

Wolfgang Rautenberg

Einführung in die Mathematische Logik

Ein Lehrbuch

3. Auflage

STUDIUM



Wolfgang Rautenberg

Einführung in die Mathematische Logik

Wolfgang Rautenberg

Einführung in die Mathematische Logik

Ein Lehrbuch

3., überarbeitete Auflage

STUDIUM



Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<<http://dnb.d-nb.de>> abrufbar.

Prof. Dr. Wolfgang Rautenberg
Fachbereich Mathematik und Informatik
Freie Universität Berlin
14195 Berlin

raut@math.fu-berlin.de

- 1. Auflage 1996
- 2., verbesserte und erweiterte Auflage 2002
- 3., überarbeitete Auflage 2008

Alle Rechte vorbehalten
© Vieweg+Teubner | GWV Fachverlage GmbH, Wiesbaden 2008

Lektorat: Ulrike Schmickler-Hirzebruch | Susanne Jähnel

Vieweg+Teubner ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Satz und Layout: Der Autor
Druck und buchbinderische Verarbeitung: Strauss Offsetdruck, Mörlenbach
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0578-2

Zum Geleit

von Lev Beklemishev, Utrecht

Das Gebiet der Mathematischen Logik – entstanden bei der Begriffsklärung von logischer Gültigkeit, Beweisbarkeit und Berechenbarkeit – wurde in der ersten Hälfte des vorigen Jahrhunderts von einer Reihe brillanter Mathematiker und Philosophen geschaffen, wie Frege, Hilbert, Gödel, Turing, Tarski, Mal'cev, Gentzen, und einigen anderen. Die Entwicklung dieser Disziplin wird als eine der größten Errungenschaften der Wissenschaft des 20. Jahrhunderts diskutiert: Sie dehnte die Mathematik in einen bislang unbekannten Bereich von Anwendungen aus, unterwarf logisches Schließen und Berechenbarkeit einer rigorosen Analyse, und führte schließlich zur Entwicklung des Computers.

Das Lehrbuch von Professor Wolfgang Rautenberg ist eine gut geschriebene Einführung in diesen schönen und zusammenhängenden Gegenstand. Es enthält klassisches Material wie logische Kalküle, die Anfänge der Modelltheorie und Gödels Unvollständigkeitssätze, ebenso wie einige von Anwendungen her motivierte Themen wie ein Kapitel über Logikprogrammierung. Der Autor hat große Sorgfalt darauf verwendet, die Darstellung lesbar und umfassend zu gestalten; jeder Abschnitt wird von einer guten Auswahl von Übungen begleitet.

Ein besonderes Lob ist dem Autor für die Darstellung des Zweiten Gödelschen Unvollständigkeitssatzes geschuldet, in welcher es dem Autor gelang, einen relativ einfachen Beweis der Ableitungsbedingungen und der beweisbaren Σ_1 -Vollständigkeit zu geben; ein technisch diffiziler Punkt, der in Lehrbüchern vergleichbaren Niveaus gewöhnlich ausgelassen wird. Dieses Lehrbuch kann allen Studenten empfohlen werden, die die Grundlagen der Mathematischen Logik erlernen wollen.

Vorwort

zur 3. Auflage

Die dritte Auflage unterscheidet sich von der zweiten nicht nur in der Korrektur von Druckfehlern sondern in zahlreichen sachlichen und stilistischen Änderungen, verbesserten Beweisen und Übungen. Das Buch dürfte dadurch für den Anfänger noch leichter lesbar sein. Auch Stichwort- und Literaturverzeichnis wurden vollständig revidiert und eine historisch orientierte Einleitung wurde hinzugefügt.

Das Buch wendet sich an Studenten und Dozenten der Mathematik oder Informatik, und wegen der ausführlich diskutierten Gödelschen Unvollständigkeitssätze, die ja von hohem erkenntnistheoretischem Interesse sind, auch an Fachstudenten der Philosophischen Logik. Es enthält in den ersten drei Kapiteln den Stoff einer einsemestrigen Vorlesung über Mathematische Logik, die sowohl für den Masterstudiengang als auch den Bachelor-Studiengang geeignet ist. Das 1. Kapitel beginnt mit Elementen der Logik, wie sie für die Grundlagenphase des Bachelor-Studiums verlangt werden, und es enthält zu Beginn des 2. Kapitels das Wichtigste über algebraische und relationale Strukturen, Homomorphismen und Isomorphismen, was zur Aufbauphase eines wie auch immer gearteten Mathematikstudiums gehören sollte. Eine wie in **3.4** geführte Diskussion der Axiomatik der Mengenlehre ist zwar grundlagentheoretisch wichtig, hängt aber von den Zielen der Einführungsvorlesung ab.

Nicht alles über den Gödelschen Vollständigkeitssatz (Kapitel **3**) muss den Bachelor-Studenten vorbewiesen werden. Es genügt, den aussagenlogischen Kalkül zu behandeln und die nötigen Schritte einer Erweiterung auf die Prädikatenlogik nur zu beschreiben. Die letzten Abschnitte von Kapitel **3** befassen sich mit Anwendungen der Vollständigkeit und haben teilweise beschreibenden Charakter, mit Ausblicken auf aktuelle Themen wie z.B. die automatische Beweisverifikation.

Das Buch enthält auch das Basismaterial für eine Vorlesung *Logik für Informatiker*, über die weiter unten gesprochen wird, in Kapitel **5** das Material für eine die Logik fortsetzende Vorlesung *Modelltheorie* und in Kapitel **6** für eine Vorlesung *Rekursionstheorie* mit Anwendungen auf Entscheidungsprobleme.

Das Buch kann ganz unabhängig von Vorlesungen aber auch zum Selbststudium genutzt werden. Nicht zuletzt deshalb wurden Stichwort- und Symbolverzeichnis recht ausführlich verfasst und vor Beginn des Haupttextes ein Abschnitt *Notationen* eingefügt. Für den Großteil der Übungen gibt es Lösungshinweise in einem gesonderten Abschnitt am Ende des Buches. Außer einer hinreichenden Schulung im logischen Schließen sind spezielle Vorkenntnisse nicht erforderlich; lediglich für Teile von Kapitel **5** sind algebraische Grundkenntnisse nützlich, und für den letzten Abschnitt in Kapitel **7** gewisse Kenntnisse über Modelle der Mengenlehre.

Stil und Darstellung wurden in den ersten drei Kapiteln breit genug gehalten, so dass auch der Student noch vor dem Einstieg in eine Spezialdisziplin den Stoff durchaus selbstständig bewältigen kann. Ab Kapitel 4 steigen die Anforderungen allmählich, die man am sichersten durch selbstständiges Lösen der Übungen meistert. Auch verdichtet sich von dort an etwas die Darstellung, jedoch nicht auf Kosten sprachlicher Präzision. Klarheit und angemessener Umgang mit Notationen bleiben oberstes Gebot. Der Leser sollte Bleistift und Papier zum Nachrechnen stets parat halten.

Eine Besonderheit dieser Darstellung ist die eingehende Behandlung der Gödelschen Unvollständigkeitssätze. Diese beruhen auf der Repräsentierbarkeit rekursiver Prädikate in formalisierten Theorien, die in ihrer Urform den Hauptteil der Gödelschen Arbeit [Gö2] ausmacht. Dieser Linie folgend gewinnt wir in Kapitel 6 den ersten Unvollständigkeitssatz, die Unentscheidbarkeit des Tautologieproblems der Logik nach Church und die Resultate über Nichtdefinierbarkeit des Wahrheitsbegriffs von Tarski in einem Zuge. Das letzte Kapitel ist ausschließlich dem zweiten Unvollständigkeitssatz und seinem Umfeld gewidmet. Von besonderem Interesse ist dabei, dass Fragen über selbstbezügliche Aussagen aufgrund der Solovayschen und weiterführender Vollständigkeitssätze algorithmisch entscheidbar sind.

Die Klassifikation definierender Formeln für arithmetische Prädikate wird recht frühzeitig, schon bei der Repräsentation rekursiver Prädikate in 6.3 eingeführt. Denn sie trägt in besonderem Maße dazu bei, den engen Zusammenhang zwischen Logik und Rekursionstheorie sichtbar zu machen. Weitere Unentscheidbarkeitsresultate über formalisierte Theorien werden in den Abschnitten 6.5 und 6.6 behandelt, einschließlich einer Skizze über die Lösung des 10. Hilbertschen Problems.

In Kapitel 4 werden berechenbare Funktionen in natürlicher Weise durch PROLOG-Programme präzisiert. Dies ist für Studierende der Informatik interessant, heißt dies doch einerseits, PROLOG ist eine universelle Programmiersprache, in der prinzipiell alle Algorithmen beschrieben werden können. Andererseits werden durch den Unentscheidbarkeitnachweis des Existenzproblems erfolgreicher Resolutionen in 4.4 die prinzipiellen Schwierigkeiten erklärt, die mit der Problemlösung durch Anfragen an Logik-Programme zusammenhängen. Kapitel 4 muss in einer Vorlesung für Informatiker mit Abschnitt 6.1 über Grundbegriffe der traditionellen Rekursionstheorie natürlich in Zusammenhang gebracht werden.

Kapitel 5 behandelt die Grundlagen der erst um 1950 entstandenen und inzwischen weit gefächerten Modelltheorie. Hier werden in der mathematischen Logik entwickelte Techniken mit Konstruktionstechniken anderer Gebiete zum gegenseitigen Nutzen miteinander verbunden. Durch den Einsatz weitreichender Methoden gelingt es, klassische Resultate wie die Eliminierbarkeit der Quantoren in der Theorie des reellen und der des komplexen Zahlenkörpers recht schnell zu gewinnen.

Trotz seiner Themenvielfalt umfasst dieses Buch bei weitem nicht alles was die Mathematische Logik vorzuweisen hat. Lehrbücher mit enzyklopädischem Anspruch lassen sich heute selbst für deren Teilgebiete nicht mehr verfassen. Bei der Stoffauswahl können bestenfalls Akzente gesetzt werden. Das bezieht sich vor allem auf die über elementare Dinge hinausführenden Kapitel **4**, **5**, **6** und **7**. Die Auswahl orientiert sich durchweg an Grundergebnissen der Mathematischen Logik, die mit hoher Wahrscheinlichkeit von bleibendem Bestand sind.

Wo immer dies gelang, wurden in der Literatur vorliegende Beweise vereinfacht. Philosophische und grundagentheoretische Probleme der Mathematik ebenso wie rein beweistheoretische Aspekte werden nicht systematisch behandelt, aber diesbezügliche Fragen werden an geeigneten Stellen im Text angeschnitten, vor allem im Zusammenhang mit den Gödelschen Sätzen. Wir haben uns dabei bemüht, einem Auseinanderdriften von Modell- und Beweistheorie entgegen zu wirken.

Es gibt in diesem Buche keine Formeltrennungen im fließenden Text. Dies kommt nicht nur dem Schriftbild zugute sondern auch einem unbehinderten Informationsfluß. Bemerkungen im Kleindruck enthalten in der Regel weiterführende Informationen oder verweisen auf das Literaturverzeichnis, das angesichts der Literaturfülle nur eine Auswahl repräsentieren kann. Die Einträge im Literaturverzeichnis sind alphabetisch nach ihren beim Zitieren verwendeten Kürzeln sortiert.

Die sieben Kapitel des Buches sind in Abschnitte gegliedert. Eine Referenz wie z.B. **4.5** bedeutet Kapitel **4**, Abschnitt **5** und Satz 4.5 meint den Satz Nr. 5 in Abschnitt **4** eines gegebenen Kapitels. Bei Rückbezug auf diesen Satz in einem anderen Kapitel wird die Kapitelnummer hinzugefügt. So ist Satz 6.4.5 beispielsweise Satz 4.5 in Kapitel **6**.

Auf der Website www.math.fu-berlin.de/~raut finden sich weitere Informationen zu dem Buch und zu verwandten Themen, z.B. Mengenlehre. Für hilfreiche Kritik danke ich zahlreichen Kollegen und Studenten; die Namensliste ist zu lang, um sie hier anzugeben. Besonderer Dank gilt Lev Beklemishev (Utrecht), Wilfried Buchholz (München), Peter Agricola, Michael Knoop, sowie dem durch einen tragischen Unfall aus zu früh dem Leben geschiedenen Mathematiker und Informatiker Ullrich Fuchs. Dem Vieweg+Teubner Verlag bin ich für die gute Zusammenarbeit verbunden.

Berlin, Mai 2008,

Wolfgang Rautenberg

Inhaltsverzeichnis

Einleitung	xv
Notationen	xix
1 Aussagenlogik	1
1.1 Boolesche Funktionen und Formeln	2
1.2 Semantische Äquivalenz und Normalformen	9
1.3 Tautologien und aussagenlogisches Folgern	14
1.4 Ein vollständiger aussagenlogischer Kalkül	18
1.5 Anwendungen des Kompaktheitssatzes	25
1.6 Hilbert-Kalküle	29
2 Prädikatenlogik	33
2.1 Mathematische Strukturen	34
2.2 Syntax elementarer Sprachen	43
2.3 Semantik elementarer Sprachen	49
2.4 Allgemeingültigkeit und logische Äquivalenz	58
2.5 Logisches Folgern und der Theoriebegriff	62
2.6 Spracherweiterungen	67
3 Der Gödelsche Vollständigkeitssatz	71
3.1 Ein Kalkül des natürlichen Schließens	72
3.2 Der Vollständigkeitsbeweis	76

3.3	Erste Anwendungen – Nichtstandardmodelle	81
3.4	ZFC und die Paradoxie von Skolem	87
3.5	Aufzählbarkeit und Entscheidbarkeit	92
3.6	Vollständige Hilbert-Kalküle	95
3.7	Fragmente der 1. Stufe und Erweiterungen	99
4	Grundlagen der Logikprogrammierung	105
4.1	Termmodelle und der Satz von Herbrand	106
4.2	Aussagenlogische Resolution	112
4.3	Unifikation	119
4.4	Logikprogrammierung	122
4.5	Der Beweis des Hauptsatzes	129
5	Elemente der Modelltheorie	131
5.1	Elementare Erweiterungen	132
5.2	Vollständige und κ -kategorische Theorien	137
5.3	Das Ehrenfeucht-Spiel	142
5.4	Einbettungs- und Charakterisierungssätze	145
5.5	Modellvollständigkeit	151
5.6	Quantorenelimination	157
5.7	Reduzierte Produkte und Ultraprodukte	163
6	Unvollständigkeit und Unentscheidbarkeit	167
6.1	Rekursive und primitiv-rekursive Funktionen	169
6.2	Gödelisierung	176
6.3	Repräsentierbarkeit arithmetischer Prädikate	182
6.4	Der Repräsentationssatz	189
6.5	Die Sätze von Gödel, Tarski, Church	194
6.6	Übertragung durch Interpretation	200
6.7	Die arithmetische Hierarchie	205

7 Zur Theorie der Selbstreferenz	209
7.1 Die Ableitungsbedingungen	210
7.2 Die Theoreme von Gödel und Löb	217
7.3 Die Modallogik G	221
7.4 Modale Behandlung der Selbstreferenz	223
7.5 Eine bimodale Beweislogik für PA	226
7.6 Modale Operatoren in ZFC	228
 Lösungshinweise zu den Übungen	 231
 Literatur	 241
 Stichwortverzeichnis	 247
 Symbolverzeichnis	 255

Einleitung

Ein wichtiges Merkmal der modernen Logik ist die klare Unterscheidung zwischen Objektsprache und Metasprache. Erstere ist in der Regel formalisiert oder mindestens formalisierbar. Letztere ist eine Art Umgangssprache, die sich von Autor zu Autor unterscheidet und nicht unerheblich von der Zielgruppe des Autors abhängt. Sie ist oft mit halbformalen Elementen verwoben, von denen die meisten ihren Ursprung in der Mengenlehre haben. Das Ausmaß der involvierten Mengenlehre ist unterschiedlich. Semantik und Modelltheorie nutzen strengere mengentheoretische Werkzeuge als die Beweistheorie. Aber im Mittel wird wenig mehr vorausgesetzt als Kenntnisse der mengentheoretischen Terminologie und der elementaren Mengenalgebra, wie sie in jedem mathematischen Kurs für Anfänger präsentiert werden. Vieles davon ist im Grunde nur eine *façon de parler*.

Da dieses Buch die *mathematische* Logik betrifft, ist seine Sprache die gemeinsame Umgangssprache aller mathematischen Disziplinen. Doch gibt es einen wesentlichen Unterschied. In der Mathematik interagieren Objekt- und Metasprache tiefgehend miteinander. Erstere ist bestenfalls partiell formalisiert, was sich als erfolgreich erwiesen hat. Eine Trennung von Objekt- und Metasprache ist nur im speziellen Kontext relevant, zum Beispiel in der axiomatischen Mengenlehre, wo Formalisierung nötig ist um anzugeben wie gewisse Axiome aussehen. Strikt formale Sprachen werden häufiger in der Informatik angetroffen. Ähnlich wie in der Logik gehören formale linguistische Elemente zu den Untersuchungsobjekten, etwa bei der Analyse komplexer Software oder einer Programmiersprache.

Der Darstellungsrahmen formaler Sprachen und Theorien wird traditionell die *Metatheorie* genannt. Eine wichtige Aufgabe einer metatheoretischen Analyse ist es, Verfahren für logische Schlüsse mittels sogenannter logischer Kalküle anzugeben, welche rein syntaktisch operieren. Es gibt sehr unterschiedliche logische Kalküle. Die Wahl kann von der formalisierten Sprache, der logischen Basis und anderen Faktoren abhängen. Grundlegende metatheoretische Werkzeuge sind in jedem Falle die naiven natürlichen Zahlen und induktive Beweisverfahren. Diese werden auch Beweise durch Metainduktion genannt, insbesondere wenn formalisierte Theorien in Objektsprachen behandelt werden, die über natürliche Zahlen und Induktion selbst sprechen. Induktion kann auch über gewissen Wortmengen eines Alphabets, oder über dem Regelsystem eines logischen Kalküls ausgeführt werden.

Die logischen Hilfsmittel der Metatheorie dürfen sich von denen der Objektsprache unterscheiden. Mitunter wird dies sogar explizit gefordert. Aber in diesem Buche ist die Logik der Objektsprachen und die der Metasprache stets dieselbe, nämlich die

klassische zweiwertige Logik. Es gibt gute Gründe dafür, Letztere als die Logik des gesunden Menschenverstandes anzusehen. Mathematiker, Informatiker, Physiker, Linguisten und andere verwenden sie als gemeinsame Kommunikations-Plattform.

Es sollte bemerkt werden, dass sich die in den Wissenschaften verwendete Logik erheblich von der Logik der Alltagssprache unterscheidet, wo diese mehr eine Kunst ist als ein ernsthafter Versuch zu sagen was denn woraus folgt. Im Alltagsleben hängt die Bedeutung fast jeder Äußerung vom Kontext ab. In den meisten Fällen sind logische Relationen nur angedeutet, selten explizit ausgedrückt. Oft fehlen grundlegende Voraussetzungen der zweiwertigen Logik, zum Beispiel eine kontextfreie Verwendung der logischen Verknüpfungen. Probleme dieser Art werden in diesem Buche nur am Rande behandelt. Bis zu einem gewissen Grad kann eine mehrwertige Logik oder eine Kripke-Semantik helfen die Situation zu klären, und manchmal müssen komplexe mathematische Methoden genutzt werden, um derartige Probleme zu analysieren. In diesem Buch dient die Kripke-Semantik einem anderen Zweck, nämlich der Analyse selbstbezüglicher Aussagen in Kapitel 7.

Wir ergänzen die bisherigen allgemeinen Ausführungen durch einige historische Bemerkungen, welche der Anfänger vermutlich eher zu schätzen weiß, wenn er zuvor zumindest Teile dieses Buches gelesen hat.

Die traditionelle Logik ist als Teil der Philosophie eine der ältesten wissenschaftlichen Disziplinen und kann bis in die Antike zurückverfolgt werden ¹⁾. Sie ist eine der Wurzeln der heute so genannten Philosophischen Logik. Die Mathematische Logik ist hingegen eine relativ junge Disziplin, entstanden durch das Bemühen von Peano, Frege und Russell um 1900, Mathematik insgesamt auf die Logik zu reduzieren. Sie entwickelte sich während des 20. Jahrhunderts zu einer Disziplin mit mehreren Teilgebieten und zahlreichen Anwendungen in Mathematik, Informatik, Linguistik und Philosophie. Von den Glanzpunkten der relativ kurzen Entwicklungsperiode der Mathematischen Logik nennen wir nur die wichtigsten. Siehe hierzu auch [Hei].

Den Anfang bildeten verschiedene Axiomatisierungen der Geometrie, der Algebra, und insbesondere der Mengenlehre. Davon sind die wichtigsten diejenige von Zermelo, ergänzt durch Fraenkel und von Neumann, ZFC genannt, und die Typentheorie von Whitehead und Russell. Letztere ist das Überbleibsel des Fregeschen Versuchs einer Reduktion der Mathematik auf die Logik. Stattdessen stellte es sich heraus, dass die Mathematik gänzlich auf der Mengenlehre als einer Theorie erster Stufe aufgebaut werden kann. Tatsächlich wurde diese Einsicht erst allmählich gewonnen und auch erst nachdem um 1915 der Rest verborgener Annahmen aus der Mengen-

¹⁾Insbesondere zu den Stoikern und zu Aristoteles. Die aristotelischen Syllogismen sind nützliche Beispiele für Schlüsse in einer Sprache erster Stufe mit einstelligen Prädikatensymbolen. Einer dieser Syllogismen dient als ein Beispiel im Abschnitt 4.4 über Logikprogrammierung.

lehre entfernt wurde. Zum Beispiel ist der Begriff des geordneten Paares in Wahrheit ein mengentheoretischer oder kann zumindest als ein solcher verstanden werden. Es handelt sich nicht um einen logischen Begriff.

Gleich nachdem diese Axiomatisierungen abgeschlossen waren, entdeckte Skolem, dass es abzählbare Modelle von ZFC gibt; ein Rückschlag für die Hoffnung auf eine axiomatische Definition des abstrakten Begriffs einer Menge. Näheres hierzu in den Ausführungen in Abschnitt 3.4. Skolem wies damit erstmals auf Grenzen der bis dahin so erfolgreichen axiomatischen Methode hin.

Etwa um dieselbe Zeit betraten zwei herausragende Mathematiker, Hilbert und Brouwer, die Szene und begannen ihren berühmten Streit über die Grundlagen der Mathematik. Dieser ist in zahlreichen Darstellungen und besonders ausführlich in [Kl2, Chapter IV] beschrieben worden und wird daher hier nicht wiedergegeben.

Der nächste Glanzpunkt ist die von Gödel bewiesene Vollständigkeit der von Hilbert im ersten modernen Lehrbuch über Mathematische Logik ([HA]) präsentierten Regeln der Prädikatenlogik. Damit wurde ein Traum von Leibniz in gewissem Umfange Wirklichkeit, nämlich die Schaffung einer *ars inveniendi* (einer Kunst des Erfindens) mathematischer Wahrheiten in Gestalt eines formalen Kalküls. Siehe hierzu 3.5.

Hilbert hatte inzwischen seine Ansichten über die Grundlagen der Mathematik zu einem Programm entwickelt. Dieses zielte darauf ab, die Konsistenz der Arithmetik und darüber hinaus der Gesamtheit der Mathematik einschließlich der nichtfiniten mengentheoretischen Methoden mit finiten Mitteln zu beweisen. Dieses Programm fand zuerst begeisterte Zustimmung. Aber bereits 1931 zeigte Gödel mit seinen Unvollständigkeitssätzen, dass Hilberts ursprüngliches Programm fehlschlagen muss oder zumindest einer sorgfältigen Revision bedarf.

Viele Logiker betrachten die Gödelschen Sätze als das Top-Ergebnis der Mathematischen Logik des 20. Jahrhunderts. Eine Konsequenz dieser Sätze ist die Existenz konsistenter Erweiterungen der Peano-Arithmetik, in welchen wahre und falsche Sätze in friedlicher Koexistenz miteinander leben (siehe Abschnitt 7.2) und deshalb von uns auch „Traumtheorien“ genannt werden. Damit war auch Hilberts Ansatz gescheitert, Widerspruchsfreiheit als ein Wahrheitskriterium in der Mathematik zu betrachten. Selbst wenn ZFC widerspruchsfrei sein sollte, ist damit die Frage nicht geklärt, wie dieses oder ein erweitertes axiomatische System an der Realität zu messen ist. Ein integraler Bestandteil der Mengenlehre ist das Unendlichkeitsaxiom, und dieses überschreitet klar die Grenzen physikalischer Erfahrung.

Die von Gödel in [Gö2] entwickelten Methoden waren gleichermaßen bahnbrechend für die Entstehung der Rekursionstheorie um das Jahr 1936. Churchs Beweis der Unentscheidbarkeit des Tautologieproblems markiert einen weiteren herausragen-

den Erfolg. Nachdem Church hinreichende Belege durch eigene Forschungen sowie durch diejenigen von Turing, Kleene, und anderen gesammelt hatte, formulierte er 1936 seine berühmte These (Abschnitt **6.1**), obwohl zu der Zeit keine Computer im heutigen Sinne existierten, noch vorhersehbar war, dass Berechenbarkeit jemals die weitreichende Rolle spielen würde, die sie heute einnimmt.

Wie bereits erwähnt, musste Hilberts Programm revidiert werden. Von Gentzen wurde ein entscheidender Schritt unternommen, der als ein weiterer durchbrechender Erfolg der Mathematischen Logik und als Startpunkt der heutigen Beweistheorie angesehen wird. Die logischen Kalküle in **1.4** und **3.1** sind mit Gentzens Kalkülen des natürlichen Schließens verwandt. Eine Diskussion der speziellen beweistheoretischen Ziele und Methoden liegt jedoch nicht im Rahmen dieses Buches.

Wir erwähnen ferner Gödels Entdeckung, dass es weder das Auswahlaxiom (AC) noch die Kontinuumshypothese (CH) sind, welche das Konsistenzproblem der Mengenlehre verursachen. Die Mengenlehre mit AC und CH ist konsistent, falls die Mengenlehre ohne AC und ohne CH dies ist. Dieses Grundresultat der Mathematischen Logik hätte ohne die Nutzung strikt formaler Methoden nicht gewonnen werden können. Das gilt auch für den 1963 von P. Cohen erbrachten Beweis der Unabhängigkeit von AC und CH von den Axiomen der Mengenlehre.

Das bisher Gesagte zeigt, dass die Mathematische Logik eng mit dem Ziel verbunden ist, der Mathematik eine solide Grundlage zu geben. Wir beschränken uns in dieser Hinsicht jedoch auf die Logik und ihr faszinierendes Wechselspiel mit der Mathematik. Die Geschichte lehrt, dass es unmöglich ist, eine programmatische Ansicht über die Grundlagen der Mathematik zu etablieren, welche die Gemeinschaft der Mathematiker als Ganzes zufriedenstellt. Die Mathematische Logik ist das richtige Werkzeug um die technischen Grundlagenprobleme der Mathematik zu behandeln, sie kann aber nicht deren epistemologische Fragen klären. Ungeachtet dessen ist die Mathematische Logik wegen ihrer zahlreichen Anwendungen und ihres übergreifenden Charakters zu einer der für die Mathematik und Informatik gleichermaßen bedeutsamen Disziplinen herangewachsen.

Notationen

Diese Notationen betreffen formale und terminologische Elemente der mathematischen Umgangssprache. Sie sind für Leser aufgelistet, die nicht regelmäßig mit Mathematik zu tun haben und müssen nicht in einem Zuge gelesen werden. Fast alle verwendeten Notationen sind Standard. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bezeichnen die Mengen der natürlichen Zahlen einschließlich 0, der ganzen, rationalen bzw. der reellen Zahlen. n, m, i, j, k bezeichnen immer natürliche Zahlen, solange nichts anderes gesagt wird. Daher werden Zusätze wie $n \in \mathbb{N}$ in der Regel unterlassen.

$M \cup N$, $M \cap N$ und $M \setminus N$ bezeichnen wie üblich *Vereinigung*, *Durchschnitt*, bzw. *Differenz* der Mengen M , N , und \subseteq die *Inklusion*. $M \subset N$ steht für $M \subseteq N$ und $M \neq N$, wird aber nur benutzt, wenn der Umstand $M \neq N$ besonders betont werden soll. Ist M in einer Betrachtung fest und $N \subseteq M$, darf $M \setminus N$ auch mit $\setminus N$ (oder $\neg N$) bezeichnet werden. \emptyset bezeichnet die *leere Menge*, $\mathfrak{P}M$ die *Potenzmenge* von M , die Menge aller ihrer Teilmengen. Will man hervorheben, dass die Elemente einer Menge F selbst Mengen sind, heißt F auch eine *Mengenfamilie*. $\bigcup F$ bezeichnet die Vereinigung einer Mengenfamilie F , d.h. die Menge der Elemente, die in wenigstens einem $M \in F$ liegen, und $\bigcap F$ für $F \neq \emptyset$ den Durchschnitt, d.h. die Menge der zu allen $M \in F$ gehörenden Elemente. Ist $F = \{M_i \mid i \in I\}$ indiziert (siehe unten), bezeichnet man $\bigcup F$ und $\bigcap F$ meistens mit $\bigcup_{i \in I} M_i$ bzw. $\bigcap_{i \in I} M_i$.

$M \times N$ bezeichnet die Menge aller geordneten Paare (a, b) mit $a \in M$ und $b \in N$. Eine *Relation* zwischen M und N ist eine Teilmenge von $M \times N$. Ist $f \subseteq M \times N$ und gibt es zu jedem $a \in M$ genau ein $b \in N$ mit $(a, b) \in f$, heißt f eine *Funktion* (*Abbildung*) *von M nach N* . Das durch a eindeutig bestimmte Element b mit $(a, b) \in f$ wird mit $f(a)$ oder fa (die von uns bevorzugte Schreibweise) oder a^f bezeichnet. Man nennt fa den *Wert von f bei a* sowie $\text{ran } f = \{fx \mid x \in M\}$ das *Bild* (range) von f , während $\text{dom } f = M$ der *Definitionsbereich* (domain) von f heißt. Man schreibt $f: M \rightarrow N$ für ‘ f ist Funktion mit $\text{dom } f = M$ und $\text{ran } f \subseteq N$ ’¹⁾. Oft wird aber auch f selbst durch $f: M \rightarrow N$ zitiert. Ist $f(x) = t(x)$ für einen Term t , wird f auch mit $f: x \mapsto t$ oder $x \mapsto t$ bezeichnet. Terme werden in **2.2** erklärt.

$f: M \rightarrow N$ heißt *injektiv*, wenn $fx = fy \Rightarrow x = y$, für alle $x, y \in M$, *surjektiv*, wenn $\text{ran } f$ ganz N ausfüllt, und *bijektiv*, wenn f injektiv und surjektiv ist. Für $M = N$ ist die *identische Abbildung* $\text{id}_M: x \mapsto x$ Beispiel einer Bijektion. Sind f, g Abbildungen mit $\text{ran } g \subseteq \text{dom } f$, heißt die Funktion $h: x \mapsto f(g(x))$ auch deren *Produkt* (oder deren *Komposition*), oft notiert als $h = f \circ g$.

¹⁾Hochkommata dienen hier wie überall in diesem Buch der Abgrenzung gewisser Sprachpartikel, wie z.B. in Worten formulierter Prädikate, vom umgebenden Text.

Seien I, M beliebige Mengen, wobei I , ziemlich willkürlich, die *Indexmenge* genannt werde. M^I bezeichne die Menge aller $f: I \rightarrow M$. Oft wird eine Funktion $f \in M^I$ mit $i \mapsto a_i$ durch $(a_i)_{i \in I}$ bezeichnet und heißt je nach Zusammenhang eine indizierte *Familie*, ein *I -Tupel* oder eine *Folge*. Diese heißt *endlich* oder *unendlich*, je nachdem ob I endlich oder unendlich ist. Falls, wie in der Mengenlehre üblich, 0 mit \emptyset , und $n > 0$ mit $\{0, 1, \dots, n-1\}$ identifiziert wird, lässt M^n sich verstehen als die Menge der Folgen oder n -Tupel $(a_i)_{i < n}$ aus Elementen von M der Länge n . Einziges Element von $M^0 (= M^\emptyset)$ ist \emptyset , auch die *leere Folge* genannt. Diese hat die Länge 0. Gleichwertige Schreibweisen für $(a_i)_{i < n}$ bzw. $(a_i)_{i \leq n}$ sind (a_0, \dots, a_{n-1}) und (a_0, \dots, a_n) . Das Aneinanderfügen endlicher Folgen heißt auch deren *Verkettung*. So ist (a_0, a_1, a_2) verkettet mit (b_0, b_1) die Folge $(a_0, a_1, a_2, b_0, b_1)$.

Für $k \leq n$ heißt $(a_i)_{i \leq k}$ ein *Anfang* von $(a_i)_{i \leq n}$, und zwar ein *echter* Anfang, falls $k < n$. Häufig betrachten wir auch Folgen der Gestalt (a_1, \dots, a_n) , im Text durchweg mit \vec{a} bezeichnet. Hier ist für $n = 0$ die leere Folge gemeint, genau wie $\{a_1, \dots, a_n\}$ für $n = 0$ grundsätzlich die leere Menge bedeutet.

Ist A ein *Alphabet*, d.h. sind die Elemente von A *Symbole* oder werden sie als solche bezeichnet, wird (a_1, \dots, a_n) meistens in der Weise $a_1 \cdots a_n$ geschrieben und heißt ein *Wort* oder eine *Zeichenfolge* über A . Die leere Folge wird dann konsequenterweise das *leere Wort* genannt. Ein Anfang einer Zeichenfolge ξ heißt auch ein *Anfangswort* von ξ . Die Verkettung zweier Worte ξ und η werde mit $\xi\eta$ bezeichnet. Falls $\xi = \xi_1\eta\xi_2$ für gewisse Worte ξ_1, ξ_2 und $\eta \neq \emptyset$, heißt η auch ein *Teilwort* von ξ .

Teilmengen $P, Q, R, \dots \subseteq M^n$ heißen *n -stellige Prädikate* oder *Relationen* von M , $n \geq 1$. Einstellige Prädikate werden mit den entsprechenden Teilmengen von M identifiziert, z.B. das Primzahlprädikat mit der Menge aller Primzahlen. Statt $\vec{a} \in P$ schreiben wir $P\vec{a}$, statt $\vec{a} \notin P$ auch $\neg P\vec{a}$. Falls $P \subseteq M^2$ und P ein Symbol ist wie z.B. $\triangleleft, <, \leq, \in$, wird aPb statt Pab geschrieben, also $a \triangleleft b$ statt $\triangleleft ab$ usw. Für $P \subseteq M^n$ heiße die durch

$$\chi_P \vec{a} = \begin{cases} 1 & \text{falls } P\vec{a}, \\ 0 & \text{falls } \neg P\vec{a} \end{cases}$$

definierte n -stellige Funktion χ_P die *charakteristische Funktion* von P . Dabei ist unerheblich, ob man die Werte 0, 1 als Wahrheitswerte oder als natürliche Zahlen versteht wie dies in Kapitel 6 geschieht, oder ob 0 und 1 in der Definition gar vertauscht werden. Wichtig ist nur, dass P durch χ_P eindeutig bestimmt ist.

Jedes $f: M^n \rightarrow M$ heißt eine *n -stellige Operation* von M . Meistens schreiben wir $f\vec{a}$ für $f(a_1, \dots, a_n)$. Eine 0-stellige Operation von M hat wegen $A^0 = \{\emptyset\}$ die Gestalt $\{(\emptyset, c)\}$ mit $c \in M$; diese wird kurz mit c bezeichnet und heißt eine *Konstante*. Jede n -stellige Operation von f von M wird durch

$$\text{graph } f := \{(a_1, \dots, a_{n+1}) \in M^{n+1} \mid f(a_1, \dots, a_n) = a_{n+1}\}$$

eindeutig beschrieben. Es handelt sich hier um eine $(n + 1)$ -stellige Relation, welche der *Graph von f* genannt wird. f und $\text{graph } f$ sind dasselbe, wenn – wie dies gelegentlich geschieht – M^{n+1} mit $M^n \times M$ identifiziert wird.

Am häufigsten werden 2-stellige Operationen angetroffen. Bei diesen wird das entsprechende Operationssymbol in der Regel zwischen die Argumente gesetzt. Eine derartige, hier mit \circ bezeichnete Operation $\circ : M^2 \rightarrow M$ heißt

<i>kommutativ</i>	wenn $a \circ b = b \circ a$ für alle $a, b \in M$,
<i>assoziativ</i>	wenn $a \circ (b \circ c) = (a \circ b) \circ c$ für alle $a, b, c \in M$,
<i>idempotent</i>	wenn $a \circ a = a$ für alle $a \in M$,
<i>invertierbar</i>	wenn zu allen $a, b \in M$ Elemente $x, y \in M$ existieren mit $x \circ a = b$ und $a \circ y = b$.

Als Verallgemeinerung von $M_1 \times M_2$ lässt sich das *direkte Produkt* $N = \prod_{i \in I} M_i$ einer Mengenfamilie $(M_i)_{i \in I}$ verstehen. Jedes $a \in N$ ist eine auf I erklärte Funktion $a = (a_i)_{i \in I}$ mit $a_i \in M_i$ (eine *Auswahlfunktion*). a_i heißt auch die *i -te Komponente* von a . Falls $M_i = M$ für alle $i \in I$, ist $\prod_{i \in I} M_i$ offenbar mit M^I identisch. Dies gilt auch für $I = \emptyset$, weil $\prod_{i \in I} M_i = \{\emptyset\}$ und auch $M^I = \{\emptyset\}$.

Bezeichnen A, B metasprachliche Ausdrücke, stehen $A \Leftrightarrow B$, $A \Rightarrow B$, $A \& B$ und $A \vee B$ für *A genau dann wenn B* , *wenn A so B* , *A und B* bzw. *A oder B* . Dabei sollen die Symbole $\Rightarrow, \Leftrightarrow, \dots$ stärker trennen als sprachliche Bindungspartikel. Deshalb darf in einem Textteil wie z.B. ‘ $T \models \alpha \Leftrightarrow \alpha \in T$, für alle $\alpha \in \mathcal{L}^0$ ’ (Seite 64) das Komma nicht fehlen, weil ‘ $\alpha \in T$ für alle $\alpha \in \mathcal{L}^0$ ’ fälschlicherweise gelesen werden könnte als ‘ T ist inkonsistent’.

$s := t$ bedeutet, dass s durch den Term t definiert wird, oder wenn s eine Variable ist, auch die Zuweisung des Wertes von t zu s . Für Terme s, t sei $s > t$ grundsätzlich nur eine andere Schreibweise für $t < s$. Dieselbe Bemerkung bezieht sich auch auf andere unsymmetrische Relationssymbole wie \leq, \subseteq usw.

In der mathematischen Umgangssprache werden Formeln oft direkt in den Text integriert und man bedient sich dabei auch gewisser verkürzender Schreibweisen. So wie man z.B. ‘ $a < b$ und $b < c$ ’ häufig zu ‘ $a < b < c$ ’, oder ‘ $a < b$ und $b \in M$ ’ zu ‘ $a < b \in M$ ’ verkürzt, darf ‘ $X \vdash \alpha \equiv \beta$ ’ für ‘ $X \vdash \alpha$ und $\alpha \equiv \beta$ ’ geschrieben werden (‘aus der Formelmenge X ist die Formel α beweisbar und α ist äquivalent zu β ’). Das Symbol \equiv wird in diesem Buch nur metasprachlich verwendet, kommt also in keiner der behandelten formalen Sprachen vor.

Kapitel 1

Aussagenlogik

Die Aussagenlogik, worunter hier die 2-wertige Aussagenlogik verstanden sei, entstand aus der Analyse von Verknüpfungen gegebener Aussagen A, B , wie z.B.

A und B, A oder B, nicht A, wenn A so B.

Dies sind Verknüpfungen, die sich mit 2-wertiger Logik näherungsweise beschreiben lassen. Es gibt andere Aussagenverknüpfungen mit temporalem oder lokalem Aspekt, wie etwa *erst A dann B*, oder *hier A dort B* sowie modale Verknüpfungen aller Art, deren Analyse den Rahmen einer 2-wertigen Logik übersteigt und die Gegenstand einer temporalen, modalen oder sonstigen Teildisziplin einer mehrwertigen oder nichtklassischen Logik sind. Auch die anfänglich erwähnten Verknüpfungen haben in anderen Auffassungen von Logik und auch in der natürlichen Sprache oft einen Sinn, der mit 2-wertiger Logik nur unvollständig zu erfassen ist.

Von diesen Phänomenen wird in der 2-wertigen Aussagenlogik abstrahiert. Das vereinfacht die Betrachtungen erheblich und hat überdies den Vorteil, dass sich viele Begriffe wie der des Folgerns, der Regelinduktion, der Resolution usw. auf einer einfachen und durchsichtigen Ebene präsentieren lassen. Dies spart viele Worte, wenn in Kapitel 2 die entsprechenden prädikatenlogischen Begriffe zur Debatte stehen.

Wir behandeln hier nicht alles, was im Rahmen 2-wertiger Aussagenlogik einer Behandlung zugänglich ist, etwa 2-wertige Fragmente und Probleme der Definierbarkeit und Interpolation. Der Leser sei diesbezüglich z.B. auf [KK] oder [Ra1] verwiesen. Dafür wird etwas mehr über aussagenlogische Kalküle gesagt.

Es gibt vielfältige Anwendungen der Aussagenlogik. Wir verzichten aber auf die Darstellung direkter technischer Anwendungen, etwa in der Synthese logischer Schaltungen und dazugehörigen Optimierungsproblemen, sondern beschreiben ausführlich einige nützliche Anwendungen des Kompaktheitssatzes.

1.1 Boolesche Funktionen und Formeln

Die 2-wertige Logik beruht auf zwei Grundprinzipien, dem *Zweiwertigkeitsprinzip*, welches nur zwei Wahrheitswerte in Betracht zieht, nämlich *wahr* und *falsch*, sowie dem *Extensionalitätsprinzip*. Danach hängt der Wahrheitswert einer zusammengesetzten Aussage nur von den Wahrheitswerten ihrer Bestandteile ab, nicht aber noch von deren Sinn. Es ist plausibel, dass durch diese beiden Prinzipien in der Regel nur eine Idealisierung tatsächlicher Verhältnisse formuliert wird.

Fragen nach Wahrheitsgraden oder dem Sinngehalt von Aussagen werden in der 2-wertigen Logik ignoriert. Dennoch oder gerade deswegen ist dies eine erfolgreiche wissenschaftliche Methode. Man muss nicht einmal wissen, was genau die beiden nachfolgend mit 1 und 0 bezeichneten Wahrheitswerte *wahr* und *falsch* eigentlich sind. Man darf sie, wie dies im Folgenden auch geschieht, getrost mit den beiden Symbolen 1 und 0 identifizieren, oder mit anderen gefälligen Symbolen, z.B. \top und \perp , oder \mathbf{t} und \mathbf{f} . Das hat den Vorteil, dass alle denkbaren Interpretationen von *wahr* und *falsch* offengehalten werden, z.B. auch solche rein technischer Natur, etwa die beiden Zustände eines Schaltelements in einem logischen Schaltkreis.

Unter einer *n*-stelligen *Booleschen Funktion* oder *Wahrheitsfunktion* verstehe man eine beliebige Funktion $f: \{0, 1\}^n \mapsto \{0, 1\}$. Deren Gesamtheit sei mit \mathbf{B}_n bezeichnet. \mathbf{B}_0 enthält nur die beiden Konstanten 0 und 1. Die *Negation* \neg mit $\neg 1 = 0$ und $\neg 0 = 1$ ist eine der vier 1-stelligen Booleschen Funktionen. Weil es 2^n viele *n*-Tupel aus 0, 1 gibt, sieht man leicht, dass \mathbf{B}_n genau 2^{2^n} viele Funktionen enthält.

Die Konjunktion *A und B* aus den beiden Aussagen *A, B*, die in formalisierten Sprachen meist mit $A \wedge B$ oder $A \& B$ bezeichnet wird, ist nach dem Wortsinn von *und* genau dann wahr, wenn *A, B* beide wahr sind, und sonst falsch. Der Konjunktion entspricht also eine 2-stellige Boolesche Funktion, die \wedge -Funktion oder *et-Funktion* und häufig kurz mit \wedge bezeichnet. Diese ist durch ihre *Wertetabelle* oder *Wertematrix* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ gegeben. Dabei bezeichne stets $\begin{pmatrix} 1 \circ 1 & 1 \circ 0 \\ 0 \circ 1 & 0 \circ 0 \end{pmatrix}$ die Wertematrix einer 2-stelligen Booleschen Funktion \circ , also $1 \wedge 1 = 1$, sowie $1 \wedge 0 = 0 \wedge 1 = 0 \wedge 0 = 0$.

Die Tabelle auf der nächsten Seite enthält in der ersten Spalte die gebräuchlichen 2-stelligen Aussagenverknüpfungen mit Beispielen ihrer sprachlichen Realisierung, in der zweiten Spalte ihre wichtigsten Symbole und in der dritten die Wertematrix der entsprechenden Wahrheitsfunktion. Die Disjunktion ist das *nichtausschließende oder*. Sie ist klar zu unterscheiden von der *Antivalenz* (dem *ausschließenden oder*). Letztere entspricht der Addition modulo 2, deswegen die Bezeichnung durch $+$. In schalttechnischen Systemen werden die Funktionen $+$, \downarrow , \uparrow oft durch *xor*, *nor* und *nand* symbolisiert. Die letztgenannte heißt auch die *Sheffer-Funktion*.

Man muss eine Aussagenverknüpfung und die entsprechende Wahrheitsfunktion nicht gleichbezeichnen – z.B. könnte man \wedge für die Konjunktion und *et* für die entsprechende Boolesche Funktion wählen – aber damit erschafft man nur neue Bezeichnungen, keine neuen Einsichten. Die Bedeutung eines Symbols wird stets aus dem Zusammenhang hervorgehen. Sind α, β Aussagen einer formalen Sprache, so bezeichnet z.B. $\alpha \wedge \beta$ deren Konjunktion; sind a, b hingegen Wahrheitswerte, bezeichnet $a \wedge b$ eben einen Wahrheitswert. Mitunter möchte man allerdings auch über die logischen Symbole $\wedge, \vee, \neg, \dots$ selbst reden und ihre Bedeutungen vorübergehend in den Hintergrund drängen. Man spricht dann von den *Junktoren* $\wedge, \vee, \neg, \dots$.

Aussagenverknüpfung	Symbol	Wertematrix
Konjunktion <i>A und B;</i> <i>Sowohl A als auch B</i>	$\wedge, \&$	$\begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix}$
Disjunktion (Alternative) <i>A oder B</i>	\vee	$\begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$
Implikation (Subjunktion) <i>Wenn A so B; Aus A folgt B;</i> <i>A nur dann wenn B</i>	\rightarrow, \Rightarrow	$\begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}$
Äquivalenz (Bijunktion) <i>A genau dann wenn B;</i> <i>A dann und nur dann wenn B</i>	$\leftrightarrow, \Leftrightarrow$	$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$
Antivalenz <i>Entweder A oder B</i>	$+$	$\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$
Nihilation <i>Weder A noch B</i>	\downarrow	$\begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix}$
Unverträglichkeit <i>Nicht zugleich A und B</i>	\uparrow	$\begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}$

Aussagen, die mit den in der Tabelle angegebenen oder weiteren Verknüpfungen zusammengesetzt sind, können in dem Sinne bedeutungsgleich oder logisch äquivalent sein, dass ihnen bei jeweils gegebenen Wahrheitswerten ihrer Bestandteile stets derselbe Wahrheitswert entspricht. Dies ist z.B. der Fall bei den Aussagen

$$A \text{ sofern } B, \quad A \text{ falls } B, \quad A \text{ oder nicht } B.$$

Diese Verknüpfung wird gelegentlich auch mit $A \leftarrow B$ bezeichnet und heie die *konverse Implikation*. Sie erschien deswegen nicht in der Tabelle, weil sie durch Vertauschen der Argumente A, B aus der Implikation hervorgeht. Diese und hnliche

Gründe sind dafür verantwortlich, warum nur wenige der 16 zweistelligen Booleschen Funktionen einer Bezeichnung überhaupt bedürfen.

Um logische Äquivalenzen zu erkennen und zu beschreiben ist die Schaffung eines Formalismus oder einer formalen Sprache nützlich. Die Situation ist vergleichbar mit derjenigen in der Arithmetik, wo sich allgemeine Gesetzmäßigkeiten bequemer und klarer mittels gewisser Formeln zum Ausdruck bringen lassen.

Wir betrachten aussagenlogische Formeln genau wie arithmetische Terme als Zeichenfolgen, die in bestimmter Weise aus Grundsymbolen aufgebaut sind. Zu den Grundsymbolen zählen hier wie dort sogenannte Variablen, die im vorliegenden Falle *Aussagenvariablen* heißen und deren Gesamtheit mit AV bezeichnet sei. Meist wählt man hierfür einer Tradition entsprechend die Symbole p_0, p_1, \dots . Die Variablennummerierung unten beginnt aber mit p_1 , was einer bequemer Darstellung Boolescher Funktionen dient. Zu den Grundsymbolen gehören ferner gewisse logische Zeichen wie $\wedge, \vee, \neg, \dots$, die auf der arithmetischen Ebene den Zeichen $+, \cdot, \dots$ entsprechen. Schließlich verwendet man meistens gewisse technische Hilfssymbole, nachfolgend nur die beiden Klammern $(,)$.

Jedesmal, wenn von einer aussagenlogischen Sprache die Rede ist, muss die Menge AV ihrer Variablen und die Menge der logischen Symbole, ihre *logische Signatur*, vorgegeben sein. So ist für Anwendungen der Aussagenlogik wie z.B. in Abschnitt 1.5 wichtig, dass AV eine beliebige Menge sein kann und nicht wie oben angedeutet abzählbar sein muss. Um konkret zu sein definieren wir ausgehend von den Symbolen $(,), \wedge, \vee, \neg, p_1, p_2, \dots$ eine aussagenlogische Sprache \mathcal{F} wie folgt:

Rekursive Formelbestimmung

(F1) Die Variablen p_1, p_2, \dots sind Formeln, auch *Primformeln* genannt.

(F2) Sind α, β Formeln, so auch die Zeichenfolgen $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$ und $\neg \alpha$.

Diese Erklärung ist so zu verstehen, dass nur die nach (F1) und (F2) bestimmten Zeichenfolgen in diesem Zusammenhang Formeln sind. Mit anderen Worten, \mathcal{F} ist die kleinste (d.h. der Durchschnitt) aller Mengen Z von Zeichenfolgen aus obigen Symbolen mit den Eigenschaften

$$(f1) \ p_1, p_2, \dots \in Z, \quad (f2) \ \alpha, \beta \in Z \Rightarrow (\alpha \wedge \beta), (\alpha \vee \beta), \neg \alpha \in Z.$$

Beispiel. $(p_1 \wedge (p_2 \vee \neg p_1))$ ist eine Formel. Deren Anfang $(p_1 \wedge (p_2 \vee \neg p_1)$ hingegen nicht, weil eine schließende Klammer fehlt. Denn es ist anschaulich klar und wird weiter unten streng bewiesen, dass die Anzahl der in einer Formel vorkommenden Linksklammern identisch ist mit der Anzahl der dort vorkommenden Rechtsklammern. Jeder echte Anfang der obigen Formel verletzt offenbar diese Bedingung.

Die so definierten Formeln bezeichnen wir etwas genauer als *Boolesche Formeln*, weil sie mit der *Booleschen Signatur* $\{\wedge, \vee, \neg\}$ erzeugt wurden. Wenn weitere Junktoren zur logischen Signatur gehören sollen wie etwa \rightarrow oder \leftrightarrow , muss (F2) entsprechend erweitert werden. Solange aber nichts anderes gesagt wird, sind $(\alpha \rightarrow \beta)$ und $(\alpha \leftrightarrow \beta)$ nur Abkürzungen: $(\alpha \rightarrow \beta) := \neg(\alpha \wedge \neg\beta)$ und $(\alpha \leftrightarrow \beta) := ((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha))$. Einem solchen Vorgehen liegen natürlich entsprechende logische Äquivalenzen zugrunde. Gelegentlich ist es nützlich, Symbole für das stets Falsche und das stets Wahre in der logischen Signatur zu haben, etwa \perp und \top , *Falsum* und *Verum* genannt und auch mit 0 und 1 bezeichnet. Diese sind als zusätzliche Primformeln zu verstehen, und Klausel (F1) ist entsprechend zu erweitern. In der Booleschen Signatur lassen sich \perp und \top etwa durch $\perp := (p_1 \wedge \neg p_1)$ und $\top := \neg \perp$ definieren.

Vorerst sei \mathcal{F} die Menge aller Booleschen Formeln. Doch gilt alles, was nachfolgend über \mathcal{F} gesagt wird, sinngemäß auch für Formeln einer beliebigen aussagenlogischen Sprache. Aussagenvariablen werden im Folgenden mit den Buchstaben p, q, \dots bezeichnet, Formeln mit $\alpha, \beta, \gamma, \delta, \varphi, \dots$, Primformeln auch mit π , und Formelmengen mit X, Y, Z , wobei diese Buchstaben auch indiziert sein können.

Zwecks Klammerersparnis bei der Niederschrift von Formeln verabreden wir gewisse Regeln, die in ähnlicher Form auch bei der Niederschrift arithmetischer Terme verwendet werden. Hierin bezeichnet \circ einen beliebigen 2-stelligen Junktor.

1. Außenklammern in Formeln der Gestalt $(\alpha \circ \beta)$ dürfen weggelassen werden. Es darf also z.B. $\neg p_1 \vee (p_2 \wedge p_1)$ für $(\neg p_1 \vee (p_2 \wedge p_1))$ geschrieben werden;
2. In der Reihenfolge $\wedge, \vee, \rightarrow, \leftrightarrow$ trennt jeder Junktor stärker als alle vorangehenden. Man darf z.B. $\neg p_1 \vee p_2 \wedge p_1$ statt $(\neg p_1 \vee (p_2 \wedge p_1))$ schreiben;
3. Bei mehrfacher Zusammensetzung mit demselben Junktor wird Rechtsklammerung¹⁾ verwendet. So steht $\alpha_0 \rightarrow \alpha_1 \rightarrow \alpha_2$ für $\alpha_0 \rightarrow (\alpha_1 \rightarrow \alpha_2)$. Anstelle von $\alpha_0 \wedge \dots \wedge \alpha_n$ und $\alpha_0 \vee \dots \vee \alpha_n$ wird auch $\bigwedge_{i \leq n} \alpha_i$ bzw. $\bigvee_{i \leq n} \alpha_i$ geschrieben.

Solche Verabredungen beruhen auf einer verlässlichen Syntax, in deren Rahmen auch anschaulich klare Tatsachen – z.B. die Übereinstimmung der Anzahlen der Links- und Rechtsklammern in einer Formel – streng beweisbar sind. Derartige Beweise führt man in der Regel induktiv über den Formelaufbau. Um dies zu verdeutlichen, notieren wir das Zutreffen einer Eigenschaft \mathcal{E} auf eine Zeichenfolge φ einfach durch $\mathcal{E}\varphi$. Zum Beispiel bedeute \mathcal{E} ‘In φ kommen gleichviele Rechts- wie Linksklammern vor’. Dann gilt \mathcal{E} trivialerweise für Primformeln, und gelten $\mathcal{E}\alpha, \mathcal{E}\beta$, so offenbar auch $\mathcal{E}(\alpha \wedge \beta), \mathcal{E}(\alpha \vee \beta)$ und $\mathcal{E}\neg\alpha$. Daraus darf man schließen, dass \mathcal{E} auf alle Formeln zutrifft. Denn dies ist ein besonders einfacher Anwendungsfall von folgendem

¹⁾Diese hat gegenüber Linksklammerung Vorteile bei der Niederschrift von Tautologien in \rightarrow , siehe 1.3.

Beweisprinzip durch Formelinduktion. *Es sei \mathcal{E} eine Eigenschaft von Zeichenfolgen derart, dass*

- (o) $\mathcal{E}\pi$ für alle Primformeln π ,
- (s) $\mathcal{E}\alpha, \mathcal{E}\beta \Rightarrow \mathcal{E}(\alpha \wedge \beta), \mathcal{E}(\alpha \vee \beta), \mathcal{E}\neg\alpha$, für alle $\alpha, \beta \in \mathcal{F}$.

Dann gilt $\mathcal{E}\varphi$ für alle Formeln φ .

Die Rechtfertigung dieses Prinzips ist einfach: Die Menge Z aller Zeichenfolgen mit der Eigenschaft \mathcal{E} genügt wegen (o) und (s) den Bedingungen (f1) und (f2) Seite 4. Nun ist \mathcal{F} aber die kleinste Menge dieser Art. Also $\mathcal{F} \subseteq Z$, d.h. $\mathcal{E}\varphi$ gilt für alle φ .

Man bestätigt induktiv leicht den anschaulich klaren Sachverhalt, dass eine zusammengesetzte Formel $\varphi \in \mathcal{F}$ (d.h. φ ist keine Primformel) entweder von der Gestalt $\neg\alpha$ oder $(\alpha \circ \beta)$ mit $\alpha, \beta \in \mathcal{F}$ und $\circ \in \{\wedge, \vee\}$ ist. Weniger einfach ist der Nachweis, dass eine derartige Zerlegung eindeutig ist, auch die *eindeutige Rekonstruktionseigenschaft* genannt. Zum Beispiel hat $(\alpha \wedge \beta)$ keine Zerlegung $(\alpha' \vee \beta')$ mit anderen Formeln α', β' . Um aber den Fluss der Dinge nicht aufzuhalten, behandeln wir diese Sachverhalte mit ausreichenden Hinweisen in den Übungen,

Bemerkung 1. Klammern werden für die eindeutige Rekonstruktionseigenschaft nicht wirklich benötigt. Vielmehr lassen sich aussagenlogische Formeln, ebenso wie z.B. auch arithmetische Terme, klammerfrei notieren, und zwar in *polnischer Notation*, oder auch in umgekehrter polnischer Notation, die in einigen Programmiersprachen Verwendung findet. Die Idee besteht darin, (F2) wie folgt zu verändern: Mit α, β sind auch die Zeichenfolgen $\wedge\alpha\beta$, $\vee\alpha\beta$, $\neg\alpha$ Formeln. Die umgekehrte polnische Notation unterscheidet sich von der angegebenen nur dadurch, dass die Junktoren den Argumenten nachgestellt werden. Die Entzifferung dieser Notationen ist für ungeübte Leser etwas mühsam, denn sie haben eine sehr hohe Informationsdichte. Dafür können Computer sie besonders schnell lesen und verarbeiten. Die Klammernotation hat gegenüber den klammerfreien im Grunde nur den Vorteil, dass sie die optische Entzifferung durch „Informationsverdünnung“ erleichtert. Obwohl die eindeutige Rekonstruktion für die Polnische Notation nicht unmittelbar evident ist, ist der Beweis nicht schwieriger als für die Klammernotation. Ganz einfach wird dieser Nachweis übrigens dann, wenn man eine Boolesche Formel nicht als Zeichenfolge, sondern als ein spezielles Tupel von Zeichenfolgen definiert, das die Entstehungsgeschichte der Formel kodiert. Es gibt demnach durchaus mehrere Präzisionsmöglichkeiten des Begriffs einer aussagenlogischen Formel.

Anschaulich ist klar, was eine *Subformel* (oder *Teilformel*) einer Formel φ ist. Zum Beispiel ist $(p_2 \wedge p_1)$ eine Subformel von $(\neg p_1 \vee (p_2 \wedge p_1))$. Auch sollte jede Formel Subformel von sich selbst sein. Für manche Zwecke ist es jedoch bequemer, die Menge $Sf\varphi$ aller Subformeln von φ wie folgt zu kennzeichnen:

$$Sf\pi = \{\pi\} \text{ für Primformeln } \pi \quad ; \quad Sf\neg\alpha = Sf\alpha \cup \{\neg\alpha\},$$

$$Sf(\alpha \circ \beta) = Sf\alpha \cup Sf\beta \cup \{(\alpha \circ \beta)\} \text{ für einen 2-stelligen Junktor } \circ.$$

Hier liegt eine rekursive (oder induktive) Definition über den Formelaufbau vor. Ähnlich erklärt man z.B. auch den mit $\text{rg } \varphi$ bezeichneten *Rang* von φ , der ein mitunter bequemer Komplexitätsmaß für φ darstellt als die Länge von φ als Zeichenfolge. Sei $\text{rg } \pi = 0$ für Primformeln π , und wenn $\text{rg } \alpha$ und $\text{rg } \beta$ schon definiert sind, sei

$$\text{rg } \neg \alpha = \text{rg } \alpha + 1, \quad \text{rg}(\alpha \wedge \beta) = \text{rg}(\alpha \vee \beta) = \max\{\text{rg } \alpha, \text{rg } \beta\} + 1.$$

Wir verzichten auf eine allgemeine Formulierung dieses Definitionsverfahrens, weil es sehr anschaulich ist und durch die obigen und noch folgenden Beispiele ausreichend verdeutlicht wird. Seine Rechtfertigung beruht, wie man sich denken kann, wesentlich auf der eindeutigen Rekonstruktionseigenschaft. Ist eine Eigenschaft durch Formelinduktion über den Aufbau von φ zu beweisen, wird dies oft schlagwortartig als *Beweis durch Induktion über φ* angekündigt. Analog wird die rekursive Definition einer auf \mathcal{F} erklärten Funktion f oft kurz durch die Redewendung *wir definieren f rekursiv* (nicht ganz treffend auch *induktiv*) über φ angekündigt.

Da die Wahrheitswerte zusammengesetzter Aussagen nur abhängen von den Wahrheitswerten ihrer aussagenlogischen Bestandteile, dürfen wir den Aussagenvariablen in Formeln φ statt Aussagen auch Wahrheitswerte zuordnen, oder wie man zu sagen pflegt, diese mit Wahrheitswerten *belegen*. Für jede solche Belegung lässt φ sich auswerten, also ein Wahrheitswert errechnen. Ähnlich wird in der reellen Arithmetik ein Term ausgewertet, nur ist dessen Wert dann eine reelle Zahl. Ein arithmetischer Term t in den Variablen x_1, \dots, x_n beschreibt eine n -stellige reelle Funktion, eine Formel φ in den Variablen p_1, \dots, p_n hingegen eine n -stellige Boolesche Funktion. Dabei müssen nicht alle Variablen p_1, \dots, p_n in φ wirklich vorkommen.

Um das Gesagte kurz zu formulieren, heiße eine Abbildung $w: AV \rightarrow \{0, 1\}$ eine aussagenlogische *Belegung*, auch (aussagenlogisches) *Modell* genannt. w lässt sich rekursiv über den Formelaufbau eindeutig zu einer ebenfalls mit w bezeichneten Abbildung von ganz \mathcal{F} nach $\{0, 1\}$ fortsetzen: Es sei einfach $w(\alpha \wedge \beta) = w\alpha \wedge w\beta$, $w(\alpha \vee \beta) = w\alpha \vee w\beta$ und $w\neg\alpha = \neg w\alpha$. Dabei bezeichnen \wedge , \vee , \neg auf der rechten Seite dieser Gleichungen natürlich die entsprechenden Booleschen Funktionen. Wenn vom *Wert $w\alpha$ einer Formel α bei der Belegung w der Variablen* die Rede ist, meint man den sich gemäß dieser Fortsetzung ergebenden Wert. Man könnte die erweiterte Abbildung z.B. auch mit \hat{w} bezeichnen, doch ist eine Bezeichnungs-Unterscheidung dieser Abbildung von $w: AV \rightarrow \{0, 1\}$ nicht zwingend.

Enthält die logische Signatur auch andere Junktoren, ist die Wertbestimmung entsprechend zu ergänzen, z.B. durch $w(\alpha \rightarrow \beta) = w\alpha \rightarrow w\beta$. Ist $\alpha \rightarrow \beta$ hingegen definiert wie bei uns, muss diese Gleichung beweisbar sein. In der Tat, sie ist es, denn $w(\alpha \rightarrow \beta) = w\neg(\alpha \wedge \neg\beta) = \neg w(\alpha \wedge \neg\beta) = \neg(w\alpha \wedge \neg w\beta) = w\alpha \rightarrow w\beta$. Auch \perp und \top wurden so definiert, dass stets $w\perp = 0$ und $w\top = 1$.

Es bezeichne \mathcal{F}_n die Menge der Formeln von \mathcal{F} in höchstens den Variablen p_1, \dots, p_n , $n > 0$. Dann ist plausibel, dass $w\alpha$ für $\alpha \in \mathcal{F}_n$ lediglich abhängt von den Werten der p_1, \dots, p_n . Also $(*)$: $w\alpha = w'\alpha$, wenn $wp_i = w'p_i$ für $i = 1, \dots, n$. Der einfache Beweis erfolgt durch Induktion über den Aufbau der Formeln aus \mathcal{F}_n : $(*)$ ist richtig für $p \in \mathcal{F}_n$, und gilt $(*)$ für $\alpha, \beta \in \mathcal{F}_n$, so offenbar auch für $\neg\alpha, \alpha \wedge \beta$ und $\alpha \vee \beta$.

Definition. Die Formel $\alpha \in \mathcal{F}_n$ repräsentiert die n -stellige Boolesche Funktion f , falls $w\alpha = fw\vec{p}$ für alle Belegungen w ; dabei sei $w\vec{p} := (wp_1, \dots, wp_n)$.

Weil $w\alpha$ für $\alpha \in \mathcal{F}_n$ durch wp_1, \dots, wp_n schon eindeutig festgelegt ist, repräsentiert α nur genau eine Funktion $f \in \mathbf{B}_n$, die gelegentlich auch mit $\alpha^{(n)}$ bezeichnet wird. So repräsentieren $p_1 \wedge p_2$ und $\neg(\neg p_1 \vee \neg p_2)$ beide die \wedge -Funktion, wie man sich anhand einer Tabelle leicht klarmacht. $\neg p_1 \vee p_2$ und $\neg(p_1 \wedge \neg p_2)$ repräsentieren beide die \rightarrow -Funktion, und $p_1 \vee p_2$, $\neg(\neg p_1 \wedge \neg p_2)$ und $(p_1 \rightarrow p_2) \rightarrow p_2$ allesamt die \vee -Funktion. Die *oder*-Verknüpfung ist demnach allein durch die Implikation ausdrückbar.

Man beachte hierbei: Da z.B. $\alpha := p_1 \vee p_2$ nicht nur zu \mathcal{F}_2 , sondern auch zu \mathcal{F}_3 gehört, wird auch die Boolesche Funktion $f: (x_1, x_2, x_3) \mapsto x_1 \vee x_2$ durch α repräsentiert. Das dritte Argument ist allerdings nur ein „fiktives“, oder anders formuliert, f ist „nicht wesentlich“ 3-stellig, ebensowenig wie $(x_1, x_2, x_3) \mapsto x_1 \vee x_3$.

Bemerkung 2. Allgemein heißt eine Operation $f: M^n \rightarrow M$ *wesentlich n -stellig*, wenn f keine fiktiven Argumente hat. Dabei heißt das i -te Argument von f ein *fiktives*, wenn

$$f(x_1, \dots, x_i, \dots, x_n) = f(x_1, \dots, x'_i, \dots, x_n), \text{ für alle } x_1, \dots, x_n, x'_i \in M.$$

Die identische und die \neg -Funktion sind die wesentlich einstelligen Booleschen Funktionen, und von den 16 zweistelligen Funktionen sind nur 10 wesentlich zweistellig. Ist v_n die Anzahl aller und w_n die Anzahl aller wesentlich n -stelligen Booleschen Funktionen, beweist man unschwer $v_n = \sum_{i \leq n} \binom{n}{i} w_i$. Auflösung nach w_n ergibt $w_n = \sum_{i \leq n} (-1)^{n-i} \binom{n}{i} v_i$.

Übungen

1. $f \in \mathbf{B}_n$ heißt *linear*, wenn $f(x_1, \dots, x_n) = a_0 + a_1x_1 + \dots + a_nx_n$ für gewisse $a_0, \dots, a_n \in \{0, 1\}$. Dabei bezeichne $+$ die Addition modulo 2 (exklusive Disjunktion) und es sei $a_ix_i = x_i$ für $a_i = 1$ und $a_ix_i = 0$ sonst. Man bestimme für jedes n die Anzahl der n -stelligen linearen Booleschen Funktionen.
2. Man beweise: ein echter Anfang ξ einer Formel α ist keine Formel.
3. Man beweise mit Hilfe von Übung 2 die eindeutige Rekonstruktionseigenschaft für \mathcal{F} : $(\alpha \circ \beta) = (\alpha' \circ' \beta')$ impliziert $\alpha = \alpha'$, $\circ = \circ'$ und $\beta = \beta'$.
4. Sei ξ eine Zeichenfolge. Man zeige, mit $\neg\xi$ ist auch ξ eine Formel. Ähnlich zeigt man $\alpha, (\alpha \wedge \xi) \in \mathcal{F} \Rightarrow \xi \in \mathcal{F}$ und $\alpha, (\alpha \rightarrow \xi) \in \mathcal{F} \Rightarrow \xi \in \mathcal{F}$.

1.2 Semantische Äquivalenz und Normalformen

Der Buchstabe w bezeichnet bis zum Ende dieses Kapitels immer eine aussagenlogische Belegung oder ihre Fortsetzung auf ganz \mathcal{F} . Formeln α, β heißen (logisch oder semantisch) *äquivalent*, auch *wertverlaufsgleich*, symbolisch $\alpha \equiv \beta$, wenn $w\alpha = w\beta$ für alle w . So ist z.B. $\alpha \equiv \neg\neg\alpha$. Offenbar gilt $\alpha \equiv \beta$ genau dann, wenn für ein beliebiges n mit $\alpha, \beta \in \mathcal{F}_n$ beide Formeln dieselbe n -stellige Boolesche Funktion repräsentieren. Daher können höchstens 2^{2^n} viele Formeln aus \mathcal{F}_n paarweise nicht äquivalent sein, denn es gibt nicht mehr als 2^{2^n} viele Funktionen $f \in \mathbf{B}_n$.

In der Arithmetik schreibt man oft einfach $s = t$ um auszudrücken, dass die Terme s, t dieselbe Funktion repräsentieren; z.B. soll $(x + y)^2 = x^2 + 2xy + y^2$ die Wertverlaufsgleichheit des linken und rechten Terms zum Ausdruck bringen. Das kann man sich erlauben, weil die Termsyntax in der Arithmetik eine untergeordnete Rolle spielt. In der formalen Logik, wie immer dann, wenn syntaktische Betrachtungen im Vordergrund stehen, benutzt man das Gleichheitszeichen in $\alpha = \beta$ nur für die syntaktische Übereinstimmung der Zeichenfolgen α und β . Die Wertverlaufsgleichheit musste daher anders bezeichnet werden. Offenbar gelten für alle α, β, γ

$$\begin{aligned} (\alpha \wedge \beta) \wedge \gamma &\equiv \alpha \wedge \beta \wedge \gamma, & (\alpha \vee \beta) \vee \gamma &\equiv \alpha \vee \beta \vee \gamma && \text{(Assoziativität);} \\ \alpha \wedge \beta &\equiv \beta \wedge \alpha, & \alpha \vee \beta &\equiv \beta \vee \alpha && \text{(Kommutativität);} \\ \alpha \wedge \alpha &\equiv \alpha, & \alpha \vee \alpha &\equiv \alpha && \text{(Idempotenz);} \\ \alpha \wedge (\alpha \vee \beta) &\equiv \alpha, & \alpha \vee \alpha \wedge \beta &\equiv \alpha && \text{(Absorption);} \\ \alpha \wedge (\beta \vee \gamma) &\equiv \alpha \wedge \beta \vee \alpha \wedge \gamma, & \alpha \vee \beta \wedge \gamma &\equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma) && \text{(Distributivität);} \\ \neg(\alpha \wedge \beta) &\equiv \neg\alpha \vee \neg\beta, & \neg(\alpha \vee \beta) &\equiv \neg\alpha \wedge \neg\beta && \text{(DeMorgansche Regeln).} \end{aligned}$$

Ferner ist $\alpha \vee \neg\alpha \equiv \top$, $\alpha \wedge \neg\alpha \equiv \perp$ und $\alpha \wedge \top \equiv \alpha \vee \perp \equiv \alpha$. Es ist nützlich, auch gewisse Äquivalenzen für Formeln aufzulisten, die \rightarrow enthalten, zum Beispiel

$$\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta \equiv \neg\alpha \vee \alpha \wedge \beta; \quad \alpha \rightarrow \beta \rightarrow \gamma \equiv \alpha \wedge \beta \rightarrow \gamma \equiv \beta \rightarrow \alpha \rightarrow \gamma.$$

Eine Verallgemeinerung ist $\alpha_1 \rightarrow \dots \rightarrow \alpha_n \equiv \alpha_1 \wedge \dots \wedge \alpha_{n-1} \rightarrow \alpha_n$. Ferner sei die „Links-distributivität“ von \rightarrow bezüglich \wedge und \vee erwähnt, d.h.

$$\alpha \rightarrow \beta \wedge \gamma \equiv (\alpha \rightarrow \beta) \wedge (\alpha \rightarrow \gamma) \quad ; \quad \alpha \rightarrow \beta \vee \gamma \equiv (\alpha \rightarrow \beta) \vee (\alpha \rightarrow \gamma).$$

Steht das Symbol \rightarrow hingegen rechts, so gelten

$$\alpha \wedge \beta \rightarrow \gamma \equiv (\alpha \rightarrow \gamma) \vee (\beta \rightarrow \gamma) \quad ; \quad \alpha \vee \beta \rightarrow \gamma \equiv (\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma).$$

Bemerkung 1. Diese beiden letzten Äquivalenzen sind verantwortlich für ein kurioses Phänomen in der Alltagssprache. Zum Beispiel haben die beiden Aussagen

A: *Studenten und Rentner zahlen die Hälfte*, B: *Studenten oder Rentner zahlen die Hälfte* offenbar denselben Sinn. Wie lässt sich dies erklären? Seien die Sprachpartikel *Student*, *Rentner*, *die Hälfte zahlen* durch S , R bzw. H abgekürzt. Dann drücken

$$\alpha : (S \rightarrow H) \wedge (R \rightarrow H), \quad \beta : (S \vee R) \rightarrow H$$

die Sachverhalte A bzw. B etwas präziser aus. Nun sind α und β aber logisch äquivalent. Die umgangssprachlichen Formulierungen A, B von α bzw. β verschleiern den strukturellen Unterschied von α und β durch einen scheinbar synonymen Gebrauch von *und*, *oder*.

Offenbar ist \equiv eine Äquivalenzrelation, d.h. es gelten

$$\begin{aligned} \alpha &\equiv \alpha && \text{(Reflexivität),} \\ \alpha &\equiv \beta \Rightarrow \beta \equiv \alpha && \text{(Symmetrie),} \\ \alpha &\equiv \beta, \beta \equiv \gamma \Rightarrow \alpha \equiv \gamma && \text{(Transitivität).} \end{aligned}$$

Darüber hinaus ist \equiv eine *Kongruenz*²⁾ auf \mathcal{F} , d.h. für alle $\alpha, \alpha', \beta, \beta'$ gilt

$$\alpha \equiv \alpha', \beta \equiv \beta' \Rightarrow \alpha \circ \beta \equiv \alpha' \circ \beta', \neg \alpha \equiv \neg \alpha' \quad (\circ \in \{\wedge, \vee\}).$$

Deshalb gilt das sogenannte *Ersetzungstheorem*: $\alpha \equiv \alpha' \Rightarrow \varphi \equiv \varphi'$, wobei φ' aus φ dadurch hervorgeht, dass man die in φ eventuell vorkommende Subformel α an einer oder mehreren Stellen ihres Vorkommens durch α' ersetzt. So ergibt sich etwa aus $\varphi = (\neg p \vee \neg q) \wedge (p \vee q)$ durch Ersetzen der Subformel $\neg p \vee \neg q$ durch die äquivalente Formel $\neg(p \wedge q)$ die zu φ äquivalente Formel $\varphi' = \neg(p \wedge q) \wedge (p \vee q)$.

Ein ähnliches Ersetzungstheorem gilt übrigens auch für arithmetische Terme und wird bei Termumformungen ständig verwendet. Dies fällt deswegen nicht auf, weil $=$ statt \equiv geschrieben wird und mit der Ersetzung meist richtig umgegangen wird. Der sehr einfache Beweis des Ersetzungstheorems wird in **2.4** in einem etwas erweiterten Rahmen ausgeführt. Ausgerüstet mit den Äquivalenzen $\neg(\alpha \wedge \beta) \equiv \neg \alpha \vee \neg \beta$, $\neg(\alpha \vee \beta) \equiv \neg \alpha \wedge \neg \beta$ und $\neg \neg \alpha \equiv \alpha$ konstruiert man mit dem Ersetzungstheorem zu jeder Formel φ leicht eine äquivalente Formel, in der das Negationszeichen nur noch unmittelbar vor Variablen steht. Zum Beispiel ergibt sich auf diese Weise $\neg(p \wedge q \vee r) \equiv \neg(p \wedge q) \wedge \neg r \equiv (\neg p \vee \neg q) \wedge \neg r$. Solche Umformungen führen auch syntaktisch zu den unten betrachteten konjunktiven und disjunktiven Normalformen.

Für den Lernenden ist immer eine gewisse Überraschung, dass *jede* Boolesche Funktion durch eine Boolesche Formel repräsentierbar ist. Es gibt dafür unterschiedliche Beweise. Wir wollen bei dieser Gelegenheit jedoch gewisse Normalformen kennenlernen und beginnen daher mit der folgenden

Definition. Primformeln und deren Verneinungen heißen *Literale*. Eine Disjunktion $\alpha_1 \vee \dots \vee \alpha_n$, wobei jedes α_i eine Konjunktion von Literalen ist, heiße eine *disjunktive Normalform*, kurz eine DNF. Eine Konjunktion $\beta_1 \wedge \dots \wedge \beta_n$, wobei jedes β_i eine Disjunktion von Literalen ist, heiße eine *konjunktive Normalform*, kurz eine KNF.

²⁾Dieser ursprünglich aus der Geometrie stammende Begriff ist in jeder algebraischen Struktur sinnvoll definiert und gehört zu den wichtigsten mathematischen Begriffen, siehe hierzu **2.1**.

Beispiele. $p \vee (q \wedge \neg p)$ ist eine DNF. Die Formel $p \vee q$ ist zugleich eine DNF und eine KNF, während $p \vee \neg(q \wedge \neg p)$ weder eine DNF noch eine KNF darstellt.

Satz 2.1 besagt, dass jede Boolesche Funktion durch eine Boolesche Formel repräsentiert wird, sogar durch eine DNF, und auch durch eine KNF. Dazu genügt z.B. der recht einfache Nachweis, dass es zu vorgegebenem n mindestens 2^{2^n} viele paarweise nichtäquivalente DNFs (bzw. KNFs) gibt. Doch führen wir den Beweis konstruktiv. Zu einer durch eine Wertetabelle gegebenen Booleschen Funktion wird eine sie repräsentierende DNF (bzw. KNF) explizit angegeben.

In der Formulierung von Satz 2.1 verwenden wir vorübergehend folgende Notation. Für Variablen p sei $p^1 = p$ und $p^0 = \neg p$. Wie man sich induktiv über n (≥ 1) leicht klarmacht, gilt für alle $x_1, \dots, x_n \in \{0, 1\}$

$$(*) \quad w(p_1^{x_1} \wedge \dots \wedge p_n^{x_n}) = 1 \Leftrightarrow w\vec{p} = \vec{x} \quad (\text{d.h. } wp_1 = x_1, \dots, wp_n = x_n).$$

Satz 2.1. Jede Boolesche Funktion f , sagen wir $f \in \mathbf{B}_n$, ist repräsentierbar durch eine DNF, und zwar durch

$$\alpha := \bigvee_{f(x_1, \dots, x_n)=1} p_1^{x_1} \wedge \dots \wedge p_n^{x_n}.^{3)}$$

f ist zugleich repräsentierbar durch die KNF

$$\beta := \bigwedge_{f(x_1, \dots, x_n)=0} p_1^{\neg x_1} \vee \dots \vee p_n^{\neg x_n}.$$

Beweis. Unter Beachtung der Definition von α gilt für eine beliebige Belegung w

$$\begin{aligned} w\alpha = 1 &\Leftrightarrow \text{es gibt ein } \vec{x} \text{ mit } w(p_1^{x_1} \wedge \dots \wedge p_n^{x_n}) = 1 \text{ und } f\vec{x} = 1 \\ &\Leftrightarrow \text{es gibt ein } \vec{x} \text{ mit } w\vec{p} = \vec{x} \text{ und } f\vec{x} = 1 \quad (\text{nach } (*)) \\ &\Leftrightarrow fw\vec{p} = 1. \end{aligned}$$

Aus $w\alpha = 1 \Leftrightarrow fw\vec{p} = 1$ folgt wegen der Zweiwertigkeit sofort $w\alpha = fw\vec{p}$. Analog beweist man die Repräsentierbarkeit von f durch β , oder man benutzt Satz 2.3. \square

Beispiel. Für die *entweder-oder*-Funktion $+$ liefert das Konstruktionsverfahren von Satz 2.1 die repräsentierende DNF $p_1 \wedge \neg p_2 \vee \neg p_1 \wedge p_2$. Denn $(1, 0)$, $(0, 1)$ sind die beiden Tupel, für die $+$ den Wert 1 hat. Die durch den Satz gelieferte KNF hingegen lautet $(p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2)$. Die äquivalente Formel $(p_1 \vee p_2) \wedge \neg(p_1 \wedge p_2)$ gibt den Sinn der exklusiven oder-Verknüpfung besonders anschaulich wieder.

³⁾Die Disjunktionsglieder der Formel α seien z.B. gemäß lexikographischer Anordnung der n -Tupel $(x_1, \dots, x_n) \in \{0, 1\}^n$ angeordnet. Falls die Disjunktion leer ist, also f den Wert 1 nicht annimmt, sei α die Formel $\perp (= p_1 \wedge \neg p_1)$. Analog sei $\top (= \neg \perp)$ die leere Konjunktion. Dies entspricht den Konventionen, wonach die leere Summe hat den Wert 0, das leere Produkt den Wert 1 hat.

Die durch Satz 2.1 gegebene DNF für \rightarrow , nämlich $p_1 \wedge p_2 \vee \neg p_1 \wedge p_2 \vee \neg p_1 \wedge \neg p_2$, ist länger als die \rightarrow ebenfalls repräsentierende DNF $\neg p_1 \vee p_2$. Die erstere ist aber dadurch ausgezeichnet, dass jede ihrer Disjunktionen jede der beiden vorkommenden Variablen genau einmal enthält. Eine DNF in n Variablen mit der analogen Eigenschaft heißt *kanonisch*. Satz 2.1 liefert die Repräsentierbarkeit durch kanonische Normalformen, wobei der Begriff der kanonischen KNF entsprechend erklärt sei. So wird z.B. \leftrightarrow durch die kanonische KNF $(\neg p_1 \vee p_2) \wedge (p_1 \vee \neg p_2)$ repräsentiert.

Eine logische Signatur (eigentlich das ihr entsprechende System Boolescher Funktionen) heißt *funktional vollständig*, genauer *term-funktional vollständig*, wenn jede Boolesche Funktion durch eine Formel dieser Signatur repräsentierbar ist. Nach Satz 2.1 ist $\{\neg, \wedge, \vee\}$ funktional vollständig. Wegen $p_1 \vee p_2 \equiv \neg(\neg p_1 \wedge \neg p_2)$ und $p_1 \wedge p_2 \equiv \neg(\neg p_1 \vee \neg p_2)$ kann auf \vee oder aber auf \wedge auch noch verzichtet werden. Man erhält damit das

Korollar 2.2. $\{\neg, \wedge\}$ und $\{\neg, \vee\}$ sind funktional vollständig.

Um eine logische Signatur L als funktional vollständig nachzuweisen, genügt es daher, \neg, \wedge oder \neg, \vee durch Formeln in L zu repräsentieren. Weil z.B. $\neg p \equiv p \rightarrow 0$ und $p \wedge q \equiv \neg(p \rightarrow \neg q)$, ist $\{\rightarrow, 0\}$ funktional vollständig, ebenso wie z.B. $\{\rightarrow, \neg\}$. Dagegen ist z.B. $\{\rightarrow, \wedge, \vee\}$ und erst recht $\{\rightarrow\}$ funktional unvollständig. Denn induktiv über den Aufbau von Formeln α in $\rightarrow, \wedge, \vee$ folgt leicht $w\alpha = 1$ für jedes w mit $w p = 1$ für alle p . Daher gibt es kein derartiges α mit $\alpha \equiv \neg p$.

Bemerkenswerterweise ist die lediglich \downarrow enthaltende Signatur bereits funktional vollständig. Denn $\neg p \equiv p \downarrow p$, sowie $p \wedge q \equiv \neg p \downarrow \neg q$ nach der Wertetafel für \downarrow . Analoges gilt auch für $\{\uparrow\}$, denn $\neg p \equiv p \uparrow p$ und $p \vee q \equiv \neg p \uparrow \neg q$. Dass mit $\{\downarrow\}$ auch $\{\uparrow\}$ funktional vollständig ist, entnimmt man auch dem Dualitätssatz unten.

Es gibt bis auf Termäquivalenz immer noch unendlich viele Signaturen. Dabei heißen Signaturen *termäquivalent*, wenn deren Formeln jeweils die gleichen Booleschen Funktionen repräsentieren wie z.B. die in Übung 2 genannten Signaturen.

Wir erklären eine Abbildung $\delta : \mathcal{F} \rightarrow \mathcal{F}$ rekursiv über die Formeln von \mathcal{F} durch

$$p^\delta = p, \quad (\neg \alpha)^\delta = \neg \alpha^\delta, \quad (\alpha \wedge \beta)^\delta = \alpha^\delta \vee \beta^\delta, \quad (\alpha \vee \beta)^\delta = \alpha^\delta \wedge \beta^\delta.$$

α^δ heißt die zu α *duale Formel*. Sie entsteht aus α dadurch, dass \wedge und \vee miteinander vertauscht werden. Für eine DNF α ist α^δ offenbar eine KNF und umgekehrt. Die zu $f \in \mathbf{B}_n$ *duale Funktion* sei definiert durch $f^\delta(x_1, \dots, x_n) = \neg f(\neg x_1, \dots, \neg x_n)$. Offenbar gilt $(f^\delta)^\delta = f$. So ist $\wedge^\delta = \vee$, $\vee^\delta = \wedge$, $\leftrightarrow^\delta = +$, $\downarrow^\delta = \uparrow$, aber $\neg^\delta = \neg$. Mit anderen Worten, \neg ist *selbstdual*. Auch $d_3 : (x_1, x_2, x_3) \mapsto x_1 \wedge x_2 \vee x_1 \wedge x_3 \vee x_2 \wedge x_3$ ist ein oft zitiertes Beispiel. Wesentlich 2-stellige selbstduale Funktionen gibt es nicht, wie ein Blick auf die Wertetafeln zeigt. Die Dualisierungsbegriffe verbindet

Satz 2.3 (Dualitätssatz der 2-wertigen Logik). *Repräsentiert α die Funktion f , so repräsentiert die duale Formel α^δ die duale Funktion f^δ .*

Der recht einfache Beweis des Satzes, der sich kurz durch $(\alpha^{(n)})^\delta = (\alpha^\delta)^{(n)}$ wiedergeben lässt, sei hier übergangen. Statt dessen seien einige Anwendungen vorgestellt. \leftrightarrow wird z.B. durch $p \wedge q \vee \neg p \wedge \neg q$ repräsentiert, die duale Funktion $+$ $= \leftrightarrow^\delta$ also durch die duale Formel $(p \vee q) \wedge (\neg p \vee \neg q)$. Die erste ist eine DNF, die letzte eine KNF. Allgemeiner: wird $f \in \mathbf{B}_n$ durch eine DNF α repräsentiert, so f^δ nach Satz 2.3 durch eine KNF, nämlich α^δ , und diese ist kanonisch falls α kanonisch ist wie im vorliegenden Beispiel. Falls wir nur wissen, dass jedes $f \in \mathbf{B}_n$ durch eine DNF repräsentierbar ist, so notwendigerweise auch durch eine KNF; denn die Abbildung $f \mapsto f^\delta$ ist wegen $\delta^2 = id_{\mathbf{B}_n}$ eine Bijektion von \mathbf{B}_n auf sich.

Bemerkung 2. $\{\wedge, \vee, 0, 1\}$ ist *maximal funktional unvollständig*, d.h. ist eine Boolesche Funktion f nicht durch eine Formel in $\wedge, \vee, 0, 1$ repräsentierbar, so ist $\{\wedge, \vee, 0, 1, f\}$ bereits funktional vollständig, Übung 4. Es gibt bis auf Termäquivalenz nur fünf maximal unvollständige Signaturen wie E. Post 1920 bewies, außer der angegebenen nur $\{\rightarrow, \wedge\}$ und deren duale, sowie $\{\leftrightarrow, \neg\}$ und $\{d_3, \neg\}$. Die Formeln der letztgenannten Signatur repräsentieren genau alle selbstdualen Booleschen Funktionen. Schreibt man vorübergehend \cdot statt \wedge , so ist wegen $\neg p \equiv 1 + p$ auch $\{0, 1, +, \cdot\}$ funktional vollständig. Das hat einen tieferen Grund: es ist dies zugleich die Signatur der Körper (siehe hierzu 2.1) und in jedem endlichen Körper sind alle Funktionen seines Trägers als Polynome darstellbar. Für endliche Gruppen ist dies in der Regel falsch. Ferner gibt es für jede endliche Menge E eine verallgemeinerte 2-stellige Sheffer-Funktion, durch welche man jede Operation über E in einem analogen Sinne wie im 2-wertigen Falle erhält. Die Beweise dieser Behauptungen haben mehr mit Algebra als mit Logik zu tun. Wir verweisen daher z.B. auf [Ih].

Übungen

1. Man verifiziere die Äquivalenzen $(p \rightarrow q_1) \wedge (\neg p \rightarrow q_2) \equiv p \wedge q_1 \vee \neg p \wedge q_2$ und $p_1 \wedge q_1 \rightarrow p_2 \vee q_2 \equiv (p_1 \rightarrow p_2) \vee (q_1 \rightarrow q_2)$.
2. Man zeige, die Signaturen $\{+, 1\}$, $\{+, \neg\}$ und $\{\leftrightarrow, \neg\}$ sind termäquivalent. Deren Formeln repräsentieren genau die linearen Booleschen Funktionen.
3. Man beweise, die Formeln in $\{\wedge, \vee, 0, 1\}$ repräsentieren genau die *monotonen* Booleschen Funktionen, d.h. die Konstanten aus \mathbf{B}_0 und die $f \in \mathbf{B}_n$ mit

$$f(\dots, x_{i-1}, 0, x_{i+1}, \dots) \leq f(\dots, x_{i-1}, 1, x_{i+1}, \dots) \quad (i = 1, \dots, n)$$

für alle $x_1, \dots, x_n \in \{0, 1\}$.

4. Man zeige, die Signatur $\{\wedge, \vee, 0, 1\}$ ist maximal funktional unvollständig.

1.3 Tautologien und aussagenlogisches Folgern

Statt $w\alpha = 1$ schreibt man auch $w \models \alpha$ und sagt w *erfüllt* α . Wir werden dieser Schreibweise in der Regel den Vorzug geben. Ferner schreibt man $w \models X$, wenn $w \models \alpha$ für alle $\alpha \in X$, und nennt dann w ein *Modell für die Formelmeng*e X . Falls es ein w mit $w \models \alpha$ bzw. mit $w \models X$ gibt, heißen α bzw. X auch *erfüllbar*. Die Relation \models , auch die *Erfüllungsrelation* genannt, hat offenbar die folgenden Eigenschaften:

$$\begin{aligned} w \models p &\Leftrightarrow wp = 1 \quad (p \in AV); & w \models \neg\alpha &\Leftrightarrow w \not\models \alpha; \\ w \models \alpha \wedge \beta &\Leftrightarrow w \models \alpha \text{ und } w \models \beta; & w \models \alpha \vee \beta &\Leftrightarrow w \models \alpha \text{ oder } w \models \beta. \end{aligned}$$

Im Hinblick auf die Erweiterungen der Erfüllungsbedingungen in 2.3 ist wichtig, dass die Erfüllungsrelation $w \models \alpha$ für vorgegebenes $w: AV \rightarrow \{0, 1\}$ auch direkt definiert werden kann, und zwar rekursiv über α , entsprechend den soeben niedergeschriebenen Klauseln. w ist offenbar eindeutig durch eine Vorgabe darüber festgelegt, für welche Variablen $w \models p$ gelten soll. Auch ist die Notation $w \models \alpha$ für $\alpha \in \mathcal{F}_n$ bereits dann sinnvoll, wenn w nur für p_1, \dots, p_n erklärt wurde. Ein solches w kann man sich, wenn gewünscht, zu einer globalen Belegung fortgesetzt denken, indem man wp für die in α nicht vorkommenden Variablen z.B. identisch 0 setzt.

Falls die Formeln auch andere Junktoren enthalten, sind für diese die Erfüllungsbedingungen sinngemäß zu formulieren. Zum Beispiel erwarten wir

$$w \models \alpha \rightarrow \beta \Leftrightarrow \text{wenn } w \models \alpha, \text{ so } w \models \beta.$$

Ist \rightarrow ein eigenständiger Junktor, wird dies gefordert. Wir haben \rightarrow hingegen durch andere Junktoren so definiert, dass diese Erfüllungsklausel beweisbar ist.

Definition. α heißt *allgemeingültig* oder *logisch gültig*, auch eine 2-wertige *Tautologie* genannt, wenn $w \models \alpha$ (gleichwertig $w\alpha = 1$) für alle w . Wir schreiben dann $\models \alpha$. Eine nicht erfüllbare Formel heißt auch eine *Kontradiktion*.

Beispiele. Alle Formeln der Gestalt $\alpha \vee \neg\alpha$ sind Tautologien. \perp , $\alpha \wedge \neg\alpha$ und $\alpha \leftrightarrow \neg\alpha$ sind hingegen Kontradiktionen. So wird die Russellsche Antinomie auf Seite 58 so gewonnen, dass für die „Russellsche Menge“ u die Kontradiktion $u \in u \leftrightarrow u \notin u$ gefolgert wird. In der aussagenlogischen Literatur oft zitiert werden die Tautologien

$$\begin{array}{ll} p \rightarrow p & (\text{Selbstimplikation}), \\ p \rightarrow q \rightarrow p & (\text{Prämissenbelastung}), \\ (p \rightarrow q \rightarrow r) \rightarrow (q \rightarrow p \rightarrow r) & (\text{Prämissenvertauschung}), \\ (p \rightarrow q) \rightarrow (q \rightarrow r) \rightarrow (p \rightarrow r) & (\text{gewöhnlicher Kettenschluß}), \\ (p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow (p \rightarrow r) & (\text{Frege'scher Kettenschluß}), \\ ((p \rightarrow q) \rightarrow p) \rightarrow p & (\text{Formel von Peirce}). \end{array}$$

Es ist offenbar entscheidbar, ob eine Formel α eine Tautologie ist oder nicht, indem man z.B. alle Belegungen der Variablen von α durchprobiert. Leider gibt es bis heute keine wesentlich effizienteren Verfahren. Diese gibt es nur für Formeln in gewisser Gestalt, siehe hierzu 4.2. Auch das Prüfen einer Äquivalenz kann auf das Tautologieproblem reduziert werden. Denn offenbar gilt $\alpha \equiv \beta \Leftrightarrow \models \alpha \leftrightarrow \beta$.

Definition. Aus X folgt α im aussagenlogischen Sinne, symbolisch $X \models \alpha$, wenn $w \models \alpha$ für jedes Modell w von X .

Wir benutzen hier \models zugleich als Zeichen für das Folgern als einer Relation zwischen Formelmengen X und Formeln α . Der Kontext wird stets klar erkennen lassen, was gemeint ist. Offensichtlich ist α allgemeingültig genau dann, wenn $\emptyset \models \alpha$, so dass die Notation $\models \alpha$ auch als verkürzte Schreibweise für $\emptyset \models \alpha$ verstanden werden kann.

$X \models \alpha, \beta$ meine in diesem Buch stets $X \models \alpha$ und $X \models \beta$, sowie $X \models Y$ stets $X \models \beta$ für alle $\beta \in Y$. Ferner schreiben wir meistens $\alpha_1, \dots, \alpha_n \models \beta$ anstelle von $\{\alpha_1, \dots, \alpha_n\} \models \beta$, und ebenso $X, \alpha \models \beta$ anstelle von $X \cup \{\alpha\} \models \beta$.

Bevor wir Beispiele angeben, notieren wir die offensichtlichen Eigenschaften

- (R) $\alpha \in X \Rightarrow X \models \alpha$ (*Reflexivität*),
- (M) $X \models \alpha \ \& \ X \subseteq X' \Rightarrow X' \models \alpha$ (*Monotonie*),
- (T) $X \models Y \ \& \ Y \models \alpha \Rightarrow X \models \alpha$ (*Transitivität*).

Beispiele für Folgerungsbeziehungen. (a) $\alpha, \beta \models \alpha \wedge \beta$ und $\alpha \wedge \beta \models \alpha, \beta$. Dies ist klar gemäß Wertematrix für \wedge . Angesichts der Transitivität (T) lässt (a) sich auch in der Weise $X \models \alpha, \beta \Leftrightarrow X \models \alpha \wedge \beta$ formulieren. (b) $\alpha, \alpha \rightarrow \beta \models \beta$. Denn $1 \rightarrow x = 1$ impliziert $x = 1$ nach der Wertetabelle für \rightarrow . (c) $X \models \perp \Rightarrow X \models \alpha$ für alle α . Denn $X \models \perp (= p_1 \wedge \neg p_1)$ kann nur dann gelten wenn X unerfüllbar ist, d.h. kein Modell hat, wie etwa $X = \{p, \neg p\}$. Das hat offenbar $X \models \alpha$ für beliebiges α zur Folge. (d) $X, \alpha \models \beta$ und $X, \neg \alpha \models \beta$ impliziert $X \models \beta$. Denn sei $w \models X$. Falls $w \models \alpha$, ergibt $X, \alpha \models \beta$ auch $w \models \beta$; falls aber $w \models \neg \alpha$, folgt $w \models \beta$ aus $X, \neg \alpha \models \beta$.

Eigenschaft (b) wird auch der *Modus Ponens* genannt, wenn man (b) als Regel formuliert. Siehe hierzu auch 1.6. Durch (d) wird das häufig verwendete Beweisverfahren durch Fallunterscheidung wiedergegeben. Um eine Aussage β aus einer Prämissenmenge X zu erschließen, genügt es, diese unter einer Zusatzannahme α und ebenso auch unter der Annahme $\neg \alpha$ herzuleiten.

Für viele Zwecke nützlich ist die Abgeschlossenheit des Folgerns unter Substitutionen. Sie verallgemeinert die Beobachtung, dass z.B. aus $p \vee \neg p$ alle Tautologien der Gestalt $\alpha \vee \neg \alpha$ durch Substitution von α für p entstehen.

Definition. Eine (*aussagenlogische*) *Substitution* ist eine Abbildung $\sigma : AV \rightarrow \mathcal{F}$, die sich wie folgt in natürlicher Weise zu einer Abbildung $\sigma : \mathcal{F} \rightarrow \mathcal{F}$ erweitern lässt:

$$(\alpha \wedge \beta)^\sigma = \alpha^\sigma \wedge \beta^\sigma, \quad (\alpha \vee \beta)^\sigma = \alpha^\sigma \vee \beta^\sigma, \quad (\neg \alpha)^\sigma = \neg \alpha^\sigma.$$

Genau wie Belegungen lassen sich daher auch Substitutionen als auf ganz \mathcal{F} erklärte Abbildungen auffassen, die durch ihre Einschränkungen auf AV eindeutig bestimmt sind. Ist z.B. $p^\sigma = \alpha$ für ein p und $q^\sigma = q$ sonst, so entsteht φ^σ aus φ durch Ersetzung von p durch α an allen Stellen des Vorkommens von p in φ . Dass mit φ auch φ^σ eine Tautologie ist, ist der Sonderfall $X = \emptyset$ der allgemeinen *Substitutionsinvarianz*

$$(S) \quad X \models \alpha \Rightarrow X^\sigma \models \alpha^\sigma \quad (X^\sigma := \{\varphi^\sigma \mid \varphi \in X\}).$$

Beweis. Sei w eine Belegung und sei w^σ erklärt durch $w^\sigma p = wp^\sigma$. Wir zeigen

$$(*) \quad w \models \alpha^\sigma \Leftrightarrow w^\sigma \models \alpha$$

induktiv über α . Für Primformeln ist dies klar und die Induktionsannahme ergibt

$$w \models (\alpha \wedge \beta)^\sigma \Leftrightarrow w \models \alpha^\sigma \wedge \beta^\sigma \Leftrightarrow w \models \alpha^\sigma, \beta^\sigma \Leftrightarrow w^\sigma \models \alpha, \beta \Leftrightarrow w^\sigma \models \alpha \wedge \beta.$$

Das Analoge beweist man für \vee und \neg . Damit gilt (*). Zum Nachweis von (S) sei $X \models \alpha$, sowie $w \models X^\sigma$. Wegen (*) ist $w^\sigma \models X$. Also $w^\sigma \models \alpha$, und damit $w \models \alpha^\sigma$. \square

Die Folgerungsrelation hat eine weitere, insbesondere auch für mathematische Anwendungen bedeutsame Eigenschaft, die im nächsten Abschnitt bewiesen wird:

$$(F) \quad X \models \alpha \Rightarrow X_0 \models \alpha \text{ für eine endliche Teilmenge } X_0 \subseteq X.$$

Eine weitere wichtige und leicht beweisbare Folgerungseigenschaft ist ferner

$$(D) \quad X, \alpha \models \beta \Rightarrow X \models \alpha \rightarrow \beta.$$

Denn sei $X, \alpha \models \beta$ und w Modell für X . Wenn $w \models \alpha$, ist wegen $X, \alpha \models \beta$ auch $w \models \beta$. Damit ist $X \models \alpha \rightarrow \beta$ schon gezeigt. (D) heißt auch das (semantische) *Deduktionstheorem*. Auch die Umkehrung von (D) ist richtig, wie man leicht sieht, d.h. man darf \Rightarrow in (D) durch \Leftrightarrow ersetzen. Wiederholte Anwendung hiervon liefert

$$\alpha_1, \dots, \alpha_n \models \beta \Leftrightarrow \models \alpha_1 \rightarrow \alpha_2 \rightarrow \dots \rightarrow \alpha_n \rightarrow \beta \Leftrightarrow \models \alpha_1 \wedge \alpha_2 \wedge \dots \wedge \alpha_n \rightarrow \beta.$$

Damit wird das Folgern von β aus einer endlichen Prämissenmenge gänzlich auf die Allgemeingültigkeit einer geeigneten Formel zurückgeführt.

Mit (D) lassen sich bequem Tautologien gewinnen. Um etwa $\models p \rightarrow q \rightarrow p$ zu beweisen, genügt nach (D) der Nachweis von $p \models q \rightarrow p$; dazu genügt, wiederum nach (D), der Nachweis von $p, q \models p$, und dies ist trivial. Durch einfache Anwendung von (D) erhält man leicht auch die beiden in Übung 1 genannten Kettenschlußformeln.

$X \subseteq \mathcal{F}$ heißt *X deduktiv abgeschlossen*, wenn $X \models \alpha \Rightarrow \alpha \in X$ für alle $\alpha \in \mathcal{F}$. Wegen (R) kann diese Bedingung gleichwertig durch $X \models \alpha \Leftrightarrow \alpha \in X$ ersetzt werden.

Beispiele sind die Menge aller Tautologien und ganz \mathcal{F} . Der Durchschnitt deduktiv abgeschlossener Mengen ist wieder deduktiv abgeschlossen. Daher ist jedes $X \subseteq \mathcal{F}$ Teilmenge einer kleinsten deduktiv abgeschlossenen Obermenge von X .

Bemerkung. Die Eigenschaften (R), (M), (T) und (S) teilt \models mit fast allen nichtklassischen (mehrwertigen oder sonstigen) logischen Systemen. Eine Relation \vdash zwischen Formelmengen und Formeln einer vorgegebenen aussagenlogischen Sprache \mathcal{F} mit den für \vdash sinngemäß formulierten Eigenschaften (R), (M), (T) und (S) heie eine (aussagenlogische) *Konsequenzrelation*. Diese sind das Ausgangsmaterial fur eine von Tarski begrundete, sehr allgemeine und tragfahige Theorie logischer Systeme, der sich fast alle in der Literatur betrachteten logischen Systeme unterordnen. Alle in diesem Buch vorgestellten Logik-Kalkule haben z.B. diese Eigenschaften. Begriffe wie Tautologie, konsistent, deduktiv abgeschlossen usw. beziehen sich auf eine gegebene Konsequenzrelation \vdash . Eine Formelmenge X heit z.B. *inkonsistent*, wenn $X \vdash \alpha$ fur alle α , und anderenfalls konsistent. \vdash selbst heit inkonsistent, wenn $\vdash \alpha$ fur alle α . Erfüllt \vdash die oben fur \models formulierte, noch nicht bewiesene und im allgemeinen Falle auch nicht vorausgesetzte Eigenschaft (F), so heit \vdash *finitr*. (F) gilt fur das Folgern uber einer beliebigen endlichen logischen Matrix. Dies wird in bung 3 in 5.7 als Beispiel einer Anwendung des Ultraproduktsatzes bewiesen und zugleich wesentlich verallgemeinert.

bungen

1. Man beweise mit Hilfe des Deduktionstheorems

$$\models (p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow (p \rightarrow r) \text{ und } \models (p \rightarrow q) \rightarrow (q \rightarrow r) \rightarrow (p \rightarrow r).$$

2. Man bestatige die Korrektheit der *Regel der disjunktiven Fallunterscheidung*:
Wenn $X, \alpha \models \gamma$ und $X, \beta \models \gamma$, so $X, \alpha \vee \beta \models \gamma$. In suggestiver Schreibweise

$$\frac{X, \alpha \models \gamma \mid X, \beta \models \gamma}{X, \alpha \vee \beta \models \gamma}.$$

3. Man verifiziere die Korrektheit der folgenden *Kontrapositionsregeln*:

$$\frac{X, \alpha \models \beta}{X, \neg \beta \models \neg \alpha} \quad ; \quad \frac{X, \neg \beta \models \neg \alpha}{X, \alpha \models \beta}.$$

4. Sei \vdash eine beliebige Konsequenzrelation in \mathcal{F} und $X^\perp := \{\alpha \in \mathcal{F} \mid X \vdash \alpha\}$.
Man zeige, X^\perp ist die kleinste deduktiv abgeschlossene Obermenge von X .
5. Sei \vdash eine Konsequenzrelation in \mathcal{F} und fur beliebiges $X \subseteq \mathcal{F}$ erklare man $X \vdash_0 \alpha :\Leftrightarrow X_0 \vdash \alpha$ fur ein endliches $X_0 \subseteq X$. Man zeige, \vdash_0 ist eine finitre Konsequenzrelation und $\vdash_0 \subseteq \vdash$.

1.4 Ein vollständiger aussagenlogischer Kalkül

Wir werden nun mittels eines Regelkalküls eine Ableitungsrelation \vdash definieren, die sich als identisch mit der Folgerungsrelation \models erweist. Dieser Kalkül ist vom Typus der sogenannten Gentzen-Kalküle. Seine Regeln beziehen sich auf Paare (X, α) von Formelmengen X und Formeln α , wobei X – anders als in [Ge] – hier nicht endlich sein muss, da die von uns verfolgten Ziele dies nicht erfordern. In Anlehnung an [Ge] heißen die Paare (X, α) auch *Sequenzen*. Trifft \vdash auf die Sequenz (X, α) zu, schreibt man $X \vdash \alpha$ (sprich X *ableitbar* α) und andernfalls $X \not\vdash \alpha$.

Der Kalkül wird für \wedge und \neg formuliert und umfasst die umrahmten *Basisregeln* unten. Jede dieser Regel hat oberhalb des Trennstrichs gewisse *Prämissen* und darunter eine *Konklusion*. Nur (AR) hat keine Prämissen und erlaubt die Herleitung der Sequenzen $\alpha \vdash \alpha$, den *Anfangssequenzen*. Die Wahl der Signatur $\{\wedge, \neg\}$ ist eine Sache der Bequemlichkeit und gerechtfertigt durch ihre funktionale Vollständigkeit. Weitere Junktoren werden fortan gemäß den Definitionen

$$\alpha \vee \beta := \neg(\neg\alpha \wedge \neg\beta), \quad \alpha \rightarrow \beta := \neg(\alpha \wedge \neg\beta), \quad \alpha \leftrightarrow \beta := (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha).$$

verwendet. Man kann auch eine andere funktional vollständige Signatur wählen, muss aber in Kauf nehmen, dass die Formulierung eines Logik-Kalküls länger wird, weil dieser wesentlich von der gewählten Signatur abhängt. So muss ein vollständiger Kalkül etwa in $\{\neg, \wedge, \vee, \rightarrow\}$ auch auf \vee und \rightarrow bezogene Basisregeln enthalten.

(AR) $\frac{}{\alpha \vdash \alpha}$ (Anfangsregel)	(MR) $\frac{X \vdash \alpha}{X' \vdash \alpha}$ ($X' \supseteq X$, Monotonieregel)
(\wedge 1) $\frac{X \vdash \alpha, \beta}{X \vdash \alpha \wedge \beta}$	(\wedge 2) $\frac{X \vdash \alpha \wedge \beta}{X \vdash \alpha, \beta}$
(\neg 1) $\frac{X \vdash \alpha, \neg\alpha}{X \vdash \beta}$	(\neg 2) $\frac{X, \alpha \vdash \beta \mid X, \neg\alpha \vdash \beta}{X \vdash \beta}$

Dabei meint $X \vdash \alpha, \beta$ hier und im Folgenden immer $X \vdash \alpha$ und $X \vdash \beta$. Diese Vereinbarung ist wichtig, denn $X \vdash \alpha, \beta$ hat einen anderen Sinn in Gentzen-Kalkülen, die sich auf Paare von Formelmengen beziehen und die für beweistheoretische Untersuchungen wichtig sind. Die Regeln (\wedge 1) und (\neg 1) haben eigentlich zwei Prämissen, genau wie (\neg 2). Nur lässt (\neg 2) sich nicht in derselben Weise abgekürzt notieren. Man beachte ferner, dass (\wedge 2) eigentlich aus zwei Teilregeln besteht, entsprechend den Konklusionen $X \vdash \alpha$ und $X \vdash \beta$. In (\neg 2) steht X, α für $X \cup \{\alpha\}$. Diese verkürzende Schreibweise wird immer dann verwendet, wenn Missverständnisse ausgeschlossen sind. Auch wird $\alpha_1, \dots, \alpha_n \vdash \beta$ für $\{\alpha_1, \dots, \alpha_n\} \vdash \beta$ geschrieben, und $\vdash \alpha$ für $\emptyset \vdash \alpha$,

analog wie für \models . Die Regel (MR) wird beweisbar, wenn *alle* Sequenzen (X, α) mit $\alpha \in X$ als Anfangssequenzen angesehen werden. Mit anderen Worten, wenn (AR) verschärft wird zu $X \vdash \alpha$ für beliebige $\alpha \in X$.

$X \vdash \alpha$ bedeutet genauer, dass die Sequenz (X, α) durch schrittweises Anwenden der Basisregeln gewonnen werden kann. Die Redeweise vom schrittweisen Anwenden der Basisregeln kann streng formal wie folgt präzisiert werden. Eine *Herleitung* sei eine endliche Folge $(S_0; \dots; S_n)$ von Sequenzen S_i derart, dass jedes Folgenglied eine Anfangssequenz ist oder aus vorangehenden Folgengliedern durch Anwendung einer der Basisregeln gewonnen wurde. *Aus X ist α ableitbar* oder *beweisbar*, $X \vdash \alpha$, wenn es eine Herleitung $(S_0; \dots; S_n)$ gibt mit $S_n = (X, \alpha)$. Dies ist eine der möglichen Definitionen der Relation \vdash . Einfaches Beispiel einer Herleitung mit der Endsequenz $\alpha, \beta \vdash \alpha \wedge \beta$ ist $(\alpha \vdash \alpha; \alpha, \beta \vdash \alpha; \beta \vdash \beta; \alpha, \beta \vdash \beta; \alpha, \beta \vdash \alpha \wedge \beta)$.

Interessanter noch ist das Ableiten von Regeln. Wir erläutern dies anhand nachfolgender Beispiele. Das zweite, eine Verallgemeinerung des ersten, gibt das oft verwendete Beweisverfahren der *reductio ad absurdum* wieder: α wird aus X bewiesen, indem die Annahme $\neg\alpha$ zum Widerspruch geführt wird. Die weiteren Beispiele beziehen sich auf den definierten Junktore \rightarrow . Weil dieser durch \wedge, \neg wie angegeben definiert wurde, lautet beispielsweise die unten erwähnte \rightarrow -Elimination in der Originalsprache $\frac{X \vdash \neg(\alpha \wedge \neg\beta)}{X, \alpha \vdash \beta}$.

Beispiele beweisbarer Regeln

$\frac{X, \neg\alpha \vdash \alpha}{X \vdash \alpha}$ (\neg -Elimination)	<i>Beweis</i>	<i>angewendet</i>
	1 $X, \alpha \vdash \alpha$	(AR), (MR)
	2 $X, \neg\alpha \vdash \alpha$	Annahme
	3 $X \vdash \alpha$	(\neg 2)
$\frac{X, \neg\alpha \vdash \beta, \neg\beta}{X \vdash \alpha}$ (reductio ad absurdum)	1 $X, \neg\alpha \vdash \beta, \neg\beta$	Annahme
	2 $X, \neg\alpha \vdash \alpha$	(\neg 1)
	3 $X \vdash \alpha$	\neg -Elimination
$\frac{X \vdash \alpha \rightarrow \beta}{X, \alpha \vdash \beta}$ (\rightarrow -Elimination)	1 $X, \alpha, \neg\beta \vdash \alpha, \neg\beta$	(AR), (MR)
	2 $X, \alpha, \neg\beta \vdash \alpha \wedge \neg\beta$	(\wedge 1)
	3 $X \vdash \neg(\alpha \wedge \neg\beta)$ ($= \alpha \rightarrow \beta$)	Annahme
	4 $X, \alpha, \neg\beta \vdash \neg(\alpha \wedge \neg\beta)$	(MR)
	5 $X, \alpha, \neg\beta \vdash \beta$	(\neg 1) auf 2 und 4
	6 $X, \alpha \vdash \beta$	\neg -Elimination

$\frac{X \vdash \alpha \mid X, \alpha \vdash \beta}{X \vdash \beta}$ (Schnittregel)	<i>Beweis</i>	<i>angewendet</i>
	1 $X, \neg\alpha \vdash \alpha$	Annahme, (MR)
	2 $X, \neg\alpha \vdash \neg\alpha$	(AR), (MR)
	3 $X, \neg\alpha \vdash \beta$	(\neg 1)
	4 $X, \alpha \vdash \beta$	Annahme
	5 $X \vdash \beta$	(\neg 2) auf 4 und 3
$\frac{X, \alpha \vdash \beta}{X \vdash \alpha \rightarrow \beta}$ (\rightarrow -Einführung)	1 $X, \alpha \wedge \neg\beta, \alpha \vdash \beta$	Annahme, (MR)
	2 $X, \alpha \wedge \neg\beta \vdash \alpha$	(AR), (MR), (\wedge 2)
	3 $X, \alpha \wedge \neg\beta \vdash \beta$	Schnittregel
	4 $X, \alpha \wedge \neg\beta \vdash \neg\beta$	(AR), (MR), (\wedge 2)
	5 $X, \alpha \wedge \neg\beta \vdash \alpha \rightarrow \beta$	(\neg 1)
	6 $X, \neg(\alpha \wedge \neg\beta) \vdash \alpha \rightarrow \beta$	(AR), (MR)
	7 $X \vdash \alpha \rightarrow \beta$	(\neg 2) auf 5 und 6

Die \rightarrow -Einführung ist nichts anderes als die syntaktische Form des in **1.3** semantisch formulierten Deduktionstheorems. Eine einfache Folge der \rightarrow -Elimination und der Schnittregel ist die *Abtrennungsregel*

$$\frac{X \vdash \alpha, \alpha \rightarrow \beta}{X \vdash \beta}.$$

Denn $X \vdash \alpha \rightarrow \beta$ liefert $X, \alpha \vdash \beta$ (\rightarrow -Elimination). Mit $X \vdash \alpha$ folgt daher $X \vdash \beta$ (Schnittregel). Angewendet mit $X = \{\alpha, \alpha \rightarrow \beta\}$ erhält man so $\alpha, \alpha \rightarrow \beta \vdash \beta$. Diese Schar von Sequenzen heißt auch der *Modus Ponens*. Mehr hierüber in **1.6**.

Viele Eigenschaften von \vdash beweist man durch Regelinduktion. Zwecks bequemer Formulierung erklären wir zuerst einige Redeweisen. Eine Eigenschaft \mathcal{E} von Sequenzen identifizieren wir mit der Menge aller Paare (X, α) , auf die \mathcal{E} zutrifft. In diesem Sinne ist z.B. die Folgerungsrelation \models auch eine Eigenschaft, bestehend aus allen Paaren (X, α) mit $X \models \alpha$. Die hier betrachteten Regeln haben die Gestalt

$$R : \frac{X_1 \vdash \alpha_1 \mid \cdots \mid X_n \vdash \alpha_n}{X \vdash \alpha}$$

und seien als *Gentzen-Stil-Regeln* bezeichnet. Wir sagen, \mathcal{E} sei *abgeschlossen unter R*, wenn $\mathcal{E}(X_1, \alpha_1), \dots, \mathcal{E}(X_n, \alpha_n) \Rightarrow \mathcal{E}(X, \alpha)$. Für eine Regel ohne Prämissen, also für $n = 0$, heißt dies einfach nur $\mathcal{E}(X, \alpha)$. So sind z.B. alle Regeln unseres Kalküls (semantisch) *korrekt*, was heißen soll, die Folgerungseigenschaft ' $X \models \alpha$ ' ist unter allen Basisregeln abgeschlossen. Im Einzelnen bedeutet dies

$$\alpha \models \alpha, \quad X \models \alpha \Rightarrow X' \models \alpha \text{ für } X' \supseteq X, \quad X \models \alpha, \beta \Rightarrow X \models \alpha \wedge \beta, \quad \text{usw.}$$

Damit formulieren wir das sehr einfach zu rechtfertigende

Beweisprinzip durch Regelinduktion. *Ist eine Eigenschaft \mathcal{E} ($\subseteq \mathfrak{P}\mathcal{F} \times \mathcal{F}$) abgeschlossen unter allen Basisregeln von \vdash , so gilt $\mathcal{E}(X, \alpha)$ immer wenn $X \vdash \alpha$.*

Dies ergibt sich leicht durch Induktion über die Länge einer Herleitung der Sequenz $S = (X, \alpha)$. Ist 1 diese Länge, ist alles klar, weil S dann Anfangssequenz ist. Nun sei $(S_0; \dots; S_n)$ eine Herleitung von $S = S_n$, und nach Induktionsannahme sei $\mathcal{E}S_i$ für alle $i < n$. Ist S Anfangssequenz, so gilt $\mathcal{E}S$ gemäß Voraussetzung; andernfalls wurde S durch Anwendung einer Basisregel auf gewisse der S_i für $i < n$ gewonnen. Damit gilt aber auch $\mathcal{E}S$, denn \mathcal{E} ist unter allen Basisregeln abgeschlossen.

Es gibt mehrere gleichwertige Definitionen von \vdash , darunter rein mengentheoretische. Die Gleichwertigkeitsbeweise solcher Definitionen sind ziemlich wortreich, aber nicht besonders inhaltsreich. Daher verzichten wir auf weitere Ausführungen hierüber, zumal im weiteren Verlauf der Ausführungen nur noch die Regelinduktion verwendet wird, nicht mehr die Definition von \vdash .

Wie bereits erwähnt, sind alle Basisregeln korrekt, d.h. die Folgerungseigenschaft ist unter allen Basisregeln abgeschlossen. Daher ergibt Regelinduktion sofort die *Korrektheit* des Kalküls $\vdash \subseteq \models$, oder ausführlich

$$X \vdash \alpha \Rightarrow X \models \alpha, \text{ für alle } X, \alpha.$$

Mit Regelinduktion beweist man z.B. auch $X \vdash \alpha \Rightarrow X^\sigma \vdash \alpha^\sigma$, und speziell den

Satz 4.1 (Endlichkeitssatz für \vdash). *Ist $X \vdash \alpha$, so ist bereits $X_0 \vdash \alpha$ für eine endliche Teilmenge $X_0 \subseteq X$.*

Beweis. Sei $\mathcal{E}(X, \alpha)$ die Eigenschaft ‘ $X_0 \vdash \alpha$ für ein gewisses endliches $X_0 \subseteq X$ ’. Sicher gilt $\mathcal{E}(X, \alpha)$ für $X = \{\alpha\}$, mit $X_0 = X$. Und hat X eine endliche Teilmenge X_0 mit $X_0 \vdash \alpha$, so auch jede Obermenge $X' \supseteq X$. Also ist \mathcal{E} unter (MR) abgeschlossen. Sei $\mathcal{E}(X, \alpha)$, $\mathcal{E}(X, \beta)$, etwa $X_1 \vdash \alpha$, $X_2 \vdash \beta$ für endliche $X_1, X_2 \subseteq X$. Dann ist auch $X_0 \vdash \alpha, \beta$ für $X_0 = X_1 \cup X_2$. Daher ist $X_0 \vdash \alpha \wedge \beta$ nach $(\wedge 1)$. Also gilt $\mathcal{E}(X, \alpha \wedge \beta)$, womit \mathcal{E} auch unter $(\wedge 1)$ abgeschlossen ist. Analog zeigt man dies für alle übrigen Basisregeln für \vdash . Also ergibt sich die Behauptung gemäß Regelinduktion. \square

Von großer Bedeutung ist der formale Konsistenzbegriff, der die Ableitungsrelation nach dem folgenden Lemma bereits vollkommen bestimmt. Es wird sich herausstellen, dass ‘konsistent’ den Begriff ‘erfüllbar’ adäquat beschreibt.

Definition. $X \subseteq \mathcal{F}$ heie *inkonsistent* (bezüglich unseres Kalkls), wenn $X \vdash \alpha$ für alle Formeln α , und andernfalls *konsistent*. X heit *maximal konsistent*, wenn X konsistent ist, doch jede echte Obermenge $X' \supset X$ inkonsistent ist.

Die Inkonsistenz von X lässt sich durch die Ableitbarkeit einer einzigen Formel kennzeichnen, nämlich von $\perp (= p_1 \wedge \neg p_1)$. Denn $X \vdash \perp$ impliziert $X \vdash p_1, \neg p_1$ nach $(\wedge 1)$ und damit $X \vdash \alpha$ für alle α gemäß $(\neg 1)$, d.h. X ist inkonsistent. Ist dies umgekehrt der Fall, gilt speziell $X \vdash \perp$. Wir dürfen $X \vdash \perp$ daher lesen als ‘ X ist inkonsistent’, und $X \not\vdash \perp$ als ‘ X ist konsistent’, wovon nachfolgend oft Gebrauch gemacht wird. Eine maximal konsistente Menge X ist immer deduktiv abgeschlossen, d.h. $X \vdash \alpha \Rightarrow \alpha \in X$ (Übung 3) und hat manche anderen Besonderheiten.

Lemma 4.2. \vdash hat die Eigenschaften

$$\mathcal{C}^+ : X \vdash \alpha \Leftrightarrow X, \neg\alpha \vdash \perp, \quad \mathcal{C}^- : X \vdash \neg\alpha \Leftrightarrow X, \alpha \vdash \perp.$$

Beweis. Mit $X \vdash \alpha$ gilt auch $X, \neg\alpha \vdash \alpha$. Da gewiss $X, \neg\alpha \vdash \neg\alpha$, ist $X, \neg\alpha \vdash \beta$ für alle β nach $(\neg 1)$, insbesondere $X, \neg\alpha \vdash \perp$. Sei umgekehrt Letzteres der Fall. Dann ist nach der Anmerkung oben $X, \neg\alpha \vdash \alpha$, also $X \vdash \alpha$ gemäß \neg -Elimination in den Beispielen vorhin. \mathcal{C}^- bestätigt man völlig analog. \square

Die noch nicht bewiesene Behauptung $\models \subseteq \vdash$ ist äquivalent mit $X \not\vdash \alpha \Rightarrow X \not\models \alpha$, für alle X und α , aber in dieser Formulierung erkennt man sofort, was für den Beweis zu tun ist: Da $X \not\vdash \alpha$ nach \mathcal{C}^+ mit der Konsistenz von $X' := X \cup \{\neg\alpha\}$ gleichwertig ist, sowie $X \not\models \alpha$ mit der Erfüllbarkeit von X' , müssen wir nur zeigen, dass konsistente Mengen erfüllbar sind. Dieser Nachweis stützt sich auf

Lemma 4.3 (Satz von Lindenbaum). *Jede konsistente Menge X kann erweitert werden zu einer maximal konsistenten Menge $X' \supseteq X$.*

Beweis. Sei H die bzgl. Inklusion halbgeordnete Menge aller konsistenten $Y \supseteq X$. Weil $X \in H$, ist H nichtleer. Sei $K \subseteq H$ eine Kette, d.h. $Y \subseteq Z$ oder $Z \subseteq Y$ für alle $Y, Z \in K$. Dann ist $U = \bigcup K$ eine obere Schranke für K ; denn für $Y \in K$ ist sicher $Y \subseteq U$, und darüber hinaus – und dies ist der springende Punkt – ist U auch konsistent: $U \vdash \perp$ ergibt nämlich $U_0 \vdash \perp$ für ein endliches $U_0 = \{\alpha_0, \dots, \alpha_n\} \subseteq U$ nach Satz 4.1; ist etwa $\alpha_i \in Y_i \in K$ und Y die größte der Mengen Y_0, \dots, Y_n , so ist $\alpha_i \in Y$ für alle $i \leq n$, also auch $Y \vdash \perp$ nach (MR), was $Y \in H$ widerspricht. Nach dem Zornschen Lemma (Seite 37) hat H daher ein maximales Element X' , und dies ist offenbar eine maximal konsistente Erweiterungsmenge von X . \square

Bemerkung 1. Obiger Beweis, der den Dingen ausnahmsweise etwas vorgreift, ist frei von Annahmen über die Mächtigkeit der Sprache. Lindenbaums ursprüngliche Konstruktion bezog sich hingegen auf abzählbare Sprachen \mathcal{F} und verläuft wie folgt: Sei $X_0 := X \subseteq \mathcal{F}$ konsistent und $\alpha_0, \alpha_1, \dots$ eine Aufzählung von \mathcal{F} . Man setze $X_{n+1} = X_n \cup \{\alpha_n\}$, falls diese Menge konsistent ist, und $X_{n+1} = X_n$ sonst. Dann ist $Y = \bigcup_{n \in \omega} X_n$ eine maximal konsistente Erweiterung von X , wie leicht zu verifizieren ist. Hier wird das mit dem Auswahlaxiom gleichwertige Lemma von Zorn nicht benötigt.

Lemma 4.4. *Eine maximal konsistente Menge X hat die Eigenschaft*

$$X \vdash \neg\alpha \Leftrightarrow X \not\vdash \alpha, \text{ für beliebiges } \alpha.$$

Beweis. Ist $X \vdash \neg\alpha$, so kann $X \vdash \alpha$ wegen der Konsistenz von X nicht gelten. Ist andererseits $X \not\vdash \alpha$, so ist $X, \neg\alpha$ nach \mathcal{C}^+ konsistent. Folglich $\neg\alpha \in X$, denn X ist maximal konsistent. Also auch $X \vdash \neg\alpha$. \square

Maximal konsistente Mengen erlauben eine einfache Modellkonstruktion. Dies zeigt

Lemma 4.5. *Eine maximal konsistente Menge X ist erfüllbar.*

Beweis. Sei w definiert durch $w \models p \Leftrightarrow X \vdash p$. Dann gilt für alle α

$$(*) \quad X \vdash \alpha \Leftrightarrow w \models \alpha.$$

Dies ist klar für Primformeln α gemäß Definition von w . Ferner ist

$$\begin{aligned} X \vdash \alpha \wedge \beta &\Leftrightarrow X \vdash \alpha, \beta && \text{(Regeln } (\wedge 1), (\wedge 2) \text{)} \\ &\Leftrightarrow w \models \alpha, \beta && \text{(Induktionsannahme)} \\ &\Leftrightarrow w \models \alpha \wedge \beta && \text{(Definition)} \\ X \vdash \neg\alpha &\Leftrightarrow X \not\vdash \alpha && \text{(Lemma 4.4)} \\ &\Leftrightarrow w \not\models \alpha && \text{(Induktionsannahme)} \\ &\Leftrightarrow w \models \neg\alpha && \text{(Definition).} \end{aligned}$$

Das beweist $(*)$ und damit $w \models X$, also die Behauptung. \square

Damit wurde die Gleichwertigkeit der Konsistenz und der Erfüllbarkeit einer Formelmengenge gezeigt und wir erhalten nunmehr leicht das Hauptresultat des Abschnitts:

Satz 4.6 (Vollständigkeitssatz). *Für alle X, α gilt $X \vdash \alpha \Leftrightarrow X \models \alpha$.*

Beweis. $X \vdash \alpha \Rightarrow X \models \alpha$ ist die Korrektheit des Kalküls. Ist andererseits $X \not\vdash \alpha$, so ist $X, \neg\alpha$ konsistent. Sei Y maximal konsistente Erweiterung von $X, \neg\alpha$ gemäß Lemma 4.3. Nach Lemma 4.5 ist Y erfüllbar, also auch $X, \neg\alpha$. Daher $X \not\models \alpha$. \square

Einen kürzeren, dafür aber die Substitutionen wesentlich benutzenden, eleganten Vollständigkeitsbeweis gibt Übung 5. Satz 4.6 liefert unmittelbar den

Satz 4.7 (Endlichkeitssatz für das Folgern). *Ist $X \models \alpha$, so ist $X_0 \models \alpha$ für eine gewisse endliche Teilmenge X_0 von X .*

Dies ist klar, denn für \vdash gilt ja der Endlichkeitssatz. Hieraus ergibt sich leicht der

Satz 4.8 (Endlichkeitssatz der Erfüllbarkeit, Kompaktheitssatz). *X ist erfüllbar, wenn nur jede endliche Teilmenge von X erfüllbar ist.*

Denn ist X unerfüllbar, d.h. $X \models \perp$, ist nach Satz 4.7 schon $X_0 \models \perp$ für ein endliches $X_0 \subseteq X$, und der Satz ist bewiesen. Umgekehrt ergibt Satz 4.8 leicht den Satz 4.7. Beide Sätze sind also direkt auseinander herleitbar.

Weil Satz 4.6 keine speziellen Annahmen über die Mächtigkeit der Variablenmenge erfordert, gilt dieser ebenso wie der hieraus folgende Kompaktheitssatz ohne diesbezügliche Einschränkungen. Dies macht den Satz zu einem brauchbaren Instrument für Anwendungen, die im nächsten Abschnitt erläutert werden.

Bemerkung 2. Es lassen sich auch direkte Beweise für Satz 4.8 oder geeignete Umformulierungen hiervon angeben, die mit einem Regelkalkül nichts zu tun haben. So ist dieser Satz beispielsweise äquivalent mit $\bigcap_{\alpha \in X} \text{Md } \alpha = \emptyset \Rightarrow \bigcap_{\alpha \in X_0} \text{Md } \alpha = \emptyset$ für ein endliches $X_0 \subseteq X$, wobei $\text{Md } \alpha$ die Menge aller Modelle von α bezeichnet. In dieser Formulierung wird die Kompaktheit eines gewissen, auf natürliche Weise entstehenden topologischen Raumes behauptet, dessen Punkte die Belegungen der Variablen sind. Daher auch der Name *Kompaktheitssatz*. Näheres zu diesem Thema findet man z.B. in [RS]. Übung 5 unten liefert nicht nur die Sätze 4.7 und 4.8, sondern auch die Tatsache, dass der Konsequenzrelation \models weder neue Tautologien noch neue Regeln konsistent hinzugefügt werden können (Post-Vollständigkeit und strukturelle Vollständigkeit von \models , siehe hierzu [Ra1]).

Übungen

1. Man beweise, ist $X \cup \{\neg\alpha \mid \alpha \in Y\}$ inkonsistent und $Y \neq \emptyset$, so existieren Formeln $\alpha_0, \dots, \alpha_n \in Y$ mit $X \vdash \alpha_0 \vee \dots \vee \alpha_n$.
2. Man erweitere die Signatur $\{\neg, \wedge\}$ um \vee und beweise die Vollständigkeit des Kalküls, der die bisherigen Regeln um die beiden folgenden ergänzt:
$$\frac{X \vdash \alpha}{X \vdash \alpha \vee \beta, \beta \vee \alpha} \quad ; \quad \frac{X, \alpha \vdash \gamma \mid X, \beta \vdash \gamma}{X, \alpha \vee \beta \vdash \gamma}.$$
3. Man zeige, maximal konsistente Mengen sind deduktiv abgeschlossen. Dies gilt für jeden logischen Kalkül, in dem Inkonsistenz durch die Ableitbarkeit von nur einer einzigen Formel wie etwa \perp charakterisiert ist.
4. Es sei \vdash eine finitäre Konsequenzrelation in $\mathcal{F}\{\wedge, \neg\}$ mit den Eigenschaften $(\wedge 1)$ – $(\neg 2)$. Man zeige, \vdash ist *maximal*, d.h. ist $\vdash' \supset \vdash$, so gilt $\vdash' \alpha$ für alle α .
5. Man zeige durch Rückführung auf Übung 4: es gibt genau eine Konsequenzrelation in $\mathcal{F}\{\wedge, \neg\}$, welche $(\wedge 1)$ – $(\neg 2)$ erfüllt. Dies impliziert offenbar die Vollständigkeit des Kalküls \vdash , weil auch \models diese Eigenschaften hat.

1.5 Anwendungen des Kompaktheitssatzes

Satz 4.8 ist sehr nützlich, um gewisse Eigenschaften endlicher Strukturen auf unendliche zu übertragen. Nachfolgend einige typische Beispiele. Diese könnte man auch mit dem prädikatenlogischen Kompaktheitssatz 3.3.2 behandeln, aber die Beispiele lehren, wie man die Konsistenz gewisser Aussagenmengen der Prädikatenlogik auch aussagenlogisch gewinnt. Dies erweist sich u.a. als nützlich für Kapitel 4.

1. Jede Menge M kann (total) geordnet werden.⁴⁾

Das bedeutet, es gibt eine irreflexive, transitive und konnexe Relation $<$ auf M . Für endliches M folgt dies leicht induktiv über die Elementzahl von M . Die Behauptung ist klar für $M = \emptyset$ oder 1-elementiges M , und ist $M = N \cup \{a\}$ mit einer n -elementigen Menge N und $(n+1)$ -elementigem M , erhält man aus einer nach Induktionsannahme existierenden Ordnung von N eine solche für M , indem man das Element a einfach „hintendran“ setzt, d.h. es sei $x < a$ für alle $x \in N$.

Sei nun M beliebig. Wir betrachten für jedes Paar $(a, b) \in M \times M$ je eine Aussagenvariable p_{ab} . Sei X die Formelmengende bestehend aus den Formeln

$$\begin{aligned} \neg p_{aa} & \quad (a \in M), \\ p_{ab} \wedge p_{bc} \rightarrow p_{ac} & \quad (a, b, c \in M), \\ p_{ab} \vee p_{ba} & \quad (a \neq b). \end{aligned}$$

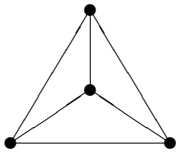
Aus einem Modell w für X gewinnen wir sofort eine Ordnung $<$ durch die Erklärung $a < b \Leftrightarrow w \models p_{ab}$. So besagt $w \models \neg p_{aa}$ dasselbe wie $a \not< a$. Analog reflektieren die weiteren Formeln jeweils die Transitivität und die Konnexität. Nach Satz 4.8 hat X ein Modell, wenn nur jede endliche Teilmenge $X_0 \subseteq X$ eines hat. Sei X_0 gegeben. Darin kommen nur endlich viele Variablen vor. Folglich gibt es endliche Mengen $M_1 \subseteq M$ und $X_1 \supseteq X_0$, wobei X_1 genau so gebildet wird wie X , nur durchlaufen a, b, c jetzt die endliche Menge M_1 anstelle von M . Nun ist X_1 und damit X_0 tatsächlich erfüllbar: ist nämlich $<$ eine Ordnung der endlichen Menge M_1 und wird w durch $w \models p_{ab} \Leftrightarrow a < b$ erklärt, so ist w offenbar Modell für X_1 .

2. Der Vierfarbensatz für unendliche planare Graphen.

Ein *einfacher Graph* sei ein Paar (E, K) mit einer Menge E , deren Elemente *Punkte* oder *Ecken* heißen, und einer Menge K von ungeordneten Paaren $\{a, b\}$ aus Punkten $a \neq b$, *Kanten* genannt (man kann K auch als irreflexive und symmetrische Relation verstehen, siehe 2.1). Ist $\{a, b\} \in K$, so heißen a, b *benachbart*. (E, K) heiße *k-chromatisch*, wenn man eine Zerlegung $E = C_1 \cup \dots \cup C_k$ mit $C_i \cap C_j = \emptyset$ für $i \neq j$

⁴⁾ Nicht erklärte Begriffe werden in 2.1 definiert. Das Beispiel ist u.a. deswegen von Interesse, weil der Kompaktheitssatz echt schwächer ist als das Auswahlaxiom, nach welchem sich jede Menge sogar wohlordnen lässt. Also ist auch die Ordnungsfähigkeit aller Mengen schwächer als dieses.

(den Färbungsklassen) so angeben kann, dass benachbarte Punkte nicht die gleiche Farbe tragen. Kurzum, $a, b \in C_i \Rightarrow \{a, b\} \notin K$ für $i = 1, \dots, k$.



Die Figur zeigt den kleinsten 4-chromatischen Graphen, der nicht 3-chromatisch ist. Alle Punkte sind zueinander benachbart. Wir zeigen, ein Graph (E, K) ist k -chromatisch, wenn dies nur für jeden endlichen Teilgraphen (E_0, K_0) der Fall ist (K_0 besteht aus den Kanten $\{a, b\} \in K$ mit $a, b \in E_0$). Dazu betrachte man folgende aus den Variablen $p_{i,a}$ für $1 \leq i \leq k$ und $a \in E$ gebildete Formelmengenge X :

$$\begin{aligned} p_{1,a} \vee \dots \vee p_{k,a}, & \quad \neg(p_{i,a} \wedge p_{j,a}) & (1 \leq i < j \leq k, a \in E), \\ & \neg(p_{i,a} \wedge p_{i,b}) & (i = 1, \dots, k, \{a, b\} \in K). \end{aligned}$$

Wieder genügt es, ein Modell w für X anzugeben. Denn w liefert eine Einteilung $E = C_1 \cup \dots \cup C_k$ in k Färbungsklassen durch die Erklärung $a \in C_i \Leftrightarrow w \models p_{i,a}$. Die erste Formel besagt nämlich, jeder Punkt gehört wenigstens einer Färbungsklasse an, die zweite sichert deren Disjunktheit, und die dritte, dass benachbarte Punkte nicht dieselbe Farbe tragen. Wir müssen also jede endliche Teilmenge X_0 von X erfüllen. Sei (E_0, K_0) der endliche Teilgraph von (E, K) mit allen Punkten, die als Indizes in den Variablen von X_0 auftreten. Die auf (E_0, K_0) bezogene Voraussetzung sichert die Erfüllbarkeit von X_0 analog wie in Beispiel 1, und alles ist gezeigt. Jeder planare (ohne Überschneidung von Kanten in die Ebene einbettbare) endliche Graph ist nach dem *Vierfarbensatz* 4-chromatisch. Also gilt dieser nach dem Bewiesenen auch für alle unendlichen Graphen, deren endliche Teilgraphen sämtlich planar sind.

3. Der Königsche Graphensatz.

Es gibt verschiedene Versionen dieses Satzes. Wir beziehen ihn hier auf gerichtete Bäume. Ein *gerichteter Baum* sei ein Paar (E, \triangleleft) mit irreflexivem $\triangleleft \subseteq E^2$, so dass für ein gewisses $c \in E$, die *Wurzel* genannt, Folgendes gilt: c ist mit jedem anderen Punkt $a \in E$ durch genau einen *Weg* verbunden. Dies sei eine Folge (a_0, \dots, a_n) von Punkten mit $a_0 = c$, $a_n = a$ und $a_i \triangleleft a_{i+1}$ für alle $i < n$. Dies hat z.B. zur Folge, dass zu jedem $b \in E \setminus \{c\}$ genau ein Vorgänger $a \triangleleft b$ in E existiert.

Der Satz besagt nun: Hat jeder Punkt a nur endlich viele Nachfolger (Punkte b mit $a \triangleleft b$) und gibt es in (E, \triangleleft) beliebig lange von c ausgehende Wege, dann gibt es auch einen unendlichen, mit c beginnenden Weg durch den Baum, d.h. eine Folge $(c_k)_{k \in \mathbb{N}}$ derart, dass $c_0 = c$ und $c_k \triangleleft c_{k+1}$. Zum Beweis erklären wir rekursiv $S_0 = \{c\}$ und $S_{k+1} = \{b \in E \mid \text{es gibt ein } a \in S_k \text{ mit } a \triangleleft b\}$. Weil jeder Punkt nur endlich viele Nachfolger hat, ist jede „Schicht“ S_k endlich, und weil es beliebig lange Wege (c, a_1, \dots, a_k) gibt und offenbar $a_k \in S_k$, ist kein S_k leer. Ferner ist klar, dass die Schichten S_0, S_1, \dots paarweise disjunkt sind. Sei nun p_a für jedes $a \in E$ je eine Aussagenvariable und X bestehe aus den Formeln

$$\begin{array}{ll} \text{(A)} & \bigvee_{a \in S_k} p_a, \quad \neg(p_a \wedge p_b) \quad (a, b \in S_k, a \neq b, k = 0, 1, \dots), \\ \text{(B)} & p_b \rightarrow p_a \quad (a, b \in E, a \triangleleft b). \end{array}$$

Ist $w \models X$, gibt es wegen (A) genau ein $c_k \in S_k$ mit $w \models p_{c_k}$. Speziell ist $c_0 = c$. Sei $a \in S_k$ so gewählt, dass $a \triangleleft c_{k+1} \in S_{k+1}$. Nach (B) ist wegen $w \models p_{c_{k+1}}$ auch $w \models p_a$, d.h. $a = c_k$, denn c_k ist der einzige Punkt in S_k mit $w \models p_{c_k}$. Also $c_k \triangleleft c_{k+1}$ für alle k . Damit ist $(c_k)_{k \in \mathbb{N}}$ tatsächlich ein Weg der gesuchten Art. Wieder ist jedes endliche $X_0 \subseteq X$ erfüllbar: Ist in X_0 von Variablen bis höchstens zur Schicht S_n die Rede, so ist X_0 Teilmenge einer endlichen Formelmengens X_1 , welche wie X definiert ist, nur läuft k lediglich bis n . Und es ist klar, dass X_1 ein Modell hat.

4. Das Heiratsproblem (in linguistischem Gewande).

Sei N eine Menge von *Namen* (oder Worten) mit *Bedeutungen* in einer Menge B . Ein Name $\nu \in N$ kann *homonym* sein, d.h. mehrere Bedeutungen besitzen, oder *synonym* sein, d.h. mit anderen Namen aus N dieselbe Bedeutung haben, oder auch beides. Wir gehen von den plausiblen Annahmen aus, jeder Name ν habe nur endlich viele Bedeutungen, und k viele Namen haben mindestens k viele Bedeutungen. Wir behaupten, es gibt eine *Bedeutungsunifizierung*. Dies sei eine injektive Abbildung $f: N \rightarrow B$, die jedem ν eine seiner ursprünglichen Bedeutungen belässt.

Für endliche Mengen N zeigt man dies induktiv über die Elementzahl n von N : Für $n = 1$ ist die Behauptung klar. Sei nun $n > 1$. **Fall 1:** Je $m (< n)$ Namen haben mindestens $m + 1$ Bedeutungen. Man ordne einem beliebig gewählten $\nu \in N$ eine seiner Bedeutungen b zu, so dass von den Namen aus $N \setminus \{\nu\}$ je k Namen immer noch k Bedeutungen $\neq b$ haben. Nach Induktionsannahme gibt es eine Bedeutungsunifizierung für $N \setminus \{\nu\}$, welche zusammen mit (ν, b) eine solche für ganz N liefert. **Fall 2:** Es gibt ein m ($0 < m < n$) und ein m -elementiges $M \subseteq N$ mit einer nur m -elementigen Menge B_M aller Bedeutungen der $\nu \in M$. Jedem $\nu \in M$ lässt sich gemäß Induktionsannahme eine seiner Bedeutungen aus B_M zuordnen. Von den Namen aus $N \setminus M$ haben je k ($\leq n - m$) Namen dann immer noch k Bedeutungen außerhalb B_M wie man leicht sieht. Es gibt nach Induktionsannahme also auch eine Bedeutungsunifizierung für $N \setminus M$ in $B \setminus B_M$. Fügt man diese mit derjenigen für M zusammen, so ergibt sich offenbar eine solche für ganz N .

Um nun die Behauptung für beliebige Namensmengen N zu beweisen, ordne man jedem Paar $(\nu, b) \in N \times B$ je eine Variable $p_{\nu,b}$ zu und betrachte die Formelmengens

$$X: \begin{cases} p_{\nu,a} \vee \dots \vee p_{\nu,e} & (\nu \in N, a, \dots, e \text{ die Bedeutungen von } \nu), \\ \neg(p_{\nu,x} \wedge p_{\nu,y}) & (\nu \in N, x, y \in B, x \neq y). \end{cases}$$

Ist $w \models X$, erhält man durch die Erklärung $f\nu = b \Leftrightarrow w \models p_{\nu,b}$ offenbar eine Bedeutungsunifizierung von N . Jedes endliche $X_0 \subseteq X$ hat ein Modell, weil dort nur endlich viele Namen als Indizes vorkommen und für diesen Fall die Behauptung bewiesen wurde. Damit hat auch X ein Modell.

5. Der Ultrafiltersatz.

Dieser Satz ist von herausragender Bedeutung in der Topologie, der Mengenlehre, der Modelltheorie (siehe 5.7) und anderswo. Eine nichtleere Familie F von Teilmengen einer nichtleeren Menge I heißt ein *Filter auf I* , wenn für alle $M, N \subseteq I$

$$(a) \ M, N \in F \Rightarrow M \cap N \in F, \quad (b) \ M \in F \ \& \ M \subseteq N \Rightarrow N \in F,$$

(a) und (b) zusammen sind gleichwertig mit $(\cap) \ M \cap N \in F \Leftrightarrow M, N \in F$, wie man leicht sieht (man beachte $M \subseteq N \Rightarrow M \cap N = M$ für den Beweis von (b) aus (\cap)). Ein Filter $F \subseteq \mathfrak{P}I$ heißt *Ultrafilter auf I* , wenn F nebst (\cap) auch noch die Bedingung $(\neg) \ \neg M \in F \Leftrightarrow M \notin F$, für alle $M \subseteq I$ erfüllt; dabei sei $\neg M = I \setminus M$.

Für festes $J \subseteq I$ ist $F = \{M \subseteq I \mid M \supseteq J\}$ Beispiel eines Filters, denn gewiss gilt $J \subseteq M \cap N \Leftrightarrow J \subseteq M, N$. Ein simpler Spezialfall ist $F = \{I\}$. Wichtiges Beispiel eines Filters für unendliches I ist die Menge aller *koendlichen* Teilmengen $K \subseteq I$, d.h. $I \setminus K$ ist endlich. Denn $K_1 \cap K_2$ ist genau dann koendlich, wenn K_1, K_2 beide koendlich sind. Ultrafilter, die keine endlichen, also sämtliche koendlichen Mengen enthalten, heißen *nichttrivial*. $\{J \subseteq I \mid i_0 \in J\}$ ist für jedes $i_0 \in I$ ein trivialer Ultrafilter. Deren Existenz ist trivial. Das Problem sind nichttriviale Ultrafilter.

Ein Filter F heiße *echt*, wenn $F \neq \mathfrak{P}I$. Dies ist nach (b) gleichwertig mit $\emptyset \notin F$. Jeder echte Filter F erfüllt mit F für E die Voraussetzung im folgendem Satz, insbesondere der Filter aller koendlichen Teilmengen einer unendlichen Menge I . Der Satz sichert also die Existenz nichttrivialer Ultrafilter auf unendlichem I .

Ultrafiltersatz. *Jedes $E \subseteq \mathfrak{P}I$ kann zu einem Ultrafilter U auf I erweitert werden, sofern $\bigcap_{i \leq n} M_i \neq \emptyset$ für alle n und alle $M_0, \dots, M_n \in E$.*

Beweis. Man betrachte mit den Aussagenvariablen p_J für $J \subseteq I$ die Formelmenge

$$X : \quad p_{M \cap N} \leftrightarrow p_M \wedge p_N, \quad p_{\neg M} \leftrightarrow \neg p_M, \quad p_K \quad (M, N \subseteq I, \ K \in E).$$

Sei $w \models X$. Dann gelten offenbar (\cap) und (\neg) für $U := \{J \subseteq I \mid w \models p_J\}$. Also ist U Ultrafilter mit $E \subseteq U$. Es genügt daher zu zeigen, dass jede endliche Teilmenge von X ein Modell hat. Dazu reicht es offenbar, den Ultrafiltersatz für endliches $E \neq \emptyset$ zu beweisen. Das ist leicht. Denn sei $E = \{M_0, \dots, M_n\}$, $D := \bigcap_{i \leq n} M_i$ und $i_0 \in D$. Dann ist $U = \{J \subseteq I \mid i_0 \in J\}$ ein Ultrafilter mit $U \supseteq E$. \square

Übungen

1. Man zeige mit dem Kompaktheitssatz: jede partielle Ordnung \leq_0 einer Menge M kann zu einer totalen Ordnung \leq von M erweitert werden.
2. Sei U ein Ultrafilter auf einer unendlichen Menge I . Man zeige, U ist genau dann trivial, wenn ein $i_0 \in I$ existiert mit $U = \{J \subseteq I \mid i_0 \in J\}$.

1.6 Hilbert-Kalküle

Die in gewissem Sinne einfachsten logischen Kalküle sind sogenannte *Hilbert-Kalküle*. Sie beruhen auf ausgewählten Tautologien als *logischen Axiomen*, deren Auswahl aber recht willkürlich ist und auch wesentlich von der logischen Signatur abhängt. Sie benutzen ferner Schlussregeln wie z.B. den Modus Ponens MP : $\alpha, \alpha \rightarrow \beta / \beta$ ⁵⁾. Ein Vorteil dieser Kalküle besteht darin, dass formale Beweise durch endliche Formelfolgen unmittelbar präzisiert und veranschaulicht werden können. Dieser Vorteil wird sich vor allem bei der Gödelisierung des Beweisens auszahlen.

Im Folgenden betrachten wir einen solchen Kalkül mit MP als einziger Schlussregel. Der Kalkül wird vorübergehend mit \vdash bezeichnet, um ihn von dem in 1.4 betrachteten Regelkalkül \vdash zu unterscheiden. Die logische Signatur enthalte nur \neg, \wedge . In den Axiomen von \vdash erscheint jedoch die durch $\alpha \rightarrow \beta := \neg(\alpha \wedge \neg\beta)$ definierte Implikation, was die Niederschrift dieser Axiome erheblich verkürzt.

Das *logische Axiomensystem* unseres Kalküls bestehe aus der Menge Λ aller Formeln der folgenden Gestalt, wobei an die Rechtsklammerung erinnert sei.

$$\begin{array}{ll} \Lambda 1 & (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma), \\ \Lambda 2 & \alpha \rightarrow \beta \rightarrow \alpha \wedge \beta, \\ \Lambda 3 & \alpha \wedge \beta \rightarrow \alpha, \quad \alpha \wedge \beta \rightarrow \beta, \\ \Lambda 4 & (\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \neg\alpha). \end{array}$$

Λ enthält nur Tautologien. Auch sind die aus Λ mit MP herleitbaren Formeln sämtlich Tautologien, denn $\models \alpha, \alpha \rightarrow \beta$ impliziert $\models \beta$. Wir werden nachweisen, dass aus Λ mittels MP alle 2-wertigen Tautologien beweisbar sind und beginnen mit folgender

Definition. Ein *Beweis* aus X (im Kalkül \vdash) sei eine Folge $(\varphi_0, \dots, \varphi_n)$, so dass für jedes $k \leq n$: $\varphi_k \in X \cup \Lambda$ oder aber es existieren Indizes $i, j < k$ mit $\varphi_i = \varphi_j \rightarrow \varphi_k$ (d.h. φ_k entsteht durch Anwendung von MP auf Folgenglieder, die φ_k vorangehen). Ein Beweis $(\varphi_0, \dots, \varphi_n)$ mit $\varphi_n = \alpha$ heißt *ein Beweis für α aus X* . Es sei $X \vdash \alpha$ (aus X ist α *beweisbar* oder *ableitbar*), wenn es einen Beweis für α aus X gibt.

Beispiel. $(p, q, p \rightarrow q \rightarrow p \wedge q, q \rightarrow p \wedge q, p \wedge q)$ ist ein Beweis für $p \wedge q$ aus $X = \{p, q\}$. Man beachte, das Folgenglied $p \rightarrow q \rightarrow p \wedge q$ dieses Beweises gehört zu Λ .

Weil ein Beweis nur endlich viele Formeln enthält, liefert obige Definition z.B. unmittelbar den wie Satz 4.1 formulierten Endlichkeitssatz für \vdash . Jeder Anfang eines Beweises ist offenbar selbst ein Beweis. Ferner ist die Verkettung von Beweisen für α und für $\alpha \rightarrow \beta$ und die Verlängerung der entstehenden Folge um β ein Beweis für

⁵⁾Diese Schreibweise soll grob gesagt zum Ausdruck bringen, dass β aus einer Formelmengende X als bewiesen gilt, wenn zuvor α und $\alpha \rightarrow \beta$ aus X bewiesen wurden. MP ist Beispiel einer 2-stelligen Hilbert-Regel. Für eine allgemeine Definition dieses Regel-Typs siehe z.B. [Ra1].

β , wie man mit bloßem Auge sieht. Damit gilt also

$$(*) \quad X \vdash \alpha, \alpha \rightarrow \beta \Rightarrow X \vdash \beta.$$

Kurzum, die Menge der aus X beweisbaren Formeln ist MP-*abgeschlossen*. Eine Anwendung von $(*)$ wird oft durch die Redeweise „MP ergibt...“ zitiert. Man sieht leicht, dass $X \vdash \alpha$ genau dann, wenn α zur kleinsten X umfassenden und unter MP abgeschlossenen Formelmengende gehört. Für die Gödelisierung des Beweises und für das automatische Beweisen ist aber ratsam, mit dem obigen finiten Begriff eines Beweises zu arbeiten und die Mengenlehre aus dem Spiel zu lassen. Zum Glück befreit uns der folgende Satz von der Pflicht, Eigenschaften von Formeln α mit $X \vdash \alpha$ jedesmal induktiv über die Länge eines Beweises von α aus X nachzuweisen.

Satz 6.1 (Induktionssatz für \vdash). *Sei X gegeben und \mathcal{E} eine Eigenschaft von Formeln mit (o) $\mathcal{E}\alpha$ gilt für alle $\alpha \in X \cup \Lambda$, (s) $\mathcal{E}\beta, \mathcal{E}(\beta \rightarrow \alpha) \Rightarrow \mathcal{E}\alpha$, für alle α, β . Dann gilt $\mathcal{E}\alpha$ für alle α mit $X \vdash \alpha$.*

Beweis durch Induktion über die Länge n eines Beweises von α aus X . Habe α einen Beweis Φ der Länge n und sei $\mathcal{E}\varphi$ für alle Formeln φ mit Beweisen einer Länge $< n$ angenommen. Ist $\alpha \in X \cup \Lambda$ – was für $n = 1$ stets der Fall ist – gilt $\mathcal{E}\alpha$ gemäß (o). Falls aber $\alpha \notin X \cup \Lambda$, so enthält Φ Glieder β und $\beta \rightarrow \alpha$ mit Beweisen einer Länge $< n$ (weil doch jeder Anfang von Φ selbst ein Beweis ist). Es gelten also $\mathcal{E}\beta$ und $\mathcal{E}(\beta \rightarrow \alpha)$ nach Induktionsannahme und somit $\mathcal{E}\alpha$ gemäß (s). \square

Eine Anwendung von Satz 6.1 ist der Nachweis von $\vdash \subseteq \models$, oder ausführlicher

$$(Kor) \quad X \vdash \alpha \Rightarrow X \models \alpha \quad (Korrektheit).$$

Denn sei $\mathcal{E}\alpha$ die Eigenschaft ‘ $X \models \alpha$ ’, mit fest vorgegebenem X . Sicher gilt $X \models \alpha$ für $\alpha \in X$. Dasselbe gilt für $\alpha \in \Lambda$. Also $\mathcal{E}\alpha$ für alle $\alpha \in X \cup \Lambda$ und (o) ist bestätigt. Sei nun $X \models \beta, \beta \rightarrow \alpha$. Dann ist auch $X \models \alpha$, was den Induktionsschritt (s) beweist. Nach Satz 6.1 gilt $\mathcal{E}\alpha$, d.h. $X \models \alpha$, wenn immer $X \vdash \alpha$. Damit ist (Kor) bewiesen.

Anders als in \vdash sind für den Vollständigkeitsbeweis von \vdash eine Reihe von Ableitungen auszuführen. Dies liegt in der Natur der Sache. Man muss Hilbert-Kalküle oft durch geduldige Ableitungen „erst einmal zum Laufen bringen“. Wir verwenden nachfolgend die offenkundige Monotonieeigenschaft $X' \supseteq X \vdash \alpha \Rightarrow X' \vdash \alpha$. Wie üblich stehe $\vdash \alpha$ für $\emptyset \vdash \alpha$.

Lemma 6.2. (a) $X \vdash \alpha \rightarrow \neg\beta \Rightarrow X \vdash \beta \rightarrow \neg\alpha$, (b) $\vdash \alpha \rightarrow \beta \rightarrow \alpha$,
(c) $\vdash \alpha \rightarrow \alpha$, (d) $\vdash \alpha \rightarrow \neg\neg\alpha$, (e) $\vdash \beta \rightarrow \neg\beta \rightarrow \alpha$.

Beweis. (a): Sicher ist $X \vdash (\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \neg\alpha)$ nach Axiom $\Lambda 4$. Daraus und aus $X \vdash \alpha \rightarrow \neg\beta$ ergibt sich $X \vdash \beta \rightarrow \neg\alpha$ mit MP. (b): Es ist $\vdash \beta \wedge \neg\alpha \rightarrow \neg\alpha$ gemäß $\Lambda 3$,

mit (a) also $\vdash \alpha \rightarrow \neg(\beta \wedge \neg\alpha) = \alpha \rightarrow \beta \rightarrow \alpha$. (c): Mit $\gamma := \alpha$, $\beta := \alpha \rightarrow \alpha$ in $\Lambda 1$ erhält man $\vdash (\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow \alpha \rightarrow \alpha$. Das ergibt mit (b) nach zweimaliger Anwendung von MP gerade (c). (d) folgt mit (a) dann aus $\vdash \neg\alpha \rightarrow \neg\alpha$. (e): Wegen $\vdash \neg\beta \wedge \neg\alpha \rightarrow \neg\beta$ und (a) ist $\vdash \beta \rightarrow \neg(\neg\beta \wedge \neg\alpha) = \beta \rightarrow \neg\beta \rightarrow \alpha$. \square

Punkt (e) dieses Lemmas ergibt sofort, dass \vdash die Regel $(\neg 1)$ aus **1.4** erfüllt, also $X \vdash \beta, \neg\beta \Rightarrow X \vdash \alpha$. Wegen $\Lambda 2, \Lambda 3$ erfüllt \vdash sicher auch $(\wedge 1)$ und $(\wedge 2)$. Wir beweisen nach Abschluß einiger Vorbereitungen auch die Regel $(\neg 2)$ für \vdash und erhalten danach leicht das gewünschte Vollständigkeitsresultat.

Lemma 6.3 (Deduktionstheorem). $X, \alpha \vdash \gamma$ impliziert $X \vdash \alpha \rightarrow \gamma$.

Beweis durch Induktion in \vdash mit der Prämissenmenge X, α . Sei $X, \alpha \vdash \gamma$. Es bedeute $\mathcal{E}\gamma$ jetzt ' $X \vdash \alpha \rightarrow \gamma$ '. Zum Nachweis von (o) sei $\gamma \in X \cup \Lambda \cup \{\alpha\}$. Ist $\gamma = \alpha$, gilt $X \vdash \alpha \rightarrow \gamma$ nach Lemma 6.2(c). Ist $\gamma \in X \cup \Lambda$, so gilt sicher $X \vdash \gamma$. Weil auch $X \vdash \gamma \rightarrow \alpha \rightarrow \gamma$ nach Lemma 6.2(b), folgt $X \vdash \alpha \rightarrow \gamma$ mit MP. Zum Nachweis von (s) sei $X, \alpha \vdash \beta$ und $X, \alpha \vdash \beta \rightarrow \gamma$, so dass $X \vdash \alpha \rightarrow \beta, \alpha \rightarrow \beta \rightarrow \gamma$ nach Induktionsannahme. Zweimalige Anwendung von MP auf $\Lambda 1$ ergibt offenbar $X \vdash \alpha \rightarrow \gamma$. Damit ist (s) bestätigt und das Lemma bewiesen. \square

Lemma 6.4. $\vdash \neg\neg\alpha \rightarrow \alpha$.

Beweis. Gemäß $\Lambda 3$ und MP ist $\neg\neg\alpha \wedge \neg\alpha \vdash \neg\alpha, \neg\neg\alpha$. Sei τ beliebig mit $\vdash \tau$. Die schon bewiesene Regel $(\neg 1)$ ergibt $\neg\neg\alpha \wedge \neg\alpha \vdash \neg\tau$, und Lemma 6.3 $\vdash \neg\neg\alpha \wedge \neg\alpha \rightarrow \neg\tau$. Nach Lemma 6.2(a) folgt $\vdash \tau \rightarrow \neg(\neg\neg\alpha \wedge \neg\alpha)$. MP liefert damit $\vdash \neg(\neg\neg\alpha \wedge \neg\alpha)$ und wegen $\neg(\neg\neg\alpha \wedge \neg\alpha) = \neg\neg\alpha \rightarrow \alpha$ die Behauptung des Lemmas. \square

Lemma 6.5. \vdash erfüllt Regel $(\neg 2)$, d.h. wenn $X, \beta \vdash \alpha$ und $X, \neg\beta \vdash \alpha$, so $X \vdash \alpha$.

Beweis. Sei $X, \beta \vdash \alpha$ und $X, \neg\beta \vdash \alpha$, also auch $X, \beta \vdash \neg\neg\alpha$ und $X, \neg\beta \vdash \neg\neg\alpha$ nach Lemma 6.2(d). Dann ist $X \vdash \beta \rightarrow \neg\neg\alpha, \neg\beta \rightarrow \neg\neg\alpha$ (Lemma 6.3), also $X \vdash \neg\alpha \rightarrow \neg\beta$ und $X \vdash \neg\alpha \rightarrow \neg\neg\beta$ nach Lemma 6.2(a). Daher $X, \neg\alpha \vdash \neg\beta, \neg\neg\beta$, also $X, \neg\alpha \vdash \neg\tau$ nach $(\neg 1)$, mit τ wie in Lemma 6.4. Folglich $X \vdash \neg\alpha \rightarrow \neg\tau$ (Lemma 6.3) und daher $X \vdash \tau \rightarrow \neg\neg\alpha$ nach Lemma 6.2(a). Wegen $X \vdash \tau$ folgt $X \vdash \neg\neg\alpha$ und mithin $X \vdash \alpha$ gemäß Lemma 6.4. \square

Satz 6.6 (Vollständigkeitssatz). $\vdash = \models$.

Beweis. Nach (Kor) ist $\vdash \subseteq \models$. Weil \vdash alle Basisregeln von \models erfüllt, ist $\models \subseteq \vdash$. Nach Satz 4.6 sind \vdash und \models identisch, also $\models \subseteq \vdash$. Damit ist alles gezeigt. \square

Danach gilt insbesondere $\vdash \alpha \Leftrightarrow \models \alpha$. Kurzum, genau die 2-wertigen Tautologien lassen sich mittels MP aus dem Axiomensystem Λ gewinnen.

Man erhält die Vollständigkeit von \vdash durch einen Beweis der einschlägigen Lemmata aus 1.4 in naheliegender Weise natürlich auch ohne Rückgriff auf \vdash .

Bemerkung. Es mag überraschend klingen, dass $\Lambda 1$ – $\Lambda 4$ bereits ausreichen, um alle aussagenlogischen Tautologien zu gewinnen. Denn diese Axiome und alle daraus mit MP herleitbaren Formeln gelten sämtlich in der intuitionistischen und sogar in der Minimallogik, siehe hierzu etwa [Ra1]. Dass Λ dennoch alle Tautologien abzuleiten gestattet, liegt daran, dass \rightarrow *definiert* wurde. Würde man \rightarrow als eigenständigen Junktor betrachten, wäre dies nicht mehr der Fall. Um dies einzusehen, ändere man die Interpretation von \neg durch die Erklärung $\neg 0 = \neg 1 = 1$. Auch dann erhalten alle Axiome von Λ bei jeder Belegung den Wert 1, ebenso wie auch alle aus Λ mit MP herleitbaren Formeln, nicht jedoch z.B. die Formel $\neg\neg p \rightarrow p$, die anders als in Lemma 6.4 behauptet, dann auch nicht herleitbar sein kann.

Mit Hilbert-Kalkülen lassen sich auch andere zwei- und mehrwertige Logiken axiomatisieren, z.B. das funktional unvollständige Fragment der zweiwertigen Logik in Übung 4. Auch das Fragment in \wedge, \vee , das zwar keine Tautologien hat, in dem aber interessante Hilbert-Regeln gelten, ist durch endlich viele derartige Regeln axiomatisierbar, darunter z.B. $p, q/p \wedge q$. Der Beweis hierfür ist jedoch weniger einfach als der Text oder die Übungen vermuten lassen. Jedes der unendlich vielen Fragmente 2-wertiger Logik mit oder ohne Tautologien ist durch einen Hilbert-Kalkül mit endlich vielen Hilbert-Regeln der betreffenden Sprache axiomatisierbar wie in [HeR] bewiesen wurde.

Neben Sequenzen- und Hilbert-Kalkülen gibt es weitere Kalküle, z.B. Tableau-Kalküle in verschiedenen Varianten, die vor allem für nichtklassische logische Systeme bedeutsam sind. In Kapitel 4 wird z.B. der für die Logikprogrammierung und das maschinelle Beweisen wichtige Resolutionskalkül behandelt.

Übungen

1. Man gebe einen Beweis für die Formel $p \rightarrow p$ aus Λ explizit an.
2. Man beweise die Vollständigkeit des Hilbert-Kalküls \vdash in $\mathcal{F}\{\rightarrow, \perp\}$ mit MP als einziger Schlussregel, der Definition $\neg\alpha := \alpha \rightarrow \perp$, sowie den Axiomen
 $A1 \ \alpha \rightarrow \beta \rightarrow \alpha, \ A2 \ (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow \alpha \rightarrow \gamma, \ A3 \ \neg\neg\alpha \rightarrow \alpha$.
3. Sei \vdash eine finitäre Konsequenzrelation und $X \not\vdash \alpha$. Man zeige mit dem Zornschen Lemma: es gibt ein $Y \supseteq X$ mit $Y \not\vdash \alpha$ und $Y, \beta \vdash \alpha$ für alle $\beta \notin Y$ (Y ist α -maximal). Ferner beweise man $Y \vdash \beta \Leftrightarrow \beta \in Y$ für α -maximales Y .
4. Man beweise die Vollständigkeit des Kalküls \vdash in $\mathcal{F}\{\rightarrow\}$ mit der Schlussregel MP und den Axiomen $A1, A2$ (Übung 2) und AP: $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$.

Kapitel 2

Prädikatenlogik

In der Mathematik und auch in anderen Wissenschaften wie z.B. der Informatik, hat man häufig mit Individuenbereichen zu tun, in denen gewisse Relationen und Operationen ausgezeichnet sind. Über Eigenschaften solcher Relationen und Funktionen kann man in der Sprache der Aussagenlogik nur teilweise und sehr eingeschränkt reden. Also muss man die sprachlichen Ausdrucksmittel verfeinern um neue Beschreibungsmöglichkeiten zu gewinnen. Dafür sind außer logischen Symbolen auch Variablen für die Individuen des betreffenden Bereichs nötig, sowie Symbole für die in Rede stehenden Relationen und Operationen.

Prädikatenlogik ist der Teil der Logik, der die Eigenschaften solcher Relationen und Operationen einer logischen Analyse unterzieht. Dabei spielen solche sprachlichen Partikel wie „für alle“ und „es gibt ein“ eine zentrale Rolle, auch *Quantoren* genannt. In formalen Sprachen werden diese meistens durch \forall und \exists symbolisiert.

Wir befassen uns vorbereitend etwas näher mit Strukturen und Strukturklassen. Diese sind nicht nur der wesentliche Gegenstand mathematischer Betrachtungen, sondern stehen auch im Blickfeld der Prädikatenlogik, der Modelltheorie, der Informatik, usw. Sodann grenzen wir die wichtigste Klasse formaler Sprachen ein, die *Sprachen der 1. Stufe* oder *elementaren Sprachen*. Charakteristisch für diese ist eine Beschränkung in den Quantifizierungsmöglichkeiten. Wir diskutieren ausführlich die Semantik dieser Sprachen und gelangen zu einem Begriff des Folgerns aus beliebigen Prämissen, der das 2-wertige logische Schließen sehr genau präzisiert. Anschließend behandeln wir den Begriff einer formalisierten Theorie und die Einführung neuer Relationen- und Operationen durch explizite Definitionen. Über formales Beweisen reden wir erst wieder in Kapitel 3.

Nichts in diesem Kapitel ist besonders tiefsinnig. Dennoch sind die Dinge wichtig für die Ausführungen in allen nachfolgenden Kapiteln.

2.1 Mathematische Strukturen

Unter einer *Struktur* \mathcal{A} versteht man eine nichtleere Menge A zusammen mit gewissen ausgezeichneten Relationen und Operationen auf A sowie gewissen ausgezeichneten Konstanten. Die Menge A heißt auch der *Träger* von \mathcal{A} , auch *Trägermenge* oder *Grundmenge*. Die ausgezeichneten Relationen, Operationen und Konstanten heißen kurz die *(Basis-)Relationen, Operationen und Konstanten von \mathcal{A}* . Gelegentlich spricht man auch von einem *Bereich*, z.B. dem Zahlenbereich $(\mathbb{N}, <, +, \cdot, 0, 1)$, der ein Beispiel einer unendlichen Struktur ist. Dabei heißt eine Struktur *endlich* bzw. *unendlich*, je nachdem ob ihre Trägermenge endlich oder unendlich ist.

Für eine Struktur \mathcal{A} soll der korrespondierende Buchstabe A künftig stets den Träger von \mathcal{A} bezeichnen, ohne dass dies extra gesagt wird. Analog bezeichnet B den Träger von \mathcal{B} usw. Falls \mathcal{A} keine Operationen oder Konstanten enthält, heißt \mathcal{A} auch eine *Relationalstruktur*; falls hingegen keine Relationen vorkommen, eine *algebraische Struktur* oder einfach eine *Algebra*. Zum Beispiel ist $(\mathbb{Z}, <)$ eine Relationalstruktur. Hingegen ist $(\mathbb{Z}, +, 0)$ eine algebraische Struktur, die *additive Gruppe* \mathbb{Z} . Auch die Menge \mathcal{F} der aussagenlogischen Formeln aus 1.1 lässt sich als eine Algebra verstehen, ausgestattet mit den Operationen $(\alpha, \beta) \mapsto (\alpha \wedge \beta)$, $(\alpha, \beta) \mapsto (\alpha \vee \beta)$ und $\alpha \mapsto \neg\alpha$. Statt von der Formelmengende spricht man daher auch von der *Formelalgebra* \mathcal{F} .

Ungeachtet des Interesses an speziellen Strukturen betrachtet man oft ganze Klassen von Strukturen, etwa die aller Gruppen oder die Klasse aller Gruppen mit bestimmten Merkmalen. Selbst wenn man zunächst eine einzelne Struktur im Auge hat, nennen wir sie die Vorbildstruktur, ist man oft gezwungen, über gleichartige Strukturen in einem Atemzug, sozusagen in einer Sprache zu sprechen. Das lässt sich dadurch realisieren, dass man von den konkreten Bedeutungen der Relations- und Operationszeichen in der Vorbildstruktur absieht; man betrachtet diese Symbole für sich selbst, um sich damit eine (formale) Sprache zu schaffen, in welcher man über alle in einem Zusammenhang interessierenden Strukturen gleichzeitig zu reden imstande ist. Man schreibt z.B. eine Struktur $\mathcal{A} = (A, +, <, 0)$ dann auch in der Weise $\mathcal{A} = (A, +^{\mathcal{A}}, <^{\mathcal{A}}, 0^{\mathcal{A}})$, wobei $+^{\mathcal{A}}$, $<^{\mathcal{A}}$ und $0^{\mathcal{A}}$ die von den Symbolen $+$, $<$, 0 in \mathcal{A} bezeichnete Relation, Operation bzw. Konstante bedeuten. Dadurch lässt sich von der Struktur \mathcal{A} einerseits und der Symbolmenge $\{+, <, 0\}$ andererseits reden. Eine so entstehende Menge L von Relations-, Operations- und Konstantensymbolen mit jeweils gegebenen Stellzahlen heiße eine nichtlogische *Signatur*.

Für die Klasse aller Gruppen ist z.B. $L = \{\circ, e\}$ eine bevorzugte Signatur, wobei \circ die Gruppenoperation und e das Einselement bezeichnet. Man kann Gruppen aber auch – wie dies weiter unten geschieht – als Strukturen der Signatur $\{\circ\}$ definieren. Natürlich könnte man statt \circ auch \cdot , $*$ oder $+$ als Operationszeichen wählen, und

Letzteres geschieht in der Regel dann, wenn man mit abelschen Gruppen zu tun hat. Auf das konkrete Aussehen eines Symbols aus L kommt es in diesem Sinne wiederum nicht an. Worauf es letztlich ankommt ist dessen Stellenzahl.

$r \in L$ bedeute stets, dass r ein Relationszeichen, und $f \in L$, dass f ein Operationszeichen ist (auch *Funktionszeichen* genannt), jeweils von einer Stellenzahl $n > 0$, die natürlich von r bzw. f abhängt¹⁾. Eine L -Struktur sei ein Paar $\mathcal{A} = (A, L^{\mathcal{A}})$, wobei $L^{\mathcal{A}}$ für jedes $r \in L$ eine Relation $r^{\mathcal{A}}$ auf A mit der Stellenzahl von r enthält, für jedes $f \in L$ eine Operation $f^{\mathcal{A}}$ auf A der Stellenzahl von f , und für jedes $c \in L$ eine Konstante $c^{\mathcal{A}} \in A$. Je nach den Umständen notiert man \mathcal{A} auch abgekürzt; z.B. spricht man oft vom Ring \mathbb{Z} oder vom Körper \mathbb{R} .

Jede Struktur ist L -Struktur für eine gewisse Signatur, nämlich derjenigen bestehend aus den Bezeichnungen ihrer Relationen, Funktionen und Konstanten. Das aber macht den Namen L -Struktur nicht überflüssig, weil wichtige Begriffe wie Isomorphie, Substruktur usw. sich auf Strukturen jeweils gleicher Signatur L beziehen. Von Abschnitt 2.2 an, nachdem die zu L gehörige elementare Sprache \mathcal{L} definiert worden ist, werden L -Strukturen meistens \mathcal{L} -Strukturen genannt.

Ist $A \subseteq B$ und f eine n -stellige Operation auf B , heißt A *abgeschlossen* bzgl. f , kurz *f -abgeschlossen*, wenn mit $\vec{a} \in A^n$ auch $f\vec{a} \in A$. Falls $n = 0$, d.h. falls f eine Konstante c ist, heiße dies einfach $c \in A$. Für ein nichtleeres System f -abgeschlossener Teilmengen von B ist auch dessen Durchschnitt wieder f -abgeschlossen. Demnach kann man von der kleinsten (dem Durchschnitt) aller f -abgeschlossenen Teilmengen von B reden, die eine gegebene Teilmenge $E \subseteq B$ enthalten. Dies alles gilt genauso, wenn f hier durch eine beliebige Familie von Operationen von B ersetzt wird.

Beispiel. Für gegebenes m ist die Menge $m\mathbb{N} := \{m \cdot n \mid n \in \mathbb{N}\}$ der durch m teilbaren natürlichen Zahlen $+$ - und \cdot -abgeschlossen in \mathbb{N} und offenbar die kleinste die Elemente 0 und m enthaltende Teilmenge von \mathbb{N} dieser Art.

Die *Einschränkung* einer n -stelligen Relation $R \subseteq B^n$ auf eine Teilmenge $A \subseteq B$ sei $R \cap A^n$. So ist die Einschränkung der üblichen Ordnung von \mathbb{R} auf \mathbb{N} die übliche Ordnung von \mathbb{N} . Es ist völlig plausibel, dass nur deswegen beide Relationen mit dem gleichen Symbol bezeichnet werden dürfen. Analog definiert man die Einschränkung f^A einer auf B erklärten Operation f auf $A \subseteq B$, vorausgesetzt, A ist f -abgeschlossen. Es sei einfach $f^A \vec{a} = f\vec{a}$ für alle $\vec{a} \in A^n$. So ist die Addition in \mathbb{N} die Einschränkung der Addition in \mathbb{Z} auf \mathbb{N} , oder Letztere ist eine Erweiterung der Ersteren. Wie im Falle von Relationen darf man sich daher erlauben, beide Operationen mit demselben Symbol zu bezeichnen.

¹⁾ In bestimmten Zusammenhängen lässt man auch $n = 0$ zu und sieht Konstanten als 0-stellige Operationen an. 0-stellige Prädikate erscheinen erst in 5.6.

Sei \mathcal{B} eine L -Struktur und $A \subseteq B$ nichtleer und gegenüber allen Operationen von \mathcal{B} abgeschlossen, wobei diese Redeweise grundsätzlich auch $c^{\mathcal{B}} \in A$ für $c \in L$ einschließen soll. Einer derartigen Teilmenge A entspricht in natürlicher Weise eine L -Struktur $\mathcal{A} = (A, L^{\mathcal{A}})$; dabei seien $r^{\mathcal{A}}$ und $f^{\mathcal{A}}$ für $r \in L$ und $f \in L$ die Einschränkungen von $r^{\mathcal{B}}$ bzw. $f^{\mathcal{B}}$ auf A . Schließlich sei $c^{\mathcal{A}} = c^{\mathcal{B}}$ für $c \in L$. Die so definierte Struktur \mathcal{A} heißt dann eine *Substruktur* von \mathcal{B} , und \mathcal{B} heißt eine *Erweiterung* von \mathcal{A} , in Zeichen $\mathcal{A} \subseteq \mathcal{B}$. So ist z.B. $\mathcal{A} = (\mathbb{N}, <, +, 0)$ Substruktur von $\mathcal{B} = (\mathbb{Z}, <, +, 0)$, weil $0 \in \mathbb{N}$ und \mathbb{N} unter der Addition von \mathbb{Z} abgeschlossen ist. Hier wurden die oberen Indizes bei $<$, $+$ und 0 weggelassen, denn dies kann zu Missverständnissen nicht führen.

Jede nichtleere Teilmenge E des Trägers einer L -Struktur \mathcal{B} definiert eine kleinste E enthaltende Substruktur \mathcal{A} von \mathcal{B} , deren Träger A die kleinste E enthaltende, unter allen Operationen von \mathcal{B} abgeschlossene Teilmenge von B ist. \mathcal{A} heißt *die von E in \mathcal{B} erzeugte Substruktur*. So ist $3\mathbb{N} (= \{3n \mid n \in \mathbb{N}\})$ der Träger der von $E = \{3\}$ in $(\mathbb{Z}, +, 0)$ erzeugten Substruktur. Denn $3\mathbb{N}$ enthält 0 und 3 , ist abgeschlossen unter $+$, und offenbar die kleinste Teilmenge von \mathbb{N} dieser Art. \mathcal{A} heißt *endlich erzeugt*, wenn für ein endliches $E \subseteq A$ die von E in \mathcal{A} erzeugte Substruktur mit \mathcal{A} identisch ist.

Ist \mathcal{A} eine L -Struktur und $L_0 \subseteq L$, so heißt die L_0 -Struktur \mathcal{A}_0 mit dem Träger A und mit $\zeta^{\mathcal{A}_0} = \zeta^{\mathcal{A}}$ für alle Zeichen $\zeta \in L_0$ das *L_0 -Redukt von \mathcal{A}* , und \mathcal{A} heißt eine *L -Expansion von \mathcal{A}_0* . So ist die Gruppe $(\mathbb{Z}, +, 0)$ das $\{+, 0\}$ -Redukt des geordneten Ringes $(\mathbb{Z}, <, +, \cdot, 0)$. Die Begriffe Redukt und Substruktur müssen klar voneinander unterschieden werden. Ein Redukt von \mathcal{A} hat stets denselben Träger wie \mathcal{A} .

Es folgt eine Liste häufig zitierter Eigenschaften einer 2-stelligen Relation R in einer Menge A . Statt $(a, b) \in R$ schreiben wir etwas bequemer $a \triangleleft b$, und $a \not\triangleleft b$ meint $(a, b) \notin R$. Auch steht $a \triangleleft b \triangleleft c$ für $a \triangleleft b$ & $b \triangleleft c$, so wie man meist $a < b < c$ für $a < b$ & $b < c$ schreibt. In der Liste bedeuten „für alle a “ und „es gibt ein a “ genauer „für alle $a \in A$ “ bzw. „es gibt ein $a \in A$ “. Die Relation $\triangleleft (\subseteq A^2)$ heißt

<i>reflexiv</i>	wenn $a \triangleleft a$ für alle a .
<i>irreflexiv</i>	wenn $a \not\triangleleft a$ für alle a .
<i>symmetrisch</i>	wenn $a \triangleleft b \Rightarrow b \triangleleft a$, für alle a, b .
<i>antisymmetrisch</i>	wenn $a \triangleleft b \triangleleft a \Rightarrow a = b$, für alle a, b .
<i>transitiv</i>	wenn $a \triangleleft b \triangleleft c \Rightarrow a \triangleleft c$, für alle a, b, c .
<i>konnex</i>	wenn $a \triangleleft b$ oder $b \triangleleft a$ oder $a = b$, für alle a, b .

Reflexive, transitive und symmetrische Relationen heißen *Äquivalenzrelationen*. Man bezeichnet diese häufig mit \sim , \approx , \equiv , \simeq oder ähnlichen Symbolen. Es folgt nun eine Übersicht über Strukturklassen, auf die erst später zurückgegriffen wird. Man kann die Lektüre daher vorerst auch mit **2.2** fortsetzen.

1. Graphen, Halbordnungen und Ordnungen. Eine Relationalstruktur (A, \triangleleft) mit einer beliebigen 2-stelligen Relation \triangleleft auf A heißt oft ein (gerichteter) *Graph*. Ist \triangleleft irreflexiv und transitiv, schreibt man meistens $<$ für \triangleleft und spricht von einer *halbgeordneten Menge* oder (*irreflexiven*) *Halbordnung*, auch *partielle Ordnung* (im strikten Sinne) genannt. Definiert man von $<$ ausgehend $x \leq y \Leftrightarrow x < y \text{ oder } x = y$, so ist \leq reflexiv, transitiv und antisymmetrisch. (A, \leq) heißt die zugehörige *reflexive Halbordnung*. Man kann auch mit einer reflexiven Halbordnung (A, \leq) starten, und erhält durch die Erklärung $x < y \Leftrightarrow x \leq y \text{ \& } x \neq y$ eine irreflexive Halbordnung.

Eine konnexe Halbordnung $\mathcal{A} = (A, <)$ heißt eine *lineare* oder *totale Ordnung*, oft auch nur eine *Ordnung* oder *Anordnung* oder *geordnete Menge*. \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} sind bzgl. ihrer üblichen Anordnung Beispiele. Hier und weiter unten folgen wir der Gewohnheit, geordnete oder halbgeordnete Mengen einfach durch ihre Träger aufzurufen, wenn klar ist, welche Ordnungsrelation gemeint ist.

Eine Teilmenge U einer geordneten Menge A heißt ein *Anfang* von A , wenn $A \neq \emptyset$ und für alle $a, b \in A$ mit $a < b$ und $b \in U$ stets auch $a \in U$. Hat $U \neq A$ kein größtes und $V := A \setminus U$ kein kleinstes Element, sagt man, das Paar (U, V) sei eine *Lücke*. Hat hingegen U ein größtes Element a und V ein kleinstes Element b , heißt (U, V) ein *Sprung*. Es gibt dann kein $c \in A$ mit $a < c < b$. Deshalb heißt dann b auch ein *unmittelbarer Nachfolger* von a , und a ein *unmittelbarer Vorgänger* von b . Eine unendliche geordnete Menge ohne Lücken und Sprünge heißt *stetig geordnet*. Standardbeispiele sind \mathbb{R} und die Intervalle von \mathbb{R} .

Eine geordnete Teilmenge K einer halbgeordneten Menge H heißt eine *Kette* von H . Diese heißt *nach oben beschränkt*, wenn es ein $b \in H$ gibt mit $x \leq b$ für alle $x \in K$. Man nennt $a \in H$ *maximal* in H , wenn es kein $b \in H$ gibt mit $b > a$. Eine unendliche Halbordnung muss keine maximalen Elemente enthalten und Ketten sind auch nicht immer nach oben beschränkt, wie das Beispiel $(\mathbb{N}, <)$ zeigt. Wir formulieren nun ein wichtiges Hilfsmittel der Mathematik, das

Lemma von Zorn. *Ist jede Kette in einer nichtleeren halbgeordneten Menge H nach oben beschränkt, so besitzt H ein maximales Element.*

Dieses Lemma gehört zu denjenigen Hilfsmitteln, die auch ohne Beweiskennntnis leicht anwendbar sind. Mit einem indirektem Beweisansatz ist es auch einigermaßen plausibel: Hat H kein maximales Element, wähle man ein $a_0 \in H$, dann ein $a_1 > a_0$ usw. Der exakte Beweis beruht auf dem in 3.4 diskutierten Auswahlaxiom.

Eine geordnete Menge A heißt *wohlgeordnet*, wenn jede nichtleere Teilmenge von A ein kleinstes Element hat. Gleichwertig, es gibt keine unendliche absteigende Folge $a_0 > a_1 > \dots$ mit $a_i \in A$. Denn gäbe es eine solche, dann hätte $\{a_n \mid n \in \mathbb{N}\}$ ja kein kleinstes Element. Beispiel einer unendlichen wohlgeordneten Menge ist \mathbb{N} .

2. Gruppoide, Halbgruppen und Gruppen. Algebren $\mathcal{A} = (A, \circ)$ mit einer beliebigen Operation $\circ: A^2 \rightarrow A$ heißen *Gruppoide*. Ist \circ assoziativ, heißt \mathcal{A} eine *Halbgruppe*, ist \circ zudem invertierbar, eine *Gruppe*. Es ist beweisbar, dass eine Gruppe (G, \circ) in diesem Sinne genau ein *Einselement* (oder *neutrales Element*) enthält, d.h. ein Element e mit $x \circ e = e \circ x = x$ für alle $x \in G$. Ist \circ auch kommutativ, spricht man von einer *kommutativen* oder *abelschen* Gruppe, auch *Modul* genannt.

Hier einige Beispiele für Halbgruppen, die keine Gruppen sind: (a) die Menge der Zeichenfolgen aus den Buchstaben eines Alphabets A bezüglich Verkettung, *die von (den Buchstaben aus) A erzeugte Worthalbgruppe*. (b) $(\mathbb{N}, +)$ und (\mathbb{N}, \cdot) ; beide sind *kommutativ*. Alle angegebenen Beispiele von Halbgruppen sind *regulär*, d.h. es gelten $x \circ y = x \circ z \Rightarrow y = z$ und $x \circ z = y \circ z \Rightarrow x = y$, für alle x, y, z .

Substrukturen von Halbgruppen sind wieder Halbgruppen. Auch Substrukturen von Gruppen sind im Allgemeinen nur Halbgruppen. So ist z.B. $(\mathbb{N}, +) \subseteq (\mathbb{Z}, +)$. Erst in der Signatur $\{\circ, e, {}^{-1}\}$, wobei e das Einselement und x^{-1} das zu x inverse Element bezeichnet, sind Substrukturen von Gruppen wieder Gruppen. In dieser Signatur lassen sich die Gruppenaxiome sogar wie folgt als Gleichungen notieren, wobei Zusätze wie ‘für alle x, y, z ’ der Kürze halber unterdrückt werden:

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

Diese bewahren offenbar ihre Gültigkeit beim Übergang zu Substrukturen. Aus den angegebenen sind die Gleichungen $e \circ x = x$ und $x^{-1} \circ x = e$ beweisbar, siehe **2.3**.

Geordnete Halbgruppen oder Gruppen enthalten nebst \circ noch eine Anordnung, bezüglich derer \circ in beiden Argumenten monoton ist. Eine kommutative geordnete Halbgruppe $(A, <, +, 0)$ mit Nullelement 0 , das zugleich kleinstes Element in A ist, und in der im Falle $a < b$ ein c mit $a + c = b$ existiert, heißt ein *Größenbereich*. Alltagsbeispiele sind die Größenbereiche der *Längen*, *Volumina*, *Massen* usw.

3. Ringe und Körper. Diese gehören zu den bekanntesten Strukturen, so dass wir die Definition hier nicht wiederholen. Die Ringaxiome seien in $+, -, \cdot, 0$ formuliert und enthalten das Axiom $x + (y - x) = y$; bei Körpern kommt noch das Symbol 1 hinzu. Streicht man aus den Ringaxiomen das zuletzt erwähnte Axiom und das Minus-Symbol aus der Signatur, spricht man von einem *Halbring*.

Substrukturen von Körpern in der Signatur $\{0, 1, +, -, \cdot\}$ sind *Integritätsbereiche*, d.h. kommutative nullteilerfreie Ringe mit 1 . Sind $\mathcal{K}, \mathcal{K}'$ Körper mit $\mathcal{K} \subseteq \mathcal{K}'$, so heißt $a \in \mathcal{K}' \setminus \mathcal{K}$ *algebraisch* oder *transzendent* über \mathcal{K} , je nachdem ob a Nullstelle eines Polynoms mit Koeffizienten aus \mathcal{K} ist oder nicht. Zerfällt wie im Körper der komplexen Zahlen jedes Polynom vom Grade ≥ 1 mit Koeffizienten aus \mathcal{K} schon in Linearfaktoren, heißt \mathcal{K} a.a. (= *algebraisch abgeschlossen*).

Jeder Körper \mathcal{K} hat einen kleinsten Teilkörper \mathcal{P} , einen *Primkörper*. Man sagt, \mathcal{K} hat die *Charakteristik* 0 bzw. die *Charakteristik* p (eine Primzahl), je nachdem ob \mathcal{P} zum Körper \mathbb{Q} oder zum Körper \mathcal{F}_p aus p Elementen isomorph ist. Andere Primkörper gibt es nicht. \mathcal{K} hat die Charakteristik p genau dann, wenn in \mathcal{K} die Aussage $\text{char}_p : \underbrace{1 + \dots + 1}_p = 0$ gilt.

Halbringe, Ringe und Körper können auch *geordnet* sein, wobei die üblichen Monotoniegesetze gefordert werden. So ist $(\mathbb{Z}, <, +, \cdot, 0, 1)$ der *geordnete Ring* der ganzen Zahlen, und $(\mathbb{N}, <, +, \cdot, 0, 1)$ der *geordnete Halbring* der natürlichen Zahlen.

4. Halbverbände und Verbände. $\mathcal{A} = (A, \circ)$ heißt ein *Halbverband*, wenn \circ assoziativ, kommutativ und idempotent ist. Ein Beispiel ist $(\{0, 1\}, \circ)$ mit $\circ = \wedge$ oder auch $\circ = \vee$. Definiert man $a \leq b \Leftrightarrow a \circ b = a$, so ist \leq eine reflexive Halbordnung auf A . Wie man leicht nachrechnet, ist $a \circ b$ gerade das *Infimum* von a, b bezüglich \leq , kurz $a \circ b = \inf\{a, b\}$, was heißen soll $a \circ b \leq a, b$ und $c \leq a, b \Rightarrow c \leq a \circ b$, für alle $a, b, c \in A$. So ist z.B. \leq wegen $a \circ a = a$ reflexiv.

$\mathcal{A} = (A, \cap, \cup)$ heißt ein *Verband*, wenn (A, \cap) und (A, \cup) jeweils Halbverbände sind und wenn in \mathcal{A} die sogenannten *Absorptionsgesetze* $a \cap (a \cup b) = a$ und $a \cup (a \cap b) = a$ gelten. Diese implizieren $a \cap b = a \Leftrightarrow a \cup b = b$, so dass A halbgeordnet wird, indem man wahlweise definiert $a \leq b \Leftrightarrow a \cap b = a$ oder $a \leq b \Leftrightarrow a \cup b = b$. Dabei erweist $a \cup b$ sich als *Supremum* von a, b , d.h. $a, b \leq a \cup b$ und $a, b \leq c \Rightarrow a \cup b \leq c$, für alle $a, b, c \in A$. Falls \mathcal{A} darüber hinaus auch die *Distributivgesetze*

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \quad ; \quad a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$$

erfüllt, heißt \mathcal{A} ein *distributiver Verband*. So ist z.B. $\mathfrak{P}M$ mit den Operationen \cap und \cup für \cap bzw. \cup ein distributiver Verband, ebenso jede nichtleere, gegenüber \cap und \cup abgeschlossene Familie von Teilmengen von M . Diese heißen *Mengenverbände*. Ein wichtiges Beispiel ist auch $(\mathbb{N}, \text{ggT}, \text{kgV})$. Dabei sei $\text{ggT}(a, b)$ bzw. $\text{kgV}(a, b)$ der größte gemeinsame Teiler bzw. das kleinste gemeinsame Vielfache von $a, b \in \mathbb{N}$. Die zugehörige Halbordnung ist hier die Teilbarkeitsrelation. Das kleinste gemeinsame Vielfache ist auch für endliche Folgen natürlicher Zahlen wohlerklärt, was in 7.1 eine wichtige Rolle spielen wird.

5. Boolesche Algebren. Eine Algebra $\mathcal{A} = (A, \cap, \cup, \neg)$, so dass (A, \cap, \cup) ein distributiver Verband ist, und in der mindestens noch die Gleichungen

$$\neg \neg x = x, \quad \neg(x \cap y) = \neg x \cup \neg y, \quad x \cap \neg x = y \cap \neg y$$

gelten, heißt eine *Boolesche Algebra*. Vorbildstruktur ist die 2-elementige Boolesche Algebra $\mathcal{2} := (\{0, 1\}, \cap, \cup, \neg)$; dabei sei \cap durch \wedge und \cup durch \vee interpretiert. Man definiert $0 := a \cap \neg a$ für beliebiges $a \in A$, und $1 := \neg 0$. Es gibt viele Kennzeichnungen Boolescher Algebren. Auch die Signatur wird oft unterschiedlich gewählt.

So ist die Signatur $\{\wedge, \vee, \neg\}$ sehr geeignet, um die 2-wertige Aussagenlogik algebraisch zu behandeln. Weitere Beispiele Boolescher Algebren sind die *Mengenalgebren* $\mathcal{A} = (A, \cap, \cup, \neg)$, bestehend aus einem System $A \neq \emptyset$ von Teilmengen einer Menge I , das unter \cap, \cup und \neg (Komplement in A) abgeschlossen ist. Dies sind bereits die allgemeinsten Beispiele; denn jede Boolesche Algebra ist nach dem *Stoneschen Repräsentationssatz* zu einer Mengenalgebra isomorph.

6. Logische L -Matrizen. Dies sind Strukturen $\mathcal{A} = (A, L^{\mathcal{A}}, D^{\mathcal{A}})$, wobei L nur Operationssymbole (die „logischen“ Symbole) enthält und D ein einstelliges Prädikat bezeichnet: *die Menge der ausgezeichneten Werte* von \mathcal{A} . Am bekanntesten ist die zweiwertige *Boolesche Matrix* $\mathcal{B} = (\{0, 1\}, L^{\mathcal{B}}, \{1\})$, mit $L = \{\wedge, \vee, \neg\}$. Die durch \mathcal{A} bestimmte Folgerungsrelation $\models_{\mathcal{A}}$ in der aussagenlogischen Sprache \mathcal{F} der Signatur L wird analog zum 2-wertigen Fall definiert: Für $X \subseteq \mathcal{F}$ und $\alpha \in \mathcal{F}$ sei $X \models_{\mathcal{A}} \alpha$, wenn $w\alpha \in D^{\mathcal{A}}$ für jede Belegung $w: AV \mapsto A$ mit $w\varphi \in D^{\mathcal{A}}$ für alle $\varphi \in X$.

Homomorphismen und Isomorphismen. Die folgenden Begriffe sind für mathematische und logisch-semantische Untersuchungen gleichermaßen wichtig.

Definition. Seien \mathcal{A}, \mathcal{B} L -Strukturen und $h: \mathcal{A} \rightarrow \mathcal{B}$ (genauer $h: A \rightarrow B$) eine Abbildung, so dass für alle $r, f, c \in L$ und $\vec{a} \in A^n$ (n Stellenzahl von f bzw. r)

$$(H) \quad hf^{\mathcal{A}}\vec{a} = f^{\mathcal{B}}h\vec{a}, \quad hc^{\mathcal{A}} = c^{\mathcal{B}}, \quad r^{\mathcal{A}}\vec{a} \Rightarrow r^{\mathcal{B}}h\vec{a} \quad (h\vec{a} = (ha_1, \dots, ha_n)).$$

Dann heie h ein *Homomorphismus*. Fgt man zu (H) noch die Bedingung

$$(S) \quad r^{\mathcal{B}}h\vec{a} \Rightarrow (\exists \vec{b} \in A^n)(h\vec{a} = h\vec{b} \ \& \ r^{\mathcal{A}}\vec{b})^2)$$

hinzu, heit h ein *strenger Homomorphismus* (bei Algebren ist dieser Begriff entbehrlich). Ein injektiver strenger Homomorphismus h heit eine *Einbettung* (*Monomorphismus*). Ist h berdies bijektiv, heit h ein *Isomorphismus* und im Falle $\mathcal{A} = \mathcal{B}$ ein *Automorphismus*. \mathcal{A} und \mathcal{B} werden *isomorph* genannt, symbolisch $\mathcal{A} \simeq \mathcal{B}$, falls ein solcher Isomorphismus existiert. \simeq ist reflexiv, symmetrisch und transitiv.

Sehr wichtig ist die quivalenz $r^{\mathcal{A}}\vec{a} \Leftrightarrow r^{\mathcal{B}}h\vec{a}$ fr einen Isomorphismus oder eine Einbettung $h: \mathcal{A} \rightarrow \mathcal{B}$. Denn wegen $h\vec{a} = h\vec{b} \Leftrightarrow \vec{a} = \vec{b}$ gilt nach (S) auch die Umkehrung der Implikation unter (H): $r^{\mathcal{B}}h\vec{a} \Rightarrow (\exists \vec{b} \in A^n)(\vec{a} = \vec{b} \ \& \ r^{\mathcal{A}}\vec{b}) \Rightarrow r^{\mathcal{A}}\vec{a}$.

Beispiele. (a) Die in 1.1 betrachteten Abbildungen w der aussagenlogischen Formelalgebra \mathcal{F} in die 2-elementige Boolesche Algebra $\mathcal{2}$ sind Homomorphismen.

(b) Sei $\mathcal{A} = (A, *)$ eine Worthalbgruppe mit der Verkettungsoperation $*$ und \mathcal{B} die additive Halbgruppe der natrlichen Zahlen. Dies sind L -Strukturen fr $L = \{\circ\}$, mit $\circ^{\mathcal{A}} = *$ und $\circ^{\mathcal{B}} = +$. Sei $lh\ a$ die Lnge eines Wortes $a \in A$. Dann ist $a \mapsto lh(a)$

²⁾ $(\exists \vec{b} \in A^n)(h\vec{a} = h\vec{b} \ \& \ r^{\mathcal{A}}\vec{b})$ bedeutet ‘es gibt ein $\vec{b} \in A^n$ mit $h\vec{a} = h\vec{b}$ und $r^{\mathcal{A}}\vec{b}$ ’.

ein Homomorphismus von \mathcal{A} auf \mathcal{B} , weil $lh(a * b) = lh a + lh b$. Ist \mathcal{A} aus nur einem Buchstaben erzeugt, so ist h offenbar bijektiv und damit ein Isomorphismus.

(c) Die Algebren $\mathcal{A} = (\{0, 1\}, +)$ und $\mathcal{B} = (\{0, 1\}, \leftrightarrow)$ sind nur äußerlich verschieden; sie sind in Wahrheit isomorph, vermittelt des Isomorphismus δ mit $\delta 0 = 1$, $\delta 1 = 0$. Mit \mathcal{A} ist daher auch \mathcal{B} eine Gruppe (siehe die allgemeinen Ausführungen in 2.3). \mathcal{A} und \mathcal{B} werden durch Hinzufügen des einstelligen Prädikats $D = \{1\}$ zu logischen Matrizen. Diese sind nicht mehr isomorph und definieren die beiden „dualen“ fragmentaren 2-wertigen Logiken für die Aussagenverknüpfungen *entweder ... oder ...* und *... genau dann wenn ...*, die viele gemeinsame Eigenschaften haben.

(d) Es sei \mathcal{A} die geordnete additive Gruppe aller reellen Zahlen und \mathcal{B} die geordnete multiplikative Gruppe der positiven reellen Zahlen. Dann gibt es zu jedem $b > 0$ mit $b \neq 1$ genau einen Isomorphismus $\eta: \mathcal{A} \rightarrow \mathcal{B}$ derart, dass $\eta 1 = b$, nämlich $\eta: x \mapsto b^x$, die Exponentialfunktion \exp_b zur Basis b , mit der Umkehrfunktion \log_b . Diese Tatsache erklärt das logarithmische Rechnen in vollkommener Weise.

(e) $x \mapsto -x$ ist ein Automorphismus der Gruppe $(\mathbb{R}, 0, +)$. Dagegen besitzt der Körper $(\mathbb{R}, 0, 1, +, \cdot)$ keine echten, d.h. von $id_{\mathbb{R}}$ verschiedenen Automorphismen. Die Abbildung $a \mapsto (a, 0)$ von \mathbb{R} nach \mathbb{C} (= Körper der komplexen Zahlen, dessen Träger wie üblich verstanden sei als Menge der geordnete Paare reeller Zahlen) ist typisches Beispiel einer Einbettung. Es handelt sich hier um eine Einbettung des Körpers \mathbb{R} in den Körper \mathbb{C} .

Kongruenzen. Von größter Bedeutung in der Algebra, Logik und anderswo ist der Begriff der *Kongruenzrelation* oder kurz *Kongruenz* in einer Algebra \mathcal{A} der Signatur L . Darunter versteht man eine Äquivalenzrelation \approx in A derart, dass für alle $f \in L$

$$\vec{a} \approx \vec{b} \Rightarrow f\vec{a} \approx f\vec{b}, \quad (\vec{a} \approx \vec{b} \text{ bedeute } a_i \approx b_i \text{ für } i = 1, \dots, n).$$

Sei A' die Menge aller Äquivalenzklassen $a/\approx := \{x \in A \mid a \approx x\}$, zuweilen auch *Kongruenzklassen* genannt. Dabei gilt $a \approx b \Leftrightarrow a/\approx = b/\approx$, für alle $a, b \in A$. Für \vec{a} aus A^n sei $\vec{a}/\approx := (a_1/\approx, \dots, a_n/\approx)$. Wichtige und leicht beweisbaren Fakten sind (a) A' wird durch die Definition $f(\vec{a}/\approx) := (f\vec{a})/\approx$ ³⁾ zu einer L -Struktur \mathcal{A}' , die auch mit \mathcal{A}/\approx bezeichnete *Faktorstruktur* von \mathcal{A} nach \approx . (b) Die Abbildung $a \mapsto a/\approx$ ist ein Homomorphismus von \mathcal{A} auf \mathcal{A}' , der sogenannte *natürliche Homomorphismus*. (c) Jeder Homomorphismus $h: \mathcal{A} \rightarrow \mathcal{B}$ definiert gemäß $a \approx_h b :\Leftrightarrow ha = hb$ eine Kongruenz in \mathcal{A} , deren Faktorstruktur zum Bild von h isomorph ist. Kongruenzen lassen sich nicht nur für Algebren, sondern auch für beliebige Strukturen so erklären, dass Eigenschaften gelten, die analog sind zu (a), (b) und (c), siehe z.B. [Ra2].

³⁾Diese Definition ist korrekt oder *repräsentantenunabhängig*, d.h. $\vec{a} \approx \vec{b} \Rightarrow f\vec{a} \approx f\vec{b}$, oder gleichwertig, $\vec{a}/\approx = \vec{b}/\approx \Rightarrow f(\vec{a}/\approx) = f(\vec{b}/\approx)$, für alle $\vec{a}, \vec{b} \in A^n$ und alle $f \in L$ der Stellenzahl n .

Direkte Produkte. Diese sind die Basis für viele Konstruktionsverfahren von Strukturen. Bekanntes Beispiel ist die n -dimensionale Vektorgruppe $(\mathbb{R}^n, 0, +)$, das n -fache direkte Produkt der Gruppe $(\mathbb{R}, 0, +)$ mit sich selbst. Die Addition in \mathbb{R}^n wird komponentenweise erklärt, und entsprechendes geschieht auch in der folgenden

Definition. Sei $(\mathcal{A}_i)_{i \in I}$ eine nichtleere Familie von L -Strukturen. Das *direkte Produkt* $\mathcal{B} = \prod_{i \in I} \mathcal{A}_i$ sei die wie folgt definierte Struktur. Der Träger sei $B = \prod_{i \in I} A_i$ mit den Elementen $a = (a_i)_{i \in I}$ (siehe die Notationen), und für $r, f, c \in L$ setzt man

$$r^{\mathcal{B}} \vec{a} \Leftrightarrow r^{\mathcal{A}_i} \vec{a}_i \text{ für alle } i \in I, \quad f^{\mathcal{B}} \vec{a} = (f^{\mathcal{A}_i} \vec{a}_i)_{i \in I}, \quad c^{\mathcal{B}} = (c^{\mathcal{A}_i})_{i \in I}.$$

Dabei ist $\vec{a} = (a^1, \dots, a^n) \in B^n$ – hier zählen ausnahmsweise die oberen Indizes die Komponenten des n -Tupels – sowie $\vec{a}_i = (a_i^1, \dots, a_i^n) \in A_i^n$ (die i -te Projektion des n -Tupels \vec{a}) und $a^\nu = (a_i^\nu)_{i \in I}$ für $\nu = 1, \dots, n$. Im Falle $\mathcal{A}_i = \mathcal{A}$ für alle $i \in I$ wird $\prod_{i \in I} \mathcal{A}_i$ auch mit \mathcal{A}^I bezeichnet und heißt eine *direkte Potenz* von \mathcal{A} .

Für $I = \{1, \dots, m\}$ bezeichnet man $\prod_{i \in I} \mathcal{A}_i$ häufig mit $\mathcal{A}_1 \times \dots \times \mathcal{A}_m$. Im Falle $I = \{0, \dots, n-1\}$ schreibt man meistens \mathcal{A}^n für \mathcal{A}^I . Durch $a \mapsto (a)_{i \in I}$ (das I -Tupel mit dem konstanten Wert a) wird \mathcal{A} in \mathcal{A}^I eingebettet.

Beispiele. (a) Für $I = \{1, 2\}$ und $\mathcal{A}_i = (A_i, <^i)$ ist $a <^{\mathcal{B}} b \Leftrightarrow a_1 <^1 b_1 \ \& \ a_2 <^2 b_2$ für alle $a, b \in B = A_1 \times A_2$. Sind $\mathcal{A}_1, \mathcal{A}_2$ Ordnungen, so ist \mathcal{B} i.a. nur noch eine partielle Ordnung. Der tiefere Grund hierfür wird sich in 5.7 offenbaren.

(b) Sei $\mathcal{B} = 2^I$ eine direkte Potenz der 2-elementigen Booleschen Algebra 2 . Die Elemente von B sind I -Tupel aus Nullen und Einsen. Diese entsprechen in natürlicher Weise umkehrbar eindeutig den Teilmengen von I . Siehe hierzu Übung 4.

Übungen

1. Man zeige, es gibt bis auf Isomorphie genau fünf 2-elementige echte Gruppoide. Dabei heiße ein mindestens 2-elementiges Gruppoid (H, \cdot) *echt*, wenn \cdot eine wesentlich 2-stellige Operation ist.
2. Die Relation $\approx (\subseteq A^2)$ heißt *euklidisch*, wenn $a \approx b \ \& \ a \approx c \Rightarrow b \approx c$, für alle $a, b, c \in A$. Man zeige, \approx ist dann und nur dann eine Äquivalenzrelation in A , wenn \approx reflexiv und euklidisch ist.
3. Man zeige, eine Äquivalenzrelation \approx auf einer algebraischen L -Struktur \mathcal{A} ist schon dann eine Kongruenz, wenn für alle $f \in L$ und alle $i = 1, \dots, n$

$$a \approx a' \Rightarrow f(a_1, \dots, a_{i-1}, a, a_{i+1}, \dots, a_n) \approx f(a_1, \dots, a_{i-1}, a', a_{i+1}, \dots, a_n).$$
4. Man zeige, 2^I ist für eine beliebige Indexmenge I isomorph zur Mengenalgebra $(\mathfrak{P}I, \cap, \cup, \neg)$.

2.2 Syntax elementarer Sprachen

Über Strukturen wie z.B. den Körper der reellen Zahlen kann man in der mathematischen Umgangssprache präzise reden. Es kommt bei logischen (und metamathematischen) Fragestellungen aber darauf an, den sprachlichen Rahmen genau abzugrenzen, den man ins Auge fassen will, und dies gelingt am einfachsten durch eine Formalisierung. Man erhält auf diese Weise eine *Objektsprache*, d.h. die formalisierten Sprachelemente werden wie die Elemente einer Struktur zu *Objekten* der Betrachtung. Damit interessante Eigenschaften einer Struktur in dieser Sprache auch formulierbar sind, benötigt man mindestens Variablen für die Elemente ihres Trägers, auch *Individuenvariable* genannt, eine ausreichende Anzahl logischer Symbole, sowie Symbole für die Relationen, Funktionen und Konstanten der Struktur, die insgesamt die nichtlogische Signatur L der zu definierenden Sprache bilden.

Auf diese Weise gelangt man zu den *Sprachen der 1. Stufe*, auch *elementare Sprachen* genannt. Man verliert nichts an Allgemeinheit, wenn die Variablenmenge für alle elementaren Sprachen dieselbe ist, mit Var bezeichnet wird und aus den abzählbar vielen Symbolen v_0, v_1, \dots besteht. Zwei derartige Sprachen unterscheiden sich daher nur durch unterschiedliche Möglichkeiten der Vorgabe nichtlogischer Symbole. Variablen etwa für Teilmengen des Trägers werden bewusst ausgeschlossen. Denn Sprachen, die gleichzeitig Variablen für Individuen und für Mengen aus diesen Individuen enthalten – Sprachen der 2. Stufe, siehe 3.7 – haben andere semantische Eigenschaften als die hier untersuchten elementaren Sprachen.

Wir bestimmen zuerst das *Alphabet*, d.h. die Menge der *Grundzeichen* einer durch eine Signatur L bestimmten Sprache der 1. Stufe. Dazu gehören stets die Variablen v_0, v_1, \dots , die vorzugsweise mit x, y, z, u, v bezeichnet werden. Im konkreten Fall können aber auch andere Buchstaben mit oder ohne Indizes denselben Dienst tun. Der Fettdruck der Originalvariablen ist nützlich, um bei der Niederschrift einer Formel mit n Variablen v_{i_1}, \dots, v_{i_n} diese in gewünschter Reihenfolge z.B. durch v_1, \dots, v_n oder x_1, \dots, x_n vertreten zu lassen. Zum Alphabet mögen ferner die logischen Symbole \wedge, \neg, \forall (für *alle*) und $=$ ⁴⁾, die Klammern $(,)$, sowie die Symbole der Signatur L gehören. Weitere logische Symbole werden später definiert, darunter \exists (*es gibt ein*) und $\exists!$ (*es gibt genau ein*). \mathcal{S}_L bezeichne die Menge aller Zeichenfolgen aus den Grundsymbolen von \mathcal{L} .

Aus der Menge \mathcal{S}_L aller Zeichenfolgen werden die sinnvollen Zeichenfolgen nach gewissen Regeln ausgesondert. Wir beginnen mit den Termen.

⁴⁾Das fettgedruckte Gleichheitszeichen soll die Identitätsrelation in der formalen Sprache bezeichnen; nimmt man einfach das übliche Gleichheitszeichen $=$, könnte es zu unbeabsichtigten Verwechslungen mit einem metasprachlichen Gebrauch dieses Symbols kommen.

Terme in L . (T1) Variablen und Konstanten sind Terme, sogenannte *Primterme*.
 (T2) Ist $f \in L$ und sind t_1, \dots, t_n Terme, so ist auch $ft_1 \cdots t_n$ ein Term.

Dabei ist n wie auf Seite 35 verabredet die Stellenzahl des Operationssymbols f . Andere als die nach (T1) und (T2) erzeugten Zeichenfolgen seien in diesem Zusammenhang keine Terme. Die klammerfreie Schreibweise vereinfacht die Syntax. Bei zweistelligen Operationen verfährt man in der Praxis meist anders und schreibt z.B. den klammerfreien Term $\cdot + xyz$ als $(x + y) \cdot z$. Informationsverdichtung in den Schreibweisen erschwert nämlich das Lesen, weil unser Gehirn Informationen nicht sequentiell verarbeitet wie ein Computer, den das „Entklammern“ der Terme nur zusätzliche Rechenzeit kostet. Übung 3 bestätigt die bei klammerfreier Schreibweise durchaus nicht auf der Hand liegende *eindeutige Termrekonstruktion*:

Aus $ft_1 \cdots t_n = gs_1 \cdots s_m$ folgt $g = f$, $m = n$ und $s_i = t_i$ für $i = 1, \dots, n$.

\mathcal{T} ($= \mathcal{T}_L$) bezeichne die Menge aller Terme gegebener Signatur L . Variablenfreie Terme, die es nur bei Vorhandensein wenigstens einer Konstanten gibt, heißen auch *Grundterme*. Terme, die keine Primterme sind, heißen *Funktionsterme*. \mathcal{T} bildet mit den durch $f^{\mathcal{T}}(t_1, \dots, t_n) = ft_1 \cdots t_n$ auf ganz \mathcal{T} erklärten Operationen eine Algebra, die z.B. für 4.1 wichtige *Termalgebra*. Die Definition des Termbegriffs ergibt ferner leicht ein auf eine beliebige Signatur bezogenes nützliches

Beweisprinzip durch Terminduktion. Sei \mathcal{E} eine Eigenschaft der $\xi \in \mathcal{S}_{\mathcal{L}}$, die auf alle Primterme zutrifft, und gelte $\mathcal{E}t_1, \dots, \mathcal{E}t_n \Rightarrow \mathcal{E}ft_1 \cdots t_n$, für jedes $f \in L$ der Stellenzahl n und alle $t_1, \dots, t_n \in \mathcal{T}$. Dann haben alle Terme die Eigenschaft \mathcal{E} .

\mathcal{T} ist nämlich nach Definition die kleinste Menge von Zeichenfolgen, welche die im Beweisprinzip genannten Voraussetzungen erfüllt. Analog steht uns ein *Definitionsprinzip durch Termrekursion* zur Verfügung, das wir nicht allgemein formulieren, sondern nur beispielhaft verdeutlichen: Sei $\text{var } t$ die Menge der in einem Term t vorkommenden Variablen. Dann lässt sich $\text{var } t$ wie folgt rekursiv erklären:

$$\text{var } c = \emptyset ; \text{ var } x = \{x\} ; \text{ var } ft_1 \dots t_n = \text{var } t_1 \cup \dots \cup \text{var } t_n.$$

$\text{var } \xi$ ist für alle $\xi \in \mathcal{S}_{\mathcal{L}}$ durch $\text{var } \xi = \{x \in \text{Var} \mid \text{es gibt } \xi_0, \xi_1 \in \mathcal{S}_{\mathcal{L}} \text{ mit } \xi = \xi_0 x \xi_1\}$, also mittels Verkettung auch direkt leicht definierbar. Speziell ist $\text{var } \varphi$ für $\varphi \in \mathcal{L}$ damit wohlerklärt. Für $X \subseteq \mathcal{S}_{\mathcal{L}}$ sei $\text{var } X := \bigcup \{\text{var } \xi \mid \xi \in X\}$. Auch der Begriff *Subterm* ($=$ *Teilterm*) eines Terms ist rekursiv definierbar. Man kann aber auch hier kürzer und allgemeiner folgende Festlegung treffen: Der Term t heiße Subterm einer Zeichenfolge ξ , wenn $\xi = \xi_1 t \xi_2$ für möglicherweise leere Zeichenfolgen ξ_1, ξ_2 .

Wir definieren nun wiederum rekursiv diejenigen Zeichenfolgen über dem Alphabet von \mathcal{L} , die man als *Formeln* bezeichnet, auch prädikatenlogische *Ausdrücke* oder *Aussageformen* genannt. Gewisse Formeln werden später *Aussagen* genannt.

Formeln in L . (F1) Sind s, t Terme, so ist die Zeichenfolge $s = t$ eine Formel.
 (F2) Sind t_1, \dots, t_n Terme und $r \in L$ (Stellenzahl n), so ist $rt_1 \cdots t_n$ eine Formel.
 (F3) Sind α, β Formeln und ist $x \in \text{Var}$, so sind auch $(\alpha \wedge \beta)$, $\neg \alpha$ und $\forall x \alpha$ Formeln.

Andere als die gemäß (F1), (F2) und (F3) erzeugten Zeichenfolgen sollen in diesem Zusammenhang keine Formeln sein. Weitere logische Symbole werden durchgehend nur zur Abkürzung verwendet, und zwar sei $\exists x \alpha := \neg \forall x \neg \alpha$ und wie bisher sei $\alpha \vee \beta := \neg(\neg \alpha \wedge \neg \beta)$, $\alpha \rightarrow \beta := \neg(\alpha \wedge \neg \beta)$, und $\alpha \leftrightarrow \beta := (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$.

Beispiele. (a) $\forall x \exists y x + y = 0$ (genauer, $\forall x \neg \forall y \neg x + y = 0$) ist eine Formel, die den Sachverhalt ‘Für alle x gibt es ein y mit $x + y = 0$ ’ zum Ausdruck bringen soll⁵⁾.
 (b) $\forall x \forall x x = y$ ist eine Formel. Denn ein wiederholtes „Quantifizieren“ derselben Variablen wurde nicht verboten; die Grammatik ist diesbezüglich liberal, weil man damit viel Schreibarbeit spart. $\forall x \forall x x = y$ hat denselben Sinn wie $\forall x x = y$; beide Formeln sind im später definierten Sinne logisch äquivalent. Auch ist mit φ stets $\forall x \varphi$ eine Formel, selbst wenn x in φ gar nicht vorkommt. Trotz dieser Großzügigkeiten entspricht die Formelsyntax in etwa der Syntax der natürlichen Sprache.

Die durch (F1) und (F2) gewonnenen Formeln heißen *Primformeln* (auch *atomare* Formeln). Solche der Gestalt $s = t$ heißen *Gleichungen*. Diese sind die einzigen Primformeln, falls L keine Relationssymbole enthält, d.h. eine *algebraische* Signatur ist. Für $\neg s = t$ wird $s \neq t$ geschrieben. Primformeln der Gestalt $rt_1 \dots t_n$ sind trotz der kompakten klammerfreien Schreibweise eindeutig lesbar (eindeutige Primformel-Rekonstruktion, Übung 3). Zweistellige Relationszeichen trennen meistens die Argumente wie z.B. in $x \leq y$. Das geschieht der besseren Lesbarkeit halber.

Wie in der Aussagenlogik heißen Primformeln und deren Negationen *Literale*. Formeln, in denen \forall, \exists nicht vorkommen, heißen *quantorenfreie* oder *offene* Formeln. Dies sind genau die Booleschen Kombinationen aus Primformeln. Allgemein seien die *Booleschen Kombinationen* der Formeln aus einer gegebenen Formelmengemenge X alle diejenigen, die sich mittels \wedge, \neg (und damit automatisch auch mittels $\vee, \rightarrow, \leftrightarrow$) aus den Formeln von X erzeugen lassen. Zeichenfolgen der Gestalt $\forall x, \exists x$ (sprich *für alle x* bzw. *es gibt ein x*) werden *Präfixe* genannt.

Die Menge aller Formeln in L werde mit \mathcal{L} bezeichnet, für $L = \{\epsilon\}$ z.B. auch mit \mathcal{L}_ϵ und analog für ähnlich einfache Signaturen. Auch der Fall $L = \emptyset$ ist zugelassen. Dieser definiert die *Sprache $\mathcal{L}_=$ der reinen Identität*.

Statt von Termen, Formeln und Strukturen der Signatur L reden wir kürzer von \mathcal{L} -Termen, \mathcal{L} -Formeln und \mathcal{L} -Strukturen und lassen den Vorsatz \mathcal{L} - auch weg, wenn

⁵⁾Wir unterstellen hier stillschweigend, dass x, y verschiedene Variablen bezeichnen. Dies geschieht auch nachfolgend überall dort, wo der Zusammenhang dies gestattet.

\mathcal{L} vorgegeben ist. Für die Formelniederschrift benutzt man dieselben Verabredungen der Klammerersparnis wie in der Aussagenlogik. Bei länglichen Formeln werden der besseren Lesbarkeit halber weitere informelle Hilfsmittel benutzt, etwa unterschiedlich gestaltete Klammerpaare wie in $\forall x \exists y \forall z [z \in y \leftrightarrow \exists u (z \in u \wedge u \in x)]$. Auch andere optisch gefällige Hilfsmittel oder verbale Beschreibungen (ganz oder teilweise) sind erlaubt, solange die gemeinte Formel eindeutig erkennbar ist. X, Y, Z bezeichnen stets Formelmengen, $\alpha, \beta, \gamma, \delta, \pi, \varphi, \dots$ Formeln und s, t Terme, während Φ, Ψ der Bezeichnung endlicher Formelfolgen und formaler Beweise vorbehalten bleiben. $\sigma, \tau, \omega, \rho$ und ι werden Substitutionen bezeichnen.

Auch für Formeln gibt es ein *Beweisprinzip durch Formelinduktion* und ein *Definitionsprinzip durch Formelrekursion*. Wir verzichten aber auf allgemeine Formulierungen und verfahren nach dem Motto *theoria docent, exempla trahunt*. Definition durch Formelrekursion basiert auf der ähnlich wie in 1.1 erklärten eindeutigen Rekonstruktion. Man definiert z.B. $\text{rg } \varphi$, den *Rang* von φ , rekursiv durch

$$\text{rg } \pi = 0 \text{ (} \pi \text{ prim)}, \text{ rg } (\alpha \wedge \beta) = \max\{\text{rg } \alpha, \text{rg } \beta\} + 1, \text{ rg } \neg \alpha = \text{rg } \forall x \alpha = \text{rg } \alpha + 1.$$

Für manche Zwecke nützlich ist auch der *Quantorenrang* $\text{qr } \varphi$, der die Maximaltiefe ineinander geschachtelter Quantoren misst. Sei $\text{qr } \pi = 0$ für Primformeln π und

$$\text{qr } (\alpha \wedge \beta) = \max\{\text{qr } \alpha, \text{qr } \beta\}, \text{ qr } \neg \alpha = \text{qr } \alpha, \text{ qr } \forall x \alpha = \text{qr } \alpha + 1.$$

Auch der analog wie in der Aussagenlogik erklärte Begriff der *Subformel* ist rekursiv gekennzeichnet. Darüber können wir uns wortreiche Erklärungen ersparen.

Wir schreiben $x \in \text{gbd } \varphi$ (x kommt gebunden vor in φ), falls φ das Präfix $\forall x$ enthält. In Subformeln von φ der Gestalt $\forall x \beta$ heißt β auch der *Wirkungsbereich* von $\forall x$. Dasselbe Präfix kann in einer Formel mehrfach und mit ineinander geschachtelten Wirkungsbereichen vorkommen, wie z.B. in $\forall x (\forall x x = 0 \wedge x < y)$. In der Praxis umgeht man dies möglichst. Ein Computer hat damit aber keine Probleme.

Intuitiv unterscheiden sich die Formeln (a) $\forall x \exists y x + y = 0$ und (b) $\exists y x + y = 0$ darin, dass die erste in jedem Bereich mit gegebener Bedeutung von $+$ und 0 entweder wahr oder falsch ist; hingegen wartet (b) auf eine Wertzuteilung für x . Man sagt auch, in (a) sind alle vorkommenden Variablen gebunden, und (b) enthält die „freie“ Variable x . In diesem Sinne ist (b) nur eine Aussageform. Man definiert ‘ x kommt in φ frei vor’ oder ‘ $x \in \text{frei } \varphi$ ’ wie folgt: Es sei $\text{frei } \alpha = \text{var } \alpha$ für Primformeln α sowie

$$\text{frei } (\alpha \wedge \beta) = \text{frei } \alpha \cup \text{frei } \beta, \text{ frei } \neg \alpha = \text{frei } \alpha, \text{ frei } \forall x \alpha = \text{frei } \alpha \setminus \{x\}.$$

Beispiele. $\text{frei } (\forall x \exists y x + y = 0) = \emptyset$, $\text{frei } (x \leq y \wedge \forall x \exists y x + y = 0) = \{x, y\}$.

Wie das letzte der Beispiele zeigt, kann x in φ sowohl gebunden als auch frei vorkommen. Auch das wird in der praktischen Handhabung möglichst vermieden.

Formeln ohne freie Variablen heißen *Aussagen*, auch *geschlossene* Formeln genannt. $\forall x \exists y x + y = 0$ ist ein Beispiel. \mathcal{L}^0 bezeichne die Menge aller Aussagen von \mathcal{L} . Allgemeiner sei \mathcal{L}^n die Menge aller Formeln φ mit $\text{frei } \varphi \subseteq \{v_0, \dots, v_{n-1}\}$. So ist z.B. $\mathcal{L}^1 = \{\varphi \in \mathcal{L} \mid \text{frei } \varphi \subseteq \{v_0\}\}$. Offenbar gilt $\mathcal{L}^0 \subseteq \mathcal{L}^1 \subseteq \dots \subseteq \mathcal{L}$. Wir treffen gleich an dieser Stelle eine wichtige und durchgehend gültige

Verabredung. Die Schreibweise $\varphi = \varphi(x)$ soll bedeuten, dass die Formel φ höchstens x frei enthält. Allgemeiner bedeute $\varphi = \varphi(x_1, \dots, x_n)$ oder $\varphi = \varphi(\vec{x})$, dass $\text{frei } \varphi \subseteq \{x_1, \dots, x_n\}$, wobei x_1, \dots, x_n paarweise verschiedene Variablen vertreten. Nicht jede dieser Variablen muss in φ wirklich vorkommen. Analog ist $t = t(\vec{x})$ für Terme t zu lesen. $ft_1 \cdots t_n$ werde auch mit $f\vec{t}$, und $rt_1 \cdots t_n$ auch mit $r\vec{t}$ bezeichnet.

Substitutionen. Wir beginnen mit der Substitution $\frac{t}{x}$ eines Terms t für eine einzelne Variable x . Es soll $\varphi \frac{t}{x}$ (gelesen „ φ t für x “) anschaulich formuliert diejenige Zeichenfolge sein, welche durch Ersetzung der Variablen x an allen Stellen ihres freien Vorkommens in der Formel φ durch den Term t entsteht. Diese Veranschaulichung wird durch folgende Erklärung präzisiert, in der $s \frac{t}{x}$ rekursiv erst für Terme und sodann für Formeln definiert wird; hierin sei $t'_i := t_i \frac{t}{x}$.

$$\begin{aligned} x \frac{t}{x} &= t, & y \frac{t}{x} &= y \ (x \neq y), & c \frac{t}{x} &= c, & (ft_1 \cdots t_n) \frac{t}{x} &= ft'_1 \cdots t'_n, \\ (t_1 = t_2) \frac{t}{x} &= t'_1 = t'_2, & (rt_1 \cdots t_n) \frac{t}{x} &= rt'_1 \cdots t'_n, & (\forall y \alpha) \frac{t}{x} &= \begin{cases} \forall y \alpha & \text{falls } x = y, \\ \forall y (\alpha \frac{t}{x}) & \text{sonst.} \end{cases} \\ (\alpha \wedge \beta) \frac{t}{x} &= \alpha \frac{t}{x} \wedge \beta \frac{t}{x}, & (\neg \alpha) \frac{t}{x} &= \neg(\alpha \frac{t}{x}), \end{aligned}$$

Termininduktion zeigt, dass $s \frac{t}{x}$ für alle $s, t \in \mathcal{T}$ wieder ein Term ist. Also ist mit φ auch $\varphi \frac{t}{x}$ eine Formel. Man zeigt leicht $(\alpha \rightarrow \beta) \frac{t}{x} = \alpha \frac{t}{x} \rightarrow \beta \frac{t}{x}$ und analog für \vee, \exists . Neben diesen *einfachen* Substitutionen $\frac{t}{x}$ sind auch *simultane Substitutionen*

$$\varphi \frac{t_1 \cdots t_n}{x_1 \cdots x_n} \quad (x_1, \dots, x_n \text{ paarweise verschieden})$$

nützlich, auch durch $\varphi \frac{\vec{t}}{\vec{x}}$ oder $\varphi_{\vec{x}}(\vec{t})$ notiert, oder nur durch $\varphi(\vec{t})$ wenn Missverständnisse ausgeschlossen sind. Hier werden die Variablen x_i durch die Terme t_i simultan ersetzt. Alle diese Substitutionsformen werden als Sonderfall *globaler* Substitutionen σ definiert. Eine solche ordnet *jeder* Variablen x einen Term $x^\sigma \in \mathcal{T}$ zu und wird auf ganz \mathcal{T} gemäß $c^\sigma = c$, $(f\vec{t})^\sigma = ft_1^\sigma \cdots t_n^\sigma$ und alsdann auf ganz \mathcal{L} entsprechend den folgenden Klauseln erweitert, so dass dann $\text{dom } \sigma = \mathcal{T} \cup \mathcal{L}$.

$$(t_1 = t_2)^\sigma = t_1^\sigma = t_2^\sigma, \quad (r\vec{t})^\sigma = rt_1^\sigma \cdots t_n^\sigma, \quad (\alpha \wedge \beta)^\sigma = \alpha^\sigma \wedge \beta^\sigma, \quad (\neg \alpha)^\sigma = \neg \alpha^\sigma,$$

sowie $(\forall x \varphi)^\sigma = \forall x \varphi^\tau$, wobei die Substitution τ erklärt sei durch $x^\tau = x$ und $y^\tau = y^\sigma$ für $y \neq x$. Für \forall -freies φ und sogar beliebige \forall -freie Zeichenfolgen $\xi \in \mathcal{S}_{\mathcal{L}}$ ist ξ^σ auf einfache Weise auch direkt definiert: Jedes $x \in \text{var } \xi$ wird durch x^σ ersetzt. Es ist dann $(\xi \eta)^\sigma = \xi^\sigma \eta^\sigma$. Zu den globalen gehört auch die durchweg mit ι bezeichnete *identische Substitution* mit $x^\iota = x$ für alle x , also $\xi^\iota = \xi$ für alle $\xi \in \mathcal{S}_{\mathcal{L}}$.

Die simultane Substitution $\frac{\vec{t}}{\vec{x}}$ fassen wir auf als diejenige globale Substitution σ mit $x_i^\sigma = t_i$ für $i = 1, \dots, n$ und $x^\sigma = x$ sonst. Man kann auch sagen: Die simultanen sind diejenigen globalen Substitutionen σ mit $x^\sigma = x$ für *fast alle* Variablen x , d.h. mit Ausnahme endlich vieler. Diese Erklärung lässt unmittelbar erkennen, dass das Produkt $\sigma_1\sigma_2$ simultaner Substitutionen – es sei $\varphi^{\sigma_1\sigma_2} = (\varphi^{\sigma_1})^{\sigma_2}$ – wieder eine solche ist. Diese bilden offensichtlich eine Halbgruppe mit dem neutralen Element ι .

Stets ist $\frac{t_1 t_2}{x_1 x_2} = \frac{t_2 t_1}{x_2 x_1}$, während i.a. $\varphi \frac{t_1}{x_1} \frac{t_2}{x_2} \neq \varphi \frac{t_2}{x_2} \frac{t_1}{x_1}$. Wir erläutern beispielhaft den Unterschied zwischen $\varphi \frac{t_1 t_2}{x_1 x_2}$ und $\varphi \frac{t_1}{x_1} \frac{t_2}{x_2}$. Will man etwa die Variablen x_1, x_2 an den Stellen ihres freien Vorkommens in φ vertauschen, ist dies $\varphi \frac{x_2 x_1}{x_1 x_2}$, und nicht etwa $\varphi \frac{x_2}{x_1} \frac{x_1}{x_2}$ – man betrachte $\varphi = x_1 < x_2$. Es gilt aber $\varphi \frac{x_2 x_1}{x_1 x_2} = \varphi \frac{y}{x_2} \frac{x_2}{x_1} \frac{x_1}{y}$ für ein geeignetes y . Dieser Sachverhalt wird verallgemeinert durch

$$(1) \quad \varphi \frac{\vec{t}}{\vec{x}} = \varphi \frac{y}{x_n} \frac{t_1 \dots t_{n-1}}{x_1 \dots x_{n-1}} \frac{t_n}{y} \quad (y \notin \text{var}\{\varphi, \vec{x}, \vec{t}\}, n \geq 2).$$

Simultane und sogar globale Substitutionen ergeben demnach lokal, d.h. auf einzelne Formeln bezogen, dasselbe wie gewisse Produkte einfacher Substitutionen, d.h. deren schrittweise Ausführung. Mitunter lässt (1) sich vereinfachen. Nützlich ist z.B.

$$(2) \quad \varphi \frac{\vec{t}}{\vec{x}} = \varphi \frac{t_1}{x_1} \dots \frac{t_n}{x_n}, \text{ falls } x_i \notin \text{var } t_j \text{ für } i \neq j.$$

Diese Gleichung gilt insbesondere dann, wenn alle Terme t_i variablenfrei sind. Der richtige Umgang mit Substitutionen ist nicht ganz einfach und erfordert Übung, weil unsere Anschauung über komplexe Zeichenfolgen nicht besonders verlässlich ist.

Übungen

1. Man beweise $\varphi \frac{t}{x} = \varphi$ für $x \notin \text{frei } \varphi$, und $\varphi \frac{y}{x} \frac{t}{y} = \varphi \frac{t}{x}$ für $y \notin \text{var } \varphi$. An Beispielen verdeutliche man, dass diese Einschränkungen unverzichtbar sind.
2. Man zeige, jedes in einem (klammerfreien) Term t vorkommende Symbol ζ ist an jeder Stelle des Vorkommens erster Buchstabe eines Subterms von t , der durch die Position von ζ nach Übung 3(a) auch eindeutig bestimmt ist. Dasselbe gilt dann auch für ein in der Formel $r\vec{t}$ vorkommendes Symbol $\zeta \neq r$.
3. Sei $t \in \mathcal{T}_L$ und $\mathcal{E}t$ die Eigenschaft ‘Kein echter Anfang von t ist ein Term und t ist kein echter Anfang eines Termes’. Man beweise (a) $\mathcal{E}t$ gilt für alle $t \in \mathcal{T}_L$, (b) die *eindeutige Termverkettung*: $t_1 \dots t_n = s_1 \dots s_m$ impliziert $n = m$ und $t_i = s_i$ für $i = 1, \dots, n$. Diese ergibt offenbar die eindeutige Termrekonstruktion und die eindeutige Primformel-Rekonstruktion.
4. Es sei ξ eine beliebige Zeichenfolge über dem Alphabet von \mathcal{L} . Man zeige (a) $\neg \xi \in \mathcal{L} \Rightarrow \xi \in \mathcal{L}$, (b) $\alpha, (\alpha \wedge \xi) \in \mathcal{L} \Rightarrow \xi \in \mathcal{L}$, (c) $\alpha, (\alpha \rightarrow \xi) \in \mathcal{L} \Rightarrow \xi \in \mathcal{L}$.

2.3 Semantik elementarer Sprachen

Es ist anschaulich klar, dass z.B. der Formel $\exists y y + y = x$ im Bereich $(\mathbb{N}, +)$ erst dann ein Wahrheitswert zugewiesen werden kann, wenn der freien Variablen x ein Wert aus \mathbb{N} entspricht. Eine Wahrheitswertzuweisung für eine Formel φ erfordert also nebst einer Interpretation der nichtlogischen Symbole auch eine Belegung mindestens der Variablen aus $\text{frei}\varphi$. Es ist jedoch technisch bequemer, von einer globalen Wertzuweisung aller Variablen auszugehen, auch wenn man im konkreten Fall nur die Werte endlich vieler Variablen benötigt. Wir beginnen daher mit folgender

Definition. Ein *Modell* \mathcal{M} sei ein Paar (\mathcal{A}, w) , bestehend aus einer \mathcal{L} -Struktur \mathcal{A} und einer *Belegung* $w: \text{Var} \rightarrow A$, $w: x \mapsto x^w$. Wir bezeichnen $r^{\mathcal{A}}, f^{\mathcal{A}}, c^{\mathcal{A}}$ und x^w auch durch $r^{\mathcal{M}}, f^{\mathcal{M}}, c^{\mathcal{M}}$ und $x^{\mathcal{M}}$. Der Träger von \mathcal{A} heißt auch der *Träger von* \mathcal{M} .

Modelle werden auch *Interpretationen* genannt und, wenn man auf \mathcal{L} Bezug nehmen will, auch *\mathcal{L} -Modelle*. Manche Autoren identifizieren Modelle von vornherein mit Strukturen, siehe hierzu auch 2.5. Der Modellbegriff wird in der Logik relativ flexibel gehalten und jeweiligen Bedürfnissen angepasst. w bezeichnet fortan Belegungen der Variablen in den Träger einer Struktur, solange nichts anderes gesagt wird.

\mathcal{M} weist jedem Term t auf natürliche Weise einen mit $t^{\mathcal{M}}$ oder auch nur durch t^w bezeichneten Wert aus A zu. Für Primterme ist der Wert bei \mathcal{M} schon gegeben. Im übrigen erfolgt die Wertzuweisung in natürlicher Weise rekursiv:

$$(ft_1 \cdots t_n)^{\mathcal{M}} = f^{\mathcal{M}}(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}).$$

Ist $\vec{t} = (t_1, \dots, t_n)$, schreiben wir kürzer $\vec{t}^{\mathcal{M}}$ für $(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}})$. Wenn immer es der Zusammenhang erlaubt, unterdrückt man die oberen Indizes und trifft nur eine gedankliche Unterscheidung zwischen Symbolen und ihrer Interpretation.

$t^{\mathcal{M}}$ hängt nur ab von den Bedeutungen der in t effektiv vorkommenden Symbole. Denn induktiv über t ergibt sich leicht folgende Behauptung: Ist $\text{var } t \subseteq V \subseteq \text{Var}$ und sind $\mathcal{M}, \mathcal{M}'$ Modelle mit demselben Träger derart, dass $x^{\mathcal{M}} = x^{\mathcal{M}'}$ für alle $x \in V$ und $\zeta^{\mathcal{M}} = \zeta^{\mathcal{M}'}$ für alle übrigen in t vorkommenden Zeichen ζ , so ist $t^{\mathcal{M}} = t^{\mathcal{M}'}$. Deshalb darf $t^{(\mathcal{A}, w)}$ für Grundterme t einfach mit $t^{\mathcal{A}}$ bezeichnet werden.

Wir definieren nun eine Erfüllungsrelation \models zwischen Modellen $\mathcal{M} = (\mathcal{A}, w)$ und Formeln φ wie in 1.3 rekursiv über φ . Man liest $\mathcal{M} \models \varphi$ als \mathcal{M} *erfüllt* φ , oder \mathcal{M} *ist ein Modell für* φ . Oft wird $\mathcal{M} \models \varphi$ auch in der Weise $\mathcal{A} \models \varphi[w]$ geschrieben. Jede dieser oder ähnlicher Notationen hat in gewissen Situationen ihre Vorteile. Ist $\mathcal{M} \models \varphi$ für alle $\varphi \in X$, so schreibt man $\mathcal{M} \models X$ und nennt \mathcal{M} ein *Modell für* X . Zur Formulierung der folgenden Erfüllungsklauseln nach [Ta1] betrachtet man für gegebenes $\mathcal{M} = (\mathcal{A}, w)$ und $a \in A$ auch das Modell $\mathcal{M}_x^a = (\mathcal{A}, w_x^a)$, das sich von \mathcal{M}

nur darin unterscheidet, dass die Variable x anstelle von $x^{\mathcal{M}}$ den Wert a erhält und alle übrigen Variablen ihre Werte behalten. Für $a = x^{\mathcal{M}}$ ist natürlich $\mathcal{M}_x^a = \mathcal{M}$.

$$\begin{aligned} \mathcal{M} \models s=t &\Leftrightarrow s^{\mathcal{M}} = t^{\mathcal{M}}, \\ \mathcal{M} \models r\vec{t} &\Leftrightarrow r^{\mathcal{M}}\vec{t}^{\mathcal{M}}, \\ \mathcal{M} \models \alpha \wedge \beta &\Leftrightarrow \mathcal{M} \models \alpha \text{ und } \mathcal{M} \models \beta, \\ \mathcal{M} \models \neg \alpha &\Leftrightarrow \mathcal{M} \not\models \alpha, \\ \mathcal{M} \models \forall x \alpha &\Leftrightarrow \mathcal{M}_x^a \models \alpha \text{ für alle } a \in A. \end{aligned}$$

Bemerkung 1. Man kann die letztgenannte Erfüllungsklausel auch anders formulieren, wenn in der Signatur für jedes $a \in A$ ein Name, sagen wir \mathbf{a} , vorhanden ist. Nämlich als

$$\mathcal{M} \models \forall x \alpha \Leftrightarrow \mathcal{M} \models \alpha \frac{\mathbf{a}}{x} \text{ für alle } a \in A.$$

Das erlaubt es unter anderem, die Erfüllungsrelation für Aussagen über \mathcal{A} unter Umgehung beliebiger Formeln durch Rekursion allein über Aussagen zu definieren. Hat nicht jedes Element $a \in A$ einen Namen in L , könnte man L vorher „auffüllen“, indem man für jedes a einen Namen \mathbf{a} zu L hinzufügt. Eine derartige Sprachexpansion ist aber nicht immer von Vorteil, z.B. in einer hier nicht näher ausgeführten Formalisierung der Semantik.

Es ist nützlich, die oben eingeführte Schreibweise $\mathcal{M}_x^a = (\mathcal{A}, w_x^a)$ geringfügig zu verallgemeinern. Es sei $\mathcal{M}_{\vec{x}}^{\vec{a}} = (\dots ((\mathcal{M}_{x_1}^{a_1})_{x_2}^{a_2}) \dots)_{x_n}^{a_n}$. Schreibt man außerdem $\forall \vec{x} \varphi$ für $\forall x_1 \dots \forall x_n \varphi$, lässt sich eine sehr nützliche Verallgemeinerung der letzten Erfüllungsklausel bequem formulieren, nämlich

$$\mathcal{M} \models \forall \vec{x} \varphi \Leftrightarrow \mathcal{M}_{\vec{x}}^{\vec{a}} \models \varphi \text{ für alle } \vec{a} \in A^n.$$

Weil \vee , \rightarrow und \leftrightarrow auf Seite 45 genauso definiert wurden wie in Kapitel 1, gelten ähnlich wie dort $\mathcal{M} \models \alpha \vee \beta$ genau dann wenn $\mathcal{M} \models \alpha$ oder $\mathcal{M} \models \beta$, $\mathcal{M} \models \alpha \rightarrow \beta$ genau dann wenn $\mathcal{M} \models \alpha \Rightarrow \mathcal{M} \models \beta$, und analog für \leftrightarrow . Auch $\exists x \varphi$ wurde in 2.2 sinnentsprechend definiert, denn man verifiziert leicht

$$\mathcal{M} \models \exists x \varphi \Leftrightarrow \mathcal{M}_x^a \models \varphi \text{ für ein gewisses } a \in A.$$

In der Tat, ist $\mathcal{M} \models \neg \forall x \neg \varphi (= \exists x \varphi)$, so gilt $\mathcal{M}_x^a \models \neg \varphi$ definitionsgemäß nicht für alle a , also gibt es ein $a \in A$ mit $\mathcal{M}_x^a \not\models \neg \varphi$, oder gleichwertig, mit $\mathcal{M}_x^a \models \varphi$. Und diese Schlusskette ist offensichtlich umkehrbar.

Beispiel 1. Für beliebiges \mathcal{M} gilt $\mathcal{M} \models \exists x x=t$, falls $x \notin \text{var } t$. Denn $\mathcal{M}_x^a \models x=t$ für ein gewisses a , nämlich $a = t^{\mathcal{M}}$, weil $t^{\mathcal{M}} = t^{\mathcal{M}_x^a}$ wegen $x \notin \text{var } t$. Schreibt man \mathcal{M}_x^t für $\mathcal{M}_x^{t^{\mathcal{M}}}$, kann man diese Begründung auch so formulieren: $\mathcal{M} \models \exists x x=t$, weil $\mathcal{M}_x^t \models x=t$. Man beachte, die Voraussetzung $x \notin \text{var } t$ ist hier wesentlich, denn es gilt z.B. $\mathcal{M} \models \exists x x = fx$ nur dann, wenn $f^{\mathcal{M}}$ einen Fixpunkt hat.

Wir führen hier bereits einige fundamentale Begriffe ein, die wir jedoch erst in 2.4 und 2.5 systematisch behandeln, weil dazu einige Vorbereitungen nötig sind.

Definition. Eine Formel bzw. Formelmenge aus \mathcal{L} heißt *erfüllbar*, wenn sie ein Modell besitzt. φ heißt *allgemeingültig*, *logisch gültig* oder eine *Tautologie*, kurz $\models \varphi$, wenn $\mathcal{M} \models \varphi$ für jedes Modell \mathcal{M} . Die Formeln α, β heißen (logisch oder semantisch) *äquivalent*, symbolisch $\alpha \equiv \beta$, wenn $\mathcal{M} \models \alpha \Leftrightarrow \mathcal{M} \models \beta$, für alle \mathcal{L} -Modelle \mathcal{M} . Ferner sei $\mathcal{A} \models \varphi$ (gelesen: *in \mathcal{A} gilt φ oder \mathcal{A} erfüllt φ), falls $(\mathcal{A}, w) \models \varphi$ für alle $w: \text{Var} \rightarrow A$. Auch schreibt man $\mathcal{A} \models X$, falls $\mathcal{A} \models \varphi$ für alle $\varphi \in X$. Schließlich sei $X \models \varphi$ (*aus X folgt φ*), wenn jedes Modell von X auch die Formel φ erfüllt.*

Wie in Kapitel 1 bezeichnet \models zugleich die Erfüllungs- und die Folgerungsrelation. Wie dort schreiben wir auch $\varphi_1, \dots, \varphi_n \models \varphi$ für $\{\varphi_1, \dots, \varphi_n\} \models \varphi$ usw. Außerdem bezeichnet \models noch die Gültigkeitsrelation in Strukturen.

Beispiel 2. Wir zeigen $\mathcal{A} \models \forall x \exists y x \neq y$, falls der Träger von \mathcal{A} mindestens zwei Elemente enthält. Denn sei $\mathcal{M} = (\mathcal{A}, w)$ und $a \in A$ vorgegeben. Dann gibt es ein $b \in A$ mit $a \neq b$, folglich $(\mathcal{M}_x^a)_y^b = \mathcal{M}_{xy}^{ab} \models x \neq y$, also $\mathcal{M}_x^a \models \exists y x \neq y$. Weil a beliebig war, folgt $\mathcal{M} \models \forall x \exists y x \neq y$. Also $(\mathcal{A}, w) \models \forall x \exists y x \neq y$ für alle w , d.h. $\mathcal{A} \models \forall x \exists y x \neq y$.

Man muss hierbei achtsam sein. Zwar gilt $\mathcal{M} \models \varphi$ oder $\mathcal{M} \models \neg \varphi$ für beliebiges φ , doch ist $\mathcal{A} \models \varphi$ oder $\mathcal{A} \models \neg \varphi$ (das *tertium non datur* für die Gültigkeit in Strukturen) i.a. nur noch für Aussagen φ richtig, wie Satz 3.1 zeigen wird. Enthält \mathcal{A} mehr als ein Element, so gilt z.B. weder $\mathcal{A} \models x = y$ noch $\mathcal{A} \models x \neq y$. Denn $x = y$ wird durch ein w mit $x^w \neq y^w$ falsifiziert, $x \neq y$ durch ein w mit $x^w = y^w$. Die Bewahrung der Eigenschaft $\mathcal{M} \models \varphi$ oder $\mathcal{M} \models \neg \varphi$ für beliebige Formeln φ ist einer der Gründe, warum Modelle nicht einfach mit Strukturen gleichgesetzt wurden.

Für $\varphi \in \mathcal{L}$ sei φ^\forall die Aussage $\forall x_1 \dots \forall x_m \varphi$, genannt die *Generalisierte* von φ ; dabei sei x_1, \dots, x_m eine Aufzählung von *frei* φ , etwa nach der Indexgröße der Variablen. Für $\varphi \in \mathcal{L}^0$ ist $\varphi^\forall = \varphi$. Aufgrund der Definitionen ergibt sich unschwer

$$(1) \quad \mathcal{A} \models \varphi \Leftrightarrow \mathcal{A} \models \varphi^\forall,$$

und allgemeiner, $\mathcal{A} \models X \Leftrightarrow \mathcal{A} \models X^\forall$ ($:= \{\varphi^\forall \mid \varphi \in X\}$). (1) erklärt, warum man φ und φ^\forall häufig gedanklich miteinander identifiziert und z.B. eine Mitteilung, die formal eigentlich φ^\forall lautet, oft zu φ verkürzt. Der Kontext muss klar erkennen lassen, ob man sich eine Generalisierung der freien Variablen von φ ausgeführt denken darf oder nicht. Unabhängig von dieser Diskussion gilt aber stets $\models \varphi \Leftrightarrow \models \varphi^\forall$. Übrigens werden Generalisierungen auch im metatheoretischen Kontext oft nicht notiert, zum Beispiel bei der Formulierung von (1). Denn diese Äquivalenz lautet genau genommen ‘für alle $\mathcal{A}, \varphi : \mathcal{A} \models \varphi \Leftrightarrow \mathcal{A} \models \varphi^\forall$ ’.

Schon nach den bisherigen noch unvollständigen Ausführungen ist klar, dass sich zahlreiche Eigenschaften von Strukturen und ganze Axiomensysteme durch Formeln und Aussagen in der 1. Stufe adäquat beschreiben lassen. So kann z.B. das in 2.1 erwähnte Axiomensystem für Gruppen in $\mathcal{L}\{\circ, e, {}^{-1}\}$ wie folgt formuliert werden:

$$\forall x \forall y \forall z \ x \circ (y \circ z) = (x \circ y) \circ z \quad ; \quad \forall x \ x \circ e = x \quad ; \quad \forall x \ x \circ x^{-1} = e.$$

Genau die aus diesen drei Axiomen folgenden Aussagen sind dann die Sätze der *elementaren Gruppentheorie in $\circ, e, {}^{-1}$* , die fortan mit $T_G^=$ bezeichnet werde. Man erhält eine mit T_G bezeichnete Formulierung der Gruppentheorie in \circ, e , wenn das letzte Axiom durch $\forall x \exists y \ x \circ y = e$ ersetzt wird. $T_G^=$ ist gemäß Übung 3 in 2.6 eine konservative Erweiterung von T_G . Ohne Beweis sei erwähnt, dass die Aussagen $\forall x \ e \circ x = x$ und $\forall x \exists y \ y \circ x = e$ in T_G und damit auch in $T_G^=$ herleitbar sind.

Auch für geordnete Mengen lässt sich ein Axiomensystem leicht angeben, indem man die Eigenschaften der Irreflexivität, Transitivität und Konnexität formalisiert; dabei steht hier und anderswo $\forall x_1 \dots x_n \varphi$ für $\forall x_1 \dots \forall x_n \varphi$.

$$\forall x \ x \not< x \quad ; \quad \forall xyz (x < y \wedge y < z \rightarrow x < z) \quad ; \quad \forall xy (x \neq y \rightarrow x < y \vee y < x).$$

Bei der Niederschrift dieser und anderer Axiome lässt man die äußeren \forall -Präfixe gelegentlich weg um Schreibarbeit zu sparen und denkt sich die Generalisierung der Variablen stillschweigend ausgeführt, worauf oben schon hingewiesen wurde.

Für Aussagen α einer gegebenen Sprache ist plausibel, dass die Werte der Variablen für die Relation $(\mathcal{A}, w) \models \alpha$ keine Rolle spielen. Den präzisen Beweis entnimmt man dem nachfolgenden Satz für $V = \emptyset$. Danach ist entweder $(\mathcal{A}, w) \models \alpha$ für alle w und damit $\mathcal{A} \models \alpha$, oder aber $(\mathcal{A}, w) \models \alpha$ für kein w , d.h. $(\mathcal{A}, w) \models \neg \alpha$ für alle w , und somit $\mathcal{A} \models \neg \alpha$. Aussagen erfüllen daher das schon zitierte tertium non datur.

Satz 3.1 (Koinzidenzsatz). *Sei $V \subseteq \text{Var}$, frei $\varphi \subseteq V$ und seien $\mathcal{M}, \mathcal{M}'$ Modelle über demselben Träger A mit $x^{\mathcal{M}} = x^{\mathcal{M}'}$ für alle $x \in V$, sowie $\zeta^{\mathcal{M}} = \zeta^{\mathcal{M}'}$ für alle in φ vorkommenden nichtlogischen Symbole ζ . Dann gilt $\mathcal{M} \models \varphi \Leftrightarrow \mathcal{M}' \models \varphi$.*

Beweis durch Induktion über φ . Sei φ die Primformel $r\vec{t}$. Der Wert eines Terms t hängt nach einer früheren Feststellung nur ab von den Bedeutungen der in t vorkommenden Symbole. Diese sind aufgrund der Voraussetzungen für t_1, \dots, t_n aber dieselben in \mathcal{M} und \mathcal{M}' . Also $\vec{t}^{\mathcal{M}} = \vec{t}^{\mathcal{M}'}$ (d.h. $t_i^{\mathcal{M}} = t_i^{\mathcal{M}'}$ für $i = 1, \dots, n$), und daher $\mathcal{M} \models r\vec{t} \Leftrightarrow r^{\mathcal{M}}\vec{t}^{\mathcal{M}} \Leftrightarrow r^{\mathcal{M}}\vec{t}^{\mathcal{M}'} \Leftrightarrow r^{\mathcal{M}'}\vec{t}^{\mathcal{M}'} \Leftrightarrow \mathcal{M}' \models r\vec{t}$. Für Gleichungen $t_1 = t_2$ schließt man analog. Ferner ergibt die Induktionsannahme für α, β

$$\mathcal{M} \models \alpha \wedge \beta \Leftrightarrow \mathcal{M} \models \alpha, \beta \Leftrightarrow \mathcal{M}' \models \alpha, \beta \Leftrightarrow \mathcal{M}' \models \alpha \wedge \beta.$$

In derselben Weise erhält man $\mathcal{M} \models \neg \alpha \Leftrightarrow \mathcal{M}' \models \neg \alpha$. Beim Induktionsschritt über \forall wird klar, dass die Induktionsannahme geschickt zu formulieren ist. Diese muss sich auf beliebige V und beliebige Modellpaare mit den genannten Voraussetzungen beziehen. Sei also $\mathcal{M} \models \forall x \varphi$ und $a \in A$, so dass $\mathcal{M}_x^a \models \varphi$. Weil für $V' := V \cup \{x\}$ gewiss frei $\varphi \subseteq V'$, und $\mathcal{M}_x^a, \mathcal{M}'_x^a$ auf allen $y \in V'$ übereinstimmen – obgleich im Allgemeinen $x^{\mathcal{M}} \neq x^{\mathcal{M}'}$ – gilt mit $\mathcal{M}_x^a \models \varphi$ auch $\mathcal{M}'_x^a \models \varphi$ nach Induktionsannahme. a war beliebig, also $\mathcal{M}' \models \forall x \varphi$. Umgekehrt schließt man genauso. \square

Danach kann ein \mathcal{L} -Modell $\mathcal{M} = (\mathcal{A}, w)$ von φ für den Fall $\varphi \in \mathcal{L} \subseteq \mathcal{L}'$ völlig beliebig zu einem \mathcal{L}' -Modell $\mathcal{M}' = (\mathcal{A}', w)$ von φ expandiert werden, d.h. legt man $\zeta^{\mathcal{A}'}$ für $\zeta \in L' \setminus L$ willkürlich fest, so ist $\mathcal{M} \models \varphi \Leftrightarrow \mathcal{M}' \models \varphi$ nach obigem Satz mit $V = \text{Var}$. Insbesondere hängen die Erfüllbarkeit oder Allgemeingültigkeit von φ nur ab von den in φ effektiv vorkommenden Symbolen. Daraus ergibt sich sehr leicht, dass die auf \mathcal{L}' bezogene Folgerungsrelation $\models_{\mathcal{L}'}$ eine *konservative* Erweiterung von $\models_{\mathcal{L}}$ in dem Sinne ist, dass $X \models_{\mathcal{L}} \varphi \Leftrightarrow X \models_{\mathcal{L}'} \varphi$, für alle $X \subseteq \mathcal{L}$ und $\varphi \in \mathcal{L}$. Eine Indizierung von \models erübrigt sich aus diesem Grunde.

Schließlich erwähnen wir als Anwendung von Satz 3.1 noch folgende Tatsache, die das bereits erwähnte „Weglassen überflüssiger Quantoren“ rechtfertigt.

$$(2) \quad \forall x \varphi \equiv \varphi \equiv \exists x \varphi, \text{ vorausgesetzt } x \notin \text{frei } \varphi.$$

Denn im Falle $x \notin \text{frei } \varphi$ gilt ja $\mathcal{M} \models \varphi \Leftrightarrow \mathcal{M}_x^a \models \varphi$ für ein beliebiges $a \in A$ nach Satz 3.1 – man wähle $\mathcal{M}' = \mathcal{M}_x^a$ und $V = \text{frei } \varphi$. Damit ergibt sich

$$\mathcal{M} \models \forall x \varphi \Leftrightarrow \mathcal{M}_x^a \models \varphi \text{ für alle } a \Leftrightarrow \mathcal{M} \models \varphi \Leftrightarrow \mathcal{M}_x^a \models \varphi \text{ für ein } a \Leftrightarrow \mathcal{M} \models \exists x \varphi.$$

Nach Satz 3.1 ist die Erfüllung von φ in (\mathcal{A}, w) nur abhängig von den Werten der freien Variablen von φ bei w . Sei etwa $\varphi = \varphi(\vec{x})$ ⁶⁾ und $\vec{a} \in A^n$. Dann lässt sich

$$w \text{ ist eine Belegung mit } x_1^w = a_1, \dots, x_n^w = a_n \text{ und } (\mathcal{A}, w) \models \varphi$$

recht suggestiv durch eine der folgenden Schreibweisen zum Ausdruck bringen:

$$\mathcal{A} \models \varphi[a_1, \dots, a_n] \quad \text{oder} \quad \mathcal{A} \models \varphi[\vec{a}] \quad \text{oder} \quad (\mathcal{A}, \vec{a}) \models \varphi.$$

mit $a_i = x_i^w$ für $i = 1, \dots, n$. Diese Schreibweisen sind auch dann sinnvoll, wenn w zu einer nur auf $\{x_1, \dots, x_n\}$ erklärten kurz mit \vec{a} bezeichneten Belegung eingeschränkt wird. In 4.1 werden wir daher den Modellbegriff entsprechend erweitern. Im Sinne obigen Notationen könnte man den Wert des Terms $t = t(\vec{x})$ mit $t^{\mathcal{A}, \vec{a}}$ bezeichnen. Meistens schreibt man dafür $t^{\mathcal{A}}[\vec{a}]$, aber auch $t^{\mathcal{A}}(\vec{a})$ oder einfach nur $t(\vec{a})$. Wichtig ist nachfolgend vor allem die für beliebige Terme t gültige Behauptung

$$(3) \quad \text{Für } \mathcal{A} \subseteq \mathcal{B}, \mathcal{M} = (\mathcal{A}, w), \mathcal{M}' = (\mathcal{B}, w) \text{ und } w: \text{Var} \rightarrow A \text{ ist } t^{\mathcal{M}} = t^{\mathcal{M}'}.$$

Kurzum, $t^{\mathcal{A}}(\vec{a}) = t^{\mathcal{B}}(\vec{a})$ für $t = t(\vec{x})$ und alle $\vec{a} \in A^n$. Also sind nebst den Basisoperationen von \mathcal{A} auch die sogenannten *Termfunktionen* $\vec{a} \mapsto t^{\mathcal{A}}(\vec{a})$ die Einschränkungen ihrer Bedeutungen in \mathcal{B} . Die Behauptung (3) ist klar für Primterme, und die Induktionsannahme $t_i^{\mathcal{M}} = t_i^{\mathcal{M}'}$ impliziert

$$(ft_1 \cdots t_n)^{\mathcal{M}} = f^{\mathcal{M}}(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}) = f^{\mathcal{M}'}(t_1^{\mathcal{M}'}, \dots, t_n^{\mathcal{M}'}) = (ft_1 \cdots t_n)^{\mathcal{M}'}$$

⁶⁾Man beachte, die Redeweise ‘Sei $\varphi = \varphi(\vec{x}) \dots$ ’ schließt nebst einer Vorgabe von φ stillschweigend auch die Vorgabe von \vec{x} ein. Sie besagt noch nicht, dass φ überhaupt freie Variablen enthält. Sie besagt nur $\text{frei } \varphi \subseteq \text{var } \vec{x}$. Auch in weiter unten benutzten Schreibweisen wie $(\mathcal{A}, \vec{a}) \models \varphi$ muss \vec{x} gegeben sein.

$\varphi^{\mathcal{A}} := \{\vec{a} \in A^n \mid \mathcal{A} \models \varphi[\vec{a}]\}$ heißt *das von der Formel $\varphi = \varphi(\vec{x})$ in der Struktur \mathcal{A} definierte Prädikat*. Ein Prädikat $P \subseteq A^n$ heißt *in \mathcal{A} (elementar) definierbar*, wenn es eine Formel $\varphi = \varphi(\vec{x})$ gibt mit $P = \varphi^{\mathcal{A}}$. So ist das \leq -Prädikat in $(\mathbb{N}, +)$ definiert durch $\varphi(x, y) := \exists z z + x = y$. Analog heie $f: A^n \rightarrow A$ in \mathcal{A} definierbar, wenn ein $\varphi(\vec{x}, y)$ existiert mit $\varphi^{\mathcal{A}} = \text{graph } f$. Man spricht dann auch von elementarer Definierbarkeit von f in \mathcal{A} .

Fr $\mathcal{A} \subseteq \mathcal{B}$ und $\varphi = \varphi(\vec{x})$ ist i.a. $\varphi^{\mathcal{A}} \neq \varphi^{\mathcal{B}} \cap A^n$. Sei etwa $\varphi = \exists z z + x = y$, $\mathcal{A} = (\mathbb{N}, +)$ und $\mathcal{B} = (\mathbb{Z}, +)$. Dann ist $\varphi^{\mathcal{A}} = \leq^{\mathcal{A}}$, whrend $\varphi^{\mathcal{B}}$ offenbar auf smtliche Paare $(a, b) \in \mathbb{Z}^2$ zutrifft. $\varphi^{\mathcal{A}} = \varphi^{\mathcal{B}} \cap A^n$ gilt aber fr quantorenfreie φ und ist unter der Voraussetzung $A \subseteq B$ nach folgendem Satz sogar kennzeichnend fr $\mathcal{A} \subseteq \mathcal{B}$.

Satz 3.2 (Substruktursatz). *Fr Strukturen \mathcal{A}, \mathcal{B} mit $A \subseteq B$ sind gleichwertig*

- (i) \mathcal{A} ist Substruktur von \mathcal{B} , also $\mathcal{A} \subseteq \mathcal{B}$,
- (ii) $\mathcal{A} \models \varphi[\vec{a}] \Leftrightarrow \mathcal{B} \models \varphi[\vec{a}]$, fr alle quantorenfreien $\varphi = \varphi(\vec{x})$ und alle $\vec{a} \in A^n$,
- (iii) $\mathcal{A} \models \varphi[\vec{a}] \Leftrightarrow \mathcal{B} \models \varphi[\vec{a}]$, fr alle Primformeln $\varphi(\vec{x})$ und alle $\vec{a} \in A^n$.

Beweis. (i) \Rightarrow (ii): Es gengt offenbar $\mathcal{M} \models \varphi \Leftrightarrow \mathcal{M}' \models \varphi$ fr alle $\mathcal{M} = (\mathcal{A}, w)$ und $\mathcal{M}' = (\mathcal{B}, w)$ mit $w: \text{Var} \rightarrow A$ zu beweisen. Dies ist nach (3) klar fr Primformeln und die Induktionsschritte ber \wedge, \neg erfolgen genau wie im Beweis von Satz 3.1. (ii) \Rightarrow (iii): Trivial. (iii) \Rightarrow (i): Die Annahme liefert

$$r^{\mathcal{A}}\vec{a} \Leftrightarrow \mathcal{A} \models r\vec{x}[\vec{a}] \Leftrightarrow \mathcal{B} \models r\vec{x}[\vec{a}] \Leftrightarrow r^{\mathcal{B}}\vec{a}.$$

Analog ist $f^{\mathcal{A}}\vec{a} = b \Leftrightarrow \mathcal{A} \models f\vec{x}=y[\vec{a}, b] \Leftrightarrow \mathcal{B} \models f\vec{x}=y[\vec{a}, b] \Leftrightarrow f^{\mathcal{B}}\vec{a} = b$, fr alle $\vec{a} \in A^n$ und $b \in A$. Diese Bedingungen besagen aber gerade $\mathcal{A} \subseteq \mathcal{B}$. \square

Hat α die Gestalt $\forall \vec{x}\beta$ mit quantorenfreiem β , wobei $\forall \vec{x}$ auch das leere Prfix sein kann, heit α eine *universale* oder \forall -*Formel* (sprich *A-Formel*), und fr $\alpha \in \mathcal{L}^0$ auch eine *universale* oder \forall -*Aussage*. Analog heit $\exists \vec{x}\beta$ (β quantorenfrei) eine \exists -*Formel* und falls $\exists \vec{x}\beta \in \mathcal{L}^0$, auch eine \exists -*Aussage*. Beispiele sind die „Anzahlaussagen“

$$\exists_1 := \exists v_0 v_0 = v_0, \quad \exists_n := \exists v_0 \cdots \exists v_{n-1} \bigwedge_{i < j < n} v_i \neq v_j \quad (n \geq 2).$$

\exists_n besagt ‘es gibt wenigstens n Elemente’, $\neg \exists_n$ demnach ‘es gibt hchstens $n - 1$ viele Elemente’ und $\exists_{=n} := \exists_n \wedge \neg \exists_{n+1}$ sagt ‘es gibt genau n Elemente’. Ferner sei $\top := \exists_1$, $\perp := \neg \top$ und $\exists_0 := \perp$. Satz 3.2 hat eine sehr ntzliche Folge, und zwar das

Korollar 3.3. *Sei $\mathcal{A} \subseteq \mathcal{B}$. Dann ist jede in \mathcal{B} geltende \forall -Aussage $\alpha = \forall \vec{x}\beta$ auch in \mathcal{A} erfllt. Dual dazu gilt jede in \mathcal{A} gltige \exists -Aussage auch in \mathcal{B} .*

Beweis. Sei $\mathcal{B} \models \forall \vec{x}\beta$ und $\vec{a} \in A^n$. Dann ist $\mathcal{B} \models \beta[\vec{a}]$, also $\mathcal{A} \models \beta[\vec{a}]$ nach (ii). Folglich $\mathcal{A} \models \forall \vec{x}\beta$, denn \vec{a} war beliebig. Dies ergibt mit indirekter Schlussweise auch die zweite Behauptung, weil $\mathcal{B} \not\models \exists \vec{x}\beta$ gleichwertig ist zu $\mathcal{B} \models \forall \vec{x}\neg \beta$. \square

Wir formulieren als nächstes eine Verallgemeinerung gewisser, häufig vorkommender Einzelargumente, nämlich den

Satz 3.4 (Invarianzsatz). *Seien \mathcal{A}, \mathcal{B} isomorphe L -Strukturen und sei $\iota: \mathcal{A} \rightarrow \mathcal{B}$ ein Isomorphismus. Dann gilt für alle $\varphi = \varphi(\vec{x})$ und alle $\vec{a} \in A^n$*

$$\mathcal{A} \models \varphi[\vec{a}] \Leftrightarrow \mathcal{B} \models \varphi[\iota\vec{a}] \quad (\iota\vec{a} = (\iota a_1, \dots, \iota a_n)).$$

Insbesondere gilt $\mathcal{A} \models \alpha \Leftrightarrow \mathcal{B} \models \alpha$ für alle Aussagen α von \mathcal{L} .

Beweis. Die Behauptung lässt sich für den Beweis bequemer formulieren als

$$(*) \quad \mathcal{M} \models \varphi \Leftrightarrow \mathcal{M}' \models \varphi \quad (\mathcal{M} = (\mathcal{A}, w), \mathcal{M}' = (\mathcal{B}, w'), w' : x \mapsto \iota x^w).$$

Man bestätigt mühelos $\iota(t^{\mathcal{M}}) = t^{\mathcal{M}'}$ für alle Terme t und ebenso mühelos $(*)$ durch Induktion über φ . Der Spezialfall für Aussagen ergibt sich für $n = 0$. \square

Damit ist z.B. ein und für allemal klar, dass das isomorphe Bild einer Gruppe wieder eine Gruppe ist, unabhängig von der gewählten Signatur. Für $\mathcal{A} \simeq \mathcal{B}$ gilt demnach $\mathcal{A} \models S \Leftrightarrow \mathcal{B} \models S$, für jede Aussagenmenge S , speziell das Axiomensystem einer Theorie. Satz 3.4 gilt übrigens ebenso für Formeln höherer Stufe (siehe 3.7). So ist z.B. auch jede Wohlordnung einer Menge invariant unter Isomorphismen.

\mathcal{L} -Strukturen \mathcal{A}, \mathcal{B} heißen *elementar-äquivalent*, wenn $\mathcal{A} \models \alpha \Leftrightarrow \mathcal{B} \models \alpha$, für alle $\alpha \in \mathcal{L}^0$. Man schreibt dann $\mathcal{A} \equiv \mathcal{B}$. Diesen wichtigen Begriff werden wir in 3.3 und genauer in 5.1 betrachten. Satz 3.4 sagt speziell $\mathcal{A} \simeq \mathcal{B} \Rightarrow \mathcal{A} \equiv \mathcal{B}$.

Es erhebt sich hier sogleich die Frage, ob auch die Umkehrung hiervon richtig ist. Für unendliche Strukturen ist die Antwort negativ (siehe 3.3), für endliche positiv; eine endliche Struktur endlicher Signatur kann bis auf Isomorphie sogar durch eine einzige Aussage beschrieben werden. So ist die 2-elementige Gruppe $\{0,1\}, +$ bis auf Isomorphie offenbar durch die folgende Aussage wohlbestimmt, die uns haargenau erzählt, wie $+$ auf dem 2-elementigen Träger operiert:

$$\exists x \exists y [x \neq y \wedge \forall z (z = x \vee z = y) \wedge x + x = x \wedge y + y = x \wedge x + y = y \wedge y + x = y].$$

Wir untersuchen nun das Verhalten der Erfüllungsrelation unter Substitutionen. Die Definition von $\varphi \frac{t}{x}$ in 2.2 nimmt keine Rücksicht auf *Variablenkollision*, was heißen soll, dass gewisse Variablen des Substitutionsterms t in φ gebunden vorkommen und nach Ausführung der Substitution in den Wirkungsbereich von Quantoren geraten können. Daher impliziert $\mathcal{M} \models \forall x \varphi$ nicht notwendig $\mathcal{M} \models \varphi \frac{t}{x}$, obwohl wir dies natürlich wünschen. Kurzum, $\forall x \varphi \models \varphi \frac{t}{x}$ ist nicht uneingeschränkt richtig. So ist nach Beispiel 2 für $\varphi := \exists y x \neq y$ gewiss $\mathcal{M} \models \forall x \varphi (= \forall x \exists y x \neq y)$, wenn \mathcal{M} mindestens 2-elementig ist, nicht aber $\mathcal{M} \models \varphi \frac{y}{x} (= \exists y y \neq y)$. Hier gerät y nach Substitution in den Wirkungsbereich des Quantors $\forall y$. Analog ist $\varphi \frac{t}{x} \models \exists x \varphi$ nicht ohne Einschränkungen richtig. Man wähle etwa $\forall y x = y$ für φ und y für t .

Man kann $\forall x \varphi \models \varphi_{\vec{x}}^{\vec{t}}$ ohne Einschränkung erzwingen, indem man durch Modifikation der rekursiven Definition von $\varphi_{\vec{x}}^{\vec{t}}$ im Quantorenschritt gebundene Variablen falls erforderlich umbenennt. Solche Maßnahmen sind aber recht unhandlich für die Gödelisierung des Beweises in 6.2. Wir nehmen daher kleine Einschränkungen bei der späteren Formulierung von Schlussregeln in Kauf.

$\varphi, \frac{t}{x}$ heißen *kollisionsfrei*, wenn $y \notin \text{gbd } \varphi$ für alle $y \in \text{var } t \setminus \{x\}$, y also nicht in den Wirkungsbereich eines Präfixes $\forall y$ geraten kann. Für $y = x$ ist dies ohnehin klar, weil t ja nur an Stellen des freien Vorkommens von x substituiert wird. Ist σ eine globale Substitution, so heißen φ, σ *kollisionsfrei*, wenn $\varphi, \frac{x^\sigma}{x}$ für jedes x kollisionsfrei sind. Im Falle $\sigma = \frac{\vec{t}}{\vec{x}}$ ist Kollisionsfreiheit nur für die Variablen in \vec{x} zu prüfen.

Für $\mathcal{M} = (\mathcal{A}, w)$ sei $\mathcal{M}^\sigma := (\mathcal{A}, w^\sigma)$, mit $x^{w^\sigma} := (x^\sigma)^\mathcal{M}$ für alle $x \in \text{Var}$. Diese Gleichung pflanzt sich induktiv fort zu $t^{\sigma\mathcal{M}} = t^{\mathcal{M}^\sigma}$ für alle t , wobei $t^{\sigma\mathcal{M}} := (x^\sigma)^\mathcal{M}$. Denn sie ist richtig für Primterme und ist $t_i^{\sigma\mathcal{M}} = t_i^{\mathcal{M}^\sigma}$ für $i = 1, \dots, n$ nach Induktionsannahme, folgt $t^{\sigma\mathcal{M}} = t^{\mathcal{M}^\sigma}$ für $t = ft_1 \dots t_n$ wegen $f^\mathcal{M} = f^{\mathcal{M}^\sigma}$ aus

$$t^{\sigma\mathcal{M}} = (ft_1 \dots t_n)^{\sigma\mathcal{M}} = f^\mathcal{M}(t_1^{\sigma\mathcal{M}}, \dots, t_n^{\sigma\mathcal{M}}) = f^{\mathcal{M}^\sigma}(t_1^{\mathcal{M}^\sigma}, \dots, t_n^{\mathcal{M}^\sigma}) = t^{\mathcal{M}^\sigma}.$$

Man beachte, \mathcal{M}^σ ist für $\sigma = \frac{\vec{t}}{\vec{x}}$ identisch mit $\mathcal{M}_x^{\vec{t}} := \mathcal{M}_x^{\vec{t}^\mathcal{M}}$. Dieser und andere Spezialfälle liefern wichtige Folgerungen aus dem etwas anspruchsvolleren

Satz 3.5 (Substitutionssatz). *Es sei \mathcal{M} ein beliebiges Modell und σ eine globale Substitution. Dann gilt für alle Formeln φ , für die φ, σ kollisionsfrei sind,*

$$\mathcal{M} \models \varphi^\sigma \Leftrightarrow \mathcal{M}^\sigma \models \varphi.$$

Speziell gilt $\mathcal{M} \models \varphi_{\vec{x}}^{\vec{t}} \Leftrightarrow \mathcal{M}_x^{\vec{t}} \models \varphi$ für kollisionsfreie $\varphi, \frac{\vec{t}}{\vec{x}}$.

Beweis durch Induktion über φ . Weil allgemein $t^{\sigma\mathcal{M}} = t^{\mathcal{M}^\sigma}$, haben wir

$$\mathcal{M} \models (t_1 = t_2)^\sigma \Leftrightarrow t_1^{\sigma\mathcal{M}} = t_2^{\sigma\mathcal{M}} \Leftrightarrow t_1^{\mathcal{M}^\sigma} = t_2^{\mathcal{M}^\sigma} \Leftrightarrow \mathcal{M}^\sigma \models t_1 = t_2.$$

Analog behandelt man Primformeln der Gestalt $r\vec{t}$. Die Induktionsschritte über \wedge, \neg sind harmlos. Interessant ist nur der \forall -Schritt $\varphi = \forall x \alpha$, der sich wie folgt ergibt:

$$\begin{aligned} \mathcal{M} \models (\forall x \alpha)^\sigma &\Leftrightarrow \mathcal{M} \models \forall x \alpha^\tau && (\text{mit } x^\tau = x \text{ und } y^\tau = y^\sigma \text{ sonst}) \\ &\Leftrightarrow \mathcal{M}_x^a \models \alpha^\tau \text{ für alle } a && (a \in A, \text{ dem Träger von } \mathcal{M}) \\ &\Leftrightarrow (\mathcal{M}_x^a)^\tau \models \alpha \text{ für alle } a && (\text{Ind.-Annahme; } \alpha, \tau \text{ sind kollisionsfrei}) \\ &\Leftrightarrow (\mathcal{M}^\sigma)_x^a \models \alpha \text{ für alle } a && (\text{weil } (\mathcal{M}_x^a)^\tau = (\mathcal{M}^\sigma)_x^a, \text{ Beweis unten}) \\ &\Leftrightarrow \mathcal{M}^\sigma \models \forall x \alpha. \end{aligned}$$

Es ist $(\mathcal{M}_x^a)^\tau = (\mathcal{M}^\sigma)_x^a$, denn $\forall x \alpha, \sigma$ sind kollisionsfrei, also auch $\forall x \alpha, \frac{y^\sigma}{y}$ für jedes y . Im Falle $y \neq x$ erhalten wir mit $y^\tau = y^\sigma$ und wegen $x \notin \text{var } y^\sigma$ daher

$$y^{(\mathcal{M}_x^a)^\tau} = y^{\tau\mathcal{M}_x^a} = y^{\sigma\mathcal{M}_x^a} = y^{\sigma\mathcal{M}} = y^{\mathcal{M}^\sigma} = y^{(\mathcal{M}^\sigma)_x^a}.$$

Ebenso ist wegen $x^\tau = x$ aber auch $x^{(\mathcal{M}_x^a)^\tau} = x^{\tau\mathcal{M}_x^a} = x^{\sigma\mathcal{M}_x^a} = x^{\mathcal{M}^\sigma} = x^{(\mathcal{M}^\sigma)_x^a}$. \square

Korollar 3.6. Für alle φ und $\frac{t}{x}$, für die $\varphi, \frac{t}{x}$ kollisionsfrei sind, gelten

- (a) $\forall \vec{x} \varphi \models \varphi_{\vec{x}}^{\vec{t}}$, und damit speziell $\forall x \varphi \models \varphi_{\vec{x}}^{\vec{t}}$, (b) $\varphi_{\vec{x}}^{\vec{t}} \models \exists \vec{x} \varphi$,
 (c) $\varphi_{\vec{x}}^{\vec{s}}, s=t \models \varphi_{\vec{x}}^{\vec{t}}$, falls $\varphi, \frac{s}{x}, \frac{t}{x}$ kollisionsfrei sind.

Beweis. Sei $\mathcal{M} \models \forall \vec{x} \varphi$, also $\mathcal{M}_{\vec{a}}^{\vec{a}} \models \varphi$ für alle $\vec{a} \in A^n$. Insbesondere $\mathcal{M}_{\vec{x}}^{\vec{t}} \models \varphi$, daher $\mathcal{M} \models \varphi_{\vec{x}}^{\vec{t}}$ nach dem Satz. (b) ist gleichwertig mit $\neg \exists \vec{x} \varphi \models \neg \varphi_{\vec{x}}^{\vec{t}}$. Dies gilt nach (a), weil $\neg \exists \vec{x} \varphi \equiv \forall \vec{x} \neg \varphi$ und $\neg(\varphi_{\vec{x}}^{\vec{t}}) \equiv (\neg \varphi)_{\vec{x}}^{\vec{t}}$. (c): Sei $\mathcal{M} \models \varphi_{\vec{x}}^{\vec{s}}, s=t$, so dass $s^{\mathcal{M}} = t^{\mathcal{M}}$ und $\mathcal{M}_{\vec{x}}^{\vec{s}} \models \varphi$ nach dem Satz. Dann gilt auch $\mathcal{M}_{\vec{x}}^{\vec{t}} \models \varphi$ und somit $\mathcal{M} \models \varphi_{\vec{x}}^{\vec{t}}$. \square

Bemerkung 2. Weil ι mit jeder Formel kollisionsfrei ist, gilt stets $\forall x \varphi \models \varphi (= \varphi')$. Ferner ist $\forall x \varphi \models \varphi_{\vec{x}}^{\vec{t}}$ uneingeschränkt richtig, falls t höchstens die Variable x enthält. Denn dann sind $\varphi, \frac{t}{x}$ kollisionsfrei. Satz 3.5 und das Korollar lassen sich leicht verschärfen. Man definiert rekursiv ein dreistelliges Prädikat ‘ t ist frei für x in φ ’, oder ‘ t ist substituierbar für x in φ ’. Dies soll anschaulich heißen, dass die Variable x an keiner Stelle ihres freien Vorkommens in φ im Wirkungsbereich eines Präfixes $\forall y$ mit $y \in \text{var } t$ steht. Satz 3.5 gilt unverändert, so dass sich in allen folgenden Beweisen nichts ändert, wenn man mit dieser Bedingung arbeitet oder ‘ $\varphi, \frac{t}{x}$ sind kollisionsfrei’ einfach liest als ‘ t ist substituierbar für x in φ ’. Die Kollisionsfreiheit ist zwar etwas gröber, dafür aber handlicher, was sich z.B. bei der Gödelisierung des Beweises in 6.2 auszahlt. Nach einer gewissen Gewöhnungsphase darf man sich erlauben, die durch Variablenkollision verursachten Einschränkungen nicht immer explizit anzugeben, sondern stillschweigend als gegeben anzunehmen.

Satz 3.5 ergibt auch, dass der mit $\exists!$ bezeichnete Quantor „es gibt genau ein“ durch

$$\exists! x \varphi := \exists x \varphi \wedge \forall xy (\varphi \wedge \varphi_{\vec{x}}^{\vec{y}} \rightarrow x=y) \quad (y \notin \text{var } \varphi)$$

richtig definiert wird, d.h. $\mathcal{M} \models \exists! x \varphi \Leftrightarrow$ es gibt genau ein $a \in A$ mit $\mathcal{M}_x^a \models \varphi$. Es gibt verschiedene formale Definitionen von $\exists! x \varphi$. Die wohl kürzeste definierende Formel ist $\exists x \forall y (\varphi_{\vec{x}}^{\vec{y}} \leftrightarrow x=y)$, mit $y \notin \text{var } \varphi$.

Übungen

1. Man zeige $\forall x \alpha, \forall x (\alpha \rightarrow \beta) \models \forall x \beta$. Damit gilt auch $\models \forall x (\alpha \rightarrow \beta) \rightarrow \forall x \alpha \rightarrow \forall x \beta$.
2. Man beweise $\exists xy (\varphi \wedge \varphi_{\vec{x}}^{\vec{y}} \wedge x \neq y) \models \forall x \exists y (\varphi_{\vec{x}}^{\vec{y}} \wedge x \neq y)$ ($y \notin \text{var } \varphi$).
3. \mathcal{A}' entstehe aus \mathcal{A} durch Aufnahme eines Konstantensymbols \mathbf{a} für ein $a \in A$. Man beweise $t(x)^{\mathcal{A}, a} = t(\mathbf{a})^{\mathcal{A}'}$ und $\mathcal{A} \models \alpha[a] \Leftrightarrow \mathcal{A}' \models \alpha(\mathbf{a})$ für $\alpha = \alpha(x)$.
4. Man zeige (a) eine Konjunktion aus den \exists_i und ihren Negationen ist äquivalent zu $\exists_n, \neg \exists_n$ oder $\exists_n \wedge \neg \exists_m$ für passende n, m . Damit verifiziere man (b): eine Boolesche Kombination der \exists_i ist äquivalent zu $\bigvee_{\nu \leq n} \exists_{=k_\nu} \vee \exists_m$, wobei $0 \leq k_0 < \dots < k_n$, $n < m$ und das Glied \exists_m auch fehlen kann.

2.4 Allgemeingültigkeit und logische Äquivalenz

Aus prädikatenlogischer Perspektive ist z.B. $\alpha \vee \neg\alpha$ für $\alpha \in \mathcal{L}$ ein triviales Beispiel einer Tautologie, weil sie aus der aussagenlogischen Tautologie $p \vee \neg p$ durch Einsetzung von α für p entstand. Jede aussagenlogische Tautologie liefert durch Einsetzung von \mathcal{L} -Formeln für die Aussagenvariablen allgemeingültige \mathcal{L} -Formeln. Aber es gibt auch Tautologien, die so nicht entstehen, wie etwa $\forall x(x < x \vee x \not< x)$. Diese entstand immerhin aus der Tautologie $x < x \vee x \not< x$ durch Generalisierung. So erzeugt man jedoch z.B. nicht die Tautologien $\exists x x = x$ und $\exists x x = t$. Erstere ist der Vereinbarung zu verdanken, dass Strukturen stets nichtleer sind, letztere der totalen Definiertheit der Basisoperationen. Hier ein weiteres lehrreiches Beispiel einer Tautologie.

Beispiel (die Russellsche Antinomie). Wir zeigen $\models \neg\exists u\forall x(x \in u \leftrightarrow x \notin x)$, die Nichtexistenz der „Russellschen Menge“ u , bestehend aus allen Mengen, die sich nicht selbst als Elemente enthalten (siehe auch 3.4). Unser Nachweis wird an keiner Stelle davon Gebrauch machen, dass \in die Elementbeziehung bedeutet. Nach Korollar 3.6(a) ist $\forall x(x \in u \leftrightarrow x \notin x) \models u \in u \leftrightarrow u \notin u$. Nun ist mit $u \in u \leftrightarrow u \notin u$ sicher auch $\forall x(x \in u \leftrightarrow x \notin x)$ unerfüllbar. Dann aber auch $\exists u\forall x(x \in u \leftrightarrow x \notin x)$. Daher ist $\neg\exists u\forall x(x \in u \leftrightarrow x \notin x)$ eine Tautologie. Die Antinomie ist hier die Erwartung, dass jede Mengenbildung, also auch $\exists u\forall x(x \in u \leftrightarrow x \notin x)$, eigentlich erlaubt sein sollte.

Die Erfüllungsklausel für $\alpha \rightarrow \beta$ ergibt leicht $\alpha \models \beta \Leftrightarrow \models \alpha \rightarrow \beta$, ein Spezialfall von $X, \alpha \models \beta \Leftrightarrow X \models \alpha \rightarrow \beta$. Dies kann nützlich sein um zu prüfen, ob in implikativer Gestalt gegebene Formeln Tautologien sind, worauf in 1.3 schon hingewiesen wurde. So erhält man aus $\forall x \alpha \models \alpha \stackrel{t}{x}$ sofort $\models \forall x \alpha \rightarrow \alpha \stackrel{t}{x}$ für kollisionsfreie $\alpha, \stackrel{t}{x}$.

Genau wie in der Aussagenlogik ist die prädikatenlogische Äquivalenz \equiv eine Äquivalenzrelation in \mathcal{L} und darüber hinaus offenbar eine *Kongruenz*. Ganz allgemein heißt eine Äquivalenzrelation \approx in \mathcal{L} mit der Eigenschaft

$$\text{CP: } \alpha \approx \alpha', \beta \approx \beta' \Rightarrow \alpha \wedge \beta \approx \alpha' \wedge \beta', \neg\alpha \approx \neg\alpha', \forall x \alpha \approx \forall x \alpha'.$$

eine *Kongruenz in \mathcal{L}* . Aus Satz 4.1 unten folgt leicht, dass CP für alle definierten Junktoren wie \rightarrow und \exists beweisbar ist, also etwa $\alpha \equiv \alpha' \Rightarrow \exists x \alpha \equiv \exists x \alpha'$.

Wie in der Aussagenlogik ist auch jetzt $\alpha \equiv \beta$ wieder gleichwertig mit $\models \alpha \leftrightarrow \beta$. Durch Einsetzung von \mathcal{L} -Formeln für die Variablen einer aussagenlogischen Äquivalenz gewinnt man automatisch eine prädikatenlogische. So ist z.B. $\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta$, weil schon $p \rightarrow q \equiv \neg p \vee q$. Da jede \mathcal{L} -Formel durch Einsetzungen aussagenlogisch unzerlegbarer \mathcal{L} -Formeln in eine aussagenlogische Formel entsteht, erkennt man auch leicht, dass sich jede \mathcal{L} -Formel in eine konjunktive Normalform überführen lässt. Es gibt aber auch zahlreiche neue Äquivalenzen, z.B. $\neg\forall x \alpha \equiv \exists x \neg\alpha$ und $\neg\exists x \alpha \equiv \forall x \neg\alpha$.

Ersteres folgt aus $\neg\forall x\alpha \equiv \neg\forall x\neg\neg\alpha (= \exists x\neg\alpha)$, einem Anwendungsfall von Satz 4.1, Letzteres in analoger Weise. Dieser Satz wird ständig verwendet aber fast nirgends explizit zitiert, ähnlich wie bei arithmetischen Termumformungen die dabei benutzten Rechengesetze fast niemals explizit genannt werden.

Satz 4.1 (Ersetzungstheorem). *Sei \approx eine Kongruenz in \mathcal{L} und sei $\alpha \approx \alpha'$. Entsteht φ' aus φ dadurch, dass die Formel α an einer oder mehreren Stellen ihres eventuellen Vorkommens in φ durch α' ersetzt wird, ist auch $\varphi \approx \varphi'$.*

Beweis durch Induktion über φ . Sei φ Primformel. Sowohl für $\varphi = \alpha$ als auch $\varphi \neq \alpha$ gilt offenbar $\varphi \approx \varphi'$. Sei nun $\varphi = \varphi_1 \wedge \varphi_2$. Für $\varphi = \alpha$ ist trivialerweise $\varphi \approx \varphi'$. Sonst ist $\varphi' = \varphi'_1 \wedge \varphi'_2$, wobei φ'_1, φ'_2 aus φ_1, φ_2 durch eventuelle Ersetzung entstehen. Nach Induktionsannahme ist $\varphi_1 \approx \varphi'_1$ und $\varphi_2 \approx \varphi'_2$ und daher $\varphi = \varphi_1 \wedge \varphi_2 \approx \varphi'_1 \wedge \varphi'_2 = \varphi'$ gemäß CP. Analog schließt man in den Induktionsschritten über \neg und \forall . \square

Prädikatenlogische Sprachen sind feiner strukturiert als aussagenlogische. Daher gibt es weitere interessante Kongruenzen in \mathcal{L} . So heißen α, β *äquivalent in einer Struktur \mathcal{A}* , symbolisch $\alpha \equiv_{\mathcal{A}} \beta$, wenn $\mathcal{A} \models \alpha[w] \Leftrightarrow \mathcal{A} \models \beta[w]$ für alle w . Der Nachweis der Kongruenzeigenschaft CP ist sehr einfach und sei dem Leser überlassen. $\alpha \equiv_{\mathcal{A}} \beta$ ist gleichwertig mit $\mathcal{A} \models \alpha \leftrightarrow \beta$. So sind in $\mathcal{A} = (\mathbb{N}, <, +, 0)$ z.B. die Formeln $x < y$ und $\exists z (z \neq 0 \wedge x + z = y)$ äquivalent. Weil $\equiv \subseteq \equiv_{\mathcal{A}}$, übertragen sich Eigenschaften wie z.B. $\neg\forall x\alpha \equiv \exists x\neg\alpha$ von \equiv unmittelbar auf $\equiv_{\mathcal{A}}$. Oft gibt es in bestimmten Strukturen oder Theorien jedoch neue interessante Äquivalenzen. So ist in gewissen Strukturen jede Formel zu einer quantorenfreien äquivalent, siehe 5.6.

Es ist eine sehr wichtige Tatsache mit einem fast banalen Beweis, dass der Durchschnitt einer Familie von Kongruenzen wieder eine Kongruenz ist. Folglich ist für eine beliebige Klasse $\mathbf{K} \neq \emptyset$ von \mathcal{L} -Strukturen $\equiv_{\mathbf{K}} := \bigcap \{\equiv_{\mathcal{A}} \mid \mathcal{A} \in \mathbf{K}\}$ immer eine Kongruenz. Für die Klasse \mathbf{K} aller \mathcal{L} -Strukturen ist $\equiv_{\mathbf{K}}$ mit der logischen Äquivalenz \equiv identisch, mit der wir uns im Rest dieses Abschnitt ausschließlich befassen. Nachfolgend seien ihre wichtigsten Eigenschaften aufgelistet. Diese sollte man sich fest einprägen, weil sie bei Anwendungen nur selten zitiert werden.

$$\begin{aligned} (1) \quad & \forall x(\alpha \wedge \beta) \equiv \forall x\alpha \wedge \forall x\beta, & (2) \quad & \exists x(\alpha \vee \beta) \equiv \exists x\alpha \vee \exists x\beta, \\ (3) \quad & \forall x\forall y\alpha \equiv \forall y\forall x\alpha, & (4) \quad & \exists x\exists y\alpha \equiv \exists y\exists x\alpha. \end{aligned}$$

Falls x in der Formel β nicht frei vorkommt, gelten darüber hinaus

$$\begin{aligned} (5) \quad & \forall x(\alpha \vee \beta) \equiv \forall x\alpha \vee \beta, & (6) \quad & \exists x(\alpha \wedge \beta) \equiv \exists x\alpha \wedge \beta, \\ (7) \quad & \forall x\beta \equiv \beta, & (8) \quad & \exists x\beta \equiv \beta, \\ (9) \quad & \forall x(\alpha \rightarrow \beta) \equiv \exists x\alpha \rightarrow \beta, & (10) \quad & \exists x(\alpha \rightarrow \beta) \equiv \forall x\alpha \rightarrow \beta. \end{aligned}$$

Die einfachen Beweise seien dem Leser überlassen. (7) und (8) wurden in Korollar 3.3 formuliert. Nur (9) und (10) überraschen auf den ersten Anblick und sollten daher

sehr sorgfältig überprüft werden. Man benutzt diese Äquivalenzen auch im praktischen Schließen sehr häufig. Betrachten wir für gegebenes $X \subseteq \mathcal{L}$ etwa die (wahre) metalogische Aussage ‘Für alle α : wenn $X \models \alpha$, $\neg\alpha$, so $X \models \forall x x \neq x$ ’. Diese ist mit ‘Wenn es ein α gibt mit $X \models \alpha$, $\neg\alpha$, so ist $X \models \forall x x \neq x$ ’ äquivalent. Ein markantes Beispiel ist auch $\forall x(x \sim y \wedge x \sim z \rightarrow y \sim z) \equiv \exists x(x \sim y \wedge x \sim z) \rightarrow y \sim z$.

Bemerkung. In der Umgangssprache bleiben Variablen meist unquantifiziert. In zahlreichen Fällen ergibt sich sogar der gleiche Sinn, ob man nun mit „es gibt ein“ oder mit „für alle“ quantifiziert. Man betrachte etwa die drei folgenden Aussagen, die offenbar dasselbe besagen und von denen die letzten beiden der Äquivalenz (9) entsprechen:

- Wenn ein Jurist eine Lücke im Gesetz findet, so muss dieses verändert werden.
- Wenn es einen Juristen gibt, der eine Lücke im Gesetz findet, muss dieses verändert werden.
- Für alle Juristen: wenn einer von diesen eine Lücke im Gesetz findet, muss dieses verändert werden.

Oft ergibt sich die Art der Quantifizierungen in sprachlichen Mitteilungen erst aus den Kontext, was nicht selten zu unbeabsichtigten (oder beabsichtigten) Missverständnissen führt. „Die logischen Verhältnisse werden durch die Sprache fast immer nur angedeutet, dem Erraten überlassen, nicht eigentlich ausgedrückt“ (Gottlob Frege, Über die Wissenschaftliche Berechtigung einer Begriffsschrift, Zeitschr. Phil. & Phil. Kritik 81 (1882)).

Zu den wichtigsten logischen Äquivalenzen zählt die *gebundene Umbenennung*

$$(11) \quad (a) \forall x \alpha \equiv \forall y \alpha \frac{y}{x}, \quad (b) \exists x \alpha \equiv \exists y \alpha \frac{y}{x} \quad (y \notin \text{var } \alpha).$$

(b) folgt aus (a) leicht durch äquivalente Umformung. (a) ergibt sich folgendermaßen:

$$\begin{aligned} \mathcal{M} \models \forall x \alpha &\Leftrightarrow \mathcal{M}_x^a \models \alpha \text{ für alle } a \\ &\Leftrightarrow \mathcal{M}_{y \frac{a}{x}}^a \models \alpha \text{ für alle } a \quad (\text{Satz 3.1; } y \notin \text{var } \alpha) \\ &\Leftrightarrow \mathcal{M}_{y \frac{y}{x}}^a \models \alpha \text{ für alle } a \quad (\text{weil } \mathcal{M}_{y \frac{y}{x}}^a = (\mathcal{M}_y^a)_x^{\mathcal{M}_y^a} = \mathcal{M}_{y \frac{a}{x}}^a) \\ &\Leftrightarrow \mathcal{M}_y^a \models \alpha \frac{y}{x} \text{ für alle } a \quad (\text{Satz 3.5; } \alpha, \frac{y}{x} \text{ sind kollisionsfrei}) \\ &\Leftrightarrow \mathcal{M} \models \forall y \alpha \frac{y}{x}. \end{aligned}$$

Bemerkenswert sind auch (12) und (13). Nach (13) werden Substitutionen durch *freie Umbenennungen* (Substitutionen der Gestalt $\frac{y}{x}$) bis auf logische Äquivalenz vollständig beschrieben. Man beachte, (13) umfasst auch den Fall $x \in \text{var } t$.

$$(12) \quad \forall x(x=t \rightarrow \alpha) \equiv \alpha \frac{t}{x} \equiv \exists x(x=t \wedge \alpha) \quad (\alpha, \frac{t}{x} \text{ kollisionsfrei, } x \notin \text{var } t).$$

$$(13) \quad \forall y(y=t \rightarrow \alpha \frac{y}{x}) \equiv \alpha \frac{t}{x} \equiv \exists y(y=t \wedge \alpha \frac{y}{x}) \quad (\alpha, \frac{t}{x} \text{ kollisionsfrei, } y \notin \text{var } \alpha, t).$$

Nachweis von (12): $\forall x(x=t \rightarrow \alpha) \models (x=t \rightarrow \alpha) \frac{t}{x} = t=t \rightarrow \alpha \frac{t}{x} \models \alpha \frac{t}{x}$ gemäß Korollar 3.6. Sei umgekehrt $\mathcal{M} \models \alpha \frac{t}{x}$, also $\mathcal{M}_x^t \models \alpha$ sowie $a \in A$. Falls $\mathcal{M}_x^a \models x=t$, ist $a = t^{\mathcal{M}}$, daher auch $\mathcal{M}_x^a \models \alpha$. Das zeigt $\mathcal{M}_x^a \models x=t \rightarrow \alpha$ für beliebiges $a \in A$, d.h. $\mathcal{M} \models \forall x(x=t \rightarrow \alpha)$. Dies beweist die linke Äquivalenz. Für die rechte beachte

man $\exists x(x=t \wedge \alpha) = \neg \forall x \neg(x=t \wedge \alpha) \equiv \neg \forall x(x=t \rightarrow \neg \alpha) \equiv \neg(\neg \alpha \frac{t}{x}) \equiv \alpha \frac{t}{x}$ nach dem soeben Bewiesenen. (13) beweist man analog: Nach Korollar 3.6 und Übung 1 in 2.2 ist $\forall y(y=t \rightarrow \alpha \frac{y}{x}) \models \alpha \frac{y}{x} \frac{t}{y} = \alpha \frac{t}{x}$. Ferner beachte man $\alpha \frac{t}{x} \models y=t \rightarrow \alpha \frac{y}{x}$.

Mit den bislang angegebenen Äquivalenzen lässt sich nun eine Formel α äquivalent so umformen, dass alle Quantoren am Beginn der Formel stehen. Dazu benötigt man allerdings beide, nachfolgend mit Q, Q_1, Q_2, \dots bezeichneten Quantoren.

Eine Formel der Gestalt $\alpha = Q_1 x_1 \cdots Q_n x_n \beta$ mit quantorenfreiem β , dem *Kern* von α , heißt eine *pränexe Formel* oder eine *pränexe Normalform*, kurz, eine PNF. Die x_1, \dots, x_n seien o.B.d.A. paarweise verschieden, was durch Weglassen überflüssiger Quantoren gemäß (2) Seite 53 erreichbar ist. \forall -Formeln und \exists -Formeln sind Beispiele pränexer Normalformen, die ein wichtiges Hilfsmittel zur Klassifikation definierbarer Prädikate sind. Anwendungen dieser Art beruhen auf folgendem

Satz 4.2 (von der pränexen Normalform). *Jede Formel φ ist äquivalent zu einer Formel in pränexer Normalform, die sich aus φ effektiv herstellen lässt.*

Beweis. Wir betrachten für jedes Präfix Qx in φ die Anzahl der vor Qx stehenden Symbole \neg, \wedge . Sei $s\varphi$ die Summe aus diesen Zahlen, summiert über alle Präfixe in φ . Offenbar ist φ genau dann eine PNF, wenn $s\varphi = 0$ ist. Sei $s\varphi \neq 0$. Wegen

$$\neg \forall x \alpha \equiv \exists x \neg \alpha, \quad \neg \exists x \alpha \equiv \forall x \neg \alpha, \quad \beta \wedge Qx \alpha \equiv Qy(\beta \wedge \alpha \frac{y}{x}) \text{ für } y \notin \text{var } \alpha, \beta$$

kann $s\varphi$ durch äquivalente Ersetzung offenbar schrittweise verkleinert werden. \square

Für $\varphi = \forall x(x \neq 0 \rightarrow \exists y x \cdot y = 1)$ z.B. ist $\forall x \exists y(x \neq 0 \rightarrow x \cdot y = 1)$ eine äquivalente PNF. φ wird oft durch $(\forall x \neq 0) \exists y x \cdot y = 1$ abgekürzt, ebenso wie $\exists x(x \neq t \wedge \alpha)$ durch $(\exists x \neq t)\alpha$. Analoge Notationen benutzt man auch bei $<, \in, \notin$ usw. Allgemein sei $(\forall x \triangleleft t)\alpha := \forall x(x \triangleleft t \rightarrow \alpha)$ und $(\exists x \triangleleft t)\alpha := \exists x(x \triangleleft t \wedge \alpha)$, wobei \triangleleft hier ein beliebiges 2-stelliges Relationssymbol vertritt und t ein Term der Sprache ist. Übung 2 zeigt, dass $(\forall x \triangleleft t)$ und $(\exists x \triangleleft t)$ sich dual zueinander verhalten, ganz wie \forall und \exists .

Übungen

1. Sei $\alpha \equiv \beta$. Man beweise $\alpha \frac{\vec{t}}{x} \equiv \beta \frac{\vec{t}}{x}$ ($\alpha, \frac{\vec{t}}{x}$ und $\beta, \frac{\vec{t}}{x}$ kollisionsfrei).
2. Man beweise $\neg(\forall x \triangleleft t)\alpha \equiv (\exists x \triangleleft t)\neg \alpha$ und $\neg(\exists x \triangleleft t)\alpha \equiv (\forall x \triangleleft t)\neg \alpha$.
3. Man zeige, die Konjunktion und Disjunktion zweier \forall -Formeln α, β ist äquivalent zu einer \forall -Formel. Dasselbe beweise man für \exists -Formeln.
4. $\alpha, \beta \in \mathcal{L}$ heißen *allgemeingültigkeitsgleich*, wenn $\models \alpha \Leftrightarrow \models \beta$. Man bestätige diese Eigenschaft für die drei (in der Regel nicht logisch äquivalenten) Formeln $\alpha, \forall x \alpha$ und $\alpha \frac{c}{x}$. Dabei komme das Konstantensymbol c in α nicht vor.

2.5 Logisches Folgern und der Theoriebegriff

Wir erinnern an die in **2.3** schon erwähnte Unempfindlichkeit des Folgerns gegenüber Spracherweiterung. Ist $\mathcal{L}' \supseteq \mathcal{L}$, so heißt die Sprache \mathcal{L}' eine *Expansion* oder *Erweiterung* der Sprache \mathcal{L} sowie \mathcal{L} ein *Redukt* oder eine *Einschränkung* von \mathcal{L}' . Satz 3.1 ergibt leicht, dass die Feststellung $X \models \alpha$ gänzlich unabhängig davon ist, welcher Sprache die Formelmengende X und die Formel α angehören. Eine Indizierung von \models etwa in der Weise $\models_{\mathcal{L}}$ kann aus diesem Grunde unterbleiben.

Wegen der unveränderten Erfüllungsbedingungen für die Junktoren \wedge, \neg gelten alle Eigenschaften des aussagenlogischen Folgerns auch für das prädikatenlogische Folgeren. Insbesondere gelten die den Regeln $(\wedge 1)$, $(\wedge 2)$, $(\neg 1)$, $(\neg 2)$ entsprechenden Eigenschaften $\frac{X \models \alpha, \beta}{X \models \alpha \wedge \beta}$ ⁷⁾ usw. Damit übertragen sich automatisch alle hieraus gewonnenen Eigenschaften wie etwa das Deduktionstheorem. Unverändert gelten ferner die in **1.3** erwähnte Reflexivität und Transitivität von \models . Aber es gibt auch neue, vorher nicht formulierbare Eigenschaften wie die folgenden

Beispiele prädikatenlogischer Folgerungseigenschaften

- (a) $\frac{X \models \forall x \alpha}{X \models \alpha \frac{t}{x}}$ ($\alpha, \frac{t}{x}$ kollisionsfrei), (b) $\frac{X \models \alpha \frac{s}{x}, s=t}{X \models \alpha \frac{t}{x}}$ ($\alpha, \frac{s}{x}$ und $\alpha, \frac{t}{x}$ kollisionsfrei),
- (c) $\frac{X, \beta \models \alpha}{X, \forall x \beta \models \alpha}$ (vordere Generalisierung), (d) $\frac{X \models \alpha}{X \models \forall x \alpha}$ ($x \notin \text{frei } X$, hintere Generalisierung),
- (e) $\frac{X, \beta \models \alpha}{X, \exists x \beta \models \alpha}$ ($x \notin \text{frei } X, \alpha$, vordere Partikularisierung), (f) $\frac{X \models \alpha \frac{t}{x}}{X \models \exists x \alpha}$ ($\alpha, \frac{t}{x}$ kollisionsfrei, hintere Partikul.).

Weil \models transitiv ist, genügt für den Nachweis von (a) und (b) der von $\forall x \alpha \models \alpha \frac{t}{x}$ und von $\alpha \frac{s}{x}, s=t \models \alpha \frac{t}{x}$. Beides formuliert Korollar 3.6. Aus $\forall x \beta \models \beta$ ergibt sich (c). Zum Nachweis von (d) sei $X \models \alpha$, $\mathcal{M} \models X$ und $x \notin \text{frei } X$. Dann ist $\mathcal{M}_x^a \models X$, also auch $\mathcal{M}_x^a \models \alpha$, für jedes $a \in A$ nach Satz 3.1. Folglich $\mathcal{M} \models \forall x \alpha$. Für (e) beachte man $X, \beta \models \alpha \Rightarrow X, \neg \alpha \models \neg \beta \Rightarrow X, \neg \alpha \models \forall x \neg \beta$ nach einer der Kontrapositionsregeln und gemäß (d), daher $X, \neg \forall x \neg \beta \models \alpha$. Eigenschaft (e) erfasst das Schließen aus einer Existenzaussage, siehe hierzu das Beispiel auf Seite 63. Schließlich gilt (f), weil $\alpha \frac{t}{x} \models \exists x \alpha$ nach Korollar 3.6. Alle diese Eigenschaften haben gewisse Varianten, z.B. (d) die folgende, die sich wegen $\forall y \alpha \frac{y}{x} \equiv \forall x \alpha$ aus (d) ergibt:

- (g) $\frac{X \models \alpha \frac{y}{x}}{X \models \forall x \alpha}$ ($y \notin \text{frei } X \cup \text{var } \alpha$).

⁷⁾Dies ist eine einprägsame in **1.3** schon benutzte Schreibweise für „ $X \models \alpha, \beta$ impliziert $X \models \alpha \wedge \beta$ “, die auch in den Beispielen weiter unten und den entsprechenden Regeln verwendet wird.

Mit diesen Eigenschaften, von denen einige in Kapitel 3 zu Basisregeln eines Logikkalküls erhoben werden, lassen sich komplizierte Schlussketten notfalls Schritt für Schritt rechtfertigen. In der Praxis ist dies aber nur in besonderen Fällen sinnvoll. Denn formalisierte Beweise sind nur mit hohem Zeitaufwand lesbar, ähnlich wie längliche Computerprogramme.

Bei der Niederschrift eines Beweises kommt es vor allem darauf an, dass er verstanden und reproduziert werden kann. Deswegen vollzieht sich mathematisches Schließen überwiegend *informell*, d.h. sowohl die Behauptungen als auch deren Beweise werden unter Zuhilfenahme einer flexiblen Formalisierung in allgemein verständlicher mathematischer Umgangssprache formuliert. Der Grad der Formalisierung bei der Ausführung eines Beweises ist situationsbedingt und muss nicht von vornherein bestimmt sein. Hierdurch werden die strengen syntaktischen Strukturen formaler Beweise aufgebrochen, was die Unvollkommenheiten unseres Gehirns in Bezug auf syntaktische Informationsverarbeitung recht gut kompensiert. Auch werden beim informellen Schließen gewisse Beweisschritte oft mit mehr oder weniger deutlich formulierten Appellen an das sogenannte Hintergrundwissen nur beschrieben, nicht eigentlich ausgeführt. Diese Methode hat sich als ausreichend zuverlässig erwiesen. Sie ist, von Spezialfällen abgesehen, bislang von keinem der existierenden automatischen Beweiser erreicht worden. Hier ein einfaches Beispiel eines informellen Beweises in einer Sprache \mathcal{L} über natürliche Zahlen, die nebst $0, 1, +, \cdot$ das Symbol $|$ für die durch $m|n \leftrightarrow \exists k m \cdot k = n$ definierte Teilbarkeitsrelation enthalte, und ein Symbol c für eine beliebige Funktion von \mathbb{N} nach \mathbb{N} ; wir schreiben c_i für $c(i)$.

Beispiel. Es soll $\forall n \exists x (\forall i \leq n) c_i | x$ bewiesen werden, d.h. für jedes n haben c_0, \dots, c_n ein gemeinsames Vielfaches. Der Beweis erfolgt üblicherweise induktiv über n , wobei wir uns ganz auf den Induktionsschritt $X, \exists x (\forall i \leq n) c_i | x \models \exists x (\forall i \leq n+1) c_i | x$ konzentrieren. Dabei repräsentiert X hier unser Vorwissen, z.B. über die Eigenschaften der Teilbarkeit. Informel schließt man wie folgt: Sei $\exists x (\forall i \leq n) c_i | x$ angenommen und etwa x gemeinsames Vielfaches von c_0, \dots, c_n . Dann ist $x \cdot c_{n+1}$ offenbar gemeinsames Vielfaches von c_0, \dots, c_{n+1} , also gilt auch $\exists x (\forall i \leq n+1) c_i | x$. Hier wurde die hintere Partikularisierung (f) mit $X, (\forall i \leq n) c_i | x$ für X , sowie $\alpha = (\forall i \leq n+1) c_i | x$ und $t = x \cdot c_{n+1}$ benutzt, und anschließend die vordere Partikularisierung.

In einigen Lehrbüchern wird eine etwas strengere, wie folgt erklärte und hier mit \vDash bezeichnete Folgerungsrelation bevorzugt, die man im Unterschied zur *lokalen* Folgerungsrelation \models als die *globale* bezeichnen könnte: Für $X \subseteq \mathcal{L}$ und $\varphi \in \mathcal{L}$ sei $X \vDash \varphi$, falls $\mathcal{A} \models \varphi$ für alle \mathcal{L} -Strukturen \mathcal{A} mit $\mathcal{A} \models X$. Der Grund ist, dass man in der Mathematik überwiegend mit dem Folgern in Theorien zu tun hat. Bevor wir hierauf näher eingehen, stellen wir einige Eigenschaften von \vDash zusammen. Nach (a) und (d) oben folgt eine Formel aus einer *Aussagenmenge* – z.B. einem

Axiomensystem – im lokalen Sinne genau dann, wenn ihre Generalisierte daraus folgt. Diese Eigenschaft hat \vDash^{\forall} schlechthin. Denn die Definition ergibt für beliebige Formelmengen X leicht $X \vDash^{\forall} \varphi \Leftrightarrow X \vDash^{\forall} \varphi^{\forall}$. Es gilt stets $X \vDash \varphi \Rightarrow X \vDash^{\forall} \varphi$, i.a. aber nicht umgekehrt. So ist z.B. $x=y \vDash^{\forall} \forall xy x=y$, nicht aber $x=y \vDash \forall xy x=y$. Eine Reduktion von \vDash^{\forall} auf \vDash wird geliefert durch

$$(1) \quad X \vDash^{\forall} \varphi \Leftrightarrow X^{\forall} \vDash \varphi.$$

Das folgt leicht aus $\mathcal{M} \vDash X^{\forall} \Leftrightarrow \mathcal{A} \vDash X^{\forall}$, für beliebige Modelle $\mathcal{M} = (\mathcal{A}, w)$. Für Aussagenmengen S ergibt (1) wegen $S^{\forall} = S$ offenbar

$$(2) \quad S \vDash \varphi \Leftrightarrow S \vDash^{\forall} \varphi.$$

Ein Unterschied zwischen \vDash und \vDash^{\forall} zeigt sich nur dann, wenn man mit Prämissen zu tun hat, die keine Aussagen sind. In einer solchen Situation ist mit der Relation \vDash^{\forall} äußerst vorsichtig umzugehen. Denn es gelten weder die Fallunterscheidungsregel $(-2) \frac{X, \alpha \vDash^{\forall} \beta \mid X, \neg \alpha \vDash^{\forall} \beta}{X \vDash^{\forall} \beta}$ noch das Deduktionstheorem $\frac{X, \alpha \vDash^{\forall} \beta}{X \vDash^{\forall} \alpha \rightarrow \beta}$ uneingeschränkt.

So gilt z.B. $x=y \vDash^{\forall} \forall xy x=y$, nicht jedoch $\vDash^{\forall} x=y \rightarrow \forall xy x=y$. Während \vDash die aussagenlogische Folgerungsrelation in dem Sinne konservativ erweitert, dass sich Eigenschaften wie etwa das Deduktionstheorem auf \vDash uneingeschränkt übertragen, ist dies für \vDash^{\forall} nicht mehr der Fall. Auch widerspiegelt \vDash^{\forall} nur unvollkommen die tatsächlichen Abläufe des natürlichen Schließens, in denen auch bei Deduktionen von Aussagen aus Aussagen ständig Formeln mit freien Variablen benutzt werden.

Wir präzisieren nun den Begriff einer in \mathcal{L} formalisierten Theorie, wobei man an die Beispiele aus 2.3 denken möge, etwa die Gruppentheorie.

Definition. Eine *elementare Theorie* oder eine *Theorie der 1. Stufe* in \mathcal{L} , auch eine \mathcal{L} -Theorie genannt, sei eine in \mathcal{L}^0 deduktiv abgeschlossene Menge $T \subseteq \mathcal{L}^0$ von Aussagen, d.h. $T \vDash \alpha \Leftrightarrow \alpha \in T$, für alle $\alpha \in \mathcal{L}^0$. Ist $\alpha \in T$, sagt man α *gilt in* T oder α *ist ein Satz* von T . Die nichtlogischen Symbole von \mathcal{L} heißen die Symbole von T . Falls $T \subseteq T'$, heißt T auch eine *Subtheorie* von T' , und T' eine *Erweiterung* von T . Eine \mathcal{L} -Struktur \mathcal{A} mit $\mathcal{A} \vDash T$ heißt auch ein *Modell von* T , oder kurz ein *T -Modell*. $\text{Md } T$ bezeichne die Klasse aller Modelle von T in diesem Sinne.

Für jede Aussagenmenge S ist z.B. $\{\alpha \in \mathcal{L}^0 \mid S \vDash \alpha\}$ offenbar eine Theorie. Der erweiterte Modellbegriff für Theorien T ist sehr sinnvoll. Denn für herkömmliche Modelle $\mathcal{M} = (\mathcal{A}, w)$ gilt $\mathcal{M} \vDash T \Leftrightarrow \mathcal{A} \vDash T$, weil w für die Erfüllung von Aussagen belanglos ist. Offenbar ist $\alpha \in T$ genau dann, wenn $\mathcal{A} \vDash \alpha$ für alle $\mathcal{A} \vDash T$. Nach (2) gibt es keinen Unterschied zwischen \vDash und \vDash^{\forall} , was das Folgern aus Theorien anbelangt. Für beliebige Formeln $\varphi \in \mathcal{L}$ ist stets $T \vDash \varphi \Leftrightarrow T \vDash^{\forall} \varphi$. Diese Tatsache sollte man sich einprägen, weil sie ständig verwendet wird. Die von verschiedenen Autoren

gewählten Definitionen einer Theorie können sich leicht voneinander unterscheiden. So wird z.B. nicht immer verlangt, dass Theorien nur Aussagen enthalten. Festlegungen dieser Art haben jeweils ihre Vor- und Nachteile. Beweise über Theorien sind durchweg flexibel genug, um sie einer leichten Begriffs-Modifikation anzupassen. Ausgehend von obiger Definition treffen wir hier noch folgende

Vereinbarung: Wenn für eine Aussagenmenge S von der *Theorie* S die Rede ist, meinen wir immer die durch S bestimmte Theorie $\{\alpha \in \mathcal{L}^0 \mid S \models \alpha\}$.

Es gibt eine kleinste Theorie in \mathcal{L} – nämlich die Menge \mathbf{Taut} ($= \mathbf{Taut}_{\mathcal{L}}$) aller allgemeingültigen Aussagen von \mathcal{L} . Es gibt auch eine größte Theorie: die Menge \mathcal{L}^0 aller Aussagen, die sogenannte *inkonsistente* Theorie, die keine Modelle hat. Alle übrigen Theorien heißen *erfüllbar* oder *konsistent*⁸⁾. Ferner ist der Durchschnitt $T = \bigcap_{i \in I} T_i$ einer jeden nichtleeren Familie von Theorien T_i wieder eine Theorie: ist $T \models \alpha \in \mathcal{L}^0$, gilt auch $T_i \models \alpha$, also $\alpha \in T_i$ für jedes i , und damit $\alpha \in T$. In diesem Buch bezeichnen T und T' , eventuell mit Indizes versehen, ausschließlich Theorien.

Für und $\alpha \in \mathcal{L}^0$ bezeichne $T + \alpha$ die kleinste α enthaltende Erweiterungstheorie von T . Analog sei $T + S$ für $S \subseteq \mathcal{L}^0$ die kleinste Theorie $\supseteq T \cup S$. Ist S endlich, so heißt $T' = T + S = T + \bigwedge S$ eine *endliche Erweiterung von T* . ($\bigwedge S$ bezeichnet die Konjunktion aller Aussagen aus S .) Die Aussage α heie *erfüllbar in T* , auch *verträglich* oder *konsistent mit T* , wenn $T + \alpha$ erfüllbar ist, und *widerlegbar in T* , wenn $T + \neg\alpha$ erfüllbar ist. So ist die Körpertheorie T_K mit der Aussage $1 + 1 = 0$ verträglich, oder $1 + 1 \neq 0$ ist in T_K widerlegbar. Denn es gibt Körper, in denen $1 + 1 = 0$ gilt. Theorien T_1, T_2 heißen *verträglich*, wenn die Theorie $T_1 + T_2$ konsistent ist.

Sind sowohl α als auch $\neg\alpha$ mit T verträglich, so heißt die Aussage α *unabhängig* in T . Klassisches Beispiel ist die Unabhängigkeit des Parallelenaxioms von den übrigen Axiomen der ebenen Geometrie, die die *absolute* Geometrie definieren. Weitaus schwieriger zu beweisen ist z.B. die Unabhängigkeit der Kontinuumshypothese von den Axiomen der Mengenlehre, die in 3.4 vorgestellt werden.

Eine Formelmenge X heißt ein *Axiomensystem* für T , wenn $T = \{\alpha \in \mathcal{L}^0 \mid X^\forall \models \alpha\}$, oder gleichwertig, wenn $\mathcal{A} \models T \Leftrightarrow \mathcal{A} \models X \Leftrightarrow \mathcal{A} \models X^\forall$, für alle \mathcal{L} -Strukturen \mathcal{A} . Das leere Axiomensystem $X = \emptyset$ axiomatisiert offenbar die „logische“ Theorie \mathbf{Taut} .

Wir gehen stets davon aus, dass alle Axiome einer Theorie Aussagen sind, folgen aber der üblichen Praxis, längliche Axiome als Formeln zu notieren und sich die Generalisierung der in den Axiomen eventuell frei vorkommenden Variablen stillschweigend ausgeführt zu denken. Sind alle Axiome \forall -Aussagen, heißt T auch eine

⁸⁾ *konsistent* bezieht sich meistens auf einen Logik-Kalkül, z.B. den Kalkül in Kapitel 3. Dort wird aber gezeigt, dass Konsistenz und Erfüllbarkeit übereinstimmen. Ein mehrdeutiger Gebrauch des Wortes hat keine tragischen Folgen und wird nachträglich gerechtfertigt.

universale oder \forall -Theorie. Für eine solche ist $\text{Md } T$ nach Korollar 3.3 stets gegenüber Substrukturen abgeschlossen, d.h. $\mathcal{A} \subseteq \mathcal{B} \models T \Rightarrow \mathcal{A} \models T$. Beispiele solcher Theorien sind die der Halbordnungen und Ordnungen.

Häufig sind Theorien nicht durch Axiome, sondern durch Strukturen oder Klassen von Strukturen definiert. Die elementare Theorie $\text{Th } \mathcal{A}$ einer Struktur \mathcal{A} und die Theorie $\text{Th } \mathbf{K}$ einer nichtleeren Klasse \mathbf{K} von Strukturen seien definiert durch

$$\text{Th } \mathcal{A} := \{\alpha \in \mathcal{L}^0 \mid \mathcal{A} \models \alpha\}, \quad \text{Th } \mathbf{K} := \bigcap \{\text{Th } \mathcal{A} \mid \mathcal{A} \in \mathbf{K}\}.$$

Man verifiziert leicht, dass es sich hierbei um Theorien im präzisierten Sinne handelt. Statt $\alpha \in \text{Th } \mathbf{K}$ schreibt man auch $\mathbf{K} \models \alpha$. Dies gilt definitionsgemäß genau dann wenn $\mathcal{A} \models \alpha$ für alle $\mathcal{A} \in \mathbf{K}$.

Wir führen an dieser Stelle noch einen weiteren wichtigen Begriff ein. $\alpha, \beta \in \mathcal{L}$ heißen *äquivalent in oder modulo* T , $\alpha \equiv_T \beta$, wenn $\alpha \equiv_{\mathcal{A}} \beta$ für alle $\mathcal{A} \models T$. Als Durchschnitt von Kongruenzen ist \equiv_T wieder eine Kongruenz, erfüllt also das Ersetzungstheorem. Dies wird fortan ohne Erwähnung benutzt, ebenso wie die evidente Gleichwertigkeit von $\alpha \equiv_T \beta$, $T \models \alpha \leftrightarrow \beta$ und $T \models (\alpha \leftrightarrow \beta)^\forall$. Terme s, t heißen *äquivalent in* T , wenn $T \models s = t$, d.h. s, t sind in allen T -Modellen wertverlaufsgleich.

Beispiel. In T_G (Seite 52) ist $x \circ x = x \equiv_{T_G} \exists y y \circ x = y \equiv_{T_G} \forall y y \circ x = y \equiv_{T_G} x = e$.

Bemerkung. Die Formeln zerfallen modulo T (genauer, modulo \equiv_T) in Äquivalenzklassen, deren Gesamtheit mit $B_\omega T$ bezeichnet sei. Auf diesen lassen sich in natürlicher Weise repräsentantenweise Operationen \wedge, \vee, \neg definieren – z.B. $\bar{\alpha} \wedge \bar{\beta} = \overline{\alpha \wedge \beta}$ wobei $\bar{\varphi}$ die Äquivalenzklasse bezeichnet, welcher φ angehört – und man zeigt leicht, dass $B_\omega T$ bezüglich \wedge, \vee, \neg eine Boolesche Algebra bildet. Auch ist für jedes n die Menge $B_n T$ aller $\bar{\varphi}$ aus $B_\omega T$ mit $\text{frei } \varphi \subseteq \{v_0, \dots, v_{n-1}\}$ eine Subalgebra von $B_\omega T$, und $B_0 T$ ist die Boolesche Algebra aller Aussagen modulo \equiv_T . Diese Algebren entfalten ihre Bedeutung erst in der höheren Modelltheorie und werden deshalb hier nur am Rande erwähnt.

Übungen

1. Sei $x \notin \text{frei } X$ und c nicht in X , α . Man beweise die Gleichwertigkeit von

$$(i) X \models \alpha, \quad (ii) X \models \forall x \alpha, \quad (iii) X \models \alpha \frac{c}{x}.$$

Das gilt also insbesondere, wenn X eine Theorie ist.

2. Man zeige, für Formelmengen X , Formeln α, β mit $x \notin \text{frei } \beta$ und eine in X, α, β nicht vorkommende Konstante c gilt $X \models \alpha \frac{c}{x} \rightarrow \beta \Leftrightarrow X \models \exists x \alpha \rightarrow \beta$.
3. Man zeige, für alle $\alpha, \beta \in \mathcal{L}^0$ ist $\beta \in T + \alpha \Leftrightarrow \alpha \rightarrow \beta \in T$.
4. Sei $T \subseteq \mathcal{L}$ eine Theorie, $\mathcal{L}_0 \subseteq \mathcal{L}$, und $T_0 := T \cap \mathcal{L}_0$. Man zeige, T_0 ist eine Theorie in \mathcal{L}_0 , die sogenannte *Redukt-Theorie* von T auf die Sprache \mathcal{L}_0 .

2.6 Spracherweiterungen

Die deduktive Entwicklung einer Theorie, sei sie durch ein Axiomensystem gegeben oder durch eine einzelne Struktur \mathcal{A} oder eine Klasse \mathbf{K} von solchen, geht fast immer Hand in Hand mit schrittweise vorgenommenen Spracherweiterungen. So ist z.B. für die Entwicklung der elementaren Zahlentheorie die Einführung der Teilbarkeitsrelation durch die Definition $x|y \leftrightarrow \exists z \, x \cdot z = y$ gewiss von Vorteil. Dieses und ähnliche Beispiele motivieren die folgende

Definition I. Sei r ein in \mathcal{L} nicht vorkommendes n -stelliges Relationssymbol. Eine *explizite Definition von r in \mathcal{L}* ist eine Formel der Gestalt

$$\eta_r : \quad r\vec{x} \leftrightarrow \delta(\vec{x}) \quad (x_1, \dots, x_n \text{ paarweise verschieden})$$

mit $\delta(\vec{x}) \in \mathcal{L}$, der *definierenden Formel*. Für eine Theorie T heißt $T_r := T + \eta_r$ dann eine *definitorische Erweiterung von T um r* . Dies ist eine Theorie in $\mathcal{L}[r]$, womit die aus \mathcal{L} durch Expansion um r entstehende Sprache bezeichnet sei.

T_r ist eine konservative Erweiterung von T und insofern eine „harmlose“. Dabei heißt eine Theorie $T' \supseteq T$ in $\mathcal{L}' \supseteq \mathcal{L}$ allgemein eine *konservative Erweiterung* von T , wenn $T' \cap \mathcal{L} = T$. Die Behauptung ist Teil von Satz 6.1. Für $\varphi \in \mathcal{L}[r]$ sei dort die *Reduzierte* $\varphi^{rd} \in \mathcal{L}$ wie folgt erklärt: jede in φ vorkommende, mit r beginnende Primformel $r\vec{t}$ wird (z.B. von links beginnend) durch $\delta(\vec{t})$ ersetzt.

Satz 6.1 (Eliminationssatz). Sei $T_r \subseteq \mathcal{L}[r]$ eine definitorische Erweiterung von $T \subseteq \mathcal{L}^0$ um die Definition $r\vec{x} \leftrightarrow \delta(\vec{x})$. Dann gilt für alle $\varphi \in \mathcal{L}[r]$

$$(*) \quad T_r \models \varphi \Leftrightarrow T \models \varphi^{rd}.$$

Für $\varphi \in \mathcal{L}$ gilt speziell $T_r \models \varphi \Leftrightarrow T \models \varphi$ (weil dann $\varphi^{rd} = \varphi$), und für $\alpha \in \mathcal{L}^0$ daher $\alpha \in T_r \Leftrightarrow \alpha \in T$. Kurzum, T_r ist eine konservative Erweiterung von T .

Beweis. Jedes Modell $\mathcal{A} \models T$ kann durch die Erklärung $r^{\mathcal{A}}\vec{a} \Leftrightarrow \mathcal{A} \models \delta[\vec{a}]$ zu einem $\mathcal{A}' \models T_r$ mit gleichem Träger expandiert werden. Weil $r\vec{t} \equiv_{T_r} \delta(\vec{t})$ für Termfolgen \vec{t} , gilt $\varphi \equiv_{T_r} \varphi^{rd}$ für alle $\varphi \in \mathcal{L}[r]$ (Ersetzungstheorem). Damit ergibt (*) sich aus

$$\begin{aligned} T_r \models \varphi &\Leftrightarrow \mathcal{A}' \models \varphi \text{ für alle } \mathcal{A}' \models T \quad (\text{weil } \text{Md } T_r = \{\mathcal{A}' \mid \mathcal{A}' \models T\}) \\ &\Leftrightarrow \mathcal{A}' \models \varphi^{rd} \text{ für alle } \mathcal{A}' \models T \quad (\text{weil } \varphi \equiv_{T_r} \varphi^{rd}) \\ &\Leftrightarrow \mathcal{A} \models \varphi^{rd} \text{ für alle } \mathcal{A} \models T \quad (\text{Satz 3.1}) \\ &\Leftrightarrow T \models \varphi^{rd}. \quad \square \end{aligned}$$

Ähnlich können auch Operationssymbole und Konstanten in Theorien neu eingeführt werden. Hierbei sind aber gewisse Bedingungen zu beachten. So lässt sich in der Gruppentheorie T_G (Seite 52) die Operation $^{-1}$ durch $y = x^{-1} \leftrightarrow x \circ y = e$ definieren, was durch $T_G \models \forall x \exists! y \, x \circ y = e$ gewissermaßen legitimiert wird, Übung 3. Diese

Bedingung sichert nämlich, dass $T_G + \eta^\forall$ eine konservative Erweiterung von T_G ist. Wir ergänzen Definition I daher wie folgt, wobei bis zum Ende des Abschnitts auch Konstantensymbole zu den Operationssymbolen rechnen.

Definition II. Eine *explizite Definition* eines in \mathcal{L} nicht vorkommenden n -stelligen Operationssymbols f ist eine Formel der Gestalt

$$\eta_f : \quad y = f\vec{x} \leftrightarrow \delta(\vec{x}, y) \quad (\delta \in \mathcal{L} \text{ und } y, x_1, \dots, x_n \text{ paarweise verschieden}).$$

η_f heißt *legitim* in $T \subseteq \mathcal{L}$, wenn $T \models \forall \vec{x} \exists! y \delta$, und $T_f := T + \eta_f^\forall$ heißt dann eine *definitorische Erweiterung um f* . Im Falle $n = 0$ schreibt man c für f und nennt dann $y = c \leftrightarrow \delta(y)$ eine *explizite Definition des Konstantensymbols c* .

Oft werden einige der freien Variablen von δ nicht explizit genannt und zu Parametervariablen degradiert. Diesbezüglich verweisen wir auf die Diskussion der Axiome in 3.4. Man beweist den Eliminationssatz fast wörtlich genauso für T_f , sofern η_f legitim in T ist. Dabei sei im Konstantenfall ($n = 0$) einfach $\varphi^{rd} := \exists z(\varphi \stackrel{z}{\leftarrow} \delta \stackrel{z}{\rightarrow})$, wobei $\varphi \stackrel{z}{\leftarrow}$ das Ersetzungsergebnis von z ($\notin \text{var } \varphi, \delta$) für c in φ bezeichnet. Für $n > 0$ konstruiere man φ^{rd} wie folgt: Kommt f in φ nicht vor, sei $\varphi^{rd} = \varphi$. Andernfalls hat φ offenbar die Gestalt $\varphi_0 \stackrel{f\vec{t}}{\rightarrow}$ für geeignete φ_0, \vec{t} und $y \notin \text{var } \varphi$. Dabei ist $\varphi \equiv_{T_f} \exists y(\varphi_0 \wedge y = f\vec{t}) \equiv_{T_f} \varphi_1 := \exists y(\varphi_0 \wedge \delta_f(\vec{t}, y))$. Falls f in φ_1 noch erscheint, wiederhole man diese Konstruktion. So schreitet man fort, bis in sagen wir m Schritten eine Formel φ_m entstanden ist, die f nicht mehr enthält. Es sei dann $\varphi^{rd} = \varphi_m$.

Häufig werden Operationssymbole f auch durch Definitionen der Gestalt

$$(*) \quad f\vec{x} := t(\vec{x})$$

eingeführt, wobei f im Term $t(\vec{x})$ selbstverständlich nicht vorkommen darf. Diese Verfahrensweise ordnet sich der Definition II unter, denn es handelt sich hierbei um nichts anderes als eine definitorische Erweiterung von T mit der expliziten Definition $\eta_f: y = f\vec{x} \leftrightarrow y = t(\vec{x})$. Diese ist legitim in T , weil $\models \forall \vec{x} \exists! y y = t(\vec{x})$. Man zeigt leicht, η_f^\forall ist logisch äquivalent zu $\forall \vec{x} f\vec{x} = t(\vec{x})$. Daher darf $(*)$ verstanden werden als eine hinreichend informative Kurzschrift einer legitimen expliziten Definition gemäß Definition II, mit der definierenden Formel $y = t(\vec{x})$.

Bemerkung. Statt neue Operationssymbole einzuführen, kann man auch die sogenannten ι -Terme aus [HB] benutzen. Ist $\varphi = \varphi(\vec{x}, y)$ eine Formel, so sei $\iota y \varphi$ ein Term, in welchem y als eine *durch ι gebundene Variable* erscheint. Falls $T \models \forall \vec{x} \exists! y \varphi$, wird T um das Axiom $\forall \vec{x} \forall y[y = \iota y \varphi(\vec{x}, y) \leftrightarrow \varphi(\vec{x}, y)]$ erweitert, so dass $\iota y \varphi(\vec{x}, y)$ den Funktionsterm $f\vec{x}$ sozusagen vertritt, den man durch eine explizite Definition hätte einführen können. Definitorische Spracherweiterungen sind nicht zwingend erforderlich. Man kann Formeln der Erweiterungssprache im Prinzip immer als Abkürzungen von Formeln der Originalsprache verstehen, nämlich ihrer Reduzierten, und so wird oft auch verfahren.

Allgemein heißt T' eine *definitorische Erweiterung* von T , wenn $T' = T + \Delta$ für eine Liste Δ von in T legitimen expliziten Definitionen neuer Symbole mittels derer von T (*legitim* bezieht sich hier nur auf Operationssymbole und Konstanten). Δ muss nicht endlich sein, aber es genügt im Prinzip, sich auf diesen Fall zu beschränken. Ist \mathcal{L}' die Sprache von T' , konstruiert man zu jedem $\varphi \in \mathcal{L}'$ wie oben schrittweise eine Reduzierte $\varphi^{rd} \in \mathcal{L}$. Damit führt man den etwas langatmigen Beweis des folgenden Satzes auf den Fall der Erweiterung um jeweils ein Symbol zurück:

Satz 6.2 (allgemeiner Eliminationssatz). *Es sei T' definitorische Erweiterung von T . Dann gilt $\alpha \in T' \Leftrightarrow \alpha^{rd} \in T$, und T' ist konservative Erweiterung von T .*

Ein in $T \subseteq \mathcal{L}$ vorkommendes Relations- oder Operationssymbol ζ heißt in T *explizit definierbar*, wenn T definitorische Erweiterung von $T_0 := T \cap \mathcal{L}_0$ ist, wobei \mathcal{L}_0 die Sprache \mathcal{L} ohne ζ bezeichnet. Anders formuliert, T_0 wurde mittels einer expliziten Definition von ζ zu T erweitert. In einer solchen Situation kann jedes T_0 -Modell offenbar auf nur genau eine Weise zu einem T -Modell expandiert werden. Wenn nun lediglich diese spezielle Bedingung erfüllt ist, heißt ζ auch *implizit definierbar* in T . Man kann diese auch wie folgt formulieren: Unterscheiden sich T' von T nur dadurch, dass das Symbol ζ überall durch ein neues Symbol ζ' ersetzt wird, so ist $T \cup T' \models \zeta \vec{x} \leftrightarrow \zeta' \vec{x}$ bzw. $T \cup T' \models \zeta \vec{x} = \zeta' \vec{x}$, je nachdem, ob ζ, ζ' Relations- oder Operationssymbole sind. Bemerkenswert ist nun, dass dies für die explizite Definierbarkeit von ζ in T bereits hinreicht. Wir verzichten aber auf den Beweis und zitieren nur den

Definierbarkeitssatz von Beth. Ein in einer Theorie T implizit definierbares Relations- oder Operationssymbol ist in T auch explizit definierbar.

Definitorische Spracherweiterungen müssen sorgfältig von Spracherweiterungen unterschieden werden, die durch Einführung sogenannter *Skolem-Funktionen* entstehen. Diese sind für viele Zwecke nützlich und seien daher kurz beschrieben.

Skolemsche Normalformen. Nach Satz 4.2 lässt sich jede Formel α in eine äquivalente PNF überführen, $\alpha \equiv Q_1 x_1 \cdots Q_k x_k \alpha'$, mit quantorenfreiem α' . Offenbar ist dann $\neg \alpha \equiv \overline{Q}_1 x_1 \cdots \overline{Q}_k x_k \neg \alpha'$, mit $\overline{\forall} = \exists$ und $\overline{\exists} = \forall$. Weil $\models \alpha$ genau dann wenn $\neg \alpha$ unerfüllbar ist, lässt sich das Entscheidungsproblem über Allgemeingültigkeit zunächst auf das Erfüllbarkeitsproblem für Formeln in PNF reduzieren. Letzteres wird nun – allerdings auf Kosten der Einführung neuer Operationssymbole – durch Satz 6.3 unten gänzlich auf das Erfüllbarkeitsproblem für \forall -Formeln zurückgeführt.

Formeln α und β heißen *erfüllbarkeitsgleich*, wenn beide (nicht notwendig im selben Modell) erfüllbar sind, oder beide nicht erfüllbar sind. Wir konstruieren zu jeder o.B.d.A. in pränexer Form vorliegenden Formel $\alpha = Q_1 x_1 \cdots Q_k x_k \alpha'$ eine erfüllbarkeitsgleiche \forall -Formel $\hat{\alpha}$ mit $\text{frei } \hat{\alpha} = \text{frei } \alpha$ und zusätzlichen Operationssymbolen. Die

Konstruktion von $\hat{\alpha}$ erfolgt in m Schritten, wobei m die Anzahl der \exists -Quantoren unter den Q_1, \dots, Q_k zähle. Es sei $\alpha = \alpha_0$ und α_i schon konstruiert. Falls α_i bereits eine \forall -Formel ist, so sei $\hat{\alpha} = \alpha_i$. Andernfalls hat α_i die Gestalt $\forall x_1 \dots \forall x_n \exists y \beta_i$ für ein gewisses $n \geq 0$. Mit einem bisher noch nicht benutzten n -stelligen Operationssymbol f sei $\alpha_{i+1} = \forall \vec{x} \beta_i \frac{f\vec{x}}{y}$. So erhält man nach m Schritten eine \forall -Formel $\hat{\alpha}$ mit $\text{frei } \hat{\alpha} = \text{frei } \alpha$, die eine SNF (*Skolemsche Normalform*) von α genannt wird.

Beispiel. Für $\alpha = \forall x \exists y x < y$ ist $\hat{\alpha} = \forall x x < f x$. Für $\alpha = \exists x \forall y \exists z x = y \cdot z$ (hier ist $n = 0$) ist $\hat{\alpha} = \forall y c = y \cdot f(y)$, mit neuen Funktionssymbolen f bzw. c und f .

Satz 6.3 (über die Skolemsche Normalform). *Sei $\hat{\alpha}$ eine SNF für die Formel $\alpha = \alpha(\vec{z})$. Dann gelten (a) $\hat{\alpha} \models \alpha$, (b) α ist erfüllbarkeitsgleich mit $\hat{\alpha}$.*

Beweis. (a): Es genügt, $\alpha_{i+1} \models \alpha_i$ für jeden der beschriebenen Konstruktionsschritte zu zeigen. Das ist einfach. Denn $\beta_i \frac{f\vec{x}}{y} \models \exists y \beta_i$, so dass nach (c) und (d) in **2.5** $\alpha_{i+1} = \forall \vec{x} \beta_i \frac{f\vec{x}}{y} \models \forall \vec{x} \exists y \beta_i = \alpha_i$. (b): Mit $\hat{\alpha}$ ist gemäß (a) auch α erfüllbar. Sei umgekehrt $\mathcal{A} \models \forall \vec{x} \exists y \beta_i(\vec{x}, y, \vec{z})[\vec{c}]$. Zu jedem $\vec{a} \in A^n$ denken wir uns ein $b \in A$ mit $\mathcal{A} \models \beta[\vec{a}, b, \vec{c}]$ ausgewählt und expandieren \mathcal{A} zu \mathcal{A}' , indem wir für das neue Operationssymbol $f^{\mathcal{A}'} \vec{a} = b$ setzen. Dann ist offenbar $\mathcal{A}' \models \alpha_{i+1}[\vec{c}]$. So erhalten wir schließlich ein Modell für $\hat{\alpha}$ als Expansion des Ausgangsmodells. \square

Damit gewinnt man zu jedem α auch eine allgemeingültigkeitsgleiche \exists -Formel $\check{\alpha}$, d.h. $\models \alpha \Leftrightarrow \models \check{\alpha}$. Man stellt nach obigem Satz zu $\beta := \neg \alpha$ eine erfüllbarkeitsgleiche SNF $\hat{\beta}$ her und setzt $\check{\alpha} := \neg \hat{\beta}$. Dann gilt in der Tat $\models \alpha \Leftrightarrow \models \check{\alpha}$, denn

$$\models \alpha \Leftrightarrow \beta \text{ unerfüllbar} \Leftrightarrow \hat{\beta} \text{ unerfüllbar} \Leftrightarrow \models \check{\alpha}.$$

Übungen

1. T_f entstehe aus T durch Hinzufügen einer expliziten Definition η für f und α^{rd} sei konstruiert wie im Text beschrieben. Man zeige, T_f ist genau dann konservative Erweiterung von T , wenn η eine legitime explizite Definition ist.
2. Man zeige, $Th(\mathbb{N}, 0, 1, \mathbf{S}, +, \cdot, <)$ ist definitorische Erweiterung von $Th(\mathbb{N}, +, \cdot)$. Dabei bezeichnet $\mathbf{S}: n \mapsto n + 1$ die Nachfolgerfunktion.
3. Man zeige, $y = x^{-1} \leftrightarrow x \circ y = e$ ist eine legitime explizite Definition in der Gruppentheorie T_G . Man zeige ferner, die entstehende definitorische Erweiterung ist identisch mit $T_G^=$. Also ist $T_G^=$ konservative Erweiterung von T_G . In diesem Sinne sind T_G und $T_G^=$ äquivalent.
4. Man zeige, in $(\mathbb{Z}, 0, +)$ ist die $<$ -Relation nicht elementar definierbar.

Kapitel 3

Der Gödelsche Vollständigkeitssatz

Unser Ziel ist die Charakterisierung der Folgerungsrelation in Sprachen 1. Stufe durch einen Kalkül ähnlich dem aussagenlogischen. Dass dieses Ziel grundsätzlich erreichbar ist, wurde zuerst von K. Gödel in [Gö1] gezeigt. Insbesondere lassen sich dann auch alle Tautologien deduktiv gewinnen. Die letztere, ursprüngliche Fassung des Gödelschen Satzes impliziert nicht unmittelbar den Kompaktheitssatz, während die allgemeine Formulierung diesen einschließt.

Die Charakterisierbarkeit des logischen Folgerns durch einen Kalkül, der sogenannte Vollständigkeitssatz, ist ein zentrales Ergebnis der mathematischen Logik mit weitreichenden Konsequenzen. Trotz seines metalogischen Ursprungs ist der Vollständigkeitssatz wesentlich ein mathematischer Satz. Er erklärt in zufriedenstellender Weise das Phänomen der Wohldefiniertheit logischer Schlussweisen in der Mathematik, so dass die Suche nach deren Erweiterung sich ausnehmen würde wie die Suche nach dem Perpetuum mobile in der Physik. Das betrifft natürlich nicht die Entwicklung neuartiger Methoden der Beweisfindung. Etwas mehr über den metamathematischen Aspekt des Satzes und den Nutzen der mit seinem Beweis verbundenen Modellkonstruktion wird in den Abschnitten **3.3**, **3.4** und **3.5** gesagt.

Wir behandeln ohne Umschweife gleich den Fall einer beliebigen, nicht notwendig abzählbaren Sprache der 1. Stufe. Gleichwohl ist der hier ausgeführte Beweis nach der Henkinschen Idee der Konstantenerweiterung [He] nicht zuletzt durch vorteilhafte Wahl der logischen Basis relativ kurz. Zwar sind mathematische Theorien in der Regel abzählbar, aber der Erfolg der Anwendung von Methoden der mathematischen Logik z.B. in der Algebra – siehe hierzu Kapitel **5** – beruht wesentlich auf einer uneingeschränkten Formulierung des Vollständigkeitssatzes. Erst in dieser Allgemeinheit gewinnt auch sein Beweis die innere Geschlossenheit, die die Beweise herausragender mathematischer Sätze meistens auszeichnet.

3.1 Ein Kalkül des natürlichen Schließens

Es sei \mathcal{L} eine beliebig vorgegebene elementare Sprache in der logischen Signatur $\neg, \wedge, \forall, =$ wie bisher. Wir definieren einen Kalkül \vdash durch das umrahmte System von Schlussregeln, den *Basisregeln*, der ebenso wie der entsprechende aussagenlogische mit Sequenzen arbeitet und die Basisregeln aus 1.4 durch drei prädikatenlogische Basisregeln ergänzt. Auch wird die Anfangsregel (AR) etwas erweitert.

(AR) $\frac{}{X \vdash \alpha} \ (\alpha \in X \cup \{t=t\})$	(MR) $\frac{X \vdash \alpha}{X' \vdash \alpha} \ (X \subseteq X')$
(\wedge 1) $\frac{X \vdash \alpha, \beta}{X \vdash \alpha \wedge \beta}$	(\wedge 2) $\frac{X \vdash \alpha \wedge \beta}{X \vdash \alpha, \beta}$
(\neg 1) $\frac{X \vdash \beta, \neg \beta}{X \vdash \alpha}$	(\neg 2) $\frac{X, \beta \vdash \alpha \mid X, \neg \beta \vdash \alpha}{X \vdash \alpha}$
(\forall 1) $\frac{X \vdash \forall x \alpha}{X \vdash \alpha \frac{t}{x}} \ (\alpha, \frac{t}{x} \text{ kollisionsfrei})$	(\forall 2) $\frac{X \vdash \alpha \frac{y}{x}}{X \vdash \forall x \alpha} \ (y \notin \text{frei } X \cup \text{var } \alpha)$
(=) $\frac{X \vdash s=t, \alpha \frac{s}{x}}{X \vdash \alpha \frac{t}{x}} \ (\alpha \text{ Primformel})$	

Nach (AR) ist immer $\vdash t=t$, wobei t ein beliebiger Term ist und hier wie überall $\vdash \varphi$ für $\emptyset \vdash \varphi$ steht. Wir übernehmen auch die sonstigen Schreibweisen aus Kapitel 1, z.B. steht $\alpha \vdash \beta$ für $\{\alpha\} \vdash \beta$ usw. (AR) wurde nur der Bequemlichkeit halber schärfer formuliert als nötig und ließe sich wegen (MR) zu $\frac{}{\alpha \vdash \alpha}$ und $\frac{}{\vdash t=t}$ einschränken.

Wir nennen \vdash einen *Kalkül des natürlichen Schließens*, weil er das informelle prädikatenlogische Schließen in Mathematik und anderen exakten Wissenschaften hinreichend gut modelliert¹⁾. Unser Ziel ist der Nachweis, dass \models durch \vdash vollständig charakterisiert ist. Der Kalkül wird nur soweit entwickelt, wie dies der Vollständigkeitsbeweis erfordert. Weitere Ableitungen auszuführen ist zwar lehrreich (siehe hierzu die Übungen), aber nicht der prinzipielle Zweck einer Formalisierung des Beweisens, es sei denn man verfolgt spezielle beweistheoretische Ziele.

Alle Basisregeln sind in dem in 1.4 definierten Sinne korrekt. Die Einschränkungen in den Regeln (\forall 1), (\forall 2) und (=) sichern deren Korrektheit, die in den Beispielen (a),(g) und (b) in 2.5 nachgewiesen wurde. (=) ist wegen der Beschränkung auf

¹⁾ Es handelt sich hier um eine unseren Bedürfnissen angepasste Version des Kalküls NK aus [Ge]; Sequenzenkalküle sind in erster Linie Gegenstand von Lehrbüchern der Beweistheorie.

Primformeln korrekt und für beliebige α beweisbar, solange $\alpha, \frac{s}{x}, \frac{t}{x}$ kollisionsfrei sind. Die Kollisionsfreiheit ließe sich noch weiter mildern, z.B. genügt es, in $(\forall 1)$ lediglich $gbd\alpha \cap \text{var } t = \emptyset$ zu fordern. Wie in **2.3** schon gesagt wurde, lässt sich durch eine etwas kompliziertere Definition der Substitution sogar jede Einschränkung vermeiden. Durch solche Maßnahmen werden die Basisregeln jedoch unnötig verschärft, denn schwach formulierte Logikkalküle wie der angegebene erleichtern oft gewisse Induktionen, etwa den Korrektheitsnachweis. Im übrigen erbringt der Ehrgeiz eines sparsamen Umgangs mit Axiomen oder Regeln für semantisch orientierte Betrachtungen allerdings nur bescheidenen praktischen Nutzen.

Weil \vdash als Erweiterung des entsprechenden Kalküls aus **1.4** verstanden werden kann, übertragen sich automatisch alle dort genannten Beispiele beweisbarer Regeln, z.B. die Schnittregel. Alle weiteren korrekten Regeln, z.B. die formalen Versionen der Generalisierung und Partikularisierung aus **2.5**, sind wegen der Vollständigkeit des Kalküls beweisbar. Das betrifft auch die Regel $\frac{X \vdash \alpha}{X \vdash \forall x \alpha}$ ($x \notin \text{frei } X$), denn diese ist nach **2.5** korrekt, ergibt sich aber nicht direkt aus $(\forall 2)$. Wir halten uns aber mit Beweisen dieser und anderer Regeln nicht auf, weil sie für den Vollständigkeitsbeweis belanglos sind und durch diesen nachträglich gerechtfertigt werden.

Wie im aussagenlogischen Falle gilt auch jetzt wieder ein nützliches

Beweisprinzip der Regelinduktion. *Sei \mathcal{E} eine Eigenschaft von Paaren X, α aus Formelmengen X und Formeln α derart, dass*

- (o) $\mathcal{E}(X, \alpha)$ für $\alpha \in X$ oder α von der Form $t=t$,
- (s) $\mathcal{E}(X, \alpha) \Rightarrow \mathcal{E}(X', \alpha)$ falls $X' \supseteq X$, und analog für $(\wedge 1)$ bis $(=)$.

Dann gilt $\mathcal{E}(X, \alpha)$ für alle X, α mit $X \vdash \alpha$.

Dies gilt, weil der Nachweis des ähnlich formulierten Prinzips in **1.4** weder von der Art der Sprache noch von der konkreten Gestalt der Regeln abhängt. Weil die Basisregeln offenbar korrekt sind, folgt damit genau wie im aussagenlogischen Falle die *Korrektheit des Kalküls*, d.h. $\vdash \subseteq \models$, oder ausführlicher

$$(Kor) \quad X \vdash \alpha \Rightarrow X \models \alpha, \text{ für alle } X, \alpha.$$

Mit Regelinduktion zeigt man auch die Monotonie bezüglich Spracherweiterungen

$$(Mon) \quad \mathcal{L} \subseteq \mathcal{L}' \Rightarrow \vdash_{\mathcal{L}} \subseteq \vdash_{\mathcal{L}'}.$$

Hier wurden die Ableitungsrelationen indiziert. Denn man beachte, dass jede elementare Sprache ihre eigene Ableitungsrelation definiert, und wir werden vorübergehend mit dem Vergleich dieser Relationen in verschiedenen Sprachen zu tun haben. Erst

der Vollständigkeitssatz ergibt, dass sich eine Indizierung erübrigt, ganz analog wie bei der Folgerungsrelation \models . Zum Beweis von *(Mon)* betrachte man die Eigenschaft ‘ $X \vdash_{\mathcal{L}} \alpha$ und $X, \alpha \subseteq \mathcal{L}$ ’, für die die Bedingungen (o) und (s) der Regelinduktion leicht zu verifizieren sind.

Wie in der Aussagenlogik gilt natürlich auch hier der

Endlichkeitssatz. *Wenn $X \vdash \alpha$, so ist bereits $X_0 \vdash \alpha$ für ein endliches $X_0 \subseteq X$.*

Wir benötigen eine vorübergehend nützliche Verschärfung dieser Tatsache, nämlich

(End) Ist $X \vdash_{\mathcal{L}} \alpha$, so gibt es ein $\mathcal{L}_0 \subseteq \mathcal{L}$ endlicher Signatur und eine endliche Teilmenge $X_0 \subseteq X$ mit $X_0 \vdash_{\mathcal{L}_0} \alpha$.

Die Schreibweise $X_0 \vdash_{\mathcal{L}_0} \alpha$ schließt $X_0 \cup \{\alpha\} \subseteq \mathcal{L}_0$ selbstverständlich ein. Zum Beweis betrachte man die Eigenschaft ‘es gibt endliche $X_0 \subseteq X$ und $\mathcal{L}_0 \subseteq \mathcal{L}$ mit $X_0 \vdash_{\mathcal{L}_0} \alpha$ ’. Dabei sei wie stets L die Signatur von \mathcal{L} , L_0 die Signatur von \mathcal{L}_0 usw. Es genügt, die Bedingungen (o), (s) des Beweisprinzips der Regelinduktion zu bestätigen. Für $\alpha \in X \cup \{t=t\}$ ist $X_0 \vdash_{\mathcal{L}_0} \alpha$ mit $X_0 = \{\alpha\}$ oder $X_0 = \emptyset$, wobei \mathcal{L}_0 alle in α vorkommenden nichtlogischen Symbole enthalte. Damit ist (o) gezeigt. Der Induktionsschritt über (MR) ist trivial. Beim Schritt über $(\wedge 1)$ sei angenommen $X_1 \vdash_{\mathcal{L}_1} \alpha_1$ und $X_2 \vdash_{\mathcal{L}_2} \alpha_2$ für endliche $X_i \subseteq X$ und $L_i \subseteq L$, $i = 1, 2$. Dann ergibt *(Mon)* offenbar $X_0 \vdash_{\mathcal{L}_0} \alpha_i$, mit $X_0 = X_1 \cup X_2$ und $L_0 = L_1 \cup L_2$. Gemäß $(\wedge 1)$ ist $X_0 \vdash_{\mathcal{L}_0} \alpha_1 \wedge \alpha_2$ und wir haben, was wir wollten. Ähnlich verlaufen die Induktionsschritte für alle übrigen Regeln. Damit ist auch (s) bestätigt und *(End)* bewiesen.

Das in diesem Beweis konstruierte \mathcal{L}_0 enthält mindestens die nichtlogischen Symbole von X_0 und α , aber möglicherweise einige mehr. Erst der Vollständigkeitssatz wird ergeben, dass man mit den in X_0, α vorkommenden Symbolen tatsächlich auskommt. Diese Unempfindlichkeit des Ableitens gegenüber Spracherweiterung lässt sich, wenn auch mit erheblichem Aufwand, rein beweistheoretisch bestätigen, also rein kombinatorisch und ohne Bezug auf die infinitäre Semantik. Einen ersten und relativ bescheidenen Einblick in derartige Methoden vermittelt die Konstantenelimination in Lemma 2.1 und 2.2 im nächsten Abschnitt.

Hier noch einige weitere später auch benötigte Beispiele beweisbarer Regeln.

Beispiel 1. (a) $\frac{X \vdash s=t, s=t'}{X \vdash t=t'}$, (b) $\frac{X \vdash s=t}{X \vdash t=s}$, (c) $\frac{X \vdash t=s, s=t'}{X \vdash t=t'}$.

Zum Beweis von (a) sei $x \notin \text{var } t'$ und sei α die Formel $x=t'$. Dann schreibt sich die Prämisse von (a) als $X \vdash s=t, \alpha \frac{s}{x}$. Regel $(=)$ ergibt $X \vdash \alpha \frac{t}{x}$. Nun ist $\alpha \frac{t}{x}$ wegen $x \notin \text{var } t'$ aber gerade die Formel $t=t'$, also $X \vdash t=t'$. Aus (a) erhält man für $t' = s$ wegen $X \vdash s=s$ sofort (b). Damit folgt auch (c); denn die Prämisse ergibt wegen (b) offenbar $X \vdash s=t, s=t'$ und damit gemäß (a) die Konklusion von (c).

Beispiel 2. In (a)–(d) sei n wie üblich die Stellenzahl der Symbole f bzw. r .

$$\begin{aligned} \text{(a)} \quad & \frac{X \vdash t_i = t}{X \vdash f\vec{t} = ft_1 \cdots t_{i-1} t t_{i+1} \cdots t_n}, & \text{(b)} \quad & \frac{X \vdash t_1 = t'_1, \dots, t_n = t'_n}{X \vdash f\vec{t} = f\vec{t}'}, \\ \text{(c)} \quad & \frac{X \vdash t_i = t, r\vec{t}}{X \vdash r t_1 \cdots t_{i-1} t t_{i+1} \cdots t_n}, & \text{(d)} \quad & \frac{X \vdash t_1 = t'_1, \dots, t_n = t'_n, r\vec{t}}{X \vdash r\vec{t}'}. \end{aligned}$$

Denn sei $X \vdash t_i = t$ und $\alpha := f\vec{t} = ft_1 \cdots t_{i-1} x t_{i+1} \cdots t_n$, wobei x in keinem der t_j vorkomme. Weil $X \vdash \alpha \frac{t_i}{x}$ ($= f\vec{t} = f\vec{t}$) nach (AR), folgt $X \vdash \alpha \frac{t}{x}$ nach ($=$), also die Konklusion von (a). Sodann ergibt sich (b) unter Berücksichtigung von Beispiel 1(c) durch n -fache Wiederholung von (a), wie man sich beginnend mit $n = 2$ leicht klarmacht. (c) folgt durch Betrachtung von $\alpha := r t_1 \cdots t_{i-1} x t_{i+1} \cdots t_n$ ganz ähnlich wie (a). Eine n -fach wiederholte Anwendung von (c) ergibt dann (d).

Beispiel 3. $\vdash \exists x t = x$ für alle x, t mit $x \notin \text{var } t$, sowie $\vdash \exists x x = x$.

Denn ($\forall 1$) ergibt offenbar $\forall x t \neq x \vdash t \neq t$ ($= (t \neq x) \frac{t}{x}$; hier benötigt man $x \notin \text{var } t$). Nach (AR) ist zugleich auch $\forall x t \neq x \vdash t = t$ und nach ($\neg 1$) damit $\forall x t \neq x \vdash \exists x t = x$. Trivialerweise ist auch $\neg \forall x t \neq x \vdash \exists x t = x$ ($= \neg \forall x t \neq x$). Also $\vdash \exists x t = x$ gemäß ($\neg 2$). Analog zeigt man $\vdash \exists x x = x$ mit Hilfe von $\frac{x}{x}$ anstelle von $\frac{t}{x}$.

Wie in der Aussagenlogik heißt $X (\subseteq \mathcal{L})$ *inkonsistent*, falls $X \vdash \alpha$ für alle $\alpha \in \mathcal{L}$, und sonst *konsistent*. Jede erfüllbare Menge X ist offenbar konsistent. Die Inkonsistenz von X ist wegen ($\neg 1$) gleichwertig mit $X \vdash \alpha, \neg \alpha$ für beliebiges α . Aber auch mit $X \vdash \perp$ ($= \neg \exists \mathbf{v}_0 \mathbf{v}_0 = \mathbf{v}_0$), weil $X \vdash \exists \mathbf{v}_0 \mathbf{v}_0 = \mathbf{v}_0$ nach Beispiel 3. Auch ist \vdash wie in 1.4 durch die Inkonsistenz vollständig charakterisiert. Denn die Beweise von

$$\mathcal{C}^+ : \quad X \vdash \alpha \Leftrightarrow X, \neg \alpha \vdash \perp, \quad \mathcal{C}^- : \quad X \vdash \neg \alpha \Leftrightarrow X, \alpha \vdash \perp$$

aus Lemma 1.4.2 bleiben mit jeder sinnvollen Definition von \perp unverändert richtig.

Übungen

1. Man beweise die Regel $\frac{X \vdash \alpha \frac{t}{x}}{X \vdash \exists x \alpha}$ ($\alpha, \frac{t}{x}$ kollisionsfrei).
2. Man beweise $\forall x \alpha \vdash \forall y \alpha \frac{y}{x}$ und $\forall y \alpha \frac{y}{x} \vdash \forall x \alpha$ für $y \notin \text{var } \alpha$.
3. Man beweise mit Übung 2 und der Schnittregel $\frac{X \vdash \forall y \alpha \frac{y}{x}}{X \vdash \forall z \alpha \frac{z}{x}}$ ($y, z \notin \text{var } \alpha$).
4. Man zeige, eine konsistente Menge X ist maximal konsistent genau dann wenn entweder $\varphi \in X$ oder $\neg \varphi \in X$.
5. Ist X ein Axiomensystem einer Theorie T , so heißt eine Aussage α *unabhängig* von X (oder *unabhängig in T*), wenn weder $X \vdash \alpha$ noch $X \vdash \neg \alpha$. Man zeige, dies ist gleichwertig mit der Konsistenz von $X \cup \{\alpha\}$ und $X \cup \{\neg \alpha\}$.

3.2 Der Vollständigkeitsbeweis

Sei \mathcal{L} eine Sprache und c eine Konstante (genauer, ein Konstantensymbol). $\mathcal{L}c$ gehe aus \mathcal{L} durch Adjunktion von c hervor. Es ist $\mathcal{L}c = \mathcal{L}$ genau dann, wenn c in \mathcal{L} bereits vorkommt. Analog bezeichnet $\mathcal{L}C$ die aus \mathcal{L} durch Adjunktion einer Menge C von Konstanten hervorgehende Sprache, eine *Konstantenexpansion* von \mathcal{L} . Solche Expansionen werden uns in Kapitel 5 ziemlich häufig begegnen. Sei $\alpha \frac{z}{c}$ das aus der Formel α entstehende Ergebnis der Ersetzung von c durch die Variable z , und sei $X \frac{z}{c} := \{\alpha \frac{z}{c} \mid \alpha \in X\}$. Die Konstante c kommt in $X \frac{z}{c}$ dann nicht mehr vor. Die folgende Aussage benötigen wir später nur für eine einzige Variable. Wie so oft lässt sich problemlos aber nur die strengere Aussage induktiv beweisen.

Lemma 2.1 (über die Konstantenelimination). *Es sei $X \vdash_{\mathcal{L}c} \alpha$. Für fast alle Variablen z gilt dann auch $X \frac{z}{c} \vdash_{\mathcal{L}} \alpha \frac{z}{c}$.*

Beweis durch Regelinuktion in $\vdash_{\mathcal{L}c}$. Für $\alpha \in X$ ist auch $\alpha \frac{z}{c} \in X \frac{z}{c}$. Ist α von der Gestalt $t=t$, so auch $\alpha \frac{z}{c}$. Also $X \frac{z}{c} \vdash_{\mathcal{L}} \alpha \frac{z}{c}$ in beiden Fällen, sogar für alle z . Nur die Induktionsschritte über $(\forall 1)$, $(\forall 2)$ und $(=)$ sind nicht unmittelbar ersichtlich. Wir beschränken uns auf $(\forall 1)$, weil die Schritte über $(\forall 2)$ und $(=)$ analog verlaufen. Sei $X \frac{z}{c} \vdash_{\mathcal{L}} (\forall x \alpha) \frac{z}{c}$ für fast alle z gemäß Induktionsannahme, $\alpha, \frac{t}{x}$ kollisionsfrei, und o.B.d.A. $z \notin \text{var} \forall x \alpha, t$. Mit einer gesonderten Induktion über α zeigt man $\alpha \frac{t}{x} \frac{z}{c} = \alpha' \frac{t'}{x}$ mit $\alpha' := \alpha \frac{z}{c}$ und $t' := t \frac{z}{c}$. Auch sind $\alpha', \frac{t'}{x}$ offenbar kollisionsfrei. Wegen $X \frac{z}{c} \vdash_{\mathcal{L}} (\forall x \alpha) \frac{z}{c} = \forall x \alpha'$ ergibt $(\forall 1)$ dann $X \frac{z}{c} \vdash_{\mathcal{L}} \alpha' \frac{t'}{x} = \alpha \frac{t}{x} \frac{z}{c}$, und zwar immer noch für fast alle z . \square

Hieraus ergibt sich leicht die folgende Regel der „Konstantenquantifizierung“

$$(\forall 3) \quad \frac{X \vdash \alpha \frac{c}{x}}{X \vdash \forall x \alpha} \quad (c \text{ nicht in } X, \alpha).$$

Denn sei $X \vdash \alpha \frac{c}{x}$. Wegen des Endlichkeitssatzes darf man o.B.d.A. annehmen, X sei endlich. Nach Lemma 2.1 – wobei $\mathcal{L}c = \mathcal{L}$ im vorliegenden Falle – findet man ein in X, α nicht vorkommendes y mit $X \frac{y}{c} \vdash \alpha \frac{c}{x} \frac{y}{c} = \alpha \frac{y}{x}$ (Letzteres gilt, weil c in α nicht vorkommt). Weil $X \frac{y}{c} = X$, heißt dies $X \vdash \alpha \frac{y}{x}$. Daher $X \vdash \forall x \alpha$ gemäß $(\forall 2)$. Eine ebenso nützliche Folge der Konstantenelimination ist das

Lemma 2.2. *Sei C eine beliebige Menge von Konstanten und $\mathcal{L}' = \mathcal{L}C$. Dann gilt $X \vdash_{\mathcal{L}} \alpha \Leftrightarrow X \vdash_{\mathcal{L}'} \alpha$ für alle $X \subseteq \mathcal{L}$ und $\alpha \in \mathcal{L}$.*

Beweis. (*Mon*) besagt $X \vdash_{\mathcal{L}} \alpha \Rightarrow X \vdash_{\mathcal{L}'} \alpha$. Sei umgekehrt $X \vdash_{\mathcal{L}'} \alpha$. Zum Nachweis von $X \vdash_{\mathcal{L}} \alpha$ darf man wegen (*End*) und (*MR*) offenbar annehmen, C sei endlich. Da sich die Hinzunahme endlich vieler Konstanten schrittweise vollziehen lässt, dürfen wir für den Zweck des Beweises sogar annehmen, $\mathcal{L}' = \mathcal{L}c$ für eine einzige, in \mathcal{L} nicht

vorkommende Konstante c . Lemma 2.1 liefert dann $X \stackrel{z}{c} \vdash_{\mathcal{L}} \alpha \stackrel{z}{c}$ für mindestens eine Variable z , d.h. $X \vdash_{\mathcal{L}} \alpha$, denn c kommt in X und in α nicht vor. \square

Wir bezeichnen im Folgenden die Ableitungsrelationen in \mathcal{L} und in jeder Konstantenexpansion \mathcal{L}' von \mathcal{L} mit dem gleichen Symbol \vdash . Daraus können wegen Lemma 2.2 keine Missverständnisse erwachsen. Weil die Konsistenz von X gleichwertig ist mit $X \not\vdash \perp$, muss auch nicht zwischen der Konsistenz von $X \subseteq \mathcal{L}$ bzgl. \mathcal{L} und bzgl. \mathcal{L}' unterschieden werden. Das ist ganz wesentlich für den Beweis von Lemma 2.3.

Der Beweis des Vollständigkeitsatzes läuft im Wesentlichen auf eine Modellkonstruktion aus dem syntaktischen Material einer gewissen Konstantenexpansion von \mathcal{L} hinaus. Dazu wählen wir für jede Variable x und jedes $\alpha \in \mathcal{L}$ eine in \mathcal{L} nicht vorhandene Konstante $c_{x,\alpha}$, und zwar für jedes Paar x, α jeweils genau eine. Es sei

$$\alpha^x := \neg \forall x \alpha \wedge \alpha \stackrel{c}{x} \quad (c := c_{x,\alpha}).$$

Wieviele freie Variablen α enthält und ob x in α überhaupt vorkommt, ist dabei unerheblich. $\neg \alpha^x$ ist in jedem Falle logisch äquivalent zu $\exists x \neg \alpha \rightarrow \neg \alpha \stackrel{c}{x}$ und besagt inhaltlich, dass c unter der Annahme $\exists x \neg \alpha$ ein Beispiel für das Zutreffen von $\neg \alpha$, d.h. ein Gegenbeispiel für die Gültigkeit von α repräsentiert.

Lemma 2.3. *Sei $\Gamma_{\mathcal{L}} := \{\neg \alpha^x \mid \alpha \in \mathcal{L}, x \in \text{Var}\}$. Dann ist mit $X \subseteq \mathcal{L}$ auch $X \cup \Gamma_{\mathcal{L}}$ konsistent.*

Beweis. Annahme $X \cup \Gamma_{\mathcal{L}} \vdash \perp$. Dann existieren Formeln $\neg \alpha_0^{x_0}, \dots, \neg \alpha_n^{x_n} \in \Gamma_{\mathcal{L}}$ mit (a): $X \cup \{\neg \alpha_i^{x_i} \mid i \leq n\} \vdash \perp$. Sei n hierbei minimal gewählt, so dass wegen $X \not\vdash \perp$ (b): $X' := X \cup \{\neg \alpha_i^{x_i} \mid i < n\} \not\vdash \perp$, und sei $x := x_n$, $\alpha := \alpha_n$, $c := c_{x,\alpha}$. Nach (a) ist $X' \cup \{\neg \alpha^x\} \vdash \perp$. Mit \mathcal{C}^+ folgt daraus $X' \vdash \alpha^x$. Daher $X' \vdash \neg \forall x \alpha, \alpha \stackrel{c}{x}$ nach ($\wedge 2$). Aber $X' \vdash \alpha \stackrel{c}{x}$ ergibt $X' \vdash \forall x \alpha$ nach ($\forall 3$), weil c in X' und α nicht vorkommt. Also $X' \vdash \forall x \alpha, \neg \forall x \alpha$ und somit $X' \vdash \perp$, im Widerspruch zu (b). \square

$X \subseteq \mathcal{L}$ heiße eine *Henkin-Menge*, wenn X die beiden folgenden Bedingungen erfüllt:

- (H1) $X \vdash \neg \alpha \Leftrightarrow X \not\vdash \alpha$,
- (H2) $X \vdash \forall x \alpha \Leftrightarrow X \vdash \alpha \stackrel{c}{x}$ für alle Konstanten c in \mathcal{L} .

Eine Henkin-Menge hat immer die bemerkenswerte und nützliche Eigenschaft

- (H3) Zu jedem Term t gibt es eine Konstante c mit $X \vdash t = c$.

Denn $X \vdash \exists x t = x$ ($= \neg \forall x t \neq x$) für ein x nach Beispiel 3 in 3.1. Daher $X \not\vdash \forall x t \neq x$ nach (H1). Folglich gibt es nach (H2) ein c mit $X \not\vdash t \neq c$ und (H1) liefert dann $X \vdash t = c$. Es sei erwähnt, dass konsistente Mengen im Rahmen der Ausgangssprache in der Regel nicht in Henkin-Mengen einbettbar sind.

Lemma 2.4. *Sei $X \subseteq \mathcal{L}$ konsistent. Dann existiert eine Henkin-Menge $Y \supseteq X$ in einer geeigneten Konstantenexpansion \mathcal{LC} von \mathcal{L} .*

Beweis. Sei $\mathcal{L}_0 := \mathcal{L}$, $X_0 := X$ und seien \mathcal{L}_n , X_n schon erklärt. \mathcal{L}_{n+1} entstehe aus \mathcal{L}_n durch Hinzunahme neuer Konstanten $c_{x,\alpha,n}$ für alle $x \in \text{Var}$, $\alpha \in \mathcal{L}_n$; genauer $\mathcal{L}_{n+1} = \mathcal{L}_n C_n$, mit der Menge C_n der Konstanten $c_{x,\alpha,n}$. Ferner sei $X_{n+1} = X_n \cup \Gamma_{\mathcal{L}_n}$, wobei $\Gamma_{\mathcal{L}_n}$ definiert sei wie in Lemma 2.3, also $X_{n+1} \subseteq \mathcal{L}_{n+1}$. Nach Lemma 2.3 ist $X_n \not\vdash \perp$ für alle n . Sei $U := \bigcup_{n \in \mathbb{N}} X_n$, also $U \subseteq \bigcup_{n \in \mathbb{N}} \mathcal{L}_n = \mathcal{LC}$ mit $C := \bigcup_{n \in \mathbb{N}} C_n$. Es ist $U \not\vdash \perp$. Denn U ist als Vereinigung einer Kette konsistenter Mengen sicher konsistent in \mathcal{LC} . Sei $\alpha \in \mathcal{LC}$ und $x \in \text{Var}$, sagen wir $\alpha \in \mathcal{L}_n$ mit minimalem n , und sei α^x die wie vor Lemma 2.3, jetzt aber bezüglich \mathcal{L}_n konstruierte Formel. Dann gehört $\neg \alpha^x$ zu X_{n+1} . Also gilt $(*) \neg \alpha^x \in U$. Sei (H, \subseteq) die Halbordnung aller konsistenten Erweiterungen von U in \mathcal{LC} . Jede Kette $K \subseteq H$ hat die obere Schranke $\bigcup K$ in H , weil mit allen Gliedern der Kette K auch $\bigcup K$ konsistent ist. Auch ist $H \neq \emptyset$, denn $U \in H$. Nach dem Zornschen Lemma enthält H daher ein maximales Element Y . Kurzum, Y ist eine maximal konsistente Obermenge von U , und was hier wesentlich ist, zugleich eine Henkin-Menge. Hier der einfache Nachweis:

(H1) \Rightarrow : $Y \vdash \neg \alpha$ impliziert $Y \not\vdash \alpha$ wegen der Konsistenz von Y . \Leftarrow : Mit $Y \not\vdash \alpha$ ist sicher $\alpha \notin Y$. Folglich $Y, \alpha \vdash \perp$ wegen der maximalen Konsistenz von Y , und gemäß C^- somit $Y \vdash \neg \alpha$.

(H2) \Rightarrow : Klar nach $(\forall 1)$. \Leftarrow : Sei $Y \vdash \alpha \frac{c}{x}$ für alle c in \mathcal{LC} , also auch $Y \vdash \alpha \frac{c}{x}$ mit $c := c_{x,\alpha,n}$, wobei n minimal sei mit $\alpha \in \mathcal{L}_n$. Angenommen $Y \not\vdash \forall x \alpha$. Dann gilt $Y \vdash \neg \forall x \alpha$ gemäß (H1). Das ergibt $Y \vdash \neg \forall x \alpha \wedge \alpha \frac{c}{x} = \alpha^x$ nach $(\wedge 1)$. Nun steht $Y \vdash \alpha^x$ wegen der Konsistenz von Y aber im Widerspruch mit $Y \vdash \neg \alpha^x$, was wegen $(*)$ weiter oben trivial ist. Es gilt also doch $Y \vdash \forall x \alpha$. \square

Lemma 2.5. *Jede Henkin-Menge $Y \subseteq \mathcal{L}$ besitzt ein Modell.*

Beweis. Das im Folgenden konstruierte Modell heißt auch ein *Termmodell*. Es sei $t \approx t'$, falls $Y \vdash t = t'$. Dies ist eine Kongruenz in der Termalgebra \mathcal{T} von \mathcal{L} , d.h.

- (a) \approx ist eine Äquivalenzrelation,
- (b) $t_1 \approx t'_1, \dots, t_n \approx t'_n \Rightarrow f\vec{t} \approx f\vec{t}'$, für jedes $f \in L$.

Die Behauptung (a) folgt unmittelbar aus $Y \vdash t = t$ und Beispiel 1 in 3.1, und (b) ist nur eine andere Formulierung von Beispiel 2(b).

Es sei nun $A := \{\bar{t} \mid t \in \mathcal{T}\}$, wobei \bar{t} die Äquivalenzklasse von t bezüglich \approx bezeichnet, so dass also $\bar{t} = \bar{s} \Leftrightarrow Y \vdash t = s$. Diese Menge A der Äquivalenzklassen von \mathcal{T} ist der Träger des gesuchten Modells $\mathcal{M} = (\mathcal{A}, w)$ für Y . Die Faktorisierung von \mathcal{T} wird sichern, dass $=$ die Identität im Modell bedeutet. Sei C die Menge der Konstanten von \mathcal{L} . Nach (H3) gibt es zu jedem Term t aus \mathcal{T} ein $c \in C$ mit $c \approx t$.

Daher ist sogar $A = \{\bar{c} \mid c \in C\}$. Sei $x^{\mathcal{M}} := \bar{x}$ und $c^{\mathcal{M}} := \bar{c}$ für Variablen und Konstanten von \mathcal{L} . Operationszeichen f seien interpretiert durch

$$f^{\mathcal{M}}(\bar{t}_1, \dots, \bar{t}_n) = \overline{ft_1 \cdots t_n}.$$

Diese Definition ist korrekt, d.h. repräsentantenunabhängig, weil \approx eine Kongruenz ist. Schließlich erklären wir $r^{\mathcal{M}}$ für ein n -stelliges Relationszeichen r durch

$$r^{\mathcal{M}}\bar{t}_1 \cdots \bar{t}_n \Leftrightarrow Y \vdash r\vec{t}.$$

Auch diese Definition ist korrekt, weil $Y \vdash r\vec{t} \Rightarrow Y \vdash r\vec{t}'$, wenn $t_1 \approx t'_1, \dots, t_n \approx t'_n$ gemäß Beispiel 2(d) in 3.1. Induktiv ergeben sich nunmehr

$$(c) \quad t^{\mathcal{M}} = \bar{t} \quad ; \quad (d) \quad \mathcal{M} \models \alpha \Leftrightarrow Y \vdash \alpha,$$

von denen (d) als das Ziel der Konstruktionen angesehen werden kann. (c) ist klar für Primterme, und die Induktionsannahme $t_i^{\mathcal{M}} = \bar{t}_i$ für $i = 1, \dots, n$ liefert

$$(f\vec{t})^{\mathcal{M}} = f^{\mathcal{M}}(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}) = f^{\mathcal{M}}(\bar{t}_1, \dots, \bar{t}_n) = \overline{ft_1 \cdots t_n}.$$

(d) ergibt sich durch Induktion über $\text{rg } \alpha$. Man beginnt mit Formeln vom Rang 0 (Primformeln). Die Induktionsschritte verlaufen unter Beachtung von $\text{rg } \alpha < \text{rg } \neg\alpha$, $\text{rg } \alpha, \text{rg } \beta < \text{rg } (\alpha \wedge \beta)$ und $\text{rg } \alpha \frac{c}{x} < \text{rg } \forall x \alpha$ genau wie bei der Formelinduktion.

$$\begin{aligned} \mathcal{M} \models t \equiv s &\Leftrightarrow t^{\mathcal{M}} = s^{\mathcal{M}} &\Leftrightarrow \bar{t} = \bar{s} &\quad (\text{wegen (c)}) \\ &&\Leftrightarrow Y \vdash t = s. \\ \mathcal{M} \models r\vec{t} &\Leftrightarrow r^{\mathcal{M}}t_1^{\mathcal{M}} \cdots t_n^{\mathcal{M}} &\Leftrightarrow r^{\mathcal{M}}\bar{t}_1 \cdots \bar{t}_n &\Leftrightarrow Y \vdash r\vec{t}. \\ \mathcal{M} \models \alpha \wedge \beta &\Leftrightarrow \mathcal{M} \models \alpha, \beta &\Leftrightarrow Y \vdash \alpha, \beta &\quad (\text{Induktionsannahme}) \\ &&\Leftrightarrow Y \vdash \alpha \wedge \beta &\quad (\text{gemäß } (\wedge 1), (\wedge 2)). \\ \mathcal{M} \models \neg\alpha &\Leftrightarrow \mathcal{M} \not\models \alpha &\Leftrightarrow Y \not\vdash \alpha &\quad (\text{Induktionsannahme}) \\ &&\Leftrightarrow Y \vdash \neg\alpha &\quad (\text{gemäß (H1)}). \\ \mathcal{M} \models \forall x \alpha &\Leftrightarrow \mathcal{M}_x^{\bar{c}} \models \alpha \text{ für alle } c \in C &\quad (\text{weil } A = \{\bar{c} \mid c \in C\}) \\ &\Leftrightarrow \mathcal{M}_x^{c^{\mathcal{M}}} \models \alpha \text{ für alle } c \in C &\quad (\text{weil } c^{\mathcal{M}} = \bar{c}) \\ &\Leftrightarrow \mathcal{M} \models \alpha \frac{c}{x} \text{ für alle } c \in C &\quad (\text{Substitutionssatz}) \\ &\Leftrightarrow Y \vdash \alpha \frac{c}{x} \text{ für alle } c \in C &\quad (\text{Induktionsannahme}) \\ &\Leftrightarrow Y \vdash \forall x \alpha &\quad (\text{gemäß (H2)}). \end{aligned}$$

Weil $Y \vdash \alpha$ für $\alpha \in Y$, folgt aus (d) unmittelbar $\mathcal{M} \models Y$. \square

Hiermit ergibt sich nun genau wie in der Aussagenlogik die Gleichwertigkeit von Konsistenz und Erfüllbarkeit, sowie auch die Vollständigkeit von \vdash .

Satz 2.6 (Modellexistenzsatz). *Sei $X \subseteq \mathcal{L}$ konsistent. Dann hat X ein Modell.*

Beweis. Sei $Y \supseteq X$ eine Henkin-Menge in einer Konstantenerweiterung \mathcal{LC} gemäß Lemma 2.4. Nach Lemma 2.5 hat Y und damit auch X ein \mathcal{LC} -Modell \mathcal{M}' . Sei \mathcal{M} das \mathcal{L} -Redukt von \mathcal{M}' , d.h. man „vergesse“ die Interpretation der nicht in \mathcal{L} vorkommenden Konstanten. Nach Satz 2.3.1 ist dann auch $\mathcal{M} \models X$. \square

Satz 2.7 (Vollständigkeitssatz). *Für $X \subseteq \mathcal{L}$ und $\alpha \in \mathcal{L}$ ist $X \vdash \alpha \Leftrightarrow X \models \alpha$.*

Beweis. Die Korrektheit von \vdash besagt $X \vdash \alpha \Rightarrow X \models \alpha$. Die Umkehrung folgt indirekt. Sei $X \not\models \alpha$, so dass $X, \neg\alpha$ nach \mathcal{C}^+ konsistent ist. Satz 2.6 liefert dann ein Modell für $X \cup \{\neg\alpha\}$. Folglich ist $X \not\models \alpha$. \square

Nach diesem Satz können die Symbole \models und \vdash künftig wechselseitig ausgetauscht werden. Oft schreibt man $X \vdash \alpha$ und verifiziert dies durch den Nachweis von $X \models \alpha$. Speziell für Theorien T ist $T \models \alpha$ gleichwertig mit $T \vdash \alpha$, wofür fortan meist $\vdash_T \alpha$ geschrieben wird. Allgemeiner stehe $X \vdash_T \alpha$ für $X \cup T \vdash \alpha$, und $\alpha \vdash_T \beta$ für $\{\alpha\} \vdash_T \beta$. Auch wird z.B. $\alpha \vdash_T \beta \ \& \ \beta \vdash_T \gamma$ gelegentlich zu $\alpha \vdash_T \beta \vdash_T \gamma$ verkürzt.

Gleichwertigkeiten wie z.B. die von $\alpha \vdash_T \beta$, $\vdash_T \alpha \rightarrow \beta$ und $\vdash_{T+\alpha} \beta$, ebenso wie die von $\vdash_T \alpha$ und $\vdash_T \alpha^\forall$, werden in den folgenden Kapiteln ohne besonderen Hinweis benutzt. Das betrifft auch die in Übung 5 genannten Eigenschaften.

Übungen

1. Man zeige, $X \subseteq \mathcal{L}$ ist maximal konsistent genau dann, wenn es ein Modell \mathcal{M} gibt mit $\alpha \in X \Leftrightarrow \mathcal{M} \models \alpha$, für alle $\alpha \in \mathcal{L}$.
2. Sei $X \subseteq \mathcal{L}$ eine konsistente Menge *gleichheitsfreier* oder $=$ -freier \forall -Formeln, d.h. $=$ kommt in X nicht vor. Sei etwa $\mathcal{M} \models X$. Man konstruiere ein Modell $\mathfrak{T} \models X$, dessen Träger die Menge \mathcal{T} aller \mathcal{L} -Terme ist. Dabei sei $c^{\mathfrak{T}} := c$, $f^{\mathfrak{T}}\vec{t} := f\vec{t}$, $x^{\mathfrak{T}} = x$ (was leicht $t^{\mathfrak{T}} := t$ für alle t impliziert), und $r^{\mathfrak{T}}\vec{t} := r^{\mathcal{M}}\vec{t}$. In diesem „Termmodell“ \mathfrak{T} gilt also $\mathfrak{T} \models t_1 = t_2 \Leftrightarrow t_1 = t_2$.
3. Sei K eine nichtleere Kette von Theorien in \mathcal{L} , was heißen soll $T \subseteq T'$ oder $T' \subseteq T$ für alle $T, T' \in K$. Man zeige, auch $\bigcup K$ ist eine Theorie, und diese ist konsistent genau dann, wenn alle $T \in K$ konsistent sind.
4. Sei T konsistent und $Y \subseteq \mathcal{L}$. Man beweise die Gleichwertigkeit von
(i) $Y \vdash_T \perp$, (ii) $\vdash_T \neg\alpha$ für eine Konjunktion α von Formeln aus Y .
5. Sei $x \notin \text{var } t$ und $\alpha, \frac{t}{x}$ kollisionsfrei. Man beweise die Gleichwertigkeit von
(i) $\vdash_T \alpha \frac{t}{x}$, (ii) $x = t \vdash_T \alpha$, (iii) $\vdash_T \forall x(x = t \rightarrow \alpha)$, (iv) $\vdash_T \exists x(x = t \wedge \alpha)$.

3.3 Erste Anwendungen – Nichtstandardmodelle

Wir werden in diesem Abschnitt wichtige Konsequenzen aus dem Vollständigkeitssatz und dem entsprechenden Modellkonstruktionsverfahren ziehen. Weil für die Beweisbarkeitsrelation \vdash der Endlichkeitssatz gilt, ergibt Satz 2.7 unmittelbar den

Satz 3.1 (Endlichkeitssatz für das Folgern). $X \models \alpha$ impliziert $X_0 \models \alpha$ für eine endliche Teilmenge $X_0 \subseteq X$.

Betrachten wir ein erstes Anwendungsbeispiel. Die Theorie der Körper der Charakteristik 0 ist axiomatisiert durch die Menge X , bestehend aus den Körperaxiomen und den Formeln $\neg \text{char}_p$ (Seite 39). Wir behaupten

- (1) *Eine in allen Körpern der Charakteristik 0 gültige Aussage α gilt bereits in allen Körpern hinreichend hoher, von α abhängiger Primzahlcharakteristik p .*

Denn wegen $X \models \alpha$ ist schon $X_0 \models \alpha$ für eine endliche Teilmenge $X_0 \subseteq X$. Ist p eine Primzahl größer als alle Primzahlen q mit $\neg \text{char}_q \in X_0$, so gilt α schon in allen Körpern der Charakteristik p , denn diese erfüllen X_0 . Also gilt (1). Daraus erhält man z.B. den in $\mathcal{L}\{0, 1, +, \cdot\}$ leicht formulierbaren Sachverhalt, dass zwei vorgegebene, über allen Körpern der Charakteristik 0 teilerfremde Polynome bereits über allen Körpern hinreichend hoher Primzahlcharakteristik teilerfremd sind.

Eine bemerkenswerte Folge von Satz 3.1 ist auch die nichtendliche Axiomatisierbarkeit vieler elementarer Theorien. Bevor wir Beispiele präsentieren, erläutern wir endliche Axiomatisierbarkeit gleich in einem etwas größeren Rahmen.

Eine Menge Z von Zeichenfolgen über einem vorgegebenen Alphabet A heißt *entscheidbar*, wenn es einen Algorithmus (ein mechanisches Rechenverfahren) gibt, welches uns nach endlich vielen Rechenschritten die Frage beantwortet, ob eine Zeichenfolge ξ aus Symbolen von A zu Z gehört oder nicht; andernfalls heißt Z *unentscheidbar*. So ist gewiss entscheidbar, ob ξ eine Formel ist. Das alles ist zwar anschaulich plausibel, bedarf jedoch einer (in 6.2 vorgenommenen) Präzisierung. Eine Theorie T heißt *rekursiv axiomatisierbar*, oft auch nur *axiomatisierbar* genannt, wenn sie ein entscheidbares Axiomensystem besitzt. Dies ist z.B. der Fall, wenn T *endlich axiomatisierbar* ist, d.h. ein endliches Axiomensystem besitzt.

Aus (1) folgt sofort, dass die Theorie der Körper der Charakteristik 0 nicht endlich axiomatisierbar ist. Denn wäre E eine endliche Axiomenmenge, so hätte deren Konjunktion $\bigwedge E$ nach (1) als Modell auch einen Körper endlicher Charakteristik.

Hier noch ein weiteres instruktives Beispiel. Eine abelsche Gruppe \mathcal{G} heißt *n -dividierbar*, wenn $\mathcal{G} \models \vartheta_n := \forall x \exists y x = ny$, und *dividierbar*, wenn $\mathcal{G} \models \vartheta_n$ für alle $n \geq 1$, wobei

$$ny := \underbrace{y + \cdots + y}_n.$$

Die Theorie **DAG** dieser Gruppen ist axiomatisiert durch die Menge X , bestehend aus den Axiomen für abelsche Gruppen plus allen ϑ_n . Auch **DAG** ist nicht endlich axiomatisierbar. Dies folgt wie oben leicht aus

- (2) *Jede in allen dividierbaren abelschen Gruppen gültige Aussage $\alpha \in \mathcal{L}\{+, 0\}$ gilt auch in mindestens einer nichtdividierbaren abelschen Gruppe.*

Zum Nachweis von (2) sei $\alpha \in \mathbf{DAG}$, oder gleichwertig, $X \models \alpha$. Nach Satz 3.1 ist bereits $X_0 \models \alpha$ für ein endliches $X_0 \subseteq X$. Sei \mathbb{Z}_p die zyklische Gruppe der Ordnung p , wobei p eine Primzahl $> n$ für alle n mit $\vartheta_n \in X_0$ sei. Die Abbildung $x \mapsto nx$ von \mathbb{Z}_p in sich ist für $1 \leq n < p$ surjektiv – sonst wäre $\{na \mid a \in \mathbb{Z}_p\}$ doch echte Untergruppe von \mathbb{Z}_p . Daher ist $\mathbb{Z}_p \models \vartheta_n$ für $1 \leq n < p$. Also $\mathbb{Z}_p \models X_0$ und somit $\mathbb{Z}_p \models \alpha$. Aber \mathbb{Z}_p ist nicht p -dividierbar, weil $px = 0$ für $x \in \mathbb{Z}_p$. Genauso zeigt man auch die nichtendliche Axiomatisierbarkeit der Theorie der *torsionsfreien* abelschen Gruppen, d.h. $na \neq 0$ für alle $n \neq 0$ und $a \neq 0$.

Auf ähnliche Weise lässt sich die nichtendliche Axiomatisierbarkeit vieler Theorien beweisen. Oft erfordert dies tiefere Hilfsmittel als in den obigen Beispielen. Betrachten wir z.B. die mit **ACF** (von algebraically closed fields) bezeichnete Theorie der algebraisch abgeschlossenen Körper, welche aus der Körpertheorie durch Hinzufügen des Schemas aller Aussagen

$$\forall a_0 \dots \forall a_n \exists x \, x^{n+1} + a_n x^n + \dots + a_1 x + a_0 = 0 \quad (n = 0, 1, \dots)$$

entsteht. Diese Formeln besagen, dass jedes *normierte* Polynom (der Term links in der Gleichung, der Kürze halber *Hauptpolynom* genannt; diese sind immer von positivem Grade) eine Nullstelle hat. Die nichtendliche Axiomatisierbarkeit von **ACF** läuft auf den keineswegs trivialen Existenznachweis von Körpern hinaus, für die alle Polynome bis zu einem gegebenen Grad zerfallen, aber immer noch irreduzible Polynome von höherem Grade existieren.

Wie in der Aussagenlogik ergibt der Endlichkeitssatz für das Folgern leicht den

Satz 3.2 (Kompaktheitssatz). *Eine Formelmenge X ist erfüllbar, falls jede endliche Teilmenge von X erfüllbar ist.*

Dieser Satz ist wegen der größeren Ausdruckskraft prädikatenlogischer Sprachen in gewissen Anwendungen etwas handlicher als der aussagenlogische Kompaktheitsatz. Er liefert seinerseits leicht einen Beweis von Satz 3.1 und lässt sich auf unterschiedliche Weise auch ohne Bezug auf einen Logikkalkül beweisen, z.B. mittels Ultraprodukten, siehe 5.7. Er kann auch auf den aussagenlogischen Kompaktheitsatz zurückgeführt werden, siehe die Bemerkung 1 Seite 108. In den Anwendungen des Satzes beschränken wir uns zunächst auf die Konstruktion sogenannter Nichtstandardmodelle, führen vorher aber noch einige wichtige Begriffe ein.

Eine Theorie T ($\subseteq \mathcal{L}^0$) heie *vollstndig*, wenn sie konsistent ist und keine echte konsistente Erweiterungstheorie in derselben Sprache mehr besitzt. Entweder ist dann $\vdash_T \alpha$ oder $\vdash_T \neg\alpha$, fr jedes $\alpha \in \mathcal{L}^0$. So ist $Th\mathcal{A}$ fr beliebiges \mathcal{A} , immer vollstndig. Oft wird uns z.B. die Theorie $Th\mathcal{N}$ mit $\mathcal{N} = (\mathbb{N}, 0, \mathbf{S}, +, \cdot)$ begegnen, mit der *Nachfolgerfunktion* $\mathbf{S}: n \mapsto n+1$. Von den in \mathcal{N} definierbaren Relationen und Funktionen nennen wir hier nur \leq , definiert z.B. durch $x \leq y \leftrightarrow \exists z z + x = y$, und die *Vorgngerfunktion* $\mathbf{R}: \mathbb{N} \rightarrow \mathbb{N}$, definiert durch $y = \mathbf{R}x \leftrightarrow x = 0 \wedge y = 0 \vee x = \mathbf{S}y$.

Noch hufiger werden uns gewisse axiomatische Theorien in der arithmetischen Sprache $\mathcal{L}_{ar} := \mathcal{L}\{0, \mathbf{S}, +, \cdot\}$ begegnen, speziell die sogenannte *Peano-Arithmetik* PA. Die Axiome dieser fr viele Fragen der mathematischen Grundlagenforschung und auch der theoretischen Informatik bedeutsamen Theorie lauten wie folgt:

$$\begin{aligned} &\forall x \mathbf{S}x \neq 0, & \forall x x + 0 = x, & \forall x x \cdot 0 = 0, \\ &\forall xy (\mathbf{S}x = \mathbf{S}y \rightarrow x = y), & \forall xy x + \mathbf{S}y = \mathbf{S}(x + y), & \forall xy x \cdot \mathbf{S}y = x \cdot y + x, \\ &\text{IS: } \varphi \frac{0}{x} \wedge \forall x (\varphi \rightarrow \varphi \frac{\mathbf{S}x}{x}) \rightarrow \forall x \varphi. \end{aligned}$$

IS heit das *Induktionsschema*. Darin ist $\varphi = \varphi(x, \vec{y})$ eine beliebige Formel aus \mathcal{L}_{ar} . Daher lautet IS eigentlich $(\varphi \frac{0}{x} \wedge \forall x (\varphi \rightarrow \varphi \frac{\mathbf{S}x}{x}) \rightarrow \forall x \varphi)^\forall$ wie in 2.5 verabredet. IS ergibt z.B. $\vdash_{PA} (\forall x \neq 0) \exists v \mathbf{S}v = x$, was man obigen Axiomen nicht unmittelbar ansieht. Denn sei $\varphi := x \neq 0 \rightarrow \exists v \mathbf{S}v = x$. Gewiss ist $\vdash_{PA} \varphi \frac{0}{x}$ (*Induktionsanfang*). Weil $\mathbf{S}v = x \vdash_{PA} \mathbf{S}\mathbf{S}v = \mathbf{S}x$, folgt $\exists v \mathbf{S}v = x \vdash_{PA} \exists v \mathbf{S}v = \mathbf{S}x$ nach (f) und (e) Seite 62. Das ergibt leicht (i) $\varphi \vdash_{PA} \varphi \frac{\mathbf{S}x}{x}$ oder gleichwertig (ii) $\vdash_{PA} \forall x (\varphi \rightarrow \varphi \frac{\mathbf{S}x}{x})$. Damit folgt $\vdash_{PA} \forall x \varphi$ gem IS. Der Nachweis von (i) oder gleichwertig (ii) heit hier und bei anderen Anwendungen von IS der *Induktionsschritt*.

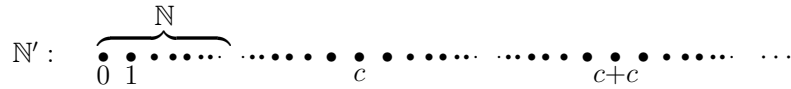
Bemerkung 1. In 7.1 begegnen uns sehr komplexe Induktionen und es wird schnell klar, dass PA die elementare Zahlentheorie voll umfasst. Nicht nur diese, sondern praktisch die gesamte sogenannte diskrete Mathematik kann in PA entwickelt werden. Die Wahl der Signatur ist eine Sache der Bequemlichkeit. Man knnte z.B. \mathbf{S} durch die Konstante 1 ersetzen und mit etwas Umstndlichkeit die Axiome auch allein in $+, \cdot$ formulieren. Dass in PA nicht unbeschrnkt subtrahiert werden kann, ist unerheblich. Eine hnlich wie PA formulierte Theorie der ganzen Zahlen ist fr zahlentheoretische Zwecke gelegentlich zwar bequemer, nicht aber strenger als PA, weil sie in PA interpretierbar ist, siehe hierzu 6.6.

Satz 3.2 ergibt leicht, dass nicht nur PA, sondern auch die vollstndige Theorie $Th\mathcal{N}$ neben dem Standardmodell \mathcal{N} weitere, zu \mathcal{N} nicht isomorphe Modelle besitzt, sogenannte *Nichtstandardmodelle*. In diesen gelten genau dieselben Stze wie in \mathcal{N} . Der Existenzbeweis fr ein Nichtstandardmodell \mathcal{N}' von $Th\mathcal{N}$ ist frappierend einfach. Sei $x \in \text{Var}$ und $X := Th\mathcal{N} \cup \{\underline{n} < x \mid n \in \mathbb{N}\}^2$. Dabei bezeichne \underline{n} hier und berall den Term $\mathbf{S}^n 0 := \underbrace{\mathbf{S} \cdots \mathbf{S}}_n 0$ (statt $\underline{0}$ schreibt man nur 0). Also $\underline{1} = \mathbf{S}0$, $\underline{2} = \mathbf{S}\underline{1}$ usw.

²⁾ $\underline{n} < x$ ist die \mathcal{L}_{ar} -Formel $\exists z z + x = \underline{n} \wedge \underline{n} \neq x$. Oft wird hier x durch eine neue Konstante ersetzt, also eine Spracherweiterung vorgenommen. Beide Anstze liefern jedoch dasselbe.

Jede endliche Teilmenge $X_0 \subseteq X$ besitzt ein Modell. Denn offenbar gibt es ein m mit $X_0 \subseteq X_1 := Th\mathcal{N} \cup \{\underline{n} < x \mid n < m\}$, und X_1 hat sicher ein Modell; man braucht x in \mathcal{N} ja nur mit der Zahl m zu belegen. Nach Satz 3.2 hat X ein Modell (\mathcal{N}', c) mit dem Träger \mathbb{N}' , wobei $c \in \mathbb{N}'$ die Interpretation von x bezeichnet. Weil \mathcal{N}' alle in \mathcal{N} gültigen Aussagen erfüllt – wozu insbesondere die Aussagen $\underline{Sn} = \underline{Sn}$, $\underline{n} + \underline{m} = \underline{n+m}$, $\underline{n} \cdot \underline{m} = \underline{n \cdot m}$, sowie $\underline{n} \neq \underline{m}$ für $n \neq m$ gehören – ist klar, dass $n \mapsto \underline{n}^{\mathcal{N}'}$ eine Einbettung von \mathcal{N} in \mathcal{N}' darstellt, deren Bild man sich mit \mathcal{N} identifiziert denken kann³⁾. Man darf also von $\underline{n}^{\mathcal{N}'} = n$, d.h. von $\mathcal{N} \subseteq \mathcal{N}'$ ausgehen.

Wegen $\mathcal{N}' \models X$ ist \mathcal{N}' einerseits elementar-äquivalent zu \mathcal{N} , andererseits ist $n < a$ für alle n und $a \in \mathbb{N}' \setminus \mathbb{N}$, denn in \mathcal{N} und damit in \mathcal{N}' gilt $x \leq \underline{n} \rightarrow x = 0 \vee \dots \vee x = \underline{n}$. Kurzum, \mathbb{N} ist ein (echter) Anfang von \mathbb{N}' , oder \mathcal{N}' ist eine *Enderweiterung* von \mathcal{N} . Die Elemente aus $\mathbb{N}' \setminus \mathbb{N}$ heißen die *Nichtstandardzahlen* von \mathcal{N}' . Nebst c sind auch $c+c$ und alle $c+n$ für $n \in \mathbb{N}$ Beispiele. Auch muss c einen unmittelbaren Vorgänger bezüglich der Anordnung von \mathcal{N}' haben, weil $\mathcal{N}' \models (\forall x \neq 0) \exists y x = Sy$. Folgende Figur gibt eine grobe Veranschaulichung eines Nichtstandardmodells \mathcal{N}' :



\mathcal{N}' hat dieselben zahlentheoretischen Eigenschaften wie \mathcal{N} – jedenfalls alle in der Sprache \mathcal{L}_{ar} formulierbaren und dazu gehören fast alle interessanten wie sich in 7.1 herausstellen wird. So gilt z.B. $\forall x \exists y (x = \underline{2y} \vee x = \underline{2y+1})$ in jedem Modell von $Th\mathcal{N}$, also ist auch jede Nichtstandardzahl gerade oder ungerade. Wie man sieht, enthält \mathbb{N}' Lücken im Sinne von 2.1, z.B. ist $(\mathbb{N}, \mathbb{N}' \setminus \mathbb{N})$ eine solche.

Bemerkung 2. Satz 4.1 wird zeigen, dass $Th\mathcal{N}$ auch abzählbare Nichtstandardmodelle \mathcal{N}' hat. Die Anordnung eines derartigen \mathcal{N}' ist leicht zu veranschaulichen: Sie entsteht aus dem halboffenen Intervall $[0, 1)$ rationaler Zahlen dadurch, dass man 0 durch \mathbb{N} und jedes andere $r \in [0, 1)$ durch ein Exemplar von \mathbb{Z} ersetzt. Trotz dieser einfachen Kennzeichnung von $<^{\mathcal{N}'}$ sind weder $+^{\mathcal{N}'}$ noch $\cdot^{\mathcal{N}'}$ effektiv beschreibbar, siehe [BJ] oder [HP].

Ersetzt man IS im Axiomensystem für PA durch das sogenannte *Induktionsaxiom*

$$\text{IA: } \forall P (P0 \wedge \forall x (Px \rightarrow P Sx) \rightarrow \forall x Px) \quad (P \text{ eine Prädikatenvariable}),$$

so ist das entstehende Axiomensystem *kategorisch*, d.h. es hat bis auf Isomorphie nur genau ein Modell (siehe z.B. [Ra3]). Wie erklärt sich, dass \mathcal{N} durch wenige Axiome bis auf Isomorphie eindeutig festgelegt ist, andererseits aber Nichtstandardmodelle für $Th\mathcal{N}$ existieren? Die Antwort ist: IA ist in \mathcal{L}_{ar} nicht adäquat formulierbar. Es ist kein Axiom der elementaren Sprache von \mathcal{N} oder irgendeiner anderen Sprache der

³⁾Immer wenn \mathcal{A} in \mathcal{B} einbettbar ist, gibt es eine zu \mathcal{B} isomorphe Struktur \mathcal{B}' mit $\mathcal{A} \subseteq \mathcal{B}'$, welche dadurch entsteht, dass man die Bilder der Elemente von \mathcal{A} durch ihre Originale „austauscht“.

1. Stufe. IA ist eine Aussage der 2. Stufe, über die in **3.7** mehr gesagt wird. Die sich hier andeutende Beschränktheit in den Formulierungsmöglichkeiten durch Sprachen 1. Stufe ist in Wahrheit aber nur eine scheinbare, wie die weiteren Ausführungen, speziell zur axiomatischen Mengenlehre, zeigen werden.

In keinem Nichtstandardmodell \mathcal{N}' ist das Anfangssegment \mathbb{N} definierbar, auch nicht *parameterdefinierbar*, d.h. es gibt kein $\alpha = \alpha(x, \vec{y})$ und keine $b_1, \dots, b_n \in \mathbb{N}'$ derart, dass $\mathbb{N} = \{a \in \mathbb{N}' \mid \mathcal{N}' \models \alpha[a, \vec{b}]\}$. Sonst nämlich wäre $\mathcal{N}' \models \alpha \frac{0}{x} \wedge \forall x(\alpha \rightarrow \alpha \frac{sx}{x})[\vec{b}]$. Das ergibt $\mathcal{N}' \models \forall x \alpha[\vec{b}]$ nach IS, im Widerspruch zu $\mathbb{N}' \setminus \mathbb{N} \neq \emptyset$. Dasselbe Argument zeigt: kein echter Anfang $A \subset \mathbb{N}'$ ohne größtes Element ist in \mathbb{N}' definierbar. Weil ein solches A offenbar eine Lücke in der Ordnung von \mathbb{N}' definiert, lässt sich dies auch so formulieren: Lücken in \mathbb{N}' sind „von innen nicht erkennbar“.

Grundkurse über Analysis vermitteln oft den Eindruck, eine sinnvoll betriebene Analysis erfordere unabdingbar das Stetigkeitsaxiom: *Jede nichtleere beschränkte Menge reeller Zahlen hat ein Supremum*. Darauf gründet sich die von Cauchy und Weierstraß geformte Analysis, welche die ursprünglichen, etwas mysteriösen Infinitesimalargumente von Leibniz, Newton und Euler aus der Mathematik verbannte. Die mathematische Logik hat nun aber Hilfsmittel entwickelt, die die ursprünglichen Argumente weitgehend rechtfertigen. Dies geschieht im Rahmen der vor allem von A. Robinson entwickelten *Nichtstandard-Analysis*, deren Grundidee wir nachfolgend andeutungsweise beschreiben.

Dieselbe Konstruktion wie für \mathcal{N} liefert auch Nichtstandardmodelle für die Theorie von $\mathcal{R} = (\mathbb{R}, +, \cdot, <, \{\mathbf{a} \mid a \in \mathbb{R}\})$, wobei für jede reelle Zahl a ein Name \mathbf{a} in die Signatur mit aufgenommen wurde. Durch Betrachtung der konsistenten Formelmengen $\text{Th } \mathcal{R} \cup \{\mathbf{a} < x \mid a \in \mathbb{R}\}$ – jede endliche Teilmenge hat ein Modell mit dem Träger \mathbb{R} – erhält man wie oben echte Erweiterungen \mathcal{R}^* von \mathcal{R} , sogenannte *Nichtstandardmodelle der Analysis*, in denen dieselben Sätze gelten wie in \mathcal{R} . So zerfällt auch in \mathcal{R}^* jedes Polynom von positivem Grade in lineare und quadratische Faktoren.

Für die Analysis ist nun entscheidend, dass die Sprache von vornherein bereichert werden kann, etwa durch Hinzunahme der Symbole \exp, \ln, \sin, \cos für die exponentialen, logarithmischen, trigonometrischen Funktionen und weiterer Symbole für weitere Funktionen. Wir bezeichnen ein so expandiertes Standardmodell wiederum mit \mathcal{R} und ein entsprechendes Nichtstandardmodell mit \mathcal{R}^* . Die erwähnten, in \mathcal{R} vorhandenen reellen Funktionen setzen sich unter Bewahrung aller derjenigen Eigenschaften auf \mathcal{R}^* fort, die sich elementar formulieren lassen, und dazu zählen fast alle für die Anwendungen interessanten. Bekannte Beispiele sind

$$\forall xy \exp(x+y) \equiv \exp x \cdot \exp y, \quad (\forall x > 0) \exp \ln x \equiv x, \quad \forall x \sin^2 x + \cos^2 x = 1,$$

ferner die Additionstheoreme für die trigonometrischen Funktionen usw. Alle diese

Funktionen bleiben stetig und beliebig oft differenzierbar. Die Übertragbarkeit betrifft allerdings nicht den Satz von Bolzano-Weierstraß und andere topologische Eigenschaften in ihrer vollen Allgemeinheit. An ihre Stelle treten die erwähnten, im Grunde nur etwas aufpolierten Jahrhunderte alten Infinitesimalargumente.

In einem Nichtstandardmodell \mathcal{R}^* von $Th\mathcal{R}$ gibt es nicht nur unendlich große reelle Zahlen c (d.h. $r < c$ für alle $r \in \mathbb{R}$), sondern $\frac{1}{c}$ ist wegen $\frac{1}{r} < c \Leftrightarrow \frac{1}{c} < r$ kleiner als alle positiven reellen Zahlen r . Kurzum, $\frac{1}{c}$ ist eine *Infinitesimalzahl*. Ein etwas genaueres Hinschauen ergibt folgendes Bild: Jede reelle Zahl a sitzt in einem Nest von Nichtstandardzahlen $a^* \in \mathcal{R}^*$, die sich von a nur infinitesimal unterscheiden, d.h. $|a^* - a|$ ist eine Infinitesimalzahl. Auch solche Größen wie dx, dy dürfen ganz im Sinne ihres Erfinders Leibniz wieder als Infinitesimalzahlen betrachtet werden.

Aus der Existenz von Nichtstandardmodellen für $Th\mathcal{R}$ lässt sich schließen, dass das erwähnte und mit der Lückenlosigkeit von \mathbb{R} gleichwertige Stetigkeitsaxiom ähnlich wie IA nicht elementar formulierbar ist. Denn fügt man dieses den Axiomen für geordnete Körper hinzu, charakterisiert das entstehende Axiomensystem den Zahlenbereich \mathcal{R} bis auf Isomorphie eindeutig, siehe etwa [Ra3]. Die Ordnung eines Nichtstandardmodells \mathcal{R}^* von $Th\mathcal{R}$ besitzt folglich Lücken. Auch hier sind Lücken „von innen nicht erkennbar“. Denn jede nichtleere beschränkte parameterdefinierbare Teilmenge von \mathbb{R}^* besitzt ein Supremum in \mathbb{R}^* , weil in \mathcal{R} und damit auch in \mathcal{R}^* das folgende *Stetigkeitsschema* gilt, das die Existenz des Supremums für nichtleere beschränkte parameterdefinierbare Mengen sichert; hierbei durchläuft $\varphi = \varphi(x, \vec{y})$ alle Formeln der gemeinsamen Sprache von \mathcal{R} und \mathcal{R}^* und es sei $y, z \notin \text{frei } \varphi$:

$$\exists x \varphi \wedge \exists y \forall x (\varphi \rightarrow x \leq y) \rightarrow \exists y \forall x \forall z [(\varphi \rightarrow x \leq y) \wedge ((\varphi \rightarrow x \leq z) \rightarrow y \leq z)].$$

Analoge Bemerkungen gelten auch bezüglich der komplexen Zahlen. \mathcal{R}^* hat einen algebraisch abgeschlossenen Erweiterungskörper $\mathcal{R}^*[i]$, der den komplexen Zahlkörper notwendigerweise echt erweitert und in welchem bekannte Dinge wie etwa die Eulersche Formel $e^{ix} = \cos x + i \cdot \sin x$ weiterhin gelten.

Übungen

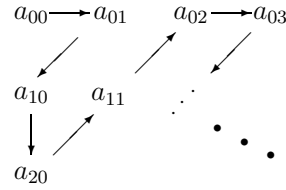
1. Man beweise $\forall x \, x \neq Sx$ und $\forall xy \, Sy + x = y + Sx$ in PA.
2. Man beweise in PA die Assoziativ- und Kommutativgesetze für $+$, \cdot , sowie das Distributivgesetz. Weitere Rechengesetze (auch \leq und $<$ betreffend) beweist man dann analog. Wichtig für Übung 3 ist z.B. $\vdash_{\text{PA}} x < Sy \leftrightarrow x \leq y$.
3. Man beweise (a) $\vdash_{\text{PA}} \forall x ((\forall y < x) \alpha \frac{y}{x} \rightarrow \alpha) \rightarrow \forall x \alpha$ (*Schema der $<$ -Induktion*), (b) $\vdash_{\text{PA}} \exists x \beta \rightarrow \exists x (\beta \wedge (\forall y < x) \neg \beta \frac{y}{x})$ (*Schema der Minimalzahl*), sowie auch (c) $\vdash_{\text{PA}} (\forall x < v) \exists y \gamma \rightarrow \exists z (\forall x < v) (\exists y < z) \gamma$ (*Schrankschema*).
Dabei seien α, β, γ beliebige Formeln aus \mathcal{L}_{ar} mit $y \notin \text{var } \{\alpha, \beta\}$ und $z \notin \text{var } \gamma$.

3.4 ZFC und die Paradoxie von Skolem

Bevor wir uns weiteren Folgerungen aus den Ergebnissen in 3.2 zuwenden, stellen wir einige Grundfakten über abzählbare Mengen zusammen, zu denen wir auch die endlichen Mengen rechnen. Eine Menge M heißt *abzählbar*, wenn $M = \emptyset$ oder wenn es eine surjektive Abbildung $f: \mathbb{N} \rightarrow M$ gibt, also $M = \{a_n \mid n \in \mathbb{N}\}$ mit $fn = a_n$, und sonst *überabzählbar*. Jede Teilmenge einer abzählbaren Menge ist wieder abzählbar. Mengen M, N heißen *gleichmächtig*, kurz $M \sim N$, wenn eine Bijektion von M auf N existiert. Ist $M \sim \mathbb{N}$, so heißt M *abzählbar unendlich*. Wie man leicht zeigt, kann eine abzählbare Menge nur abzählbar unendlich oder *endlich* sein, d.h. gleichmächtig zu $\{1, \dots, n\}$ für ein $n \in \mathbb{N}$.

Die bekannteste überabzählbare Menge ist \mathbb{R} ; sie ist gleichmächtig zu $\mathfrak{P}\mathbb{N}$ wie man unschwer beweist. Die Überabzählbarkeit von $\mathfrak{P}\mathbb{N}$ ist ein Spezialfall eines wichtigen Satzes von Cantor: *Die Potenzmenge $\mathfrak{P}M$ einer jeden Menge M hat eine größere Mächtigkeit als M* , d.h. keine Injektion von M nach $\mathfrak{P}M$ ist surjektiv.

Sind M, N abzählbar, so auch $M \cup N$ und $M \times N$, wie man leicht sieht. Auch ist eine abzählbare Vereinigung $U = \bigcup_{i \in \mathbb{N}} M_i$ abzählbarer Mengen M_i wieder abzählbar. Ein bekannter Beweis besteht darin, U als unendliche Matrix aufzuschreiben, mit der n -ten Zeile als Abzählung von $M_n = \{a_{nm} \mid m \in \mathbb{N}\}$. Dann zählt man mit dem in der Figur rechts angedeuteten Zick-Zack-Verfahren diese Matrix ab, beginnend mit a_{00} ⁴⁾. Für abzählbares M ist demnach insbesondere $\bigcup_{n \in \mathbb{N}} M^n$, die Menge aller endlichen Folgen von Elementen aus M , wieder abzählbar, weil jedes M^n abzählbar ist. Damit ist jede elementare Sprache abzählbarer Signatur selbst abzählbar, genauer, abzählbar unendlich.



Unter einer *abzählbaren Theorie* sei stets eine solche einer abzählbaren Sprache \mathcal{L} verstanden. Wir formulieren nun den aus vielen Gründen bedeutsamen

Satz 4.1 (von Löwenheim-Skolem). *Eine abzählbare konsistente Theorie T hat immer auch ein abzählbares Modell.*

Beweis. $T (\subseteq \mathcal{L})$ hat gemäß dem Beweis von Satz 2.6 ein Modell \mathcal{M} mit einem Träger A , bestehend aus den Äquivalenzklassen \bar{c} für $c \in C$ in der Menge aller Terme von $\mathcal{L}C$, wobei $C = \bigcup_{n \in \mathbb{N}} C_n$ eine Menge neuer Konstanten ist. Nach Konstruktion ist C_0 gleichmächtig mit $\text{Var} \times \mathcal{L}$ und damit abzählbar. Dasselbe gilt für jedes C_n , also auch für C . Die Abbildung $c \mapsto \bar{c}$ von C auf A ist trivialerweise surjektiv. Daher hat \mathcal{M} wie behauptet einen abzählbaren (eventuell endlichen) Träger. \square

⁴⁾ Hier wurde das Auswahlaxiom verwendet, weil für jedes M_i eine Abzählung ausgewählt wurde. Ohne Auswahlaxiom ist der Beweis nachweislich nicht ausführbar, siehe z.B. [Ba, Part B].

Dieser Satz wird in 5.1 noch einmal wesentlich verallgemeinert. Aber bereits in der obigen Formulierung hat er bemerkenswerte Konsequenzen. Danach gibt es z.B. auch abzählbare angeordnete Körper $\mathcal{R} = (\mathbb{R}, 0, 1, +, <, \cdot, \exp, \sin, \dots)$ als Nicht-standardmodelle von $Th\mathcal{R}$, in denen die üblichen Sätze über die elementaren reellen Funktionen gelten. Man muss also das Abzählbare nicht notwendig überschreiten, um anspruchsvolle Analysis betreiben zu können.

Besonders überraschend ist die nach Satz 4.1 gesicherte Existenz abzählbarer Modelle der formalisierten Mengenlehre – vorausgesetzt deren Axiome sind insgesamt konsistent, wovon für den weiteren Verlauf der Diskussion stets ausgegangen wird. Die schon in 2.2 mit \mathcal{L}_ϵ bezeichnete mengentheoretische Sprache ist nämlich eine der denkbar einfachsten und gewiss abzählbar. Sie enthält nebst $=$ nur das Symbol ϵ , das vom \in -Symbol der Metasprache klar zu unterscheiden ist.

Die Mengenlehre, obwohl sie als Basis für die gesamte derzeit existierende Mathematik angesehen werden kann, umfasst nur wenige Mengenbildungsprinzipien. Diese werden in Gestalt von Axiomen formuliert. Das wichtigste Axiomensystem dieser Art ist ZFC⁵⁾. Dieses geht davon aus, dass jedes Element einer Menge wieder eine Menge ist, so dass eine Unterscheidung zwischen Mengen und Mengenfamilien entfällt. ZFC redet also ausschließlich über Mengen, anders als z.B. das typentheoretische System von B. Russell, in welchem nebst Mengen auch *Urelemente* (Objekte, die Elemente von Mengen, selbst aber keine Mengen sind) betrachtet werden. Eine Mengenlehre ohne Urelemente reicht jedoch sowohl für die Grundlegung der Mathematik als auch für die meisten praktischen Zwecke vollkommen aus.

Um zu verdeutlichen, dass ZFC eine Theorie 1. Stufe ist, geben wir nachfolgend deren Axiome an. Jedes Axiom wird kurz erläutert. Die Variablen heißen jetzt *Mengenvariablen* und werden durch Kleinbuchstaben bezeichnet wie in anderen elementaren Sprachen auch. Wir benutzen die folgenden üblichen Abkürzungen in \mathcal{L}_ϵ :

$$x \subseteq y := \forall z(z \in x \rightarrow z \in y), \quad (\forall y \in x)\varphi := \forall y(y \in x \rightarrow \varphi), \quad (\exists y \in x)\varphi := \exists y(y \in x \wedge \varphi).$$

Die Axiome der Theorie ZFC sind im Einzelnen die folgenden:

$$\text{AE} : \forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y \quad (\text{Extensionalitätsaxiom}).$$

$$\text{AS} : \forall x \exists y \forall z(z \in y \leftrightarrow \varphi \wedge z \in x) \quad (\text{Aussonderungsschema}).$$

Hier durchläuft φ alle \mathcal{L}_ϵ -Formeln mit $y \notin \text{frei}\varphi$. Sei etwa $\varphi = \varphi(x, z, \vec{a})$. Dann ergeben AE und AS leicht $\forall x \exists! y \forall z(z \in y \leftrightarrow \varphi \wedge z \in x)$; denn wegen $y \notin \text{frei}\varphi$ ist aus $z \in y \leftrightarrow \varphi \wedge z \in x$ und $z \in y' \leftrightarrow \varphi \wedge z \in x$ mit AE offenbar $y = y'$ beweisbar. Daher ist

$$y = \{z \in x \mid \varphi\} \leftrightarrow \forall z(z \in y \leftrightarrow \varphi \wedge z \in x)$$

⁵⁾Nach E. Zermelo und A. Fraenkel; C steht für axiom of choice, Auswahlaxiom. Die bei Entfall dieses Axioms verbleibende Theorie wird auch mit ZF bezeichnet.

eine legitime Definition im Sinne von **2.6**. $\{z \in x \mid \varphi\}$ heißt ein *Mengenterm* und ist nur eine suggestive Schreibweise für die von den „Parametern“ \vec{a} abhängige, nach **AS** und **AE** eindeutig bestimmte Menge. Wir erweitern nun \mathcal{L}_\in um die Konstante \emptyset für die leere Menge durch $y = \emptyset \leftrightarrow \forall z z \notin y$. Da $\exists y \forall z (z \in y \leftrightarrow z \notin x \wedge z \in x)$ gemäß **AS** gilt und weil $z \in y \leftrightarrow z \notin x \wedge z \in x$ zu $z \notin y$ logisch äquivalent ist, folgt erst einmal $\exists y \forall z z \notin y$. Nun impliziert $\forall z z \notin y \wedge \forall z z \notin y'$ nach **AE** aber $y = y'$, was $\exists! y \forall z z \notin y$ und damit die Legitimität dieser Definition zeigt. Das nächste Axiom ist

$$\text{AU} : \quad \forall x \exists y \forall z (z \in y \leftrightarrow (\exists u \in x) z \in u) \quad (\text{Vereinigungsaxiom}).$$

Wieder kann hier $\exists y$ wegen **AE** durch $\exists! y$ ersetzt werden, um damit nach **2.6** eine durch $x \mapsto \bigcup x$ bezeichnete Operation⁶⁾ zu definieren. Gleichwertig mit **AU** ist auch $\exists y \forall z ((\exists u \in x) z \in u \rightarrow z \in y)$, weil $\bigcup x$ aus einem solchen y ausgesondert werden kann. Analog ließe sich auch das folgende Axiom abschwächen.

$$\text{AP} : \quad \forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x) \quad (\text{Potenzmengenaxiom}).$$

$\mathfrak{P}x$ bezeichne das nach **AP** und **AE** durch x eindeutig bestimmte y , die Potenzmenge von x . Für $\mathfrak{P}\emptyset, \mathfrak{P}\mathfrak{P}\emptyset, \dots$ schreibt man auch $\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots$. Man beweist nämlich leicht $\forall x (x \in \mathfrak{P}\emptyset \leftrightarrow x = \emptyset)$, $\forall x (x \in \mathfrak{P}\mathfrak{P}\emptyset \leftrightarrow x = \emptyset \vee x = \{\emptyset\})$ usw. Das nächste Axiom fügte Fraenkel den übrigen Zermeloschen Axiomen hinzu.

$$\text{AR} : \quad \forall x \exists! y \varphi \rightarrow \forall u \exists v \forall y (y \in v \leftrightarrow (\exists x \in u) \varphi) \quad (\text{Ersetzungsschema}).$$

Dabei ist $\varphi = \varphi(x, y, \vec{a})$ und $u, v \notin \text{frei } \varphi$. Ist hier $\forall x \exists! y \varphi$ beweisbar, so darf nach **2.6** eine Operation $x \mapsto Fx$ eingeführt werden, die noch von den eventuell vorhandenen „Parametern“ a_1, \dots, a_n abhängt, $F = F_{\vec{a}}$. Nach **AR** ist das Bild einer Menge u unter F wieder eine Menge v , die oft mit $\{Fx \mid x \in u\}$ bezeichnet wird. Ein instruktives Beispiel, für das $\forall x \exists! y \varphi$ sicher beweisbar ist, liefert die Formel

$$\varphi(x, y, a, b) := x = \emptyset \wedge y = a \vee x \neq \emptyset \wedge y = b.$$

Für die durch φ definierte Operation $F = F_{a,b}$ ist offenbar $F\emptyset = a$ und $Fx = b$ für $x \neq \emptyset$. Demnach enthält das Bild von $u = \mathfrak{P}\mathfrak{P}\emptyset = \{\emptyset, \{\emptyset\}\}$ unter dem Operator $F_{a,b}$ genau die beiden Elemente a, b . Wir erklären daher $\{a, b\} := \{F_{a,b}(x) \mid x \in \{\emptyset, \{\emptyset\}\}\}$ und nennen diese die *Paarmenge* aus a, b . Man erklärt sodann $a \cup b := \bigcup \{a, b\}$ (während $a \cap b := \{z \in a \mid z \in b\}$ bereits nach **AS** existiert). Ferner sei $\{a\} := \{a, a\}$ und $\{a_1, \dots, a_{n+1}\} = \{a_1, \dots, a_n\} \cup \{a_{n+1}\}$ für $n \geq 2$. Damit werden die Formeln $\mathfrak{P}\emptyset = \{\emptyset\}, \mathfrak{P}\mathfrak{P}\emptyset = \{\emptyset, \{\emptyset\}\}, \dots$ nunmehr beweisbar. Das *geordnete Paar* aus a, b wird nach Kuratowski definiert als $(a, b) := \{\{a\}, \{a, b\}\}$.

Bereits jetzt verfügt man über das nötige Rüstzeug zur Entwicklung der Theorie. Ausgehend von Mengen geordneter Paare lassen sich nunmehr der Relations- und Funktionsbegriff und alle darauf aufbauenden Begriffe vollkommen befriedigend

⁶⁾ Der Name Funktion wird hier vermieden, weil Funktionen spezielle Objekte eines Universums (= Träger eines ZFC-Modells) sind, nämlich Mengen geordneter Paare.

modellieren, obwohl über die Existenz unendlicher Mengen noch gar nichts gesagt wurde. Diese zu fordern diktieren uns mathematische Bedürfnisse, aber wir überschreiten damit auch die Grenzen gesicherter Erfahrungen mit endlichen Mengen.

AI : $\exists u(\emptyset \in u \wedge (\forall x \in u) Sx \in u)$, mit $Sx := x \cup \{x\}$ (Unendlichkeitsaxiom).

u enthält \emptyset , sowie $S\emptyset = \emptyset \cup \{\emptyset\} = \{\emptyset\}$, $SS\emptyset = \{\emptyset, \{\emptyset\}\}$, ... und ist daher im naiven Sinne unendlich. Das gilt speziell für die kleinste Menge u dieser Art, die man mit ω bezeichnet. ω vertritt in der formalisierten Mengenlehre die Menge der natürlichen Zahlen. ω enthält $0 := \emptyset$, $1 := \{\emptyset\} = \{0\}$, $2 := \{\emptyset, \{\emptyset\}\} = \{0, 1\}$ und man beweist induktiv leicht $n + 1 := Sn = \{0, \dots, n\}$. Die metatheoretischen natürlichen Zahlen werden so in ω durch Grundterme repräsentiert, die auch ω -Terme heißen.

Das folgende Axiom ist in der Alltagsmathematik im Grunde entbehrlich:

AF : $(\forall x \neq \emptyset)(\exists y \in x)(\forall z \in x) z \notin y$ (Fundierungsaxiom).

Anschaulich gesprochen: Jedes $x \neq \emptyset$ enthält ein \in -minimales Element y . Durch AF werden u.a. „ \in -Kreise“ $x_0 \in \dots \in x_n \in x_0$ ausgeschlossen. Die wichtigste Folgerung ist die von Neumannsche Hierarchie, was hier nur erwähnt sei.

Aus der mit ZF bezeichneten Theorie mit den bisherigen Axiomen entsteht ZFC durch Hinzufügen des *Auswahlaxioms*, das viele äquivalente Formulierungen hat. Es besagt, dass zu jeder Mengenfamilie u aus disjunkten nichtleeren Mengen eine Menge z existiert, eine „Auswahlmenge“, welche mit jedem $x \in u$ genau ein Element gemeinsam hat. Formal notiert

AC : $\emptyset \notin u \wedge (\forall x \in u)(\forall y \in u)(x \neq y \rightarrow x \cap y = \emptyset) \rightarrow \exists z(\forall x \in u)\exists! y(y \in x \wedge y \in z)$.

Die Ausführungen zeigen klar, dass ZFC als Theorie 1. Stufe verstanden werden kann. In gewissem Sinne ist ZFC sogar die reinste Theorie 1. Stufe. Denn alle in der Mathematik vorkommenden höheren Beweismethoden, wie z.B. die transfinite Induktion und Rekursion (siehe z.B. [De1]) und jede andere Art von Induktion und Rekursion sind ohne große Mühe in ZFC rein prädikatenlogisch beweisbar. Während der Mathematiker den Rahmen einer Theorie, selbst wenn sie eindeutig durch Axiome der 1. Stufe definiert ist, regelmäßig überschreitet und zur Entwicklung der Theorie kombinatorische, zahlentheoretische oder mengentheoretische Hilfsmittel heranzieht wann immer dies nützlich erscheint, setzt die Mengenlehre hier nach dem Stand der Dinge eine Obergrenze. Im Rahmen von ZFC erhalten alle höheren Beweis- und Definitionsmittel sozusagen elementaren Charakter.

Es gibt jedenfalls keine sachlichen Argumente gegen die Behauptung, dass die gesamte Mathematik mit all ihren Teilgebieten als eine einzige Theorie 1. Stufe verstanden werden kann, nämlich die Theorie ZFC. Diese Einsicht basiert auf Erfahrung. Allerdings sollte daraus keine Religion gemacht werden, denn für die mathematische Praxis hat diese Einsicht wiederum nur eingeschränkte Bedeutung.

Wenn nun ZFC konsistent ist – und daran wird nicht ernsthaft gezweifelt – so hat diese Theorie nach Satz 4.1 auch ein abzählbares Modell. Die Existenz eines derartigen ZFC-Modells $\mathcal{V} = (V, \in^{\mathcal{V}})$ erscheint auf den ersten Blick deswegen paradox, weil *im Rahmen von ZFC* die Existenz überabzählbarer Mengen leicht beweisbar ist. Ein Beispiel ist $\mathfrak{P}\omega$. Andererseits enthält $(\mathfrak{P}\omega)^{\mathcal{V}}$ wegen $(\mathfrak{P}\omega)^{\mathcal{V}} \subseteq V$ sicher nur wieder abzählbar viele Elemente. Der Begriff ‘abzählbar’ hat also „innerhalb und außerhalb der Welt \mathcal{V} “ einen unterschiedlichen Sinn, was gar nicht beabsichtigt war.

Die Erklärung dieser sogenannten Paradoxie von Skolem ist, dass das abzählbare Modell \mathcal{V} , bildlich gesprochen, ziemlich „ausgedünnt“ ist und weniger Mengen und Funktionen enthält als man erwartet – grob gesprochen gerade so viele, um die Axiome zu erfüllen. \mathcal{V} enthält deshalb z.B. keine – von außen gesehen durchaus existierende – Bijektion von $\omega^{\mathcal{V}}$ auf $(\mathfrak{P}\omega)^{\mathcal{V}}$. Daher ist die abzählbare Menge $(\mathfrak{P}\omega)^{\mathcal{V}}$ aus der Perspektive der Welt \mathcal{V} tatsächlich überabzählbar.

Auch ist das Universum V eines ZFC-Modells jedenfalls eine Menge, während leicht $(*) \vdash_{\text{ZFC}} \neg \exists v \forall z z \in v$ beweisbar ist, d.h. es gibt keine „Allmenge“. Von innen gesehen ist V zu groß, um eine Menge zu sein. $(*)$ ergibt sich wie folgt: $\exists v \forall z z \in v$ liefert mit AE und AS leicht die Existenz der „Russellschen Menge“ $u = \{x \in v \mid x \notin x\}$. Kurzum, $\exists v \forall z z \in v \vdash_{\text{ZFC}} \exists u \forall x (x \in u \leftrightarrow x \notin x)$. Nun ist nach dem Beispiel auf Seite 58 aber $\vdash_{\text{ZFC}} \neg \exists u \forall x (x \in u \leftrightarrow x \notin x)$ und aus logischen Gründen daher $\vdash_{\text{ZFC}} \neg \exists v \forall z z \in v$. Demnach hat der Mengenbegriff an sich keinen vom Modell unabhängigen Sinn.

Dies alles hat damit nichts zu tun, dass ZFC unvollständig ist⁷⁾. Die Mathematik kann ganz gut damit leben, dass ihre Basistheorie nicht nur unvollständig ist, sondern auch prinzipiell nicht übersehbar vervollständigt werden kann. Problematischer ist eher das Fehlen unumstrittener Kriterien zur Erweiterung von ZFC überhaupt.

Übungen

1. Sei T eine elementare Theorie mit beliebig großen endlichen Modellen. Man beweise mit dem Kompaktheitssatz, T besitzt auch ein unendliches Modell.
2. Sei $\mathcal{A} = (A, <)$ eine unendliche wohlgeordnete Menge (siehe 2.1). Man zeige, es gibt eine zu \mathcal{A} elementar-äquivalente, nicht wohlgeordnete Menge.
3. Man bestätige mit den angegebenen ZFC-Axiomen die Wohldefiniertheit von ω im Text. Dazu genügt zu beweisen $\vdash_{\text{ZFC}} \exists u [\emptyset \in u \wedge \forall x (x \in u \rightarrow x \cup \{x\} \in u)]$.
4. Sei $\mathcal{V} \models \text{ZFC}$. Man zeige, es gibt ein $\mathcal{V}' \models \text{ZFC}$ mit $\mathcal{V}' \supseteq \mathcal{V}$ und ein $U \in V'$ mit $a \in {}^{\mathcal{V}'}U$ für alle $a \in V$. Es ist dann notwendig $V' \supset V$.

⁷⁾In 6.5 wird die Unvollständigkeit von ZFC und aller ihrer axiomatischen Erweiterungen nachgewiesen. Beispiel einer von ZFC unabhängigen Aussage ist die Kontinuumshypothese (Seite 135).

3.5 Aufzählbarkeit und Entscheidbarkeit

Von den weitreichenden Konsequenzen des Vollständigkeitssatzes ist vielleicht die effektive Aufzählbarkeit aller Tautologien einer abzählbaren elementaren Sprache die wesentlichste. Nachdem Gödel dies bewiesen hatte, wuchs die Hoffnung, nun auch das Tautologie-Entscheidungsproblem lösen zu können, die aber nur kurze Zeit währte; denn wenige Jahre nach Gödels Ergebnis bewies Church die Unlösbarkeit dieses Problems für hinreichend ausdrucksfähige Sprachen. Dieser Abschnitt vermittelt nur einen ersten Eindruck von Aufzählungs- und Entscheidungsproblemen, die in der Logik auftreten. Mehr wird in den Kapiteln 5 und 6 darüber gesagt.

Die Redeweise *effektiv aufzählbar* wird in 6.1 durch den Begriff *rekursiv aufzählbar* präzisiert. An dieser Stelle müssen wir hinsichtlich der Erläuterung dieses Begriffs etwas oberflächlich bleiben, aber er ist ebenso wie der Begriff der entscheidbaren Menge recht einfach zu veranschaulichen. Grob gesagt heißt eine Menge M , etwa von natürlichen Zahlen, von syntaktischen Objekten, von endlichen Strukturen oder von noch ganz anderen Objekten, *rekursiv* (oder *effektiv*) *aufzählbar*, wenn es einen Algorithmus gibt, der uns die Elemente von M schrittweise ausgibt, der also bei unendlichem M den Ausgabeprozess nicht von selbst unterbricht.

Der Kalkül des natürlichen Schließens ermöglicht zunächst einmal eine effektive Aufzählung aller beweisbaren endlichen Sequenzen einer Sprache der 1. Stufe mit höchstens abzählbar vielen logischen Symbolen, d.h. aller Paare (X, α) mit $X \vdash \alpha$ und endlichem X , jedenfalls im Prinzip. Dazu denke man sich zuerst alle Anfangssequenzen in einer fortlaufenden, explizit herstellbaren Folge S_0, S_1, \dots aufgezählt. Dann wird systematisch geprüft, ob eine der Sequenzenregeln anwendbar ist, die Ergebnissequenzen werden in einer zweiten Folge aufgezählt usw. Es ist nur eine Frage der Organisation, ein Programm zu erstellen, das alle beweisbaren endlichen Sequenzen aufzählt, wenn man einmal absieht von den Problemen des Speicherbedarfs einer entsprechenden „Deduktionsmaschine“ und den Schwierigkeiten der Auswertung der Informationsflut, die einer solchen Deduktionsmaschine entspränge.

Ferner lässt sich unschwer einsehen, dass die Tautologien einer abzählbaren Sprache \mathcal{L} effektiv aufzählbar sind. Man braucht ja in einem Aufzählungsverfahren der beweisbaren Sequenzen (X, α) nur diejenigen mit $X = \emptyset$ auszusondern. Kurz, die oben erwähnte Deduktionsmaschine produziert sukzessive eine Folge $\alpha_0, \alpha_1, \dots$, sogar ohne Wiederholungen, die genau aus den Tautologien von \mathcal{L} besteht (mit dem Kalkül in 3.6 ginge dies etwas bequemer). Allerdings erhalten wir so kein Entscheidungsverfahren darüber, ob eine beliebig vorgegebene Formel $\alpha \in \mathcal{L}$ eine Tautologie ist oder nicht; denn man weiß nicht, ob α in der produzierten Folge jemals erscheint. In 6.5 werden wir rigoros beweisen, dass es einen derartigen Algorithmus nicht gibt,

falls \mathcal{L} ein mindestens 2-stelliges Prädikaten- oder Operationssymbol enthält. Entscheidungsalgorithmen gibt es nur für $\mathcal{L}_=$ (siehe 5.2) oder wenn die Signatur außer Individuenkonstanten nur einstellige Prädikatensymbole enthält, sowie höchstens noch ein einstelliges Operationssymbol, siehe hierzu auch [BGG].

Die Deduktionsmaschine kann auch benutzt werden, um die Sätze einer rekursiv axiomatisierten Theorie T aufzuzählen. Es muss nur parallel zum Aufzählungsprozess aller beweisbaren Sequenzen der Sprache ein Aufzählungsprozess aller Axiome von T in Gang gesetzt werden. Sodann müssen die aufgezählten Sequenzen laufend daraufhin geprüft werden, ob alle ihre Prämissen unter den bereits aufgezählten Axiomen vorkommen; wenn ja, ist die Konklusion der betreffenden Sequenz in T beweisbar. Wir haben damit den folgenden Satz informell bewiesen; einen rigorosen, von anschaulichen Argumenten unabhängigen Beweis gibt Satz 6.2.4.

Satz 5.1. *Die Sätze einer axiomatisierbaren Theorie sind effektiv aufzählbar.*

Fast alle in der Mathematik betrachteten Theorien sind axiomatisierbar, darunter die formalisierte Mengenlehre ZFC und die Peano-Arithmetik PA. Die Axiomensysteme dieser beiden Theorien sind zwar unendlich und auch durch endliche nicht ersetzbar, aber diese Formelmengen sind offensichtlich entscheidbar. Weil nach bisheriger Erfahrung alle in der Mathematik als bewiesen geltenden Sätze auch in ZFC beweisbar sind, lassen sich nach Satz 5.1 alle mathematischen Sätze im Prinzip schrittweise durch Computer erzeugen. Diese Tatsache ist prinzipiell bedeutsam, auch wenn sie noch keine weitreichende praktische Bedeutung erlangt hat.

Wir erinnern an den Begriff einer vollständigen Theorie. Zu den wichtigsten Beispielen gehört die Theorie der reell abgeschlossenen Körper (Satz 5.5.5), die damit identisch ist mit $Th \mathcal{R}$ für $\mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot, <)$, der Vorbildstruktur solcher Körper. Eine bemerkenswerte Eigenschaft vollständiger und axiomatisierbarer Theorien ist ihre *Entscheidbarkeit*. Dabei heißt eine Theorie *entscheidbar*, wenn die Menge ihrer Sätze eine entscheidbare Formelmenge ist, und sonst *unentscheidbar*. Wir beweisen den folgenden Satz, von dem Übung 3 eine Verallgemeinerung formuliert, zunächst anschaulich. Einen strengen, auf der Präzisierung des Begriffs entscheidbar in 6.1 beruhenden Beweis erbringen wir mit Satz 6.4.4 auf Seite 191.

Satz 5.2. *Eine vollständige axiomatisierbare Theorie T ist entscheidbar.*

Beweis. Sei $\alpha_0, \alpha_1, \dots$ eine nach Satz 5.1 existierende effektive Aufzählung aller in T beweisbaren Aussagen. Ein Entscheidungsverfahren besteht einfach darin, für vorgegebenes $\alpha \in \mathcal{L}^0$ die Aussagen α und $\neg\alpha$ im n -ten Konstruktionsschritt von $\alpha_0, \alpha_1, \dots$ mit α_n zu vergleichen. Ist $\alpha = \alpha_n$, so ist $\vdash_T \alpha$; ist $\alpha = \neg\alpha_n$, so ist $\not\vdash_T \alpha$. Dieses Verfahren terminiert, weil wegen der Vollständigkeit von T entweder α oder $\neg\alpha$ in der Aufzählungsfolge $\alpha_0, \alpha_1, \dots$ irgendwann erscheint. \square

Weil eine vollständige entscheidbare Theorie T umgekehrt trivial axiomatisierbar ist (durch T selbst), sind für vollständige Theorien ‘entscheidbar’ und ‘axiomatisierbar’ vollkommen gleichwertige Eigenschaften. Jede konsistente Theorie hat, weil sie ein Modell hat, mindestens eine *Vervollständigung*, d.h. eine vollständige Erweiterungstheorie in derselben Sprache. Eine entscheidbare Theorie hat darüber hinaus immer auch eine axiomatisierbare und damit entscheidbare Vervollständigung, Übung 4

In der Anfangsphase der Entwicklung schneller elektronischer Rechner war man sehr optimistisch, was die praktische Ausführung maschineller Entscheidungsverfahren betrifft. Dieser Optimismus hat sich aus unterschiedlichen Gründen gedämpft. Mit Bedacht eingesetzt, können Computer aber nicht nur bei der Beweisverifikation, sondern auch bei der Beweisfindung nützlich sein. Dafür gibt es überzeugende Beispiele, darunter der computergestützte Beweis der Vierfarbenvermutung. Nähere Informationen über dieses Gebiet, das sich ATP (= Automated Theorem Proving) nennt, findet man im Internet.

Allerdings hat auch ein hochentwickeltes System künstlicher Intelligenz vorläufig keine Chance, die heuristische Vorgehensweise des Mathematikers zu simulieren, bei welcher ein präziser Beweis aus gewissen Annahmen oft erst der Schlussstein einer Serie von Überlegungen ist, die aus gedanklichen Vorstellungen fließen. Aber ein derartiges System könnte auf neuartige Weise kreativ sein. Denn es ist nicht gesagt, dass unsere von gedanklichen Bildern aller Art geprägte Verfahrensweise die einzige ist, die Erkenntnisgewinn in der Mathematik zu erbringen vermag.

Übungen

1. Sei $T' = T + \alpha$ ($\alpha \in \mathcal{L}^0$) eine endliche Erweiterung von T . Man zeige: Ist T entscheidbar, so auch T' (vgl. Lemma 6.5.3).
2. Man zeige, für eine konsistente Theorie T sind gleichwertig
 - (i) T hat endlich viele Erweiterungen,
 - (ii) T hat endlich viele Vervollständigungen⁸⁾,
 - (iii) jede Erweiterung $T' \supseteq T$ ist eine endliche.
3. Sei T eine axiomatisierbare Theorie mit nur endlich vielen Vervollständigungen. Man beweise, T ist entscheidbar. Für Anwendungsbeispiele siehe 5.2.
4. Man zeige mit der Lindenbaumschen Konstruktion aus 1.4: eine entscheidbare (abzählbare) Theorie hat immer auch eine entscheidbare Vervollständigung.

⁸⁾Das betrifft z.B. die elementare absolute Geometrie T mit genau zwei Vervollständigungen, die euklidische und die hyperbolische Geometrie. Den einfachen Zusammenhang zwischen der Anzahl der Vervollständigungen und der Erweiterungen einer Theorie formuliert Übung 4 in 5.2.

3.6 Vollständige Hilbert-Kalküle

Der Regelkalkül aus 3.1 modelliert zwar das natürliche Schließen recht gut, aber für manche Zwecke, z.B. die Gödelisierung des Beweisens, ist es vorteilhafter, einen Hilbert-Kalkül zu benutzen. Solche Kalküle beruhen auf logischen Axiomen und Schlussregeln wie z.B. dem Modus Ponens MP: $\alpha, \alpha \rightarrow \beta / \beta$, die auch *Regeln vom Hilbert-Typ* genannt werden und sich als Sequenzenregeln ohne Prämissen verstehen lassen. In einem Hilbert-Kalkül wird aus einer fest vorgegebenen Formelmengemenge X , z.B. dem Axiomensystem einer Theorie, unter Einbeziehung der logischen Axiome deduziert, ähnlich wie in 1.6. Im Falle $X = \emptyset$ wird aus den logischen Axiomen allein abgeleitet und man gewinnt lediglich Tautologien.

Im folgenden beweisen wir die Vollständigkeit eines derartigen, hier mit \vdash bezeichneten Kalküls in $\neg, \wedge, \vee, \equiv$ mit der einzigen Schlussregel MP. Der Kalkül bezieht sich auf eine beliebig vorgegebene elementare Sprache \mathcal{L} und ist eine Erweiterung des entsprechenden, in 1.6 behandelten aussagenlogischen Hilbert-Kalküls. Wieder spielt die Implikation, definiert durch $\alpha \rightarrow \beta := \neg(\alpha \wedge \neg\beta)$, eine nützliche Rolle.

Das *logische Axiomensystem* Λ unseres Kalküls bestehe aus der Menge aller Formeln $\forall x_1 \cdots \forall x_n \varphi$ für $n \geq 0$, wobei φ eine Formel der Gestalt $\Lambda 1$ – $\Lambda 10$ ist und x_1, \dots, x_n beliebig sind. So sind wegen $\Lambda 9$ z.B. auch $\forall x x \equiv x$ und $\forall y \forall x x \equiv x$ Axiome, auch wenn das Präfix $\forall y$ hier bedeutungslos ist. Man kann auch sagen, Λ ist die Menge aller Formeln, die sich aus $\Lambda 1$ – $\Lambda 10$ mittels der *Generalisierungsregel* MQ: $\alpha / \forall x \alpha$ ableiten lassen. MQ ist aber keine Schlussregel des Kalküls und auch nicht beweisbar.

- | | |
|--|---|
| $\Lambda 1: (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma),$ | $\Lambda 2: \alpha \rightarrow \beta \rightarrow \alpha \wedge \beta,$ |
| $\Lambda 3: \alpha \wedge \beta \rightarrow \alpha, \quad \alpha \wedge \beta \rightarrow \beta,$ | $\Lambda 4: (\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \neg\alpha),$ |
| $\Lambda 5: \forall x \alpha \rightarrow \alpha \frac{t}{x} \quad (\alpha, \frac{t}{x} \text{ kollisionsfrei}),$ | $\Lambda 6: \alpha \rightarrow \forall x \alpha \quad (x \notin \text{frei } \alpha)$ |
| $\Lambda 7: \forall x (\alpha \rightarrow \beta) \rightarrow \forall x \alpha \rightarrow \forall x \beta,$ | $\Lambda 8: \forall y \alpha \frac{y}{x} \rightarrow \forall x \alpha \quad (y \notin \text{var } \alpha),$ |
| $\Lambda 9: t = t,$ | $\Lambda 10: x = y \rightarrow \alpha \rightarrow \alpha \frac{y}{x} \quad (\alpha \text{ Primformel}).$ |

Es ist leicht einzusehen, dass $\Lambda 1$ – $\Lambda 10$ Tautologien sind. Für $\Lambda 1$ – $\Lambda 4$ ist dies klar nach 1.6. Für $\Lambda 5$ – $\Lambda 10$ ist dies unter Beachtung von Korollar 2.3.6 und der Äquivalenzen in 2.3 leicht nachzurechnen.

Axiom $\Lambda 5$ entspricht der Regel ($\forall 1$) des Kalküls aus 3.1, während $\Lambda 6$ der formalen Behandlung überflüssiger Präfixe dient. Die Rolle von $\Lambda 7$ wird im Vollständigkeitsbeweis klar, und $\Lambda 8$ ist Teil der gebundenen Umbenennung. $\Lambda 9$ und $\Lambda 10$ regeln den Umgang mit der Identität. Weil mit φ für einen beliebigen Präfixblock $\forall \vec{x}$ auch $\forall \vec{x} \varphi$ eine Tautologie ist, besteht auch Λ nur aus Tautologien. Dasselbe gilt für alle aus Λ mit MP herleitbaren Formeln. Denn $\models \alpha, \alpha \rightarrow \beta$ impliziert bekanntlich $\models \beta$.

Sei $X \vdash \alpha$, falls es einen *Beweis* $\Phi = (\varphi_0, \dots, \varphi_n)$ für α aus X gibt, d.h. $\alpha = \varphi_n$, und für alle $k \leq n$ ist $\varphi_k \in X \cup \Lambda$ oder es gibt ein φ , so dass φ und $\varphi \rightarrow \varphi_k$ als Glieder in Φ vor φ_k auftreten. Diese Definition und ihre Folgerungen sind genau dieselben wie in 1.6. Daher gilt wie dort $X \vdash \alpha, \alpha \rightarrow \beta \Rightarrow X \vdash \beta$. Ferner überträgt sich auch der Induktionssatz 1.6.1 unverändert. Seine Anwendung wird meistens schlagwortartig als „Beweis durch Induktion über $X \vdash \alpha$ “ angekündigt, z.B. beweist man leicht die Korrektheit von \vdash durch Induktion über $X \vdash \alpha$, d.h. für alle X und α gilt $X \vdash \alpha \Rightarrow X \models \alpha$.

Die Vollständigkeit von \vdash lässt sich nun ziemlich einfach auf die Vollständigkeit des Regelkalküls \vdash aus 3.1 zurückführen. Die erforderliche Arbeit hierfür wurde in 1.6 im Wesentlichen schon geleistet. Daher formulieren wir sogleich den

Satz 6.1 (Vollständigkeitssatz). $\vdash = \models$.

Beweis. $\vdash \subseteq \models$ wurde bereits gezeigt. $\models \subseteq \vdash$ folgt aus der Behauptung, dass \vdash alle Basisregeln von \models erfüllt. Denn dann ist $\vdash \subseteq \models$ und wegen $\vdash = \models$ gilt damit $\models \subseteq \vdash$. Für die aussagenlogischen Regeln $(\wedge 1)$ – $(\neg 2)$ ist die Behauptung klar nach dem entsprechenden Beweis für den Hilbert-Kalkül in 1.6. Denn die dort bewiesenen Lemmata 1.6.2 – 1.6.5 übertragen sich wörtlich, weil ja die vier Axiome, auf denen die Beweise beruhen, beibehalten wurden und keine neue Regel hinzugekommen ist. $(\forall 1)$ folgt mit MP unmittelbar aus $\Lambda 5$, und was (AR) betrifft, ist alles klar nach $\Lambda 9$. Lediglich $(\forall 2)$ und $(=)$ machen etwas Arbeit.

$(\forall 2)$: Wir beweisen zuerst $X \vdash \alpha \Rightarrow X \vdash \forall x \alpha$ für $x \notin \text{frei } X$ durch Induktion über $X \vdash \alpha$. *Anfangsschritt*: Im Falle $\alpha \in X$ ist x auch nicht frei in α . Also $X \vdash \alpha \rightarrow \forall x \alpha$ gemäß $\Lambda 6$, und MP ergibt $X \vdash \forall x \alpha$. Falls $\alpha \in \Lambda$, ist auch $\forall x \alpha \in \Lambda$, und damit ebenfalls $X \vdash \forall x \alpha$. *Induktionsschritt*: Sei $X \vdash \alpha, \alpha \rightarrow \beta$ und $X \vdash \forall x \alpha, \forall x(\alpha \rightarrow \beta)$ nach Induktionsannahme. Das ergibt $X \vdash \forall x \alpha, \forall x \alpha \rightarrow \forall x \beta$ nach Axiom $\Lambda 7$, also liefert MP die Induktionsbehauptung $X \vdash \forall x \beta$. Zum Nachweis von $(\forall 2)$ sei nun $X \vdash \alpha \frac{y}{x}$, mit $y \notin \text{frei } X \cup \text{var } \alpha$. Nach dem soeben Bewiesenen ist $X \vdash \forall y \alpha \frac{y}{x}$, und MP ergibt wegen $X \vdash \forall y \alpha \frac{y}{x} \rightarrow \forall x \alpha$ (Axiom $\Lambda 8$) die Konklusion $X \vdash \forall x \alpha$ von $(\forall 2)$.

$(=)$: Sei α Primformel und $X \vdash s = t, \alpha \frac{s}{x}$. Ferner sei y eine in s und α nicht vorkommende Variable $\neq x$. Gewiss ist $X \vdash \forall x \forall y (x = y \rightarrow \alpha \rightarrow \alpha \frac{y}{x})$, weil letztere Formel wegen $\Lambda 10$ zu Λ gehört. Regel $(\forall 1)$ ergibt aufgrund der Wahl von y

$$X \vdash [\forall y (x = y \rightarrow \alpha \rightarrow \alpha \frac{y}{x})] \frac{s}{x} = \forall y (s = y \rightarrow \alpha \frac{s}{x} \rightarrow \alpha \frac{y}{x}).$$

Nochmalige Anwendung von $(\forall 1)$ liefert wegen $y \notin \text{var } \alpha, s$ und wegen $\alpha \frac{y}{x} \frac{t}{y} = \alpha \frac{t}{x}$

$$X \vdash [s = y \rightarrow \alpha \frac{s}{x} \rightarrow \alpha \frac{y}{x}] \frac{t}{y} = s = t \rightarrow \alpha \frac{s}{x} \rightarrow \alpha \frac{y}{x} \frac{t}{y} = s = t \rightarrow \alpha \frac{s}{x} \rightarrow \alpha \frac{t}{x}.$$

2-malige Anwendung von MP ergibt dann die gewünschte Konklusion $X \vdash \alpha \frac{t}{x}$. \square

Korollar 6.2. *Für beliebiges $\alpha \in \mathcal{L}$ sind folgende Eigenschaften äquivalent:*

- (i) $\vdash \alpha$, d.h. α ist mittels MP ableitbar aus Λ ,
- (ii) α ist mittels MP und MQ ableitbar aus $\Lambda 1$ – $\Lambda 10$,
- (iii) $\models \alpha$, d.h. α ist eine Tautologie.

Die Äquivalenz von (i) und (iii) macht die prinzipielle Möglichkeit der Konstruktion einer „Deduktionsmaschine“ besonders anschaulich, die **Taut**, die Menge aller Tautologien einer gegebenen Sprache der 1. Stufe, effektiv aufzählt. Man hat hier ja nur mit einer einzigen Regel, dem Modus Ponens, zu tun. Man braucht also nur eine Hilfsmaschine für die schrittweise Auflistung der logischen Axiome, sodann einen „Deduzierer“, der nur prüft, ob MP anwendbar ist und gegebenenfalls anwendet, und eine Organisationseinheit, die die Ergebnisse ausgibt und dem Deduzierer zur weiteren Verarbeitung zurückliefert. Ähnlich wie im Falle eines Sequenzenkalküls ist ein solches Verfahren jedoch nicht praktikabel. Denn die Unterscheidung von Wesentlichem und Unwesentlichem bleibt hierbei unberücksichtigt.

Wir zeigen gleich noch, dass auch die in 2.5 definierte globale Folgerungsrelation \Vdash durch einen Hilbertkalkül vollständig charakterisiert werden kann. Man muss zum Kalkül \vdash nur die Generalisierungsregel MQ hinzufügen. Der so entstehende und mit \Vdash bezeichnete Hilbert-Kalkül hat dann zwei Basisregeln, MP und MQ. Wie jeder Hilbert-Kalkül ist \Vdash transitiv, also $X \Vdash Y$ & $Y \Vdash \alpha \Rightarrow X \Vdash \alpha$. Denn sei $X \Vdash Y$, $Y \Vdash \alpha$ und Φ ein Beweis von α aus Y . Ersetzt man jede in Φ vorkommende Formel $\varphi \in Y$ durch einen Beweis von φ aus X , so ist die resultierende Folge offenbar ein Beweis für α aus X . Diese Einsicht erleichtert den Beweis von

Satz 6.3 (Vollständigkeitssatz für \Vdash). *Es ist $\vdash = \Vdash$.*

Beweis. Gewiss ist $\vdash \subseteq \Vdash$, denn MP und MQ sind korrekt für \Vdash . Sei nun $X \Vdash \alpha$, so dass $X^\vee \models \alpha$ nach (1) aus 2.5. Das ergibt $X^\vee \vdash \alpha$ nach Satz 6.1, und somit erst recht $X^\vee \Vdash \alpha$. Weil nun aber $X \Vdash X^\vee$, liefert die Transitivität $X \Vdash \alpha$. \square

Wir diskutieren nun einen für Logik und Informatik gleichermaßen interessanten Begriff. $\alpha \in \mathcal{L}^0$ heißt *allgemeingültig im Endlichen*, wenn $\mathcal{A} \models \alpha$ für alle endlichen Strukturen \mathcal{A} . Beispiele solcher Aussagen α , die keine Tautologien sind, gibt es in jeder Signatur, die ein mindestens 1-stelliges Funktions- oder ein mindestens 2-stelliges Relationssymbol enthält. Im ersten Falle etwa die Aussage

$$\forall xy(fx = fy \rightarrow x = y) \rightarrow \forall y \exists x y = fx.$$

Diese besagt in (A, f) , dass f^A , falls injektiv, auch schon surjektiv ist. Hier wird **Taut** durch die Menge **Tautfin** der im Endlichen allgemeingültigen Aussagen echt erweitert. **Tautfin** ist in beliebiger Signatur Beispiel einer Theorie T mit der *endlichen Modell-*

eigenschaft, d.h. jede mit T verträgliche Aussage α hat bereits ein endliches T -Modell. Es gilt allgemeiner: Die Theorie $T = Th \mathbf{K}$ einer beliebigen Klasse \mathbf{K} endlicher \mathcal{L} -Strukturen hat die endliche Modelleigenschaft. Denn ist $T + \alpha$ konsistent, also $\neg\alpha \notin T$, so ist $\mathcal{A} \models \neg\alpha$ für ein $\mathcal{A} \in \mathbf{K}$, also $\mathcal{A} \models \alpha$. Das betrifft z.B. die Theorien FSG und FG aller endlichen Halbgruppen bzw. endlichen Gruppen in $\mathcal{L}\{\circ\}$. Beide Theorien sind unentscheidbar. Für FSG ist der Beweis nicht schwer, siehe 6.6.

Anders als *Taut* ist *Tautfin* in der Regel nicht axiomatisierbar. Dies besagt

Satz 6.4 (Satz von Trachtenbrot). *Tautfin_L ist für keine Signatur L mit mindestens einem 2-stelligen Operations- oder Relationssymbol (rekursiv) axiomatisierbar.*

Beweis. Wir beschränken uns auf ersteren Fall; für ein 2-stelliges Relationssymbol folgt dasselbe leicht durch Interpretation (Satz 6.6.3). Wäre *Tautfin_L* axiomatisierbar, so wäre *Tautfin_L* wegen der endlichen Modelleigenschaft auch entscheidbar, Übung 2. Das gilt dann offenbar auch für *Tautfin_L*. Nach Übung 1 in 3.5 ist dann auch FSG entscheidbar, denn FSG ist endliche Erweiterung von *Tautfin_L* um das Assoziativgesetz. Wie aber schon erwähnt, ist FSG unentscheidbar. \square

Bemerkung. Der Satz ist mithin ein Korollar von inzwischen gewonnenen weitaus schärferen Resultaten. Für neuere Literatur über Entscheidungsprobleme dieser Art sei z.B. auf [Id] verwiesen. Anders als FG ist die Theorie der endlichen abelschen Gruppen wie die aller abelschen Gruppen entscheidbar, Wanda Szmielew. Erstere ist echte Erweiterung der Letzteren, z.B. gilt $\forall x \exists y y + y = x \rightarrow \forall x (x + x = 0 \rightarrow x = 0)$ nicht in allen, wohl aber in allen endlichen abelschen Gruppen. Dieser Nachweis ist eine überaus lehrreiche Übung.

Bereits 1922 entdeckte Behmann durch Quantorenelimination, dass *Taut* die endliche Modelleigenschaft besitzt, falls die Signatur nur einstellige Prädikatensymbole enthält (man kann dies auch unschwer mit dem Ehrenfeucht-Spiel aus 5.3 beweisen). In diesem Falle ist *Tautfin* = *Taut*. Denn für $\alpha \notin Taut$ ist $\neg\alpha$ erfüllbar, hat also ein endliches Modell, d.h. $\alpha \notin Tautfin$. Folglich ist *Tautfin* \subseteq *Taut* und damit *Tautfin* = *Taut*.

Übungen

1. Man zeige, MQ ist in \sim unbeweisbar ($X \vdash \alpha \Rightarrow X \vdash \forall x \alpha$ ist i.a. falsch).
2. Eine Theorie T habe (i) die endliche Modelleigenschaft, und (ii) die endlichen T -Modelle seien effektiv aufzählbar (genauer, ein Repräsentantensystem hiervon bis auf Isomorphie). Man zeige: (a) die in T widerlegbaren Aussagen α sind effektiv aufzählbar, (b) Ist T axiomatisierbar, so ist T auch entscheidbar.
3. Sei T eine *endlich* axiomatisierbare Theorie mit der endlichen Modelleigenschaft. Man zeige durch Rückführung auf Übung 2, T ist entscheidbar.

3.7 Fragmente der 1. Stufe und Erweiterungen

Der Gödelsche Vollständigkeitssatz legt es nahe, auch Fragmente und Erweiterungen von Sprachen der 1. Stufe auf eine möglichst vollständige formale Charakterisierung des Folgerns in der betreffenden Sprache hin zu untersuchen. Wir wollen in diesem Abschnitt einige diesbezügliche Resultate vorstellen.

Fragmente der 1. Stufe sind Formalismen, bei denen auf die volle Ausdrucksfähigkeit elementarer Sprachen verzichtet wird, z.B. durch Weglassen einiger oder aller logischen Verknüpfungen, eingeschränkte Quantifizierungen usw. Diese Formalismen sind aus verschiedenen Gründen interessant, auch wegen des gestiegenen Interesses an Systemen automatischer Informationsverarbeitung, mit denen der Nutzer meist in gewissen Fragmenten kommuniziert. Je ärmer ein linguistisches Fragment, um so bescheidener auch die darin gegebenen Formulierungsmöglichkeiten für korrekte Regeln. Daher ist das Vollständigkeitsproblem für Fragmente i.a. nichttrivial.

Ein besonders nützliches Beispiel ist die Sprache der Gleichungen einer gegebenen algebraischen Signatur L . Die in den Gleichungen vorkommenden Variablen denken wir uns stillschweigend generalisiert. Man nennt sie dann auch *Identitäten*. Modellklassen von Theorien mit Axiomensystemen aus Identitäten, wie z.B. die Gruppentheorie T_G^- (Seite 52), heißen *gleichungsdefinierte Klassen* oder *Varietäten*.

Mit dem Folgern von Identitäten γ aus einer Menge Γ von solchen hat man recht häufig zu tun. Ist $\Gamma \models \gamma$, so gibt es nach dem Vollständigkeitssatz auch einen Beweis für γ aus Γ . Aufgrund der speziellen Gestalt von Gleichungen kann man jedoch erwarten, dass dafür nicht der gesamte prädikatenlogische Formalismus benötigt wird. Tatsächlich genügen nach Satz 7.2 die auf [Bi] zurückgehenden *Birkhoffschen Regeln* (B0)–(B3) unten. Dieses Ergebnis ist deswegen befriedigend, weil man auch beim Operieren mit (B0)–(B3) gänzlich in der Sprache der Identitäten verbleibt. Die Regeln definieren einen mit \vdash^B bezeichneten Kalkül und lauten wie folgt:

$$\begin{array}{ll}
 \text{(B0)} \quad \frac{}{\Gamma \vdash^B t = t}, & \text{(B1)} \quad \frac{\Gamma \vdash^B s = t, s = t'}{\Gamma \vdash^B t = t'}, \\
 \text{(B2)} \quad \frac{\Gamma \vdash^B t_1 = t'_1, \dots, t_n = t'_n}{\Gamma \vdash^B f t_1 \dots t_n = f t'_1 \dots t'_n}, & \text{(B3)} \quad \frac{\Gamma \vdash^B s = t}{\Gamma \vdash^B s^\sigma = t^\sigma} \quad (\sigma \text{ Substitution}).
 \end{array}$$

Dabei bezeichne Γ eine Menge von Identitäten und alle in den Regeln vorkommenden Gleichungen seien als Identitäten verstanden, d.h. wir denken uns alle Variablen generalisiert. σ sei eine globale Substitution, obwohl es genügen würde, einfache Substitutionen zu betrachten. (B0)–(B2) sind uns schon in den Beispielen in 3.1 begegnet; wie dort zeigt man auch $\Gamma \vdash^B s = t \Rightarrow \Gamma \vdash^B t = s$. Birkhoffs Regeln garantieren, dass durch $s \approx t \Leftrightarrow \Gamma \vdash^B s = t$ eine Kongruenz \approx in der Termalgebra \mathcal{T} definiert wird.

\vdash^B ist korrekt, also $\Gamma \vdash^B \gamma \Rightarrow \Gamma \models \gamma$. Denn wegen $\Gamma^\forall = \Gamma$ ist nach (2) Seite 64 $\Gamma \models \gamma$ bereits dann, wenn $\mathcal{A} \models \Gamma \Rightarrow \mathcal{A} \models \gamma$, für alle \mathcal{A} . Daher ist nur zu bestätigen, dass $\mathcal{A} \models t=t$, $\mathcal{A} \models s=t, s=t' \Rightarrow \mathcal{A} \models t=t'$ usw. (B3) formuliert die *Substitutionsinvarianz* von \approx und ist korrekt, weil $\mathcal{A} \models \gamma \Rightarrow \mathcal{A} \models \gamma^\sigma$ für beliebige $\mathcal{A}, \gamma, \sigma$.

Zum Nachweis der Vollständigkeit betrachten wir die Faktorstruktur $\mathcal{F} = \mathcal{T}/\approx$. Es bezeichne \bar{t} die durch den Term t bestimmte Äquivalenzklasse modulo \approx , so dass

$$(1) \quad \bar{t}_1 = \bar{t}_2 \Leftrightarrow \Gamma \vdash^B t_1 = t_2.$$

Ferner sei $w: \text{Var} \rightarrow \mathcal{F}$, etwa $x^w = \bar{t}_x$ mit beliebig gewählten $t_x \in x^w$. Diese Wahl bestimmt eine Substitution $\sigma_w: x \mapsto t_x$. Induktiv über t ergibt sich leicht

$$(2) \quad t^{\mathcal{F},w} = \bar{t}^\sigma \text{ mit } \sigma = \sigma_w.$$

Lemma 7.1. $\Gamma \vdash^B \gamma$ ist gleichwertig mit $\mathcal{F} \models \gamma$.

Beweis. Sei $\Gamma \vdash^B t_1 = t_2 (= \gamma)$. Nach (B3) ist auch $\Gamma \vdash^B t_1^\sigma = t_2^\sigma$, also $\bar{t}_1^\sigma = \bar{t}_2^\sigma$. Daher ist $t_1^{\mathcal{F},w} = t_2^{\mathcal{F},w}$ nach (2). Weil w beliebig war, folgt $\mathcal{F} \models t_1 = t_2$. Nun sei $\mathcal{F} \models t_1 = t_2$. Sei \varkappa die sogenannte *kanonische Belegung* $x \mapsto \bar{x}$. Für diese gilt offenbar $\sigma_\varkappa = \iota$ (identische Substitution), so dass $t_i^{\mathcal{F},\varkappa} = \bar{t}_i$ nach (2). Weil wegen $\mathcal{F} \models t_1 = t_2$ gewiss $t_1^{\mathcal{F},\varkappa} = t_2^{\mathcal{F},\varkappa}$, folgt $\bar{t}_1 = \bar{t}_2$ und nach (1) damit $\Gamma \vdash^B t_1 = t_2 (= \gamma)$. \square

Satz 7.2 (Birkhoffscher Vollständigkeitssatz). $\Gamma \vdash^B \gamma \Leftrightarrow \Gamma \models \gamma$.

Beweis. $\Gamma \vdash^B \gamma \Rightarrow \Gamma \models \gamma$ wurde schon gezeigt. Sei nun $\Gamma \models \gamma$. Gewiss ist $\mathcal{F} \models \gamma$ nach Lemma 7.1. Mithin $\mathcal{F} \models \gamma$. Nach diesem Lemma ist dann aber auch $\Gamma \vdash^B \gamma$. \square

Dieser Beweis zeichnet sich einerseits durch Einfachheit, andererseits aber auch durch einen überaus abstrakten Charakter aus. Er hat mannigfache Variationen und gilt z.B. sinngemäß für Aussagen $\forall \vec{x} \pi$ mit *beliebigen* Primformeln π . Man ersetze jetzt die Regeln (B1),(B2) einfach durch (=) aus 3.1.

Einen speziellen Kalkül gibt es auch für Aussagen der Gestalt

$$(3) \quad \forall \vec{x} (\gamma_1 \wedge \cdots \wedge \gamma_n \rightarrow \gamma_0) \quad (n \geq 0, \text{ alle } \gamma_i \text{ Gleichungen}),$$

Quasiidentitäten genannt. Die Modellklassen von Axiomen der Gestalt (3) heißen auch *Quasivarietäten* und sind wichtig für Algebra und Logik. (B0) bleibt erhalten und (B1),(B2) werden ersetzt durch die prämissenlosen Regeln

$$\Gamma \vdash x = y \wedge x = z \rightarrow y = z, \quad \Gamma \vdash \bigwedge_{i=1}^n x_i = y_i \rightarrow f\vec{x} = f\vec{y}.$$

Nebst einer Anpassung von (B3) benötigt man noch Regeln über die formale Handhabung der Prämissen $\gamma_1, \dots, \gamma_n$ in (3), etwa deren Vertauschbarkeit (für Einzelheiten siehe z.B. [Se]), sowie eine *Schnittregel* der Gestalt

$$\frac{\Gamma \vdash \alpha \wedge \delta \rightarrow \gamma \mid \Gamma \vdash \alpha \rightarrow \delta}{\Gamma \vdash \alpha \rightarrow \gamma} \quad (\alpha \text{ eine Konjunktion von Gleichungen}).$$

Wir betrachten nun einige von zahlreichen Möglichkeiten für Erweiterungen der 1. Stufe im Sinne von erweiterter Ausdrucksfähigkeit: Eine Sprache $\mathcal{L}' \supseteq \mathcal{L}$ derselben Signatur wie \mathcal{L} heie *ausdrucksfhiger* als \mathcal{L} , wenn $\text{Md } \alpha$ fr wenigstens eine Aussage $\alpha \in \mathcal{L}'$ von allen $\text{Md } \beta$ fr $\beta \in \mathcal{L}$ verschieden ist. Einige der Eigenschaften von Sprachen der 1. Stufe gehen dabei jedoch verloren. Diese Sprachen bieten nmlich ein Optimum an anwendungsreichen Eigenschaften. Dies behauptet der

Satz von Lindstrm (siehe [EFT] oder [CK]). *Es gibt keine Sprache gegebener Signatur, welche ausdrucksfhiger ist als die Sprache 1. Stufe und fr welche sowohl der Kompaktheitssatz als auch der Satz von Lwenheim-Skolem gelten.*

Mehrsortige Sprachen. Zur Beschreibung geometrischer Sachverhalte ist es bequem, mehrere Variablensorten zu benutzen, solche fr Punkte, fr Geraden und – je nach Dimension – auch fr hherdimensionale geometrische Objekte. Es ist ratsam, fr jedes Argument eines Prdikaten- oder Operationssymbols einer solchen Sprache seine *Sorte* festzulegen, z.B. hat die Inzidenzrelation der ebenen Geometrie ein Argument fr Punkte und eines fr Geraden. Bei Funktionen muss zustzlich die Sorte ihrer Werte angegeben sein. Ist \mathcal{L} k -sortig und sind $\mathbf{v}_0^s, \mathbf{v}_1^s, \dots$ die Variablen der Sorte s ($1 \leq s \leq k$), ist jedem Relationssymbol r eine Folge (s_1, \dots, s_n) zugeordnet, und mit r beginnende Primformeln haben in Sprachen ohne Funktionssymbole die Gestalt $rx_1^{s_1} \dots x_n^{s_n}$ wobei $x_i^{s_i}$ irgendeine Variable der Sorte s_i bezeichnet.

Mehrsortige Sprachen stellen nur eine unwesentliche Erweiterung des bisherigen Konzepts dar, solange die Sorten semantisch gleichberechtigt sind. Anstelle einer Sprache \mathcal{L} mit k Variablensorten lsst sich immer auch eine einsortige Sprache \mathcal{L}' mit zustzlichen einstelligen Prdikatensymbolen P_1, \dots, P_k und unter Einschluss gewisser Zusatzaxiome betrachten: $\exists x P_i x$ fr $i = 1, \dots, k$ (keine Sorte ist leer, sonst wre sie ja entbehrlich) und $\neg \exists x (P_i x \wedge P_j x)$ fr $i \neq j$ (Sortendisjunktheit). Zum Beispiel knnte man die ebene Geometrie auch in einer einsortigen Sprache mit den zustzlichen Prdikaten *pkt* (Punkt sein) und *ger* (Gerade sein) beschreiben. Abgesehen von einigen Besonderheiten im Umgang mit der Termeinsetzung verhalten sich mehrsortige Sprachen fast genauso wie einsortige.

Sprachen der 2. Stufe. Einige oft zitierte Axiome, z.B. das Induktionsaxiom IA, knnen als Aussagen 2. Stufe angesehen werden. Die einfachste Erweiterung einer elementaren Sprache zu einer hherstufigen ist die *monadische Sprache 2. Stufe*, eine zweisortige Sprache, aber mit spezieller Interpretation der zweiten Sorte. Betrachten wir eine solche Sprache \mathcal{L} mit Variablen x, y, z, \dots fr Individuen, Variablen X, Y, Z, \dots fr Mengen aus diesen Individuen, sowie mindestens einem zweistelligen Relationssymbol \in . Primformeln seien $x = y$, $X = Y$ und $x \in X$. Eine \mathcal{L} -Struktur ist allgemein von der Form (\mathcal{A}, B, \in) mit $\in \subseteq A \times B$. Ziel ist, dass \in nach Formulierung von Zusatzaxiomen wie z.B. $\forall X, Y [\forall x (x \in X \leftrightarrow x \in Y) \rightarrow X = Y]$ – dies

entspricht dem Extensionalitätsaxiom in 3.4 – als Elementbeziehung interpretierbar ist und die Objekte aus B als Teilmengen von A . Dieses Ziel lässt sich zwar nicht vollständig, aber nahezu erreichen: Es lassen sich Axiome so formulieren, dass B in die Potenzmenge von A *einbettbar* ist. Das funktioniert auch bei Hinzunahme weiterer Sorten für Elemente von $\mathfrak{P}\mathfrak{P}A$, $\mathfrak{P}\mathfrak{P}\mathfrak{P}A$ usw. Diese „Vollständigkeit des Stufenkalküls“ (siehe etwa [As]) spielt z.B. eine Rolle in der Nichtstandard-Analyse.

Eine umfassendere Sprache \mathcal{L}_{II} der 2. Stufe gewinnt man durch Hinzunahme von quantifizierbaren Variablen für beliebige Relationen und Operationen über den Individuenbereichen. \mathcal{L}_{II} erfüllt aber schon für $\mathcal{L} = \mathcal{L}_=$ weder den Endlichkeitssatz noch den Satz von Löwenheim-Skolem. Ersterer ist verletzt, weil sich leicht ein Satz α_{fin} aus \mathcal{L}_{II} angeben lässt, so dass $\mathcal{A} \models \alpha_{\text{fin}}$ genau dann, wenn A endlich ist. Denn man beweist unschwer: A ist dann und nur dann endlich, wenn A so geordnet werden kann, dass jede nichtleere Teilmenge von A sowohl ein kleinstes als auch ein größtes Element besitzt. Dieser Sachverhalt lässt sich mittels einer zwei- und einer einstelligen Prädikatenvariablen offenbar mühelos formalisieren.

Auch der Satz von Löwenheim-Skolem ist für \mathcal{L}_{II} leicht widerlegbar. Man muss in \mathcal{L}_{II} nur die Aussage ‘Es gibt eine dichte Ordnung ohne Lücken auf A ’ niederschreiben. Diese hat nämlich kein abzählbares Modell (siehe hierzu auch Beispiel 2 in 5.2). Damit kann es natürlich auch keine formale Kennzeichnung des Folgerns in \mathcal{L}_{II} geben. Schlimmer noch: Die ZFC-Axiome – betrachtet als Axiome der Hintergrundmengenlehre – reichen nicht aus, um festzulegen, was eine Tautologie in \mathcal{L}_{II} sein soll. Dazu genügt z.B. die Einsicht, dass die von ZFC unabhängige Kontinuums-hypothese CH (siehe Seite 135) als ein \mathcal{L}_{II} -Satz α_{CH} formuliert werden kann. Sollte CH wahr sein, ist α_{CH} eine \mathcal{L}_{II} -Tautologie, sonst nicht. Es sieht nicht so aus, als ob mathematische Intuition hinreicht, diese Frage eindeutig zu entscheiden.

Neue Quantoren. Eine einfache syntaktische Erweiterung $\mathcal{L}_{\mathfrak{O}}$ einer Sprache \mathcal{L} der 1. Stufe ergibt sich durch Aufnahme eines neuen, mit \mathfrak{O} bezeichneten Quantors, der formal wie der \forall -Quantor gehandhabt wird. Eine neuartige Interpretation von \mathfrak{O} ergibt sich, ausgehend von einem Modell $\mathcal{M} = (\mathcal{A}, w)$, mit der Erfüllungsklausel

$$(0) \quad \mathcal{M} \models \mathfrak{O}x\alpha \Leftrightarrow \{a \in A \mid \mathcal{M}_x^a \models \alpha\} \text{ ist unendlich.}$$

Mit dieser Interpretation schreiben wir $\mathcal{L}_{\mathfrak{O}}^0$ statt $\mathcal{L}_{\mathfrak{O}}$, da wir noch eine andere Interpretation von \mathfrak{O} diskutieren werden. $\mathcal{L}_{\mathfrak{O}}^0$ ist ausdrucksfähiger als \mathcal{L} . Das sieht man z.B. daran, dass der Endlichkeitssatz für $\mathcal{L}_{\mathfrak{O}}^0$ nicht mehr gilt: Sei X die Menge aller Aussagen \exists_n (‘es gibt mindestens n Elemente’) plus $\alpha_{\text{fin}} := \neg \mathfrak{O}x x = x$ (‘es gibt nur endlich viele Elemente’). Jede endliche Teilmenge von X hat ein Modell, nicht aber ganz X . Immerhin erfüllt $\mathcal{L}_{\mathfrak{O}}^0$ noch den Satz von Löwenheim-Skolem. Dies lässt sich mit den Methoden des Abschnitts 5.1 unschwer nachweisen. Wegen des fehlenden

Endlichkeitssatzes kann es auch keinen vollständigen Regelkalkül für \mathcal{L}_\exists^0 geben. Andernfalls könnte man wie in 3.1 doch den Endlichkeitssatz beweisen. Es gibt aber eine Anzahl nichttrivialer korrekter Regeln für \mathcal{L}_\exists^0 , z.B.

$$\begin{array}{ll} \text{(Q1)} \frac{}{X \vdash \neg \exists x(x=y \vee x=z)} (x \neq y, z), & \text{(Q2)} \frac{X \vdash \exists x \alpha}{X \vdash \exists y \alpha} (y \notin \text{frei } \alpha), \\ \text{(Q3)} \frac{X \vdash \forall x(\alpha \rightarrow \beta)}{X \vdash \exists x \alpha \rightarrow \exists x \beta}, & \text{(Q4)} \frac{X \vdash \exists x \exists y \alpha \mid X \vdash \neg \exists y \exists x \alpha}{X \vdash \exists y \exists x \alpha}. \end{array}$$

(Q1) besagt anschaulich, die Paarmenge $\{y, z\}$ ist endlich. (Q2) ist die gebundene Umbenennung. (Q3) besagt, dass mit jeder Menge auch jede Obermenge unendlich ist. Die Korrektheit von (Q4) werde für $\mathcal{M} = (\mathcal{A}, w) \models X$ und $\alpha = \alpha(x, y)$ wie folgt veranschaulicht: Sei $A_b = \{a \in A \mid \mathcal{A} \models \alpha[a, b]\}$. Es besagt $\mathcal{M} \models \exists x \exists y \alpha$ dann ‘ $\bigcup_{b \in A} A_b$ ist unendlich’. $\mathcal{M} \models \neg \exists y \exists x \alpha$ besagt ‘es gibt nur endlich viele Indizes b mit $A_b \neq \emptyset$ ’. Die Konklusion $\mathcal{M} \models \exists y \exists x \alpha$ besagt daher ‘ A_b ist für wenigstens einen Index b unendlich’. (Q4) drückt also den nur etwas umformulierten Sachverhalt aus, dass die Vereinigung eines endlichen Systems endlicher Mengen wieder endlich ist.

Man ersetze die Erfüllungsklausel (0) nunmehr durch

$$(1) \quad \mathcal{M} \models \exists x \alpha \Leftrightarrow \{a \in A \mid \mathcal{M}_x^a \models \alpha\} \text{ ist überabzählbar.}$$

Auch mit dieser Interpretation sind (Q1)–(Q4) korrekt für \mathcal{L}_\exists^1 ($= \mathcal{L}_\exists^0$ mit der Interpretation (1)). Die Regel (Q4) bringt jetzt offenbar zum Ausdruck, dass eine abzählbare Vereinigung abzählbarer Mengen wieder abzählbar ist. Sie bleibt also korrekt. Mehr noch, der aus den Basisregeln aus 3.1 durch Hinzufügen der Regeln (Q1)–(Q4) entstehende Logik-Kalkül \vdash^1 ist überraschenderweise sogar vollständig für diese Semantik, wenn man sich auf abzählbare Sequenzen beschränkt. Es gilt also $X \vdash^1 \alpha \Leftrightarrow X \models \alpha$ für abzählbares $X \subseteq \mathcal{L}_\exists^1$, siehe [CK]. Hieraus ergibt sich ein Kompaktheitssatz für \mathcal{L}_\exists^1 in folgender Gestalt: *Hat jede endliche Teilmenge einer abzählbaren Formelmengens $X \subseteq \mathcal{L}_\exists^1$ ein Modell, so auch X .* Für überabzählbare X ist diese Behauptung im Allgemeinen falsch (Übung).

Programmiersprachen. Alle bisher erwähnten Sprachen haben insofern statischen Charakter, als den Formeln unabhängig von Ort und Zeit bei vorgegebenen Belegungen w in einer Struktur \mathcal{A} gewisse Wahrheitswerte entsprechen. Man kann eine Sprache \mathcal{L} der 1. Stufe aber auch zu einer *Programmiersprache* \mathcal{PL} mit *dynamischem* Charakter erweitern. Ein Programm $\mathcal{P} \in \mathcal{PL}$ startet die Ausführung mit einer Belegung $w: \text{Var} \rightarrow A$ (der Träger einer vorgegebenen \mathcal{L} -Struktur \mathcal{A}) und verändert schrittweise die Werte der Variablen. Falls \mathcal{P} bei Eingabe von w terminiert, d.h. die Rechnung beendet, ist das Ergebnis eine neue Belegung $w^\mathcal{P}$. Andernfalls sei $w^\mathcal{P}$ nicht definiert. Die Beschreibung dieser i.a. nur partiell definierten Operation $w \mapsto w^\mathcal{P}$ heiße die *prozedurale Semantik* von \mathcal{PL} . Auch für diese Art von Semantik können z.B. Vollständigkeitsfragen durchaus sinnvoll behandelt werden.

Wir geben jetzt eine derartige, von \mathcal{L} abhängige Sprache \mathcal{PL} an. Die logische Signatur von \mathcal{L} werde erweitert um die Symbole $:=$, WHILE, DO, END und ; (Semikolon). Programme über \mathcal{L} werden induktiv in folgender Weise als Zeichenfolgen definiert:

1. Für beliebige $x \in \text{Var}$ und Terme t von \mathcal{L} ist $x := t$ ein Programm.
2. Ist $\alpha \in \mathcal{L}$ quantorenfrei und sind \mathcal{P}, \mathcal{Q} Programme, so auch die Zeichenfolgen $\mathcal{P} ; \mathcal{Q}$ und WHILE α DO \mathcal{P} END.

Keine anderen Zeichenfolgen seien in diesem Zusammenhang Programme. $\mathcal{P} ; \mathcal{Q}$ soll bedeuten, dass erst \mathcal{P} und danach \mathcal{Q} ausgeführt wird. Es sei \mathcal{P}^n die n -fache Hintereinanderausführung von \mathcal{P} , genauer \mathcal{P}^0 sei das leere Programm (also $w^{\mathcal{P}^0} = w$) und $\mathcal{P}^{n+1} = \mathcal{P}^n ; \mathcal{P}$. Die prozedurale Semantik für \mathcal{PL} werde wie folgt präzisiert:

- (a) $w^{x:=t} = w \frac{tw}{x}$ (d.h. der Variablen x wird ein neuer Wert erteilt, nämlich tw).
- (b) Mit $w^{\mathcal{P}}$ und $(w^{\mathcal{P}})^{\mathcal{Q}}$ sei auch $w^{\mathcal{P};\mathcal{Q}}$ definiert, und es sei $w^{\mathcal{P};\mathcal{Q}} = (w^{\mathcal{P}})^{\mathcal{Q}}$.
- (c) Für $\mathcal{Q} := \text{WHILE } \alpha \text{ DO } \mathcal{P} \text{ END}$ sei $w^{\mathcal{Q}} = w^{\mathcal{P}^k}$. Dabei sei k gemäß anschaulicher Vorstellung über die „WHILE-Schleife“ die kleinste Zahl mit $\mathcal{A} \models \alpha[w^{\mathcal{P}^i}]$ für alle $i < k$ und $\mathcal{A} \not\models \alpha[w^{\mathcal{P}^k}]$, falls ein solches k existiert und alle $w^{\mathcal{P}^i}$ für $i \leq k$ wohldefiniert sind. Andernfalls sei $w^{\mathcal{Q}}$ nicht definiert – \mathcal{Q} angesetzt auf w terminiert dann nicht. Falls $k = 0$, also $\mathcal{A} \not\models \alpha[w]$, ist $w^{\mathcal{Q}} = w$, d.h. \mathcal{P} wird überhaupt nicht ausgeführt.

Beispiel. Sei $\mathcal{L} = \mathcal{L}\{0, S, R\}$ und $\mathcal{A} = (\mathbb{N}, 0, S, R)$, wobei S und R die Nachfolger- bzw. Vorgängerfunktion bezeichnen, sowie \mathcal{P} das Programm

$$z := x ; v := y ; \text{WHILE } v \neq 0 \text{ DO } z := Sz ; v := Rv \text{ END.}$$

Haben x und y zu Beginn die Werte $x^w = m$ und $y^w = n$, endet das Programm mit $z^{w^{\mathcal{P}}} = m + n$. Kurzum, \mathcal{P} terminiert und berechnet $m + n$. Es sei vermerkt, dass in \mathcal{PL} das bekannte Programmschema IF α THEN \mathcal{P} ELSE \mathcal{Q} END definiert ist durch $x := 0 ; \text{WHILE}(\alpha \wedge x = 0) \text{ DO } \mathcal{P} ; x := S0 \text{ END} ; \text{WHILE } x = 0 \text{ DO } \mathcal{Q} ; x := S0 \text{ END}$. Hierbei sei $x \notin \text{var}\{\mathcal{P}, \mathcal{Q}, \alpha\}$. \mathcal{PL} ist wie PROLOG eine universelle Programmiersprache in dem Sinne, dass jede berechenbare Funktion in \mathcal{PL} auch berechnet werden kann.

Übungen

1. Man zeige, eine Varietät \mathbf{K} ist abgeschlossen gegenüber Homomorphismen ($\mathbf{HK} \subseteq \mathbf{K}$), Subalgebren ($\mathbf{SK} \subseteq \mathbf{K}$) und direkten Produkten ($\mathbf{SK} \subseteq \mathbf{K}$)⁹⁾.
2. Man zeige, $\mathcal{L}_{\mathcal{C}}^1$ und \mathcal{L}_{II} verletzen den Satz von Löwenheim-Skolem, und $\mathcal{L}_{\mathcal{C}}^1$ verletzt auch den Endlichkeitssatz für überabzählbare Formelmengen.
3. Man drücke die Kontinuumshypothese CH als einen Satz von \mathcal{L}_{II} aus.

⁹⁾Hat \mathbf{K} umgekehrt diese drei Eigenschaften, so ist \mathbf{K} auch eine Varietät. Dies ist Birkhoffs **HSP**-Theorem (siehe z.B. [Mo]). Dieser Satz leitete die Entwicklung der Universellen Algebra ein.

Kapitel 4

Grundlagen der Logikprogrammierung

Logikprogrammierung dient weniger der Behandlung numerischer Probleme in Wissenschaft und Technik als vielmehr der Wissensverarbeitung, z.B. der praktischen Realisierung von Expertensystemen der künstlichen Intelligenz. Man muss unterscheiden zwischen Logikprogrammierung als einem theoretisch orientierten Gebiet und der für praktische Aufgaben in diesem Zusammenhang meistens benutzten Programmiersprache PROLOG. Diesbezüglich beschränken wir uns auf die Vorstellung einer stark vereinfachten Version, die aber das Typische erkennen lässt.

Die in 4.1 behandelten Begriffe, z.B. der des Termmodells, sind ziemlich allgemeiner Natur und nicht nur für praktische Anwendungen bedeutsam. Sie haben ihren Ursprung in theoretischen Fragestellungen der mathematischen Logik und sind schon vor Erfindung des Computers geprägt worden. Für gewisse Formelmengen, insbesondere für die in der logischen Programmierung wichtigen Mengen universaler Hornformeln, gewinnt man Termmodelle kanonisch. Hierbei handelt es sich um eine modelltheoretische Verallgemeinerung der sogenannten freien Strukturen wie freien Halbgruppen, Gruppen, Ringen usw.

Erst die in 4.2 vorgestellte Resolutionsmethode und ihre Verbindung mit der in 4.3 behandelten Unifikation ist durch maschinelle Informationsverarbeitung direkt inspiriert worden. Diese ist für die logische Programmierung ebenso wie für die darüber hinausgehenden Aufgaben des automatischen Beweisens von maßgeblicher Bedeutung. Resolution wird zuerst im Rahmen der Aussagenlogik erklärt. Der Resolutionsatz wird konstruktiv bewiesen, ohne Rückgriff auf den aussagenlogischen Kompaktheitssatz. Die Verbindung mit der Unifikation und ihre Anwendung auf die logische Programmierung erfolgt in 4.4. Elementare Einführungen in diesen Problemkreis bieten auch [Schö] und [Ll], anspruchsvollere sind [GH] und [Do].

4.1 Termmodelle und der Satz von Herbrand

Sei \mathcal{L} eine elementare Sprache. Unter einem *Termmodell* sei ein \mathcal{L} -Modell \mathcal{F} verstanden, dessen Träger aus den Äquivalenzklassen \bar{t} einer Kongruenz $\approx_{\mathcal{F}}$ auf der Termalgebra \mathcal{T} der \mathcal{L} -Terme t besteht; dabei sei $f^{\mathcal{F}}(\bar{t}_1, \dots, \bar{t}_n) := \overline{ft_1 \cdots t_n}$, $c^{\mathcal{F}} := \bar{c}$ und $x^{\mathcal{F}} := \bar{x}$. Diese Variablenbelegung heißt auch die *kanonische*. Es ist immer im Auge zu behalten, dass $s \approx_{\mathcal{F}} t$ und $\bar{s} = \bar{t}$ ein und dasselbe bedeuten. Falls $\approx_{\mathcal{F}}$ die Identität in \mathcal{T} ist, pflegt man den Träger von \mathcal{F} mit \mathcal{T} zu identifizieren.

Termmodelle sind uns schon des öfteren begegnet, sowohl in Lemma 3.2.5 als auch in Lemma 3.7.1. Bezeichnet \mathfrak{F} die \mathcal{F} unterliegende Struktur, so ist $\mathcal{F} = (\mathfrak{F}, w)$ mit $x^w = \bar{x}$. Unabhängig von einer Spezifikation der $r^{\mathcal{F}}$ gelten immer

- (1) $t^{\mathcal{F}} = \bar{t}$ für alle $t \in \mathcal{T}$,
- (2) $\mathcal{F} \models \forall \vec{x} \alpha \Leftrightarrow \mathcal{F} \models \alpha_{\vec{x}}^{\vec{t}}$ für alle $\vec{t} \in \mathcal{T}^n$ (α quantorenfrei).

(1) folgt leicht durch Termination. (2) ergibt sich von links nach rechts gemäß Korollar 2.3.6, und andersherum wie folgt: $\mathcal{F} \models \alpha_{\vec{x}}^{\vec{t}}$ liefert $\mathcal{F}_{\vec{x}}^{\vec{t}} \models \alpha$ nach dem Substitutionssatz 2.3.5. Nach (1) also $\mathcal{F}_{x_1 \cdots x_n}^{\bar{t}_1 \cdots \bar{t}_n} \models \alpha$, für alle $t_1, \dots, t_n \in \mathcal{T}$. Das aber bedeutet $\mathcal{F} \models \forall \vec{x} \alpha$, weil die Werte \bar{t} für $t \in \mathcal{T}$ den Träger von \mathcal{F} bereits ausschöpfen.

Wir erfassen nun die für den Vollständigkeitsbeweis aus Kapitel 3 ebenso wie für das Folgende wesentliche Konstruktion in Lemma 3.2.5 durch folgende

Definition. Das mit einer Formelmeng X assoziierte *Termmodell* $\mathcal{F}X$ sei dasjenige, für welches $\approx_{\mathcal{F}X}$ und die Relationen $r^{\mathcal{F}X}$ erklärt sind durch

$$s \approx_{\mathcal{F}X} t \Leftrightarrow X \vdash s = t \quad ; \quad r^{\mathcal{F}X} \bar{t}_1 \cdots \bar{t}_n \Leftrightarrow X \vdash r t_1 \cdots t_n.$$

Eine konsistente Menge $X \subseteq \mathcal{L}$ hat zwar nicht immer ein Termmodell in \mathcal{L} , siehe aber Satz 1.1 unten. Nach (1) ist $\mathcal{F}X \models s = t \Leftrightarrow \bar{s} = \bar{t} \Leftrightarrow X \vdash s = t$. Analog ergibt sich auch $\mathcal{F}X \models r \vec{t} \Leftrightarrow X \vdash r \vec{t}$. Deshalb gilt nebst (1) und (2) immerhin

- (3) $\mathcal{F}X \models \pi \Leftrightarrow X \vdash \pi$ (π Primformel).

Oft wird X eine Theorie T oder ein Axiomensystem von T sein. Schreibt man $s \approx_T t$ für $s \approx_{\mathcal{F}T} t$ und sagt, s, t seien *äquivalent in T* , bedeutet $s \approx_T t$ dasselbe wie $\vdash_T s = t$. In folgendem Beispiel ist das Termmodell $\mathcal{F}T$ tatsächlich ein Modell für T .

Beispiel 1. Sei T die Theorie der Halbgruppen in $\mathcal{L}\{\circ\}$. Wegen des Assoziativgesetzes ist in T jeder Term t zu einem Term in Linksklammerung äquivalent, der mit $x_0 \cdots x_n$ bezeichnet sei, d.h. $t \approx_T x_0 \cdots x_n$. Hier liste x_0, \dots, x_n die Variablen von t in der Reihenfolge ihres Vorkommens von links nach rechts auf, eventuell mit Wiederholungen. Man zeigt unschwer $(x_0 \cdots x_n) \circ (y_0 \cdots y_m) \approx_T x_0 \cdots x_n y_0 \cdots y_m$ und

$$x_0 \cdots x_n \approx_T y_0 \cdots y_m \Leftrightarrow m = n \ \& \ x_i = y_i \text{ für alle } i \leq n.$$

Deswegen kann man die Termklassen \bar{t} einfach mit den Worten über dem Alphabet Var identifizieren. Genauer formuliert, die \mathcal{FT} unterliegende Struktur ist isomorph zur Worthalbgruppe über dem Alphabet Var und folglich auch Modell für T .

Wir erweitern nun geringfügig den Modellbegriff. Sei $\text{Var}_k := \{\mathbf{v}_0, \dots, \mathbf{v}_{k-1}\}$, also $\mathcal{L}^k = \{\varphi \in \mathcal{L} \mid \text{frei } \varphi \subseteq \text{Var}_k\}$. Es heie (\mathcal{A}, w) ein \mathcal{L}^k -Modell, wenn $\text{dom } w \supseteq \text{Var}_k$, d.h. w muss für $\mathbf{v}_k, \mathbf{v}_{k+1}, \dots$ nicht erklärt sein. Ein \mathcal{L}^k -Modell ist stets auch ein \mathcal{L}^m -Modell für $m < k$. In diesem Sinne sind \mathcal{L} -Strukturen zugleich \mathcal{L}^0 -Modelle.

Sei $\mathcal{T}_k := \{t \in \mathcal{T} \mid \text{var } t \subseteq \text{Var}_k\}$. Damit \mathcal{T}_k auch für $k=0$ nicht leer ist, setzen wir bei jeder Betrachtung von \mathcal{T}_0 stillschweigend voraus, dass \mathcal{L} wenigstens eine Konstante enthält. Weil mit $t_1, \dots, t_n \in \mathcal{T}_k$ auch $f\vec{t} \in \mathcal{T}_k$, ist \mathcal{T}_k für jedes k eine Subalgebra von \mathcal{T} . Für ein Termmodell \mathcal{F} ist ebenso $\{\bar{t} \mid t \in \mathcal{T}_k\}$ gegenüber den $f^{\mathcal{F}}$ abgeschlossen, definiert also eine Substruktur der \mathcal{F} unterliegenden Struktur. Diese wird durch $x \mapsto \bar{x}$ für $x \in \text{Var}_k$ in natürlicher Weise zu einem \mathcal{L}^k -Modell erweitert, das nachfolgend mit \mathcal{F}_k bezeichnet sei. Der Träger von \mathcal{F}_k ist $\{\bar{t} \mid t \in \mathcal{T}_k\}$. Für $X \subseteq \mathcal{L}^k$ ist $(\mathcal{F}X)_k$ offenbar ein \mathcal{L}^k -Modell, das kurz mit $\mathcal{F}_k X$ bezeichnet werde. Genau wie (1), (2), (3) verifiziert man leicht

- (1_k) $t^{\mathcal{F}_k} = \bar{t}$ für alle $t \in \mathcal{T}_k$,
- (2_k) $\mathcal{F}_k \models \forall \vec{x} \alpha \Leftrightarrow \mathcal{F}_k \models \alpha_{\vec{x}}^{\vec{t}}$ für alle $\vec{t} \in \mathcal{T}_k^n$ (α quantorenfrei).
- (3_k) $\mathcal{F}_k X \models \pi \Leftrightarrow X \vdash \pi$ (π Primformel aus \mathcal{L}^k)

Ist $\alpha = \forall \vec{x} \beta$ mit quantorenfreiem β , heie $\beta_{\vec{x}}^{\vec{t}}$ eine *Instanz* von α . Falls $\vec{t} \in \mathcal{T}_k^n$, heie $\beta_{\vec{x}}^{\vec{t}}$ auch eine \mathcal{T}_k -Instanz, und für $k=0$ auch eine *Grundinstanz* von α . Man beachte, Grundinstanzen sind sowohl variablen- als auch quantorenfrei. Es bezeichne $\text{GI}(X)$ die Menge der Grundinstanzen einer Menge X aus \forall -Formeln.

Satz 1.1. *Sei $U (\subseteq \mathcal{L})$ eine Menge universaler Formeln und \tilde{U} die Menge aller Instanzen der Formeln aus U . Dann sind gleichwertig*

- (i) U ist konsistent, (ii) \tilde{U} ist konsistent, (iii) U hat ein Termmodell in \mathcal{L} .

Dasselbe gilt, falls $U \subseteq \mathcal{L}^k$ und \tilde{U} die Menge aller \mathcal{T}_k -Instanzen der Formeln aus U bezeichnet. Speziell ist eine Menge U von \forall -Aussagen einer Sprache mit Konstanten genau dann konsistent, wenn $\text{GI}(U)$ konsistent ist.

Beweis. (i) \Rightarrow (ii) ist klar, denn $U \vdash \tilde{U}$. (ii) \Rightarrow (iii): Sei $\mathcal{M} \models \tilde{U}$ und $\mathcal{F} := \mathcal{F}X$ für $X := \{\varphi \in \mathcal{L} \mid \mathcal{M} \models \varphi\}$. Nach (3) ist $\mathcal{F} \models \pi \Leftrightarrow \mathcal{M} \models \pi (\Leftrightarrow X \vdash \pi)$ für Primformeln π . Induktion über \wedge, \neg liefert dasselbe für alle quantorenfreien Formeln. Weil $\mathcal{M} \models \tilde{U}$, ist also $\mathcal{F} \models \tilde{U}$. Das ergibt $\mathcal{F} \models U$ nach (2). (iii) \Rightarrow (i): Trivial. Falls $U \subseteq \mathcal{L}^k$, verläuft der Beweis mit (3_k), (2_k) und $\mathcal{F}_k = \mathcal{F}_k X$ für $X = \{\varphi \in \mathcal{L}^k \mid \mathcal{M} \models \varphi\}$ analog. \square

Bemerkung 1. Mit diesem Satz lässt sich das Erfüllbarkeitsproblem für $X \subseteq \mathcal{L}$ grundsätzlich auf ein aussagenlogisches zurückführen. Denn nach Satz 2.6.3 ist X unter Einbeziehung neuer Operationssymbole erfüllbarkeitsgleich mit einer Menge U von \forall -Formeln und diese ist nach Satz 1.1 erfüllbarkeitsgleich mit der quantorenfreien Formelmengende \tilde{U} . Man ersetzt nun die in den Formeln von \tilde{U} vorkommenden Primformeln π wie in den Beispielen in 1.5 durch Aussagenvariablen p_π , verschiedene Primformeln durch verschiedene Variablen. Nach Hinzufügen spezieller Formeln zur adäquaten Übersetzung von Gleichungen erhält man dann leicht eine erfüllbarkeitsgleiche Menge aussagenlogischer Formeln.

Mit Satz 1.1 erhalten wir für eine konsistente Menge U universaler Aussagen ein Termmodell $\mathcal{F}_0 X$ für geeignetes $X \supseteq U$. Wichtig für die logische Programmierung ist nun der Fall, dass das Identitätssymbol in U nicht vorkommt. Dann hat U nämlich ein Modell \mathcal{M} mit $\mathcal{M} \models s=t \Leftrightarrow s = t$ (Übung 2 in 3.2), so dass im Beweis von Satz 1.1 eine Faktorisierung in der Konstruktion von $\mathcal{F}_0 = \mathcal{F}_0 X$ entfällt und \mathcal{T}_0 selbst der Träger von \mathcal{F}_0 ist. \mathcal{F}_0 heißt auch ein *Herbrand-Modell* für U . Allgemein sei eine *Herbrand-Struktur* \mathcal{A} eine solche mit dem Träger \mathcal{T}_0 , in der die Operationen $f^{\mathcal{A}}$ kanonisch, d.h. durch $f^{\mathcal{A}}(t_1, \dots, t_n) = f\vec{t}$ für $t_1, \dots, t_n \in \mathcal{T}_0$ erklärt sind. Relationssymbole können hingegen ganz beliebig interpretiert sein.

Beispiel 2. Sei U die leere Aussagenmenge in $\mathcal{L} = \mathcal{L}\{0, S\}$. Weil $=$ in U nicht vorkommt, besteht der Träger einer wie in Satz 1.1 konstruierten Herbrand-Struktur \mathcal{F}_0 aus allen Grundtermen von \mathcal{L} , d.h. aus den \underline{n} ($= S^n 0$). Mehr noch, \mathcal{F}_0 ist isomorphes Bild von $(\mathbb{N}, 0, S)$ mit dem Isomorphismus $n \mapsto \underline{n}$ wie man leicht sieht.

Um die Formulierungen übersichtlich zu halten, schreiben wir fortan auch \mathcal{L}^∞ , \mathcal{T}_∞ , $\mathcal{F}_\infty X$ für \mathcal{L} , \mathcal{T} bzw. $\mathcal{F}X$. Wie üblich sei $k < \infty$ für alle $k \in \mathbb{N}$.

Satz 1.2 (Satz von Herbrand). Sei $k \leq \infty$ und $U \subseteq \mathcal{L}^k$ eine Menge universaler Formeln, sowie $\exists \vec{x} \alpha \in \mathcal{L}^k$ mit quantorenfreiem α . Dann sind gleichwertig

- (i) $U \vdash \exists \vec{x} \alpha$,
- (ii) $U \vdash \bigvee_{i \leq m} \alpha \frac{\vec{t}_i}{\vec{x}}$ für gewisse $\vec{t}_0, \dots, \vec{t}_m \in \mathcal{T}_k^n$,
- (iii) $\tilde{U} \vdash \bigvee_{i \leq m} \alpha \frac{\vec{t}_i}{\vec{x}}$ für gewisse $\vec{t}_0, \dots, \vec{t}_m \in \mathcal{T}_k^n$ (\tilde{U} wie in Satz 1.1).

Beweis. Weil $U \vdash \tilde{U}$, gilt sicher (iii) \Rightarrow (ii) \Rightarrow (i). Daher verbleibt der Beweis von (i) \Rightarrow (iii): Wegen (i) ist $U \cup \{\forall \vec{x} \neg \alpha\}$ inkonsistent. Nach Satz 1.1 also auch $X = \tilde{U} \cup Y$ mit $Y := \{\neg \alpha \frac{\vec{t}}{\vec{x}} \mid \vec{t} \in \mathcal{T}_k^n\}$. Damit folgt (iii) bereits aussagenlogisch: Man denke sich die Formeln von X wie in Bemerkung 1 beschrieben durch Aussagenvariablen ersetzt und argumentiere wie in Übung 1 in 1.4. \square

Dieser Satz gilt i.a. nicht für beliebige Formelmengen U . So gilt z.B. $\vdash_T \exists x x \circ y = z$ in der Gruppentheorie T in $\mathcal{L}\{e, \circ\}$, aber es lässt sich (etwas aufwendig) zeigen, dass für kein m und keine Terme t_0, \dots, t_m der Originalsprache $\vdash_T \bigvee_{i \leq m} t_i \circ y = z$.

Hornformeln. Wir definieren nun den für viele Zwecke nützlichen Begriff der *Hornformel* einer Sprache \mathcal{L} und zugleich den einer aussagenlogischen Hornformel.

Definition. (a) Literale sind Basis-Hornformeln. Ist α eine Primformel und β eine Basis-Hornformel, so ist auch $\alpha \rightarrow \beta$ eine Basis-Hornformel.

(b) Basis-Hornformeln sind Hornformeln. Sind α, β Hornformeln, so auch $\alpha \wedge \beta$, sowie $\forall x\alpha$ und $\exists x\alpha$. Hornformeln ohne freie Variablen heißen *Hornaussagen*.

So ist z.B. $\forall x(y \in x \rightarrow x \notin y)$ eine Hornformel. Nach Definition ist $\alpha_1 \rightarrow \dots \rightarrow \alpha_n \rightarrow \beta$ mit $n \geq 0$ die allgemeine Form einer Basis-Hornformel von \mathcal{L} , wobei die α_i Primformeln bezeichnen und β ein Literal ist. Im aussagenlogischen Fall sind die α_i einfach nur Aussagenvariablen und β ist ein aussagenlogisches Literal.

Man pflegt eine Formel α auch dann eine Hornformel bzw. Basis-Hornformel zu nennen, wenn sie zu einer solchen im eben definierten Sinne nur äquivalent ist. Weil

$$\alpha_1 \rightarrow \dots \rightarrow \alpha_n \rightarrow \beta \equiv \alpha_1 \wedge \dots \wedge \alpha_n \rightarrow \beta \equiv \beta \vee \neg\alpha_1 \vee \dots \vee \neg\alpha_n,$$

sind Basis-Hornformeln bis auf Äquivalenz daher vom Typ

$$\text{I: } \alpha_0 \vee \neg\alpha_1 \vee \dots \vee \neg\alpha_n \quad \text{oder} \quad \text{II: } \neg\alpha_0 \vee \neg\alpha_1 \vee \dots \vee \neg\alpha_n$$

mit Primformeln $\alpha_0, \dots, \alpha_n$. Dabei sei $\beta = \alpha_0$ oder $\beta = \neg\alpha_0$. Dies sind Disjunktionen aus Literalen, von denen höchstens eines eine Primformel ist. So werden diese Formeln oft definiert. Die anfängliche Definition hat jedoch Vorteile in Induktionsbeweisen. Basis-Hornformeln des Typs I heißen *positiv* und des Typs II *negativ*. Ist der Kern einer Hornformel φ in pränexer Gestalt eine Konjunktion aus positiven Basis-Hornformeln, heiße φ eine *positive* Hornformel. Eine *aussagenlogische* Hornformel, d.h. eine Konjunktion aussagenlogischer Basis-Hornformeln, lässt sich stets als eine KNF auffassen, deren Disjunktionen höchstens ein nichtnegiertes Glied enthalten. Offenbar darf man sich eine quantorenfreie Hornformel von \mathcal{L} immer so entstanden denken, dass man in einer geeigneten aussagenlogischen Hornformel die Aussagenvariablen einfach durch Primformeln von \mathcal{L} ersetzt. Enthält das Präfix einer pränexen Hornformel φ nur \forall -Quantoren, heißt φ eine *universale Hornformel*.

Beispiel 3. (a) Identitäten und Quasiidentitäten sind universale Hornaussagen, wie auch die Transitivität $(x \leq y \wedge y \leq z \rightarrow x \leq z)^\forall$, Reflexivität $(x \leq x)^\forall$ und die Irreflexivität $(x \not\leq x)^\forall$, nicht aber die Konnexität $(x \leq y \vee y \leq x)^\forall$, wohl aber z.B. auch die folgenden Kongruenzforderungen für $=$ (mit $\vec{x} = \vec{y} := \bigwedge_{i=1}^n x_i = y_i$):

$$(4) \quad (x = x)^\forall, (x = y \wedge x = z \rightarrow y = z)^\forall, (\vec{x} = \vec{y} \rightarrow r\vec{x} \rightarrow r\vec{y})^\forall, (\vec{x} = \vec{y} \rightarrow f\vec{x} = f\vec{y})^\forall.$$

(b) $\forall x \exists y x \circ y = e$ ist eine Hornaussage, jedoch keine universale. Daher ist z.B. die Theorie der dividierbaren abelschen Gruppen in $\mathcal{L}\{\circ, e\}$ eine *Horntheorie*, worunter man allgemein eine Theorie versteht, die ein Axiomensystem aus Hornaussagen

besitzt. $\alpha := \forall x \exists y (x \neq 0 \rightarrow x \cdot y = 1)$ hingegen ist keine Hornaussage, weshalb die Körpertheorie T_K anscheinend keine Horntheorie ist. Das ist in der Tat so, d.h. α ist in T_K zu keiner Hornaussage äquivalent. Sonst wäre $\text{Md } T_K$ nach Übung 1 unter direkten Produkten abgeschlossen. Dies ist nicht der Fall: Der Ring $\mathbb{Q} \times \mathbb{Q}$ hat Nullteiler – z.B. ist $(1, 0) \cdot (0, 1) = 0$ – und ist folglich kein Körper.

Satz 1.3. *Ist U eine konsistente Menge universaler Hornformeln, so ist $\mathcal{F} = \mathcal{F}U$ Modell für U . Im Falle $U \subseteq \mathcal{L}^k$ ist auch $\mathcal{F}_k = \mathcal{F}_k U$ Modell für U .*

Beweis. Es genügt $(*) U \vdash \alpha \Rightarrow \mathcal{F} \models \alpha$ für universale Hornformeln α induktiv über den Aufbau von α zu beweisen. Für Primformeln ist dies klar, denn nach (3) ist sogar $(*) U \vdash \pi \Leftrightarrow \mathcal{F} \models \pi$. Mit $U \vdash \neg \pi$ gilt $U \not\vdash \pi$, denn U ist konsistent; nach $(*)$ also $\mathcal{F} \not\models \pi$ und somit $\mathcal{F} \models \neg \pi$. Das beweist $(*)$ für alle Literale. Es sei nun $U \vdash \pi \rightarrow \alpha$, π Primformel, α Basis-Hornformel und $\mathcal{F} \models \pi$. $(*)$ ergibt $U \vdash \pi$. Weil $U \vdash \pi \rightarrow \alpha$, folgt $U \vdash \alpha$. Die Induktionsannahme liefert $\mathcal{F} \models \alpha$, womit $\mathcal{F} \models \pi \rightarrow \alpha$ gezeigt ist. Induktion über \wedge ist klar. Damit ist $(*)$ für alle quantorenfreien Hornformeln bewiesen. Jede andere universale Hornformel ist bis auf logische Äquivalenz von der Gestalt $\forall \vec{x} \varphi$ mit einer quantorenfreien Hornformel φ wie man leicht sieht. Sei $U \vdash \forall \vec{x} \varphi$ und $\vec{t} \in \mathcal{T}^n$, also auch $U \vdash \varphi_{\vec{x}}^{\vec{t}}$. Daher $\mathcal{F} \models \varphi_{\vec{x}}^{\vec{t}}$ nach Induktionsannahme. \vec{t} war beliebig, somit $\mathcal{F} \models \forall \vec{x} \varphi$ nach (2). Das beweist $(*)$. Für den Fall $U \subseteq \mathcal{L}^k$ verläuft der Beweis unter Beachtung von (2_k) , (3_k) und mit \mathcal{F}_k für \mathcal{F} analog. \square

Sei U in Satz 1.3 das Axiomensystem einer *universalen* Horntheorie T , d.h. U besteht aus universalen Hornaussagen. Weil dann $U \subseteq \mathcal{L}^k$ für alle $k \leq \infty$, gilt nach dem Satz $\mathcal{F}_k U \models T$. Sei T überdies *nichttrivial*, was $\not\vdash_T x = y$ für $x \neq y$ heißen soll¹⁾. Die Erzeugenden \vec{v}_i ($i < k$) von $\mathcal{F}_k U$ sind dann paarweise verschieden. $\mathcal{F}_k U$ heißt auch *das freie T -Modell mit k vielen freien Erzeugenden*, siehe hierzu Beispiel 5.

Man beachte, $\mathcal{F}_0 U$ ($k=0$ in Satz 1.3) ist nur definiert, wenn die Sprache Konstantensymbole c enthält; $\mathcal{F}_0 U$ wird dann von den \bar{c} erzeugt. Kommt $=$ in U nicht vor, so ist T stets nichttrivial. $\mathcal{F}_0 U$ ist dann ein Herbrand-Modell für T , welches das *freie* oder *minimale Herbrand-Modell* von T genannt und fortan mit \mathcal{C}_U oder \mathcal{C}_T bezeichnet wird. Der Träger von \mathcal{C}_U ist stets die Menge der Grundterme. Nach Definition gilt für jedes in der Sprache von T vorkommende Relationssymbol r

$$(5) \quad \mathcal{C}_U \models r\vec{t} \Leftrightarrow U \vdash r\vec{t} \quad (\vec{t} \text{ variablenfrei}).$$

Beispiel 4. $U \subseteq \mathcal{L}\{0, \mathbf{S}, <\}$ bestehe aus den beiden universalen Hornaussagen

$$\forall x x < \mathbf{S}x \quad ; \quad \forall xyz (x < y \wedge y < z \rightarrow x < z)$$

und ist gleichheitsfrei. Wir wollen das Herbrand-Modell \mathcal{C}_U exakt bestimmen, dessen Träger jetzt aus den Termen \underline{n} ($= \mathbf{S}^n 0$) besteht, und zeigen $\mathcal{C}_U \simeq \mathcal{N}_< := (\mathbb{N}, 0, \mathbf{S}, <)$.

¹⁾ Im Falle $\vdash_T x = y$ hat T nur das „triviale“ einelementige Modell.

Wegen $\mathcal{N}_< \models U$ gilt gewiss $U \vdash \underline{m} < \underline{n} \Rightarrow m < n$. Induktion über n , beginnend mit $n = Sm$, zeigt unschwer auch die Umkehrung. Also $U \vdash \underline{m} < \underline{n} \Leftrightarrow m < n$. Mit (5) ergibt dies $\mathcal{C}_U \models \underline{m} < \underline{n} \Leftrightarrow m < n$. Kurzum, $n \mapsto \underline{n}$ ist ein Isomorphismus von $\mathcal{N}_<$ auf \mathcal{C}_U (obwohl z.B. $U \not\models \forall x x \leq x$). Ein ähnliches Beispiel präsentiert Übung 2.

Beispiel 5. Für die universale Horntheorie T der Halbgruppen erwies sich die dem Termmodell $\mathcal{F}T$ unterliegende Struktur in Beispiel 1 als isomorph zur Worthalbgruppe über dem Alphabet Var . Diese repräsentiert also die (bis auf Isomorphie eindeutig bestimmte) freie Halbgruppe mit abzählbar vielen Erzeugenden. Analoges gilt bzgl. $\mathcal{F}_k T$ ($k > 0$) und der Worthalbgruppe über einem k -elementigen Alphabet.

Bemerkung 2. Das Wort „frei“ rührt daher, dass man zur Erzeugung eines Homomorphismus auf ein anderes T -Modell über die Werte der freien Erzeugenden grob gesprochen „frei verfügen“ kann. Freie Modelle in diesem Sinne gibt es nur für (konsistente) universale Horn-Theorien, wobei nebenbei bemerkt die Konsistenz von U in Satz 1.4 nach Übung 3 a priori gewährleistet ist, wenn U nur positive Hornformeln enthält.

Wir beschließen die etwas breiter angelegte als später ausgeschöpfte Theorie dieses Abschnitts mit einer besonders anwendungsfähigen Variante von Satz 1.2.

Satz 1.4. Sei $U \subseteq \mathcal{L}^k$ eine konsistente Menge von universalen Hornformeln und γ eine Konjunktion von Primformeln mit $\exists \vec{x} \gamma \in \mathcal{L}^k$. Dann sind äquivalent

- (i) $\mathcal{F}_k U \models \exists \vec{x} \gamma$, (ii) $U \vdash \gamma_{\vec{x}}^{\vec{t}}$ für ein gewisses $\vec{t} \in \mathcal{T}_k^n$, (iii) $U \vdash \exists \vec{x} \gamma$.

Speziell ist für konsistente universale Horntheorien T einer gleichungsfreien Sprache mit Konstanten $\mathcal{C}_T \models \exists \vec{x} \gamma$ immer gleichwertig mit $\vdash_T \exists \vec{x} \gamma$.

Beweis. (i) \Rightarrow (ii): Mit $\mathcal{F}_k U \models \exists \vec{x} \gamma$ ist $\mathcal{F}_k U \models \gamma_{\vec{x}}^{\vec{t}}$ für ein \vec{t} . Sonst wäre $\mathcal{F}_k U \models \neg \gamma_{\vec{x}}^{\vec{t}}$ für alle \vec{t} , also $\mathcal{F}_k U \models \forall \vec{x} \neg \gamma$ nach (2_k) im Widerspruch zu (i). Für $\gamma = \pi_0 \wedge \dots \wedge \pi_m$ gilt dann $\mathcal{F}_k U \models \pi_i^{\vec{t}}$ für $i = 1, \dots, m$ und mithin $U \vdash \pi_i^{\vec{t}}$ nach (3_k). Daher $U \vdash \gamma_{\vec{x}}^{\vec{t}}$. (ii) \Rightarrow (iii): Trivial. (iii) \Rightarrow (i): Satz 1.3 sagt $\mathcal{F}_k U \models U$. Mit $U \vdash \exists \vec{x} \gamma$ gilt also auch $\mathcal{F}_k U \models \exists \vec{x} \gamma$. Den Spezialfall erhält man aus (i) \Leftrightarrow (iii) für den Fall $k = 0$. \square

Übungen

1. Man zeige, für eine Horntheorie T ist $\text{Md } T$ stets abgeschlossen unter direkten Produkten und, falls T eine universale Theorie ist, auch unter Substrukturen.

2. Man zeige $\mathcal{C}_U \simeq (\mathbb{N}, 0, \mathbf{S}, \leq)$ für die Menge universaler Hornaussagen

$$U = \{\forall x x \leq x, \forall x x \leq \mathbf{S}x, \forall x \forall y \forall z (x \leq y \wedge y \leq z \rightarrow x \leq z)\}.$$

Dies gilt, obwohl z.B. $\forall x \forall y (x \leq y \vee y \leq x)$ aus U nicht beweisbar ist.

3. Man beweise, eine Menge positiver Hornformeln ist immer konsistent.

4.2 Aussagenlogische Resolution

Wir erinnern an das Problem schneller Entscheidung über Erfüllbarkeit aussagenlogischer Formeln. Dieses Problem ist von eminenter praktischer Bedeutung, da sich die meisten nichtnumerischen, also „logischen“ Probleme hierauf zurückführen lassen. Die bei Formeln mit wenigen Variablen recht praktikable Wahrheitstafel-Methode wächst vom Rechenaufwand her exponentiell mit der Anzahl der Variablen und ist schon für eine Variablenzahl von 100 selbst unter Einsatz modernster Rechner auch in absehbarer Zukunft nicht durchführbar. Leider gibt es bis heute im Prinzip keine besseren Verfahren – es sei denn, man hat es mit Formeln in spezieller Gestalt zu tun, z.B. mit gewissen Normalformen. Der allgemeine Fall repräsentiert ein ungelöstes, hier aber nicht näher diskutiertes Problem der theoretischen Informatik, das $P=NP$ -Problem, siehe z.B. [GJ].

Für konjunktive Normalformen hat sich das nachfolgend vorgestellte *Resolutionsverfahren* bewährt. Rationeller Darstellung wegen geht man von einer Disjunktion $\lambda_1 \vee \dots \vee \lambda_n$ von Literalen λ_i über zur Menge $\{\lambda_1, \dots, \lambda_n\}$. Dadurch werden die für die Erfüllbarkeitsfrage unwesentliche Reihenfolge der Disjunktionsglieder und eventuell wiederholtes Auftreten derselben eliminiert. Eine endliche, möglicherweise leere Menge von Literalen heie eine (aussagenlogische) *Klausel*. K, H, G, L, P, N bezeichnen im Folgenden Klauseln, $\mathcal{K}, \mathcal{H}, \mathcal{P}, \mathcal{N}$ Klauselmengen. $K = \{\lambda_1, \dots, \lambda_n\}$ entspricht der Formel $\lambda_1 \vee \dots \vee \lambda_n$. Der mit \square bezeichneten *leeren Klausel* (es ist $n = 0$) entspricht die leere Disjunktion, die mit dem Falsum \perp identifiziert wird. Für $m > 0$ heit $K = \{q_1, \dots, q_m, \neg r_1, \dots, \neg r_k\}$ mit $q_i, r_j \in AV$ eine *positive*, für $m = 1$ auch eine *definite*, und für $m = 0$ eine *negative* Klausel. Diese Verabredungen werden übernommen, wenn die λ_i später Literale einer Sprache 1. Stufe bedeuten.

Wir schreiben $w \models K$ (eine Belegung w erfüllt die Klausel K), wenn K ein λ mit $w \models \lambda$ enthält. K heit *erfüllbar*, wenn es ein w gibt mit $w \models K$. Man beachte, die leere Klausel \square ist dem Wortlaut dieser Definition entsprechend nicht erfüllbar.

w heit *Modell* für eine Klauselmenge \mathcal{K} , wenn $w \models K$ für alle $K \in \mathcal{K}$. Hat \mathcal{K} ein Modell, heit \mathcal{K} auch *erfüllbar*. Im Unterschied zur leeren Klausel \square wird die leere Klauselmenge \emptyset von jeder Belegung erfüllt. w erfüllt eine KNF α genau dann, wenn w sämtliche Konjunktionsglieder, und damit sämtliche diesen Gliedern entsprechenden Klauseln erfüllt. Weil jede aussagenlogische Formel in eine KNF überführt werden kann, ist α erfüllbarkeitsgleich mit einer zugehörigen endlichen Klauselmenge. So ist z.B. die KNF $(p \vee q) \wedge (\neg p \vee q \vee r) \wedge (q \vee \neg r) \wedge (\neg q \vee s) \wedge \neg s$ erfüllbarkeitsgleich mit der zugehörigen Klauselmenge $\{\{p, q\}, \{\neg p, q, r\}, \{q, \neg r\}, \{\neg q, s\}, \{\neg s\}\}$.

Wir schreiben $\mathcal{K} \models H$, wenn jedes Modell von \mathcal{K} auch die Klausel H erfüllt. Eine Klauselmenge \mathcal{K} ist demnach dann und nur dann unerfüllbar, wenn $\mathcal{K} \models \square$.

Für $\lambda \notin K$ werden wir die Klausel $K \cup \{\lambda\}$ oft kurz durch K, λ bezeichnen. Ferner sei $\bar{\lambda} = \neg p$ für $\lambda = p$, $\bar{\lambda} = p$ für $\lambda = \neg p$ (so dass stets $\bar{\bar{\lambda}} = \lambda$) und $\bar{K} = \{\bar{\lambda} \mid \lambda \in K\}$.

Der *Resolutionalkül* arbeitet mit Klauselmengen und Klauseln, sowie einer einzigen auf Klauseln bezogenen Regel, der sogenannten *Resolutionsregel*

$$\text{RR: } \frac{K, \lambda \mid L, \bar{\lambda}}{K \cup L} \quad (\lambda, \bar{\lambda} \notin K \cup L).$$

Die Klausel $K \cup L$ heißt auch eine *Resolvente* der Klauseln K, λ und $L, \bar{\lambda}$. Die Einschränkung $(\lambda, \bar{\lambda} \notin K \cup L)$ ist nicht wirklich wichtig und könnte auch entfallen.

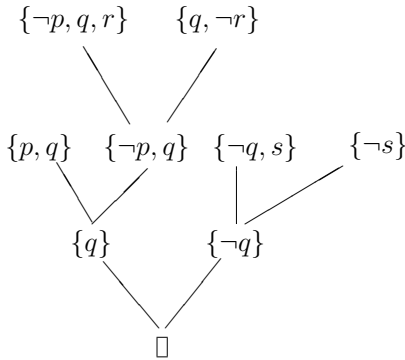
Eine Klausel H heißt *ableitbar* aus einer Klauselmenge \mathcal{K} , symbolisch $\mathcal{K} \vdash^{RR} H$, wenn H aus \mathcal{K} durch schrittweise Anwendung von RR gewonnen werden kann oder gleichwertig, wenn H zur *Resolutionshülle* $Rh\mathcal{K}$ von \mathcal{K} gehört, der kleinsten Klauselmenge $\mathcal{H} \supseteq \mathcal{K}$, die gegenüber Anwendung von RR abgeschlossen ist. Diese Erklärung entspricht völlig der einer MP-abgeschlossenen Formelmenge in 1.6.

Beispiel. Sei $\mathcal{K} = \{\{p, \neg q\}, \{q, \neg p\}\}$. Anwendung von RR liefert die beiden Resolventen $\{p, \neg p\}$ und $\{q, \neg q\}$, woran man erkennt, dass ein Klauselpaar i.a. mehrere Resolventen hat. Jede weitere Anwendung von RR ergibt bereits vorhandene Klauseln, so dass $Rh\mathcal{K}$ nur die Klauseln $\{p, \neg q\}, \{q, \neg p\}, \{p, \neg p\}, \{q, \neg q\}$ enthält.

Die Anwendung von RR auf $\{p\}, \{\neg p\}$ ergibt die leere Klausel \square . Daher $\mathcal{K} \vdash^{RR} \square$ für die unerfüllbare Klauselmenge $\mathcal{K} = \{\{p\}, \{\neg p\}\}$. Tatsächlich ist die Ableitbarkeit der leeren Klausel nach dem Resolutionssatz unten charakteristisch für die Unerfüllbarkeit einer beliebigen Klauselmenge \mathcal{K} . Es muss nur geprüft werden, ob $\mathcal{K} \vdash^{RR} \square$ (also $\square \in Rh\mathcal{K}$) oder nicht. Dies ist für endliche \mathcal{K} effektiv entscheidbar, weil $Rh\mathcal{K}$ endlich ist. In der Tat, eine bei Anwendung von RR auf Klauseln in p_1, \dots, p_n entstehende Resolvente enthält höchstens wieder diese Variablen. Ferner gibt es nur endlich viele Klauseln in den Variablen p_1, \dots, p_n , nämlich genau 2^{2n} Stück. Das sind in Abhängigkeit von n aber immer noch exponentiell viele Klauseln. Abgesehen davon hat man bei der maschinellen Implementation des Resolutionalküls meist mit potentiell unendlichen Mengen von Klauseln zu tun. Auf die damit verbundenen Probleme gehen wir am Ende von 4.4 kurz ein.

Die Ableitung einer Klausel H aus einer Klauselmenge \mathcal{K} , speziell eine solche der leeren Klausel, stellt man am besten durch einen sogenannten *Resolutionsbaum* graphisch dar. Es ist dies ein „von oben“ gerichteter Baum mit dem Endpunkt H ohne Ausgang, der auch die *Wurzel* des Baumes genannt wird. Punkte ohne Eingangsanten heißen *Blätter*. Ein Punkt, der kein Blatt ist, hat 2 Eingänge, und die Punkte, von denen sie herrühren, heißen dessen *Vorgänger*. Die Punkte des Baumes tragen Klauselmengen in der Weise, dass ein Punkt, der kein Blatt ist, gerade eine Resolvente der beiden darüberstehenden Klauseln ist, siehe die nachfolgende Figur. Diese zeigt eine von mehreren Resolutionsbäumen für die bereits erwähnte Klauselmenge

$$\mathcal{K}_0 = \{\{p, q\}, \{\neg p, q, r\}, \{q, \neg r\}, \{\neg q, s\}, \{\neg s\}\}.$$



Die Blätter dieses Baumes sind alle von Klauseln aus \mathcal{K}_0 besetzt. Es ist klar, dass eine Klausel H im allgemeinen Falle genau dann zur Resolutionshülle einer Klauselmengens \mathcal{K} gehört, wenn es einen Resolutionsbaum gibt mit Blättern aus \mathcal{K} und der Wurzel H . Ein Resolutionsbaum mit Blättern aus \mathcal{K} und der Wurzel \square wie in der Figur links für $\mathcal{K} = \mathcal{K}_0$ heißt eine *Resolution für \mathcal{K}* , genauer, eine *erfolgreiche Resolution für \mathcal{K}* . Nach dem bereits Gesagten ist \mathcal{K}_0 damit unerfüllbar, wie dann auch

die der Klauselmengens \mathcal{K}_0 entsprechende konjunktive Normalform

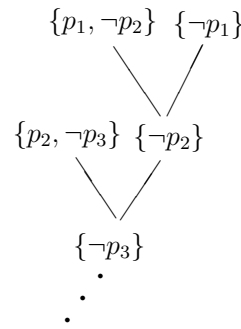
$$(p \vee q) \wedge (\neg p \vee q \vee r) \wedge (q \vee \neg r) \wedge (\neg q \vee s) \wedge \neg s.$$

Bemerkung 1. Endet ein Resolutionsbaum mit einem Punkt $\neq \square$, auf den keine weitere Anwendung von RR mehr möglich ist oder reproduzieren sich dabei die Punkte, spricht man von einer *erfolglosen* Resolution. Bei den meisten Interpreten des Resolutionskalküls wird dann ein „backtracking“ unternommen, d.h. das Programm sucht im Baum rückwärts laufend den ersten Punkt, bei dem eine von mehreren Resolutionsalternativen ausgewählt wurden und verfolgt eine andere Alternative. Eine Auswahlstrategie muss in jedem Falle implementiert sein, denn wie jeder Logikkalkül, ist auch der Resolutionskalkül nichtdeterminiert, d.h. es gibt keine natürlichen Präferenzen über die Reihenfolge der Ableitungen, die zu einer erfolgreichen Resolution führen.

Es sei vermerkt, dass es für unendliche unerfüllbare Klauselmengens \mathcal{K} trotz Ableitbarkeit der leeren Klausel auch unendliche Resolutionsbäume mit sich nicht wiederholenden Punkten geben kann, ohne dass \square je erscheint. Solche Bäume haben keine Wurzel. So ist z.B. die Klauselmengens

$$\mathcal{K} = \{\{p_1\}, \{\neg p_1\}, \{p_1, \neg p_2\}, \{p_2, \neg p_3\}, \dots\}$$

nicht erfüllbar. Wir erhalten hier den mit Blättern aus \mathcal{K} besetzten unendlichen Resolutionsbaum der Figur rechts, der keine Wurzel hat und unberücksichtigt lässt, dass \square bereits durch einmalige Anwendung von RR auf die beiden ersten Klauseln aus \mathcal{K} herleitbar ist. Diese Beispiele deuten darauf hin, dass durch den Resolutionskalkül i.a. keine Entscheidung über die Erfüllbarkeit unendlicher Klauselmengens herbeigeführt werden kann. Das ist in der Tat so wie in 4.4 gezeigt wird. Es gibt aber – falls \mathcal{K} tatsächlich unerfüllbar ist – gemäß Satz 2.2 auch eine erfolgreiche Resolution für \mathcal{K} , die in endlicher Zeit prinzipiell auch gefunden werden kann.



Wir beginnen das genauere Studium des Resolutionskalküls mit

Lemma 2.1 (Korrektheitslemma). $\mathcal{K} \vdash^{RR} H \Rightarrow \mathcal{K} \models H$.

Beweis. Wie im Falle eines Hilbert-Kalküls genügt es, die Korrektheit der Regel RR zu bestätigen, also zu beweisen, dass ein Modell für K, λ und $L, \bar{\lambda}$ auch Modell für $K \cup L$ ist. Sei also $w \models K, \lambda$ und $w \models L, \bar{\lambda}$. **Fall 1:** $w \not\models \lambda$. Dann gibt es ein Literal $\lambda' \in K$ mit $w \models \lambda'$. Also $w \models K$ und somit auch $w \models K \cup L$. **Fall 2:** $w \models \lambda$. Dann ist $w \not\models \bar{\lambda}$. Also folgt analog wie oben $w \models L$ und damit ebenfalls $w \models K \cup L$. \square

Für den Fall $\mathcal{K} \vdash^{RR} \square$ ergibt das Lemma $\mathcal{K} \models \square$, also die Unerfüllbarkeit von \mathcal{K} . Die Umkehrung von Lemma 2.1 gilt i.a. nicht – z.B. ist $\{\{p\}\} \models \{p, q\}$, nicht aber $\{\{p\}\} \vdash^{RR} \{p, q\}$. Sie gilt aber für $H = \square$. Dies folgt unmittelbar aus Satz 2.2, der oft auch in der Weise ‘ \mathcal{K} ist unerfüllbar genau dann, wenn $\mathcal{K} \vdash^{RR} \square$ ’ formuliert wird.

Satz 2.2 (Resolutionssatz). \mathcal{K} ist erfüllbar genau dann, wenn $\mathcal{K} \not\vdash^{RR} \square$.

Beweis. Für erfüllbares \mathcal{K} ist $\mathcal{K} \not\vdash^{RR} \square$, also $\mathcal{K} \not\vdash^{RR} \square$ nach Lemma 2.1. Sei nun $\mathcal{K} \not\vdash^{RR} \square$, oder gleichwertig $\square \notin \mathcal{H}$ mit $\mathcal{H} := Rh(\mathcal{K})$. Wir konstruieren schrittweise ein Modell $w = (v_1, v_2, \dots)$ für \mathcal{H} und damit auch für \mathcal{K} , d.h. wir definieren die Werte $v_n = wp_n$ induktiv. Es sei $\Lambda^{(0)} = \mathcal{H}^{(0)} = \emptyset$ und für $n \geq 1$ sei $\Lambda^{(n)}$ die Menge aller Literale in p_1, \dots, p_n (man beachte, die Variablennumerierung beginnt mit p_1), sowie $\mathcal{H}^{(n)}$ die Menge aller $K \in \mathcal{H}$ mit $K \subseteq \Lambda^{(n)}$ so dass p_n oder $\neg p_n$ oder beide zu K gehören. Gewiss ist $\text{var } \mathcal{H}^{(n)} \subseteq \{p_1, \dots, p_n\}$ und $\mathcal{H} = \bigcup_{n \in \mathbb{N}} \mathcal{H}^{(n)}$. Sei v_1, \dots, v_n schon definiert, so dass $w_n := (v_1, \dots, v_n) \models \mathcal{H}^{(i)}$ für alle $i \leq n$. Dies gilt trivial für $n = 0$, denn die „leere Belegung“ erfüllt $\mathcal{H}^{(0)} = \emptyset$. Wir werden $v_{n+1} = wp_{n+1}$ so definieren, dass

(*) $w_{n+1} := (v_1, \dots, v_{n+1}) \models \mathcal{H}^{(n+1)}$ (Induktionsbehauptung).

Wir müssen uns dabei nur um diejenigen $K \in \mathcal{H}^{(n+1)}$ kümmern, die *entweder* p_{n+1} oder $\neg p_{n+1}$ enthalten, und kein $\lambda \in \Lambda^{(n)}$ mit $w_n \models \lambda$, in diesem Beweis *sensitive* Klauseln genannt. Alle übrigen Klauseln aus $\mathcal{H}^{(n+1)}$ werden durch *jede* Expansion von w_n zu w_{n+1} erfüllt²⁾. **Behauptung:** entweder ist $p_{n+1} \in K$ für *alle* sensitiven K – dann sei $v_{n+1} = 1$ – oder aber $\neg p_{n+1} \in K$ für alle sensitiven K , in welchem Falle $v_{n+1} = 0$ gesetzt wird, so dass (*) in jedem Falle gilt. Wir zeigen die Behauptung. Angenommen es gibt sensitive K, H mit $p_{n+1} \in K$ und $\neg p_{n+1} \in H$ (also $\neg p_{n+1} \notin K$, $p_{n+1} \notin H$). Anwendung von RR auf H, K ergibt dann entweder \square (was $\square \notin \mathcal{H}$ widerspricht), oder aber eine Klausel aus $\mathcal{H}^{(i)}$ für ein $i \leq n$ deren Literale nicht von w_n erfüllt werden, ein Widerspruch zu $w_n \models \mathcal{H}^{(i)}$. Das bestätigt die Behauptung. Daher $w_n \models \mathcal{H}^{(n)}$ für alle n , so dass $w = (v_1, v_2, \dots)$ ein Modell ist für ganz \mathcal{H} . \square

²⁾ Der Anfänger sollte alle acht Kandidaten für $\mathcal{H}^{(1)} \subseteq \{\{p_1\}, \{\neg p_1\}, \{p_1, \neg p_1\}\}$ aufschreiben.

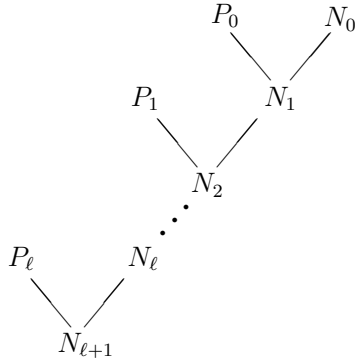
Bemerkung 2. Der obige Beweis ist konstruktiv, d.h. ist \mathcal{K} effektiv gegeben und ist $\mathcal{K} \not\models^{RR} \square$, kann eine erfüllende Belegung für \mathcal{K} auch effektiv angegeben werden. Außerdem wurde für abzählbare Formelmengen X nebenbei der in traditionellen Beweisen meistens vorausgesetzte aussagenlogische Kompaktheitssatz noch einmal mitbewiesen. In der Tat, jede Formel ist zu einer KNF äquivalent, und damit ist X zu einer Klauselmenge \mathcal{K}_X erfüllbarkeitsgleich. Ist also X nicht erfüllbar, gilt dasselbe für \mathcal{K}_X . Folglich $\mathcal{K}_X \vdash^{RR} \square$ nach Satz 2.2, und daher $\mathcal{K}_0 \vdash^{RR} \square$ für eine endliche Teilmenge $\mathcal{K}_0 \subseteq \mathcal{K}_X$. Damit ist klar, dass schon eine endliche (nämlich die der Klauselmenge \mathcal{K}_0 entsprechende) Teilmenge von X nicht erfüllbar ist.

Eine zu einer aussagenlogischen Basis-Hornformel gehörende Klausel heiße eine (ausagenlogische) *Hornklausel*. Diese ist offenbar genau dann positiv oder negativ, wenn dies für die entsprechende Hornformel zutrifft. Positive Hornklauseln haben die Gestalt $\{\neg q_1, \dots, \neg q_n, p\}$ mit $n \geq 0$, negative die Gestalt $\{\neg q_1, \dots, \neg q_k\}$. Zu den negativen Hornklauseln rechnet auch die leere Klausel ($k = 0$). Den Zusatz *aussagenlogisch* lassen wir weg, solange wir uns in der Aussagenlogik bewegen.

Für die Praxis ist wichtig, dass der Resolutionskalkül für Hornklauseln noch spezieller formuliert werden kann. Die leere Klausel lässt sich aus einer Hornklauselmenge, wenn überhaupt, bereits mit einer eingeschränkten Resolutionsregel gewinnen; ihre Anwendung wird auf Paare von Hornklauseln beschränkt, von denen eine positiv und die andere negativ ist. Dies ist die *Regel der Hornresolution*

$$\text{HR : } \frac{K, p \mid L, \neg p}{K \cup L} \quad (K, L \text{ negativ, } p, \neg p \notin K \cup L).$$

Eine positive Hornklausel ist definit. Deshalb ist die Resolvente einer Anwendung von HR eindeutig bestimmt und immer negativ. Daher hat ein *H-Resolutionsbaum* die einfache, durch die Figur links veranschaulichte Gestalt. Dabei be-



zeichnen P_0, \dots, P_ℓ positive und $N_0, \dots, N_{\ell+1}$ negative Hornklauseln. Ein solcher Baum heißt eine *H-Resolution für \mathcal{P}, N* (wobei \mathcal{P} hier und überall eine Menge positiver Hornklauseln und N eine negative Klausel $\neq \square$ bedeuten soll), wenn (1) $P_i \in \mathcal{P}$ für alle $i \leq \ell$ und (2) $N_0 = N$ & $N_{\ell+1} = \square$ erfüllt sind. Man kann eine *H-Resolution für \mathcal{P}, N* offenbar auch ansehen als eine Folge $(P_i, N_i)_{i \leq \ell}$ mit den Eigenschaften (0) $N_{i+1} = \text{HR}(P_i, N_i)$ für alle $i \leq \ell$, (1) und (2). Dabei bezeichnet $\text{HR}(P, N)$ die eindeutig bestimmte Resolvente, die durch Anwendung von HR auf die positive Klausel P und die negative Klausel N entsteht.

Der mit Hornklauseln und HR operierende Kalkül sei mit \vdash^{HR} bezeichnet. Bevor wir dessen Vollständigkeit beweisen, sind aber noch einige Vorbereitungen nötig.

Eine Menge \mathcal{P} positiver Hornklauseln hat immer das triviale Modell w_1 mit $w_1 p = 1$ für alle Variablen p . Um einen Überblick über alle Modelle von \mathcal{P} zu gewinnen, beachte man die natürlichen Korrespondenz $w \longleftrightarrow V_w := \{p \in AV \mid w \models p\}$ zwischen Belegungen w und Teilmengen von AV . Wir setzen $w \leq w'$, wenn $V_w \subseteq V_{w'}$. Offenbar ist $w \models \{\neg q_1, \dots, \neg q_n, p\}$ genau dann, wenn $w \models q_1, \dots, q_n \Rightarrow w \models p$. Daher gilt $w \models \mathcal{P}$ genau dann, wenn $V = V_w$ die beiden folgenden Bedingungen erfüllt:

- (a) $p \in V$ für $\{p\} \in \mathcal{P}$, (b) $q_1, \dots, q_n \in V \Rightarrow p \in V$, für $\{\neg q_1, \dots, \neg q_n, p\} \in \mathcal{P}$.

Unter allen (a) und (b) genügenden Teilmengen $V \subseteq AV$ gibt es offenbar eine kleinste, welche mit $V_{\mathcal{P}}$ bezeichnet sei. Das $V_{\mathcal{P}}$ entsprechende Modell von \mathcal{P} sei mit $w_{\mathcal{P}}$ bezeichnet und heiße das *Minimalmodell* von \mathcal{P} . Weil $w_{\mathcal{P}} \leq w$ für alle $w \models \mathcal{P}$, lässt sich $V_{\mathcal{P}}$ auch wie folgt definieren: Sei $V_0 = \{p \in AV \mid \{p\} \in \mathcal{P}\}$ und

$$V_{k+1} = V_k \cup \{p \in AV \mid \{\neg q_1, \dots, \neg q_n, p\} \in \mathcal{P} \text{ für gewisse } q_1, \dots, q_n \in V_k\}.$$

Dann ist $V_{\mathcal{P}} = \bigcup_{k \in \mathbb{N}} V_k$, weil notwendig $V_k \subseteq V_w$ für alle k und $w \models \mathcal{P}$ wie man leicht einsieht, also $\bigcup_{k \in \mathbb{N}} V_k \subseteq V_{\mathcal{P}}$. Das minimale m mit $p \in V_m$ heiße der *Erzeugungsrang* von p bzgl. \mathcal{P} , Bezeichnung $e_{\mathcal{P}} p$. Diejenigen p mit $\{p\} \in \mathcal{P}$ haben den Erzeugungsrang 0. Die aus diesen durch Anwendung von (b) hinzukommenden Variablen haben den Erzeugungsrang 1 wenn sie nicht schon zu V_0 gehören, usw.

Lemma 2.3. *Sei \mathcal{P} eine Menge positiver Hornklauseln und $q_0, \dots, q_k \in V_{\mathcal{P}}$. Dann gilt $(*) \mathcal{P}, N \vdash^{HR} \square$, mit $N = \{\neg q_0, \dots, \neg q_k\}$.*

Beweis. Für Variablen $r_0, \dots, r_n \in V_{\mathcal{P}}$ sei $e_{\mathcal{P}}(r_0, \dots, r_n) := \max\{e_{\mathcal{P}} r_0, \dots, e_{\mathcal{P}} r_n\}$. Sei $\mu(r_0, \dots, r_n)$ die Anzahl der $i \leq n$ mit $e_{\mathcal{P}} r_i = e_{\mathcal{P}}(r_0, \dots, r_n)$. Die Behauptung wird induktiv über $e := e_{\mathcal{P}}(q_0, \dots, q_k)$ und $\mu := \mu(q_0, \dots, q_k)$ bewiesen. Sei zuerst $e = 0$, d.h. $\{q_0\}, \dots, \{q_k\} \in \mathcal{P}$. Dann gibt es gewiss eine H -Resolution für \mathcal{P}, N , nämlich $(\{q_i\}, \{\neg q_i, \dots, \neg q_k\})_{i \leq k}$. Sei nun $e > 0$ und o.B.d.A. $e = e_{\mathcal{P}} q_0$. Dann existieren $q_{k+1}, \dots, q_m \in V_{\mathcal{P}}$ mit $P := \{\neg q_{k+1}, \dots, \neg q_m, q_0\} \in \mathcal{P}$ sowie $e_{\mathcal{P}}(q_{k+1}, \dots, q_m) < e$. Also ist $e_{\mathcal{P}}(q_1, \dots, q_m) < e$, oder es ist $e_{\mathcal{P}}(q_1, \dots, q_m) = e$ und $\mu(q_1, \dots, q_m) < \mu$. Nach Induktionsannahme ist jedenfalls $\mathcal{P}, N_1 \vdash^{HR} \square$ für $N_1 := \{\neg q_1, \dots, \neg q_m\}$. Es gibt also eine H -Resolution $(P_i, N_i)_{1 \leq i \leq \ell}$ für \mathcal{P}, N_1 . Dann aber ist $(P_i, N_i)_{i \leq \ell}$ mit $P_0 := P$ und $N_0 := N$ eine H -Resolution für \mathcal{P}, N , und alles ist bewiesen. \square

Satz 2.4 (über Horn-Resolution). *Eine Menge \mathcal{K} von Hornklauseln ist erfüllbar genau dann, wenn $\mathcal{K} \not\vdash^{HR} \square$.*

Beweis. Die Bedingung $\mathcal{K} \not\vdash^{HR} \square$ ist sicher notwendig. Sei andererseits \mathcal{K} unerfüllbar, $\mathcal{K} = \mathcal{P} \cup \mathcal{N}$, alle $P \in \mathcal{P}$ seien positiv und alle $N \in \mathcal{N}$ negativ. Weil $w_{\mathcal{P}} \models \mathcal{P}$, gibt es ein $N = \{\neg q_0, \dots, \neg q_k\} \in \mathcal{N}$ mit $w_{\mathcal{P}} \not\models N$. Folglich ist $w_{\mathcal{P}} \models q_0, \dots, q_k$, also $q_0, \dots, q_k \in V_{\mathcal{P}}$. Nach Lemma 2.3 ist dann $\mathcal{P}, N \vdash^{HR} \square$ und damit auch $\mathcal{K} \vdash^{HR} \square$. \square

Korollar 2.5. Sei $\mathcal{K} = \mathcal{P} \cup \mathcal{N}$ eine Menge aus Hornklauseln, alle $P \in \mathcal{P}$ positiv und alle $N \in \mathcal{N}$ negativ. Dann sind äquivalent

- (i) \mathcal{K} ist unerfüllbar, (ii) \mathcal{P}, N ist unerfüllbar für ein gewisses $N \in \mathcal{N}$.

Beweis. (i) impliziert $\mathcal{K} \vdash^{HR} \Box$ nach Satz 2.4. Folglich gibt es ein $N \in \mathcal{N}$ und eine H -Resolution für \mathcal{P}, N , womit auch \mathcal{P}, N unerfüllbar ist. (ii) \Rightarrow (i) ist trivial. \square

Dieses Korollar lässt sich auch direkt mit Hilfe des Minimalmodells leicht beweisen. Man kann also die Untersuchung von Hornklauselmengen hinsichtlich Erfüllbarkeit gänzlich auf den Fall mit nur einer einzigen negativen Klausel beschränken.

Die bisher geschilderten Techniken übertragen sich ohne weiteres auf quantorenfreie Formeln einer Sprache \mathcal{L} der 1. Stufe, indem man sich die Aussagenvariablen durch Primformeln von \mathcal{L} ersetzt denkt. Klauseln sind dann endliche Mengen von Literalen aus \mathcal{L} . Nach der Bemerkung in 4.1 ist eine Formelmenge aus \mathcal{L} immer auch erfüllbarkeitsgleich mit einer Menge quantorenfreier Formeln, die o.B.d.A. in konjunktiver Normalform gegeben seien. Zerlegung in die Konjunktionsglieder liefert eine erfüllbarkeitsgleiche Menge von Disjunktionen aus Literalen. Verwandelt man diese Disjunktionen in Klauseln, so erhält man eine Klauselmenge, für die sich eine Konsistenzbedingung nach der soeben zitierten Bemerkung auch aussagenlogisch formulieren lässt. Weil nun prädikatenlogische Beweise wegen der Äquivalenz von $X \vdash \alpha$ mit der Inkonsistenz von $X, \neg\alpha$ stets auf den Nachweis gewisser Inkonsistenzen reduzierbar sind, lassen sich derartige Beweise prinzipiell auch durch Resolution erbringen. Bevor wir näher hierauf eingehen, befassen wir uns erst mit einem weiteren Hilfsmittel des maschinellen Beweisens, der Unifikation.

Übungen

1. Man beweise, die erfüllbare Klauselmenge $\mathcal{P} = \{\{p_3\}, \{\neg p_3, p_1, p_2\}\}$ hat kein kleinstes Modell (die zweite Klausel ist keine Hornklausel).
2. Seien $p_{m,n,k}$ für $m, n, k \in \mathbb{N}$ Aussagenvariablen, S die Nachfolgerfunktion und \mathcal{P} die Menge aller Klauseln, die zu den folgenden Hornformeln gehören:

$$p_{m,0,m} \quad ; \quad p_{m,n,k} \rightarrow p_{m,Sn,Sk} \quad (m, n, k \in \mathbb{N}).$$

Diese Formeln werden in 4.4 als Grundinstanzen eines Logikprogramms zur Berechnung der Summe zweier natürlicher Zahlen gedeutet. Man beweise, das Minimalmodell $w_{\mathcal{P}}$ von \mathcal{P} ist gegeben durch $w_{\mathcal{P}} \models p_{m,n,k} \Leftrightarrow k = m + n$.

3. Sei \mathcal{P} die Hornklauselmenge der Übung 2. Man beweise

$$(a) \mathcal{P}, \neg p_{n,m,n+m} \vdash^{HR} \Box, \quad (b) \mathcal{P}, \neg p_{n,m,k} \vdash^{HR} \Box \Rightarrow k = n + m.$$

4.3 Unifikation

Ein entscheidendes Hilfsmittel der logischen Programmierung ist die Unifizierung. Dieser Begriff ist für beliebige Term- oder Formelmengen sinnvoll, aber wir benötigen ihn nur für \neg -freie Klauseln $K \neq \square$ einer \equiv -freien Sprache, d.h. K enthält nur unnegierte Primformeln, die keine Gleichungen sind. Ein derartiges K heie *unifizierbar*, wenn es eine (simultane) Substitution ω gibt, so dass $K^\omega := \{\lambda^\omega \mid \lambda \in K\}$ genau ein Element enthlt. Eine solches ω werde ein *Unifikator* von K genannt.

Beispiel 1. Sei $K = \{rxfxz, rfyzu\}$, r und f 2-stellig. Hier ist $\omega = \frac{fyz}{x} \frac{ffyz}{u}$ ein Unifikator, denn es ist $K^\omega = \{rfyzffyz\}$ wie man unmittelbar verifiziert.

Offenbar ist kein K unifizierbar, das mit verschiedenen Relationszeichen beginnende Literale enthlt. Allgemeiner, enthlt K zwei Literale mit verschiedenen Symbolen ζ_1, ζ_2 an gleicher Position, so ist K nicht unifizierbar, falls $\zeta_1, \zeta_2 \notin \text{Var}$. Ein weiteres Unifikationshindernis wird deutlich in

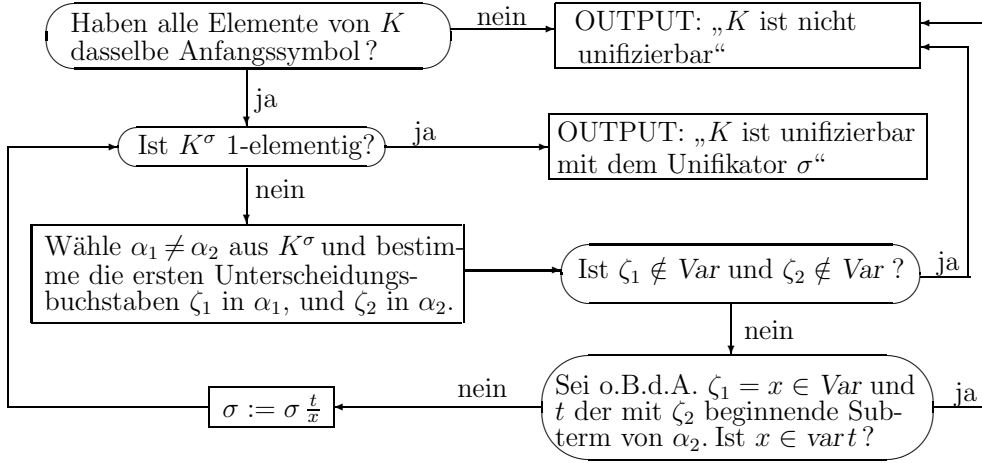
Beispiel 2. Sei $K = \{rx, rfx\}$, d.h. r und f sind 1-stellig. K ist nicht unifizierbar. Denn ist σ ein Unifikator von K , so gilt offenbar $x^\sigma = (fx)^\sigma = fx^\sigma$. Das aber ist unmglich, denn die Terme x^σ und $(fx)^\sigma$ haben verschiedene Lnge.

Mit σ ist trivialerweise auch $\sigma\tau$ fr eine beliebige Substitution τ ein Unifikator. Ein Unifikator ω heie *generisch* (oder ein *allgemeinster Unifikator*) fr K , wenn jeder andere Unifikator τ von K eine Darstellung $\tau = \omega\sigma$ fr eine Substitution σ besitzt. Nach Satz 3.1 unten gibt es fr eine unifizierbare Klauselmenge immer auch einen generischen Unifikator. So ist die Substitution ω in Beispiel 1 bereits generisch.

Unter einer *Umbenennung* verstehen wir der Einfachheit halber eine simultane Substitution ρ (von *renaming*) mit $\rho^2 = \iota$. Ein solches ρ ist notwendig bijektiv und vertauscht einige Variable miteinander, was unseren Erfordernissen gengt. Ist etwa $x_i^\rho = y_i$ ($\neq x_i$) und daher $y_i^\rho = x_i$ fr $i = 1, \dots, n$, sowie $z^\rho = z$ sonst, schreibt man auch $\rho = \begin{pmatrix} x_1 \dots x_n \\ y_1 \dots y_n \end{pmatrix}$. So vertauscht $\rho := \begin{pmatrix} xy \\ uv \end{pmatrix} = \begin{pmatrix} uv \\ xy \end{pmatrix}$ z.B. x mit u und y mit v . Fr eine Umbenennung ρ ist mit ω auch $\omega' = \omega\rho$ ein generischer Unifikator von K . Denn ist τ ein Unifikator von K , so gibt es ein σ mit $\tau = \omega\sigma$ und fr $\sigma' := \rho\sigma$ ist wegen $\rho^2 = \iota$ dann $\tau = \omega\rho^2\sigma = (\omega\rho)(\rho\sigma) = \omega'\sigma'$. Whlt man in Beispiel 1 etwa $\rho := \begin{pmatrix} yz \\ uv \end{pmatrix}$, erhlt man den generischen Unifikator $\omega' = \omega\rho$, mit $K^{\omega'} = \{rfuvffuv\}$.

Wir beschreiben nun ein Verfahren in Form eines Flussdiagramms, den mit \mathfrak{U} bezeichneten *Unifikationsalgorithmus*, der fr jede wie oben beschriebene Klausel K prft ob K unifizierbar ist, und im positiven Falle einen sogar generischen Unifikator produziert. \mathfrak{U} benutzt eine Substitutionsvariable σ mit dem Anfangswert ι . Zu Rechnungsbeginn ist also $K^\sigma = K$. Die *ersten Unterscheidungsbuchstaben* von $\alpha_1 \neq \alpha_2$ aus K seien die ersten Symbole von links gesehen, in denen α_1, α_2 sich

unterscheiden. Das Diagramm enthält eine Schleife, beginnend mit der linken unteren Testfrage und umfasst zwei weitere Testfragen auf der rechten Diagrammseite.



Bei jedem Durchlauf durch die (einzige) Schleife des Diagramms vermindert die neue Substitution $\sigma \frac{t}{x}$ wegen $x \notin \text{var } t$ die Anzahl der in K^σ vorkommenden Variablen. Daher stoppt \mathfrak{U} bei Eingabe einer Klausel K in jedem Falle und hält in einem der beiden Kästchen, in denen \mathfrak{U} einen OUTPUT (eine Ausgabe) produziert. Wir wissen nur noch nicht, ob \mathfrak{U} stets im „richtigen“ Kästchen landet, also die richtige Antwort gibt. Im unteren der beiden OUTPUT-Kästchen wird überdies der Endwert von σ ausgedruckt. Es sei σ_0 die identische Substitution und σ_i für $i > 0$ der Wert von σ nach dem i -ten Schleifendurchlauf, deren Gesamtzahl m sei.

Beispiel 3. \mathfrak{U} werde auf K aus Beispiel 1 angesetzt. Die ersten Unterscheidungsbuchstaben für die beiden Elemente $\alpha_1, \alpha_2 \in K$ sind $\zeta_1 = x$ und $\zeta_2 = f$. Der mit ζ_2 in α_2 beginnende Subterm ist $t = fyz$. Also $\sigma_1 = \frac{fyz}{x}$ und K^σ hat nach dem ersten Schleifendurchlauf den Wert $\{rfyzffyz, rfyzu\}$. Die ersten Unterscheidungsbuchstaben sind hier f und u . Der mit f (an 5. Stelle) beginnende Subterm ist $t = ffyz$. Weil $u \notin \text{var } ffyz$, wird die Schleife nochmals durchlaufen und es ist $\sigma_2 = \sigma_1 \frac{ffyz}{u} = \frac{fyz}{x} \frac{ffyz}{u}$. Dies ist bereits ein Unifikator, und \mathfrak{U} beendet die Rechnung mit dem OUTPUT „ K ist unifizierbar mit dem Unifikator $\frac{fyz}{x} \frac{ffyz}{u}$ “.

Satz 3.1. \mathfrak{U} ist korrekt, d.h. \mathfrak{U} gibt bei Eingabe einer negationsfreien Klausel K stets die richtige Antwort. Darüber hinaus unifiziert \mathfrak{U} mit generischem Unifikator.

Beweis. \mathfrak{U} ist sicher korrekt, wenn zwei Elemente von K sich schon in ihren Anfangsbuchstaben unterscheiden. Alle $\alpha \in K$ mögen daher mit gleichem Buchstaben beginnen. Stoppt \mathfrak{U} mit der Ausgabe „ K ist unifizierbar...“, ist K auch unifizierbar,

weil vorher getestet wurde, ob K^σ 1-elementig ist. Ist daher K nicht unifizierbar, stoppt \mathfrak{U} mit der korrekten Antwort „ K ist nicht unifizierbar“. Daher ist noch nachzuweisen, dass \mathfrak{U} auch im unifizierbaren Falle korrekt antwortet. Das ist trivial für 1-elementige Eingaben. Im allgemeinen Falle sei τ ein beliebig gewählter Unifikator. Es ist zu bestätigen, dass \mathfrak{U} keinen Schleifendurchlauf mit dem oberen OUTPUT abbricht, also beide Testfragen mit Auslauf zum oberen OUTPUT verneint werden. Für die obere Testfrage ist dies klar, weil die Symbole ζ_1, ζ_2 für $\zeta_1, \zeta_2 \notin \text{Var}$ bei Substitutionen erhalten bleiben und Unifizierung entgegen Annahme unmöglich wäre. Für die untere Testfrage (Ist $x \in \text{var } t$?) mögen wir uns im $(i+1)$ -ten Schleifendurchlauf ($i < m$) befinden. Es ist zu zeigen $x \notin \text{var } t$. Nur dann ist die Antwort korrekt und der Schleifendurchlauf wird fortgesetzt. Weiter unten beweisen wir

(*) es gibt ein τ_i mit $\sigma_i \tau_i = \tau$ ($\sigma_i = \text{Wert von } \sigma \text{ nach } i\text{-tem Durchlauf}$).

Angenommen im $(i+1)$ -ten Schleifendurchlauf ist $x \in \text{var } t$, mit $\alpha_1, \alpha_2 \in K^\sigma$ wie im Diagramm gewählt. Weil $\sigma_i \tau_i = \tau$ Unifikator ist, gilt $\alpha_1^{\tau_i} = \alpha_2^{\tau_i}$ und folglich auch $(*) x^{\tau_i} = t^{\tau_i}$ nach Übung 2 in 2.2. Dann ist $x \in \text{var } t$ aber unmöglich, denn sonst hätten x^{τ_i} und t^{τ_i} wie in Beispiel 2 verschiedene Länge. Dies bestätigt die Korrektheit des Diagramms auch im unifizierbaren Falle. $(*)$ besagt insbesondere $\sigma_m \tau_m = \tau$. Da τ beliebig gewählt war und die σ_i von der Wahl von τ nicht abhängen, ist $\sigma := \sigma_m$ in der Tat generischer Unifikator von K .

Es verbleibt der Beweis von $(*)$, der induktiv über $i \leq m$ erfolgt. Für $i = 0$ (vor dem ersten Durchlauf) ist $(*)$ trivial; man wähle einfach $\tau_0 := \tau$. Sei $(*)$ richtig für i mit $i < m$. Wie oben schon bewiesen wurde, gilt $(*)$ beim Durchlauf durch die Testfrage $x \in \text{var } t$? Wir setzen $\tau_{i+1} := \frac{t}{x} \tau_i$ und behaupten $\frac{t}{x} \tau_{i+1} = \tau_i$. Für $y \neq x$ gilt $y^{\frac{t}{x} \tau_{i+1}} = y^{\tau_{i+1}} = y^{\frac{t}{x} \tau_i} = y^{\tau_i}$, aber es ist auch

$$\begin{aligned} x^{\frac{t}{x} \tau_{i+1}} &= t^{\tau_{i+1}} = t^{\tau_i} \quad (\text{weil } x \text{ in } t \text{ nicht vorkommt}) \\ &= x^{\tau_i} \quad (\text{nach } (*)). \end{aligned}$$

$\frac{t}{x} \tau_{i+1} = \tau_i$ und $\sigma_{i+1} = \sigma_i \frac{t}{x}$ ergeben schließlich $\sigma_{i+1} \tau_{i+1} = \sigma_i \frac{t}{x} \tau_{i+1} = \sigma_i \tau_i = \tau$. \square

Übungen

- Man zeige, für Primformeln α, β ohne gemeinsame Variable sind gleichwertig:
 - $\{\alpha, \beta\}$ ist unifizierbar, (ii) es gibt Substitutionen σ, τ mit $\alpha^\sigma = \beta^\tau$.
- Man zeige: $\sigma = \frac{t}{x}$ ist idempotent (d.h. $\sigma^2 = \sigma$) genau dann, wenn $x_i \notin \text{var } t$.
- Für Klauseln K_0, K_1 heiße ρ ein *Separator*, wenn ρ eine Umbenennung ist mit $\text{var } K_0^\rho \cap \text{var } K_1 = \emptyset$. Seien K_0, K_1 negationsfrei. Man zeige, mit $K_0 \cup K_1$ ist auch $K_0^\rho \cup K_1$ unifizierbar (im Allgemeinen aber nicht umgekehrt).

4.4 Logikprogrammierung

Ein recht allgemeiner Ansatz der Wissensverarbeitung in Systemen der künstlichen Intelligenz besteht darin, aus gewissen, in Gestalt einer Formelmenge X gegebenen Daten und Fakten per Computer Folgerungen φ zu ziehen, also $X \vdash \varphi$ (oder $X \models \varphi$) maschinell zu beweisen. Dass dies prinzipiell möglich ist, wurde in 3.5 dargelegt. Praktisch ist dies i.a. jedoch nur durchführbar, wenn gewisse Einschränkungen über die Gestalt der Formeln in X , φ in Kauf genommen werden. Dabei beziehen wir uns auf eine der jeweiligen Problemstellung angepasste Sprache \mathcal{L} der 1. Stufe. Für die Logikprogrammierung sind folgende Einschränkungen kennzeichnend:

- \mathcal{L} ist gleichheitsfrei und enthält mindestens ein Konstantensymbol,
- X enthält nur positive universale Hornaussagen,
- φ ist eine Aussage der Gestalt $\exists \vec{x}(\gamma_0 \wedge \dots \wedge \gamma_k)$ mit Primformeln γ_i .

Man beachte, $\neg\varphi$ ist äquivalent zu $\forall \vec{x}(\neg\gamma_0 \vee \dots \vee \neg\gamma_k)$, also eine negative universale Hornaussage. Weil sich \forall -Quantoren auf Konjunktionen verteilen lassen, kann man o.B.d.A. davon ausgehen, jede Aussage $\alpha \in X$ sei von der Gestalt

$$(\beta_1 \wedge \dots \wedge \beta_m \rightarrow \beta)^\forall \quad (\beta, \beta_1, \dots, \beta_m \text{ Primformeln, } m \geq 0).$$

Eine endliche Menge von Aussagen dieser Art heie ein *Logikprogramm* und werde fortan mit dem Buchstaben \mathcal{P} bezeichnet. In der Programmiersprache PROLOG schreibt man diese Aussagen unter Weglassung der Quantoren in der Weise

$$\beta :- \beta_1, \dots, \beta_m \quad (\text{fr } m = 0 \text{ sei dies die Zeichenfolge } \beta :-).$$

$:-$ symbolisiert sozusagen die konverse Implikation. Fr $m = 0$ heien solche Programmklauseln *Fakten*, fr $m > 0$ *Regeln*. Die Aussage $\varphi = \exists \vec{x}(\gamma_0 \wedge \dots \wedge \gamma_k)$ oben ($\exists \vec{x}$ kann leer sein) heit auch eine *Anfrage* an \mathcal{P} und wird in PROLOG in der Weise $:- \gamma_0, \dots, \gamma_k$ notiert³⁾. Ursprung dieser Notation ist die quivalenz des Kerns von $\forall \vec{x}(\neg\gamma_0 \vee \dots \vee \neg\gamma_k)$ zu $\perp \leftarrow \gamma_0 \wedge \dots \wedge \gamma_k$. Mit Regeln gelangt man von vorgegebenen zu neuen Fakten, aber auch zu Antworten auf Anfragen. Den kleinen Unterschied zwischen einem Logikprogramm als Formelmenge und ihrer Niederschrift in PROLOG drfen wir ohne Nachteile vernachlssigen.

Der Verzicht auf das $=$ -Symbol ist nicht wirklich gravierend. Das wird auch in den Beispielen 1 und 4 und den Schlussausfhrungen dieses Abschnitts deutlich. Erforderlichenfalls kann $=$ durch Hinzufgen der Hornaussagen (4) in 4.1 wie ein

³⁾auch $?-\gamma_0, \dots, \gamma_k$. Wie jede Programmiersprache, hat auch PROLOG gewisse „Dialekte“. Wir halten uns daher nicht konsequent an eine bestimmte Syntax. Auch bergangen wir viele Details, etwa dass Variablen stets mit Grobuchstaben beginnen und dass PROLOG einige unvernderliche Prdikate wie *read*, ... kennt, die der Kommunikation mit dem Nutzer dienen.

2-stelliges Relationssymbol behandelt werden. Die Bedingung des Vorhandenseins eines Konstantensymbols sichert die Existenz von Herbrand-Modellen für \mathcal{P} .

Programmklauseln und negierte Anfragen können auch als Hornklauseln geschrieben werden: $\beta :- \beta_0, \dots, \beta_m$ als $\{\neg\beta_1, \dots, \neg\beta_n, \beta\}$, und $:- \gamma_0, \dots, \gamma_k$ als $\{\neg\gamma_0, \dots, \neg\gamma_k\}$. Für ein Logikprogramm \mathcal{P} werde die entsprechende Menge positiver Hornklauseln mit \mathcal{P} bezeichnet. Eine Verwechslung von \mathcal{P} und \mathcal{P} ist harmlos, weil man beide Dinge fast immer identifizieren kann. Um dies auch semantisch zu untermauern, bedeute $\mathcal{A} \models K$ ($= \{\lambda_0, \dots, \lambda_k\}$) für \mathcal{L} -Strukturen \mathcal{A} einfach $\mathcal{A} \models \bigvee_{i \leq k} \lambda_i$. Gleichwertig ist $\mathcal{A} \models (\bigvee_{i \leq k} \lambda_i)^\forall$. Und für \mathcal{L} -Modelle \mathcal{M} bedeute $\mathcal{M} \models K$ eben $\mathcal{M} \models \bigvee_{i \leq k} \lambda_i$. Es meinen dann z.B. $\mathcal{A} \models \{\neg\gamma_0, \dots, \neg\gamma_k\}$ und $\mathcal{A} \models \neg\gamma_0 \vee \dots \vee \neg\gamma_k$ ein und dasselbe.

Der leeren Klausel entspricht \perp , so dass stets $\mathcal{A} \not\models \perp$. Gibt es ein $\mathcal{A} \models K$ für alle $K \in \mathcal{K}$, so heißt \mathcal{A} ein *Modell für \mathcal{K}* und \mathcal{K} heißt *erfüllbar* oder *konsistent*, weil dies gleichwertig ist mit der Konsistenz der \mathcal{K} entsprechenden Aussagenmenge. Ferner sei $\mathcal{K} \models H$, wenn jedes Modell von \mathcal{K} auch H erfüllt. Offenbar ist $\mathcal{K} \models K^\sigma$ für $K \in \mathcal{K}$ und beliebige Substitutionen σ , weil $\mathcal{A} \models K \Rightarrow \mathcal{A} \models K^\sigma$. Die Klausel K^σ heißt auch eine *Instanz* von K , speziell eine *Grundinstanz*, wenn $\text{var } K^\sigma = \emptyset$.

Ein Logikprogramm \mathcal{P} ist als Menge positiver Hornformeln stets konsistent. Alle Fakten und Regeln von \mathcal{P} gelten im minimalen Herbrand-Modell $\mathcal{C}_{\mathcal{P}}$, welches man sich als Modell eines Gegenstandsbereichs vorstellen sollte, über den man mit \mathcal{P} Aussagen zu machen wünscht. Man schreibt Logikprogramme \mathcal{P} immer so, dass ein Sachverhalt oder ein Expertenwissen möglichst genau durch $\mathcal{C}_{\mathcal{P}}$ modelliert wird und muss $\mathcal{C}_{\mathcal{P}}$ deshalb kennen. Gilt $(*) \mathcal{P} \vdash \exists \vec{x} \gamma$, besteht ein zentrales Anliegen darin, konkrete „Lösungen“ von $(*)$ zu gewinnen. Dabei heiße $\gamma_{\vec{x}}^{\vec{t}}$ oder auch nur $\frac{\vec{t}}{\vec{x}}$ eine *Lösung* von $(*)$, wenn $\mathcal{P} \vdash \gamma_{\vec{x}}^{\vec{t}}$. Oft spricht man dann auch von der Lösung $\vec{x} = \vec{t}$. Für variablenfreies \vec{t} entsprechen ihr wohlbestimmte Objekte in $\mathcal{C}_{\mathcal{P}}$.

Logikprogrammierung folgt der Strategie eines Nachweises von $\mathcal{P} \vdash \varphi$ (φ Anfrage) durch den Inkonsistenznachweis von $\mathcal{P}, \neg\varphi$. Dafür genügt nach Satz 1.1 der Inkonsistenzbeweis von $\text{GI}(\mathcal{P}, \neg\varphi)$. In grober Beschreibung genügt hierfür nach Satz 2.2 die Herleitbarkeit der leeren Klausel aus der $\text{GI}(\mathcal{P}, \neg\varphi)$ entsprechenden Klauselmengemenge $\text{GI}(\mathcal{P}, N)$. Dabei sei $\text{GI}(\mathcal{K})$ allgemein die Menge aller Grundinstanzen der Klauseln aus einer Klauselmengemenge \mathcal{K} , und $N = \{\neg\gamma_1, \dots, \neg\gamma_n\}$ sei die der Anfrage φ entsprechende negative Klausel, die sogenannte *Zielklausel*.

Man geht nun noch etwas geschickter vor und arbeitet nicht nur mit Grundinstanzen, sondern mit beliebigen Instanzen. Die Suche nach Resolutionen geschieht auch nicht zufällig oder willkürlich, sondern mit einem möglichst sparsamen Einsatz von Substitutionen zum Zwecke der Unifizierung, wenn dadurch Resolutionen zustande kommen. Vor ihrer allgemeinen Formulierung in Satz 4.2 erläutern wir diese Methode der „unifizierten Resolution“ in zwei leicht überschaubaren Beispielen.

Beispiel 1. Wir betrachten das folgende Logikprogramm \mathcal{P}_+ in $\mathcal{L}\{0, \mathbf{S}, \mathbf{sum}\}$:

$$\forall x \mathbf{sum} \, x0x \ ; \ \forall x \forall y \forall z (\mathbf{sum} \, xyz \rightarrow \mathbf{sum} \, x\mathbf{S}y\mathbf{S}z).$$

In PROLOG könnte man diese Programmklauseln auch notieren in der Weise

$$\mathbf{sum} \, x0x :- \quad ; \quad \mathbf{sum} \, x\mathbf{S}y\mathbf{S}z :- \mathbf{sum} \, xyz$$

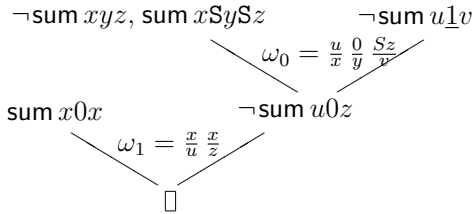
\mathcal{P}_+ entspricht der Hornklauselmengemenge $\mathcal{P}_+ = \{\{\mathbf{sum} \, x0x\}, \{\neg \mathbf{sum} \, xyz, \mathbf{sum} \, x\mathbf{S}y\mathbf{S}z\}\}$ und beschreibt den Graphen der Addition in \mathbb{N} ; genauer, $\mathcal{C}_{\mathcal{P}_+} \simeq \mathcal{N} = (\mathbb{N}, 0, \mathbf{S}, \mathbf{sum})$, mit $\mathbf{sum}^{\mathcal{N}} = \mathit{graph}+$, also $\mathcal{C}_{\mathcal{P}_+} \models \mathbf{sum} \, \underline{m} \, \underline{n} \, \underline{k} \Leftrightarrow \mathcal{N} \models \mathbf{sum} \, \underline{m} \, \underline{n} \, \underline{k}$ ($\Leftrightarrow m + n = k$). Das folgt ähnlich wie in Beispiel 4 auf Seite 110, aber noch einfacher aus Übung 2 in 4.2. Ersetzt man dort $p_{m,n,k}$ durch $\mathbf{sum} \, \underline{m} \, \underline{n} \, \underline{k}$, so entspricht die Formelmengemenge dieser Übung genau den Grundinstanzen von \mathcal{P}_+ .

Beispiele für Anfragen an \mathcal{P}_+ sind $\exists u \exists v \mathbf{sum} \, u1v$, $\exists u \mathbf{sum} \, uu6$ und $\mathbf{sum} \, \underline{n} \, \underline{2} \, \underline{n+2}$ (hier ist das \exists -Präfix leer). Für jede dieser drei Anfragen φ gilt offenbar $\mathcal{C}_{\mathcal{P}_+} \models \varphi$. Also $\mathcal{P}_+ \vdash \varphi$ nach Satz 1.4. Wie aber lässt sich dies maschinell bestätigen?

Zur Illustration sei $\varphi := \exists u \exists v \mathbf{sum} \, u1v$. Offenbar ist $\mathbf{sum} \, \underline{n} \, \underline{1} \, \underline{Sn}$ für jedes n eine Lösung von (*) $\mathcal{P}_+ \vdash \exists u \exists v \mathbf{sum} \, u1v$. Wir beweisen sogar $\mathcal{P}_+ \vdash \mathbf{sum} \, x1\mathbf{S}x$, oder gleichwertig $\mathcal{P}_+ \vdash \forall x \mathbf{sum} \, x1\mathbf{S}x$. Der Inkonsistenznachweis von $\mathcal{P}_+, \neg \varphi$ erfolgt durch Herleitung von \square aus geeigneten Instanzen von \mathcal{P}_+, N ; hier ist $N := \{\neg \mathbf{sum} \, u1v\}$ die φ entsprechende Zielklausel. Sei ferner $P := \{\neg \mathbf{sum} \, xyz, \mathbf{sum} \, x\mathbf{S}y\mathbf{S}z\}$. In \mathcal{P}_+, N ist die Resolutionsregel nicht direkt anwendbar. Sie ist mit $\omega_0 := \frac{u}{x} \frac{0}{y} \frac{\mathbf{S}z}{v}$ aber anwendbar auf das Paar $P^{\omega_0}, N^{\omega_0}$, mit der in \mathcal{P}_+ liegenden Hornklausel P . In der Tat, es ist

$$P^{\omega_0} = \{\neg \mathbf{sum} \, u0z, \mathbf{sum} \, u1\mathbf{S}z\} \quad ; \quad N^{\omega_0} = \{\neg \mathbf{sum} \, u1\mathbf{S}z\}.$$

Die Resolvente ist $N_1 := \{\neg \mathbf{sum} \, u0z\}$. Man kann dies auch so formulieren: Resolution wurde möglich durch die Unifizierbarkeit der Klausel $G = \{\mathbf{sum} \, x\mathbf{S}y\mathbf{S}z, \mathbf{sum} \, u1v\}$. Sei $P_1 := \{\mathbf{sum} \, x0x\}$ ($\in \mathcal{P}_+$). Dann kann P_1, N_1 durch Unifizierung mit $\omega_1 := \frac{x}{u} \frac{x}{z}$ zur Resolution gebracht werden. Denn $P_1^{\omega_1} = \{\mathbf{sum} \, x0x\}$ und $N_1^{\omega_1} = \{\neg \mathbf{sum} \, x0x\}$.

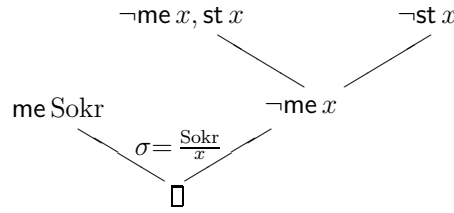


Anwendung von RR auf dieses Klauselpaar ergibt bereits \square . Die Figur links veranschaulicht diese Beschreibung (wobei die Mengenklammern der Klauseln weggelassen wurden). Diese Resolution kann sicher auch von einem Computer produziert werden – nach den passenden Unifikatoren muss er eben suchen!

Damit wurde (*) nach Satz 4.2(a) unten bewiesen. Zugleich wurde nach Satz 4.2(b) auch eine Lösung von (*) konstruiert, nämlich $(\mathbf{sum} \, u1v)^{\omega_0 \omega_1} = \mathbf{sum} \, x1\mathbf{S}x$. Dies ist im vorliegenden Falle sogar die allgemeine Lösung; denn durch Substitution erhält man hieraus alle konkreten Lösungen, nämlich alle Aussagen $\mathbf{sum} \, \underline{n} \, \underline{1} \, \underline{Sn}$.

Beispiel 2. Das Logikprogramm $\mathcal{P} = \{\forall x(\text{me } x \rightarrow \text{st } x), \text{me Sokr}\}$ formalisiert die Prämissen des antiken logischen Schlusses *Alle Menschen sind sterblich; Sokrates ist ein Mensch. Also ist Sokrates sterblich.*

$\mathcal{C}_{\mathcal{P}}$ ist hier das Einpunktmodell $\{\text{Sokr}\}$, weil Sokr die einzige Konstante ist und keine Funktionen vorkommen. Die Figur rechts zeigt einen Resolutionsbeweis für $\exists x \text{st } x$ mit der Lösung $x = \text{Sokr}$ nach Satz 4.2(b). Beweise mit MP lassen sich also auch durch Resolution gewinnen.



Natürlich ist dieses und auch Beispiel 1 viel zu einfach, um den Nutzen der Logikprogrammierung darzutun. Hier geht es nur um die Erläuterung der Methode.

Nach diesen Vorbetrachtungen kommen wir nun zu einer für alles folgende wichtigen

Definition der Regeln UR und UHR der unifizierten Resolution bzw. der unifizierten Hornresolution. Für beliebige Klauseln K_0, K_1 und Substitutionen ω sei $K \in U_{\omega}R(K_0, K_1)$, wenn es Klauseln H_0, H_1 und \neg -freie Klauseln $G_0, G_1 \neq \square$ gibt, so dass nach eventueller Vertauschung der beiden Indizes

- (a) $K_0 = H_0 \cup G_0$ und $K_1 = H_1 \cup \overline{G_1}$ ($\overline{G_1} = \{\neg \lambda \mid \lambda \in G_1\}$, Seite 113),
- (b) ω ist generischer Unifikator von $G_0 \cup G_1$ ⁴⁾ und $K = H_0^{\omega} \cup H_1^{\omega}$.

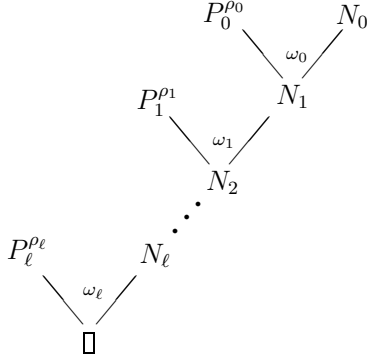
K heie eine *U-Resolvente* von K_0, K_1 oder *Anwendung der Regel UR* auf K_0, K_1 , wenn ein ρ und ein ω existieren mit $K \in U_{\omega}R(K_0^{\rho}, K_1)$. Die Einschränkung von UR auf Hornklauspaaare K_0, K_1 (K_0 positiv, K_1 negativ) werde mit UHR bezeichnet, $U_{\omega}R(K_0, K_1)$ mit $U_{\omega}HR(K_0, K_1)$, und K heie eine *UH-Resolvente* von K_0, K_1 .

Eine Anwendung von UR oder UHR auf ein Paar K_0, K_1 schliet immer eine Wahl von ρ und ω ein und $K \in U_{\omega}R(K_0^{\rho}, K_1)$ bedeutet i.a. mehr als nur $K \in U_{\omega}R(K_0, K_1)$, bung 1. In obigen Beispielen wurde UHR verwendet. Im ersten Resolutionsschritt in Beispiel 1 ist $\neg \text{sum } u0z \in U_{\omega_0}HR(P, N)$ (also $\rho = \iota$) und die Zerlegung nach (a) der Definition lautet $H_0 = \{\neg \text{sum } xyz\}$, $G_0 = \{\text{sum } xSySz\}$, $H_1 = \emptyset$ und $G_1 = \{\text{sum } u1v\}$. Auch im 2. Resolutionsschritt und in Beispiel 2 wurde UHR nach Definitionsvorschrift verwendet, wie man unschwer nachprft.

Wir schreiben $\mathcal{K} \vdash^{UR} H$, wenn H aus der Klauselmenge \mathcal{K} mittels UR ableitbar ist. Entsprechend sei $\mathcal{K} \vdash^{UHR} H$ fr Hornklauspaaare \mathcal{K} definiert, wobei nur mit der Regel UHR abgeleitet wird. Ableitungen in \vdash^{UR} oder \vdash^{UHR} kann man sich wie in der Aussagenlogik durch Bume veranschaulichen. Eine (erfolgreiche) *U-Resolution* fr \mathcal{K} sei ein U-Resolutionsbaum mit Blttern aus \mathcal{K} und der Wurzel \square .

⁴⁾ Man beachte, dass hiernach notwendigerweise $G_0^{\omega} = \{\pi\} = G_1^{\omega}$ fr eine gewisse Primformel π .

Analog sei eine *UH-Resolution* definiert, die man auch als Folge $(P_i^{\rho_i}, N_i, \omega_i)_{i \leq \ell}$ mit den Eigenschaften $N_{i+1} \in U_{\omega_i} HR(P_i^{\rho_i}, N_i)$ für $i < \ell$ und $\square \in U_{\omega_\ell} HR(P_\ell^{\rho_\ell}, N_\ell)$ ansehen kann. Ist \mathcal{P} eine Menge positiver Klauseln und N eine negative Klausel und gilt außerdem $P_i \in \mathcal{P}$ für alle $i \leq \ell$ und $N_0 = N$, spricht man von einer *UH-Resolution* für \mathcal{P}, N . Meist besteht \mathcal{P} aus den Klauseln eines Logikprogramms und N ist eine



gegebene Zielklausel. Statt von *UH-Resolution* spricht man auch von *SLD-Resolution* (*Linear resolution with Selection function for Definite clauses*), was nichts zu tun hat mit speziellen Strategien, die ein in PROLOG programmierter Rechner bei der Suche nach erfolgreichen Resolutionen verfolgt. Für Einzelheiten hierüber verweisen wir jedoch auf [Ll] oder [GH]. Die Figur links veranschaulicht eine *UH-Resolution* $(P_i^{\rho_i}, N_i, \omega_i)_{i \leq \ell}$ für \mathcal{P}, N . Diese Figur verallgemeinert offenbar die Diagramme in den

Beispielen 1 und 2. Als erstes beweisen wir die Korrektheit des Kalküls \vdash^{UR} und damit automatisch auch des Kalküls \vdash^{UHR} der unifizierten Hornresolution:

Lemma 4.1 (Korrektheitslemma). $\mathcal{K} \vdash^{UR} H$ impliziert $\mathcal{K} \models H$.

Beweis. Es genügt zu zeigen $K_0, K_1 \models H$, wenn H eine U -Resolvente von K_0, K_1 ist. Es sei $H \in U_{\omega} R(K_0^{\rho}, K_1)$, $K_0^{\rho} = H_0 \cup G_0$, $K_1 = H_1 \cup \overline{G_1}$, $G_0^{\omega} = \{\pi\} = G_1^{\omega}$, $H = H_0^{\rho\omega} \cup H_1^{\omega}$, und $\mathcal{A} \models K_0, K_1$, so dass auch $\mathcal{A} \models K_0^{\rho\omega}, K_1^{\omega}$. Ferner sei $w: \text{Var} \rightarrow A$, also $\mathcal{M} := (\mathcal{A}, w) \models K_0^{\rho\omega} = H_0^{\rho\omega} \cup \{\pi\}$, $\mathcal{M} \models H_1^{\omega} \cup \{\neg\pi\}$. Falls $\mathcal{M} \not\models \pi$ ist offenbar $\mathcal{M} \models H_0^{\rho\omega}$. Andernfalls, falls also $\mathcal{M} \models \neg\pi$, ist $\mathcal{M} \models H_1^{\omega}$. In jedem Falle gilt also $\mathcal{M} \models H_0^{\omega} \cup H_1^{\omega} = H$. Das besagt $\mathcal{A} \models H$, denn w war beliebig. \square

Dieses Lemma dient – bezogen auf den Kalkül \vdash^{UHR} – dem Nachweis von (a) in

Satz 4.2 (Hauptsatz der Logikprogrammierung). Sei \mathcal{P} ein Logikprogramm, $\exists \vec{x} \gamma = \exists \vec{x} (\gamma_0 \wedge \dots \wedge \gamma_k)$ eine Anfrage und $N = \{\neg \gamma_0, \dots, \neg \gamma_k\}$. Dann gelten

- (a) $\mathcal{P} \vdash \exists \vec{x} \gamma$ genau dann, wenn $\mathcal{P}, N \vdash^{UHR} \square$ (Adäquatheit),
- (b) Ist $(P_i^{\rho_i}, N_i, \omega_i)_{i \leq \ell}$ eine *UH-Resolution* für \mathcal{P}, N und $\omega := \omega_0 \dots \omega_{\ell}$, so ist $\mathcal{P} \vdash \gamma^{\omega}$ (Lösungskorrektheit),
- (c) Ist $\mathcal{P} \vdash \gamma_{\vec{x}}^{\vec{t}}$ mit $\vec{t} \in \mathcal{T}_0^n$, so gibt es eine *UH-Resolution* $(K_i^{\rho_i}, N_i, w_i)_{i \leq \ell}$ und ein τ mit $x_i^{\omega \tau} = t_i$ für $i = 1, \dots, n$, wobei $\omega := \omega_0 \dots \omega_{\ell}$ (Lösungsvollständigkeit).

Den auf ausgiebigem Rechnen mit Substitutionen beruhenden Beweis erbringen wir in 4.5. Hier nur einige kurze Erläuterungen. Sicher ist $(*) \mathcal{P} \vdash \exists \vec{x} \gamma$ gleichwertig

mit der Inkonsistenz von $\mathcal{P}, \forall \vec{x} \neg \gamma$, oder derjenigen der entsprechenden Hornklauselmenge \mathcal{P}, N . Teil (a) des Satzes sagt, dass $(*)$ auch mit $\mathcal{P}, N \vdash^{UHR} \square$ gleichwertig ist. Die Frage $\mathcal{P} \vdash \exists x \gamma$ ist also, wenn sie lösbar ist, auch mit Resolution lösbar.

Teil (b) des Satzes erzählt uns, wie man nach erfolgreicher Resolution zu einer konkreten Lösung von $(*)$ gelangt. Weil γ^ω in (b) i.a. noch freie Variablen enthält (wie etwa $(\text{sum } u _1 v)^\omega = \text{sum } x _1 Sx$ für $\omega = \omega_1 \omega_2$ in Beispiel 1) und weil mit $\mathcal{P} \vdash \gamma^\omega$ gewiss auch $\mathcal{P} \vdash \gamma^{\omega\tau}$ für beliebige τ , erhält man durch Substitution von Grundtermen oft ganze Lösungsscharen von $(*)$ im Herbrandmodell $\mathcal{C}_\mathcal{P}$. Auf diese Weise ergeben sich nach (c) sogar sämtliche Lösungen in $\mathcal{C}_\mathcal{P}$. Allerdings kann dies nicht immer mit einer einzigen erfolgreichen Resolution geschehen wie in Beispiel 1. Ob und unter welchen Umständen $(*)$ lösbar ist, darüber sagt der Satz allerdings nichts aus.

Logikprogrammierung ist auch für rein theoretische Zwecke nützlich. So lässt sich damit z.B. der Begriff der berechenbaren Funktion über \mathbb{N} präzisieren. Die Definition unten liefert hierfür eine von vielen ähnlich gearteten intuitiv einsichtigen Möglichkeiten. Damit gewinnt man recht einfach ein unentscheidbares Problem, das die mit einer generellen Antwort auf die Frage $\mathcal{P} \vdash \exists \vec{x} \gamma$ verbundenen Schwierigkeiten erklärt, Satz 4.3. Weil berechenbare Funktionen in 6.1 mit den rekursiven Funktionen gleichgesetzt werden, fassen wir uns diesbezüglich aber relativ kurz.

Definition. $f: \mathbb{N}^n \rightarrow \mathbb{N}$ heiße *berechenbar* ⁵⁾, wenn es ein Logikprogramm $\mathcal{P} = \mathcal{P}_f$ in einer Sprache gibt, die nebst 0 und S nur Relationssymbole enthält, darunter ein mit r_f bezeichnetes Symbol, so dass für alle $\vec{k} = (k_1, \dots, k_n)$ und alle m

$$(*) \quad \mathcal{P} \vdash r_f \vec{k} \underline{m} \Leftrightarrow f\vec{k} = m \quad (\vec{k} = (k_1, \dots, k_n)).$$

Bemerkung. Der Träger des Herbrand-Modells $\mathcal{C}_\mathcal{P}$ kann wie in Beispiel 1 mit \mathbb{N} identifiziert werden. Nach Satz 1.4 ist $\mathcal{P} \vdash r_f \vec{k} \underline{m} \Leftrightarrow \mathcal{C}_\mathcal{P} \models r_f \vec{k} \underline{m}$. Also $\mathcal{C}_\mathcal{P} \models r_f \vec{k} \underline{m} \Leftrightarrow f\vec{k} = m$, für alle \vec{k}, m . Kurzum, r_f ist in $\mathcal{C}_\mathcal{P}$ nichts anderes als $\text{graph } f$.

Eine $(*)$ erfüllende Funktion $f: \mathbb{N}^n \rightarrow \mathbb{N}$ ist sicher intuitiv berechenbar: Eine Deduktionsmaschine möge bei gegebenem \vec{k} alle aus \mathcal{P} beweisbaren Formeln aufzählen und man warte nur ab, bis eine Aussage $r \vec{k} \underline{m}$ erscheint. Dann ist $m = f\vec{k}$ berechnet. Die linke Seite von $(*)$ ist nach Satz 4.2(a) gleichwertig mit $\mathcal{P}, \{\neg r \vec{k} \underline{m}\} \vdash^{UHR} \square$. Daher ist f jedenfalls prinzipiell auch mit dem Resolutionskalkül berechenbar.

Beispiel 3. Das Programm $\mathcal{P} = \mathcal{P}_+$ in Beispiel 1 berechnet $+$, genauer $\text{graph } +$. Denn $\mathcal{C}_\mathcal{P} \models \text{sum } \underline{k} \underline{n} \underline{m} \Leftrightarrow k + n = m$ wie dort gezeigt wurde. Also gilt (2) und damit auch (1). Ein Logikprogramm \mathcal{P}_\times zur Berechnung von $\text{prd} = \text{graph } \cdot$ entsteht aus \mathcal{P}_+ durch Hinzufügen der Klauseln $\text{prd } x00 :-$ und $\text{prd } xSyu :- \text{prd } xyz, \text{sum } zxu$. \mathcal{P}_\times enthält die Relationssymbole prd , sum und es ist $\mathcal{C}_{\mathcal{P}_\times} \simeq (\mathbb{N}, 0, S, \text{sum}, \text{prd})$.

⁵⁾ Legt man eine andere Präzisierung des Berechenbarkeitsbegriffs zugrunde, könnte man f bis zum Gleichwertigkeitsbeweis beider Konzepte provisorisch z.B. auch *LP-berechenbar* nennen.

Beispiel 4. Wir behaupten, das nur aus dem Faktum $r_s xSx :-$ bestehende Programm \mathcal{P}_s berechnet den Graphen r_s der Nachfolgerfunktion. Hier argumentieren wir wie folgt. Es ist $\mathcal{P}_s \vdash r_s \underline{nS\underline{n}}$, weil $\mathcal{P}_s, \{\neg r_s \underline{nS\underline{n}}\} \vdash^{UHR} \square$; denn für $\sigma = \frac{s^n 0}{x}$ ist \square Resolvente von $\{r_s xSx\}^\sigma$ und $\{\neg r_s \underline{nS\underline{n}}\}^\sigma$. Es gilt $(\mathbb{N}, 0, S, graphS) \models \mathcal{P}_s, \neg r_s \underline{n} \underline{m}$ für $m \neq Sn$ und daher auch $\mathcal{P}_s \not\vdash r_s \underline{n} \underline{m}$. Dies beweist (\star) .

Man erkennt unschwer, dass jede rekursive Funktion f im Sinne von **6.1** durch ein Logikprogramm \mathcal{P}_f im obigen Sinne berechnet werden kann, also in einer Sprache, die nebst einigen Relationssymbolen nur die Operationssymbole $0, S$ enthält. Die Übungen 2 und 3 sind Schritte in diesem induktiv über die Erzeugungsoperationen **Oc**, **Op** und **Oμ** aus **6.1** zu führenden Nachweis. Beispiel 4 bestätigt dies für die rekursive Anfangsfunktion **S**. Das Konzept der Logikprogrammierung ist also sehr allgemein, was leider die unangenehme Konsequenz hat, dass über die Frage $\mathcal{P} \vdash \exists \vec{x} \gamma$ i.a. nicht effektiv entschieden werden kann. Es gilt nämlich

Satz 4.3. *Es gibt ein Logikprogramm \mathcal{P} , dessen Signatur mindestens ein 2-stelliges Relationssymbol r , aber außer $0, S$ keine weiteren Operationssymbole enthält, so dass kein Algorithmus die Frage $\mathcal{P} \vdash \exists x r x k$ für jedes k beantwortet.*

Beweis. Sei $f: \mathbb{N} \rightarrow \mathbb{N}$ rekursiv, mit nichtrekursivem $ran f$. Solche Funktionen f lassen sich unschwer konstruieren (Übung 4 in **6.5**). Für $\mathcal{P} := \mathcal{P}_f$ gilt dann

$$\begin{aligned} \mathcal{P} \vdash \exists x r_f x \underline{m} &\Leftrightarrow \mathcal{C}_{\mathcal{P}} \models \exists x r_f x \underline{m} && (\text{Satz 1.4}) \\ &\Leftrightarrow \mathcal{C}_{\mathcal{P}} \models r_f k \underline{m} \text{ für gewisses } k && (\mathcal{C}_{\mathcal{P}} \text{ hat Träger } \mathbb{N}) \\ &\Leftrightarrow f k = m \text{ für gewisses } k && (\text{Bemerkung Vorseite}) \\ &\Leftrightarrow m \in ran f. \end{aligned}$$

Mit der Frage $\mathcal{P} \vdash \exists x r x \underline{m}$ wäre also auch die Frage $m \in ran f$ entscheidbar, ein Widerspruch zur Wahl von f . \square

Übungen

1. Sei $H \in U_\omega R(K_0, K_1)$. Man zeige, H ist U -Resolvente von K_0, K_1 , d.h. es gibt ein (generisches) ω' und einen Separator ρ von K_0, K_1 mit $H \in U_{\omega'} R(K_0^\rho, K_1)$.
2. Seien $g: \mathbb{N}^n \rightarrow \mathbb{N}$ und $h: \mathbb{N}^{n+2} \rightarrow \mathbb{N}$ mittels der Logikprogramme \mathcal{P}_g und \mathcal{P}_h berechenbar. $f: \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ entstehe aus g, h durch primitive Rekursion, d.h. f erfülle $f(\vec{a}, 0) = g\vec{a}$ und $f(\vec{a}, k+1) = h(\vec{a}, k, f(\vec{a}, k))$ für alle $\vec{a} \in \mathbb{N}^n$. Man gebe ein Logikprogramm zur Berechnung (des Graphen) von f an.
3. Seien \mathcal{P}_h und \mathcal{P}_{g_i} Logikprogramme zur Berechnung von $h: \mathbb{N}^m \rightarrow \mathbb{N}$ und $g_i: \mathbb{N}^n \rightarrow \mathbb{N}$ ($i = 1, \dots, m$). Ferner sei f definiert durch $f\vec{a} = h(g_1\vec{a}, \dots, g_m\vec{a})$ für alle $\vec{a} \in \mathbb{N}^n$. Man gebe ein Logikprogramm zur Berechnung von f an.

4.5 Der Beweis des Hauptsatzes

Wir benötigen folgendes Lemma und Satz 5.3 eigentlich nur für die UH-Resolution, führen die Beweise aber gleich für die U-Resolution aus. Die Kalküle \vdash^{RR} und \vdash^{HR} aus 4.2 beziehen sich fortan auf variablenfreie Klauseln einer $=$ -freien Sprache.

Lemma 5.1. *Seien K_0, K_1 Klauseln mit Separator ρ und $K_0^{\sigma_0}, K_1^{\sigma_1}$ variablenfrei, sowie K eine Resolvente von $K_0^{\sigma_0}, K_1^{\sigma_1}$. Dann gibt es Substitutionen ω, τ und ein $H \in U_\omega R(K_0^\rho, K_1)$ mit $H^\tau = K$, d.h. K ist Grundinstanz einer U-Resolvente von K_0, K_1 . Ferner lassen sich ω, τ bei vorgegebener endlicher Variablenmenge V so wählen, dass $x^{\omega\tau} = x^{\sigma_1}$ für alle $x \in V$. Dasselbe gilt für die Hornresolution.*

Beweis. Es sei o.B.d.A. $K_0^{\sigma_0} = L_0, \pi$ und $K_1^{\sigma_1} = L_1, \neg\pi$ für eine Primformel π , sowie $K = L_0 \cup L_1$. Sei $H_i := \{\alpha \in K_i \mid \alpha^{\sigma_i} \in L_i\}$, $G_0 := \{\alpha \in K_0 \mid \alpha^{\sigma_0} = \pi\}$ und $G_1 := \{\beta \in K_1 \mid \beta^{\sigma_1} = \pi\}$, $i = 0, 1$. Dann ist $K_0 = H_0 \cup G_0$, $K_1 = H_1 \cup G_1$, $H_i^{\sigma_i} = L_i$, $G_i^{\sigma_i} = \{\pi\}$. Sei ρ Separator von K_0, K_1 und σ definiert durch $x^\sigma = x^{\rho\sigma_0}$ für $x \in \text{var } K_0^\rho$, sowie $x^\sigma = x^{\sigma_1}$ sonst. Dann ist $K_0^{\rho\sigma} = K_0^{\rho\rho\sigma_0} = K_0^{\sigma_0}$ (beachte $\rho^2 = \text{id}$), sowie $K_1^\sigma = K_1^{\sigma_1}$. Das liefert $(G_0^\rho \cup G_1)^\sigma = G_0^{\rho\sigma} \cup G_1^\sigma = G_0^{\sigma_0} \cup G_1^{\sigma_1} = \{\pi\}$, d.h. σ unifiziert $G_0^\rho \cup G_1$. Sei ω generischer Unifikator dieser Klausel, so dass $\sigma = \omega\tau$ für geeignetes τ . Dann ist $H := H_0^\omega \cup H_1^\omega \in U_\omega R(K_0^\rho, K_1)$ nach Definition der Regel UR. Auch ist $H^\tau = K$, denn $K_0^{\rho\sigma} = K_0^{\sigma_0}$. Dann ergeben $\omega\tau = \sigma$ und $K_1^\sigma = K_1^{\sigma_1}$

$$H^\tau = H_0^{\rho\omega\tau} \cup H_1^{\omega\tau} = H_0^{\rho\sigma} \cup H_1^\sigma = H_0^{\sigma_0} \cup H_1^{\sigma_1} = L_0 \cup L_1 = K.$$

Weil V endlich ist, lässt sich ρ so wählen, dass $V \cap \text{var } K_0^\rho = \emptyset$. Nach Definition von σ und wegen $\sigma = \omega\tau$ gilt dann $x^{\omega\tau} = x^\sigma = x^{\sigma_1}$ auch noch für $x \in V$. \square

Lemma 5.2 (Lifting-Lemma). *Sei \mathcal{K} eine Klauselmenge mit $\text{GI}(\mathcal{K}) \vdash^{RR} \square$. Dann ist auch $\mathcal{K} \vdash^{UR} \square$. Besteht \mathcal{K} nur aus Hornklauseln, gilt analog $\mathcal{K} \vdash^{UHR} \square$.*

Beweis. Dies folgt für $K = \square$ aus (*) Ist $\text{GI}(\mathcal{K}) \vdash^{RR} K$, so existieren H und σ mit $\mathcal{K} \vdash^{UR} H$ und $K = H^\sigma$ (man beachte $\square^\sigma = \square$). Dies wiederum ist unschwer durch Induktion über $\text{GI}(\mathcal{K}) \vdash^{RR} K$ beweisbar; denn (*) ist klar für $K \in \text{GI}(\mathcal{K})$, und für den Induktionsschritt ($\text{GI}(\mathcal{K}) \vdash^{RR} K_0, K_1$ und K ist Resolvente von K_0, K_1) benötigt man gerade Lemma 5.1. Völlig analog zeigt man dies für Hornklauseln. \square

Satz 5.3 (U-Resolutionssatz). *Eine Klauselmenge \mathcal{K} ist genau dann inkonsistent, wenn $\mathcal{K} \vdash^{UR} \square$; eine Hornklauselmenge \mathcal{K} genau dann, wenn $\mathcal{K} \vdash^{UHR} \square$.*

Beweis. Falls $\mathcal{K} \vdash^{UR} \square$, ist $\mathcal{K} \models \square$ nach Lemma 4.1, d.h. \mathcal{K} ist inkonsistent. Sei Letzteres nun der Fall, so dass auch die \mathcal{K} entsprechende Menge U von \forall -Aussagen inkonsistent ist. Nach Satz 1.1 ist dann $\text{GI}(U)$ und mithin auch $\text{GI}(\mathcal{K})$ inkonsistent. Also $\text{GI}(\mathcal{K}) \vdash^{RR} \square$ nach dem Resolutionssatz 2.2 und so $\mathcal{K} \vdash^{UR} \square$ nach Lemma 5.2. Für Mengen aus Hornklauseln schließt man mit diesem Lemma analog. \square

Beweis von Satz 4.2. (a): $\mathcal{P} \vdash \exists \vec{x} \gamma$ ist gleichwertig mit der Inkonsistenz von $\mathcal{P}, \forall \vec{x} \neg \gamma$ oder von \mathcal{P}, N . Dies ist nach Satz 5.3 aber gleichwertig mit $\mathcal{P}, N \vdash^{UHR} \Box$.

(b): Beweis durch Induktion über die Länge ℓ einer (erfolgreichen) UH -Resolution $(P_i^{\rho_i}, N_i, \omega_i)_{i \leq \ell}$ für \mathcal{P}, N . Sei $\ell = 0$, also $\Box \in U_\omega HR(P_0^\rho, N)$ für geeignete ρ, ω . Dann wurde $P_0^\rho \cup N = P_0^\rho \cup \{\gamma_0, \dots, \gamma_k\}$ durch ω unifiziert, d.h. $P_0^{\rho\omega} = \{\pi\} = \gamma_i^\omega$ für eine Primformel π und alle $i \leq k$. Wegen $P_0 \in \mathcal{P}$ ist $\mathcal{P} \vdash \gamma_i^\omega (= \pi)$ für jedes $i \leq k$, also $\mathcal{P} \vdash \gamma_0^\omega \wedge \dots \wedge \gamma_k^\omega = \gamma^\omega$ wie behauptet. Sei nun $\ell > 0$. Dann ist auch $(P_i^{\rho_i}, N_i, \omega_i)_{1 \leq i \leq \ell}$ eine UH -Resolution für \mathcal{P}, N_1 . Nach Induktionsannahme gilt also

$$(1) \quad \mathcal{P} \vdash \alpha^{\omega_1 \dots \omega_\ell} \text{ wenn immer } \neg \alpha \in N_1.$$

Es genügt $\mathcal{P} \vdash \gamma_i^\omega$ für jedes $i \leq k$ nachzuweisen. Dafür unterscheiden wir bei gegebenem i zwei Fälle: Für $\neg \gamma_i^{\omega_0} \in N_1$ ist $\mathcal{P} \vdash (\gamma_i^{\omega_0})^{\omega_1 \dots \omega_\ell}$ nach (1), also $\mathcal{P} \vdash \gamma_i^\omega$. Sei nun $\neg \gamma_i^{\omega_0} \notin N_1$. Dann geht $\gamma_i^{\omega_0}$ beim Resolutionsschritt von $P_0^{\rho_0}, N_0 (= N)$ zu N_1 verloren. Also hat P_0 die Gestalt $P_0 = \{\neg \beta_1, \dots, \neg \beta_m, \beta\}$ mit $\beta^{\rho_0 \omega_0} = \gamma_i^{\omega_0}$ und $\neg \beta_j^{\rho_0 \omega_0} \in N_1$ für $j = 1, \dots, m$. Damit ergibt (1) offenbar $\mathcal{P} \vdash (\beta_j^{\rho_0 \omega_0})^{\omega_1 \dots \omega_\ell}$, also $\mathcal{P} \vdash \bigwedge_{j=1}^m \beta_j^{\rho_0 \omega}$. Zugleich ist $\mathcal{P} \vdash \bigwedge_{j=1}^m \beta_j^{\rho_0 \omega} \rightarrow \beta^{\rho_0 \omega}$ wegen $\mathcal{P} \models P_0^{\rho_0 \omega}$. Mit MP erhalten wir hieraus $\mathcal{P} \vdash \beta^{\rho_0 \omega}$. Aus $\beta^{\rho_0 \omega} = \gamma_i^{\omega_0}$ folgt nach Anwendung von $\omega_1 \dots \omega_\ell$ auf beiden Seiten $\beta^{\rho_0 \omega} = \gamma_i^\omega$ und somit $\mathcal{P} \vdash \gamma_i^\omega$ auch im zweiten Falle.

(c): Sei $\mathcal{P} \vdash \gamma^\sigma$ mit $\sigma := \frac{\vec{t}}{\vec{x}}$. Dann ist $\mathcal{P}, \neg \gamma^\sigma$ inkonsistent, und nach Satz 1.1 auch $\mathcal{P}', \neg \gamma^\sigma$ mit $\mathcal{P}' := \text{GI}(\mathcal{P})$ (man beachte $\text{GI}(\neg \gamma^\sigma) = \{\neg \gamma^\sigma\}$). Nach Satz 2.4 gibt es daher eine H -Resolution $\mathbf{B} = (P'_i, Q_i)_{i \leq \ell}$ für \mathcal{P}', N^σ , also $Q_0 = N^\sigma$. Dabei sei etwa $P'_i = P_i^{\sigma_i}$ für passende $P_i \in \mathcal{P}$ und σ_i . Wir beweisen aus diesen Gegebenheiten

$$(2) \quad \text{für endliches } V \subseteq \text{Var} \text{ gibt es } \rho_i, N_i, \omega_i, \tau, \text{ so dass } (P_i^{\rho_i}, N_i, \omega_i)_{i \leq \ell} \text{ eine } UH\text{-Resolution für } \mathcal{P}, N \text{ ist und } x^{\omega \tau} = x^\sigma \text{ für } \omega := \omega_0 \dots \omega_\ell \text{ und alle } x \in V.$$

Damit sind wir fertig; denn für $V = \{x_1, \dots, x_n\}$ ergibt (2) dann $x_i^{\omega \tau} = x_i^\sigma = t_i$ für $i = 1, \dots, n$, also (c). Zum induktiven Nachweis von (2) betrachte man den ersten Resolutionsschritt $Q_1 = HR(P'_0, Q_0)$ in \mathbf{B} . Seien $\omega_0, \rho_0, \tau_0, H$ nach Lemma 5.1 (mit $K_0 := P_0, K_1 := N_0 = N, \sigma_1 := \sigma$) so gewählt, dass $H \in U_\omega HR(P_0^{\rho_0}, N_0)$ und $H^{\tau_0} = Q_1$, sowie $x^{\omega_0 \tau_0} = x^\sigma$ für alle $x \in V$. Ist $\ell = 0$, also $Q_1 = \Box$, ist auch $H = \Box$ und (2) ist mit $\tau = \tau_0$ schon bewiesen. Sei nun $\ell > 0$. Für die H -Resolution $(P'_i, Q_i)_{1 \leq i \leq \ell}$ für \mathcal{P}', Q_1 , und für $V' := \text{var}\{x^{\omega_0} \mid x \in V\}$ gibt es dann nach Induktionsannahme ρ_i, N_i, ω_i für $i = 1, \dots, \ell$ und ein τ , so dass $(P_i^{\rho_i}, N_i, \omega_i)_{1 \leq i \leq \ell}$ eine UH -Resolution für \mathcal{P}, H ist und zugleich $y^{\omega_1 \dots \omega_\ell \tau} = y^{\tau_0}$ für alle $y \in V'$ (statt $Q_0 = N^\sigma$ ist hier jetzt $Q_1 = H^{\tau_0}$). Weil $\text{var } x^{\omega_0} \subseteq V'$ und $x^{\omega_0 \tau_0} = x^\sigma$ für $x \in V$ folgt hieraus

$$(3) \quad x^{\omega \tau} = (x^{\omega_0})^{\omega_1 \dots \omega_\ell \tau} = x^{\omega_0 \tau_0} = x^\sigma, \text{ für alle } x \in V.$$

Sicher ist $(P_i^{\rho_i}, N_i, \omega_i)_{i \leq \ell}$ eine UH -Resolution. Ferner ist wegen (3) zugleich auch $x_i^{\omega \tau} = x_i^\sigma$ für $i = 1, \dots, n$. Das beweist (2) und mithin (c). Damit wurde der Beweis des Hauptsatzes vollständig erbracht.

Kapitel 5

Elemente der Modelltheorie

Die Sätze von Löwenheim und Skolem wurden in der in **5.1** angegebenen Allgemeinheit zuerst von A. Tarski formuliert und bilden zusammen mit dem Kompaktheitssatz die Grundlage der um 1950 entstandenen und inzwischen weit gefächerten Modelltheorie. Hier werden die in der mathematischen Logik entwickelten Techniken mit den Konstruktionstechniken anderer Gebiete zum gegenseitigen Nutzen miteinander verbunden. Die folgenden Ausführungen geben diesbezüglich nur einen ersten Einblick, der z.B. in [CK] vertieft werden kann. Für weiterführende Themen wie z.B. die der saturierten Modelle, der Stabilitätstheorie und Verallgemeinerungen, oder der Modelltheorie anderer als elementarer Sprachen, muss auf die Spezialliteratur verwiesen werden, z.B. [Sa], [Sh], [Bu], [BF] und [Wag]. Eine recht anspruchsvolle Einführung in die Modelltheorie mit Literaturhinweisen gibt auch [Rot].

Modelltheoretische Kernbegriffe sind die der elementaren Äquivalenz und der elementaren Erweiterung. Diese Begriffe sind nicht nur theoretisch interessant, sondern haben vielfache Anwendungen für Modellkonstruktionen, z.B. in der Mengenlehre, in der Nichtstandard-Analysis und in der Algebra.

Vollständige axiomatisierbare Theorien sind entscheidbar, siehe **3.5**. Die Frage nach der Entscheidbarkeit und Vollständigkeit mathematischer Theorien und die Entwicklung scharfsinniger Methoden, um diese Eigenschaften zu beweisen, war stets ein Motor der Weiterentwicklung der mathematischen Logik. Von zahlreichen Methoden werden hier die wichtigsten vorgestellt: der Test von Vaught, das Ehrenfeucht-Spiel, Robinsons Methode der Modellvollständigkeit sowie die Quantorenelimination. Hierbei werden für kompliziertere Fälle, wie die Theorie der algebraisch bzw. reell abgeschlossenen Körper, modelltheoretische Kriterien entwickelt und angewandt. Aus Kapitel **3** benötigt man einiges für Anwendungen der Modelltheorie zur Lösung von Entscheidungsproblemen und aus Kapitel **4** nur den Begriff der Hornformel.

5.1 Elementare Erweiterungen

Schon in 3.3 hatten wir Nichtstandardmodelle mit einer Methode erhalten, die wir jetzt verallgemeinern. Für eine Sprache \mathcal{L} und eine Menge A bezeichne $\mathcal{L}A$ die aus \mathcal{L} durch Hinzufügen von neuen Konstantensymbolen \mathbf{a} für alle $a \in A$ entstehende Sprache. Das Symbol \mathbf{a} soll nur von a , nicht von A abhängen, so dass stets $\mathcal{L}A \subseteq \mathcal{L}B$ für $A \subseteq B$. Um die Niederschriften zu vereinfachen und weil Missverständnisse nicht zu befürchten sind, werden wir ab Satz 1.3 einfach nur a statt \mathbf{a} schreiben.

Sei \mathcal{B} eine \mathcal{L} -Struktur und $A \subseteq B$. Dann heie die $\mathcal{L}A$ -Expansion \mathcal{B}_A mit $\mathbf{a}^{\mathcal{B}_A} = a$ für $a \in A$ die *natürliche $\mathcal{L}A$ -Expansion von \mathcal{B}* . Für alle $\alpha = \alpha(\vec{x}) \in \mathcal{L}$ gilt dann

$$(1) \quad \mathcal{B} \models \alpha[\vec{a}] \Leftrightarrow \mathcal{B}_A \models \alpha(\vec{a}) \quad (\vec{a} \in A^n, \alpha(\vec{a}) = \alpha \frac{a_1}{x_1} \cdots \frac{a_n}{x_n}).$$

Offenbar ist jede Aussage aus $\mathcal{L}A$ von der Gestalt $\alpha_{\vec{x}}(\vec{a})$ mit geeignetem $\alpha(\vec{x}) \in \mathcal{L}$ und $\vec{a} \in A^n$. Für $\mathcal{B}_A \models \alpha_{\vec{x}}(\vec{a})$ werden wir später nur $\mathcal{B}_A \models \alpha(\vec{a})$ oder gar nur $\mathcal{B} \models \alpha(\vec{a})$ schreiben, d.h. zwischen \mathcal{B} und \mathcal{B}_A wird in der Bezeichnung nicht unterschieden wenn der Unterschied keine Rolle spielt. Man kann $\mathcal{B} \models \alpha(\vec{a})$ angesichts von (1) aber auch lesen als $\mathcal{B} \models \alpha[\vec{a}]$. Dies sollte z.B. geschehen in (ii) von Satz 1.3 auf Seite 134.

Für eine \mathcal{L} -Struktur \mathcal{A} mit dem Träger A enthält die natürliche $\mathcal{L}A$ -Expansion \mathcal{A}_A für jedes $a \in A$ ein neues Konstantensymbol, auch wenn einzelne Elemente von \mathcal{A} bereits einen Namen in \mathcal{L} besitzen. Die Menge aller variablenfreien Literale $\lambda \in \mathcal{L}A$ mit $\mathcal{A}_A \models \lambda$ heie das *Diagramm $D\mathcal{A}$* von \mathcal{A} . So enthält z.B. $D(\mathbb{R}, <)$ für alle $a, b \in \mathbb{R}$ die Aussagen $\mathbf{a} = \mathbf{b}$, $\mathbf{a} \neq \mathbf{b}$, $\mathbf{a} < \mathbf{b}$, $\mathbf{a} \not< \mathbf{b}$ je nachdem, ob tatsächlich $a = b$, $a \neq b$, $a < b$ oder $a \not< b$. Diagramme sind wichtig für viele Modellkonstruktionen.

Schon in 2.1 wurde darauf hingewiesen, dass der Begriff der Einbettung $\iota: \mathcal{A} \rightarrow \mathcal{B}$ (d.h. das Bild von \mathcal{A} unter ι ist eine isomorphe Kopie von \mathcal{A}) den Substrukturbegriff umfasst. Denn ist $\mathcal{A} \subseteq \mathcal{B}$, so ist $\iota = id_A$ eine triviale, die *identische* Einbettung von \mathcal{A} in \mathcal{B} . Mit Einbettbarkeit einer \mathcal{L}_0 -Struktur \mathcal{A} in eine \mathcal{L} -Struktur \mathcal{B} für den Fall $\mathcal{L}_0 \subseteq \mathcal{L}$ sei in diesem Kapitel stets die Einbettbarkeit von \mathcal{A} in das \mathcal{L}_0 -Redukt \mathcal{B}_0 von \mathcal{B} gemeint. In diesem Sinne ist z.B. die Gruppe \mathbb{Z} in den Körper \mathbb{Q} einbettbar. Wird in diesem Zusammenhang die Schreibweise $\mathcal{A} \subseteq \mathcal{B}$ benutzt, heit dies eigentlich $\mathcal{A} \subseteq \mathcal{B}_0$. Nach diesen Vorbemerkungen formulieren wir den

Satz 1.1. *Sei $\mathcal{L}_0 \subseteq \mathcal{L}$ und \mathcal{A} eine \mathcal{L}_0 -Struktur. Eine $\mathcal{L}A$ -Struktur \mathcal{B} erfüllt $D\mathcal{A}$ genau dann, wenn $\iota: a \mapsto \mathbf{a}^{\mathcal{B}}$ eine Einbettung von \mathcal{A} in \mathcal{B} darstellt.*

Beweis. \Rightarrow : Sei $\mathcal{B} \models D\mathcal{A}$ und $a, b \in A$, $a \neq b$. Dann ist $\mathbf{a} \neq \mathbf{b} \in D\mathcal{A}$, also $\mathcal{B} \models \mathbf{a} \neq \mathbf{b}$ und daher $\mathbf{a}^{\mathcal{B}} \neq \mathbf{b}^{\mathcal{B}}$. Folglich ist ι injektiv. Für $r \in L_0$ und alle $\vec{a} \in A^n$ gilt

$$\begin{aligned} r^{\mathcal{A}}\vec{a} \Leftrightarrow r\vec{a} \in D\mathcal{A} &\Leftrightarrow \mathcal{B} \models r\vec{a} \quad (\text{weil } \mathcal{B} \models D\mathcal{A}) \\ &\Leftrightarrow r^{\mathcal{B}}\iota\vec{a} \quad (\text{weil } \iota\vec{a} = (\iota a_0, \dots, \iota a_n)). \end{aligned}$$

Ebenso ergibt sich $\iota f^A \vec{a} = f^B \iota \vec{a}$; denn für beliebige $\vec{a} \in A^n$ und $b \in A$ haben wir $f^A \vec{a} = b \Leftrightarrow f \vec{a} = \mathbf{b} \in D\mathcal{A} \Leftrightarrow \mathcal{B} \models f \vec{a} = \mathbf{b} \Leftrightarrow f^B \iota \vec{a} = \iota b$. Also ist ι eine Einbettung. \Leftarrow : Für variablenfreie Terme t von $\mathcal{L}_0 A$ beweist man leicht $\iota t^A = t^B$, wobei hier und anderswo kurz t^A für t^{A_A} und t^B für t^{B_A} geschrieben wird. Weil ι injektiv ist, folgt für variablenfreie Gleichungen aus $\mathcal{L}_0 A$

$$t_1 = t_2 \in D\mathcal{A} \Leftrightarrow t_1^A = t_2^A \Leftrightarrow \iota t_1^A = \iota t_2^A \Leftrightarrow t_1^B = t_2^B \Leftrightarrow \mathcal{B} \models t_1 = t_2.$$

Völlig analog zeigt man $t_1 \neq t_2 \in D\mathcal{A} \Leftrightarrow \mathcal{B} \models t_1 \neq t_2$, und auf die gleiche Weise behandelt man Primaussagen der Gestalt $r\vec{t}$. Das beweist $\mathcal{B} \models D\mathcal{A}$. \square

Korollar 1.2. *Eine Struktur \mathcal{A} ist in jedes $\mathcal{B} \models D\mathcal{A}$ isomorph einbettbar. Im Falle $A \subseteq B$ ist sogar $\mathcal{A} \subseteq \mathcal{B}$.*

Denn nach dem Satz mit $\mathcal{L}_0 = \mathcal{L}$ leistet $\iota: a \mapsto \mathbf{a}^B$ das Verlangte. Für $A \subseteq B$ ist ι die identische Abbildung, daher $\mathcal{A} \subseteq \mathcal{B}$. Versteht man unter einem *Primmodell* für eine Theorie T ein solches, das in jedes T -Modell einbettbar ist, so besagt das Korollar gerade, dass \mathcal{A}_A ein Primmodell für die von $D\mathcal{A}$ erzeugte Theorie ist. Wir verwenden diesen Begriff nur in diesem Sinne¹⁾. Das Korollar wird im Verlaufe der Ausführungen sehr oft und ohne expliziten Verweis verwendet.

Den wohl wichtigsten Begriff der Modelltheorie, für den ein erstes Beispiel auf der nächsten Seite angegeben wird, erfassen wir mit folgender

Definition. Seien \mathcal{A}, \mathcal{B} \mathcal{L} -Strukturen. \mathcal{A} heißt eine *elementare Substruktur* von \mathcal{B} , und \mathcal{B} heißt *elementare Erweiterung* von \mathcal{A} , symbolisch $\mathcal{A} \preceq \mathcal{B}$, wenn $A \subseteq B$ und

$$(2) \quad \mathcal{A} \models \alpha[\vec{a}] \Leftrightarrow \mathcal{B} \models \alpha[\vec{a}], \text{ für alle } \alpha = \alpha(\vec{x}) \in \mathcal{L} \text{ und } \vec{a} \in A^n.$$

$\mathcal{A} \preceq \mathcal{B}$ impliziert $\mathcal{A} \subseteq \mathcal{B}$ (Satz 2.3.2) und natürlich auch $\mathcal{A} \equiv \mathcal{B}$. Jedoch bedeutet $\mathcal{A} \preceq \mathcal{B}$ mehr als $\mathcal{A} \subseteq \mathcal{B}$ und $\mathcal{A} \equiv \mathcal{B}$. So gilt z.B. für $\mathcal{A} = (\mathbb{N}_+, <)$ mit $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ und $\mathcal{B} = (\mathbb{N}, <)$ sicher $\mathcal{A} \subseteq \mathcal{B}$, und weil $\mathcal{A} \simeq \mathcal{B}$, ist auch $\mathcal{A} \equiv \mathcal{B}$. Aber $\mathcal{A} \preceq \mathcal{B}$ ist falsch, weil z.B. die Aussage $\exists x x < \mathbf{1}$ in \mathcal{B}_A , nicht aber in \mathcal{A}_A gilt.

Nennt man $D_{el}\mathcal{A} := \{\alpha \in \mathcal{L}A^0 \mid \mathcal{A}_A \models \alpha\}$ das *elementare Diagramm* von \mathcal{A} , ist $\mathcal{A} \preceq \mathcal{B}$ auch gleichwertig mit $A \subseteq B$ und $\mathcal{B}_A \models D_{el}\mathcal{A}$. (2) ist nämlich schon erfüllt, wenn dort \Leftrightarrow durch \Rightarrow (oder durch \Leftarrow) ersetzt wird. Ferner ist (2) nach (1) gleichwertig mit $\mathcal{A}_A \models \alpha(\vec{a}) \Leftrightarrow \mathcal{B}_A \models \alpha(\vec{a})$, und weil jede Aussage aus $\mathcal{L}A$ für passendes $\alpha(\vec{x}) \in \mathcal{L}$ die Gestalt $\alpha(\vec{a})$ hat, ist $\mathcal{A} \preceq \mathcal{B}$ auch gekennzeichnet durch $A \subseteq B$ und $\mathcal{A}_A \equiv \mathcal{B}_A$ (Elementaräquivalenz in $\mathcal{L}A$).

Von großem Nutzen für die Angabe von nichttrivialen Beispielen für $\mathcal{A} \preceq \mathcal{B}$ und auch anderswo wird sich folgender Satz erweisen:

¹⁾Dieser Begriff muss unterschieden werden von dem eines *elementaren* Primmodells für T , d.h. \mathcal{A} ist in jedes $\mathcal{B} \models T$ im Sinne von Übung 2 elementar einbettbar.

Satz 1.3 (Tarskis Kriterium). Für Strukturen \mathcal{A}, \mathcal{B} mit $\mathcal{A} \subseteq \mathcal{B}$ sind gleichwertig

- (i) $\mathcal{A} \preceq \mathcal{B}$,
- (ii) $\mathcal{B} \models \exists y \varphi(\vec{a}, y) \Rightarrow \mathcal{B} \models \varphi(\vec{a}, a)$ für ein $a \in A$ ($\varphi(\vec{x}, y) \in \mathcal{L}$, $\vec{a} \in A^n$).

Beweis. (i) \Rightarrow (ii): Sei $\mathcal{A} \preceq \mathcal{B}$ und $\mathcal{B} \models \exists y \varphi(\vec{a}, y)$, so dass auch $\mathcal{A} \models \exists y \varphi(\vec{a}, y)$. Dann ist gewiss $\mathcal{A} \models \varphi(\vec{a}, a)$ für ein $a \in A$. Wegen $\mathcal{A} \preceq \mathcal{B}$ gilt dann aber auch $\mathcal{B} \models \varphi(\vec{a}, a)$.
(ii) \Rightarrow (i): Wegen $\mathcal{A} \subseteq \mathcal{B}$ gilt (2) sicher für Primformeln, und auch die Induktionsschritte über \wedge, \neg sind klar. Einer Betrachtung bedarf nur der Quantorenschritt:

$$\begin{aligned} \mathcal{A} \models \forall y \alpha(\vec{a}, y) &\Leftrightarrow \mathcal{A} \models \alpha(\vec{a}, a) \text{ für alle } a \in A \\ &\Leftrightarrow \mathcal{B} \models \alpha(\vec{a}, a) \text{ für alle } a \in A \quad (\text{Induktionsannahme}) \\ &\Leftrightarrow \mathcal{B} \models \forall y \alpha(\vec{a}, y) \quad (\text{Begründung unten}). \end{aligned}$$

Die Richtung \Rightarrow in der letzten Äquivalenz folgt so: Annahme $\mathcal{B} \not\models \forall y \alpha(\vec{a}, y)$, d.h. $\mathcal{B} \models \exists y \neg \alpha(\vec{a}, y)$. Mit $\varphi(\vec{x}, y) := \neg \alpha(\vec{x}, y)$ ergibt (ii) dann $\mathcal{B} \models \neg \alpha(\vec{a}, a)$ für gewisses $a \in A$, im Widerspruch zu $\mathcal{B} \models \alpha(\vec{a}, a)$ für alle $a \in A$. \square

Folgender Satz liefert auf relativ einfache Weise interessante Beispiele für $\mathcal{A} \preceq \mathcal{B}$:

Satz 1.4. Sei $\mathcal{A} \subseteq \mathcal{B}$. Für beliebige $a_1, \dots, a_n \in A$ und $b \in B$ gebe es einen Automorphismus $\iota: \mathcal{B} \rightarrow \mathcal{B}$ mit $\iota a_i = a_i$ für $i = 1, \dots, n$ und $\iota b \in A$. Dann ist $\mathcal{A} \preceq \mathcal{B}$.

Beweis. Es genügt, Bedingung (ii) in Satz 1.3 zu verifizieren: Ist $\mathcal{B} \models \exists y \varphi(\vec{a}, y)$, also $\mathcal{B} \models \varphi(\vec{a}, b)$ für ein $b \in B$, folgt $\mathcal{B} \models \varphi(\iota \vec{a}, \iota b)$ nach Satz 2.3.4, und wegen $\iota \vec{a} = \vec{a}$ daher $\mathcal{B} \models \varphi(\vec{a}, a)$ mit $a = \iota b \in A$, womit (ii) nachgewiesen ist. \square

Beispiel. Man zeigt leicht, dass für gegebene $a_1, \dots, a_n \in \mathbb{Q}$ und $b \in \mathbb{R}$ ein Automorphismus von $(\mathbb{R}, <)$ existiert, der b in eine rationale Zahl überführt und a_1, \dots, a_n festlässt. Also ist $(\mathbb{Q}, <) \preceq (\mathbb{R}, <)$. Insbesondere ist damit $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$.

Satz 1.4 ist natürlich nur verwendbar, wenn \mathcal{B} „viele Automorphismen“ hat. Ein weniger einfaches, in 5.5 näher ausgeführtes Beispiel einer elementaren Erweiterung ist folgendes: Es ist $\mathcal{A} \preceq \mathcal{C}$, wobei \mathcal{A} den Körper der algebraischen Zahlen und \mathcal{C} den Körper der komplexen Zahlen bezeichnet. Der Träger von \mathcal{A} besteht aus allen komplexen Zahlen, die Nullstellen von (normierten) Polynomen mit rationalen Koeffizienten sind, wozu z.B. die Zahl π nicht gehört. Ferner ist $\mathcal{A}_r \preceq \mathcal{R}$. Dabei sei \mathcal{A}_r der geordnete Körper aller reellen algebraischen Zahlen und \mathcal{R} der aller reellen Zahlen. Beide Körper sind reell abgeschlossen. Mehr hierzu auf Seite 153.

Bevor wir fortfahren, wollen wir uns mit transfiniten Kardinalzahlen etwas vertraut machen. Man kann nicht nur endlichen, sondern beliebigen Mengen M jeweils ein z.B. mit $|M|$ bezeichnetes mengentheoretisches Objekt so zuordnen, dass

- (3) $M \sim N \Leftrightarrow |M| = |N|$ (\sim bedeutet gleichmächtig, siehe Seite 87).

$|M|$ heißt die *Kardinalzahl* oder *Mächtigkeit* von M . Für endliches M ist $|M|$ eine natürliche Zahl, die Anzahl der Elemente von M ; für unendliches M heißt $|M|$ eine *transfinite* Kardinalzahl. Es ist an dieser Stelle unwichtig, wie $|M|$ im Einzelnen erklärt ist; wesentlich sind nur (4),(5), aus denen sich (6) und (7) leicht ergeben.

- (4) Die Kardinalzahlen sind der Größe nach geordnet und sogar wohlgeordnet, d.h. jede nichtleere Kollektion von ihnen besitzt ein kleinstes Element. Dabei sei $|M| \leq |N|$, wenn eine Injektion von M nach N existiert,²⁾
- (5) Es gilt $|M \cup N| = |M \times N| = \max\{|M|, |N|\}$ für beliebige nichtleere Mengen M, N , von denen mindestens eine unendlich ist.

Danach hat $\bigcup_{n>0} M^n$ (die Menge aller nichtleeren endlichen Folgen von Elementen aus M) für unendliches M dieselbe Mächtigkeit wie M . Kurzum,

- (6) $|M^*| = |M|$ für $M^* = \bigcup_{n>0} M^n$ (M unendlich).

Denn $|M^1| = |M|$, und die Annahme $|M^n| = |M|$ ergibt $|M^{n+1}| = |M^n \times M| = |M|$ nach (5). Also $|M^n| = |M|$ für alle n , daher $|M^*| = |\bigcup_{n>0} M^n| = |M \times \mathbb{N}| = |M|$. Ähnlich erhält man aus (4),(5) für jede transfinite Kardinalzahl κ leicht auch

- (7) Ist $|A_i| \leq \kappa$ für alle $i \in \mathbb{N}$, so ist auch $|\bigcup_{i \in \mathbb{N}} A_i| \leq \kappa$.

Die mit \aleph_0 bezeichnete kleinste transfinite Kardinalzahl ist die der abzählbar unendlichen Mengen. Die nächst größere heißt \aleph_1 . Die Kardinalzahl 2^{\aleph_0} von $\mathfrak{P}\mathbb{N}$ ist gleich der Mächtigkeit von \mathbb{R} . Sicher ist $\aleph_0 < 2^{\aleph_0}$, also $\aleph_1 \leq 2^{\aleph_0}$. Die *Kontinuumshypothese* (CH) besagt $2^{\aleph_0} = \aleph_1$. CH ist nachweislich unabhängig in ZFC (siehe z.B. [Ku]), d.h. wir wissen nicht, ob $|\mathbb{R}| = \aleph_1$ zutrifft. Zwar gibt es über ZFC hinausführende Axiome, die eine Entscheidung für oder gegen CH implizieren, aber keines dieser Axiome ist plausibel genug um für „wahr“ gehalten zu werden.

Der folgende Satz verallgemeinert wesentlich den Satz 3.4.1. Für $|\mathcal{B}| \geq |\mathcal{L}|$ garantiert er die Existenz einer Struktur $\mathcal{A} \preccurlyeq \mathcal{B}$ (speziell $\mathcal{A} \equiv \mathcal{B}$) derart, dass $|\mathcal{A}| \leq |\mathcal{L}|$.

Satz 1.5 (Satz von Löwenheim-Skolem abwärts). *Es sei \mathcal{B} eine \mathcal{L} -Struktur mit $|\mathcal{L}| \leq |\mathcal{B}|$ und $A_0 \subseteq B$ beliebig. Dann hat \mathcal{B} eine elementare Substruktur \mathcal{A} einer Kardinalzahl $\leq \max\{|A_0|, |\mathcal{L}|\}$ mit $A_0 \subseteq A$.*

Beweis. Wir konstruieren eine Folge $A_0 \subseteq A_1 \subseteq \dots \subseteq B$ wie folgt. Sei A_k gegeben. Für jedes $\alpha = \alpha(\vec{x}, y)$ und $\vec{a} \in A_k^n$ mit $\mathcal{B} \models \exists y \alpha(\vec{a}, y)$ wählen wir ein $b \in B$ mit $\mathcal{B} \models \alpha(\vec{a}, b)$ und fügen b zu A_k hinzu. Auf diese Weise erhalten wir A_{k+1} . Ist z.B. α die Formel $f\vec{x} = y$, ist gewiss $\mathcal{B} \models \exists y f\vec{a} = y$, was leicht $f^{\mathcal{B}}\vec{a} \in A_{k+1}$ ergibt. $A := \bigcup_{k \in \mathbb{N}} A_k$ ist demnach unter den Operationen von \mathcal{B} abgeschlossen, bestimmt

²⁾Mit dieser Definition ist $|M| \leq |N|$ & $|N| \leq |M| \Rightarrow |M| = |N|$ beweisbar, sogar ohne Auswahlaxiom. Dies besagt der *Satz von Cantor-Bernstein*. Für eine Struktur \mathcal{A} sei stets $|\mathcal{A}| := |A|$.

also eine Substruktur $\mathcal{A} \subseteq \mathcal{B}$. Wir zeigen $\mathcal{A} \preceq \mathcal{B}$ durch den Nachweis von (ii) in Satz 1.3. Für $\alpha = \alpha(\vec{x}, y)$ und $\mathcal{B} \models \exists y \alpha(\vec{a}, y)$ mit $\vec{a} \in A^n$ ist sicher $\vec{a} \in A_k^n$ für ein k . Daher gibt es ein $a \in A_{k+1}$, also $a \in A$, mit $\mathcal{B} \models \alpha(\vec{a}, a)$. Das zeigt (ii). Es verbleibt der Nachweis von $|A| \leq \kappa := \max\{|A_0|, |\mathcal{L}|\}$. Da es höchstens κ viele Formeln und κ viele endliche Folgen von Elementen aus A_0 gibt, werden bei der Konstruktion von A_1 höchstens κ viele neue Elemente zu A_0 hinzugefügt. Also $|A_1| \leq \kappa$. Analog ist $|A_k| \leq \kappa$ für jedes $k > 0$. (7) ergibt damit $|\bigcup_{k \in \mathbb{N}} A_k| \leq \kappa$. \square

Kombiniert mit dem Kompaktheitssatz, liefert dieser Satz den

Satz 1.6 (Satz von Löwenheim-Skolem aufwärts). *Sei die \mathcal{L} -Struktur \mathcal{C} unendlich und κ eine Kardinalzahl $\geq |\mathcal{C}|, |\mathcal{L}|$. Dann gibt es ein $\mathcal{A} \succ \mathcal{C}$ mit $|\mathcal{A}| = \kappa$.*

Beweis. Sei $D \supseteq C$ mit $|D| = \kappa$. Dann folgt aus (6) leicht $|\mathcal{L}D| = \kappa$, denn das Alphabet von $\mathcal{L}D$ hat die Mächtigkeit κ . Weil $|C| \geq \aleph_0$, hat nach dem Kompaktheitssatz $D_{el}\mathcal{C} \cup \{c \neq d \mid c, d \in D, c \neq d\}$ ein Modell \mathcal{B} . Da $d \mapsto d^{\mathcal{B}}$ injektiv ist, darf man $d^{\mathcal{B}} = d$ für alle $d \in D$, also $D \subseteq B$ annehmen. Nach Satz 1.5, mit $\mathcal{L}D$ für \mathcal{L} , und D für A_0 , gibt es ein $\mathcal{A} \preceq \mathcal{B}$ mit $D \subseteq A$ und $\kappa \leq |D| \leq |A| \leq \max\{|\mathcal{L}D|, |D|\} = \kappa$, also $|A| = \kappa$. Aus $C \subseteq D$ und $\mathcal{A} \equiv_{\mathcal{L}D} \mathcal{B} \models D_{el}\mathcal{C}$ folgt $\mathcal{A} \models D_{el}\mathcal{C}$. Da auch $C \subseteq A$, ist \mathcal{A} (genauer das \mathcal{L} -Redukt von \mathcal{A}) elementare Erweiterung von \mathcal{C} . \square

Nach diesen Sätzen hat speziell eine abzählbare Theorie T mit wenigstens einem unendlichen Modell auch Modelle in jeder unendlichen Mächtigkeit. Außerdem gilt z.B. $\vdash_T \alpha$ schon dann, wenn nur $\mathcal{A} \models \alpha$ für alle T -Modelle \mathcal{A} einer einzigen unendlichen Kardinalzahl κ , vorausgesetzt T hat nur unendliche Modelle. Dann ist nämlich jedes T -Modell zu einem solchen der Mächtigkeit κ elementar-äquivalent.

Übungen

1. Seien $\mathcal{A} \preceq \mathcal{C}$ und $\mathcal{B} \preceq \mathcal{C}$, sowie $A \subseteq B$. Man beweise $\mathcal{A} \preceq \mathcal{B}$.
2. Eine Einbettung $\iota: \mathcal{A} \rightarrow \mathcal{B}$ heißt *elementar*, wenn $\iota\mathcal{A} \preceq \mathcal{B}$, wobei $\iota\mathcal{A}$ das Bild von \mathcal{A} unter ι bezeichnet. Man zeige ähnlich wie Satz 1.1: Eine $\mathcal{L}\mathcal{A}$ -Struktur \mathcal{B} ist Modell von $D_{el}\mathcal{A}$ genau dann, wenn \mathcal{A} in \mathcal{B} elementar einbettbar ist.
3. Seien a_1, \dots, a_n rational und $b \in \mathbb{R}$. Man zeige, es gibt einen Automorphismus von $(\mathbb{R}, <)$, der b in eine rationale Zahl überführt und alle a_i fest lässt.
4. Sei $\mathcal{A} \equiv \mathcal{B}$. Man zeige, es gibt eine Struktur \mathcal{C} , in welche \mathcal{A}, \mathcal{B} beide elementar einbettbar sind.
5. Sei \mathcal{A} eine von $E \subseteq A$ erzeugte \mathcal{L} -Struktur und \mathcal{T}_E die Menge der Grundterme in $\mathcal{L}E$. Man zeige (a) zu jedem $a \in A$ gibt es ein $t \in \mathcal{T}_E$ mit $a = t^{\mathcal{A}}$, (b) ist $\mathcal{A} \models T$ und $\alpha \in \mathcal{L}E$, gilt $D\mathcal{A} \vdash_T \alpha \Rightarrow D_E\mathcal{A} \vdash_T \alpha$, mit $D_E\mathcal{A} := D\mathcal{A} \cap \mathcal{L}E$.

5.2 Vollständige und κ -kategorische Theorien

Nach 3.3 ist eine Theorie T vollständig, wenn sie konsistent ist und keine echte konsistente Erweiterungstheorie in ihrer Sprache mehr hat. Gleichwertige Formulierungen, deren Nützlichkeit von der jeweiligen Situation abhängt, liefert

Satz 2.1. *Für eine konsistente Theorie T sind folgende Bedingungen äquivalent:*³⁾

- (i) T ist vollständig,
- (ii) $T = Th\mathcal{A}$ für beliebiges $\mathcal{A} \models T$,
- (iii) $\mathcal{A} \equiv \mathcal{B}$ für alle $\mathcal{A}, \mathcal{B} \models T$,
- (iv) $\alpha \in T$ oder $\neg\alpha \in T$ für jedes $\alpha \in \mathcal{L}^0$.

Beweis. (i) \Rightarrow (ii): Da $Th\mathcal{A}$ eine konsistente Erweiterungstheorie von T ist, muss $T = Th\mathcal{A}$ sein. (ii) \Rightarrow (iii): Für $\mathcal{A}, \mathcal{B} \models T$ ist $Th\mathcal{A} = T = Th\mathcal{B}$ nach (ii), und damit $\mathcal{A} \equiv \mathcal{B}$. (iii) \Rightarrow (iv): Sei $\not\models_T \alpha$. Dann ist $T, \neg\alpha$ konsistent, also gibt es ein $\mathcal{B} \models T$ mit $\mathcal{B} \models \neg\alpha$, und in jedem T -Modell \mathcal{A} gilt $\neg\alpha$, weil $\mathcal{A} \equiv \mathcal{B}$. Deshalb folgt $\vdash_T \neg\alpha$. (iv) \Rightarrow (i): Sei $T' \supset T$ und etwa $\alpha \in T' \setminus T$, so dass $\vdash_T \neg\alpha$ und mithin auch $\vdash_{T'} \neg\alpha$. Dann ist T' wegen $\vdash_{T'} \alpha$ aber inkonsistent und T daher vollständig. \square

Man beachte, dass eine vollständige Theorie T noch nicht maximal konsistent in ganz \mathcal{L} sein muss. So gilt in der Regel weder $\vdash_T x = y$ noch $\vdash_T x \neq y$.

Wir werden unterschiedliche Methoden vorstellen, mit denen sich die vermutete Vollständigkeit einer Theorie bestätigen lässt. Die Vollständigkeitsfrage ist aus mehreren Gründen wichtig. Zum Beispiel ist eine vollständige axiomatisierbare Theorie nach Satz 3.5.2 entscheidbar, wie immer auch die Vollständigkeit erschlossen wurde.

Eine elementare Theorie mit wenigstens einem unendlichen Modell hat, selbst wenn sie vollständig ist, sehr viele Modelle. Denn nach Satz 1.6 besitzt sie immer auch Modelle beliebig großer Mächtigkeiten. Es kann aber sein, dass alle ihre Modelle einer vorgegebenen endlichen oder unendlichen Kardinalzahl κ isomorph sind. Diesem Umstand trägt die folgende Definition Rechnung.

Definition. Eine Theorie T heißt *κ -kategorisch*, wenn es bis auf Isomorphie nur genau ein T -Modell der Mächtigkeit κ gibt.

Beispiel 1. Die Theorie $T_{aut=}$ der Tautologien in $\mathcal{L}_=$ ist κ -kategorisch für jede Kardinalzahl κ ; denn κ -mächtige Modelle \mathcal{A}, \mathcal{B} sind nackte Mengen und daher trivial isomorph, mit einer beliebigen Bijektion von A auf B .

Die Theorie DO der *dicht geordneten Mengen* entstehe aus der in 2.3 formalisierten Theorie der geordneten Mengen durch Hinzufügen der Axiome

$$\exists x \exists y x \neq y \quad ; \quad \forall xy \exists z (x < y \rightarrow x < z \wedge z < y).$$

³⁾ Diese Bedingungen sind auch äquivalent (sie gelten alle), wenn man die inkonsistente Theorie zu den vollständigen rechnet, was gelegentlich von Vorteil sein kann, hier aber nicht geschieht.

Jede dicht geordnete Menge ist offenbar unendlich. DO kann durch Hinzufügen der Axiome $L := \exists x \forall y (x \leq y)$ und $R := \exists x \forall y (y \leq x)$ zur Theorie DO_{11} der dicht geordneten Mengen mit Randelementen erweitert werden. Ersetzt man hier R durch $\neg R$, entsteht die Theorie DO_{10} der dicht geordneten Mengen mit linkem aber ohne rechtes Randelement. Entsprechend bezeichne DO_{01} die Theorie mit rechtem und ohne linkes, sowie DO_{00} die der dichten Ordnungen ohne Randelemente. Alle vier zuletzt genannten Theorien sind \aleph_0 -kategorisch. Wir erbringen hier den Nachweis für DO_{00} in folgendem Beispiel nach einer auf Cantor zurückgehenden Methode.

Beispiel 2. DO_{00} ist \aleph_0 -kategorisch. Seien $A = \{a_0, a_1, \dots\}$ und $B = \{b_0, b_1, \dots\}$ abzählbare DO_{00} -Modelle – geordnete Mengen werden hier einfach durch ihre Träger bezeichnet. Die Abbildung f_0 sei definiert durch $f_0 a_0 = b_0$, also $\text{dom } f_0 = \{a_0\}$. Sei im n -ten Konstruktionsschritt eine Abbildung f_n aus A in B mit endlichem Definitionsbereich so definiert, dass $a < a' \Leftrightarrow f_n a < f_n a'$, für alle $a, a' \in \text{dom } f_n$, ein sogenannter *partieller Isomorphismus* von A nach B . Ferner sei a_m das Element mit minimalem Index aus $A \setminus \text{dom } f_n$, und $b \in B \setminus \text{ran } f_n$ sei so gewählt, dass auch $f'_n = f_n \cup \{(a_m, b)\}$ ein partieller Isomorphismus ist. Das ist möglich wegen der Dichtheit von B . Sodann wähle man für $b_m \in B \setminus \text{ran } f'_n$ mit minimalem m ein $a \in A \setminus \text{dom } f'_n$ so, dass auch $f_{n+1} = f'_n \cup \{(a, b_m)\}$ ein partieller Isomorphismus ist. Man sieht dann leicht, dass $f = \bigcup_{n \in \mathbb{N}} f_n$ ein Isomorphismus von A auf B ist. Denn obige „hin- und her“-Konstruktion sorgt sowohl für $a_n \in \text{dom } f_n$ als auch für $b_n \in \text{ran } f_n$, was offensichtlich $\text{dom } f = A$ und $\text{ran } f = B$ zur Folge hat.

Beispiel 3. Die Nachfolgertheorie T_{suc} in $\mathcal{L}\{0, S\}$ habe die Axiome

$$\forall x (0 \neq Sx), \quad \forall xy (Sx = Sy \rightarrow x = y), \quad (\forall x \neq 0) \exists y (x = Sy),$$

$$\forall x_0 \cdots x_n (\bigwedge_{i < n} Sx_i = x_{i+1} \rightarrow x_0 \neq x_n) \quad (n = 1, 2, \dots, \text{ es gibt keine „Kreise“}).$$

T_{suc} ist nicht \aleph_0 -, wohl aber \aleph_1 -kategorisch. Jedes $\mathcal{A} \models T_{\text{suc}}$ mit $|\mathcal{A}| = \aleph_1$ besteht nämlich bis auf Isomorphie aus dem (abzählbaren) Standardmodell $(\mathbb{N}, 0, S)$ und \aleph_1 vielen „Fäden“ vom Isomorphietyp (\mathbb{Z}, S) mit $S: z \mapsto z + 1$. Wäre deren Anzahl $\leq \aleph_0$, so wäre auch das Modell abzählbar. Damit leuchtet ein, dass sich je zwei T_{suc} -Modelle der Mächtigkeit \aleph_1 isomorph aufeinander abbilden lassen.

Beispiel 4. Ein berühmtes Beispiel für \aleph_1 -Kategorizität ist die Theorie ACF_p der a.a. Körper gegebener Charakteristik p ($= 0$ oder eine Primzahl). Auf einen Beweis verzichten wir, weil ACF_p in 5.5 auf eine andere Art analysiert wird.

Auch die auf Seite 152 genauer beschriebene Theorie $T_{V\mathbb{Q}}$ der \mathbb{Q} -Vektorräume ist \aleph_1 -kategorisch. Denn ein \mathbb{Q} -Vektorraum der Mächtigkeit \aleph_1 hat eine Basis derselben Mächtigkeit. Also gibt es bis auf Isomorphie nur einen solchen Vektorraum.

Es lässt sich unschwer beweisen, dass in den Beispielen 3 und 4 κ -Kategorizität für jede Kardinalzahl $\kappa > \aleph_0$ vorliegt. Dies ist kein Zufall. Es gilt nämlich der

Satz von Morley. *Ist eine abzählbare Theorie T κ -kategorisch für ein $\kappa > \aleph_0$, so gilt dasselbe für alle $\kappa > \aleph_0$.*

Der Beweis erfordert umfangreiche Hilfsmittel und muss hier übergangen werden. So gut wie keine Mühe kostet hingegen der Beweis von

Satz 2.2 (Kriterium von Vaught). *Eine abzählbare konsistente Theorie T ohne endliche Modelle ist vollständig, falls sie κ -kategorisch ist für ein gewisses κ .*

Beweis. Sicher ist $\kappa \geq \aleph_0$, denn T hat keine endlichen Modelle. Angenommen T ist unvollständig. Man wähle ein $\alpha \in \mathcal{L}^0$ mit $\not\models_T \alpha$ und $\not\models_T \neg\alpha$. Dann sind T, α und $T, \neg\alpha$ konsistent. Da die Modelle von T, α bzw. $T, \neg\alpha$ unendlich sind, haben diese Formelmengen nach Satz 1.5 abzählbare, und nach Satz 1.6 auch Modelle \mathcal{A} bzw. \mathcal{B} der Kardinalzahl κ . Wegen $\mathcal{A}, \mathcal{B} \models T$ ist nach Voraussetzung $\mathcal{A} \simeq \mathcal{B}$ und damit $\mathcal{A} \equiv \mathcal{B}$. Das aber widerspricht $\mathcal{A} \models \alpha$ und $\mathcal{B} \models \neg\alpha$. \square

Beispiel 5. (a) Die Theorie DO_{00} der dicht geordneten Mengen ohne Randelemente hat nur unendliche Modelle und ist nach Beispiel 2 \aleph_0 -kategorisch und demzufolge vollständig (was $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$ noch einmal bestätigt). Dasselbe gilt für alle DO_{ij} (Übung 1), so dass $\mathcal{A} \equiv \mathcal{B}$ für dicht geordnete \mathcal{A}, \mathcal{B} genau dann, wenn für \mathcal{A}, \mathcal{B} „dieselbe Randsituation“ vorliegt. Die $\text{DO}_{i,j}$ sind als vollständige axiomatisierbare Theorien entscheidbar. Dasselbe gilt nach Übung 3 in 3.5 daher auch für DO ⁴⁾.

(b) Die Nachfolgertheorie T_{suc} ist \aleph_1 -kategorisch und hat nur unendliche Modelle. Also ist sie vollständig und als axiomatisierbare Theorie damit entscheidbar.

(c) Nach Beispiel 4 ist ACF_p \aleph_1 -kategorisch. Also ist diese Theorie vollständig und als axiomatisierbare Theorie auch entscheidbar. Dieses bedeutsame Resultat werden wir in 5.5 auf eine andere Art vollständig beweisen.

Die Modellklassen von Aussagen heißen *elementare Klassen*. Dazu rechnen dann auch die Modellklassen endlich axiomatisierbarer elementarer Theorien. Für eine beliebige Theorie T ist $\text{Md } T = \bigcap_{\alpha \in T} \text{Md } \alpha$ ein Durchschnitt elementarer Klassen, auch eine Δ -*elementare Klasse* genannt. So ist die Klasse aller Körper elementar und die aller a.a. Körper ist Δ -elementar. Die Klasse aller endlichen Körper hingegen ist nicht Δ -elementar, denn deren Theorie hat offenbar auch unendliche Modelle.

Die Modellklassen vollständiger Theorien heißen *elementare Typen*. $\text{Md } T$ ist die Vereinigung der zu den Vervollständigungen von T gehörenden elementaren Typen. So hat z.B. DO nur die vier Vervollständigungen DO_{ij} , die durch die „Randsituation“ bestimmt sind, d.h. durch diejenigen der Aussagen $\text{L}, \text{R}, \neg\text{L}, \neg\text{R}$, die in der jeweiligen Vervollständigung gelten. In diesem Falle z.B. liefert der folgende Satz genaue Informationen über die elementaren Klassen dicht geordneter Mengen.

⁴⁾ Sogar die Theorie aller linearen Ordnungen ist entscheidbar (Ehrenfeucht), und damit jede ihrer endlichen Erweiterungen; nur ist der Beweis ungleich schwieriger als für DO .

Sei $X \subseteq \mathcal{L}$ nichtleer und T eine Theorie. $\langle X \rangle$ bezeichne die auch von T abhängige Menge aller Formeln, die in T zu Booleschen Kombinationen von Formeln aus X äquivalent sind. Stets sind $\top, \perp \in \langle X \rangle$, weil z.B. $\top \equiv_T \varphi \vee \neg\varphi$ für $\varphi \in X$. Damit ist stets $T \subseteq \langle X \rangle$. Wir nennen $X \subseteq \mathcal{L}^0$ eine *Boolesche Basis für \mathcal{L}^0 modulo T* , wenn $\langle X \rangle = \mathcal{L}^0$, d.h. wenn jede Aussage zu einer Booleschen Kombination von Formeln aus X in T äquivalent ist. $\mathcal{A} \equiv_X \mathcal{B}$ bedeute, dass $\mathcal{A} \models \alpha \Leftrightarrow \mathcal{B} \models \alpha$, für alle $\alpha \in X$.

Satz 2.3 (Basissatz für Aussagen). *Sei T eine Theorie und $X \subseteq \mathcal{L}^0$ derart, dass $\mathcal{A} \equiv_X \mathcal{B} \Rightarrow \mathcal{A} \equiv \mathcal{B}$, für alle $\mathcal{A}, \mathcal{B} \models T$ ⁵⁾. Dann ist X Boolesche Basis für \mathcal{L}^0 in T .*

Beweis. Sei $\alpha \in \mathcal{L}^0$ und $Y_\alpha := \{\beta \in \langle X \rangle \mid \alpha \vdash_T \beta\}$. Wir behaupten (a) $Y_\alpha \vdash_T \alpha$. Andernfalls sei $\mathcal{A} \models T, Y_\alpha, \neg\alpha$. Dann ist $T_X \mathcal{A} := \{\gamma \in \langle X \rangle \mid \mathcal{A} \models \gamma\} \vdash_T \neg\alpha$; denn für beliebiges $\mathcal{B} \models T_X \mathcal{A}$ ist $\mathcal{B} \equiv_X \mathcal{A}$ und damit $\mathcal{B} \equiv \mathcal{A}$. Daher $\gamma \vdash_T \neg\alpha$ für ein $\gamma \in T_X \mathcal{A}$, denn $\langle X \rangle$ ist konjunktiv abgeschlossen. Das ergibt $\alpha \vdash_T \neg\gamma$, also $\neg\gamma \in Y_\alpha$. Folglich $\mathcal{A} \models \neg\gamma$, im Widerspruch zu $\mathcal{A} \models \gamma$. Also gilt (a). Daher gibt es $\beta_0, \dots, \beta_m \in Y_\alpha$ mit (b) $\beta := \bigwedge_{i \leq m} \beta_i \vdash_T \alpha$. Weil $\alpha \vdash_T \beta_i$, gilt auch $\alpha \vdash_T \beta$. Dies und (b) besagen $\alpha \equiv_T \beta$, und wegen $\beta \in \langle X \rangle$ ist damit auch $\alpha \in \langle X \rangle$. \square

Anwendungen. (a) Für $T = \text{DO}$ und $X = \{\text{L}, \text{R}\}$ gilt $\mathcal{A} \equiv_X \mathcal{B} \Rightarrow \mathcal{A} \equiv \mathcal{B}$, für alle $\mathcal{A}, \mathcal{B} \models T$. Denn $\mathcal{A} \equiv_X \mathcal{B}$ besagt offenbar, dass \mathcal{A}, \mathcal{B} die gleiche Randsituation besitzen. Damit ist aber $\mathcal{A} \equiv \mathcal{B}$, denn die DO_{ij} sind nach Übung 1 alle vollständig. Daher ist $\{\text{L}, \text{R}\}$ nach Satz 2.3 Boolesche Basis für \mathcal{L}^0 modulo DO . Diese Theorie hat 4 Vervollständigungen. Nach Übung 4 hat sie also genau 16 ($= 2^4$) Erweiterungen.

(b) Sei $T = \text{ACF}$ und $X = \{\text{char}_p \mid p \text{ Primzahl}\}$. Wieder ist $\mathcal{A} \equiv \mathcal{B}$, wenn nur $\mathcal{A} \equiv_X \mathcal{B}$ für alle $\mathcal{A}, \mathcal{B} \models T$. Denn ACF_p ist nach Beispiel 5(c) für jedes p (einschließlich 0) vollständig. Daher bilden nach Satz 2.3 die char_p eine Boolesche Basis für Aussagen modulo ACF . Das impliziert die Entscheidbarkeit von ACF . Denn man braucht bei gegebenem $\alpha \in \mathcal{L}^0$ in einem Aufzählungsverfahren der Sätze von ACF nur abzuwarten, bis eine Aussage der Gestalt $\alpha \leftrightarrow \beta$ erscheint, wobei β eine Boolesche Kombination aus den char_p ist. Eine solche Aussage erscheint mit Sicherheit. Sodann testet man $\beta \equiv_{\text{ACF}} \top$, z.B. durch Überführung von β in eine KNF.

Korollar 2.4. *Sei T eine Theorie mit beliebig großen endlichen Modellen derart, dass alle unendlichen und alle endlichen T -Modelle mit jeweils gleicher Anzahl von Elementen elementar-äquivalent sind. Dann gelten*

- (a) *Die Aussagen \exists_n (Seite 54) bilden eine Boolesche Basis für \mathcal{L}^0 modulo T ,*
- (b) *T ist entscheidbar wenn immer T endlich axiomatisierbar ist.*

⁵⁾ Diese Annahme ist gleichbedeutend mit der Vollständigkeit von $T_X \mathcal{A} = \{\gamma \in \langle X \rangle \mid \mathcal{A} \models \gamma\}$, siehe den folgenden Beweis. Für Verfeinerungen des Satzes sei auf [HR] verwiesen.

Beweis. Sei $X := \{\exists_k \mid k \in \mathbb{N}\}$. Dann ist gemäß Voraussetzung $\mathcal{A} \equiv \mathcal{B}$, wenn nur $\mathcal{A} \equiv_X \mathcal{B}$ für $\mathcal{A}, \mathcal{B} \models T$. Daher folgt (a) nach Satz 2.3. Jede mit T verträgliche Aussage α ist nach Übung 4 in 2.3 daher zu einer Aussage der Gestalt $\bigvee_{\nu \leq n} \exists_{=k_\nu}$ oder zu $\bigvee_{\nu \leq n} \exists_{=k_\nu} \vee \exists_m$ in T äquivalent. Jede dieser beiden Aussagen hat ein endliches T -Modell, weil es beliebig große endliche Modelle gibt. Kurzum, T hat die endliche Modelleigenschaft und (b) gilt nach Übung 2 in 3.6 wie man leicht sieht. \square

Einfache Anwendungsbeispiele sind die Theorien $\mathbf{Taut}_=$ aller Tautologien der Sprache $\mathcal{L}_=$ und die Theorie \mathbf{FO} aller endlichen geordneten Mengen, von der im nächsten Abschnitt bewiesen wird, dass sie die Voraussetzungen des Korollars erfüllt. Die im Beweis erwähnten äquivalenten Formeln ermöglichen auch eine vollständige Beschreibung der elementaren Klassen von $\mathcal{L}_=$. Es sind dies endliche Vereinigungen von Klassen, die durch Aussagen der Gestalt $\exists_{=k}$ und \exists_m bestimmt sind. Eine ähnlich einfache Beschreibung haben die elementaren Klassen aus \mathbf{FO} -Modellen.

Diese Beispiele machen hinreichend deutlich: Kennt man die elementaren Typen einer Theorie T , so kennt man auch deren elementare Klassen. In der Regel gelingt die Typenklassifikation – d.h. das Auffinden einer geeigneten Menge X , die die Voraussetzungen von Satz 2.3 erfüllt – nur in besonderen Fällen. Die erforderliche Detailarbeit ist meistens sehr umfangreich. Erwähnt seien z.B. die Theorien der abelschen Gruppen und Moduln, der Booleschen Algebren und anderer lokal endlicher Varietäten (siehe hierzu etwa [MV]). Obige Beispiele sind nur die allereinfachsten.

Übungen

1. Man zeige, nebst \mathbf{DO}_{00} sind auch \mathbf{DO}_{11} , \mathbf{DO}_{01} und \mathbf{DO}_{10} \aleph_0 -kategorisch und damit vollständig. Dies sind offenbar sämtliche Vervollständigungen von \mathbf{DO} .
2. Man zeige, T_{suc} (Seite 138) ist auch vollständig axiomatisiert durch die ersten beiden der angegebenen Axiome plus IS: $\alpha \frac{0}{x} \wedge \forall x(\alpha \rightarrow \alpha \frac{Sx}{x}) \rightarrow \forall x \alpha$ (Induktionsschema für $\mathcal{L}\{0, S\}$; α durchläuft alle Formeln von $\mathcal{L}\{0, S\}$).
3. Man zeige, die Theorie T der torsionsfreien dividierbaren abelschen Gruppen ist \aleph_1 -kategorisch, also vollständig und entscheidbar. Dies zeigt speziell die elementare Äquivalenz der beiden Gruppen $(\mathbb{R}, 0, +)$ und $(\mathbb{Q}, 0, +)$.
4. T habe endlich viele Vervollständigungen, sagen wir T_1, \dots, T_m . Nach Übung 2 in 3.5 ist $T_i = T + \alpha_i$ für gewisse α_i . Man zeige (a) $\{\alpha_i \mid i = 1, \dots, m\}$ ist Boolesche Basis in T , (b) jedes $\alpha \in \mathcal{L}^0$ ist in T äquivalent zu einer Formel der Gestalt $\bigvee_{\nu \leq n} \alpha_{i_\nu}$ mit $0 \leq i_0 < \dots < i_n \leq m$ (es sei zusätzlich $\alpha_0 := \perp$). Daraus schließe man, T hat genau 2^m Erweiterungen, T und \mathcal{L}^0 inklusive.

5.3 Das Ehrenfeucht-Spiel

Das Kriterium von Vaught ist leider nur beschränkt verwendbar, denn viele vollständige Theorien sind in keiner unendlichen Mächtigkeit kategorisch. Ein Beispiel ist die Theorie \mathbf{SO}_{10} der diskret geordneten Mengen mit linkem und ohne rechtes Randelement. Hier bezeichnet \mathbf{SO} die *Theorie der diskret geordneten Mengen*, d.h. aller $(M, <)$ für die jedes $a \in M$ einen unmittelbaren Nachfolger hat, wenn a kein rechtes Randelement ist, und ebenso einen unmittelbaren Vorgänger, wenn a kein linkes Randelement ist⁶⁾. Die Modelle für \mathbf{SO}_{10} entstehen aus beliebigen Ordnungen $(M, <)$ mit linkem Randelement dadurch, dass das Randelement durch $(\mathbb{N}, <)$, und jedes andere Element durch ein Exemplar von $(\mathbb{Z}, <)$ ersetzt wird. Daraus folgt unschwer, dass \mathbf{SO}_{10} für kein $\kappa \geq \aleph_0$ κ -kategorisch sein kann. Doch ist \mathbf{SO}_{10} vollständig, ebenso wie \mathbf{SO}_{00} und \mathbf{SO}_{01} , nicht aber \mathbf{SO}_{11} , denn jede endliche geordnete Menge ist Modell für \mathbf{SO}_{11} . Die Indizierung der Theorien \mathbf{SO}_{ij} ist hier analog zu den \mathbf{DO}_{ij} .

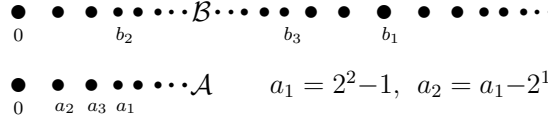
Wir werden die Vollständigkeit von \mathbf{SO}_{10} spieltheoretisch beweisen und benutzen dafür ein 2-Personen-Spiel mit den Spielern I und II, das *Ehrenfeucht-Spiel* $\Gamma_k(\mathcal{A}, \mathcal{B})$, das in k Runden gespielt wird, $k \geq 0$. Hierbei seien \mathcal{A}, \mathcal{B} vorgegebene \mathcal{L} -Strukturen, und \mathcal{L} sei eine *Relationalsprache*, d.h. \mathcal{L} enthält keine Konstanten- und Operationssymbole. Dies ist keine wirkliche Beschränkung der Allgemeinheit hinsichtlich der von uns verfolgten Ziele; denn man kann beliebige Strukturen stets in Relationalstrukturen verwandeln, indem man die Operationen durch ihre Graphen ersetzt. Ein im Folgenden auch genutzter Vorteil von Relationalstrukturen ist, dass sich ihre nichtleeren Teilmengen und ihre Substrukturen umkehrbar eindeutig entsprechen.

Es folgt nun die Beschreibung des Spiels $\Gamma_k(\mathcal{A}, \mathcal{B})$. Spieler I wählt in jeder der k Runden eine der beiden Strukturen \mathcal{A} oder \mathcal{B} . Ist dies \mathcal{A} , wählt er ein $a \in A$ aus, und Spieler II hat dann mit einem Element $b \in B$ zu antworten. Wählt I aber \mathcal{B} und ein $b \in B$, muss II mit einem Element $a \in A$ antworten. Damit ist die Beschreibung einer Runde dieses Spiels auch schon abgeschlossen. Nach k Runden wurden Elemente $a_1, \dots, a_k \in A$ und $b_1, \dots, b_k \in B$ ausgewählt, wobei a_i, b_i die in Runde i gewählten Elemente bezeichnen. Spieler II hat gewonnen, wenn die Abbildung $a_i \mapsto b_i$ für $i = 1, \dots, k$ ein partieller Isomorphismus von \mathcal{A} nach \mathcal{B} ist, d.h. wenn die Substruktur von \mathcal{A} mit dem Träger $\{a_1, \dots, a_k\}$ isomorph ist zur Substruktur von \mathcal{B} mit dem Träger $\{b_1, \dots, b_k\}$. Andernfalls hat Spieler I gewonnen.

Wir schreiben $\mathcal{A} \sim_k \mathcal{B}$, wenn Spieler II eine Gewinnstrategie im Spiel $\Gamma_k(\mathcal{A}, \mathcal{B})$ hat, d.h. in jeder Runde auf einen beliebigen Zug von I so antworten kann, dass das Spiel am Ende für II gewonnen ist. Für das „0-Runden-Spiel“ sei $\mathcal{A} \sim_0 \mathcal{B}$ per definitionem.

⁶⁾ ‘SO’ soll an ‘Schrittordnung’ erinnern, denn das Wort ‘diskret’ hat im Zusammenhang mit Ordnungen oft auch einen etwas schärferen Sinn. Offenbar ist $(\mathbb{N}, <)$ Primmodell für \mathbf{SO}_{10} .

Beispiel. Sei $\mathcal{A} = (\mathbb{N}, <)$ echter Anfang von $\mathcal{B} \models \text{SO}_{10}$. Wir zeigen $\mathcal{A} \sim_k \mathcal{B}$ für beliebiges $k > 0$. Spieler II spielt wie folgt: Wählt I in der ersten Runde ein $b_1 \in B$, antwortet II mit $a_1 = 2^{k-1} - 1$, falls $d(0, b_1) \geq 2^{k-1} - 1$, sonst mit $a_1 = d(0, b_1)$ ⁷⁾. Analog, falls I mit \mathcal{A} beginnt. Wählt I nun ein $b_2 \in B$ mit $d(0, b_2), d(b_1, b_2) \geq 2^{k-2} - 1$, antwortet II mit $a_2 = a_1 \pm 2^{k-2}$ je nachdem ob $b_2 > b_1$ oder $b_2 < b_1$, sonst mit dem Element derselben Distanz von 0 oder a_1 , wie sie b_2 von der 0 aus B bzw. von b_1 hat. Analog in der 3. Runde usw. Die Figur zeigt den Verlauf eines in der beschriebenen



Weise ausgeführten 3-Runden-Spiels, wobei I nur aus \mathcal{B} gewählt hat. Mit dieser Strategie gewinnt II jedes Spiel, wie man induktiv über k unschwer beweist.

Anders als in diesem Beispiel hat Spieler II für $\mathcal{A} = (\mathbb{N}, <)$ und $\mathcal{B} = (\mathbb{Z}, <)$ bereits in $\Gamma_2(\mathcal{A}, \mathcal{B})$ keine Gewinnchance, wenn I in der ersten Runde $0 \in \mathbb{N}$ wählt. Das hat damit zu tun, dass die Existenz eines Randelements eine Aussage vom Quantorenrang 2 ist. Man schreibe $\mathcal{A} \equiv_k \mathcal{B}$ für \mathcal{L} -Strukturen \mathcal{A}, \mathcal{B} , wenn $\mathcal{A} \models \alpha \Leftrightarrow \mathcal{B} \models \alpha$, für alle $\alpha \in \mathcal{L}^0$ mit $\text{qr } \alpha \leq k$. Stets ist $\mathcal{A} \equiv_0 \mathcal{B}$ für alle \mathcal{A}, \mathcal{B} , weil es Aussagen vom Quantorenrang 0 (d.h. quantorenfreie Aussagen) in Relationalsprachen nicht gibt. Wir beweisen weiter unten den bemerkenswerten

Satz 3.1. $\mathcal{A} \sim_k \mathcal{B}$ impliziert $\mathcal{A} \equiv_k \mathcal{B}$. Speziell ist $\mathcal{A} \equiv \mathcal{B}$, falls $\mathcal{A} \sim_k \mathcal{B}$ für alle k .

Für endliche Signaturen gilt auch eine etwas abgeschwächte Umkehrung des Satzes, die wir aber nicht diskutieren.

Bevor wir Satz 3.1 beweisen, demonstrieren wir seine Anwendbarkeit. Der Satz und das obige Beispiel ergeben $(\mathbb{N}, <) \equiv_k \mathcal{B}$ für alle k und mithin $(\mathbb{N}, <) \equiv \mathcal{B}$ für jedes $\mathcal{B} \models \text{SO}_{10}$, denn $(\mathbb{N}, <)$ ist Primmodell für SO_{10} . Damit ist SO_{10} offenbar vollständig. Aus Symmetriegründen gilt dasselbe für SO_{01} , ebenso für SO_{00} gemäß Übung 2. Hingegen hat SO_{11} nach Übung 3 die endliche Modelleigenschaft, woraus ganz leicht folgt, dass SO_{11} identisch ist mit der Theorie FO aller endlichen geordneten Mengen.

Zum Beweis von Satz 3.1 betrachten wir zuerst eine leichte Verallgemeinerung von $\Gamma_k(\mathcal{A}, B)$, das Spiel $\Gamma_k(\mathcal{A}, \mathcal{B}, \vec{a}, \vec{b})$ mit Vorgaben $\vec{a} \in A^n, \vec{b} \in B^n$. Spieler I wählt in der ersten Runde ein $a_{n+1} \in A$ oder $b_{n+1} \in B$ und II antwortet mit b_{n+1} oder a_{n+1} , usw. Das Spielprotokoll besteht am Ende aus Folgen (a_1, \dots, a_{n+k}) und (b_1, \dots, b_{n+k}) . Spieler II hat gewonnen, wenn $a_i \mapsto b_i$ ($i = 1, \dots, n+k$) ein partieller Isomorphismus ist. Für $n = 0$ erhalten wir so gerade das Original-Spiel $\Gamma_k(\mathcal{A}, \mathcal{B})$.

⁷⁾ Die „Distanz“ $d = d(a, b)$ von Elementen a, b eines SO-Modells sei 0 für $a = b$, sonst $1 + \text{Anzahl}$ der echt zwischen a und b liegenden Elemente, falls diese endlich ist; ansonsten sei $d(a, b) = \infty$.

Dieser Ansatz ermöglicht zudem eine von anderen Begriffen unabhängige Präzisierung des spieltheoretischen Konzepts einer Gewinnstrategie für Spieler II wie folgt:

Definition. Spieler II hat eine Gewinnstrategie in $\Gamma_0(\mathcal{A}, \mathcal{B}, \vec{a}, \vec{b})$, falls $a_i \mapsto b_i$ für $i = 1, \dots, n$ ein partieller Isomorphismus ist. Spieler II hat eine Gewinnstrategie in $\Gamma_{k+1}(\mathcal{A}, \mathcal{B}, \vec{a}, \vec{b})$, symbolisch $(\mathcal{A}, \vec{a}) \sim_{k+1} (\mathcal{B}, \vec{b})$, wenn zu jedem $a \in A$ ein $b \in B$ existiert, sowie zu jedem $b \in B$ ein $a \in A$, so dass Spieler II eine Gewinnstrategie in $\Gamma_k(\mathcal{A}, \mathcal{B}, \vec{a}_{\perp}a, \vec{b}_{\perp}b)$ hat. Dabei bezeichne $\vec{c}_{\perp}c$ die Verlängerung der Folge \vec{c} um c .

Speziell bedeutet $\mathcal{A} \sim_k \mathcal{B}$ dasselbe wie $(\mathcal{A}, \vec{a}) \sim_k (\mathcal{B}, \vec{b})$ für den Fall $\vec{a} = \vec{b} = \emptyset$.

Lemma 3.2. Sei $(\mathcal{A}, \vec{a}) \sim_k (\mathcal{B}, \vec{b})$ mit $\vec{a} \in A^n$, $\vec{b} \in B^n$. Für alle $\varphi = \varphi(\vec{x})$ mit $\text{qr } \varphi \leq k$ gilt dann $(*) \mathcal{A} \models \varphi(\vec{a}) \Leftrightarrow \mathcal{B} \models \varphi(\vec{b})$.

Beweis durch Induktion über k . Sei $k = 0$. Weil $a_i \mapsto b_i$ ($i = 1, \dots, n$) partieller Isomorphismus ist, gilt $(*)$ für Primformeln und sogar für alle φ mit $\text{qr } \varphi = 0$, da die Induktionsschritte über \neg , \wedge offensichtlich sind. Sei nun $(\mathcal{A}, \vec{a}) \sim_{k+1} (\mathcal{B}, \vec{b})$ und $\text{qr } \varphi \leq k + 1$. Im Falle $\text{qr } \varphi \leq k$ gilt $(*)$ gemäß Induktionsannahme, weil offenbar $\sim_{k+1} \subseteq \sim_k$. Daher darf man annehmen $\varphi = \forall y \alpha(\vec{x}, y)$ mit $\text{qr } \alpha = k$, denn jedes ψ mit $\text{qr } \psi = k + 1$ ist Boolesche Kombination aus solchen φ und Formeln vom Quantorenrang $\leq k$, wie man leicht sieht. Sei $\mathcal{A} \models \forall y \alpha(\vec{a}, y)$ und $b \in B$. Zu diesem b wähle man ein $a \in A$ mit $(\mathcal{A}, \vec{a}_{\perp}a) \sim_k (\mathcal{B}, \vec{b}_{\perp}b)$. Also $\mathcal{A} \models \alpha(\vec{a}, a) \Leftrightarrow \mathcal{B} \models \alpha(\vec{b}, b)$ nach der sich auf beliebige Elementetupel bezieht. $\mathcal{A} \models \forall y \alpha(\vec{a}, y)$ liefert $\mathcal{A} \models \alpha(\vec{a}, a)$, also $\mathcal{B} \models \alpha(\vec{b}, b)$, und weil b beliebig gewählt worden ist, ergibt sich $\mathcal{B} \models \forall y \alpha(\vec{b}, y)$. Aus Symmetriegründen erhält man ebenso $\mathcal{B} \models \forall y \alpha(\vec{b}, y) \Rightarrow \mathcal{A} \models \forall y \alpha(\vec{a}, y)$, also insgesamt die Behauptung $(*)$. \square

Satz 3.1 ist der Anwendungsfall des Lemmas für $n = 0$ und damit bewiesen. Die vorgestellte Methode ist weittragend und hat auch viele Verallgemeinerungen.

Übungen

1. Seien \mathcal{A}, \mathcal{B} zwei dicht geordnete Mengen mit derselben Randsituation. Man beweise, Spieler II hat für jedes k eine Gewinnstrategie in $\Gamma_k(\mathcal{A}, \mathcal{B})$.
2. Man zeige $\mathcal{A}, \mathcal{B} \models \text{SO}_{00} \Rightarrow \mathcal{A} \sim_k \mathcal{B}$ für alle k . Also ist SO_{00} vollständig.
3. Seien $\mathcal{A}, \mathcal{B} \models \text{SO}_{11}$, $k > 0$ und $|A|, |B| \geq 2^k - 1$. Man beweise $\mathcal{A} \sim_k \mathcal{B}$. Daraus folgere man SO_{11} hat die endliche Modelleigenschaft.
4. Man zeige, $\text{L}, \text{R}, \exists_1, \exists_2, \dots$ bilden eine Boolesche Basis für $\mathcal{L}_{<}^0$ in SO . Daraus erschließe man die Entscheidbarkeit von SO .

5.4 Einbettungs- und Charakterisierungssätze

Viele der bisher angegebenen Theorien, etwa die der Ordnungen, die Gruppentheorie in $\cdot, e, ^{-1}$, die Ringtheorie usw. sind universale oder \forall -Theorien, d.h. sie besitzen Axiomensysteme aus \forall -Aussagen. Für jede derartige Theorie T gilt wie wir bereits wissen $\mathcal{A} \subseteq \mathcal{B} \models T \Rightarrow \mathcal{A} \models T$, kurz T ist **S-invariant**. DO hat diese Eigenschaft offenbar nicht, also kann es für sie kein Axiomensystem aus \forall -Aussagen geben. Durch die **S-Invarianz** sind nun die \forall -Theorien gemäß Satz 4.3 vollständig gekennzeichnet. Dies ist das historisch erste, besonders einfache Beispiel einer modelltheoretischen Charakterisierung gewisser syntaktischer Formen von Axiomensystemen.

$T_{\forall} := \{\alpha \in T \mid \alpha \text{ ist } \forall\text{-Aussage}\}$ heie der *universale Teil* einer Theorie T . Man beachte den Unterschied zwischen der Menge T_{\forall} und der \forall -Theorie T_{\forall} , die natrlich nicht nur \forall -Aussagen enthlt. Fr $\mathcal{L}_0 \subseteq \mathcal{L}$ sei $T_{0\forall} := \mathcal{L}_0 \cap T_{\forall}$. Ist \mathcal{A} eine \mathcal{L}_0 -Struktur, \mathcal{B} eine \mathcal{L} -Struktur, so meinen $\mathcal{A} \subseteq \mathcal{B}$ und die Redeweise ‘ \mathcal{A} ist Substruktur von \mathcal{B} ’ in diesem Abschnitt oft, dass \mathcal{A} Substruktur des \mathcal{L}_0 -Redukts von \mathcal{B} ist. Analog ist die in 5.1 schon verabredete Sprechweise ‘ \mathcal{A} ist einbettbar in \mathcal{B} ’ zu verstehen. Beispiele finden sich weiter unten. Wir formulieren zuerst folgendes

Lemma 4.1. *Jedes $T_{0\forall}$ -Modell \mathcal{A} ist in ein T -Modell einbettbar.*

Beweis. Es gengt zu zeigen, $(*)$ $T, D\mathcal{A}$ ist konsistent. Denn ist $\mathcal{B} \models T, D\mathcal{A}$, so ist \mathcal{A} nach Satz 1.1 in \mathcal{B} einbettbar. Angenommen, $(*)$ sei falsch. Dann gibt es eine Konjunktion $\varkappa(\vec{a})$ von Aussagen aus $D\mathcal{A}$ mit $\vdash_T \neg \varkappa(\vec{a})$ (bung 4 in 3.2). Dabei umfasse \vec{a} alle in den Gliedern von \varkappa vorkommenden Konstanten aus $\mathcal{L}\mathcal{A}$, die in T nicht vorkommen. Konstantenquantifizierung nach 3.2 ergibt $\vdash_T \forall \vec{x} \neg \varkappa(\vec{x})$. Also $\forall \vec{x} \neg \varkappa(\vec{x}) \in T_{0\forall}$ und somit $\mathcal{A} \models \forall \vec{x} \neg \varkappa(\vec{x})$, im Widerspruch zu $\mathcal{A} \models \varkappa(\vec{a})$. \square

Lemma 4.2. *$\text{Md } T_{\forall}$ besteht genau aus den Substrukturen aller T -Modelle.*

Beweis. Jede Substruktur eines T -Modells ist natrlich ein T_{\forall} -Modell. Ferner ist jedes $\mathcal{A} \models T_{\forall}$ nach dem Lemma (fr $\mathcal{L}_0 = \mathcal{L}$) in ein $\mathcal{B} \models T$ einbettbar, was gewiss gleichwertig ist mit $\mathcal{A} \subseteq \mathcal{B}'$ fr ein $\mathcal{B}' \models T$, weil $\text{Md } T$ stets unter isomorphen Bildern abgeschlossen ist. \square

Beispiele. (a) Sei **AG** die Theorie der abelschen Gruppen in $\mathcal{L}\{+, 0\}$, deren Substrukturen dann kommutative regulre Halbgruppen sind. Umgekehrt ist unschwer beweisbar, dass jede derartige Halbgruppe in eine abelsche Gruppe einbettbar ist. Also ist die Theorie **AG_∅** nichts anderes als die der kommutativen regulren Halbgruppen. **Warnung:** Eine nichtkommutative regulre Halbgruppe muss nicht in eine Gruppe einbettbar sein. Hier sind die Einbettungs-Bedingungen in eine Gruppe etwas komplizierter.

(b) Substrukturen von Körpern in $\mathcal{L}\{0, 1, +, -, \cdot\}$ sind Integritätsbereiche. Nach einer bekannten Konstruktion ist umgekehrt jeder Integritätsbereich in einen Körper, seinen *Quotientenkörper* einbettbar, der ähnlich konstruiert wird wie der Körper \mathbb{Q} aus dem Ring \mathbb{Z} . Für die Körpertheorie T_K ist daher die Theorie $T_{K\forall}$ nach Satz 4.2 identisch mit der Theorie T_J aller Integritätsbereiche.

Satz 4.3. *T ist eine \forall -Theorie genau dann, wenn T **S**-invariant ist.*

Beweis. Dies folgt unmittelbar aus Lemma 4.2. Denn für eine **S**-invariante Theorie T ist $\text{Md } T = \text{Md } T_{\forall}$. Kurzum, T ist durch T_{\forall} axiomatisiert. \square

Interessant ist auch folgender Satz über universale Horntheorien. Das sind spezielle \forall -Theorien, die eine Hauptrolle in der Logikprogrammierung spielen. T heiße **SP**-invariant, wenn $\text{Md } T$ unter direkten Produkten und Substrukturen abgeschlossen ist.

Satz 4.4. *T ist eine universale Horntheorie genau dann, wenn T **SP**-invariant ist.*

Beweis. \Rightarrow : Übung 1 in 4.1. \Leftarrow : Sei U die Menge aller in T beweisbaren universalen Hornsätze. Wir zeigen $\text{Md } T = \text{Md } U$ und damit die Behauptung. $\text{Md } T \subseteq \text{Md } U$ ist trivial. Sei $\mathcal{A} \models U$. Zum Beweis von $\mathcal{A} \models T$ genügt es, $(*) T \cup D\mathcal{A} \not\models \perp$ zu zeigen; denn für $\mathcal{B} \models T, D\mathcal{A}$ ist o.B.d.A. $\mathcal{A} \subseteq \mathcal{B}$, also $\mathcal{A} \models T$ wegen der **S**-Invarianz. Sei $P = \{\pi \in D\mathcal{A} \mid \pi \text{ Primformel}\}$, so dass $D\mathcal{A} = P \cup \{\neg\pi_i \mid i \in I\}$ für passendes I , mit Primformeln π_i . Wir zeigen zuerst $P \not\models_T \pi_i$ für jedes $i \in I$. Andernfalls wäre $\vdash_T \neg(\vec{a}) \rightarrow \pi_i(\vec{a})$ für eine Konjunktion $\neg(\vec{a})$ von Aussagen aus P , mit dem Tupel \vec{a} aller in T nicht vorkommenden Konstanten. Daher $\vdash_T \alpha := \forall \vec{x}(\neg(\vec{x}) \rightarrow \pi_i(\vec{x}))$. Also $\alpha \in U$, denn α ist eine universale Hornaussage. Mithin $\mathcal{A} \models \alpha$. Das widerspricht aber $\mathcal{A} \models \neg(\vec{a}) \wedge \neg\pi_i(\vec{a})$ und zeigt $P \not\models_T \pi_i$. Sei $\mathcal{A}_i \models T, P, \neg\pi_i$. Dann gilt $\mathcal{B} := \prod_{i \in I} \mathcal{A}_i \models T$ wegen der **P**-Invarianz, sowie $\mathcal{B} \models P \cup \{\neg\pi_i \mid i \in I\} = D\mathcal{A}$. Das beweist $(*)$. \square

Im Beweis des folgenden Satzes wird Lemma 4.1 voll ausgeschöpft.

Satz 4.5. *Sei $\mathcal{L}_0 \subseteq \mathcal{L}$ und \mathcal{A} eine \mathcal{L}_0 -Struktur. Für $T \subseteq \mathcal{L}$ sind dann gleichwertig*

- (i) \mathcal{A} ist in ein T -Modell einbettbar,
- (ii) Jede endlich erzeugte Substruktur von \mathcal{A} ist in ein T -Modell einbettbar,
- (iii) $\mathcal{A} \models T_{0\forall} (= \mathcal{L}_0 \cap T_{\forall})$.

Beweis. (i) \Rightarrow (ii): Trivial. (ii) \Rightarrow (iii): Sei $\forall \vec{x} \alpha \in T_{0\forall}$ mit quantorenfreiem $\alpha = \alpha(\vec{x})$, $\vec{x} = (x_0, \dots, x_n)$. Sei \mathcal{A}_0 für $\vec{a} = (a_0, \dots, a_n) \in A^{n+1}$ die von a_0, \dots, a_n in \mathcal{A} erzeugte Substruktur. Nach (ii) ist $\mathcal{A}_0 \subseteq \mathcal{B}$ für ein $\mathcal{B} \models T$. Da $\forall \vec{x} \alpha \in T_{0\forall}$, also $\mathcal{B} \models \forall \vec{x} \alpha$, ist auch $\mathcal{A}_0 \models \forall \vec{x} \alpha$, daher $\mathcal{A}_0 \models \alpha(\vec{a})$, folglich $\mathcal{A} \models \alpha(\vec{a})$ (Satz 2.3.2). Weil \vec{a} beliebig war, gilt in der Tat $\mathcal{A} \models \forall \vec{x} \alpha$. (iii) \Rightarrow (i): Dies besagt gerade Lemma 4.1. \square

Illustrationsbeispiele. (a) Sei $\mathcal{L}_0 = \mathcal{L}\{0, +, -\}$, $\mathcal{L} = \mathcal{L}\{0, +, -, <\}$ und T die Theorie der geordneten abelschen Gruppen. Eine solche Gruppe ist offenbar torsionsfrei, was sich durch ein Schema von \forall -Aussagen ausdrücken lässt. Umgekehrt kann

man mit Satz 4.5 unschwer zeigen, dass eine torsionsfreie abelsche Gruppe auch ordnungsfähig ist. Es genügt nämlich, dies für jede endlich erzeugte Gruppe G dieser Art zu zeigen. Nach einem gruppentheoretischen Satz ist G bis auf Isomorphie von der Gestalt \mathbb{Z}^n für ein $n > 0$ und man überzeugt sich leicht, dass \mathbb{Z}^n nicht nur für $n = 1$ sondern auch für $n > 1$ angeordnet werden kann, nämlich lexikographisch. Wir erwähnen, dass auch für nichtabelsche Gruppen übersichtliche Bedingungen der Ordnungsfähigkeit angebar sind, die aber etwas komplizierter aussehen.

(b) Ohne Algebra zu betreiben wissen wir: Es gibt eine Menge universaler Aussagen in $0, 1, +, -, \cdot$, deren Hinzunahme zur Körpertheorie die ordnungsfähigen Körper charakterisiert. Denn nach Satz 4.5 reicht die Menge aller aus den Axiomen für geordnete Körper beweisbaren \forall -Aussagen in $0, 1, +, -, \cdot$ dafür hin. Tatsächlich genügt schon das Aussagenschema ‘ -1 ist keine Summe von Quadraten’ (E. Artin).

Nicht nur \forall -Theorien, sondern auch \forall -Formeln lassen sich modelltheoretisch kennzeichnen. $\alpha(\vec{x})$ heie **S-persistent** oder einfach persistent in T , wenn

$$(sp) \quad \mathcal{B} \models \alpha(\vec{a}) \Rightarrow \mathcal{A} \models \alpha(\vec{a}), \text{ fur alle } \mathcal{A}, \mathcal{B} \models T \text{ mit } \mathcal{A} \subseteq \mathcal{B} \text{ und alle } \vec{a} \in A^n.$$

Diese Eigenschaft charakterisiert bis auf Äquivalenz die \forall -Formeln:

Satz 4.6. *Ist $\alpha = \alpha(\vec{x})$ persistent in T , so ist α zu einer \forall -Formel α' in T quivalent, die so gewhlt werden kann, dass $frei\alpha' \subseteq frei\alpha$.*

Beweis. Sei Y die Menge aller Formeln der Gestalt $\forall \vec{y} \beta(\vec{x}, \vec{y})$ mit $\alpha \vdash_T \forall \vec{y} \beta(\vec{x}, \vec{y})$ und β quantorenfrei; dabei mogen die Tupel \vec{x} und \vec{y} die Lngen $n \geq 0$ bzw. $m \geq 0$ haben. Wir beweisen (a) $Y \vdash_T \alpha(\vec{x})$. Damit wre der Beweis erbracht; denn wegen $freiY \subseteq \{x_1, \dots, x_n\}$ existiert dann eine Konjunktion $\varkappa = \varkappa(\vec{x})$ von Formeln aus Y mit $\varkappa \vdash_T \alpha$. Weil auch $\alpha \vdash_T \varkappa$, ist $\alpha \equiv_T \varkappa$, und \varkappa ist als Konjunktion von \forall -Formeln wieder zu einer solchen quivalent. Zum Nachweis von (a) sei $\vec{a} \in A^n$ und $(\mathcal{A}, \vec{a}) \models T, Y$. Es ist $(\mathcal{A}, \vec{a}) \models \alpha$ zu zeigen. Dies folgt aus (b) $T, \alpha(\vec{a}), D\mathcal{A}$ ist konsistent. Denn fur $\mathcal{B} \models T, \alpha(\vec{a}), D\mathcal{A}$ ist o.B.d.A. $\mathcal{A} \subseteq \mathcal{B}$ und daher $\mathcal{A} \models \alpha(\vec{a})$, weil α persistent ist. Angenommen (b) ist falsch. Dann ist $\alpha(\vec{a}) \vdash_T \neg \varkappa(\vec{a}, \vec{b})$ fur eine Konjunktion $\varkappa(\vec{a}, \vec{b})$ von Aussagen aus $D\mathcal{A}$ mit dem m -Tupel \vec{b} der Konstanten von \varkappa aus $A \setminus \{a_1, \dots, a_n\}$. Also $\alpha(\vec{a}) \vdash_T \forall \vec{y} \neg \varkappa(\vec{a}, \vec{y})$. Weil auch die a_1, \dots, a_n in T nicht vorkommen, ist $\alpha(\vec{x}) \vdash_T \forall \vec{y} \neg \varkappa(\vec{x}, \vec{y}) \in Y$. Daher ist $(\mathcal{A}, \vec{a}) \models \forall \vec{y} \neg \varkappa(\vec{x}, \vec{y})$, oder gleichwertig $\mathcal{A} \models \forall \vec{y} \neg \varkappa(\vec{a}, \vec{y})$, im Widerspruch zu $\mathcal{A} \models \varkappa(\vec{a}, \vec{b})$. \square

Bemerkung. Ist T abzhlbar und sind alle T -Modelle unendlich, so ist α bereits dann zu einer \forall -Formel in T quivalent, falls (sp) nur fur alle T -Modelle einer gewissen Kardinalzahl $\kappa \geq \aleph_0$ gilt, weil man sich in diesem Falle beim Nachweis von (a) im obigen Beweis nach den Stzen von Lowenheim-Skolem auf Modelle der Kardinalzahl κ beschrnken kann.

Aussagen der Gestalt $\forall \vec{x} \exists \vec{y} \alpha$ mit quantorenfreiem α heißen $\forall\exists$ -Aussagen. Viele Theorien, z.B. die der Körper, der reell bzw. der algebraisch abgeschlossenen Körper, der dividierbaren Gruppen u.a. sind $\forall\exists$ -Theorien, d.h. sie besitzen Axiomensysteme aus $\forall\exists$ -Aussagen. Wir charakterisieren nun die $\forall\exists$ -Theorien modelltheoretisch. Eine *Kette K von Strukturen* sei einfach eine Menge K von \mathcal{L} -Strukturen mit $\mathcal{A} \subseteq \mathcal{B}$ oder $\mathcal{B} \subseteq \mathcal{A}$ für alle $\mathcal{A}, \mathcal{B} \in K$. Oft sind z.B. Ketten durch Folgen $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \dots$ von Strukturen gegeben. Wie K auch gegeben ist, stets lässt sich eine Struktur $\mathcal{C} := \bigcup K$ wie folgt definieren: $\mathcal{C} := \bigcup \{A \mid A \in K\}$ sei der Träger. Ferner sei $r^{\mathcal{C}} \vec{a} \Leftrightarrow r^{\mathcal{A}} \vec{a}$ für $\vec{a} \in C^n$, wobei $\mathcal{A} \in K$ so gewählt sei, dass $\vec{a} \in A^n$. Ein solches $\mathcal{A} \in K$ gibt es. Diese Definition von $r^{\mathcal{C}}$ ist unabhängig von der Wahl von \mathcal{A} ; denn ist $\mathcal{A}' \in K$ und auch $a_1, \dots, a_n \in A'$, so ist entweder $\mathcal{A} \subseteq \mathcal{A}'$ oder $\mathcal{A}' \subseteq \mathcal{A}$, also $r^{\mathcal{C}} \vec{a} \Leftrightarrow r^{\mathcal{A}'} \vec{a}$ in jedem Falle. Schließlich sei $f^{\mathcal{C}} \vec{a} = f^{\mathcal{A}} \vec{a}$, wobei $\mathcal{A} \in K$ so gewählt werde, dass $\vec{a} \in A^n$. Auch hier ist die Wahl von $\mathcal{A} \in K$ belanglos. \mathcal{C} wurde gerade so definiert, dass jedes Kettenglied $\mathcal{A} \in K$ Substruktur von \mathcal{C} ist.

Beispiel. Sei \mathcal{D}_n die additive Gruppe der n -stelligen Dezimalzahlen (Kommazahlen, die nach der n -ten Nachkommastelle abbrechen). Offenbar gilt $\mathcal{D}_n \subseteq \mathcal{D}_{n+1}$, und $\mathcal{D} = \bigcup_{n \in \mathbb{N}} \mathcal{D}_n$ ist gerade die additive Gruppe der abbrechenden Dezimalzahlen.

Es ist nun leicht zu sehen, dass eine $\forall\exists$ -Aussage $\alpha = \forall \vec{x} \exists \vec{y} \beta(\vec{x}, \vec{y})$, die in allen Gliedern \mathcal{A} einer Kette K von Strukturen gilt, auch in $\mathcal{C} = \bigcup K$ richtig ist. Denn sei $\vec{a} \in C^n$ und damit $\vec{a} \in A^n$ für ein $\mathcal{A} \in K$. Dann gilt $\mathcal{A} \models \beta(\vec{a}, \vec{b})$ für ein $\vec{b} \in A^m$. Weil $\mathcal{A} \subseteq \mathcal{C}$ und $\beta(\vec{x}, \vec{y})$ quantorenfrei ist, folgt $\mathcal{C} \models \beta(\vec{a}, \vec{b})$, also $\mathcal{C} \models \exists \vec{y} \beta(\vec{a}, \vec{y})$. Da \vec{a} hier beliebig gewählt worden ist, gilt in der Tat $\mathcal{C} \models \forall \vec{x} \exists \vec{y} \beta(\vec{x}, \vec{y})$.

Demnach ist $\text{Md } T$ für eine $\forall\exists$ -Theorie T immer gegenüber Vereinigung von Ketten abgeschlossen, oder wie man sagt, T ist *induktiv*. Diese Eigenschaft ist nun wiederum charakteristisch für $\forall\exists$ -Theorien. Allerdings ist dieser Nachweis etwas weniger einfach. Wir benötigen dazu den Begriff der *elementaren Kette*. Darunter sei eine Kette $K \neq \emptyset$ von \mathcal{L} -Strukturen mit $\mathcal{A} \preceq \mathcal{B}$ oder $\mathcal{B} \preceq \mathcal{A}$ für alle $\mathcal{A}, \mathcal{B} \in K$ verstanden.

Lemma 4.7 (Kettenlemma von Tarski). *Sei K eine elementare Kette und sei $\mathcal{C} = \bigcup K$. Dann ist $\mathcal{A} \preceq \mathcal{C}$ für jedes Kettenglied $\mathcal{A} \in K$.*

Beweis. Wir zeigen $(*) \mathcal{A} \models \alpha(\vec{a}) \Leftrightarrow \mathcal{C} \models \alpha(\vec{a})$ für $\vec{a} \in A^n$ durch Induktion über $\alpha = \alpha(\vec{x})$. Dies ist klar für Primformeln. Auch die Induktionsschritte über \wedge, \neg sind klar. Sei $\mathcal{A} \models \forall y \alpha(\vec{a}, y)$ und $b \in C$. Es gibt gewiss ein $\mathcal{B} \in K$ mit $a_1, \dots, a_n, b \in B$ und $\mathcal{A} \preceq \mathcal{B}$, so dass auch $\mathcal{B} \models \forall y \alpha(\vec{a}, y)$ und damit $\mathcal{B} \models \alpha(\vec{a}, b)$. Da sich die Induktionsannahme auf beliebige Kettenglieder bezieht, folgt $\mathcal{C} \models \alpha(\vec{a}, b)$. Weil $b \in C$ beliebig war, ergibt sich $\mathcal{C} \models \forall y \alpha(\vec{a}, y)$. Umgekehrt sei $\mathcal{C} \models \forall y \alpha(\vec{a}, y)$ und $b \in A$. Dann ist $\mathcal{C} \models \alpha(\vec{a}, b)$ und daher $\mathcal{A} \models \alpha(\vec{a}, b)$ nach Induktionsannahme. Da b beliebig gewählt war, ergibt sich auch $\mathcal{A} \models \forall y \alpha(\vec{a}, y)$. \square

Wir benötigen noch einen weiteren nützlichen Begriff, für den sich viele Beispiele in 5.5 befinden. Sei $\mathcal{A} \subseteq \mathcal{B}$. Dann heißt \mathcal{A} *existentiell abgeschlossen in \mathcal{B}* , symbolisch $\mathcal{A} \subseteq_{ec} \mathcal{B}$, wenn $(\star) \mathcal{B} \models \exists \vec{x} \alpha(\vec{x}, \vec{a}) \Rightarrow \mathcal{A} \models \exists \vec{x} \alpha(\vec{x}, \vec{a})$, wobei $\alpha = \alpha(\vec{x}, \vec{a})$ eine beliebige Konjunktion aus Literalen aus $\mathcal{L}\mathcal{A}$ bezeichnet. (\star) gilt dann automatisch auch für sämtliche quantorenfreien $\alpha \in \mathcal{L}\mathcal{A}$. Das sieht man sofort, indem α in eine disjunktive Normalform überführt und $\exists \vec{x}$ auf die Disjunktionsglieder verteilt wird.

Es ist klar, dass $\mathcal{A} \preceq \mathcal{B} \Rightarrow \mathcal{A} \subseteq_{ec} \mathcal{B} \Rightarrow \mathcal{A} \subseteq \mathcal{B}$. Auch für \subseteq_{ec} gilt ein leicht beweisbares Kettenlemma: Ist K eine Kette von Strukturen derart, dass $\mathcal{A} \subseteq_{ec} \mathcal{B}$ oder $\mathcal{B} \subseteq_{ec} \mathcal{A}$ für alle $\mathcal{A}, \mathcal{B} \in K$, so ist $\mathcal{A} \subseteq_{ec} \bigcup K$ für jedes $\mathcal{A} \in K$ (Übung!).

Lemma 4.8 enthält unterschiedliche Kennzeichnungen von $\mathcal{A} \subseteq_{ec} \mathcal{B}$. Darin bezeichne $D_{\forall} \mathcal{A}$ das *universale Diagramm* von \mathcal{A} , die Menge aller in \mathcal{A} gültigen \forall -Aussagen von $\mathcal{L}\mathcal{A}$. In (iii) wie auch an einigen Stellen im Beweis des Lemmas müsste \mathcal{B} eigentlich mit \mathcal{A} indiziert werden, was nur der schnelleren Lesbarkeit halber unterbleibt.

Lemma 4.8. *Seien \mathcal{A}, \mathcal{B} \mathcal{L} -Strukturen mit $\mathcal{A} \subseteq \mathcal{B}$. Dann sind äquivalent*

- (i) $\mathcal{A} \subseteq_{ec} \mathcal{B}$, (ii) *es gibt ein $\mathcal{A}' \supseteq \mathcal{B}$ mit $\mathcal{A} \preceq \mathcal{A}'$,* (iii) $\mathcal{B} \models D_{\forall} \mathcal{A}$.

Beweis. (i) \Rightarrow (ii): Sei $\mathcal{A} \subseteq_{ec} \mathcal{B}$. Wir erhalten ein $\mathcal{A}' \supseteq \mathcal{B}$ mit $\mathcal{A} \preceq \mathcal{A}'$ offenbar als Modell von $D_{el} \mathcal{A} \cup D\mathcal{B}$ (genauer, als das \mathcal{L} -Redukt eines derartigen Modells), so dass nur die Konsistenz dieser Menge nachzuweisen ist. Angenommen, diese wäre inkonsistent, so dass $D_{el} \mathcal{A} \vdash \neg \kappa(\vec{b})$ für eine Konjunktion $\kappa(\vec{b})$ von Aussagen aus $D\mathcal{B}$ mit dem n -Tupel \vec{b} der in κ vorkommenden Konstanten aus $B \setminus A$. Weil b_1, \dots, b_n in $D_{el} \mathcal{A}$ nicht vorkommen, ist $D_{el} \mathcal{A} \vdash \forall \vec{x} \neg \kappa(\vec{x})$ und damit $\mathcal{A} \models \forall \vec{x} \neg \kappa(\vec{x})$. Andererseits ist $\mathcal{B} \models \kappa(\vec{b})$, also $\mathcal{B} \models \exists \vec{x} \kappa(\vec{x})$. Wegen (i) und $\kappa(\vec{x}) \in \mathcal{L}\mathcal{A}$ ist auch $\mathcal{A} \models \exists \vec{x} \kappa(\vec{x})$, im Widerspruch zu $\mathcal{A} \models \forall \vec{x} \neg \kappa(\vec{x})$. (ii) \Rightarrow (iii): Wegen $\mathcal{A} \preceq \mathcal{A}'$ ist $\mathcal{A}' \models D_{el} \mathcal{A} \supseteq D_{\forall} \mathcal{A}$. Daher ist auch $\mathcal{B} \models D_{\forall} \mathcal{A}$, denn $\mathcal{B} \subseteq \mathcal{A}'$. (iii) \Rightarrow (i): $\mathcal{B} \models D_{\forall} \mathcal{A}$ besagt, jede in \mathcal{A} gültige \forall -Aussage aus $\mathcal{L}\mathcal{A}$ gilt auch in \mathcal{B} , was mit (i) offenbar gleichwertig ist. \square

Satz 4.9. *Eine Theorie T ist eine $\forall\exists$ -Theorie genau dann, wenn T induktiv ist.*

Beweis. Wie schon gezeigt, ist eine $\forall\exists$ -Theorie T induktiv. Sei T umgekehrt induktiv. Wir zeigen $\text{Md } T = \text{Md } T_{\forall\exists}$, wobei $T_{\forall\exists}$ die Menge aller in T beweisbaren $\forall\exists$ -Sätze ist. Nichttrivial ist nur der Nachweis von $\text{Md } T_{\forall\exists} \subseteq \text{Md } T$. Sei also $\mathcal{A} \models T_{\forall\exists}$. Behauptung: $T \cup D_{\forall} \mathcal{A}$ ist konsistent. Andernfalls ist $\vdash_T \neg \kappa$ für eine gewisse Konjunktion $\kappa = \kappa(\vec{a})$ von Aussagen aus $D_{\forall} \mathcal{A}$ mit dem Tupel \vec{a} der in κ aber nicht in T vorkommenden Konstanten aus A . Also $\vdash_T \forall \vec{x} \neg \kappa(\vec{x})$. Weil aber $\kappa(\vec{x})$ zu einer \forall -Formel, also $\neg \kappa(\vec{x})$ zu einer \exists -Formel äquivalent ist, gehört $\forall \vec{x} \neg \kappa(\vec{x})$ bis auf Äquivalenz zu $T_{\forall\exists}$, d.h. $\mathcal{A} \models \forall \vec{x} \neg \kappa(\vec{x})$. Das aber widerspricht $\mathcal{A} \models \kappa(\vec{a})$. Sei nun $\mathcal{A}_1 \models T \cup D_{\forall} \mathcal{A}$ und o.B.d.A. $\mathcal{A}_1 \supseteq \mathcal{A}$. Dann ist $\mathcal{A} \subseteq_{ec} \mathcal{A}_1$ nach Lemma 4.8. Nach demselben Lemma gibt es also ein $\mathcal{A}_2 \supseteq \mathcal{A}_1$ mit $\mathcal{A}_0 := \mathcal{A} \preceq \mathcal{A}_2$, so dass auch $\mathcal{A}_2 \models T_{\forall\exists}$. Nun wiederholen

wir diese Konstruktion mit \mathcal{A}_2 statt mit \mathcal{A}_0 und erhalten Strukturen $\mathcal{A}_3, \mathcal{A}_4$ derart, dass $\mathcal{A}_2 \subseteq_{ec} \mathcal{A}_3 \models T$, $\mathcal{A}_3 \subseteq \mathcal{A}_4$ und $\mathcal{A}_2 \preccurlyeq \mathcal{A}_4$. Fortsetzung dieser Konstruktion ergibt eine Folge $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \dots$ von Strukturen mit den in der folgenden Figur angegebenen Inklusionsbeziehungen:

$$\mathcal{A} = \mathcal{A}_0 \xrightarrow{\subseteq} \mathcal{A}_1 \xrightarrow{\subseteq} \mathcal{A}_2 \xrightarrow{\subseteq} \mathcal{A}_3 \xrightarrow{\subseteq} \mathcal{A}_4 \cdot \cdot \cdot \subseteq \mathcal{C}$$

Sei $\mathcal{C} := \bigcup_{i \in \mathbb{N}} \mathcal{A}_i$. Offenbar ist auch $\mathcal{C} = \bigcup_{i \in \mathbb{N}} \mathcal{A}_{2i}$, und weil $\mathcal{A} = \mathcal{A}_0 \preccurlyeq \mathcal{A}_2 \preccurlyeq \dots$, gilt $\mathcal{A} \preccurlyeq \mathcal{C}$ nach dem Kettenlemma. Andererseits ist auch $\mathcal{C} = \bigcup_{i \in \mathbb{N}} \mathcal{A}_{2i+1}$, und weil nach Konstruktion $\mathcal{A}_{2i+1} \models T$ für alle i , ist $\mathcal{C} \models T$, denn T ist induktiv. Wegen $\mathcal{A} \preccurlyeq \mathcal{C}$ ist dann aber auch $\mathcal{A} \models T$, wie zu beweisen war. \square

Für konsistente Theorien T_0, T_1 , so muss $T_0 + T_1$ nicht notwendig wieder konsistent sein, selbst dann nicht, wenn T_0 und T_1 in folgendem Sinne *modellverträglich* sind: jedes T_0 -Modell ist in ein T_1 -Modell einbettbar und umgekehrt, oder gleichwertig $T_{0\forall} = T_{1\forall}$. Ein Beispiel präsentiert Übung 3. Deshalb ist die Voraussetzung der Induktivität in der an einer Stelle in 5.5 benötigten Übung 4 eine wesentliche.

Übungen

1. Man zeige, ein Halbverband ist einbettbar in einen (distributiven) Verband. Die Theorie der Halbverbände axiomatisiert also die \forall -Sätze der Verbandstheorie in nur einer der beiden Operationen.
2. Sei X eine Menge *negationsloser* Aussagen, d.h. die $\alpha \in X$ seien aus Primformeln nur mittels $\wedge, \vee, \forall, \exists$ aufgebaut. Man zeige für beliebige \mathcal{A}, \mathcal{B} : Ist $\mathcal{A} \models X$ und \mathcal{B} homomorphes Bild von \mathcal{A} , so auch $\mathcal{B} \models X$. Es gilt auch hier wieder die Umkehrung (siehe z.B. [CK]; negationslose Aussagen heißen dort *positiv*).
3. Man zeige, die Theorie **DO** der dichten und die Theorie **SO** der diskreten Ordnungen sind modellverträglich, obwohl **DO** + **SO** sicher inkonsistent ist. Weil **DO** induktiv ist, kann damit **SO** nach Übung 4 nicht induktiv und folglich keine $\forall\exists$ -Theorie sein. Inspektion der Axiome zeigt, sie ist eine (echte) $\forall\exists\forall$ -Theorie.
4. Seien T_0 und T_1 modellverträglich und induktiv. Dann ist auch $T = T_0 + T_1$ eine induktive, mit T_0 und T_1 modellverträgliche Theorie.
5. Sei T induktiv. Man zeige, unter allen mit T modellverträglichen induktiven Erweiterungen gibt es eine größte, die *induktive Vervollständigung* von T .

5.5 Modellvollständigkeit

Eine Theorie T heißt nach [Ro1] *modellvollständig*, wenn für jedes Modell $\mathcal{A} \models T$ die Theorie $T + D\mathcal{A}$ in $\mathcal{L}\mathcal{A}$ vollständig ist. Für $\mathcal{A}, \mathcal{B} \models T$ mit $\mathcal{A} \subseteq \mathcal{B}$, mit anderen Worten $\mathcal{A}_A, \mathcal{B}_A \models D\mathcal{A}$, bedeutet dies offenbar $\mathcal{A}_A \equiv_{\mathcal{L}\mathcal{A}} \mathcal{B}_A$ und folglich $\mathcal{A} \preceq \mathcal{B}$. Kurzum, eine modellvollständige Theorie T hat die Eigenschaft

$$(\star) \quad \mathcal{A} \subseteq \mathcal{B} \Rightarrow \mathcal{A} \preceq \mathcal{B}, \text{ für alle } \mathcal{A}, \mathcal{B} \models T.$$

Ist umgekehrt (\star) erfüllt, so ist $T + D\mathcal{A}$ auch vollständig. Denn sei $\mathcal{B} \models T, D\mathcal{A}$, so dass o.B.d.A. $\mathcal{A} \subseteq \mathcal{B}$ und mithin $\mathcal{A} \preceq \mathcal{B}$. Dann sind alle diese \mathcal{B} in $\mathcal{L}\mathcal{A}$ zu \mathcal{A}_A und damit untereinander elementar-äquivalent, d.h. $T + D\mathcal{A}$ ist vollständig. (\star) ist demnach eine gleichwertige Definition der Modellvollständigkeit.

Nach (\star) ist mit $T \subseteq \mathcal{L}$ auch jede Erweiterungstheorie in \mathcal{L} modellvollständig. Ferner ist T dann induktiv und damit eine $\forall\exists$ -Theorie. Denn eine Kette K von T -Modellen ist wegen (\star) immer schon eine elementare. Da nach dem Kettenlemma 4.7 $\mathcal{A} \preceq \bigcup K$ für ein beliebiges $\mathcal{A} \in K$, ist wegen $\mathcal{A} \models T$ dann auch $\bigcup K \models T$. Demnach können nur $\forall\exists$ -Theorien modellvollständig sein.

Eine modellvollständige Theorie muss nicht vollständig sein, wie z.B. Satz 5.4 zeigen wird. Auch die Umkehrung ist i.a. falsch. So hat die nach 5.3 vollständige Theorie SO_{10} die Modelle $\mathcal{A} = (\mathbb{N}_+, <)$ und $\mathcal{B} = (\mathbb{N}, <)$ mit $\mathcal{A} \subseteq \mathcal{B}$ und $\mathcal{A} \not\preceq \mathcal{B}$, wie auf Seite 133 schon bemerkt wurde. Es gilt aber der folgende Satz, mit dem man die Vollständigkeit einer Theorie oft leichter nachweisen kann als mit anderen Methoden.

Satz 5.1. *Ist T modellvollständig und hat T ein Primmodell, so ist T vollständig.*

Beweis. Sei $\mathcal{A} \models T$ und $\mathcal{P} \models T$ ein Primmodell. Dann ist $\mathcal{P} \subseteq \mathcal{A}$ bis auf Isomorphie, also $\mathcal{P} \preceq \mathcal{A}$ und damit $\mathcal{P} \equiv \mathcal{A}$. Folglich sind alle T -Modelle zu \mathcal{P} und damit auch untereinander elementar-äquivalent, d.h. T ist vollständig. \square

Der folgende Satz gibt weitere Charakterisierungen der Modellvollständigkeit an. Insbesondere (ii) – eine Abschwächung von (\star) – ist oft einfacher verifizierbar als die Definition und wird sehr häufig benutzt. Die Äquivalenz (i) \Leftrightarrow (ii) heißt auch *Robinsons Test* für Modellvollständigkeit.

Satz 5.2. *Für eine beliebige Theorie T sind gleichwertig*

- (i) *T ist modellvollständig,*
- (ii) *Für alle $\mathcal{A}, \mathcal{B} \models T$ mit $\mathcal{A} \subseteq \mathcal{B}$ ist $\mathcal{A} \subseteq_{ec} \mathcal{B}$,*
- (iii) *Jede \exists -Formel α ist in T zu einer \forall -Formel β mit $\text{frei}\beta \subseteq \text{frei}\alpha$ äquivalent,*
- (iv) *Jede Formel α ist in T zu einer \forall -Formel β mit $\text{frei}\beta \subseteq \text{frei}\alpha$ äquivalent.*

Beweis. (i) \Rightarrow (ii): evident, denn $\mathcal{A} \subseteq \mathcal{B} \Rightarrow \mathcal{A} \preceq \mathcal{B} \Rightarrow \mathcal{A} \subseteq_{ec} \mathcal{B}$. (ii) \Rightarrow (iii): Nach Satz 4.6 genügt es zu zeigen, dass jede \exists -Formel $\alpha = \alpha(\vec{x}) \in \mathcal{L}$ persistent in T ist. Es seien $\mathcal{A}, \mathcal{B} \models T$, $\mathcal{A} \subseteq \mathcal{B}$. Mit $\vec{a} \in A^n$ und $\mathcal{B} \models \alpha(\vec{a})$ gilt dann auch $\mathcal{A} \models \alpha(\vec{a})$, denn wegen (ii) ist $\mathcal{A} \subseteq_{ec} \mathcal{B}$. (iii) \Rightarrow (iv): Induktion über α ; (iii) wird beim \neg -Schritt benötigt. (iv) \Rightarrow (i): Seien $\mathcal{A}, \mathcal{B} \models T$, $\mathcal{A} \subseteq \mathcal{B}$ und $\mathcal{B} \models \alpha(\vec{a})$, mit $\vec{a} \in A^n$. Weil $\alpha(\vec{x})$ zu einer \forall -Formel in T äquivalent ist, gilt dann gewiss auch $\mathcal{A} \models \alpha(\vec{a})$. Damit wurde $\mathcal{A} \preceq \mathcal{B}$ und wegen der Kennzeichnung (\star) auch (i) bewiesen. \square

Bemerkung. Ist T abzählbar und hat nur unendliche Modelle, kann man sich bei der Formulierung des Kriteriums von Robinson (ii) auf Modelle \mathcal{A}, \mathcal{B} einer beliebig gewählten unendlichen Kardinalzahl κ beschränken. Denn nach der Bemerkung Seite 147 folgt daraus bereits (iii) und damit auch (i). Dies ist bedeutsam für Lindströms Kriterium Satz 5.7.

Ein relativ einfaches Beispiel einer modellvollständigen Theorie ist $T_{V\mathbb{Q}}$, die Theorie der (nichttrivialen) \mathbb{Q} -Vektorräume $\mathcal{V} = (V, +, 0, \mathbb{Q})$, wobei 0 den Nullvektor bezeichnet und jedes $r \in \mathbb{Q}$ als einstellige Operation auf der Vektormenge V zu verstehen ist. $T_{V\mathbb{Q}}$ formuliert die bekannten Vektoraxiome, wobei z.B. das Axiom $r(a+b) = ra + rb$ durch ein Schema von Aussagen, nämlich $\forall ab(r(a+b) = ra + rb)$ für jedes $r \in \mathbb{Q}$, wiedergegeben wird. Seien $\mathcal{V}, \mathcal{V}' \models T_{V\mathbb{Q}}$ mit $\mathcal{V} \subseteq \mathcal{V}'$. Wir behaupten $\mathcal{V} \subseteq_{ec} \mathcal{V}'$. Nach Satz 5.2(iii) ist $T_{V\mathbb{Q}}$ damit modellvollständig. Zum Nachweis der Behauptung sei $\mathcal{V}' \models \exists \vec{x} \alpha$, mit einer Konjunktion α von Literalen in x_1, \dots, x_n und Konstanten $a_1, \dots, a_n, b_1, \dots, b_k \in V$. Dann ist α o.B.d.A. ein System der Gestalt

$$(s) \quad \begin{cases} r_{11}x_1 + \dots + r_{1n}x_n = a_1 & s_{11}x_1 + \dots + s_{1n}x_n \neq b_1 \\ \vdots & \vdots \\ r_{m1}x_1 + \dots + r_{mn}x_n = a_m & s_{k1}x_1 + \dots + s_{kn}x_n \neq b_k \end{cases}$$

Denn die einzigen Primformeln sind Termgleichungen, und jeder Term in x_1, \dots, x_n ist in $T_{V\mathbb{Q}}$ äquivalent zu einem Term der Gestalt $r_1x_1 + \dots + r_nx_n$. Nach den Eigenschaften linearer Gleichungssysteme ist plausibel, dass das System (s) schon eine Lösung in \mathcal{V} hat, wenn es überhaupt eine Lösung hat. Eine andere Schlussweise beruht auf der leicht beweisbaren \aleph_1 -Kategorizität von $T_{V\mathbb{Q}}$, siehe die Beispiele am Ende des Abschnitts. Für Verallgemeinerungen sei z.B. auf [Zi] verwiesen.

Für den Rest dieses Abschnitts werden einige Kenntnisse der klassischen Algebra vorausgesetzt. Dort werden häufig sogenannte *Abschlusskonstruktionen* ausgeführt. So hat jeder Körper einen *algebraischen Abschluss* (eine *Primmodellerweiterung* in ACF, siehe hierzu [Sa] oder [Sh]), jeder geordnete Körper hat einen reellen Abschluss, jede torsionsfreie abelsche Gruppe hat einen dividierbaren Abschluss usw.

Sei T eine Theorie und $\mathcal{A} \models T_{\forall}$. Unter dem *Abschluss von \mathcal{A} in T* verstehen wir ein T -Modell $\bar{\mathcal{A}} \supseteq \mathcal{A}$, so dass für jedes $\mathcal{B} \models T$ mit $\mathcal{A} \subseteq \mathcal{B}$ eine Einbettung von $\bar{\mathcal{A}}$ in \mathcal{B} existiert, die \mathcal{A} punktweise festlässt; ferner soll $\bar{\mathcal{A}}$ in folgendem Sinne minimal

sein: ist $\mathcal{A} \subseteq \mathcal{A}' \subseteq \bar{\mathcal{A}}$ und $\mathcal{A}' \models T$, so ist $\mathcal{A}' \simeq \bar{\mathcal{A}}$. Wir sagen dann, T *gestatte eine Abschlussoperation*. $\bar{\mathcal{A}}$ ist bis auf Isomorphie eindeutig bestimmt, wie man leicht beweist. Sei ferner $\mathcal{A}, \mathcal{B} \models T$, $\mathcal{A} \subset \mathcal{B}$ und $b \in B \setminus A$. Dann gibt es ein kleinstes $A \cup \{b\}$ enthaltendes T_V -Submodell von \mathcal{B} , das mit $\mathcal{A}(b)$ bezeichnet sei. Nach dem Gesagten gibt es ein $\mathcal{C} \simeq \bar{\mathcal{A}(b)}$ mit $\mathcal{A} \subset \mathcal{C} \subseteq \mathcal{B}$, das nachfolgend mit \mathcal{A}^b bezeichnet und eine *unmittelbare Erweiterung* von \mathcal{A} in T genannt werde. Stets ist $\mathcal{A} \subset \mathcal{A}^b$.

Beispiel 1. Sei $T := \text{ACF}$. Ein T_V -Modell \mathcal{A} ist hier ein Integritätsbereich. T gestattet eine Abschlussoperation, und zwar ist $\bar{\mathcal{A}}$ der *algebraische Abschluss* des Quotientenkörpers von \mathcal{A} . Dass eine in jeden a.a. Körper $\mathcal{B} \supseteq \mathcal{A}$ einbettbare a.a. Körpererweiterung $\bar{\mathcal{A}}$ existiert, ist der Hauptsatz von Steinitz über a.a. Körper, [Wae, S. 201]. Für $\mathcal{A}, \mathcal{B} \models T$ mit $\mathcal{A} \subset \mathcal{B}$ und $b \in B \setminus A$ ist b offenbar transzendent über \mathcal{A} , denn \mathcal{A} ist schon a.a. Also $a_0 + a_1b + \dots + a_nb^n \neq 0$ für alle $a_i \in A$ mit $a_n \neq 0$. Deswegen ist $\mathcal{A}(b)$ isomorph zum Ring aller Polynome $a_0 + a_1x + \dots + a_nx^n$ mit der „Unbestimmten“ x , und dessen Quotientenkörper besteht aus allen Quotienten dieser Polynome (oder den rationalen Funktionen mit Koeffizienten aus A). Ist daher $\mathcal{A}, \mathcal{B}, \mathcal{C} \models T$ mit $\mathcal{A} \subset \mathcal{B}, \mathcal{C}$, sowie $b \in B \setminus A$ und $c \in C \setminus A$, so ist $\mathcal{A}(b) \simeq \mathcal{A}(c)$. Dieser Isomorphismus setzt sich auf natürliche Weise fort zu einem solchen des Abschlusses \mathcal{A}^b von $\mathcal{A}(b)$ auf den Abschluss \mathcal{A}^c von $\mathcal{A}(c)$. Daher hat ein T -Modell im vorliegenden Falle bis auf Isomorphie nur eine unmittelbare Erweiterung in T .

Beispiel 2. Sei $T := \text{RCF}$ die Theorie der reell abgeschlossenen Körper. Darunter sei ein geordneter Körper \mathcal{K} verstanden, in welchem jedes Polynom ungeraden Grades mit Koeffizienten aus \mathcal{K} eine Nullstelle hat und jedes positive Element ein Quadrat in \mathcal{K} ist. Die Vorbildstruktur ist hier der Körper \mathbb{R} . In der Algebra wird auf die Ordnung oft verzichtet, weil diese wegen $\mathcal{K} \models x \leq y \leftrightarrow \exists z y - x = z^2$ definierbar ist. Ein T_V -Modell \mathcal{A} ist ein geordneter Integritätsbereich, dessen Quotientenkörper wieder geordnet ist. Nach dem Hauptsatz von Artin über reell abgeschlossene Körper [Wae, S. 244] ist ein $\bar{\mathcal{A}} \models \text{RCF}$ konstruierbar, das den Abschluss von \mathcal{A} in T im obigen Sinne darstellt. Für $\mathcal{A}, \mathcal{B} \models \text{RCF}$, $\mathcal{A} \subset \mathcal{B}$, $b \in B \setminus A$ ist b wieder transzendent über \mathcal{A} , weil keine algebraische Erweiterung von \mathcal{A} mehr ordnungsfähig ist – dies ist eine von vielen Kennzeichnungen reeller Abgeschlossenheit. $\mathcal{A}(b)$ ist eine (einfache) transzendente Erweiterung von \mathcal{A} und lässt sich als geordneter Polynomring über \mathcal{A} verstehen, dessen Anordnung den Isomorphietyp seines Quotientenkörpers und auch den des (reellen) Abschlusses \mathcal{A}^b eindeutig bestimmt.

Für induktives T darf man sich bei Robinsons Test zum Nachweis der Modellvollständigkeit ganz auf unmittelbare Erweiterungen beschränken. Und zwar wegen

Lemma 5.3. *Sei T induktiv, und T gestatte eine Abschlussoperation. Es gelte ferner $\mathcal{A} \subseteq_{ec} \mathcal{A}'$ für alle $\mathcal{A}, \mathcal{A}' \models T$ für den Fall, dass \mathcal{A}' unmittelbare Erweiterung von \mathcal{A} ist. Dann ist T modellvollständig.*

Beweis. Seien $\mathcal{A}, \mathcal{B} \models T$, $\mathcal{A} \subseteq \mathcal{B}$. Nach Satz 5.2(ii) genügt zu zeigen $\mathcal{A} \subseteq_{ec} \mathcal{B}$. Sei H die Menge aller $\mathcal{C} \subseteq \mathcal{B}$ mit $\mathcal{A} \subseteq_{ec} \mathcal{C} \models T$. Trivialerweise ist $\mathcal{A} \in H$. Weil T induktiv ist, liegt für jede Kette $K \subseteq H$ auch $\bigcup K$ wieder in H , denn $\mathcal{A} \subseteq_{ec} \bigcup K$, wenn nur $\mathcal{A} \subseteq_{ec} \mathcal{C}$ für jedes $\mathcal{C} \in K$. Nach dem Zornschen Lemma hat H ein maximales Element \mathcal{A}_m . Wir zeigen $\mathcal{A}_m = \mathcal{B}$. Angenommen $\mathcal{A}_m \subset \mathcal{B}$. Dann gibt es eine unmittelbare Erweiterung $\mathcal{A}'_m \models T$ von \mathcal{A}_m mit $\mathcal{A}_m \subset \mathcal{A}'_m \subseteq \mathcal{B}$. Nach Voraussetzung ist $\mathcal{A} \subseteq_{ec} \mathcal{A}_m$ und $\mathcal{A}_m \subseteq_{ec} \mathcal{A}'_m$, also $\mathcal{A} \subseteq_{ec} \mathcal{A}'_m$. Das widerspricht aber der Maximalität von \mathcal{A}_m in H . Folglich muss $\mathcal{A}_m = \mathcal{B}$ sein, also $\mathcal{A} \subseteq_{ec} \mathcal{B}$. \square

Satz 5.4. *ACF ist modellvollständig und damit auch ACF_p , die Theorie der a.a. Körper vorgegebener Charakteristik p . Darüber hinaus ist ACF_p auch vollständig.*

Beweis. Sei $\mathcal{A}, \mathcal{B} \models \text{ACF}$, $\mathcal{A} \subset \mathcal{B}$ und $b \in B \setminus A$. Nach Lemma 5.3 genügt zu zeigen $\mathcal{A} \subseteq_{ec} \mathcal{A}^b$, mit der unmittelbaren Erweiterung \mathcal{A}^b von \mathcal{A} in ACF . Sei $\alpha := \exists \vec{x} \beta(\vec{x}, \vec{a})$ eine \exists -Aussage aus \mathcal{L}_A mit $\mathcal{A}^b \models \alpha$. Zum Beweise von $\mathcal{A} \models \alpha$ betrachten wir

$$X := \text{ACF} \cup D\mathcal{A} \cup \{P(x) \neq 0 \mid P(x) \text{ Hauptpolynom über } A\}.$$

Interpretiert man hier x durch b aus \mathcal{A}^b , so sieht man, dass (\mathcal{A}^b, b) Modell ist für X . Sei (\mathcal{C}, c) ein beliebiges Modell für X , wobei c der Wert von x ist. Wegen $D\mathcal{A} \subseteq X$ ist o.B.d.A. $\mathcal{A} \subseteq \mathcal{C}$. Weil $\mathcal{A}^b \simeq \mathcal{A}^c$ nach Beispiel 1, ist auch $\mathcal{A}^c \models \alpha$, und wegen $\mathcal{A}^c \subseteq \mathcal{C}$ folgt $\mathcal{C} \models \alpha$, denn α ist eine \exists -Aussage. Da (\mathcal{C}, c) hier völlig beliebig gewählt worden war, erhalten wir $X \vdash \alpha$ und hieraus offenbar

$$D\mathcal{A} \vdash_{\text{ACF}} \bigwedge_{i \leq k} P_i(x) \neq 0 \rightarrow \alpha \text{ für gewisse Hauptpolynome } P_0, \dots, P_k.$$

Vordere Partikularisierung liefert $D\mathcal{A} \vdash_{\text{ACF}} \exists x \bigwedge_{i \leq k} P_i(x) \neq 0 \rightarrow \alpha$. Nun ist jeder a.a. Körper unendlich, und jedes Polynom hat in einem Körper nur endlich viele Nullstellen. Daher ist $D\mathcal{A} \vdash_{\text{ACF}} \exists x \bigwedge_{i \leq k} P_i(x) \neq 0$. Also $D\mathcal{A} \vdash_{\text{ACF}} \alpha$ und somit $\mathcal{A} \models \alpha$. Damit wurde $\mathcal{A} \subseteq_{ec} \mathcal{A}^b$ bewiesen und mithin der erste Teil des Satzes. Der algebraische Abschluss des Primkörpers der Charakteristik p ist offenbar Primmodell von ACF_p . Folglich ist ACF_p nach Satz 5.1 auch vollständig. \square

Ähnlich erhalten wir auch den folgenden bedeutsamen Satz, der von Tarski in [Ta2] zuerst durch Quantorenelimination bewiesen wurde; die darin behauptete Vollständigkeit wäre übrigens mit dem Kriterium von Vaught nicht zu gewinnen.

Satz 5.5. *Die Theorie RCF der reell abgeschlossenen Körper ist modellvollständig und vollständig. Sie ist also identisch mit der Theorie des geordneten Körpers der reellen Zahlen und als vollständige axiomatisierbare Theorie auch entscheidbar.*

Beweis. Sei $\mathcal{A} \models \text{RCF}$. Es genügt wieder zu zeigen $\mathcal{A} \subseteq_{ec} \mathcal{A}^b$ für eine unmittelbare Erweiterung \mathcal{A}^b von \mathcal{A} in RCF . Sei $U_b = \{a \in A \mid a <^{\mathcal{B}} b\}$ und $V_b = \{a \in A \mid b <^{\mathcal{B}} a\}$, mit $\mathcal{B} := \mathcal{A}^b$. Dann ist $U_b \cup V_b = A$. Sei nun $\mathcal{A}^b \models \exists \vec{x} \beta(\vec{x}, \vec{a})$ eine \exists -Aussage mit $\vec{a} \in A^m$. Das Modell (\mathcal{B}, b) erfüllt dann offensichtlich die Formelmenge

$$X := \text{RCF} \cup D\mathcal{A} \cup \{a < x \mid a \in U_b\} \cup \{x < a \mid a \in V_b\}.$$

Sei $(\mathcal{C}, c) \models X$, mit der Interpretation c von x , wobei \mathcal{C} wegen $D\mathcal{A} \subseteq X$ als Erweiterung von \mathcal{A} verstanden werden kann. c ist nach einer Bemerkung in Beispiel 2 transzendent über \mathcal{A} , also ist $\mathcal{A}(c)$ isomorph zum angeordneten Polynomring über \mathcal{A} mit der Unbestimmten c , dessen Anordnung durch diejenige von $\mathcal{A} \cup \{c\}$ bereits eindeutig bestimmt ist. Folglich ist $\mathcal{A}(b) \simeq \mathcal{A}(c)$, und dieser Isomorphismus setzt sich über die Quotientenkörper fort auf einen solchen zwischen dem reellen Abschluss \mathcal{A}^b und \mathcal{A}^c von $\mathcal{A}(b)$ bzw. $\mathcal{A}(c)$. Wie in Satz 5.4 erhalten wir damit $X \vdash \alpha$, also

$$D\mathcal{A} \vdash_{\text{RCF}} \exists x (\bigwedge_{i < k} a_i < x \wedge \bigwedge_{i < m} x < b_i) \rightarrow \alpha \quad (a_i \in U_b, b_i \in V_b, k + m > 0).$$

Nun ist bereits $\vdash_{\text{RCF}} \exists x (\bigwedge_{i < k} a_i < x \wedge \bigwedge_{i < m} x < b_i)$; denn ein geordneter Körper ist dicht geordnet ohne Randelemente (man beachte auch die Fälle $k = 0$ oder $m = 0$). Damit folgt $D\mathcal{A} \vdash_{\text{RCF}} \alpha$. Also $\mathcal{A} \models \alpha$, und $\mathcal{A} \subseteq_{ec} \mathcal{A}^b$ ist gezeigt. RCF hat ein Primmodell, nämlich den reellen Abschluss von \mathbb{Q} , den geordneten Körper der reellen algebraischen Zahlen. Mithin ist RCF nach Satz 5.1 vollständig. \square

Eine Theorie T heie die *Modellvervollständigung* einer Theorie T_0 derselben Sprache, wenn $T_0 \subseteq T$ und $T + D\mathcal{A}$ vollständig ist für jedes $\mathcal{A} \models T_0$. Weiter unten wird die eindeutige Bestimmtheit von T gezeigt, wenn ein solches T existiert. Offensichtlich ist T dann modellvollständig und mit T_0 modellverträglich. Die Existenz einer modellvollständigen Erweiterung ist daher eine notwendige Bedingung für die Existenz der Modellvervollständigung einer Theorie. Nicht jede Theorie hat eine Modellvervollständigung. Einfache Gegenbeispiele präsentiert Übung 1.

Nun zum Eindeutigkeitsbeweis. Seien T, T' Modellvervollständigungen von T_0 . Beide Theorien sind mit T_0 , also auch untereinander modellverträglich. Weil T, T' als modellvollständige Theorien überdies induktiv sind, ist $T + T'$ nach Übung 4 in 5.4 mit T modellverträglich. Ist also $\mathcal{A} \models T$, so gibt es ein $\mathcal{B} \models T + T'$ mit $\mathcal{A} \subseteq \mathcal{B}$, und da T modellvollständig ist, haben wir $\mathcal{A} \preceq \mathcal{B}$. Daher ist $\mathcal{A} \equiv \mathcal{B} \models T'$, und folglich $\mathcal{A} \models T'$. Aus Symmetriegründen gilt auch $\mathcal{A} \models T' \Rightarrow \mathcal{A} \models T$, also $T = T'$.

Beispiel 3. ACF ist die Modellvervollständigung der Theorie T_J aller Integritätsbereiche und damit erst recht der Theorie T_K aller Körper. Denn mit ACF und $\mathcal{A} \models T_J$ ist offenbar auch $T := \text{ACF} + D\mathcal{A}$ modellvollständig. Weil T ein Primmodell hat – den algebraischen Abschluss des Quotientenkörpers von \mathcal{A} – ist T überdies vollständig. Völlig analog zeigt man, dass RCF die Modellvervollständigung der Theorie der kommutativen geordneten Ringe mit Einselement ist.

$\mathcal{A} \models T$ heie *existentiell abgeschlossen* (kurz \exists -abgeschlossen) in T , wenn $\mathcal{A} \subseteq_{ec} \mathcal{B}$ für jedes $\mathcal{B} \models T$ mit $\mathcal{A} \subseteq \mathcal{B}$. So ist z.B. jeder a.a. Körper \exists -abgeschlossen in der Körpertheorie. Denn ist $\mathcal{A} \models \text{ACF}$, $\mathcal{B} \supseteq \mathcal{A}$ ein Körper und \mathcal{C} eine a.a. Erweiterung von \mathcal{B} , so ist $\mathcal{A} \preceq \mathcal{C}$ wegen der Modellvollständigkeit von ACF und damit $\mathcal{A} \subseteq_{ec} \mathcal{B}$.

nach Lemma 4.8. Der folgende Satz verallgemeinert in gewissem Sinne die Tatsache, dass jeder Körper in einen a.a. Körper einbettbar ist. Danach ist z.B. auch eine Gruppe in eine in der Gruppentheorie \exists -abgeschlossene Gruppe einbettbar.

Satz 5.6. *Sei T eine $\forall\exists$ -Theorie einer abzählbaren Sprache \mathcal{L} . Dann kann jedes unendliche Modell \mathcal{A} von T zu einem Modell \mathcal{A}^* von T mit $|\mathcal{A}^*| = |\mathcal{A}|$ erweitert werden, welches \exists -abgeschlossen ist in T .*

Beweis. Für den Beweis werde der Einfachheit halber angenommen, \mathcal{A} sei abzählbar. Dann ist auch $\mathcal{L}\mathcal{A}$ abzählbar. Sei $\alpha_0, \alpha_1, \dots$ eine Abzählung der \exists -Aussagen von $\mathcal{L}\mathcal{A}$ ⁸⁾ und $\mathcal{A}_0 = \mathcal{A}$, sowie \mathcal{A}_{n+1} eine Erweiterung von \mathcal{A}_n in $\mathcal{L}\mathcal{A}$ mit $\mathcal{A}_{n+1} \models T + \alpha_n$, falls eine solche Erweiterung existiert; sonst sei $\mathcal{A}_{n+1} = \mathcal{A}_n$. Weil T induktiv ist, folgt $\mathcal{B}_0 = \bigcup_{n \in \mathbb{N}} \mathcal{A}_n \models T$. Ist $\alpha = \alpha_n$ eine in einer Erweiterung $\mathcal{B} \models T$ von \mathcal{B}_0 gültige \exists -Aussage aus $\mathcal{L}\mathcal{A}$, ist schon $\mathcal{A}_{n+1} \models \alpha$ und damit auch $\mathcal{B}_0 \models \alpha$. Nun wiederholen wir diese Konstruktion mit \mathcal{B}_0 statt \mathcal{A}_0 bzgl. einer Aufzählung aller \exists -Aussagen aus $\mathcal{L}\mathcal{B}_0$ und erhalten eine $\mathcal{L}\mathcal{B}_0$ -Struktur $\mathcal{B}_1 \models T$. Fortlaufende Wiederholung liefert eine Folge $\mathcal{B}_1 \subseteq \mathcal{B}_2 \subseteq \dots$ von $\mathcal{L}\mathcal{B}_n$ -Strukturen $\mathcal{B}_{n+1} \models T$. Für das \mathcal{L} -Redukt \mathcal{A}^* von $\bigcup_{n \in \mathbb{N}} \mathcal{B}_n \models T$ ist die Behauptung des Satzes dann unschwer zu verifizieren. Man beachte dabei, dass eine \exists -Aussage aus $\mathcal{L}\mathcal{A}^*$ schon in einem gewissen $\mathcal{L}\mathcal{B}_m$ liegt. \square

Hiermit erhält man leicht das folgende sehr anwendungsfähige Kriterium zum Nachweis der Modellvollständigkeit von gewissen Theorien, die nach dem Kriterium von Vaught immer auch zugleich vollständig sind:

Satz 5.7 (Lindströms Kriterium). *Eine abzählbare κ -kategorische $\forall\exists$ -Theorie T ist modellvollständig, sofern sie nur unendliche Modelle besitzt.*

Beweis. Weil alle T -Modelle unendlich sind, hat T ein Modell der Mächtigkeit κ und nach Satz 5.6 auch ein solches, das \exists -abgeschlossen ist in T . Dann aber sind sämtliche κ -mächtigen T -Modelle \exists -abgeschlossen in T , denn alle diese Modelle sind isomorph. Also $\mathcal{A} \subseteq \mathcal{B} \Rightarrow \mathcal{A} \subseteq_{ec} \mathcal{B}$, für alle $\mathcal{A}, \mathcal{B} \models T$ der Mächtigkeit κ . Nach der Bemerkung auf Seite 152 ist T damit bereits modellvollständig. \square

Anwendungsbeispiele. (a) Die (\aleph_0 -kategorische) Theorie der atomlosen Booleschen Algebren. (b) Die (\aleph_1 -kategorische) Theorie der nichttrivialen \mathbb{Q} -Vektorräume. (c) Die (\aleph_1 -kategorische) Theorie der a.a. Körper gegebener Charakteristik.

Aus (c) folgt auf neue Weise auch die Modellvollständigkeit von ACF. Denn ist $\mathcal{A}, \mathcal{B} \models \text{ACF}$ und $\mathcal{A} \subseteq \mathcal{B}$, so haben beide Körper dieselbe Charakteristik p . Da ACF_p nach (c) modellvollständig ist, folgt $\mathcal{A} \preceq \mathcal{B}$. Also ist auch ACF modellvollständig.

⁸⁾Für überabzählbares \mathcal{A} muss man hier wegen $|\mathcal{L}\mathcal{A}| = |\mathcal{A}|$ statt von einer gewöhnlichen von einer ordinalen Abzählung der Elemente von \mathcal{A} ausgehen. Der Beweis ist aber fast derselbe.

Übungen

1. Man zeige, von den vier Theorien DO_{ij} ist nur DO_{00} modellvollständig und die übrigen drei besitzen auch keine Modellvervollständigung.
2. Sei T die Theorie der dividierbaren torsionsfreien abelschen Gruppen. Man zeige (a) T ist modellvollständig, (b) T ist die Modellvervollständigung der Theorie T_0 der torsionsfreien abelschen Gruppen.
3. T^* heißt der *Modellbegleiter* von T , wenn T, T^* modellverträglich sind und T^* modellvollständig ist. Man zeige, existiert T^* , so ist T^* eindeutig bestimmt, und $\text{Md } T^*$ besteht aus allen Modellen, die \exists -abgeschlossen sind in T .
4. Man zeige, eine in allen endlichen Körpern gültige $\forall\exists$ -Aussage gilt in allen a.a. Körpern. Diese Tatsache ist sehr nützlich in der algebraischen Geometrie.

5.6 Quantorenelimination

Wegen $\exists x(y < x \wedge x < z) \equiv_{\text{DO}} y < z$ lässt sich in der Theorie der dicht geordneten Mengen der Quantor aus der Formel links eliminieren. In einigen Theorien, darunter der Theorie DO_{00} (siehe 5.2) lassen sich nun die Quantoren sogar aus jeder Formel eliminieren. Man sagt, $T (\subseteq \mathcal{L}^0)$ erlaubt *Quantorenelimination*, wenn es zu jedem $\varphi \in \mathcal{L}$ ein quantorenfreies $\varphi' \in \mathcal{L}$ mit $\varphi \equiv_T \varphi'$ gibt. Quantorenelimination ist die älteste Methode, um gewisse Theorien als entscheidbar und gegebenenfalls auch als vollständig nachzuweisen. In einigen Darstellungen wird in der Definition zusätzlich *frei* $\varphi' = \text{frei } \varphi$ verlangt, doch ist dies ganz unwesentlich.

Eine die Quantorenelimination erlaubende Theorie T ist nach Satz 5.2 modellvollständig, denn quantorenfreie Formeln sind auch \forall -Formeln. T ist damit eine $\forall\exists$ -Theorie, was eine höchst bemerkenswerte notwendige Bedingung darstellt.

Um die Quantorenelimination für eine Theorie T zu bestätigen, genügt es zunächst einmal, das Präfix $\exists x$ aus jeder Formel der Gestalt $\exists x\alpha$ zu eliminieren, wobei α quantorenfrei ist. Dazu denke man sich in einer Formel φ alle Subformeln der Gestalt $\forall x\alpha$ durch $\neg\exists x\neg\alpha$ äquivalent ersetzt, so dass in φ nur noch der \exists -Quantor erscheint. Schaut man auf das in φ am weitesten rechts vorkommende Präfix $\exists x$ in φ , lässt sich schreiben $\varphi = \dots\exists x\alpha\dots$ mit quantorenfreiem α . Ist nun $\exists x\alpha$ durch eine quantorenfreie Formel α' äquivalent ersetzbar, so lässt sich dieses Verfahren solange wiederholen, bis alle \exists -Quantoren aus φ verschwunden sind.

Nun darf man wegen der \vee -Distributivität des \exists -Quantors außerdem voraussetzen, dass der quantorenfreie Teil α der Formel $\exists x\alpha$, in der $\exists x$ eliminiert werden soll, eine Konjunktion von Literalen ist und dass x in jedem dieser Literale vorkommt. Denn man bringe α in disjunktive Normalform und verteile das Präfix $\exists x$ auf die Disjunktionsglieder. $\exists x$ steht dann nur noch vor einer Konjunktion von Literalen.

Erscheint x in keinem dieser Literale, kann $\exists x$ einfach weggelassen werden. Andernfalls entferne man die x nicht enthaltenden Literale aus dem Wirkungsbereich von $\exists x$. Das geht wegen $\exists x(\alpha \wedge \beta) \equiv \exists x\alpha \wedge \beta$ für $x \notin \text{var}\beta$. Man kann überdies annehmen, dass keines der Konjunktionsglieder die Gestalt $x=t$ mit $x \notin \text{var}t$ hat. Denn $\exists x(x=t \wedge \alpha) \equiv \alpha \frac{t}{x}$, und der Quantor ist rechts bereits eliminiert. Ferner darf man annehmen, dass x nicht die Variable v_0 ist (gebundene Umbenennung) und dass $x=x$ und $x \neq x$ nicht zu den Konjunktionsgliedern gehören. Denn $x=x$ kann durch \top und $x \neq x$ durch \perp äquivalent ersetzt werden. Dabei empfiehlt sich, \top und \perp jetzt durch $v_0=v_0$ bzw. $v_0 \neq v_0$ zu definieren. Bei der Ersetzung wird dann v_0 möglicherweise als neue freie Variable eingeführt, aber das ist harmlos und durch Hinzufügen von \top als 0-stelliges Aussagensymbol zur logischen Signatur von T auch vermeidbar. Eine solche Spracherweiterung ist aber nicht zwingend.

Nennt man eine \exists -Formel *einfach*, wenn sie die Gestalt $\exists x \bigwedge_i \alpha_i$ hat, wobei jedes α_i ein Literal ist mit $x \in \text{var}\alpha_i$, ergeben obige Überlegungen offenbar den

Satz 6.1. *T erlaubt Quantorenelimination, wenn jede einfache \exists -Formel $\exists x \bigwedge_i \alpha_i$ zu einer quantorenfreien Formel in T äquivalent ist. Dabei ist o.B.d.A. keines der α_i die Formel $x=x$, $x \neq x$ oder von der Gestalt $x=t$ mit $x \notin \text{var}t$.*

Beispiel 1. DO_{00} erlaubt Quantorenelimination. Wegen $y \not< z \equiv_T z < y \vee z=y$ und $z \neq y \equiv_T z < y \vee y < z$ und weil allgemein $(\alpha \vee \beta) \wedge \gamma \equiv (\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$, dürfen wir offenbar annehmen, dass die Konjunktion der α_i in Satz 6.1 das Negationszeichen nicht enthält. Wir haben es daher mit einer Formel der Gestalt

$$\exists x(y_1 < x \wedge \dots \wedge y_m < x \wedge x < z_1 \wedge \dots \wedge x < z_k)$$

zu tun, die für $m, k \neq 0$ zu $\bigwedge_{i,j} y_i < z_j$ äquivalent ist, für $m=0$ oder $k=0$ zu \top , falls x keine der Variablen y_i, z_j ist, und sonst zu \perp . Damit ist bereits alles erledigt.

DO selbst erlaubt die Quantorenelimination nicht, weil z.B. in $\alpha(y) := \exists x x < y$ der Quantor nicht eliminierbar ist. Wäre $\alpha(y)$ zu einer quantorenfreien Formel in DO äquivalent, müsste für $\mathcal{A}, \mathcal{B} \models \text{DO}$ mit $\mathcal{A} \subseteq \mathcal{B}$, $a \in A$ und $\mathcal{A} \models \alpha(a)$ auch $\mathcal{B} \models \alpha(a)$ gelten. Das ist aber nicht der Fall für die Intervalle $\mathcal{A} = [1, 2]$, $\mathcal{B} = [0, 2]$ und $a = 1$. Quantorenelimination wird aber wieder möglich in der Signatur, die $\{<\}$ um die 0-stelligen Prädikatensymbole L, R expandiert. Man erhält auch so ein bereits in 5.2 bewiesenes Resultat, wonach $\{L, R\}$ eine Boolesche Basis für DO ist.

Beispiel 2. Ein klassisches Resultat der Quantorenelimination nach M. Presburger bezieht sich auf $Th(\mathbb{N}, 0, 1, +, <)$, mit den durch die expliziten Definitionen

$$m|x \leftrightarrow \exists y \, my = x \quad (my := \underbrace{y + \dots + y}_m)$$

für $m > 1$ zusätzlich eingeführten einstelligigen Prädikatensymbolen $m|$. Wir beweisen ein verwandtes, auf die Gruppe \mathbb{Z} in der Signatur $0, 1, +, -, <, 2|, 3|, \dots$ bezogenes Resultat. k bezeichnet auch den Term $\underbrace{1 + \dots + 1}_k$. Es sei $(-m)x = -mx$.

Sei \mathbf{ZG} die elementare Theorie in $\mathcal{L}\{0, 1, +, -, <, 2|, 3|, \dots\}$, deren Axiome diejenigen für geordnete abelsche Gruppen umfassen, sowie ferner die Aussagen

$$\forall x(0 < x \leftrightarrow 1 \leq x), \forall x(m|x \leftrightarrow \exists y \, my = x) \text{ und } \vartheta_m := \forall x \bigvee_{k < m} m|x + k$$

für $m = 2, 3, \dots$. Die Modelle von \mathbf{ZG} heißen \mathbb{Z} -Gruppen. Diese sind geordnet mit kleinstem positiven Element 1. Die Axiome ϑ_m besagen für das Gruppenredukt von \mathbb{Z} -Gruppen G : die Faktorgruppen G/mG (mit $mG = \{mx \mid x \in G\}$) sind zyklisch von der Ordnung m . Auch gilt $\vdash_{\mathbf{ZG}} \eta_n := 0 \leq x \wedge x < n \rightarrow \bigvee_{k < n} x = k$ für alle n . \mathbf{ZG} ist eine definitorische und daher eine konservative Erweiterung von \mathbf{ZG}_0 , der in $\mathcal{L}_0 := \mathcal{L}\{0, 1, +, -, <\}$ formulierten Theorie der \mathbb{Z} -Gruppen mit obigen Axiomen. Es wird sich herausstellen, dass deren Modelle genau diejenigen geordneten abelschen Gruppen sind, die zur Vorbildstruktur $(\mathbb{Z}, 0, 1, +, -, <)$ elementar-äquivalent sind.

Wir zeigen nun: \mathbf{ZG} erlaubt die Quantorenelimination. Zum Nachweis darf wegen

$$t \neq s \equiv_{\mathbf{ZG}} s < t \vee t < s, m \nmid t \equiv_{\mathbf{ZG}} \bigvee_{i=1}^{m-1} m|t + i \text{ und } m|t \equiv_{\mathbf{ZG}} m| - t$$

angenommen werden, dass der Kern einer einfachen \exists -Formel eine Konjunktion von Formeln der Gestalt $n_i x = t_i^0$, $n'_i x < t_i^1$, $t_i^2 < n''_i x$, $m_i | n'''_i x + t_i^3$ mit $x \notin \text{var } t_i^j$ ist. Durch Multiplikation dieser Formeln mit passenden Zahl kann man unter Beachtung von $t < s \equiv_{\mathbf{ZG}} nt < ns$ und $m|t \equiv_{\mathbf{ZG}} nm|nt$ leicht erreichen, dass die n_i, n'_i, n''_i, n'''_i alle einer Zahl $n > 1$ gleich sind. Dabei verändern sich natürlich die t_i^j und die „Module“ m_i . Aber das Eliminationsproblem reduziert sich so auf Formeln folgender Gestalt, wobei das j -te Konjunktionsglied verschwindet, wenn $k_j = 0$:

$$(1) \quad \exists x \left(\bigwedge_{i=1}^{k_0} nx = t_i^0 \wedge \bigwedge_{i=1}^{k_1} t_i^1 < nx \wedge \bigwedge_{i=1}^{k_2} nx < t_i^2 \wedge \bigwedge_{i=1}^{k_3} m_i | nx + t_i^3 \right).$$

Mit y für nx und $m_0 = n$ ist (1) in \mathbf{ZG} sicher äquivalent zu

$$(2) \quad \exists y \left(\bigwedge_{i=1}^{k_0} y = t_i^0 \wedge \bigwedge_{i=1}^{k_1} t_i^1 < y \wedge \bigwedge_{i=1}^{k_2} y < t_i^2 \wedge \bigwedge_{i=1}^{k_3} m_i | y + t_i^3 \wedge m_0 | y \right).$$

Hier dürfen wir nach Satz 6.1 sogleich $k_0 = 0$ annehmen, so dass sich das Eliminationsproblem nach Rückbenennung von y in x auf Formeln der Gestalt

$$(3) \quad \exists x \left(\bigwedge_{i=1}^{k_1} t_i^1 < x \wedge \bigwedge_{i=1}^{k_2} x < t_i^2 \wedge \bigwedge_{i=0}^{k_3} m_i | x + t_i^3 \right)$$

reduziert. Sei m das kleinste gemeinsame Vielfache der m_0, \dots, m_{k_3} .

Fall 1: $k_1 = k_2 = 0$. Dann ist (3) in ZG äquivalent zu $\bigvee_{j=1}^m \bigwedge_{i=0}^{k_3} m_i | j + t_i^3$. Denn wenn es überhaupt ein x gibt mit $\bigwedge_{i=0}^{k_3} m_i | x + t_i^3$, so schon ein $x = j \in \{1, \dots, m\}$. Dazu bestimme man j nach Axiom ϑ_m so, dass $m | x + (m - j)$, also auch $m | x - j$ und folglich $m_i | x - j$ für alle $i \leq k_3$. Dann gilt auch $m_i | x + t_i^3 - (x - j) = j + t_i^3$ für $i = 0, \dots, k_3$ wie behauptet.

Fall 2: $k_1 \neq 0$ und j wie oben. Dann ist (3) äquivalent zu

$$(4) \quad \bigvee_{\mu=1}^{k_1} [\bigwedge_{i=1}^{k_1} t_i^1 \leq t_\mu^1 \wedge \bigvee_{j=1}^m (\bigwedge_{i=1}^{k_2} t_\mu^1 + j < t_i^2 \wedge \bigwedge_{i=0}^{k_3} m_i | t_\mu^1 + j + t_i^3)]$$

Dies ist eine Fallunterscheidung nach dem Maximum unter den Werten der t_i^1 . Aus jedem Alternativglied von (4) folgt in ZG sicher (3) (man beachte $t_i^1 < t_\mu^1 + j$). Nun sei umgekehrt x eine Lösung von (3). Dann gilt im Falle $\bigwedge_{i=1}^{k_1} t_i^1 \leq t_\mu^1$ auch das μ -te Alternativglied von (4). Hierzu ist nur $t_\mu^1 + j < t_i^2$ zu bestätigen, und dazu nur $t_\mu^1 + j \leq x$. Wäre $x < t_\mu^1 + j$, also $0 < x - t_\mu^1 < j$, so folgt $x - t_\mu^1 = k$ für ein $k < j$ nach η_j , also $x = t_\mu^1 + k$. Daher $m_i | t_\mu^1 + j - x = j - k$ für alle $i \leq k_3$. Das aber impliziert den Widerspruch $m | j - k < m$ aufgrund der Bestimmung von m .

Fall 3: $k_1 = 0$ und $k_2 \neq 0$. Dann argumentiert man analog, mit einer Fallunterscheidung nach dem kleinsten Term unter den $t_i^{k_2}$.

Aus diesem bemerkenswerten Beispiel folgt leicht das

Korollar 6.2. *ZG ist modellvollständig und vollständig.*

Beweis. Weil \mathbb{Z} offenbar Primmodell für ZG ist, ergibt sich die Vollständigkeit aus der Modellvollständigkeit, die sofort aus der Quantoreneliminierbarkeit folgt. \square

Bemerkung 1. Damit ist auch ZG_0 vollständig. Ferner sind ZG und ZG_0 als vollständige axiomatisierbare Theorien auch entscheidbar. ZG_0 ist selbst modellvollständig, Übung 1. Es ist dies gerade die Modellvervollständigung der Theorie der diskret geordneten abelschen Gruppen, denn jede solche Gruppe ist in eine \mathbb{Z} -Gruppe einbettbar (siehe z.B. [Pr]). Dennoch erlaubt ZG_0 die Quantorenelimination nicht; dieser Nachweis ist jedoch weit weniger einfach als man vermutet.

Wir wollen nun zeigen, dass die Theorien ACF und RCF der algebraisch bzw. der reell abgeschlossenen Körper die Quantorenelimination erlauben, und zwar ohne jede Erweiterung ihrer Signaturen. Wir führen den Beweis mit Hilfe von Satz 6.4, der ein modelltheoretisches Kriterium für die Quantorenelimination formuliert.

$X \subseteq \mathcal{L}$ heie eine Boolesche Basis für \mathcal{L} in T , wenn jedes $\varphi \in \mathcal{L}$ zu $\langle X \rangle$ gehört, siehe Seite 140. Für \mathcal{L} -Modelle \mathcal{M} sei $T_X \mathcal{M} := \{\varphi \in \langle X \rangle \mid \mathcal{M} \models \varphi\}$. Falls für jedes φ mit $\mathcal{M} \models \varphi$ bereits $T_X \mathcal{M} \vdash \varphi$, so ist $T_X \mathcal{M}$ offenbar maximal konsistent. Daher könnte man die Voraussetzung in folgender Variante von Satz 2.3 auch wie folgt formulieren: $\mathcal{M} \equiv_X \mathcal{M}' \Rightarrow \mathcal{M} \equiv \mathcal{M}'$, für alle $\mathcal{M}, \mathcal{M}' \models T$. Dabei sei $\mathcal{M} \equiv_X \mathcal{M}'$, falls $\mathcal{M} \models \varphi \Leftrightarrow \mathcal{M}' \models \varphi$, für alle $\varphi \in X$, sowie \equiv die Elementaräquivalenz in \mathcal{L} . Erstere Formulierung ist aber etwas bequemer für die Anwendung in Satz 6.4.

Satz 6.3 (Basissatz für Formeln). *Sei T eine Theorie, $X \subseteq \mathcal{L}$, und für jedes Modell $\mathcal{M} = (\mathcal{A}, w) \models T$ und jedes $\varphi \in L$ mit $\mathcal{M} \models \varphi$ sei $T_X \mathcal{M} \vdash \varphi$. Dann ist X eine Boolesche Basis für \mathcal{L} in T .*

Beweis. Sei $\alpha \in \mathcal{L}$ und $Y_\alpha := \{\gamma \in \langle X \rangle \mid \alpha \vdash_T \gamma\}$. Man zeigt dann $Y_\alpha \vdash_T \alpha$ wie im Beweis von Satz 2.3, indem man mit einem Modell \mathcal{M} statt mit einer Struktur \mathcal{A} argumentiert. Auch der Rest des Beweises verläuft genau wie dort. \square

Eine Theorie T heie *substrukturvollstndig*, wenn fr alle \mathcal{A}, \mathcal{B} mit $\mathcal{A} \subseteq \mathcal{B} \models T$ die Theorie $T + \mathcal{DA}$ vollstndig ist. T ist dann die Modellvervollstndigung von T_\forall . In der Tat, ist $\mathcal{A} \models T_\forall$, so ist nach Lemma 4.1 $\mathcal{A} \subseteq \mathcal{B}$ fr ein $\mathcal{B} \models T$ und $T + \mathcal{DA}$ somit vollstndig. Umgekehrt folgt daraus, dass T die Modellvervollstndigung von T_\forall ist, leicht auch die Substrukturvollstndigkeit. Jede dieser beiden Eigenschaften kennzeichnet nach folgendem Satz die Quantoreneliminierbarkeit.⁹⁾

Satz 6.4. *Fr jede Theorie T sind folgende Eigenschaften quivalent:*

- (i) T erlaubt Quantorenelimination, (ii) T ist substrukturvollstndig.

Beweis. (i) \Rightarrow (ii): Sei \mathcal{A} Substruktur eines T -Modells, $\alpha(\vec{x}) \in \mathcal{L}$ und $\vec{a} \in A^n$ mit $\mathcal{A} \models \alpha[\vec{a}]$. Ferner sei $\mathcal{B} \models T, \mathcal{DA}$, wobei ohne Einschrnkung $\mathcal{B} \supseteq \mathcal{A}$ vorausgesetzt werden darf. Dann ist auch $\mathcal{B} \models \alpha(\vec{a})$, denn wegen (i) darf man o.B.d.A. annehmen, α enthlt keine Quantoren. Weil \mathcal{B} beliebig war, gilt $\mathcal{DA} \vdash_T \alpha(\vec{a})$. Damit ist $T + \mathcal{DA}$ offenbar vollstndig, d.h. T ist substrukturvollstndig.

(ii) \Rightarrow (i): Sei $\mathcal{M} := (\mathcal{A}, w) \models T, \varphi$ und X die Menge der Literale λ von \mathcal{L} . Wir zeigen $T_X \mathcal{M} \vdash \varphi$. Nach Satz 6.3 bilden also die Literale eine Boolesche Basis fr \mathcal{L} in T , also ist jede Formel in T zu einer quantorenfreien quivalent und (i) ist bewiesen. Sei \mathcal{A}^E die von $E := \{x^w \mid x \in \text{Var}\}$ in \mathcal{A} erzeugte Substruktur und $\vec{a} = \vec{x}^w$. Weil $T + \mathcal{DA}^E$ vollstndig und mit $\varphi(\vec{a})$ konsistent ist (man beachte $\mathcal{A}_A \models T + \mathcal{DA}^E + \varphi$), gilt dann $\mathcal{DA}^E \vdash_T \varphi(\vec{a})$. Nun ist fr $\mathcal{DA}^E \vdash_T \varphi(\vec{a})$ aber schon $D_E \mathcal{A}^E \vdash_T \varphi(\vec{a})$ mit $D_E \mathcal{A}^E := \mathcal{DA}^E \cap \mathcal{LE}$, weil \mathcal{A}^E von E erzeugt wird, bung 5 in 5.1. Es gibt also Literale $\lambda_0(\vec{x}), \dots, \lambda_k(\vec{x})$ mit $\lambda_i(\vec{a}) \in D_E \mathcal{A}^E$ und $\bigwedge_{i \leq k} \lambda_i(\vec{a}) \vdash_T \varphi(\vec{a})$. Folglich ist $\bigwedge_{i \leq k} \lambda_i(\vec{x}) \vdash_T \varphi(\vec{x})$, denn die a_1, \dots, a_n kommen in T nicht vor. Offenbar ist $\lambda_i(\vec{x}) \in T_X \mathcal{M}$ fr alle $i \leq k$, also $T_X \mathcal{M} \vdash_T \varphi(\vec{x})$. \square

Korollar 6.5. *Eine \forall -Theorie T gestattet die Quantorenelimination genau dann, wenn sie modellvollstndig ist.*

Beweis. Wegen $\mathcal{A} \subseteq \mathcal{B} \models T \Rightarrow \mathcal{A} \models T$ ist (ii) in Satz 6.4 schon erfllt, wenn $T + \mathcal{DA}$ vollstndig ist fr alle $\mathcal{A} \models T$, d.h. wenn T modellvollstndig ist. \square

⁹⁾Es gibt dafr noch weitere Kriterien, insbesondere die Amalgamierbarkeit der Modelle von T_\forall . Diesbezglich sei z.B. auf [CK] verwiesen.

Satz 6.6 wurde zuerst von Tarski in [Ta2] bewiesen. Der folgende Beweis ist dank des Einsatzes weitreichender modelltheoretischer Methoden zwar wesentlich kürzer als Tarskis Originalbeweis, doch bleibt dieser für algorithmische Fragen weiterhin bedeutsam. Übrigens sind in RCF die Quantoren nicht eliminierbar, wenn auf die (in RCF definierbare) Ordnungsrelation verzichtet wird.

Satz 6.6. *ACF und RCF erlauben die Quantorenelimination.*

Beweis. Nach Satz 6.4 genügt zu zeigen ACF und RCF sind substrukturvollständig, oder anders formuliert, ACF und RCF sind die Modellvervollständigungen von ACF_\forall bzw. RCF_\forall . Beides ist klar nach Beispiel 3 in 5.5; denn ACF_\forall ist identisch mit der Theorie der Integritätsbereiche, und RCF_\forall ist offensichtlich nichts anderes als die Theorie der geordneten kommutativen Ringe mit Einselement. \square

Bemerkung 2. Wegen der Sätze 5.5 und 6.6 bedeutet Quantorenelimination in RCF dasselbe wie in der elementaren Theorie des geordneten Körpers der reellen Zahlen. Für die sehr viel reichere (vollständige) Theorie $T := \text{Th}(\mathbb{R}, <, 0, 1, +, -, \cdot, \exp)$ mit der Exponentialfunktion \exp ist Quantorenelimination in der Originalsprache zwar nachweislich unmöglich, immerhin ist T aber modellvollständig, [Wi]. Das Entscheidungsproblem für T reduziert sich wegen deren Vollständigkeit also auf das noch offene Axiomatisierungsproblem. Dessen Lösung hängt pikanterweise ab von der eines ungelösten Problems über transzendente Zahlen, der *Vermutung von Schanuel*. Auch scheint immer noch die Frage offen zu sein – ein Spezialfall dieser Vermutung – ob e^e transzendent ist.

Übungen

1. Man zeige, die Theorie ZG_0 ist modellvollständig in ihrer Sprache, und sogar in der Sprache $\mathcal{L}\{0, 1, +, -\}$.
2. Sei RCF° die Theorie der reell abgeschlossenen Körper ohne Ordnung. Man beweise, der \exists -Quantor ist aus $\alpha(x) = \exists y \, y + y = x$ in RCF° nicht eliminierbar.
3. Man zeige, die Theorie T der dividierbaren geordneten abelschen Gruppen erlaubt die Quantorenelimination.
4. Man entferne 1 aus der Signatur von ZG und auch das zugehörige Axiom und ersetze die Axiome ϑ_m durch $\exists z (\bigwedge_{0 < i < m} m \nmid iz \wedge \forall x \bigvee_{i < m} m \mid x + iz)$. Man zeige, die so entstehende Theorie erlaubt keine Quantorenelimination.
5. Eine zu $(\mathbb{N}, 0, 1, +, <)$ elementar-äquivalente Struktur heiße eine \mathbb{N} -Halbgruppe. Man axiomatisiere die Theorie der \mathbb{N} -Halbgruppen und zeige (durch Rückführung auf ZG), sie erlaubt Quantorenelimination in $\mathcal{L}\{0, 1, +, <, 1!, 2!, \dots\}$.

5.7 Reduzierte Produkte und Ultraprodukte

Um den Nutzen der folgenden Konstruktionen zunächst nur anzudeuten, betrachte man z.B. $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, das direkte Produkt der additiven Gruppe \mathbb{Z} mit sich selbst. Komponentenweises Nachrechnen der Axiome zeigt, dass \mathbb{Z}^2 wieder eine abelsche Gruppe ist. Dies kann man sich in diesem und analogen Beispielen aber ersparen. Denn nach Satz 7.5 gilt eine in allen \mathcal{A}_i gültige Hornaussage auch im Produkt $\prod_{i \in I} \mathcal{A}_i$, und die Gruppenaxiome sind Hornaussagen in jeder üblichen Signatur.

Sei $(\mathcal{A}_i)_{i \in I}$ eine nichtleere Familie von \mathcal{L} -Strukturen und F ein echter Filter auf I . Man erkläre eine Relation \approx_F auf dem Träger B des Produkts $\mathcal{B} := \prod_{i \in I} \mathcal{A}_i$ durch

$$a \approx_F b :\Leftrightarrow \{i \in I \mid a_i = b_i\} \in F \quad (a, b \in B).$$

Dies ist eine Äquivalenzrelation auf $B = \prod_{i \in I} A_i$. Denn sei $I_{a=b} := \{i \in I \mid a_i = b_i\}$. Dann ist \approx_F reflexiv, weil stets $I_{a=a} = I \in F$, trivialerweise symmetrisch, und auch transitiv, weil $I_{a=b}, I_{b=c} \in F \Rightarrow I_{a=c} \in F$ wegen $I_{a=b} \cap I_{b=c} \subseteq I_{a=c}$. Darüber hinaus ist \approx_F sogar eine *Kongruenz* im algebraischen Redukt von \mathcal{B} . Denn sei f ein n -stelliges Funktionssymbol von \mathcal{L} und $\vec{a} \approx_F \vec{b}$, d.h. für $\vec{a} = (a^1, \dots, a^n)$, $\vec{b} = (b^1, \dots, b^n)$ aus B^n sei $a^1 \approx_F b^1, \dots, a^n \approx_F b^n$. Dann gehört $I_{\vec{a}=\vec{b}} := \bigcap_{\nu=1}^n I_{a^\nu=b^\nu}$ zu F . Weil offenbar $I_{\vec{a}=\vec{b}} \subseteq I_{f\vec{a}=f\vec{b}}$, ist auch $I_{f\vec{a}=f\vec{b}} \in F$, also ist in der Tat $f^{\mathcal{B}}\vec{a} \approx_F f^{\mathcal{B}}\vec{b}$.

Sei nun $C := \{a/F \mid a \in B\}$, wobei a/F überall die Äquivalenzklasse von $a \in B$ bzgl. \approx_F bezeichne. C wird zum Träger einer \mathcal{L} -Struktur \mathcal{C} , indem zunächst die Operationen $f^{\mathcal{C}}$ repräsentantenweise erklärt werden. Mit $\vec{a}/F := (a^1/F, \dots, a^n/F)$ setzt man $f^{\mathcal{C}}(\vec{a}/F) := (f^{\mathcal{B}}\vec{a})/F$. Diese Erklärung ist repräsentantenunabhängig, weil \approx_F eine Kongruenz ist. Für Konstantensymbole c sei natürlich $c^{\mathcal{C}} := c^{\mathcal{B}}/F$.

Ähnlich wie die Identität seien die Relationen in \mathcal{C} wie folgt erklärt:

$$r^{\mathcal{C}}\vec{a}/F :\Leftrightarrow \{i \in I \mid r^{A_i}\vec{a}_i\} \in F.$$

Auch diese Definition ist repräsentantenunabhängig. Denn mit $\{i \in I \mid r^{A_i}\vec{a}_i\} \in F$ und $\vec{a} \approx_F \vec{b}$ ist auch $\{i \in I \mid r^{A_i}\vec{b}_i\} \in F$, weil $I_{\vec{a}=\vec{b}} \cap \{i \in I \mid r^{A_i}\vec{a}_i\} \subseteq \{i \in I \mid r^{A_i}\vec{b}_i\}$.

Die so definierte \mathcal{L} -Struktur \mathcal{C} heißt ein *reduziertes Produkt der \mathcal{A}_i nach dem Filter F* und werde mit $\prod_{i \in I}^F \mathcal{A}_i$ bezeichnet. Es ist vorteilhaft, sich unter einem Filter F ein System von Teilmengen von I vorzustellen, von denen jede „fast alle Indizes“ enthält. Besonders nützlich ist diese Vorstellung bei Ultrafiltern. Dann darf man sich \mathcal{C} aus $\mathcal{B} = \prod_{i \in I} \mathcal{A}_i$ durch Identifikation derjenigen Elemente aus B entstanden denken, bei denen die i -ten Projektionen für fast alle Indizes i übereinstimmen.

Für $w: \text{Var} \rightarrow B (= \prod_{i \in I} A_i)$ bezeichne w_i die Belegung $x \mapsto (x^w)_i$ nach A_i , so dass $x^w = (x^{w_i})_{i \in I}$. Induktion über t ergibt leicht $t^w = (t^{w_i})_{i \in I}$. Ferner ist $w/F: x \mapsto x^w/F$ dann eine Belegung nach \mathcal{C} , dem Träger von \mathcal{C} . Abermalige Induktion ergibt

(1) $t^{w/F} = t^w/F$, für alle Terme t und Belegungen $w: \text{Var} \rightarrow B$.

Man beachte hierbei nur $(f\vec{t})^{w/F} = f^{\mathcal{C}}(\vec{t}^{w/F}) = f^{\mathcal{C}}(\vec{t}^w/F) = f^{\mathcal{B}}(\vec{t}^w)/F = (f\vec{t})^w/F$.

Für beliebiges $\alpha \in \mathcal{L}$ sei $I_\alpha^w := \{i \in I \mid \mathcal{A}_i \models \alpha[w_i]\}$. Wir benötigen mehrfach

(2) Ist $I_{\exists x\beta}^w \in F$, $a \in B$, $w' = w \frac{a}{x}$ und $I_\beta^{w'} \in F \Rightarrow \mathcal{C} \models \beta[w'/F]$, so $\mathcal{C} \models \exists x\beta[w/F]$.

Zum Beweis wähle man zu jedem Index $i \in I_{\exists x\beta}^w$ (d.h. $\mathcal{A}_i \models \exists x\beta[w_i]$) ein $a_i \in A_i$ mit $\mathcal{A}_i \models \alpha[w_i \frac{a_i}{x}]$; sonst sei $a_i \in A_i$ beliebig. Mit $a := (a_i)_{i \in I}$ und w' wie in (2) ist dann $I_{\exists x\beta}^w \subseteq I_\beta^{w'}$. Also $I_\beta^{w'} \in F$ und damit $\mathcal{C} \models \beta[w'/F]$. Das ergibt $\mathcal{C} \models \exists x\beta[w/F]$.

Besonders konsequenzenreich ist nun der Fall, dass F ein Ultrafilter auf I ist. Dann übertragen sich nämlich alle elementaren Eigenschaften, die in fast allen Faktoren gelten, nach Satz 7.1 auch auf das reduzierte Produkt, das für diesen Fall auch ein *Ultraprodukt* genannt wird. Ist $\mathcal{A}_i = \mathcal{A}$ für alle $i \in I$, wird $\prod_{i \in I}^F \mathcal{A}_i$ meistens mit \mathcal{A}^I/F bezeichnet und heißt auch eine *Ultrapotenz von \mathcal{A}* .

Satz 7.1 (Ultraproduktsatz von Łoś). Sei $\mathcal{C} = \prod_{i \in I}^F \mathcal{A}_i$ ein Ultraprodukt der \mathcal{L} -Strukturen \mathcal{A}_i . Dann gilt für alle $\alpha \in \mathcal{L}$ und alle $w: \text{Var} \rightarrow \prod_{i \in I} A_i$

$$\mathcal{C} \models \alpha[w/F] \Leftrightarrow \{i \in I \mid \mathcal{A}_i \models \alpha[w_i]\} \in F.$$

Beweis durch Induktion über α . Es ist $(*)$: $\mathcal{C} \models \alpha[w/F] \Leftrightarrow I_\alpha^w \in F$ zu bestätigen.

$(*)$ ergibt sich für Formeln der Gestalt $t_1 = t_2$ wegen $t^w = (t^{w_i})_{i \in I}$ wie folgt:

$$\begin{aligned} \mathcal{C} \models t_1 = t_2[w/F] &\Leftrightarrow t_1^{w/F} = t_2^{w/F} \Leftrightarrow t_1^w/F = t_2^w/F \quad (\text{nach (1)}) \\ &\Leftrightarrow \{i \in I \mid t_1^{w_i} = t_2^{w_i}\} \in F \Leftrightarrow I_{t_1 = t_2}^w \in F \end{aligned}$$

Analog beweist man $(*)$, wenn α von der Gestalt $r\vec{t}$ ist. Induktionsschritte:

$$\begin{aligned} \mathcal{C} \models \alpha \wedge \beta[w/F] &\Leftrightarrow \mathcal{C} \models \alpha, \beta[w/F] \Leftrightarrow I_\alpha^w, I_\beta^w \in F \quad (\text{Induktionsannahme}) \\ &\Leftrightarrow I_\alpha^w \cap I_\beta^w \in F \quad (\text{Filtereigenschaft}) \\ &\Leftrightarrow I_{\alpha \wedge \beta}^w \in F \quad (\text{weil } I_{\alpha \wedge \beta}^w = I_\alpha^w \cap I_\beta^w). \end{aligned}$$

Ferner folgt $\mathcal{C} \models \neg\alpha[w/F] \Leftrightarrow \mathcal{C} \not\models \alpha[w/F] \Leftrightarrow I_\alpha^w \notin F \Leftrightarrow I \setminus I_\alpha^w \in F \Leftrightarrow I_{\neg\alpha}^w \in F$. Sei nun $I_{\forall x\alpha}^w \in F$, $a \in \prod_{i \in I} A_i$ und $w' := w \frac{a}{x}$. Weil $I_{\forall x\alpha}^w \subseteq I_\alpha^{w'}$, ist auch $I_\alpha^{w'} \in F$ und damit $\mathcal{C} \models \alpha[w'/F]$ nach Induktionsannahme. a war beliebig, also $\mathcal{C} \models \forall x\alpha[w/F]$. Die Umkehrung ist für $\beta := \neg\alpha$ offenbar zu $I_{\exists x\beta}^w \in F \Rightarrow \mathcal{C} \models \exists x\beta[w/F]$ gleichwertig. Dies folgt aus (2), weil $(*)$ für β schon vorausgesetzt werden kann. \square

Korollar 7.2. Eine Aussage α gilt im Ultraprodukt $\mathcal{C} = \prod_{i \in I}^F \mathcal{A}_i$ genau dann, wenn α in „fast allen“ Faktoren \mathcal{A}_i gilt, d.h. wenn $\{i \in I \mid \mathcal{A}_i \models \alpha\} \in F$. Speziell ist $\mathcal{A}^I/F \models \alpha \Leftrightarrow \mathcal{A} \models \alpha$, d.h. eine Ultrapotenz von \mathcal{A} ist zu \mathcal{A} elementar-äquivalent.

Dies ist klar, weil die Gültigkeit von α in einer Struktur nicht von einer gewählten Belegung abhängt. Der Spezialfall lässt sich nach Übung 2 noch verschärfen und

ist z.B. für die Konstruktion von speziellen Nichtstandardmodellen nützlich. Von unzähligen Anwendungen der Ultraprodukte nennen wir insbesondere einen sehr kurzen Beweis des Kompaktheitssatzes. Dieser Satz folgt unmittelbar aus

Korollar 7.3. *Sei $X \subseteq \mathcal{L}$ und I die Menge aller endlichen Teilmengen von X . Jedes $i \in I$ möge ein Modell (\mathcal{A}_i, w_i) besitzen. Dann existiert ein Ultrafilter F auf I mit $\prod_{i \in I}^F \mathcal{A}_i \models X[w/F]$ und $x^w = (x^{w_i})_{i \in I}$ für $x \in \text{Var}$.*

Beweis. Sei $\alpha \in X$ und $J_\alpha := \{i \in I \mid \alpha \in i\}$. Der Durchschnitt endlich vieler Elemente von $E := \{J_\alpha \mid \alpha \in X\}$ ist $\neq \emptyset$; z.B. ist $\{\alpha_0, \dots, \alpha_n\} \in J_{\alpha_0} \cap \dots \cap J_{\alpha_n}$. Nach dem Ultrafiltersatz (Seite 28) existiert daher ein Ultrafilter $F \supseteq E$. Ist $\alpha \in X$ und $i \in J_\alpha$, also $\alpha \in i$, gilt $\mathcal{A}_i \models \alpha[w_i]$. Folglich ist $J_\alpha \subseteq I_\alpha^w = \{i \in I \mid \mathcal{A}_i \models \alpha[w_i]\}$, daher $I_\alpha^w \in F$. Also gilt $\prod_{i \in I}^F \mathcal{A}_i \models \alpha[w/F]$ nach Satz 7.1 wie behauptet. \square

Eine bemerkenswerte Folgerung von Satz 7.1 ist ferner

Satz 7.4. *Sei $\mathbf{K}_{\mathcal{L}}$ die Klasse aller \mathcal{L} -Strukturen und $\mathbf{K} \subseteq \mathbf{K}_{\mathcal{L}}$. Dann gelten*

- (a) \mathbf{K} ist Δ -elementar $\Leftrightarrow \mathbf{K}$ ist abgeschlossen unter elementarer Äquivalenz und unter Ultraprodukten,
- (b) \mathbf{K} ist elementar $\Leftrightarrow \mathbf{K}$ ist abgeschlossen unter elementarer Äquivalenz und sowohl \mathbf{K} als auch $\setminus \mathbf{K}$ ($= \mathbf{K}_{\mathcal{L}} \setminus \mathbf{K}$) sind unter Ultraprodukten abgeschlossen.

Beweis. (a) \Rightarrow : klar nach Korollar 7.3. \Leftarrow : Sei $T := \text{Th } \mathbf{K}$ und $\mathcal{A} \models T$ und I die Menge aller endlichen Teilmengen von $\text{Th } \mathcal{A}$. Für jedes $i = \{\alpha_1, \dots, \alpha_n\} \in I$ gibt es ein $\mathcal{A}_i \in \mathbf{K}$ mit $\mathcal{A}_i \models i$ – sonst wäre $\bigvee_{\nu=1}^n \neg \alpha_\nu \in T$, was $i \subseteq T$ offenbar widerspricht. Nach Korollar 7.3 (mit $X = \text{Th } \mathcal{A}$) existiert ein $\mathcal{C} := \prod_{i \in I}^F \mathcal{A}_i \models \text{Th } \mathcal{A}$, und mit $\mathcal{A}_i \in \mathbf{K}$ ist auch $\mathcal{C} \in \mathbf{K}$. Wegen $\mathcal{C} \models \text{Th } \mathcal{A}$ ist $\mathcal{C} \equiv \mathcal{A}$, mithin auch $\mathcal{A} \in \mathbf{K}$. Das zeigt $\mathcal{A} \models T \Rightarrow \mathcal{A} \in \mathbf{K}$. Also $\mathcal{A} \models T \Leftrightarrow \mathcal{A} \in \mathbf{K}$. Kurzum, \mathbf{K} ist Δ -elementar. (b) \Rightarrow : klar nach (a), denn für $\mathbf{K} = \text{Md } \alpha$ ist $\setminus \mathbf{K} = \text{Md } \neg \alpha$. \Leftarrow : (a) ergibt $\mathbf{K} = \text{Md } S$ für ein $S \subseteq \mathcal{L}^0$. Sei I die Menge aller nichtleeren endlichen Teilmengen von S . Wir behaupten (*) es gibt ein $i = \{\alpha_0, \dots, \alpha_n\} \in I$ mit $\text{Md } i \subseteq \mathbf{K}$. Andernfalls sei $\mathcal{A}_i \models i$ mit $\mathcal{A}_i \in \setminus \mathbf{K}$ für alle $i \in I$. Dann gibt es ein Ultraprodukt \mathcal{C} der \mathcal{A}_i mit $\mathcal{C} \in \setminus \mathbf{K}$ und $\mathcal{C} \models i$ für $i \in I$, also $\mathcal{C} \models S$. Das ist ein Widerspruch zu $\text{Md } S \subseteq \mathbf{K}$. Also gilt (*). Weil auch $\mathbf{K} = \text{Md } S \subseteq \text{Md } i$, ist $\mathbf{K} = \text{Md } i = \text{Md } \bigwedge_{\nu \leq n} \alpha_\nu$. \square

Anwendungsbeispiel. Sei \mathbf{K} die (Δ -elementare) Klasse aller Körper der Charakteristik 0. Wir zeigen, \mathbf{K} ist nicht elementar und damit auf neue Weise, dass $\text{Th } \mathbf{K}$ nicht endlich axiomatisierbar ist. Sei \mathcal{P}_i der Primkörper der Charakteristik p_i (mit $p_0 = 2, p_1 = 3, \dots$) und F ein nichttrivialer Ultrafilter auf \mathbb{N} . Dann hat $\prod_{i \in \mathbb{N}}^F \mathcal{P}_i$ die Charakteristik 0. Denn $\{i \in I \mid \mathcal{P}_i \models \neg \text{char}_p\}$ ist bei vorgegebener Primzahl p sicher koendlich und gehört damit zu F . Also ist $\setminus \mathbf{K}$ nicht unter Ultraprodukten abgeschlossen und nach Satz 7.4(b) auch nicht elementar.

Wir kehren nun zu den allgemeineren reduzierten Produkten zurück. Alles, was darüber gesagt wird, gilt speziell auch für direkte Produkte. Denn diese sind der Spezialfall mit dem trivialen Filter $F = \{I\}$; genauer, es ist $\prod_{i \in I}^{\{I\}} \mathcal{A}_i \simeq \prod_{i \in I} \mathcal{A}_i$.

Satz 7.5. *Sei $\mathcal{C} = \prod_{i \in I}^F \mathcal{A}_i$ ein reduziertes Produkt, $w: \text{Var} \rightarrow \prod_{i \in I} \mathcal{A}_i$, und α eine Hornformel. Dann gilt $(\star) \ I_\alpha^w \in F \Rightarrow \mathcal{C} \models \alpha[w/F]$, mit $I_\alpha^w = \{i \in I \mid \mathcal{A}_i \models \alpha[w_i]\}$. Speziell gilt eine in allen (oder nur in fast allen) \mathcal{A}_i gültige Hornaussage auch in \mathcal{C} .*

Beweis durch Induktion über den Aufbau von Hornformeln. Für Primformeln gilt wie in Satz 7.1 auch die Umkehrung von (\star) . Daher ist (\star) für alle Literale richtig. Sei α nun Primformel, β Basis-Hornformel und $I_\alpha^w \rightarrow_\beta \in F$. Um $\mathcal{C} \models \alpha \rightarrow \beta[w/F]$ nachzuweisen, sei $\mathcal{C} \models \alpha[w]$ angenommen. Dann ist $I_\alpha^w \in F$, denn α ist Primformel. $I_\alpha^w \cap I_\alpha^w \rightarrow_\beta \subseteq I_\beta^w$ liefert $I_\beta^w \in F$, also $\mathcal{C} \models \beta[w/F]$ nach Induktionsannahme. Induktion über \wedge und \forall erfolgt wie in Satz 7.1, und der \exists -Schritt ergibt sich aus (2). \square

Nach diesem Satz sind die Modellklassen von Horntheorien stets gegenüber reduzierten Produkten abgeschlossen, insbesondere gegenüber direkten Produkten, was Übung 1 in 4.1 wesentlich verschärft. Wir erwähnen, dass umgekehrt jede Theorie mit einer gegenüber reduzierten Produkten abgeschlossenen Modellklasse auch eine Horntheorie ist. Der z.B. in [CK] ausgeführte Nachweis ist allerdings erheblich schwieriger als der des ähnlich lautenden Satzes 4.4.

Übungen

1. Man zeige: Für endliches $\{\mathcal{A}_i \mid i \in I\}$ ist jedes Ultraprodukt $\prod_{i \in I}^F \mathcal{A}_i$ zu einem der Faktoren \mathcal{A}_i elementar äquivalent und, falls I endlich ist, sogar isomorph. Jede Ultrapotenz einer endlichen Struktur \mathcal{A} ist damit isomorph zu \mathcal{A} .
2. Man zeige, \mathcal{A} ist in jede Ultrapotenz \mathcal{A}^I/F elementar einbettbar.
3. Sei $\models_{\mathbf{K}} := \bigcap \{\models_{\mathcal{A}} \mid \mathcal{A} \in \mathbf{K}\}$ die durch eine Klasse \mathbf{K} von L -Matrizen (Seite 40) definierte Konsequenz. Man zeige, $\models_{\mathbf{K}}$ ist finitär, wenn \mathbf{K} unter Ultraprodukten abgeschlossen ist. Das betrifft z.B. $\mathbf{K} = \{\mathcal{A}\}$, \mathcal{A} endlich (Übung 1). Also ist die von einer endlichen logischen Matrix definierte Konsequenzrelation finitär.
4. Seien \mathcal{A}, \mathcal{B} Boolesche Algebren. Man beweise $\mathcal{A} \models \alpha \Leftrightarrow \mathcal{B} \models \alpha$ für alle universalen Hornaussagen α . Das betrifft speziell Identitäten und Quasiidentitäten. Jede derartige in \mathcal{A} gültige Aussage gilt damit in allen Booleschen Algebren.

Kapitel 6

Unvollständigkeit und Unentscheidbarkeit

Die fundamentalen Resultate von Gödel über Unvollständigkeit genügend reichhaltiger formaler Systeme sowie von Tarski über Nichtdefinierbarkeit des Wahrheitsbegriffs und von Church über die Unentscheidbarkeit der Logik und andere Unentscheidbarkeitsresultate beruhen sämtlich auf gewissen Diagonalargumenten. Eine bekannte Popularisierung des 1. Gödelschen Unvollständigkeitssatzes ist diese:

Man betrachte eine formalisierte axiomatische Theorie T , die im Rahmen der T zugrundeliegenden Sprache \mathcal{L} über deren Syntax und das Beweisen aus den Axiomen von T zu reden imstande ist. Dies ist häufig auch dann möglich, wenn in T offiziell von anderen Dingen die Rede ist (etwa von Zahlen oder Mengen), nämlich vermittels einer internen Kodierung der Syntax von \mathcal{L} , siehe 6.2. Dann gehört zu \mathcal{L} – was für einen formalen Begriff von Beweisbarkeit im Einzelnen zu begründen ist – auch die Aussage γ : „Ich bin in T unbeweisbar“, wobei sich das *Ich* genau auf die Aussage γ selbst bezieht. Nehmen wir weiter an, T soll einen gewissen Gegenstandsbereich \mathcal{A} korrekt und möglichst vollständig beschreiben, und alle Aussagen von T haben in \mathcal{A} einen adäquaten Sinn. *Dann ist γ in \mathcal{A} wahr, in T aber unbeweisbar.*

In der Tat, wäre γ beweisbar, so wäre γ wie jede in T beweisbare Aussage auch wahr in \mathcal{A} und damit aber unbeweisbar, weil γ genau dies behauptet. Die Annahme führt zum Widerspruch. Also ist γ in T tatsächlich unbeweisbar und damit zugleich wahr in \mathcal{A} , weil die Behauptung von γ ja zutrifft. Das Ziel, die in \mathcal{A} gültigen Sätze durch T vollständig zu erfassen, ist also nicht erreicht.

Das ist natürlich nur eine grob vereinfachte Beschreibung des 1. Unvollständigkeitssatzes, der über Gegenstandsbereiche gar nicht redet, sondern ein *beweistheoretischer* Satz ist, dessen Beweis im Rahmen der finiten Metamathematik Hilberts ausführbar ist, was grob gesagt dasselbe bedeutet wie die Ausführbarkeit des Beweises in

PA. Dies war ein entscheidender Punkt für eine begründete Kritik am *Hilbertschen Programm*, das auf eine durchgehend finite Formulierung der Metamathematik zur Rechtfertigung infinitistischer Methoden abzielte, siehe hierzu [HB].

Paradigma eines Gegenstandsbereichs im anfänglich erwähnten Sinne ist aus verschiedenen Gründen die Struktur $\mathcal{N} = (\mathbb{N}, 0, \mathbf{S}, +, \cdot)$. Der 1. Unvollständigkeitssatz besagt, dass eine vollständige axiomatische Charakterisierung von \mathcal{N} unmöglich ist. Das ist eine Erkenntnis mit weitreichenden Konsequenzen. Insbesondere erweist sich die Peano-Arithmetik PA als unvollständig. Diese Theorie steht im Mittelpunkt von Kapitel 7. Sie ist deshalb besonders wichtig, weil in ihr nebst der klassischen Zahlentheorie und weiten Teilen der diskreten Mathematik ziemlich genau diejenigen Hilfsmittel der mathematischen Grundlagenforschung formulierbar und beweisbar sind, die nach allgemeiner Ansicht jeder Kritik standhalten.

Für wesentliche Schritte im Gödelschen Beweis benötigt man nur bescheidene Voraussetzungen über T , nämlich die ziffernweise Repräsentierbarkeit der relevanten syntaktischen Prädikate und Funktionen in T im Sinne von 6.3. Es war eine der entscheidenden Entdeckungen Gödels, dass alle zur Konstruktion von γ erforderlichen Prädikate primitiv-rekursiv sind ¹⁾ und *alle* derartigen Prädikate und Funktionen unter ziemlich allgemeinen Voraussetzungen in T repräsentierbar sind.

Wie von Tarski und Mostowski bemerkt, funktioniert dies bereits in gewissen endlich axiomatisierbaren, hochgradig unvollständigen Theorien T . Die in 6.4 ausführlich bewiesene Repräsentierbarkeit aller rekursiven Funktionen ergibt – wieder durch ein Diagonalargument – leicht die rekursive Unentscheidbarkeit von T und sämtlicher Teiltheorien, insbesondere der Theorie $\mathbf{Taut}_{\mathcal{L}}$ aller tautologischen Aussagen von \mathcal{L} , sowie aller konsistenten Erweiterungstheorien von T . Daher lassen sich der erste Unvollständigkeitssatz und die Resultate von Church und Tarski einheitlich gewinnen, und zwar im Wesentlichen durch das Fixpunktlema in 6.5.

In 6.1 wird die Theorie der rekursiven und primitiv-rekursiven Funktionen im erforderlichen Maße entwickelt. 6.2 behandelt die Gödelisierung der Syntax und des Beweisens. 6.3 und 6.4 befassen sich mit der Repräsentierbarkeit rekursiver Funktionen. In 6.5 werden alle oben erwähnten Resultate bewiesen, während der tieferliegende zweite Unvollständigkeitssatz in Kapitel 7 behandelt wird. 6.6 befasst sich mit der Übertragbarkeit von Entscheidbarkeit und Unentscheidbarkeit durch Interpretation, und 6.7 mit der arithmetischen Hierarchie der 1. Stufe, die den engen Zusammenhang zwischen Logik und Rekursionstheorie plastisch verdeutlicht.

¹⁾Alle diese Prädikate sind bereits elementar im Sinne der Rekursionstheorie, siehe etwa [Mo]. Doch erfordert dieser Nachweis mehr Aufwand. Die elementaren sind grob gesagt die nicht zu schnell wachsenden primitiv rekursiven Funktionen. Die Exponentialfunktion $(m, n) \mapsto m^n$ ist noch elementar, nicht aber die auf Seite 186 definierte Hyper-Exponentialfunktion.

6.1 Rekursive und primitiv-rekursive Funktionen

Im Folgenden bezeichnen nebst i, \dots, n auch a, \dots, e durchweg natürliche Zahlen. Die Menge aller n -stelligen Funktionen mit Argumenten und Werten aus \mathbb{N} werde mit \mathbf{F}_n bezeichnet. \mathbf{F}_0 besteht aus allen Konstanten. Sind $h \in \mathbf{F}_m$ und $g_1, \dots, g_m \in \mathbf{F}_n$, so heie $f : \vec{a} \mapsto h(g_1\vec{a}, \dots, g_m\vec{a})$ die durch *Komposition* aus h und den g_i entstehende Funktion, Schreibweise: $f = h[g_1, \dots, g_m]$. Die Stellenzahl von f ist n . Analog sei $P[g_1, \dots, g_m]$ fr $P \subseteq \mathbb{N}^m$ das n -stellige Prädikat $\{\vec{a} \in \mathbb{N}^n \mid P(g_1\vec{a}, \dots, g_m\vec{a})\}$.

$f \in \mathbf{F}_n$ ist im intuitiven Sinne berechenbar, wenn es einen Algorithmus gibt, der zu jedem $\vec{a} \in \mathbb{N}^n$ den Wert $f\vec{a}$ in endlich vielen Schritten zu berechnen gestattet. Einfache Beispiele sind Summe und Produkt. Es gibt berabzählbar viele einstellige Funktionen ber \mathbb{N} ; davon knnen wegen der Endlichkeit einer jeden Berechnungsvorschrift nur abzählbar viele berechenbar sein. Folglich gibt es nicht berechenbare Funktionen. Dieser Existenzbeweis erinnert an denjenigen transzendenter reeller Zahlen, wie ihn die Abzählbarkeit aller algebraischen Zahlen liefert. Konkrete Beispiele anzugeben ist in dem einen wie dem anderen Falle weniger einfach.

Die im intuitiven Sinne berechenbaren Funktionen mit Argumenten und Werten aus \mathbb{N} haben ganz offensichtlich die Eigenschaften

Oc : Mit $h \in \mathbf{F}_m$ und $g_1, \dots, g_m \in \mathbf{F}_n$ ist auch $f = h[g_1, \dots, g_m]$ berechenbar.

Op : Sind $g \in \mathbf{F}_n$ und $h \in \mathbf{F}_{n+2}$ berechenbar, so auch $f \in \mathbf{F}_{n+1}$, bestimmt durch

$$f(\vec{a}, 0) = g\vec{a} \quad \text{und} \quad f(\vec{a}, Sb) = h(\vec{a}, b, f(\vec{a}, b)),$$

die sogenannten *Rekursionsgleichungen*. f heit die aus g, h durch *primitive Rekursion* entstehende Funktion und werde auch als $f = \mathbf{Op}(g, h)$ notiert.

Oμ : Ist $g \in \mathbf{F}_{n+1}$ und gilt $\forall \vec{a} \exists b g(\vec{a}, b) = 0$, so ist mit g auch f berechenbar, wobei $f\vec{a} = \mu b[g(\vec{a}, b) = 0]$ (das kleinste b mit $g(\vec{a}, b) = 0$), die μ -Operation.

Wir betrachten nun **Oc**, **Op** und **Oμ** als Erzeugungsoperationen zur Gewinnung neuer Funktionen und beginnen mit der folgenden auf Kleene zurckgehenden

Definition. Die Menge der p.r. (*primitiv-rekursiven*) Funktionen bestehe aus allen Funktionen ber \mathbb{N} , die sich mittels **Oc** und **Op** erzeugen lassen aus folgenden

Anfangsfunktionen: die Konstante 0, die Nachfolgerfunktion **S** und die Projektionsfunktionen $\Gamma_\nu^n : \vec{a} \mapsto a_\nu$ ($1 \leq \nu \leq n$, $n = 1, 2, \dots$).

Mit dem zustzlichen Operation **Oμ** erhlt man die Menge aller *rekursiven* Funktionen, auch μ -*rekursive* Funktionen genannt. $P \subseteq \mathbb{N}^n$ heit p.r. bzw. *rekursiv* (oder *entscheidbar*), wenn die charakteristische Funktion χ_P p.r. bzw. rekursiv ist.

Bemerkung 1. Nach dem Dedekindschen Rekursionssatz (siehe z.B. [Ra3]) wird durch **Op** genau eine Funktion $f \in \mathbf{F}_{n+1}$ definiert. Man beachte, für $n = 0$ reduzieren sich diese Gleichungen auf $f0 = c$ und $fSb = h(b, fb)$, mit $c \in \mathbf{F}_0$ und $h \in \mathbf{F}_2$. Lässt man in **Op** die Bedingung $\forall \vec{a} \exists b g(\vec{a}, b) = 0$ weg, sagt man gelegentlich auch, f sei an allen Stellen \vec{a} mit $\neg \exists b g(\vec{a}, b) = 0$ nicht definiert. Man gelangt so zu den sogenannten partiell-rekursiven Funktionen, die wir aber nicht benötigen werden.

Die folgenden Beispiele verdeutlichen, dass sich mittels der I_ν^n die normierten Stellenzahlvorschriften in **Oc** und **Op** weitgehend liberalisieren lassen. Eine normgerechte Niederschrift wird hierbei zunächst noch in Klammern hinzugesetzt.

Beispiele. Sei $S^0 = I_1^1$ und $S^{k+1} = S[S^k]$, so dass offenbar $S^k: a \mapsto a + k$. Diese einstelligen Funktionen sind nach **Oc** alle p.r. Die n -stelligen *konstanten Funktionen* $K_c^n: \vec{a} \mapsto c$ erweisen sich wie folgt als primitiv rekursiv: $K_0^0 = 0$, $K_c^0 = S^c[0]$, sowie $K_c^1 0 = c (= K_c^0)$ und $K_c^1 Sb = c (= I_2^2(b, K_c^1 b))$. Für $n > 1$ hat man $K_c^n = K_c^1[I_1^n]$. Also sind sämtliche konstanten Funktionen p.r. Ferner bestimmen

$$a + 0 = a (= I_1^1(a)), \quad a + Sb = S(a + b) (= SI_3^3(a, b, a + b))$$

die Addition als p.r. Funktion. Durch $a \cdot 0 = 0 (= K_0^1 a)$ sowie $a \cdot Sb = a \cdot b + a (= I_3^3(a, b, a \cdot b) + I_1^1(a, b, a \cdot b))$ gewinnt man \cdot als p.r. Funktion und völlig analog auch $(a, b) \mapsto a^b$. Ferner ist die Vorgängerfunktion **R** p.r. Denn

$$R0 = 0 \quad ; \quad R(Sb) = b (= I_1^2(b, Rb)).$$

Die „gestutzte Subtraktion“ \div , definiert durch $a \div b = a - b$ für $a \geq b$ und $a \div b = 0$ sonst, ist p.r. Denn $a \div 0 = a$ und $a \div Sb = R(a \div b) (= RI_3^3(a, b, a \div b))$. Damit ist die absolute Differenz p.r. Denn $|a - b| = (a \div b) + (b \div a)$.

Man sieht leicht, dass mit jeder Funktion f auch jede Funktion p.r. bzw. rekursiv ist, die aus f durch Vertauschung, Gleichsetzung oder Hinzufügen von fiktiven Argumenten hervorgeht. Sei z.B. $f \in \mathbf{F}_2$. Für $g = f[I_2^2, I_1^2]$ ist dann $g(a, b) = f(b, a)$. Für $h = f[I_1^1, I_1^1]$ ist $ha = f(a, a)$, und für $f' = f[I_1^3, I_2^3]$ ist $f'(a, b, c) = f(a, b)$. Hier wurde der Funktion f die fiktive Variable c hinzugefügt.

Ab jetzt sind wir großzügiger bei den Niederschriften der Anwendungen von **Oc** und **Op**. Mit $f \in \mathbf{F}_{n+1}$ ist auch $(\vec{a}, b) \mapsto \prod_{k < b} f(\vec{a}, k)$ p.r., definiert durch

$$\prod_{k < 0} f(\vec{a}, k) = 1 \quad ; \quad \prod_{k < Sb} f(\vec{a}, k) = (\prod_{k < b} f(\vec{a}, k)) \cdot f(\vec{a}, b).$$

Analoges gilt für $(\vec{a}, b) \mapsto \sum_{k < b} f(\vec{a}, k)$, mit der Startbedingung $\sum_{k < 0} f(\vec{a}, k) = 0$.

Durch $\delta 0 = 1$ und $\delta Sn = 0$ wird die p.r. δ -Funktion definiert. Damit erkennt man z.B. die Identitätsrelation leicht als p.r. Es ist $\chi_=(a, b) = \delta|a - b|$. Das wiederum impliziert jede endliche Teilmenge $E = \{a_1, \dots, a_n\}$ von \mathbb{N} ist p.r. Denn $\chi_\emptyset = K_0^1$ und $\chi_E(a) = \chi_=(a, a_1) + \dots + \chi_=(a, a_n)$ für $E \neq \emptyset$.

Das Prädikat \neq ist p.r. weil $\chi_{\neq}(a, b) = \text{sg } |a - b|$, wobei sg definiert ist durch $\text{sg } 0 = 0$, $\text{sg } n = 1$. Das ergibt die Abgeschlossenheit der p.r. bzw. rekursiven Funktionen gegenüber *Definition durch p.r. (bzw. rekursive) Fallunterscheidung*: Mit P, g, g' ist auch h p.r. (bzw. rekursiv), definiert durch $h\vec{a} = g\vec{a} \cdot \chi_P\vec{a} + g'\vec{a} \cdot \delta(\chi_P\vec{a})$, d.h.

$$h\vec{a} = \begin{cases} g\vec{a}, & \text{falls } P\vec{a}, \\ g'\vec{a}, & \text{falls } \neg P\vec{a}. \end{cases}$$

Ein simples Beispiel ist gegeben durch $h(a, b, c) = \text{Sc}$, falls $c < b \div 1$ und $h(a, b, c) = 0$ sonst. h ist nützlich um nachzuweisen, dass $\text{rest}(a, b)$ p.r. ist, der *Divisionsrest von a durch b*, definiert durch $\text{rest}(0, b) = 0$, $\text{rest}(\text{Sa}, b) = \text{S rest}(a, b)$ für $\text{rest}(a, b) < b \div 1$, und $\text{rest}(\text{Sa}, b) = 0$ sonst. Mit obigem h schreibt sich die Rekursionsgleichung der rest -Funktion normgerecht als $\text{rest}(\text{Sa}, b) = h(a, b, \text{rest}(a, b))$.

Auch weitere Standardfunktionen sind p.r., darunter $n \mapsto n!$ und die *Primzahl-aufzählung* $n \mapsto p_n$ (mit $p_0 = 2$, $p_1 = 3, \dots$), sowie Prädikate wie \mid (teilt), prim (Primzahl sein), usw. Siehe hierzu (B) und (C) unten sowie die Übungen.

Von grundlegender Bedeutung, speziell für die Gewinnung von Unentscheidbarkeitsresultaten, ist die Hypothese, dass die rekursiven Funktionen alle irgendwie berechenbaren Funktionen über \mathbb{N} bereits ausschöpfen, die sogenannte *Churchsche These*. Der Definition rekursiver Funktionen ist dies kaum anzusehen, aber alle auf unterschiedliche Weise definierten Berechenbarkeitskonzepte erwiesen sich als äquivalent und stützen damit die These. Für einige dieser oft langwierigen Beweise sei auf [Ob] verwiesen. Ein solches Konzept ist z.B. die Berechenbarkeit mittels einer *Turing-Maschine*, eines einfachen Modells rein mechanischer Informationsverarbeitung.

Es folgt eine Zusammenstellung leicht beweisbarer Grundfakten über primitiv und μ -rekursive Prädikate (‘ μ -rekursiv’ akzentuiert hier nur den Unterschied zu ‘primitiv rekursiv’). Weitere Einsichten, vor allem über die Gestalt definierender Formeln werden sich ab 6.3 ergeben. P, Q, R bezeichnen jetzt ausschließlich Prädikate über \mathbb{N} . Um die formale Niederschrift von Eigenschaften solcher Prädikate zu erleichtern, benutzen wir weitere metasprachliche Abkürzungen, z.B. die Präfixe $(\exists k < a)$, $(\exists k \leq a)$, $(\forall k < a)$ und $(\forall k \leq a)$, deren Sinn sich von selbst erklärt.

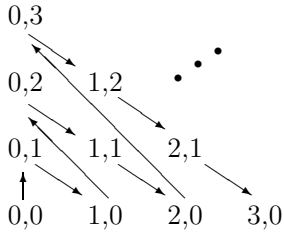
(A) Die Menge der p.r. bzw. rekursiven Prädikate ist abgeschlossen gegenüber Komplementbildung, Vereinigung und Durchschnitt von Prädikaten derselben Stellenzahl und gegenüber Einsetzung p.r. bzw. rekursiver Funktionen sowie gegenüber Gleichsetzung, Vertauschung und Hinzufügung von fiktiven Argumenten. Das ergibt sich wie folgt: Für $P \subseteq \mathbb{N}^n$ ist $\delta[\chi_P]$ gerade die charakteristische Funktion von $\neg P = \mathbb{N}^n \setminus P$; ferner ist offenbar $\chi_{P \cup Q} = \text{sg}[\chi_P + \chi_Q]$, $\chi_{P \cap Q} = \chi_P \cdot \chi_Q$ und $\chi_{P[g_1, \dots, g_m]} = \chi_P[g_1, \dots, g_m]$. Die übrigen Abgeschlossenheitseigenschaften folgen einfach aus entsprechenden Eigenschaften der charakteristischen Funktionen.

(B) Seien $P, Q, \dots \subseteq \mathbb{N}^{n+1}$. Ist $Q(\vec{a}, b) \Leftrightarrow (\forall k < b) P(\vec{a}, k)$, $R(\vec{a}, b) \Leftrightarrow (\exists k < b) P(\vec{a}, k)$, $Q'(\vec{a}, b) \Leftrightarrow (\forall k \leq b) P(\vec{a}, k)$ und $R'(\vec{a}, b) \Leftrightarrow (\exists k \leq b) P(\vec{a}, k)$ sagt man, Q, R, Q', R' entstünden aus P durch *beschränkte Quantifizierung*. Mit P sind alle diese Prädikate p.r. So ist $\chi_Q(\vec{a}, b) = \prod_{k < b} \chi_P(\vec{a}, k)$ und $\chi_R(\vec{a}, b) = \text{sg}(\sum_{k < b} \chi_P(\vec{a}, k))$. Die Beweise dieser Gleichungen sind so einfach, dass wir sie übergehen können. Kurzum, die Menge der p.r. bzw. rekursiven Prädikate ist abgeschlossen gegenüber beschränkter Quantifizierung. Weil z.B. $a|b \Leftrightarrow (\exists k \leq b)[a \cdot k = b]$, ist $|$ p.r. Auch prim ist wegen $\text{prim } p \Leftrightarrow p \neq 0, 1 \ \& \ (\forall k < p)[k|p \Rightarrow k = 1]$ p.r., denn $a|p \Rightarrow a = 1$ ist gleichwertig zu $a \nmid p \vee a = 1$ und als Vereinigung p.r. Prädikate wieder p.r.

(C) $P \subseteq \mathbb{N}^{n+1}$ erfülle $\forall \vec{a} \exists m P(\vec{a}, m)$. Ist $f(\vec{a}) = \mu k[P(\vec{a}, k)]$ das kleinste k mit $P(\vec{a}, k)$, so ist nach **Op** mit P auch f rekursiv, denn $f\vec{a} = \mu k[\delta \chi_P(\vec{a}, k) = 0]$; doch ist f in der Regel nicht mehr p.r. Das gilt aber noch für die *beschränkte μ -Operation*: Mit $P \subseteq \mathbb{N}^{n+1}$ ist auch $f: (\vec{a}, m) \mapsto \mu k \leq m[P(\vec{a}, k)]$ p.r. Dabei sei

$$\mu k \leq m[P(\vec{a}, k)] = \begin{cases} \text{kleinstes } k \leq m \text{ mit } P(\vec{a}, k), & \text{falls ein solches } k \text{ existiert,} \\ m & \text{sonst, d.h. falls } \neg P(\vec{a}, k) \text{ für alle } k \leq m. \end{cases}$$

Offenbar ist $f(\vec{a}, 0) = 0$, sowie $f(\vec{a}, Sm) = f(\vec{a}, m)$ falls $(\exists k \leq m) P(\vec{a}, k)$, und sonst ist $f(\vec{a}, Sm) = Sm$. In der normierten Notation $f = \text{Op}(g, h)$ bedeutet dies wie bei rest eine p.r. Fallunterscheidung in der Definition von h . Also ist f p.r.



Durch Einsetzung einer p.r. Funktion h für m erkennt man leicht auch $\vec{a} \mapsto \mu k \leq h\vec{a}[P(\vec{a}, k)]$ als p.r. Eine nützliche Anwendung ist die *Paarkodierung* \wp , die \mathbb{N}^2 bijektiv auf \mathbb{N} abbildet (Übung 3), und zwar gemäß der in der Figur gezeigten Abzählung der Zahlenpaare a, b . Es ist $\wp(a, b) = a + \frac{1}{2}(a+b)(a+b+1)$. Eine Darstellung mit Hilfe der beschränkten μ -Operation erhalten wir in $\wp(a, b) = \mu k \leq (3a+b+1)^2 [2k = 2a + (a+b)(a+b+1)]$.

Man erkennt aber auch auf andere Weise, dass \wp p.r. ist. Denn nach einer bekannten Summationsformel ist $\wp(a, b) = a + \sum_{i \leq a+b} i$. Eine weitere Anwendung ist diese: Sei $\text{kgV}\{a_\nu | \nu \leq n\}$ das kleinste gemeinsame Vielfache von a_0, \dots, a_n . Dann ist mit f auch $n \mapsto \text{kgV}\{f\nu | \nu \leq n\}$ p.r. Denn $\text{kgV}\{f\nu | \nu \leq n\} = \mu k \leq \prod_{\nu \leq n} f\nu [(\forall \nu \leq n) f\nu | k]$.

Hier noch eine Anwendung. Ist p Primzahl, so ist $p! + 1$ gewiss durch keine Primzahl $q \leq p$ teilbar; denn $q|p! + 1$ und $q|p!$ liefern den Widerspruch $q|1$. Ein Primteiler von $p! + 1$ ist mithin eine neue Primzahl. Daher ist die kleinste auf p folgende Primzahl $\leq p! + 1$. Also ist $n \mapsto p_n$ wohldefiniert und charakterisiert durch

$$(\star) \quad p_0 = 2 \quad ; \quad p_{n+1} = \mu q \leq p_n! + 1 [q \text{ prim} \ \& \ q > p_n].$$

Auch (\star) ist eine Anwendung von **Op**. Denn mit $f: (a, b) \mapsto \mu q \leq b [q \text{ prim} \ \& \ q > a]$

ist auch $g: a \mapsto f(a, a! + 1)$ p.r. und die zweite Gleichung in (\star) lässt sich einfach schreiben als $p_{n+1} = g(p_n)$. Folglich ist die Primzahlaufzählung $n \mapsto p_n$ p.r.

(C) macht den Unterschied zwischen p.r. und rekursiven Funktionen etwas deutlicher. Erstere sind mit einem im Prinzip abschätzbaren Aufwand berechenbar, während die Existenzbedingung $\forall \vec{a} \exists m P(\vec{a}, m)$ in (C) nichtkonstruktiv sein kann, so dass selbst grobe Abschätzungen über den Berechnungsaufwand unmöglich sind.

Bemerkung 2. Anders als alle p.r. Funktionen lassen sich die μ -rekursiven Funktionen nicht mehr effektiv aufzählen, auch nicht alle einstelligen. Denn wäre $(f_n)_{n \in \mathbb{N}}$ eine solche Aufzählung, so wäre $f: n \mapsto f_n(n) + 1$ sicher berechenbar und nach der Churchschen These rekursiv. Also $f = f_m$ für ein m , was den Widerspruch $f_m(m) = f(m) = f_m(m) + 1$ ergibt. Das spricht anscheinend gegen die These, die mit etwas Rekursionstheorie aus dem Argument aber eliminierbar ist. Wiederholt man die Argumentation mit einer tatsächlich existierenden Aufzählung aller p.r. einstelligen Funktionen, haben wir einen (nichtkonstruktiven) Existenzbeweis für eine berechenbare aber nicht p.r. Funktion vor uns.

Die nachfolgenden Ausführungen dieses Abschnitts benötigen wir in 6.2. Es geht um die Kodierung endlicher Zahlenfolgen durch natürliche Zahlen. Dafür gibt es grundsätzlich mehrere Möglichkeiten. Eine davon ist, mit Hilfe der Paarkodierung \wp (oder einer ähnlichen Funktion, siehe z.B. [Shoe]) den 1-Tupeln (a) die Zahlen $\wp(a, 0)$, den Paaren (a, b) die Zahlen $\wp(\wp(a, b), 1)$ zuzuordnen, usw. Das ergibt eine Bijektion zwischen $\bigcup_{k \geq 0} \mathbb{N}^k$ und \mathbb{N} . Wir wählen indes die besonders anschauliche, auf der eindeutigen Primfaktorzerlegung beruhende Kodierung nach [Gö2].

Definition. Die natürliche Zahl $\langle a_0, \dots, a_n \rangle := p_0^{a_0+1} \cdot \dots \cdot p_n^{a_n+1}$ heiße die *Gödelzahl* der Zahlenfolge (a_0, \dots, a_n) . Dabei sei $k \mapsto p_k$ die Primzahlaufzählung. Die leere Folge habe die Gödelzahl $\langle \rangle := 1$. Es bezeichne Gz die Menge aller Gödelzahlen.

$\langle a_0, \dots, a_n \rangle = \langle b_0, \dots, b_m \rangle$ impliziert offenbar $m = n$ & $a_i = b_i$ für alle $i \leq n$. Diese unabdingbare Eindeutigkeits-Eigenschaft ist der Grund, warum in obiger Definition die Exponenten „um 1 erhöht“ wurden. Auch ist $\vec{a} \mapsto \langle a_1, \dots, a_n \rangle$ sicher p.r. Und nach (A), (B) oben auch Gz . Denn

$$a \in Gz \Leftrightarrow a \neq 0 \text{ \& } (\forall p \leq a)(\forall q \leq p)[\text{prim } p, q \text{ \& } p|a \Rightarrow q|a].$$

Wir verschaffen uns einen kleinen Vorrat p.r. Funktionen, die u.a. in 6.2 wichtig sind. Nach (C) wird eine p.r. Funktion $a \mapsto \ell a$ definiert durch $\ell a = \mu k \leq a [p_k \nmid a]$. ℓa gibt für Gödelzahlen a gerade die „Länge“ von a an. Denn offenbar ist $\ell 1 = 0$, und für $a = \langle a_0, \dots, a_n \rangle = \prod_{i \leq n} p_i^{a_i+1}$ ist $\ell a = n + 1$, weil $k = n + 1$ der kleinste Index ist mit $p_k \nmid a$, der wegen $n + 1 < p_n \leq a$ zugleich auch die Bedingung $k \leq a$ erfüllt. Was ℓa für Zahlen a bewirkt, die keine Gödelzahlen sind, ist gänzlich belanglos. Man könnte auch einfach $\ell a = 0$ setzen für alle $a \notin Gz$.

Auch die wie folgt definierte 2-stellige Operation $(a, i) \mapsto (a)_i$ ist primitiv rekursiv:

$$(a)_i = \mu k \leq a [p_i^{k+2} \nmid a].$$

Dies ist die „Komponenten-Erkennungsfunktion“. Denn für $p_i^{k+1} \mid a$ und $p_i^{k+2} \nmid a$ gilt gewiss $k = (a)_i$. Daher $(\langle a_0, \dots, a_n \rangle)_i = a_i$ für alle $i \leq n$. Diese durch leichten Fettdruck auffallende Funktion beginnt die Komponentenzählung stets mit $i = 0$, so dass $(a)_{last} := (a)_{\ell a - 1}$ die letzte Komponente einer Gödelzahl $a \neq 1$ ist.

Obige Definitionen liefern leicht $a = \prod_{i < \ell a} p_i^{(a)_i + 1}$ für alle $a \in Gz$. Sei die der Wort-Verkettung entsprechende p.r. *arithmetische Verkettung* $*$ erklärt durch

$$a * b = a \cdot \prod_{i < \ell b} p_{\ell a + i}^{(b)_i + 1} \text{ für } a, b \in Gz, \text{ sowie } a * b = 0 \text{ sonst.}$$

Offenbar gilt $\langle a_1, \dots, a_n \rangle * \langle b_1, \dots, b_m \rangle = \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle$. Das ergibt leicht $a, b \in Gz \Leftrightarrow a * b \in Gz$, sowie $a, b \leq a * b$. Die Operation $*$ ist u.a. nützlich für folgende Verallgemeinerung von **Op**, die *Wertverlaufsrekursion*. Jedem $f \in \mathbf{F}_{n+1}$ entspricht eine Funktion $\bar{f} \in \mathbf{F}_{n+1}$, die definiert sei durch

$$\bar{f}(\vec{a}, 0) = \langle \rangle \quad (= 1) \quad ; \quad \bar{f}(\vec{a}, b) = \langle f(\vec{a}, 0), \dots, f(\vec{a}, b-1) \rangle \text{ für } b > 0.$$

\bar{f} kodiert den Wertverlauf von f im letzten Argument. Sei nun $F \in \mathbf{F}_{n+2}$. Dann gibt es ganz ähnlich wie bei **Op** genau ein $f \in \mathbf{F}_{n+1}$, das der Funktionalgleichung

$$\mathbf{Oq} \quad f(\vec{a}, b) = F(\vec{a}, b, \bar{f}(\vec{a}, b))$$

genügt. Es gilt nämlich $f(\vec{a}, 0) = F(\vec{a}, 0, \langle \rangle) = F(\vec{a}, 0, 1)$, $f(\vec{a}, 1) = F(\vec{a}, 1, \langle f(\vec{a}, 0) \rangle)$, $f(\vec{a}, 2) = F(\vec{a}, 2, \langle f(\vec{a}, 0), f(\vec{a}, 1) \rangle)$ usw. $f(\vec{a}, b)$ hängt für $b > 0$ i.a. von allen Werten $f(\vec{a}, 0), \dots, f(\vec{a}, b-1)$ ab, nicht nur von $f(\vec{a}, b-1)$ wie bei **Op**. Daher heißt **Oq** das Schema der *Wertverlaufsrekursion*. Ein einfaches Beispiel ist die Folge $(fn)_{n \in \mathbb{N}}$ von Fibonacci, definiert durch $f0 = 0$, $f1 = 1$ und $fn = f(n-1) + f(n-2)$ für $n \geq 2$. In der „Normalform“ **Oq** ist hier $F \in \mathbf{F}_2$ gegeben durch $F(b, c) = b$ für $b \leq 1$ und $F(b, c) = (c)_{b-1} + (c)_{b-2}$ sonst. Mit diesem F gilt nämlich $fn = F(n, \bar{f}n)$ für alle n .

Op ist ein Sonderfall von **Oq**. Ist $f = \mathbf{Op}(g, h)$ und wird die Funktion F durch $F(\vec{a}, 0, c) = g(\vec{a})$ und $F(\vec{a}, Sb, c) = h(\vec{a}, b, (c)_b)$ erklärt, so erfüllt f mit diesem F auch **Oq**, wie man unter Beachtung von $f(\vec{a}, b) = (\bar{f}(\vec{a}, Sb))_b$ leicht nachrechnet.

Satz 1.1. *Sei f durch F mittels **Oq** definiert. Dann ist mit F auch f p.r.*

Beweis. Weil allgemein $\langle c_0, \dots, c_b \rangle * \langle c_{b+1} \rangle = \langle c_0, \dots, c_{b+1} \rangle$, genügt \bar{f} dem Schema

$$(\star) \quad \bar{f}(\vec{a}, 0) = 1 \quad ; \quad \bar{f}(\vec{a}, Sb) = \bar{f}(\vec{a}, b) * \langle F(\vec{a}, b, \bar{f}(\vec{a}, b)) \rangle.$$

Die zweite Gleichung lässt sich offenbar schreiben als $\bar{f}(\vec{a}, Sb) = h(\vec{a}, b, \bar{f}(\vec{a}, b))$, mit $h(\vec{a}, b, c) = c * \langle F(\vec{a}, b, c) \rangle$, also ist h p.r. Nach (\star) ist dann aber \bar{f} p.r. Somit aber auch f , denn f ist nach **Oq** eine simple Komposition p.r. Funktionen. \square

Neben der Wertverlaufsrekursion gibt es noch andere Rekursionsvorschriften, die zwar berechenbare, aber nicht mehr p.r. Funktionen definieren. Berühmtes Beispiel ist die rekursive aber nicht p.r. *Ackermann-Funktion* $\circ \in \mathbf{F}_2$, definiert durch

$$0 \circ b = Sb \quad ; \quad Sa \circ 0 = a \circ 1 \quad ; \quad Sa \circ Sb = a \circ (Sa \circ b)$$

Obwohl \circ nicht p.r. ist, ist $\text{graph } \circ$ p.r. (siehe z.B. [Fe1, Seite 76–84]). Daher ist \circ nach Übung 1 durch eine p.r. Funktion nicht einmal majorisierbar. Umgekehrt ist mit f stets auch $\text{graph } f$ p.r., denn $\chi_{\text{graph } f}(\vec{a}, b)$ ist identisch mit $\chi_=(f\vec{a}, b)$.

Wir präzisieren noch den fundamentalen und recht anschaulichen Begriff rekursiv (oder effektiv) aufzählbar. Eine Menge $M \subseteq \mathbb{N}$ heißt r.a. (= *rekursiv aufzählbar*), wenn $M = \{b \in \mathbb{N} \mid (\exists a \in \mathbb{N}) Rab\}$ für eine rekursive Relation $R \subseteq \mathbb{N}^2$. Kurzum, M ist der *Nachbereich* von R . In jedem Falle ist M dann zugleich auch der *Vorbereich* einer rekursiven Relation, denn $a \in M \Leftrightarrow (\exists b \in \mathbb{N}) R'ab$ mit $R'ab \Leftrightarrow Rba$.

Allgemein heie $P \subseteq \mathbb{N}^n$ r.a., falls $P\vec{a} \Leftrightarrow (\exists x \in \mathbb{N}) Q(x, \vec{a})$ für ein $(n+1)$ -stelliges rekursives Prädikat Q . Jedes rekursive Prädikat P ist auch r.a. Und zwar deshalb weil $P\vec{a} \Leftrightarrow (\exists b \in \mathbb{N}) P'(b, \vec{a})$, mit $P'(b, \vec{a}) \Leftrightarrow P\vec{a}$ (Hinzufügen einer fiktiven Variablen). Man beweist unschwer $M \neq \emptyset$ ist r.a. genau dann, wenn $M = \text{ran } f$ für eine rekursive Funktion $f \in \mathbf{F}_1$, Übung 4. Diese Kennzeichnung entspricht der Intuition in vollkommener Weise: Die schrittweise Berechnung von $f0, f1, \dots$ liefert eine effektive Aufzählung von M im anschaulichen Sinne. Vorteil der anfänglichen Definition ist jedoch ihre natürliche Ausdehnung auf den n -dimensionalen Fall. Die leere Menge ist trivial r.a. Sie ist der Vorbereich der sogar p.r. leeren 2-stelligen Relation. Deren charakteristische Funktion ist gerade die eingangs vorgestellte Funktion K_0^2 .

Übungen

1. Sei $f \in \mathbf{F}_n$. Man zeige, f ist rekursiv genau dann, wenn $\text{graph } f$ dies ist. Ferner zeige man: Ist $\text{graph } f$ p.r. so ist f dann und nur dann p.r. falls f durch ein p.r. $h \in \mathbf{F}_n$ majorisiert wird, d.h. $f\vec{a} \leq h\vec{a}$ für alle \vec{a} .
2. Sei $a \leq fa$ für alle a . Man zeige mittels p.r. Fallunterscheidung, mit f ist auch $\text{ran } f$ p.r. bzw. rekursiv. Damit ist $\text{ran } f$ z.B. auch für jede echt wachsende rekursive Funktion $f \in \mathbf{F}_1$ wieder rekursiv.
3. Man beweise, die Paarkodierung $\wp: \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ ist bijektiv.
4. Sei M eine nichtleere Teilmenge natürlicher Zahlen. Man zeige, M ist genau dann r.a. wenn $M = \text{ran } f$ für ein rekursives $f \in \mathbf{F}_1$.
5. Sei $\text{bz}_i^m \in \{0, 1\}$ die i -te Binärziffer der Binärdarstellung $m = \sum_{i \geq 0} \text{bz}_i^m \cdot 2^i$. Man zeige, die Funktion $(m, n) \mapsto \text{bz}_n^m$ ist p.r. Man beweist hierzu beispielsweise $\text{bz}_n^m = 0 \Leftrightarrow \text{rest}(m, 2^{n+1}) < 2^n$.

6.2 Gödelisierung

Gödelisierung oder Arithmetisierung ist etwas grob formuliert die Beschreibung der Syntax einer formalen Sprache \mathcal{L} und des Beweisens durch arithmetische Operationen mit natürlichen Zahlen. Sie setzt die Kodierung von Zeichenfolgen über dem Alphabet von \mathcal{L} durch natürliche Zahlen voraus. Wortfunktionen und Wortprädikate entsprechen auf diese Weise wohlbestimmten Funktionen und Prädikaten über \mathbb{N} . Dadurch lassen sich gleich mehrere Ziele erreichen. Erstens lässt sich die intuitive Vorstellung von einer berechenbaren Wortfunktion durch den Begriff der rekursiven Funktion präzisieren. Zweitens kann man syntaktische Prädikate wie z.B. ' $x \in \text{var } \alpha$ ' durch entsprechende Prädikate von \mathbb{N} ersetzen. Drittens lassen sich in formalen Theorien $T \subseteq \mathcal{L}$ mittels der Kodierung auch Aussagen über Wortfunktionen, oder allgemeiner, über syntaktische Prädikate formulieren, die das Beweisen in T mit vorgegebenen Mitteln betreffen.

Wir behandeln die Gödelisierung der Syntax exemplarisch am Beispiel der formalen Sprache $\mathcal{L} = \mathcal{L}_{ar}$ in den nichtlogischen Symbolen $0, S, +, \cdot$, die z.B. der Peanoarithmetik PA zugrundliegt. Entsprechendes lässt sich für andere formale Sprachen völlig analog durchführen, wie im Verlaufe der Betrachtungen leicht einzusehen ist. Der erste Schritt ist, jedem Grundzeichen ζ von \mathcal{L} umkehrbar eindeutig eine *Nummer* $\# \zeta$ aus \mathbb{N} zuzuordnen. Für $\mathcal{L} = \mathcal{L}_{ar}$ z.B. durch folgende Tabelle:

ζ	$=$	\neg	\wedge	\forall	$($	$)$	0	S	$+$	\cdot	v_0	v_1	\dots
$\# \zeta$	1	3	5	7	9	11	13	15	17	19	21	23	\dots

Danach kodieren wir das Wort $\xi = \zeta_0 \cdots \zeta_n$ durch seine *Gödelzahl*

$$\langle \# \zeta_0, \dots, \# \zeta_n \rangle = p_0^{1+\# \zeta_0} \cdot \dots \cdot p_n^{1+\# \zeta_n}.$$

Beispiel. Der Term 0 und die Primformel $0=0$ haben die noch recht kleinen Gödelzahlen $2^{1+\#0} = 2^{14}$ und $2^{14} \cdot 3^2 \cdot 5^{14}$. Diese Kodierung ist nicht gerade ökonomisch. Aber darauf kommt es hier nicht an. Es stört nicht, dass die Nummer von $=$ zugleich Gödelzahl des leeren Wortes ist. Denn $=$ als *Wort* hat die Gödelzahl $2^2 = 4$.

Weil die Symbolnummern ungerade sind, kommt 2 immer in gerader Potenz in der Primzerlegung der Gödelzahl eines nichtleeren Wortes vor. Das hat die angenehme Folge, dass sich die Gödelzahlen von Formeln und Termen von den unten definierten Gödelzahlen endlicher Formelfolgen bequem unterscheiden lassen. ξ, η, ϑ bezeichnen wie schon in 2.2 beliebige Elemente (Zeichenfolgen oder Worte) aus $\mathcal{S}_{\mathcal{L}}$. Es sei $\dot{\xi}$ die Gödelzahl des Wortes ξ und $\dot{\alpha}$ daher die der Formel α . Schreibt man $\xi\eta$ für die Verkettung von $\xi, \eta \in \mathcal{S}_{\mathcal{L}}$, gilt offenbar $(\xi\eta)^{\cdot} = \dot{\xi} * \dot{\eta}$, mit der arithmetischen Verkettung $*$ aus 6.1. $\dot{\mathcal{S}}_{\mathcal{L}} = \{\dot{\xi} \mid \xi \in \mathcal{S}_{\mathcal{L}}\}$ ist eine p.r. Teilmenge der Menge aller Gödelzahlen, denn $n \in \dot{\mathcal{S}}_{\mathcal{L}} \Leftrightarrow n \in Gz \ \& \ (\forall k < \ell n) 2 \nmid (n)_k$.

Man muss wenigstens vorübergehend zwischen dem *Symbol* ζ und dem *Wort* ζ unterscheiden, welches eigentlich die Einerfolge (ζ) ist. $\dot{\zeta} = 2^{1+\# \zeta}$ ist die Gödelzahl des Wortes ζ . So hat der Primterm 0 die Gödelzahl $\dot{0} = 2^{1+\#0}$ (Terme sind Worte!). Ebenso muss zwischen dem Symbol v_0 und dem Term v_0 begrifflich unterschieden werden. Der Term v_0 hat eine Gödelzahl, das Symbol v_0 nur eine Nummer.

Bemerkung 1. Man könnte von Anfang Formeln auch mit ihren Gödelzahlen identifizieren, so dass syntaktische Prädikate von vornherein arithmetische sind und zwischen $\dot{\varphi}$ und φ nicht unterschieden wird. Das sollte aber erst geschehen, wenn die arithmetische Formulierbarkeit der Syntax restlos klar ist. Ferner ließe sich das Alphabet von \mathcal{L}_{ar} leicht durch ein endliches ersetzen, z.B. bestehend aus $=, \neg, \dots, \cdot, v$, indem man v_0 durch $v0$, v_1 durch $vS0$ usw. ersetzt. Andere oft anzutreffende Kodierungen entstehen durch Identifikation der Buchstaben solcher Alphabete mit den Ziffern passender p -adischer Systeme.

Nachfolgend sei stets $\dot{W} = \{\dot{\xi} \mid \xi \in W\}$ für eine Menge $W \subseteq \mathcal{S}_{\mathcal{L}}$. Eine entsprechende Notation sei auch für mehrstellige Wortprädikate P verwendet. P heiße p.r. bzw. *rekursiv*, falls \dot{P} p.r. bzw. rekursiv ist. Wenn also z.B. von einem rekursiven Axiomensystem $X \subseteq \mathcal{L}$ die Rede ist, meint man stets, \dot{X} sei rekursiv. Auch andere Redeweisen wie rekursiv aufzählbar oder repräsentierbar seien mittels obiger oder einer ähnlichen Gödelisierung auf Wortprädikate übertragen.

Alles Obige bezieht sich nicht nur auf $\mathcal{L} = \mathcal{L}_{ar}$, sondern auf eine beliebige *gödelisierbare* (oder *arithmetisierbare*) Sprache \mathcal{L} . Hiermit ist gemeint, dass \mathcal{L} ein genau spezifiziertes Alphabet A besitzt damit die Zeichenfolgen über A in berechenbarer Weise durch Zahlen kodierbar sind. Damit erhalten auch die in 3.3 schon benutzten Begriffe einer axiomatisierbaren oder entscheidbaren Theorie einen restlos klaren Sinn. Zwischen den Axiomen und den Sätzen einer axiomatischen Theorie ist natürlich klar zu unterscheiden. Nur die Axiomensysteme wichtiger Theorien wie etwa PA und ZFC erweisen sich als p.r., nicht aber diese Theorien selbst.

Unser Hauptziel ist die Arithmetisierung des formalen Beweisens. Deshalb bezeichne \vdash der Eindeutigkeit halber den Hilbertkalkül aus 3.6, bestehend aus dem Axiomensystem Λ mit den dort genannten Axiomenschemata $\Lambda 1$ – $\Lambda 10$ und MP als einziger Schlussregel, jeweils bezogen auf eine fest gewählte gödelisierbare Sprache \mathcal{L} .

Analog wie bei Zeichenfolgen heiße für eine Formelfolge $\Phi = (\varphi_0, \dots, \varphi_n)$ von \mathcal{L} -Formeln $\dot{\Phi} := \langle \dot{\varphi}_0, \dots, \dot{\varphi}_n \rangle$ deren *Gödelzahl*. Das betrifft speziell den Fall, dass Φ ein Beweis aus $X (\subseteq \mathcal{L})$ im Sinne von 3.6 ist, der in der Regel auch Formeln aus Λ enthält. Stets ist $\dot{\Phi} \neq \dot{\xi}$ für alle $\xi \in \mathcal{S}_{\mathcal{L}}$. Denn $(\dot{\Phi})_0 = \dot{\varphi}_0$ ist gerade, also $2 \mid (\dot{\Phi})_0$, während immer $2 \nmid (\dot{\xi})_0$, weil die Symbolnummern ungerade sind. Dies setzen wir wie im Beispiel $\mathcal{L} = \mathcal{L}_{ar}$ stets voraus, um eben in dieser Weise schließen zu können.

Sei nun $T (\subseteq \mathcal{L}^0)$ eine durch ein Axiomensystem $X \subseteq T$ axiomatisierte Theorie, etwa PA oder auch die Theorie ZFC, deren Sprache einfacher ist als \mathcal{L}_{ar} , was natürlich

auch die Kodierung vereinfacht. Ein Beweis $\Phi = (\varphi_0, \dots, \varphi_n)$ aus X heiße auch *ein Beweis in T* – man fasst X hierbei stillschweigend als wesentlichen Bestandteil von T auf. Dem syntaktischen Prädikat ‘ Φ ist ein Beweis in T ’ möge das einstellige arithmetische Prädikat $beweis_T$ entsprechen, und den Prädikaten ‘ Φ ist ein Beweis für α ’ (dem letztem Glied von Φ) und ‘es gibt einen Beweis für α in T ’ die arithmetischen Prädikate bew_T bzw. bwb_T . Ihre präzisen Definitionen lauten:

- $$(1) \quad \begin{aligned} &beweis_T(b) \Leftrightarrow b \in Gz \ \& \ b \neq 1 \\ &\quad \& \ (\forall k < \ell b)(b)_k \in \dot{X} \cup \dot{\Lambda} \vee (\exists i, j < k)(b)_i = (b)_j \dot{\sim} (b)_k, \end{aligned}$$
- $$(2) \quad bew_T(b, a) \Leftrightarrow bewis_T(b) \ \& \ a = (b)_{last}, \quad (3) \quad bwb_T(a) \Leftrightarrow \exists b \ bew_T(b, a).$$

Dabei definiert man die p.r. Funktionen $\dot{\sim}, \dot{\wedge}, \dot{\vee}$ durch $\dot{\sim}a = \dot{\sim} * a, a \dot{\wedge} b = (\dot{*} a * \dot{\wedge} * b *)$ und $a \dot{\vee} b = \dot{\vee}(a \dot{\wedge} \dot{\vee} b)$. Den Definitionen (1), (2), (3) entnimmt man leicht

- $$(4) \quad \vdash_T \alpha \Leftrightarrow \text{es gibt ein } n \text{ mit } bew_T(n, \dot{\alpha}) \Leftrightarrow bwb_T(\dot{\alpha}),$$
- $$(5) \quad bew_T(c, a) \ \& \ bew_T(d, a \dot{\sim} b) \Rightarrow bew_T(c * d * \langle b \rangle, b), \text{ für alle } a, b, c, d,$$
- $$(6) \quad bwb_T(a) \ \& \ bwb_T(a \dot{\sim} b) \Rightarrow bwb_T(b), \text{ für alle } a, b,$$
- $$(7) \quad bwb_T(\dot{\alpha}) \ \& \ bwb_T((\alpha \rightarrow \beta) \dot{\cdot}) \Rightarrow bwb_T(\dot{\beta}), \text{ für alle Formeln } \alpha, \beta.$$

(4) ist klar, denn ist $\vdash_T \alpha \Leftrightarrow$ es gibt einen Beweis Φ für $\alpha \Leftrightarrow \exists n \ bew_T(n, \dot{\alpha})$ (man wähle $n = \dot{\Phi}$). (5) erzählt uns in arithmetischer Sprache die bekannte Geschichte, dass Verkettungen von Beweisen für $\alpha, \alpha \rightarrow \beta$ und Anhängen von β einen Beweis für β ergibt. Partikularisierung liefert sofort (6). Hieraus ergibt sich (7) mit $a = \dot{\alpha}, b = \dot{\beta}$.

Bemerkung 2. Wir benötigen (5),(6),(7) erst in 7.1, aber es ist für die spätere Beweisübertragung nach PA lehrreich, (5) zuerst naiv zu verifizieren. Dies ist einfach, wenn man folgende Fakten benutzt: Für alle $a, b \in Gz$ ist $\ell(a * b) = \ell a + \ell b$, $(a * b)_i = (a)_i$ für $i < \ell a$, $(a * b)_{\ell a + i} = (b)_i$ für $i < \ell b$, und $\ell \langle c \rangle = 1$, $(\langle c \rangle)_0 = c$ für alle c . Man beachte, dass die Bedingung $(\forall k < b)(b)_k \in \dot{\mathcal{L}}$ rechts in (1) nicht erscheint. Dies ist auch nicht nötig, denn induktiv über die Beweislänge folgt leicht $beweis_T(b) \Rightarrow (\forall k < \ell b)(b)_k \in \dot{\mathcal{L}}$.

Nun machen wir uns an die eigentliche Arbeit und zeigen, dass die syntaktischen Grundbegriffe bis hin zum Prädikat bew_T alle p.r. sind. In 6.5 spielt im Grunde nur ihre Rekursivität eine Rolle; erst in Kapitel 7 wird wesentlich von ihrem p.r. Charakter Gebrauch gemacht. Wir kehren dabei zu unserer Beispielsprache $\mathcal{L} = \mathcal{L}_{ar}$ mit ihrer spezifischen Termmenge \mathcal{T} zurück, weil die Beweise der folgenden Lemmata von der Syntax der Sprache und der Kodierung nicht ganz unabhängig sind.

Wir erklären nun auch $n \dot{=} m := n * \dot{=} * m (= n * 2^2 * m)$ und $\dot{\vee}(i, n) := \dot{\vee} * i * n$. Für $S, +, \cdot$ definieren wir gemäß der offiziellen klammerfreien Termnotation $\dot{\sim}n = \dot{S} * n$, $n \dot{+} m = \dot{+} * n * m$ und $n \dot{\cdot} m = \dot{\cdot} * n * m$. Dann gelten z.B. $(s = t) \dot{\cdot} = \dot{s} \dot{=} \dot{t}$, $(St) \dot{\cdot} = \dot{S} \dot{t}$, $(+st) \dot{\cdot} = \dot{s} \dot{+} \dot{t}$ und $(\forall x \alpha) \dot{\cdot} = \dot{\vee}(x, \dot{\alpha})$. Alle diese Funktionen sind offenbar p.r.

Die Menge \mathcal{V} der Variablenterme ist p.r. Denn $n \in \dot{\mathcal{V}} \Leftrightarrow (\exists k \leq n) n = 2^{22+2k}$. Damit ist auch $\mathcal{T}_{prim} := \mathcal{V} \cup \{0\}$, die Menge aller Primterme von \mathcal{L} , p.r. Für beliebige Worte ξ, η bedeute $\xi < \eta$, dass $\dot{\xi} < \dot{\eta}$. Stets ist $\xi < \eta$, falls ξ echtes Teilwort von η ist. Das folgt leicht aus der Eigenschaft $a, b < a * b$ für Gödelzahlen $a, b \neq 1$.

Lemma 2.1. *Die Menge \mathcal{T} aller Terme von \mathcal{L} ($= \mathcal{L}_{ar}$) ist primitiv rekursiv.*

Beweis. Entsprechend der rekursiven Definition von \mathcal{T} ist $t \in \mathcal{T}$ genau dann, wenn

$$t \in \mathcal{T}_{prim} \vee (\exists t_1, t_2 < t)[t_1, t_2 \in \mathcal{T} \ \& \ (t = \mathbf{S}t_1 \vee t = +t_1t_2 \vee t = \cdot t_1t_2)].$$

Daher gilt auch die entsprechende arithmetische Äquivalenz, nämlich

$$(\star) \quad n \in \dot{\mathcal{T}} \Leftrightarrow n \in \dot{\mathcal{T}}_{prim} \vee (\exists i, k < n)[i, k \in \dot{\mathcal{T}} \ \& \ Q(n, i, k)]$$

mit $Q(n, i, k) \Leftrightarrow (n = \tilde{\mathbf{S}}i \vee n = i\tilde{+}k \vee n = i\tilde{\cdot}k)$. Wir zeigen nun, wie man diese „informelle Definition“ von $\dot{\mathcal{T}}$, die auf der rechten Seite aber nur Bezug nimmt auf kleinere Elemente von $\dot{\mathcal{T}}$, in eine Wertverlaufsrekursion von $\chi_{\dot{\mathcal{T}}}$ verwandelt, womit $\chi_{\dot{\mathcal{T}}}$ (also $\dot{\mathcal{T}}$) als p.r. nachgewiesen wäre. Wir betrachten zu diesem Zwecke das sicher p.r. zweistellige arithmetische Prädikat P , definiert durch

$$P(a, n) \Leftrightarrow n \in \dot{\mathcal{T}}_{prim} \vee (\exists i, k < n)[(a)_i = (a)_k = 1 \ \& \ Q(n, i, k)].$$

Für den Zweck des Beweises werde die charakteristische Funktion $\chi_{\dot{\mathcal{T}}}$ von $\dot{\mathcal{T}}$ mit f bezeichnet. Wir behaupten, f erfüllt die Rekursionsgleichung

$$\mathbf{Oq}: \quad fn = \chi_P(\bar{f}n, n) \quad (\bar{f}n = \langle f(0), \dots, f(n-1) \rangle)$$

und ist nach Satz 1.1 damit p.r. **Oq** gilt, weil $fi = fk = 1 \Leftrightarrow i, k \in \dot{\mathcal{T}}$ und

$$\begin{aligned} n \in \dot{\mathcal{T}} &\Leftrightarrow n \in \dot{\mathcal{T}}_{prim} \vee (\exists i, k < n)[fi = fk = 1 \ \& \ Q(n, i, k)] \quad (\text{nach } (\star)) \\ &\Leftrightarrow P(\bar{f}n, n) \quad (\text{weil } (\bar{f}n)_i = fi \text{ und } (\bar{f}n)_k = fk). \end{aligned}$$

Hieraus folgt aber sofort $fn = 1 \Leftrightarrow \chi_P(\bar{f}n, n) = 1$ und damit offenbar auch **Oq**. \square

Lemma 2.2. *Die Menge \mathcal{L} ($= \mathcal{L}_{ar}$) aller Formeln ist primitiv rekursiv.*

Beweis. Wegen $n \in \dot{\mathcal{L}}_{prim} \Leftrightarrow (\exists i, k < n)[i, k \in \dot{\mathcal{T}} \ \& \ n = i \dot{=} k]$ ist die Menge \mathcal{L}_{prim} aller Primformeln p.r. Beachtet man $\dot{x} < \dot{\xi}$ für jedes $\xi \in \mathbb{S}_{\mathcal{L}}$ und $x \in \text{var}\xi$, so ist das Prädikat ‘ $\varphi \in \mathcal{L}$ ’ offenbar gekennzeichnet durch

$$\varphi \in \mathcal{L}_{prim} \vee (\exists \alpha, \beta, x < \varphi)[\alpha, \beta \in \mathcal{L} \ \& \ x \in \mathcal{V} \ \& \ (\varphi = \neg\alpha \vee \varphi = (\alpha \wedge \beta) \vee \varphi = \forall x\alpha)].$$

Diese informelle Definition verwandelt man nun ganz analog wie in Lemma 2.1 in eine Wertverlaufsrekursion der charakteristischen Funktion von $\dot{\mathcal{L}}$ mittels der charakteristischen Funktion des gewiss p.r. Prädikats P , das definiert sei durch

$$\begin{aligned} P(a, n) &\Leftrightarrow n \in \dot{\mathcal{L}}_{prim} \vee (\exists i, k, j < n)[(a)_i = (a)_k = 1 \ \& \ j \in \dot{\mathcal{V}} \\ &\quad \& \ (n = \tilde{\neg}i \vee n = i \tilde{\wedge} k \vee n = \tilde{\forall}(j, k))]. \quad \square \end{aligned}$$

Ausgehend von der Substitution $\xi \mapsto \xi \frac{t}{x}$, die sowohl für Terme als auch für Formeln benötigt wird, lässt sich nunmehr eine p.r. Funktion $(m, i, k) \mapsto [m]_i^k$ definieren mit

$$(*) \quad [\dot{\xi}]_x^t = (\xi \frac{t}{x}) \text{ für alle } \xi \in \mathcal{T} \cup \mathcal{L}, x \in \text{Var}, t \in \mathcal{T}.$$

Die Konstruktion von $[m]_i^k$ erfolgt durch p.r. Fallunterscheidung und Wertverlaufsrekursion über m in zwei Schritten, erst für $m \in \dot{\mathcal{T}}$ und dann für $m \in \dot{\mathcal{L}}$. Nur Schritt 1 wird ausführlich behandelt. Sei $[m]_i^k = 0$, falls $m \notin \dot{\mathcal{T}}$ oder $i \notin \dot{\mathcal{V}}$ oder $k \notin \dot{\mathcal{T}}$, und nunmehr $m \in \dot{\mathcal{T}}$, $i \in \dot{\mathcal{V}}$ und $k \in \dot{\mathcal{T}}$. Sei zuerst $m \in \dot{\mathcal{T}}_{\text{prim}}$. Falls $m = i$ sei $[m]_i^k = k$ (entspricht $x \frac{t}{x} = t$), und falls $m \neq i$ sei $[m]_i^k = m$. Nun sei $m \in \dot{\mathcal{T}} \setminus \dot{\mathcal{T}}_{\text{prim}}$. Zuerst betrachten wir den Fall $(\exists m_0 < m)(m = \tilde{S}m_0 \& m_0 \in \dot{\mathcal{T}})$. Ein solches m_0 ist durch m eindeutig bestimmt. In diesem Falle sei $[m]_i^k = \tilde{S}[m_0]_i^k$. Entsprechend sei $[m]_i^k = [m_1]_i^k \dot{+} [m_2]_i^k$, falls $(\exists m_1, m_2 < m)(m = m_1 \dot{+} m_2 \& m_1, m_2 \in \dot{\mathcal{T}})$, und analog für $\dot{-}$. Auch jetzt sind m_1, m_2 durch m jeweils eindeutig bestimmt, so dass diese Erklärungen korrekt sind. $[m]_i^k$ ist damit wohldefiniert und p.r., erfüllt aber $(*)$ zunächst nur für $\xi \in \mathcal{T}$, weil $[m]_i^k = 0$ für $m \in \dot{\mathcal{L}}$ gesetzt wurde.

In Schritt 2 verändern wir obige Definition von $[m]_i^k$ für $m \in \dot{\mathcal{L}}$, $i \in \dot{\mathcal{V}}$ und $k \in \dot{\mathcal{T}}$ in p.r. Weise, schreiben aber a statt m . Für $a = (t_1 = t_2)$ sei $[a]_i^k = [\dot{t}_1]_i^k \dot{=} [\dot{t}_2]_i^k$ ($t_1, t_2 \in \mathcal{T}$, Primformel-Fall, entspricht $(t_1 = t_2) \frac{t}{x} = t_1 \frac{t}{x} = t_2 \frac{t}{x}$). Dabei wird $[m]_i^k$ für $m \in \dot{\mathcal{T}}$ voll benutzt. Sonst ist $a \in \dot{\mathcal{L}}$ von der Gestalt $\dot{\sim} a_0$ oder $a_0 \dot{\wedge} a_1$ oder $\dot{\forall}(b, a_0)$ mit eindeutigen $a_0, a_1 < a$ aus $\dot{\mathcal{L}}$, $b \in \dot{\mathcal{V}}$ und $[a]_i^k$ werde durch Wertverlaufsrekursion erklärt, entsprechend der rekursiven Definition von $\alpha \frac{t}{x}$. Das verläuft völlig analog zu Schritt 1. Damit wurde eine ganz $(*)$ erfüllende p.r. Funktion konstruiert.

Man sieht leicht, dass das Prädikat ‘ x kommt in ξ vor’, kurz ‘ $x \in \text{var} \xi$ ’ p.r. ist. Denn $x \in \text{var} \xi \Leftrightarrow x \in \mathcal{V} \& (\exists \eta, \vartheta \leq \xi)(\xi = \eta x \vartheta)$. Ersetzt man rechts x durch $\forall x$, ergibt sich ‘ $x \in \text{gbd} \alpha$ ’ als p.r. zu erkennen. Auch das Prädikat ‘ $x \in \text{frei} \alpha$ ’ ist p.r. Denn $x \in \text{frei} \alpha \Leftrightarrow x \in \mathcal{V} \& \alpha \frac{0}{x} \neq \alpha$ ($\Leftrightarrow x \in \mathcal{V} \& [\dot{\alpha}]_x^0 \neq \dot{\alpha}$). Hier wird $[m]_i^k$ erstmals verwendet. Mithin ist auch \mathcal{L}^0 p.r. Nach diesen Vorbereitungen beweisen wir

Lemma 2.3. *Die Menge Λ der logischen Axiome ist primitiv rekursiv.*

Beweis. $\Lambda 1$ ist p.r. weil $\varphi \in \Lambda 1$ genau dann, wenn

$$(\exists \alpha, \beta, \gamma < \varphi)[\alpha, \beta, \gamma \in \mathcal{L} \& \varphi = (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma)].$$

Die Kennzeichnung des entsprechenden arithmetischen Prädikats verwendet die p.r. Funktion $\dot{\sim}$. Ähnlich argumentiert man für $\Lambda 2$ – $\Lambda 4$. Für eine p.r. Kennzeichnung von $\Lambda 5$ benutzt man, dass ‘ $\alpha, \frac{t}{x}$ kollisionsfrei’ p.r. ist, denn dies trifft zu genau dann, wenn $(\forall y < \alpha)(y \in \text{gbd} \alpha \& y \in \text{var} t \Rightarrow y = x)$. Ferner ist das von φ, α, x, t abhängige Prädikat ‘ $\varphi = \forall x \alpha \rightarrow \alpha \frac{t}{x}$ ’ p.r. wie man unter Verwendung von $(m, i, k) \mapsto [m]_i^k$ leicht sieht. Mithin ist auch $\Lambda 5$ p.r. Denn φ gehört zu $\Lambda 5$ genau dann, wenn

$$(\exists \alpha, x, t < \varphi)(\alpha \in \mathcal{L} \& x \in \mathcal{V} \& t \in \mathcal{T} \& \varphi = \forall x \alpha \rightarrow \alpha \frac{t}{x} \& \alpha, \frac{t}{x} \text{ kollisionsfrei}).$$

Analog sieht man, dass auch Λ_6 – Λ_{10} p.r. sind, also ist jedes der Schemata Λ_i p.r. und somit auch $\Lambda_0 := \Lambda_1 \cup \dots \cup \Lambda_{10}$. Dann gilt dasselbe aber für Λ . Denn weil $k \mapsto \#v_k$ sicher p.r. ist, und weil jedes $\alpha \in \Lambda$ eine Darstellung $\alpha = \forall \vec{x} \alpha_0$ mit einem (eventuell leeren) Präfix $\forall \vec{x}$ und einem $\alpha_0 \in \Lambda_0$ hat, gilt offenbar

$$n \in \dot{\Lambda} \Leftrightarrow n \in \dot{\mathcal{L}} \ \& \ (\exists m, k < n)[n = m * k \ \& \ 2 \mid \ell m \ \& \ k \in \dot{\Lambda}_0 \\ \& \ (\forall i < \ell m)(2 \nmid i \ \& \ (m)_i = \#v \ \vee \ 2 \mid i \ \& \ (\exists k \leq n)(m)_i = \#v_k)].$$

Die zweite Zeile dieser Formel erzählt uns, dass m die Gödelzahl eines Präfixes der Gestalt $\forall x_1 \dots \forall x_l$ mit $2l = \ell m$ ist. \square

Diese Lemmata gelten völlig analog für jede gödelisierbare Sprache. Damit ist für jedes p.r. bzw. rekursive Axiomensystem X auch $X \cup \Lambda$ p.r. bzw. rekursiv. Das betrifft insbesondere die Axiomensysteme von **PA** und **ZFC**. Diese sind wie fast alle gebräuchlichen Axiomensysteme trotz ihrer unterschiedlichen Stärke p.r. und damit aus rekursionstheoretischer Perspektive ziemlich banal. Dies zeigt man ähnlich wie Lemma 2.3. Auch der erste Teil von Satz 2.4 unten ist unabhängig von der Stärke von T . Diese kommt erst ins Spiel, wenn man etwas über bew_T oder bwb_T im Rahmen von T beweisen will, wie dies in 7.1 geschehen wird. Der Satz kann nur unter besonderen Umständen verbessert werden. bwb_T ist z.B. für $T = \mathbf{Q}$ zwar r.a., nicht aber rekursiv, wie in 6.5 nachgewiesen wird.

Satz 2.4. *Sei X ein p.r. Axiomensystem für eine Theorie T in gödelisierbarer Sprache. Dann ist das Prädikat bew_T p.r. Hingegen sind bwb_T und T in der Regel nur rekursiv aufzählbar. Dasselbe gilt, wenn hier überall rekursiv statt p.r. gesagt wird.*

Beweis. (1) und (2) Seite 178 zeigen, dass bew_T p.r. ist. Damit ist bwb_T r.a. gemäß Definition dieses Begriffs, und zwar auch dann, wenn X und damit bew_T nur rekursiv statt p.r. sind. Dasselbe gilt für T ; denn $a \in \dot{T} \Leftrightarrow \exists b \text{ bew}_T(b, a) \ \& \ a \in \dot{\mathcal{L}}^0$, und \mathcal{L}^0 ist rekursiv, sogar p.r. wie vor Lemma 2.3 festgestellt wurde. \square

Übungen

1. Man beweise: hat eine Theorie T ein rekursiv aufzählbares Axiomensystem, so besitzt T auch ein rekursives Axiomensystem (W. Craig).
2. Man zeige (für $\mathcal{L} = \mathcal{L}_{ar}$): $a, a \dot{\sim} b \in \dot{\mathcal{L}} \Rightarrow b \in \dot{\mathcal{L}}$, für alle $a, b \in \mathbb{N}$ (die arithmetische Version von $\alpha, \alpha \rightarrow \xi \in \mathcal{L} \Rightarrow \xi \in \mathcal{L}$, vergleiche Übung 4 in 2.2).
3. Es sei $T (\subseteq \mathcal{L}_{ar}^0)$ axiomatisierbar und $\alpha \in \mathcal{L}_{ar}^0$. Man definiere ein p.r. $f \in \mathbf{F}_2$ mit $\text{bew}_{T+\alpha}(\dot{\Phi}, \dot{\varphi}) \Rightarrow \text{bew}_T(f(\dot{\Phi}, \dot{\alpha}), (\alpha \rightarrow \varphi)^\cdot)$ für alle φ (Arithmetisierung des Deduktionstheorems). Daraus schließe man $\text{bwb}_{T+\alpha}(\dot{\varphi}) \Leftrightarrow \text{bwb}_T(\alpha \rightarrow \varphi)^\cdot$.
4. Man zeige, die Menge Tr_0 aller quantorenfreien $\alpha \in \mathcal{L}_{ar}^0$ mit $\mathcal{N} \models \alpha$ ist p.r.

6.3 Repräsentierbarkeit arithmetischer Prädikate

Wir betrachten zuerst die endlich axiomatisierte Theorie \mathbf{Q} mit den Axiomen

$$\begin{aligned} \text{Q1: } \forall x \, Sx \neq 0 & \quad \text{Q2: } \forall x \forall y (Sx = Sy \rightarrow x = y) & \quad \text{Q3: } (\forall x \neq 0) \exists y \, x = Sy \\ \text{Q4: } \forall x \, x + 0 = x & \quad \text{Q5: } \forall x \forall y \, x + Sy = S(x + y) \\ \text{Q6: } \forall x \, x \cdot 0 = 0 & \quad \text{Q7: } \forall x \forall y \, x \cdot Sy = x \cdot y + x \end{aligned}$$

Diese Axiome kennzeichnen \mathbf{Q} als bescheidene Subtheorie der Peano-Arithmetik \mathbf{PA} . Beide Theorien sind formuliert in \mathcal{L}_{ar} , der Sprache 1. Stufe in $0, S, +, \cdot$. In \mathbf{Q} , \mathbf{PA} und allen weiteren Theorien in \mathcal{L}_{ar} seien \leq durch $x \leq y \leftrightarrow \exists z \, z + x = y$, und $<$ durch $x < y \leftrightarrow x \leq y \wedge x \neq y$ explizit definiert. Wie bisher sei $\underline{n} = S^n 0$, speziell $\underline{0} = 0$.

Aus den Resultaten dieses und des nächsten Abschnitts wird sich nicht nur die rekursive Unentscheidbarkeit von \mathbf{Q} ergeben, sondern auch die jeder Subtheorie und jeder konsistenten Erweiterung von \mathbf{Q} , siehe 6.5. Wären wir nur auf Unentscheidbarkeitsresultate aus, ließe sich der Beweis des Repräsentationssatzes 4.2 durch Vermehrung der Anfangsfunktionen und Elimination des Schemas **Op** etwas vereinfachen, doch verwischt ein solches Vorgehen einige für Kapitel 7 wichtige Details.

Wir zeigen induktiv $\vdash_{\mathbf{Q}} \underline{n} \neq S\underline{n}$ für alle n . Denn $\vdash_{\mathbf{Q}} 0 \neq S0$ ist klar nach Q1 und der Induktionsschritt $\vdash_{\mathbf{Q}} \underline{n} \neq S\underline{n} \Rightarrow \vdash_{\mathbf{Q}} S\underline{n} \neq SS\underline{n}$ folgt aus $S\underline{n} = SS\underline{n} \vdash_{\mathbf{Q}} \underline{n} = S\underline{n}$, einer Anwendung von Q2. Hier handelt es sich um eine *Metainduktion* (Induktion in der Metatheorie, zu der die natürlichen Zahlen stets gehören). In \mathbf{PA} ist $\forall x \, x \neq Sx$ leicht durch Induktion *in der Theorie* beweisbar. \mathbf{Q} aber ist so schwach, dass diese Aussage dort unbeweisbar ist. In der Tat, $(\mathbb{N} \cup \{\infty\}, 0, S, +, \cdot)$ erfüllt alle Axiome von \mathbf{Q} , nicht aber $\forall x \, x \neq Sx$. Dabei sei ∞ ein neues Objekt und die Operationen $S, +, \cdot$ seien wie folgt auf $\mathbb{N} \cup \{\infty\}$ erweitert: Es sei $S\infty = \infty$, $\infty \cdot 0 = 0$, sowie

$$\infty + n = n + \infty = \infty + \infty = n \cdot \infty = \infty \cdot m = \infty \text{ für alle } n \text{ und alle } m \neq 0.$$

Dieses Modell zeigt, dass viele bekannte Rechengesetze in \mathbf{Q} unbeweisbar sind, die das stets mit \mathcal{N} bezeichnete Standardmodell $(\mathbb{N}, 0, S, +, \cdot)$ als diskret geordneten kommutativen Halbring mit kleinstem Element 0 und Einselement $1 := \underline{1} (= S0)$ kennzeichnen, in dem Sx der unmittelbare Nachfolger von x ist. Die dies leistenden Rechengesetze denken wir uns in folgendem Axiomensystem \mathbf{N} zusammengefasst, wobei \leq und $<$ wie oben definiert sind. Quantoren in den Axiomen werden unterdrückt. Die Theorie \mathbf{N} wird in der Literatur auch mit \mathbf{PA}^- bezeichnet.

$$\begin{aligned} \text{N0: } x + 0 = x & \quad \text{N1: } x + y = y + x & \quad \text{N2: } (x + y) + z = x + (y + z) \\ \text{N3: } x \cdot 1 = x & \quad \text{N4: } x \cdot y = y \cdot x & \quad \text{N5: } (x \cdot y) \cdot z = x \cdot (y \cdot z) \\ \text{N6: } x \cdot (y + z) = x \cdot y + x \cdot z & \quad \text{N7: } Sx = x + 1 & \quad \text{N8: } x + z = y + z \rightarrow x = y \\ \text{N9: } x \leq y \vee y \leq x & \quad \text{N10: } x \leq 0 \rightarrow x = 0 & \quad \text{N11: } x < y \leftrightarrow Sx \leq y \end{aligned}$$

Eine empfehlenswerte Übung ist der Nachweis aller Q-Axiome in \mathbf{N} . Auch sind alle Axiome von \mathbf{N} in \mathbf{PA} beweisbar (vgl. die Übungen in 3.3). Also $\mathbf{Q} \subseteq \mathbf{N} \subseteq \mathbf{PA}$.

In diesem Abschnitt schreiben wir meistens nur $\vdash \alpha$ für $\vdash_{\mathbf{Q}} \alpha$ und $\alpha \vdash \beta$ für $\alpha \vdash_{\mathbf{Q}} \beta$ usw. Auch schreiben wir häufig $\alpha \vdash \beta \vdash \gamma$ für $\alpha \vdash \beta$ und $\beta \vdash \gamma$, und ebenso $\vdash t_1 = t_2 = t_3$ für $\vdash t_1 = t_2 \wedge t_2 = t_3$. Die Benutzung von \vdash in den folgenden Ableitungen macht die dabei verwendete Metainduktion etwas plastischer. Einige der Beweise kann man als „Verlegungen von Induktionen in \mathbf{PA} in die Metatheorie“ ansehen. So entspricht dem unten ausgeführten metainduktiven Beweis von C0 über n in \mathbf{Q} dem induktiven Beweis von $Sx + y = x + Sy$ über y in \mathbf{PA} . Wir zeigen für alle n, m

$$\begin{aligned} \text{C0: } & \vdash Sx + \underline{n} = x + S\underline{n}, \\ \text{C1: } & \vdash \underline{m} + \underline{n} = \underline{m + n}, \quad \underline{m \cdot n} = \underline{m \cdot n}, \quad \text{C2: } \vdash \underline{m} \neq \underline{n} \text{ falls } m \neq n, \\ \text{C3: } & \vdash \underline{m} \leq \underline{n} \text{ falls } m \leq n, \quad \text{C4: } \vdash \underline{m} \not\leq \underline{n} \text{ falls } m \not\leq n, \\ \text{C5: } & x \leq \underline{n} \vdash x = \underline{0} \vee \dots \vee x = \underline{n}, \quad \text{C6: } \vdash x \leq \underline{n} \vee \underline{n} \leq x. \end{aligned}$$

C3 ergibt leicht die Umkehrung von C5. Kurzum, $x \leq \underline{n} \equiv_{\mathbf{Q}} \bigvee_{i \leq n} x = \underline{i}$. Das liefert auch $x < \underline{n} \equiv_{\mathbf{Q}} \bigvee_{i < n} x = \underline{i}$ ($\equiv \perp$ für $n = 0$). Die folgenden Beweise verlaufen induktiv, genauer metainduktiv, über n . Man beachte dabei stets $S\underline{n} = \underline{S n} (= \underline{n + 1})$.

C0: Klar für $n = 0$, weil $\vdash Sx + 0 = Sx = S(x + 0) = x + S0$ nach Q4, Q5. Annahme: $\vdash Sx + \underline{n} = x + S\underline{n}$. Dann folgt $\vdash Sx + S\underline{n} = S(Sx + \underline{n}) = S(x + S\underline{n}) = x + SS\underline{n}$. Das beweist $\vdash Sx + S\underline{n} = x + SS\underline{n}$ und damit den Induktionsschritt.

C1: Nach Q4 ist $\vdash \underline{m} + 0 = \underline{m}$, und weil $\underline{m} = \underline{m + 0}$, ist $\vdash \underline{m} + 0 = \underline{m + 0}$. Aus $\vdash \underline{m} + \underline{n} = \underline{m + n}$ (Induktionsannahme) folgt mit Q5 $\vdash \underline{m} + S\underline{n} = S(\underline{m + n}) = S\underline{m + n}$ und der letzte Term ist derselbe wie $\underline{m + S n}$. Das beweist den Induktionsschritt. Analog zeigt man $\vdash \underline{m \cdot n} = \underline{m \cdot n}$ mit Q6, Q7 und dem schon Bewiesenen.

C2: $m \neq 0$ impliziert $m = Sk$ für ein k . Damit $\vdash \underline{m} \neq 0$ nach Q1. Sei $m \neq Sn$. Dann ist sicher $\vdash \underline{m} \neq S\underline{n}$ falls $m = 0$ oder $m = n$ (wegen $\vdash \underline{n} \neq S\underline{n}$, siehe Vorseite). Andernfalls ist $m = Sk$ für ein k mit $k \neq n$ – sonst wäre $m = Sn$. Weil $\vdash \underline{k} \neq \underline{n}$ nach Induktionsannahme, ergibt sich $\vdash \underline{m} \neq S\underline{n}$ nach Q2.

C3: $m \leq n$ impliziert $k + m = n$ für ein k , also $\underline{k + m} = \underline{n}$. Das ergibt $\vdash \underline{k + m} = \underline{n}$ nach C1, und folglich $\vdash \underline{m} \leq \underline{n}$. Der Beweis von C4 sei dem Leser als Übung überlassen. Als Hinweis möge die leicht beweisbare Äquivalenz $x \leq y \equiv_{\mathbf{Q}} Sx \leq Sy$ genügen.

C5: Klar für $n = 0$, weil $x \leq 0, x \neq 0 \vdash \exists v Sv = 0 \vdash \perp$ nach Q3, Q5, Q1. Gleichwertig mit der Induktionsbehauptung ist $x \neq 0, x \leq \underline{S n} \vdash \bigvee_{i=1}^{n+1} x = \underline{i}$. Dies folgt aus

$$\begin{aligned} x \neq 0, x \leq \underline{S n} & \vdash \exists y (x = Sy \wedge y \leq \underline{n}) & (\text{Q3, Q5, and Q2}) \\ & \vdash \exists y (x = Sy \wedge \bigvee_{i \leq n} y = \underline{i}) & (\text{Induktionsannahme}) \\ & \vdash \exists y (x = Sy \wedge \bigvee_{i=1}^{n+1} Sy = \underline{i}) \vdash \bigvee_{i=1}^{n+1} x = \underline{i}. \end{aligned}$$

C6: Klar für $n = 0$, weil $\vdash 0 \leq x$ nach Q4. Sonst ist $\underline{n} < x \vdash \exists y \mathbf{S}y + \underline{n} = x \vdash \underline{\mathbf{S}n} \leq x$ nach C0 und $\vdash 0 + \underline{n} = \underline{n}$ gemäß C1. Ferner ergibt C5 leicht $x \leq \underline{n} \vdash x \leq \underline{\mathbf{S}n}$. Damit folgt der Induktionsschritt aus $x \leq \underline{n} \vee \underline{n} \leq x \vdash x \leq \underline{n} \vee \underline{n} < x \vdash x \leq \underline{\mathbf{S}n} \vee \underline{\mathbf{S}n} \leq x$.

Nach diesen Vorbereitungen nun die folgende entscheidende

Definition. $P \subseteq \mathbb{N}^n$ heie (ziffernweise) reprsentierbar in der Theorie $T \supseteq \mathbf{Q}$ ²⁾, falls es ein $\alpha = \alpha(\vec{x})$ gibt, eine reprsentierende Formel, derart dass

$$\mathbf{R}^+: P\vec{a} \Rightarrow \vdash_T \alpha(\vec{a}) \quad ; \quad \mathbf{R}^-: \neg P\vec{a} \Rightarrow \vdash_T \neg \alpha(\vec{a}).$$

Ein in \mathbf{Q} reprsentiertes Prdikat P ist offenbar in jeder Theorie $T \supseteq \mathbf{Q}$ mit derselben Formel reprsentierbar, speziell in $\mathbf{Th}\mathcal{N}$. Weil $\mathcal{N} \models \alpha(\vec{a}) \Leftrightarrow \mathcal{N} \models \alpha[\vec{a}]$, bedeuten Reprsentierbarkeit von P in $\mathbf{Th}\mathcal{N}$ und Definierbarkeit von P in \mathcal{N} durch α im Sinne von 2.3 ein und dasselbe. Mglichst scharfer Resultate wegen betrachten wir fast nur den Fall $T = \mathbf{Q}$. Deshalb wird der Zusatz „in \mathbf{Q} “ oft weggelassen, wenn von Reprsentierbarkeit die Rede ist wie in den folgenden Beispielen.

Beispiele. Die Identittsrelation $\{(a, a) \mid a \in \mathbb{N}\}$ wird reprsentiert durch die Formel $x = y$. Denn $\vdash \underline{a} = \underline{b}$ fr $a = b$ ist trivial, und $\vdash \underline{a} \neq \underline{b}$ fr $a \neq b$ gilt nach C2. Die Formel $x \leq y$ reprsentiert gem C3, C4 das \leq -Prdikat. Die leere Menge wird durch $x \neq x$ reprsentiert, aber auch durch jede Aussage α mit $\neg \alpha \in \mathbf{Q}$.

Ein in \mathbf{Q} durch α reprsentiertes P ist im anschaulichen Sinne rekursiv: Man braucht ja nur die Aufzhlungsmaschine fr \mathbf{Q} einzuschalten und abzuwarten bis $\alpha(\vec{a})$ oder $\neg \alpha(\vec{a})$ erscheint. Mehr darber in 6.4. Fr konsistente $T \supseteq \mathbf{Q}$ gelten mit \mathbf{R}^+ , \mathbf{R}^- offenbar auch deren Umkehrungen, also $P\vec{a} \Leftrightarrow \vdash_T \alpha(\vec{a})$ und $\neg P\vec{a} \Leftrightarrow \vdash_T \neg \alpha(\vec{a})$. Die Menge der in T reprsentierbaren n -stelligen Prdikate ist abgeschlossen gegenber Vereinigung, Durchschnitt und Komplementen, sowie gegenber Vertauschung, Gleichsetzung und Hinzufgen fiktiver Argumente. Werden z.B. P, Q durch $\alpha(\vec{x}), \beta(\vec{x})$ reprsentiert, so $P \cap Q$ offenbar durch $\alpha(\vec{x}) \wedge \beta(\vec{x})$ und $\neg P$ durch $\neg \alpha(\vec{x})$.

Man knnte eine Funktion $f \in \mathbf{F}_n$ als reprsentierbar bezeichnen, wenn $\mathbf{graph} f$ reprsentierbar ist. Dies erweist sich jedoch als quivalent mit einer schrferen Form der Reprsentierbarkeit von Funktionen, der wir uns spter zuwenden werden.

Die in \mathcal{N} (d.h. mit $0, \mathbf{S}, +, \cdot$) elementar definierbaren Prdikate heien nach [G2] *arithmetisch*. Von jetzt ab habe dieses Wort stets diese Bedeutung. Um mehr ber die reprsentierbaren arithmetischen Prdikate zu erfahren, betrachten wir genauer deren definierende Formeln. Ein erstes Resultat wird Korollar 3.2 sein.

²⁾Die Annahme $T \supseteq \mathbf{Q}$ ist nicht zwingend, umfasst aber den interessantesten Fall. In [G2] heien reprsentierbare Prdikate *entscheidungsdefinit* (bersetzt als *decidable* in [Hei]), in [HB] *vertretbar*, in [K11] *numeralwise expressible*, in [TMR] *definable* und in [En] *representable*.

Primformeln in \mathcal{L}_{ar} sind Gleichungen, auch *diophantische Gleichungen* genannt. Ist $\delta(\vec{x}, \vec{y})$ eine solche Gleichung mit $P\vec{a} \Leftrightarrow \mathcal{N} \models \exists \vec{y} \delta(\vec{a}, \vec{y})$, so heißt das Prädikat P *diophantisch*. Ein einfaches Beispiel ist \leq , denn $a \leq b \Leftrightarrow \exists y y + a = b$ ³⁾. Es sind alle durch \exists -Formeln $\exists \vec{y} \varphi$ in \mathcal{N} definierbaren Prädikate diophantisch. Der Nachweis ist recht einfach: man denke man sich die quantorenfreie Formel φ mittels \wedge, \vee aus Literalen aufgebaut und nutze beim induktiven Nachweis über φ die Äquivalenzen

$$\begin{aligned} s \neq t &\equiv_{\mathcal{N}} \exists z (Sz + s = t \vee Sz + t = s), \\ s_1 = t_1 \wedge s_2 = t_2 &\equiv_{\mathcal{N}} s_1^2 + t_1^2 + s_2^2 + t_2^2 = 2(s_1 t_1 + s_2 t_2), \\ s_1 = t_1 \vee s_2 = t_2 &\equiv_{\mathcal{N}} s_1 s_2 + t_1 t_2 = s_1 t_2 + s_2 t_1. \end{aligned}$$

Eine nicht nur für Fragen der Repräsentierbarkeit nützliche Klassifikation arithmetischer Formeln und Prädikate liefert folgende in 6.7 verallgemeinerte

Definition. Eine Formel heiße Δ_0 oder eine Δ_0 -Formel, wenn sie aus Primformeln in \mathcal{L}_{ar} durch \wedge, \neg und *beschränkte Quantifizierung* erzeugt wird, d.h. mit α ist auch $(\forall x \leq t) \alpha$ eine Δ_0 -Formel ($\forall x \leq t$ hat den Wirkungsbereich α); hier sei t ein Term in \mathcal{L}_{ar} mit $x \notin \text{var } t$. Ist φ Δ_0 und \vec{x} beliebig, so heißt $\exists \vec{x} \varphi$ eine Σ_1 -Formel und $\forall \vec{x} \varphi$ eine Π_1 -Formel. Ferner: $P \subseteq \mathbb{N}^n$ heißt Δ_0, Σ_1 bzw. Π_1 , wenn P durch eine Δ_0 -Formel, eine Σ_1 -Formel bzw. eine Π_1 -Formel in \mathcal{N} definiert ist. Δ_0, Σ_1 und Π_1 bezeichnen die Mengen der Δ_0 -, Σ_1 - bzw. Π_1 -Prädikate. Es sei $\Delta_1 := \Sigma_1 \cap \Pi_1$.

Man nennt eine Formel schon dann Δ_0, Σ_1 bzw. Π_1 , wenn sie zu einer oben genannten nur äquivalent ist. In diesem Sinne sind mit α z.B. auch $(\exists x \leq t) \alpha$ ($\equiv \neg(\forall x \leq t) \neg \alpha$) und $(\forall x < t) \alpha$ ($\equiv (\forall x \leq t)(x = t \vee \alpha)$) Δ_0 -Formeln. Man beachte, Δ_1 besteht aus den Prädikaten, die sowohl Σ_1 - als auch Π_1 -definierbar sind; gleichwertig, P und $\neg P$ gehören beide zu Σ_1 , denn Π_1 besteht offenbar gerade aus den Komplementen der $P \in \Sigma_1$. Nach Übung 3 in 2.4 sind Σ_1 und Π_1 unter Vereinigung und Durchschnitt von Prädikaten gleicher Stellenzahl abgeschlossen, und Δ_1 zudem unter Komplementen. Ist f (genauer $\text{graph } f$) Σ_1 , so ist f zugleich auch Π_1 und damit Δ_1 . Denn $f\vec{a} \neq b \Leftrightarrow \exists c (f\vec{a} = c \ \& \ c \neq b)$. Daher ist auch $\neg \text{graph } f$ wieder Σ_1 .

Beispiele. Diophantische Gleichungen sind die einfachsten Δ_0 -Formeln. Dazu gehören die Formeln $y = t(\vec{x})$ mit $y \notin \text{var } t$, die die Termfunktionen $\vec{a} \mapsto t^{\mathcal{N}}(\vec{a})$ definieren. Weil $a|b \Leftrightarrow (\exists c \leq b) a \cdot c = b$, sind Teilbarkeit und damit auch das Prädikat prim Δ_0 . Dasselbe gilt für die durch $a \perp b \Leftrightarrow (\forall c \leq a+b)(c|a, b \Rightarrow c = 1)$ definierte Relation \perp der Teilerfremdheit. Weil $\varphi(a, b) = c \Leftrightarrow 2c = (a+b)^2 + 3a + b$, ist die Paarkodierung Δ_0 . Diophantische Prädikate sind Σ_1 . Nach Satz 5.6 gilt bemerkenswerterweise auch die Umkehrung, obwohl man längere Zeit vermutet hatte, dass z.B. die Menge $\{a \in \mathbb{N} \mid (\forall p \leq a)(\text{prim } p \ \& \ p|a \Rightarrow p = 2)\}$ der Potenzen von 2 nicht diophantisch sei. Diese ist sicher Δ_0 . Unersichtlich ist hingegen, dass auch $\text{graph } n \mapsto 2^n$ Δ_0 ist.

³⁾eine der schnelleren Lesbarkeit halber benutzte informelle Schreibweise für $\mathcal{N} \models \exists y y + \underline{a} = \underline{b}$.

Bemerkung 1. Sogar das Prädikat ‘ $a^b = c$ ’ ist Δ_0 , aber dieser Nachweis ist aufwendig. Schon der in 6.4 erbrachte Nachweis, dass dieses Prädikat überhaupt arithmetisch ist, kostet Mühe. Frühere Resultate von Bennet, Paris, Pudlak u.a. werden in [BD] wie folgt verallgemeinert: Ist $f \in \mathbf{F}_{n+1} \Delta_0$, so auch $g: (\vec{a}, n) \mapsto \prod_{i \leq n} f(\vec{a}, i)$, und die Rekursionsgleichung $g(\vec{x}, Sy) = g(\vec{x}, y) \cdot f(\vec{x}, y)$ ist bereits in $I\Delta_0$ beweisbar, einer wichtigen Abschwächung von PA. Diese Theorie entsteht aus Q durch Hinzufügen des auf Δ_0 -Formeln beschränkten Induktionsschemas und spielt eine vielseitige Rolle, siehe z.B. [Kra] oder [HP]. Induktiv über die Δ_0 -Formeln folgt leicht, dass alle Δ_0 -Prädikate p.r. sind. Die Umkehrung gilt nicht. Ein Beispiel ist die sehr schnell wachsende p.r. *Hyperexponentiation* mit $\text{hex}(a, 0) = 1$ und $\text{hex}(a, Sb) = a^{\text{hex}(a, b)}$. Anschaulich formuliert $\text{hex}(a, n) = \underbrace{a^{a^{\dots^a}}}_n$.

Satz 3.1 unten besagt, dass schon die relativ schwache Theorie Q in dem im Satz erklärten Sinne Σ_1 -vollständig ist. Es gibt unterschiedliche Beweise für den Satz. Zum Beispiel könnte man modelltheoretisch vorgehen und u.a. ausnutzen, dass \mathcal{N} nach C1 und C2 Primmodell von Q im Sinne von 5.1 ist. Wir wählen hier indes einen konstruktiven Weg, der zusätzliche Informationen liefert. Der Satz wird für PA in 7.1 zur sogenannten beweisbaren Σ_1 -Vollständigkeit verschärft.

Satz 3.1 (über die Σ_1 -Vollständigkeit der Theorie Q). *Jede in \mathcal{N} wahre Σ_1 -Aussage ist in Q und damit in jeder Theorie $T \supseteq Q$ schon beweisbar.*

Beweis. Wir behaupten zuerst, es genügt zu zeigen

(\star) Entweder $\vdash_Q \alpha$ oder $\vdash_Q \neg \alpha$, für jede Δ_0 -Aussage α .

Denn sei $\mathcal{N} \models \exists \vec{x} \varphi(\vec{x})$ mit der Δ_0 -Formel $\varphi(\vec{x})$, etwa $\mathcal{N} \models \alpha := \varphi(\vec{a})$. Nach (\star) ist dann $\vdash_Q \alpha$ weil $\vdash_Q \neg \alpha$ entfällt, und mithin $\vdash_Q \exists \vec{x} \varphi(\vec{x})$. Wir beweisen (\star) zuerst für Primaussagen α . Ist t ein variablenfreier Term so folgt mit C1 leicht $\vdash_Q t = t^{\mathcal{N}}$, z.B. ergibt sich $\vdash_Q (3+4) \cdot 5 = 35$. Ist α also die Primaussage $t_1 = t_2$, so ist $\vdash_Q t_1^{\mathcal{N}} = t_2^{\mathcal{N}}$ oder $\vdash_Q t_1^{\mathcal{N}} \neq t_2^{\mathcal{N}}$ nach C2, was (\star) für α bestätigt. Die Induktionsschritte über \wedge, \neg sind einfach. So gilt $\vdash_Q \alpha \wedge \beta$ falls $\vdash_Q \alpha, \beta$ und $\vdash_Q \neg \alpha \vee \neg \beta \equiv_Q \neg(\alpha \wedge \beta)$ falls $\vdash_Q \neg \alpha$ oder $\vdash_Q \neg \beta$. Diese Schritte genügen bereits zum Beweis von (\star), denn die beschränkten Quantoren sind aus einer Δ_0 -Aussage α modulo Q gänzlich eliminierbar! In der Tat, es stehe $(\forall x \leq t)$ am weitesten links in α und habe den Wirkungsbereich β . Dann ist $\text{var } t = \emptyset$, denn $x \notin \text{var } t$ und ein $y \in \text{var } t$ müsste weiter links gebunden sein. Ferner gilt $(\forall x \leq t) \beta(x) \equiv_Q (\forall x \leq \underline{n}) \beta(x)$ mit $n := t^{\mathcal{N}}$, weil $\vdash_Q t = \underline{n}$. Mit C3 und C5 ergibt sich aber leicht $(\forall x \leq \underline{n}) \beta(x) \equiv_Q \beta(\underline{0}) \wedge \dots \wedge \beta(\underline{n})$. Damit kann $(\forall x \leq t)$ aus α eliminiert werden und dieser Prozess lässt sich nötigenfalls wiederholen. \square

Ist $\varphi(\vec{x}) \Delta_0$, gilt nach diesem Satz mit $\mathcal{N} \models \varphi(\vec{a})$ auch $\vdash_Q \varphi(\vec{a})$ und mit $\mathcal{N} \models \neg \varphi(\vec{a})$ auch $\vdash_Q \neg \varphi(\vec{a})$. Denn $\varphi(\vec{a})$ und $\neg \varphi(\vec{a})$ sind trivialerweise Σ_1 . Wir erhalten so das

Korollar 3.2. *Jede Δ_0 -Formel repräsentiert in Q das durch diese Formel in \mathcal{N} definierte Prädikat.*

Lemma 3.3. *Es sei $P \subseteq \mathbb{N}^{n+1}$ repräsentiert durch $\alpha(\vec{x}, y)$, sowie $z \notin \text{frei } \alpha$. Dann repräsentieren $(\exists z \leq y)\alpha(\vec{x}, z)$ und $(\forall z \leq y)\alpha(\vec{x}, z)$ die Prädikate Q und R mit*

$$Q(\vec{a}, b) \Leftrightarrow (\exists c \leq b)P(\vec{a}, c) \text{ bzw. } R(\vec{a}, b) \Leftrightarrow (\forall c \leq b)P(\vec{a}, c).$$

Analoges gilt, wenn \leq hier überall durch $<$ ersetzt wird.

Beweis. R^+ : Es gelte $Q(\vec{a}, b)$, d.h. $P(\vec{a}, c)$ für ein $c \leq b$. Dann ist $\vdash \alpha(\vec{a}, \underline{c}) \wedge \underline{c} \leq \underline{b}$ nach C3 Seite 183. Somit $\vdash (\exists z \leq \underline{b})\alpha(\vec{a}, z)$. Zum Beweis von R^- sei $\neg Q(\vec{a}, b)$, also $\vdash \neg \alpha(\vec{a}, \underline{i})$ für alle $i \leq b$. Mit C5 ergibt dies $z \leq \underline{b} \vdash \bigvee_{i \leq b} z = \underline{i} \vdash \neg \alpha(\vec{a}, z)$ und folglich $\vdash (\forall z \leq \underline{b})\neg \alpha(\vec{a}, z) \equiv \neg(\exists z \leq \underline{b})\alpha(\vec{a}, z)$, womit R^- gezeigt ist. Für das Prädikat R genügt der Hinweis auf $R(\vec{a}, b) \Leftrightarrow \neg(\exists c \leq b)\neg P(\vec{a}, c)$. Der Beweis bleibt wörtlich derselbe, wenn \leq überall durch $<$ ersetzt wird. \square

Wir erklären nun den Begriff der repräsentierbaren Funktion nach [TMR] und [Gö2]. Auch wenn dieser neue Begriff deutlich strenger als die Repräsentierbarkeit von $\text{graph } f$ ist, werden sich beide Begriffe in Lemma 3.4(b) als gleichwertig erweisen.

Definition. $f \in \mathbf{F}_n$ heie repräsentierbar in T (ohne den Zusatz ‘in T ’ sei stets $T = \mathbf{Q}$ gemeint), wenn für eine (repräsentierende) Formel $\varphi(\vec{x}, y)$ und alle $\vec{a} \in \mathbb{N}^n$

$$R^+ : \vdash_T \varphi(\vec{a}, \underline{f\vec{a}}), \quad R^- : \varphi(\vec{a}, y) \vdash_T y = \underline{f\vec{a}}.$$

Ist f durch φ repräsentiert, so durch dasselbe φ auch $\text{graph } f$. Denn ist $f\vec{a} = b$, gilt $\vdash_T \varphi(\vec{a}, \underline{b})$ nach R^+ , und aus $f\vec{a} \neq b$ folgt $\vdash_T \neg \varphi(\vec{a}, \underline{b})$ nach C2 und R^- . Weil R^+ offenbar gleichwertig ist mit $y = \underline{f\vec{a}} \vdash_T \varphi(\vec{a}, y)$, sind R^+ und R^- zusammen ersetzbar durch die einzige Bedingung $y = \underline{f\vec{a}} \equiv_T \varphi(\vec{a}, y)$ für alle \vec{a} .

Hat P eine repräsentierende Δ_0 -, Σ_1 - bzw. Π_1 -Formel, heie P auch Δ_0 -, Σ_1 - bzw. Π_1 -repräsentierbar. Ist P zugleich Σ_1 - und Π_1 -repräsentierbar, so werde P Δ_1 -repräsentierbar genannt. Analoge Redeweisen verwenden wir für Funktionen. Satz 4.5 wird zeigen, dass repräsentierbare Prädikate immer auch Δ_1 -repräsentierbar sind.

Lemma 3.4. (a) *Sei $P \subseteq \mathbb{N}^{n+1}$ durch $\alpha(\vec{x}, y)$ repräsentiert und $\forall \vec{a} \exists b P(\vec{a}, b)$. Dann wird $f : \vec{a} \mapsto \mu b [P(\vec{a}, b)]$ durch $\varphi(\vec{x}, y) := \alpha(\vec{x}, y) \wedge (\forall z < y)\neg \alpha(\vec{x}, z)$ repräsentiert. Ist P Δ_1 -repräsentierbar, so ist f Σ_1 -repräsentierbar. (b) f ist repräsentierbar, falls $\text{graph } f$ repräsentierbar ist, und insbesondere Δ_0 -repräsentierbar, falls $\text{graph } f$ dies ist. (c) Ist f Σ_1 -repräsentierbar, so ist f auch Π_1 -repräsentierbar. (d) Ist χ_P Σ_1 -repräsentierbar, so ist P Δ_1 -repräsentierbar.*

Beweis. (a) Die Formel $\varphi(\vec{x}, y)$ repräsentiert nach Lemma 3.3 das durch sie definierte Prädikat und dies ist offenbar $\text{graph } f$. Es verbleibt daher der Beweis von

$$R_\varphi^- : \alpha(\vec{a}, y) \wedge (\forall z < y)\neg \alpha(\vec{a}, z) \vdash y = \underline{f\vec{a}}.$$

Sei $b := f\vec{a}$. Dann ist $\underline{b} < y \vdash (\exists z < y)\alpha(\vec{a}, z)$, weil $\vdash \alpha(\vec{a}, \underline{b})$. Kontraposition liefert $(\forall z < y)\neg \alpha(\vec{a}, z) \vdash \underline{b} \not< y$. Nach C5 und R^- gilt $y < \underline{b} \vdash \bigvee_{i < b} y = \underline{i} \vdash \neg \alpha(\vec{a}, y)$. Daher

$\alpha(\vec{a}, y) \vdash y \not\leq \underline{b}$. Also $\alpha(\vec{a}, y) \wedge (\forall z < y) \neg \alpha(\vec{a}, z) \vdash y \not\leq \underline{b} \wedge \underline{b} \not\leq y \vdash y = \underline{b}$ gemäß C6. Das beweist R_φ^- . Zum Beweis der Zusatzbehauptung betrachte man einfach nur die Σ_1 -Formel $\alpha(\vec{x}, y) \wedge (\forall v < y) \neg \alpha'(\vec{x}, v)$, wobei P durch α Σ_1 - und durch α' Π_1 -repräsentiert wird. (b) ist eine Anwendung von (a) auf $P = \text{graph } f$, einfach weil $f\vec{a} = \mu b[P(\vec{a}, b)]$. (c): Sei f durch die Σ_1 -Formel $\varphi(\vec{x}, y)$ repräsentiert und $z \notin \text{var } \varphi$. Dann ist die Formel $\varphi'(\vec{x}, y) := \forall z(\varphi(\vec{x}, z) \rightarrow y = z)$ sicher Π_1 und f wird auch durch φ' repräsentiert. Denn nach R^- für φ ist $\vdash \varphi'(\vec{a}, f\vec{a})$, und es gilt auch

$$\varphi'(\vec{a}, y) = \forall z(\varphi(\vec{a}, z) \rightarrow y = z) \vdash \varphi(\vec{a}, f\vec{a}) \rightarrow y = f\vec{a} \vdash y = f\vec{a} \quad (\text{weil } \vdash \varphi(\vec{a}, f\vec{a})).$$

(d): Sei χ_P durch $\varphi(\vec{x}, y)$ Σ_1 -repräsentiert. Dann ist P durch $\varphi(\vec{x}, \underline{1})$ und $\neg \varphi(\vec{x}, \underline{0})$ zugleich Σ_1 - und Π_1 -repräsentiert wie man leicht verifiziert. \square

Bemerkung 2. Nach Lemma 3.4(b) ist z.B. die Paarkodierung \wp in \mathcal{Q} durch die Δ_0 -Formel $\pi(x, y, z) \wedge (\forall u < z) \neg \pi(x, y, u)$ repräsentiert; dabei ist $\pi(x, y, z)$ hier die Primformel $(x + y) \cdot S(x + y) + \underline{2} \cdot x = \underline{2} \cdot z$. Man beachte, in \mathcal{N} wird \wp durch π explizit definiert.

Lemma 3.5. (a) Sei $P \subseteq \mathbb{N}^k$ durch $\alpha(\vec{y})$ repräsentiert und $g_i \in \mathbf{F}_n$ für $i = 1, \dots, k$ durch $\gamma_i(\vec{x}, y_i)$. Dann wird $Q := P[g_1, \dots, g_k]$ durch $\beta(\vec{x}) := \exists \vec{y}[\alpha(\vec{y}) \wedge \bigwedge_i \gamma_i(\vec{x}, y_i)]$ repräsentiert. Sind die γ_i Σ_1 , so ist mit P auch das Prädikat Q Δ_1 -repräsentierbar. (b) Mit $h \in \mathbf{F}_m$ und $g_1, \dots, g_m \in \mathbf{F}_n$ ist auch $f = h[g_1, \dots, g_m]$ (Δ_1 -)repräsentierbar.

Beweis. (a): Sei $b_i := g_i \vec{a}$, so dass $\vdash \gamma_i(\vec{a}, b_i)$, $i = 1, \dots, k$, sowie $\vec{b} = (b_1, \dots, b_k)$, $\vec{b} = (b_1, \dots, b_k)$. Gilt $Q\vec{a}$, also $P\vec{b}$, so ist $\vdash \alpha(\vec{b})$. Mithin $\vdash \alpha(\vec{b}) \wedge \bigwedge_i \gamma_i(\vec{a}, b_i)$, also $\vdash \beta(\vec{a})$. Falls aber $\neg Q\vec{a}$ und damit $\neg P\vec{b}$, so ist $\vdash \neg \alpha(\vec{b})$. Mit $R_{\gamma_i}^-$ ergibt sich hieraus $\bigwedge_i \gamma_i(\vec{a}, y_i) \vdash \bigwedge_i y_i = b_i \vdash \neg \alpha(\vec{y})$. Daher $\vdash \forall \vec{y}[\bigwedge_i \gamma_i(\vec{a}, y_i) \rightarrow \neg \alpha(\vec{y})] \equiv \neg \beta(\vec{a})$. Sind die γ_i und auch α Σ_1 , so auch β . Wird P zugleich durch die Π_1 -Formel $\alpha'(\vec{x})$ repräsentiert, so Q durch die Π_1 -Formel $\forall \vec{y}[\bigwedge_i \gamma_i(\vec{x}, y_i) \rightarrow \alpha'(\vec{y})]$. (b): $\beta(\vec{x}, z)$ repräsentiere h . Wie in (a) zeigt man leicht $\exists \vec{y}[\beta(\vec{y}, z) \wedge \bigwedge_i \gamma_i(\vec{x}, y_i)]$ repräsentiert $h[g_1, \dots, g_m]$. \square

Übungen

1. Man zeige, jede Σ_1 -Formel ist in \mathcal{N} äquivalent zu einer Σ_1 -Formel $\exists y \varphi$, jede Π_1 -Formel zu $\forall y \varphi$ für eine gewisse Δ_0 -Formel φ (*Quantorenkompression*).
2. Man zeige, Σ_1 ist abgeschlossen unter beschränkter Quantifizierung. Genauer, definiert $\alpha = \alpha(x, y, \vec{v})$ ein Σ_1 -Prädikat, so auch $(\forall y < x) \alpha$ und $(\exists y < x) \alpha$. Dasselbe zeige man für Π_1 . Dies gilt demnach auch für Δ_1 .
3. Man zeige, $\alpha(\vec{x}) \wedge y = \underline{1} \vee \neg \alpha(\vec{x}) \wedge y = \underline{0}$ repräsentiert χ_P , falls α P repräsentiert.
4. Man beweise durch „Hineintreiben der Negation“ (Übung 2 in 2.4): jede Δ_0 -Formel ist äquivalent zu einer aus Literalen allein mit \wedge, \vee und den beschränkten Quantoren $(\forall x \leq t)$ und $(\exists x \leq t)$ aufgebauten Formel.

6.4 Der Repräsentationssatz

Zur Repräsentierbarkeit aller rekursiven oder auch nur aller p.r. Funktionen ist eine repräsentierbare Funktion $g \in \mathbf{F}_2$ hilfreich, für die zu jedem n und jeder Zahlenfolge c_0, \dots, c_n eine Zahl c existiert derart, dass $g(c, i) = c_i$ für alle $i \leq n$. Kurzum, c lässt sich so wählen, dass die Werte $g(c, 0), g(c, 1), \dots, g(c, n)$ die vorgegebenen sind. Es gibt nun viele sogar p.r. Funktionen g , die dies leisten. So gilt für $g(c, i) = (c)_i$ und $c = p_0^{1+c_0} \cdot \dots \cdot p_n^{1+c_n}$ in der Tat $g(c, i) = c_i$, wenn $i \leq n$. Nur ist zunächst kein Weg erkennbar, die Repräsentierbarkeit einer solchen Funktion g in \mathbf{Q} (oder einer Erweiterung von \mathbf{Q}) im Rahmen der Sprache \mathcal{L}_{ar} nachzuweisen. Deswegen hat K. Gödel, der um 1930 mit diesem und ähnlichen Problemen befasst war, nach den Worten von A. Mostowski „mit Gott telefoniert“. Man kennt heute mehrere Möglichkeiten, aber wir folgen der ursprünglichen, die ihren Reiz nicht verloren hat.

Es sei $\alpha(a, b, i) := \text{rest}(a, (1 + (1 + i)b))$. Die Funktion α ist wegen

$$\alpha(a, b, i) = k \Leftrightarrow (\exists c \leq a)[a = c(1 + (1 + i)b) + k \ \& \ k < 1 + (1 + i)b]$$

nach Korollar 3.2 und Lemma 3.4(b) Δ_0 -repräsentierbar. Dasselbe gilt für die Paar-kodierung \wp , Bemerkung 2 in 6.3. Weil \wp bijektiv ist, gibt es gewiss Funktionen \varkappa_1, \varkappa_2 mit $\wp(\varkappa_1 k, \varkappa_2 k) = k$ für alle k . Deren explizite Darstellung ist hier unwesentlich. Es werden nur die Ungleichungen $\varkappa_1 k, \varkappa_2 k \leq k$ benötigt. Die Funktion $\beta: (c, i) \mapsto \alpha(\varkappa_1 c, \varkappa_2 c, i)$ heie die β -Funktion. Auch diese ist Δ_0 -repräsentierbar, denn weil $\beta(c, i) = k \Leftrightarrow (\exists a \leq c)(\exists b \leq c)[\wp(a, b) = c \ \& \ \alpha(a, b, i) = k]$, gewinnen wir wie für α und \wp eine β repräsentierende Δ_0 -Formel $\text{beta} = \text{beta}(x, y, z)$. Damit ist die β -Funktion sogar durch eine Δ_0 -Formel in \mathcal{N} definierbar.

Man benötigt folgenden einfachen zahlentheoretischen Satz, um die wesentliche, in Lemma 4.1 formulierte Eigenschaft der β -Funktion zu erkennen.

Chinesischer Restsatz. Sei $c_i < d_i$ für $i = 0, \dots, n$ und seien d_0, \dots, d_n paarweise teilerfremd. Dann existiert ein $a \in \mathbb{N}$ mit $\text{rest}(a, d_i) = c_i$ für $i = 0, \dots, n$.

Beweis durch Induktion über n . Für $n = 0$ ist dies klar mit $a = c_0$. Seien nun die Voraussetzungen für $n > 0$ erfüllt. Nach Induktionsannahme ist $\text{rest}(a, d_i) = c_i$ für ein a und alle $i < n$. Auch $k := \text{kgV}\{d_\nu \mid \nu < n\}$ und d_n sind teilerfremd (Übung 2). Also existieren nach Übung 1 Zahlen $x, y \in \mathbb{N}$ mit $xk + 1 = yd_n$. Multipliziert man beide Seiten mit $c_n(k - 1) + a$, folgt $x'k + c_n(k - 1) + a = y'd_n$ mit neuen Werten $x', y' \in \mathbb{N}$. Sei $a' := (x' + c_n)k + a = y'd_n + c_n$. Dann ist $\text{rest}(a', d_i) = \text{rest}(a, d_i) = c_i$ für alle $i < n$ (weil $d_i \mid k$), aber auch $\text{rest}(a', d_n) = c_n$, denn $c_n < d_n$. \square

Dieser Beweis ist – anders als die Beweise in vielen Lehrbüchern der Zahlentheorie – konstruktiv und nach PA übertragbar wie 7.1 zeigen wird. In der Mathematischen

Logik kommt es gelegentlich nicht nur darauf an was man beweist, sondern wie man es beweist.

Lemma 4.1 (über die β -Funktion). *Zu jedem k und jeder Folge c_0, \dots, c_k gibt es ein c mit $\beta(c, i) = c_i$ für $i = 0, \dots, k$.*

Beweis. Wir geben Werte a und b mit $\alpha(a, b, i) = c_i$ an. Die Behauptung ist wegen $\beta(\wp(a, b), i) = \alpha(a, b, i)$ dann mit $c = \wp(a, b)$ erfüllt. Sei $m = \max\{k, c_0, \dots, c_k\}$ und $b := \text{kgV}\{i + 1 \mid i < m\}$. Wir behaupten, die Zahlen $d_i := 1 + (1 + i) \cdot b > c_i$ ($i \leq k$) sind paarweise teilerfremd. Denn angenommen p sei ein Primteiler von d_i, d_j mit $i < j \leq k$. Dann gilt $p \mid d_j - d_i = (j - i)b$, also $p \mid j - i$ oder $p \mid b$. Nun gilt wegen $j - i \leq k \leq m$ aber $j - i \nmid b$ aufgrund der Definition von b , d.h. $p \nmid b$ in jedem Falle. Wegen $b \mid d_i - 1$ folgt $p \mid d_i - 1$ im Widerspruch zu $p \mid d_i$, was die behauptete Teilerfremdheit bestätigt. Nach dem Chinesischen Restsatz existiert daher ein a mit $\text{rest}(a, d_i) = c_i$ für $i = 0, \dots, k$, d.h. $\alpha(a, b, i) = c_i$. \square

Bemerkung 1. Schon an dieser Stelle gewinnt man die interessante Einsicht, dass die Exponentialfunktion $(a, b) \mapsto a^b$ in \mathcal{N} elementar definierbar ist, nämlich durch

$$(*) \quad \delta_{\text{exp}}(x, y, z) := \exists u [\beta(u, 0) = \mathbf{S}0 \wedge (\forall v < y) \beta(u, \mathbf{S}v) = \beta(u, v) \cdot x \wedge \beta(u, y) = z].$$

Genauer, δ_{exp} ist die *Beschreibung* einer Σ_1 -Formel, die durch Elimination der β -Terme mittels der Δ_0 -Formel **beta** unter Benutzung weiterer \exists -Quantoren aus $(*)$ entsteht. Man beweist induktiv über b leicht $\mathcal{N} \models \delta_{\text{exp}}(\underline{a}, \underline{b}, \underline{c}) \Rightarrow a^b = c$. Sei umgekehrt $a^b = c$. Dann garantiert uns Lemma 4.1 ein gesuchtes u mit $\mathcal{N} \models \delta_{\text{exp}}(\underline{a}, \underline{b}, \underline{c})$: man wähle ein u mit $\beta(u, i) = a^i$ für alle $i \leq b$. Diese Argumentation wird in Satz 4.2 verallgemeinert.

Im folgenden Satz sei nur der Übersicht halber $T \supseteq \mathbf{Q}$ angenommen; er gilt genauso, wenn z.B. \mathbf{Q} im Sinne von 6.6 in T nur interpretierbar ist, etwa für ZFC. Für viele Anwendungen, z.B. die Herleitung von Unentscheidbarkeitsresultaten und einer vereinfachten Version des 1. Unvollständigkeitssatzes reicht bereits der erste Teil des Satzes aus. Die Verfeinerung im zweiten Teil wird z.B. in Satz 4.5 angewendet.

Satz 4.2 (Repräsentationssatz). *Jede rekursive Funktion f – und somit auch jedes rekursive Prädikat P – ist in \mathbf{Q} und damit in jeder konsistenten Theorie $T \supseteq \mathbf{Q}$ repräsentierbar. f ist sogar Σ_1 -repräsentierbar.*

Beweis. Es genügt, eine f repräsentierende Σ_1 -Formel anzugeben. Für die Anfangsfunktionen $0, \mathbf{S}, I_\nu^n$ leisten dies $\mathbf{v}_0 = 0, \mathbf{v}_1 = \mathbf{S}\mathbf{v}_0$ und $\mathbf{v}_n = \mathbf{v}_\nu$. Für **Oc** sei $f = h[g_1, \dots, g_m]$ und es seien $\beta(\vec{y}, z)$ und $\gamma_i(\vec{x}, y_i)$ repräsentierende Σ_1 -Formeln für h und die g_i . Dann ist $\varphi(\vec{x}, z) := \exists \vec{y} [\bigwedge_i \gamma_i(\vec{x}, y_i) \wedge \beta(\vec{y}, z)]$ eine derartige Formel für f (Lemma 3.5). Nun sei $f = \mathbf{Op}(g, h)$ und g, h seien beide Σ_1 -repräsentierbar. Erklärt man P durch $P(\vec{a}, b, c) \Leftrightarrow \beta(c, 0) = g\vec{a} \ \& \ (\forall v < b) \beta(c, \mathbf{S}v) = h(\vec{a}, v, \beta(c, v))$, so ist P nach Lemma 3.5 und 3.3 Δ_1 -repräsentierbar (Komposition und Einsetzung

Σ_1 -repräsentierbarer Funktionen, sowie beschränkte Quantifizierung und Konjunktion). Man sieht leicht, dass $P(\vec{a}, b, c)$ gleichwertig ist mit

$$(*) \quad \beta(c, i) = f(\vec{a}, i) \text{ für alle } i \leq b.$$

Nach Lemma 4.1 gibt es zu gegebenen \vec{a}, b eine den Gleichungen $(*)$ genügendes c , also gilt $\forall \vec{a} \forall b \exists c P(\vec{a}, b, c)$. Daher ist $f^*: (\vec{a}, b) \mapsto \mu c P(\vec{a}, b, c)$ nach Lemma 3.4(a) Σ_1 -repräsentierbar. Mit $i = b$ ergibt $(*)$ dann offenbar $\beta(f^*(\vec{a}, b), b) = f(\vec{a}, b)$. Wie oben bei **0c** gezeigt wurde, ist f als Komposition Σ_1 -repräsentierbarer Funktionen wieder Σ_1 -repräsentierbar. Schließlich entstehe f aus g mittels **0μ**, also $f\vec{a} = \mu b[P(\vec{a}, b)]$, mit $P(\vec{a}, b) \Leftrightarrow g(\vec{a}, b) = 0$; dabei sei g Σ_1 -repräsentierbar. Nach Lemma 3.4(c) ist g auch Π_1 -repräsentierbar und P damit sicher Δ_1 -repräsentierbar. Dann aber ist f nach Lemma 3.4(a) auch Σ_1 -repräsentierbar. \square

Sei $T \supseteq \mathbf{Q}$ eine Theorie in \mathcal{L}_{ar} . Der Gödelzahl $n = \dot{\varphi}$ von $\varphi \in \mathcal{L}_{ar}$ entspricht in T der Term \underline{n} , der fortan mit $\ulcorner \varphi \urcorner$ bezeichnet werde und der *Gödelterm* von φ heiße. Es ist z.B. $\ulcorner v_0 = 0 \urcorner = \dot{v}_0 \doteq \dot{0} = \underline{2^{22} \cdot 3^2 \cdot 5^{14}}$. Analog sei $\ulcorner t \urcorner$ definiert. Beispielsweise ist $\ulcorner \underline{1} \urcorner = \ulcorner S0 \urcorner = \underline{2^{16} \cdot 3^{14}}$. Ist T axiomatisierbar, so ist $\ulcorner \Phi \urcorner$ auch für Beweise Φ wohldefiniert. Z.B. ist $\Phi = (Sv_0 = Sv_0)$ ein trivialer Beweis der Länge 1 nach Axiom $\Lambda 9$ in **3.6**. Sein Gödelterm ist $\ulcorner \Phi \urcorner = \underline{2^{\tilde{s}v_0} \doteq \tilde{s}v_0 + 1} = \underline{2^{2^{16} \cdot 3^{22} \cdot 5^2 \cdot 7^{16} \cdot 11^{22} + 1}}$.

Weil das auf Seite 178 definierte Prädikat bew_T p.r. ist (Satz 2.4), ist bew_T Σ_1 -repräsentierbar nach dem Repräsentationssatz 4.2, sagen wir durch $\text{bew}_T(y, x)$. Ferner sei $\text{bwb}_T(x) := \exists y \text{bew}_T(y, x)$. Satz 4.2 liefert damit folgendes

Korollar 4.3. *Sei $T \supseteq \mathbf{Q}$ axiomatisierbar. Dann gilt $\vdash_T \varphi \Rightarrow \vdash_T \text{bew}_T(\underline{n}, \ulcorner \varphi \urcorner)$ für ein n (daher $\vdash_T \varphi \Rightarrow \vdash_T \text{bwb}_T(\ulcorner \varphi \urcorner)$), und $\nvdash_T \varphi \Rightarrow \vdash_T \neg \text{bew}_T(\underline{n}, \ulcorner \varphi \urcorner)$ für alle n .*

Die Umkehrung $\vdash_T \text{bwb}_T(\ulcorner \varphi \urcorner) \Rightarrow \vdash_T \varphi$ muss nicht gelten; siehe dazu **7.1**. Vor der Formulierung weiterer Folgerungen aus Satz 4.2 stellen wir noch eine Methode vor, welche die Churchsche These aus anschaulichen Entscheidbarkeits-Argumenten zu eliminieren erlaubt. Das muss im Prinzip immer gesichert sein, sonst verlöre die These ihre Berechtigung. Diese wird z.B. in Satz 3.5.2 verwendet. Wir formulieren diesen Satz jetzt etwas präziser und beweisen ihn anschließend rigoros.

Satz 4.4. *Eine vollständige axiomatisierbare Theorie T ist rekursiv.*

Beweis. Wegen der angenommenen Vollständigkeit ist die Funktion f mit

$$f(a) = \mu b[a \in \dot{\mathcal{L}}^0 \Rightarrow \text{bew}_T(b, a) \vee \text{bew}_T(b, \tilde{a})]$$

wohldefiniert. Denn bezeichnet $P(a, b)$ das p.r. Prädikat in eckigen Klammern, gilt offenbar $\forall a \exists b P(a, b)$, wobei für $a \notin \dot{\mathcal{L}}^0$ bereits $P(a, 0)$ zutrifft. Gemäß **0μ** ist f also rekursiv. Ferner gilt $(*)$ $a \in \dot{T} \Leftrightarrow a \in \dot{\mathcal{L}}^0 \ \& \ \text{bew}_T(fa, a)$, was sofort die Rekursivität

von T impliziert. Zum Nachweis von $(*)$ sei $a \in \dot{T}$, und damit gewiss $a \in \dot{\mathcal{L}}^0$. Dann gilt für $b = fa$ – das kleinste b mit $\text{bew}_T(b, a) \vee \text{bew}_T(b, \neg a)$ – sicher das erste Alternativglied, weil wegen der Konsistenz von T überhaupt kein b mit $\text{bew}_T(b, \neg a)$ existiert. Also $\text{bew}_T(fa, a)$. Die Richtung \Leftarrow in $(*)$ ist offensichtlich. \square

Dieser Beweis illustriert zugleich den Unterschied zwischen einem p.r. und einem rekursiven Entscheidungsverfahren. Auch wenn X und damit das Prädikat P p.r. sind, muss die dort definierte rekursive Funktion f nicht mehr p.r. sein, denn die Vollständigkeit von T könnte ja auf nichtkonstruktive Weise erschlossen worden sein. Der Gebrauch der Churchschen These in den Beweisen von (i) \Rightarrow (ii) und (iii) \Rightarrow (ii) im folgenden Satz kann in fast derselben Weise eliminiert werden wie oben, nur ist der Beweis dann etwas weniger anschaulich und seine Lektüre wird erschwert.

Satz 4.5. *Für ein Prädikat $P \subseteq \mathbb{N}^n$ und eine beliebige konsistente axiomatisierbare Theorie $T \supseteq Q$ sind folgende Eigenschaften äquivalent:*

- (i) P ist repräsentierbar in T , (ii) P ist rekursiv, (iii) P ist Δ_1 .

Beweis. (i) \Rightarrow (ii): P werde in T durch $\alpha(\vec{x})$ repräsentiert. Wir starten bei gegebenem \vec{a} die Aufzählungsmaschine von T und warten, bis $\alpha(\vec{a})$ oder $\neg\alpha(\vec{a})$ erscheint. Also ist P entscheidbar und damit rekursiv. (ii) \Rightarrow (i),(iii): Nach Satz 4.2 ist χ_P in T durch eine Σ_1 -Formel repräsentiert. Daher ist P gemäß Lemma 3.4(d) Δ_1 -repräsentierbar und zugleich wurde $P \in \Delta_1$ gezeigt. (iii) \Rightarrow (ii): Sei P definiert durch die Σ_1 -Formel $\alpha(\vec{x})$ und durch die Π_1 -Formel $\beta(\vec{x})$. Wir starten bei gegebenem \vec{a} die Aufzählungsmaschine für T und warten, bis eine der Σ_1 -Aussagen $\alpha(\vec{a})$ oder $\neg\beta(\vec{a})$ erscheint. Im ersten Falle gilt $P\vec{a}$, im zweiten nicht. Das Verfahren terminiert, denn T ist Σ_1 -vollständig nach Satz 3.1. Also ist P entscheidbar und damit rekursiv. \square

Nach dem Satz sind in jeder konsistenten axiomatischen Erweiterung von Q dieselben Prädikate repräsentierbar, nämlich genau die rekursiven. Ferner besteht Δ_1 danach genau aus den rekursiven, und wie man unter Beachtung von Übung 1 in 6.3 leicht folgert, Σ_1 genau aus den r.a. Prädikaten. Satz 4.5 macht den engen Zusammenhang zwischen Logik und Rekursionstheorie besonders deutlich. Er ist unabhängig von der Churchschen These. Selbst wenn diese irgendwie revidiert werden müsste, würde die ausgezeichnete Rolle der μ -rekursiven Funktionen dadurch nicht angetastet.

Bemerkung 2. Man wünscht sich natürlich ein übersehbares Repräsentantensystem von Formeln, welche die rekursiven Prädikate in hinreichend starken Theorien repräsentieren oder in \mathcal{N} zumindest definieren. Leider kann man ein solches Formelsystem nicht rekursiv aufzählen. Denn angenommen es gibt eine solche Aufzählung. Sei $\alpha_0, \alpha_1, \dots$ die hieraus entstehende Folge ihrer Glieder aus \mathcal{L}_{ar}^1 , die in \mathcal{N} dann die rekursiven Mengen definieren. Dann ist auch $\{n \in \mathbb{N} \mid n \notin \alpha_n^{\mathcal{N}}\}$ rekursiv, also etwa durch α_m in \mathcal{N} definiert, so dass $n \in \alpha_m^{\mathcal{N}} \Leftrightarrow n \notin \alpha_n^{\mathcal{N}}$. Das ergibt für $n = m$ aber den Widerspruch $m \in \alpha_m^{\mathcal{N}} \Leftrightarrow m \notin \alpha_m^{\mathcal{N}}$.

In 6.5 benötigen wir eine p.r. „Substitutionsfunktion“ sb_x und in 7.1 eine Verallgemeinerung davon. Bezeichne $zf\ a := \underline{a}$ ($= (\underline{a})^\cdot$) die Gödelzahl des Terms \underline{a} ($= S^a 0$). Dann ist $a \mapsto zf\ a$ p.r., da $zf\ 0 = \underline{0}$ und $zf\ Sa = \dot{S} * zf\ a$. Sei $sb_x(m, a) = [m]_{\dot{x}}^{zf\ a}$, sowie $sb_{\vec{x}} \in \mathbf{F}_{n+1}$ induktiv über die Länge von $\vec{x} \in Var^n$ erklärt durch $sb_{\emptyset}(m) := m$ und $sb_{\vec{x}x}(m, \vec{a}, a) = sb_x(sb_{\vec{x}}(m, \vec{a}), a)$. Dabei seien x_1, \dots, x_n, x paarweise verschieden. Speziell ist $sb_x(m, a)$ wohldefiniert. Das Parametertupel \vec{x} kann beliebig umgeordnet werden, wenn zugleich das Variablentupel \vec{a} entsprechend umgeordnet wird. So ist z.B. $sb_{xy}(m, a, b) = sb_{yx}(m, b, a)$. Die Funktionen $sb_{\vec{x}}$ sind offenbar alle p.r.

Es sei $\dot{\alpha}_{\vec{x}}^{\vec{t}} := (\alpha_{\vec{x}}^{\vec{t}})^\cdot$ und speziell $\dot{\alpha}_{\vec{x}}(\vec{a})$ die Gödelzahl der Aussage $\alpha_{\vec{x}}(\vec{a})$. Dann gilt

Satz 4.6. Für beliebiges $\alpha \in \mathcal{L}$ ist $sb_{\vec{x}}(\dot{\alpha}, \vec{a}) = \dot{\alpha}_{\vec{x}}(\vec{a})$ für alle $\vec{a} \in \mathbb{N}^n$.

Beweis. Weil $\alpha_{\vec{x}}(\vec{a})$ durch schrittweise Ausführung einfacher Substitutionen entsteht (siehe (2) in 2.2), muss nur $sb_x(\dot{\alpha}, a) = \dot{\alpha}_x(a)$ für alle a gezeigt werden. Nach (*) Seite 180 gilt aber $sb_x(\dot{\alpha}, a) = [\dot{\alpha}]_{\dot{x}}^{zf\ a} = [\dot{\alpha}]_{\dot{x}}^{\underline{a}} = (\alpha_x(\underline{a}))^\cdot = \dot{\alpha}_x(\underline{a})$. \square

Beispiel. α sei $Sx=y$. Dann ist $sb_{xy}(\dot{\alpha}, a, b) = (S\underline{a}=\underline{Sb})^\cdot$ für alle $a, b \in \mathbb{N}$. Ferner gilt $sb_{xy}(\dot{\alpha}, a, Sa) = (S\underline{a}=\underline{Sa})^\cdot = (S\underline{a}=\underline{Sa})^\cdot = sb_x(\dot{\alpha}_{\frac{Sx}{y}}, a)$. Diese Gleichung wird mit etwas anderen Bezeichnungen in Übung 4(c) verallgemeinert.

Übungen

- Man beweise das im Beweis des Chinesischen Restsatzes wesentlich benutzte **Lemma von Euklid**: Sind $a, b \in \mathbb{N}_+$ teilerfremd, so gibt es Zahlen $x, y \in \mathbb{N}$ mit $xa + 1 = yb$. (Die Umkehrung ist trivial: $c|a, b \Rightarrow c|yb - xa = 1 \Rightarrow c=1$.)
- Man zeige (a) $\text{prim } p \ \& \ p|ab \Rightarrow p|a \vee p|b$, (b) $\text{prim } p \ \& \ p|\text{kgV}\{a_\nu | \nu \leq n\} \Rightarrow p|a_\nu$ für ein $\nu \leq n$, (c) $\text{kgV}\{d_\nu | \nu < n\}$ und d_n sind teilerfremd ($n > 0$), falls die Zahlen d_0, \dots, d_n paarweise teilerfremd sind.
- Man gebe eine definierende Σ_1 -Formel für die Primzahlaufzählung $n \mapsto p_n$ an.
- Man expandiere die \mathcal{L}_{ar} -Struktur \mathcal{N} um die Funktionen $\hat{\wedge}, \hat{\neg}, \hat{\rightarrow}, \hat{\vee}$, sowie alle $sb_{\vec{x}}$ und nötigenfalls weitere p.r. Grundfunktionen zu einer Struktur \mathcal{N}^* , so dass die Terme $sb_{\vec{x}}(\ulcorner \varphi \urcorner, \vec{x})$ für $\varphi \in \mathcal{L}_{ar}$ in der Theorie von \mathcal{N}^* wohldefiniert sind. Man beweise, in \mathcal{N}^* gelten für beliebige $\alpha, \beta \in \mathcal{L}_{ar}$ folgende Gleichungen, die in 7.1 nach PA übertragen werden:
 (a) $sb_{\vec{x}}(\ulcorner \alpha \wedge \beta \urcorner, \vec{x}) = sb_{\vec{x}}(\ulcorner \alpha \urcorner, \vec{x}) \hat{\wedge} sb_{\vec{x}}(\ulcorner \beta \urcorner, \vec{x})$, und analog für \neg, \rightarrow und \vee .
 (b) $sb_{\vec{x}}(\ulcorner \alpha \urcorner, \vec{x}) = sb_{\vec{x}'}(\ulcorner \alpha \urcorner, \vec{x}')$, mit $\text{var } \vec{x}' := \text{var } \vec{x} \cap \text{frei } \alpha$.
 (c) $sb_{\vec{x}x}(\ulcorner \alpha \urcorner, \vec{x}, t) = sb_{\vec{x}}(\ulcorner \alpha_{\frac{t}{x}} \urcorner, \vec{x})$ für Terme $t \in \{0, y, Sy\}$ falls $x \notin \text{frei } \alpha$ oder $y \in \text{var } \vec{x}$. Sonst ist $sb_{\vec{x}x}(\dot{\alpha}, \vec{x}, t) \equiv sb_{\vec{x}y}(\dot{\alpha}_{\frac{t}{x}}, \vec{x}, y)$. Hier sei $x \notin \text{var } \vec{x}$, sowie $y \notin \text{gbd } \alpha$ (damit $\alpha, \frac{y}{x}$ kollisionsfrei sind).

6.5 Die Sätze von Gödel, Tarski, Church

Eine Theorie $T \subseteq \mathcal{L}$ heie *gdelisierbar* (oder auch *arithmetisierbar*), wenn \mathcal{L} gdelisierbar ist und eine Folge $(\underline{n})_{n \in \mathbb{N}}$ von Grundtermen vorhanden ist, so dass $\vdash_T \underline{n} \neq \underline{m}$ fr $n \neq m$ und $\text{zf}: n \mapsto \underline{n}$ p.r. ist, siehe 6.4. Dies sind minimale Voraussetzungen fr die Reprsentierbarkeit arithmetischer Prdikate in T . Sie gelten fr jedes $T \supseteq \mathcal{Q}$, aber z.B. auch fr ZFC mit wesentlich derselben Termfolge (ω -Terme genannt, $\underline{0}$ sei \emptyset und $\underline{n+1}$ sei $\underline{n} \cup \{\underline{n}\}$). Auch im allgemeinen Falle sei $\alpha \in \mathcal{L}$ in T durch den Term $\ulcorner \alpha \urcorner = \underline{\alpha}$ kodiert. Um bei den folgenden allgemeinen Lemmata eine konkrete Vorstellung zu haben, denke man etwa an $\mathcal{L} = \mathcal{L}_{ar}$ und $T = \text{PA}$.

Eine Aussage γ heie ein *Fixpunkt von* $\alpha(x) \in \mathcal{L}$ in T , falls $\gamma \equiv_T \alpha(\ulcorner \gamma \urcorner)$, oder gleichwertig, $\vdash_T \gamma \leftrightarrow \alpha(\ulcorner \gamma \urcorner)$. In anschaulicher Formulierung besagt γ dann offenbar „ α trifft auf mich zu“. Die Funktion sb_x aus 6.4 ist fr beliebig gewhltes x unter relativ schwachen Voraussetzungen in T reprsentierbar (Satz 4.2). Daher haben die folgenden beiden Lemmata ein breites Anwendungsspektrum.

Fixpunktlemma. *Sei T gdelisierbar und sei sb_x in T reprsentierbar. Dann gibt es zu jedem $\alpha = \alpha(x) \in \mathcal{L}$ ein $\gamma \in \mathcal{L}^0$ mit*

$$(1) \quad \gamma \equiv_T \alpha(\ulcorner \gamma \urcorner).$$

Beweis. Sei $x_1, x_2, y \neq x$ und $\text{sb}(x_1, x_2, y)$ eine sb_x in T reprsentierende Formel, die sich im Prinzip auch effektiv angeben lsst. Fr alle Formeln $\varphi = \varphi(x)$ und alle n gilt also $\text{sb}(\ulcorner \varphi \urcorner, \underline{n}, y) \equiv_T y = \ulcorner \varphi(\underline{n}) \urcorner$. Fr $n = \dot{\varphi}$, also $\underline{n} = \ulcorner \varphi \urcorner$ folgt speziell

$$(2) \quad \text{sb}(\ulcorner \varphi \urcorner, \ulcorner \varphi \urcorner, y) \equiv_T y = \ulcorner \varphi(\ulcorner \varphi \urcorner) \urcorner.$$

Sei $\beta(x) := \forall y (\text{sb}(x, x, y) \rightarrow \alpha \frac{y}{x})$. Dann leistet $\gamma := \beta(\ulcorner \beta \urcorner)$ das Verlangte. Denn

$$\begin{aligned} \gamma &= \forall y (\text{sb}(\ulcorner \beta \urcorner, \ulcorner \beta \urcorner, y) \rightarrow \alpha \frac{y}{x}) \\ &\equiv_T \forall y (y = \ulcorner \beta(\ulcorner \beta \urcorner) \urcorner \rightarrow \alpha \frac{y}{x}) && ((2) \text{ mit } \varphi = \beta(x)) \\ &= \forall y (y = \ulcorner \gamma \urcorner \rightarrow \alpha \frac{y}{x}) && (\text{weil } \gamma = \beta(\ulcorner \beta \urcorner)) \\ &\equiv \alpha(\ulcorner \gamma \urcorner). && \square \end{aligned}$$

Auch das folgende Lemma formuliert ein hufig wiederkehrendes Argument.

Nichtreprsentierbarkeitslemma. *Sei T eine Theorie wie im Fixpunktlemma. Dann ist T (genauer, \dot{T}) in T selbst nicht reprsentierbar.*

Beweis. Angenommen, T wird durch $\tau(x)$ reprsentiert. Wir zeigen, dass bereits die schwchere Annahme (a) $\not\vdash_T \alpha \Leftrightarrow \vdash_T \neg \tau(\ulcorner \alpha \urcorner)$ zum Widerspruch fhrt. Denn sei γ Fixpunkt von $\neg \tau(x)$ gem (1) oben, also (b) $\vdash_T \gamma \Leftrightarrow \vdash_T \neg \tau(\ulcorner \gamma \urcorner)$. Whlt man $\alpha = \gamma$ in (a), ergibt sich mit (b) offenbar der Widerspruch $\not\vdash_T \gamma \Leftrightarrow \vdash_T \gamma$. \square

Wir formulieren nun den 1. Gödelschen Unvollständigkeitssatz, und zwar in drei Versionen, von denen die zweite im Wesentlichen der originalen entspricht. Von nun an sei der Einfachheit halber $\mathcal{L} \supseteq \mathcal{L}_{ar}$ und $T \supseteq Q$. Doch gilt alles folgende auch für Theorien T wie z.B. ZFC, in denen Q im Sinne von 6.6 nur interpretierbar ist.

Satz 5.1 (Die populäre Version). *Jede hinreichend starke konsistente rekursiv axiomatisierbare arithmetische Theorie T (genauer, $T \supseteq Q$) ist unvollständig.*

Beweis. Wäre T vollständig, so nach Satz 3.5.2 auch entscheidbar, also in Q und damit in T repräsentierbar, was das Nichtrepräsentierbarkeitslemma ausschließt. \square

Dieser Beweis ist, anders als die Beweise der Sätze 5.1' und 5.1'', nicht konstruktiv. Denn er gestattet nicht, eine Aussage α mit $\not\vdash_T \alpha$ und $\not\vdash_T \neg\alpha$ explizit anzugeben.

Eine Verschärfung der Konsistenz einer Theorie T in \mathcal{L}_{ar} ist ihre ω -Konsistenz, d.h. für alle $\varphi = \varphi(x)$ mit $\vdash_T \exists x\varphi(x)$ ist $\not\vdash_T \neg\varphi(\underline{n})$ für mindestens ein n , oder gleichwertig, $(\forall n \in \mathbb{N}) \vdash_T \neg\varphi(\underline{n})$ impliziert $\not\vdash_T \exists x\varphi(x)$. Ist \mathcal{N} Modell für T , so ist T sicher ω -konsistent; denn die Annahme $\vdash_T \exists x\varphi$ und $\vdash_T \neg\varphi(\underline{n})$ für alle n impliziert den Widerspruch $\mathcal{N} \models \exists x\varphi, \forall x\neg\varphi$. Also sind z.B. Q und PA aus semantischer Perspektive gewiss ω -konsistent und konsistent.⁴⁾

Satz 5.1' (Die Originalversion). *Zu jeder durch ein p.r. Axiomensystem X axiomatisierten ω -konsistenten Theorie $T \supseteq Q$ gibt es eine Π_1 -Aussage α , so dass weder $\vdash_T \alpha$ noch $\vdash_T \neg\alpha$, d.h. α ist unabhängig in T . Es gibt eine p.r. Funktion, die einer X repräsentierenden Formel ein solches α zuordnet.*

Beweis. Sei bew_T in T repräsentiert durch die Σ_1 -Formel bew_T , siehe Seite 191. Für $\text{bwb}(x) = \exists y \text{bew}_T(y, x)$ gilt dann (a) $\vdash_T \varphi \Rightarrow \vdash_T \text{bwb}(\ulcorner \varphi \urcorner)$ gemäß Korollar 4.3. Sei γ Fixpunkt von $\neg \text{bwb}(x)$ nach (1), also (b) $\gamma \equiv_T \neg \text{bwb}(\ulcorner \gamma \urcorner)$. Die Annahme $\vdash_T \gamma$ ergibt $\vdash_T \text{bwb}(\ulcorner \gamma \urcorner)$ nach (a), aber $\vdash_T \neg \text{bwb}(\ulcorner \gamma \urcorner)$ nach (b), im Widerspruch zur Konsistenz von T . Also $\not\vdash_T \gamma$. Angenommen $\vdash_T \neg\gamma$, so dass $\vdash_T \text{bwb}(\ulcorner \gamma \urcorner)$ nach (b), d.h. (c) $\vdash_T \exists y \text{bew}_T(y, \ulcorner \gamma \urcorner)$. Da T konsistent ist, gilt $\not\vdash_T \gamma$. Wiederum nach Korollar 4.3 ist also $\vdash_T \neg \text{bew}(\underline{n}, \ulcorner \gamma \urcorner)$ für alle n . Dies und (c) widersprechen aber der ω -Konsistenz von T . Daher ist auch $\not\vdash_T \neg\gamma$. Mit γ ist offenbar auch die Π_1 -Aussage $\alpha = \neg \text{bwb}(\ulcorner \gamma \urcorner)$ unabhängig in T . Die Behauptung über die p.r. Zuordnung folgt ersichtlich aus der Konstruktion von γ in (1). \square

Dieser Satz bleibt uneingeschränkt richtig, wenn das Axiomensystem X nur r.a. ist. Denn X kann durch ein rekursives X' ersetzt werden (Übung 1 in 6.2). Damit ist auch bew_T rekursiv, mithin in T repräsentierbar und nach Satz 4.5 auch Σ_1 .

⁴⁾Die Beweistheorie versucht, die nichtfinite Semantik den Betrachtungen fernzuhalten, und es gibt berühmte Konsistenzbeweise von PA , die weit weniger voraussetzen als die mengentheoretischen Hilfsmittel der Semantik.

Satz 5.1'' (Rossers Verschärfung von Satz 5.1'). *Die Voraussetzung der ω -Konsistenz in Satz 5.1' kann zur Konsistenz von T abgeschwächt werden.*

Beweis. Sei T konsistent und $\text{prov}(x) := \exists y[\text{bew}(y, x) \wedge (\forall z < y) \neg \text{bew}(z, \neg x)]$. Die p.r. Funktion \neg denken wir uns mittels einer sie repräsentierenden Formel hieraus wie üblich eliminiert. $\text{prov}(x)$ besagt wegen der Konsistenz von T im Prinzip dasselbe wie $\text{bwb}(x)$ und hat folgende Fundamenteigenschaften:

$$(a) \vdash_T \text{prov}(\ulcorner \alpha \urcorner) \text{ falls } \vdash_T \alpha, \quad (b) \vdash_T \neg \text{prov}(\ulcorner \alpha \urcorner) \text{ falls } \vdash_T \neg \alpha^5).$$

Denn sei $\vdash_T \alpha$, also $\vdash_T \text{bew}(\underline{n}, \ulcorner \alpha \urcorner)$ für ein n (Korollar 4.3). Da $\not\vdash_T \neg \alpha$ wegen der Konsistenz von T , folgt $\vdash_T \neg \text{bew}(\underline{k}, \ulcorner \neg \alpha \urcorner)$ für alle k . Daher liefert C5 aus 6.3 $\vdash_T (\forall z < \underline{n}) \neg \text{bew}(z, \ulcorner \neg \alpha \urcorner)$. Somit $\vdash_T \text{prov}(\ulcorner \alpha \urcorner)$. Nachweis von (b): Sei $\vdash_T \neg \alpha$, etwa $\vdash_T \text{bew}(\underline{m}, \ulcorner \neg \alpha \urcorner)$. Weil $\not\vdash_T \alpha$, ist $\vdash_T (\forall y \leq \underline{m}) \neg \text{bew}(y, \ulcorner \alpha \urcorner)$ nach C5. Das ergibt $\text{bew}(y, \ulcorner \alpha \urcorner) \vdash_T \underline{m} < y$ nach C6. Weil $\underline{m} < y \vdash_T (\exists z < y) \text{bew}(z, \ulcorner \neg \alpha \urcorner)$ (wähle $z = \underline{m}$), folgt $\vdash_T \forall y[\text{bew}(y, \ulcorner \alpha \urcorner) \rightarrow (\exists z < y) \text{bew}(z, \ulcorner \neg \alpha \urcorner)] \equiv \neg \text{prov}(\ulcorner \alpha \urcorner)$. Das beweist (b). Sei nun (c): $\gamma \equiv_T \neg \text{prov}(\ulcorner \gamma \urcorner)$ nach (1). Die Annahme $\vdash_T \gamma$ führt mit (a) und (c) zum Widerspruch $\vdash_T \text{prov}(\ulcorner \gamma \urcorner), \neg \text{prov}(\ulcorner \gamma \urcorner)$, und die Annahme $\vdash_T \neg \gamma$ führt mit (b) und (c) zu demselben Widerspruch. Also ist weder $\vdash_T \gamma$ noch $\vdash_T \neg \gamma$. \square

$T \subseteq \mathcal{L}_{ar}^0$ heißt ω -unvollständig, wenn es ein $\varphi = \varphi(x)$ gibt mit $\vdash_T \varphi(\underline{n})$ für alle n und dennoch $\not\vdash_T \forall x \varphi$. Wir zeigen, PA ist auch ω -unvollständig: Sei γ ein Fixpunkt von $\neg \text{bwb}_{\text{PA}}(x)$ und $\varphi(x) := \neg \text{bew}_{\text{PA}}(x, \ulcorner \gamma \urcorner)$. Weil $\not\vdash_{\text{PA}} \gamma$ (siehe den Beweis von Satz 5.1'), ist auch $\not\vdash_{\text{PA}} \forall x \varphi$ ($\equiv \neg \exists x \text{bew}_{\text{PA}}(x, \ulcorner \gamma \urcorner) \equiv_{\text{PA}} \gamma$). Wohl aber ist $\vdash_{\text{PA}} \varphi(\underline{n})$ für alle n wegen Korollar 4.3. Hier ist φ sogar Π_1 .

$\alpha \in \mathcal{L}^0$ heie *wahr* in einer Struktur \mathcal{A} , wenn $\mathcal{A} \models \alpha$. Insbesondere heit $\alpha \in \mathcal{L}_{ar}^0$ *wahr*, wenn $\mathcal{N} \models \alpha$. Falls es ein $\tau(x) \in \mathcal{L}$ gibt mit $\mathcal{A} \models \alpha \Leftrightarrow \mathcal{A} \models \tau(\ulcorner \alpha \urcorner)$ für alle $\alpha \in \mathcal{L}^0$, sagt man *der Wahrheitsbegriff von \mathcal{A} sei in \mathcal{A} definierbar*. Gleichwertig: $\text{Th}\mathcal{A}$ ist in $\text{Th}\mathcal{A}$ repräsentierbar. Das Nichtrepräsentierbarkeitslemma schließt dies für $\mathcal{A} = \mathcal{N}$ aber aus. Damit erhalten wir

Satz 5.2 (Tarskis Nichtdefinierbarkeitstheorem). *$\text{Th}\mathcal{N}$ ist nicht definierbar in \mathcal{N} ; mit anderen Worten, $\text{Th}\mathcal{N}$ ist nicht arithmetisch.*

In diesem Satz hat eine weit entwickelte Theorie über Definierbarkeit in \mathcal{N} ihren Ursprung (siehe auch 6.7). Er gilt sinngemäß für jeden Gegenstandsbereich \mathcal{A} , dessen Sprache gödelisierbar und in dem eine der Funktionen sb_x repräsentierbar ist.

Wir kommen nun zu Unentscheidbarkeitsresultaten. Zuerst wird die in Übung 1 in 3.5 formulierte Behauptung ohne Rückgriff auf die Churchsche These gezeigt.

⁵⁾Demnach ist speziell $\vdash_T \neg \text{prov}_T(\ulcorner \perp \urcorner)$. Dass dies, wenn hier bwb_T statt prov_T geschrieben wird, z.B. für $T = \text{PA}$ nicht der Fall ist, besagt der 2. Gödelsche Unvollständigkeitssatz 7.2.2. Obwohl also $\text{bwb}_T(x) \equiv_{\mathcal{N}} \text{prov}_T(x)$, verhalten sich bwb_T und prov_T innerhalb von T sehr verschieden.

Lemma 5.3. *Jede endliche Erweiterung T' einer entscheidbaren Theorie T in und derselben Sprache \mathcal{L} ist entscheidbar.*

Beweis. Sei T' Erweiterung von T um $\alpha_0, \dots, \alpha_m$, $\alpha := \bigwedge_{i \leq m} \alpha_i$, also $T' = T + \alpha$. Weil $\beta \in T' \Leftrightarrow \alpha \rightarrow \beta \in T$, erhalten wir $n \in \dot{T}' \Leftrightarrow n \in \dot{\mathcal{L}}^0 \ \& \ \dot{\alpha} \dot{\sim} n \in \dot{T}$. Mit \dot{T} , $\dot{\mathcal{L}}^0$ und $\dot{\sim}$ ist dann aber auch \dot{T}' rekursiv. \square

Dass T' derselben Sprache wie T angehört, ist hier wichtig. Eine durch $X \subseteq \mathcal{L}^0$ axiomatisierte entscheidbare Theorie T kann – betrachtet als Theorie in $\mathcal{L}' \supset \mathcal{L}$ mit demselben Axiomensystem X – wegen der hinzukommenden Tautologien von \mathcal{L}' durchaus unentscheidbar sein. Dieses Lemma wird oft so angewendet, dass man aus der Unentscheidbarkeit von T' die von T folgert, siehe etwa Satz 5.5 unten.

$T_0 \subseteq \mathcal{L}_0$ heie *streng unentscheidbar*, wenn T_0 konsistent ist und jede mit T_0 verträgliche Theorie $T \subseteq \mathcal{L}_0$ unentscheidbar ist. Dann ist sogar jede mit $T_0 \subseteq \mathcal{L}$ verträgliche Theorie T mit $\mathcal{L} \supseteq \mathcal{L}_0$ unentscheidbar, weil andernfalls auch $T \cap \mathcal{L}_0$ entscheidbar wäre. Mit T_0 ist jede konsistente Theorie $T_1 \supseteq T_0$ ebenfalls streng unentscheidbar; denn ist T mit T_1 verträglich, dann auch mit T_0 . Ferner ist dann auch jede Subtheorie von T_0 in \mathcal{L}_0 unentscheidbar, oder T_0 ist *erblich unentscheidbar* in der Terminologie von [TMR]. Je schwächer eine streng unentscheidbare Theorie, um so größer ihr Anwendungsbereich. Das wird noch deutlich werden durch

Satz 5.4. ([TMR]). *\mathcal{Q} ist streng unentscheidbar.*

Beweis. Seien T, \mathcal{Q} verträglich. Offenbar ist $T' := T + \mathcal{Q}$ eine konsistente endliche Erweiterung von T . Annahme T ist entscheidbar. Dann gilt dasselbe nach Lemma 5.3 auch für T' . Also ist T' nach Satz 4.2 in \mathcal{Q} und damit in sich selbst repräsentierbar, was das Nichtrepräsentierbarkeitslemma ausschließt. Also ist T unentscheidbar. \square

Satz 5.5 (Unentscheidbarkeitssatz von Church). *Die Menge $\text{Taut}_{\mathcal{L}}$ aller tautologischen Aussagen ist für $\mathcal{L} \supseteq \mathcal{L}_{ar}$ unentscheidbar.*

Beweis. $\text{Taut}_{\mathcal{L}}$ ist mit \mathcal{Q} sicher verträglich, also unentscheidbar nach Satz 5.4. \square

Dieses Resultat lässt sich durch Interpretation unschwer auf die Sprache mit einer zweistelligen Relation und damit auf alle Expansionen dieser Sprache übertragen, siehe 6.6, sowie überhaupt auf alle Sprachen mit Ausnahme derjenigen, die nur einstellige Prädikatensymbole und höchstens ein einstelliges Funktionssymbol enthalten. Für deren Tautologien gibt es tatsächlich auch Entscheidungsverfahren.

Nach Satz 5.4 ist speziell $\text{Th}\mathcal{N}$ unentscheidbar. Ebenso jede Subtheorie von $\text{Th}\mathcal{N}$, z.B. die Peano-Arithmetik PA, sowie deren Subtheorien und auch alle konsistenten Erweiterungen von PA. Denn diese sind mit \mathcal{Q} alle verträglich. $\text{Th}\mathcal{N}$ ist nicht einmal

axiomatisierbar, weil eine axiomatisierbare vollständige Theorie doch entscheidbar ist. Weitere Folgerungen über unentscheidbare Theorien werden in **6.6** gezogen.

Neben Unentscheidbarkeitsresultaten, die formalisierte Theorien betreffen, lassen sich auf ähnliche Weise auch zahlreiche spezielle Ergebnisse dieser Art gewinnen, etwa negative Lösungen von Wortproblemen aller Art, von Halteproblemen usw. (siehe z.B. [Ob], [Ba]). Von diesen war vielleicht die spektakulärste die Lösung des 10. Hilbertschen Problems: Gibt es einen Algorithmus, welcher für jedes Polynom $p(\vec{x})$ mit ganzzahligen Koeffizienten entscheidet, ob die diophantische Gleichung $p(\vec{x}) = 0$ ganzzahlig lösbar ist? Die Antwort ist nein, wie Matiyasevich 1970 bewies.

Wir skizzieren kurz den Beweisgang. Es genügt zu zeigen, dass es keinen Algorithmus für die Lösbarkeit aller diophantischen Gleichungen in \mathbb{N} gibt. Denn nach einem bekannten Satz von Lagrange ist jede natürliche Zahl Summe von vier Quadraten ganzer Zahlen. Folglich ist $p(\vec{x}) = 0$ in \mathbb{N} genau dann lösbar, wenn in \mathbb{Z} die Gleichung $p(u_1^2 + v_1^2 + w_1^2 + z_1^2, \dots, u_n^2 + v_n^2 + w_n^2 + z_n^2) = 0$ lösbar ist. Könnte man also über die Lösbarkeit diophantischer Gleichungen in \mathbb{Z} entscheiden, so auch über das entsprechende Problem in \mathbb{N} . Dazu beachte man zunächst, dass die Frage der Lösbarkeit von $p(\vec{x}) = 0$ in natürlichen Zahlen gleichwertig ist zur Lösbarkeit einer diophantischen Gleichung, d.h. einer Gleichung $s(\vec{x}) = t(\vec{x})$ mit Termen s, t aus \mathcal{L}_{ar} , indem man alle mit einem Minuszeichen versehenen Glieder von $p(x)$ „auf die andere Seite bringt“. Hilberts Problem reduziert sich so offenbar auf die Frage nach einem Entscheidungsalgorithmus für das Problem $\mathcal{N} \models \exists \vec{x} \delta(\vec{x})$, wobei $\delta(\vec{x})$ alle diophantischen Gleichungen aus \mathcal{L}_{ar} durchläuft.

Die negative Lösung des Hilbertschen Problems folgt leicht aus dem viel weitergehenden Satz 5.6, der eine überraschende Verbindung zwischen Zahlen- und Rekursionstheorie herstellt und z.B. in [Mat] ausführlich bewiesen wird. Dieser Satz ist ein Paradebeispiel dafür, dass gewisse Fragen zu Ergebnissen führen können, die in ihrer Bedeutung weit über die einer Antwort auf die ursprüngliche Frage hinausreichen.

Satz 5.6. *Ein arithmetisches Prädikat P ist diophantisch dann und nur dann, wenn P rekursiv aufzählbar ist.*

Um den Beweis wenigstens anzudeuten, sei das diophantische Prädikat $P \subseteq \mathbb{N}^n$ definiert durch $P\vec{a} \Leftrightarrow \mathcal{N} \models \exists \vec{y} \delta^{\mathcal{N}}(\vec{a}, \vec{y})$, mit der Gleichung $\delta(\vec{x}, \vec{y})$. Die definierende Formel für P ist Σ_1 , also ist P nach Übung 1 in **6.3** rekursiv aufzählbar. Dies ist sozusagen die triviale Richtung der Behauptung. Die Umkehrung – jedes r.a. Prädikat ist diophantisch – kann ihres Umfangs wegen hier nicht ausgeführt werden. Zahlreiche arithmetische Prädikate und Funktionen müssen durch trickreiche Überlegungen als diophantisch nachgewiesen werden, darunter das dreistellige Prädikat ‘ $a^b = c$ ’, das diesem Nachweis lange widerstanden hatte. Dieser Satz ergibt leicht das

Korollar 5.7. (a) *Das zehnte Hilbertsche Problem hat eine negative Antwort.*
 (b) *Für jede axiomatisierbare Theorie $T \supseteq \mathbf{Q}$, speziell für $T = \mathbf{PA}$, gibt es eine unlösbare diophantische Gleichung, deren Unlösbarkeit in T unbeweisbar ist.*

Beweis. $bwb_{\mathbf{Q}}$ ist nach 6.2 r.a. Gemäß Satz 5.6 existiert daher eine diophantische Gleichung $\delta(x, \vec{y})$ mit $(*)$ $bwb_{\mathbf{Q}}(n) \Leftrightarrow \mathcal{N} \models \exists \vec{y} \delta(\underline{n}, \vec{y})$. Wir behaupten, schon für die Schar $\exists \vec{y} \delta(\underline{n}, \vec{y})$ diophantischer Aussagen ($n = 0, 1, \dots$) gibt es kein Entscheidungsverfahren. Sonst wäre $\{n \in \mathbb{N} \mid \mathcal{N} \models \exists \vec{y} \delta(\underline{n}, \vec{y})\}$ rekursiv, und damit gemäß $(*)$ auch $bwb_{\mathbf{Q}}$ im Widerspruch zu Satz 5.4. Das beweist (a). Wäre die Unlösbarkeit jeder unlösbaren diophantischen Gleichung $\delta(\vec{x})$ in T beweisbar, so wäre entweder $\vdash_T \neg \exists \vec{x} \delta(\vec{x})$ (falls $\delta(\vec{x})$ unlösbar ist) oder $\vdash_T \exists \vec{x} \delta(\vec{x})$, wegen der Σ_1 -Vollständigkeit von T . Weil die Sätze von T r.a. sind, hätte man so eine Entscheidungsverfahren für die Lösbarkeit diophantischer Gleichungen vor sich, im Widerspruch zu (a). \square

Satz 5.6 kann noch weiter verschärft werden. Der gesamte Beweis ist nämlich in \mathbf{PA} ausführbar. Man erhält so folgendes Theorem, dessen Name von Matiyasevich, J. Robinson, Davis und Putnam herrührt, die alle wesentliche Beiträge zur Lösung des 10. Hilbertschen Problems lieferten. Wir werden es seines langwierigen Beweises wegen nicht benutzen, obwohl manches damit vereinfacht werden könnte.

MRDP-Theorem. *Zu jeder Σ_1 -Formel α gibt es schon eine \exists -Formel α' aus \mathcal{L}_{ar} mit $\alpha \equiv_{\mathbf{PA}} \alpha'$. Dabei ist α' o.B.d.A. von der Gestalt $\exists \vec{x} s = t$.*

Bemerkung. Die Fermatsche Vermutung $(*)$ $(\forall x y z \neq 0)(\forall n > 2) x^n + y^n \neq z^n$ ist eine Π_1 -Aussage, weil $(x, y) \mapsto x^y$ nach Satz 4.5 Δ_1 ist. Sie ist also ein Kandidat für eine von \mathbf{PA} unabhängige Aussage. Es wäre interessant zu erfahren, ob ein Beweis dieser Vermutung auch in \mathbf{PA} ausführbar ist. Ein Nachweis, dass dies nicht der Fall ist, wäre kaum weniger sensationell als die Lösung des Problems selbst. Weil \mathbf{PA} schon für Π_1 -Formeln ω -unvollständig ist (Seite 196), könnte es sogar sein, dass $\vdash_{\mathbf{PA}} (\forall x \forall y \forall z \neq 0) x^n + y^n \neq z^n$ für alle $n > 2$, obwohl $(*)$ in \mathbf{PA} nicht beweisbar ist.

Übungen

1. Man zeige, eine ω -unvollständige Theorie in \mathcal{L}_{ar} hat eine konsistente, aber ω -inkonsistente Erweiterung.
2. Sei T vollständig. Man zeige die Gleichwertigkeit von
 (i) T ist streng unentscheidbar, (ii) T ist erblich unentscheidbar.
3. Sei Δ eine endliche Liste expliziter Definitionen neuer Symbole mittels derjenigen von \mathcal{L} . Man zeige, mit T ist auch $T + \Delta$ entscheidbar. Es genügt im Prinzip zu fordern Δ ist r.a., damit $\varphi^{rd} \in \mathcal{L}$ für $\varphi \in T + \Delta$ wohldefiniert ist.
4. Man konstruiere eine p.r. Funktion f mit nichtrekursivem $ran f$.

6.6 Übertragung durch Interpretation

Interpretierbarkeit ist ein mächtiges Werkzeug zur Übertragung modelltheoretischer und rekursionstheoretischer Eigenschaften wie z.B. Unentscheidbarkeit von einer Theorie auf die andere. Wir behandeln hier die wichtigsten Konzepte, die (relative) Interpretierbarkeit nach Tarski und die Modellinterpretierbarkeit nach Rabin. Eine weitere, hier aber nicht näher diskutierte Anwendung der Interpretierbarkeit sind relative Konsistenzbeweise. Alle hier betrachteten Theorien seien konsistent.

Sei P ein 1-stelliges Prädikatsymbol. Die P -Relativierte φ^P der Formel φ entsteht aus φ durch Ersetzung aller Subformeln der Gestalt $\forall x\alpha$ durch $\forall x(Px \rightarrow \alpha)$, d.h. $(\forall x\varphi)^P = \forall x(Px \rightarrow \varphi^P)$. Natürlich kann φ^P auch rekursiv erklärt werden. Für offenes φ ist definitionsgemäß $\varphi^P = \varphi$. Man zeigt leicht $(\exists x\varphi)^P \equiv \exists x(Px \wedge \varphi^P)$.

Beispiel 1. $(\forall x\exists y y=Sx)^P = \forall x[Px \rightarrow \neg\forall y(Py \rightarrow y \neq Sx)]$. Diese Formel ist logisch äquivalent zu $\forall x(Px \rightarrow \exists y(Py \wedge y=Sx))$ und diese wiederum zu $\forall x(Px \rightarrow PSx)$.

Definition. $T_0 \subseteq \mathcal{L}_0$ heie *interpretierbar* in $T \subseteq \mathcal{L}$ (wobei die Signatur von T_0 der Einfachheit halber endlich sei), wenn es eine Liste Δ von in T legitimen expliziten Definitionen der in T nicht vorkommenden Symbole von T_0 und eines neuen Prädikatsymbols P gibt mit $T_0^P \subseteq T^\Delta$. Dabei sei stets $X^P := \{\alpha^P \mid \alpha \in X\}$ und $T^\Delta := T + \Delta$, eine Theorie in \mathcal{L}^Δ , der Δ -Expansion von \mathcal{L} (Signatur $L_0 \cup L \cup \{P\}$).

Diese technisch etwas komplizierte Definition soll nur präzisieren, dass die Begriffe von T_0 in T „verstanden werden“ und T_0 in T „bewahrt“ wird. P soll den Träger der T_0 -Modelle in T abgrenzen. Interpretierbarkeit verallgemeinert den Begriff der Subtheorie: Falls $T_0 \subseteq T$, ist T_0 trivial interpretierbar in T , mit $\Delta = \{Px \leftrightarrow x=x\}$.

CA bezeichne die Menge aller sogenannten *Abschlussaxiome* $\exists xPx$ ($\equiv (\exists x x=x)^P$), Pc ($\equiv (\exists x x=c)^P$) und $\forall \vec{x}(\bigwedge_{i=1}^n Px_i \rightarrow Pf\vec{x})$ ($\equiv (\forall \vec{x}\exists y y=f\vec{x})^P$) für $c, f \in L_0$. Offenbar ist CA eine endliche Teilmenge von T_0^P und damit auch von T^Δ . Auch ist CA bis auf Äquivalenz eine Menge der Gestalt E^P für ein endliches $E \subseteq \text{Taut}_{\mathcal{L}_0}$. Die CA -Axiome garantieren, dass für jedes \mathcal{B} der Signatur $L_0 \cup L \cup \{P\}$ mit $\mathcal{B} \models \Delta$ eine wohldefinierte \mathcal{L}_0 -Struktur \mathcal{A} existiert, mit dem Träger $A = P^{\mathcal{B}}$ und den auf A eingeschränkten, durch Δ definierten Relationen und Operationen. Diese \mathcal{L}_0 -Struktur \mathcal{A} wird mit \mathcal{B}_Δ bezeichnet und ist Substruktur des \mathcal{L}_0 -Redukts von \mathcal{B} .

Lemma 6.1. *Sei $\mathcal{B} \models CA$. Dann gilt $\mathcal{B}_\Delta \models \alpha \Leftrightarrow \mathcal{B} \models \alpha^P$, für alle Aussagen $\alpha \in \mathcal{L}_0^0$.*

Beweis. Sei $\mathcal{A} := \mathcal{B}_\Delta$. Induktiv über $\varphi \in \mathcal{L}_0$ zeigen wir $(\mathcal{A}, w) \models \varphi \Leftrightarrow (\mathcal{B}, w) \models \varphi^P$, für beliebiges $w: \text{Var} \rightarrow A$, wovon das Lemma nur der Spezialfall $\varphi \in \mathcal{L}_0^0$ ist. Die Behauptung ist klar für Primformeln α wegen $\alpha^P = \alpha$. Die Induktionsschritte über \wedge, \neg verlaufen routinemäßig und der Induktionsschritt über \forall ergibt sich wie folgt:

$$\begin{aligned}
(\mathcal{A}, w) \models \forall x \varphi &\Leftrightarrow (\mathcal{A}, w_x^a) \models \varphi \text{ für alle } a \in A \\
&\Leftrightarrow (\mathcal{B}, w_x^a) \models \varphi^P \text{ für alle } a \in A \quad (\text{Induktionsannahme}) \\
&\Leftrightarrow (\mathcal{B}, w_x^a) \models Px \rightarrow \varphi^P \text{ für alle } a \in B \quad (\text{weil } A = P^B) \\
&\Leftrightarrow (\mathcal{B}, w) \models \forall x (Px \rightarrow \varphi^P) = (\forall x \varphi)^P. \quad \square
\end{aligned}$$

Ist T_0 durch X_0 axiomatisiert, genügt es in obiger Definition statt $T_0^P \subseteq T^\Delta$ nur $X_0^P \cup CA \subseteq T^\Delta$ zu fordern. Dies ist sehr wichtig und folgt unmittelbar aus

$$(*) \quad X \vdash \alpha \Rightarrow X^P \cup CA \vdash \alpha^P, \text{ für alle } X, \alpha \subseteq \mathcal{L}_0^0.$$

Zum Nachweis von $(*)$ sei $X \vdash \alpha$ und $\mathcal{B} \models X^P, CA$, also $\mathcal{B}_\Delta \models X$ nach dem Lemma, daher $\mathcal{B}_\Delta \models \alpha$ und somit $\mathcal{B} \models \alpha^P$. Weil \mathcal{B} beliebig war, ist $X^P \cup CA \vdash \alpha^P$.

Satz 6.2. *Ist T_0 in T interpretierbar, so ist mit T_0 auch T streng unentscheidbar.*

Beweis. Sei $T_1 (\subseteq \mathcal{L})$ mit T verträglich. Dann ist mit $T + T_1$ auch die Theorie $(T + T_1)^\Delta$ konsistent. Nun ist $S := \{\alpha \in \mathcal{L}_0^0 \mid \alpha^P \in T_1^\Delta + CA\}$ eine Theorie; denn $S \vdash \alpha$ impliziert $T_1^\Delta + CA \supseteq S^P \cup CA \vdash \alpha^P$ nach $(*)$ und folglich $\alpha^P \in T_1^\Delta + CA$. Mit $\mathcal{B} \models (T + T_1)^\Delta \supseteq T^\Delta, T_1^\Delta, CA$ ist wegen $T_0^P \subseteq T^\Delta$ gewiss auch $\mathcal{B} \models T_0^P, S^P$. Mithin $\mathcal{B}_\Delta \models T_0, S$ nach dem Lemma, d.h. S ist mit T_0 verträglich, also unentscheidbar. Wäre T_1 entscheidbar, dann auch T_1^Δ (Übung 3 in 6.5), daher auch $T_1^\Delta + CA$ (Lemma 5.3) und folglich also auch S . Dies aber ist ein Widerspruch. \square

Beispiel 2. \mathbf{Q} ist in der Theorie T_d der diskret geordneten Ringe interpretierbar, d.h. der geordneten Ringe $\mathcal{R} = (R, 0, +, \times, <)$ mit kleinstem positiven Element e , das kein Einselement von \mathcal{R} sein muss. Man wähle folgende Definitionen für $\mathbf{P}, \mathbf{S}, \cdot$:

$$\begin{aligned}
Px &\leftrightarrow x \geq 0 \wedge x \times e = e \times x \wedge \forall y \exists z \, z \times e = y \times x, \\
y = Sx &\leftrightarrow y = x + e, \quad z = x \cdot y \leftrightarrow z \times e = x \times y \vee \forall u (u \times e \neq x \times y \wedge z = x).
\end{aligned}$$

Aus diesen Formeln ist e wegen $x = e \leftrightarrow 0 < x \wedge \forall y (0 < y \rightarrow x \leq y)$ eliminierbar. $0, +$ bleiben unverändert. Mit etwas geduldigem Rechnen beweist man in T_d^Δ alle auf \mathbf{P} relativierten Axiome von \mathbf{Q} , sowie die Abschlussaxiome.

Damit erweist sich T_d als streng unentscheidbar. \mathbf{Q} ist zwar nicht direkt interpretierbar in der Theorie T_R der Ringe oder der Theorie T_K der Körper, wohl aber in einer gewissen endlichen Erweiterung von T_K (Julia Robinson), womit deren Subtheorien T_K und T_R sich als unentscheidbar erweisen. Dasselbe gilt auch für die Gruppentheorie T_G (Tarski). Keine dieser Theorien ist jedoch streng unentscheidbar. Sie haben sämtlich entscheidbare mathematisch interessante Erweiterungen, etwa die entscheidbare Theorie der abelschen Gruppen (Wanda Szmielew).

\mathbf{Q} und sogar \mathbf{PA} sind auch in \mathbf{ZFC} interpretierbar: Sei $Px \leftrightarrow x \in \omega$ und seien $\mathbf{S}, +, \cdot$ so erklärt, dass ihre Einschränkungen auf ω mit den üblichen Operationen übereinstimmen. Speziell sei $y = Sx \leftrightarrow y = x \cup \{x\}$. Damit ergibt sich sofort die Unentscheid-

barkeit und nebenher auch die Unvollständigkeit von ZFC – die Konsistenz von ZFC natürlich vorausgesetzt. \mathbf{Q} ist auch in bemerkenswert schwachen Subtheorien von ZFC interpretierbar, etwa in der Theorie mit folgenden drei Axiomen in \mathcal{L}_\in , dem *Tarski-Fragment* TF (nach [TMR, S. 34]), das dann auch streng unentscheidbar ist:

$$\begin{aligned} \forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y) & \quad (\text{Extensionalität}), \\ \exists x \forall y y \notin x & \quad (\emptyset \text{ existiert}), \\ \forall x \forall y \exists z \forall u (u \in z \leftrightarrow u \in x \vee u = y) & \quad (x \cup \{y\} \text{ existiert}). \end{aligned}$$

Der anspruchsvolle Interpretationsbeweis wird ausgeführt in [Mo, S. 283–290]. Damit ist auch TF streng unentscheidbar. Mithin ist die Menge der Tautologien in einer binären Relation unentscheidbar, sogar ohne $=$ in der Sprache, denn $=$ ist in TF mittels der expliziten Definition $x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y)$ offenbar eliminierbar.

Bemerkung 1. Hochinteressant ist auch die gegenseitige Interpretierbarkeit von PA und ZFC_{fin} . Dies ist die Theorie der (erblich) endlichen Mengen; sie entsteht aus ZFC durch Ersetzung von AI durch das Axiom ‘alle Mengen sind endlich’ sowie Ersetzung des Fundierungsaxioms AF durch das Fundierungsschema $\exists x \varphi \rightarrow \exists x (\varphi \wedge (\forall y \in x) \neg \varphi \frac{y}{x})$ oder das gleichwertige \in -Induktionsschema $\text{IS}_\in : \forall a ((\forall x \in a) \varphi \rightarrow \varphi \frac{a}{x}) \rightarrow \forall x \varphi$ ($\varphi \in \mathcal{L}_\in$; ohne AI ist AF zu schwach um die Existenz transitiver Hüllen zu sichern, [De2]). Die einfachste Interpretation von ZFC_{fin} in PA ist die Ackermannsche, welche *alle* natürlichen Zahlen als endliche Mengen ansieht. Sei bz_n^m die n -te Binärziffer von m (siehe Übung 5 in 6.1) und \in in PA definiert durch $n \in m \leftrightarrow \text{bz}_n^m = 1$. Dann gelten alle ZFC_{fin} -Axiome, Übung 4. Nach Satz 7.1.1 ist $(n, m) \mapsto \text{bz}_n^m$ und damit auch \in in PA explizit definierbar.

\mathbf{Q} ist trivial interpretierbar in $\text{Th}\mathcal{N}$, und $\text{Th}\mathcal{N}$ nach dem Satz von Lagrange wiederum in $\text{Th}\mathcal{Z}$ mit $\mathcal{Z} = (\mathbb{Z}, 0, 1, +, \cdot)$. Also ist $\text{Th}\mathcal{Z}$ streng, und damit jede Subtheorie schlechthin unentscheidbar, z.B. die Theorie der kommutativen Ringe. Umgekehrt ist $\text{Th}\mathcal{Z}$ auch in $\text{Th}\mathcal{N}$ interpretierbar, z.B. indem nichtnegative ganze Zahlen durch gerade, negative durch ungerade natürliche Zahlen vertreten werden.

Wir erläutern jetzt eine strengere Form der Interpretierbarkeit, lassen der Einfachheit halber aber gewisse Feinheiten weg. Seien \mathbf{K}_0 und \mathbf{K} Klassen von \mathcal{L}_0 - bzw. \mathcal{L} -Strukturen und $\text{Th}\mathbf{K} = \{\alpha \in \mathcal{L}^0 \mid \mathbf{K} \models \alpha\}$. Sei Δ eine Liste der Definitionen der \mathcal{L}_0 -Symbole und eines Prädikatsymbols \mathbf{P} , sowie \mathcal{L}^Δ , \mathcal{C}_Δ und \mathcal{B}_Δ für $\mathcal{B} \models \mathcal{C}_\Delta$ definiert wie vorhin. \mathcal{A}^Δ bezeichne die Δ -Expansion von $\mathcal{A} \in \mathbf{K}$.

Definition. \mathbf{K}_0 heie *modellinterpretierbar* in \mathbf{K} (oder auch $\text{Th}\mathbf{K}_0$ in $\text{Th}\mathbf{K}$), wenn für eine passende Definitionsliste Δ und eine passende Aussage $\gamma \in \mathcal{L}^\Delta$

- (1) $\mathbf{K}_\gamma \models \mathcal{C}_\Delta$ und $\mathcal{B}_\Delta \in \mathbf{K}_0$ für alle $\mathcal{B} \in \mathbf{K}_\gamma$,
- (2) Für jedes $\mathcal{A} \in \mathbf{K}_0$ gibt es ein $\mathcal{B} \in \mathbf{K}_\gamma$ mit $\mathcal{A} \simeq \mathcal{B}_\Delta$.

Dabei sei $\mathbf{K}_\gamma := \{\mathcal{A}^\Delta \mid \mathcal{A} \in \mathbf{K}, \mathcal{A}^\Delta \models \gamma\}$. Zu jeder Aussage $\beta \in \mathcal{L}^\Delta$ lässt sich wie in 2.6 eine Reduzierte $\beta^{\text{rd}} \in \mathcal{L}$ effektiv konstruieren mit

(3) $\mathcal{A}^\Delta \models \beta \Leftrightarrow \mathcal{A} \models \beta^{rd}$, für alle $\mathcal{A} \in \mathbf{K}$.

Satz 6.3. *Sei \mathbf{K}_0 modellinterpretierbar in \mathbf{K} . Dann ist mit der Theorie $Th \mathbf{K}_0$ auch die Theorie $Th \mathbf{K}$ unentscheidbar.*

Beweis. Es genügt zu zeigen (*) $\mathbf{K}_0 \models \alpha \Leftrightarrow \mathbf{K} \models \gamma^{rd} \rightarrow \alpha^{P^{rd}}$. Denn ein Entscheidungsverfahren für $Th \mathbf{K}$ hätte wegen (*) ein solches für $Th \mathbf{K}_0$ zur Folge. \Rightarrow : Sei $\mathbf{K}_0 \models \alpha$, $\mathcal{A} \in \mathbf{K}$ und $\mathcal{A} \models \gamma^{rd}$, also $\mathcal{A}^\Delta \models \gamma$ nach (3), d.h. $\mathcal{B} := \mathcal{A}^\Delta \in \mathbf{K}_\gamma$. Nach (1) ist $\mathcal{B}_\Delta \in \mathbf{K}_0$, also $\mathcal{B}_\Delta \models \alpha$, d.h. $\mathcal{B} \models \alpha^P$ nach Lemma 6.1, daher $\mathcal{A} \models \alpha^{P^{rd}}$. Das zeigt $\mathbf{K} \models \gamma^{rd} \rightarrow \alpha^{P^{rd}}$. \Leftarrow folgt indirekt: Sei $\mathbf{K}_0 \not\models \alpha$, etwa $\mathcal{A} \in \mathbf{K}_0$, $\mathcal{A} \not\models \alpha$. Sei $\mathcal{B} \in \mathbf{K}_\gamma$ gemäß (2) gewählt, also $\mathcal{B} \models \gamma$ und $\mathcal{B}_\Delta \simeq \mathcal{A} \not\models \alpha$. Daher $\mathcal{B} \not\models \alpha^P$ (Lemma 6.1). Somit $\mathcal{B} \not\models \gamma \rightarrow \alpha^P$, d.h. $\mathcal{B}' \not\models \gamma^{rd} \rightarrow \alpha^{P^{rd}}$ für das \mathcal{L} -Redukt $\mathcal{B}' \in \mathbf{K}$ von \mathcal{B} . \square

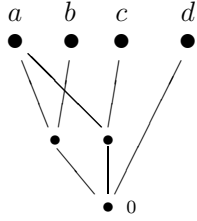
Beispiel 3. Sei \mathbf{K}_0 die Klasse aller Graphen (A, R) und \mathbf{K} die Klasse aller einfachen Graphen (B, S) , d.h. S ist irreflexiv und symmetrisch. Wir zeigen, \mathbf{K}_0 ist in \mathbf{K} modellinterpretierbar, d.h. beliebige Graphen können durch einfache vollständig kodiert werden. Die Figur zeigt links ein $\mathcal{A} \in \mathbf{K}_0$ mit aRa , aRb , bRa und bRc ,



und rechts den \mathcal{A} gemäß (2) entsprechenden einfachen Graphen \mathcal{B} mit $\mathcal{A} \simeq \mathcal{B}_\Delta$, die „Kodierungs-Struktur“ von \mathcal{A} . Grob gesagt, wurden zu \mathcal{A} neue Punkte so hinzugefügt, dass \mathcal{A} durch \mathcal{B} vollständig beschrieben wird. Dick gezeichnete Punkte in \mathcal{B} vertreten die Punkte aus \mathcal{A} . Es sind dies genau die Punkte aus P^B , kurz, die „alten“ Punkte. Alle übrigen Punkte aus B heißen „neue“ Punkte. Die Definition von P lautet informell ‘ $Px \Leftrightarrow x$ ist zu zwei oder drei Endpunkten benachbart’ (in Endpunkten endet nur eine Kante). Die zu zwei Endpunkten benachbarten alten Punkte kennzeichnen die irreflexen, die zu drei Endpunkten benachbarten die reflexiven Punkte von \mathcal{A} . Führt in \mathcal{A} eine Kante von x nach y so wird in \mathcal{B} ein neuer Punkt zwischen x und y gesetzt, wobei für Richtungsanzeige ein weiterer Punkt benutzt wird, falls nötig. Informell lautet die Definition für R dann ‘ $xRy \Leftrightarrow x, y \in P^B$ und entweder $x=y$ und x ist zu drei Endpunkten benachbart, oder es gibt genau einen neuen Punkt z mit $xSzSy$, oder es gibt genau zwei neue Punkte u, v mit $xSuSvSy$ und uSy ’. Und γ lautet ‘ $P^B \neq \emptyset$ und jeder neue Punkt ist entweder Endpunkt oder zu einem oder zwei alten Punkten benachbart’. Es liegt auf der Hand, dass mit diesen Definitionen von P , R und γ die Bedingungen (1) und (2) erfüllt sind.

Im Beispiel ist $Th \mathbf{K}_0$ die logische Theorie einer binären Relation, die wie schon festgestellt unentscheidbar ist. Demnach ist auch die Theorie aller einfachen Graphen unentscheidbar. Dies kann man nun wieder nutzen, um die Theorie SL der

Halbverbände als unentscheidbar nachzuweisen. Daraus folgt nach Satz 5.4 dasselbe für die Theorie **SG** der Halbgruppen, denn **SL** ist endliche Erweiterung von **SG**. Analog zum letzten Beispiel genügt es, für einen einfachen Graphen (A, S) den



Kodierungshalbverband (B, \circ) anzugeben. Die Figur links zeigt das Ordnungsdiagramm von B für $A = \{a, b, c, d\}$ und $S = \{\{a, b\}, \{a, c\}\}$, S verstanden als Kantenmenge, siehe 1.5. Die alten Punkte sind gerade die maximalen Punkte von B . Nach Konstruktion hat B ein kleinstes Element 0 und ist von der Länge 3, d.h. es gibt bzgl. $<$ höchstens drei aufeinanderfolgende Punkte in B . Das muss die geforderte Aussage γ jetzt zum Ausdruck bringen. Diese Interpretationsmethode ist sehr flexibel. Sie macht z.B. hinreichend deutlich, dass die Theorie der Halbverbände nicht weniger kompliziert ist als die aller gerichteten Graphen schlechthin.

Bemerkung 2. Dieselbe Konstruktion zeigt, dass auch die Theorie der *endlichen* einfachen Graphen in der Theorie der endlichen Halbverbände modellinterpretierbar ist. Weil erstere unentscheidbar ist – siehe z.B. [RZ] – gilt dies auch für die Theorie **FSG** der endlichen Halbgruppen. Setzt man über die maximalen Elemente der Figur noch ein Einselement, entstehen jeweils endliche Verbände. Also ist auch deren Theorie unentscheidbar. Das gilt auch für die Theorie der Klasse **FPO** aller endlichen partiellen Ordnungen, denn man braucht zur Beschreibung von (A, S) nur die partielle Ordnung von B .

Auch positive Resultate sind übertragbar. Viele Theorien sind z.B. in der Theorie der Bäume interpretierbar (siehe [KR]), insbesondere in der monadischen Theorie 2. Stufe der Bäume. Deren Entscheidbarkeit ist besonders weittragend. Für Einzelheiten und Literaturhinweise sei auf [Ba, C.2] oder [BGG] verwiesen.

Übungen

1. Eine konsistente Theorie $T_0 \subseteq \mathcal{L}_0$ heißt wesentlich unentscheidbar, wenn jedes konsistente $T \supseteq T_0$ unentscheidbar ist. Man zeige, $T_1 \subseteq \mathcal{L}_1$ ist wesentlich unentscheidbar, falls T_0 dies ist und T_0 in T_1 interpretierbar ist.
2. Man zeige, eine endlich axiomatisierbare Theorie T ist wesentlich unentscheidbar genau dann, wenn sie streng unentscheidbar ist.
3. Man zeige (informell), **PA** ist interpretierbar in **ZF**.
4. Man beweise für die \in -Relation in **PA** (Bemerkung 1) die Axiome von **TF**, das Schema **Fin** : $\varphi \frac{\emptyset}{x} \wedge \forall xy(\varphi \rightarrow \varphi \frac{x \cup \{y\}}{x}) \rightarrow \forall x \varphi$ und das Schema der \in -Induktion. Es lässt sich mühelos zeigen, dass aus **TF** + **Fin** + **IS** _{\in} sämtliche Axiome von **ZFC**_{fin} herleitbar sind, also ist **ZFC**_{fin} in **PA** interpretierbar.

Weiter unten geben wir ein Beispiel eines Π_2 -Prädikats. Σ_n -definierbare Funktionen sind immer auch Δ_n , wie eine leichte Verallgemeinerung von Lemma 3.4 zeigt. Man vereinbart als bloße Redeweise, dass Σ_n - bzw. Π_n -*Aussagen* 0-stellige Σ_n - bzw. Π_n -Prädikate definieren. In diesem Sinne ist z.B. die Konsistenz von PA ein Π_1 -Prädikat.

Jede Formel ist zu einer Σ_n - oder einer Π_n -Formel für passendes n äquivalent; man braucht sie ja nur in pränexer Normalform zu bringen und die Quantoren zu Blöcken mit gleichen Quantoren zusammenzufassen. Bei neueren Untersuchungen betrachtet man z.B. oft auch Δ_0 - oder Σ_n - oder Π_n -*Induktion*, d.h. man schränkt das Induktionsschema IS auf die jeweiligen Formelklassen ein. Ein wichtiges Beispiel ist IA_0 .

Wie in 6.4 schon gezeigt wurde, sind die Σ_1 -Prädikate die rekursiv aufzählbaren, die Π_1 -Prädikate sind deren Komplemente, und die Δ_1 -Prädikate sind genau die rekursiven. Damit haben wir eine rein rekursionstheoretische Veranschaulichung von Σ_1 , Π_1 und Δ_1 vor uns. Das unterstreicht die Bedeutung der arithmetischen Hierarchie, die im übrigen ziemlich stabil ist gegenüber leichten Veränderungen der Definition von Δ_0 . Wegen Satz 5.6 könnte man z.B. mit einem Δ_0 starten, das aus allen in \mathcal{N} polynomial (oder gleichwertig, quantorenfrei) definierbaren Relationen besteht. In einigen Darstellungen wird ein System von Formeln effektiv aufgezählt (und mit Δ_0 bezeichnet), durch welche bereits alle p.r. Prädikate in \mathcal{N} definiert werden. 7.1 wird zeigen, wie sich ein solches System von Formeln gewinnen lässt. Zwischen diesen und den Δ_0 -Formeln liegen noch viele r.a. Formelklassen, deren zugehörige Prädikate rekursiv sind und die für Theorie und Praxis der Berechenbarkeit bedeutsam sind, z.B. die in der Kapitel-Einleitung erwähnte Klasse der elementaren Funktionen.

Allerdings lässt sich nach Bemerkung 2 in 6.4 kein Formelsystem in \mathcal{L}_{ar} effektiv aufzählen, durch das bereits alle rekursiven, d.h. alle Δ_1 -Prädikate definiert werden, so dass die Definition der arithmetischen Hierarchie nicht in übersehbarer Weise mit einer repräsentativen „Menge von Δ_1 -Formeln“ beginnen kann.

Ähnlich wie für den Fall $n = 1$ zeigt man, dass eine Konjunktion oder Disjunktion von Σ_n -Formeln wieder zu einer solchen äquivalent ist, und Analoges gilt für Π_n -Formeln. Auch ist die Negation einer Σ_n -Formel zu einer Π_n -Formel äquivalent und umgekehrt. Denn dies ist richtig für $n = 1$, womit der Induktionsanfang einer leicht ausführbaren Induktion über n bereits klar ist. Das Komplement eines Σ_n -Prädikats ist daher ein Π_n -Prädikat und umgekehrt. Daraus folgt leicht, dass Δ_n unter allen erwähnten Operationen abgeschlossen ist.

Durch Quantorenkompression (Übung 1 in 6.3) erhält man noch eine etwas einfachere Darstellung der Quantorenblöcke. Es lassen sich die abwechselnd aufeinanderfolgenden \exists - und \forall -Blöcke zu jeweils einem Quantor zusammenziehen:

Satz 7.1. *Jedes Σ_n -Prädikat ist durch eine Formel der Gestalt $\exists x_1 \forall x_2 \cdots Q_n x_n \alpha$ mit einer Δ_0 -Formel α definiert; dabei ist Q_n der \forall - bzw. der \exists -Quantor, je nachdem ob n gerade oder ungerade ist. Entsprechend ist ein Π_n -Prädikat durch eine Formel der Gestalt $\forall x_1 \exists x_2 \cdots Q_n x_n \alpha$ definiert.*

Beweis. Für Σ_1 -Prädikate und Π_1 -Prädikate zeigt dies Übung 1 in 6.3. Für den allgemeinen Fall beachte man $Q\vec{x}\varphi \equiv_{\mathcal{N}} Qy(Qx_1 < y) \cdots (Qx_n < y)\varphi$. Dabei ist Q der \forall - oder \exists -Quantor. Es genügt daher zu zeigen, dass die Klassen Σ_n und Π_n unter beschränkter Quantifizierung abgeschlossen sind. Dies behauptet Übung 1. \square

Häufig wird auch die Paarkodierung verwendet um Quantoren zu komprimieren. Es ist nicht immer einfach, die genaue Position eines vorgegebenen Prädikats in der arithmetischen Hierarchie zu bestimmen. Besser gesagt, dies erfordert wie jedes anspruchsvolle Spiel hinreichendes Training. Es ist z.B. nicht schwer zu sehen, dass die ω -Konsistenz der Form nach Π_3 ist. Aber erst Satz 7.5.2 wird zeigen, sie ist *echt* Π_3 , d.h. nicht Σ_n , Π_n oder Δ_n für $n < 3$. Der Übersichtlichkeit halber benutzen wir im folgenden einfacheren Beispiel an einer Stelle die Churchsche These, die jedoch mit etwas Rekursionstheorie in erprobter Weise wieder eliminiert werden kann.

Beispiel. Sei \mathcal{L}_r die Menge der $\alpha \in \mathcal{L}_{ar}^1$, welche in \mathbb{Q} die rekursiven Teilmengen von \mathbb{N} repräsentieren. Dazu gehören z.B. alle Δ_0 -Formeln aus \mathcal{L}_{ar}^1 . Weil \mathbb{N} und \emptyset rekursiv sind, gehören zu \mathcal{L}_r auch alle Aussagen α aus $\mathbb{Q}^* := \mathbb{Q} \cup \{\alpha \mid \neg\alpha \in \mathbb{Q}\}$. Denn die $\alpha \in \mathbb{Q}$ repräsentieren trivialerweise \mathbb{N} und die α mit $\neg\alpha \in \mathbb{Q}$ gerade \emptyset . Offenbar ist $\mathbb{Q}^* = \mathcal{L}_r \cap \mathcal{L}_{ar}^0$. Wir zeigen nun, \mathcal{L}_r ist arithmetisch; genauer, eine echte Π_2 -Menge, also weder Σ_1 noch Π_1 . Gemäß Definition ist

$$\alpha \in \mathcal{L}_r \Leftrightarrow \alpha \in \mathcal{L}_{ar}^1 \ \& \ \forall n \exists \Phi [\Phi \text{ ist Beweis für } \alpha(\underline{n}) \text{ oder für } \neg\alpha(\underline{n})].$$

Daraus gewinnt man unschwer eine Definition von $\dot{\mathcal{L}}_r$ durch eine Π_2 -Formel $\varphi(x)$. In der Tat, sei das p.r. Prädikat ' $a \in \dot{\mathcal{L}}_{ar}^1$ ' etwa durch die Σ_1 -Formel $\lambda_1(x)$ definiert. Mit $sb = sb_{v_0}$ setze man dann

$$\varphi(x) := \lambda_1(x) \wedge \forall y \exists u [\text{bew}_{\mathbb{Q}}(u, sb(x, y)) \vee \text{bew}_{\mathbb{Q}}(u, \neg sb(u, y))],$$

genauer, die Reduzierte dieser Formel in \mathcal{L}_{ar} nach Elimination der vorkommenden p.r. Funktionsterme mit weiteren \exists -Quantoren innerhalb der eckigen Klammern. Also beschreibt φ eine Π_2 -Formel, d.h. \mathcal{L}_r ist eine Π_2 -Menge. Sie ist nicht Σ_1 , weil \mathcal{L}_r nach Bemerkung 2 in 6.4 nicht r.a. ist. Sie ist aber auch nicht Π_1 . Angenommen dies sei der Fall. Dann ist $\mathbb{Q}^* = \mathcal{L}_r \cap \mathcal{L}_{ar}^0$ ebenfalls Π_1 , denn \mathcal{L}_r ist Δ_1 . Nun ist \mathbb{Q}^* sicher r.a. und damit Σ_1 , also ist \mathbb{Q}^* nach Satz 4.5 rekursiv. Wir erhalten daraus aber ein Entscheidungsverfahren für \mathbb{Q} , also einen Widerspruch: Sei $\alpha \in \mathcal{L}_{ar}^0$ gegeben. Ist $\alpha \notin \mathbb{Q}^*$, so auch $\alpha \notin \mathbb{Q}$; ist $\alpha \in \mathbb{Q}^*$, setzen wir die Aufzählungsmaschine für \mathbb{Q} in Aktion und warten, bis α oder $\neg\alpha$ erscheint.

In Vorbereitung auf 7.1 zeigen wir abschließend, dass die Σ_1 -Formeln in PA durch spezielle Formeln vertreten werden können. In Satz 7.2 unten könnte PA allerdings durch eine wesentlich schwächere Theorie, z.B. **N** ersetzt werden.

Definition. *Spezielle* Σ_1 -Formeln seien wie folgt erklärt:

- (i) $Sx=y$, $x+y=z$ und $x \cdot y=z$ sind spezielle Σ_1 -Formeln, wobei x, y, z paarweise verschiedene Variablen bezeichnen,
- (ii) Mit α, β sind auch $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \frac{0}{x}$ und $\alpha \frac{y}{x}$ ($y \notin \text{gbd } \alpha$, Primterm-Substitution) spezielle Σ_1 -Formeln, sowie $\exists x\alpha$ und $(\forall x < y)\alpha$ für $y \notin \text{var } \alpha$.

Satz 7.2. (a) Jede originale Σ_1 -Formel ist in PA zu einer speziellen Σ_1 -Formel äquivalent. (b) Jede spezielle Σ_1 -Formel ist modulo PA eine Σ_1 -Formel.

Beweis. (a): Es genügt offenbar, dies für alle Δ_0 -Formeln zu beweisen, denn auch die Menge aller speziellen Σ_1 -Formeln ist unter \exists -Quantifikation abgeschlossen. Weil $s=t \equiv \exists x(x=s \wedge x=t)$ mit $x \notin \text{var } s, t$ genügt es, Primformeln der Gestalt $x=t$ zu betrachten. Wir beweisen (a) für Formeln $x=t$ durch Termination. Ist t ein Primterm, ergibt sich die Behauptung offensichtlich aus $x=0 \equiv (x=y) \frac{0}{y}$, sowie $x=y \equiv_{\text{PA}} (x+z=y) \frac{0}{z}$. Induktion über $\mathbb{S}, +, \cdot$ folgt aus $x=St \equiv \exists y(x=Sy \wedge y=t)$, $x=s+t \equiv \exists yz(x=y+z \wedge y=s \wedge z=t)$, und ganz analog verläuft der Beweis für \cdot . $x \neq y \equiv_{\text{PA}} \exists uz(Su=z \wedge (x+z=y \vee y+z=x))$ und $s \neq t \equiv \exists yz(x \neq y \wedge x=s \wedge y=t)$ zeigen, dass (a) für alle Literale gilt. Nach Übung 4 in 6.3 genügt es daher, die Induktionsschritte über $\wedge, \vee, (\forall x \leq t)$ und $(\exists x \leq t)$ auszuführen. Für \wedge, \vee ist dies klar. Im übrigen beachte man $(\forall x \leq t)\alpha \equiv_{\text{PA}} \exists y(y=t \wedge (\forall x < y)\alpha \wedge \alpha \frac{y}{x})$ mit $y \notin \text{var } \alpha$, sowie $(\exists x \leq t)\alpha \equiv_{\text{PA}} \exists xyz(x+y=z \wedge z=t \wedge \alpha)$ mit $y, z \notin \text{var } \alpha, t$. (b) erfordert lediglich den Nachweis, dass für eine Σ_1 -Formel $\exists z\varphi$ auch die Formel $(\forall x < y)\exists z\varphi$ zu einer Σ_1 -Formel in PA äquivalent ist. Dieser Nachweis ist leicht, denn das Schrankenschema (Übung 3(c) Seite 86) zeigt $(\forall y < x)\exists z\varphi \equiv_{\text{PA}} \exists u(\forall y < x)(\exists z < u)\varphi$. \square

Übungen

1. Man zeige (induktiv über n) Σ_n, Π_n und damit auch Δ_n sind abgeschlossen unter beschränkter Quantifizierung. Ferner zeige man, Δ_n ist auch abgeschlossen unter primitiver Rekursion.
2. Man bestätige $\Delta_0 \subset \Delta_1 \subset \Sigma_1, \Pi_1$, womit gezeigt ist, dass diese vier Klassen arithmetischer Prädikate paarweise verschieden sind.
3. Eine Inspektion zeigt, dass alle Axiome von **N** schon in $I\Delta_0$ beweisbar sind (Seite 186; sogar offene Formeln im Induktionsschema in 0, $\mathbb{S}, +, \cdot, \leq$ würden genügen, siehe etwa [HA]). Man beweise in $I\Delta_0$ die Schemata der $<$ -Induktion und der Minimalzahl für Δ_0 -Formeln. Siehe hierzu die Übungen in 3.3.

Kapitel 7

Zur Theorie der Selbstreferenz

Mit Selbstreferenz ist grob gesagt die Möglichkeit gemeint, in einer Theorie T über T selbst oder verwandte Theorien zu reden. Vorliegendes Kapitel kann nur einen Einblick in eine im letzten Viertel des 20. Jahrhunderts weit entwickelte Theorie geben. Wir beweisen den zweiten Unvollständigkeitssatz von Gödel, das Löbsche Theorem und andere mit der Selbstreferenz zusammenhängende Ergebnisse. Einige weiterführende Resultate werden anhand von geeigneten Anwendungen nur erläutert. Diese Thematik ist insgesamt von hohem erkenntnistheoretischen Wert.

Der Nachweis der sogenannten Ableitungsbedingungen für PA und andere Theorien in **7.1** ist der Berg, der zunächst erstiegen werden muss. Wer sich jedoch mit einem Überfliegen von **7.1** zufriedengibt, kann gleich in **7.2** beginnen; von dort ab sind nur Früchte zu ernten. Allerdings entgeht einem dabei ein wirkliches Abenteuer, die Verschmelzung von Logik und Zahlentheorie bei der Analyse von PA .

Schon Gödel hat versucht, den Begriff ‘beweisbar’ durch einen modalen Operator im Rahmen des Modalsystems S4 zu interpretieren. Dieser Ansatz widerspiegelt seine eigenen Resultate aber nicht adäquat. Erst nachdem die Modallogik nach 1970 einen hinreichend hohen Entwicklungsstand erreicht hatte, konnte ein entsprechendes Programm erfolgreich ausgeführt werden. Als geeignetes Instrument hat sich dafür eine mit G (oder GL) bezeichnete Modallogik erwiesen. Deren in **7.3** vorgestellte Kripke-Semantik ist ein handliches Werkzeug zur Untersuchung der Selbstreferenz.

Ein Hauptresultat der modallogischen Behandlung der Selbstreferenz ist der Solovaysche Vollständigkeitssatz in **7.4**. Glücklicherweise gehört dieser Satz ebenso wie die Vollständigkeit der Kripke-Semantik für G zu jener Art von Hilfsmitteln, die man bequem anwenden kann, ohne ihre Beweise im Detail zu kennen. Es gibt einige Erweiterungen von G , die für die Analyse anderer Begriffe oder ihren Vergleich nützlich sind, z.B. die in **7.5** behandelte bimodale Expansion von G oder die Interpretierbarkeitslogik, siehe [Vi]. Einen umfassenden Überblick gibt [Bu, Chapter VII].

7.1 Die Ableitungsbedingungen

Der zweite Unvollständigkeitssatz 2.2 besagt etwas vereinfacht, dass für eine hinreichend strenge konsistente axiomatisierbare Theorie $T \subseteq \mathcal{L}$ nicht $\vdash_T \text{Con}_T$ gelten kann, wobei Con_T eine Aussage ist, welche die Konsistenz von T in \mathcal{L} zum Ausdruck bringt. In populärer Formulierung: *Ist T konsistent, so ist dies im Rahmen von T nicht beweisbar.* Darüber hinaus ist die kursiv gesetzte Aussage unter gewissen Bedingungen in T schon formulierbar und dort auch beweisbar.

Diese Bedingungen sind die sogenannten *Ableitungsbedingungen* D1–D3 unten, die durchaus eigenes Interesse verdienen. Ihre Formulierung setzt die Gödelisierbarkeit von T voraus, was die Auszeichnung einer Termfolge $\underline{0}, \underline{1}, \dots$ einschließt, Seite 194. Es sei $\text{bew}_T(y, x)$ wie in 6.4 eine Σ_1 -Formel, die das p.r. Prädikat bew_T in T repräsentiere. $\text{bwb}_T(x)$ ($= \exists y \text{bew}_T(y, x)$) werde durch $\Box(x)$ abgekürzt, und $\text{bwb}_T \frac{[\alpha]}{x}$ durch $\Box\alpha$, gelesen als ‘box α ’ oder ‘beweisbar α ’, weil es sich um die Formalisierung des Sachverhalts ‘ $\vdash_T \alpha$ ’ in T handelt. $\Box\alpha$ ist stets eine Aussage, auch wenn $\text{frei } \alpha \neq \emptyset$. Bezieht \Box sich auf eine Theorie $T' \neq T$, ist \Box entsprechend zu indizieren. In 7.3 wird \Box zudem als modallogischer Operator in Erscheinung treten.

Wir erklären ferner $\Diamond\alpha := \neg\Box\neg\alpha$ für $\alpha \in \mathcal{L}^0$. Diese Aussage darf man lesen als α ist verträglich mit T , denn sie ist die Formalisierung von ‘ $\not\vdash_T \neg\alpha$ ’, oder gleichwertig ‘ $T + \alpha$ ist konsistent’. Schließlich wird Con_T in natürlicher Weise durch

$$\text{Con}_T := \neg\Box\perp \quad (= \neg\text{bwb}_T(\ulcorner \perp \urcorner))$$

definiert. Dabei sei \perp eine beliebige Kontradiktion, etwa $\underline{0} \neq \underline{0}$. Es wird sich gleich herausstellen, dass Con_T modulo T unabhängig ist von der Wahl von \perp . Die erwähnten Ableitungsbedingungen lauten wie folgt:

$$D1: \vdash_T \alpha \Rightarrow \vdash_T \Box\alpha, \quad D2: \vdash_T \Box\alpha \wedge \Box(\alpha \rightarrow \beta) \rightarrow \Box\beta, \quad D3: \vdash_T \Box\alpha \rightarrow \Box\Box\alpha.$$

Dabei durchlaufen α, β alle Aussagen aus \mathcal{L}^0 . Oft formuliert man D2 auch in der gleichwertigen Form $\Box(\alpha \rightarrow \beta) \vdash_T \Box\alpha \rightarrow \Box\beta$ oder D3 in der Form $\Box\alpha \vdash_T \Box\Box\alpha$. Die Ableitungsbedingungen stammen in der angegebenen Gestalt von Löb, wurden in etwas anderer Gestalt aber schon in [HB] formuliert.

Eine unmittelbare Konsequenz aus D1, D2 ist D0: $\alpha \vdash_T \beta \Rightarrow \Box\alpha \vdash_T \Box\beta$. Denn $\alpha \vdash_T \beta \Rightarrow \vdash_T \alpha \rightarrow \beta \Rightarrow \vdash_T \Box(\alpha \rightarrow \beta) \Rightarrow \vdash_T \Box\alpha \rightarrow \Box\beta \Rightarrow \Box\alpha \vdash_T \Box\beta$. Folglich kann „unter \Box “ äquivalent ersetzt werden. Die Wahl von \perp in Con_T ist also frei.

Bemerkung 1. Jeder nur d1: $\vdash_T \alpha \Rightarrow \vdash_T \partial\alpha$ und d2: $\partial(\alpha \rightarrow \beta) \vdash_T \partial\alpha \rightarrow \partial\beta$ erfüllende Operator $\partial: \mathcal{L} \rightarrow \mathcal{L}$ erfüllt demnach immer auch d0: $\alpha \vdash_T \beta \Rightarrow \partial\alpha \vdash_T \partial\beta$. Er erfüllt zudem $d\wedge$: $\partial(\alpha \wedge \beta) \equiv_T \partial\alpha \wedge \partial\beta$. Denn $\alpha \wedge \beta \vdash_T \alpha, \beta$, also $\partial(\alpha \wedge \beta) \vdash_T \partial\alpha, \partial\beta \vdash_T \partial\alpha \wedge \partial\beta$ nach d0. Ähnlich folgt $\partial\alpha \wedge \partial\beta \vdash_T \partial(\alpha \wedge \beta)$ mit d0, d2 leicht aus $\alpha \vdash_T \beta \rightarrow \alpha \wedge \beta$. Aus d0 schließt man unmittelbar auf $d00$: $\alpha \equiv_T \beta \Rightarrow \partial\alpha \equiv_T \partial\beta$.

Während $D2$ und $D3$ Aussagen(schemata) in T darstellen, ist $D1$ metatheoretischer Natur. $D1$ folgt unmittelbar aus der Repräsentierbarkeit von bew_T und gilt daher schon für relativ schwache Theorien wie z.B. $T = \mathbf{Q}$. Die Umkehrung von $D1$,

$$D1^*: \vdash_T \Box \alpha \Rightarrow \vdash_T \alpha, \text{ für alle } \alpha \in \mathcal{L}^0$$

muss nicht richtig sein, gilt aber für alle ω -konsistenten axiomatischen Erweiterungen $T \supseteq \mathbf{Q}$ wie z.B. $T = \mathbf{PA}$. Denn aus $\not\vdash_T \alpha$ folgt $\vdash_T \neg \text{bew}_T(\underline{n}, \ulcorner \alpha \urcorner)$ für alle n nach Korollar 6.4.3, also $\not\vdash_T \exists y \text{bew}_T(y, \ulcorner \alpha \urcorner) = \Box \alpha$ wegen der ω -Konsistenz von T .

Anders als $D1$ sind $D2$ und $D3$ nicht so billig zu haben. T muss direkt oder indirekt (via Gödelisierung) über das Beweisen in T reden können. $D3$ ist nichts anderes als die in T formalisierte Bedingung $D1$, während $D2$ den Abschluss von T unter MP reflektiert, siehe (7) aus 6.3. Wir zeigen zuerst, dass $D2$ aus

$$D2^*: \text{bew}_T(u, x) \wedge \text{bew}_T(v, x \dot{\sim} y) \vdash_T \text{bew}_T(u * v * \langle y \rangle, y)$$

folgt, sofern die hier auftretenden p.r. Funktionen $\dot{\sim}$, $*$, und $y \mapsto \langle y \rangle$ Symbole von T oder in T definierbar sind. Allgemein heie eine Funktion $f \in \mathbf{F}_n$ in der arithmetisierbaren Theorie T definierbar, falls es ein $\delta = \delta(\vec{x}, y) \in \mathcal{L}$ gibt mit

$$(1) \quad (a) \vdash_T \delta(\underline{\vec{a}}, \underline{f\vec{a}}) \text{ für alle } \vec{a} \in \mathbb{N}^n, \quad (b) \vdash_T \forall \vec{x} \exists! y \delta(\vec{x}, y).$$

f wird durch $\delta(\vec{x}, y)$ in T zugleich repräsentiert. Auch ist $y = f\vec{x} \leftrightarrow \delta(\vec{x}, y)$ dann eine legitime explizite Definition eines wiederum mit f bezeichneten Symbols in T . Nach Einführung von f in T folgt $\vdash_T f\vec{a} = \underline{f\vec{a}}$ für alle $\vec{a} \in \mathbb{N}^n$, z.B. $\vdash_T \underline{a} \dot{\sim} \underline{b} = \underline{a} \dot{\sim} \underline{b}$. Dabei unterscheiden wir von nun an nicht mehr zwischen T und definitorischen Erweiterungen. Wegen $\ulcorner \alpha \rightarrow \beta \urcorner = \underline{\dot{\alpha}} \dot{\sim} \underline{\dot{\beta}} = \underline{\dot{\alpha}} \dot{\sim} \underline{\dot{\beta}} = \ulcorner \alpha \urcorner \dot{\sim} \ulcorner \beta \urcorner$ liefert $D2^*$ dann $\text{bew}_T(u, \ulcorner \alpha \urcorner) \wedge \text{bew}_T(v, \ulcorner \alpha \rightarrow \beta \urcorner) \vdash_T \text{bew}_T(u * v * \langle \ulcorner \beta \urcorner \rangle, \ulcorner \beta \urcorner)$. Partikularisierung ergibt $D2$. Beim Beweis von $D2^*$ kommt es vor allem auf die Definierbarkeit der dort erscheinenden p.r. Funktionen an, der wir uns zuerst zuwenden.

Der Übersicht halber begrenzen wir alle folgenden Ausführungen auf die Theorien ZFC und PA, die bei fast allen grundlagentheoretischen Fragestellungen im Blickpunkt des Interesses stehen. ZFC wird nur kurz diskutiert, weil der Nachweis von $D2$, $D3$ hier ungleich einfacher ist als für PA. So sind $D2^*$ und damit $D2$ in ZFC deshalb klar, weil der naive Nachweis von $D2^*$ mit $\text{bew}_T = \text{bew}_{\text{ZFC}}$ unschwer in ZFC formalisiert werden kann. Das schließt die Definierbarkeit der in $D2^*$ erscheinenden arithmetischen Funktionen natürlich ein. Diese wurden in 6.1 aber definiert – setze z.B. $a * b = \emptyset$ falls nicht $a, b \in \omega$. Man gödelisiert \mathcal{L}_ϵ nach dem Muster von 6.2¹⁾. Eine Formel $\varphi \in \mathcal{L}_\epsilon$ wird so zum ω -Term $\ulcorner \varphi \urcorner$ in ZFC. \mathcal{L}_{ar} -Formeln identifizieren wir mit

¹⁾Dazu ist man eigentlich nicht benötigt, weil in ZFC über üblich definierte endliche Folgen und damit über \mathcal{L}_ϵ -Formeln nahezu direkt geredet werden kann. Dies geschieht nur, um die Kohärenz mit den Ausführungen in 6.2 zu wahren.

ihren Relativierten auf ω , den *arithmetischen* Formeln von \mathcal{L}_ϵ . Darüber hinaus wird das arithmetische Prädikat bew_{ZFC} nach Satz 6.4.2 in ZFC durch bew_{ZFC} repräsentiert. Dieser Satz ist wie jeder andere in diesem Buch ein Satz *in* ZFC . Gewiss kann der auf Satz 6.4.2 (bisher zu Korollar 6.4.3) beruhende naive Beweis von $D1$ ganz in ZFC ausgeführt werden und damit ist $D3$ bewiesen. Die Ableitungsbedingungen für ZFC folgen grob gesagt einfach daraus, dass die gewohnte Mathematik in ZFC formalisierbar ist. Bei alledem braucht man keine typisch mengentheoretischen Konstruktionen wie z.B. ordinale Rekursion; man benötigt nur simple kombinatorische Fakten. Daher überrascht es nicht, dass $D2$ und $D3$ in hinreichend strengen arithmetischen Theorien wie PA beweisbar sind. Das ist natürlich nur dann nichttrivial, wenn diese Theorien konsistent sind, was wir meist stillschweigend voraussetzen.

Unser erstes Etappenziel ist es zu zeigen, dass nicht nur die Funktionen in $D2^*$, sondern sogar alle p.r. Funktionen in $T = \text{PA}$ definierbar sind²⁾. Danach kann man mit diesen Funktionen umgehen, als wären sie von Anfang an in PA vorhanden. Erst diese grundlegende Tatsache erlaubt die Behandlung der elementaren Zahlentheorie und Kombinatorik in den Grenzen von PA . Die p.r. Funktionen erweisen sich sogar als definierbar in folgendem Sinne, einer Verschärfung von (1) auf Seite 211:

Definition. Eine n -stellige rekursive Funktion f heie Σ_1 -*definierbar* in PA oder auch *beweisbar rekursiv*, wenn es eine Σ_1 -Formel $\delta_f(\vec{x}, y)$ gibt mit

$$(2) \quad (a) \quad \mathcal{N} \models \delta_f(\vec{a}, f\vec{a}) \text{ fur alle } \vec{a} \in \mathbb{N}^n, \quad (b) \quad \vdash_{\text{PA}} \forall \vec{x} \exists! y \delta_f(\vec{x}, y).$$

Wegen der Σ_1 -Vollstandigkeit von PA ist (a) gleichwertig mit $\vdash_{\text{PA}} \delta_f(\vec{a}, f\vec{a})$ fur alle \vec{a} . Daher wird (1) fur $T = \text{PA}$ durch (2) verschrft. Falls $\delta_f(\vec{x}, y)$ bereits Δ_0 ist, so heie f Δ_0 -*definierbar* in PA . Beispiele sind die Funktionen rest und β , bung 1.

Wichtig fur die Σ_1 -Definierbarkeit aller p.r. Funktionen ist Lemma 6.4.1, die Haupteigenschaft von β , von der eine gewisse Variante auch in PA verfugbar sein mu. Dabei wird auch der Chinesische Restsatz bentigt, obwohl noch unklar ist wie dieser in \mathcal{L}_{ar} zu formulieren ist, weil ja ber endliche Zahlenfolgen quantifiziert wird.

Zwecks berwindung dieser Hrde mgen c, d Symbole fur in PA definitorisch eingefuhrte einstellige Funktionen bezeichnen, die noch von weiteren Parametern abhngen drfen. Eine solches c bestimmt fur gegebenes n die Zahlenfolge c_0, \dots, c_n mit $c_\nu := c(\nu)$ fur $\nu \leq n$. Damit ist dann der Chinesische Restsatz in PA wie folgt formulierbar: Fur beliebige c, d wie oben verabredet gilt

$$(3) \quad \vdash_{\text{PA}} \forall n [(\forall \nu, i, j \leq n) (c_\nu < d_\nu \wedge (i \neq j \rightarrow d_i \perp d_j)) \rightarrow \exists a (\forall \nu \leq n) \text{rest}(a, d_\nu) = c_\nu].$$

²⁾Godel gab in [G2] eine Liste von 45 p.r. Funktionen an, deren letzte χ_{bew} war. Er betrachtet dort in Anlehnung an [WR] eine arithmetische Theorie hoherer Stufe. Dass Godels Stze auch in einer Arithmetik 1. Stufe gelten, wurde in [HB] erstmals nachgewiesen.

Aus suggestiven Gründen bezeichnen hier auch n, ν, \dots Variablen von \mathcal{L}_{ar} . Der Beweis von (3) verläuft fast genauso wie der des Restsatzes auf Seite 189 durch Induktion. Im weiteren Verlauf beschränken wir uns auf den Fall, dass die einstelligen Funktionen c, d beweisbar rekursiv sind. Man erhält dann auch eine definierende Σ_1 -Formel für $f: n \mapsto \text{kgV}\{d_\nu \mid \nu \leq n\}$. In der Tat, weil die Teilbarkeit Δ_0 ist, leistet dies $\delta_f(x, y) := (\forall \nu \leq x) d_\nu \mid y \wedge (\forall z < y) (\exists \nu \leq x) d_\nu \nmid z$. Genauer, $\delta_f(x, y)$ beschreibt eine Σ_1 -Formel, ähnlich wie δ_{exp} Seite 190. Weil $\mathcal{N} \models \delta_f(\underline{n}, \text{kgV}\{d_\nu \mid \nu \leq n\})$ für jedes n , gilt 2(a). Sei $\gamma(x, y) := (\forall \nu \leq x) d_\nu \mid y$, so dass $\delta_f(x, y) = \gamma(x, y) \wedge (\forall z < y) \neg \gamma(x, z)$. Das Schema der Minimalzahl (Übung 3 in 3.3) ergibt dann $\vdash_{\text{PA}} \exists y \delta_f(x, y)$ (und damit offenbar auch $\vdash_{\text{PA}} \exists! y \delta_f(x, y)$), wenn zuvor nur $\vdash_{\text{PA}} \exists y \gamma(x, y)$ bewiesen wurde. Das erfolgt induktiv über x . Klar ist $\vdash_{\text{PA}} \exists y \gamma(0, y)$. Der Induktionsschritt, nämlich $\exists y \gamma(x, y) \vdash_{\text{PA}} \exists y' \gamma(Sx, y')$, wurde schon auf Seite 63 ausgeführt. Das beweist 2(b). Also ist f beweisbar rekursiv und damit in PA explizit definierbar, was für den Beweis der folgenden Version von Lemma 6.4.1 (Seite 190) wichtig ist. Dabei wird hier und nachfolgend βst für $\beta(s, t)$ geschrieben:

$$(4) \quad \vdash_{\text{PA}} \forall x \exists u (\forall v \leq x) c_v = \beta uv, \quad \text{für jede beweisbar rekursive Funktion } c.$$

Satz 1.1. *Jede p.r. Funktion f ist beweisbar rekursiv und somit explizit definierbar in PA . Auch sind im Falle $f = \mathbf{Op}(g, h)$ die Rekursionsgleichungen für f beweisbar.*

Beweis. Für die Anfangsfunktionen und $+, \cdot$ sind $v_0 = 0$, $v_1 = Sv_0$, $v_n = v_\nu$, sowie $v_2 = v_0 + v_1$ und $v_2 = v_0 \cdot v_1$ definierende Σ_1 -Formeln. (2) ist hier offensichtlich. Für $f = h[g_1, \dots, g_m]$ sei $\delta_f(\vec{x}, y)$ die Formel $y = h(g_1 \vec{x}, \dots, g_m \vec{x})$ – genauer, deren Reduzierte $\exists \vec{y} (\bigwedge_i \delta_{g_i}(\vec{x}, y_i) \wedge \delta_h(\vec{y}, y))$ in \mathcal{L}_{ar} – und auch hier ist (2) offensichtlich. Geschick verlangt nur die Definition von δ_f für $f = \mathbf{Op}(g, h)$, in der wir nebst β auch die Symbole g, h nach Induktionsannahme schon benutzen dürfen. Man betrachte

$$(5) \quad \delta_f(\vec{x}, y, z) := \exists u \underbrace{[\beta u 0 = g\vec{x} \wedge (\forall v < y) \beta u Sv = h(\vec{x}, v, \beta uv) \wedge \beta uy = z]}_{\gamma(u, \vec{x}, y, z)}.$$

δ_f ist Σ_1 , weil β, g, h Σ_1 -definierbar sind. Für $c_i := f(\vec{a}, i)$ mit $i \leq b$ gibt es nach Lemma 6.4.1 ein $c \in \mathbb{N}$ mit $\mathcal{N} \models \gamma(\underline{c}, \underline{\vec{a}}, \underline{b}, f(\vec{a}, b))$, was 2(a) bestätigt. Eindeutigkeit in 2(b) ergibt sich aus $\gamma(u, \vec{x}, y, z) \wedge \gamma(u', \vec{x}, y, z') \vdash_{\text{PA}} z = z'$. Dazu beweist man induktiv über y leicht $\gamma(u, \vec{x}, y, z) \wedge \gamma(u', \vec{x}, y, z') \vdash_{\text{PA}} (\forall v \leq y) \beta uv = \beta u'v$. Auch folgt $\vdash_{\text{PA}} \exists z \delta_f(\vec{x}, y, z)$ induktiv über y . Für $y = 0$ beachte man $\vdash_{\text{PA}} \exists u \beta u 0 = g\vec{x}$ (daher $\vdash_{\text{PA}} \exists z \delta_f(\vec{x}, 0, z)$) gemäß (4); man wähle darin c so, dass $c_0 = g\vec{x}$ und $c_v = 0$ sonst. Den Induktionsschritt $\exists z \delta_f(\vec{x}, y, z) \vdash_{\text{PA}} \exists z' \delta_f(\vec{x}, Sy, z')$ beweisen wir wieder informell. Angenommen $\gamma(u, \vec{x}, y, z)$ mit gegebenen u, \vec{x}, y, z . Dann ist das durch $c_v = \beta uv$ für $v < Sy$ und $c_{Sv} = h(\vec{x}, y, \beta uv)$ definierte c offenbar beweisbar rekursiv. Nach (4) mit Sy für x gibt es ein u' mit $\beta u'v = c_v = \beta uv$ für $v \leq y$ und $c_{Sv} = \beta u'Sy = h(\vec{x}, y, \beta uv)$. Mit diesem u' und $z' := \beta u'Sy$ folgt $\gamma(u', \vec{x}, Sy, z')$, also $\exists z' \delta_f(\vec{x}, Sy, z')$. Das beweist

den Induktionsschritt und somit 2(b). Schließlich zeigen wir für $f = \mathbf{Op}(g, h)$ noch

$$(A) \vdash_{\mathbf{PA}} f(\vec{x}, 0) = g\vec{x}, \quad (B) \vdash_{\mathbf{PA}} f(\vec{x}, Sy) = h(\vec{x}, y, f(\vec{x}, y)).$$

(A) gilt nach (2), weil $\vdash_{\mathbf{PA}} \delta_f(\vec{x}, 0, g\vec{x}), \delta_f(\vec{x}, 0, f(\vec{x}, 0))$. (B) folgt durch $<$ -Induktion über y . Sei $\alpha := f(\vec{x}, Sy) = h(\vec{x}, y, f(\vec{x}, y))$. Angenommen $(\forall v < y) \alpha \frac{v}{y}$. Nach (5) gilt $\gamma(u, \vec{x}, Sy, f(\vec{x}, Sy))$ für gewisses u , was $f(\vec{x}, Sy) = h(\vec{x}, y, \beta uy)$ ergibt, sowie auch $(\forall v \leq y) \beta uv = f(\vec{x}, v)$, also $f(\vec{x}, Sy) = h(\vec{x}, y, f(\vec{x}, y))$. Dies zeigt $\forall y ((\forall v < y) \alpha \frac{v}{y} \rightarrow \alpha)$, die Prämisse der $<$ -Induktion, womit $\vdash_{\mathbf{PA}} \forall y \alpha$ bewiesen ist. \square

Damit ist unser erstes Etappenziel erreicht. Wegen der Definierbarkeit ihrer charakteristischen Funktionen lassen sich die auf Seite 178 formulierten Eigenschaften der Prädikate $\text{bew}_{\mathbf{PA}}$ und $\text{bwb}_{\mathbf{PA}}$ nun auch im Rahmen von \mathbf{PA} herleiten. Dazu sind nur die in der dortigen Bemerkung formulierten Eigenschaften von $*$, ℓ , ... auch in \mathbf{PA} zu beweisen. Das ist ein kleines, dem Leser überlassenes Extraprogramm mit Einschluss des Beweises der eindeutigen Primzerlegung (Übung 3). Damit sind $D2^*$ und somit auch $D2$ für $T = \mathbf{PA}$ bewiesen. Durch Übertragung des naiven Beweises von (6) auf Seite 178 nach \mathbf{PA} erhalten wir nunmehr sogar

$$(6) \quad \Box(x) \wedge \Box(x \dot{\sim} y) \vdash_{\mathbf{PA}} \Box(y) \quad (\text{gleichwertig } \Box(x \dot{\sim} y) \vdash_{\mathbf{PA}} \Box(x) \rightarrow \Box(y)).$$

Bemerkung 2. Nun sind auch die Gleichungen (a),(b),(c) der Übung 4 in 6.4 in \mathbf{PA} beweisbar, denn alle dort erscheinenden Funktionen sind p.r. und in \mathbf{PA} damit explizit definierbar. (b) lautet z.B. $\vdash_{\mathbf{PA}} \text{sb}_{\vec{x}}(\ulcorner \alpha \urcorner, \vec{x}) = \text{sb}_{\vec{x}'}(\ulcorner \alpha \urcorner, \vec{x}')$ mit $\text{var } \vec{x}' := \text{var } \vec{x} \cap \text{frei } \alpha$. Für $\text{frei } \alpha = \emptyset$ gilt demnach $\vdash_{\mathbf{PA}} \text{sb}_{\vec{x}}(\ulcorner \alpha \urcorner, \vec{x}) = \text{sb}_{\emptyset}(\ulcorner \alpha \urcorner) = \ulcorner \alpha \urcorner$. Eine der Gleichungen von (c) lautet formalisiert z.B. $\vdash_{\mathbf{PA}} \text{sb}_{\vec{x}}(\ulcorner \alpha \urcorner, \vec{x}, Sy) = \text{sb}_{\vec{x}}(\ulcorner \alpha \frac{Sy}{x} \urcorner, \vec{x})$ und das Beispiel Seite 193 zeigt $\vdash_{\mathbf{PA}} \text{sb}_{xy}(\ulcorner \varphi \urcorner, x, Sy) = \text{sb}_x(\ulcorner \varphi \frac{Sx}{y} \urcorner, x)$. Zum Beweis benötigt man im Wesentlichen nur $\vdash_{\mathbf{PA}} \text{zf } Sx = S \text{zf } x$. Details dieser Übertragung seien dem Leser überlassen.

Der Beweis von $D3$ erfordert noch einige weitergehende Vorbereitungen. Wegen ihres Umfangs werden auch in guten Lehrbüchern nicht alle Beweisschritte dargeboten. Aber alle nachfolgend nur beschriebenen Beweisschritte können vom Leser mit ausreichender Geduld leicht explizit ausgeführt werden. Man könnte sich das Leben durch die gegenseitige Interpretierbarkeit von \mathbf{PA} und $\mathbf{ZFC}_{\text{fin}}$ (S. 202) erleichtern, weil in $\mathbf{ZFC}_{\text{fin}}$ über endliche Mengen und Folgen direkt geredet werden kann.

Wir führen nun einen weiteren Gebrauch von \Box ein, wobei $\Box(x)$ bis zum Ende des Abschnitts die Formel $\text{bwb}_{\mathbf{PA}}(x)$ meint. Der Eindeutigkeit halber sei x hier v_0 .

Definition. Für $\varphi = \varphi(\vec{x})$ sei $\Box[\varphi] := \Box(\text{sb}_{\vec{x}}(\ulcorner \varphi \urcorner, \vec{x}))$ ($= \text{bwb}_{\mathbf{PA}} \frac{\text{sb}_{\vec{x}}(\ulcorner \varphi \urcorner, \vec{x})}{x}$).

Nach Bemerkung 2 ist $\vdash_{\mathbf{PA}} \text{sb}_{\vec{x}}(\ulcorner \varphi \urcorner, \vec{x}) = \text{sb}_{\vec{x}'}(\ulcorner \varphi \urcorner, \vec{x}')$ mit $\text{var } \vec{x}' = \text{frei } \varphi$. Daher darf man o.B.d.A. von $\text{frei } \Box[\varphi] = \text{frei } \varphi$ ausgehen. Es ist $\Box[\alpha] \equiv_{\mathbf{PA}} \Box \alpha$ für Aussagen α , weil $\vdash_{\mathbf{PA}} \text{sb}_{\vec{x}}(\ulcorner \alpha \urcorner, \vec{x}) = \ulcorner \alpha \urcorner$ nach Bemerkung 2. Durch $\vdash_{\mathbf{PA}} \Box[\varphi]$ (gleichwertig $\vdash_{\mathbf{PA}} \forall \vec{x} \Box[\varphi]$) wird in \mathbf{PA} der Sachverhalt ' $\vdash_{\mathbf{PA}} \varphi(\vec{a})$ für alle \vec{a} ', also die Existenz

einer *Schar von Beweisen* in nur einer Aussage formuliert. Dies kann wegen der ω -Unvollständigkeit von PA weniger sein als $\vdash_{\text{PA}} \Box\varphi$, oder gleichwertig $\vdash_{\text{PA}} \Box\forall\vec{x}\varphi$.

Beispiel. Sei $\varphi(x, y) = \text{S}x = y$. Wir zeigen $\varphi \vdash_{\text{PA}} \Box[\varphi]$, gleichwertig $\vdash_{\text{PA}} (\Box[\varphi])^{\frac{\text{S}x}{y}}$, wobei o.B.d.A. $x, y \notin \text{gbd}\Box(x)$. Weil $\vdash_{\text{PA}} \text{sb}_{xy}(\ulcorner\varphi\urcorner, x, \text{S}x) \equiv \text{sb}_x(\ulcorner\varphi^{\frac{\text{S}x}{y}}\urcorner, x)$ (Bemerkung 2), genügt es $\vdash_{\text{PA}} \Box[\alpha]$ oder gleichwertig $\vdash_{\text{PA}} \forall x\Box[\alpha]$ für $\alpha(x) := \varphi^{\frac{\text{S}x}{y}} = \text{S}x \equiv \text{S}x$ zu verifizieren, was in PA die Aussage ‘für alle $a \in \mathbb{N}$ gilt $\alpha(\underline{a})$ ’ reflektiert. Wir begründen $\vdash_{\text{PA}} \Box[\alpha]$ im Detail: Man betrachte die p.r. Funktion $\tilde{\alpha}: a \mapsto \text{sb}_x(\dot{\alpha}, a)$ (die Gödelzahl von $\alpha(\underline{a})$). Nach Axiom $\Lambda 9$ ist $\langle \tilde{\alpha}(a) \rangle$ ein besonders einfacher arithmetisierter Beweis für $\tilde{\alpha}(a) = \text{S}\underline{a} = \text{S}\underline{a}$. In PA formalisiert: $\vdash_{\text{PA}} \text{bew}_{\text{PA}}(\langle \tilde{\alpha}(x) \rangle, \tilde{\alpha}(x))$. Das ergibt $\vdash_{\text{PA}} \exists y \text{bew}_{\text{PA}}(y, \tilde{\alpha}(x)) = \Box(\text{sb}_x(\ulcorner\alpha\urcorner, x)) = \Box[\alpha]$.

Es gelten folgende Varianten von $D1, D2$ für $\alpha = \alpha(\vec{x})$ und $\beta = \beta(\vec{x})$:

$$(7) \quad (a) \vdash_{\text{PA}} \alpha \Rightarrow \vdash_{\text{PA}} \Box[\alpha] \quad ; \quad (b) \Box[\alpha \rightarrow \beta] \vdash_{\text{PA}} \Box[\alpha] \rightarrow \Box[\beta].$$

Zum Beweis von (a) sei $\vdash_{\text{PA}} \alpha$, also auch $\vdash_{\text{PA}} \forall\vec{x}\alpha$ und $\vdash_{\text{PA}} \Box\forall\vec{x}\alpha$. Ein Beweis von $\forall\vec{x}\alpha$ liefert ähnlich wie im Beispiel für jedes $\vec{a} \in \mathbb{N}^n$ in p.r. Weise einen solchen für $\alpha(\vec{a})$ (man beachte $\Lambda 5$). In PA formuliert, $\Box\forall\vec{x}\alpha \vdash_{\text{PA}} \Box(\text{sb}_{\vec{x}}(\ulcorner\alpha\urcorner, \vec{x})) = \Box[\alpha]$. Daher $\vdash_{\text{PA}} \Box[\alpha]$. (b) folgt aus (6) mit $\text{sb}_{\vec{x}}(\ulcorner\alpha\urcorner, \vec{x})$ und $\text{sb}_{\vec{x}}(\ulcorner\beta\urcorner, \vec{x})$ für x und y . Denn $\vdash_{\text{PA}} \text{sb}_{\vec{x}}(\ulcorner\alpha \rightarrow \beta\urcorner, \vec{x}) = \text{sb}_{\vec{x}}(\ulcorner\alpha\urcorner, \vec{x}) \dot{\sim} \text{sb}_{\vec{x}}(\ulcorner\beta\urcorner, \vec{x})$ nach Übung 4 in 6.4. Die nach PA übertragenen Gleichungen (c) der Übung ergeben mit etwas Rechnung ferner

$$(8) \quad \Box[\alpha]^{\frac{t}{\vec{x}}} \equiv_{\text{PA}} \Box[\alpha^{\frac{t}{\vec{x}}}] \quad (t \in \{0, y, \text{S}y\} \text{ mit } y \notin \text{gbd}\alpha).$$

Die Einschränkung in (8) ist unerheblich, aber der Beweis wäre schwieriger und wir benötigen nur (8). $D3$ ist nun lediglich ein Sonderfall der Schlüsselbehauptung

$$(9) \quad \varphi \vdash_{\text{PA}} \Box[\varphi] \text{ für alle } \Sigma_1\text{-Formeln } \varphi \text{ (die beweisbare } \Sigma_1\text{-Vollständigkeit).}$$

Denn wählt man in (9) für φ die Σ_1 -Aussage $\Box\alpha$ für beliebiges $\alpha \in \mathcal{L}_{ar}^0$, ergibt sich $\Box\alpha \vdash_{\text{PA}} \Box[\Box\alpha] = \Box\Box\alpha$, und $D3$ ist bewiesen. Man erhält (9) durch eine Anwendung des folgenden Satzes, weil der Operator $\partial: \alpha \mapsto \Box[\alpha]$ nach (7), (8) und wegen $\text{frei}\alpha = \text{frei}\Box[\alpha]$ die Voraussetzungen des Satzes erfüllt.

Satz 1.2. Sei $\partial: \mathcal{L}_{ar} \rightarrow \mathcal{L}_{ar}$ ein Operator mit $\text{frei}\partial\alpha \subseteq \text{frei}\alpha$ und den Eigenschaften

$$\begin{aligned} d1: & \vdash_{\text{PA}} \alpha \Rightarrow \vdash_{\text{PA}} \partial\alpha, & d2: & \partial(\alpha \rightarrow \beta) \vdash_{\text{PA}} \partial\alpha \rightarrow \partial\beta, \\ ds: & (\partial\alpha)^{\frac{t}{\vec{x}}} \equiv_{\text{PA}} \partial(\alpha^{\frac{t}{\vec{x}}}) & (t \in \{0, y, \text{S}y\}, y \notin \text{gbd}\alpha). \end{aligned}$$

Dann gilt $\varphi \vdash_{\text{PA}} \partial\varphi$ (gleichwertig $\vdash_{\text{PA}} \varphi \rightarrow \partial\varphi$) für alle Σ_1 -Formeln φ aus \mathcal{L}_{ar} .

Beweis. ∂ erfüllt nach Bemerkung 1 auch $d0, d00$ und $d\wedge$. Es genügt nach Satz 6.7.2, die Behauptung für spezielle Σ_1 -Formeln zu beweisen. Sei φ zuerst die Formel $\text{S}x = y$. Hier ist $\varphi \vdash_{\text{PA}} \partial\varphi$ gleichwertig mit $\vdash_{\text{PA}} \partial\varphi^{\frac{\text{S}x}{y}} (= (\partial\varphi)^{\frac{\text{S}x}{y}})$, und dies nach ds mit $\vdash_{\text{PA}} \partial\text{S}x = \text{S}x$ was nach $d1$ gilt. Ähnlich folgt $y = z \vdash_{\text{PA}} \partial y = z$. Das wird für den

Induktionsbeweis von $\vdash_{\text{PA}} \forall yz(\varphi \rightarrow \partial\varphi)$ mit $\varphi := x + y = z$ über x in PA benötigt: $\varphi \frac{0}{x} \vdash_{\text{PA}} y = z \vdash_{\text{PA}} \partial(y = z) \vdash_{\text{PA}} \partial(\varphi \frac{0}{x}) \vdash_{\text{PA}} \partial\varphi \frac{0}{x}$ und damit $\vdash_{\text{PA}} \forall yz(\varphi \rightarrow \partial\varphi) \frac{0}{x}$. Weil $\varphi \frac{sy}{y} \equiv_{\text{PA}} \varphi \frac{sx}{x}$, ist auch $\partial\varphi \frac{sy}{y} \equiv_{\text{PA}} \partial\varphi \frac{sx}{x}$. Das liefert den Induktionsschritt, denn $\forall yz(\varphi \rightarrow \partial\varphi) \vdash \varphi \frac{sy}{y} \rightarrow \partial\varphi \frac{sy}{y} \vdash_{\text{PA}} \varphi \frac{sx}{x} \rightarrow \partial\varphi \frac{sx}{x} = (\varphi \rightarrow \partial\varphi) \frac{sx}{x}$. Die Formel $x \cdot y = z$ sei dem Leser überlassen. (*Hinweis:* $Sx \cdot y = z \equiv_{\text{PA}} \exists u(x \cdot y = u \wedge u + y = z)$, $d \wedge$, $d2$). Die Schritte über \wedge, \vee, \exists sind einfach: $\alpha \wedge \beta \vdash \alpha, \beta \vdash_{\text{PA}} \partial\alpha \wedge \partial\beta \vdash_{\text{PA}} \partial(\alpha \wedge \beta)$ nach $d \wedge$. Bei \vee beachte man $\alpha \vdash_{\text{PA}} \partial\alpha \vdash_{\text{PA}} \partial(\alpha \vee \beta)$ nach $d0$, analog für β . Ferner ist wegen $\alpha \vdash \exists x \alpha$ auch $\alpha \vdash_{\text{PA}} \partial\alpha \vdash_{\text{PA}} \partial\exists x \alpha$ nach $d0$, und weil $x \notin \text{frei} \partial\exists x \alpha$ folgt $\exists x \alpha \vdash_{\text{PA}} \partial\exists x \alpha$ mit Partikularisierung. Auch der Schritt über die Primterm-Substitution ist einfach: $\alpha \vdash_{\text{PA}} \partial\alpha$ hat offenbar $\alpha \frac{t}{x} \vdash_{\text{PA}} \partial\alpha \frac{t}{x} \vdash_{\text{PA}} \partial(\alpha \frac{t}{x})$ zur Folge.

Es verbleibt der Schritt über die beschränkte Quantifizierung. Sei $\alpha \vdash_{\text{PA}} \partial\alpha$ und $y \notin \text{var} \alpha$. Wir zeigen $\varphi \vdash_{\text{PA}} \partial\varphi$ für $\varphi := (\forall x < y)\alpha$ induktiv über y . Wegen $\vdash_{\text{PA}} \varphi \frac{0}{y}$ ist $\vdash_{\text{PA}} \partial(\varphi \frac{0}{y}) \vdash_{\text{PA}} \partial\varphi \frac{0}{y}$ nach $d1, ds$ und erst recht $\varphi \frac{0}{y} \vdash_{\text{PA}} \partial\varphi \frac{0}{y}$ (Induktionsanfang). Nun ist $\varphi \frac{sy}{y} \equiv_{\text{PA}} \varphi \wedge \alpha \frac{y}{x}$, und $\alpha \vdash_{\text{PA}} \partial\alpha$ liefert $\alpha \frac{y}{x} \vdash_{\text{PA}} \partial\alpha \frac{y}{x} \vdash_{\text{PA}} \partial(\alpha \frac{y}{x})$. Das ergibt $\varphi \frac{sy}{y} \wedge (\varphi \rightarrow \partial\varphi) \vdash_{\text{PA}} \varphi \wedge \alpha \frac{y}{x} \wedge (\varphi \rightarrow \partial\varphi) \vdash_{\text{PA}} \partial\varphi \wedge \partial(\alpha \frac{y}{x}) \vdash_{\text{PA}} \partial(\varphi \wedge \alpha \frac{y}{x}) \vdash_{\text{PA}} \partial(\varphi \frac{sy}{y})$, also $\varphi \rightarrow \partial\varphi \vdash_{\text{PA}} \varphi \frac{sy}{y} \rightarrow \partial(\varphi \frac{sy}{y})$, was zum Induktionsschritt gleichwertig ist. \square

Bemerkung 3. $D1$ – $D3$ sind noch für erheblich schwächere Theorien als PA beweisbar, z.B. für die sogenannte *Elementare Arithmetik* $\text{EA} = I\Delta_0 + \forall xy \exists z \delta_{\text{exp}}(x, y, z)$. Hier sei δ_{exp} als Δ_0 -Formel verstanden (Bemerkung 1 Seite 186). Die in EA beweisbar rekursiven Funktionen sind die elementaren ([Si]). Fast alles was hier für PA bewiesen wurde, Satz 1.1 eingeschlossen, ist auch beweisbar in $I\Sigma_1$ ($= \mathbb{Q} + \text{IS}$ beschränkt auf Σ_1 -Formeln). Beweisbar rekursiv sind dort genau die p.r. Funktionen, und dies sind auch die beweisbar rekursiven Funktionen in EA erweitert um das Π_2 -Induktionsschema ohne Parameter ([Be3]). Mehr über die Metatheorie von PA und ihrer Fragmente findet man in [HP].

Übungen

1. Man beweise in PA die Definierbarkeit der Restfunktion rest , der Paarfunktion φ und der β -Funktion durch geeignete Δ_0 -Formeln.
2. Man beweise in PA (a) $(\forall a > 1) \exists p(\text{prim } p \wedge p|a)$, (b) das Lemma von Euklid (Seite 193), (c) $\vdash_{\text{PA}} \forall abp(\text{prim } p \wedge p|ab \rightarrow p|a \vee p|b)$.
3. $(\forall n \geq 2)(\exists m \geq 2)n = \prod_{i \leq \ell_m} p_i^{(m)i}$ formalisiert in PA die Existenz der Primfaktorzerlegung³⁾. Man bestätige dies und beweise auch deren Eindeutigkeit.
4. Sei $T' = T + \alpha$ und T erfülle $D1$ – $D3$. Man zeige (a) $\vdash_T \Box_{T'} \varphi \leftrightarrow \Box_T(\alpha \rightarrow \varphi)$ (das formalisierte Deduktionstheorem), (b) $D1$ – $D3$ gelten auch für T' .

³⁾Hier dient m als Variable für die Darstellung der Primzahlexponenten-Folge. Man könnte hierfür z.B. auch die β -Funktion verwenden.

7.2 Die Theoreme von Gödel und Löb

Wir werden nun die Früchte der Bemühungen in 7.1 ernten. Solange nichts anderes vereinbart wird, sei eine Theorie T immer eine gödelisierbare und axiomatische, welche nebst dem Fixpunktlemma aus 6.5 die Ableitungsbedingungen $D1$ – $D3$ aus 7.1 erfüllt. Wir richten unser Augenmerk sogleich auf die Eindeutigkeitsaussage in Lemma 2.1(b) unten. Danach kann bis auf Äquivalenz in T höchstens $\Box\alpha \rightarrow \alpha$ Fixpunkt der Formel $\Box(x) \rightarrow \alpha$ sein. Der Beweis von Satz 2.2 wird zeigen, dass auch $\neg\Box(x)$ bis auf T -Äquivalenz nur einen Fixpunkt hat. Dahinter verbirgt sich nach Korollar 4.6 eine ganz allgemeine Tatsache.

Lemma 2.1. *Sei T wie oben vereinbart und α, γ Aussagen aus \mathcal{L}^0 derart, dass*

$$(\star) \quad \gamma \equiv_T \Box\gamma \rightarrow \alpha.$$

Dann gelten (a) $\Box\gamma \equiv_T \Box\alpha$, sowie (b) $\gamma \equiv_T \Box\alpha \rightarrow \alpha$.

Beweis. (\star) liefert $\Box\gamma \vdash_T \Box(\Box\gamma \rightarrow \alpha) \vdash_T \Box\Box\gamma \rightarrow \Box\alpha$ mit $D0, D2$. Nach $D3$ ist aber $\Box\gamma \vdash_T \Box\Box\gamma$, also $\Box\gamma \vdash_T \Box\alpha$. Weil $\alpha \vdash_T \Box\gamma \rightarrow \alpha \vdash_T \gamma$ nach (\star) , folgt $\alpha \vdash_T \gamma$ und wegen $D0$ daher auch $\Box\alpha \vdash_T \Box\gamma$. Das beweist (a). Ersetzung von $\Box\gamma$ durch $\Box\alpha$ in (\star) gemäß (a) ergibt (b). \square

Satz 2.2 (Zweiter Unvollständigkeitssatz). *PA erfüllt nebst dem Fixpunktlemma auch $D1$ – $D3$. Jede Theorie T dieser Art hat die folgenden Eigenschaften:*

- (1) *Ist T konsistent, so ist $\not\vdash_T \text{Con}_T$,*
- (2) *$\vdash_T \text{Con}_T \rightarrow \neg\Box \text{Con}_T$.*

Beweis. Der Beweis von $D1$ – $D3$ für PA war Gegenstand von 7.1. (1) folgt leicht aus (2). Denn angenommen $\vdash_T \text{Con}_T$. Dann ist $\vdash_T \Box \text{Con}_T$ nach $D1$ und $\vdash_T \neg\Box \text{Con}_T$ nach (2), daher ist T inkonsistent. Das beweist (1). Zum Nachweis von (2) sei γ ein Fixpunkt von $\neg\text{bwb}_T(x)$, also $\gamma \equiv_T \neg\Box\gamma \equiv \Box\gamma \rightarrow \perp$. Mit Lemma 2.1(b) für $\alpha = \perp$ folgt $\gamma \equiv_T \Box\perp \rightarrow \perp \equiv \neg\Box\perp = \text{Con}_T$. Aus $\gamma \equiv_T \text{Con}_T$ und $\gamma \equiv_T \neg\Box\gamma$ ergibt sich offenbar $\text{Con}_T \equiv_T \neg\Box \text{Con}_T$. Eine Hälfte hiervon ist die Behauptung (2). \square

Keine noch so starke der hier betrachteten konsistenten Theorien kann demnach ihre eigene Konsistenz beweisen. Speziell gilt $\not\vdash_{\text{PA}} \text{Con}_{\text{PA}}$. Der Beweis zeigt ferner, dass Con_T modulo T der einzige Fixpunkt von $\neg\text{bwb}_T$ ist. Er zeigt sogar

$$(3) \quad \text{Con}_T \equiv_T \neg\Box \text{Con}_T.$$

Das verschärft (2) aber nur leicht. Denn $\neg\Box \text{Con}_T \vdash_T \text{Con}_T$ ist ein Sonderfall von

$$(4) \quad \neg\Box\alpha \vdash_T \text{Con}_T \text{ (gleichwertig } \neg\text{Con}_T \vdash_T \Box\alpha), \text{ für jedes } \alpha \in \mathcal{L}.$$

Dies folgt wegen $\perp \vdash_T \alpha$ und $\neg \text{Con}_T \equiv \Box \perp$ bereits mit $D0$ und reflektiert in T den Sachverhalt ‘Ist T inkonsistent, so ist jede Formel beweisbar’. Nach (1) und (3) ist z.B. $\not\vdash_{\text{PA}} \neg \Box_{\text{PA}} \text{Con}_{\text{PA}}$, obwohl ‘in PA ist Con_{PA} unbeweisbar’ wegen (1) wahr ist.

Alle diese Behauptungen gelten unabhängig vom „Wahrheitsgehalt“ der Sätze von T . Eine Folge des 2. Unvollständigkeitssatzes ist nämlich die Existenz konsistenter arithmetischer Theorien $T \supseteq \text{PA}$, die auch Behauptungen beweisen, die in \mathcal{N} falsch sind, in denen also Wahrheiten und Unwahrheiten über \mathcal{N} friedlich miteinander leben. Solche „Traumtheorien“ sind überaus reichhaltig und umfassen die gewöhnliche Zahlentheorie. Eine solche ist speziell $\text{PA}^\perp := \text{PA} + \neg \text{Con}_{\text{PA}}$, denn *die Unbeweisbarkeit von Con_{PA} in PA ist gleichwertig mit der Konsistenz von PA^\perp* . Die kursiv hervorgehobene Aussage ist in PA sogar beweisbar. In der Tat, nach dem Deduktionstheorem ist $\vdash_{\text{PA}+\alpha} \perp \Leftrightarrow \vdash_{\text{PA}} \alpha \rightarrow \perp \equiv \neg \alpha$, und dies lässt sich auch in PA verifizieren, also $\vdash_{\text{PA}} \Box_{\text{PA}+\alpha} \perp \leftrightarrow \Box_{\text{PA}} \neg \alpha$ (Übung 4 in 7.1), oder gleichwertig

$$(5) \quad \text{Con}_{\text{PA}+\alpha} \equiv_{\text{PA}} \neg \Box_{\text{PA}} \neg \alpha; \quad \text{allgemeiner } \text{Con}_{T+\alpha} \equiv_T \neg \Box \neg \alpha.$$

Dies ergibt $\text{Con}_{\text{PA}^\perp} \equiv_{\text{PA}} \neg \Box_{\text{PA}} \neg \neg \text{Con}_{\text{PA}} \equiv \neg \Box_{\text{PA}} \text{Con}_{\text{PA}}$, und mit (3) folgt

$$(6) \quad \text{Con}_{\text{PA}} \equiv_{\text{PA}} \text{Con}_{\text{PA}^\perp}; \quad \text{allgemeiner } \text{Con}_T \equiv_T \text{Con}_{T+\neg \text{Con}_T}.$$

Zusammengefasst: Die Theorie PA^\perp umfasst einerseits die aus PA vertraute Zahlentheorie, beweist aber $\neg \text{Con}_{\text{PA}}$ und damit nach (6) auch $\neg \text{Con}_{\text{PA}^\perp}$, also ihre eigene Inkonsistenz, obwohl mit PA auch PA^\perp konsistent ist. Con_T kann somit in T eine andere Bedeutung haben als die Konsistenz von T in unserer Metatheorie, ähnlich wie die Bedeutungen von ‘abzählbar’ divergieren, je nachdem ob man sich in ZFC befindet oder auf ZFC blickt. Man mag zugespitzt auch sagen, PA^\perp belügt uns mit $\neg \text{Con}_{\text{PA}^\perp}$, d.h. der Existenzbehauptung eines Beweises von \perp . Wir lernen hieraus, dass mit einer konsistenten Theorie T nicht notwendig auch $T^+ := T + \text{Con}_T$ konsistent sein muss, PA^\perp ist ein Beispiel. Mehr zur Bedeutung von $\neg \text{Con}_T$ in Satz 2.4.

Wir diskutieren nun das neben (3) berühmteste Beispiel einer selbstbezüglichen Aussage. Offenbar behauptet ein Fixpunkt α von bwb_T gerade seine eigene Beweisbarkeit, also $\alpha \equiv_T \Box \alpha$. Ein triviales Beispiel ist $\alpha = \top$, denn mit $\vdash_T \top$ ist auch $\vdash_T \Box \top$, also $\top \equiv_T \Box \top$. Es wird sich wiederum zeigen, dass \top modulo T einziger Fixpunkt von $\text{bwb}_T(x)$ ist. Ein Satz kann also seine eigene Beweisbarkeit nur dann behaupten, wenn er tatsächlich beweisbar ist. $\vdash_T \alpha$ folgt sogar schon aus $\vdash_T \Box \alpha \rightarrow \alpha$. Damit gilt Letzteres nicht für jedes α , obwohl man $\vdash_T \Box \alpha \rightarrow \alpha$ für alle $\alpha \in \mathcal{L}^0$ z.B. für $T = \text{PA}$ durchaus erwarten könnte, weil diese Aussagen wahr sind.

Satz 2.3 (Löbsches Theorem). *T erfülle $D1$ – $D3$ und das Fixpunktlemma. Dann hat T die Eigenschaften*

$$D4: \quad \vdash_T \Box(\Box \alpha \rightarrow \alpha) \rightarrow \Box \alpha, \quad D4^\circ: \quad \vdash_T \Box \alpha \rightarrow \alpha \Rightarrow \vdash_T \alpha \quad (\alpha \in \mathcal{L}^0).$$

Beweis. Sei γ ein Fixpunkt von $\Box(x) \rightarrow \alpha$ gemäß Fixpunktlemma, $\gamma \equiv_T \Box\gamma \rightarrow \alpha$. Also $\gamma \equiv_T \Box\alpha \rightarrow \alpha$ nach Lemma 2.1(b). Hieraus folgt $\Box\gamma \equiv_T \Box(\Box\alpha \rightarrow \alpha)$ nach D0. Lemma 2.1(a) besagt $\Box\gamma \equiv_T \Box\alpha$, also $\Box\alpha \equiv_T \Box(\Box\alpha \rightarrow \alpha)$. Eine Hälfte hiervon ist D4. Nachweis von $D4^\circ$: Es gelte $\vdash_T \Box\alpha \rightarrow \alpha$. Dann ist $\vdash_T \Box(\Box\alpha \rightarrow \alpha)$ nach D1. Mit D4 folgt hieraus $\vdash_T \Box\alpha$, und $\vdash_T \Box\alpha \rightarrow \alpha$ liefert alsdann $\vdash_T \alpha$. \square

D4 ist die in T formalisierte Version von $D4^\circ$. Eine von vielen Anwendungen des Satzes ist folgender Kurzbeweis des Gödelschen Resultats (1). Für $\alpha = \perp$ ergibt $D4^\circ$ $\not\vdash_T \perp \Rightarrow \not\vdash_T \Box\perp \rightarrow \perp \equiv \text{Con}_T$. Analog folgt (2) sofort aus D4 durch Kontraposition.

Anders als PA^+ geht $\text{PA}^+ = \text{PA} + \text{Con}_{\text{PA}}$ mit der Wahrheit in \mathcal{N} konform, weil $\mathcal{N} \models \text{Con}_{\text{PA}}$. Leider weiß man nicht genau, was Con_{PA} zahlentheoretisch bedeutet. Das weiß man aber von einer von Paris und Harrington entdeckten und in ZFC beweisbaren arithmetischen Aussage α mit $\vdash_{\text{PA}} \alpha \rightarrow \text{Con}_{\text{PA}}$, die nach (1) in PA nicht beweisbar sein kann. Inzwischen kennt man mehrere derartige Aussagen, die alle kombinatorisch gefärbt sind. Ein populäres Beispiel einer derartigen Aussage ist der

Satz von Goodstein. *Jede Goodstein-Folge endet mit 0.*

Darunter sei eine Zahlenfolge $(a_n)_{n \in \mathbb{N}}$ mit beliebig vorgegebenem a_0 verstanden, so dass sich a_{n+1} aus a_n wie folgt ergibt: Sei $b_n = n + 2$, also $b_0 = 2$. Man stelle a_n für $b := b_n$ in b -adischer Basis dar. Für ein gewisses k gilt dann

$$(*) \quad a_n = \sum_{i \leq k} b^{k-i} c_i, \text{ mit } 0 \leq c_i < b.$$

Dabei werden auch die Exponenten $k - i$ in b -adischer Darstellung geschrieben, auch die Exponenten der Exponenten, usw. Nun ersetze man b überall durch $b + 1$ und subtrahiere von der so entstehenden Zahl die Zahl 1. Das Ergebnis heißt dann a_{n+1} . Die Tabelle unten enthält ein Beispiel, beginnend mit $a_0 = 11$. Schon a_5 hat den Wert 134 217 728. Wie man an diesem Beispiel sieht, wächst a_n zunächst enorm an und es ist kaum glaubhaft, dass diese Folge mit 0 endet. Der Beweis hierfür ist nicht einmal schwierig. Man schätzt a_n nach oben ab durch eine Ordinalzahl ξ_n , die aus a_n grob gesagt dadurch entsteht, dass man die Basis b in $(*)$ durch ω ersetzt. Solange $a_{n+1} \neq 0$, gilt dann $\xi_{n+1} < \xi_n$. Da es keine unendlichen echt fallenden Folgen von Ordinalzahlen gibt, muss a_n schließlich mit 0 enden. Siehe hierzu auch [HP].

$a_0 = 11 = 2^{2+1} + 2 + 1$	$2 \rightsquigarrow 3$	$3^{3+1} + 3 + 1 = 85$
$a_1 = 84 = 3^{3+1} + 3$	$3 \rightsquigarrow 4$	$4^{4+1} + 4 = 1028$
$a_2 = 1027 = 4^{4+1} + 3$	$4 \rightsquigarrow 5$	$5^{5+1} + 3 = 15\,628$
$a_3 = 15\,627 = 5^{5+1} + 2$	$5 \rightsquigarrow 6$	$6^{6+1} + 2 = 279\,938$
$a_4 = 279\,937 = 6^{6+1} + 1$	$6 \rightsquigarrow 7$	$7^{7+1} + 1 = 5\,764\,802$

Viele metatheoretische Eigenschaften können durch Benutzung des Beweisoperators \Box in T ausgedrückt werden, oft durch Aussagenschemata. Die folgenden Beispiele

sind hilfreich, um die Bedeutung von $\neg \text{Con}_T$ innerhalb von T zu erfassen. Keine dieser Eigenschaften trifft in unserer Metatheorie auf ein konsistentes T zu.

- (i) $\neg \text{Con}_T : \Box \perp$ (beweisbare Inkonsistenz),
- (ii) $\text{SyVo} : \Box \alpha \vee \Box \neg \alpha$ (syntaktische Vollständigkeit),
- (iii) $\text{SeVo} : \alpha \rightarrow \Box \alpha$ (semantische Vollständigkeit),
- (iv) $\omega\text{-Vo} : \forall x \Box [\varphi(x) \rightarrow \Box \forall x \varphi(x)]$ (ω -Vollständigkeit).

Satz 2.4. *Die Eigenschaften (i)–(iv) sind in T alle äquivalent.*

Beweis. Nach (4) sind (i) \Rightarrow (ii),(iii),(iv) klar. (ii) \Rightarrow (i): Rossers Theorem 6.5.1'' ergibt formalisiert (siehe 7.4) ein α mit $\text{Con}_T \vdash_T \neg \Box \alpha, \neg \Box \neg \alpha$, also $\Box \alpha \vee \Box \neg \alpha \vdash_T \neg \text{Con}_T$. (iii) \Rightarrow (i): Nach SeVo ist $\text{Con}_T \vdash_T \Box \text{Con}_T$, Satz 2.2 sagt aber $\text{Con}_T \vdash_T \neg \Box \text{Con}_T$, also $\vdash_T \neg \text{Con}_T$. (iv) \Rightarrow (i): $\neg \text{bew}_T(x, \ulcorner \perp \urcorner) \vdash_T \Box [\neg \text{bew}_T(x, \ulcorner \perp \urcorner)]$ gilt gemäß (9) in 7.1, also $\text{Con}_T = \forall x \neg \text{bew}_T(x, \ulcorner \perp \urcorner) \vdash_T \forall x \Box [\neg \text{bew}_T(x, \ulcorner \perp \urcorner)]$. Mit $\omega\text{-Vo}$ und (2) also $\text{Con}_T \vdash_T \Box \forall x \neg \text{bew}_T(x, \ulcorner \perp \urcorner) = \Box \text{Con}_T \vdash_T \neg \text{Con}_T$. Folglich gilt $\vdash_T \neg \text{Con}_T$. \square

Bemerkung. Auch Con_T ist in T mit anderen Eigenschaften äquivalent, etwa mit dem Schema $\Box \alpha \rightarrow \alpha$ für Π_1 -Aussagen α (*lokales Π_1 -Reflektionsprinzip*), sowie mit dem *uniformen Π_1 -Reflektionsprinzip* $\forall x \Box [\alpha(x) \rightarrow \forall x \alpha(x)]$ für Π_1 -Formeln α , siehe z.B. [Ba, D.1]. Sowohl der Satz von Paris-Harrington als auch der von Goodstein sind in PA zur uniformen Σ_1 -Reflektion äquivalent, siehe etwa [Ba, D.8].

Wir erklären rekursiv $T^0 = T$ und $T^{n+1} = T^n + \text{Con}_{T^n}$. Diese *n-fach iterierte Konsistenzweiterung* hat nach Übung 3 die Darstellung $T^n = T + \neg \Box^n \perp$; dabei ist $\Box = \text{bwb}_T$, $\Box^0 \alpha = \alpha$ und $\Box^{n+1} \alpha = \Box \Box^n \alpha$. Es sei $T^\omega := \bigcup_{n \in \omega} T^n$. Da $T^n \subseteq T^{n+1}$, ist T^ω konsistent genau dann, wenn alle T^n konsistent sind, d.h. $\not\vdash_T \Box^n \perp$ für alle n . Beispiel 2(a) in 7.3 wird zeigen $\text{PA} \subset \text{PA}^1 \subset \text{PA}^2 \subset \dots$. Wie $\text{PA}^1 = \text{PA} + \text{Con}_{\text{PA}}$, geht auch PA^ω mit der Wahrheit konform, was kritisch beleuchtet allerdings nur heißt, dass PA^ω relativ konsistent ist zu ZFC, d.h. $\vdash_{\text{ZFC}} \text{Con}_{\text{PA}^\omega}$. Hier das (in ZFC zu formalisierende) Argument: Wäre $\vdash_{\text{PA}^\omega} \perp$, so folgt schon $\vdash_{\text{PA}^n} \perp$ für ein n und mithin $\vdash_{\text{PA}} \neg \Box^n \perp \rightarrow \perp \equiv \Box^n \perp$. Dies aber ist unmöglich, wie eine wiederholte Anwendung von $D1^*$ auf Seite 211 zeigt.

Übungen

1. Man beweise $D4^\circ$ für T durch Anwendung von Satz 2.2 auf $T' = T + \neg \alpha$.
2. Man zeige mit dem Löbschen Theorem, $\text{Con}_{\text{PA}} \rightarrow \Diamond \text{Con}_{\text{PA}}$ ist in PA unbeweisbar (wohl aber wahr).
3. Man beweise $T^n = T + \neg \Box^n \perp$ und $\text{Con}_{T^n} \equiv_T \neg \Box^{n+1} \perp$. Dabei sei $\Box = \Box_T$.
4. Man beweise $\vdash_{\text{ZFC}} \Box_{\text{PA}} \alpha \rightarrow \alpha$ für jede arithmetische Aussage $\alpha \in \mathcal{L}_\epsilon^0$.

7.3 Die Modallogik G

In 7.2 wurde Prädikatenlogik kaum benötigt. Daher überrascht nicht, dass sich viele der dortigen Resultate aussagenlogisch, genauer, in einem sogenannten modalen Aussagenkalkül gewinnen lassen. Dieser enthalte nebst \wedge, \neg auch das Falsumsymbol \perp , sowie einen weiteren einstelligen Junktor \Box , der den Beweisoperator interpretieren soll. Wir definieren zuerst eine aussagenlogische Sprache \mathcal{F}_\Box , deren Formeln durch H, G, F bezeichnet werden: (a) Die Aussagenvariablen p_1, p_2, \dots und \perp gehören zu \mathcal{F}_\Box . (b) Mit $H, G \in \mathcal{F}_\Box$ sind auch $(H \wedge G), \neg H, \Box H \in \mathcal{F}_\Box$. Weitere Formeln gibt es in diesem Zusammenhang nicht. $H \vee G, H \rightarrow G, H \leftrightarrow G$ seien wie in 1.4 definiert, $\top := \neg \perp$. Ferner sei $\Box^0 H = H$ und $\Box^{n+1} H = \Box \Box^n H$, sowie $\Diamond H := \neg \Box \neg H$.

Sei \mathbf{G} die Menge der Formeln von \mathcal{F}_\Box , die man mit Substitutionen $\sigma: \mathcal{F}_\Box \rightarrow \mathcal{F}_\Box$, dem Modus Ponens MP und der „Box-Regel“ MN: $H/\Box H$ ableiten kann aus den Tautologien der 2-wertigen Aussagenlogik, vermehrt um die modalen Axiome

$$\Box(p \rightarrow q) \rightarrow \Box p \rightarrow \Box q, \quad \Box p \rightarrow \Box \Box p, \quad \Box(\Box p \rightarrow p) \rightarrow \Box p \text{ (Löbsches Axiom)}.$$

Auf das Axiom $\Box p \rightarrow \Box \Box p$ könnte im Prinzip verzichtet werden; es ist aus den übrigen Axiomen beweisbar, siehe [Boo] oder [Ra1]. Für $H \in \mathbf{G}$ schreiben wir meistens $\vdash_{\mathbf{G}} H$ (gelesen: \mathbf{G} beweist H). Die Regel MN entspricht offenbar der Bedingung D1. Das erste Axiom von \mathbf{G} gibt D2 wieder, das mittlere D3, und das letzte entspricht D4. Eine Beschreibung der Beziehung zwischen \mathbf{G} und PA gibt 7.4. Zunächst geht es nur um das formale System \mathbf{G} und seine nachfolgend erläuterte Kripke-Semantik. Wir beschränken uns hier ganz auf endliche Kripke-Strukturen für \mathbf{G} , kurz \mathbf{G} -Strukturen genannt, und beginnen ohne lange Vorrede mit folgender

Definition. Eine \mathbf{G} -Struktur sei eine endliche irreflexive Halbordnung $(g, <)$. Eine Belegung sei eine Abbildung w , die jeder Variablen p eine Teilmenge wp von g zuordnet. Die von w abhängige Relation $P \Vdash H$ zwischen Punkten $P \in g$ und Formeln $H \in \mathcal{F}_\Box$ (gelesen: P akzeptiert H) wird induktiv erklärt durch

$$\begin{aligned} P \Vdash p &\Leftrightarrow P \in wp, & P \not\Vdash \perp, & & P \Vdash H \wedge G &\Leftrightarrow P \Vdash H, G, \\ P \Vdash \neg H &\Leftrightarrow P \not\Vdash H, & P \Vdash \Box H &\Leftrightarrow P' \Vdash H \text{ für alle } P' > P. \end{aligned}$$

Falls $P \Vdash H$ für alle \mathbf{G} -Strukturen g , alle $P \in g$ und alle Belegungen w , schreiben wir $\models_{\mathbf{G}} H$ und sagen H sei \mathbf{G} -gültig.

$\begin{matrix} P_1 & & P_2 \\ \bullet & \longrightarrow & \bullet \end{matrix}$ Die links dargestellte \mathbf{G} -Struktur aus den Punkten P_1, P_2 mit $P_1 < P_2$ zeigt $\not\models_{\mathbf{G}} p \rightarrow \Box p$. Denn sei $wp = \{P_1\}$. Dann ist $P_1 \Vdash p$, nicht aber $P_1 \Vdash \Box p$, weil $P_2 \not\Vdash p$. Ebenso gilt $\not\models_{\mathbf{G}} \Box p \rightarrow p$, da $P_2 \Vdash \Box p$. Ferner besagt $P \Vdash \Diamond H$ offenbar $P' \Vdash H$ für ein $P' > P$. Es stehe $H \equiv_{\mathbf{G}} H'$ für $\models_{\mathbf{G}} H \leftrightarrow H'$. Dies ist eine Kongruenz in \mathcal{F}_\Box , welche die logische Äquivalenz der Formeln ohne \Box konservativ erweitert. So gelten z.B. die wichtigen Äquivalenzen $\neg \Box H \equiv_{\mathbf{G}} \Diamond \neg H$ und $\neg \Diamond H \equiv_{\mathbf{G}} \Box \neg H$.

Beispiele. (a) Es ist $P \Vdash \Box H$ für beliebiges H , falls P *maximal* ist in g , d.h. es gibt kein $P' > P$. Speziell werden $\Box \perp$ und $\Box \neg \Box \perp$ nur genau an den maximalen Punkten von g akzeptiert. Daher ist $\Box \perp \equiv_G \Box \neg \Box \perp$, also $\neg \Box \perp \equiv_G \neg \Box \neg \Box \perp$. Dies reflektiert in G den zweiten Unvollständigkeitssatz wie Beispiel 1 in 7.4 zeigen wird.

(b) Sei $\{P_0, \dots, P_n\}$ die G -Struktur mit $P_n < \dots < P_0$. Induktion über n zeigt leicht $P_n \Vdash \Box^m \perp$ für $m > n$, jedoch $P_n \nVdash \Box^n \perp$. Daher auch $P_n \nVdash \Box^{n+1} \perp \rightarrow \Box^n \perp$. Folglich $\nVdash_G \Box^{n+1} \perp \rightarrow \Box^n \perp$ ($\equiv_G \neg \Box^n \perp \rightarrow \neg \Box^{n+1} \perp$) für jedes n . Erst recht also $\nVdash_G \Box^n \perp$.

(c) $\models_G \Box(\Box p \rightarrow p) \rightarrow \Box p$. Denn seien g und $P \in g$ beliebig. Ist $P \nVdash \Box p$, gibt es – weil g endlich ist – ein $Q > P$ mit $Q \nVdash p$ und $Q' \Vdash p$ für alle $Q' > Q$, also $Q \Vdash \Box p$. Das zeigt $Q \nVdash \Box p \rightarrow p$ und daher $P \nVdash \Box(\Box p \rightarrow p)$. Somit $P \Vdash \Box(\Box p \rightarrow p) \rightarrow \Box p$, was die Behauptung offenbar beweist. Ebenso einfach folgt $\models_G \Box p \rightarrow \Box \Box p$ aus der Transitivität von $<$. Ganz leicht ist der Beweis von $\models_G \Box(p \rightarrow q) \rightarrow \Box p \rightarrow \Box q$.

(d) Für $R_n := \bigwedge_{i=1}^n (\Box p_i \rightarrow p_i)$ ist $\models_G \neg \Box^{n+1} \perp \rightarrow \Diamond R_n$. Denn sei $P \Vdash \neg \Box^{n+1} \perp$. Dann muss eine Kette $P = P_0 < \dots < P_{n+1}$ in g existieren. Ein Konjunktionsglied von R_n wird aber von höchstens einem der $n+1$ Punkte P_1, \dots, P_{n+1} nicht akzeptiert, wie man leicht einsieht. Also $P_i \Vdash R_n$ für wenigstens ein $i > 0$. Folglich $P \Vdash \Diamond R_n$. Die Formel R_n ist sehr wichtig für unseren Beweis von Satz 6.1 auf Seite 228.

Induktion in \vdash_G zeigt $\vdash_G H \Rightarrow \models_G H$. Beispiel (c) ist ein Teil des Induktionsanfangs. Bei MN schließe man indirekt: mit $P \nVdash \Box H$ folgt $P' \nVdash H$ für ein $P' > P$. Etwas mehr Anstrengung kostet der Nachweis von $\models_G H \Rightarrow \vdash_G H$ in folgendem Satz, den wir ohne Beweis benutzen werden. Danach kann $\vdash_G H$ durch den Nachweis von $\models_G H$ auch bestätigt werden. Die besondere Bedeutung des Satzes und seines Korollars wird erst klar durch Satz 4.2. Für einen Beweis des Satzes siehe [Boo], [Ra1], oder auch [Kr] mit sehr allgemeinen Kriterien der endlichen Modelleigenschaft, die auf alle in diesem Kapitel betrachteten Modallogiken zutreffen.

Satz 3.1 (Vollständigkeit der Kripke-Semantik für G). $\vdash_G H \Leftrightarrow \models_G H$.

Die in G beweisbaren Formeln sind damit rekursiv aufzählbar. Aber auch die dort widerlegbaren Formeln; denn G ist endlich axiomatisierbar und die G -Strukturen sind sicher aufzählbar. Damit ergibt sich in völliger Analogie zu Übung 3 in 3.6 das

Korollar 3.2. G ist entscheidbar.

Bemerkung. Sei \mathcal{F}_\Box^0 die Menge der variablenfreien Formeln. $G^0 := G \cap \mathcal{F}_\Box^0$ ist ein wichtiges Fragment von G . Dessen interessanteste Formeln sind die $\neg \Box^n \perp$ ($\equiv_G \Diamond^n \top$). Denn diese bilden eine Boolesche Basis für G^0 . Das sieht man leicht, indem man zeigt G^0 ist vollständig bzgl. aller linearen G -Strukturen und den Basissatz 5.2.3 entsprechend anpaßt. Zwei lineare G -Strukturen, die dieselben „Basisformeln“ $\Box^n \perp$ erfüllen, sind entweder beide endlich und bereits isomorph, oder beide sind unendlich und ununterscheidbar bzgl. aller $H \in \mathcal{F}_\Box^0$.

7.4 Modale Behandlung der Selbstreferenz

Sei T eine Theorie in \mathcal{L} wie in 7.2. T erfüllt also $D1$ – $D4$. Eine Abbildung $\iota: p_i \mapsto \alpha_i$ ($\in \mathcal{L}^0$), *Einsetzung* genannt, liefert zu jedem $H \in \mathcal{F}_\square$ eine \mathcal{L} -Aussage H^ι , indem ι durch $\perp^\iota = \perp$, $(\neg H)^\iota = \neg H^\iota$, $(H \wedge G)^\iota = H^\iota \wedge G^\iota$ und $(\Box H)^\iota = \Box H^\iota$ ($= \text{bwb}_T(\ulcorner H^\iota \urcorner)$) auf ganz \mathcal{F}_\square fortgesetzt wird. H^ι entsteht aus $H = H(p_1, \dots, p_n)$ einfach durch Ersetzung der p_ν durch die α_ν . So ist zum Beispiel $(\Box p \wedge \neg \Box \perp)^\iota = \Box \alpha \wedge \neg \Box \perp$, falls $p^\iota = \alpha$. Das folgende Lemma zeigt $\vdash_G H \Rightarrow \vdash_T H^\iota$. Allein dieser Umstand erleichtert Beweise über selbstbezügliche Aussagen erheblich.

Lemma 4.1. *Für jedes H mit $\vdash_G H$ und jede Einsetzung ι in \mathcal{L} gilt $\vdash_T H^\iota$.*

Beweis durch Induktion über $\vdash_G H$. Für eine aussagenlogische Tautologie H ist $H^\iota \in \text{Taut}_\mathcal{L} \subseteq T$. Ist H eines der modalen Axiome von G , gilt $\vdash_T H^\iota$ nach $D2$, $D3$ bzw. $D4$. Ist $\vdash_G H$ und $\sigma: \mathcal{F}_\square \rightarrow \mathcal{F}_\square$ eine Substitution, gilt $\vdash_T H^{\sigma\iota}$, weil $H^{\sigma\iota} = H^{\iota'}$ mit $\iota': p \mapsto p^{\sigma\iota}$ und $\vdash_T H^{\iota'}$ gemäß Induktionsannahme. Wurde MN verwendet, gilt also $\vdash_T H^\iota$ nach Induktionsannahme, folgt mit $D1$ sicher auch $\vdash_T \Box H^\iota = (\Box H)^\iota$. Für den Schritt über MP beachte man $(F \rightarrow G)^\iota = F^\iota \rightarrow G^\iota$. \square

Beispiel 1. (a) Wir beweisen (3) und damit (2) aus 7.2. Gemäß Lemma 4.1 und Satz 3.1 genügt zu zeigen $\models_G \neg \Box \perp \leftrightarrow \neg \Box \neg \Box \perp$, was nach Beispiel (a) aus 7.3 richtig ist. (b) Man sieht leicht $\models_G \Box(p \leftrightarrow \Diamond p) \rightarrow \Box \neg p$. Also $\vdash_{PA} \Box(\alpha \leftrightarrow \Diamond \alpha) \rightarrow \Box \neg \alpha$. Das sagt in PA ‘Eine Aussage, die ihre eigene Konsistenz mit PA behauptet, ist mit PA unverträglich’. Obwohl dies im ersten Moment wenig plausibel erscheint, ist hiervon auch die Umkehrung richtig und in PA beweisbar. Denn $\models_G \Box \neg p \rightarrow \Box(p \leftrightarrow \Diamond p)$.

Wir erläutern nun einige Fakten, die die bisherigen Ausführungen in interessanter Weise ergänzen. Für PA und verwandte Theorien gilt auch die Umkehrung von Lemma 4.1. Mit anderen Worten, die Ableitungsbedingungen und das Löbsche Theorem enthalten bereits alles Wissenswerte über selbstreferierende Aussagenschemata. Für die subtilen Beweise der Sätze 4.2, 4.4 und 4.5 verweisen wir auf [Boo].

Satz 4.2 (Solovayscher Vollständigkeitssatz). *Für beliebiges $H \in \mathcal{F}_\square$ gilt $\vdash_G H$ (oder gleichwertig $\models_G H$) genau dann, wenn $\vdash_{PA} H^\iota$ für alle Einsetzungen ι .*

Beispiel 2. (a) $\not\vdash_{PA} \Box^{n+1} \perp \rightarrow \Box^n \perp$. Denn $\not\models_G \Box^{n+1} \perp \rightarrow \Box^n \perp$, Beispiel (b) in 7.3. Das zeigt $PA \subset PA^1 \subset PA^2 \subset \dots$, denn $PA^n = PA + \neg \Box^n \perp$ (Übung 3 in 7.2). (b) Man zeigt leicht $\not\models_G \neg \Box \perp \rightarrow \Box \neg \Box \perp$. Daher $\not\vdash_{PA} \text{Con}_{PA} \rightarrow \Box \text{Con}_{PA}$ nach Satz 4.2. (c) $PA_n := PA + \Box^n \perp$ ist konsistent für $n > 0$ (folgt aus (a)), aber ω -inkonsistent, denn $D1^*$ Seite 211 ergibt $\vdash_{PA_n} \Box^n \perp \Rightarrow \vdash_{PA_n} \Box^{n-1} \perp \Rightarrow \dots \Rightarrow \vdash_{PA_n} \perp$, im Widerspruch zu $\not\vdash_{PA_n} \perp$. Weil $\vdash_{PA} \Box^n \perp \rightarrow \Box^{n+1} \perp$ nach $D3$, gilt $PA_n \supseteq PA_{n+1}$, und weil $PA_{n+1} \neq PA_{n+2}$ sich leicht aus (a) ergibt, ist $PA_0 \supset PA_1 \supset \dots \supset PA$.

Infolge der Entscheidbarkeit von \mathbf{G} ist Satz 4.2 ein sehr effizientes Instrument zur Entscheidung über die Beweisbarkeit selbstbezüglicher Aussagenschemata. Weil z.B. $\not\models_{\mathbf{G}} \Box p \rightarrow p$, muss es ein $\alpha \in \mathcal{L}_{ar}^0$ mit $\not\models_{\mathbf{PA}} \Box \alpha \rightarrow \alpha$ geben. Ein Beispiel ist $\alpha = \perp$.

Viele andere Theorien haben dieselbe Beweislogik wie \mathbf{PA} . Dabei heie eine modale Aussagenlogik \mathbf{M} allgemein die *Beweislogik* fur T , wenn das Analogon von Satz 4.2 bzgl. T und \mathbf{M} gilt. Fur spezielle Theorien kann die Beweislogik allerdings auch eine echte Erweiterung von \mathbf{G} sein. So hat z.B. die ω -inkonsistente Theorie \mathbf{PA}_n aus Beispiel 2(c) gerade die Beweislogik $\mathbf{G}_n := \mathbf{G} + \Box^n \perp$, die kleinste gegenuber allen Regeln von \mathbf{G} abgeschlossene Erweiterung von \mathbf{G} mit dem Zusatzaxiom $\Box^n \perp$, bung 1 (man beachte, $\mathbf{G}_0 := \mathbf{G} + \perp$ ist inkonsistent). Andere Erweiterungen von \mathbf{G} kommen nach folgendem Satz von Visser als Beweislogiken nicht in Frage.

Satz 4.3. *T sei mindestens so stark wie \mathbf{PA} . Dann gelten*

- (a) *Ist T^ω konsistent, so ist \mathbf{G} die Beweislogik von T (Beweis erfolgt in 7.6),*
- (b) *Ist $\vdash_{T^\omega} \perp$ und n minimal mit $\vdash_{T^n} \perp$, so ist \mathbf{G}_n die Beweislogik von T .*

Es lassen sich nun auch die Formeln $H \in \mathcal{F}_\Box$ mit $\mathcal{N} \models H^\iota$ fur alle Einsetzungen ι in \mathcal{L}_{ar} uberraschenderweise recht einfach charakterisieren. Offenbar gehoren dazu alle $H \in \mathbf{G}$. Aber z.B. gehort dazu auch $\Box p \rightarrow p$, weil $\mathcal{N} \models \Box \alpha \rightarrow \alpha$ fur alle $\alpha \in \mathcal{L}_{ar}^0$.

Sei $\mathbf{GS} (\supseteq \mathbf{G})$ die Menge aller Formeln aus \mathcal{F}_\Box , die sich aus denen von $\mathbf{G} \cup \{\Box p \rightarrow p\}$ mittels Substitution und alleiniger Anwendung von MP, also ohne Box-Regel gewinnen lassen. Induktion uber die Erzeugung von \mathbf{GS} zeigt $H \in \mathbf{GS} \Rightarrow \mathcal{N} \models H^\iota$, fur alle Einsetzungen ι . Auch hier gilt nach [So] wieder die Umkehrung:

Satz 4.4. *$H \in \mathbf{GS}$ genau dann, wenn $\mathcal{N} \models H^\iota$ fur alle Einsetzungen ι .*

Auch \mathbf{GS} ist entscheidbar, denn man zeigt unschwer $H \in \mathbf{GS} \Leftrightarrow H^* \in \mathbf{G}$, wobei

$$H^* := [\bigwedge_{\Box G \in Sf^\Box H} (\Box G \rightarrow G)] \rightarrow H.$$

Hier ist $Sf^\Box H$ die Menge der Subformeln von H der Gestalt $\Box G$. Nach Satz 4.4 sind viele, die Beziehungen zwischen *beweisbar* und *wahr* betreffende Fragen effektiv entscheidbar. So ist z.B. $H(p) := \neg \Box (\neg \Box \perp \rightarrow \neg \Box p \wedge \neg \Box \neg p) \notin \mathbf{GS}$ leicht zu bestatigen. Aufgrund von Satz 4.4 ist also $\mathcal{N} \models \neg H(\alpha) \equiv \Box (\neg \Box \perp \rightarrow \neg \Box \alpha \wedge \neg \Box \neg \alpha)$ fur ein gewisses $\alpha \in \mathcal{L}_{ar}^0$. Dies bedeutet: Fur eine gewisse Aussage α ist in \mathbf{PA} *beweisbar*, dass die Konsistenz von \mathbf{PA} die Unabhangigkeit von α impliziert. Genau dies besagt der im Rahmen von \mathbf{PA} formulierte Satz von Rosser. Nach [Be1] kann \Box in den $H \in \mathbf{GS}$ in Satz 4.4 auch \mathbf{bwb}_T fur eine beliebige axiomatisierbare Theorie T mit $\mathbf{PA} \subseteq T \subseteq Th\mathcal{N}$ bedeuten; beweist T hingegen falsche Satze, (wie z.B. \mathbf{PA}^\perp), kann \mathbf{GS} vollkommen ubersehbar neu definiert werden und ist stets entscheidbar.

Eine in H vorkommende Variable p heie *modalisiert in H* , wenn p nur im Wirkungsbereich eines \Box -Operators steht, wie z.B. in $\neg \Box p$ und $\Box(p \rightarrow q)$, nicht aber in $\Box p \rightarrow p$. Ein weiterer hochinteressanter Satz ist

Satz 4.5 (Fixpunktsatz von DeJongh-Sambin). *Sei p modalisiert in $H(p, \vec{q})$, $\vec{q} = (q_1, \dots, q_n)$, $n \geq 0$. Dann gibt es ein $F = F(\vec{q}) \in \mathcal{F}_\square$ mit (a) $F \equiv_G H(F, \vec{q})$. Ferner gilt (b) $\vdash_G \bigwedge_{i=1,2} [(p_i \leftrightarrow H(p_i, \vec{q})) \wedge \square(p_i \leftrightarrow H(p_i, \vec{q}))] \rightarrow (p_1 \leftrightarrow p_2)$.*

Dieser Satz ergibt für alle D1–D4 erfüllende Theorien T leicht das

Korollar 4.6. *Sei p modalisiert in $H = H(p, \vec{q})$. Dann gibt es ein $F = F(\vec{q}) \in \mathcal{F}_\square$ mit $F(\vec{\alpha}) \equiv_T H(F(\vec{\alpha}), \vec{\alpha})$ für alle $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in \mathcal{L}^0$. Bis auf Äquivalenz in T existiert zu jedem $\vec{\alpha}$ nur genau ein $\beta \in \mathcal{L}^0$ mit $\beta \equiv_T H(\beta, \vec{\alpha})$.*

Beweis. Sei F gemäß Satz 4.5 beliebig gewählt. Dann gilt $F(\vec{\alpha}) \equiv_T H(F(\vec{\alpha}), \vec{\alpha})$ nach Lemma 4.1, mit $\vec{q}^* = \vec{\alpha}$. Zum Nachweis der Eindeutigkeit sei $\beta_i \equiv_T H(\beta_i, \vec{\alpha})$ für $i = 1, 2$. Das ergibt $\vdash_T (\beta_i \leftrightarrow H(\beta_i, \vec{\alpha})) \wedge \square(\beta_i \leftrightarrow H(\beta_i, \vec{\alpha}))$ mit D1. Einsetzung von $\beta_i, \vec{\alpha}$ für p_i bzw. \vec{q} in Satz 4.5(b) liefert nach Lemma 4.1 dann $\beta_1 \equiv_T \beta_2$. \square

Beispiel 3. Für $H = \neg \square p$, d.h. $n = 0$, ist $F = \neg \square \perp$ eine „Lösung“ von (a) in Satz 4.5, weil $\neg \square \perp \equiv_G \neg \square(\neg \square \perp)$. Nach dem Korollar ist $\text{Con}_T = \neg \square \perp$ einziger Fixpunkt von $\neg \text{bwb}_T$ modulo T . Das ist die Aussage von (3) in 7.2.

Viele Spezialfälle des Korollars repräsentieren ältere Resultate über Selbstreferenz von Gödel, Löb, Rogers, Jeroslow und Kreisel, die – modallogisch formuliert – Fixpunkte p von $\neg \square p$, $\square p$, $\neg \square \neg p$, $\square \neg p$ und $\square(p \rightarrow q)$ betreffen. Der Reihe nach sind dies $\neg \square \perp$, \top , \perp , $\square \perp$, und $\square q$. Diese Fixpunkte erhält man übrigens nach einem ganz einfachen Rezept. Denn die erstgenannten Formeln haben alle die Gestalt

$$H(p, \vec{q}) = G \frac{\square H'}{p} \quad (p \text{ in } G(p, \vec{q}) \text{ nicht modalisiert, } H'(p, \vec{q}) \text{ passend gewählt}).$$

Dann nämlich ist $F = H \frac{G(\top, \vec{q})}{p}$ Fixpunkt von H , wie sich nachrechnen lässt. Für $H = \neg \square p$ wie in Beispiel 3 ist $G = \neg p$. Daher ist $F = \neg \square p \frac{\neg \top}{p} = \neg \square \neg \top \equiv_G \neg \square \perp$. Für Kreisels Formel $\square(p \rightarrow q)$ ist $G = p$, also $F = \square(p \rightarrow q) \frac{\top}{p} = \square(\top \rightarrow q) \equiv_G \square q$. Das Rezept betrifft auch $H = \square p \rightarrow q$, mit $G = p \rightarrow q$. Der einzige Fixpunkt von H modulo T ist demnach $F = (\square p \rightarrow q) \frac{\top \rightarrow q}{p} = \square(\top \rightarrow q) \rightarrow q \equiv_G \square q \rightarrow q$. Genau dies war die Behauptung (b) des für Gödels Satz 2.2 wichtigen Lemmas 2.1.

Übungen

1. Man beweise, die Theorie PA_n aus Beispiel 2(c) hat die Beweislogik \mathbf{G}_n .
2. Man zeige $\text{PA}_\perp^n := \text{PA}^n + \neg \text{Con}_{\text{PA}^n}$ ist identisch mit $\text{PA} + \square^{n+1} \perp \wedge \neg \square^n \perp$. Dabei ist $\square = \square_{\text{PA}}$. Ferner zeige man PA_\perp^n hat die Beweislogik $\mathbf{G}_1 = \mathbf{G} + \square \perp$.
3. Man zeige \top , \perp und $\square \perp$ sind die Fixpunkte von $\square p$, $\neg \square \neg p$ und $\square \neg p$.
4. (Mostowski). Sei $T \supseteq \text{PA}$ axiomatisierbar und $\mathcal{N} \models T$. Man zeige, es gibt zwei relativ unabhängige (Σ_1 -)Aussagen α, β über T , d.h. $\alpha \rightarrow \beta$, $\alpha \rightarrow \neg \beta$, $\neg \alpha \rightarrow \beta$, $\neg \alpha \rightarrow \neg \beta$ (und damit auch α , β , $\neg \beta$) sind unbeweisbar in T .

7.5 Eine bimodale Beweislogik für PA

Nach einer Bemerkung von Hilbert lässt sich das Unvollständigkeitsphänomen durch Benutzung der sogenannten ω -Regel $\rho_\omega : \frac{X \vdash \varphi(\underline{n}) \text{ für alle } n}{X \vdash \forall x \varphi}$ sozusagen gewaltsam aus der Welt schaffen. ρ_ω hat unendlich viele Prämissen und es ist einfach, mittels ρ_ω jede in \mathcal{N} gültige Aussage α aus den Axiomen von PA (sogar aus denen von Q) herzuleiten. Denn dies ist wegen der Σ_1 -Vollständigkeit von Q sicher möglich für Primaussagen und deren Negationen; jede andere Aussage lässt sich aus diesen bis auf Äquivalenz mit $\wedge, \vee, \forall, \exists$ erzeugen und die Induktionsschritte über diese Junktoren sind einfach. Beim \forall -Schritt verwendet man gerade ρ_ω . Der uneingeschränkte Gebrauch der infinitären Regel ρ_ω widerspricht jedoch Hilberts eigenen Intentionen einer finiten Grundlegung der Mathematik. Schränkt man ρ_ω aber auf eine *einmalige* Anwendung beim Beweis von α ein, d.h. definiert man $1bwb_{\text{PA}}(\alpha)$ durch

$$1bwb_{\text{PA}}(\alpha) := (\exists \varphi \in \mathcal{L}_{ar}^1) [\forall n \, bwb_{\text{PA}}(\varphi(\underline{n})) \ \& \ bwb_{\text{PA}}(\forall v_0 \varphi \rightarrow \alpha)],$$

so ist dieses Prädikat immerhin arithmetisch; genauer, es ist Σ_3 wegen des in bwb_{PA} noch verborgenen \exists -Quantors. Im Sinne der Bemerkung 1 in 6.2 unterscheiden wir dabei nicht mehr zwischen α und $\dot{\alpha}$; wir lesen $1bwb_{\text{PA}}(\alpha)$ als ‘ α ist 1-beweisbar’. Sei $1bwb(z)$ die $1bwb_{\text{PA}}$ definierende Σ_3 -Formel, $\Box\alpha := 1bwb(\ulcorner \alpha \urcorner)$ und $\Diamond\alpha := \neg \Box \neg \alpha$. Für $\alpha \in \mathcal{L}_{ar}^0$ darf man $\Box\alpha$ bekanntlich lesen als ‘PA + $\neg\alpha$ ist inkonsistent’, $\Box\alpha$ nach Lemma 5.1 hingegen als ‘PA + $\neg\alpha$ ist ω -inkonsistent’. $\Diamond\top$ ($\equiv \neg \Box \perp$) meint demnach ‘PA ($= \text{PA} + \neg \perp$) ist ω -konsistent’. Dies erklärt das Interesse an dem Operator \Box .

Mit $bwb_{\text{PA}}(\alpha)$ gilt gewiss auch $1bwb_{\text{PA}}(\alpha)$ (man wähle $\varphi = \alpha$). Dies lässt sich auch in PA beweisen: $\vdash_{\text{PA}} \Box\alpha \rightarrow \Box\Box\alpha$, für jedes $\alpha \in \mathcal{L}_{ar}^0$. Die Umkehrung gilt nicht. Denn sicher ist $\not\vdash_{\text{PA}} \text{Con}_{\text{PA}}$, doch ist Con_{PA} leicht 1-beweisbar: mit $\varphi(v_0) := \neg \text{bew}_{\text{PA}}(v_0, \perp)$ ist $\vdash_{\text{PA}} \varphi(\underline{n})$ für jedes n , und $\vdash_{\text{PA}} \forall v_0 \varphi \rightarrow \text{Con}_{\text{PA}}$ ist wegen $\forall v_0 \varphi \equiv \text{Con}_{\text{PA}}$ trivial.

Sei $\text{PA}^\Omega := \text{PA} + \Omega$ mit $\Omega := \{\forall x \varphi \mid \varphi \in \mathcal{L}_{ar}^1, \vdash_{\text{PA}} \varphi(\underline{n}) \text{ für alle } n\}$ und $x = v_0$. Wie Satz 5.2 zeigen wird, ist PA^Ω echt Σ_3 , also nicht mehr rekursiv axiomatisierbar.

Lemma 5.1. *Folgende Eigenschaften sind für beliebiges $\alpha \in \mathcal{L}_{ar}^0$ gleichwertig:*

- (i) $1bwb_{\text{PA}}(\alpha)$, (ii) $\vdash_{\text{PA}^\Omega} \alpha$, (iii) $\text{PA} + \neg\alpha$ ist ω -inkonsistent.

Beweis. (i) \Rightarrow (ii) folgt unmittelbar aus den Definitionen. (ii) \Rightarrow (iii): Sei $\vdash_{\text{PA}^\Omega} \alpha$. Nun ist Ω modulo PA konjunktiv abgeschlossen. Also gibt es nach dem Deduktionstheorem ein $\forall x \varphi(x) \in \Omega$ mit $\vdash_{\text{PA}} \forall x \varphi \rightarrow \alpha$ und $\vdash_{\text{PA}} \varphi(\underline{n})$ für alle n . Weil dann offenbar $\vdash_{\text{PA} + \neg\alpha} \exists x \neg \varphi$, ist $\text{PA} + \neg\alpha$ ω -inkonsistent. (iii) \Rightarrow (i): Sei etwa $\vdash_{\text{PA} + \neg\alpha} \beta(\underline{n})$ für alle n , sowie $\vdash_{\text{PA} + \neg\alpha} \exists x \neg \beta(x)$, folglich $\vdash_{\text{PA}} \forall x \beta \rightarrow \alpha$. Mit $\varphi(x) := \neg \alpha \rightarrow \beta(x)$ ist dann $\vdash_{\text{PA}} \varphi(\underline{n})$ für alle n und weil $\forall x \varphi \equiv \alpha \vee \forall x \beta \vdash_{\text{PA}} \alpha$, ist auch $\vdash_{\text{PA}} \forall x \varphi \rightarrow \alpha$. Daher ist α 1-beweisbar. \square

Satz 5.2. *Alle in \mathcal{N} gültigen Σ_3 -Aussagen sind 1-beweisbar. Für jedes derartige α ist sogar $\vdash_{\text{PA}} \alpha \rightarrow \Box \alpha$ (die 1-beweisbare Σ_3 -Vollständigkeit von PA).*

Beweis. Sei $\mathcal{N} \models \alpha = \exists x \forall y \gamma(x, y)$ und $\gamma(x, y) \Sigma_1$. Dann gibt es ein m derart, dass $\mathcal{N} \models \gamma(\underline{m}, \underline{n})$ für alle n . Daher $\vdash_{\text{PA}} \gamma(\underline{m}, \underline{n})$ für alle n , wegen der Σ_1 -Vollständigkeit von PA. Also $\forall y \gamma(\underline{m}, y) \in \Omega$ und mithin $\vdash_{\text{PA}^\Omega} \exists x \forall y \gamma$, oder gleichwertig $1bwb_{\text{PA}}(\alpha)$ nach Lemma 5.1. Diese Argumentation ist wegen der beweisbaren Σ_1 -Vollständigkeit von PA in PA nachvollziehbar, so dass auch $\alpha \vdash_{\text{PA}} \Box \alpha$. \square

$D1$ – $D4$ gelten auch für den Operator $\Box : \mathcal{L}_{ar}^0 \rightarrow \mathcal{L}_{ar}^0$. In der Tat, $D1$ trifft zu wegen $\vdash_{\text{PA}} \alpha \Rightarrow \vdash_{\text{PA}} \Box \alpha \Rightarrow \vdash_{\text{PA}} \Box \alpha$. $D2$ formalisiert ‘ $\vdash_{\text{PA}^\Omega} \alpha, \alpha \rightarrow \beta \Rightarrow \vdash_{\text{PA}^\Omega} \beta$ ’ nach Lemma 5.1, und $D3$ ist eine Anwendung von Satz 5.2 auf die Σ_3 -Aussage $\Box \alpha$. In 7.2 wurden für den Beweis von $D4$ nebst dem Fixpunktlemma nur $D1$ – $D3$ benutzt. Also gilt auch $D4$. Damit überträgt sich fast alles aus 7.2 auf \Box , speziell der Gödelsche Satz 2.2, der jetzt die Formulierung $\not\vdash_{\text{PA}} \neg \Box \perp$ ($\equiv \Diamond \top$) annimmt. Demnach ist die ω -Konsistenz von PA auch mit den erweiterten Mitteln nicht beweisbar. Ferner kann diese nach Satz 5.2 nicht Σ_3 sein. Sie ist der Form nach Π_3 und daher echt Π_3 .

Nebst $\Box \alpha \rightarrow \Box \alpha$ gibt es weitere interessante Interaktionen zwischen \Box und \Box . So ist $\vdash_{\text{PA}} \neg \Box \alpha \rightarrow \Box \neg \Box \alpha$ für alle $\alpha \in \mathcal{L}_{ar}^0$, die Formalisierung von ‘wenn $\not\vdash_{\text{PA}} \alpha$, so ist $\neg \Box \alpha$ 1-beweisbar’ in PA. Dies ist richtig; denn $\not\vdash_{\text{PA}} \alpha$ impliziert $\vdash_{\text{PA}} \varphi(\underline{n})$ für alle n mit $\varphi(x) := \neg \text{bew}_{\text{PA}}(x, \ulcorner \alpha \urcorner)$ und sicher ist $\vdash_{\text{PA}} \forall x \varphi \rightarrow \neg \Box \alpha$, also ist $\neg \Box \alpha$ 1-beweisbar. Hingegen ist $\vdash_{\text{PA}} \neg \Box \alpha \rightarrow \Box \neg \Box \alpha$ i.a. falsch, siehe etwa Beispiel 2(b) Seite 223.

Die Sprache der nunmehr definierten bimodalen Aussagenlogik GD entstehe aus \mathcal{F}_\Box durch Aufnahme eines weiteren Junktors \Box , der syntaktisch wie \Box zu handhaben ist. Axiome von GD seien die von G, formuliert für \Box und auch für \Box , zuzüglich

$$\Box p \rightarrow \Box p, \quad \neg \Box p \rightarrow \Box \neg \Box p.$$

Die Regeln von GD seien dieselben wie für G. Einsetzungen ι nach \mathcal{L}_{ar}^0 seien definiert wie in 7.4, mit der Zusatzklausel $(\Box H)^\iota = \Box H^\iota$ ($= 1bwb_{\text{PA}}(\ulcorner H^\iota \urcorner)$). Nach obigen Ausführungen sind die Axiome und Regeln von GD korrekt, was eine (die leichtere) Hälfte des folgenden bemerkenswerten Satzes von Dzjaparidze (1985) beweist:

Satz 5.3. $\vdash_{\text{GD}} H \Leftrightarrow \vdash_{\text{PA}} H^\iota$ für alle Einsetzungen ι . Auch GD ist entscheidbar.

Durch GD werden also die Interaktionen zwischen bwb_{PA} und $1bwb_{\text{PA}}$ vollkommen erfasst. Ferner überträgt sich auch Satz 4.5. Allerdings hat GD keine adäquate Kripke-Semantik mehr, was das Entscheidungsverfahren kompliziert gestaltet. Diesbezüglich und für Literaturangaben sei jedoch auf [Boo] und [Be3] verwiesen.

Zur Übung empfehlen wir $\Box(\Box p \rightarrow p)$ aus den Axiomen von GD zu beweisen. Also $\vdash_{\text{PA}} \Box(\Box \alpha \rightarrow \alpha)$ für jedes $\alpha \in \mathcal{L}_{ar}^0$, während $\vdash_{\text{PA}} \Box(\Box \alpha \rightarrow \alpha)$ nur im Falle $\vdash_{\text{PA}} \alpha$ richtig ist. *Vorsicht:* GD erweitert G konservativ, also $\not\vdash_{\text{GD}} \Box p \rightarrow p$.

7.6 Modale Operatoren in ZFC

Betrachtungen über Selbstreferenz in ZFC oder ZF sind etwas komplizierter, weil es keine übergeordnete Theorie mehr gibt. Ist ZFC konsistent – wovon wir ausgehen – so ist Con_{ZFC} arithmetisch wahr (in \mathcal{N} gültig), aber in ZFC nicht mehr beweisbar. Es liegt daher nahe, gleich $\text{ZFC}^+ := \text{ZFC} + \text{Con}_{\text{ZFC}}$ zu betrachten. Denn wir wollen doch, dass die Mengentheorie möglichst viele plausible Tatsachen erfasst, aus denen sich vielleicht interessante mengentheoretische Einsichten ergeben.

Wie aber 7.2 lehrt, garantiert die bloße Konsistenzannahme von ZFC noch nicht die tatsächliche Konsistenz von ZFC^+ . Der zweite Unvollständigkeitssatz verbietet zwar $\vdash_{\text{ZFC}} \text{Con}_{\text{ZFC}}$, nicht aber $\vdash_{\text{ZFC}} \neg \text{Con}_{\text{ZFC}}$. Dies hieße, ZFC ginge so weit über gesicherte Erfahrungen mit endlichen Mengen hinaus, dass ihre im eigenen Rahmen formulierte Konsistenz ihren äußerlichen Sinn verlöre. Gewisse Existenzannahmen über große Kardinalzahlen, die unschwer die Konsistenz von ZFC^+ implizieren, müssten dann ad acta gelegt werden. Und man müsste in Kauf nehmen, dass ZFC dann nebst wahren auch äußerlich falsche arithmetische Sätze beweist wie etwa $\neg \text{Con}_{\text{ZFC}}$.

Selbst wenn $\not\vdash_{\text{ZFC}} \neg \text{Con}_{\text{ZFC}}$, könnte immer noch eine der Aussagen aus der Folge $\Box \neg \text{Con}_{\text{ZFC}}, \Box \Box \neg \text{Con}_{\text{ZFC}}, \dots$ in ZFC beweisbar sein. Dies wird erst ausgeschlossen durch die Konsistenzannahme der ω -iterierten Konsistenzenerweiterung ZFC^ω (siehe Seite 220), so dass \mathbf{G} nach Satz 4.3 die Beweislogik von ZFC wäre. Diese Konsistenzannahme ist mit Letzterem sogar äquivalent. Das ist ein Spezialfall des folgenden Satzes, worin $Rf_T = \{\Box \alpha \rightarrow \alpha \mid \alpha \in \mathcal{L}^0\}$ das lokale Reflektionsprinzip bezeichne. Auch Satz 4.3(a) ist ein Korollar des Satzes, denn $(\forall n \in \mathbb{N}) \not\vdash_T \Box^{n+1} \perp$ ist gleichwertig mit der Konsistenz von T^ω . Die Äquivalenz (i) \Leftrightarrow (ii) ist rein beweistheoretischer Natur und heißt auch *Satz von Goryachev*, siehe hierzu [Be2].

Satz 6.1. *Für eine hinreichend ausdrucksstarke Theorie T^4 sind äquivalent*

(i) T^ω ist konsistent, (ii) $T + Rf_T$ ist konsistent, (iii) \mathbf{G} ist die Beweislogik von T .

Beweis. (i) \Rightarrow (ii) indirekt: Sei $T + Rf_T$ inkonsistent. Dann gibt es $\alpha_0, \dots, \alpha_n$ mit $\vdash_T \neg \varphi$ für $\varphi = \bigwedge_{i \leq n} (\Box \alpha_i \rightarrow \alpha_i)$, also auch $\vdash_T \neg \Diamond \varphi$ ($\equiv_T \Box \neg \varphi$). Weil $\vdash_{T^\omega} \neg \Box^{n+1} \perp$, ist nach Beispiel (d) in 7.3 und Lemma 4.1 dann auch $\vdash_{T^\omega} \Diamond R_n^i$ mit $\iota: p_i \mapsto \alpha_i$. Offenbar ist $R_n^i = \varphi$, also $\vdash_{T^\omega} \Diamond \varphi$. Folglich ist T^ω inkonsistent. (ii) \Rightarrow (iii): Der Beweis von Satz 4.2 für PA wie z.B. präsentiert in [Boo], verläuft für T genauso; denn nur an einer Stelle wird PA überschritten: es wird genutzt dass $\mathcal{N} \models Rf_{\text{PA}}$. Die Existenz eines entsprechenden T -Modells ist aber gemäß (ii) gewährleistet. (iii) \Rightarrow (i): $\not\vdash_{\mathbf{G}} \Box^{n+1} \perp$, also $\not\vdash_T \Box^{n+1} \perp \equiv_T \neg \text{Con}_{T^n}$ für alle n . Daher ist T^ω konsistent. \square

⁴⁾ Das heiße hier die Ausführbarkeit der PA nicht überschreitenden Beweisschritte im Solovayschen Satz 4.2 in T , was noch nicht die Beweisbarkeit des Satzes selbst bedeutet.

Modellen V , genauer die Formalisierung dieser Eigenschaft in \mathcal{L}_ϵ . Es besagt dann $\Diamond\alpha (= \neg\Box\neg\alpha)$ offenbar ' $V \models \alpha$ für ein gewisses transitives V '.

Satz 6.3. $\vdash_{Gi} H \Leftrightarrow \vdash_{ZFC} H^i$ für alle Einsetzungen i .

Wir beweisen hier nur die Richtung \Rightarrow , also die Korrektheit. Was die Axiome von Gi betrifft, so genügt wegen der in 7.3 erwähnten Beweisbarkeit von $\Box p \rightarrow \Box\Box p$ aus den übrigen Axiomen von G offenbar der Nachweis von

$$(A) \Box(\alpha \rightarrow \beta) \wedge \Box\alpha \vdash_{ZFC} \Box\beta, \quad (B) \Box(\Box\alpha \rightarrow \alpha) \vdash_{ZFC} \Box\alpha,$$

$$(C) \vdash_{ZFC} \Box(\Box\alpha \rightarrow \Box\beta) \vee \Box(\Box\beta \rightarrow \alpha), \quad \text{für alle } \alpha, \beta \in \mathcal{L}_\epsilon^0.$$

(A) ist trivial, denn die Menge der in allen transitiven Modellen gültigen Aussagen ist sicher MP-abgeschlossen. (B) ist gleichwertig mit (B') $\Diamond\neg\alpha \vdash_{ZFC} \Diamond(\Box\alpha \wedge \neg\alpha)$. Hier der Beweis: Wenn es ein transitives Modell V gibt mit $V \models \neg\alpha$, dann auch ein derartiges V mit minimalem Rang ρV . Wir behaupten $V \models \Box\alpha$. Andernfalls wäre $V \models \Diamond\neg\alpha$, also gibt es ein transitives $U \in V$ mit $U \models \neg\alpha$ und $\rho U < \rho V$, im Widerspruch zur Wahl von V . Das zeigt $V \models \Box\alpha \wedge \neg\alpha$ und damit (B'). Wir beweisen (C) indirekt. Angenommen es existieren transitive Modelle V, W und α, β mit

- (a) $V \models$ 'α gilt in jedem transitiven Modell und $\neg\beta$ gilt in einem solchen Modell',
- (b) $W \models$ 'β gilt in allen transitiven Modellen, (c) $W \models \neg\alpha$.

Hieraus folgt zuerst $\rho W < \rho V$. Denn sei $U \in V$ ein transitives Modell für $\neg\beta$ nach (a). Wäre $\rho V \leq \rho W$, so auch $\rho U < \rho W$. Also gilt nach Lemma 6.2 $W \models$ 'es gibt ein transitives Modell für $\neg\beta$ ', im Widerspruch zu (b). Nun ist $W \models \neg\alpha$ nach (c) und $\rho W < \rho V$. In V gilt also 'es gibt ein transitives Modell für $\neg\alpha$ ' nach dem Lemma, im Widerspruch zu (a). Das beweist (C). Für die Substitutionsregel folgt die Korrektheit wie für G . Auch MN ist trivial korrekt, denn wenn $\vdash_{ZFC} \alpha$, so gilt α natürlich in allen transitiven Modellen.

Eine andere interessante modelltheoretische Interpretation von $\Box\alpha$ ist 'α gilt in allen V_κ '. Hier durchläuft κ alle unerreichbaren Kardinalzahlen. Unter der Annahme, dass es genügend viele solcher κ gibt, ist $Gj := G + \Box(\Box p \wedge p \rightarrow q) \vee \Box(\Box q \rightarrow p)$ nach [So] die adäquate Modallogik für diese Interpretation von \Box . Diese auch mit G.3 bezeichnete Logik ist vollständig bzgl. aller endlichen linearen Ordnungen. Diese



sind sicher Gi -Strukturen, also $Gi \subseteq Gj$. Die Figur zeigt eine Gi -Struktur, auf dem das Zusatzaxiom mit $wp = \{P\}$ und $wq = \emptyset$ leicht widerlegt werden kann. Folglich $Gi \subset Gj$. Aus der endlichen Modelleigenschaft folgt

wie üblich auch die Entscheidbarkeit von Gj . Wir empfehlen dem Leser abschließend, den Korrektheitsbeweis von Gj für diese Interpretation von \Box auszuführen; er ist dem obigen ähnlich. Man nutzt hier nur, dass V_κ ein transitives Modell ist, sowie $V_\kappa \in V_\lambda$ oder $V_\lambda \in V_\kappa$ für beliebige unerreichbare Kardinalzahlen $\kappa \neq \lambda$.

Lösungshinweise zu den Übungen

Abschnitt 1.1

1. Jedes lineare $f \in \mathbf{B}_n$ hat eine *eindeutige* Darstellung der angegebenen Art. Daher ist 2^{n+1} (= Anzahl der $(n+1)$ -gliedrigen Folgen aus $0, 1$) die gesuchte Anzahl.
2. Induktion über α zeigt: Ist ξ echter Anfang von α oder α echter Anfang von ξ , so ist ξ keine Formel.
3. Sei etwa $(\alpha \circ \beta) = (\alpha' \circ' \beta')$. Wäre $\alpha \neq \alpha'$, so wäre α echter Anfang von α' oder umgekehrt. Das ist unmöglich nach Übung 2.
4. Für $\xi \notin \mathcal{F}$ genügt $\mathcal{F} \setminus \{\neg\xi\}$ den Bedingungen der Formeldefinition. Also $\neg\xi \notin \mathcal{F}$.

Abschnitt 1.2

2. $\neg p \equiv p + 1$, $1 \equiv p + \neg p$, $p \leftrightarrow q \equiv p + \neg q$ und $p + q \equiv p \leftrightarrow \neg q$.
3. Induktion über α zeigt $\alpha^{(n)}$ ist monoton, weil mit $f, g \in B$ auch $\vec{x} \mapsto f\vec{x} \wedge g\vec{x}$ und $\vec{x} \mapsto f\vec{x} \vee g\vec{x}$ monoton sind. Induktionsschritt über die Stellenzahl von f zeigt, mit $f \in \mathbf{B}_{n+1}$ sind auch $f_k: \vec{x} \mapsto f(\vec{x}, k)$ monoton, $k = 0, 1$. Werden f_0, f_1 durch α_0 bzw. α_1 repräsentiert, so f durch die Formel $\alpha_0 \vee \alpha_1 \wedge p_{n+1}$.
4. Sei f nicht durch eine Formel in $\{\wedge, \vee, 0, 1\}$ repräsentierbar. Dann ist f nicht monoton. Passende Einsetzung von Konstanten in f liefert die Negation.

Abschnitt 1.3

1. MP ergibt leicht $p \rightarrow q \rightarrow r$, $p \rightarrow q$, $p \models r$. Durch 3-malige Anwendung von (D) folgt hieraus $\models (p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow (p \rightarrow r)$.
4. Sei $X^\perp \vdash \alpha$, also $X \vdash X^\perp \vdash \alpha$. Das ergibt $X \vdash \alpha$ nach (T).
5. $\vdash_0 \subseteq \vdash$: Sei $X \vdash_0 \alpha$, also $X_0 \vdash \alpha$ für ein endliches $X_0 \subseteq X$. Dann auch $X \vdash \alpha$.

Abschnitt 1.4

1. $X \cup \{\neg\alpha \mid \alpha \in Y\} \vdash \perp \Rightarrow X \cup \{\neg\alpha_0, \dots, \neg\alpha_n\} \vdash \perp$, für gewisse $\alpha_0, \dots, \alpha_n \in Y$. Das ergibt $X \vdash (\bigwedge_{i \leq n} \neg\alpha_i) \rightarrow \perp \equiv \bigvee_{i \leq n} \alpha_i$.
2. Lemma 4.4 wie folgt ergänzen: $X \vdash \alpha \vee \beta \Leftrightarrow X \vdash \alpha$ oder $X \vdash \beta$.

4. Sei $X \not\vdash \varphi$, $X \vdash' \varphi$ und $Y \supseteq X \cup \{\neg\varphi\}$ maximal konsistent in \vdash , sowie σ definiert durch $p^\sigma = \top$ für $p \in Y$ und $p^\sigma = \perp$ sonst. Simultane Induktion über α , $\neg\alpha$ zeigt $\alpha \in Y \Rightarrow \vdash \alpha^\sigma$ und $\alpha \notin Y \Rightarrow \vdash \neg\alpha^\sigma$. Folglich $\vdash \neg\varphi^\sigma$. Daher $\vdash' \neg\varphi^\sigma$ und so $X^\sigma \vdash' \neg\varphi^\sigma$. Wegen $X \vdash' \varphi$ ist auch $X^\sigma \vdash' \varphi^\sigma$. Daher $\vdash' \alpha$ für alle α nach $(\neg 1)$.
5. Unter allen Konsequenzen mit den Eigenschaften $(\wedge 1)$ – $(\neg 2)$ gibt es eine kleinste, \vdash , und \vdash ist finitär (Übung 5 in 1.3). Weil \vdash maximal ist, kann nur $\vdash = \models$ gelten.

Abschnitt 1.5

1. Man muss den Formeln unter Beispiel 1 nur die Formeln $\{p_{ab} \mid a \leq_0 b\}$ hinzufügen.
2. Sei U trivial, $K \subseteq I$ koendlich, $K \notin U$, also $E = I \setminus K \in U$. Für jede Zerlegung $E = E_0 \cup E_1$ ist $E_0 \in U$ oder $E_1 \in U$. So erschließe man $\{i_0\} \in U$ für ein $i_0 \in I$.

Abschnitt 1.6

2. Kalküle mit MP als einziger Regel und A1, A2 unter den Axiomen erfüllen das Deduktionstheorem (Beweis wie Lemma 6.3). Für maximal konsistentes X beweist man $X \vdash \alpha \rightarrow \beta \Leftrightarrow$ wenn $X \vdash \alpha$ so $X \vdash \beta$.
3. Man wende das Lemma von Zorn an auf $H = \{Y \supseteq X \mid Y \not\vdash \alpha\}$.
4. Sei $X \not\vdash \alpha_0$ und X o.B.d.A. α_0 -maximal (Übung 3). Definiert man $w \models X$ durch $w \models p \Leftrightarrow p \in X$, so gilt: $X \vdash \alpha \rightarrow \beta \Leftrightarrow (X \vdash \alpha \Rightarrow X \vdash \beta)$.

Abschnitt 2.1

1. Es gibt 10 wesentlich 2-stellige Boolesche Funktionen f . Die Menge der entsprechenden 10 Gruppoide $(\{0, 1\}, f)$ zerfällt in 5 Paare isomorpher Algebren.
4. Man ordne dem Element $a \in 2^I$ die Teilmenge $I_a = \{i \in I \mid a_i = 1\} \subseteq I$ zu.

Abschnitt 2.2

2. Induktion über t . Klar für Primterme oder falls ζ erster Buchstabe von t ist. Sonst ist $t = ft_1 \cdots t_n$ und ζ kommt in der Zeichenfolge $t_1 \cdots t_n$ vor, also in einem t_i und ist erster Buchstabe eines Subterms in t_i gemäß Induktionsannahme.
3. (a): \mathcal{E} gilt für Primterme. Annahme: \mathcal{E} gilt nicht für $f\vec{t}$. Dann ist entweder $f\vec{t} = gs_1 \dots s_m \xi$ oder $f\vec{t}\xi = gs_1 \dots s_m$ für einen Term $gs_1 \dots s_m$ und eine Zeichenfolge $\xi \neq \emptyset$. In jedem Falle $g = f$ und damit $m = n$. Die Induktionsannahme $\mathcal{E}t_1, \dots, \mathcal{E}t_n$ ergibt schrittweise $t_1 = s_1, \dots, t_n = s_n$. Damit ist $\xi = \emptyset$ im Widerspruch zu $\xi \neq \emptyset$. (b) folgt leicht aus (a).

Abschnitt 2.3

1. $\forall x\alpha, \forall x(\alpha \rightarrow \beta) \models \alpha \rightarrow \beta, \alpha \models \beta$. Sodann hintere Generalisierung.
2. Sei $\mathcal{M}_{xy}^{cd} \models \varphi \wedge \varphi \frac{y}{x}$ mit $c \neq d$. Dann gilt $\mathcal{M}_x^a \models \exists y(\varphi \frac{y}{x} \wedge x \neq y)$ für alle $a \in A$.
3. Nach Satz 3.1 und Satz 3.5 ist $\mathcal{A} \models \alpha(x) [a] \Leftrightarrow \mathcal{A}' \models \alpha(x) [a] \Leftrightarrow \mathcal{A}' \models \alpha \frac{a}{x}$.
4. (b): $\exists_n \wedge \neg \exists_m$ ist für $n \leq m$ äquivalent zu $\bigvee_{k=n}^m \exists_{=k}$, für $n > m$ zu $\exists_{=0}$ ($\equiv \perp$).

Abschnitt 2.4

1. $\alpha \equiv \beta \Rightarrow \models \forall \vec{x}(\alpha \leftrightarrow \beta) \Rightarrow \models (\alpha \leftrightarrow \beta) \frac{\vec{t}}{\vec{x}} (= \alpha \frac{\vec{t}}{\vec{x}} \leftrightarrow \beta \frac{\vec{t}}{\vec{x}})$.
2. $\neg \forall x(x \triangleleft y \rightarrow \alpha) \equiv \exists x \neg(x \triangleleft y \rightarrow \alpha) \equiv \exists x(x \triangleleft y \wedge \neg \alpha)$ (Ersetzungstheorem).
3. O.B.d.A. ist $\alpha \equiv \forall \vec{y}\alpha'(\vec{x}, \vec{y})$ und $\beta \equiv \forall \vec{z}\beta'(\vec{x}, \vec{z})$ mit disjunkten Tupeln $\vec{x}, \vec{y}, \vec{z}$.

Abschnitt 2.5

2. \Rightarrow : $X \models \varphi \rightarrow \beta \Leftrightarrow X, \varphi \models \beta$ und (e) Seite 62. \Leftarrow : (10) in 2.4.
3. Beweise zuerst $T_\alpha := \{\beta \in \mathcal{L}^0 \mid T, \alpha \models \beta\}$ ist eine Theorie und dann $T_\alpha = T + \alpha$.

Abschnitt 2.6

1. Man folge dem Beweis von Satz 6.1 (beachte $f\vec{t} = y \equiv_{T_f} \delta_f(\vec{t}, y)$). Für den „nur dann“-Teil beachte man $(y = f\vec{x} \leftrightarrow \delta(\vec{x}, y))^\forall \models \forall \vec{x} \exists! y \delta(\vec{x}, y)$.
2. In $(\mathbb{N}, 0, 1, \mathbf{S}, +, \cdot)$ gelten $x = 0 \leftrightarrow x + x = x$, $x = 1 \leftrightarrow x \neq 0 \wedge x \cdot x = x$, sowie $y = \mathbf{S}x \leftrightarrow y = x + 1$ ($\equiv \exists z(y = x + z \wedge z + z \neq z \wedge z \cdot z = z)$).
3. Sei $xy = xz = e$ (\circ, \models werden nicht geschrieben) und ein y' mit $yy' = e$ gewählt. Dann ist auch $yx = (yx)(yy') = y(xy)y' = yey' = e$. Analog folgt $zx = e$. Also $y = z$, denn $y = y(xz) = (yx)z = ez = (zx)z = z(xz) = ze = z$.
4. Wäre $<$ definierbar, wäre $<$ unter jedem Automorphismus von $(\mathbb{Z}, 0, +)$ invariant. Das ist nicht der Fall für den Automorphismus $n \mapsto -n$ (Methode von Padoa).

Abschnitt 3.1

1. Sei $X \vdash \alpha \frac{t}{x}$. Dann ist $X, \forall x \neg \alpha \vdash \alpha \frac{t}{x}, \neg \alpha \frac{t}{x}$. Daher $X, \forall x \neg \alpha \vdash \exists x \alpha$. Gewiß ist auch $X, \neg \forall x \neg \alpha \vdash \exists x \alpha$. Also $X \vdash \exists x \alpha$ nach ($\neg 2$).
2. Sei $\alpha' := \alpha \frac{y}{x}$, $u \notin \text{var } \alpha$, $u \neq y$. Dann ist $\forall x \alpha \vdash \alpha' \frac{u}{y}$ ($= \alpha \frac{u}{x}$) nach ($\forall 1$). Also $\forall x \alpha \vdash \forall y \alpha'$ ($= \forall y \alpha \frac{y}{x}$) nach ($\forall 2$).

Abschnitt 3.2

1. Modellexistenzssatz und Übung 4 in 3.1.
2. Es gilt $t^{\mathfrak{T}} = t$ (Induktion über t). Danach beweise man $(*) \mathfrak{T} \models \forall \vec{x} \varphi \Leftrightarrow \mathfrak{T} \models \varphi^{\vec{t}}$ für alle $\vec{t} \in \mathcal{T}^n$ (φ offen). Es gilt $\mathcal{M} \models \tilde{X} := \{\varphi^{\vec{t}}_{\vec{x}} \mid \forall \vec{x} \varphi \in X, \vec{t} \in \mathcal{T}^n\}$. Induktion über \wedge, \neg zeigt $\mathcal{M} \models \varphi \Leftrightarrow \mathfrak{T} \models \varphi$. Also $\mathfrak{T} \models \tilde{X}$ und so $\mathfrak{T} \models X$ nach $(*)$.

Abschnitt 3.3

2. $\vdash_{\text{PA}} \forall z[(x + (y + z) = (x + y) + z)]$ folgt durch Induktion über z . Zum Beweis von $\vdash_{\text{PA}} \forall x x + y = y + x$ benötigt man $\vdash_{\text{PA}} \forall y 0 + y = y$ und $\vdash_{\text{PA}} \forall y x + Sy = Sx + y$ (Übung 1). Induktion über die jeweils quantifizierte Variable.
3. (a): Sei $\varphi := (\forall y < x) \alpha^y_x$ und $\vdash_{\text{PA}} \forall x(\varphi \rightarrow \alpha)$. Um $\vdash_{\text{PA}} \forall x \alpha$ zu zeigen, genügt es $\vdash_{\text{PA}} \forall x \varphi$ induktiv über x zu beweisen, weil $\vdash_{\text{PA}} \varphi^{\frac{Sx}{x}} \rightarrow \alpha$. Trivial gilt $\vdash_{\text{PA}} \varphi^0_x$. Der Induktionsschritt $\varphi \vdash_{\text{PA}} \varphi^{\frac{Sx}{x}}$ folgt wegen $y < Sx \equiv_{\text{PA}} y \leq x$ aus $\vdash_{\text{PA}} \varphi \rightarrow \alpha$. (b): Folgt aus (a) durch Kontraposition, also durch Anwendung von IS auf $\neg \varphi$. (c): Für $\varphi := (\forall x < v) \exists y \gamma \rightarrow \exists z (\forall x < v) (\exists y < z) \gamma$ gilt $\vdash_{\text{PA}} \varphi^0_v$ und man beweist unschwer $\varphi \vdash_{\text{PA}} \varphi^{\frac{Sv}{v}}$. Dies liefert die Behauptung gemäß IS.

Abschnitt 3.4

1. $X = T \cup \{v_i \neq v_j \mid i \neq j\}$ ist erfüllbar, weil jede endliche Teilmenge dies ist.
2. $X = Th\mathcal{A} \cup \{v_{n+1} < v_n \mid n \in \mathbb{N}\}$ hat ein Modell mit unendlich absteigender Kette.
4. Sei $u \in \text{Var}$. Folgende Formelmengen (mit Symbolen \mathbf{a} für die $a \in V$) ist konsistent:
 $Th(V, \in^V) \cup \{\mathbf{a} \in \mathbf{b} \mid a, b \in V, a \in^V b\} \cup \{\mathbf{a} \notin \mathbf{b} \mid a, b \in V, a \notin^V b\} \cup \{\mathbf{a} \in u \mid a \in V\}$.

Abschnitt 3.5

1. $\beta \in T' \Leftrightarrow \alpha \rightarrow \beta \in T$. Wesentlich ist, dass T' zur selben Sprache gehört wie T .
2. (ii) \Rightarrow (iii): Ist $T + \{\alpha_i \mid i \in \mathbb{N}\}$ nichtendliche Erweiterung, kann $\bigwedge_{i \leq n} \alpha_i \not\vdash_T \alpha_{n+1}$ angenommen werden. Sei T_n Vervollständigung von $T + \bigwedge_{i \leq n} \alpha_i + \neg \alpha_{n+1}$. Dann ist $T_m \neq T_n$. (iii) \Rightarrow (ii): Annahme $T + \alpha_0, T + \alpha_1, \dots$ sei eine unendliche Folge paarweise verschiedener Vervollständigungen von T . Dann ist $T + \{\neg \alpha_n \mid n \in \mathbb{N}\}$ eine unendliche Erweiterung von T , weil $T + \bigwedge_{n \leq \nu} \neg \alpha_n \not\vdash \neg \alpha_{n+1}$. (ii) \Rightarrow (i): Man zeigt leicht, jede konsistente Theorie ist identisch mit dem Durchschnitt ihrer Vervollständigungen. Das gilt speziell für die Erweiterungen von T .
3. $\alpha \in T \Leftrightarrow \alpha \in T_i$ für alle $i \leq n$; dabei seien T_0, \dots, T_n alle Vervollständigungen von T . Diese sind sämtlich axiomatisierbar, also entscheidbar.

Abschnitt 3.6

1. Es ist $x = y \not\models \forall x x = y$. Wegen $\vdash \subseteq \models$ gilt daher auch nicht $x = y \vdash \forall x x = y$.
2. (a): Seien $(\varphi_n)_{n \in \mathbb{N}}$ und $(\mathcal{A}_n)_{n \in \mathbb{N}}$ effektive Aufzählungen aller Aussagen bzw. aller endlichen T -Modelle. Man notiere im n -ten Schritt alle φ_i für $i \leq n$ mit $\mathcal{A}_n \models \varphi_i$.
(b): Seien $(\alpha_n)_{n \in \mathbb{N}}$ und $(\beta_n)_{n \in \mathbb{N}}$ effektive Aufzählungen der in T beweisbaren bzw. widerlegbaren Aussagen. Jedes $\alpha \in \mathcal{L}^0$ kommt in genau einer dieser Folgen vor.
3. Auch Bedingung (ii) aus Übung 2 ist erfüllt, weil nur endliche viele Axiome in einer endlichen Struktur auf ihre Gültigkeit getestet werden müssen.

Abschnitt 3.7

1. Für **H**: Sei h Homomorphismus: $ht^{A,w} = t^{\beta,hw}$ mit $x^{hw} = hx^w$. Für **S** siehe (3) in 2.3. Für **P**: Sei $\mathcal{B} = \prod_{i \in I} \mathcal{A}_i$. Dann ist $t^{\mathcal{B},w} = (t^{\mathcal{A}_i,w_i})_{i \in I}$ mit $x^w = (x^{w_i})_{i \in I}$.
2. In \mathcal{L}_Q^1 ist $\alpha_{\text{üa}} := \exists x x = x$ eine Aussage mit $\mathcal{A} \models \alpha_{\text{üa}} \Leftrightarrow A$ ist überabzählbar. In \mathcal{L}_{II} formalisiere man die Aussage ‘es gibt eine lückenlose Ordnung ohne größtes Element’. Eine solche ist immer überabzählbar.
3. Sei α die Konjunktion aller Axiome für geordnete Körper unter Einschluss des in \mathcal{L}_{II} leicht formulierbaren Stetigkeitsaxioms Seite 86. Diese legt den Körper der reellen Zahlen bis auf Isomorphie eindeutig fest. Sei ferner β die in \mathcal{L}_{II} ebenfalls leicht formulierbare Aussage ‘Jede überabzählbare Teilmenge des Trägers \mathbb{R} ist zu \mathbb{R} gleichmächtig’. Es gibt eine $\gamma := \alpha \wedge \beta$ erfüllende \mathcal{L}_{II} -Struktur genau dann, wenn CH gilt. Andernfalls ist $\neg \gamma$ eine Tautologie.

Abschnitt 4.1

1. Sei $\mathcal{B} = \prod_{i \in I} \mathcal{A}_i$. Es genügt, $(\star) \mathcal{A}_i \models \alpha[w_i] \Leftrightarrow \beta \models \alpha[w]$ mit $x^w = (x^{w_i})_{i \in I}$ induktiv für Basis-Hornformeln zu beweisen. Beachte dabei $t^{\mathcal{B},w} = (t^{\mathcal{A}_i,w_i})_{i \in I}$.
(\star) ergibt leicht die Induktionsschritte über \wedge, \forall, \exists .
3. Eine Menge positiver Hornformeln hat stets ein 1-elementiges Modell.

Abschnitt 4.2

1. Für $w_1 \models p_1, p_3, \neg p_2$ und $w_2 \models p_2, p_3, \neg p_1$ ist $w_1 \models \mathcal{P}$ und $w_2 \models \mathcal{P}$, aber es gibt keine Belegung $w \leq w_1, w_2$ mit $w \models \mathcal{P}$.
2. Für beliebiges $w \models \mathcal{P}$ folgt $w \models p_{m,n,m+n}$ induktiv über n , also $w_{\mathcal{P}} \leq w$.
3. (a) Resolutionssatz. (b) $w_{\mathcal{P}} \models \neg p_{n,m,k}$ für $k \neq n + m$.

Abschnitt 4.3

2. \Rightarrow : Annahme $x_i \in \text{var } t_j$. Dann $x_i^\sigma = t_j \neq t_j^\sigma = x_i^{\sigma^2}$.
3. Sei ω Unifikator von $K_0 \cup K_1$, also $K_0^\omega = K_1^\omega$. Sei $x^{\omega'} = x^{\rho\omega}$ für $x \in \text{var } K_0$ und $x^{\omega'} = x^\omega$ sonst. Dann ist $K_0^{\rho\omega'} = K_0^{\rho^2\omega} = K_0^\omega$ (beachte $\rho^2 = \iota$), sowie $K_1^{\omega'} = K^\omega$.

Abschnitt 4.4

1. Seien K_0, K_1 zerlegt wie in der Definition von UR und sei ρ ein Separator von K_0, K_1 , sowie ω' definiert wie im Hinweis zu Übung 3 in 4.3.
2. Man vereinige \mathcal{P}_g und \mathcal{P}_h und füge dem Resultat noch folgende Klauseln hinzu:
 $r_f(\vec{x}, 0, u) := r_g(\vec{x}, u)$ und $r_f(\vec{x}, Sy, u) := r_f(\vec{x}, y, v), r_h(\vec{x}, y, v, u)$.
3. Man füge den Programmen noch $r_f\vec{x}u := r_{g_1}\vec{x}y_1, \dots, r_{g_m}\vec{x}y_m, r_h\vec{y}u$ hinzu.

Abschnitt 5.1

3. Seien $a, b, c \in \mathbb{R}$ mit $a < b, c$. Die lineare Funktion $x \mapsto \frac{a-c}{a-b} \cdot x + \frac{c-b}{a-b} \cdot a$ vermittelt einen Automorphismus des (reellen) Intervalls $[a, b]$ auf das Intervall $[a, c]$.
4. O.B.d.A. sei $A \cap B = \emptyset$. Es genügt zu zeigen $D_{el}\mathcal{A} \cup D_{el}\mathcal{B}$ ist konsistent.
5. (a): $\{t^A \mid t \in \mathcal{T}_E\}$ ist abgeschlossen gegenüber allen f^A , ist also identisch mit dem Träger von \mathcal{A} . (b): $\mathcal{B} \models T + D_E\mathcal{A}$ lässt sich zu einem $\mathcal{B}' \models T + D\mathcal{A}$ expandieren: Für $a \in A \setminus E$ mit $a = t^A$ und $t \in \mathcal{T}_E$ gemäß (a) sei $a^{\mathcal{B}'} = t^{\mathcal{B}} (= t^A)$.

Abschnitt 5.2

2. IS auf $\alpha(x_n) = \forall x_0 \dots x_{n-1} (\bigwedge_{i < n} \mathbf{S}x_i = x_{i+1} \rightarrow x_n \neq x_0)$ anwenden.
3. Sei $a \in G \models T$ und $\frac{a}{n}$ das Element mit $n \frac{a}{n} = a$, sowie $\frac{m}{n} : a \mapsto m \frac{a}{n}$ für $\frac{m}{n} \in \mathbb{Q}$. Dadurch wird G zur Vektorgruppe eines \mathbb{Q} -Vektorraums.
4. (b): Behauptung zuerst für beliebige Konjunktion aus den α_i und ihren Negationen beweisen. Beachte $\alpha_i \wedge \alpha_j \equiv_T \perp$ für $i \neq j$ und $\vdash_T \bigvee_{i \leq m} \alpha_i$.

Abschnitt 5.3

1. $(\mathcal{A}, \vec{a}) \sim_k (\mathcal{B}, \vec{b}) \Leftrightarrow a_i \mapsto b_i \ (i = 1, \dots, n)$ ist partieller Isomorphismus.
2. In Runde 1 spiele II beliebig, danach gemäß den Gewinnstrategien für Modelle von SO_{01} bzw. SO_{10} in den beiden Zerlegungshälften.

3. Falls I mit $a \in A$ beginnt und rechts und links von a mindestens 2^{n-1} Elemente verbleiben, wähle II entsprechend. Sonst mit Elementen derselben Distanz vom linken bzw. rechten Randelement antworten.
4. Fallunterscheidung ob $\mathcal{A} \models \text{SO}$ unendlich oder endlich ist. Im ersten Falle folgt die Behauptung aus der Vollständigkeit aller Theorien $\text{SO}_{ij} \cup \{\exists_i \mid i > 0\}$.

Abschnitt 5.4

1. Jeder Halbverband (A, \cap) ist durch $a \mapsto \{x \in A \mid x \leq a\}$ in den Mengenhalfverband $(\mathfrak{P}A, \cap)$ einbettbar. Dabei sei \leq die Halbordnung von (A, \cap) , Seite 39.
3. Sei A geordnet. Ersetzt man jedes $a \in A$ durch ein Exemplar von $(\mathbb{Z}, <)$ bzw. von $(\mathbb{Q}, <)$, so entsteht eine diskrete Ordnung bzw. eine dichte Ordnung $B \supseteq A$.
4. Sei $\mathcal{A}_0 \models T_0$. Wähle \mathcal{A}_1 mit $\mathcal{A}_0 \subseteq \mathcal{A}_1 \models T_1$, \mathcal{A}_2 mit $\mathcal{A}_1 \subseteq \mathcal{A}_2 \models T_0$ usw. Das ergibt eine Kette $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \dots$ mit $\mathcal{A}_{2i} \models T_0$, $\mathcal{A}_{2i+1} \models T_1$. Dann ist $\bigcup_{i \in \mathbb{N}} \mathcal{A}_{2i} = \bigcup_{i \in \mathbb{N}} \mathcal{A}_{2i+1} \models T$. Also sind T, T_i modellverträglich.
5. Die Vereinigung S einer Kette von mit T modellverträglichen induktiven Theorien ist wieder induktiv. S hat denselben \forall -Teil wie T , ist mit T also auch modellverträglich. Also gibt es nach dem Zornschen Lemma eine maximale, und nach Übung 4 damit auch eine größte Theorie dieser Art.

Abschnitt 5.5

1. Für $i \neq 0$ oder $j \neq 0$ besitzt DO_{ij} Modelle $\mathcal{A} \subseteq \mathcal{B}$ mit $\mathcal{A} \not\models \mathcal{B}$.
2. (a) Lindströms Kriterium. T ist \aleph_1 -kategorisch, denn ein T -Modell kann als \mathbb{Q} -Vektorraum verstanden werden. (b) Jedes T_0 -Modell G ist in ein T -Modell H einbettbar; man gewinnt ein solches H , indem auf der Menge aller Paare $\frac{a}{n}$ mit $a \in G$ und $n \in \mathbb{Z} \setminus \{0\}$ eine geeignete Äquivalenzrelation definiert wird.
3. Eindeutigkeit folgt ähnlich wie die der Modellvervollständigung.
4. Der algebraische Abschluß $\overline{\mathcal{F}_p}$ des Primkörpers \mathcal{F}_p der Charakteristik p hat die Darstellung $\overline{\mathcal{F}_p} = \bigcup_{n \geq 1} \mathcal{F}_{p^n}$, wobei \mathcal{F}_{p^n} den endlichen Körper aus p^n Elementen bezeichnet. Ferner gilt eine in allen a.a. Körpern mit Primzahlcharakteristik gültige Aussage bereits in allen a.a. Körpern.

Abschnitt 5.6

1. Seien $\mathcal{A}, \mathcal{B} \models \mathbf{ZG}_0$, $\mathcal{A} \subseteq \mathcal{B}$. Dann auch $\mathcal{A}', \mathcal{B}'$, denn das Prädikat $m|$ hat in \mathbf{ZG} eine \forall - und eine \exists -Definition. Also $\mathcal{A}' \subseteq_{ec} \mathcal{B}'$, mithin $\mathcal{A} \subseteq_{ec} \mathcal{B}$.
2. Induktiv über quantorenfreies $\varphi = \varphi(x)$ ergibt sich: für jedes $\mathcal{A} \models \mathbf{RCF}^\circ$ ist $\varphi^{\mathcal{A}}$ oder $(\neg\varphi)^{\mathcal{A}}$ endlich, was für $\alpha(x)$ nicht der Fall ist.
4. Die Gruppe $2\mathbb{Z}$ ist Substruktur der geordneten Gruppe \mathbb{Z} , aber nicht $2\mathbb{Z} \preceq \mathbb{Z}$.

Abschnitt 5.7

1. Sei $\{\mathcal{A}_i \mid i \in I\} = \{\mathcal{A}_0, \dots, \mathcal{A}_n\}$ und $I_\nu = \{i \in I \mid \mathcal{A}_i = \mathcal{A}_\nu\}$, also $I = I_0 \cup \dots \cup I_n$. Damit gehört genau eines der I_ν zu F (Induktion über n).
3. Behauptung indirekt beweisen. Seien I, J_α, F definiert wie in Korollar 7.3, sowie $\mathcal{A}_i \in \mathbf{K}$ und $w_i: AV \rightarrow A_i$ derart, dass $w_i\alpha \in D^{\mathcal{A}_i}$ für $\alpha \in i$, $w_i\varphi \notin D^{\mathcal{A}_i}$, $C := \prod_{i \in I}^F \mathcal{A}_i$ ($\in \mathbf{K}$) und $w = (w_i)_{i \in I}$. Dann ist $wX \subseteq D^C$, also $X \not\models_C \varphi$.
4. O.B.d.A. ist $\mathcal{A} = \mathcal{Q}$ und $\mathcal{Q} \subseteq \mathcal{B} \subseteq \mathcal{Q}^I$ für gewisses I nach dem Stoneschen Repräsentationssatz (siehe 2.1). $\mathcal{Q} \models \alpha \Rightarrow \mathcal{Q}^I \models \alpha \Rightarrow \mathcal{B} \models \alpha$ nach Satz 7.2.

Abschnitt 6.1

1. $\Rightarrow: \chi_{\text{graph} f} = \delta|f\vec{a} - b|$. $\Leftarrow: f\vec{a} = \mu b[f\vec{a} = b]$. Ferner: $f\vec{a} = \mu b \leq h\vec{a}[f\vec{a} = b]$.
3. Sei $s_m := \sum_{i \leq m} i$ und damit $\wp(a, b) = s_{a+b} + a$. *Injektivität*: Sei $\wp(a, b) = \wp(a', b')$. Angenommen $a+b \neq a'+b'$ und o.B.d.A. $a+b < a'+b'$. Dann $\wp(a, b) < \wp(a, b) + b + 1 = s_{a+b} + a + b + 1 = s_{a+b+1} \leq s_{a'+b'} \leq \wp(a', b')$. Also $a + b = a' + b'$ und so $a = \wp(a, b) - s_{a+b} = \wp(a', b') - s_{a'+b'} = a'$, also auch $b = b'$. *Surjektivität*: Da $0 = \wp(0, 0) \in \text{ran } \wp$, genügt zu zeigen $\wp(a, b) + 1 \in \text{ran } \wp$ für alle a, b . Im Falle $b = 0$ ist $\wp(a, 0) + 1 = s_{a+0} + a + 1 = s_{a+1} = \wp(0, a+1)$. Für $b > 0$ ist $\wp(a+1, b-1) = s_{a+1+b-1} + a + 1 = s_{a+b} + a + 1 = \wp(a, b) + 1$. Dieser Beweis bestätigt auch die Korrektheit der Paarkodierungs-Figur.
4. \Rightarrow : Sei $M = \{b \in \mathbb{N} \mid \exists a Rab\}$, R rekursiv, $c \in M$ fest gewählt. Sei $fn = b$, falls $(\exists a \leq n) n = \wp(a, b) \ \& \ Rab$, und $fn = c$ im anderen Falle. Dann gilt $M = \text{ran } f$. \Leftarrow : $M = \{b \in \mathbb{N} \mid (\exists a \in \mathbb{N}) fa = b\}$ und Übung 1.

Abschnitt 6.2

1. Es sei $\alpha_0, \alpha_1, \dots$ eine rekursive Aufzählung von X . Nach Übung 2 in 6.1 ist dann $\{\beta_n \mid n \in \mathbb{N}\}$ mit $\beta_n = \underbrace{\alpha_n \wedge \dots \wedge \alpha_n}_n$ rekursiv und ein Axiomensystem für T .

3. Sei $\Phi_n = (\varphi_0, \dots, \varphi_n)$ ein Beweis von $\varphi = \varphi_n$ in $T + \alpha$ und seien Beweise Φ'_k für $\alpha \rightarrow \varphi_k$ zu $\Phi_i = (\varphi_0, \dots, \varphi_i)$ für alle $i < n$ schon konstruiert. Man definiere einen Beweis Φ'_n für $\alpha \rightarrow \varphi$ durch p.r. Fallunterscheidung entsprechend dem Beweis von Lemma 1.6.3.
4. Zeige zuerst die Menge P der Primaussagen aus Tr_0 ist p.r. Dazu konstruiere eine p.r. Funktion f mit $f\dot{t} = t^N$ falls $\text{var } t = \emptyset$. Schließlich beachte man

$$\alpha \in Tr_0 \Leftrightarrow \alpha \in P \vee (\exists \beta, \gamma < \alpha) [\alpha = \beta \wedge \gamma \ \& \ \beta, \gamma \in Tr_0 \vee \alpha = \neg \beta \ \& \ \beta \notin Tr_0].$$

Abschnitt 6.3

1. $\exists \vec{x} \alpha \equiv_N \exists y (\exists x_1 \leq y) \dots (\exists x_n \leq y) \alpha$ mit $y \notin \text{var } \alpha$. Für eine Belegung \vec{a} von \vec{x} belege y mit $\max\{a_1, \dots, a_n\}$. Analog ist $\forall \vec{x} \alpha \equiv_N \forall y (\forall x_1 \leq y) \dots (\forall x_n \leq y) \alpha$
2. $(\forall x < v) \exists y \alpha \equiv_{PA} \exists z (\forall x < v) (\exists y < z) \alpha$ nach Übung 3(c) in **3.3**.

Abschnitt 6.4

1. $<$ -Induktion über $s = a + b$. Richtig für $a = b = 1$ mit $x = 0, y = 1$. Sei $s > 2$. Dann ist $a \neq b$. Falls $a > b$ ist auch $a - b \perp b$. Da $(a - b) + b < s$, gibt es nach Induktionsannahme $x, y \in \mathbb{N}$ mit $x(a - b) + 1 = yb$. Also $xa + 1 = y'b$ mit $y' = x + y$. Falls $a < b$ ist $a \perp b - a$ und man schließt analog.
2. (a): $p \nmid a \Rightarrow a \perp p \Rightarrow \exists xy \, xa + 1 = yp \Rightarrow \exists xy \, b = ybp - xab \Rightarrow p \mid b$. (b): führe $p \mid \text{kgV}\{a_\nu \mid \nu \leq n\}$ und $(\forall \nu \leq n) p \nmid a_\nu$ zum Widerspruch. (c) folgt leicht aus (b).
4. (a): Beweise dies zuerst für x statt \vec{x} . (b): Zeige $\text{sb}_x(\ulcorner \varphi \urcorner, x) = \ulcorner \varphi \urcorner$ für $x \notin \text{frei } \varphi$.

Abschnitt 6.5

3. Klar falls $T + \Delta$ inkonsistent ist. Andernfalls ist $T + \Delta$ nach **2.6** konservative Erweiterung von T und $\alpha \in T + \Delta \Leftrightarrow \alpha^{rd} \in T$. Da α^{rd} aus α effektiv hergestellt werden kann, ist mit T auch $T + \Delta$ entscheidbar.
4. $f \in \mathbf{F}_1$ mit $fa = (a)_{\text{last}}$ falls a einen Beweis in \mathbf{Q} kodiert und $fa = (0 = 0)'$ sonst, ist p.r. und zählt \mathbf{Q} rekursiv auf.

Abschnitt 6.6

1. Sei $T \supseteq T_1$ konsistent. $S = \{\alpha \in \mathcal{L}_0 \mid \alpha^P \in T^\Delta\}$ ist eine Theorie, die T_0 konsistent erweitert und daher unentscheidbar. Dasselbe gilt für T^Δ und T .
4. $n \in m \rightarrow n < m$, sowie $m \cup \{n\} = m + 2^n$ falls $n \notin m$. Für den Nachweis von Fin und IS_\in wird die $<$ -Induktion benötigt.

Abschnitt 6.7

1. Hinweis zu Übung 1 in **6.3** führt auch im Induktionsschritt zum Ziel.
2. Δ_0 ist r.a. aber Δ_1 nicht (Bemerkung 2 in **6.3**). \dot{Q} ist Σ_1 aber nicht Δ_1 .
3. Der Hinweis zu Übung 3 in **3.3** zeigt, dass $<$ -Induktion in $I\Delta_0$ durch Standard-Induktion über x für $\varphi := (\forall y < x) \alpha_x^y$ bewiesen wird. Da das Minimalschema durch Kontraposition folgt, benötigen wir hierfür Induktion für $\neg\varphi$. Beides sind Δ_0 -Formeln, sofern α Δ_0 ist.

Abschnitt 7.1

1. Für rest wähle man $\varphi(a, b, r) := (\exists q \leq a)(a = b \cdot q + r \wedge r < b) \vee b = r = 0$ und beweise $\vdash_{\text{PA}} \exists r \varphi(a, b, r)$ durch Induktion über a . Nutze die Axiome von \mathbf{N} in **6.3**.
2. (a): $<$ -Induktion. (b): Hinweis zu Übung 1 in **6.4** in PA formalisieren.
4. Für $\Box_{T+\alpha} \varphi \vdash_T \Box_T (\alpha \rightarrow \varphi)$ nutze man Übung 3 in **6.2**.

Abschnitt 7.2

1. $\vdash_T \Box \alpha \rightarrow \alpha \Rightarrow \vdash_{T'} \neg \Box \alpha \Rightarrow \vdash_{T'} \text{Con}_{T'}$, weil nach (5) $\text{Con}_{T'} \equiv_T \neg \Box \neg \neg \alpha \equiv_T \neg \Box \alpha$. Damit ist T' nach Satz 2.2 inkonsistent, also $\vdash_T \alpha$.
3. Angenommen $T^n = T + \neg \Box^n \perp$ und $\text{Con}_{T^n} \equiv_T \neg \Box^{n+1} \perp$. Wegen $\Box^n \perp \vdash_T \Box^{n+1} \perp$ gilt $\neg \Box^{n+1} \perp \vdash_T \neg \Box^n \perp$. Somit $T^{n+1} = (T + \neg \Box^n \perp) + \neg \Box^{n+1} \perp = T + \neg \Box^{n+1} \perp$. Ferner ist nach (5) in **7.2** $\text{Con}_{T^{n+1}} \equiv_T \neg \Box \neg (\neg \Box^{n+1} \perp) \equiv \neg \Box^{n+2} \perp$.
4. Für jede arithmetische Aussage α ist der Satz ‘Wenn α in PA beweisbar ist, so gilt α ’ in ZFC beweisbar (PA ist interpretierbar in ZFC, siehe **6.6**). Formalisiert: $\vdash_{\text{ZFC}} \Box_{\text{PA}} \alpha \rightarrow \alpha$.

Abschnitt 7.4

1. Man beweist zuerst $G_n = \{H \in \mathcal{F}_\Box \mid \vdash_G \Box^{n+1} \perp \rightarrow H\}$. Damit ist

$$\begin{aligned} \vdash_{G_n} H &\Leftrightarrow \vdash_G \Box^{n+1} \perp \rightarrow H \Leftrightarrow \vdash_{\text{PA}} (\Box^{n+1} \perp \rightarrow H)^i \text{ für alle } i \quad (\text{Satz 4.2}) \\ &\Leftrightarrow \vdash_{\text{PA}} \Box^{n+1} \perp \rightarrow H^i \text{ für alle } i \quad (\text{Eigenschaft von } i) \\ &\Leftrightarrow \vdash_{\text{PA}_n} H^i \text{ für alle } i \quad (\text{PA}_n = \text{PA} + \Box^n \perp). \end{aligned}$$
2. Die erste Behauptung ergibt sich unschwer aus Übung 3 in **7.2**. Die Bestimmung der Beweislogik folgt aus Satz 4.3 und $\text{Con}_{\text{PA}_n^\perp} \equiv_{\text{PA}^n} \text{Con}_{\text{PA}^n}$ nach (6) in **7.2**.
4. $\not\models_{\text{GS}} \neg[\neg \Box(p \rightarrow q) \wedge \neg \Box(\neg p \rightarrow q) \wedge \neg \Box(p \rightarrow \neg q) \wedge \neg \Box(\neg p \rightarrow \neg q)]$ und Satz 4.4.

Literatur

- [As] G. ASSER, *Einführung in die mathematische Logik, Teil III*, Teubner 1981.
- [Ba] J. BARWISE (Hrsg.), *Handbook of Mathematical Logic*, North-Holland 1977.
- [BD] A. BERARDUCCI, P. D'AQUINO, Δ_0 -complexity of the relation $y = \prod_{i \leq n} F(i)$, Ann. Pure Appl. Logic 75 (1995), 49–56.
- [Be1] L. D. BEKLEMISHEV, *On the classification of propositional provability logics*, Math. USSR – Izvestiya 35 (1990), 247–275.
- [Be2] ———, *Iterated local reflection versus iterated consistency*, Ann. Pure Appl. Logic 75 (1995), 25–48.
- [Be3] ———, *Bimodal logics for extensions of arithmetical theories*, J. Symb. Logic 61 (1996), 91–124.
- [BF] J. BARWISE, S. FEFERMAN (Hrsg.), *Model-Theoretic Logics*, Springer 1985.
- [BGG] E. BÖRGER, E. GRÄDEL, Y. GUREVICH, *The Classical Decision Problem*, Springer 1997.
- [Bi] G. BIRKHOFF, *On the structure of abstract algebras*, Proceedings of the Cambridge Philosophical Society 31 (1935), 433–454.
- [BJ] G. BOLOS, R. JEFFREY, *Computability and Logic*, 3. Aufl. Cambridge Univ. Press 1989.
- [BM] J. BELL, M. MACHOVER, *A Course in Mathematical Logic*, North-Holland 1977.
- [Boo] G. BOLOS, *The Logic of Provability*, Cambridge Univ. Press 1993.
- [BP] P. BENACERRAF, H. PUTNAM (Hrsg.), *Philosophy of Mathematics, Selected Readings*, (Englewood Cliffs NJ 1964) 2. Aufl. Cambridge Univ. Press 1997.
- [Bu] S. R. BUSS (Hrsg.), *Handbook of Proof Theory*, Elsevier 1998.
- [Bue] S. BUECHLER, *Essential Stability Theory*, Springer 1996.

- [Ca] G. CANTOR, *Gesammelte Abhandlungen*, (Berlin 1932) Springer 1980.
- [Ch] A. CHURCH, *A note on the Entscheidungsproblem*, J. Symb. Logic 1 (1936), 40–41.
- [CK] C. C. CHANG, H. J. KEISLER, *Model Theory*, (Amsterdam 1973) 3. Aufl. North-Holland 1990.
- [CZ] A. CHAGROV, M. ZAKHARYASHEV, *Modal Logic*, Clarendon Press 1997.
- [Da] D. VAN DALEN, *Logic and Structure*, (Berlin 1980) 4. Aufl. Springer 2004.
- [Dav] M. DAVIS (Hrsg.), *The Undecidable*, Raven Press 1965.
- [De1] O. DEISER, *Einführung in die Mengenlehre*, (Berlin 2002) 2. Aufl. Springer 2004.
- [De2] ———, *Axiomatische Mengenlehre*, voraussichtlich Springer 2009.
- [Do] K. DOETS, *From Logic to Logic Programming*, MIT Press 1994.
- [EFT] H.-D. EBBINGHAUS, J. FLUM, W. THOMAS, *Einführung in die Mathematische Logik*, (Darmstadt 1978) 5. Aufl. Spectrum Akad. Verlag 2007.
- [En] H. ENDERTON, *A Mathematical Introduction to Logic*, (New York 1972) 2. Aufl. Academic Press 2001.
- [Fe1] W. FELSCHER, *Berechenbarkeit*, Springer 1993.
- [Fe2] ———, *Lectures on Mathematical Logic*, Vol. 1–3, Gordon & Breach 2000.
- [Fef] S. FEFERMAN, *In the Light of Logic*, Oxford Univ. Press 1998.
- [Fr] G. FREGE, *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*, (Halle 1879) G. Olms Verlag 1971, oder in [Hei, 1–82].
- [Ge] G. GENTZEN, *Untersuchungen über das logische Schließen*, Mathematische Zeitschrift 39 (1935), 176–210, 405–431.
- [GH] H.-J. GOLTZ, H. HERRE, *Grundlagen der logischen Programmierung*, Akademie-Verlag 1990.
- [GJ] M. GAREY, D. JOHNSON, *Computers and Intractability, A Guide to the Theory of NP-Completeness*, Freeman 1979.
- [Gö1] K. GÖDEL, *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*, Monatshefte für Mathematik und Physik 37 (1930), 349–360, oder *Collected Works I*.
- [Gö2] ———, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik 38 (1931), 173–198.
- [Gö3] ———, *Collected Works*, Vol. I–V, Oxford Univ. Press, Vol. I 1986, Vol. II 1990, Vol. III 1995, Vol. IV, V 2003.

- [Gor] S. N. GORYACHEV, *On the interpretability of some extensions of arithmetic*, Mathematical Notes 40 (1986), 561–572.
- [Gr] G. GRÄTZER, *Universal Algebra*, (New York 1968) 2. Aufl. Springer 1979.
- [HA] D. HILBERT, W. ACKERMANN, *Grundzüge der theoretischen Logik*, (Berlin 1928) 6. Aufl. Springer 1972.
- [HB] D. HILBERT, P. BERNAYS, *Grundlagen der Mathematik*, Bd. I, II, (Berlin 1934, 1939) 2. Aufl. Springer, Band I 1968, Band II 1970.
- [He] L. HENKIN, *The completeness of the first-order functional calculus*, J. Symb. Logic 14 (1949), 159–166.
- [Hei] J. VAN HEIJENOORT (Hrsg.), *From Frege to Gödel*, Harvard Univ. Press 1967.
- [Her] J. HERBRAND, *Recherches sur la théorie de la démonstration*, C. R. Soc. Sci. Lett. Varsovie, Cl. III (1930), oder in [Hei, 525–581].
- [HeR] B. HERRMANN, W. RAUTENBERG, *Finite replacement and finite Hilbert-style axiomatizability*, Zeitsch. Math. Logik Grundlagen Math. 38 (1982), 327–344.
- [Hi] P. HINMAN, *Fundamentals of Mathematical Logic*, A. K. Peters 2005.
- [Ho] W. HODGES, *Model Theory*, Cambridge Univ. Press 1993.
- [HP] P. HÁJEK, P. PUDLÁK, *Metamathematics of First-Order Arithmetic*, Springer 1993.
- [HR] H. HERRE, W. RAUTENBERG, *Das Basistheorem und einige Anwendungen in der Modelltheorie*, Wiss. Z. Humboldt-Univ., Math. Nat. R. 19 (1970), 579–583.
- [Id] P. IDZIAK, *A characterization of finitely decidable congruence modular varieties*, Trans. Amer. Math. Soc. 349 (1997), 903–934.
- [Ig] K. IGNATIEV, *On strong provability predicates and the associated modal logics*, J. Symb. Logic 58 (1993), 249–290.
- [Ih] T. IHRINGER, *Allgemeine Algebra*, (Stuttgart 1988) 2. Aufl. Heldermann 2003.
- [JK] R. JENSEN, C. KARP, *Primitive recursive set functions*, in *Axiomatic Set Theory, Vol. I* (Hrsg. D. SCOTT), Proc. Symp. Pure Math. 13, I, AMS 1971, 143–167.
- [Ka] R. KAYE, *Models of Peano Arithmetic*, Clarendon Press 1991.
- [Ke] H. J. KEISLER, *Logic with the quantifier “there exist uncountably many”*, Annals of Mathematical Logic 1 (1970), 1–93.
- [KK] G. KREISEL, J.-L. KRIVINE, *Modelltheorie*, Springer 1972.

- [K11] S. KLEENE, *Introduction to Metamathematics*, (Amsterdam 1952) 2. Aufl. Wolters-Noordhoff 1988.
- [K12] ———, *Mathematical Logic*, Wiley & Sons 1967.
- [KR] I. KOREC, W. RAUTENBERG, *Model interpretability into trees and applications*, Arch. math. Logik 17 (1976), 97–104.
- [Kr] M. KRACHT, *Tools and Techniques in Modal Logic*, Elsevier 1999.
- [Kra] J. KRAJÍČEK, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge Univ. Press 1995.
- [Ku] K. KUNEN, *Set Theory, An Introduction to Independence Proofs*, North-Holland 1980.
- [Li] P. LINDSTRÖM, *On extensions of elementary logic*, Theoria 35 (1969), 1–11.
- [Ll] J. W. LLOYD, *Foundations of Logic Programming*, (Berlin 1984) 2. Aufl. Springer 1987.
- [Lö] M. LÖB, *Solution of a problem of Leon Henkin*, J. Symb. Logic 20 (1955), 115–118.
- [Ma] A. I. MAL'CEV, *The Metamathematics of Algebraic Systems*, North-Holland 1971.
- [Mal] J. MALITZ, *Introduction to Mathematical Logic*, Springer 1979.
- [Mat] Y. MATIYASEVICH, *Hilbert's Tenth Problem*, MIT Press 1993.
- [Me] E. MENDELSON, *Introduction to Mathematical Logic*, (Princeton 1964) 4. Aufl. Chapman & Hall 1997.
- [ML] G. MÜLLER, W. LENSKI (Hrsg.), *The Ω -Bibliography of Mathematical Logic*, Springer 1987.
- [Mo] D. MONK, *Mathematical Logic*, Springer 1976.
- [MV] R. MCKENZIE, M. VALERIOTE, *The Structure of Decidable Locally Finite Varieties*, Progress in Mathematics 79, Birkhäuser 1989.
- [Ob] A. OBERSCHHELP, *Rekursionstheorie*, BI-Wiss.-Verlag 1993.
- [Po] W. POHLERS, *Proof Theory, An Introduction*, Lecture Notes in Mathematics 1407, Springer 1989.
- [Pr] A. PRESTEL, *Einführung in die Mathematische Logik und Modelltheorie*, Vieweg 1986.

- [Pre] M. PRESBURGER, *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Congrès des Mathématiciens des Pays Slaves 1 (1930), 92–101.
- [Ra1] W. RAUTENBERG, *Klassische und Nichtklassische Aussagenlogik*, Vieweg 1979.
- [Ra2] ———, *A Concise Introduction to Mathematical Logic*, Springer 2006.
- [Ra3] ———, *Messen und Zählen, Eine einfache Konstruktion der reellen Zahlen*, Heldermann 2007.
- [Ri] M. RICHTER, *Logikkalküle*, Teubner 1978.
- [Ro1] A. ROBINSON, *Introduction to Model Theory and to the Metamathematics of Algebra*, (Amsterdam 1963) 2. Aufl. North-Holland 1974.
- [Ro2] ———, *Non-Standard Analysis*, (Amsterdam 1966) 3. Aufl. North-Holland 1974.
- [Rob] J. ROBINSON, *A machine-oriented logic based on the resolution principle*, Journal of the ACM 12 (1965), 23–41.
- [Rog] H. ROGERS, *Theory of Recursive Functions and Effective Computability*, 2. Aufl. MIT Press 1988.
- [Ros] J. B. ROSSER, *Extensions of some theorems of Gödel and Church*, J. Symb. Logic 1 (1936), 87–91.
- [Rot] P. ROTHMALER, *Einführung in die Modelltheorie*, Spectrum Akad. Verlag 1995.
- [RS] H. RASIOWA, R. SIKORSKI, *The Mathematics of Metamathematics*, (Warschau 1963) 3. Aufl. Polish Scientific Publ. 1970.
- [RZ] W. RAUTENBERG, M. ZIEGLER, *Recursive inseparability in graph theory*, Notices Amer. Math. Soc. 22 (1975), A–523.
- [Sa] G. SACKS, *Saturated Model Theory*, W. A. Benjamin 1972.
- [Sam] G. SAMBIN, *An effective fixed point theorem in intuitionistic diagonalizable algebras*, Studia Logica 35 (1976), 345–361.
- [Schö] U. SCHÖNING, *Logik für Informatiker*, (Mannheim 1987) 5. Aufl. Spectrum Akad. Verlag 2000.
- [Se] A. SELMAN, *Completeness of calculi for axiomatically defined classes of algebras*, Algebra Universalis 2 (1972), 20–32.
- [Sh] S. SHELAH, *Classification Theory and the Number of Nonisomorphic Models*, (Amsterdam 1978) 2. Aufl. North-Holland 1990.
- [Shoe] J. R. SHOENFIELD, *Mathematical Logic*, (Reading Mass. 1967) A. K. Peters 2001.

- [Si] W. SIEG, *Herbrand analyses*, Arch. Math. Logic 30 (1991), 409–441.
- [Sm] R. SMULLYAN, *Diagonalization and Self-Reference*, Clarendon Press 1994.
- [So] R. SOLOVAY, *Provability interpretation of modal logic*, Israel Journal of Mathematics 25 (1976), 287–304.
- [Sz] W. SZMIELEW, *Elementary properties of abelian groups*, Fund. Math. 41 (1954), 203–271.
- [Ta1] A. TARSKI, *Der Wahrheitsbegriff in den formalisierten Sprachen*, Studia Philosophica 1 (1936), 261–405, oder in [Ta3, 152–278].
- [Ta2] ———, *A Decision Method for Elementary Algebra and Geometry*, (Santa Monica 1948, Berkeley 1951) Paris 1967.
- [Ta3] ———, *Logic, Semantics, Metamathematics*, (Oxford 1956) 2. Aufl. Hackett 1983.
- [TMR] A. TARSKI, A. MOSTOWSKI, R. M. ROBINSON, *Undecidable Theories*, North-Holland 1953.
- [Tu] A. TURING, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc., 2nd Ser. 42 (1937), 230–265, oder in [Dav].
- [TW] H.-P. TUSCHIK, H. WOLTER, *Mathematische Logik – kurzgefaßt*, (Mannheim 1994) 2. Aufl. Spectrum Akad. Verlag 2002.
- [Vi] A. VISSER, *An overview of interpretability logic*, in *Advances in Modal Logic, Vol. 1* (Hrsg. M. KRACHT et al.), CSLI Lecture Notes 87 (1998), 307–359.
- [Wae] B. L. VAN DER WAERDEN, *Algebra I*, (Berlin 1930) 4. Aufl. Springer 1955.
- [Wag] F. WAGNER, *Simple Theories*, Kluwer 2000.
- [Wi] A. WILKIE, *Model completeness results for expansions of the ordered field of real numbers ...*, Journal Amer. Math. Soc. 9 (1996), 1051–1094.
- [WP] A. WILKIE, J. PARIS, *On the scheme of induction for bounded arithmetic formulas*, Ann. Pure Appl. Logic 35 (1987), 261–302.
- [WR] A. WHITEHEAD, B. RUSSELL, *Principia Mathematica*, I–III, (Cambridge 1910, 1912, 1913) 2. Aufl. Cambridge Univ. Press, Vol. I 1925, Vol. II, III 1927.
- [Zi] M. ZIEGLER, *Model theory of modules*, Ann. Pure Appl. Logic 26 (1984), 149–213.

Stichwortverzeichnis

A

a.a. (algebraisch abgeschlossen), 38
 \forall -Formel, \forall -Aussage, 54
 \forall -Theorie, 66
 $\forall\exists$ -Aussage, $\forall\exists$ -Theorie, 148
Abbildung (Funktion), xix
 bijektive, xix
 identische, xix
 injektive, surjektive, xix
abelsche Gruppe, 38
 dividierbare, 81
 torsionsfreie, 82
ableitbar, 18, 29
Ableitungsbedingungen, 210
Abschlußaxiome, 200
Abschluss (eines Modells in T), 152
Absorptionsgesetze, 39
Ackermann-Funktion, 175
Algebra, 34
algebraisch, 38
allgemeingültig, 14, 51
allgemeingültigkeitsgleich, 61
Alphabet, xx
Anfang, xx, 37
Anfangssequenz, 18
Anfrage, 122
Anordnung, 37
Antivalenz, 2
äquivalent, 9, 51
 in (oder modulo) T , 66
 in einer Struktur, 59
Äquivalenz, 3
Äquivalenzklasse, 41
Äquivalenzrelation, 36

arithmetisch, 184
arithmetische Hierarchie, 205
arithmetisierbar, 177, 194
Artin, 153
assoziativ, xxi
aufzählbar, 92, 175
Aussage, 47
Aussagenvariable, 4
 modalisierte, 224
Auswahlaxiom, 90
Auswahlfunktion, xxi
Automorphismus, 40
axiomatisierbar, 81
 endlich, rekursiv, 81
Axiomensystem, 65
 logisches, 29, 95

B

β -Funktion, 189
Basisregeln, 18, 72
Basissatz, 140, 161
Baum, 26
Belegung, 7, 49, 221
benachbart, 25
berechenbar, 127, 169
beschränkt, 37
Beweis (formaler), 29, 96
beweisbar, 19, 29
beweisbar rekursiv, 212
Beweislogik, 224
Bild, xix
Birkhoffsche Regeln, 99
Blatt, 113
Boolesche Algebra, 39
Boolesche Basis, 140, 160

Boolesche Funktion, 2
 duale, selbstduale, 12
 lineare, 8
 monotone, 13
 Boolesche Kombination, 45
 Boolesche Matrix, 40
 Boolesche Signatur, 5

C

Charakteristik eines Körpers, 39
 Chinesischer Restsatz, 189
 Church, 92
 Churchsche These, 171
 Cohen, xviii

D

δ -Funktion, 170
 Δ_0 -Formel, Δ_0 -Prädikat, 185
 Δ_0 -Induktion, 206
 Davis, 199
 Deduktionstheorem, 16, 31
 deduktiv abgeschlossen, 16, 64
 definierbar
 (elementar) in einer Struktur, 54
 Δ_0 -definierbar, 212
 explizit, implizit, 69
 in Theorien, 211
 mit Parametern, 85
 Σ_1 -definierbar, 212
 Definitionsbereich, xix
 DeJongh, 225
 Diagramm, 132
 elementares, 133
 universales, 149
 direkte Potenz, 42
 Disjunktion, 2
 Distributivgesetze, 39
 Durchschnitt, xix

E

\exists -abgeschlossen, 155
 \exists -Formel, 54
 einfache, 158

Ehrenfeucht-Spiel, 142
 Einbettung, 40
 elementare, 136
 Einschränkung, 35
 Einselement, 38
 Einsetzung, 58, 223
 elementar-äquivalent, 55
 elementarer Typ, 139
 Enderweiterung, 84
 endliche Modelleigenschaft, 98
 Endlichkeitssatz, 21, 24, 74, 81
 entscheidbar, 81, 169
 erfüllbar, 14, 51, 65, 112
 erfüllbarkeitsgleich, 69
 Erfüllungsrelation, 14, 49
 Ersetzungstheorem, 10, 59
 Erweiterung, 36, 62, 64
 definitorische, 69
 elementare, 133
 endliche, 65
 konservative, 53, 67
 transzendente, 153
 unmittelbare, 153
 existentiell abgeschlossen, 149, 155
 Expansion, 36, 62
 explizite Definition, 67, 68
 Extensionalitätsprinzip, 2

F

f -abgeschlossen, 35
 Faktorstruktur, 41
 Falsum, 5
 fast alle, 48, 163
 Fermatsche Vermutung, 199
 Fibonacci-Folge, 174
 fiktives Argument, 8
 Filter, 28
 Fixpunktlemma, 194
 Folge, xx
 Folgerungsrelation
 aussagenlogische, 15
 globale, lokale, 63

- prädikatenlogische, 51
- Formel, 4, 45
 - arithmetische, 185, 212
 - atomare, 45
 - Boolesche, 5
 - definierende, 67
 - duale, 12
 - geschlossene, 47
 - pränexe, 61
 - quantorenfreie (= offene), 45
 - repräsentierende, 8, 184, 187
 - universale, 54
- Formelalgebra, 34
- Formelinduktion, 6, 46
- Frege, 60
- Funktion, xix
 - charakteristische, xx
 - n -stellige, xx
 - primitiv-rekursive, 169
 - rekursive (= μ -rekursive), 169
- funktional vollständig, 12
- Funktionsterm, 44

G

- Generalisierte, 51
- Generalisierung, 62
- Gentzen-Kalkül, 18
- geordnetes Paar, 89
- gleichheitsfrei, 80
- gleichmächtig, 87
- Gleichung, 45
 - diophantische, 185, 198
- Gödel, xvii, 71, 189, 225
- gödelisierbar, 177, 194
- Gödelterm, 191
- Gödelzahl, 173
 - einer Zeichenfolge, 176
 - eines Beweises, 177
- Graph, 37
 - einfacher, 25
 - k -chromatischer, 25
 - einer Operation, xxi

- planarer, 26
- Größenbereich, 38
- Grundinstanz, 107, 123
- Grundterm, 44
- Gruppe, Gruppoid, 38
 - geordnete, 38

H

- Halbgruppe, 38
- Halbordnung, 37
- Halbring, 38
- Halbverband, 39
- Harrington, 219
- Hauptpolynom, 82
- Henkin-Menge, 77
- Herbrand-Modell, 108
 - minimales, 110
- Herbrand-Struktur, 108
- Herleitung, herleitbar, 19
- Hilbert, xvii
- Hilbert-Kalkül, 29, 95
- Hilberts Programm, xvii, 168
- Homomorphismus, 40
 - natürlicher, 41
 - strenger, 40
- Horn-Resolution (H -Resolution), 116
- Hornformel, 109
 - Basis-Hornformel, 109
 - positive, negative, 109
 - universale, 109
- Hornklausel, 116
- Horntheorie, 109
 - nichttriviale, 110
 - universale, 110
- Hyperexponentiation, 186

I

- i.a. (im Allgemeinen), 42
- I -Tupel, xx
- idempotent, xxi
- Identität, 99
- Implikation, 3
 - konverse, 3

Individuenvariable, 43

Induktion

über φ , 7, 46

über t , 44

<-Induktion, 86

Induktionsaxiom, 84

Induktionsschema, 83

Induktionsschritt, 83

Infimum, 39

Infinitesimalzahl, 86

informell, 63

inkonsistent, 17, 21, 75

Instanz, 107, 123

Integritätsbereich, 38

Interpretation, 49

(relativ) interpretierbar, 200

Invariansatz, 55

invertierbar, xxi

Isomorphismus, 40

partieller, 138

J

ι -Term, 68

Jeroslow, 225

Junktor, 3

K

κ -kategorisch, 137

Kardinalzahl, 135

Kern (einer pränexen Formel), 61

Kette, 37

von Strukturen, 148

elementare, 148

von Theorien, 80

Kettenschluß, 14

Fregescher, 14

Klammerersparnis, 5, 46

Klasse

elementare, Δ -elementare, 139

von \mathcal{L} -Strukturen, 98

Klausel, 112, 118

definite, positive, negative, 112

Kleene, 169, 205

koendlich, 28

Koinzidenzatz, 52

kollisionsfrei, 56

kommutativ, xxi

Kompaktheitssatz, 24, 82

Komposition, xix, 169

Kongruenz(relation), 41, 58

Königscher Graphensatz, 26

Konjunktion, 2

Konsequenzrelation

aussagenlogische, 17

finitäre, 17

maximale, 24

konsistent, 21, 65, 75, 123

Konsistenzerweiterung, 220

Konstante, xx

Konstantenexpansion, 76

Konstantenquantifizierung, 76

Kontinuumshypothese, 135

Kontradiktion, 14

Kontrapositionsregel, 17

Körper, 38

algebraisch abgeschlossener, 82

der algebraischen Zahlen, 134

geordneter, 39

reell abgeschlossener, 153

Korrektheit, 21, 73

Kreisel, 225

Kripke-Struktur, 221

L

\mathcal{L} -Formel, 45

\mathcal{L} -Modell, 49

\mathcal{L} -Struktur (= L -Struktur), 35

legitim, 68

Lemma von Euklid, 193

Lemma von Zorn, 37

Lindenbaum, 23

Literal, 10, 45

Löbsches Axiom, 221

Löbsches Theorem, 218, 225

Logikprogramm, 122

logisch gültig, 14, 51
logische Matrix, 40
Lösung, 123
Lücke, 37

M

μ -Operation, 169
 beschränkte, 172
Mächtigkeit, 135
Matiyasevich, 199
maximal konsistent, 21
maximales Element, 37
Menge
 abzählbare, überabzählbare, 87
 dicht geordnete, 137
 diskret geordnete, 142
 endliche, 87
 geordnete, 37
 stetig geordnete, 37
 wohlgeordnete, 37
Mengenalgebra, 40
Mengenfamilie, xix
Metainduktion, xv, 182
Metatheorie, xv
Minimalmodell, 117
Modell
 aussagenlogisches, 7
 einer Theorie, 64
 freies, 110
 prädikatenlogisches, 49
 transitives, 229
Modellbegleiter, 157
modellinterpretierbar, 202
modellverträglich, 150
Modellvervollständigung, 155
modellvollständig, 151
Modus Ponens, 15, 29
Monotonieregel, 18
Mostowski, 168, 189, 225
MP-abgeschlossen, 30

N

n -Tupel, xx

Nachfolgerfunktion, 83
Negation, 2
Nichtrepräsentierbarkeitslemma, 194
Nichtstandard-Analysis, 85
Nichtstandardmodell, 83
Nichtstandardzahl, 84
Normalform
 disjunktive, 10
 kanonische, 12
 konjunktive, 10, 58
 pränexe, 61
 Skolemsche, 70

O

ω -konsistent, 195
 ω -Regel, 226
 ω -Term, 90
 ω -unvollständig, 196
Objektsprache, xv
Operation, xx
 wesentlich n -stellige, 8
Ordnung, 37
 dichte, 137
 diskrete, 142
 lineare, partielle, 37

P

p.r. (primitiv rekursiv), 169
 Π_1 -Formel, Π_1 -Prädikat, 185
Paarkodierung, 172
Paarmenge, 89
Paradoxie von Skolem, 91
parameterdefinierbar, 85
Paris, 219
Partikularisierung, 62
Peano-Arithmetik, 83
Peirce-Axiom, 14
persistent, 147
Potenzmenge, xix
Potenzmengenaxiom, 89
Prädikat, xx
 arithmetisches, 184
 diophantisches, 185

(primitiv) rekursives, 169
rekursiv aufzählbares, 175

Präfix, 45

Prämisse, 18

Presburger, 159

Primformel, 4, 45

primitive Rekursion, 169

Primkörper, 39

Primmodell, 133

Primterm, 44

Produkt, xxi

direktes, 42

reduziertes, 163

von Abbildungen, xix

Programmiersprache, 103

Projektionsfunktion, 169

PROLOG, 122

Putnam, 199

Q

Quantifizierung

beschränkte, 172, 185

Quantor, 33

Quantorenelimination, 157

Quantorenkompression, 188

Quantorenrang, 46

Quasiidentität, Quasivarietät, 100

Quotientenkörper, 146

R

r.a. (rekursiv aufzählbar), 175

Rabin, 200

Rang (einer Formel), 7, 46

reductio ad absurdum, 19

Redukt, 36, 62

Redukt-Theorie, 66

Reduzierte (einer Formel), 67, 68

reduziertes Produkt, 163

Reflektionsprinzip, 220

Regel, 18

der Hornresolution, 116

korrekte, 20, 72

vom Gentzen-Typ, 20

vom Hilbert-Typ, 95

Regelinduktion, 21, 73

Rekursionsgleichungen, 169

rekursive (=induktive) Definition, 7

Relation, xix, xx

antisymmetrische, 36

konnexe, 36

reflexive, irreflexive, 36

symmetrische, 36

transitive, 36

Relationalstruktur, 34

(P-)Relativierte, 200

repräsentantenunabhängig, 41

Repräsentationssatz, 190

Stonescher, 40

Repräsentierbarkeit

einer Booleschen Funktion, 8

einer Funktion, 187

eines Prädikates, 184

Resolution, erfolgreiche, 114

Resolutionsbaum, 113

Resolutionshülle, 113

Resolutionskalkül, 113

Resolutionsregel, 113

Resolutionssatz, 115

Resolvente, 113

Ring, 38

Abraham Robinson, 85

Julia Robinson, 199, 201

Rogers, 225

S

S-invariant, 145

Σ_1 -Formel, 185

spezielle, 208

Σ_1 -Prädikat, 185

Σ_1 -Vollständigkeit, 186

beweisbare, 215

Sambin, 225

Satz

von Cantor, 87

von Cantor-Bernstein, 135

- von Dzhaparidze, 227
- von Goodstein, 219
- von Goryachev, 228
- von Herbrand, 108
- von Lagrange, 198
- von Lindenbaum, 22
- von Lindström, 101
- von Łoś, 164
- von Löwenheim-Skolem, 87, 135, 136
- von Morley, 139
- von Rosser, 196
- von Steinitz, 153
- von Trachtenbrot, 98
- von Visser, 224
- Schnittregel, 20, 100
- Separator, 121
- Sequenz, 18
- Sheffer-Funktion, 2
- Signatur, 34
 - algebraische, 45
 - logische, 4
 - nichtlogische, 34
- Skolem-Funktionen, 69
- SLD-Resolution, 126
- SP**-invariant, 146
- Sprache
 - der 1. Stufe (= elementare), 43
 - der 2. Stufe, 102
- Spracherweiterung, 62
- Stetigkeitsschema, 86
- Struktur, 34
 - algebraische, 34
- Subformel, 6, 46
- Substitution, 16, 47
 - aussagenlogische, 16
 - einfache, simultane, 47
 - globale, 47
 - identische, 47
- Substitutionsfunktion, 193
- Substitutionssatz, 56
- Substruktur, 36
 - (endlich) erzeugte, 36

- elementare, 133
- substrukturvollständig, 161
- Subterm, 44
- Subtheorie, 64
- Supremum, 39
- Symbol, xx
 - (explizit) definiertes, 67, 68
 - logisches, 3, 43
 - von T , 64

T

- T -Modell, 64
- Tarski, 17, 131, 168
- Tarski-Fragment, 202
- Tautologie, 14, 51
- teilbar, 185
- teilerfremd, 185
- Teilwort, xx
- Term, 44
- termäquivalent, 12
- Termalgebra, 44
- Termfunktion, 53
- Terminduktion, 44
- Termmodell, 78, 106
- tertium non datur, 51
- Theorie
 - (endlich) axiomatisierbare, 81
 - abzählbare, 87
 - elementare (oder 1. Stufe), 64
 - entscheidbare, 93, 177
 - erblich unentscheidbare, 197
 - gödelisierbare, 194
 - induktive, 148
 - konsistente (erfüllbare), 65
 - streng unentscheidbare, 197
 - unentscheidbare, 93
 - universale, 66
 - vollständige, 83
 - wesentlich unentscheidbare, 204
- Träger, 34
- transzendent, 38
- Turing-Maschine, 171

U

U -Resolution, U -Resolvente, 125
 UH -Resolution, 126
Ultrafilter, Ultrafiltersatz, 28
Ultraprodukt, Ultrapotenz, 164
Umbenennung, 60, 119
 freie, gebundene, 60
unabhängig, 65, 75
Unendlichkeitsaxiom, 90
unentscheidbar, 81, 93
Unifikationsalgorithmus, 119
Unifikator, 119
 generischer (= allgemeinsten), 119
unifizierbar, 119
universaler Teil, 145
Universum, 89
unmittelbarer Nachfolger, 37
Unvollständigkeitssatz
 erster, 195
 zweiter, 217
Urelement, 88

V

Variable, 43
 freie, gebundene, 46
Variablenkollision, 55
Varietät, 99
Vaught, 139
Verband, 39
Vereinigung, xix
 einer Kette von Strukturen, 148
Verkettung, xx
 arithmetische, 174
verträglich, 65
Verum, 5
Vervollständigung, 94
 induktive, 150
Vierfarbensatz, 26
Vollständigkeitssatz, 80, 96, 97, 222
 aussagenlogischer, 23
 Birkhoffscher, 100
 Gödelscher, 80

Solovayscher, 223

Vorgängerfunktion, 83

W

wahr (in einer Struktur), 196
Wahrheitsfunktion, 2
Wahrheitswerte, 2
Wertematrix, 2
wertverlaufsgleich, 9, 66
Wertverlaufsrekursion, 174
widerlegbar, 65
Wirkungsbereich, 46
Wohlordnung, 37
Wort (über A), xx
Worthalbgruppe, 38

Z

\mathbb{Z} -Gruppe, 159
Zeichenfolge, xx
Zielklausel, 123

Symbolverzeichnis

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$	xix	\mathcal{Z}	39	$t^{\mathcal{A}}(\vec{a})$	53
$\cup, \cap, \setminus, \subseteq, \subset$	xix	$\mathcal{A} \simeq \mathcal{B}$	40	$\varphi^{\mathcal{A}}$	54
$\emptyset, \wp M$	xix	lh	40	$\exists_n, \exists_{=n}, \top, \perp$	54
$\bigcup F, \bigcap F$	xix	$\approx, a/\approx, \mathcal{A}/\approx$	41	$\mathcal{A} \equiv \mathcal{B}$	55
$(a, b), M \times N$	xix	$\prod_{i \in I} \mathcal{A}_i, \mathcal{A}^I$	42	$\mathcal{M}^\sigma, \mathcal{M}_{\vec{x}}^{\vec{t}}$	56
$f(a), fa, a^f$	xix	$\forall, =$	43	$\exists!$	57
$dom f, ran f$	xix	$\mathcal{S}_{\mathcal{L}}$	43	$\equiv_{\mathcal{A}}, \equiv_K$	59
$f: M \rightarrow N$	xix	$\mathcal{T} (= \mathcal{T}_L)$	44	PNF	61
$x \mapsto t, id_M$	xix	$var \xi, var X$	44	$(\forall x \triangleleft t), (\exists x \triangleleft t)$	61
M^I, M^n	xx	\exists, \neq	45	\mid (teilt)	63
$P\vec{a}, \neg P\vec{a}, \chi_P$	xx	$\mathcal{L}, \mathcal{L}_{\in}, \mathcal{L}_{=}$	45	\vDash	63
$f\vec{a}$	xx	$rg \alpha, qr \alpha$	46	$T, Md T$	64
$graph f$	xxi	$frei \varphi, gbd \varphi$	46	$Taut$	65
$\prod_{i \in I} M_i$	xxi	$\mathcal{L}^0, \mathcal{L}^1, \dots$	47	$T + \alpha, T + S$	65
$\Leftrightarrow, \Rightarrow, \&, \vee$	xxi	$\varphi(x_1, \dots, x_n)$	47	$Th \mathcal{A}, Th \mathbf{K}$	66
$:=$	xxi	$\varphi(\vec{x}), t(\vec{x})$	47	$\mathbf{K} \models \alpha$	66
B_n	2	$f\vec{t}, r\vec{t}$	47	\equiv_T	66
\wedge, \vee, \neg	3	$\varphi \frac{t}{x}, \varphi \frac{\vec{t}}{\vec{x}}, \varphi_{\vec{x}}(\vec{t})$	47	$\mathcal{L}[r], \varphi^{rd}$	67
\mathcal{F}, AV	4	ι	47	SNF	70
$\rightarrow, \leftrightarrow, \top, \perp$	5	$\mathcal{M} = (\mathcal{A}, w)$	49	\vdash	72
$Sf \alpha$	6	$r^{\mathcal{M}}, f^{\mathcal{M}}, c^{\mathcal{M}}$	49	Mon, End	74
$w \alpha$	7	$t^w, t^{\mathcal{M}}, \vec{t}^{\mathcal{M}}, t^{\mathcal{A}}$	49	$\mathcal{Lc}, \mathcal{LC}$	76
$\mathcal{F}_n, \alpha^{(n)}$	8	$\mathcal{M} \models \varphi, \mathcal{A} \models \varphi[w]$	49	$\vdash_T, X \vdash_T \alpha$	80
$\alpha \equiv \beta$	9	$\mathcal{M}_x^a, \mathcal{M}_{\vec{x}}^{\vec{a}}, \mathcal{M}_x^t$	50	ACF	82
DNF, KNF	10	$\forall \vec{x} \varphi$	50	$\mathcal{N}, \mathbf{S}, \mathbf{R}$	83
$w \models \alpha, \models \alpha$	14	$\models \varphi, \alpha \equiv \beta$	51	\mathcal{L}_{ar}	83
$X \models \alpha, X \models Y$	15	$\mathcal{A} \models \varphi, \mathcal{A} \models X$	51	PA, IS	83
$\vdash, \not\vdash$	18	$X \models \varphi$	51	$\underline{n} (= \mathbf{S}^n 0)$	83
$\mathbf{C}^+, \mathbf{C}^-$	22	$\varphi^{\forall}, X^{\forall}$	51	$M \sim N$	87
\vdash, MP	29	T_G, T_G^{\equiv}	52	ZF, ZFC	88
$r^{\mathcal{A}}, f^{\mathcal{A}}, c^{\mathcal{A}}$	35	$\mathcal{A} \models \varphi[\vec{a}]$	53	$\{z \in x \mid \varphi\}$	89
$\mathcal{A} \subseteq \mathcal{B}$	36	$(\mathcal{A}, \vec{a}) \models \varphi$	53	ω	90

AI, AF, AC	90	SO, SO ₀₀ , ...	142	$\Delta_0, \Sigma_1, \Pi_1, \Delta_1$	185
\vdash , MP, MQ	95	$\Gamma_k(\mathcal{A}, \mathcal{B}), \sim_k$	142	\perp (teilerfremd)	185
$\Lambda, \Lambda_1\text{--}\Lambda_{10}$	95	$\mathcal{A} \equiv_k \mathcal{B}$	143	$I\Delta_0$	186
<i>Tautfin</i>	97	T_{\forall}	145	β , beta	189
\vdash^B	99	$\mathcal{A} \subseteq_{ec} \mathcal{B}$	149	$\lceil \varphi \rceil, \lceil t \rceil, \lceil \Phi \rceil$	191
$\mathcal{L}_{II}, \mathcal{L}_{\mathcal{O}}$	102	$D_{\forall} \mathcal{A}$	149	bew_T , bwb_T	191
$\mathcal{F}, \mathcal{F}X$	106	RCF	153	$\underline{a}, \underline{z}, \dot{\alpha}_{\vec{x}}(\underline{a})$	193
$\mathcal{L}^k, \text{Va}\Gamma_k, \mathcal{T}_k$	107	ZG, ZG ₀	159	sb _x , sb _{\vec{x}} , sb _{\emptyset}	193
$\mathcal{F}_k, \mathcal{F}_k X$	107	$\approx_F, \prod_{i \in I}^F \mathcal{A}_i$	163	prov	196
GI(<i>X</i>)	107	\mathcal{A}^I/F	164	α^P, X^P, CA	200
$\mathcal{L}_{\infty}, \mathcal{T}_{\infty}, \mathcal{F}_{\infty}$	108	\mathbf{F}_n	169	$\Delta, T^{\Delta}, \mathcal{B}_{\Delta}$	200
$\mathcal{C}_U, \mathcal{C}_T$	110	$h[g_1, \dots, g_m]$	169	TF, ZFC _{fin}	202
\square	112	$P[g_1, \dots, g_m]$	169	$\Sigma_n, \Pi_n, \Delta_n$	205
$\mathcal{K} \models H$	112	Oc , Op , Oμ	169	$\square(x), \square\alpha, \diamond\alpha$	210
K, λ	113	$f = \mathbf{Op}(g, h)$	169	Con_T	210
$\bar{\lambda}, \bar{K}$	113	Γ_{ν}^n	169	D0–D3	210
RR, \vdash^{RR}, Rh	113	K_c^n, \div, δ	170	$d0, d1, \dots$	210
HR, $\vdash^{HR}, \mathcal{P}, N$	116	sg, prim, rest	171	D1*	211
$V_{\mathcal{P}}, w_{\mathcal{P}}, e_{\mathcal{P}}$	117	$\mu k[P(\vec{a}, k)]$	172	$\square[\varphi]$	214
\mathfrak{U}	119	$\mu k \leq m[P(\vec{a}, k)]$	172	PA^{\perp}	218
\vdash	122	\wp	172	D4, D4°	218
GI(\mathcal{K})	123	$\text{kgV}\{a_{\nu} \mid \nu \leq n\}$	172	T^n, T^{ω}	220
UR, \vdash^{UR}	125	$\langle a_1, \dots, a_n \rangle$	173	$\square^n \alpha$	220
UHR, \vdash^{UHR}	125	Gz, ℓ	173	$\square, \square^n, \diamond$	221
$U_{\omega}R, U_{\omega}HR$	125	$(a)_i, (a)_{last}$	174	$\mathfrak{F}_{\square}, \text{MN}$	221
$\mathcal{A}_A, \mathcal{B}_A$	132	$*, \mathbf{Oq}, \bar{f}$	174	G, \vdash_G	221
$D\mathcal{A}$	132	bz_n^m	175	$P \Vdash H$	221
$D_{el} \mathcal{A}$	133	$\dot{\xi}, \dot{\varphi}$	176	\models_G, \equiv_G	221
$\mathcal{A} \preceq \mathcal{B}$	133	$\dot{W}, \dot{P}, \dot{X}, \dots$	177	H^r	223
$ M $	134	<i>bew_T</i> , <i>bwb_T</i>	178	G_n, GS	224
$\aleph_0, \aleph_1, 2^{\aleph_0}$	135	$\tilde{\neg}, \tilde{\wedge}, \tilde{\rightarrow}$	178	\square, \diamond	226
CH	135	$\tilde{=}, \tilde{\vee}, \tilde{\S}, \tilde{+}, \tilde{\cdot}$	178	GD	227
DO, DO ₀₀ , ...	137	$\mathcal{T}_{prim}, \mathcal{L}_{prim}$	179	Rf_T	228
L, R	138	$[m]_i^k$	180	Gi, Gj	229
ACF _p	138	$\leq, <$	182		
$\langle X \rangle, \equiv_X$	140	Q, N	182		