

Kapitel • Chapitre 22

Zum Stand der Arbeiten

22.1 Geplante Teile

Einführung in die Graphentheorie (für die Informatik): Noch in Arbeit — Handskript vorhanden. Wird bei Gelegenheit mit LaTeX gefasst. Bitte Geduld!

Weitere geplante Teile:

1. Ausbau der Einführung in die Kryptologie und der Graphentheorie (für die Informatik)
2. Übungen zu Mathematik II (im DIYMU vorhanden)
3. Weitere Themen (u.a. für die Architektur, Informatik und den Baubereich):
   (a) Einführung in die Planungsforschung
   (b) Alternativauswahl und Entscheidungstheorie, Spieltheorie, Nullsummenspiel
   (c) Formen, Symmetrien, Muster, Ornamente (in Arbeit)
   (d) Mathematik und Computer, Grenzen der Computermethode
   (e) Spezielles aus der Geometrie, Fraktale
   (f) Vertiefte Behandlung der Geometrie der platonischen, archimedischen Körper sowie der Johnson–Körper, ihrer Sternformen und polaren Gebilde
   (g) Anwendungen im Baubereich

Bearbeitungstermine noch unbekannt

22.2 Alte Gliederung — Vieille classification

- Teil 1 ⇝ Grundlagen (Skript über Grundlagen)
- Teil 2 ⇝ Logik • *Partie 2 ⇝ Logique*
- Teil 3 ⇝ Mengenlehre
- Teil 4 ⇝ Boolsche Algebra
- Teil 5 ⇝ Standardfunktionen (Skript über Grundlagen)
- Teil 6 ⇝ Kombinatorik • *Partie 6 ⇝ Analyse combinatoire*

22.3 Abbildungsverzeichnis

Das früher nachstehend eingefügte Abbildungsverzeichnis wird seiner Grösse und daher seiner Unhandlichkeit und geringen Nützlichkeit wegen nicht mehr herausgegeben.

Literaturverzeichnis

[1] Asser. Einführung in die mathematische Logik *Teile 1, 2 und 3*. Verlag Harri Deutsch (Bibl.: asser)

[2] Church. Introduction to Mathematical Logic. Princeton University Press (Bibl.: church)

[3] Deller. Boolscha Algebra. Diesterweg (Bibl.: deller)

[4] Hermes. Einführung in die mathematische Logik. Teubner Verlag Stuttgart (Bibl.: hermes)

[5] Hilbert, Ackermann. Grundzüge der theoretischen Logik. Springer-Verlag (Grundlehren der math. Wiss. in Einzeldarst., Bd. 27) (Bibl.: hilbert)

[6] Jehle. Boolsche Algebra. Bayrischer Schulbuchverlag (Bibl.: jehle)

[7] Lipschutz. Finite Mathematik. Reihe SCHAUM, Mac Graw Hill (Bibl.: lipschutz)

[8] Mendelson. Boolscha Algebra und logische Schaltungen. Reihe SCHAUM, Mac Graw Hill (Bibl.: mendelson)

[9] Shoenfield. Mathematical Logic. Addison–Wesley Publishing Company (Bibl.: shoen)

[10] Tarski. Einführung in die mathematische Logik. Vandenhoeck & Ruprecht-Verlag (Bibl.: tarski)

[11] van Dahlen. Logic and Structure. Springer-Verlag (Universitätstext) (Bibl.: vandalen)

[12] Vom Autor. *DIYMU* (Do it yourself Mathematik Übungsbuch). Ingenieurschule Biel 1991 (Bibl.: wirz)

[13] Vom Autor. Mathematik für Ingenieure *Teil 1* Einführung. Ingenieurschule Biel 1993 (Bibl.: wirz1)

[14] Ayres. Algebra, Theorie und Anwendung. Reihe SCHAUM, Mac Graw Hill (Bibl.: ayres)

[15] Leupold u.a.. Mathematik, ein Studienbuch für Ingenieure. Fachbuchverlag Leipzig – Köln (Bibl.: leupold)

[16] Lipschutz. Finite Mathematik, Theorie und Anwendung. Reihe SCHAUM, Mac Graw Hill (Bibl.: lipschutz1)

[17] Lipschutz. Lineare Algebra, Theorie und Anwendung. Reihe SCHAUM, Mac Graw Hill (Bibl.: lipschutz2)

[18] Papula. Mathematik für Ingenieure Bd. 1, 2, 3. Vieweg-Verlag (Bibl.: papula)

[19] Potter. Mengentheorie. Spektrum–Verlag (Bibl.: potter)

[20] Schmidt. Mengenlehre. BI Mannheim (Bibl.: schmidt)

[21] Spiegel. Einführung in die höhere Mathematik, Theorie und Anwendung. Reihe SCHAUM, Mac Graw Hill (Bibl.: spiegel)

[22] Brenner, Lesky. Mathematik für Ingenieure und Naturwissenschaftler. AULA-Verlag Wiesbaden (Bibl: brennerlesky)

[23] Deller. Boolsche Algebra. Diesterweg Salle (Bibl: deller)

[24] Dörfler, Peschek. Einführung in die Mathematik für Informatiker. Hanser Verlag München, Wien, 1998 (Bibl: dorflerPeschek)

[25] Gellert, Küstner, Hellwich, Kästner. Grosses Handbuch der Mathematik. Buch und Zeit Verlagsges. m.b.H. Köln (Bibl: gellert)

[26] Jehle. Boolsche Algebra. bsv, Bayrischer Schulbuchverlag (Bibl: jehle)

[27] Mendelson. Boolsche Algebra und logische Schaltungen, Theorie und Anwendung. Reihe SCHAUM, Mac Graw Hill (Bibl: mendelson)

[28] Fachlexikon *a b c*. Verlag Harri Deutsch Bibliographisches Institut Mannheim, Wien, Zürich. Dudenverlag (Bibl.: abc)

[29] Brenner, Lesky. Mathematik für Ingenieure und Naturwissenschaftler. AULA-Verlag Wiesbaden (Bibl.: brennerlesky)

[30] Claus, Schwill. Schüler–Duden, Die Informatik. Bibliographisches Institut Mannheim, Wien, Zürich. Dudenverlag (Bibl.: clausschwill)

[31] Iyanaga, Kawada. Encyclopedic Dictionary of Mathematics. MIT Press, Cambridge Mass., London GB (Bibl.: iyanagakawada)

[32] Meschkowski. Mathematisches Begriffswörterbuch. BI Hochschultaschenbücher. Bibliographisches Institut Mannheim (Bibl.: meschkowski)

[33] Vom Autor. Mathematik für Ingenieure *Teile 1 ff* (Bibl.: wirz)

[34] Vom Autor. *DIYMU* (Do it yourself Mathematik Übungsbuch). Ingenieurschule Biel 1991 (Bibl.: wirz1)

[35] Manfred Brill, Mathematik für Informatiker, Hanser Verlag München, Wien, 2001 (Bibl: brill)

Ende • Fin