Einführung in die mathematische Logik

Prof. Dr. Holger Brenner
Universität Osnabrück
Fachbereich Mathematik/Informatik

Sommersemester 2018

Inhaltsverzeichnis

Vorwort 9
1. Vorlesung - Probleme 10
1.1. Probleme 10
1.2. Offene mathematische Probleme 11
1.3. Das Goldbach-Problem 12
1.4. Mersenne-Primzahlen 13
1.5. Primzahlzwillinge 14
1.6. Der große Fermat und der Satz von Wiles 15
1.7. Helfen Maschinen? 16
1.8. Universelle Lösungsverfahren 17
1. Arbeitsblatt 19
1.1. Übungsaufgaben 19
1.2. Aufgaben zum Abgeben 25
1.3. Die Aufgabe zum Aufgeben 26
2. Vorlesung - Formale Sprachen 26
2.1. Sprache als Symbolketten 26
2.2. Rekursive Definitionen 28
2.3. Die Sprache der Aussagenlogik 31
2.4. Aussagenlogische Interpretationen 33
2. Arbeitsblatt 35
2.1. Übungsaufgaben 35
2.2. Aufgaben zum Abgeben 40
3. Vorlesung - Tautologien 41
3.1. Tautologien 41
3.2. Die Folgerungsbeziehung 43
3.3. Ein Ableitungskalkül für die aussagenlogischen Tautologien 43
3.4. Weitere Tautologien und Regeln 45
3. Arbeitsblatt 50
3.1. Übungsaufgaben 50
3.2. Aufgaben zum Abgeben 58
4. Vorlesung - Vollständigkeit der Aussagenlogik 59

4.1. Die Ableitungsbeziehung 59
4.2. Der Vollständigkeitssatz der Aussagenlogik I 60
4.3. Auffüllungsstrategien 62
4. Arbeitsblatt 63
4.1. Übungsaufgaben 63
4.2. Aufgaben zum Abgeben 66
5. Vorlesung - Das Lemma von Zorn 67
5.1. Das Lemma von Zorn 67
5.2. Der Vollständigkeitssatz der Aussagenlogik II 71
5. Arbeitsblatt 73
5.1. Übungsaufgaben 73
5.2. Aufgaben zum Abgeben 77
6. Vorlesung - Prädikatenlogik 78
6.1. Terme 79
6.2. Relationen 83
6.3. Quantoren 84
6.4. Junktoren 85
6. Arbeitsblatt 86
6.1. Übungsaufgaben 86
6.2. Aufgaben zum Abgeben 89
7. Vorlesung - Semantik der Prädikatenlogik 90
7.1. Sprachen erster Sufe 90
7.2. Strukturen und Interpretationen 91
7.3. Interpretation von Termen 93
7.4. Interpretation von Ausdrücken 94
7.5. Beispiele 95
7. Arbeitsblatt 96
7.1. Übungsaufgaben 96
7.2. Aufgaben zum Abgeben 102
8. Vorlesung - Folgerungen 104
8.1. Allgemeingültige Ausdrücke 104
8.2. Gültigkeit von Ausdrucksmengen 105
8.3. Axiomensysteme 105

8.4. Die Folgerungsbeziehung 107
8.5. Sortenprädikate 109
8. Arbeitsblatt 110
8.1. Übungsaufgaben 110
8.2. Aufgaben zum Abgeben 114
9. Vorlesung - Substitution 116
9.1. Freie Variablen 116
9.2. Das Koinzidenzlemma 117
9.3. Substitution 118
9. Arbeitsblatt 123
9.1. Übungsaufgaben 123
9.2. Aufgaben zum Abgeben 126
10. Vorlesung - Ableitungskalkül 128
10.1. Ableitungskalkül der Prädikatenlogik 128
10.2. Gleichheitstautologien 132
10. Arbeitsblatt 134
10.1. Übungsaufgaben 134
10.2. Aufgaben zum Abgeben 136
10.3. Die Aufgabe zum Aufgeben 137
11. Vorlesung - Quantorenregeln 137
11.1. Quantorenaxiome und -regeln 137
11.2. Abgeleitete Regeln und weitere Tautologien 141
11.3. Die Ableitungsbeziehung 144
11. Arbeitsblatt 144
11.1. Übungsaufgaben 144
11.2. Aufgaben zum Abgeben 148
12. Vorlesung - Natürliche Zahlen 148
12.1. Dedekind-Peano-Axiome 149
12.2. Addition auf natürlichen Zahlen 152
12.3. Multiplikation auf natürlichen Zahlen 153
12.4. Erststufige Peanoaxiome 154
12. Arbeitsblatt 156
12.1. Übungsaufgaben 156

12.2. Aufgaben zum Abgeben 160
13. Vorlesung - Peano-Arithmetik 161
13.1. Erststufige Peano-Arithmetik - Folgerungen und Ableitungen 161
13. Arbeitsblatt 167
13.1. Übungsaufgaben 167
13.2. Aufgaben zum Abgeben 173
13.3. Die Aufgabe zum Aufgeben 174
14. Vorlesung - Satz von Henkin 174
14.1. Die Korrektheit des Ableitungskalküls 174
14.2. Der Satz von Henkin 175
14. Arbeitsblatt 179
14.1. Übungsaufgaben 179
14.2. Aufgaben zum Abgeben 184
15. Vorlesung - Der Vollständigkeitssatz 185
15.1. Auffüllungsstrategien 185
15.2. Der Vollständigkeitssatz 188
15. Arbeitsblatt 190
15.1. Übungsaufgaben 190
15.2. Aufgaben zum Abgeben 192
16. Vorlesung - Elementare Äquivalenz I 192
16.1. S-Homomorphismen und elementare Äquivalenz 192
16.2. Elementare Äquivalenz und Isomorphiesatz 194
16.3. Elementare Äquivalenz für Elemente 196
16. Arbeitsblatt 199
16.1. Übungsaufgaben 199
16.2. Aufgaben zum Abgeben 205
17. Vorlesung - Elementare Äquivalenz II 206
17.1. Isomorphie und elementare Äquivalenz im endlichen Fall 206
17.2. Nichtstandardmodelle 211
17.3. Reell-abgeschlossene Körper 212
17. Arbeitsblatt 214
17.1. Übungsaufgaben 214
17.2. Aufgaben zum Abgeben 218

18. Vorlesung - Registermaschinen 219
18.1. Registermaschinen 219
18.2. Programmbeispiele 221
18. Arbeitsblatt 225
18.1. Übungsaufgaben 225
18.2. Aufgaben zum Abgeben 228
19. Vorlesung - Das Halteproblem 228
19.1. Entscheidbarkeit und Berechenbarkeit 228
19.2. Die Churchsche These 229
19.3. Das Halteproblem 230
19.4. Aufzählbarkeit von Programmen 233
19. Arbeitsblatt 234
19.1. Übungsaufgaben 234
19.2. Aufgaben zum Abgeben 236
20. Vorlesung - Arithmetische Repräsentierungen 237
20.1. Arithmetische Repräsentierbarkeit 237
20.2. Registerprogramme als Abbildungen 238
20.3. Repräsentierbarkeit der Registerbefehle 239
20.4. Die β-Funktion 241
20. Arbeitsblatt 243
20.1. Übungsaufgaben 243
20.2. Aufgaben zum Abgeben 246
21. Vorlesung - Die Unentscheidbarkeit der Arithmetik 247
21.1. Repräsentierbarkeit der Halteeigenschaft 247
21.2. Die Unentscheidbarkeit der Arithmetik 249
21.3. Folgerungen aus der Unentscheidbarkeit 250
21. Arbeitsblatt 252
21.1. Übungsaufgaben 252
21.2. Aufgaben zum Abgeben 254
22. Vorlesung - Der Fixpunktsatz 254
22.1. Repräsentierbarkeit in einer Theorie 254
22.2. Der Fixpunktsatz 257
22. Arbeitsblatt 259

22.1. Übungsaufgaben 259
22.2. Aufgaben zum Abgeben 262
23. Vorlesung - Die Unvollständigkeitssätze 263
23.1. Der erste Gödelsche Unvollständigkeitssatz 263
23.2. Der zweite Gödelsche Unvollständigkeitssatz 265
23. Arbeitsblatt 269
23.1. Übungsaufgaben 269
23.2. Aufgaben zum Abgeben 271
24. Vorlesung - Modallogik I 273
24.1. Modallogik 273
24.2. Die formale Sprache der Modallogik 275
24.3. Das System K 275
24.4. Einige modallogische Axiomenschemata 277
24. Arbeitsblatt 280
24.1. Übungsaufgaben 280
24.2. Aufgaben zum Abgeben 282
25. Vorlesung - Modallogik II 282
25.1. Weitere Axiomenschemata 282
25.2. Paradoxe Axiome 284
25.3. Einige klassische modallogische Systeme 285
25.4. Gerichtete Graphen 287
25. Arbeitsblatt 288
25.1. Übungsaufgaben 288
25.2. Aufgaben zum Abgeben 292
26. Vorlesung - Semantik der Modallogik 293
26.1. Semantik der Modallogik 293
26.2. Semantik der einzelnen modallogischen Systeme 297
26. Arbeitsblatt 301
26.1. Übungsaufgaben 301
26.2. Aufgaben zum Abgeben 303
27. Vorlesung - Vollständigkeit der Modallogik 304
27.1. Maximal widerspruchsfreie modallogische Ausdrucksmengen 304
27.2. Das universelle modallogische Modell 305

27.3. Die Vollständigkeit der Modallogik 308
27. Arbeitsblatt 309
27.1. Übungsaufgaben 309
27.2. Aufgaben zum Abgeben 310
Anhang A: Bildlizenzen 312
Abbildungsverzeichnis 312

Vorwort

Dieses Skript gibt die Vorlesung Mathematische Logik wieder, die ich im Sommersemester 2018 an der Universität Osnabrück im Studiengang Mathematik gehalten habe.

Beim Übungsgruppenleiter Dinh bedanke ich mich für die Durchführung des Übungsbetriebs. Bei Frau Marianne Gausmann bedanke ich mich für die Erstellung der Pdf-Files und bei Dinh und den Studierenden für einzelne Korrekturen.

Holger Brenner

1. Vorlesung - Probleme

> Kultur ist Reichtum an Problemen.
>
> Egon Friedell

1.1. **Probleme.**

In vielen Lebensbereichen gibt es Probleme: Alltagsprobleme, Beziehungsprobleme, Gesundheitsprobleme, Gewichtsprobleme, Umweltprobleme, Finanzierungsprobleme, technische Probleme, politische Probleme, philosophische Probleme. Zu diesen Problemen gehören jeweils Vorstellungen, wie eine Lösung aussehen könnte oder zumindest eine Ahnung, in welche Richtung man nach einer Lösung suchen könnte; eine präzise Formulierung, wann ein Problem gelöst wäre, fehlt allerdings in den meisten Fällen.

Für Probleme gibt es in der Regel verschiedene Lösungsansätze oder Lösungsstrategien. Ihr Erfolg variiert und hängt stark von unbeeinflussbaren Begleitumständen, aber auch von der Unschärfe der Problemstellung und den eigenen Bewertungsmaßstäben ab. Eine Strategie, die für dieses und jenes Problem erfolgreich war, stellt sich bei einem neuen Problem plötzlich als unbrauchbar heraus.

Könnte es eine (Meta)-strategie geben, die bei allen Problemen hilft bzw. alle Probleme löst? Eine solche Strategie kann es für die oben formulierten Problembereiche allein schon wegen der angesprochenen Unschärfe nicht geben. Die Probleme sind nie so klar umrissen, dass Einigkeit darüber besteht, ob etwas eine Lösung ist oder nicht.

Dies sieht bei mathematischen Problemen anders aus. Diese sind klar formuliert, zumeist als eine offene Frage, die grundsätzlich nur eine positive oder eine negative Antwort haben kann, und wobei die Schwierigkeit darin besteht, dies herauszufinden und zu begründen (beweisen), was denn nun der Fall ist.[1]

In der Schule beschränkt man sich typischerweise auf mathematische Probleme, für die dann eine Lösungsstrategie vorgestellt wird. Beispielsweise das Multiplizieren von zwei natürlichen Zahlen, das Lösen eines linearen Gleichungssystems, das Ableiten einer aus einfachen Grundfunktionen zusammengesetzten Funktion. Daher fragen viele Menschen, ob es denn in der

[1] Es gibt natürlich auch anders gelagerte Probleme in der Mathematik. Beispielsweise, wie man intuitive Konzepte wie einen Punkt in der Ebene mathematisch präzisiert bzw. axiomatisiert, ob eine mathematische Modellierung für ein reales Weltphänomen angemessen ist, wie man mathematisches Wissen geschickt aufbereitet und didaktisch vermittelt, wie man Algorithmen optimiert, usw.

Mathematik noch was zu entdecken gibt. In Wahrheit sind die mathematischen Probleme die treibende Kraft der wissenschaftlichen Beschäftigung mit Mathematik.

Wir wollen zunächst einige offene mathematische Probleme vorstellen. Im Laufe der Vorlesung werden wir dann die Frage präzisieren, ob es wenigstens für diesen Teilbereich des menschlichen Denkens eine universelle Lösungsstrategie geben kann. Die Antwort wurde um 1930 von Kurt Gödel gegeben: Er bewies, dass es eine solche Strategie nicht geben kann.

1.2. **Offene mathematische Probleme.**

Unter den natürlichen Zahlen versteht man die Menge

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Wir setzen im Moment diese Menge als gegeben voraus und auch die darauf definierten Operationen, also die Addition und die Multiplikation. Die natürlichen Zahlen werden zum Zählen und Berechnen von endlichen Mengen verwendet, und im Allgemeinen gibt es dabei keine Probleme. Addition und Multiplikation sind durch einfache Algorithmen durchführbar (in der mathematischen Logik spricht man von „berechenbar“) und können auch durch eine Maschine ausgeführt werden. Man muss aber nicht viel weiter gehen, um Probleme über natürliche Zahlen formulieren zu können, für die derzeit keine Lösung bekannt ist.

Eine natürliche Zahl k heißt Teiler einer natürlichen Zahl n, wenn es eine weitere natürliche Zahl m mit $n = km$ gibt.

Definition 1.1. Eine natürliche Zahl $n \geq 2$ heißt eine *Primzahl*, wenn die einzigen natürlichen Teiler von ihr 1 und n sind.

Die ersten Primzahlen sind

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots .$$

Jede natürliche Zahl lässt sich als ein Produkt von Primzahlen schreiben, z.B. ist $100 = 2 \cdot 2 \cdot 5 \cdot 5$. Dies ist ein Satz der elementaren Zahlentheorie, siehe Aufgabe 1.9 für die Existenz, die Eindeutigkeitsaussage ist schwieriger. Ein anderer wichtiger Satz geht auf Euklid zurück und besagt, dass es unendlich viele Primzahlen gibt. Der Beweis dafür ist ein Widerspruchsbeweis.

Satz 1.2. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, die Menge aller Primzahlen sei endlich, sagen wir $\{p_1, p_2, \ldots, p_r\}$. Man betrachtet die Zahl

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_r + 1.$$

Diese Zahl ist durch keine der Primzahlen p_i teilbar, da bei Division von N durch p_i immer ein Rest 1 verbleibt. Damit sind die Primfaktoren von N nicht in der Ausgangsmenge enthalten - Widerspruch. □

Dieser Satz ist für den handwerklichen, alltagstauglichen Umgang mit den natürlichen Zahlen nicht besonders wichtig, er macht aber eine wichtige Aussage über die Natur der natürlichen Zahlen. Der Beweis ist recht einfach nachvollziehbar, aber es ist nicht unmittelbar klar, wie man einen solchen Beweis findet. Man beachte auch, dass es durchaus möglich ist, in einem endlichen Text Aussagen über die Unendlichkeit zu formulieren und zu beweisen.

Es gibt nun in der Mathematik, insbesondere in der Zahlentheorie, einfach zu formulierende und leicht zu verstehende Aussagen, von denen man bis heute nicht weiß, ob sie wahr oder falsch sind. Dazu geben wir einige prominente Beispiele.

1.3. **Das Goldbach-Problem.**

Problem 1.3. Gibt es für jede gerade natürliche Zahl $n \geq 4$ Primzahlen p und q mit

$$n = p + q?$$

Die Frage ist also, ob man jede gerade natürliche Zahl ab 4 als Summe von zwei Primzahlen schreiben kann. Dies kann wahr oder falsch sein, diese Eigenschaft kann gelten oder nicht. Bisher ist es aber niemandem gelungen, diese Eigenschaft zu beweisen oder zu widerlegen. Man spricht von einem *offenen Problem*. Die sogenannte *Goldbachsche Vermutung* besagt, dass dieses Problem eine positive Antwort besitzt. Es ist eine treibende Kraft in der Mathematik, eine Vermutung zu bestätigen (zu beweisen) oder zu widerlegen.

Für jede gegebene gerade Zahl $n \geq 4$ lässt sich in endlich vielen Schritten entscheiden, ob sie eine Summe von zwei Primzahlen ist. Dazu überprüft man einfach der Reihe nach für die ungeraden Zahlen $k < n$, ob sie und der komplementäre Summand $n - k$ Primzahlen sind. Falls es ein solches Paar $(k, n-k)$ gibt, hat man die Goldbach-Eigenschaft für diese eine Zahl n bestätigt. Für alle geraden Zahlen $n \geq 4$, für die diese Eigenschaft überprüft wurde, hat man stets solche Primsummanden gefunden. Inzwischen sind alle Zahlen bis zur Größenordnung 10^{18} überprüft. Zum Beispiel ist (es gibt im Allgemeinen mehrere Darstellungen)

$$4 = 2 + 2,\ 6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 5 + 5 = 3 + 7,\ 12 = 5 + 7,$$
$$14 = 3 + 11 = 7 + 7,\ 16 = 3 + 13 = 5 + 11,\ \textit{etc.}$$

Doch solche rechnerischen Ergebnisse sagen letztlich nichts über die Gültigkeit der Goldbachschen Vermutung aus, bei der es ja nicht darum geht, für möglichst viele und große Zahlen zu zeigen, dass die Goldbach-Eigenschaft gilt, sondern für alle.

Grundsätzlich gibt es mehrere Möglichkeiten, wie diese Frage beantwortet werden könnte. Der einfachste Fall wäre, wenn man eine konkrete gerade Zahl $n \geq 4$ angibt und von dieser zeigt, dass sie nicht die Summe von zwei Primzahlen ist. Der Beweis dafür wäre dann eventuell sehr lang, man

müsste alle möglichen Summanden überprüfen, aber ansonsten anspruchslos. Dann wäre die Goldbachsche Vermutung falsch. Es ist auch denkbar, dass man zeigt, dass es eine Zahl geben muss, die die Goldbach-Eigenschaft nicht erfüllt, ohne eine solche konkret anzugeben. Dann wäre die Goldbachsche Vermutung ebenfalls falsch, ein solcher Beweis könnte beliebig kompliziert sein. Oder man zeigt, das es für jede gerade Zahl $n \geq 4$ eine Summendarstellung mit zwei Primzahlen geben muss, wobei ein solcher Beweis wieder beliebig kompliziert sein könnte und die Goldbachsche Vermutung beweisen würde. Oder man zeigt sogar, wie man zu einem jeden n ein Primzahlsummandenpaar explizit berechnen kann.

1.4. **Mersenne-Primzahlen.**

Marin Mersenne (1588-1648)

Definition 1.4. Eine Primzahl der Form $2^n - 1$ heißt *Mersennesche Primzahl*.

Generell nennt man die Zahl

$$M_n = 2^n - 1$$

die n-te *Mersenne-Zahl*. Mit dieser Bezeichnung sind die Mersenne-Primzahlen genau diejenigen Mersenne-Zahlen, die Primzahlen sind. Die Mersenne-Zahl $M_n = 2^n - 1$ hat im Dualsystem eine Entwicklung, die aus genau n Einsen besteht. Die ersten Mersenne-Primzahlen sind

$$2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31, 2^7 - 1 = 127\,.$$

Die Zahl $2^{11} - 1 = 2047 = 23 \cdot 89$ ist die erste Mersenne-Zahl, wo der Exponent zwar prim (der Exponent einer Mersenne-Primzahl muss selbst eine Primzahl sein, siehe Aufgabe 1.15) ist, die aber selbst keine Mersenne-Primzahl ist. Dies wurde 1536 von Hudalrichus Regius (Walter Hermann

Ryff) gezeigt. Der nächste Kandidat, nämlich $2^{13} - 1 = 8191$, ist wieder prim. Bis ca. 1950 war bekannt, dass für die Exponenten

$$2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ und } 127$$

Mersenne-Primzahlen vorliegen, und keine weiteren unterhalb dem Exponenten 258. Von verschiedenen Leuten, unter anderem von Cataldi und Mersenne selbst, wurden falsche Behauptungen aufgestellt. Ab ca. 1950 kamen Computer zum Bestimmen von Mersenne-Primzahlen zum Einsatz, und es wurden bisher insgesamt 50 Mersenne-Primzahlen gefunden (Stand 2018). Alle größten bekannten Primzahlen sind Mersenne-Zahlen. Das liegt daran, dass es für diese Zahlen einen vergleichsweise einfachen Primzahltest gibt, nämlich den *Lucas-Lehmer-Test*. Mit diesem Test wird etwa alle zwei Jahre eine neue größte Primzahl gefunden. Eine Rekordliste findet sich unter Mersenne-Primzahlen auf Wikipedia.

Das Auffinden von großen (Mersenne)-Primzahlen, also der konkrete Nachweis, dass eine bestimmte Zahl diese Eigenschaft besitzt, ist aber etwas anderes als der Existenznachweis, dass es innerhalb oder oberhalb gewisser Schranken solche Zahlen gibt oder dass es überhaupt nur endlich oder unendlich viele solcher Zahlen gibt. Aufgrund des Satzes von Euklid weiß man, dass es jenseits jeder beliebig großen natürlichen Zahl noch Primzahlen gibt. Für Mersenne-Primzahlen ist das unbekannt.

Problem 1.5. Gibt es unendlich viele Mersenne-Primzahlen?

Wie gesagt, dies ist unbekannt, es wird aber vermutet, dass es unendlich viele gibt.

1.5. **Primzahlzwillinge.**

Definition 1.6. Ein *Primzahlzwilling* ist ein Paar bestehend aus p und $p+2$, wobei diese beiden Zahlen Primzahlen sind.

Die ersten Beispiele für Primzahlzwillinge sind

$$(3, 5),\ (5, 7),\ (11, 13),\ (17, 19),\ (29, 31), \ldots .$$

Übrigens ist $3, 5, 7$ der einzige Primzahldrilling, siehe Aufgabe 1.32

Problem 1.7. Gibt es unendlich viele Primzahlzwillinge?

Bemerkung 1.8. Die Frage, ob es unendlich viele Primzahlzwillinge gibt, besitzt verschiedene schwächere Varianten. Man kann sich zum Beispiel fragen, ob es unendlich oft vorkommt, dass es in einem Zehnerintervall zwei Primzahlen gibt, oder dass es in einem Hunderterintervall zwei Primzahlen gibt, und so weiter. Die ersten Primzahlen vermitteln dabei ein Bild, dass Primzahlen ziemlich häufig sind. Sie werden aber zunehmend seltener, so dass es für hohe Hunderterintervalle, sagen wir für die Zahlen von

$$1000000000000000 \text{ bis } 1000000000000100$$

ziemlich unwahrscheinlich ist, eine Primzahl zu enthalten, geschweige denn zwei Primzahlen. Bis vor kurzem war es nicht bekannt, ob es überhaupt eine Zahl m mit der Eigenschaft gibt, dass es unendlich viele Intervalle der Länge m gibt, die zwei Primzahlen enthalten ($m = 2$ wäre die positive Lösung des Primzahlzwillingsproblems). Im Jahr 2013 bewies Zhang Yitang, dass man

$$m = 70000000$$

nehmen kann, dass es also unendlich viele Intervalle der Form

$$[k, k + 70000000]$$

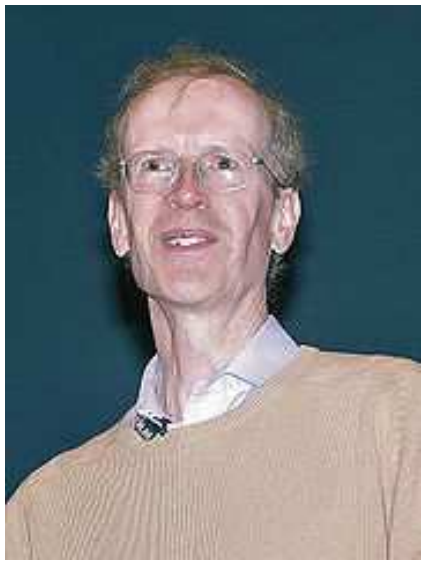
gibt, in denen zwei Primzahlen liegen. Dieses Resultat ist ein Durchbruch in der Primzahlzwillingforschung, da es erstmals zeigt, dass sich Primzahlen unendlich oft „ziemlich nahe“ kommen. Zwischenzeitlich wurde die Schranke von 70000000 auf 252 gesenkt, siehe http://arxiv.org/pdf/1402.4849v2.pdf.

1.6. **Der große Fermat und der Satz von Wiles.**

Aus dem siebzehnten Jahrhundert stammt das Problem, ob die Fermat-Gleichungen

$$x^n + y^n = z^n$$

für alle $n \geq 3$ nur triviale ganzzahlige Lösungen, bei denen $x = 0$ oder $y = 0$ ist, besitzen. Die entsprechende *Fermatsche Vermutung*, der sogenannte „Große Fermat“, galt lange Zeit als das berühmteste offene Problem der Mathematik. Nach rund 350 Jahren wurde der Große Fermat schließlich 1995 von Andrew Wiles bewiesen (Abelpreis 2016).



Andrew Wiles (*1953)

Satz 1.9. *Die diophantische Gleichung*

$$x^n + y^n = z^n$$

besitzt für kein $n \geq 3$ eine ganzzahlige nichttriviale Lösung.

Mathematik-geschichtlich gesprochen kann man sagen, dass mathematische Probleme sehr hartnäckig sind, aber früher oder später doch gelöst werden. Beispielsweise wurden alle Probleme der antiken Mathematik wie etwa die Frage nach der *Quadratur des Kreises* im Laufe des 19. Jahrhunderts gelöst. Eine wichtige geschichtliche Beobachtung ist auch, dass die Lösungen zwar auch mit individuellen Höchstleistungen zusammenhängen, aber doch stark von der allgemeinen Entwicklung des mathematischen Apparats abhängen. Viele elementar formulierbare Probleme wurden nicht elementar bewiesen, sondern erst durch neue komplexe Theorien und Methoden, die neue Sichtweisen auf das Problem ermöglichten.

Eine solche geschichtliche Beobachtung trägt aber nichts zu der Frage bei, ob es eine allgemeine Lösungsstratgie für mathematische Probleme geben könnte.

1.7. **Helfen Maschinen?**

Betrachten wir das Goldbach-Problem und nehmen wir für einen Moment an, dass die Goldbachsche Vermutung nicht stimmt, dass es also eine gerade natürliche Zahl ≥ 4 gibt, die nicht die Summe von zwei Primzahlen ist. Ein Computer, eine Rechenmaschine, nennen wir sie M_1, die der Reihe nach alle geraden Zahlen auf die Goldbach-Eigenschaft überprüft, wird früher oder später auch diese Zahl erreichen und feststellen, dass sie nicht diese Eigenschaft besitzt und wird damit die Vermutung widerlegen.

Nehmen wir nun an, dass die Goldbachsche Vermutung stimmt, und dass es dafür einen Beweis gibt, der in „normaler Sprache“ formuliert werden kann. Eine zweite Rechenmaschine M_2 drucke nach und nach alle möglichen Texte (in aufsteigender Länge) aus. Nehmen wir an, dass M_2 erkennen kann, ob ein Text aus sinnvollen Wörtern und Sätzen besteht, ob es sich um einen korrekten mathematischen Beweis handelt und ob dieser die Goldbachsche Vermutung beweist. Dann wird M_2 früher oder später einen Beweis für die Goldbachsche Vermutung ausgeben und dieses auch erkennen.

Da wir nicht wissen, ob die Goldbachsche Vermutung wahr ist oder nicht, kombinieren wir die beiden Maschinen zu einer einzigen Maschine M, die abwechselnd die M_1-Funktion und die M_2-Funktion ausführt. D.h., dass M abwechselnd eine Zahl überprüft, ob sie der Goldbachschen Vermutung widerspricht, und sodann einen Text überprüft, ob er einen Beweis für die Goldbachsche Vermutung beinhaltet. Da die Goldbachsche Vermutung wahr oder falsch ist, wird früher oder später M ein Gegenbeispiel oder einen Beweis finden und somit das Problem entscheiden.[2] Vorausgesetzt, dass es für

[2]Die beiden anderen oben erwähnten Probleme über Mersenne-Primzahlen und Primzahlzwillinge sind von einer anderen „Bauart“ und für M_1 gibt es keine direkte Entsprechung. Man kann allerdings die Idee von M_2 radikalisieren und M_1 analog zu M_2 aufbauen,

jede wahre Aussage einen (maschinell überprüfbaren) Beweis gibt. Für eine Präzisierung dieses Ansatzes siehe Aufgabe 21.13.

1.8. **Universelle Lösungsverfahren.**

Wir haben anhand einiger Beispiele gesehen, dass man mit sehr elementaren Mitteln offene Probleme formulieren kann, für die Mathematiker trotz jahrhundertelanger Bemühungen keine Antwort finden konnten. Zugleich gab es ähnliche Fragen, die lange Zeit offen waren, und dann irgendwann „plötzlich“ gelöst werden konnten.

Alles in allem ist die Lösung von mathematischen Problemen ein extrem zäher Prozess. Warum hatte Wiles den Schlüssel zum Fermat-Problem, aber nicht auch zu den drei anderen oben genannten Problemen? Wird es irgendwann einmal einen Menschen geben, der alle bis dahin offenen Probleme lösen kann? Gibt es außerirdische Intelligenz, die alle mathematischen Probleme lösen kann?

In dieser Vorlesung soll es u.A. um eine Variante dieser Fragestellung gehen, nämlich um die Frage, ob es eine universelle Strategie geben kann, mit der man sämtliche mathematische Probleme angehen könnte, oder zumindest solche Probleme, die sich über den natürlichen Zahlen in einfacher Weise formulieren lassen. Von einer solchen Strategie würde man die folgenden Eigenschaften erwarten.

(1) Die Strategie ist fixiert (durch einen endlichen Text, ein Programm, eine Maschine).
(2) Die Strategie ist deterministisch und ist nicht auf neue Einfälle, Intuition, Genialität angewiesen.
(3) Sie führt, angesetzt auf jedes Problem, zu einer (richtigen) Lösung.
(4) Dabei braucht die Durchführung der Strategie nur endlich viele Schritte (die Anzahl der benötigten Schritte darf vom Problem abhängen).

Die Präzisierung dieser Idee führt zu der Frage, ob es einen Algorithmus geben kann, der alle (zahlentheoretischen) Probleme löst. In vielen mathematischen Teilbereichen gibt es solche Algorithmen, z.B. das eingangs erwähnte Addieren oder Multiplizieren von natürlichen Zahlen, die Bestimmung, ob eine vorgegebene natürliche Zahl eine Primzahl ist, das Lösen von linearen Gleichungssystemen, u.s.w. Ein solcher universeller Algorithmus bzw. eine Maschine, worauf dieser universelle Algorithmus läuft, wäre sicher eine Sensation und würde die mathematische Welt enorm verändern. Selbst dann, wenn er so aufwändig wäre, dass er nie in der Zeitspanne eines Menschen

---

indem man M_1 ebenfalls Beweise ausgeben lässt, jetzt aber überprüft, ob es sich um einen korrekten Beweis für die Negation der Behauptung handelt. Natürlich kann man dann M_1 und M_2 unmittelbar zu einer Maschine M kombinieren, die Beweise ausgibt und überprüft, ob sie die Aussage oder ihre Negation beweist.

(oder des Universums) zu einem einzigen Resultat gelangen würde, so wäre doch allein schon der Nachweis der prinzipiellen Existenz eine gewaltige theoretische Erkenntnis. Gedanken zu einer solchen Maschine finden sich schon bei Llull und bei Leibniz.

In dieser Vorlesung werden wir mathematisch beweisen, dass es einen solchen universellen Algorithmus nicht geben kann, und zwar noch nicht einmal für den Bereich der natürlichen Zahlen. Dies ist einer der Hauptsätze von Kurt Gödel, der (erste) *Gödelsche Unvollständigkeitssatz*. Wichtig ist an dieser Stelle zu betonen, dass es sich dabei um mathematische Sätze handelt, nicht um philosophische Sätze, auch wenn sie erkenntnistheoretisch interpretiert werden können. Es gibt auch keinen philosophischen Ersatz für diese Sätze, etwa im Sinne, „weil die Welt komplex und die Sprache unscharf ist, gibt es immer Probleme“. Das wäre etwa so, wie wenn man die Relativitätstheorie mit den Worten „alles ist relativ“ gleichsetzt. Das eine ist eine mathematisch-physikalische Theorie, das andere ein nichtssagender Allgemeinplatz.

Ramon Llull (1232-1316)

Gottfried Wilhelm Leibniz (1646-1716)

Obwohl die Unvollständigkeitssätze deutliche Schranken für die maschinelle Entscheidbarkeit und Beweisbarkeit von mathematischen Sätzen setzen, gibt es auch starke Resultate, die besagen, dass viele mathematische Tätigkeiten maschinell durchführbar sind. Der ebenfalls auf Gödel zurückgehende Vollständigkeitssatz sagt, dass Beweise für Sätze der „ersten Stufe“ als eine formale Ableitung aus Axiomen realisiert werden können, und dass damit die Korrektheit von Beweisen grundsätzlich mechanisch überprüft werden kann und dass alle korrekten Beweise mechanisch aufzählbar sind. Das oben am Beispiel der Goldbachschen Vermutung angedachte Aufzählungsprinzip für mathematische Beweise ist also prinzipiell realistisch (ein Problem ist dabei, dass die natürlichen Zahlen nicht erststufig axiomatisierbar sind, siehe Satz 21.12).

Die Behandlung der Ergebnisse von Gödel setzt mehrere mathematische Präzisierungen voraus: Eine axiomatische Präzisierung der natürlichen Zahlen, eine Präzisierung der mathematischen Sprache, in der mathematische Aussagen formuliert werden können, eine Präzisierung von Beweis, eine Präzisierung von Algorithmus (mit Hilfe von rekursiven Funktionen, Turing-Maschine, Registermaschine, etc.). Dies alles ist der Inhalt der folgenden Vorlesungen.

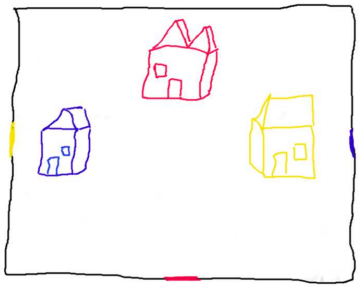
1. Arbeitsblatt

1.1. **Übungsaufgaben.**

Aufgabe 1.1. Warum ist Mathematik schwierig, obwohl darin doch alles logisch ist?

Aufgabe 1.2. Intelligenz wird häufig als „allgemeine Problemlösekompetenz“ bezeichnet. Welche Probleme können Sie lösen, welche nicht?

Aufgabe 1.3. Lege in der Skizze für die drei Häuser überschneidungsfrei Wege zu den zugehörigen gleichfarbigen Gartentoren an.



Aufgabe 1.4.*

Anfang März beträgt die Zeitdifferenz zwischen Deutschland und Paraguay 4 Stunden (in Paraguay wurde es 4 Stunden später hell). Am 25. März 2018 wurde in Deutschland die Uhr von der Winterzeit auf die Sommerzeit umgestellt, die Uhr wurde also um eine Stunde nachts von 2 auf 3 vorgestellt. In der gleichen Nacht wurde die Uhr in Paraguay umgestellt. Wie groß war die Zeitdifferenz nach der Umstellung?

Aufgabe 1.5.*

In einer psychologischen Längsschnittstudie wird die Entwicklung von Einstellungen und Verhaltensweisen von Personen untersucht. Ein Fallbeispiel: Im Alter von 20 Jahren geht Linda regelmäßig auf Demonstrationen, sie hilft im Eine-Welt-Laden mit, braut ökologisches Bier, kocht Bio-Gemüse und studiert manchmal Soziologie.

Welcher der folgenden Befunde ist nach 10 Jahren am unwahrscheinlichsten?

(1) Linda arbeitet für eine Versicherungsagentur.
(2) Linda engagiert sich bei Attac und arbeitet für eine Versicherungsagentur.
(3) Linda engagiert sich bei Attac.

Aufgabe 1.6.*

In einem Hörsaal befindet sich ein Tafelgestell mit drei hintereinander liegenden, vertikal verschiebbaren Tafeln. Diese seien mit V (vordere Tafel), M (mittlere Tafel) und H (hintere Tafel) bezeichnet. Aufgrund der Höhe des Gestells sind nur (maximal) zwei Tafeln gleichzeitig einsehbar. Die Lehrperson schreibt in der Vorlesung jede Tafel genau einmal voll. In welcher Reihenfolge (alle Möglichkeiten!) muss sie die Tafeln einsetzen, wenn beim Beschreiben einer Tafel stets die zuletzt beschriebene Tafel sichtbar sein soll.

Aufgabe 1.7. Finde die kleinste Zahl N der Form $N = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1$, die keine Primzahl ist, wobei $p_1, p_2, \ldots, p_r$ die ersten r Primzahlen sind.

Aufgabe 1.8. Sei $r \in \mathbb{N}$.

a) Finde r aufeinander folgende natürliche Zahlen (also $n, n+1, \ldots, n+r-1$), die alle nicht prim sind.

b) Finde unendlich viele solcher primfreien r-„Intervalle“.

Aufgabe 1.9.*

Zeige durch Induktion, dass jede natürliche Zahl $n \geq 2$ eine Zerlegung in Primzahlen besitzt.

Aufgabe 1.10. Berechne den Ausdruck

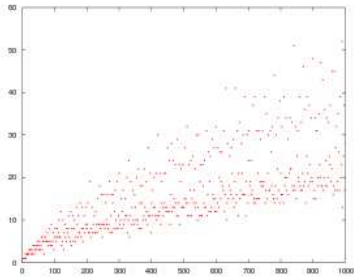
$$n^2 + n + 41$$

für $n = 0, 1, 2, \ldots$. Handelt es sich dabei um Primzahlen?

Aufgabe 1.11.*

Es sei n eine natürliche Zahl. Wann ist die Zahl $n^2 - 1$ eine Primzahl?

Aufgabe 1.12. Das Schaubild unten bezieht sich auf die Goldbachsche Vermutung. Was wird dadurch dargestellt?



Aufgabe 1.13. Zeige, dass man jede natürliche Zahl $n \geq 12$ als Summe

$$n = a + b$$

schreiben kann, wobei sowohl a als auch b zusammengesetzte Zahlen sind.

Aufgabe 1.14. Welche Zifferenentwicklung hat eine Mersennesche Primzahl im Dualsystem?

Aufgabe 1.15.*

Zeige: Ist $2^n - 1$ eine Primzahl, so ist auch n eine Primzahl.

In der folgenden Aufgabe wird ein weiteres offenes Problem formuliert. Man mache sich die Wirkungsweise des beschriebenen Algorithmus für die Zahlen bis 20 klar.

Aufgabe 1.16. Für positive ganze Zahlen n betrachten wir folgenden Algorithmus.

Wenn n gerade ist, so ersetze n durch die Hälfte.

Wenn n ungerade ist, so multipliziere n mit 3 und addiere dann 1 dazu.

Frage (Collatz-Problem): Ist es wahr, dass man bei jeder Startzahl n früher oder später bei 1 landet?

Aufgabe 1.17. Zwei Spieler sitzen an einem runden Tisch und legen abwechselnd eine Münze (alle von der gleichen Größe, die kleiner als die Größe der Tischplatte ist) auf den Tisch, wobei sich die Münzen nicht überdecken dürfen. Es verliert der Spieler, der keine Münze mehr platzieren kann. Entwerfe eine Gewinnstrategie für den Spieler, der anfängt.

Aufgabe 1.18. Bei der Fußball-Europameisterschaft 2016 qualifizieren sich die vier besten Drittplatzierten (der Vorrundengruppen A,B,C,D,E,F) für das Achtelfinale, und zwar nach dem Schema

$$\text{Sieger Gruppe } D \text{ spielt gegen einen Dritten aus } (B, E, F)\,,$$

$$\text{Sieger Gruppe } B \text{ spielt gegen einen Dritten aus } (A, C, D)\,,$$

$$\text{Sieger Gruppe } C \text{ spielt gegen einen Dritten aus } (A, B, F)\,,$$

und

$$\text{Sieger Gruppe } A \text{ spielt gegen einen Dritten aus } (C, D, E)\,.$$

(1) Zeige, dass dies stets durchführbar ist.
(2) Bestimme (abhängig von der Reihenfolge der Drittplatzierten) die minimale Anzahl an Möglichkeiten für die Aufteilung der Drittplatzierten.
(3) Bestimme (abhängig von der Reihenfolge der Drittplatzierten) die maximale Anzahl an Möglichkeiten für die Aufteilung der Drittplatzierten.

In den folgenden Aufgaben wird an einige wichtige Beweisverfahren erinnert. Überlegen Sie sich typische Beispiele dazu. Inwiefern kommen diese Argumentationsmuster auch im Alltag vor?

Aufgabe 1.19.*

Erläutere das Prinzip *Beweis durch Widerspruch* für eine Aussage der Form „Aus A folgt B“.

Aufgabe 1.20.*

Erläutere das Beweisprinzip der vollständigen Induktion.

Aufgabe 1.21. Erläutere das Prinzip *Beweis durch Fallunterscheidung.*

Aufgabe 1.22.*

Franziska möchte mit ihrem Freund Heinz Schluss machen. Sie erwägt die folgenden drei Begründungen.

(1) „Du hast dich schon am ersten Tag voll daneben benommen. Seitdem ist es von jedem Tag zum nächsten Tag nur noch schlimmer geworden. Du wirst Dich also immer völlig daneben benehmen“.
(2) „Wenn ich mit Dir zusammenbleiben würde, so würde ich irgendwann als eine traurige, gelangweilte, vom Leben enttäuschte Person enden, das möchte ich aber auf gar keinen Fall“.
(3) „Also, wenn Du mich nicht liebst, will ich Dich sowieso nicht. Wenn Du mich aber liebst, so komme ich zu dem Schluss, dass Du dein Verhalten mit Deinen Gefühlen nicht zur Deckung bringen kannst. Dann bist Du also unreif und dann will ich Dich auch nicht“.

Welche mathematischen Beweisprinzipien spiegeln sich in den drei Begründungen wieder?

Aufgabe 1.23. Zeige, dass $\sqrt{2}$ eine irrationale Zahl ist.

Wie sieht es mit $\sqrt{3}, \sqrt{4}, \sqrt{5}, \sqrt{6}$ aus?

Aufgabe 1.24. Beweise durch Induktion die folgenden Formeln.

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

(2)
$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6},$$

(3)
$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Aufgabe 1.25. Die Städte $S_1, \ldots, S_n$ seien untereinander durch Straßen verbunden und zwischen zwei Städten gibt es immer genau eine Straße. Wegen Bauarbeiten sind zur Zeit alle Straßen nur in eine Richtung befahrbar. Zeige, dass es trotzdem mindestens eine Stadt gibt, von der aus alle anderen Städte erreichbar sind.

Aufgabe 1.26. In der folgenden Argumentation wird durch Induktion bewiesen, dass alle Pferde die gleiche Farbe haben. „Es sei $A(n)$ die Aussage, dass je n Pferde stets untereinander die gleiche Farbe haben. Wenn nur ein Pferd da ist, so hat dieses eine bestimmte Farbe und die Aussage ist richtig. Für den Induktionsschritt sei vorausgesetzt, dass je n Pferde stets untereinander die gleiche Farbe haben. Es seien jetzt $n+1$ Pferde gegeben. Wenn man eines herausnimmt, so weiß man nach der Induktionsvoraussetzung, dass die verbleibenden n Pferde untereinander die gleiche Farbe haben. Nimmt man ein anderes Pferd heraus, so haben die jetzt verbleibenden Pferde wiederum untereinander die gleiche Farbe. Also haben all diese $n+1$ Pferde überhaupt die gleiche Farbe."

Aufgabe 1.27. Es seien $v \geq u \geq 0$ natürliche Zahlen. Zeige, dass

$$x = v^2 - u^2,\ y = 2uv,\ z = u^2 + v^2$$

die Gleichung

$$x^2 + y^2 = z^2$$

erfüllen.

Aufgabe 1.28. Betrachte die „Definition"

Ein Hinz ist ein Kunz, dessen Schlonz ein Ranz ist,

und nehmen wir an, dass es sich um eine sinnvolle Definition handelt. Beantworte folgende Fragen.

(1) Welcher Begriff wird neu eingeführt, welche sind schon bekannt?
(2) Besitzt jeder Kunz einen Schlonz?
(3) Besitzt jeder Hinz einen Schlonz?
(4) Ist jeder Hinz ein Kunz?
(5) Ist jeder Kunz ein Hinz?
(6) Ist der Schlonz von jedem Kunz ein Ranz?
(7) Ist der Schlonz von jedem Hinz ein Ranz?
(8) Ist jeder Hinz ein Ranz?
(9) Kann es einen Schlonz geben, der nicht zu einem Kunz gehört?
(10) Wie kann man die Vermutung widerlegen, dass jeder Kunz ein Hinz ist?

Aufgabe 1.29. Erläutere das Konzept der *Wohldefiniertheit* anhand eines typischen Beispiels.

Aufgabe 1.30. Wir betrachten eine Maschine, die nach und nach sämtliche Texte ausdruckt und damit auch früher oder später jeden Beweis ausgibt. Welche Eigenschaft eines in der Vorlesung 1 beschriebenen universellen Lösungsverfahrens besitzt diese Maschine nicht?

Aufgabe 1.31. Führe folgendes Gedankenexperiment durch: Es sei eine Maschine gegeben, die eine Aussage (eine Vermutung) über die natürlichen Zahlen nach und nach überprüft. Wenn sie alle Zahlen überprüft hätte, stünde die Antwort fest, doch da die Maschine Schritt für Schritt arbeitet, hat sie zu jedem Zeitpunkt immer nur eine endliche Teilmenge der natürlichen Zahlen überprüft und kann so, wenn die Aussage wahr ist, keinen Beweis für die Aussage liefern.

Im Allgemeinen braucht die Rechenmaschine für große Zahlen länger. Die Maschine wird jetzt beschleunigt, so dass sie für große Zahlen immer weniger Zeit braucht.

Die Maschine wird so beschleunigt, dass sie für die Überprüfung der ersten Zahl (also 1) $\frac{1}{2}$ Sekunden braucht, für die Überprüfung der zweiten Zahl $\frac{1}{4}$ Sekunden, für die Überprüfung der dritten Zahl $\frac{1}{8}$ Sekunden. Für die Überprüfung der n-ten Zahl benötigt die Maschine also genau $\left(\frac{1}{2}\right)^n$ Sekunden. Damit ist die Gesamtlaufzeit der Maschine

$$\frac{1}{2} + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^3 + \dots .$$

Diese Summe ist wohldefiniert, und zwar gleich 1 (im Zweiersystem ist es die Zahl $0,111111111\ldots$, deren Wert 1 ist). Nach einer Sekunde hat also die Maschine die unendlich vielen Zahlen durchgearbeitet und überprüft, und damit die Aussage bewiesen oder widerlegt.

1.2. **Aufgaben zum Abgeben.**

Aufgabe 1.32. (3 Punkte)

Zeige, dass es außer $3, 5, 7$ kein weiteres Zahlentripel der Form $p, p+2, p+4$ gibt, in dem alle drei Zahlen Primzahlen sind.

Aufgabe 1.33. (4 Punkte)

Zeige, dass es unendlich viele Primzahlen gibt, die modulo 4 den Rest 3 besitzen.

Aufgabe 1.34. (3 Punkte)

Zeige, dass es eine gerade Zahl g, $2 \leq g \leq 252$, mit der Eigenschaft gibt, dass es unendlich viele Primzahlen p derart gibt, dass auch $p + g$ eine Primzahl ist.

Aufgabe 1.35. (4 Punkte)

Die Räuberbande „Robin Hood“ besteht aus sieben Personen. Sie legt für ihr Diebesgut eine Schatztruhe an, die sie mit verschiedenen Schlössern sichern möchte, wobei die (mehrfachen) Schlüssel an die Mitglieder verteilt werden sollen. Dabei soll erreicht werden, dass je drei Bandenmitglieder allein nicht an den Schatz kommen, dass aber je vier Bandenmitglieder die Truhe aufschließen können. Wie viele Schlösser braucht man dafür und wie müssen die Schlüssel verteilt werden?

1.3. **Die Aufgabe zum Aufgeben.**

Lösungen zu der folgenden Aufgabe direkt an den Dozenten. Bis Ende April.

Aufgabe 1.36. Wir betrachten die Abbildung

$$\Psi\colon\ \mathbb{N}^4 \longrightarrow \mathbb{N}^4,$$

die einem Vierertupel (a,b,c,d) das Vierertupel

$$(|b-a|\,,|c-b|\,,|d-c|\,,|a-d|)$$

zuordnet. Man gebe ein Beispiel für ein Vierertupel (a,b,c,d) mit der Eigenschaft an, dass sämliche Iterationen $\Psi^n(a,b,c,d)$ für $n \leq 25$ nicht das Nulltupel liefern.

Überprüfe das Ergebnis auf http://www.vier-zahlen.bplaced.net/stufe4.php .

2. Vorlesung - Formale Sprachen

2.1. **Sprache als Symbolketten.**

Wir knüpfen an die Überlegungen der ersten Vorlesung an, ob es eine Maschine (einen Computer, einen Algorithmus) gibt, der (alle korrekten) mathematische Aussagen ausdrücken, ausdrucken, überprüfen, beweisen oder widerlegen kann. Eine solche Maschine operiert mit Zeichenreihen, die wir in diesem Zusammenhang Wörter einer (formalen) Sprache nennen. Wir beschreiben daher den Aufbau einer formalen Sprache.

Definition 2.1. Es sei A eine Menge von Symbolen. Dann nennt man jede endliche Zeichenreihe, die man mit den Elementen aus A aufstellen kann, ein *Wort über dem Alphabet A*.

Die Menge aller Wörter über dem Alphabet A bezeichnen wir mit A^*.

Das zugrunde liegende Alphabet kann endlich oder unendlich sein, für praktische Anwendungen reicht ein endliches Alphabet. Die Elemente des Alphabets nennt man Buchstaben, Zeichen oder Symbole. Mit einer Zeichenreihe meint man eine hintereinander geschriebene Buchstabenkette (oder Symbolkette). Dazu gehören die einelementigen Ketten, also die Elemente aus A

selbst, aber auch die leere Kette (das leere Wort), die wir mit $\emptyset$ bezeichnen. Bei dieser Definition kommt es nicht auf irgendeine Sinnhaftigkeit der Wörter an, es handelt sich um eine rein formale Definition.

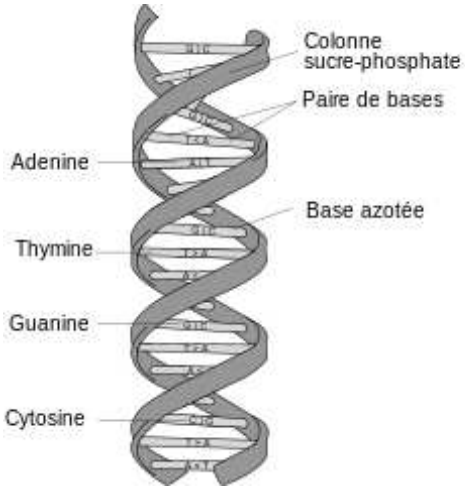
Beispiel 2.2. Es sei ein einelementiges Alphabet $A = \{|\}$ gegeben. Dann besitzt jedes Wort über A die Gestalt

$$|||\ldots|$$

mit einer gewissen Anzahl von Strichen. Zwei solche Wörter sind genau dann gleich, wenn ihre Strichanzahl übereinstimmt. In diesem Fall entsprechen also die Wörter den natürlichen Zahlen (das leere Wort entspricht der 0).

Der Binärcode besteht aus den beiden Symbolen 0 und 1, der Morsecode besteht aus drei Zeichen: kurzes Signal, langes Signal, Pause. Grundsätzlich führt jedes nichtleere endliche Alphabet zu einer abzählbar-unendlichen Menge an Wörtern und hat somit prinzipiell die gleiche Ausdrucksstärke.

Beispiel 2.3. Die DNA-Stränge, die die Erbinformationen aller Lebewesen tragen, sind Doppelketten in Helixform aus Nukleotiden. Die entscheidenden Bestandteile der Nukleotiden sind die Basen, wofür es nur vier Möglichkeiten gibt, nämlich Adenin (A), Thymin (T), Guanin (G) und Cytosin (C). Die Nukleotiden treten in der Helix stets mit einem festen Partner (nämlich Adenin mit Thymin und Guanin mit Cytosin) auf, so dass die Struktur durch die eine Hälfte der Helix festgelegt ist. Daher entspricht (bis auf die Leserichtung und die Strangauswahl) die genetische Information eines DNA-Stranges einem Wort über dem Alphabet mit den Buchstaben A,T,G,C.



Wenn zu einem Alphabet A ein neues Zeichen $-$ als „Leerzeichen“ hinzugenommen wird, so werden manchmal die Wörter aus A als (eigentliche) Wörter und die Wörter aus dem Alphabet $A \cup \{-\}$ als Texte (oder Sätze)

bezeichnet. Mit der Hinzunahme eines weiteren Satzbeendungssymbols kann man auch zwischen Sätzen und Texten unterscheiden.

Die geschriebene natürliche Sprache umfasst das Alphabet, das aus den Großbuchstaben A,B,C,...,Z,Ä,Ö,Ü, den Kleinbuchstaben a,b,c,...,z,ä,ö,ü,ß, den Ziffern, den Satzzeichen und einem Leerzeichen für den Abstand zwischen den Wörtern besteht. Jede lineare Hintereinanderreihung dieser Zeichen gilt für uns als Text. Im Moment interessieren wir uns nicht dafür, ob die geschriebenen Texte syntaktisch richtig gebildet oder semantisch sinnvoll sind. Im Moment ist also z.B.

$$!!fL33kAs.,r$$

ein erlaubter Text.

2.2. **Rekursive Definitionen.**

In der Definition von einem Wort über einem Alphabet haben wir von einer Menge gesprochen und somit eine naive Mengenlehre vorausgesetzt. Im endlichen Fall wird die Symbolmenge einfach durch Auflisten ihrer Elemente gegeben. Für die gebildeten Wörter haben wir implizit verwendet, dass das Bilden von linearen Zeichenreihen unproblematisch ist.

Ein wichtiges Prinzip, Mengen zu definieren, ist das der *rekursiven Definition*. Eine rekursive Definition besteht aus zwei Sorten von Regeln. (1) Einerseits gewisse Startregeln, die sagen, was direkt zu der Menge gehört, und (2) Rekursionsregeln (Generierungsregeln), die die Form einer Bedingung haben, und besagen, dass wenn gewisse Objekte zu der Menge gehören, und wenn neue Objekte aus diesen Objekten in bestimmter Weise gebildet sind, dass dann diese neuen Objekte ebenfalls dazu gehören (die dritte stillschweigende Bedingung an eine rekursive Definition ist, dass es keine weitere Möglichkeit gibt, zu der Menge zu gehören, außer den in (1) und (2) genannten).

Beispiel 2.4. Die Menge der Wörter über einem Alphabet A kann man auch folgendermaßen rekursiv definieren.

(1) $\emptyset$ ist ein Wort über A.
(2) Wenn x ein Wort ist und $a \in A$ ein Buchstabe, so ist auch xa ein Wort.

Hier repräsentiert x (eine Variable) ein beliebiges schon konstruiertes Wort. Dabei ist $\emptyset a$ als a zu lesen, so dass die beiden erlaubten Konstruktionsschritte (also der Anfangsschritt und der Rekursionsschritt) sichern, dass die einzelnen Symbole aus A Wörter sind. Wenn das Alphabet durch $A = \{a, b, c\}$ gegeben ist, so würde der rekursive Nachweis, dass *abbac* ein Wort ist, folgendermaßen gehen.

(1) Wegen der Anfangsbedingung ist $\emptyset$ ein Wort.
(2) Deshalb und wegen des Rekursionsschrittes ist $\emptyset a = a$ ein Wort.

(3) Deshalb und wegen des Rekursionsschrittes ist ab ein Wort (hier ist also $x = a$ das schon nachgewiesene Wort und der Buchstabe b wird angehängt).
(4) Deshalb und wegen des Rekursionsschrittes ist abb ein Wort (hier ist also $x = ab$ das schon nachgewiesene Wort und der Buchstabe b wird angehängt).
(5) Deshalb und wegen des Rekursionsschrittes ist $abba$ ein Wort (hier ist also $x = abb$ das schon nachgewiesene Wort und der Buchstabe a wird angehängt).
(6) Deshalb und wegen des Rekursionsschrittes ist $abbac$ ein Wort (hier ist also $x = abba$ das schon nachgewiesene Wort und der Buchstabe c wird angehängt).

Natürlich kann man $abbac$ sofort ansehen, dass es sich um eine linear angeordnete Zeichenreihe über $\{a, b, c\}$ handelt, und der rekursive Nachweis scheint übertrieben pedantisch zu sein. Bei komplexer gebildeten Mengen ist aber die rekursive Definition unerlässlich, vor allem auch deshalb, da sie ermöglicht, Eigenschaften der Elemente einer Menge über den rekursiven Aufbau nachzuweisen.

Bemerkung 2.5. Es sei M eine rekursiv definierte Menge, die durch eine Startmenge $S \subseteq M$ und gewisse Rekursionsvorschriften gegeben sei. Nehmen wir an, wir möchten für alle Elemente der Menge M eine gewisse Eigenschaft E nachweisen. Das *Beweisprinzip durch Rekursion*[3] oder *Beweisprinzip über den rekursiven Aufbau der Menge* funktioniert folgendermaßen.

(1) Man zeigt, dass jedes Element aus der Startmenge die Eigenschaft E erfüllt (Rekursionsanfang).
(2) Man zeigt für jede Rekursionsvorschrift, dass unter der Voraussetzung, dass die in dieser Vorschrift verwendeten Elemente die Eigenschaft E besitzen, dann auch das durch die Vorschrift produzierte Element die Eigenschaft besitzt (Rekursionsschritt).

Daraus kann man dann schließen, dass jedes Element aus M die Eigenschaft erfüllt. Die Richtigkeit dieses Beweisprinzips beruht auf folgender Betrachtung: Es sei $N \subseteq M$ die Menge aller Elemente, für die die Eigenschaft E gilt. Aufgrund des Rekursionsanfangs gilt $S \subseteq N$. Aufgrund des Rekursionsschrittes ist N abgeschlossenen unter sämtlichen Rekursionsvorschriften. Dies ist aber die Definition für M, also ist $N = M$ und die Eigenschaft gilt für ganz M.

Ein Spezialfall dieses Beweisprinzips ist das Prinzip der vollständigen Induktion für natürliche Zahlen. Die natürlichen Zahlen sind rekursiv durch das

[3]Oft spricht man einfach von einem Beweis durch Induktion.

Startelement 0 und eine einzige Rekursionsregel, nämlich die Nachfolgerregel festgelegt: Wenn n eine natürliche Zahl ist, so ist auch der Nachfolger $n' = n + 1$ von n eine natürliche Zahl.

Bemerkung 2.6. Es sei M eine rekursiv definierte Menge mit der Startmenge $S \subseteq M$. Verwandt mit dem Beweisprinzip über den rekursiven Aufbau der Menge ist das Prinzip, eine Abbildung φ von M in eine weitere Menge N rekursiv zu definieren. Dazu geht man folgendermaßen vor.

(1) Man legt eine Abbildung
$$\varphi_0 \colon S \longrightarrow N$$
fest.
(2) Für jede Rekursionsvorschrift erklärt man, wie man aus den schon festgelegten Werten $\varphi(m_1), \ldots, \varphi(m_k)$ der Elemente $m_1, \ldots, m_k$, auf die die Vorschrift Bezug nimmt, den Wert unter φ für das durch die Vorschrift produzierte Element m festlegt.
(3) Man muss sicherstellen, dass, falls es für ein Element mehrere Möglichkeiten gibt, dieses rekursiv zu erzeugen, die verschiedenen Möglichkeiten zum gleichen Wert führen.

Wenn diese Bedingungen erfüllt sind, ist eine wohldefinierte Abbildung
$$\varphi \colon M \longrightarrow N$$
definiert.

Eine Sprache besteht aus sinnvollen Wörtern und sinnvollen Sätzen, nicht aus der beliebigen Aneinanderreihung von Symbolen oder Buchstaben (oder Lauten). Es ist aber vorteilhaft, erstmal alle Möglichkeiten zuzulassen und daraus durch eine Vorgabe von Regeln die sinnvollen Ausdrücke, Wörter, Lautkombinationen herauszufiltern. So funktioniert auch der kleinkindliche Spracherwerb und der Aufbau der formalen Sprachen. Wir werden nun den rekursiven Aufbau von syntaktisch korrekten Aussagen besprechen.

Aussagenlogik

Die mathematische Logik beschäftigt sich hauptsächlich mit Prädikatenlogik, da in dieser ein Großteil der Mathematik beschrieben werden kann. Als Vorstufe dazu behandeln wir jetzt die Aussagenlogik. Wie bei der Prädikatenlogik später folgen wir dem Schema

Formale Sprache - Interpretationen und semantische Tautologien - Syntaktische Tautologien und Ableitungskalkül - Vollständigkeit.

2.3. **Die Sprache der Aussagenlogik.**

Die formallogische Sprache der Aussagenlogik wird ausgehend von einer Variablenmenge V und einer einfachen Menge an Junktoren rekursiv aufgebaut. Die Aussagenvariablen werden wir zumeist mit $p, q, r, p_1, \ldots, p_k, p_n$ $(n \in \mathbb{N})$ etc. bezeichnen. Sie repräsentieren Aussagen, haben aber keinen eigenen Inhalt, sondern teilen mit Aussagen lediglich gewisse syntaktische Eigenschaften (semantische Eigenschaften werden hier noch nicht besprochen). Beispiele für solche syntaktischen Eigenschaften sind, dass man zu einer Aussage eine Negation bilden kann, oder dass man zwei Aussagen durch „und“ verknüpfen kann. Die Aussagenvariablen repräsentieren Grundaussagen, die durch solche Verknüpfungen zu komplexeren Aussagen zusammengesetzt werden können, die selbst wiederum zu weiter verschachtelten Aussagen verbunden werden können. Die folgende Definition fixiert die formale Sprache der Aussagenlogik; es handelt sich um eine rekursive Definition, wobei die Aussagenvariablen die Startelemente sind und die logischen Operationen als Generierungsregeln auftreten. Das dieser rekursiven Definition zugrunde liegende Alphabet besteht neben einer Menge V an Aussagenvariablen aus den Symbolen

$$\neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow,\ (,\ ),$$

die als

nicht, und, oder, impliziert, genau dann, wenn, Klammer auf, Klammer zu

gelesen werden; die zugehörigen Substantive sind *Negation*, *Konjunktion*, *Disjunktion*, *Implikation* und *Äquivalenz*. Die Bezeichnungen orientieren sich natürlich an den später einzuführenden Bedeutungen, im Moment sind es lediglich Wörter für bestimmte Symbole. Die Sprache der Aussagenlogik wird als Teilmenge von A^* realisiert, wobei $A = V \cup \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, (,)\}$ ist.

Definition 2.7. Es sei V eine Menge (deren Elemente wir als *Aussagenvariable* bezeichnen). Dann wird die zugehörige *Sprache der Aussagenlogik* L^V (zu V) rekursiv durch folgende Regeln definiert.

(1) Jedes $p \in V$ gehört zu L^V.
(2) Wenn $\alpha \in L^V$, so ist auch $\neg(\alpha) \in L^V$.
(3) Wenn $\alpha, \beta \in L^V$, so sind auch $(\alpha) \wedge (\beta)$, $(\alpha) \vee (\beta)$, $(\alpha) \rightarrow (\beta)$, $(\alpha) \leftrightarrow (\beta) \in L^V$.

Häufig verwendet man weniger Symbole, beispielsweise verzichtet man auf $\rightarrow, \leftrightarrow$. Die Klammerungen werden oft auch anders gesetzt. Z.B. erlaubt man manchmal $\neg\alpha$ (ohne Klammer) oder man macht die Klammern außen, also $(\alpha \wedge \beta)$. Sehr oft lässt man Klammern, um die Lesbarkeit der Aussagen zu erhöhen, einfach weg, obwohl dies vom syntaktischen Standpunkt aus ein schweres Vergehen ist.

Beispiel 2.8. Es seien p, q, r Aussagenvariablen. Dann sind beispielsweise

$$p,\ \neg(p),\ \neg(\neg(\neg(p))),\ (p) \wedge (\neg(q)),\ ((p) \wedge (\neg(q))) \wedge (\neg(r)),$$
$$(((\neg(\neg(p))) \to (\neg(q))) \vee ((\neg(r))) \leftrightarrow (\neg(r)) \wedge (q))$$

korrekt gebildete Aussagen, d.h. sie gehören zu L^V. Dagegen sind

$$\neg,\ \to,\ p\wedge,\ p \wedge q,\ (p) \wedge (\neg q,\ (p) \wedge (q) \wedge (r),$$

keine Aussagen in L^V (aber natürlich Wörter über dem gegebenen Alphabet).

Der Nachweis, dass ein gegebenes Wort eine korrekt gebildete Aussage ist, erfolgt über eine Ableitungskette oder einen Aussagestammbaum. Bei einer *Ableitungskette* listet man Zeile für Zeile korrekt gebildete Aussagen auf, wobei diese Aussagen entweder Aussagenvariablen oder aber mittels einer Rekursionsregel aus vorhergehenden Aussagen entstanden sind. Die letzte Zeile enthält die Aussage, deren Korrektheit man zeigen will.

Beispiel 2.9. Eine Ableitungskette für

$$((p) \wedge (r)) \to ((\neg(q)) \vee (r))$$

sieht folgendermaßen aus.

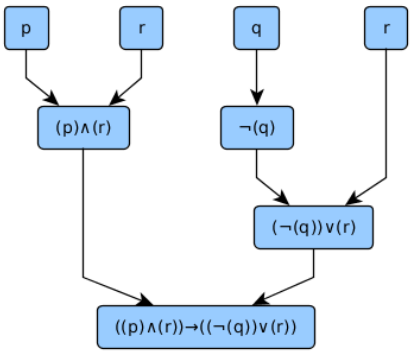
(1) p (Aussagenvariable),
(2) q (Aussagenvariable),
(3) r (Aussagenvariable),
(4) $\neg(q)$ (Negation auf 2),
(5) $(p) \wedge (r)$ (Konjunktion auf 1 und 3),
(6) $(\neg(q)) \vee (r)$ (Disjunktion auf 3 und 4),
(7) $((p) \wedge (r)) \to ((\neg(q)) \vee (r))$ (Implikation auf 5 und 6).

Ein Aussagenstammbaum ist eine graphisch übersichtliche Version einer Ableitungskette. Er beginnt mit den verwendeten Aussagenvariablen als Blättern und erzeugt dann Schritt für Schritt durch Vereinigungen von Zweigen die beteiligten Teilaussagen, bis schließlich die in Frage stehende Aussage als Stamm erzeugt ist.

Beispiel 2.10. Wir wollen uns anhand eines Stammbaumes klar machen, dass die Zeichenkette

$$((p) \wedge (r)) \to ((\neg(q)) \vee (r))$$

eine Aussage ist, also gemäß den Regeln korrekt gebildet ist. Der Abstammungsbaum entsteht ausgehend von den Blättern, die die vorkommenden Aussagenvariablen (mit ihrer Häufigkeit) repräsentieren, indem man Schritt für Schritt komplexere Teilaussagen zusammensetzt.



Jede Aussage hat eine eindeutige „rekursive Geschichte“, d.h. es gibt für jede Aussage nur eine Abfolge von Rekursionsschritten, um sie aus Aussagenvariablen aufzubauen, siehe Aufgabe 2.19.

2.4. **Aussagenlogische Interpretationen.**

Wir kommen zur Interpretation einer aussagenlogischen Sprache und insbesondere der darin auftretenden Junktoren. Der Ansatz ist, dass eine Aussagenvariable nur wahr oder falsch sein kann.

Definition 2.11. Es sei V eine Menge von Variablen und L^V die zugehörige aussagenlogische Sprache. Unter einer *Wahrheitsbelegung* versteht man eine Abbildung

$$\lambda\colon\ V \longrightarrow \{0,1\}$$

(oder mit $\{f,w\}$ als Wertebereich).

Eine Wahrheitsbelegung ist also einfach dadurch gegeben, dass einer jeden Aussagenvariablen ein Wahrheitswert, nämlich 0 oder 1 bzw. f oder w zugeordnet wird. Eine solche Wahrheitsbelegung möchte man auf die gesamte Sprache fortsetzen, wobei die folgenden Festlegungen die inhaltliche Bedeutungen der Junktoren widerspiegeln. Die folgende Definition ist möglich, da der rekursive Aufbau einer Aussage eindeutig bestimmt ist.

Definition 2.12. Es sei V eine Menge von Variablen, L^V die zugehörige aussagenlogische Sprache und

$$\lambda\colon\ V \longrightarrow \{0,1\}$$

eine Wahrheitsbelegung. Unter der zugehörigen *Interpretation* $I = I^\lambda$ versteht man die über den rekursiven Aufbau der Sprache festgelegte Abbildung

$$I\colon\ L^V \longrightarrow \{0,1\}$$

mit

(1) $I(v) = \lambda(v)$ für jede Aussagenvariable $v \in V$.

(2) Bei $\alpha = \neg(\beta)$ ist

$$I(\alpha) = \begin{cases} 1, \text{ falls } I(\beta) = 0\,, \\ 0, \text{ falls } I(\beta) = 1\,. \end{cases}$$

(3) Bei $\alpha = (\beta) \wedge (\gamma)$ ist

$$I(\alpha) = \begin{cases} 1, \text{ falls } I(\beta) = I(\gamma) = 1\,, \\ 0 \text{ sonst}\,. \end{cases}$$

(4) Bei $\alpha = (\beta) \vee (\gamma)$ ist

$$I(\alpha) = \begin{cases} 1, \text{ falls } I(\beta) = 1 \text{ oder } I(\gamma) = 1\,, \\ 0, \text{ falls } I(\beta) = I(\gamma) = 0\,. \end{cases}$$

(5) Bei $\alpha = (\beta) \to (\gamma)$ ist

$$I(\alpha) = \begin{cases} 1, \text{ falls } I(\beta) = 0 \text{ oder } I(\gamma) = 1\,, \\ 0, \text{ falls } I(\beta) = 1 \text{ und } I(\gamma) = 0\,. \end{cases}$$

(6) Bei $\alpha = (\beta) \leftrightarrow (\gamma)$ ist

$$I(\alpha) = \begin{cases} 1, \text{ falls } I(\beta) = I(\gamma)\,, \\ 0, \text{ falls } I(\beta) \neq I(\gamma)\,. \end{cases}$$

Bei

$$I(\alpha) = 1$$

sagt man, dass der Ausdruck α bei der Wahrheitsbelegung λ (oder der Interpretation I) wahr wird (oder gilt), andernfalls, dass er falsch wird (nicht gilt). Dafür schreibt man auch $I \vDash \alpha$ bzw. $I \nvDash \alpha$. Mit $I^{\vDash}$ bezeichnen wir die Menge aller bei der Interpretation I wahren Ausdrücke aus der Sprache. Wenn $\Gamma \subseteq L^V$ eine Menge an Ausdrücken ist, so bedeutet $I \vDash \Gamma$, dass $I \vDash \alpha$ für alle $\alpha \in \Gamma$ gilt. Dafür sagt man auch, dass Γ bei der Interpretation I gilt oder dass I ein *Modell* für Γ ist.

Beispiel 2.13. Es sei $V = \{p, q, r\}$ und λ sei die Wahrheitsbelegung mit $\lambda(p) = 1$, $\lambda(q) = 1$, $\lambda(r) = 0$. Es sei I die zugehörige Interpretation. Zur Berechnung des Wahrheitswertes von

$$\alpha = (\neg\,((p) \wedge (\neg(q)))) \to (r)$$

unter dieser Interpretation muss man rekursiv gemäß Definition 2.12 die einzelnen Bestandteile auswerten. Es ist

$$I(\neg q) = 0$$

und somit

$$I((p) \wedge (\neg(q))) = 0.$$

Also ist

$$I\,(\neg\,((p) \wedge (\neg(q)))) = 1.$$

Andererseits ist

$$I(r) = 0$$

und daher ist

$$I(\alpha) = 0.$$

Der Ausdruck ist also bei dieser Wahrheitsbelegung nicht wahr.

2. Arbeitsblatt

2.1. Übungsaufgaben.

Aufgabe 2.1. Sei $S = \{A, B, C\}$. Betrachte die rekursiv definierte Teilmenge $T \subseteq S^*$, die wie folgt festgelegt wird.

(1) Jedes Element aus S gehört zu T.
(2) Wenn $X, Y \in T$ sind, so gehört auch XXY zu T.

Bestimme, welche der folgenden Wörter zu T gehören.

A, $ABABC$, $AABBB$, $AABAABA$, $AAAA$, $AABABAAB$, $AAAAAABBB$.

Zeige die folgenden Aussagen.

(1) Jedes Element aus T besitzt eine ungerade Wortlänge.
(2) Jede ungerade Zahl kommt als Wortlänge eines Elements aus T vor.
(3) Es gibt Elemente in T, die auf mehrfache Weise generiert werden können.
(4) Jedes Wort $t \in T \setminus S$ beginnt mit zwei gleichen Buchstaben.

Aufgabe 2.2. Ein Geldfälscher stellt 3- und 7-Euro-Scheine her.

(1) Beschreibe die Menge M der vollen Eurobeträge, die er mit seinen Scheinen (exakt) begleichen kann, als eine rekursive Teilmenge von $\mathbb{N}$, also durch eine Startmenge und Rekursionsvorschriften.
(2) Zeige, dass es nur endlich viele Beträge gibt, die er nicht begleichen kann. Was ist der höchste Betrag, den er nicht begleichen kann?
(3) Was ist der kleinste Betrag, den er auf zwei verschiedene Weisen begleichen kann.

Aufgabe 2.3. Wir betrachten die rekursiv definierte Teilmenge M von $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, die durch die Startmenge $S = \{(0, 0)\}$ und die folgenden Rekursionsvorschriften gegeben ist.

(1) Wenn $P \in M$ ist, so ist auch $P + (3, 0) \in M$.
(2) Wenn $P \in M$ ist, so ist auch $P + (-1, -2) \in M$.
(3) Wenn $P \in M$ ist, so ist auch $P + (2, 7) \in M$.

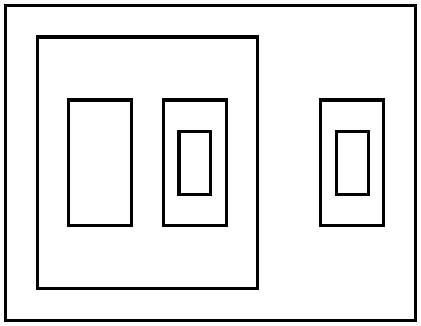
Zeige die folgenden Aussagen.

(1) Der Punkt $(-3, 0)$ gehört zu M.
(2) Der Punkt $(0, 3)$ gehört zu M.
(3) Der Punkt $(0, -3)$ gehört zu M.
(4) Ein Punkt $Q \in M$ besitzt im Allgemeinen keine eindeutige Generierung.
(5) Jeder Punkt $Q = (a, b) \in M$ besitzt die Eigenschaft, dass $a + b$ ein Vielfaches von 3 ist.
(6) Wenn $Q = (a, b) \in \mathbb{Z}^2$ die Eigenschaft besitzt, dass $a+b$ ein Vielfaches von 3 ist, so ist $Q \in M$.

Aufgabe 2.4. Eine Geschenkfabrik verfügt über leere, offene Schachteln (unterschiedlicher Größe) und über Maschinen, die die beiden folgenden Abläufe durchführen können.

(1) Eine offene Schachtel schließen.
(2) Eine geschlossene Schachtel in eine größere offene Schachtel (in der schon andere Schachteln liegen dürfen) hineinlegen.

Ein Produkt der Fabrik ist das Ergebnis aus diesen (beliebig verschachtelten) Abläufen.



(1) Definiere (induktiv) die Schachtelanzahl eines Produkts der Fabrik.
(2) Definiere die Verschachtelungstiefe eines Produkts der Fabrik.
(3) Definiere die Arbeitsschrittanzahl eines Produkts der Fabrik.
(4) Bestimme die Schachtelanzahl, die Verschachtelungstiefe und die Arbeitsschrittanzahl des gezeigten Produkts (die Schachteln seien geschlossen).
(5) Zeige, dass jedes Produkt der Fabrik nur maximal eine offene Schachtel enthält.
(6) Welche Gleichheitsbegriffe sind für die Produkte der Firma sinnvoll? Welche Produkte lassen sich auf unterschiedliche Arten generieren?

Sind die unter (1), (2), (3) definierten Begriffe wohldefiniert, also unabhängig vom Generierungsprozess?

Aufgabe 2.5. Erstelle eine rekursive Definition für die Menschheit.

Aufgabe 2.6.*

Bei einem Zwei-Personen-Regel-Spiel (wie Schach) spielen zwei Personen (A und B) nach gewissen Regeln gegeneinander. Die Personen ziehen abwechselnd. Es ist klar, was eine Mattgewinnstellung für A ist, da ist A am Zug und kann B schlagen und das Spiel ist beendet. Definiere rekursiv, was innerhalb der Menge S aller Stellungen eine Gewinnstellung für A (mit A am Zug) ist.

Aufgabe 2.7. Artikuliere die beiden folgenden Brüche mit „tel“

(1) $\frac{5700}{23}$
(2) $\frac{5000}{723}$.

Die folgende Aufgabe verwendet den Begriff abzählbar.

Eine Menge M heißt *abzählbar*, wenn sie leer ist oder wenn es eine surjektive Abbildung

$$\varphi\colon \mathbb{N} \longrightarrow M$$

gibt.

Für diesen Begriff und das Mächtigkeitskonzept im Allgemeinen siehe den Anhang über Mächtigkeiten. Eine Menge M ist genau dann abzählbar unendlich, wenn es eine bijektive Abbildung

$$\psi\colon \mathbb{N} \longrightarrow M$$

gibt. Die Menge der rationalen Zahlen sind abzählbar unendlich, die Menge der reellen Zahlen nicht.

Aufgabe 2.8. Es sei A ein abzählbares Alphabet. Zeige, dass auch die Menge A^* der Wörter über A abzählbar ist.

Aufgabe 2.9. Es sei A ein Alphabet mit 5 Symbolen. Wie viele Wörter über A der Länge 7 gibt es, wenn man nicht zwischen den Leserichtungen unterscheiden kann?

Aufgabe 2.10. Es sei ein DNA-Doppelstrang der Länge n gegeben. Wie viele Möglichkeiten gibt es dafür bei $n = 1, 2$, wenn man weder die beiden Stränge noch die Leserichtungen unterscheiden kann.

Aufgabe 2.11. Bei einer Leiter sollen die an den Holmen austretenden Sprossenenden farblich markiert werden. Es stehen drei Farben zur Verfügung, und die Leiter hat sechs Sprossen. Wie viele Färbungsmöglichkeiten gibt es, wenn die farblose Leiter weder oben/unten noch links/rechts kennt?

Aufgabe 2.12. Es seien A und B Alphabete und sei $\varphi\colon\ A \to B$ eine Abbildung. Zeige, dass dies eine natürliche Abbildung

$$\tilde{\varphi}\colon\ A^* \longrightarrow B^*$$

zwischen den Wortmengen induziert. Zeige, dass φ genau dann injektiv (surjektiv) ist, wenn $\tilde{\varphi}$ injektiv (surjektiv) ist.

Aufgabe 2.13. Es sei A ein Alphabet mit 4 Symbolen. Wie viele Wörter der Länge 9 gibt es über A, wenn man Symbole in einem Wort simultan vertauschen kann?

Aufgabe 2.14. Zeige, dass das erste Symbol in jeder Aussage aus L^V entweder eine Aussagenvariable $p \in V$ oder das Negationszeichen $\neg$ oder eine linksseitige Klammer (ist.

Aufgabe 2.15.*

Beweise durch Induktion über den rekursiven Aufbau der Sprache L^V, dass in jeder Aussage $\alpha \in L^V$ die Anzahl der linken Klammern mit der Anzahl der rechten Klammern übereinstimmt.

Aufgabe 2.16. Zeichne einen Abstammungsbaum für die Aussage

$$((p) \wedge (\neg(q))) \wedge (\neg(r))\,.$$

Aufgabe 2.17. Zeichne einen Abstammungsbaum für die Aussage

$$((\neg(\neg(p))) \leftrightarrow (\neg(q))) \vee ((p) \to ((\neg(r)) \wedge (\neg(q))))\,.$$

Aufgabe 2.18. Es sei ein aussagenlogischer Ausdruck der Form

$$(...) * (...)$$

gegeben, wobei $* = \wedge, \vee, \to, \leftrightarrow$ ist. Es sei vorausgesetzt, dass die Klammer) links von $*$ die linke öffnende Klammer abschließt (wie ist das zu definieren?). Zeige, dass dann die Zeichenketten innerhalb der beiden Klammern Aussagen sind, und dass der Gesamtausdruck durch einen dritten Schritt im rekursiven Aufbau der Sprache aus diesen beiden Aussagen entstanden ist. Zeige, dass dies ohne die Klammervoraussetzung nicht der Fall sein muss.

Aufgabe 2.19. Zeige, dass der letzte Konstruktionsschritt einer Aussage eindeutig bestimmt ist. Folgere, dass sich die rekursive Entstehung einer Aussage eindeutig rekonstruieren lässt.

Aufgabe 2.20.*

Definiere zu jeder Aussage $\alpha \in L^V$ die Menge Var (α) der in α vorkommenden Aussagenvariablen.

Aufgabe 2.21. Es seien V und W Aussagenvariablenmengen und $\varphi\colon\ V \to W$ eine Abbildung. Zeige, dass dies eine natürliche Abbildung

$$L^{\varphi}\colon\ L^V \longrightarrow L^W$$

induziert.

Aufgabe 2.22. Finde einen möglichst einfachen aussagenlogischen Ausdruck, der die folgende tabellarisch dargestellte Wahrheitsfunktion ergibt.

p	q	?
w	w	w
w	f	f
f	w	f
f	f	f

Aufgabe 2.23. Bestimme den Wahrheitswert der Aussage

$$((\neg(\neg(p))) \leftrightarrow (\neg(q))) \vee ((p) \to ((\neg(r)) \wedge (\neg(q))))$$

bei der Belegung $\lambda(p) = 0$ und $\lambda(q) = \lambda(r) = 1$.

Aufgabe 2.24. Bestimme zu jedem Ausdruck $\alpha \in L^V$ mit maximal acht Zeichen zur Aussagenvariablenmenge $V = \{p, q\}$, ob er bei der durch $\lambda(p) = 1$, $\lambda(q) = 0$ fetgelegten Interpretation wahr oder falsch ist.

Aufgabe 2.25. Finde möglichst einfache aussagenlogische Ausdrücke, die die folgenden tabellarisch dargestellten Wahrheitsfunktionen ergeben.

p	q	?
w	w	w
w	f	f
f	w	f
f	f	w

p	q	?
w	w	f
w	f	f
f	w	w
f	f	f

p	q	?
w	w	f
w	f	f
f	w	f
f	f	f

Aufgabe 2.26. Zeige, dass die Interpretation einer Aussage $\alpha \in L^V$ nur von der Wahrheitsbelegung der in α vorkommenden Aussagenvariablen abhängt.

Aufgabe 2.27. Es seien V und W Aussagenvariablenmengen, $\varphi\colon V \to W$ eine Abbildung und $L^\varphi\colon L^V \to L^W$ die nach Aufgabe 2.21 zugehörige Abbildung. Es sei λ eine Wahrheitsbelegung auf W. Zeige

$$I^{\lambda\circ\varphi} = I^\lambda \circ L^\varphi.$$

Aufgabe 2.28. Die Aussage $\alpha \vee \neg\alpha$ ist eine Tautologie. Ist somit die Frage „Gilt α oder $\neg\alpha$?“ unsinnig?

2.2. **Aufgaben zum Abgeben.**

Aufgabe 2.29. (4 (1+2+1) Punkte)

Ein Geldfälscher stellt 4-, 9- und 11-Euro-Scheine her.

(1) Beschreibe die Menge M der vollen Eurobeträge, die er mit seinen Scheinen (exakt) begleichen kann, als eine rekursive Teilmenge von $\mathbb{N}$, also durch eine Startmenge und Rekursionsvorschriften.
(2) Zeige, dass es nur endlich viele Beträge gibt, die er nicht begleichen kann. Was ist der höchste Betrag, den er nicht begleichen kann?
(3) Was ist der kleinste Betrag, den er auf zwei verschiedene Weisen begleichen kann.

Aufgabe 2.30. (2 Punkte)

Es sei ein DNA-Doppelstrang der Länge n gegeben. Wie viele Möglichkeiten gibt es dafür bei $n = 3, 4$, wenn man weder die Stränge noch die Leserichtungen unterscheiden kann.

Aufgabe 2.31. (2 Punkte)

Zeichne einen Abstammungsbaum für die Aussage

$$(((\neg(\neg(p))) \to (\neg(q))) \vee (\neg(r))) \leftrightarrow ((\neg(r)) \wedge (q))\,.$$

Aufgabe 2.32. (2 Punkte)

Bestimme den Wahrheitswert der Aussage

$$(((\neg(\neg(p))) \to (\neg(q))) \vee (\neg(r))) \leftrightarrow ((\neg(r)) \wedge (q))$$

bei der Belegung $\lambda(p) = \lambda(r) = 0$ und $\lambda(q) = 1$.

Aufgabe 2.33. (3 Punkte)

Es seien $p_1, \ldots, p_n$ Aussagenvariablen und $\beta_1, \ldots, \beta_n$ Aussagen. Zeige durch Induktion über den Aufbau der aussagenlogischen Sprache, dass man zu jeder Aussage α in den gegebenen Variablen eine Aussage erhält, wenn man jedes Vorkommen von p_i in α durch β_i ersetzt.

Aufgabe 2.34. (4 Punkte)

Beweise durch Induktion über den rekursiven Aufbau der Sprache L^V, dass in jeder Aussage $\alpha \in L^V$ und für jedes Symbol s in α, das keine Klammer ist, folgendes zutrifft: Links von s ist die Anzahl der linken Klammern mindestens so groß wie die Anzahl der rechten Klammern.

3. Vorlesung - Tautologien

3.1. **Tautologien.**

In der letzten Vorlesung haben wir erklärt, wie man ausgehend von einer Wahrheitsbelegung λ der Aussagenvariablen aus V zu einer Interpretation $I = I^\lambda$ einer jeden Aussage $\alpha \in L^V$ kommt. Dabei hängt der Wahrheitsgehalt im Allgemeinen von λ und von α ab. Eine besondere Situation liegt vor, wenn der Wahrheitswert von α nicht von der Belegung abhängt, also der Aussage immanent ist.

Definition 3.1. Ein Ausdruck

$$\alpha \in L^V$$

(zu einer Menge von Aussagenvariablen V) heißt *allgemeingültig* (oder eine semantische *Tautologie*,) wenn für jede Wahrheitsbelegung λ die Beziehung

$$I^\lambda(\alpha) = 1$$

gilt.

Bemerkung 3.2. Den Wahrheitswert eines Ausdrucks $\alpha \in L^V$ unter der Interpretation I^λ zu einer Belegung λ kann man übersichtlich berechnen, wenn man abhängig von den Variablenwerten (für die in α auftretenden Variablen) sukzessive die Werte der konstituierenden Bestandteile von α berechnet. Um festzustellem, ob eine Tautologie vorliegt, legt man eine *Wahrheitstabelle* an, bei der die Zeilen durch die möglichen Kombinationen an 0, 1-Werten der einzelnen (in α vorkommenden) Variablen gegeben sind. Am übersichtlichsten wird die Tabelle, wenn man sich bei der Zeilenreihenfolge an das Dualsystem hält. Bei n Variablen gibt es (neben der Kopfzeile) 2^n Zeilen.

Beispiel 3.3. Der Ausdruck (wir verzichten hier und im Folgenden häufig auf Klammern)

$$\varphi \;=\; (\alpha \to \beta) \leftrightarrow (\neg\beta \to \neg\alpha),$$

genannt *Kontraposition*, ist eine Tautologie (unabhängig davon, ob α, β Aussagenvariablen oder Aussagen bezeichnen). Um dies nachzuweisen, muss man den Wahrheitswert dieses Ausdruckes bei jeder Wahrheitsbelegung berechnen, was wir mit einer Wahrheitstabelle durchführen.

Kontraposition

α	β	$\alpha \to \beta$	$\neg\alpha$	$\neg\beta$	$\neg\beta \to \neg\alpha$	$(\alpha \to \beta) \leftrightarrow (\neg\beta \to \neg\alpha)$
w	w	w	f	f	w	w
w	f	f	f	w	f	w
f	w	w	w	f	w	w
f	f	w	w	w	w	w

Dagegen ist der Ausdruck

$$\varphi \;=\; (\neg\,((p) \wedge (\neg(q)))) \to (r)$$

keine Tautologie, da wir in Beispiel 2.13 eine Wahrheitsbelegung mit dem Gesamtwert f angegeben haben.

Definition 3.4. Ein Ausdruck

$$\alpha \in L^V$$

(zu einer Menge von Aussagenvariablen V) heißt (semantische) *Kontradiktion* (oder *Widerspruch*), wenn für jede Wahrheitsbelegung λ die Beziehung

$$I(\alpha) \;=\; 0$$

gilt.

Definition 3.5. Es sei V eine Menge von Aussagenvariablen und L^V die zugehörige aussagenlogische Sprache. Eine Teilmenge $\Gamma \subseteq L^V$ heißt *erfüllbar*, wenn es eine Wahrheitsbelegung λ mit zugehöriger Interpretation I derart gibt, dass $I(\alpha) = 1$ für alle $\alpha \in \Gamma$ gilt.

Diese Sprechweise verwendet man insbesondere für einen einzelnen Ausdruck $\alpha \in \Gamma^V$.

Lemma 3.6. *Ein Ausdruck*

$$\alpha \in L^V$$

(zu einer Menge von Aussagenvariablen V) ist genau dann eine (semantische) Tautologie, wenn $\neg\alpha$ nicht erfüllbar ist.

Beweis. Wir beweisen die kontraponierte Aussage, dass α genau dann keine Tautologie ist, wenn $\neg\alpha$ erfüllbar ist. Dass keine Tautologie vorliegt, bedeutet, dass es eine Wahrheitsbelegung λ derart gibt, dass

$$I^\lambda(\alpha) = 0.$$

Dies bedeutet aber

$$I^\lambda(\neg\alpha) = 1,$$

was gerade die Erfüllbarkeit von $\neg\alpha$ besagt. □

3.2. **Die Folgerungsbeziehung.**

In gewissen Situationen interessiert man sich dafür, welche Ausdrücke aus einer bestimmten Menge von Ausdrücken, etwa einem Axiomensystem, gefolgert werden können.

Definition 3.7. Es sei V eine Menge von Variablen und L^V die zugehörige aussagenlogische Sprache. Es sei $\Gamma \subseteq L^V$ eine Teilmenge und $\alpha \in L^V$. Man sagt, dass α aus Γ *folgt*, geschrieben $\Gamma \vDash \alpha$, wenn für jede Interpretation I (gegeben durch eine Wahrheitsbelegung λ) mit $I \vDash \Gamma$ auch $I \vDash \alpha$ gilt.

Für die Menge aller Aussagen, die aus der Aussagenmenge Γ folgt, schreiben wir $\Gamma^\vDash$. Tautologien sind genau die aus der leeren Ausdrucksmenge $\Gamma = \emptyset$ folgerbaren Aussagen. Daher schreibt man für Tautologien auch $\vDash \alpha$.

3.3. **Ein Ableitungskalkül für die aussagenlogischen Tautologien.**

Wir formulieren nun einen syntaktischen Ableitungskalkül für (syntaktische) Tautologien. Dieser generiert, ausgehend von gewissen axiomatisch fixierten Grundtautologien, rekursiv eine Menge von Aussagen, die, wie wir später sehen werden, mit der Menge der allgemeingültigen Sätzen (semantische Tautologien) übereinstimmt. Wir arbeiten allein mit den logischen Symbolen $\neg, \wedge, \rightarrow$, d.h. wir verzichten auf $\vee$ und auf $\leftrightarrow$. Dies reduziert die Ausdrucksstärke der Sprache nicht, da man $\alpha \leftrightarrow \beta$ als Abkürzung für $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$ und $\alpha \vee \beta$ als Abkürzung für $\neg\alpha \rightarrow \beta$ einführen kann. Um Klammern zu sparen verwenden wir die Konvention, dass die Negation sich auf das folgende Zeichen bezieht und dass die Konjunktion stärker bindet als die Implikation. Man könnte auch die Implikation $\alpha \rightarrow \beta$ durch $\neg(\alpha \wedge \neg\beta)$ definieren und eliminieren, doch dann würden die Ausdrücke sehr unübersichtlich. Ferner ist die Grundform einer mathematischen Aussage vom Typ $\alpha_1 \wedge \ldots \wedge \alpha_n \rightarrow \beta$.

Axiom 3.8. Für eine Aussagenvariablenmenge V und beliebige Ausdrücke α, β, γ legt man folgende (syntaktische) *Tautologien* axiomatisch fest.

(1)
$$\vdash \alpha \to (\beta \to \alpha)\,.$$

(2)
$$\vdash (\alpha \to \beta) \wedge (\beta \to \gamma) \to (\alpha \to \gamma)\,.$$

(3)
$$\vdash (\alpha \to \beta) \wedge (\alpha \to \gamma) \to (\alpha \to \beta \wedge \gamma)\,.$$

(4)
$$\vdash (\alpha \wedge \beta \to \gamma) \to (\alpha \to (\beta \to \gamma))$$

und
$$\vdash (\alpha \to (\beta \to \gamma)) \to (\alpha \wedge \beta \to \gamma)\,.$$

(5)
$$\vdash \neg\alpha \wedge \alpha \to \beta\,.$$

(6)
$$\vdash (\alpha \to \beta) \wedge (\neg\alpha \to \beta) \to \beta\,.$$

Man spricht häufig auch genauer von *Axiomenschemata*, da jedes Axiom bei unterschiedlichen Einsetzungen eine Vielzahl von Axiomen representiert. Das *Kettenschlussaxiom* (2) besagt die *Transitivität der Implikation*, Axiom (5) heißt *Widerspruchsaxiom* und Axiom (6) heißt *Fallunterscheidungsaxiom*. Diese Tautologien sind die axiomatisch fixierten Grundtautologien und fungieren als die Startglieder im rekursiven Aufbau der syntaktischen Tautologien. Um überhaupt aus diesen Axiomen weitere Tautologien generieren zu können, braucht man Ableitungsregeln. Davon gibt es lediglich eine.

Modus Ponens

Aus $\vdash \alpha$ und $\vdash (\alpha) \to (\beta)$ folgt $\vdash \beta$.

Definition 3.9. Unter einer *syntaktischen Tautologie* versteht man einen Ausdruck $\alpha \in L^V$ (zu einer Aussagenvariablenmenge V), den man aus den Grundtautologien rekursiv mittels Modus Ponens erhalten kann.

Die Menge aller syntaktischen Tautologien bilden also eine rekursiv definierte Teilmenge von L^V.

Bemerkung 3.10. Eine Durchsicht der Grundtautologien zeigt, dass es sich jeweils auch um semantische Tautologien handelt, siehe Aufgabe 3.32. Wenn ferner α und $(\alpha) \to (\beta)$ semantische Tautologien sind, so ist auch β eine semantische Tautologie. D.h. die semantischen Tautologien sind unter Modus Ponens abgeschlossen. Dies bedeutet insgesamt, dass syntaktische Tautologien stets semantische Tautologien sind. Diese Eigenschaft nennt man auch die *Korrektheit* des syntaktischen Kalküls, er leitet ausschließlich semantische Tautologien, also wahre Aussagen ab. Die umgekehrte Aussage, dass sich jede

semantische Tautologie auch syntaktisch in dem angegebenen Kalkül ableiten lässt, nennt man die *Vollständigkeit* des Kalküls.

3.4. **Weitere Tautologien und Regeln.**

Lemma 3.11. *Es ist*

$$\vdash \alpha \to \alpha\,.$$

Beweis. Es ist

$$\vdash (\alpha \to (\alpha \to \alpha)) \wedge (\neg\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$$

nach Axiom 3.8 (6), woraus sich nach Axiom 3.8 (4) mit Modus Pones auch

$$\vdash (\alpha \to (\alpha \to \alpha)) \to ((\neg\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha))$$

ergibt. Wegen Axiom 3.8 (1) ist

$$\vdash \alpha \to (\alpha \to \alpha)$$

und daher mit Modus Ponens auch

$$\vdash (\neg\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)\ .$$

Wegen Axiom 3.8 (5) ist

$$\vdash \neg\alpha \wedge \alpha \to \alpha$$

und damit mit Axiom 3.8 (4) auch

$$\vdash \neg\alpha \to (\alpha \to \alpha)\ ,$$

so dass sich

$$\vdash \alpha \to \alpha$$

ergibt. □

Lemma 3.12. *Für $\alpha, \beta \in L^V$ ist*

$$\vdash \alpha \wedge \beta \to \alpha$$

und

$$\vdash \alpha \wedge \beta \to \beta\,.$$

Beweis. Nach Axiom 3.8 (4) ist

$$\vdash (\alpha \to (\beta \to \alpha)) \to (\alpha \wedge \beta \to \alpha)$$

und wegen Axiom 3.8 (1) ist

$$\vdash \alpha \to (\beta \to \alpha)\ ,$$

so dass mit Modus Ponens auch

$$\vdash \alpha \wedge \beta \to \alpha$$

gilt. Für die andere Behauptung gehen wir von Lemma 3.11 aus, was

$$\vdash \beta \to \beta$$

liefert. Wegen Axiom 3.8 (1) haben wir

$$\vdash (\beta \to \beta) \to (\alpha \to (\beta \to \beta)) \ ,$$

also mit Modus Ponens auch

$$\vdash \alpha \to (\beta \to \beta) \ .$$

Nach Axiom 3.8 (4) ist

$$\vdash (\alpha \to (\beta \to \beta)) \to (\alpha \wedge \beta \to \beta) \ ,$$

woraus sich nach dem bisher Bewiesenen

$$\alpha \wedge \beta \to \beta$$

ergibt. □

Bemerkung 3.13. Die aussagenlogischen Axiome der Form $\vdash \alpha \to \beta$ führen zu entsprechenden Schlussregeln, d.h. Vorschriften, wie man aus (schon etablierten) syntaktischen Tautologien neue Tautologien erhält. Wir gehen unter diesem Gesichtspunkt die Axiome durch.

Aus $\vdash \alpha$ folgt $\vdash \beta \to \alpha$.

Dies ergibt sich aus der Voraussetzung $\vdash \alpha$ aus $\vdash \alpha \to (\beta \to \alpha)$ und dem Modus ponens.

Aus $\vdash \alpha \wedge \beta$ folgt $\vdash \alpha$ (und ebenso $\vdash \beta$).

Dies ergibt sich aus $\vdash \alpha \wedge \beta \to \alpha$ nach Lemma 3.12 und der Voraussetzung $\vdash \alpha \wedge \beta$ mittels Modus Ponens. Umgekehrt gilt die sogenannte *Konjunktionsregel*, d.h. aus $\vdash \alpha$ und $\vdash \beta$ folgt auch $\vdash \alpha \wedge \beta$. Dies ergibt sich aus

$$\vdash \alpha \to (\beta \to \alpha \wedge \beta)$$

(was aus den Axiomen folgt, siehe Aufgabe 3.33) aus den Voraussetzungen durch eine zweifache Anwendung des Modus Ponens.

Aus $\vdash \alpha \to \beta$ und $\vdash \beta \to \gamma$ ergibt sich $\vdash \alpha \to \gamma$. Diese Regel heißt *Kettenschlussregel*. Nach der obigen abgeleiteten Konjunktionsregel folgt aus den Voraussetzungen direkt $\vdash (\alpha \to \beta) \wedge (\beta \to \gamma)$ und daraus und dem Kettenschlussaxiom mit dem Modus Ponens $\vdash \alpha \to \gamma$.

Lemma 3.14. *Es ist*

$$\vdash \alpha \wedge \beta \to \beta \wedge \alpha \, .$$

Beweis. Nach Axiom 3.8 (3) ist

$$\vdash ((\alpha \wedge \beta) \to \beta) \wedge ((\alpha \wedge \beta) \to \alpha) \to (\alpha \wedge \beta \to \beta \wedge \alpha) \, .$$

Die beiden Bestandteile des Vordersatzes gelten nach Lemma 3.12, so dass auch ihre Konjunktion ableitbar ist. Daher ist auch der Nachsatz ableitbar. □

Lemma 3.15. *Es ist*

$$\vdash (\alpha \wedge \beta) \wedge \gamma \to \alpha \wedge (\beta \wedge \gamma) \ .$$

Beweis. Siehe Aufgabe 3.34. □

Lemma 3.16. (1)

$$\vdash (\alpha \to \beta) \to (\alpha \wedge \gamma \to \beta)\,.$$

(2)

$$\vdash (\alpha \to \beta) \wedge (\gamma \to \delta) \to (\alpha \wedge \gamma \to \beta \wedge \delta)\,.$$

Beweis. (1) Nach Axiom 3.8 (2) ist

$$\vdash (\alpha \wedge \gamma \to \alpha) \wedge (\alpha \to \beta) \to (\alpha \wedge \gamma \to \beta)$$

und daher mit Axiom 3.8 (4) auch

$$\vdash (\alpha \wedge \gamma \to \alpha) \to ((\alpha \to \beta) \to (\alpha \wedge \gamma \to \beta))\,.$$

Der Vordersatz ist nach Lemma 3.12 ableitbar, also auch der Nachsatz.

(2) Nach Teil (1) ist

$$\vdash (\alpha \to \beta) \to (\alpha \wedge \gamma \to \beta)$$

und (unter Verwendung von Lemma 3.14 und Aufgabe 3.38)

$$\vdash (\gamma \to \delta) \to (\alpha \wedge \gamma \to \delta)\,.$$

Daher gilt auch (nach der Regelversion zu Teil (1))

$$\vdash (\alpha \to \beta) \wedge (\gamma \to \delta) \to (\alpha \wedge \gamma \to \beta)$$

und

$$\vdash (\alpha \to \beta) \wedge (\gamma \to \delta) \to (\alpha \wedge \gamma \to \delta)$$

bzw. unter Verwendung von Axiom 3.8 (4) und der Assoziativität der Konjunktion

$$\vdash (\alpha \to \beta) \wedge (\gamma \to \delta) \wedge \alpha \wedge \gamma \to \beta$$

und

$$\vdash (\alpha \to \beta) \wedge (\gamma \to \delta) \wedge \alpha \wedge \gamma \to \delta\,.$$

Nach Axiom 3.8 (3) ist mit der Abkürzung $\varphi = (\alpha \to \beta) \wedge (\gamma \to \delta) \wedge \alpha \wedge \gamma$

$$\vdash (\varphi \to \beta) \wedge (\varphi \to \delta) \to (\varphi \to \beta \wedge \delta)\,.$$

Da die beiden Teilaussagen im Vordersatz ableitbar sind, ist auch der Nachsatz ableitbar, was unter Verwendung von Axiom 3.8 (4) zur Behauptung umformulierbar ist.

□

Die folgende Aussage gibt eine „interne Version“ des Modus Ponens, der ja nach Definition eine Schlussregel ist.

Lemma 3.17. *Es ist*

$$\vdash \alpha \wedge (\alpha \to \beta) \to \beta\,.$$

Beweis. Nach Axiom 3.8 (6) ist

$$\vdash (\alpha \to \beta) \wedge (\neg\alpha \to \beta) \to \beta\,,$$

und Axiom 3.8 (5) kann man wegen Axiom 3.8 (4) zu

$$\vdash \alpha \to (\neg\alpha \to \beta)$$

umformulieren. Daraus und aus (Lemma 3.11)

$$\vdash (\alpha \to \beta) \to (\alpha \to \beta)$$

ergibt sich mit der Regelversion zu Lemma 3.16 (2)

$$\vdash \alpha \wedge (\alpha \to \beta) \to (\neg\alpha \to \beta) \wedge (\alpha \to \beta)$$

und daraus durch den Kettenschluss die Behauptung. □

Lemma 3.18. (1) *Aus* $\vdash \alpha \to (\beta \to \gamma)$ *und* $\vdash \gamma \to \delta$ *folgt* $\vdash \alpha \to (\beta \to \delta)$.

(2) *Aus* $\vdash \alpha$ *und* $\vdash \alpha \wedge \beta \to \gamma$ *ergibt sich* $\vdash \beta \to \gamma$.

Beweis. (1) Sei

$$\vdash \alpha \to (\beta \to \gamma)$$

und

$$\vdash \gamma \to \delta\,.$$

Nach Bemerkung 3.13 gilt auch

$$\vdash \alpha \to (\gamma \to \delta)$$

und daraus ergibt sich mit Axiom 3.8 (3), der Konjunktionsregel und dem Modus Ponens

$$\vdash \alpha \to (\beta \to \gamma) \wedge (\gamma \to \delta)\,.$$

Mittels des Kettenschlusses ergibt sich daraus und aus Axiom 3.8 (2) die Behauptung.

(2) Siehe Aufgabe 3.48.

□

Die folgenden Tautologien machen wichtige Aussagen über das Negationszeichen. Die Tautologie (2) ist eine wichtige Variante der *Widerspruchstautologie* und die in (5) und (6) ausgedrückte Äquivalenz heißt *Kontraposition*.

Lemma 3.19. (1)

$$\vdash (\neg\alpha \to \alpha) \to \alpha\,.$$

(2)

$$\vdash (\neg\beta \to \neg\alpha) \wedge (\neg\beta \to \alpha) \to \beta$$

(3)

$$\vdash \alpha \to \neg\neg\alpha\,.$$

(4)

$$\vdash \neg\neg\alpha \to \alpha\,.$$

(5)
$$\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)\,.$$
(6)
$$\vdash (\neg\beta \to \neg\alpha) \to (\alpha \to \beta)\,.$$

Beweis. (1) Die Fallunterscheidungstautologie liefert
$$\vdash (\alpha \to \alpha) \wedge (\neg\alpha \to \alpha) \to \alpha\,.$$
Aus (Lemma 3.11)
$$\vdash \alpha \to \alpha$$
ergibt sich daraus die Behauptung.

(2) Nach Axiom 3.8 (3) gilt
$$\vdash (\neg\beta \to \neg\alpha) \wedge (\neg\beta \to \alpha) \to (\neg\beta \to \neg\alpha \wedge \alpha)$$
und nach Axiom 3.8 (5) gilt
$$\vdash \neg\alpha \wedge \alpha \to \beta\,.$$
Nach Lemma 3.18 (1) folgt
$$\vdash (\neg\beta \to \neg\alpha) \wedge (\neg\beta \to \alpha) \to (\neg\beta \to \beta)\,,$$
woraus nach Teil (1) die Behauptung mit der Kettenschlussregel folgt.

(3) Nach Axiom 3.8 (1) ist
$$\vdash \neg\neg\alpha \to (\alpha \to \neg\neg\alpha)\,.$$
Nach Axiom 3.8 (5) ist
$$\vdash \neg\alpha \wedge \alpha \to \neg\neg\alpha\,,$$
was wir mit Axiom 3.8 (4) zu
$$\vdash \neg\alpha \to (\alpha \to \neg\neg\alpha)\,,$$
umformulieren können. Daraus ergibt sich
$$\vdash \alpha \to \neg\neg\alpha$$
mit der Fallunterscheidungsregel.

(4) Nach Axiom 3.8 (1) ist
$$\vdash \alpha \to (\neg\neg\alpha \to \alpha)\,.$$
Nach Axiom 3.8 (5) ist
$$\vdash \neg\alpha \wedge \neg\neg\alpha \to \alpha\,,$$
was wir zu
$$\vdash \neg\alpha \to (\neg\neg\alpha \to \alpha)\,,$$
umformulieren können. Daraus ergibt sich
$$\vdash \neg\neg\alpha \to \alpha$$
mit der Fallunterscheidungsregel.

(5) Es ist nach Axiom 3.8 (1)

$$\vdash \neg\alpha \to (\neg\beta \to \neg\alpha)$$

und damit auch

$$\vdash \neg\alpha \to ((\alpha \to \beta) \to (\neg\beta \to \neg\alpha))\,.$$

Ferner ist nach einer Variante von Axiom 3.8 (5)

$$\vdash \beta \to (\neg\beta \to \neg\alpha)\,.$$

Nach Lemma 3.17 ist

$$\vdash \alpha \to ((\alpha \to \beta) \to \beta)\,,$$

woraus sich

$$\vdash \alpha \to ((\alpha \to \beta) \to (\neg\beta \to \neg\alpha))$$

ergibt. Mit der Fallunterscheidungsregel folgt die Behauptung.

(6) Dies folgt aus (3), (4) und (5).

□

3. Arbeitsblatt

3.1. Übungsaufgaben.

Aufgabe 3.1. Beweise mittels Wahrheitstabellen, dass die folgenden Aussagen Tautologien sind.[4]

(1) $(\alpha \wedge \alpha) \leftrightarrow \alpha$.
(2) $\alpha \wedge \beta \to \alpha$.
(3) $\alpha \to (\beta \to \alpha)$.
(4) $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$.
(5) $(\alpha \to \beta) \leftrightarrow (\neg\alpha \vee \beta)$.

Aufgabe 3.2. Man beweise mittels Wahrheitstabellen die *Regeln von de Morgan*, nämlich dass

$$\neg(\beta \vee \gamma) \leftrightarrow (\neg\beta \wedge \neg\gamma)$$

und

$$\neg(\beta \wedge \gamma) \leftrightarrow (\neg\beta \vee \neg\gamma)$$

Tautologien sind.

Aufgabe 3.3. Skizziere ein Entscheidungsverfahren, das für eine gegebene Aussage $\alpha \in L^V$ entscheidet, ob es sich um eine aussagenlogische Tautologie handelt oder nicht.

[4]Wir verzichten hier und im Folgenden häufig auf Klammern, um die Lesbarkeit zu erhöhen. Gemeint sind immer die korrekt geklammerten Aussagen.

Aufgabe 3.4. Zu einer Aussage $\alpha \in L^V$ und $n \in \mathbb{N}$ bezeichne $\neg^n\alpha$ die n-fache Negation von α. Zeige, dass $\neg^n\alpha \leftrightarrow \neg^m\alpha$ genau dann allgemeingültig ist, wenn $n - m$ ein Vielfaches von 2 ist.

Aufgabe 3.5. Es seien $p_1, \ldots, p_n$ Aussagenvariablen und $\beta_1, \ldots, \beta_n$ Aussagen. Zeige, dass man, wenn man in einer allgemeingültigen Aussage α jedes Vorkommen von p_i durch β_i ersetzt, wieder eine allgemeingültige Aussage erhält. Zeige, dass die Umkehrung davon nicht gilt.

Aufgabe 3.6. Zeige, dass eine Aussage $\alpha \in L^V$ genau dann eine Kontradiktion ist, wenn $\neg\alpha$ eine Tautologie ist.

Aufgabe 3.7. Man gebe möglichst viele Beispiele für aussagenlogische Kontradiktionen an.

Aufgabe 3.8. Es sei V eine Menge von Aussagenvariablen und α eine Aussage in der zugehörigen formalen Sprache L^V. Es sei

$$\varphi\colon\ V \longrightarrow V$$

eine Abbildung und es sei $\varphi(\alpha)$ diejenige Aussage, die entsteht, wenn man in α jede Aussagenvariable p durch $\varphi(p)$ ersetzt. Zeige die folgenden Aussagen.

(1) Wenn α eine Tautologie ist, so ist auch $\varphi(\alpha)$ eine Tautologie.
(2) Wenn φ injektiv ist, so ist α genau dann eine Tautologie, wenn dies für $\varphi(\alpha)$ gilt.
(3) $\varphi(\alpha)$ kann eine Tautologie sein, auch wenn α keine Tautologie ist.
(4) Die Aussagen gelten ebenso, wenn man überall Tautologie durch Kontradiktion ersetzt.

Aufgabe 3.9. Es sei $\Gamma \subseteq L^V$ eine Teilmenge, die ausschließlich aus Aussagenvariablen oder aus negierten Aussagenvariablen besteht, wobei jede Aussagenvariable höchstens direkt oder in ihrer Negation auftritt. Zeige, dass Γ erfüllbar ist.

Aufgabe 3.10.*

Wenn Karl an Susanne denkt, bekommt er feuchte Hände, einen Kloß im Hals und einen roten Kopf. Einen roten Kopf bekommt er genau dann, wenn er an Susanne denkt oder wenn er das leere Tor nicht trifft. Wenn Karl das leere Tor trifft, bekommt er feuchte Hände. Karl bekommt den Ball vor dem leeren Tor. Kurz darauf bekommt er feuchte Hände, einen roten Kopf, aber keinen Kloß im Hals. Hat er an Susanne gedacht? Hat er das leere Tor getroffen?

Aufgabe 3.11.*

Folgende Aussagen seien bekannt.

(1) Der frühe Vogel fängt den Wurm.
(2) Doro wird nicht von Lilly gefangen.
(3) Lilly ist ein Vogel oder ein Igel.
(4) Für Igel ist 5 Uhr am Morgen spät.
(5) Doro ist ein Wurm.
(6) Für Vögel ist 5 Uhr am Morgen früh.
(7) Lilly schläft bis 5 Uhr am Morgen und ist ab 5 Uhr unterwegs.

Beantworte folgende Fragen.

(1) Ist Lilly ein Vogel oder ein Igel?
(2) Ist sie ein frühes oder ein spätes Tier?
(3) Fängt der späte Igel den Wurm?

Aufgabe 3.12.*

Der Professor kommt gelegentlich mit verschiedenen Socken und/oder mit verschiedenen Schuhen in die Universität. Er legt folgende Definitionen fest.

(1) Ein Tag heißt *sockenzerstreut*, wenn er verschiedene Socken anhat.
(2) Ein Tag heißt *schuhzerstreut*, wenn er verschiedene Schuhe anhat.
(3) Ein Tag heißt *zerstreut*, wenn er sockenzerstreut oder schuhzerstreut ist.
(4) Ein Tag heißt *total zerstreut*, wenn er sowohl sockenzerstreut als auch schuhzerstreut ist.

a) Vom Jahr 2015 weiß man, dass 17 Tage sockenzerstreut und 11 Tage schuhzerstreut waren. Wie viele Tage waren in diesem Jahr maximal zerstreut und wie viele Tage waren minimal zerstreut? Wie viele Tage waren in diesem Jahr maximal total zerstreut und wie viele Tage waren minimal total zerstreut?

b) Vom Jahr 2013 weiß man, dass 270 Tage sockenzerstreut und 120 Tage schuhzerstreut waren. Wie viele Tage waren in diesem Jahr maximal zerstreut und wie viele Tage waren minimal total zerstreut?

c) Erstelle eine Formel, die die Anzahl der sockenzerstreuten, der schuhzerstreuten, der zerstreuten und der total zerstreuten Tage in einem Jahr miteinander in Verbindung bringt.

Die folgenden Aufgaben verwenden den Begriff einer Äquivalenzrelation. Dieser ist für viele Konstruktionen in der Mathematik und in der mathematischen Logik entscheidend. Siehe den Anhang zu Äquivalenzrelationen.

Eine *Äquivalenzrelation* auf einer Menge M ist eine Relation $R \subseteq M \times M$, die die folgenden drei Eigenschaften besitzt (für beliebige $x, y, z \in M$).

(1) Es ist $x \sim x$ (*reflexiv*).
(2) Aus $x \sim y$ folgt
$y \sim x$ (*symmetrisch*).
(3) Aus $x \sim y$ und $y \sim z$ folgt $x \sim z$ (*transitiv*).

Dabei bedeutet $x \sim y$, dass das Paar (x, y) zu R gehört.

Aufgabe 3.13. Auf den ganzen Zahlen $\mathbb{Z}$ lebe eine Kolonie von Flöhen, und jeder Flohsprung geht fünf Einheiten weit (in beide Richtungen). Wie viele Flohpopulationen gibt es? Wie kann man einfach charakterisieren, ob zwei Flöhe zur gleichen Population gehören oder nicht?

Aufgabe 3.14. Wir betrachten die ganzen Zahlen $\mathbb{Z}$ und eine fixierte natürliche Zahl $a \geq 0$. Zeige, dass auf $\mathbb{Z}$ durch

$$x \sim y, \text{ wenn die Differenz } x - y \text{ ein Vielfaches von } a \text{ ist},$$

eine Äquivalenzrelation definiert wird. Wie viele Äquivalenzklassen gibt es?

Aufgabe 3.15. Es sei K ein Körper, V ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum. Wir betrachten die Relation auf V, die durch

$$v_1 \sim v_2 \text{ genau dann, wenn } v_1 - v_2 \in U$$

definiert ist. Zeige, dass diese Relation eine Äquivalenzrelation ist.

Aufgabe 3.16. Es sei K ein Körper und V ein K-Vektorraum. Zeige, dass die Relation auf V, die durch

$$v \sim w, \text{ falls es ein } \lambda \in K, \lambda \neq 0, \text{ mit } v = \lambda w \text{ gibt}$$

eine Äquivalenzrelation ist. Was sind die Äquivalenzklassen?

Aufgabe 3.17. Wir betrachten für je zwei Teilmengen $A, B \subseteq \mathbb{N}$ die symmetrische Differenz

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Wir setzen

$$A \sim B,$$

falls $A \triangle B$ endlich ist. Zeige, dass dadurch eine Äquivalenzrelation auf $\mathfrak{P}(\mathbb{N})$ definiert wird.

Aufgabe 3.18.*

Betrachte auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ die Relation

$$(a, b) \sim (c, d), \text{ falls } ad = bc \text{ ist}.$$

a) Zeige, dass $\sim$ eine Äquivalenzrelation ist.

b) Zeige, dass es zu jedem (a, b) ein äquivalentes Paar (a', b') mit $b' > 0$ gibt.

c) Es sei M die Menge der Äquivalenzklassen dieser Äquivalenzrelation. Wir definieren eine Abbildung

$$\varphi\colon\ \mathbb{Z} \longrightarrow M,\ z \longmapsto [(z, 1)].$$

Zeige, dass φ injektiv ist.

d) Definiere auf M (aus Teil c) eine Verknüpfung $+$ derart, dass M mit dieser Verknüpfung und mit $[(0, 1)]$ als neutralem Element eine Gruppe wird, und dass für die Abbildung φ die Beziehung

$$\varphi(z_1 + z_2) \ = \ \varphi(z_1) + \varphi(z_2)$$

für alle $z_1, z_2 \in \mathbb{Z}$ gilt.

Aufgabe 3.19.*

Seien M und N Mengen und sei $f\colon\ M \to N$ eine Abbildung. Zeige, dass durch die Festlegung

$$x \ \sim \ y,$$

wenn

$$f(x) \ = \ f(y),$$

eine Äquivalenzrelation auf M definiert wird.

Aufgabe 3.20.*

Es sei M die Menge der zweimal stetig differenzierbaren Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Definiere auf M eine Relation durch

$$f \sim g \text{ falls } f(0) = g(0),\ f'(0) = g'(0) \text{ und } f''(1) = g''(1)\,.$$

a) Zeige, dass dies eine Äquivalenzrelation ist.

b) Finde für jede Äquivalenzklasse dieser Äquivalenzrelation einen polynomialen Vertreter.

c) Zeige, dass diese Äquivalenzrelation mit der Addition von Funktionen verträglich ist.

d) Zeige, dass diese Äquivalenzrelation nicht mit der Multiplikation von Funktionen verträglich ist.

Aufgabe 3.21. Es sei $U \subseteq \mathbb{R}^n$ eine Teilmenge mit der induzierten Metrik. Betrachte die Relation R auf U, wobei xRy bedeutet, dass es eine stetige Abbildung

$$\gamma\colon\ [0,1] \longrightarrow \mathbb{R}^n,\ t \longmapsto \gamma(t),$$

mit $\gamma(0) = x$ und $\gamma(1) = y$ gibt. Zeige, dass dies eine Äquivalenzrelation auf U ist.

Aufgabe 3.22. Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M mit den Äquivalenzklassen $[x]$. Es sei I die Menge aller Äquivalenzklassen. Zeige folgende Aussagen.

(1) Es ist $x \sim y$ genau dann, wenn $[x] = [y]$ ist, und dies gilt genau dann, wenn $[x] \cap [y] \neq \emptyset$.
(2) $M = \bigcup_{x \in I} [x]$ ist eine disjunkte Vereinigung.

Aufgabe 3.23. Sei B ein Blatt Papier (oder ein Taschentuch). Man versuche, sich die folgenden Äquivalenzrelationen auf B und die zugehörige Identifizierungsabbildungen vorzustellen (möglichst geometrisch).

(1) Die vier Eckpunkte sind untereinander äquivalent, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(2) Alle Randpunkte sind untereinander äquivalent, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(3) Jeder Punkt des linken Randes ist äquivalent zu seinem horizontal gegenüber liegenden Punkt am rechten Rand, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(4) Jeder Punkt des linken Randes ist äquivalent zu seinem horizontal gegenüber liegenden Punkt am rechten Rand und jeder Punkt des oberen Randes ist äquivalent zu seinem vertikal gegenüber liegenden Punkt, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(5) Jeder Punkt des Randes ist äquivalent zu seinem punktsymmetrisch (bezüglich des Mittelpunktes des Blattes) gegenüber liegenden Punkt, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(6) Sei K ein Kreis (d.h. eine Kreislinie) auf dem Blatt. Alle Kreispunkte seien untereinander äquivalent, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(7) Es gebe zwei Punkte $P \neq Q$, die untereinander äquivalent seien, ansonsten sind die Punkte nur zu sich selbst äquivalent.
(8) Sei H die horizontale Halbierungsgerade des Blattes. Zwei Punkte sind genau dann äquivalent, wenn sie achsensymmetrisch zu H sind.

Aufgabe 3.24. Zeige, dass die Beziehung

$$\alpha \sim \beta, \text{ falls } (\alpha) \leftrightarrow (\beta) \text{ allgemeingültig ist},$$

eine Äquivalenzrelation auf L^V definiert. Zeige, dass sowohl alle Tautologien als auch alle Kontradiktionen eine Äquivalenzklasse bilden. Wie viele Äquivalenzklassen besitzt diese Äquivalenzrelation, falls V n Elemente besitzt?

Aufgabe 3.25. Es sei $\sim$ die in Aufgabe 3.24 diskutierte Äquivalenzrelation auf L^V und sei Q die zugehörige Quotientenmenge. Es sei λ eine Wahrheitsbelegung auf V. Zeige, dass dies eine wohldefinierte Abbildung auf Q induziert.

Unter einer *disjunktiven Normalform* versteht man einen aussagenlogischen Ausdruck, der eine $\vee$-Verknüpfung von Ausdrücken der Form $\pm p_1 \wedge \ldots \wedge \pm p_n$ ist, wobei $\pm$ bedeutet, dass entweder die Aussagenvariable direkt oder in ihrer Negation genommen wird.

Aufgabe 3.26.*

Man bringe die Aussage

$$((p \vee (r \to q)) \wedge (q \to p)) \vee (((p \wedge \neg q) \wedge (\neg r \vee \neg p)) \wedge (r \to (p \vee \neg q)))$$

in disjunktive Normalform.

Aufgabe 3.27. Es sei $\sim$ die in Aufgabe 3.24 diskutierte Äquivalenzrelation auf L^V. Zeige, dass jede Äquivalenzklasse $[\alpha]$ einen Repräsentanten in disjunktiver Normalform besitzt.

Aufgabe 3.28. Es sei α ein aussagenlogischer Ausdruck in disjunktive Normalform, in dem die Aussagenvariablen $p_1, \ldots, p_n$ vorkommen. Zeige, dass α genau dann eine Tautologie ist, wenn α die $\vee$-Verknüpfung von sämtlichen Kombinationen $\pm p_1 \wedge \ldots \wedge \pm p_n$ ist.

Aufgabe 3.29. Es sei T die Menge aller Tautologien in einer aussagenlogischen Sprache L^V. Zeige $T^{\models} = T$.

Aufgabe 3.30. Die Ausdrucksmenge $\Gamma \subseteq L^V$ enthalte eine Kontradiktion. Zeige $\Gamma^{\models} = L^V$.

Aufgabe 3.31. Interpretiere die Wahrheitstabellen zu den Junktoren $\neg$, $\wedge, \vee, \to, \leftrightarrow$ als Wertetabellen von Funktionen. Was sind die Definitions-, die Werte- und die Bildmengen dieser Funktionen?

Aufgabe 3.32. Zeige, dass die axiomatisch fixierten syntaktischen Grundtautologien allgemeingültig sind

Aufgabe 3.33.*

Beweise die aussagenlogische Tautologie

$$\vdash \alpha \to (\beta \to \alpha \wedge \beta)$$

aus den aussagenlogischen Axiomen.

Aufgabe 3.34. Zeige das Assoziativgesetz für die Konjunktion, also

$$\vdash (\alpha \wedge \beta) \wedge \gamma \to \alpha \wedge (\beta \wedge \gamma) \ .$$

Aufgabe 3.35. Es seien $\alpha_1, \ldots, \alpha_n$ Ausdrücke und es seien $i_1, \ldots, i_k$ Elemente aus $\{1, \ldots, n\}$. Zeige, dass

$$\vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \alpha_{i_1} \wedge \ldots \wedge \alpha_{i_k}$$

gilt.

Aufgabe 3.36.*

Zeige

$$\vdash \alpha \wedge \neg\alpha \to \beta$$

unter Verwendung von

$$\vdash \gamma \wedge \delta \to \delta \wedge \gamma$$

(Lemma 3.14).

Aufgabe 3.37. Zu einer Aussage $\alpha \in L^V$ und $n \in \mathbb{N}$ bezeichne $\neg^n\alpha$ die n-fache Negation von α. Zeige, dass $\vdash \neg^n\alpha \to \neg^m\alpha$ genau dann gilt, wenn $n - m$ ein Vielfaches von 2 ist.

Aufgabe 3.38. Zeige die folgende Ableitungsregel für die Aussagenlogik.

Aus $\vdash \alpha \to (\beta \to \gamma)$ und $\vdash \delta \to \beta$ folgt $\vdash \alpha \to (\delta \to \gamma)$.

Aufgabe 3.39. Zeige, dass aus $\vdash \alpha_1, \ldots, \vdash \alpha_n$ und $\vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \beta$ die Ableitbarkeit $\vdash \beta$ folgt.

Aufgabe 3.40.*

Zeige, dass eine Regel der Form

Wenn $\vdash \alpha$, dann $\vdash \beta$ gelten kann, ohne dass $\vdash \alpha \to \beta$ gilt.

Aufgabe 3.41. Es seien $p_1, \ldots, p_n$ Aussagenvariablen und $\beta_1, \ldots, \beta_n$ Aussagen. Zeige, dass man, wenn man in einer syntaktischen Tautologie α jedes Vorkommen von p_i durch β_i ersetzt, wieder eine Tautologie erhält.

Aufgabe 3.42. Es sei α eine ableitbare Tautologie. Zeige, dass es eine Ableitung für α gibt, bei der in jedem Ableitungsschritt nur Aussagenvariablen auftreten, die in α vorkommen.

Aufgabe 3.43. Skizziere ein Verfahren, wie man (bei V abzählbar) eine Auflistung sämtlicher syntaktischer Tautologien aus L^V erhalten kann.

3.2. **Aufgaben zum Abgeben.**

Aufgabe 3.44. (3 Punkte)

Zeige, dass in einer aussagenlogischen Tautologie (und ebenso in einer aussagenlogischen Kontradiktion) mindestens eine Aussagenvariable mehrfach vorkommen muss.

Aufgabe 3.45. (2 Punkte)

Zeige, dass die Aussage

$$(\alpha \to \beta) \wedge (\beta \to \gamma) \wedge (\neg\alpha \to \beta) \to \gamma$$

allgemeingültig ist.

Aufgabe 3.46. (2 Punkte)

Es sei $\Gamma \subseteq L^V$ eine Aussagenmenge derart, dass in keiner Aussage $\alpha \in \Gamma$ das Negationszeichen $\neg$ vorkommt. Zeige, dass dann die Wahrheitsbelegung, die jeder Aussagenvariablen den Wert 1 zuweist, zu einer Interpretation I mit $\Gamma \subseteq I^{\models}$ führt.

Aufgabe 3.47. (3 Punkte)

Zeige

$$\vdash (\alpha \to \beta) \wedge (\beta \to \gamma) \wedge (\neg\alpha \to \beta) \to \gamma\,.$$

Aufgabe 3.48. (2 Punkte)

Begründe die folgende Ableitungsregel: Aus $\vdash \alpha$ und $\vdash \alpha \wedge \beta \to \gamma$ folgt $\vdash \beta \to \gamma$.

Aufgabe 3.49. (3 Punkte)

Zeige, dass folgende rekursive Definition zur gleichen Menge an syntaktischen Tautologien führt:

Die Grundtautologien werden nur mit Aussagenvariablen formuliert.

Neben dem Modus Ponens gibt es die Ersetzungsregel, d.h. wenn $\vdash \alpha$, so ist auch $\vdash \alpha'$, wobei α' ein Ausdruck ist, der ensteht, wenn man in α Aussagenvariablen durch beliebige Aussagen ersetzt.

Zeige, dass ohne diese Ersetzungsregel nicht die gleiche Menge beschrieben wird.

4. Vorlesung - Vollständigkeit der Aussagenlogik

4.1. **Die Ableitungsbeziehung.**

Die syntaktische Entsprechung zur Folgerungsbeziehung ist die folgende Ableitungsbeziehung.

Definition 4.1. Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V und sei $\alpha \in L^V$. Man sagt, dass α aus Γ *ableitbar* ist, geschrieben

$$\Gamma \vdash \alpha\,,$$

wenn es endlich viele Ausdrücke $\alpha_1, \ldots, \alpha_n \in \Gamma$ derart gibt, dass

$$\vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \alpha$$

gilt.

Die vorgegebene Ausdrucksmenge kann endlich oder unendlich sein, in der Ableitungsbeziehung kommen aber stets nur endlich viele Ausdrücke aus Γ vor (eine „unendliche Konjunktion“ ist gar nicht definiert). Die Menge der aus einer gegebenen Ausdrucksmenge Γ ableitbaren Ausdrücke bezeichnet man mit $\Gamma^{\vdash}$, also

$$\Gamma^{\vdash} = \left\{\alpha \in L^V \,|\, \Gamma \vdash \alpha\right\}.$$

Wegen $\vdash \alpha \to \alpha$ (nach Lemma 3.11) gilt $\Gamma \subseteq \Gamma^{\vdash}$. Bei $\Gamma = \Gamma^{\vdash}$ sagt man, dass Γ *abgeschlossenen unter Ableitungen* ist. Die aus der leeren Menge ableitbaren Ausdrücke sind gerade die (syntaktischen) Tautologien.

Aus den (Grund- oder abgeleiteten) Tautologien ergeben sich direkt Regeln für die Ableitungsbeziehung.

Lemma 4.2. *Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V. Dann gelten folgende Regeln für die Ableitungsbeziehung (dabei seien $\alpha, \beta, \gamma, \alpha_i$ Aussagen).*

(1) *Konjunktionsregel: $\Gamma \vdash \alpha \wedge \beta$ genau dann, wenn $\Gamma \vdash \alpha$ und $\Gamma \vdash \beta$.*

(2) *Kettenschlussregel: Wenn* $\Gamma \vdash \alpha \to \beta$ *und* $\Gamma \vdash \beta \to \gamma$*, dann auch* $\Gamma \vdash \alpha \to \gamma$.
(3) *Modus Ponens: Wenn* $\Gamma \vdash \alpha$ *und* $\Gamma \vdash \alpha \to \beta$*, dann ist auch* $\Gamma \vdash \beta$.
(4) *Wenn* $\Gamma \vdash \alpha$*, so auch* $\Gamma \vdash \beta \to \alpha$.
(5) *Wenn* $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$ *und* $\Gamma \vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \beta$*, dann auch* $\Gamma \vdash \beta$.
(6) *Widerspruchsregel: Wenn* $\Gamma \vdash \alpha$ *und* $\Gamma \vdash \neg\alpha$*, dann auch* $\Gamma \vdash \beta$.
(7) *Fallunterscheidungsregel: Wenn* $\Gamma \vdash \alpha \to \beta$ *und* $\Gamma \vdash \neg\alpha \to \beta$*, dann auch* $\Gamma \vdash \beta$.

Beweis. Siehe Aufgabe 4.6. □

Definition 4.3. Eine Ausdrucksmenge $\Gamma \subseteq L^V$ in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V heißt *widersprüchlich*, wenn es einen Ausdruck $\alpha \in L^V$ mit $\Gamma \vdash \alpha$ und $\Gamma \vdash \neg\alpha$ gibt. Eine nicht widersprüchliche Ausdrucksmenge heißt *widerspruchsfrei*.

4.2. **Der Vollständigkeitssatz der Aussagenlogik I.**

Wir zeigen, dass für die Aussagenlogik die Ableitbarkeitsbeziehung mit der Folgerungsbeziehung übereinstimmt. Im Beweisaufbau orientieren wir uns an dem Vollständigkeitssatz für die Prädikatenlogik, der deutlich schwieriger ist und der später folgen wird.

Definition 4.4. Eine Teilmenge $\Gamma \subseteq L^V$ zu einer Menge V an Aussagenvariablen heißt *maximal widerspruchsfrei*, wenn Γ widerspruchsfrei ist und jede echt größere Menge $\Gamma \subset \Gamma'$ widersprüchlich ist.

Lemma 4.5. *Es sei* L^V *die Sprache der Aussagenlogik zu einer Aussagenvariablenmenge* V *und es sei* λ *eine Wahrheitsbelegung der Variablen mit zugehöriger Interpretation* I*. Dann ist* $I^{\models}$ *maximal widerspruchsfrei.*

Beweis. Siehe Aufgabe 4.15. □

Lemma 4.6. *Es sei* V *eine Menge an Aussagenvariablen und* $\Gamma \subseteq L^V$ *eine maximal widerspruchsfreie Teilmenge der zugehörigen Sprache der Aussagenlogik. Dann gelten folgende Aussagen.*

(1) *Für jedes* $\alpha \in L^V$ *ist entweder* $\alpha \in \Gamma$ *oder* $\neg\alpha \in \Gamma$.
(2) *Aus* $\Gamma \vdash \alpha$ *folgt* $\alpha \in \Gamma$.
(3) *Es ist* $\alpha \wedge \beta \in \Gamma$ *genau dann, wenn* $\alpha \in \Gamma$ *und* $\beta \in \Gamma$.
(4) *Es ist* $\alpha \to \beta \in \Gamma$ *genau dann, wenn* $\alpha \notin \Gamma$ *oder* $\beta \in \Gamma$.

Beweis. (1). Wegen der Widerspruchsfreiheit können nicht sowohl α als auch $\neg\alpha$ zu Γ gehören. Wenn weder α noch $\neg\alpha$ zu Γ gehören, so ist entweder $\Gamma \cup \{\alpha\}$ oder $\Gamma \cup \{\neg\alpha\}$ widerspruchsfrei. Wären nämlich beide widersprüchlich, so würde für einen beliebigen Ausdruck β sowohl

$$\Gamma \cup \{\alpha\} \vdash \beta$$

als auch

$$\Gamma \cup \{\neg\alpha\} \vdash \beta$$

gelten. Dies bedeutet nach Aufgabe 4.9

$$\Gamma \vdash \alpha \to \beta$$

und

$$\Gamma \vdash \neg\alpha \to \beta\,,$$

woraus aufgrund der Fallunterscheidungsregel

$$\Gamma \vdash \beta$$

folgt. Dies bedeutet aber, dass Γ widersprüchlich ist. (2). Sei $\Gamma \vdash \alpha$. Nach (1) ist $\alpha \in \Gamma$ oder $\neg\alpha \in \Gamma$. Das zweite kann nicht sein, da sich daraus sofort ein Widerspruch ergeben würde. Also ist $\alpha \in \Gamma$. (3) folgt aus (2) und der Konjunktionsregel. (4). Aufgrund von (1) müssen wir die Äquivalenz $\neg(\alpha \to \beta) \in \Gamma$ genau dann, wenn $\alpha \in \Gamma$ und $\neg\beta \in \Gamma$ zeigen. Dies ergibt sich aus (3). □

Lemma 4.7. *Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V. Es sei Γ widerspruchsfrei, abgeschlossen unter Ableitungen und für jede Aussagenvariable $p \in V$ gelte $p \in \Gamma$ oder $\neg p \in \Gamma$. Dann ist Γ maximal widerspruchsfrei.*

Beweis. Wir zeigen zuerst durch Induktion über den Aufbau der Sprache, dass für jedes $\alpha \in L^V$ die Alternative $\alpha \in \Gamma$ oder $\neg\alpha \in \Gamma$ gilt. Daraus folgt die maximale Widerspruchsfreiheit. Für $\alpha = p$ eine Aussagenvariable ist dies Teil der Voraussetzung. Bei $\alpha = \neg\beta$ folgt wegen $\vdash \neg(\neg\beta) \leftrightarrow \beta$ die Aussage aus der Induktionsvoraussetzung, da Γ abgeschlossen unter Ableitungen ist. Sei nun $\alpha = \beta \wedge \gamma$. Bei $\beta \in \Gamma$ und $\gamma \in \Gamma$ ist wegen der Ableitungsabgeschlossenheit auch $\beta \wedge \gamma \in \Gamma$. Wenn hingegen $\beta \notin \Gamma$ ist, so folgt nach Induktionsvoraussetzung $\neg\beta \in \Gamma$. Aufgrund der Tautologie $\vdash \neg\beta \to \neg(\beta \wedge \gamma)$ ergibt sich $\neg\alpha = \neg(\beta \wedge \gamma) \in \Gamma$. Der Beweis für die Implikation verläuft ähnlich, siehe Aufgabe 4.16.

Zum Nachweis, dass Γ maximal widerspruchsfrei ist, sei $\alpha \notin \Gamma$ angenommen. Nachdem, was wir eben bewiesen haben, gilt dann $\neg\alpha \in \Gamma$. Dann ist aber $\alpha, \neg\alpha \in \Gamma \cup \{\alpha\}$ und somit ist diese erweiterte Menge widersprüchlich. □

Oben haben wir gesehen, dass Interpretationen maximal widerspruchsfreie Ausdrucksmengen liefern. Davon gilt auch die Umkehrung.

Lemma 4.8. *Es sei V eine Menge an Aussagenvariablen und $\Gamma \subseteq L^V$ eine maximal widerspruchsfreie Teilmenge der zugehörigen Sprache der Aussagenlogik. Dann ist Γ erfüllbar.*

Beweis. Da Γ maximal widerspruchsfrei ist, gilt nach Lemma 4.6 (1) für jede Aussagenvariable die Alternative $p \in \Gamma$ oder $\neg p \in \Gamma$. Wir betrachten die Wahrheitsbelegung

$$\lambda(p) \;=\; \begin{cases} 1\,, \text{ falls } p \in \Gamma\,, \\ 0\,, \text{ falls } \neg p \in \Gamma\,, \end{cases}$$

mit der zugehörigen Interpretation I. Wir behaupten

$$I^{\models} \;=\; \Gamma,$$

was wir über den Aufbau der Sprache beweisen. Der Induktionsanfang ist durch die gewählte Belegung gesichert, der Induktionsschritt folgt aus Lemma 4.6. □

4.3. **Auffüllungsstrategien.**

Wir wollen zeigen, dass jede widerspruchsfreie Ausdrucksmenge erfüllbar ist. Die Strategie ist hierbei, sie zu einer maximal widerspruchsfreien Ausdrucksmenge aufzufüllen und dann die vorstehende Aussage anzuwenden. Wir unterscheiden die beiden Fälle, wo die Aussagenvariablenmenge abzählbar ist und den allgemeinen Fall einer beliebigen Aussagenvariablenmenge. Letzteres erfordert stärkere mengentheoretische Hilfsmittel, nämlich das Lemma von Zorn.

Lemma 4.9. *Es sei V eine abzählbare Menge an Aussagenvariablen und $\Gamma \subseteq L^V$ eine widerspruchsfreie Teilmenge der zugehörigen Sprache der Aussagenlogik. Dann kann man Γ durch sukzessive Hinzunahme von entweder p_n oder $\neg p_n$ und durch Abschluss unter der Ableitungsbeziehung zu einer maximal widerspruchsfreien Teilmenge $\Gamma' \supseteq \Gamma$ ergänzen.*

Beweis. Es sei p_n, $n \in \mathbb{N}_+$, eine (surjektive, aber nicht notwendigerweise injektive) Aufzählung der Aussagenvariablen. Die Voraussetzung bedeutet, dass $\Gamma_0 := \Gamma^{\vdash}$ keinen Widerspruch enthält. Wir konstruieren eine (endliche oder abzählbar unendliche) Folge von aufsteigenden widerspruchsfreien Teilmengen $\Gamma_n \subseteq \Gamma_{n+1}$, wobei in Γ_n für jede Variable p_i, $1 \leq i \leq n$, die Alternative entweder $p_i \in \Gamma_n$ oder $\neg p_i \in \Gamma_n$ gilt. Das Konstruktionsverfahren definieren und diese Aussage beweisen wir durch Induktion über $n \in \mathbb{N}$. Für Γ_0 ist dies richtig. Sei Γ_n schon konstruiert. Bei $p_{n+1} \in \Gamma_n$ oder $\neg p_{n+1} \in \Gamma_n$ setzen wir

$$\Gamma_{n+1} \;:=\; \Gamma_n.$$

Wegen der Widerspruchsfreiheit von Γ_n können nicht sowohl p_{n+1} als auch $\neg p_{n+1}$ zu Γ_n gehören. Wenn weder p_{n+1} noch $\neg p_{n+1}$ zu Γ_n gehören, so setzen wir

$$\Gamma_{n+1} \;:=\; (\Gamma_n \cup p_{n+1})^{\vdash}$$

(man könnte genauso gut $\neg p_{n+1}$ hinzunehmen). Nach Konstruktion ist Γ_{n+1} abgeschlossen unter der Ableitungsbeziehung und erfüllt die (Oder)-Alternative für alle Variablen p_i, $i \leq n+1$. Wenn Γ_{n+1} widersprüchlich wäre, so gelte

insbesondere $\Gamma_n \cup \{p_{n+1}\} \vdash \neg p_{n+1}$. Dann würde aber auch $\Gamma_n \vdash p_{n+1} \to \neg p_{n+1}$ gelten und somit nach der Fallunterscheidungsregel auch $\Gamma_n \vdash \neg p_{n+1}$, also $\neg p_{n+1} \in \Gamma_n$ im Widerspruch zu dem Fall, in dem wir uns befinden. Daher liegt für die Aussagenvariablen auch die Entweder-Oder-Alternative vor.

Mit dieser induktiven Definition setzen wir

$$\Gamma' := \bigcup_{n \in \mathbb{N}} \Gamma_n.$$

Diese Menge Γ' ist widerspruchsfrei, da andernfalls schon eines der Γ_n einen Widerspruch enthalten würde, und auch abgeschlossen unter Ableitungen, da dies für die einzelnen Γ_n gilt und eine Ableitung nur endlich viele Voraussetzungen besitzt. Ferner gilt für jedes $n \in \mathbb{N}$ die Alternative $p_n \in \Gamma'$ oder $\neg p_n \in \Gamma'$. Damit sind die Voraussetzungen von Lemma 4.7 erfüllt und Γ' ist maximal widerspruchsfrei. □

Beispiel 4.10. Wir betrachten die Aussagenvariablenmenge $\{p_1, p_2, p_3, \ldots\}$ und die Ausdrucksmenge

$$\Gamma = \{p_1 \to p_2,\ p_2 \to p_3,\ p_3 \to p_4,\ \ldots\}.$$

Diese wollen wir zu einer maximal widerspruchsfreien Menge gemäß Lemma 4.9 ergänzen. Wenn wir im ersten Schritt p_1 hinzunehmen, so ergibt sich sukzessive $p_i \in \Gamma_1$ für alle $i \in \mathbb{N}$. Es ist dann Γ_1 schon maximal widerspruchsfrei. Wählt man hingegen im ersten Schritt $\neg p_1$, so gehört weder p_2 noch $\neg p_2$ zu Γ_1. Beim zweiten Schritt hat man dann die Freiheit, ob man p_2 oder $\neg p_2$ zur Definition von Γ_2 hinzunimmt, und so weiter.

4. Arbeitsblatt

4.1. Übungsaufgaben.

Aufgabe 4.1. Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V und $\alpha \in L^V$. Es gelte $\Gamma \vdash \alpha$. Zeige, dass es dann auch eine endliche Teilmenge $\Delta \subseteq \Gamma$ mit $\Delta \vdash \alpha$ gibt.

Aufgabe 4.2. Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V. Es gelte $p \to q \in \Gamma$ und $q \to r \in \Gamma$. Folgt daraus $p \to r \in \Gamma$?

Aufgabe 4.3. Es sei $\Gamma = \{p, \neg q, r \to s\} \subseteq L^V$ (p, q, r, s seien Aussagenvariablen). Welche der folgenden Aussagen lassen sich aus Γ ableiten?

$$p \to q,\ \neg p \to q,\ p \to \neg q,\ \neg p \to \neg q,\ r \to q,\ (r \to q) \to \neg p,\ (s \to p) \to (r \to \neg q),\ (\neg q \to \neg p) \to s.$$

Aufgabe 4.4. Zeige, dass man aus $\Gamma = \{p\}$ unendlich viele Aussagen ableiten kann, die keine Tautologien sind.

Aufgabe 4.5.*

Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V. Zeige

$$\Gamma^{\vdash} = \left(\Gamma^{\vdash}\right)^{\vdash}.$$

Aufgabe 4.6. Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V. Zeige die folgenden Regeln für die Ableitungsbeziehung (dabei seien $\alpha, \beta, \gamma, \alpha_i$ Aussagen).

(1) Konjunktionsregel: $\Gamma \vdash \alpha \wedge \beta$ genau dann, wenn $\Gamma \vdash \alpha$ und $\Gamma \vdash \beta$.
(2) Kettenschlussregel: Wenn $\Gamma \vdash \alpha \to \beta$ und $\Gamma \vdash \beta \to \gamma$, dann auch $\Gamma \vdash \alpha \to \gamma$.
(3) Modus Ponens: Wenn $\Gamma \vdash \alpha$ und $\Gamma \vdash \alpha \to \beta$, dann ist auch $\Gamma \vdash \beta$.
(4) Wenn $\Gamma \vdash \alpha$, so auch $\Gamma \vdash \beta \to \alpha$.
(5) Wenn $\Gamma \vdash \alpha_1, \ldots, \Gamma \vdash \alpha_n$ und $\Gamma \vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \beta$, dann auch $\Gamma \vdash \beta$.
(6) Widerspruchsregel: Wenn $\Gamma \vdash \alpha$ und $\Gamma \vdash \neg\alpha$, dann auch $\Gamma \vdash \beta$.
(7) Fallunterscheidungsregel: Wenn $\Gamma \vdash \alpha \to \beta$ und $\Gamma \vdash \neg\alpha \to \beta$, dann auch $\Gamma \vdash \beta$.

Aufgabe 4.7. Es sei $V = \{p, q, r\}$ eine Aussagenvariablenmenge. Welche der folgenden Aussagen aus L^V lassen sich aus $\Gamma = V$ ableiten?

(1)
$$p\,,$$
(2)
$$p \wedge q \to r\,,$$
(3)
$$\neg p \wedge q \to r\,,$$
(4)
$$\neg p \wedge \neg q \to \neg r\,,$$
(5)
$$p \to (q \to r)\,,$$
(6)
$$p \to (q \to \neg r)\,,$$
(7)
$$\neg q\,.$$

Aufgabe 4.8. Es sei $\Gamma_1 = \{p \wedge q \to r\}$ und $\Gamma_2 = \{p \to (q \to r)\}$. Zeige

$$\Gamma_1^{\vdash} = \Gamma_2^{\vdash}.$$

Aufgabe 4.9.*

Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik über einer Aussagenvariablenmenge V und es seien $\alpha, \beta \in L^V$. Zeige, dass

$$\Gamma \cup \{\alpha\} \vdash \beta$$

zu

$$\Gamma \vdash \alpha \to \beta$$

äquivalent ist.

Aufgabe 4.10.*

Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik über einer Aussagenvariablenmenge V und es sei $\alpha \in L^V$. Es gelte

$$\Gamma \nvdash \alpha\,.$$

Zeige, dass dann

$$\Gamma \cup \{\neg\alpha\}$$

widerspruchsfrei ist.

Aufgabe 4.11. Es seien $\Gamma_1, \Gamma_2 \subseteq L^V$ Ausdrucksmengen in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V und seien $\alpha, \beta \in L^V$.

(1) Es gelte $\Gamma_1 \vdash \alpha$ und $\Gamma_2 \vdash \beta$. Zeige $\Gamma_1 \cup \Gamma_2 \vdash \alpha \wedge \beta$.
(2) Es gelte $\Gamma_1 \vdash \alpha$ und $\Gamma_2 \vdash \alpha$. Folgt daraus $\Gamma_1 \cap \Gamma_2 \vdash \alpha$?

Aufgabe 4.12.*

Sei $n \in \mathbb{N}_+$. Man gebe ein Beispiel für eine aussagenlogische widersprüchliche Ausdrucksmenge

$$\Gamma = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

derart, dass jede echte Teilmenge davon widerspruchsfrei ist.

Aufgabe 4.13. Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V. Zeige, dass die Ableitungsbeziehung $\Gamma \vdash \alpha$ die Folgerungsbeziehung $\Gamma \vDash \alpha$ impliziert.

Aufgabe 4.14. Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V und es sei $\alpha \in L^V$. Es gebe eine Interpretation I mit $I \vDash \Gamma$ und $I \vDash \neg\alpha$. Zeige $\Gamma \nvdash \alpha$.

Aufgabe 4.15.*

Es sei L^V die Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V und es sei λ eine Wahrheitsbelegung der Variablen mit zugehöriger Interpretation I. Zeige, dass $I^{\models}$ maximal widerspruchsfrei ist.

Aufgabe 4.16. Führe die Einzelheiten im Beweis zu Lemma 4.7 für die Implikation durch.

Aufgabe 4.17. Es sei $\Delta \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V, die zu jeder Aussagenvariablen $p \in V$ entweder p oder $\neg p$ enthalte. Zeige, dass $\Delta^{\vdash}$ maximal widerspruchsfrei ist.

Aufgabe 4.18. Es sei $\Gamma \subseteq L^V$ eine widerspruchsfreie, aber nicht maximal widerspruchsfreie Aussagenmenge, die unter Ableitungen abgeschlossen sei. Zeige, dass Γ nicht durch die Hinzunahme von endlich vielen Aussagen zu einer maximal widerspruchsfreien Aussagenmenge aufgefüllt werden kann.

4.2. **Aufgaben zum Abgeben.**

Aufgabe 4.19. (3 Punkte)

Es sei $\Gamma = \{p, \neg q \to r\} \subseteq L^V$ (p, q, r seien Aussagenvariablen). Welche der folgenden Aussagen lassen sich aus Γ ableiten?

$$p \to q,\ \neg q \to p,\ \neg p \to r,\ \neg q \to r \wedge p,\ \neg r \to q,\ r \to (q \to \neg p)\ .$$

Aufgabe 4.20. (3 Punkte)

Es sei $\Gamma \subseteq L^V$ eine Ausdrucksmenge in der Sprache der Aussagenlogik zu einer Aussagenvariablenmenge V. Zeige, dass folgende Aussagen äquivalent sind.

(1) Γ ist widersprüchlich.
(2) Für jedes $\beta \in L^V$ ist $\Gamma \vdash \beta$ und $\Gamma \vdash \neg\beta$.
(3) Es ist $\Gamma^{\vdash} = L^V$.

Aufgabe 4.21. (4 Punkte)

Es sei p eine Aussagenvariable und $\alpha \in L^V$ eine Aussage, in der die Variable p nicht vorkommt. Es gelte

$$\{p\} \vdash \alpha\,.$$

Zeige, dass bereits

$$\vdash \alpha$$

gilt.

Aufgabe 4.22. (3 Punkte)

Es sei V eine Aussagenvariablenmenge. Konstruiere eine Ausdrucksmenge $\Gamma \subseteq L^V$, die abgeschlossen unter Ableitungen und nicht maximal widerspruchsfrei ist, die aber die Eigenschaft besitzt, dass für jede Aussagenvariable p sowohl $(\Gamma \cup \{p\})^\vdash$ als auch $(\Gamma \cup \{\neg p\})^\vdash$ maximal widerspruchsfrei ist.

5. Vorlesung - Das Lemma von Zorn

5.1. Das Lemma von Zorn.

Wir möchten im Folgenden zeigen, dass eine widerpruchsfreie Menge $\Gamma \subseteq L^V$ von Aussagen nicht nur bei einer abzählbaren Aussagenvariablenmenge V zu einer maximal widerspruchsfreien Aussagenmenge aufgefüllt werden kann, sondern dass dies bei einer beliebigen Variablenmenge möglich ist. Bei einer Variablenmenge mit einer großen Mächtigkeit gibt es im Allgemeinen kein konstruktiv durchführbares Auffüllungsverfahren; es gibt lediglich Existenzaussagen, dass es solche maximal widerspruchsfreien Mengen geben muss. Diese Existenzaussagen beruhen auf stärkeren mengentheoretischen Konzepten, nämlich auf dem *Auswahlaxiom* und dem *Lemma von Zorn*.

Axiom 5.1. Es sei I eine Menge und M_i, $i \in I$, eine Familie von nichtleeren Mengen M_i. Dann gibt es eine Abbildung

$$f\colon\ I \longrightarrow \bigcup_{i \in I} M_i$$

mit $f(i) \in M_i$ für alle $i \in I$.

Das Auswahlaxiom ist intuitiv einleuchtend, da es lediglich die Existenz eines Tupels $(f(i) : i \in I)$ garantiert, wobei es für jedes i im Allgemeinen viele Kandidaten gibt. Da jedes M_i nicht leer ist, gibt es zu einem festen i mindestens ein $f(i) \in M_i$. Der Inhalt des Auswahlaxiomes ist, dass man diese Elemente als Werte einer Abbildung realisieren kann. Die Abbildung wählt also in jeder der Mengen ein Element aus. Das Auswahlaxiom ist ein starkes Axiom mit teilweise überraschenden (und manchmal kontraintuitiven?) Konsequenzen.

Das Lemma von Zorn wird für geordnete Mengen formuliert. Wir erinnern an die relevanten Definitionen.

Definition 5.2. Eine Relation $\preccurlyeq$ auf einer Menge I heißt *Ordnungsrelation* oder *Ordnung*, wenn folgende drei Bedingungen erfüllt sind.

(1) Es ist $i \preccurlyeq i$ für alle $i \in I$.
(2) Aus $i \preccurlyeq j$ und $j \preccurlyeq k$ folgt stets $i \preccurlyeq k$.
(3) Aus $i \preccurlyeq j$ und $j \preccurlyeq i$ folgt $i = j$.

Diese Eigenschaften heißen *Reflexivität*, *Transitivität* und *Antisymmetrie*. Eine Menge mit einer fixierten Ordnung heißt *geordnete Menge*. Eine Ordnung heißt *total* (oder *linear*), wenn $i \preccurlyeq j$ oder $j \preccurlyeq i$ für je zwei Elemente $i, j \in I$ gilt. Die reellen Zahlen $\mathbb{R}$ sind mit der üblichen Ordnung $\leq$ total geordnet, die Potenzmenge $\mathfrak{P}(M)$ zu einer Menge M ist mit der Inklusion $\subseteq$ eine nicht total geordnete Menge. Die Menge der natürlichen Zahlen mit der Teilbarkeitsbeziehung als Ordnungsrelation ist ebenfalls nicht total geordnet.

Definition 5.3. Sei $(I, \preccurlyeq)$ eine geordnete Menge. Ein Element $x \in I$ heißt *größtes Element* von I, wenn $y \preccurlyeq x$ für jedes $y \in I$ gilt.

Definition 5.4. Sei $(I, \preccurlyeq)$ eine geordnete Menge. Ein Element $x \in I$ heißt *maximal* (in I) oder ein *maximales Element* (von I), wenn es kein Element $y \in I$, $y \neq x$, mit $x \preccurlyeq y$ gibt.

Bei einer total geordneten Menge fallen diese beiden Begriffe zusammen. Ein größtes Element ist, wenn es existiert, eindeutig bestimmt, maximale Elemente im Allgemeinen nicht.

Definition 5.5. Sei $(I, \preccurlyeq)$ eine geordnete Menge und $J \subseteq I$ eine Teilmenge. Ein Element $x \in I$ heißt *obere Schranke* für J, wenn $y \preccurlyeq x$ für jedes $y \in J$ gilt.

Die folgende Aussage heißt Lemma von Zorn.

Lemma 5.6. *Sei $(I, \preccurlyeq)$ eine geordnete Menge mit der Eigenschaft, dass jede total geordnete Teilmenge $J \subseteq I$ eine obere Schranke in I besitzt. Dann gibt es in I maximale Elemente.*

Beweis. Diese Aussage kann man aus dem Auswahlaxiom herleiten; der Beweis ist aber ziemlich kompliziert und wenig erhellend, so dass wir auf ihn verzichten. □

Da die leere Menge total geordnet ist, kann insbesondere die Menge I nicht leer sein. Dies wird manchmal in Formlierungen des Lemmas extra mitaufgeführt. Häufig nennt man die total geordneten Teilmengen auch *Ketten*. Eine geordnete Menge, die die Voraussetzung des Lemmas erfüllt, in der also jede Kette eine obere Schranke besitzt, heißt induktiv geordnet. Das Lemma von Zorn ist ein grundlegender mengentheoretischer Sachverhalt, der zum Auswahlaxiom äquivalent ist. Wir geben einige typische Beispiele, wie man mittels des Lemmas von Zorn die Existenz von gewissen mathematischen Objekten nachweisen kann.

Definition 5.7. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Definition 5.8. Ein Ideal $\mathfrak{m}$ in einem kommutativen Ring R heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und wenn es zwischen $\mathfrak{m}$ und R keine weiteren Ideale gibt.

Lemma 5.9. *In einem kommutativen Ring $R \neq 0$ gibt es maximale Ideale.*

Beweis. Wir betrachten die Menge

$$M := \{I \subseteq R | \, 1 \notin I, \text{ Ideal in } R\}.$$

Diese Menge enthält das Nullideal 0 und ist somit nicht leer. Wir wollen das Lemma von Zorn auf M (mit der Inklusion als Ordnungsrelation) anwenden. Dazu sei $N \subseteq M$ eine total geordnete Teilmenge. Wir setzen

$$I := \bigcup_{J \in N} J.$$

Man zeigt nun, dass I ein Ideal ist, das nicht die 1 enthält. Also gehört es zu M und es bildet eine obere Schranke für N. Das Lemma von Zorn liefert dann maximale Elemente in M, und dies sind maximale Ideale. □

Eine Variante dieser Aussage ist, dass jedes Ideal $\mathfrak{a} \subseteq R$, das nicht die 1 enthält, in einem maximalen Ideal enthalten ist. Für verhältnismäßig einfache Ringe kann man die Existenz maximaler Ideale auch ohne das Lemma von Zorn sichern. Das Lemma von Zorn etabliert aber auch in überraschenden Situationen die Existenz von maximalen Idealen, wie das folgende Beispiel zeigt.

Beispiel 5.10. Wir betrachten die Menge

$$R := \mathbb{R}^{\mathbb{N}} = \left\{(x_n)_{n \in \mathbb{N}} \,|\, \text{reelle Folge}\right\}.$$

Diese Menge ist mit komponentenweiser Addition und Multiplikation ein kommutativer Ring (mit der konstanten Nullfolge bzw. Einsfolge als 0 und 1). Zu jedem festen $k \in \mathbb{N}$ ist die Menge

$$I_k = \left\{(x_n)_{n \in \mathbb{N}} \in R | \, x_k = 0\right\}$$

ein maximales Ideal. Die Idealeigenschaft kann man unmittelbar nachprüfen, die Maximalität ergibt sich daraus, dass ein größeres Ideal

$$I_k \subset I$$

ein Element $y = (y_n)_{n \in \mathbb{N}}$ mit $y_k \neq 0$ enthält. Dann ist

$$\frac{1}{y_k} y + \left(1 - \frac{1}{y_k} y\right) = 1$$

mit $1 - \frac{1}{y_k} y \in I_k$ und daher ist $1 \in I$. Mit dieser Konstruktion bekommt man also direkt maximale Ideale. Die Restklassenkörper zu diesen maximalen Idealen sind (isomorph zu) $\mathbb{R}$, der Restklassenhomomorphismus ist einfach die Projektion auf die k-te Komponente.

Wir betrachten nun das Ideal

$$I = \left\{(x_n)_{n\in\mathbb{N}} \,|\, x_n \neq 0 \text{ für endlich viele } n \in \mathbb{N}\right\},$$

das ist also die Menge aller Folgen, die bis auf endlich viele Glieder mit der Nullfolge übereinstimmen. Es gibt daher nach (einer Variante von) Lemma 5.9 maximale Ideale $\mathfrak{m}$ mit

$$I \subseteq \mathfrak{m}.$$

Es ist

$$\mathfrak{m} \not\subseteq I_k,$$

da die Folge, die an der k-ten Stelle eine 1 und sonst überall eine 0 stehen hat, links dazu gehört, aber nicht rechts. Ein solches maximales Ideal kann man nicht explizit beschreiben. Selbst wenn man sich auf Folgen beschränkt, die lediglich die beiden Werte 0 oder 1 annehmen, so ist kein explizites Verfahren bekannt, zu bestimmen, ob die Folge zu $\mathfrak{m}$ gehören soll oder nicht. Für jede Folge mit unendlich vielen Nullen und mit unendlich vielen Einsen gibt es ein solches maximales Ideal $\mathfrak{m}$, das diese Folge enthält, und auch eines, das sie nicht enthält.

Die Restklassenkörper zu einem solchen maximalen Ideal sind nicht isomorph zu $\mathbb{R}$. Die dabei auftretenden Körper sind vielmehr der Gegenstand der sogenannten *Nichtstandardanalysis*.

Definition 5.11. Sei X ein topologischer Raum. Ein System F aus offenen Teilmengen von X heißt *Filter*, wenn folgende Eigenschaften gelten (U, V seien offen).

(1) $X \in F$.
(2) Mit $U \in F$ und $U \subseteq V$ ist auch $V \in F$.
(3) Mit $U \in F$ und $V \in F$ ist auch $U \cap V \in F$.

Definition 5.12. Ein topologischer Filter F heißt *Ultrafilter*, wenn $\emptyset \notin F$ und wenn F maximal mit dieser Eigenschaft ist.

Lemma 5.13. *Es sei X ein topologischer Raum und F ein topologischer Filter auf X mit $\emptyset \notin F$. Dann gibt es einen Ultrafilter $G \supseteq F$.*

Beweis. Siehe Aufgabe 5.14. □

Wir beweisen den *Satz von Hamel* über die Existenz von Vektorraumbasen als eine weitere Anwendung des Lemmas von Zorn. Eine Basis eines Vektorraumes über einem Körper ist ein linear unabhängiges Erzeugendensystem. Für endlich erzeugte Vektorräume (wie den $\mathbb{R}^n$) ist dieser Satz auch ohne das Lemma von Zorn direkt beweisbar. Das Problem sind Vektorräume ohne endliches Erzeugendensystem, beispielsweise die Menge der reellen Zahlen als Vektorraum über den rationalen Zahlen oder der oben betrachtete Folgenraum.

Satz 5.14. *Jeder Vektorraum besitzt eine Basis.*

Beweis. Sei V ein Vektorraum über einem Körper K. Es sei

$$M = \{T \subseteq V | \text{ Die Elemente aus } T \text{ sind linear unabhängig}\}.$$

Die leere Menge gehört zu M, also ist M nicht leer. Es sei $N \subseteq M$ eine total geordnete Teilmenge. Wir behaupten, dass

$$S = \bigcup_{T \in N} T$$

ebenfalls linear unabhängig ist und daher eine obere Schranke von N in M bildet. Andernfalls gäbe es nämlich eine endliche Teilmenge $E \subseteq S$, deren Elemente linear abhängig sind, und es gäbe auch ein $T \in N$, das E umfasst und daher selbst linear abhängig wäre. Nach dem Lemma von Zorn besitzt M also maximale Elemente, d.h. es gibt eine Teilmenge $T \subseteq V$, die linear unabhängig ist und derart, dass es keine echt größere linear unabhängige Teilmenge von V gibt. Wir behaupten, dass T auch ein Erzeugendensystem von V ist. Sei dazu $v \in V$. Bei $v \in T$ sind wir fertig. Bei $v \notin T$ ist $T \cup \{v\}$ linear abhängig, d.h. es gibt eine Linearkombination

$$\sum_{i=1}^{n} c_i t_i + cv = 0$$

mit Elementen $t_i \in T$ und Koeffizienten $c_i, c \in K$, die nicht alle 0 sind. Dabei kann c nicht 0 sein, da sonst eine lineare Abhängigkeit zwischen Elementen aus T vorliegen würde. Also kann man v als Linearkombination der $t_1, \ldots, t_n$ ausdrücken. □

Definition 5.15. Eine totale Ordnung $\preccurlyeq$ auf einer Menge M heißt *Wohlordnung*, wenn jede nichtleere Teilmenge $T \subseteq M$ ein kleinstes Element besitzt.

Beispielsweise sind die natürlichen Zahlen wohlgeordnet, die reellen Zahlen nicht, siehe Aufgabe 5.25. Da eine totale Ordnung vorliegt, stimmen jeweils die Begriffe kleinstes Element und minimales Element überein. Die folgende Aussage heißt *Wohlordnungssatz*. Er folgt aus dem Auswahlaxiom und ist zu diesem und zum Lemma von Zorn äquvalent. Wir verzichten auf einen Beweis.

Satz 5.16. *Auf jeder Menge M gibt es eine Wohlordnung.*

Auch diese Aussage ist lediglich eine Existenzaussage. Es ist im Allgemeinen nicht möglich, explizit eine Wohlordnung zu konstruieren. Auf den reellen Zahlen ist keine Wohlordnung bekannt.

5.2. **Der Vollständigkeitssatz der Aussagenlogik II.**

Lemma 5.17. *Es sei V eine Menge an Aussagenvariablen und $\Gamma \subseteq L^V$ eine widerspruchsfreie Teilmenge der zugehörigen Sprache der Aussagenlogik. Dann gibt es eine maximal widerspruchsfreie Teilmenge $\Gamma' \subseteq L^V$, die Γ enthält.*

Beweis. Wir betrachten die Menge

$$M := \left\{ \Delta \subseteq L^V \,|\, \Delta \supseteq \Gamma,\ \Delta \text{ widerspruchsfrei} \right\}$$

mit der durch Inklusion gegebenen Ordnung. Wegen $\Gamma \in M$ ist diese Menge nicht leer. Es sei $N \subseteq M$ eine nichtleere total geordnete Teilmenge. Die Vereinigung

$$\Theta = \bigcup_{\Delta \in N} \Delta$$

ist ebenfalls widerspruchsfrei, da ein Widerspruch schon aus einer endlichen Teilmenge ableitbar wäre, die ganz in einem der Δ enthalten wäre. Also besitzt die Kette in M eine obere Schranke. Nach dem Lemma von Zorn gibt es also in M maximale Elemente. Ein solches ist maximal widerspruchsfrei. □

Satz 5.18. *Es sei V eine Menge an Aussagenvariablen und $\Gamma \subseteq L^V$ eine widerspruchsfreie Teilmenge der zugehörigen Sprache der Aussagenlogik. Dann ist Γ erfüllbar.*

Beweis. Nach Lemma 5.17 (bzw. Lemma 4.9 im abzählbaren Fall) kann man Γ zu einer maximal widerspruchsfreien Ausdrucksmenge Γ' auffüllen. Nach Lemma 4.8 ist Γ' erfüllbar, d.h., es gibt eine Wahrheitsbelegung λ derart, dass unter der zugehörigen Interpretation alle Ausdrücke aus Γ' gültig sind. Dann sind unter dieser Belegung insbesondere die Ausdrücke aus Γ gültig. □

Die folgende Aussage ist der *Vollständigkeitssatz für die Aussagenlogik.*

Satz 5.19. *Es sei V eine Menge an Aussagenvariablen und $\Gamma \subseteq L^V$ eine Teilmenge der zugehörigen Sprache der Aussagenlogik. Es sei $\alpha \in L^V$. Dann ist*

$$\Gamma \vdash \alpha \text{ genau dann, wenn } \Gamma \vDash \alpha\,.$$

Beweis. Dass die Ableitungsbeziehung die Folgerungsbeziehung impliziert, wurde bereits im Rahmen der Korrektheitsüberlegungen zu den Ableitungsregeln gezeigt. Für die Umkehrung nehmen wir $\Gamma \nvdash \alpha$ an. Dies bedeutet nach Aufgabe 4.10, dass $\Gamma \cup \{\neg\alpha\}$ widerspruchsfrei ist. Nach Satz 5.18 ist dann auch $\Gamma \cup \{\neg\alpha\}$ erfüllbar. Es gibt also eine Wahrheitsbelegung mit $I \vDash \Gamma$ und $I \vDash \neg\alpha$. Also ist $\Gamma \nvDash \alpha$. □

Korollar 5.20. *Es sei V eine Menge an Aussagenvariablen und $\alpha \in L^V$. Dann ist*

$$\vdash \alpha \text{ genau dann, wenn } \vDash \alpha\,.$$

Ein Ausdruck ist also eine semantische Tautologie genau dann, wenn es eine syntaktische Tautologie ist.

Beweis. Dies ist der Spezialfall von Satz 5.19 bei $\Gamma = \emptyset$. □

5. Arbeitsblatt

5.1. Übungsaufgaben.

Aufgabe 5.1. Zeige mit Hilfe des Auswahlaxioms, dass es zu jeder Äquivalenzrelation $\sim$ auf einer Menge M ein Repräsentantensystem für die Äquivalenzklassen gibt.

Aufgabe 5.2. Skizziere ein Teilerdiagramm für die Menge M der echten natürlichen Teiler von 100 (dabei gelte 1 als echter Teiler, 100 nicht). Was sind die maximalen, die minimalen Elemente, gibt es ein größtes und ein kleinstes Element, was sind die total geordneten Teilmengen?

Aufgabe 5.3. Skizziere ein Inklusionsdiagramm für sämtliche Teilmengen einer dreielementigen Menge.

Aufgabe 5.4. Es sei $(I, \preccurlyeq)$ eine total geordnete Menge. Zeige durch Induktion, dass jede nichtleere endliche Teilmenge $T \subseteq I$ ein eindeutiges Maximum besitzt.

Aufgabe 5.5. Besitzt die Menge $\mathbb{N}$ der natürlichen Zahlen in $\mathbb{R}$ eine obere Schranke? Wie sieht das in anderen angeordneten Körpern aus?

Aufgabe 5.6.*

Es sei M eine endliche Menge. Betrachte die Relation auf der Potenzmenge $\mathfrak{P}(M)$, die durch

$$S \preccurlyeq T, \text{ falls } \#(S) \leq \#(T)\,,$$

gegeben ist. Handelt es sich dabei um eine Ordnungsrelation?

Aufgabe 5.7. Es sei M eine Menge und I die Menge der echten Teilmengen von M, also

$$I = \{T \subseteq M | \, T \neq \emptyset \text{ und } T \neq M\}\ .$$

Diese Menge ist durch die Inklusion eine geordnete Menge. Bestimme die minimalen und die maximalen Elemente von I.

Aufgabe 5.8. Es sei A eine endliche total geordnete Menge. Es sei $I = \{1, 2, \ldots, n\}$ eine endliche Indexmenge. Definiere auf der Produktmenge

$$A^I = \underbrace{A \times \cdots \times A}_{n-\text{mal}}$$

die „lexikographische Ordnung“, und zeige, dass es sich dabei ebenfalls um eine totale Ordnung handelt.

Aufgabe 5.9. Es sei $(I, \preccurlyeq)$ eine nichtleere geordnete Menge mit der Eigenschaften, dass alle Ketten in I endlich seien. Beweise in dieser Situation direkt, dass es in I maximale Elemente gibt.

Aufgabe 5.10.*

Es sei G eine unendliche Menge und $M \subset \mathfrak{P}(G)$ die Menge, die aus sämtlichen endlichen Teilmengen von G besteht.

(1) Ist $(M, \subseteq)$ induktiv geordnet?
(2) Besitzt M maximale Elemente?

Aufgabe 5.11.*

Es sei G eine Menge und $M \subseteq \mathfrak{P}(G)$ eine Teilmenge der Potenzmenge, die unter beliebigen Vereinigungen abgeschlossen ist.

(1) Zeige, dass $(M, \subseteq)$ induktiv geordnet ist.
(2) Zeige, dass M ein größtes Element besitzt.

Aufgabe 5.12. Zeige, dass in $\mathbb{Z}$ die maximalen Ideale genau die von Primzahlen p erzeugten Ideale $\mathbb{Z}p = \{kp | \, k \in \mathbb{Z}\}$ sind.

Aufgabe 5.13. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Zeige, dass I genau dann ein maximales Ideal ist, wenn der Restklassenring R/I ein Körper ist.

Aufgabe 5.14. Es sei X ein topologischer Raum und F ein topologischer Filter auf X mit $\emptyset \notin F$. Zeige, dass es einen Ultrafilter $G \supseteq F$ gibt.

Wenn man die natürlichen Zahlen $\mathbb{N}$ mit der diskreten Topologie versieht, so dass also jede Teilmenge offen ist, so ist ein topologischer Filter auf $\mathbb{N}$ einfach eine Teilmenge $F \subseteq \mathfrak{P}(\mathbb{N})$ mit

(1) $\mathbb{N} \in F$.
(2) Mit $U \in F$ und $U \subseteq V$ ist auch $V \in F$.

(3) Mit $U \in F$ und $V \in F$ ist auch $U \cap V \in F$.

Aufgabe 5.15. Ein Filter $F \subseteq \mathfrak{P}(\mathbb{N})$ ist genau dann ein Ultrafilter, wenn für jede Teilmenge $T \subseteq \mathbb{N}$ entweder $T \in F$ oder $\mathbb{N} \setminus T \in F$ gilt

Die einfachen Ultrafilter in $\mathbb{N}$ werden in der folgenden Aufgabe beschrieben.

Aufgabe 5.16. Es sei $n \in \mathbb{N}$ eine fixierte Zahl. Dann ist

$$F = \{T \subseteq \mathbb{N} | \, n \in T\}$$

ein Ultrafilter.

Aufgabe 5.17. Zeige, dass es in $\mathbb{N}$ Ultrafilter gibt, die keine endlichen Teilmengen enthalten.

Aufgabe 5.18. Wir betrachten den Folgenring $R = \mathbb{R}^{\mathbb{N}}$. Zu einer Folge $x = (x_n)_{n\in\mathbb{N}} \in R$ sei

$$Z(x) = \{n \in \mathbb{N} | \, x_n = 0\}.$$

Zeige, dass über die Zuordnungen

$$I \longmapsto \{T \subseteq \mathbb{N} | \, T = Z(x) \text{ für ein } x \in I\}$$

und

$$F \longmapsto \{x \in R | \, Z(x) \in F\}$$

sich die Ideale aus R und die Filter aus $\mathbb{N}$ entsprechen.

Aufgabe 5.19. Wir betrachten die Menge

$$\mathcal{G} = \left\{ T \subseteq \mathbb{N}_+ | \, \sum_{n\in T} \frac{1}{n} \text{ ist eine divergente Reihe} \right\}.$$

Ist $\mathcal{G}$ ein Filter?

Aufgabe 5.20. Man mache sich an den folgenden Beispielen klar, dass der Satz von Hamel keineswegs selbstverständlich ist.

(1) Die reellen Zahlen $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum betrachtet.
(2) Die Menge der reellen Folgen

$$\mathbb{R}^{\mathbb{N}} = \left\{ (x_n)_{n\in\mathbb{N}} \, | \, x_n \in \mathbb{R} \right\}.$$

(3) Die Menge aller stetigen Funktionen von $\mathbb{R}$ nach $\mathbb{R}$.

Aufgabe 5.21.*

Betrachte die reellen Zahlen $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum. Zeige, dass die Menge der reellen Zahlen $\ln p$, wobei p durch die Menge der Primzahlen läuft, linear unabhängig ist. Tipp: Verwende, dass jede positive natürliche Zahl eine eindeutige Darstellung als Produkt von Primzahlen besitzt.

Aufgabe 5.22. Zeige, dass es keine Abbildung

$$\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}$$

gibt, die die folgende Eigenschaft erfüllt: Es ist $k \geq n$ genau dann, wenn $\varphi(k) \leq \varphi(n)$.

Aufgabe 5.23. Beweise durch Induktion, dass die natürliche Ordnung auf den natürlichen Zahlen $\mathbb{N}$ eine Wohlordnung ist.

Aufgabe 5.24. Zeige, dass die natürliche Ordnung auf den ganzen Zahlen keine Wohlordnung ist.

Aufgabe 5.25. Zeige, dass die natürliche Ordnung auf den reellen Zahlen keine Wohlordnung ist.

Aufgabe 5.26. Es sei $\Gamma \subseteq L^V$ eine widerspruchsfreie aussagenlogische Ausdrucksmenge, die unter Ableitungen abgeschlossen sei. Zeige, dass Γ der Durchschnitt von maximal widerspruchsfreien Ausdrucksmengen ist.

Aufgabe 5.27. Es sei V eine beliebige Aussagenvariablenmenge und sei $\Gamma \subseteq L^V$ eine abzählbare Ausdrucksmenge. Zeige, dass man in diesem Fall den Vollständigkeitssatz der Aussagenlogik ohne das Lemma von Zorn beweisen kann.

Die folgenden beiden Aussagen ergeben zusammen einen konstruktiven Beweis für den Vollständigkeitssatz der Aussagenlogik in der Version von Korollar 5.20, d.h. für eine semantische Tautologie α weiß man nicht nur die Existenz einer Ableitung $\vdash \alpha$, sondern man kann konstruktiv eine Ableitung angeben.

Aufgabe 5.28.*

Es sei α eine aussagenlogische Aussage und es seien $p_1, \ldots, p_n$ die darin vorkommenden Aussagenvariablen. Es sei

$$\gamma \;=\; \pm p_1 \wedge \ldots \wedge \pm p_n$$

eine fixierte Konjunktion dieser (negierten) Aussagenvariablen. Zeige, dass dann

$$\vdash \gamma \to \alpha \text{ oder } \vdash \gamma \to \neg\alpha$$

gilt.

Aufgabe 5.29.*

Skizziere einen konstruktiven Beweis für die Tautologieversion der Vollständigkeit der Aussagenlogik.

Aufgabe 5.30.*

Es sei $\Gamma \subseteq L^V$ eine endliche Menge an Aussagen. Skizziere ein Entscheidungsverfahren, mit dem man feststellen kann, ob Γ widersprüchlich ist oder nicht.

5.2. **Aufgaben zum Abgeben.**

Aufgabe 5.31. (2 Punkte)

Beweise das Lemma von Zorn für eine total geordnete Menge.

Aufgabe 5.32. (3 Punkte)

Wir betrachten die Menge

$$\mathcal{F} \;=\; \left\{ T \subseteq \mathbb{N}_+ | \sum_{n \notin T} \frac{1}{n} \text{ ist eine konvergente Reihe} \right\}.$$

Zeige, dass $\mathcal{F}$ ein Filter auf $\mathbb{N}_+$ ist.

Aufgabe 5.33. (3 Punkte)

Zeige, dass sich bei der in Aufgabe 5.18 beschriebenen Korrespondenz maximale Ideale und Ultrafilter entsprechen.

Aufgabe 5.34. (3 Punkte)

Definiere eine Wohlordnung auf der Menge der ganzen Zahlen $\mathbb{Z}$.

Aufgabe 5.35. (5 Punkte)

Es sei $(M, \preccurlyeq)$ eine total geordnete Menge, die sowohl nach unten als auch nach oben wohlgeordnet ist. Zeige, dass M endlich ist.

Aufgabe 5.36. (2 Punkte)

Beweise den *Endlichkeitssatz für die Aussagenlogik*: Wenn die Aussage α aus der Aussagenmenge $\Gamma \subseteq L^V$ folgt, dann gibt es eine endliche Teilmenge $\Gamma_0 \subseteq \Gamma$, aus der diese Aussage folgt.

6. Vorlesung - Prädikatenlogik

Prädikatenlogik

Mit der Aussagenlogik kann man keine gehaltvollen mathematischen Aussagen behandeln. Beispielsweise fehlt in ihr das Gleichheitszeichen, und man kann nicht über Variabeln, die sich auf eine Grundmenge beziehen, quantifizieren, man kann keine Terme bilden und Funktionen auswerten. Dies führt zur Prädikatenlogik, der wir uns nun zuwenden, und mit der man einen Großteil der (in einem gewissen Sinn die ganze) Mathematik ausdrücken kann. Von der mathematischen Praxis her ist sie aber immer noch recht restriktiv. Wir erinnern kurz an den Abbildungsbegriff und den Relationsbegriff der Mathematik und setzen eine naive Mengenlehre und die natürlichen Zahlen „zum Zählen“ voraus.

Definition 6.1. Seien L und M Mengen. Eine *Abbildung* F von L nach M ist dadurch gegeben, dass jedem Element der Menge L genau ein Element der Menge M zugeordnet wird. Das zu $x \in L$ eindeutig bestimmte Element wird mit $F(x)$ bezeichnet. Die Abbildung drückt man als Ganzes häufig durch

$$F\colon\ L \longrightarrow M,\ x \longmapsto F(x),$$

aus.

Definition 6.2. Es seien zwei Mengen L und M gegeben. Dann nennt man die Menge

$$L \times M\ =\ \{(x,y) |\, x \in L,\ y \in M\}$$

die *Produktmenge* der beiden Mengen.

Für uns ist insbesondere das n-fache Produkt einer Menge M mit sich selbst, also

$$M^n\ =\ M \times M \times \cdots \times M$$

(mit n Faktoren) wichtig.

Definition 6.3. Es sei M eine Menge. Unter einer *n- stelligen Abbildung* auf M versteht man eine Abbildung

$$f\colon M \times \cdots \times M \longrightarrow M,\ (x_1, \ldots, x_n) \longmapsto f(x_1, \ldots, x_n),$$

vom n-fachen Produkt von M mit sich selbst nach M.

Definition 6.4. Unter einer *n- stelligen Relation* R auf einer Menge M versteht man eine Teilmenge der n-fachen Produktmenge $M \times \cdots \times M$.

Eine n-stellige Funktion kann auch als eine $(n+1)$-stellige Relation aufgefasst werden, bei der es zu jedem n-Tupel $(x_1, \ldots, x_n)$ genau ein x_{n+1} derart gibt, dass $(x_1, \ldots, x_n, x_{n+1})$ zur Relation gehört. Dieses x_{n+1} ist dann der Funktionswert der zugehörigen Funktion an der Stelle $(x_1, \ldots, x_n)$.

6.1. **Terme.**

Betrachten wir die sinnvollen Ausdrücke, die für eine natürliche Zahl stehen können. Mit dem Ziffernalphabet $Z = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ kann man mit der rekursiven Vorschrift zur Generierung von Zeichenreihen aus einem Alphabet alle natürlichen Zahlen (im Zehnersystem) aufschreiben, z.B. 530386275. Allerdings gibt es hier ein paar Schwierigkeiten, es sind nämlich auch die Zahlen 0530386275, 00530386275, u.s.w. erlaubt (und untereinander verschieden, da sie eben unterschiedliche Symbolfolgen sind). Der „Zahlenwert“ steht im Moment noch nicht zur Verfügung. Ferner möchte man das leere Zahlwort nicht als erlaubte Ziffernfolge ansehen.

Mit dieser Menge an erlaubten Zahlwörtern kann man Telefonnummern oder Internetadressen bezeichnen, aber noch nicht das machen, was man eigentlich mit Zahlen machen möchte, nämlich Zählen, Rechnen, Probleme formulieren und lösen. Für die innerhalb der natürlichen Zahlen ausführbaren Rechenoperationen, insbesondere das Nachfolgernehmen (also das Zählen) und die Addition und die Multiplikation, brauchen wir neue Symbole. Eine Aussage wie

$$5 \cdot 3 = 8 + 7$$

ist natürlich wahr, da links und rechts 15 „steht“, wie man durch „ausrechnen“ (also das korrekte Anwenden der Rechenregeln) überprüfen kann. Wenn man allerdings solche Gleichungen logisch verstehen und analysieren möchte, so sollte man die beiden Seiten nicht als 15 lesen, sondern jeweils als ein neues „komplexes Zahlwort“, das sich aus den Ziffernsymbolen 5 und 3 und dem Malzeichen $\cdot$ bzw. den Ziffernsymbolen 8 und 7 und dem Pluszeichen $+$ zusammensetzt. Die linke und die rechte Seite sind hier sogenannte Terme, also sinnvolle mathematische Ausdrücke, die einen Zahlwert annehmen können bzw. formal den Charakter einer Zahl haben (der Vergleich der beiden Terme durch $=$ macht aus den beiden Termen eine Aussage, das spielt jetzt aber noch keine Rolle). Ein weiteres Beispiel ist eine Gleichung der Form

$$4 \cdot x = 3 \cdot (8 + y),$$

wo vermutlich nach den erlaubten Werten für x und y gesucht wird, die diese Gleichung erfüllen. Aber unabhängig von dieser typischen Interpretation stehen links und rechts ebenfalls Terme, in denen jeweils eine Variable vorkommt. Solche Terme sind ein konstitutiver Bestandteil der Prädikatenlogik und werden, ausgehend von einer Variablenmenge (keine Aussagenvariablenmenge), einer Konstantenmenge und verschiedenen Funktionssymbolmengen, rekursiv definiert.

Definition 6.5. Eine *Grundtermmenge* besteht aus den folgenden (untereinander disjunkten[5]) Mengen.

(1) eine Variablenmenge V,
(2) eine Konstantenmenge K,
(3) zu jedem $n \in \mathbb{N}_+$ eine Menge F_n von Funktionssymbolen.

Dabei können die auftretenden Mengen leer sein, es ist für die Funktionssymbole sogar typisch, dass es nicht zu jeder Stelligkeit (zu jedem n) ein Funktionssymbol gibt (die Variablenmenge wird hingegen meistens als nicht leer angesetzt, und zwar mit unendlich vielen Variablen, die häufig als $x_1, x_2, x_3, \ldots$ angesetzt wird.). Die Konstanten kann man auch als nullstellige Funktionssymbole auffassen. Unter dem *Termalphabet* versteht man die Vereinigung $A = V \cup K \cup \bigcup_{n\in\mathbb{N}_+} F_n$.

Die arithmetische Grundtermmenge besteht aus den beiden Konstanten $0, 1$, den beiden zweistelligen Funktionssymbolen $\{+, \cdot\}$ und einer Variablenmenge.

Definition 6.6. Zu einer Grundtermmenge $G = (V, K, F_n)$ ist die zugehörige *Termmenge* (oder die Menge der G-Terme) diejenige Teilmenge $T = T(G)$ der Wörter A^* über dem Termalphabet $A = V \cup K \cup \bigcup_{n\in\mathbb{N}_+} F_n$, die durch die folgenden rekursiven Vorschriften festgelegt wird.

(1) Jede Variable $v \in V$ ist ein Term.
(2) Jede Konstante $c \in K$ ist ein Term.
(3) Für jedes $f \in F_n$ und n Terme $t_1, t_2, \ldots, t_n$ ist auch $ft_1t_2 \ldots t_n$ ein Term.

Hierbei sind (1) und (2) die Anfangsbedingungen und (3) die Rekursionsregel, da darin auf schon gebildete Terme Bezug genommen wird. Wie bei jeder rekursiven Definition ist ein Wort nur dann ein Term, wenn es gemäß dieser Regeln gebildet werden kann.

Gemäß dieser Definition verzichten wir auf Klammern, und die Funktionssymbole werden einheitlich links geschrieben[6] und daran werden rechts davon die Terme angefügt (das wird später so interpretiert, dass in n-stellige Funktionen n Elemente eingesetzt werden). Schon in einfachen Beispielen ist es

[5]Zwei Mengen L und M heißen *disjunkt*, wenn ihr Durchschnitt $L \cap M = \emptyset$ ist.
[6]Man spricht von *polnischer Notation*.

aber wegen der Lesbarkeit sinnvoll, auch Klammern zu verwenden und von der strengen Reihenfolge bei den Funkltionssymbolen abzuweichen und beispielsweise $s + t$ statt $+st$ zu schreiben. Solche Schreibweisen sind als Ersatz für die formal korrekt gebildeten Terme zu interpretieren, sie gehören aber nicht zu den Termen.

Beispiel 6.7. Eine Grundtermmenge sei durch die Variablenmenge $V = \{x, y, z\}$, eine Konstantenmenge $K = \{c_1, c_2\}$, die einstelligen Funktionssymbole $F_1 = \{f, g\}$ und die zweistelligen Funktionssymbole $F_2 = \{\alpha, \beta, \gamma\}$ gegeben. Dann sind die folgenden Wörter Terme.

$$x, y, z, c_1, c_2, fx, fc_1, gz, \alpha xy, \alpha xx, \alpha xfy, \alpha fxgc_1, \gamma\gamma xxx, \beta\alpha xgc_2\gamma fy\alpha gzx\,.$$

Auch wenn es für das Auge etwas ungewohnt aussieht, so sind diese Terme auch ohne Klammern allesamt wohldefiniert. Davon überzeugt man sich, indem man die Terme von links nach rechts liest, und dabei bei jedem Funktionssymbol die zugehörige Stelligkeit bestimmt (zu welchem F_n gehört das Funktionssymbol?) und dann die folgenden Symbole in die geforderten n Terme aufspaltet (wenn dies nicht geht, so ist das Wort kein Term). Dabei entsteht schnell eine große Verschachtelungstiefe. Den letzten angeführten Term, also

$$\beta\alpha xgc_2\gamma fy\alpha gzx\,,$$

kann man mit (suggestiven) Klammern und Kommata nach und nach lesbarer gestalten. Er beginnt mit dem zweistelligen Funktionssymbol β, also muss das Folgende aus zwei Termen bestehen. Es folgt zunächst das ebenfalls zweistellige Funktionssymbol α, worauf zwei Terme folgen müssen. Wenn diese gefunden sind, muss der verbleibende Rest (also alles, was weiter rechts steht) den zweiten Term bilden, der von β verlangt wird. Die zwei Terme des an zweiter Stelle stehenden α sind x und gc_2. Man kann also den Term nach dieser Analyse auch als

$$\beta(\alpha(x, g(c_2)), \gamma fy\alpha gzx)$$

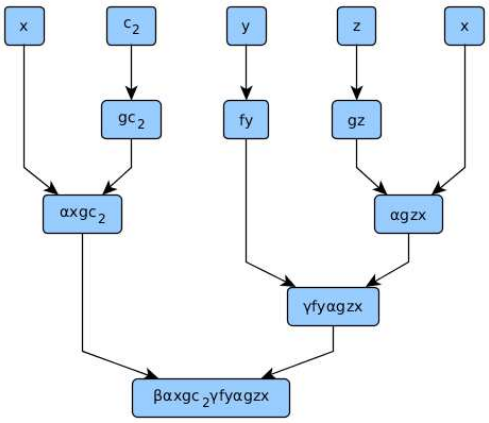
schreiben. Wenn man ebenso den zweiten Term für das äußere β auflöst, so erhält man

$$\beta(\alpha(x, g(c_2)), \gamma(fy, \alpha(g(z), x)))\,.$$

Übrigens kann man auch bei einem beliebigen Funktionssymbol mittendrin beginnen und die zugehörigen Terme, auf die es Bezug nimmt, bestimmen. Besonders übersichtlich wird die Termstruktur durch einen *Termstammbaum* ausgedrückt. Dabei werden die verwendeten Variablen und Konstanten (mehrfach, um die unterschiedlichen Stellen, in die sie eingesetzt werden, beachten zu können) als Blätter[7] nebeneinander aufgeführt. Sie bilden die 0-te Reihe des Baumes. Wenn ein n-stelliges Funktionssymbol auf n solche Blätter angewendet wird, so zeichnet man einen Knoten, bezeichnet ihn mit dem Funktionssymbol (bzw. dem Funktionssymbol mit den eingelesenen Termen) und verbindet es mit den eingelesenen Blättern (die Einlesungsreihenfolge

[7]Dies ist die graphentheoretische Bezeichnung für die Startpunkte eines Baumes.

entspricht der Blätterreihenfolge). So entsteht aus allen Funktionssymbolen, die nur auf Variablen und Konstanten Bezug nehmen, die erste Reihe des Baumes. Die Funktionssymbole, die auf solche Knoten (und Blätter) Bezug nehmen, bilden die nächste Reihe, u.s.w. Der Stamm des Baumes ist dann der in Frage stehende Term. In unserem Beispiel sieht das so aus:



Beispiel 6.8. Wir betrachten ein Modell für die Termmenge der natürlichen Zahlen. Als Grundtermmenge nehmen wir eine Variablenmenge V, die Konstantenmenge $K = \{0\}$, die einstelligen Funktionssymbolmenge $F_1 = \{N\}$ (N steht für Nachfolger) und die zweistellige Funktionssymbolmenge $F_2 = \{\alpha, \mu\}$ (für Addition und Multiplikation). Allein aus der Konstante 0 und dem Nachfolgersymbol N kann man dann für jede natürliche Zahl eine Repräsentierung finden, nämlich

$$N0\,, NN0,\ NNN0,\ NNNN0,\ \textit{etc.}$$

Typische Terme sind dann Ausdrücke wie (u, v, w seien Variablen)

$$\alpha NN0NNNv,\ \mu NN0\alpha NN0NNN0,\ \mu\alpha NNN0\mu NNuN0NNNNw, \text{ etc.}$$

Wenn man x' statt Nx, $(x + y)$ statt αxy und $(x \cdot y)$ statt μxy schreibt, so „verschönern“ sich diese Terme zu

$$(0'' + v'''),\ (0'' \cdot (0'' + 0''')),\ ((0''' + (u'' \cdot 0')) \cdot w''''), \text{ etc.}$$

Mit den Abkürzungen $1 = 0'$, $2 = 0''$ etc. wird daraus

$$2 + v''',\ (2 \cdot (2 + 3)),\ ((3 + (u'' \cdot 1)) \cdot w''''), \text{ etc.}\,.$$

Man beachte, dass die Einführung dieser Abkürzungen nicht bedeutet, dass dadurch die üblicherweise mit diesen Symbolen verwendeten Rechenregeln erlaubt sind. Der zweite Term oben ist nicht gleich 10, dem zehnten Nachfolger der 0.

Wir erklären noch, was die *Variablenmenge eines Terms* ist. Diese ist stets eine Teilmenge der Variablenmenge V und enthält diejenigen Variablen, die

in dem Term irgendwo vorkommen. Die rekursive Definition lautet folgendermaßen.

(1) Wenn $t = x$ eine Variable ist, so ist $\mathrm{Var}(x) = \{x\}$.
(2) Wenn $t = c$ eine Konstante ist, so ist $\mathrm{Var}(c) = \emptyset$.
(3) Wenn f ein n-stelliges Funktionssymbol ist und wenn $t_1, \ldots, t_n$ Terme sind, so ist $\mathrm{Var}(ft_1, \ldots, t_n) = \mathrm{Var}(t_1) \cup \ldots \cup \mathrm{Var}(t_n)$.

Aristoteles (384-322 v.C.) gilt als Erfinder der Prädikatenlogik. Er verwendet in seiner Analytik Variablen, einstellige Prädikate, Quantoren und die logischen Junktoren.

Nachdem wir die Terme zur Verfügung haben, fahren mit dem syntaktischen Aufbau der Ausdrücke in der Prädikatenlogik (mit Identität) fort. Um den Aufbau dieser formalen Sprache zu motivieren und das Verständnis der zunächst rein formalen Ausdrücke zu erleichtern, ist es hilfreich, an Bildungsweisen von mathematischen Aussagen zu erinnern. Der konsequente Aufbau der Syntax und der Semantik folgt in der nächsten Vorlesung.

6.2. **Relationen.**

Ein Term kann weder wahr noch falsch sein, und zwar unabhängig davon, ob man ihn einfach als ein nach gewissen formalen Regeln aufgebautes Symbolwort auffasst oder ihn in einer bestimmten Menge (etwa den natürlichen Zahlen) interpretiert. Wahr oder falsch können nur Aussagen sein. Wichtig sind für uns zunächst die formalen Eigenschaften einer Aussage. In mathematischen Aussagen kommen häufig Terme zusammen mit einem Vergleichssymbol vor, z. B. in der (wahren) Gleichung

$$2 \cdot (2 + 3) = 10$$

oder der (falschen) Abschätzung

$$2 \cdot (2+3) \; < \; 10.$$

Mit zwei Termen und dem Gleichheitszeichen oder Kleinerzeichen gelangt man also zu Aussagen, man spricht von zweistelligen Relationen (in Logik und Grammatik auch von zweistelligen Prädikaten). Der Wahrheitsgehalt hängt dabei von den zwei Eingaben ab.

Eine einstellige Relation oder ein Prädikat ist eine Eigenschaftsform, die einem Element zukommen kann oder nicht, z.B. die Eigenschaft einer natürlichen Zahl, prim zu sein oder gerade zu sein oder eine Quadratzahl zu sein, oder das Positivitätsprädikat, das besagt, dass eine reelle Zahl positiv ist. Einstellige Prädikate definieren eine Teilmenge einer gegebenen Grundmenge: Einem einstelligen Prädikat wird diejenige Teilmenge zugeordnet, die aus allen Elementen besteht, für die das Prädikat gilt. Daher entspricht die Mengenlehre weitgehend der Prädikatenlogik mit nur einstelligen Prädikaten.

Mit n-stelligen Relationenssymbolen und n Termen gelangt man ebenfalls zu einer Aussage. Wenn z.B. A, B, C als Punkte in der Ebene interpretiert werden können, und G die Relation „bildet ein gleichseitiges Dreieck“ bedeutet, so bedeutet $G(A, B, C)$, dass diese drei Punkte ein gleichseitiges Dreieck bilden. Der Wahrheitsgehalt hängt natürlich von der Lage der Punkte A, B, C ab, hier interessiert aber lediglich, dass $G(A, B, C)$ eine sinnvolle Aussageform repräsentiert.

Andere geometrische Beispiele für dreistellige Relationen sind die Eigenschaften, dass die drei Punkte A, B, C auf einer Geraden liegen, sagen wir $L(A, B, C)$, oder dass die drei Punkte ein rechtwinkliges Dreieck bilden, wobei der rechte Winkel an dem zuerst genannten Eckpunkt liegen muss, sagen wir $R(A, B, C)$. Man kann sich darüber streiten, ob bei einem Dreieck die Eckpunkte alle verschieden sein müssen, jedenfalls kann man die Eigenschaft der drei Punkte, dass sie paarweise verschieden sind, durch ein dreistelliges Prädikat ausdrücken, sagen wir $V(A, B, C)$.

6.3. **Quantoren.**

Mathematische Aussage enthalten häufig auch Existenzaussagen. Wenn wir bei dem eben erwähnten Beispiel bleiben, so bedeutet

$$\text{es gibt } z \, G(A, B, z)$$

die Aussage, dass es zu gegebenen festen A und B ein z gibt derart, dass die drei Punkte A, B, z ein gleichseitiges Dreieck bilden (diese Aussage ist in der reellen Zahlenebene wahr). In dem Beispielsatz wird nur über z quantifiziert, nicht über A und B. Dies kann man durch die folgenden Aussagen erreichen.

$$\text{es gibt } x \text{ und es gibt } y \text{ und es gibt } z \, G(x, y, z)\,,$$

was bedeutet, dass es Punkte x, y, z gibt, die ein gleichseitiges Dreieck bilden, die wahr ist, aber deutlich schwächer als die Aussage

$$\text{für alle } x \text{ und } \text{ für alle } y \text{ gibt es } z\, G(x, y, z)$$

ist, die behauptet, dass es zu (beliebig vorgegebenen) Eckpunkten x und y stets einen dritten Punkt gibt, so dass ein gleichseitiges Dreieck entsteht.[8] Die Ausdrücke „es gibt“ und „für alle“ nennt man *Quantoren*. Für diese Quantoren gibt es spezielle Symbole, nämlich $\exists$ für „es gibt“ und $\forall$ für „für alle“. Die obigen Beispielsätze schreibt man dann formal als

$$\exists x \exists y \exists z G(x, y, z)$$

bzw. als

$$\forall x \forall y \exists z G(x, y, z)\,.$$

Auf die Reihenfolge bei gleichartigen Quantoren kommt es nicht an (dies ist von der inhaltlichen Bedeutung her klar, wird später aber auch formal im Ableitungskalkül nachgebildet), sie ist aber bei wechselnden Quantoren entscheidend. Beispielsweise ist die Aussage

$$\exists z \forall x \forall y G(x, y, z)$$

(also die Aussage, dass es einen Punkt gibt, der mit je zwei beliebigen weiterer Punkten ein gleichseitiges Dreieck bildet) im Gegensatz zur vorherigen Aussage nicht wahr.

6.4. **Junktoren.**

Eine weitere Art von mathematischen Aussagen entsteht dadurch, dass man Aussagen selbst zueinander in eine logische Beziehung setzt, indem man beispielsweise sagt, dass aus der Aussage α die Aussage β folgt, oder dass α und β zueinander äquivalent sind. Der Satz des Pythagoras besagt, dass wenn zwischen drei Punkten A, B, C in der Ebene die Beziehung der Rechtwinkligkeit am Punkt A besteht, dass dann zwischen den durch die drei Punkte definierten Streckenlängen ebenfalls eine bestimmte Beziehung zwischen den Abständen[9] besteht. Wenn man die Rechtwinkligkeit wie oben mit dem dreistelligen Relationssymbol R und die pythagoreische Längenbeziehung mit dem dreistelligen Relationssymbol S bezeichnet, so gilt also

$$\text{aus } R(A, B, C) \text{ folgt } S(A, B, C)\,,$$

was wir formal als

$$\forall A \forall B \forall C (R(A, B, C) \longrightarrow S(A, B, C))$$

schreiben. Gilt davon auch die Umkehrung? Folgt also aus $S(A, B, C)$, dass ein rechter Winkel an A vorliegt? Dies ist in der Tat der Fall! Der Kosinussatz

[8] Die Gültigkeit dieser Aussagen setzt voraus, dass wir über den reellen Zahlen bzw. in der reellen Zahlenebene arbeiten. Siehe Aufgabe 6.18.

[9] Zur Erinnerung: Das Quadrat der Streckenlänge zwischen B und C (die Hypotenuse) ist gleich der Summe der Quadrate der beiden Streckenlängen zwischen A und B und A und C (den Katheten).

besagt für ein beliebiges (echtes) Dreieck mit einem an A anliegenden Winkel α, dass

$$d(B,C)^2 \;=\; d(A,B)^2 + d(A,C)^2 - 2d(A,B)d(A,C)\cos\,\alpha$$

gilt, wobei d den Abstand zwischen zwei Punkten bezeichne. Der „Störterm“ rechts entfällt genau dann, wenn $\cos\,\alpha \;=\; 0$ ist, und dies ist nur bei 90 Grad der Fall. Daher gilt die Äquivalenz

$$\forall A \forall B \forall C (R(A,B,C) \longleftrightarrow S(A,B,C))$$

(ein Dreieck, bei dem zwei Eckpunkte zusammenfallen, akzeptieren wir als rechtwinklig an dem doppelten Punkt).

Unser Rechtwinkligkeitsprädikat $R(A,B,C)$ besagt, dass der Winkel am Eckpunkt A ein Rechter ist. Wenn man sich dafür interessiert, ob überhaupt ein rechtwinkliges Dreieck vorliegt, so muss $R(A,B,C)$ oder $R(B,C,A)$ oder $R(C,A,B)$ gelten. Die Oderverknüpfung wird formal als

$$(R(A,B,C) \vee R(B,C,A)) \vee R(C,A,B)$$

geschrieben (die Assoziativität der oder-Verknüpfung steht im Moment noch nicht zur Verfügung).

Für ein echtes Dreieck haben wir oben gefordert, dass die konstituierenden Punkte A, B, C paarweise verschieden sind. Die Gleichheit von zwei Punkten wird durch $A \;=\; B$ und die Negation davon, also die Verschiedenheit der beiden Punkte, wird in der Mathematik durch $A \neq B$, in der Logik aber durch $\neg\,(A = B)$ ausgedrückt. Dass drei Punkte paarweise verschieden sind, erfordert ein logisches und, das durch $\wedge$ symbolisiert wird, so dass sich die Echtheit eines Dreiecks durch

$$(\neg\,(A = B) \wedge \neg\,(A = C)) \wedge \neg\,(B = C)$$

ausdrücken lässt.

6. Arbeitsblatt

6.1. **Übungsaufgaben.**

Aufgabe 6.1. Entwerfe einen Termstammbamm für den Term

$$f\alpha\alpha g x \alpha c_2 f \beta g y \alpha c_1 g f z \beta g c_1 f c_1$$

wie in Beispiel 6.7.

Aufgabe 6.2. Wir betrachten die arithmetische Grundtermmenge, die aus den Konstanten 0 und 1, den Variablen x_n, $n \in \mathbb{N}$, dem einstelligen Funktionssymbol N und den beiden zweistelligen Funktionssymbolen α und μ besteht. Entscheide, ob die folgenden Wörter über diesem Termalphabet Terme sind oder nicht.

(1) $NNNNNNN01$,
(2) $NNNNNNx_1NNNNNNNNNNNx_2$,
(3) $\alpha NNNNNN0NNNNNNNNNNN1$,
(4) $NNN\mu NNN\mu 0NNNNNNNNNNN1$,
(5) $\mu\alpha\mu\alpha\mu\alpha 0101010$,
(6) $\alpha\alpha\alpha Nx_1Nx_2x_3x_4x_3$.

Schreibe diejenigen Wörter, die Terme sind, mit Klammern, $'$, $+$ und $\cdot$.

Aufgabe 6.3.*

Es seien x, y, z, w Variablen und V ein zweistelliges Funktionssymbol. Welche der folgenden Wörter sind Terme?

(1) $VxyzVVw$,
(2) $VVxyVzw$,
(3) $VVxyzVw$,
(4) $VxVyVzw$,
(5) $xVyVzVw$,
(6) $VVVxyzw$,
(7) $VxyVVzw$,
(8) $VVxVyzw$,
(9) $VxyVzw$,
(10) $VxVyzVw$,
(11) $VxVVyzw$,
(12) $VxyVzVw$.

Aufgabe 6.4. Erläutere den Unterschied zwischen $G = (V, K, F_n, n \in \mathbb{N}_+)$ und $A = V \cup K \cup \bigcup_{n\in\mathbb{N}_+} F_n$ in Definition 6.6.

Aufgabe 6.5. Es sei V eine Variablenmenge, K eine Konstantenmenge und F eine Menge aus Funktionssymbolen (mit einer gewissen Stelligkeit). Es sei

$$A = V \cup K \cup F$$

das zugehörige Alphabet. Es sei vorausgesetzt, dass dieses Alphabet nicht leer sei. Zeige, dass es nichtleere Wörter über A gibt, die keine Terme sind.

Aufgabe 6.6. Es sei G eine Grundtermmenge und $t \in T(G)$ ein G-Term. Es sei u das am weitesten links stehende Symbol von t und v das am weitesten rechts stehende Symbol von t. Zeige die folgenden Eigenschaften.

(1) Wenn u eine Variable oder eine Konstante ist, so ist $t = u$.
(2) v ist eine Variable oder eine Konstante.
(3) Wenn t_1 und t_2 Terme sind, so ist t_1t_2 kein Term.

Aufgabe 6.7. Es sei G eine Grundtermmenge und t ein G-Term. Es sei n die Gesamtzahl der Variablen und Konstanten in t, wobei mehrfaches Vorkommen auch mehrfach gezählt wird. Es sei k die Summe über alle Stelligkeiten der in t vorkommenden Funktionssymbole, wobei wiederum mehrfach auftretende Symbole auch mehrfach gezählt werden.

(1) Bestimme n und k im Term
$$ggxyhfxfzgyfy\,,$$
wobei f einstellig, g zweistellig und h dreistellig sei.
(2) Es sei t weder eine Variable noch eine Konstante. Zeige $k \geq n$.
(3) Zeige, dass die Differenz $n - k$ beliebig groß sein kann.

Aufgabe 6.8. Diskutiere, ob es sich bei
$$n!,\ \binom{n}{k},\ \pi,\ e^u, x^y,\ 5^x,\ \sqrt{x},\ \heartsuit$$
um Terme handelt.

Aufgabe 6.9. Es sei f ein zweistelliges Funktionssymbol und x, y Variablen. Formuliere das Kommutativgesetz (für f) als eine Allaussage mit Hilfe der Identität von zwei Termen.

Aufgabe 6.10. Es sei K ein Körper und $V = \{x_1, \ldots, x_n\}$ eine Variablenmenge. Eine Grundtermmenge G sei durch K als Konstantenmenge, V als Variablenmenge und den beiden zweistelligen Funktionssymbolen $+$ und $\cdot$ festgelegt. In welcher Beziehung steht die Termmenge $T(G)$ zum Polynomring $K[x_1, \ldots, x_n]$.

Aufgabe 6.11. Es sei T die Termmenge zur Konstantenmenge $\{0, 1\}$, zur Variablenmenge x_i, $i \in I$ und zur zweistelligen Funktionssymbolmenge $\{+, \cdot\}$. Definiere eine natürliche Abbildung von T in den Polynomring $\mathbb{Z}[x_i : i \in I]$. Ist diese Abbildung injektiv? Ist sie surjektiv? Was ist das Bild?

Aufgabe 6.12. Für Punkte A, B, C in der Ebene bedeute $R(A, B, C)$ die Rechtwinkligkeit des durch A, B, C gegebenen Dreiecks an der Ecke A und $S(A, B, C)$ die pythagoreische Längenbeziehung. Betrachte die beiden formalen Aussagen
$$\forall A \forall B \forall C(R(A, B, C) \longrightarrow S(A, B, C))$$
und
$$\forall A \forall B \forall C R(A, B, C) \longrightarrow \forall A \forall B \forall C S(A, B, C)\,.$$

Welche ist (sind) eine Formalisierung des Satzes von Pythagoras, welche ist (sind) wahr?

Aufgabe 6.13. Formuliere mit arithmetischen Grundsymbolen, Gleichheit, Quantoren und Junktoren die Eigenschaft (das Prädikat) einer natürlichen Zahl, gerade oder ungerade zu sein. Formuliere ebenso die Aussage, dass jede natürliche Zahl entweder gerade oder ungerade ist. Formuliere ferner die Aussage, dass zu jeder natürlichen Zahl n die Zahl $n^2 - n$ gerade ist.

6.2. **Aufgaben zum Abgeben.**

Aufgabe 6.14. (3 Punkte)

Seien M, N, L Mengen. Stifte eine Bijektion zwischen

$$\text{Abb}\,(M \times N, L) \;\text{ und }\; \text{Abb}\,(M, \text{Abb}\,(N, L))\;.$$

Aufgabe 6.15. (2 Punkte)

Eine Grundtermmenge sei durch die Variablenmenge $V = \{x, y, z\}$, eine Konstantenmenge $K = \{c_1, c_2\}$, die einstelligen Funktionssymbole $F_1 = \{f, g\}$ und die zweistelligen Funktionssymbole $F_2 = \{\alpha, \beta, \gamma\}$ gegeben. Entwerfe einen Termstammbaum für den Term

$$gf\beta\beta\alpha fxy\gamma c_1 zggc_2\,.$$

Aufgabe 6.16. (2 Punkte)

Es sei f ein zweistelliges Funktionssymbol und x, y, z Variablen. Formuliere das Assoziativgesetz (für f) als eine Allaussage mit Hilfe der Identität von zwei Termen.

Aufgabe 6.17. (3 Punkte)

Eine Grundtermmenge G sei durch eine einelementige Konstantenmenge $K = \{c\}$, eine leere Variablenmenge und eine einelementige einstellige Funktionssymbolmenge

$$F_1 = \{f\}$$

gegeben. Zeige durch Induktion, dass es eine bijektive Abbildung

$$\varphi\colon \mathbb{N} \longrightarrow T(G)$$

mit $\varphi(0) = c$ und $\varphi(n+1) = f\varphi(n)$ für alle $n \in \mathbb{N}$ gibt.

Aufgabe 6.18. (5 Punkte)

Zeige, dass es kein gleichseitiges Dreieck im $\mathbb{R}^2$ gibt, dessen sämtliche Ecken rationale Koordinaten besitzen.

Tipp: Verwende, dass $\sqrt{3}$ irrational ist und den Satz des Pythagoras.

7. Vorlesung - Semantik der Prädikatenlogik

7.1. **Sprachen erster Sufe.**

Die in der letzten Vorlesung erwähnten Konstruktionsmöglichkeiten für Aussagen sind im Wesentlichen schon erschöpfend. Mit ihnen kann man ausgehend von einer Grundtermmenge formale Sprachen aufbauen, deren Aussagekraft prinzipiell groß genug ist, um die gesamte Mathematik auszudrücken (für viele Bereiche wäre es aber künstlich, sich auf diese Sprachen zu beschränken). Diese formalen Sprachen nennt man *Sprachen erster Stufe*, deren syntaktischen Aufbau wir hier beschreiben. Wir beginnen mit den zugehörigen Alphabeten.

Definition 7.1. Ein *Alphabet einer Sprache erster Stufe* umfasst die folgenden Daten.

(1) Eine Grundtermmenge, also eine Menge aus Variablen, Konstanten und Funktionssymbolen.
(2) Zu jeder natürlichen Zahl $n \in \mathbb{N}_+$ eine Menge R_n von n-stelligen Relationssymbolen.
(3) Die aussagenlogischen Junktoren
$$\neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow\ .$$
(4) Das Gleichheitszeichen $=$.
(5) Die Quantoren $\forall$ und $\exists$.
(6) Klammern, also (und).

Die aussagenlogischen Junktoren sind von der Aussagenlogik her bekannt und werden sowohl semantisch als auch syntaktisch ihre Rolle behalten. Der Quantor $\forall$ heißt *Allquantor* und $\exists$ heißt *Existenzquantor*. Diese Liste ist etwas redundant, da man, von der späteren Interpretation her gesehen, einige aussagenlogische Junktoren durch andere ersetzen kann, wie wir das schon im aussagenlogischen Kontext gesehen und verwendet haben. Ebenso kann man den einen Quantor mit Hilfe des anderen und der Negation ausdrücken, es ist nämlich $\forall x \alpha$ gleichbedeutend mit $\neg\exists x \neg\alpha$. Um die Lesbarkeit der Ausdrücke zu erhöhen, ist es aber alles in allem vorteilhaft, nicht allzu minimalistisch sein zu wollen (man könnte die unnötigen Symbole auch als Abkürzungen einführen). Das Gleichheitszeichen könnte man zwar auch als ein weiteres zweistelliges Relationssymbol auffassen, allerdings sind die weiter unten einzuführenden Schlussregeln für das Gleichheitszeichen (insbesondere die Möglichkeit einzusetzen) für die Logik erster Stufe konstitutiv. Da ein

Alphabet einer Sprache erster Stufe eine Termgrundmenge enthält, ist klar, was als Term in der Sprache zu gelten hat. Als nächstes erklären wir formal, was wir als einen Ausdruck (oder eine formale Aussage) in dieser Sprache ansehen.

Definition 7.2. Es sei ein Alphabet einer Sprache erster Stufe gegeben. Dann nennt man die folgenden rekursiv definierten Wörter über diesem Alphabet die *Ausdrücke* dieser Sprache.

(1) Wenn t_1 und t_2 Terme sind, so ist
$$t_1 = t_2$$
ein Ausdruck.

(2) Wenn R ein n-stelliges Relationssymbol ist und $t_1, \ldots, t_n$ Terme sind, so ist
$$Rt_1 \ldots t_n$$
ein Ausdruck.

(3) Wenn α und β Ausdrücke sind, so sind auch
$$\neg(\alpha)\,,\ (\alpha) \wedge (\beta)\,,\ (\alpha) \vee (\beta)\,,\ (\alpha) \to (\beta)\,,\ (\alpha) \leftrightarrow (\beta)$$
Ausdrücke.

(4) Wenn α ein Ausdruck ist und x eine Variable, so sind auch
$$\forall x\,(\alpha) \ \text{ und } \exists x\,(\alpha)$$
Ausdrücke.

Die Klammern sind hier auch nur nötig, weil wir die zweistelligen Junktoren anders als die Funktionssymbole in der Mitte schreiben. Die Menge der Konstanten, der Variablen, der Funktionssymbole und der Relationssymbole nennt man zusammen auch das *Symbolalphabet* der Sprache, das wir mit S bezeichnen. Die anderen Symbole (Junktoren, Quantoren, Gleichheitszeichen, Klammern) sind immer gleich, so dass eine Sprache erster Stufe im Wesentlichen nur von der gewählten Symbolmenge S abhängt. Für die zugehörige Sprache schreibt man L^S.

7.2. **Strukturen und Interpretationen.**

Gelegentlich haben wir schon angedeutet, was die zuletzt eingeführten prädikatenlogischen Symbole, die wir rein formal als Zeichenreihen behandelt haben, eigentlich bedeuten sollen, was also ihr logisch-mathematischer Gehalt sein soll. Bei einer solchen Interpretation werden die Junktoren, die Quantoren und das Gleichheitszeichen stets in der gleichen Weise interpretiert (die Junktoren werden wie im aussagenlogischen Kontext interpretiert), die Variablen, Konstanten, Funktions- und Relationssymbole aber unterschiedlich.

Definition 7.3. Es sei S das Symbolalphabet einer Sprache erster Stufe. Unter einer *S- Struktur* versteht man eine nichtleere Menge M mit den folgenden Festlegungen.

(1) Für jede Konstante $c \in K$ ist ein Element $c^M \in M$ festgelegt.
(2) Zu jedem n-stelligen Funktionssymbol f (aus S) ist eine n-stellige Funktion
$$f^M \colon M^n \longrightarrow M$$
festgelegt.
(3) Zu jedem n-stelligen Relationssymbol R (aus S) ist eine n-stellige Relation
$$R^M \subseteq M^n$$
festgelegt.

Unter einer S- *(Variablen)belegung* in M versteht man eine Festlegung $x^M \in M$ für jede Variable $x \in V$.

Unter einer S- *Interpretation* versteht man eine S-Struktur zusammen mit einer S-Belegung.

Die Menge M heißt auch *Grundmenge* der S-Struktur bzw. der S-Interpretation. Die Festlegung für die Konstanten und die Variablen ist einfach eine Abbildung von K bzw. von der Variablenmenge in die Menge M. Statt c^M, x^M, F^M, R^M schreibt man auch $I(c), I(x), F^I, R^I$, wobei I eine Interpretation bezeichnet. Die Strukturen sind die üblichen Gegenstände der Mathematik (die Belegung von freien Variablen ist der mathematischen Praxis eigentlich fremd; durch sie wird sichergestellt, dass bei einer Interpretation jeder Ausdruck wahr oder falsch wird).

Beispiel 7.4. Es sei S ein Symbolalphabet, das außer einer Variablenmenge V aus einem einzigen einstelligen Funktionssymbol F bestehe (die Konstantenmenge und die Relationssymbolmengen seien also leer). Eine S-Struktur besteht dann aus einer nichtleeren Menge M zusammen mit einer Abbildung
$$f = F^M \colon M \longrightarrow M,\ a \longmapsto f(a).$$
Beispiele sind $M = \mathbb{N}$ mit der Nachfolgerfunktion, $M = \mathbb{R}$ mit dem Quadrieren $x \mapsto x^2$ oder der Sinusfunktion oder der Exponentialfunktion, oder eine beliebige Menge mit der Identität, eine endliche Menge mit einer Permutation, u.s.w.

Beispiel 7.5. Es sei S ein Symbolalphabet, das außer einer Variablenmenge V aus einem einzigen zweistelligen Funktionssymbol F bestehe (die Konstantenmenge und die Relationssymbolmengen seien also leer). Eine S-Struktur besteht dann aus einer nichtleeren Menge M zusammen mit einer Abbildung
$$f = F^M \colon M \times M \longrightarrow M,\ (a, b) \longmapsto f(a, b).$$
Eine solche Abbildung nennt man auch eine Verknüpfung auf M

sie ordnet

(einem geordneten Paar aus) zwei Elementen der Menge ein weiteres Element der Menge zu. Die Addition oder die Multiplikation auf den natürlichen Zahlen sind jeweils eine solche Verknüpfung. Weitere Beispiele sind die

Verknüpfung in einer Gruppe, die Vektorraumaddition, das Maximum von zwei reellen Zahlen, u.s.w.

Beispiel 7.6. Es sei S ein Symbolalphabet, das außer einer Variablenmenge V aus einem einzigen einstelligen Relationssymbol R bestehe (die Konstantenmenge und die Funktionssymbolmengen seien also leer). Eine S-Struktur besteht dann aus einer nichtleeren Menge M zusammen mit einer fixierten Teilmenge $U \subseteq M$. Beispiele sind $M = \mathbb{N}$ mit der Teilmenge der Primzahlen, oder der Teilmenge der Quadratzahlen, oder $M = \mathbb{R}$ mit der Teilmenge der positiven Zahlen, oder der Teilmenge der rationalen Zahlen, u.s.w.

7.3. **Interpretation von Termen.**

Mit einer solchen Interpretation in M wird das Symbolalphabet, das neben den Junktoren, Quantoren, dem Gleichheitszeichen und den Klammern das Alphabet der Sprache bildet, interpretiert. Man möchte aber die gesamte Sprache in M, ausgehend von der Interpretation dieser Symbole, interpretieren. Der erste Schritt dazu ist die Interpretation der Terme. Die Wohldefiniertheit der folgenden Festlegung ergibt sich durch einen Beweis über den Aufbau der Terme.

Definition 7.7. Zu einem Symbolalphabet S erster Stufe und einer S-Interpretation in einer Menge M wird induktiv über den Aufbau der Terme für jeden S-Term t eine Interpretation $I(t)$ in M definiert.

(1) Für jede Konstante c und jede Variable x ist die Terminterpretation durch die Interpretation bzw. die Belegung direkt gegeben, also $I(c) = c^M$ und $I(x) = x^M$.
(2) Wenn $t_1, \ldots, t_n$ Terme mit den Interpretationen $I(t_1), \ldots, I(t_n)$ sind und wenn f ein n-stelliges Funktionssymbol ist, so wird der Term $ft_1 \ldots t_n$ als $f^M(I(t_1), \ldots, I(t_n))$ interpretiert.

Damit werden alle Terme in der Grundmenge M interpretiert. Es wird also die auf $K \cup V$ gegebene Interpretation auf die gesamte Termmenge T fortgesetzt, oder, mit anderen Worten, es liegt ein kommutatives Diagramm

$$\begin{array}{ccc} K \cup V & \longrightarrow & M \\ \downarrow & \nearrow & \\ T & & \end{array}$$

vor, wobei der Diagonalpfeil durch den horizontalen Pfeil eindeutig festgelegt ist.

In vielen Situationen bleibt die Grundmenge und die Interpretation der Konstanten und der Relations- und Funktionssymbole gleich, während man die Variablenbelegung ändern möchte. Insbesondere möchte man Interpretationen für eine einzelne Variable abändern. Dafür gibt es das Konzept der Uminterpretation.

Definition 7.8. Es sei ein Symbolalphabet S erster Stufe und eine S-Interpretation I in einer Menge M gegeben. Es sei x eine Variable und $m \in M$ ein Element der Grundmenge. Dann versteht man unter der *Uminterpretation* $I\frac{m}{x}$ diejenige Interpretation von S in M, die strukturgleich zu I ist und für deren Variablenbelegung

$$\left(I\frac{m}{x}\right)(y) = \begin{cases} I(y), & \text{falls } y \neq x\,, \\ m, & \text{falls } y = x\,, \end{cases}$$

gilt.

Entsprechend schreibt man $I\frac{m_1,\ldots,m_k}{x_1,\ldots,x_k}$ für $\left(\left(I\frac{m_1}{x_1}\right)\frac{m_2}{x_2}\right)\ldots\frac{m_k}{x_k}$, wobei es bei verschiedenen Variablen nicht auf die Reihenfolge ankommt.

7.4. **Interpretation von Ausdrücken.**

Nachdem wir alle Terme bei einer gegebenen S-Interpretation interpretieren können, wenden wir uns nun den Ausdrücken zu. Es ist das Ziel, jedem S-Ausdruck eine Aussage (unter Bezug auf die Grundmenge M und die Interpretation des Symbolalphabets) zuzuordnen, die wahr oder falsch ist.

Definition 7.9. Zu einem Symbolalphabet S erster Stufe und einer S-Interpretation I in einer Menge M werden die S-Ausdrücke folgendermaßen (induktiv über den Aufbau der Ausdrücke) interpretiert und als gültig (oder ungültig) charakterisiert (die Gültigkeit einer Aussage α unter der Interpretation wird dabei als $I \vDash \alpha$ geschrieben). Es seien $s, t, t_1, \ldots, t_n$ Terme und α, β Ausdrücke.

(1) $I \vDash s = t$, wenn $I(s) = I(t)$.
(2) $I \vDash Rt_1 \ldots t_n$, wenn $(I(t_1), \ldots, I(t_n)) \in R^M$.
(3) $I \vDash \neg(\alpha)$, wenn nicht $I \vDash \alpha$ gilt.
(4) $I \vDash (\alpha) \wedge (\beta)$, wenn $I \vDash \alpha$ und $I \vDash \beta$ gilt.
(5) $I \vDash (\alpha) \to (\beta)$, wenn die Gültigkeit $I \vDash \alpha$ die Gültigkeit $I \vDash \beta$ impliziert.
(6) $I \vDash \exists x\alpha$, wenn es ein $m \in M$ mit $I\frac{m}{x} \vDash \alpha$ gibt.
(7) $I \vDash \forall x\alpha$, wenn für alle $m \in M$ die Beziehung $I\frac{m}{x} \vDash \alpha$ gilt.

Dabei ist, wie bei jeder Definition, „wenn“ als „genau dann, wenn“ zu lesen. Auf der linken Seite stehen die formalen Ausdrücke zusammen mit der Erklärung, ob sie in der Interpretation gelten, und auf der rechten Seite steht eine logisch-mathematische Bedingung. Diese ist im Sinne des üblichen Gebrauchs in der Mathematik zu verstehen. Für die Gültigkeitsbeziehung $I \vDash \alpha$ sagt man auch, dass die Interpretation I ein *Modell* für den Ausdruck α ist oder den Ausdruck α erfüllt.

Da bei dieser Zuordnung alle möglichen Konstruktionsweisen für Ausdrücke auftreten, ergibt sich eine Erklärung für jeden Ausdruck durch deren induktiven Aufbau. Für jeden Ausdruck α gilt in einer Interpretation I entweder $I \vDash \alpha$ oder nicht, wobei die Nichtgültigkeit zur Gültigkeit von $I \vDash \neg\alpha$ äquivalent ist. Eine Interpretation liefert also insbesondere eine *vollständige Aufteilung* der S-Ausdrücke in wahre und falsche Ausdrücke.

7.5. **Beispiele.**

Beispiel 7.10. Es sei S ein Symbolalphabet, das außer einer Variablenmenge V aus einem einzigen einstelligen Funktionssymbol F bestehe (die Konstantenmenge und die Relationssymbolmengen seien also leer), so dass eine S-Struktur aus einer Menge M zusammen mit einer Abbildung

$$f = F^M \colon\ M \longrightarrow M,\ a \longmapsto f(a),$$

besteht. In einer solchen Interpretation wird jeder S-Ausdruck interpretiert. Der Ausdruck

$$\alpha\ =\ \forall x(\exists y(Fy = x))$$

besagt die Surjektivität von $f\ =\ F^M$. D.h. in einer S-Interpretation gilt

$$I \vDash \alpha$$

genau dann, wenn die durch die Interpretation festgelegte Abbildung f surjektiv ist. Der Ausdruck

$$\beta\ =\ \forall x(\forall y((Fx = Fy) \to (x = y)))$$

besagt die Injektivität von f. D.h. in einer S-Interpretation gilt

$$I \vDash \beta$$

genau dann, wenn die durch die Interpretation festgelegte Abbildung f injektiv ist.

Beispiel 7.11. Es sei S das Symbolalphabet für einen angeordneten Körper, d.h. es gebe eine zweielementige Konstantenmenge $K\ =\ \{0, 1\}$, eine zweielementige Menge für die zweistelligen Funktionssymbole $\{+, \cdot\}$ und eine einelementige Menge $\{\geq\}$ für ein zweistelliges Relationssymbol.[10] Wir betrachten die Interpretation I_1 mit der Grundmenge $\mathbb{Q}$ und die Interpretation I_2 mit der Grundmenge $\mathbb{R}$, wobei Konstanten, Funktionssymbole und das Relationssymbol in natürlicher Weise interpretiert werden (und die Variablenbelegung irgendwie festgelegt sei).

Der S-Ausdruck $1 + 1\ \geq\ 1$ (also der Ausdruck $\geq +111$ in vorgestellter Notation) wird unter den Interpretationen als $1_{\mathbb{Q}} + 1_{\mathbb{Q}}\ \geq\ 1_{\mathbb{Q}}$ bzw. als $1_{\mathbb{R}} + 1_{\mathbb{R}}\ \geq\ 1_{\mathbb{R}}$ interpretiert und daher gelten $I_1 \vDash 1 + 1 \geq 1$ und $I_2 \vDash 1 + 1 \geq 1$.

[10] Es ist typisch, dass man sich bei der Wahl der Symbole im Smbolalphabet von einer beabsichtigten Interpretation leiten lässt. Daher stimmen häufig die Symbole mit den mathematischen Bezeichnungen überein.

Dagegen ist der Ausdruck $\forall x(x \geq 0 \to \exists y(x = y \cdot y))$ unter I_1 falsch und unter I_2 richtig, also

$$I_1 \vDash \neg(\forall x(x \geq 0 \to \exists y(x = y \cdot y))) \text{ und } I_2 \vDash \forall x(x \geq 0 \to \exists y(x = y \cdot y)) .$$

Das vorstehende Beispiel zeigt, dass die Gültigkeit von Ausdrücken unter einer bestimmten Interpretation von Eigenschaften der Grundmenge abhängt und durch eine mathematische Argumentation erwiesen oder zurückgewiesen werden muss. Diese kann beliebig kompliziert sein. Insbesondere bedeutet die Modellbeziehung nicht, dass man für jeden Ausdruck entscheiden kann, ob er in einer Interpretation wahr oder falsch ist.

7. Arbeitsblatt

7.1. Übungsaufgaben.

Aufgabe 7.1.*

Wir betrachten den Satz „Diese Vorlesung versteht keine Sau“. Negiere diesen Satz durch eine Existenzaussage.

Aufgabe 7.2.*

Negiere die Aussage „Martina findet alle Jungs im Kurs außer Markus zuckersüß“ durch eine Aussage, in der eine Existenzaussage und eine Oder-Verknüpfung vorkommen.

Aufgabe 7.3. Man formalisiere die folgenden Aussagen, indem man geeignete Prädikate erklärt. Man gebe die Negation der Aussagen (umgangssprachlich und formal) an.

(1) Alle Vögel sind schon da.
(2) Alle Wege führen nach Rom.
(3) Faulheit ist aller Laster Anfang.
(4) Alle Menschen werden Brüder, wo dein sanfter Flügel weilt.
(5) Wem der große Wurf gelungen, eines Freundes Freund zu sein, wer ein holdes Weib errungen, mische seinen Jubel ein![11]
(6) Freude trinken alle Wesen an den Brüsten der Natur.
(7) Alle Macht geht vom Volk aus.
(8) Alle Achtung.
(9) Alle Neune.

[11] Dieser Satz ist im Konjunktiv formuliert, was eher auf eine Aufforderung hindeutet als auf eine Aussage. Man kann hier „soll mischen“ als Prädikat nehmen und damit arbeiten.

Aufgabe 7.4. Es sei S das erststufige Symbolalphabet, das aus den Variablen x, y, z, den Konstanten $0, c$, dem einstelligen Funktionssymbol F, den zweistelligen Funktionssymbolen α, β und dem zweistelligen Relationssymbol R bestehe. Überprüfe, ob die folgenden Wörter zur Sprache L^S (bei korrekter Klammerung) gehören.

(1) Fx,
(2) $\forall x\,(Fx = c)$,
(3) $x = w$,
(4) $(Fx = c) \to (\alpha)$,
(5) $(Fx = c) \to (\neg\,(\exists y\,(Fx = c)))$,
(6) $R0$,
(7) $(\forall z\,(R0x)) \wedge (\neg\,(\beta\alpha yzy = Rcz))$,
(8) $(\forall z\,(R0x)) \wedge (\neg\,(\beta\alpha yzy = \beta cz))$.

Aufgabe 7.5. Bestimme die kleinsten Symbolmengen, mit denen die folgenden Ausdrücke formulierbar sind.

(1) $\exists y\,(fx = y)$,
(2) $\forall x\,(fx = gyc) \wedge \exists z\,(Rzxy)$,
(3) $\forall x \exists y Sxhuy$.

Aufgabe 7.6. Man gebe für die folgenden Teilmengen der natürlichen Zahlen quantorenlogische Beschreibungen.

(1) Die Menge der geraden Zahlen,
(2) Die Menge der Zahlen, die durch vier teilbar sind,
(3) Die Menge der ungeraden Zahlen,
(4) Die Menge der Quadratzahlen,
(5) Die Menge der Primzahlen,
(6) Die Menge der Zahlen, die als Summe von drei Quadratzahlen geschrieben werden können.

In der folgenden Aufgabe geht es nicht um die Wahrheit der Aussagen, sondern nur um die quantorenlogische Formulierung. Man darf und soll sich natürlich trotzdem Gedanken über die Gültigkeit machen.

Aufgabe 7.7. Formuliere die folgenden Aussagen über die natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ allein mittels Gleichheit, Addition, Multiplikation und unter Verwendung von aussagenlogischen Junktoren und Quantoren.

(1) $5 \geq 3$.
(2) $5 > 3$.
(3) $5 \leq 3$.
(4) 7 ist eine Primzahl.

(5) 8 ist eine Primzahl.
(6) 8 ist keine Primzahl.
(7) Jede natürliche Zahl besitzt mindestens einen Primfaktor.
(8) Jede natürliche Zahl größer gleich 2 besitzt mindestens einen Primfaktor.
(9) Wenn eine Primzahl ein Produkt teilt, so teilt sie auch mindestens einen der Faktoren.
(10) Es gibt Zahlen, die ein Produkt teilen, obwohl sie keinen der Faktoren teilen.

Aufgabe 7.8. Formuliere die folgenden Beziehungen (ein- oder mehrstellige Prädikate) innerhalb der natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ allein mittels Gleichheit, Addition, Multiplikation und unter Verwendung von aussagenlogischen Junktoren und Quantoren.

(1) $x \geq y$.
(2) $x > y$.
(3) x teilt y.
(4) x teilt nicht y.
(5) x ist eine Quadratzahl.
(6) x ist eine Primzahl.
(7) x ist keine Primzahl.
(8) x ist das Produkt von genau zwei verschiedenen Primzahlen.
(9) x wird von einer Primzahl geteilt.

Aufgabe 7.9. Formalisiere die folgenden mengentheoretischen Fassungen einiger aristotelischer Syllogismen in der Prädikatenlogik erster Stufe.

(1) Modus Barbara: Aus $B \subseteq A$ und $C \subseteq B$ folgt $C \subseteq A$.
(2) Modus Celarent: Aus $B \cap A = \emptyset$ und $C \subseteq B$ folgt $C \cap A = \emptyset$.
(3) Modus Darii: Aus $B \subseteq A$ und $C \cap B \neq \emptyset$ folgt $C \cap A \neq \emptyset$.
(4) Modus Ferio: Aus $B \cap A = \emptyset$ und $C \cap B \neq \emptyset$ folgt $C \not\subseteq A$.
(5) Modus Baroco: Aus $B \subseteq A$ und $B \not\subseteq C$ folgt $A \not\subseteq C$.

Aufgabe 7.10. Finde Parallelen zwischen Aussagen- und Quantorenlogik einerseits und Mengentheorie andererseits.

Aufgabe 7.11. Man mache sich den Unterschied zwischen den Aussagenvariablen in der Sprache der Aussagenlogik und den Variablen in der Sprache der Prädikatenlogik klar.

Aufgabe 7.12. Formalisiere in der arithmetischen Sprache (mit $+$ und $\cdot$) die folgenden (wahren) Aussagen.

(1) Wenn $x \geq y$ und $y \geq z$, so ist $x \geq z$.
(2) Wenn $x \geq y$ und $y \geq x$ gilt, so ist $x = y$.
(3) Für jede natürliche Zahl gibt es eine größere natürliche Zahl.
(4) Eine natürliche Zahl, für die es keine kleinere natürliche Zahl gibt, ist gleich 0.

Aufgabe 7.13. Formalisiere in der arithmetischen Sprache die folgenden wahren Aussagen.

(1) Es gibt unendlich viele Primzahlen.
(2) Jede natürliche Zahl ≥ 2 wird von einer Primzahl geteilt.

Wie sieht es mit der Aussage aus, dass jede natürliche Zahl eine Primfaktorzerlegung besitzt?

Aufgabe 7.14. Erstelle einen prädikatenlogischen Ausdruck α, der in einer Struktur genau dann gilt, wenn die Grundmenge der Struktur genau 7 Elemente besitzt.

Aufgabe 7.15. Das Symbolalphabet S bestehe neben Variablen aus dem einzigen einstelligen Funktionssymbol f. Finde für die folgenden Ausdrücke aus L^S jeweils Interpretationen, in denen der Ausdruck gilt, und Interpretationen, in denen er nicht gilt.

(1) $\forall x(x = fffx)$.
(2) $\exists x(x = fffx)$.
(3) $\forall x(fx = fffx)$.
(4) $\forall x(x = ffx) \wedge \forall x(\neg(x = fx))$.

Aufgabe 7.16. Formalisiere mit dem Symbolalphabet, das neben Variablen aus $\{f, g\}$ besteht, wobei f, g einstellige Funktionssymbole sind, die Aussage, dass die Hintereinanderschaltung von injektiven Abbildungen auf einer Menge wieder injektiv ist.

Aufgabe 7.17.*

Es sei ein Symbolalphabet S erster Stufe mit der Variablenmenge

$$V = \{x, y, z, w\}$$

gegeben und eine S-Interpretation I in der Menge $\mathbb{R}$ mit

$$I(x) = 5,\ I(y) = \pi,\ I(z) = -\sqrt{2},\ I(w) = -3\,.$$

Bestimme die Werte von $I\frac{e,-\sqrt{2},\frac{4}{7},I(x)}{x,z,x,y}$ auf V.

Aufgabe 7.18.*

Es sei $K = \{E, m, c\}$ eine Konstantenmenge, Q ein einstelliges Funktionssymbol und P ein zweistelliges Funktionssymbol. Es sei I die Interpretation mit $M = \mathbb{N}$ als Grundmenge, bei der Q als Quadrieren, P als Multiplikation und die Konstanten als $I(E) = 9000000000$ $I(m) = 1$ und $I(c) = 300000$ interpretiert wird. Ist der Ausdruck

$$E = PmQc$$

unter dieser Interpretation gültig?

Aufgabe 7.19. Es sei das arithmetische Alphabet $\{0, 1, +, \cdot\}$ zusammen mit der Variablenmenge $\{x, y\}$ gegeben. Interpretiere den Term

$$((0 + 1) + x) \cdot (1 + (y + 1))$$

unter den folgenden Interpretationen.

(1) $M = \mathbb{N}$ mit der Standardinterpretation und der Variablenbelegung $I(x) = 5$ und $I(y) = 3$.
(2) $M = \mathrm{Mat}_2(\mathbb{R})$ mit der Standardinterpretation

$$I(0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \; I(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und der üblichen Matrizenaddition und Matrizenmultiplikation und der Variablenbelegung $I(x) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ und $I(y) = \begin{pmatrix} 3 & -2 \\ 0 & 5 \end{pmatrix}$.
(3) $M = \mathbb{N}$, mit

$$I(0) = 1,\; I(1) = 4,\; I(x) = 2,\; I(y) = 1\,,$$

und wo $+$ als Multiplikation und $\cdot$ als Addition interpretiert wird.
(4) $M = \mathbb{Z}$, mit

$$I(0) = 5,\; I(1) = -1,\; I(x) = 0,\; I(y) = 0\,,$$

und wo sowohl $+$ als auch $\cdot$ als Subtraktion interpretiert werden.
(5) $M =$ Potenzmenge von $\{1, 2, 3, 4, 5\}$ mit

$$I(0) = \emptyset,\; I(1) = \{1, 2, 3, 4, 5\},\; I(x) = \emptyset,\; I(y) = \{2, 4\}\,,$$

und wo $+$ als $\cup$ und $\cdot$ als $\cap$ interpretiert wird.

Aufgabe 7.20. Es sei N ein einstelliges Funktionssymbol, F ein zweistelliges Funktionssymbol, 0 sei eine Konstante und x, y seien Variablen. Interpretiere den Term

$$NFN0NFxy$$

unter den folgenden Interpretationen, wobei M die Grundmenge der Interpretation bezeichne.

(1) $M = \mathbb{N}$, N ist die Nachfolgerfunktion, F die Addition, $I(0) = 0$, $I(x) = 3$ und $I(y) = 4$.
(2) $M = \mathbb{Q}$, N ist das Quadrieren, F die Mutiplikation, $I(0) = -2$, $I(x) = 3$ und $I(y) = \frac{3}{4}$.
(3) $M = C^\infty(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} | \, f \text{ unendlich oft differenzierbar}\}$, N ist das Differenzieren von Funktionenn, F die Multiplikation von Funktionen, $I(0)$ ist die Identität, $I(x)$ ist die Sinusfunktion und $I(y)$ ist die Exponentialfunktion zur Basis e.

Aufgabe 7.21. Es sei das arithmetische Alphabet $\{0, 1, +, \cdot\}$ zusammen mit der Variablenmenge $\{x, y\}$ gegeben. Interpretiere den Ausdruck

$$\forall x \exists y (x = y + y \vee x + 1 = y + y)$$

unter den in Aufgabe 7.19 angeführten Interpretationen und überprüfe die Gültigkeit.

Aufgabe 7.22.*

Es sei L^S die prädikatenlogische Sprache, die neben Variablen aus einem zweistelligen Relationssymbol A und einem dreistelligen Relationssymbol B bestehe. Wir betrachten S-Interpretationen I, wobei die Grundmenge jeweils aus einem Vektorraum V über einem Körper K bestehe und A als die lineare Unabhängigkeit von zwei und B als die lineare Unabhängigkeit von drei Vektoren interpretiert werde.

(1) Zeige
$$I \vDash Bxyz \to Axy\,.$$
(2) Gilt
$$I \vDash Axy \wedge Axz \wedge Ayz \to Bxyz$$
für einen beliebigen Vektorraum?
(3) Gibt es Vektorräume, für die die Aussage in Teil 2 gilt?
(4) Es sei $V = \mathbb{R}^3$ und e_1, e_2, e_3 sei die Standardbasis. Gilt
$$I\frac{e_1, e_2, e_3}{x, y, z} \vDash Bxyz\,?$$
(5) Es sei $V = \mathbb{R}$ als $\mathbb{Q}$-Vektorraum betrachtet. Gilt
$$I\frac{1, \sqrt{2}}{x, y} \vDash Axy\,?$$

Aufgabe 7.23. Es sei

$$\varphi\colon \mathbb{N} \longrightarrow \mathbb{Z}$$

die durch

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

gegebene bijektive Abbildung mit der Umkehrabbildung φ^{-1}. Auf $\mathbb{Z}$ seien die zweistelligen Funktionen $\circ$ und $\heartsuit$ durch

$$m \circ n \;:=\; \varphi(\varphi^{-1}(m) + \varphi^{-1}(n))$$

und

$$m \heartsuit n \;:=\; \varphi(\varphi^{-1}(m) \cdot \varphi^{-1}(n))$$

gegeben, wobei $+$ und $\cdot$ die üblichen Verknüpfungen auf $\mathbb{N}$ seien. Die Menge $\mathbb{Z}$ zusammen mit diesen Verknüpfungen nennen wir M.

a) Berechne in M

$$(5 \heartsuit (-2)) \circ ((-6) \heartsuit 3)\,.$$

b) Es sei S das Symbolalphabet, das aus den Variablen x, y, einer Konstanten c und zwei zweistelligen Funktionssymbolen α, β bestehe. Es sei I die Interpretation von L^S in M, die α als $\circ$, β als $\heartsuit$, c als 1 und die Variablen als 2 interpretiere. Berechne $I(t)$ für den Term

$$t \;=\; \beta\alpha cc\beta xc.$$

c) Gilt bei der Interpretation I der Ausdruck

$$\forall x\,(\exists y\,(c \circ y = x))\,?$$

7.2. **Aufgaben zum Abgeben.**

Aufgabe 7.24. (2 Punkte)

Es sei S das erststufige Symbolalphabet, das aus den Variablen x, y, z, den Konstanten $0, 1, 2$, den einstelligen Funktionssymbolen F, G, den zweistelligen Funktionssymbolen α, β, den einstelligen Relationssymbolen P, Q und dem zweistelligen Relationssymbol R bestehe. Überprüfe, ob die folgenden Wörter zur Sprache L^S (bei korrekter Klammerung) gehören.

(1) $Fx = P2$,
(2) $Fx = G1$,
(3) $\forall x\,(0 = 1)$,
(4) $(\beta 12 = 22) \to (Q0)$,
(5) $(Fx = 1) \to (\neg\,(G2 = 0))$,
(6) $\exists 0\,(P0)$,
(7) $(\exists x\,(R0x)) \wedge (\neg\,(\alpha\beta 012 = Rcz))$,
(8) $(R\alpha 0xGy) \wedge (\neg Q1)$.

Es genügt, die korrekten Ausdrücke aufzuschreiben; Punkte gibt es nur bei einer komplett richtigen Lösung.

Aufgabe 7.25. (2 Punkte)

Es sei S ein Symbolalphabet einer Sprache erster Stufe, T die Menge der S-Terme und I eine S-Interpretation. Zeige, dass auf T durch

$$s \sim t, \text{ falls } I(s) = I(t)\,,$$

eine Äquivalenzrelation definiert wird.

Aufgabe 7.26. (2 Punkte)

Schreibe die folgenden Aussagen mit Quantoren:

(1) Für jede natürliche Zahl gibt es eine größere natürliche Zahl.
(2) Für jede natürliche Zahl gibt es eine kleinere natürliche Zahl.
(3) Es gibt eine natürliche Zahl, die größer oder gleich jeder anderen natürlichen Zahl ist.
(4) Es gibt eine natürliche Zahl, die kleiner oder gleich jeder anderen natürlichen Zahl ist.

Welche sind wahr, welche falsch?

Aufgabe 7.27. (1 Punkt)

Formalisiere mit dem Symbolalphabet, das neben Variablen aus $\{f, g\}$ besteht, wobei f, g einstellige Funktionssymbole sind, dass die Hintereinanderschaltung von surjektiven Abbildungen auf einer Menge wieder surjektiv ist.

Aufgabe 7.28. (3 Punkte)

Formalisiere in der arithmetischen Sprache die folgenden zahlentheoretischen Vermutungen.

(1) Die Goldbach-Vermutung.
(2) Die Vermutung über die Unendlichkeit der Primzahlzwillinge.
(3) Die Vermutung über die Unendlichkeit der Mersenne-Primzahlen.

Man beachte bei (3), dass das Potenzieren mit einem unbekannten Exponenten nicht zur arithmetischen Sprache gehört.

Aufgabe 7.29. (4 Punkte)

Es sei das arithmetische Alphabet $\{0, 1, +, \cdot\}$ zusammen mit der Variablenmenge $\{x, y\}$ gegeben. Interpretiere den Term

$$((0 + x) + 1) \cdot (1 + ((y \cdot x) + 1))$$

unter den folgenden Interpretationen.

(1) $M = \mathbb{N}$ mit der Standardinterpretation und der Variablenbelegung $I(x) = 7$ und $I(y) = 2$.
(2) $M = \mathrm{Mat}_2(\mathbb{R})$ mit der Standardinterpretation

$$I(0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \; I(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und der üblichen Matrizenaddition und Matrizenmultiplikation und der Variablenbelegung $I(x) = \begin{pmatrix} -1 & 3 \\ 4 & 5 \end{pmatrix}$ und $I(y) = \begin{pmatrix} 2 & -3 \\ 2 & 0 \end{pmatrix}$.
(3) $M = \mathbb{Z}$, mit

$$I(0) = 6, \; I(1) = -4, \; I(x) = 0, \; I(y) = 5\,,$$

und wo sowohl + als auch $\cdot$ als Subtraktion interpretiert werden.
(4) $M =$ Potenzmenge von $\{1, 2, 3, 4, 5, 6\}$ mit

$$I(0) = \{5, 6\}, \; I(1) = \{1, 2, 3, 4, 5, 6\}, \; I(x) = \emptyset, \; I(y) = \{1, 3, 5\}\,,$$

und wo + als $\cup$ und $\cdot$ als $\cap$ interpretiert wird.

8. Vorlesung - Folgerungen

8.1. **Allgemeingültige Ausdrücke.**

Es sei L^S eine Sprache erster Stufe über einem Symbolalphabet S. Für einen Ausdruck $\alpha \in L^S$ und eine Interpretation I haben wir in der letzten Vorlesung die Gültigkeit $I \vDash \alpha$ über den Aufbau der Sprache rekursiv definiert. Wie im aussagenlogischen Kontext führen wir semantische Tautologien über die Gültigkeit bei jeder Interpretation ein.

Definition 8.1. Es sei S ein Symbolalphabet und α ein S-Ausdruck in der Prädikatenlogik erster Stufe. Man nennt α *allgemeingültig* (oder eine *semantische Tautologie*), wenn er in jeder S-Interpretation I gilt, also $I \vDash \alpha$ wahr ist.

Allgemeingültige Ausdrücke sind *Tautologien* im semantischen Sinn. Wir werden später noch Tautologien im syntaktischen Sinn kennenlernen und die Übereinstimmung der beiden Konzepte zeigen (Vollständigkeitssatz der Prädikatenlogik). Beispiele sind die Ausdrücke

$$\forall x \forall y \forall z((x = y \wedge y = z) \to x = z)$$

oder

$$(\forall x \alpha) \to \alpha$$

(wobei α ein Ausdruck ist), siehe Aufgabe 8.1. Wenn man in eine aussagenlogische Tautologie für die Aussagenvariablen beliebige prädikatenlogische Ausdrücke einsetzt,[12] so erhält man auch eine Tautologie im obigen Sinn,

[12]Insofern ist auch die Bezeichnung Aussagenvariable gerechtfertigt, da für sie prädikatenlogische Ausdrücke eingesetzt werden können.

siehe Aufgabe 8.4 (die entprechende syntaktische Version wird in Lemma 10.2 behandelt). Beispielsweise erhält man aus der aussagenlogischen Tautologie

$$\alpha \to (\beta \to \alpha)$$

die prädikatenlogische Tautologie (mit naheliegenden Zugehörigkeiten der Symbole)

$$\forall x(fx = y) \to (\exists u(Rgzu) \to \forall x(fx = y)) \ ,$$

die aber keinen eigentlichen prädikatenlogischen Sachverhalt ausdrückt.

8.2. **Gültigkeit von Ausdrucksmengen.**

Für eine Menge $\Gamma \subseteq L^S$ von Ausdrücken und einer S-Interpretation I schreibt man $I \vDash \Gamma$, wenn in I jeder Ausdruck aus Γ gilt. Man sagt, dass I ein *Modell* für Γ ist. Eine S-Struktur heißt ein *Modell* für Γ, wenn jede Variablenbelegung zu dieser Struktur eine Interpretation liefert, die ein Modell für Γ ist.

Diese Sprechweise wird insbesondere für Axiomensysteme Γ verwendet, die eine mathematisch wichtige Struktur festlegen. Die erfüllenden Modelle heißen dann so, wie der Definitionsname in der Definition lautet, die dieses Axiomensystem verwendet. Die Modelle nennt man im üblichen mathematischen Sprachgebrauch Beispiele für diejenige mathematische Struktur, die durch die Definition festgelegt wird.

8.3. **Axiomensysteme.**

Grundsätzlich gibt es zwei Bedeutungen von Axiomensystemen. Einerseits wird ein Axiomensystem aufgestellt, um eine in einem gewissen Sinn vertraute Struktur präzise zu erfassen und ihre Eigenschaften aus den fixierten Grundeigenschaften zu folgern. Man spricht von einem *intendierten Modell*, das durch das Aufstellen eines Axiomensystems mathematisch beschrieben werden soll. Die Axiome selbst werden dann durch die Gültigkeit im intendierten Modell gerechtfertigt und können nicht weiter hinterfragt werden. In diesem Sinne gibt es in der Geometrie die euklidische Axiome für die Ebene bzw. den Raum, oder die Dedekind-Peano-Axiome für die natürlichen Zahlen, die wir später behandeln werden, oder die Axiome für die reellen Zahlen, die man in der Analysis I einführt, oder die Axiome für die Mengenlehre (typischerweise Zermelo-Fraenkel mit Auswahlaxiom), die eine Festlegung für den mengentheoretischen Rahmen der gesamten Mathematik bilden. Eine wichtige Fragestellung hierbei ist, ob die Axiome die Struktur eindeutig festlegen.

Andererseits kann man jede willkürliche Vorgabe einer Menge von Ausdrücken als ein Axiomensystem ansehen. Es gibt dann jeweils mehrere verschiedene Strukturen, die diese Axiome erfüllen. Ein Axiomensystem in diesem Sinn will nicht ein bestimmtes Modell charakterisieren, sondern abstrakte Eigenschaft, die in unterschiedlichen Kontexten auftreten, bereitstellen.

Eigenschaften, die man aus den Axiomen erschließen kann, gelten dann für sämtliche Modelle, die die Axiome erfüllen. Die Ökonomie dieses mathematischen Ansatzes liegt eben darin, dass man Schlüsse nicht am Objekt durchführt, sondern abstrakt und allgemein. Wichtige Axiomensysteme in diesem zweiten Sinn sind die Axiome für Gruppen, Ringe, Körper, angeordnete Körper, Vektorräume, metrische Räume, topologische Räume, Maßräume, Mannigfaltigkeiten.

Wichtige Bewertungskriterien für beide Arten von Axiomensystemen sind.

(1) Die Axiome sollen möglichst einfach formuliert sein.
(2) Die Axiome sollen möglichst einfach (in einem Modell) überprüfbar sein.
(3) Die Axiome sollen reichhaltige Folgerungen erlauben.
(4) Die Axiome eines Systems sollen untereinander unabhängig sein; es darf kein Axiom redundant sein.

Für uns stehen zunächst Axiomensysteme im zweiten Sinne im Mittelpunkt; grundsätzlich kann man jede Ausdrucksmenge $\Gamma \subseteq L^S$ als ein Axiomensystem auffassen. Als Beispiele betrachten wir aber nur mathematisch relevante Axiomensysteme. Um ein Axiomensystem prädikatenlogisch zu repräsentieren, muss man zuerst das Symbolalphabet und anschließend die Axiome festlegen. Betrachten wir beispielsweise die mathematische Definition einer Gruppe.

Definition 8.2. Eine Menge G mit einem ausgezeichneten Element $e \in G$ und mit einer Verknüpfung

$$G \times G \longrightarrow G,\ (g,h) \longmapsto g * h,$$

heißt *Gruppe*, wenn folgende Eigenschaften erfüllt sind.

(1) Die Verknüpfung ist *assoziativ*, d.h. für alle $f, g, h \in G$ gilt
$$(f * g) * h \ = \ f * (g * h).$$
(2) Das Element e ist ein *neutrales Element*, d.h. für alle $g \in G$ gilt
$$g * e \ = \ g \ = \ e * g.$$
(3) Zu jedem $g \in G$ gibt es ein *inverses Element*, d.h. es gibt ein $h \in G$ mit
$$h * g \ = \ g * h \ = \ e.$$

In formal-prädikatenlogischer Formulierung besteht das Symbolalphabet (neben den Variablen) aus einer Konstanten e und aus einem zweistelligen Funktionssymbol μ. Die in der Gruppendefinition auftretenden Axiome (die Gruppenaxiome, also die drei auftretenden Bedingungen) kann man mit diesen Symbolen einfach schreiben als

(1)
$$\forall x(\forall y(\forall z\, \mu x \mu y z = \mu \mu x y z))\,.$$

(2)
$$\forall x(\mu xe = x \wedge \mu ex = x)\,.$$
(3)
$$\forall x \exists y(\mu xy = e \wedge \mu yx = e)\,.$$

Nennen wir diese drei Ausdrücke zusammen Γ. Dann ist eine Gruppe eine Menge G mit einer Interpretation I für e und für μ, d.h. es muss ein ausgezeichnetes Element e^G (häufig schreibt man e_G oder e) geben und eine zweistellige Funktion auf G (eine Verknüpfung), derart, dass $I \vDash \Gamma$ gilt. Eine Gruppe ist also ein Modell für Γ.

Als weiteres Beispiel wiederholen wir die Definition der Ordnungsrelation, die wir in der fünften Vorlesung behandelt haben.

Eine Relation $\preccurlyeq$ auf einer Menge I heißt *Ordnungsrelation* oder *Ordnung*, wenn folgende drei Bedingungen erfüllt sind.

(1) Es ist $i \preccurlyeq i$ für alle $i \in I$.
(2) Aus $i \preccurlyeq j$ und $j \preccurlyeq k$ folgt stets $i \preccurlyeq k$.
(3) Aus $i \preccurlyeq j$ und $j \preccurlyeq i$ folgt $i = j$.

Neben den Variablen besteht das zugehörige Symbolalphabet allein aus einem zweistelligen Relationssymbol, das wir ebenfalls mit $\preccurlyeq$ bezeichnen. Die für eine Ordnung verlangten Eigenschaften führen zu dem folgenden Axiomensystem Γ.

(1)
$$\forall x(x \preccurlyeq x)\,.$$
(2)
$$\forall x \forall y \forall z(x \preccurlyeq y \wedge y \preccurlyeq z \to x \preccurlyeq z)\,.$$
(3)
$$\forall x \forall y(x \preccurlyeq y \wedge y \preccurlyeq x \to x = y)\,.$$

In einer Menge M mit einer zweistelligen Relation R gilt das Axiomensystem Γ genau dann, wenn die Relation eine Ordnungsrelation ist. Eine geordnete Menge ist also ein Modell für Γ.

8.4. **Die Folgerungsbeziehung.**

Mit Axiomensystemen verbindet man die Vorstellung, dass daraus „wichtige“ weitere Eigenschaften beweisbar sind. In einer jeden Gruppe gelten nicht nur die Gruppenaxiome, sondern auch alle Gesetzmäßigkeiten, die man aus den Gruppenaxiomen folgern kann. Dies wird in der mathematischen Logik durch den Folgerungsbegriff präzisiert.

Definition 8.3. Es sei S ein Symbolalphabet erster Stufe, Γ eine Menge von S-Ausdrücken und α ein S-Ausdruck. Man sagt, dass α aus Γ *folgt*, geschrieben $\Gamma \vDash \alpha$, wenn für jede S-Interpretation I mit $I \vDash \Gamma$ auch $I \vDash \alpha$ gilt.

Die Folgerungsbeziehung verwendet also (wie schon im aussagenlogischen Kontext) das gleiche Symbol wie die Gültigkeitsbeziehung. Dass aus einer gewissen Ausdrucksmenge Γ ein gewisser Audruck α folgt, erfordert eine mathematische Argumentation, die aufzeigt, dass eine Menge mit gewissen zusätzlichen Strukturen, die Γ erfüllt, stets auch α erfüllen muss.

Beispiel 8.4. In einer Gruppe ist das inverse Element zu einem jeden Element, das es aufgrund der Definition einer Gruppe geben muss, eindeutig bestimmt. Mathematisch wird dies so bewiesen: Sei e das neutrale Element der Gruppe, sei $x \in G$ vorgegeben und seien $y, z \in G$ inverse Elemente zu x, d.h. es gelte $yx = xy = e$ und $zx = xz = e$. Dann ist insgesamt

$$y = ye = y(xz) = (yx)z = ez = z.$$

Die Eindeutigkeit des inversen Elementes kann man mit den Symbolen $\{e, \mu\}$, wobei e eine Konstante und μ ein zweistelliges Funktionssymbol ist, als den Ausdruck

$$\alpha := \forall x(\forall y(\forall z(\mu yx = e \wedge \mu xy = e \wedge \mu zx = e \wedge \mu xz = e \rightarrow y = z)))$$

ansetzen, und die obige mathematische Argumentation bedeutet, dass der Ausdruck α aus den Gruppenaxiomen Γ folgt, also die Folgerungsbeziehung

$$\Gamma \vDash \alpha$$

vorliegt.

Da ein allgemeingültiger Ausdruck α in jeder Interpretation gilt, kann man auch sagen, dass α aus der leeren Ausdrucksmenge folgt, also $\emptyset \vDash \alpha$ gilt. Wenn $\alpha_1, \alpha_2, \alpha_3$ die Gruppenaxiome sind, und α die im obigen Beispiel erwähnte Eindeutigkeitsausssage für das inverse Element ist, so ist

$$\alpha_1 \wedge \alpha_2 \wedge \alpha_3 \rightarrow \alpha$$

allgemeingültig.

Definition 8.5. Es sei S ein Symbolalphabet und es sei α ein S-Ausdruck in der Prädikatenlogik erster Stufe. Man nennt α *erfüllbar*, wenn es eine S-Interpretation I mit $I \vDash \alpha$ gibt.

Für eine Ausdrucksmenge Γ bedeutet die Erfüllbarkeit, dass die darin enthaltenen Ausdrücke simultan in einer Interpretation erfüllbar sind. Zwischen Allgemeingültigkeit und Erfüllbarkeit besteht die Beziehung, dass α genau dann allgemeingültig ist, wenn die Negation $\neg\alpha$ nicht erfüllbar ist.

Zwischen Folgerung und Erfüllbarkeit besteht der folgende Zusammenhang.

Lemma 8.6. *Es gilt $\Gamma \vDash \alpha$ genau dann, wenn $\Gamma \cup \{\neg\alpha\}$ nicht erfüllbar ist.*

Beweis. Siehe Aufgabe 8.15. □

8.5. **Sortenprädikate.**

Bei vielen mathematischen Strukturen bewegen sich die Objekte, über die quantifiziert werden soll, nicht in einer einzigen Menge, sondern in mehreren. Beispielsweise interessiert man sich nicht nur für Abbildungen von einer Menge in sich selbst, sondern auch für Abbildungen zwischen zwei Mengen. Bei einem Vektorraum wird ein Körper zugrunde gelegt, aus dem die „Skalare“ herrühren, während die Vektoren aus dem Vektorraum sind; die Axiome eines Vektorraums nehmen Bezug auf beide Arten. Bei einem metrischen Raum ist der Abstand zwischen zwei Punkten des Raumes eine reelle Zahl bzw. ein Element in einem angeordneten Körper. Man spricht von verschiedenen „Sorten“ (von Termen, von Objekten). Solche mathematische Strukturen lassen sich ebenfalls mit der Sprache erster Stufe beschreiben, wobei man einen einfachen Kniff anwendet, der von der mathematischen Praxis her etwas künstlich wirkt. Man wirft die Mengen zunächst zusammen und führt dann für jede Sorte ein *Sortenprädikat* ein, um sie wieder trennen zu können. Ein Sortenprädikat ist eine einstellige Relation, und Pt bedeutet inhaltlich gesprochen, dass der Term t zur Sorte gehört, die durch P repräsentiert wird. Wir erläutern dieses Vorgehen an zwei Beispielen.

Beispiel 8.7. Eine angemessene prädikatenlogische Formulierung für Abbildungen zwischen zwei Mengen wird durch das Symbolalphabet beschrieben, das neben Variablen aus $\{F, D, Z\}$ besteht, wobei F ein einstelliges Funktionssymbol und D (für „Definitionsbereich“) und Z (für „Zielbereich“) zwei einstellige Relationssymbole sind, mit denen man den Definitionsbereich und den Zielbereich einer Abbildung erfassen möchte. Bei Interpretation in einer Menge M ist die Funktion $f = F^M$ zwar auf jedes Element aus M anwendbar, man kann aber relevante Eigenschaften einer Abbildung spezifisch für die durch D bzw. Z bestimmten Teilmengen (den Definitionsbereich bzw. Zielbereich) formulieren. Beispielsweise besagt der Ausdruck

$$\forall x(Dx \to Zfx)\,,$$

dass für jedes x, das zum Definitionsbereich gehört, der Funktionswert zu Z gehören muss. Die Surjektivität (als Abbildung von der durch D beschriebenen Menge, also D^M, in die durch Z beschriebene Menge, also Z^M) wird durch

$$\forall y\,(Zy \to \exists x\,(Dx \wedge fx = y))$$

beschrieben.

Beispiel 8.8. Eine angemessene prädikatenlogische Formulierung für Vektorräume wird neben Variablen durch

$$\{0_K, 1, +_K, \cdot_K, 0_V, +_V, \cdot, K, V\}$$

beschrieben, wobei $\{0_K, 1, 0_V\}$ Konstanten, $\{+_K, \cdot_K, +_V, \cdot\}$ zweistellige Funktionssymbole und K (für Körper) und V (für Vektorraum) zwei einstellige Relationssymbole sind, mit denen man den Körper und den Vektorraum

erfassen möchte. Die grundlegende Skalarmultiplikation wird durch

$$\forall x \forall y \left(Kx \wedge Vy \to Vx \cdot y \right)$$

beschrieben, die beiden Distributivgesetze durch

$$\forall x \forall y \forall z \left(Kx \wedge Ky \wedge Vz \to (x +_K y) \cdot z = ((x \cdot z) +_V (y \cdot z)) \right)$$

und

$$\forall x \forall y \forall z \left(Kx \wedge Vy \wedge Vz \to x \cdot (y +_V z) = (x \cdot y) +_V (x \cdot z) \right) .$$

8. Arbeitsblatt

8.1. Übungsaufgaben.

Aufgabe 8.1. Zeige, dass die folgenden prädikatenlogischen Ausdrücke allgemeingültig sind.

(1)
$$\forall x \forall y \forall z ((x = y \wedge y = z) \to x = z) .$$

(2)
$$(\forall x \alpha) \to \alpha$$
(wobei α ein Ausdruck ist).

(3)
$$\alpha_1 \wedge \alpha_2 \wedge \alpha_3 \to \beta ,$$
wobei $\alpha_1, \alpha_2, \alpha_3$ die Gruppenaxiome sind und
$$\beta := \forall z (\forall x (zx = x \wedge xz = x) \to z = e)$$
ist.

Aufgabe 8.2. Es sei S ein erststufiges Symbolalphabet und $f \in S$ ein n-stelliges Funktionssymbol. Zeige, dass der Ausdruck

$$\exists y \left((fx_1 \ldots x_n = y) \wedge \forall z \left((fx_1 \ldots x_n = z) \to y = z \right) \right)$$

allgemeingültig ist.

Aufgabe 8.3. Es sei S ein erststufiges Symbolalphabet und $f \in S$ ein 2-stelliges Funktionssymbol. Zeige, dass der Ausdruck

$$(\forall x \forall y \forall z (ffxyz = fxfyz)) \to (\forall x \forall y \forall z \forall w (fffxyzw = fxfyfzw))$$

allgemeingültig ist.

Aufgabe 8.4. Es seien $p_1, \ldots, p_n$ Aussagenvariablen und $\beta_1, \ldots, \beta_n$ prädikatenlogische Ausdrücke. Zeige, dass man, wenn man in einer allgemeingültigen aussagenlogischen Aussage α, in dem keine weiteren Aussagenvariablen vorkommen, jedes Vorkommen von p_i durch β_i ersetzt, einen allgemeingültigen prädikatenlogischen Ausdruck erhält.

Aufgabe 8.5. Formuliere ein Axiomensystem für das Konzept Äquivalenzrelation in einer prädikatenlogischen Sprache erster Stufe.

Aufgabe 8.6. Axiomatisiere den Körperbegriff in einer geeigneten Sprache erster Stufe.

Eine Menge K heißt ein *Körper*, wenn es zwei Verknüpfungen (genannt Addition und Multiplikation)

$$+ : K \times K \longrightarrow K \text{ und } \cdot : K \times K \longrightarrow K$$

und zwei verschiedene Elemente $0, 1 \in K$ gibt, die die folgenden Eigenschaften erfüllen.

(1) Axiome der Addition
   (a) Assoziativgesetz: Für alle $a, b, c \in K$ gilt: $(a+b)+c = a+(b+c)$.
   (b) Kommutativgesetz: Für alle $a, b \in K$ gilt $a + b = b + a$.
   (c) 0 ist das neutrale Element der Addition, d.h. für alle $a \in K$ ist $a + 0 = a$.
   (d) Existenz des Negativen: Zu jedem $a \in K$ gibt es ein Element $b \in K$ mit $a + b = 0$.

(2) Axiome der Multiplikation
   (a) Assoziativgesetz: Für alle $a, b, c \in K$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
   (b) Kommutativgesetz: Für alle $a, b \in K$ gilt $a \cdot b = b \cdot a$.
   (c) 1 ist das neutrale Element der Multiplikation, d.h. für alle $a \in K$ ist $a \cdot 1 = a$.
   (d) Existenz des Inversen: Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein Element $c \in K$ mit $a \cdot c = 1$.

(3) Distributivgesetz: Für alle $a, b, c \in K$ gilt $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Aufgabe 8.7. Axiomatisiere den Begriff eines angeordneten Körpers in einer geeigneten Sprache erster Stufe.

Ein Körper K heißt *angeordnet*, wenn es eine totale Ordnung „$\geq$“ auf K gibt, die die beiden Eigenschaften

(1) Aus $a \geq b$ folgt $a + c \geq b + c$ (für beliebige $a, b, c \in K$),
(2) Aus $a \geq 0$ und $b \geq 0$ folgt $ab \geq 0$ (für beliebige $a, b \in K$),

erfüllt.

Aufgabe 8.8. Sei $S = \{0, 1, +, \cdot, \geq\}$ die Symbolmenge für einen angeordneten Körper. Zeige

$$\mathbb{R} \vDash \forall x \forall y \left(x \geq y \leftrightarrow \exists z \left(x - y = z^2 \right) \right)$$

und

$$\mathbb{Q} \vDash \neg \left(\forall x \forall y \left(x \geq y \leftrightarrow \exists z (x - y = z^2) \right) \right) .$$

Über den reellen Zahlen kann man also das Symbol $\geq$ mit anderen Symbolen ausdrücken.

Aufgabe 8.9. Sei $S = \{0, 1, +, \cdot, \geq\} \cup V$ die Symbolmenge für einen angeordneten Körper und f ein einstelliges Funktionssymbol. Formuliere über $S' = S \cup \{f\}$ folgende Eigenschaften.

(1) Die Stetigkeit von f.
(2) Die gleichmäßige Stetigkeit von f.
(3) Die Differenzierbarkeit von f.

Gesucht ist also ein Ausdruck α aus $L^{S'}$ mit der Eigenschaft, dass α in einer Interpretation von S' (gegeben durch einen angeordneten Körper K und eine Funktion $f\colon\ K \to K$) genau dann gilt, wenn f stetig ist.

Aufgabe 8.10. Zeige, dass die Polynomfunktionen in einer Variablen über einem angeordneten Körper stetig sind. Formuliere diese Aussage über dem Symbolalphabet $S = \{0, 1, +, \cdot, \geq\}$ für Polynome eines festes Grades.

Aufgabe 8.11. Sei $S = \{0, 1, +, \cdot, \geq\} \cup V$ die Symbolmenge für einen angeordneten Körper und f ein einstelliges Funktionssymbol. Formuliere über $S' = S \cup \{f\}$ die Aussage des Zwischenwertsatzes.

Aufgabe 8.12. Sei $S = \{0, 1, +, \cdot, \geq\} \cup V$ die Symbolmenge für einen angeordneten Körper. Formuliere über S die Aussage des Zwischenwertsatzes für Polynome vom Grad d.

In welchem Zusammenhang stehen die beiden vorstehenden Formulierungen?

Aufgabe 8.13. Es seien $\alpha_1, \alpha_2, \alpha_3$ die Gruppenaxiome und

$$\alpha := \forall x(\forall y(\forall z(\mu yx = e \wedge \mu xy = e \wedge \mu zx = e \wedge \mu xz = e \rightarrow y = z))),$$

also die Aussage, dass das inverse Element eindeutig bestimmt ist. Zeige, dass α aus keiner echten Teilmenge $\Gamma \subset \{\alpha_1, \alpha_2, \alpha_3\}$ folgt.

Aufgabe 8.14. Zeige, dass der prädikatenlogische Ausdruck

$$\exists x(\forall y(x = y))$$

erfüllbar ist.

Aufgabe 8.15. Es sei Γ eine Ausdrucksmenge und α ein Ausdruck in einer Sprache erster Stufe. Zeige, dass $\Gamma \vDash \alpha$ genau dann gilt, wenn $\Gamma \cup \{\neg\alpha\}$ nicht erfüllbar ist.

Aufgabe 8.16.*

Formuliere die Injektivität für eine Abbildung

$$f\colon\ D \longrightarrow Z$$

prädikatenlogisch mit Hilfe der Verwendung von Sorten.

Aufgabe 8.17. Formalisiere mit dem Symbolalphabet $S = \{f, g\} \cup V$, wobei f, g einstellige Funktionssymbole sind, die Aussage, dass die Hintereinanderschaltung von injektiven Abbildungen zwischen Mengen wieder injektiv ist.

Häufig sind in mathematische Strukturen gewisse Teilmengen wichtig, die Bezug auf die umgebende Struktur nehmen. Eine solche Teilmenge wird prädikatenlogisch durch eine einstellige Relation mit zusätzlichen Eigenschaften wiedergegeben.

Aufgabe 8.18.*

Formalisiere prädikatenlogisch mit einem geeigneten Symbolalphabet S, dass ein Untervektorraum in einem Vektorraum über einem Körper vorliegt.

Aufgabe 8.19. Formalisiere prädikatenlogisch mit einem geeigneten Symbolalphabet S den Sachverhalt, dass der Durchschnitt von zwei Untervektorräumen in einem Vektorraum über einem Körper wieder ein Untervektorraum ist.

Aufgabe 8.20. Formalisiere prädikatenlogisch mit einem geeigneten Symbolalphabet S, dass ein Ideal in einem kommutativen Ring vorliegt.

8.2. **Aufgaben zum Abgeben.**

Aufgabe 8.21. (2 Punkte)

Formalisiere in der prädikatenlogischen Sprache, dass die Hintereinanderschaltung von surjektiven Abbildungen zwischen Mengen wieder surjektiv ist.

Aufgabe 8.22. (2 Punkte)

Welche der folgenden prädikatenlogischen Ausdrücke sind allgemeingültig (x, y seien Variablen)?

(1) $\forall x(\exists y(x = y))$,
(2) $\forall x(\forall y(x = y))$,
(3) $\exists x(\forall y(x = y))$,
(4) $\exists x(\exists y(x = y))$.

Aufgabe 8.23. (5 (2+2+1) Punkte)

Es seien $\alpha, \beta \in L^S$.

a) Zeige, dass

$$(\exists x\,(\alpha \to \beta)) \to (\exists x\alpha \to \exists x\beta)$$

nicht allgemeingültig ist.

b) Zeige, dass

$$(\exists x\alpha \to \exists x\beta) \to (\exists x\,(\alpha \to \beta))$$

allgemeingültig ist.

c) Zeige, dass

$$(\exists x\alpha \to \exists x\beta) \to (\exists x\,(\alpha \to \beta))$$

nicht allgemeingültig wäre, wenn man auch leere Grundmengen zulassen würde.

Aufgabe 8.24. (3 Punkte)

Es sei f ein einstelliges Funktionssymbol. Bestimme, welche der folgenden Ausdrücke untereinander äquivalent[13] sind.

(1) $\forall x\exists y(fx = y)$,
(2) $\forall x\exists x(fx = x)$,
(3) $\exists x(fx = x)$.

[13]Zwei Ausdrücke α und β heißen äquivalent, wenn $\alpha \leftrightarrow \beta$ allgemeingültig ist.

Aufgabe 8.25. (5 Punkte)

Es seien u, x, y, z Variablen und f, g einstellige Funktionssymbole. Bestimme, welche der folgenden Ausdrücke untereinander äquivalent sind.

a)

(1) $\forall x \forall y((fx = fy \to x = y) \wedge (gx = gy \to x = y))$,
(2) $\forall x \forall y(fx = fy \to x = y) \wedge \forall x \forall y(gx = gy \to x = y)$,
(3) $\forall x \forall y \forall u \forall z((fx = fy \to x = y) \wedge (gu = gz \to u = z))$.

b)

(1) $\forall x \exists y(fy = x) \wedge \forall x \exists y(gy = x)$,
(2) $\forall x \exists y\,(fy = x \wedge gy = x)$,
(3) $\forall x \exists y \forall u \exists z(fy = x \wedge gz = u)$,
(4) $\forall x \forall u \exists y \exists z(fy = x \wedge gz = u)$.

Aufgabe 8.26. (2 Punkte)

Zeige, dass die Kommutativität der Addition aus den übrigen Körperaxiomen folgt.

Tipp: Zeige zuerst, dass $0x = 0$ ist.

Aufgabe 8.27. (2 Punkte)

Sei $S = \{0, 1, +, \cdot, \geq\} \cup V$ die Symbolmenge für einen angeordneten Körper und f, g zwei einstellige Funktionssymbole. Formuliere über $S' = S \cup \{f, g\}$ die Aussage, dass die Hintereinanderschaltung von zwei stetigen Funktionen wieder stetig ist.

Aufgabe 8.28. (3 Punkte)

Formuliere ein prädikatenlogisches Axiomensystem für einen metrischen Raum über einem angeordneten Körper mit Hilfe von Sortenprädikaten.

Aufgabe 8.29. (3 Punkte)

Sei $k \in \mathbb{N}$ fixiert. Formalisiere prädikatenlogisch mit einem geeigneten Symbolalphabet S den Sachverhalt, dass k Elemente eines kommutativen Ringes ein gegebenes Ideal erzeugen.

9. Vorlesung - Substitution

9.1. **Freie Variablen.**

In einem Ausdruck $\alpha \in L^S$ über einem Symbolalphabet S nennt man die Variablen, die (und zwar für jedes Vorkommen) innerhalb der Reichweite eines Quantors stehen, *gebunden*, die anderen *frei*. Dies wird streng über den Aufbau der Ausdrücke definiert.

(1)
$$\text{Frei}\,(t_1 = t_2) = \text{Var}\,(t_1) \cup \text{Var}\,(t_2)$$

(2)
$$\text{Frei}\,(Rt_1 \dots t_n) = \text{Var}\,(t_1) \cup \text{Var}\,(t_2) \cup \dots \cup \text{Var}\,(t_n)$$

für ein n-stelliges Relationssymbol R und n Terme $t_1, t_2, \dots, t_n$.

(3)
$$\text{Frei}\,(\neg\alpha) = \text{Frei}\,(\alpha)$$

für einen Ausdruck α.

(4)
$$\text{Frei}\,(\alpha \to \beta) = \text{Frei}\,(\alpha) \cup \text{Frei}\,(\beta)$$

für Ausdrücke α und β. Ebenso für $\leftrightarrow, \wedge, \vee$.

(5)
$$\text{Frei}\,(\forall x\alpha) = \text{Frei}\,(\alpha) \setminus \{x\}$$

für einen Ausdruck α und eine Variable x.

(6)
$$\text{Frei}\,(\exists x\alpha) = \text{Frei}\,(\alpha) \setminus \{x\}$$

für einen Ausdruck α und eine Variable x.

Einen Ausdruck ohne freie Variablen nennt man einen *Satz*, auch wenn diese Bezeichnung nicht ganz glücklich ist, da „Satz“ die Gültigkeit einer Aussage suggeriert. Die Menge der Sätze wird mit L_0^S bezeichnet, die Menge der Ausdrücke mit genau einer freien Variablen (die aber in dem Ausdruck beliebig oft vorkommen darf) mit L_1^S.

Beispielsweise ist in
$$\forall x(\exists y(fx = z)) \vee \exists x(Ryzx)$$
die Variable x gebunden, während die Variablen y, z frei sind, wobei die Freiheit von y auf dem freien Vorkommen im hinteren Ausdruck beruht.

9.2. **Das Koinzidenzlemma.**

Die folgende Aussage, das Koinzidenzlemma, zeigt, dass der Wert eines Terms und die Gültigkeit eines Ausdrucks unter einer Interpretation (bei einer fixierten S-Struktur) nur von den in dem Term vorkommenden Variablen bzw. in dem Ausdruck vorkommenden freien Variablen abhängt. Ihr Beweis ist ein typisches Beispiel für einen Beweis durch Induktion über den Aufbau der Terme bzw. Ausdrücke.

Lemma 9.1. *Es sei S ein Symbolalphabet erster Stufe und $U \subseteq S$ eine Teilmenge. Es sei t ein U-Term und α ein U-Ausdruck. Es seien zwei S-Interpretationen I_1 und I_2 in einer gemeinsamen Grundmenge M gegeben, die auf U identisch seien. Dann gelten folgende Aussagen.*

(1) *Es ist $I_1(t) = I_2(t)$.*
(2) *Es ist $I_1 \vDash \alpha$ genau dann, wenn $I_2 \vDash \alpha$ (dazu genügt bereits, dass die Interpretationen auf den Symbolen aus U und auf den in α frei vorkommenden Variablen identisch sind).*

Beweis. (1). Wir führen Induktion über den Aufbau der U-Terme. Für den Induktionsanfang müssen wir Variablen und Konstanten aus U betrachten. Für eine Variable x (oder eine Konstante) aus U ist nach Voraussetzung $I_1(x) = I_2(x)$. Im Induktionsschritt können wir annehmen, dass ein n-stelliges Funktionssymbol f aus U gegeben ist sowie U-Terme $t_1, \ldots, t_n$, für die die Interpretationsgleichheit schon gezeigt wurde. Nach Voraussetzung wird f in beiden Interpretationen durch die gleiche Funktion f^M interpretiert. Daher ist

$$\begin{aligned} I_1(ft_1 \ldots t_n) &= f^M(I_1(t_1), \ldots, I_1(t_n)) \\ &= f^M(I_2(t_1), \ldots, I_2(t_n)) \\ &= I_2(ft_1 \ldots t_n). \end{aligned}$$

(2). Wir führen Induktion über den Aufbau der U-Ausdrücke, wobei die zu beweisende Aussage über je zwei Interpretationen zu verstehen ist. Für die Gleichheit und ein Relationssymbol R aus U folgt die Aussage unmittelbar aus (1), da ja R in beiden Interpretationen als die gleiche Relation zu interpretieren ist. Der Induktionsschritt ist für Ausdrücke der Form $\neg\alpha$, $\alpha \wedge \beta$, $\alpha \to \beta$ aufgrund der Modellbeziehung unmittelbar klar. Sei nun ein U-Ausdruck der Form $\exists x\alpha$ gegeben, und es gelte $I_1 \vDash \exists x\alpha$. Dies bedeutet aufgrund der Modellbeziehung, dass es ein $m \in M$ derart gibt, dass $I_1\frac{m}{x} \vDash \alpha$ gilt. Die beiden umbelegten Interpretationen $I_1\frac{m}{x}$ und $I_2\frac{m}{x}$ stimmen auf den Symbolen aus U und den in α frei vorkommenden Variablen überein: Die Variable x wird so oder so als m interpretiert und die anderen freien Variablen aus α sind auch in $\exists x\alpha$ frei. Nach Induktionsvoraussetzung gilt $I_2\frac{m}{x} \vDash \alpha$ und daher wiederum $I_2 \vDash \exists x\alpha$. □

9.3. **Substitution.**

Wir besprechen nun die Variablensubstitution, wobei wir weitgehend der Darstellung von Ebbinghaus, Flum, Thomas folgen.

Variablen repräsentieren verschiedene Werte (in einer Grundmenge M), die man für sie einsetzen kann. Auf formaler Ebene bedeutet dies, dass eine oder mehrere Variablen durch gewisse Terme ersetzt werden. Im semantischen Kontext wird dies durch die Uminterpretation von Variablen bei einer Interpretation präzise gemacht. Im syntaktischen Kontext spricht man von Substitution, die wir nun definieren werden. In der Ersetzung macht es einen großen Unterschied, ob gebundene oder freie Variablen vorliegen. Der Ausdruck

$$x \geq 0 \to \exists y(x = y \cdot y)$$

bedeutet in einem angeordneten Körper interpretiert, dass die nichtnegative Zahl x als Quadrat darstellbar ist (also eine Quadratwurzel besitzt), was für $\mathbb{R}$ wahr ist, für $\mathbb{Q}$ im Allgemeinen (das hängt von der Interpretation für x ab) nicht. Gleichbedeutend (bei einer inhaltlichen Interpretation) mit diesem Ausdruck ist

$$x \geq 0 \to \exists z(x = z \cdot z)\,,$$

aber nicht

$$x \geq 0 \to \exists x(x = x \cdot x)\,,$$

das nur bei $x = 0$ oder $x = 1$ wahr ist. Von daher wird die weiter unten zu gebende Definition für die Substitution von Ausdrücken berücksichtigen, ob Variablen frei oder gebunden sind. Ferner wird es wichtig sein, in einem Ausdruck neue Variablen einzuführen. Damit diese Konstruktion eindeutig definiert ist, legen wir entweder eine durchnummerierte (und abzählbare) Variablenmenge $v_1, v_2, v_3 \ldots$ zugrunde, oder aber eine beliebig große Variablenmenge, die mit einer Wohlordnung versehen sei.

Definition 9.2. Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k$ paarweise verschiedene Variablen und $t_1, \ldots, t_k$ fixierte S-Terme. Dann definiert man rekursiv über den Aufbau der Terme die Substitution $s\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ für jeden S-Term s.

(1) Für eine Variable x ist

$$x\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := \begin{cases} x, & \text{falls } x \neq x_i \text{ für alle } i\,, \\ t_i, & \text{falls } x = x_i\,. \end{cases}$$

(2) Für eine Konstante c ist

$$c\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := c.$$

(3) Für ein n-stelliges Funktionssymbol f und n Terme $s_1, \ldots, s_n$ ist

$$fs_1 \ldots s_n\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := fs_1\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} \ldots s_n\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}.$$

Beispiel 9.3. Es seien c, d Konstanten einer erststufigen Sprache, x, y, z, v Variablen, p ein einstelliges und f, g, h zweistellige Funktionssymbole. Wir betrachten den Term

$$t = fpxgcy$$

und die Substitution

$$\frac{d,\ \ hvx,\ \ v}{x,\quad y,\quad z}.$$

Die Substitution wird durchgeführt, indem man die kleinsten Bestandteile des Termes, also x, y, c, ersetzt und ansonsten den funktionalen Aufbau des Termes übernimmt. Für diese gilt

$$x\frac{d,\ \ hvx,\ \ v}{x,\quad y,\quad z} = d,$$

$$y\frac{d,\ \ hvx,\ \ v}{x,\quad y,\quad z} = hvx$$

und

$$c\frac{d,\ \ hvx,\ \ v}{x,\quad y,\quad z} = c.$$

Also ist

$$fpxgcy\frac{d,\ \ hvx,\ \ v}{x,\quad y,\quad z} = fpdgchvx.$$

Man beachte, dass das letzte x nicht zu ersetzen ist.

Definition 9.4. Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k$ paarweise verschiedene Variablen und $t_1, \ldots, t_k$ fixierte S-Terme. Dann definiert man rekursiv über den Aufbau der S-Ausdrücke die Substitution $\alpha\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ für jeden S-Ausdruck α.

(1) Für Terme s_1, s_2 setzt man[14]

$$(s_1 = s_2)\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := s_1\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} = s_2\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}.$$

(2) Für ein n-stelliges Relationssymbol R und n Terme $s_1, \ldots, s_n$ setzt man

$$(Rs_1 \ldots s_n)\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := Rs_1\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} \ldots s_n\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}.$$

(3) Für einen Ausdruck α setzt man

$$(\neg\alpha)\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := \neg\alpha\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}.$$

(4) Für Ausdrücke α und β setzt man

$$(\alpha \wedge \beta)\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := \alpha\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} \wedge \beta\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}$$

und ebenso für die anderen zweistelligen Junktoren.

[14]Die Klammern unterstreichen hier lediglich den Gesamtausdruck, für den die Substitution durchgeführt wird

(5) Für einen Ausdruck α seien $x_{i_1}, \ldots, x_{i_r}$ diejenigen Variablen (unter den $x_1, \ldots, x_k$), die in $\forall x\alpha$ frei vorkommen. Es sei $v = x$, falls x nicht in $t_{i_1}, \ldots, t_{i_r}$ vorkommt. Andernfalls sei v die erste Variable (in einer fixierten Variablenaufzählung, falls es abzählbar viele Variablen gibt, bzw. in einer fixierten Wohlordnung der Variablenmenge), die weder in α noch in $t_{i_1}, \ldots, t_{i_r}$ vorkommt. Dann setzt man

$$(\forall x\alpha)\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} := \forall v\alpha\frac{t_{i_1}, \ldots, t_{i_r}, v}{x_{i_1}, \ldots, x_{i_r}, x}$$

und ebenso für den Existenzquantor.

Bemerkung 9.5. Die sonderbare Bedingung in Definition 9.4 im Quantorenfall mit der „Hilfsvariablen“ v bedeutet insbesondere: Wenn in $\forall x\alpha$ keine der Variablen $x_1, \ldots, x_n$ frei vorkommt, so ist die Indexmenge $\{i_1, \ldots, i_r\}$ der „relevanten Variablen“ leer und damit auch die Menge der „relevanten Terme“. In diesem Fall kommt x auch nicht in dieser Menge vor und somit ist als Hilfsvariable $v = x$ zu nehmen, und es ist

$$(\forall x\alpha)\frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} = \forall x(\alpha\frac{x}{x}) = \forall x\alpha$$

nach Aufgabe 9.6.

Beispiel 9.6. Es seien c, d Konstanten einer erststufigen Sprache, x, y, z, u Variablen (so geordnet), f, g einstellige Funktionssymbole und R ein zweistelliges Relationssymbol. Wir betrachten den Ausdruck

$$\alpha = \forall x\neg Ryfx$$

und die Substitution

$$\frac{u, \quad gc}{x, \quad y}.$$

Von den zu substituierenden Variablen ist x gebunden und y frei. Die Variable x kommt in den substituierenden Termen nicht vor. Also ist

$$(\forall x\neg Ryfx)\,\frac{u, \quad gc}{x, \quad y} = \forall x\left(\neg Ryfx\frac{gc}{y}\right) = \forall x\neg Rgcfx.$$

Bei der Substitution

$$\frac{u, \quad gx}{x, \quad y}$$

kommt jetzt die gebundene Variable x in dem substituierenden Term gx vor. Es ist $v = z$ die nächste Variable in der gegebenen Reihenfolge. Somit ist

$$(\forall x\neg Ryfx)\,\frac{u, \quad gx}{x, \quad y} = \forall z\left(\neg Ryfx\frac{gx, \quad z}{y, \quad x}\right) = \forall z\neg Rgxfz.$$

Die folgende Aussage, das Substitutionslemma, stiftet eine Beziehung zwischen Substitutionen und Uminterpretationen.

In Verallgemeinerung der Schreibweise $I\frac{m}{x}$ für eine Uminterpretation schreiben wir $I\frac{m_1,\ldots,m_k}{x_1,\ldots,x_k}$ für die sukzessive Uminterpretation der untereinander verschiedenen Variablen $x_1,\ldots,x_k$ (dabei seien $m_1,\ldots,m_k$ Elemente der Grundmenge M der Interpretation). Es werden also die x_i als m_i interpretiert und alle anderen Variablen werden gemäß I interpretiert.

Lemma 9.7. *Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben und es seien $x_1,\ldots,x_k$ paarweise verschiedene Variablen und $t_1,\ldots,t_k$ fixierte S-Terme. Es sei eine S-Interpretation I gegeben. Dann gelten folgende Aussagen.*

(1) *Für jeden S-Term s gilt*

$$I\left(s\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right) = \left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(s).$$

(2) *Für jeden S-Ausdruck α gilt*

$$I \vDash \alpha\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k} \text{ genau dann, wenn } \left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right) \vDash \alpha\,.$$

Beweis. Dies wird über den induktiven Aufbau der Terme bzw. der Ausdrücke bewiesen. (1). Für eine Konstante c ist die Aussage richtig, da ihre Interpretation unverändert ist. Für eine Variable x macht man eine Fallunterscheidung. Wenn

$$x = x_i$$

mit einer der an der Substitution beteiligten Variablen ist, so ist

$$I\left(x_i\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right) = I(t_i) = \left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(x_i).$$

Bei einer an der Substitution nicht beteiligten Variablen x ist

$$I\left(x\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right) = I(x) = \left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(x).$$

Wenn f ein n-stelliges Funktionssymbol ist und $s_1,\ldots,s_n$ Terme sind, für die die Gleichheit schon bekannt ist, so ist

$$\begin{aligned}
& I\left((fs_1\ldots s_n)\,\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\\
= \;& I\left(fs_1\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\ldots s_n\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\\
= \;& I(f)\left(I\left(s_1\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right),\ldots,I\left(s_n\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\right)\\
= \;& I(f)\left(\left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(s_1),\ldots,\left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(s_n)\right)\\
= \;& \left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(f)\left(\left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(s_1),\ldots,\left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(s_n)\right)\\
= \;& \left(I\frac{I(t_1),\ldots,I(t_k)}{x_1,\ldots,x_k}\right)(fs_1\ldots s_n)\,.
\end{aligned}$$

(2). Für einen Ausdruck der Form $s = t$ bedeutet

$$I \vDash (s = t)\, \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}$$

einfach

$$I \vDash s \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} = t \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}\,.$$

Dies ist äquivalent zu

$$I\left(s \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}\right) \;=\; I\left(t \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}\right),$$

was nach dem ersten Teil einfach

$$I \frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k}(s) \;=\; I \frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k}(t)$$

bedeutet. Dies wiederum ist äquivalent zu

$$I \frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k} \vDash s = t\,.$$

Sei nun R ein n-stelliges Relationssymbol und seien $s_1, \ldots, s_n$ Terme. Die Gültigkeit

$$I \vDash (Rs_1 \ldots s_n)\, \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}$$

bedeutet

$$I \vDash Rs_1 \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k} \ldots s_n \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}$$

und dies bedeutet, dass

$$\left(I\left(s_1 \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}\right), \ldots, I\left(s_n \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}\right)\right)$$

zur Relation $I(R)$ gehört. Nach dem ersten Teil ist dieses Tupel gleich

$$\left(I \frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k}(s_1), \ldots, I \frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k}(s_n)\right)\,.$$

Wegen $R(I) \;=\; R\left(I \frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k}\right)$ ist dies äquivalent zu

$$I \frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k} \vDash Rs_1 \ldots s_n\,.$$

Für die weiteren Aussagen beweist man die Äquivalenz durch Induktion über den Aufbau der Ausdrücke, und zwar über alle Interpretationen simultan; dies ist für die aussagenlogischen Junktoren unmittelbar klar. Betrachten wir also einen Ausdruck der Form $\forall x \alpha$. Die Gültigkeit

$$I \vDash (\forall x \alpha)\, \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}$$

bedeutet gemäß der Festlegung in Definition 9.4, dass

$$I \vDash \forall v \alpha \frac{t_{i_1}, \ldots, t_{i_r}, v}{x_{i_1}, \ldots, x_{i_r}, x}$$

gilt, wobei v in $t_{i_1}, \ldots, t_{i_r}$ nicht vorkommt. Dies bedeutet, dass für jedes $m \in M$ der Grundmenge der Interpretation die Beziehung

$$I\frac{m}{v} \vDash \alpha \frac{t_{i_1}, \ldots, t_{i_r}, v}{x_{i_1}, \ldots, x_{i_r}, x}$$

gilt. Nach Induktionsvoraussetzung (angewendet auf die Interpretation $I\frac{m}{v}$) bedeutet dies

$$\left(I\frac{m}{v}\right) \frac{\left(I\frac{m}{v}\right)(t_{i_1}), \ldots, \left(I\frac{m}{v}\right)(t_{i_r}), \left(I\frac{m}{v}\right)(v)}{x_{i_1}, \ldots, x_{i_r}, x} \vDash \alpha$$

für alle $m \in M$. Aufgrund des Koinzidenzlemmas ist dies äquivalent zu

$$\left(I\frac{m}{v}\right) \frac{I(t_{i_1}), \ldots, I(t_{i_r}), m}{x_{i_1}, \ldots, x_{i_r}, x} \vDash \alpha\,.$$

Dies ist äquivalent (für alle $m \in M$) zu

$$I\frac{I(t_{i_1}), \ldots, I(t_{i_r}), m}{x_{i_1}, \ldots, x_{i_r}, x} \vDash \alpha\,,$$

was bei $v = x$ klar ist und bei $v \neq x$ aus dem Koinzidenzlemma folgt, da dann v nicht in α vorkommt. Dies bedeutet wiederum

$$I\frac{I(t_{i_1}), \ldots, I(t_{i_r})}{x_{i_1}, \ldots, x_{i_r}} \vDash \forall x \alpha$$

und damit

$$I\frac{I(t_1), \ldots, I(t_k)}{x_1, \ldots, x_k} \vDash \forall x \alpha\,.$$

□

9. Arbeitsblatt

9.1. **Übungsaufgaben.**

Aufgabe 9.1. Bestimme die freien Variablen in den folgenden Ausdrücken, wobei x, y, z Variablen seien und f ein einstelliges Funktionssymbol und R ein zweistelliges Relationssymbol sei.

(1) $\forall x\,(fx = y)$,
(2) $\forall x\,(fx = y) \wedge \exists z\,(fx = y)$,
(3) $\forall x \exists y R x f y$,
(4) $(\forall x \exists y R x f y) \rightarrow x = y$.

Aufgabe 9.2. Es sei $\alpha \in L_0^S$ ein Satz einer erststufigen Sprache über einem Symbolalphabet S. Es sei eine S-Struktur mit Trägermenge M gegeben und I_1 und I_2 zwei auf M definierte S-Interpretationen. Zeige $I_1 \vDash \alpha$ genau dann, wenn $I_2 \vDash \alpha$ gilt.

Aufgabe 9.3. Es seien c, d Konstanten einer erststufigen Sprache, x, y, z, v Variablen, f ein einstelliges und g, h zweistellige Funktionssymbole. Bestimme die Substitution

$$ghhxcdfz\frac{fx, \quad gxz, \quad hvfx}{x, \qquad y, \qquad z}.$$

Aufgabe 9.4. Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k$ paarweise verschiedene Variablen und $t_1, \ldots, t_k$ fixierte S-Terme.

a) Interpretiere die Termsubstitution $\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ als Abbildung.

b) Interpretiere die Substitution von Ausdrücken $\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ als Abbildung.

Aufgabe 9.5.*

Es seien x, y, z Variablen (mit der angegebenen Reihenfolge), c eine Konstante und f ein einstelliges Funktionssymbol.

(1) Bestimme
$$(\exists x(x = c))\frac{z}{x}.$$
(2) Bestimme
$$(\exists x(x = c))\frac{x}{x}.$$
(3) Bestimme
$$(\exists x(x = c))\frac{fx}{x}.$$

Aufgabe 9.6.*

Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben.

(1) Zeige, dass die Substitution $\frac{x}{x}$ für die Terme die Identität ist.
(2) Zeige, dass die Substitution $\frac{x}{x}$ für die Ausdrücke die Identität ist.

Aufgabe 9.7. Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben, es sei x eine Variable und t ein fixierter S-Term. Gehört die Symbolkette (!) $\alpha\frac{t}{x}$ zu L^S?

Aufgabe 9.8. Es sei c eine Konstante einer erststufigen Sprache, x, y, z, u Variablen, f ein einstelliges Funktionssymbol, g, h zweistellige Funktionssymbole und R ein zweistelliges Relationssymbol. Bestimme die Substitution

$$(\forall y R x y \wedge \neg R y f z)\, \frac{f x, \quad g x z, \quad h c f x}{x, \qquad y, \qquad z}\,.$$

Aufgabe 9.9. Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Man gebe ein Beispiel für eine Substitution $\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ und einen S-Ausdruck α derart, dass die sukzessive substituierten Ausdrücke

$$\alpha \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}, \left(\alpha \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right) \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}, \left(\left(\alpha \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right) \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right) \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}, \ldots$$

immer länger werden.

Aufgabe 9.10.*

Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k$ paarweise verschiedene Variablen und $t_1, \ldots, t_k$ fixierte S-Terme. Zeige, dass für jeden S-Satz $\alpha \in L_0^S$ die Gleichheit

$$\alpha \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k} = \alpha$$

gilt.

Aufgabe 9.11. Es sei $\alpha \in L^S$. Zeige, dass die Gleichheit

$$\left(\alpha \frac{y}{x}\right) \frac{z}{y} = \alpha \frac{y, z}{x, y}$$

im Allgemeinen nicht gilt.

Aufgabe 9.12.*

Es seien x_1, x_2 Variablen, t_1, t_2 Terme und α ein Ausdruck in einer prädikatenlogischen Sprache. Zeige, dass

$$\alpha \frac{t_1, t_2}{x_1, x_2} \to \left(\alpha \frac{t_1}{x_1}\right) \frac{t_2}{x_2}$$

im Allgemeinen nicht allgemeingültig ist.

Aufgabe 9.13.*

Es seien x_1, x_2 Variablen, t_1, t_2 Terme und α ein Ausdruck in einer prädikatenlogischen Sprache. Zeige, dass

$$\left(\alpha \frac{t_1}{x_1}\right) \frac{t_2}{x_2} \to \alpha \frac{t_1, t_2}{x_1, x_2}$$

im Allgemeinen nicht allgemeingültig ist.

Aufgabe 9.14.*

Es seien x, y Variablen, s, t Terme und α ein Ausdruck in einer prädikatenlogischen Sprache. Es seien u, v neue Variablen, die weder in s noch in t noch in α vorkommen. Zeige, dass

$$\alpha \frac{s, t}{x, y} \leftrightarrow \alpha \frac{s\frac{v}{y}\, t\frac{u}{x}}{x\ y}\frac{x}{u}\frac{y}{v}$$

allgemeingültig ist, wobei der Ausdruck rechts als die Hintereinanderausführung von vier Einzelsubstitutionen (von links nach rechts) zu lesen ist.

Aufgabe 9.15.*

Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben, $\alpha \in L^S$ und I eine Interpretation mit $I \vDash \alpha$. Zeige durch ein Beispiel, dass daraus nicht im Allgemeinen die Gültigkeit $I \vDash \alpha \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ unter einer Substitution folgt.

Aufgabe 9.16. Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k$ paarweise verschiedene Variablen und $t_1, \ldots, t_k$ fixierte S-Terme. Zeige, dass zu einem allgemeingültigen Ausdruck α auch die Substitution $\alpha \frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ allgemeingültig ist. Gilt hiervon auch die Umkehrung?

9.2. **Aufgaben zum Abgeben.**

Aufgabe 9.17. (2 Punkte)

Es sei α ein S-Ausdruck. Zeige, dass es einen S-Ausdruck β der Form $\beta = \alpha \wedge \gamma$ derart gibt, dass

$$\mathrm{Frei}\,(\beta) \;=\; \mathrm{Var}\,(\alpha) \;=\; \mathrm{Var}\,(\beta)$$

gilt.

Aufgabe 9.18. (2 Punkte)

Es seien c, d Konstanten einer erststufigen Sprache, x, y, z, u, v, w Variablen (in dieser Reihenfolge), f ein einstelliges Funktionssymbol, g ein zweistelliges Funktionssymbol und P, R einstellige Relationssymbole. Bestimme die Substitution

$$(\forall y(y = c) \vee (\neg Rfz \to \exists x \neg Pu) \frac{gzz, \quad c, \quad fu}{x, \quad y, \quad z}.$$

Aufgabe 9.19. (3 Punkte)

Man gebe für jedes $r \in \mathbb{N}_+$ ein Beispiel für eine Substitution $\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}$ und einen S-Ausdruck α derart, dass die sukzessive substituierten Ausdrücke

$$\alpha\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}, \left(\alpha\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}, \left(\left(\alpha\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}, \ldots$$

eine Periode der Länge r besitzen.

Aufgabe 9.20. (3 Punkte)

Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k, y_1, \ldots, y_\ell$ paarweise verschiedene Variablen und $t_1, \ldots, t_k, s_1, \ldots, s_\ell$ fixierte S-Terme. Zeige, dass für Terme τ, in denen $y_1, \ldots, y_\ell$ nicht vorkommen, die Gleichheit

$$\left(\tau\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\frac{s_1,\ldots,s_\ell}{y_1,\ldots,y_\ell} = \tau\frac{t_1\frac{s_1,\ldots,s_\ell}{y_1,\ldots,y_\ell},\ldots,t_k\frac{s_1,\ldots,s_\ell}{y_1,\ldots,y_\ell}}{x_1,\ldots,x_k}$$

gilt.

Aufgabe 9.21. (2 Punkte)

Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k, y_1, \ldots, y_\ell$ paarweise verschiedene Variablen und $t_1, \ldots, t_k, s_1, \ldots, s_\ell$ fixierte S-Terme. Zeige durch ein Beispiel, dass für Terme τ die Gleichheit

$$\left(\tau\frac{t_1,\ldots,t_k}{x_1,\ldots,x_k}\right)\frac{s_1,\ldots,s_\ell}{y_1,\ldots,y_\ell} = \tau\frac{t_1\frac{s_1,\ldots,s_\ell}{y_1,\ldots,y_\ell},\ldots,t_k\frac{s_1,\ldots,s_\ell}{y_1,\ldots,y_\ell}}{x_1,\ldots,x_k}$$

nicht gelten muss.

Aufgabe 9.22. (4 Punkte)

Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien $x_1, \ldots, x_k, y_1, \ldots, y_\ell$ paarweise verschiedene Variablen und $t_1, \ldots, t_k, s_1, \ldots, s_\ell$ fixierte S-Terme. Zeige durch ein Beispiel, dass für Ausdrücke α die Gleichheit (von Ausdrücken)

$$\left(\alpha \frac{t_1, \ldots, t_k}{x_1, \ldots, x_k}\right) \frac{s_1, \ldots, s_\ell}{y_1, \ldots, y_\ell} = \alpha \frac{t_1 \frac{s_1, \ldots, s_\ell}{y_1, \ldots, y_\ell}, \ldots, t_k \frac{s_1, \ldots, s_\ell}{y_1, \ldots, y_\ell}}{x_1, \ldots, x_k}$$

nicht gelten muss.

Aufgabe 9.23. (3 Punkte)

Es sei ein Symbolalphabet S einer Sprache erster Stufe gegeben. Es seien x, z verschiedene Variablen, t ein S-Term und α ein S-Ausdruck, wobei z weder in t noch in α vorkomme. Gilt dann die Gleichheit

$$\left(\alpha \frac{z}{x}\right) \frac{t}{z} = \alpha \frac{t}{x}?$$

10. Vorlesung - Ableitungskalkül

10.1. **Ableitungskalkül der Prädikatenlogik.**

Gegeben sei ein Symbolalphabet S einer Sprache erster Stufe und damit die zugehörige Termmenge und die zugehörige Ausdrucksmenge L^S. Wir möchten die logisch wahren Aussagen einer solchen Sprache syntaktisch charakterisieren. Mathematische Aussagen sind im Allgemeinen „wenn-dann“-Aussagen, d.h. sie behaupten, dass, wenn gewisse Voraussetzungen erfüllt sind, dann auch eine gewisse Folgerung erfüllt ist.

Wenn man einen Beweis eines Satzes der Gruppentheorie oder der elementaren Arithmetik entwirft, so sind dabei die Axiome der Gruppentheorie bzw. die Peano-Axiome stets präsent. Wenn $\alpha_1, \alpha_2, \alpha_3$ die Gruppenaxiome bezeichnen und α die Aussage, dass das inverse Element eindeutig bestimmt ist, bezeichnet, so folgt α aus $\alpha_1, \alpha_2, \alpha_3$. Mit der Folgerungsbeziehung kann man dies als

$$\{\alpha_1, \alpha_2, \alpha_3\} \vDash \alpha$$

formulieren. Dies kann man auch so ausdrücken, dass

$$\alpha_1 \wedge \alpha_2 \wedge \alpha_3 \to \alpha$$

allgemeingültig ist, also dass

$$\vDash \alpha_1 \wedge \alpha_2 \wedge \alpha_3 \to \alpha$$

gilt. So kann man jede Folgerung $\Gamma \vDash \alpha$ aus einer endlichen Ausdrucksmenge Γ „internalisieren“, also durch einen allgemeingültigen Ausdruck der Form

$$\vDash \alpha_1 \wedge \ldots \wedge \alpha_n \to \alpha$$

wiedergegeben, wobei vorne die Ausdrücke aus Γ konjugiert werden. Die Folgerungsbeziehung (zumindest aus endlichen Ausdrucksmengen) kann also vollständig durch allgemeingültige Ausdrücke verstanden werden.

Wir besprechen nun die syntaktische Variante der allgemeingültigen Ausdrücke, nämlich die syntaktischen prädikatenlogischen Tautologien. Über den soeben besprochenen Zusammenhang ergibt sich daraus auch ein Ableitungskalkül, der das syntaktische Analogon zur Folgerungsbeziehung ist. Da wir Ausdrücke der Form $\alpha_1 \wedge \ldots \wedge \alpha_n \to \alpha$ als Grundtyp für eine mathematische Aussage ansehen, arbeiten wir allein mit den Junktoren $\neg, \wedge, \to$ und lesen $\vee$ und $\leftrightarrow$ als Abkürzungen. Man könnte auch noch $\wedge$ bzw. $\to$ eliminieren und durch die verbleibenden beiden Junktoren ausdrücken, doch würde dies zu recht unleserlichen Formulierungen führen.

Der prädikatenlogische Kalkül, den wir vorstellen wollen, soll es erlauben, „alle“ prädikatenlogischen allgemeingültigen Ausdrücke formal abzuleiten. Der Aufbau dieses Kalküls geschieht (wie für den Ableitungskalkül der Aussagenlogik) rekursiv (und für beliebige Symbolalphabete gleichzeitig). D.h. man hat eine Reihe von Anfangstautologien (oder Grundtautologien) und gewisse Schlussregeln, um aus schon nachgewiesenen Tautologien neue zu produzieren. Sowohl die Anfangstautologien als auch die Schlussregeln sind aus der mathematischen Beweispraxis vertraut.

Zur Formulierung dieses Kalküls verwenden wir die Schreibweise

$$\vdash \alpha\,.$$

Sie bedeutet, dass der Ausdruck α in der Prädikatenlogik (erster Stufe zu einem gegebenen Alphabet) ableitbar ist, also eine Tautologie (im syntaktischen Sinne) ist. Wir beschreiben nun rekursiv die syntaktischen Tautologien in der Prädikatenlogik, die sich in aussagenlogische Tautologien, Gleichheitstautologien und Quantorentautologien und zwei Ableitungsregeln untergliedern. Wir beginnen mit den schon bekannten, allerdings in einer anderen Sprache formulierten aussagenlogischen Tautologien.

Axiom 10.1. Zu einem beliebigen Symbolalphabet S und beliebige Ausdrücke $\alpha, \beta, \gamma \in L^S$ legt man folgende (syntaktische) *Tautologien* axiomatisch fest.

(1)
$$\vdash \alpha \to (\beta \to \alpha)\,.$$

(2)
$$\vdash (\alpha \to \beta) \wedge (\beta \to \gamma) \to (\alpha \to \gamma)\,.$$

(3)
$$\vdash (\alpha \to \beta) \wedge (\alpha \to \gamma) \to (\alpha \to \beta \wedge \gamma)\,.$$

(4)
$$\vdash (\alpha \wedge \beta \to \gamma) \to (\alpha \to (\beta \to \gamma))$$

und

$$\vdash (\alpha \to (\beta \to \gamma)) \to (\alpha \wedge \beta \to \gamma)\,.$$

(5)
$$\vdash \alpha \wedge \neg\alpha \to \beta\,.$$

(6)
$$\vdash (\alpha \to \beta) \wedge (\neg\alpha \to \beta) \to \beta\,.$$

Als (erste) Schlussregel erlaubt man wieder den Modus Ponens, so dass die Prädikatenlogik in einem gewissen Sinne die Aussagenlogik umfasst. Die Einschränkung in dieser Formulierung beruht darauf, dass es in der Sprache der Prädikatenlogik keine Aussagenvariablen gibt. Man kann sich vorstellen, dass die oben angeführten Tautologien aus den entsprechenden aussagenlogischen (in Aussagenvariablen formulierten) Tautologien entstehen, indem man für die Aussagenvariablen beliebige prädikatenlogische Ausdrücke einsetzt. Dies führt zu folgendem *Einsetzungsprinzip*. Wir schreiben $\varphi\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n}$, wenn in einem aussagenlogischen Ausdruck φ die darin vorkommenden Aussagenvariablen p_i durch prädikatenlogische Ausdrücke β_i ersetzt werden (diese Ersetzung ist deutlich einfacher als die Ersetzung von Variablen durch Terme.)

Lemma 10.2. *Es sei φ eine in den Aussagenvariablen $p_1, \ldots, p_n$ formulierte aussagenlogische Tautologie und es seien $\beta_1, \ldots, \beta_n \in L^S$ prädikatenlogische Ausdrücke über einem Symbolalphabet S. Dann ist auch der prädikatenlogische Ausdruck φ', der entsteht, wenn man in φ jedes Auftreten der Aussagenvariablen p_i durch β_i ersetzt, eine prädikatenlogische Tautologie.*

Beweis. Wir führen Induktion über den Aufbau der aussagenlogischen Tautologien. Es sei φ eines der aussagenlogischen Axiome in den Ausdrücken α, β, γ und es seien $p_1, \ldots, p_n$ die darin auftretenden Aussagenvariablen. Wir schreiben die zugrunde liegende aussagenlogische Tautologie in den Aussagenvariablen p, q, r und nennen diese ψ. Dann ist

$$\varphi \;=\; \psi\frac{\alpha, \beta, \gamma}{p,\;\; q,\;\; r}.$$

Somit ist insgesamt

$$\varphi' \;=\; \varphi\frac{\beta_1, \ldots, \beta_n}{p_1, \ldots, p_n} \;=\; \psi\frac{\alpha\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n}, \beta\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n}, \gamma\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n}}{p,\qquad\quad q,\qquad\quad r}.$$

D.h. φ' entsteht durch Einsetzung von prädikatenlogischen Ausdrücken in eine Basistautologie und gehört somit zu den in Axiom 10.1 gelisteten Tautologien. Es sei nun φ eine aussagenlogische Tautologie, die durch Modens Ponens erhalten wird. Dann gibt es also eine aussagenlogische Tautologie ψ und $\psi \to \varphi$ ist ebenfalls eine aussagenlogische Tautologie. Nach Induktionsvoraussetzung sind dann $\psi\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n}$ und $(\psi \to \varphi)\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n} = \psi\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n} \to \varphi\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n}$ prädikatenlogische Tautologien. Da der Modus Ponens eine erlaubte

Schlussregel in der Prädikatenlogik ist, folgt, dass $\varphi\frac{\beta_1,\ldots,\beta_n}{p_1,\ldots,p_n}$ eine prädikatenlogische Tautologie ist. □

Beispiel 10.3. Wir betrachten die aussagenlogische Tautologie der Form

$$\alpha \to (\beta \to \alpha)$$

mit

$$\alpha = p_1 \wedge p_2 \text{ und } \beta = p_3 \to p_4\,,$$

also

$$\begin{aligned} \varphi &= (\alpha \to (\beta \to \alpha))\,\frac{p_1 \wedge p_2,\, p_3 \to p_4}{\alpha,\, \beta} \\ &= (p_1 \wedge p_2) \to ((p_3 \to p_4) \to (p_1 \wedge p_2))\,. \end{aligned}$$

In diese aussagenlogische Tautologie soll

$$p_1 \text{ durch } \beta_1 := Rxy,\ p_2 \text{ durch } \beta_2 := \forall uu = c,\ p_3 \text{ durch } \beta_3 := \exists y \forall x f x z = y,\ p_4 \text{ durch } \beta_4 := \neg Pu,$$

ersetzt werden. Das ergibt die prädikatenlogische Tautologie

$$(Rxy \wedge \forall uu = c) \to (((\exists y \forall x f x z = y) \to \neg Pu) \to (Rxy \wedge \forall uu = c))\ .$$

Im Laufe der Einführung der prädikatenlogischen Tautologien und der zugehörigen Schlussregeln werden wir sogleich die Korrektheit feststellen, d.h., dass es sich auch um allgemeingültige Ausdrücke (semantische Tautologien) handelt. Für die aussagenlogischen Tautologien wurde die Korrektheit für aussagenlogische Modelle schon gezeigt, eine einfache Variante davon liefert die Korrektheit innerhalb von prädikatenlogischen Modellen.

Lemma 10.4. *Jede aussagenlogische Tautologie im Sinne von Axiom 10.1 ist allgemeingültig in der Prädikatenlogik.*

Beweis. Es sei I eine Interpretation von L^S und φ eine aussagenlogische Grundtautologie in den prädikatenlogischen Ausdrücken α, β, γ. Dann ist der Wahrheitswert von φ in I nur abhängig von den Wahrheitswerten von α, β, γ in I und den Junktoren in φ. Da es sich um eine aussagenlogische Tautologie handelt und die Wahrheitsvorschrift für die Junktoren in einem prädikatenlogischen Modell mit der in einem aussagenlogischen Modell übereinstimmt, besitzt φ den Wahrheitswert w. Also ist φ allgemeingültig. □

Da allgemeingültige Aussagen unter Modus Ponens abgeschlossen sind, folgt daraus, dass generell alle prädikatenlogisch formulierten aussagenlogischen Tautologien allgemeingültig sind.

10.2. **Gleichheitstautologien.**

In der Prädikatenlogik gelten die beiden folgenden Tautologien für die Gleichheit.

Axiom 10.5. Es sei S ein Symbolalphabet, s, t seien S-Terme und α sei ein S-Ausdruck. Dann sind die beiden folgenden Ausdrücke syntaktische Tautologien.

(1)
$$\vdash t = t\,.$$

(2)
$$\vdash s = t \wedge \alpha\frac{s}{x} \to \alpha\frac{t}{x}\,.$$

Diese beiden Axiome (oder genauer Axiomenschemata) heißen *Gleichheitsaxiom* und *Substitutionsaxiom*. Mit einer aussagenlogischen Umformulierung sieht man, dass das Substitutionsaxiom äquivalent zu

$$\vdash s = t \to \left(\alpha\frac{s}{x} \to \alpha\frac{t}{x}\right)$$

ist.

Lemma 10.6. *Die Gleichheitsaxiome sind korrekt.*

Beweis. Sei I eine beliebige S-Interpretation. (1). Aufgrund der Bedeutung des Gleichheitszeichens unter jeder Interpretation gilt

$$I(t) = I(t)\,,$$

also

$$I \vDash t = t\,.$$

(2). Es gelte

$$I \vDash s = t \wedge \alpha\frac{s}{x}\,,$$

also $I \vDash s = t$ und $I \vDash \alpha\frac{s}{x}$. Das bedeutet einerseits $I(s) = I(t)$. Andererseits gilt nach dem Substitutionslemma

$$I\frac{I(s)}{x} \vDash \alpha\,.$$

Wegen der Termgleichheit gilt somit auch

$$I\frac{I(t)}{x} \vDash \alpha$$

und daher, wiederum aufgrund des Substitutionslemmas, auch

$$I \vDash \alpha\frac{t}{x}\,.$$

□

Lemma 10.7. *Aus den Gleichheitsaxiomen lassen sich folgende Gleichheitstautologien ableiten (dabei sind $r, s, t, s_1, \ldots, s_n, t_1, \ldots, t_n$ Terme, f ein n-stelliges Funktionssymbol und R ein n-stelliges Relationssymbol).*

(1)
$$\vdash s = t \to t = s\,.$$

(2)
$$\vdash r = s \wedge s = t \to r = t\,.$$

(3)
$$\vdash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \to fs_1 \ldots s_n = ft_1 \ldots t_n\,.$$

(4)
$$\vdash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \wedge Rs_1 \ldots s_n \to Rt_1 \ldots t_n\,.$$

Beweis. (1). Aufgrund der Gleichheitsaxiome haben wir

$$\vdash s = s$$

und

$$\vdash s = t \wedge (x = s)\frac{s}{x} \to (x = s)\frac{t}{x}\,,$$

wobei x eine Variable sei, die weder in s noch in t vorkomme. Daher sind die beiden substituierten Ausdrücke gleich $s = s$ bzw. $t = s$. Eine aussagenlogische Umstellung der zweiten Zeile ist

$$\vdash s = s \to (s = t \to t = s)\,,$$

so dass sich aus der ersten Zeile mittels Modus ponens

$$\vdash s = t \to t = s$$

ergibt. (2). Es sei wieder x eine Variable, die weder in r noch in s noch in t vorkomme. Eine Anwendung des Substitutionsaxioms liefert

$$\vdash s = t \wedge (r = x)\frac{s}{x} \to (r = x)\frac{t}{x}\,.$$

Nach Einsetzen und einer aussagenlogischen Umstellung ist dies die Behauptung. Für (3) siehe Aufgabe 10.5. (4). Es sei u eine Variable, die weder in einem der s_i noch in einem der t_i vorkommt. Für jedes $i = 1, \ldots, n$ gilt nach Axiom 10.5 (2) (mit $\alpha = \alpha_i = Rt_1 \ldots t_{i-1}us_{i+1} \ldots s_n$) dann

$$\vdash s_i = t_i \to \left(Rt_1 \ldots t_{i-1}us_{i+1} \ldots s_n\frac{s_i}{u} \to Rt_1 \ldots t_{i-1}us_{i+1} \ldots s_n\frac{t_i}{u}\right)\,,$$

also

$$\vdash s_i = t_i \to (Rt_1 \ldots t_{i-1}s_is_{i+1} \ldots s_n \to Rt_1 \ldots t_{i-1}t_is_{i+1} \ldots s_n)\,.$$

Diese Ableitbarkeiten gelten auch, wenn man die Vordersätze durch ihre Konjunktion

$$(s_1 = t_1) \wedge \ldots \wedge (s_n = t_n)$$

ersetzt. Durch die Transitivität der Implikation ergibt sich daher

$$\vdash (s_1 = t_1) \wedge \ldots \wedge (s_n = t_n) \to (Rs_1 \ldots s_n \to Rt_1 \ldots t_n)\,.$$

□

10. Arbeitsblatt

10.1. **Übungsaufgaben.**

Aufgabe 10.1. Ersetze in den folgenden aussagenlogischen Tautologien

$$p_1 \text{ durch } \beta_1 := \exists x Rxy,\ p_2 \text{ durch } \beta_2 := \forall u\,(fu = c \to Pc)\,,$$
$$p_3 \text{ durch } \beta_3 := \exists y \forall x gxz = y,\ p_4 \text{ durch } \beta_4 := Rcu \to c = u.$$

(1) $p_1 \wedge p_2 \to p_1$,
(2) $(p_1 \wedge p_4 \to \neg p_2) \wedge (p_1 \wedge p_4 \to (p_2 \to p_1)) \to (p_1 \wedge p_4 \to \neg p_2 \wedge (p_2 \to p_1))$,
(3) $p_3 \wedge \neg p_3 \to p_4$,
(4) $(p_1 \wedge p_4 \to p_3) \wedge (\neg\,(p_1 \wedge p_4) \to p_3) \to p_3$.

Aufgabe 10.2. Unterscheide zwischen den verschiedenen Bedeutungen von Gleichheit.

(1) Gleichheit von Elementen in einer Menge.
(2) Gleichheit von Zeichenketten.
(3) Das Gleichheitssymbol in einer erststufigen Sprache.

Aufgabe 10.3. Es sei S ein Symbolalphabet einer Sprache erster Stufe. Es seien S-Terme s, t mit

$$\vdash s = t$$

gegeben. Zeige, dass es sich bei s und t um eine identische Zeichenreihe handelt.

Aufgabe 10.4. Es sei S ein Symbolalphabet und $t_1, \ldots, t_n$ seien S-Terme. Zeige die Ableitbarkeit

$$\vdash t_1 = t_2 \wedge t_2 = t_3 \wedge \ldots \wedge t_{n-1} = t_n \to t_1 = t_n\,.$$

Aufgabe 10.5.*

Es seien $s_1, \ldots, s_n, t_1, \ldots, t_n$ Terme und f ein n-stelliges Funktionssymbol. Zeige, dass die Ableitbarkeit

$$\vdash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \to f s_1 \ldots s_n = f t_1 \ldots t_n$$

gilt.

Aufgabe 10.6. Zeige direkt (ohne die Verwendung der Ableitungsbeziehung), dass die folgenden Ausdrücke allgemeingültig sind (dabei seien r, s, t, $s_1, \ldots, s_n, t_1, \ldots, t_n$ Terme, f ein n-stelliges Funktionssymbol und R ein n-stelliges Relationssymbol).

(1)
$$\vDash s = t \to t = s\,.$$

(2)
$$\vDash r = s \wedge s = t \to r = t\,.$$

(3)
$$\vDash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \to f s_1 \ldots s_n = f t_1 \ldots t_n\,.$$

(4)
$$\vDash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \wedge R s_1 \ldots s_n \to R t_1 \ldots t_n\,.$$

Aufgabe 10.7.*

Es seien $x_1, \ldots, x_n$ Variablen, $s_1, \ldots, s_n, t_1, \ldots, t_n$ Terme und α ein Ausdruck in einer prädikatenlogischen Sprache L^S. Zeige, dass

$$s_1 = t_1 \wedge \ldots \wedge s_n = t_n \to \left(\alpha \frac{s_1, \ldots, s_n}{x_1, \ldots, x_n} \to \frac{t_1, \ldots, t_n}{x_1, \ldots, x_n} \right)$$

allgemeingültig ist.

Aufgabe 10.8. Es seien r_1, r_2, s, t Terme einer prädikatenlogischen Sprache L^S und sei x eine Variable. Zeige durch ein Beispiel, dass

$$s = t \to r_1 \frac{s}{x} = r_2 \frac{t}{x}$$

nicht ableitbar sein muss.[15]

Aufgabe 10.9.*

Zeige durch ein Beispiel, dass für Terme r_1, r_2, s und eine Variable x einer prädikatenlogischen Sprache L^S der Ausdruck

$$r_1 = r_2 \to r_1 \frac{s}{x} = r_2 \frac{s}{x}$$

nicht ableitbar sein muss.

Aufgabe 10.10. Gehört in einem Ausdruck der Form $(x = y)\,\frac{t}{x}$ die Symbolfolge $\frac{t}{x}$ zur prädikatenlogischen Sprache? Gehört $(x = y)\,\frac{t}{x}$ dazu?

[15] Die Nicht-Ableitbarkeit wird durch die Angabe eines Modells gezeigt; dies verwendet die Korrektheit des Ableitungskalküls, den wir noch nicht vollständig behandelt haben.

10.2. **Aufgaben zum Abgeben.**

Aufgabe 10.11. (2 Punkte)

Es seien c, d Konstanten, es sei f ein zweistelliges Funktionssysmbol und es R ein dreistelliges Relationssymbol. Man erläutere, wie man die prädikatenlogische Tautologie

$$(Rxcfyd \vee z = x) \wedge \neg (Rxcfyd \vee z = x) \rightarrow (\exists x fxc = d)$$

aus einer aussagenlogischen Tautologie im Sinne von Lemma 10.2 erhält.

Aufgabe 10.12. (4 Punkte)

Es seien $r, s_1, \ldots, s_n, t_1, \ldots, t_n$ Terme einer prädikatenlogischen Sprache L^S und seien $x_1, \ldots, x_n$ verschiedene Variablen. Zeige durch Induktion über den Aufbau des Termes r die Ableitbarkeit

$$\vdash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \rightarrow \left(r\frac{s_1, \ldots, s_n}{x_1, \ldots, x_n} = r\frac{t_1, \ldots, t_n}{x_1, \ldots, x_n} \right) .$$

Aufgabe 10.13. (4 Punkte)

Es seien $s_1, \ldots, s_n, t_1, \ldots, t_n$ Terme einer prädikatenlogischen Sprache L^S und seien $x_1, \ldots, x_n$ verschiedene Variablen.

(1) Es sei R ein k-stelliges Relationssymbol und $r_1, \ldots, r_k$ seien Terme. Zeige die Ableitbarkeit

$$\vdash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \rightarrow \left((Rr_1 \ldots r_k)\frac{s_1, \ldots, s_n}{x_1, \ldots, x_n} \rightarrow (Rr_1 \ldots r_k)\frac{t_1, \ldots, t_n}{x_1, \ldots, x_n} \right) .$$

(2) Es seien r_1 und r_2 Terme. Zeige die Ableitbarkeit

$$\vdash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \rightarrow \left(r_1\frac{s_1, \ldots, s_n}{x_1, \ldots, x_n} = r_2\frac{s_1, \ldots, s_n}{x_1, \ldots, x_n} \rightarrow r_1\frac{t_1, \ldots, t_n}{x_1, \ldots, x_n} = r_2\frac{t_1, \ldots, t_n}{x_1, \ldots, x_n} \right) .$$

Tipp: Verwende Aufgabe 10.12

Aufgabe 10.14. (4 Punkte)

Es sei S ein Symbolalphabet, $s_1, \ldots, s_n, t_1, \ldots, t_n$ seien S-Terme, $x_1, \ldots, x_n$ verschiedene Variablen und α sei ein S-Ausdruck. Zeige die Allgemeingültigkeit

$$\vDash s_1 = t_1 \wedge \ldots \wedge s_n = t_n \rightarrow \left(\alpha\frac{s_1, \ldots, s_n}{x_1, \ldots, x_n} \rightarrow \alpha\frac{t_1, \ldots, t_n}{x_1, \ldots, x_n} \right) .$$

Aufgabe 10.15. (4 Punkte)

Zeige durch ein Beispiel, dass bei einem ableitbaren Ausdruck der Form

$$\vdash s = t \to \left((\exists z \beta) \frac{s}{x} \to (\exists z \beta) \frac{t}{x} \right)$$

die durch die Existenzquantoren gebundenen Variablen (nach der durchgeführten Substitution) nicht übereinstimmen müssen.

10.3. **Die Aufgabe zum Aufgeben.**

Lösungen zu der folgenden Aufgabe direkt an den Dozenten. Bis Ende Mai.

Aufgabe 10.16. Wir betrachten eine Variante des Ableitungskalkül (geschrieben $\vdash_V$) der Aussagenlogik, bei dem die Grundtautologien aus Axiom 3.8 unverändert übernommen werden, bei der aber der Modus Ponens durch die Schlussregel

Wenn $\vdash_V \alpha \wedge (\alpha \to \beta)$, dann ist $\vdash_V \beta$

ersetzt wird. Stimmen $\vdash$, $\vdash_V$ überein?

11. Vorlesung - Quantorenregeln

11.1. **Quantorenaxiome und -regeln.**

Wir besprechen nun die Tautologien und Ableitungsregeln, die mit den Quantoren zusammenhängen. Wir arbeiten allein mit dem Existenzquantor und wir arbeiten nur mit nichtleeren Grundmengen. Letzteres ist Voraussetzung dafür, dass es überhaupt eine Variablenbelegung geben kann. Bei den jetzt einzuführenden Axiomen handelt es sich um eine Tautologie (genauer gesagt um ein Schema von Tautologien), nämlich die *Existenzeinführung im Sukzedens* und um eine Schlussregel, nämlich die *Existenzeinführung im Antezedens*. Für letztere ist die exakte Formulierung und der Korrektheitsnachweis nicht trivial.

Axiom 11.1. Es sei S ein Symbolalphabet erster Stufe, α ein S-Ausdruck, x eine Variable und t ein S-Term. Dann ist

$$\vdash \alpha \frac{t}{x} \to \exists x \alpha \,.$$

Diese Tautologie bedeutet inhaltlich gesprochen, dass man bei einem Ausdruck, für den man einen erfüllenden Term gefunden hat, auf die entsprechende Existenzaussage schließen kann. Diese Tautologie ist allgemeingültig: Wenn in einer Interpretation I die Beziehung

$$I \vDash \alpha \frac{t}{x}$$

gilt, so ist dies nach dem Substitutionslemma äquivalent zu

$$I\frac{I(t)}{x} \vDash \alpha\,,$$

und das bedeutet wiederum

$$I \vDash \exists x\alpha\,.$$

Einen wichtigen Spezialfall dieser Tautologie erhält man für $t = x$, nämlich (unabhängig davon, ob x in α vorkommt oder nicht)

$$\vdash \alpha \to \exists x\alpha\,.$$

Für den Allquantor (den wir als Abkürzung verstehen) ergibt sich die entsprechende Tautologie

$$\vdash \forall x\alpha \to \alpha\frac{t}{x}\,.$$

Streng genommen ergibt sich diese Variante in dieser Form aber erst unter Verwendung der Existenzeinführung im Antezedens, siehe weiter unten und Aufgabe 11.8 und Aufgabe 11.1.

Axiom 11.2. Es sei S ein Symbolalphabet erster Stufe, α und β seien S-Ausdrücke, x und y seien Variablen. Dann gilt die folgende Regel: Wenn

$$\vdash \alpha\frac{y}{x} \to \beta$$

gilt und wenn y weder in $\exists x\alpha$ noch in β frei vorkommt, so gilt auch

$$\vdash \exists x\alpha \to \beta\,.$$

Ein Spezialfall dieser Ableitungsregel (bei $x = y$) ist, dass man aus $\vdash \alpha \to \beta$ unter der Bedingung, dass x nicht frei in β vorkommt, auf $\vdash \exists x\alpha \to \beta$ schließen kann.

Die Allvariante dieser Schlussregel ist die *Alleinführung im Sukzedens*. Sie besagt, dass man aus

$$\vdash \beta \to \alpha\frac{y}{x}$$

unter der Bedingung, dass y weder in $\forall x\alpha$ noch in β frei vorkommt, auf

$$\vdash \beta \to \forall x\alpha$$

schließen kann. Wir geben ein Beispiel für diese Version (mit $x = y$), wie sie in der mathematischen Praxis vorkommt.

Beispiel 11.3. Nehmen wir an, wir möchten die Aussage beweisen, dass in einem jeden Monoid das neutrale Element eindeutig bestimmt ist. Wir formalisieren diese Aussage als

$$\beta \to \forall x\alpha\,,$$

wobei β die Konjunktion der zwei Monoidaxiome (also Assoziativität und Existenz des neutralen Elementes) und $\alpha := \forall z(xz = z) \to x = e$ ist. In α ist x nicht gebunden, in $\forall x\alpha$ schon. In einem mathematischen Beweis

wird man sich dann ein „festes, aber beliebiges“ Monoid M „denken“, und darin ein „festes, aber beliebiges“ $x \in M$. Für dieses x beweist man dann die Aussage, dass wenn $xz = z$ für alle $z \in M$ gilt, dass dann $x = e$ sein muss. Im Beweis selbst wird nicht über x quantifiziert, dies steckt gewissermaßen in der gewählten Beliebigkeit drin. Man beweist also eher[16] die Aussage

$$\beta \to \alpha\,,$$

und betrachtet dies als einen Beweis für die oben notierte Version. Da x in β gar nicht oder allenfalls gebunden vorkommt, ist die Ableitbarkeit beider Versionen auch prädikatenlogisch gleichwertig. Insofern spiegelt sich in der Alleinführung im Sukzedens eine wichtiger Aspekt der mathematischen Praxis.

Die Existenzeinführung im Antezedens ist die einzige syntaktische Gesetzßigkeit, deren Korrektheit nicht unmittelbar klar ist.

Lemma 11.4. *Die Existenzeinführung im Antezedens ist eine korrekte Regel.*

Beweis. Es sei $\alpha\frac{y}{x} \to \beta$ allgemeingültig, d.h.

$$I \vDash \alpha\frac{y}{x} \to \beta$$

für jede S-Interpretation I. Wir müssen zeigen, dass dann auch $\exists x\alpha \to \beta$ allgemeingültig ist (unter den gegebenen Voraussetzungen). Sei dazu I eine Interpretation mit

$$I \vDash \exists x\alpha\,.$$

Aufgrund der Modellbeziehung bedeutet dies, dass es ein $m \in M$ (aus der Grundmenge der Interpretation) mit

$$I\frac{m}{x} \vDash \alpha$$

gibt. Die Variable y kommt nach Voraussetzung in $\exists x\alpha$ nicht frei vor, d.h. bei $y \neq x$, dass y in α nicht frei vorkommt. Wir können daher das Koinzidenzlemma anwenden und erhalten

$$\left(I\frac{m}{x}\right)\frac{m}{y} \vDash \alpha\,.$$

Diese Aussage gilt trivialerweise auch bei $x = y$. Damit gilt auch

$$\left(I\frac{m}{y}\right)\frac{m}{x} \vDash \alpha\,.$$

[16] Diese Unschärfe in der Begrifflichkeit ist kaum zu vermeiden, da eine formale Interpretation oder Rekonstruktion dessen, was in der mathematischen Praxis passiert, nie ganz eindeutig ist.

Wir schreiben dies (etwas künstlich) als

$$\left(I\frac{m}{y}\right)\frac{\left(I\frac{m}{y}\right)(y)}{x} \vDash \alpha\,.$$

Darauf können wir das Substitutionslemma (für die Interpretation $J = I\frac{m}{y}$ und den Term y) anwenden und erhalten

$$I\frac{m}{y} \vDash \alpha\frac{y}{x}\,.$$

Wegen der vorausgesetzten Allgemeingültigkeit von $\alpha\frac{y}{x} \to \beta$ folgt

$$I\frac{m}{y} \vDash \beta\,.$$

Da y in β nicht frei vorkommt, liefert das Koinzidenzlemma

$$I \vDash \beta\,.$$

□

Bemerkung 11.5. Die Variablenbedingung in der Existenzeinführung im Antezedenz ist wesentlich. Das zeigt am besten die Betrachtung $\beta = \alpha$, wobei darin die Variable $x = y$ frei vorkommen möge (also z.B. $\alpha = Rx$, wobei R ein einstelliges Relationssymbol sei). Dann ist natürlich

$$\vdash \alpha \to \alpha$$

richtig, und die Variablenbedingung an x, bezogen auf diesen Ausdruck, ist nicht erfüllt. Die Aussage

$$\exists x\alpha \to \alpha\,,$$

die man unter Missachtung dieser Variablenbedingung ableiten könnte, ist keine Tautologie. Aus der Existenz eines Elementes $m \in M$, das die Relation R^M erfüllt, folgt ja keineswegs, dass die Relation für alle Elemente gilt. Diese Ableitungsregel lässt sich also insbesondere nicht durch eine interne Tautologie ersetzen.

Definition 11.6. Ein Ausdruck $\alpha \in L^S$ heißt *ableitbar* im Prädikatenkalkül (oder eine *syntaktische Tautologie*), wenn er sich aus den Grundtautologien, also

- den aussagenlogischen syntaktischen Tautologien,
- den Gleichheitsaxiomen,
- der Existenzeinführung im Sukzedens,

durch sukzessive Anwendung der Ableitungsregeln Modus Ponens und der Existenzeinführung im Antezedens erhalten lässt. Die Ableitbarkeit wird durch

$$\vdash \alpha$$

ausgedrückt.

11.2. **Abgeleitete Regeln und weitere Tautologien.**

Bisher haben wir lediglich den Modus Ponens und die Existenzeinführung im Antezedens als Ableitungsregeln für den syntaktischen Kalkül zur Verfügung. Daraus ergeben sich allerdings sofort neue Ableitungsregeln, mit denen man neue Tautologien herleiten kann. Die Hinrichtung in der folgenden Aussage kommt häufig implizit in einer mathematischen Argumentation vor. Man beweist eine Aussage für beliebige, aber feste Elemente, und fasst dies als einen Beweis für die entsprechende Allaussage auf.

Lemma 11.7. *Es sei S ein Symbolalphabet erster Stufe, α ein S-Ausdruck und x eine Variable. Dann ist $\vdash \alpha$ genau dann, wenn $\vdash \forall x \alpha$ ist.*

Beweis. Nach der Allquantorversion von Axiom 11.1 ist

$$\vdash \forall x \alpha \to \alpha \frac{x}{x},$$

also

$$\vdash \forall x \alpha \to \alpha .$$

Daher folgt aus

$$\vdash \forall x \alpha$$

mittels Modus Ponens direkt

$$\vdash \alpha .$$

Sei umgekehrt $\vdash \alpha$ gegeben. Es sei β ein beliebiger Ausdruck, in dem x nicht vorkomme. Nach Axiom 3.8 (2) und Modus Ponens ergibt sich

$$\vdash \beta \to \alpha$$

und

$$\vdash \neg\beta \to \alpha .$$

Auf diese beiden abgeleiteten Ausdrücke wird nun die Allquantorversion der Existenzeinführung im Antezedens (also die Alleinführung im Sukzedens) angewendet. Dies ist möglich, da x in β überhaupt nicht und in $\forall x \alpha$ nicht frei vorkommt. Man erhält

$$\vdash \beta \to \forall x \alpha$$

und

$$\vdash \neg\beta \to \forall x \alpha .$$

Daraus ergibt sich mit der Fallunterscheidungsregel

$$\vdash \forall x \alpha .$$

□

Diese Aussage bedeutet aber keineswegs, dass man den Allquantor überall weglassen oder hinzufügen könnte. Sie bedeutet lediglich, dass bei einem Ausdruck, der als Ganzes als eine Tautologie erwiesen ist, auch der entsprechende Allausdruck eine Tautologie ist und umgekehrt. Semantisch betrachtet beruht diese Äquivalenz darauf, dass die Allgemeingültigkeit von α bedeutet,

dass bei einer beliebigen (Struktur- und) Variablenbelegung die entstehende Aussage ohne freie Variable wahr wird. Da ist also eine Allaussage schon miteingebunden. Insbesondere gilt *nicht* $\vdash \alpha \leftrightarrow \forall x \alpha$.

Für den Existenzquantor gilt die entsprechende Äquivalenz nicht. Zwar ergibt sich aus $\vdash \alpha$ direkt $\vdash \exists x \alpha$ (und zwar unabhängig davon, ob x in α vorkommt oder nicht; die Allgemeingültigkeit beruht darauf, dass nur nichtleere Grundmengen betrachtet werden), aber nicht umgekehrt. Beispielsweise ist

$$\vdash \exists x (x = y)\,,$$

aber $x = y$ ist keine Tautologie.

Lemma 11.8. *Die folgenden Ausdrücke sind im Prädikatenkalkül ableitbar.*

(1)
$$\vdash \exists x \exists y \alpha \to \exists y \exists x \alpha\,.$$

(2)
$$\vdash \forall x \forall y \alpha \to \forall y \forall x \alpha\,.$$

Beweis. (1). Durch Existenzeinführung im Sukzedenz haben wir

$$\vdash \alpha \to \exists x \alpha$$

und

$$\vdash \exists x \alpha \to \exists y \exists x \alpha$$

und daraus

$$\vdash \alpha \to \exists y \exists x \alpha\,.$$

Dabei ist y hinten gebunden und somit kann man mit der Existenzeinführung im Antezedens auf

$$\vdash \exists y \alpha \to \exists y \exists x \alpha$$

schließen. Da auch x hinten gebunden ist, ergibt sich

$$\vdash \exists x \exists y \alpha \to \exists y \exists x \alpha\,.$$

(2) wird ähnlich wie (1) bewiesen oder darauf zurückgeführt. □

Für die (Nicht)-Vertauschbarkeit des Allquantors mit dem Existenzquantor siehe Aufgabe 11.22.

Lemma 11.9. *Die folgenden Ausdrücke sind im Prädikatenkalkül ableitbar.*

(1)
$$\vdash \forall x \alpha \wedge \forall x (\alpha \to \beta) \to \forall x \beta\,.$$

(2)
$$\vdash \forall x \alpha \wedge \forall x \beta \leftrightarrow \forall x \,(\alpha \wedge \beta)\ .$$

(3)
$$\vdash \exists x \alpha \wedge \forall x (\alpha \to \beta) \to \exists x \beta\,.$$

(4)
$$\vdash \exists x(\alpha \wedge \beta) \to \exists x\alpha \wedge \exists x\beta\,.$$

Beweis. (1). Aufgrund der Alleinführung im Antezedens ist
$$\vdash \forall x\alpha \to \alpha$$
und
$$\vdash \forall x(\alpha \to \beta) \to (\alpha \to \beta)\,.$$
Dies konjugiert (unter Verwendung von Lemma 3.16 (2)) ergibt
$$\vdash \forall x\alpha \wedge \forall x(\alpha \to \beta) \to \alpha \wedge (\alpha \to \beta)\,.$$
Ferner haben wir die aussagenlogische Tautologie
$$\vdash \alpha \wedge (\alpha \to \beta) \to \beta\,.$$
Damit ergibt sich aufgrund der Transitivität der Implikation die Ableitung
$$\vdash \forall x\alpha \wedge \forall x(\alpha \to \beta) \to \beta\,.$$
Da x vorne und in $\forall x\beta$ gebunden vorkommt, gilt nach der Alleinführung im Sukzedens auch
$$\vdash \forall x\alpha \wedge \forall x(\alpha \to \beta) \to \forall x\beta\,.$$

Zu (2) siehe Aufgabe 11.9 und Aufgabe 11.10.

(3). Aufgrund der Alleinführung im Antezedens ist
$$\vdash \forall x(\alpha \to \beta) \to (\alpha \to \beta)\,,$$
was wir als
$$\vdash \alpha \wedge \forall x(\alpha \to \beta) \to \beta$$
schreiben. Wegen $\vdash \beta \to \exists x\beta$ ist auch
$$\vdash \alpha \wedge \forall x(\alpha \to \beta) \to \exists x\beta\,,$$
was wir als
$$\vdash \alpha \to (\forall x(\alpha \to \beta) \to \exists x\beta)$$
schreiben. Im Sukzedens ist x gebunden, daher folgt aus der Existenzeinführung im Antezedens
$$\vdash \exists x\alpha \to (\forall x(\alpha \to \beta) \to \exists x\beta)\,,$$
was aussagenlogisch äquivalent zur Behauptung ist.

Zu (4) siehe Aufgabe 11.12. □

Die folgende Aussage zeigt, dass man quantifizierte Aussagen im Wesentlichen mit beliebigen Variablen formulieren kann.

Lemma 11.10. *Es sei α ein Ausdruck über einem erststufigen Symbolalphabet S und seien x, y Variablen. Die Variable y komme in α nicht und die Variable x komme in α allenfalls frei vor. Dann ist*
$$\vdash \exists x\alpha \to \exists y\left(\alpha\frac{y}{x}\right)\,.$$

Beweis. Nach Axiom 11.1, angewendet auf $\alpha\frac{y}{x}$, ist

$$\vdash \alpha\frac{y}{x} \to \exists y \left(\alpha\frac{y}{x}\right) .$$

Da y in $\exists y \left(\alpha\frac{y}{x}\right)$ gebunden vorkommt und in $\exists x\alpha$ gar nicht, kann man Axiom 11.2 anwenden und erhält

$$\vdash \exists x\alpha \to \exists y \left(\alpha\frac{y}{x}\right) .$$

□

11.3. **Die Ableitungsbeziehung.**

Analog zur Folgerungsbeziehung definieren wir die Ableitungsbeziehung aus einer Ausdrucksmenge.

Definition 11.11. Es sei S ein Symbolalphabet, Γ eine Menge an S-Ausdrücken und α ein weiterer S-Ausdruck. Man sagt, dass α aus Γ *ableitbar* ist, geschrieben

$$\Gamma \vdash \alpha ,$$

wenn es endlich viele Ausdrücke $\alpha_1, \ldots, \alpha_n \in \Gamma$ derart gibt, dass

$$\vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \alpha$$

gilt.

Man kann sich also wieder fragen, welche Ausdrücke aus einer vorgegebenen Ausdrucksmenge Γ, beispielsweise einem Axiomensystem einer Sprache erster Stufe, ableitbar sind. Unser „unbedingter“ Prädikatenkalkül, der die syntaktischen Tautologien generiert, führt zu einem entsprechenden Regelsatz für die Ableitbarkeit aus Γ. Dies ist näher an der mathematischen Praxis, da man sich dort in einem bestimmten mathematischen Kontext bewegt (z.B. der Gruppentheorie) und daher unter der Voraussetzung arbeitet, dass eine gewisse Ausdrucksmenge (z.B. die Gruppenaxiome) vorliegt, aus der heraus man etwas beweisen möchte.

11. Arbeitsblatt

11.1. **Übungsaufgaben.**

Aufgabe 11.1. Beweise allein aus der Existenzeinführung im Sukzedens und aussagenlogischen Gesetzen die *Alleinführung im Antezedens*, also dass für eine Variable x, einen Term t und einen Ausdruck α

$$\vdash \forall x\neg\alpha \to \neg\alpha\frac{t}{x}$$

eine Tautologie ist.

Aufgabe 11.2. Zeige

$$\vDash \exists x(x = y)\,.$$

Aufgabe 11.3. Zeige

$$\vdash \exists x(x = y)\,.$$

Aufgabe 11.4. Beweise aus der Existenzeinführung im Antezedens die *Alleinführung im Sukzedens*. Sie besagt, dass man aus

$$\vdash \beta \to \alpha\frac{y}{x}$$

unter der Bedingung, dass y weder in $\forall x\alpha$ noch in β frei vorkommt, auf

$$\vdash \beta \to \forall x\alpha$$

schließen kann.

Aufgabe 11.5. Zeige, dass der Ausdruck

$$\left(\alpha\frac{y}{x} \to \beta\right) \to (\exists x\alpha \to \beta)$$

keine Tautologie ist (auch nicht, wenn y weder in $\exists x\alpha$ noch in β frei vorkommt).

Aufgabe 11.6. Es sei α ein Ausdruck in einer Sprache L^S erster Stufe. Zeige, dass

$$\alpha \leftrightarrow \forall x\alpha$$

keine Tautologie ist.

Aufgabe 11.7.*

Zeige, dass mit

$$\vdash \alpha \to \beta$$

auch

$$\vdash \forall x\alpha \to \forall x\beta$$

gilt.

Aufgabe 11.8. Zeige, dass in der Prädikatenlogik die *Alleinführung im Antezedens* ableitbar ist, also dass für eine Variable x, einen Term t und einen Ausdruck α

$$\vdash \forall x\alpha \to \alpha\frac{t}{x}$$

gilt.

Aufgabe 11.9.*

Zeige

$$\vdash \forall x\alpha \wedge \forall x\beta \to \forall x\,(\alpha \wedge \beta)\ .$$

Aufgabe 11.10.*

Zeige

$$\vdash \forall x\,(\alpha \wedge \beta) \to \forall x\alpha \wedge \forall x\beta\,.$$

Aufgabe 11.11. a) Zeige

$$\vdash \exists x(\alpha \wedge \beta) \to \exists x\alpha \wedge \exists x\beta\,.$$

b) Zeige, dass

$$\exists x\alpha \wedge \exists x\beta \to \exists x(\alpha \wedge \beta)$$

keine Tautologie ist.

Aufgabe 11.12. Es sei S ein erststufiges Symbolalphabet und $f \in S$ ein n-stelliges Funktionssymbol. Erstelle eine Ableitung für den Ausdruck

$$\exists y\,((fx_1 \ldots x_n = y) \wedge \forall z\,((fx_1 \ldots x_n = z) \to y = z))\ .$$

Aufgabe 11.13.*

Es seien A, B, C einstellige Relationssymbole. Zeige, dass der *Modus Barbara*, also die Aussage

$$(\forall x(Ax \to Bx) \wedge \forall x(Bx \to Cx)) \to (\forall x(Ax \to Cx))$$

im Prädikatenkalkül ableitbar ist.

Aufgabe 11.14.*

Es seien A, B, C einstellige Relationssymbole. Zeige, dass der *Modus Darii*, also die Aussage

$$(\forall x(Ax \to Bx) \wedge \exists x(Ax \wedge Cx)) \to (\exists x(Bx \wedge Cx))$$

im Prädikatenkalkül ableitbar ist.

Aufgabe 11.15.*

Es seien x, y, u, v Variablen und $\Gamma = \{\forall x \forall y\,(x = y)\}$ und $\Delta = \{x = y\}$.

(1) Zeige (ohne Bezug auf den Vollständigkeitssatz) $\Gamma \vdash u = v$.
(2) Charakterisiere die Modelle M mit $M \vDash \Gamma$.
(3) Zeige $\Delta \nvdash u = v$.

Aufgabe 11.16.*

Es sei G ein dreistelliges Relationssymbol und L die zugehörige prädikatenlogische Sprache. Es sei I die Interpretation, bei der die Grundmenge die euklidische Ebene ist und G durch die dreistellige Relation interpretiert wird, bei der $G(A, B, C)$ zutrifft, wenn die Punkte A, B, C auf einer Geraden liegen.

(1) Zeige $I \vDash Gxyz \leftrightarrow Gyxz$.
(2) Zeige, dass im Allgemeinen nicht $I \vDash \forall x \forall y \forall z \, (Gxyz \to Gxyu)$ gelten muss.
(3) Es sei $\Gamma = \{\forall x \forall y \forall z \, (Gxyz \leftrightarrow Gyxz) \, , \forall x \forall y \forall z \, (Gxyz \leftrightarrow Gxzy)\}$. Erstelle eine Ableitung für $\Gamma \vdash Gxyz \leftrightarrow Gyzx$.
(4) Zeige, dass der Ausdruck $Gxyz \wedge Gxyu$ bei der gegebenen Interpretation nicht bedeutet, dass die die freien Variablen x, y, z, u belegenden Punkte auf einer Geraden liegen.
(5) Formuliere einen Ausdruck aus L in vier freien Variablen, der bei der gegebenen Interpretation besagt, dass die die freien Variablen belegenden Punkte auf einer Geraden liegen.

Die beiden folgenden Aufgaben sind vermutlich mühselig.

Aufgabe 11.17. Man gebe einen formalen Beweis für die Aussage, dass die Hintereinanderschaltung von zwei surjektiven Abbildungen auf einer Menge wieder surjektiv ist.

Aufgabe 11.18. Man gebe einen formalen Beweis für die Aussage, dass die Hintereinanderschaltung von zwei injektiven Abbildungen auf einer Menge wieder injektiv ist.

Aufgabe 11.19. Es sei Γ eine Ausdrucksmenge aus einer Sprache erster Stufe und α ein weiterer Ausdruck. Es sei α nicht aus Γ ableitbar. Zeige, dass man aus $\Gamma \cup \{\neg\alpha\}$ keinen Widerspruch (also keinen Ausdruck der Form $\beta \wedge \neg\beta$) ableiten kann.

Aufgabe 11.20. Begründe die folgenden Ableitungsregeln (es seien s, t Terme, α, β Ausdrücke und Γ eine Ausdrucksmenge).

(1) Wenn $\Gamma \vdash s = t$, dann ist auch $\Gamma \vdash \alpha\frac{s}{x} \to \alpha\frac{t}{x}$,
(2) Wenn $\Gamma \vdash \alpha\frac{t}{x}$, dann ist auch $\Gamma \vdash \exists x \alpha$,
(3) Wenn $\Gamma \vdash \alpha\frac{y}{x} \to \beta$, dann ist auch $\Gamma \vdash \exists x \alpha \to \beta$, unter der Bedingung, dass y nicht frei in $\Gamma, \exists x \alpha, \beta$ vorkommt.

11.2. **Aufgaben zum Abgeben.**

Aufgabe 11.21. (2 Punkte)

Sei $\alpha \in L^S$. Zeige die Ableitbarkeit

$$\vdash \exists x \exists x \alpha \leftrightarrow \exists x \alpha \,.$$

Aufgabe 11.22. (4 Punkte)

Sei $\alpha \in L^S$. Zeige die Ableitbarkeit

$$\vdash \exists x \forall y \alpha \to \forall y \exists x \alpha \,.$$

Zeige, dass

$$\forall y \exists x \alpha \to \exists x \forall y \alpha$$

nicht ableitbar ist.

Aufgabe 11.23. (4 Punkte)

Formuliere mit dem zweistelligen Funktionssymbol $\cdot$ die Aussage, dass wenn eine Zahl a die Zahl b teilt und b die Zahl c teilt, dass dann a auch c teilt.

Erstelle eine Ableitung für diese Aussage.

Aufgabe 11.24. (3 Punkte)

Zeige, dass es eine Ausdrucksmenge Γ mit der Eigenschaft gibt, dass für jede Interpretation I genau dann $I \vDash \Gamma$ gilt, wenn die Grundmenge der Interpretation unendlich ist.

12. Vorlesung - Natürliche Zahlen

Wir haben bisher nur von Axiomensystemen im Sinne einer beliebigen Ausdrucksmenge $\Gamma \subseteq L^S$ gesprochen, die im Allgemeinen eine Vielzahl von Modellen besitzt und aus der gewisse Ableitungen bzw. Folgerungen gezogen werden können, die für alle Modelle gelten. Es gibt aber auch Axiomensysteme, mit denen man ein intendiertes mathematisches Objekt wie beispielsweise die vertrauten natürlichen Zahlen charakterisieren möchte. Die natürlichen Zahlen haben wir bisher nur zum Indizieren von Aussagen- oder Termvariablen verwendet (wobei wir an einzelnen Stellen Induktion über die natürlichen Zahlen geführt haben) und als wichtige Quelle für offene mathematische Probleme erwähnt. Hier sprechen für von Axiomensystemen für die natürlichen Zahlen, und zwar sowohl von zweitstufigen als auch von erststufigen. Der Sprachgebrauch ist in der Literatur nicht einheitlich, wir werden von den (zweitstufigen) *Dedekind-Peano-Axiomen* und den erststufigen *Peano-Axiomen* sprechen.

12.1. **Dedekind-Peano-Axiome.**

Richard Dedekind (1831 - 1916)

Giuseppe Peano (1858 - 1932)

Wir besprechen nun die Dedekind-Peano-Axiome, eine zweitstufige Axiomatik, die eine vollständige Charakterisierung der natürlichen Zahlen erlauben.

Axiom 12.1. Eine Menge N mit einem ausgezeichneten Element $0 \in N$ (die *Null*) und einer (Nachfolger)-Abbildung

$$' \colon N \longrightarrow N,\ n \longmapsto n',$$

heißt *natürliche Zahlen* (oder *Dedekind-Peano-Modell* für die natürlichen Zahlen), wenn die folgenden *Dedekind-Peano-Axiome* erfüllt sind.

(1) Das Element 0 ist kein Nachfolger (die Null liegt also nicht im Bild der Nachfolgerabbildung).
(2) Jedes $n \in N$ ist Nachfolger höchstens eines Elementes (d.h. die Nachfolgerabbildung ist injektiv).
(3) Für jede Teilmenge $T \subseteq N$ gilt: Wenn die beiden Eigenschaften
   - $0 \in T$,
   - mit jedem Element $n \in T$ ist auch $n' \in T$,

   gelten, so ist $T = N$.

Mit zweitstufig ist gemeint, dass nicht nur über die Elemente der Menge N, die man axiomatisch charakterisieren will, quantifiziert wird, sondern (im dritten sogenannten *Induktionsaxiom*) auch über beliebige Teilmengen dieser Menge. Eine solche Situation wird erststufig nicht (zumindest nicht unmittelbar) erfasst.[17] Mit dieser Axiomatik werden wir zeigen, dass je zwei Modelle

[17] Eine andere wichtige Frage ist, inwiefern man in der ersten Stufe zweitstufige Phänome nachbilden kann. Das ist weitgehend möglich.

für diese zweistufigen Dedekind-Peano-Axiome „isomorph“ sind, dass es also zwischen ihnen eine strukturerhaltende Bijektion (einen *Isomorphismus*) gibt, und dass man ausgehend von der Nachfolgerfunktion die Addition und die Multiplikation rekursiv einführen kann.

Die folgende Aussage ist das *induktive Definitionsprinzip für Abbildungen.*

Satz 12.2. *Es sei $(N, 0, ')$ ein Dedekind-Peano-Modell der natürlichen Zahlen und es sei M eine Menge mit einem fixierten Element $s \in M$ und einer Abbildung $F\colon M \to M$. Dann gibt es genau eine Abbildung*

$$\varphi\colon N \longrightarrow M,\, n \longmapsto \varphi(n),$$

die die beiden Eigenschaften

$$\varphi(0) = s \text{ und } \varphi(n') = F(\varphi(n)) \text{ für alle } n \in \mathbb{N}$$

erfüllt.

Beweis. Wir betrachten Teilmengen $S \subseteq N$ mit den Eigenschaften

(1) $0 \in S$
(2) Für jedes $n \in S$, $n \neq 0$, gibt es ein $k \in S$ mit $n = k'$.
(3) Es gibt eine eindeutig bestimmte Abbildung

$$\varphi_S\colon S \longrightarrow M$$

mit $\varphi_S(0) = s$ und

$$\varphi_S(n') = F(\varphi_S(n))$$

für alle $n \in N$ mit $n, n' \in S$.

Wir betrachten nun die Menge

$$T = \{k \in N \mid \text{Es gibt ein } S \text{ mit den beschriebenen Eigenschaften und mit } k \in S\}.$$

Wir zeigen durch Induktion, dass $T = N$ ist. Für $k = 0$ können wir

$$S = \{0\}$$

wählen, wobei $\varphi_{\{0\}}$ durch die erste Abbildungseigenschaft eindeutig festgelegt ist. Sei nun $k \in T$ vorausgesetzt. Das bedeutet, dass es $k \in S$ und eine Abbildung φ_S mit den angegebenen Eigenschaften gibt. Bei $k' \in S$ sind wir fertig, sei also $k' \notin S$. Wir setzen $S' = S \cup \{k'\}$ und wir definieren

$$\varphi_{S'}(n) = \begin{cases} \varphi_S(n)\,, \text{ falls } n \in S\,, \\ F(\varphi_S(k))\,, \text{ falls } n = k'\,. \end{cases}$$

Dies erfüllt die Eigenschaften und ist auch die einzige Möglichkeit, da die Einschränkung von $\varphi_{S'}$ auf S wegen der Eindeutigkeit mit φ_S übereinstimmen muss. Also ist $T = N$.

Wir zeigen nun durch Induktion über k, dass $\varphi_S(k)$ unabhängig von der gewählten Menge $k \in S$ ist. Bei $k = 0$ ist dies klar, sei diese Aussage für ein gewisses k schon bekannt, und sei $k' \in S_1, S_2$ mit zugehörigen Abbildungen $\varphi_1 = \varphi_{S_1}, \varphi_2 = \varphi_{S_2}$. Aufgrund der zweiten Eigenschaft ist $k \in S_1, S_2$, daher ist nach Induktionsvoraussetzung

$$\varphi_1(k') = F(\varphi_1(k)) = F(\varphi_2(k)) = \varphi_2(k').$$

Damit erhält man durch

$$\varphi(k) := \varphi_S(k)$$

mit einem beliebigen $k \in S$ eine wohldefinierte Abbildung auf ganz N mit den in der Formulierung des Satzes geforderten Eigenschaften. Die Eindeutigkeit von φ ergibt sich aus der Eindeutigkeit der Einschränkungen. □

Satz 12.3. *Es seien N_1 und N_2 Dedekind-Peano-Modelle für die natürlichen Zahlen. Dann gibt es eine eindeutig bestimmte bijektive Abbildung*

$$\varphi\colon N_1 \longrightarrow N_2$$

mit $\varphi(0_1) = 0_2$ und

$$\varphi(n') = (\varphi(n))'$$

für alle $n \in N_1$. Insbesondere sind je zwei Dedekind-Peano-Modelle isomorph.

Beweis. Aufgrund von Satz 12.2, angewendet auf N_1 und die Nachfolgerabbildung auf N_2, gibt es genau eine Abbildung

$$\varphi\colon N_1 \longrightarrow N_2$$

mit den angegebenen Eigenschaften. Wenn man die Rollen vertauscht, so erhält man eine eindeutige Abbildung

$$\psi\colon N_2 \longrightarrow N_1$$

mit den gleichen Eigenschaften. Wir betrachten nun die Verknüpfung

$$\psi \circ \varphi\colon N_1 \longrightarrow N_1.$$

Diese erfüllt ebenfalls diese Eigenschaften. Da aber die Identität auf N_1 auch diese Eigenschaften erfüllt, folgt aus der Eindeutigkeitsaussage aus Satz 12.2, dass $\psi \circ \varphi = \mathrm{Id}_{N_1}$ ist. Ebenso ist $\varphi \circ \psi = \mathrm{Id}_{N_2}$ und somit sind φ und ψ invers zueinander. □

Für das im Wesentlichen eindeutig bestimmte Modell der Dedekind-Peano-Axiome verwenden wir das Symbol $\mathbb{N}$ und sprechen von den *natürlichen Zahlen*.

12.2. **Addition auf natürlichen Zahlen.**

Wir wollen die Addition auf den natürlichen Zahlen definieren, und zwar ausgehend von den Dedekind-Peano-Axiomen. Die Addition mit 0 soll dabei das Element wiedergeben - d.h. 0 soll das neutrale Element der Addition sein - und die Addition eines Elementes n mit $1 := 0'$ soll der Nachfolger von n sein. Die Grundidee ist dabei, die Summe $n + k$ dadurch zu definieren, dass man sukzessive den ersten Summanden um eins erhöht (also den Nachfolger nimmt) und den zweiten um eins vermindert (also den Vorgänger nimmt, falls $k \neq 0$ ist). Man spricht vom *Umlegungsprinzip* (oder Umlegungsmodell) für die Addition. Um dies präzise durchzuführen verwenden wir das induktive Definitionsprinzip für Abbildungen. Wir wenden dieses Prinzip für die Nachfolgerabbildung und für eine natürliche Zahl $n \in \mathbb{N}$ als Startglied an. Die daraus gewonnene Abbildung beschreibt das Addieren mit dieser Zahl n (es wird also die zweistellige Addition auf einstellige Operationen zurückgeführt).

Definition 12.4. Es sei $(\mathbb{N}, 0, ')$ ein Dedekind-Peano-Modell der natürlichen Zahlen und $n \in \mathbb{N}$. Dann definieren wir die *Addition mit* n als diejenige aufgrund von Satz 12.2 eindeutig bestimmte Abbildung

$$\alpha_n \colon \mathbb{N} \longrightarrow \mathbb{N},\ k \longmapsto \alpha_n(k),$$

für die

$$\alpha_n(0) = n \text{ und } \alpha_n(k') = (\alpha_n(k))' \text{ für alle } k \in \mathbb{N}$$

gilt.

Damit definieren wir

$$n + k := \alpha_n(k)$$

und nennen das die *Addition von natürlichen Zahlen*. Man beachte, dass hier die Addition in einer Weise definiert wird, in der die Kommutativität keineswegs offensichtlich ist.

Lemma 12.5. *Es sei* $(\mathbb{N}, 0, ')$ *ein Dedekind-Peano-Modell der natürlichen Zahlen. Dann gibt es genau eine Verknüpfung*

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},\ (x, y) \longmapsto x + y,$$

mit

$$x + 0 = x \text{ für alle } x \in \mathbb{N} \text{ und } x + y' = (x + y)' \text{ für alle } x, y \in \mathbb{N}\,.$$

Beweis. Siehe Aufgabe 12.10. □

Lemma 12.6. *Es sei* $(\mathbb{N}, 0, ')$ *ein Dedekind-Peano-Modell der natürlichen Zahlen mit der in Definition 12.4 festgelegten Addition. Dann gelten folgende Aussagen.*

(1)
$$n + 0 = n = 0 + n$$
für alle n*, d.h.* 0 *ist das neutrale Element für die Addition.*

(2)
$$n + k' = (n + k)' = n' + k$$
für alle $n, k \in \mathbb{N}$.

(3) *Die Addition ist kommutativ.*

(4) *Die Addition ist assoziativ.*

(5) *Aus einer Gleichung* $n + k = m + k$ *folgt*
$$n = m$$
*(*Abziehregel*).*

Beweis. (1). Die Gleichung links ergibt sich direkt aus der Definition, die rechte Gleichung, also $\alpha_0(n) = n$, folgt aus einer einfachen Induktion nach n.

(2). Die linke Gleichung folgt direkt aus der Definition, die rechte besagt $\alpha_{n'}(k) = (\alpha_n(k))'$. Wir beweisen sie für beliebiges n durch Induktion über k. Bei $k = 0$ steht beidseitig n'. Sei die Aussage nun für k schon bewiesen und betrachten wir k'. Dann ist
$$\alpha_{n'}(k') = (\alpha_{n'}(k))' = ((\alpha_n(k))')' = (\alpha_n(k'))'.$$
Für die anderen Aussagen siehe Aufgabe 12.11. □

12.3. **Multiplikation auf natürlichen Zahlen.**

Zur Definition der Multiplikation verwenden wir erneut das Prinzip der induktiven Definition. Zu einer natürlichen Zahl $n \in \mathbb{N}$ betrachten wir den Startwert 0 und die durch die Addition mit n definierte Abbildung $\alpha_n \colon \mathbb{N} \to \mathbb{N}$.

Definition 12.7. Es sei $(\mathbb{N}, 0, ')$ ein Dedekind-Peano-Modell der natürlichen Zahlen und $n \in \mathbb{N}$. Dann definieren wir die *Multiplikation mit* n als diejenige aufgrund von Satz 12.2 eindeutig bestimmte Abbildung
$$\mu_n \colon \mathbb{N} \longrightarrow \mathbb{N},\ k \longmapsto \mu_n(k),$$
für die
$$\mu_n(0) = 0 \text{ und } \mu_n(k') = \mu_n(k) + n \text{ für alle } k \in \mathbb{N}$$
gilt.

Damit definieren wir die Multiplikation von zwei natürlichen Zahlen $n, k \in \mathbb{N}$ durch
$$n \cdot k := \mu_n(k).$$
Es gilt also $n \cdot 0 = 0$ und $n \cdot k' = n \cdot k + n$. Diese beiden Eigenschaften legen bereits die Multiplikationsverknüpfung eindeutig fest.

Lemma 12.8. *Es sei* $(\mathbb{N}, 0, ')$ *ein Dedekind-Peano-Modell der natürlichen Zahlen. Dann gibt es eine eindeutig bestimmte Verknüpfung*

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},\ (x, y) \longmapsto x \cdot y,$$

die

$$x \cdot 0 = 0 \text{ für alle } x \in \mathbb{N} \text{ und } x \cdot y' = x \cdot y + x \text{ für alle } x, y \in \mathbb{N}$$

erfüllt.

Beweis. Siehe Aufgabe 12.15. □

Lemma 12.9. *Es sei* $(\mathbb{N}, 0, ')$ *ein Dedekind-Peano-Modell der natürlichen Zahlen mit der in Definition 12.7 festgelegten Multiplikation. Dann gelten folgende Aussagen.*

(1) *Es gilt*
$$0 \cdot n = 0 = n \cdot 0$$
für alle n*,*
(2) *Es gilt*
$$1 \cdot n = n = n \cdot 1$$
für alle n*, d.h.* $1 = 0'$ *ist das neutrale Element für die Multiplikation.*
(3) *Es ist*
$$n \cdot k' = n \cdot k + n = k' \cdot n$$
für alle $n, k \in \mathbb{N}$*.*
(4) *Die Multiplikation ist kommutativ.*
(5) *Die Multiplikation ist assoziativ.*
(6) *Aus einer Gleichung* $n \cdot k = m \cdot k$ *mit* $k \neq 0$ *folgt* $n = m$ *(*Kürzungsregel*).*
(7) *Für beliebige* $k, m, n \in \mathbb{N}$ *gilt*
$$k \cdot (m + n) = k \cdot m + k \cdot n$$
(Distributivgesetz).

Beweis. Siehe Aufgabe 12.24. □

12.4. **Erststufige Peanoaxiome.**

Wir betrachten zwei erststufige Varianten der Dedekind-Peano-Axiome. Dabei wird in der ersten Variante die Nachfolgerfunktion beibehalten und das Induktionsaxiom, das oben für beliebige Teilmengen formuliert wurde, wird durch ein Induktionsaxiom für die in der Sprache erster Stufe formulierbaren Ausdrücke ersetzt. Das Induktionsaxiom gilt somit lediglich für Teilmengen, die in der gegebenen Sprache charakterisierbar sind. Man spricht vom *Induktionsschema*, da es sich nicht um ein einzelnes Axiom handelt, sondern um eine ganze Familie von Axiomen.

Axiom 12.10. Die *Peano-Axiome für die Nachfolgerfunktion in der ersten Stufe* werden (in der Sprache L zur Symbolmenge mit einer Konstanten 0 und einem einstelligen Funktionssymbol N) folgendermaßen definiert.

(1) $\forall x(\neg(Nx = 0))$.
(2) $\forall x \forall y((Nx = Ny) \to (x = y))$.
(3) Für jeden Ausdruck α von L mit einer freien Variablen x gilt

$$\alpha\frac{0}{x} \wedge \forall x \left(\alpha \to \alpha\frac{Nx}{x}\right) \to \forall x \alpha\,.$$

Aus der obigen zweitstufigen Formulierung der Axiomatik, die nur die Nachfolgerabbildung verwendet, kann man in jedem Modell in eindeutiger Weise eine Addition und eine Multiplikation definieren. Dafür ist das obige erststufige Axiomensystem zu schwach. Stattdessen werden wir unter der *Peano-Arithmetik* das folgende Axiomensystem verstehen, das mit zwei Konstanten 0 und 1 und zwei zweistelligen Operationen + und · auskommt. Die Nachfolgerfunktion ist dann durch $Nx = x + 1$ definiert und es braucht dafür kein eigenes Funktionssymbol.

Axiom 12.11. Die *Peano-Axiome für Addition und Multiplikation in der ersten Stufe* werden (in der Sprache L^{Ar} zur Symbolmenge mit den beiden Konstanten 0 und 1 und zwei zweistelligen Funktionssymbolen + und ·) folgendermaßen definiert.

(1) $\forall x(\neg(x + 1 = 0))$.
(2) $\forall x \forall y((x + 1 = y + 1) \to (x = y))$.
(3) $\forall x(x + 0 = x)$.
(4) $\forall x \forall y(x + (y + 1) = (x + y) + 1))$.
(5) $\forall x(x \cdot 0 = 0)$.
(6) $\forall x \forall y(x \cdot (y + 1) = (x \cdot y) + x)$.
(7) Für jeden Ausdruck α von L^{Ar} mit einer freien Variablen x gilt

$$\alpha\frac{0}{x} \wedge \forall x \left(\alpha \to \alpha\frac{x+1}{x}\right) \to \forall x \alpha\,.$$

Die Axiome (1), (2) und (7) entsprechen dabei direkt den Nachfolgeraxiomen von oben. Die Axiome (3) und (4) spiegeln die Grundregeln in der zweistufigen Peano-Arithmetik für die rekursive Definition der Addition wider, und die Axiome (5) und (6) entsprechen den Grundregeln für die rekursive Definition der Multiplikation. Diese Axiome gelten für die (zweitstufig festgelegten) natürlichen Zahlen. Anders als bei der obigen zweitstufigen Axiomatik gibt es aber von $\mathbb{N}$ verschiedene Modelle (nicht Standard-Arithmetiken), die die erststufige Peano-Arithmetik erfüllen. Dies ist aber kein „zufälliges“ Defizit der gewählten Axiomatik, sondern dahinter verbirgt sich eine grundsätzliche Schwäche der Sprache erster Stufe, die durch die Gödelschen Unvollständigkeitssätze präzisiert werden wird.

12. Arbeitsblatt

12.1. Übungsaufgaben.

Aufgabe 12.1. Erläutere Vor- und Nachteile des axiomatischen Aufbaus der Mathematik.

Aufgabe 12.2. Definiere auf der Menge der Wörter zum einelementigen Alphabet $A = \{|\}$ ein Dedekind-Peano-Modell. Worauf beruht die Gültigkeit der Dedekind-Peano-Axiome?

Aufgabe 12.3. Zeige ausgehend von den Dedekind-Peano-Axiomen, dass jedes Element $n \in \mathbb{N}$, $n \neq 0$, einen Vorgänger besitzt.

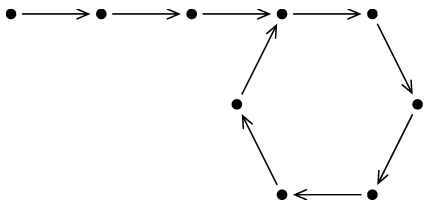
Aufgabe 12.4. Sei $\mathbb{N}$ die Menge der natürlichen Zahlen und $n \in \mathbb{N}$. Zeige, dass die Menge

$$\mathbb{N}_{\geq n} = \{x \in \mathbb{N} | \, x \geq n\}$$

ebenfalls die Dedekind-Peano-Axiome (mit welchem ausgezeichneten Element und mit welcher Nachfolgerabbildung?) erfüllt.

Aufgabe 12.5. Man gebe Beispiele $(M, 0, ')$ für Mengen mit einem ausgezeichneten Element $0 \in M$ und einer Abbildung $' \colon M \to M$ an, die je zwei der Dedekind-Peano-Axiome erfüllen, aber nicht das dritte.

Aufgabe 12.6. Es sei $N_1 = (\mathbb{N}, 0, \prime)$ und es sei N_2 die unten angegebene Menge mit dem Startsymbol oben links und der durch die Pfeile ausgedrückten Nachfolgerabbildung. An welcher Stelle bricht der Beweis von Satz 12.3 in dieser Situation zusammen?



Aufgabe 12.7. Berechne im Strichsystem

$$||||||||||| + ||||||$$

allein unter Verwendung des Umlegungsprinzips.

Aufgabe 12.8. Wir zählen

heute, morgen, übermorgen, überübermorgen, überüberübermorgen, ...

und wollen mit diesen Zahlen Addieren.

(1) Welche alltagssprachliche Formulierung besitzt die Addition in diesem Zählmodell?
(2) Welche sprachlichen Formulierungen drücken aus, das heute das neutrale Element der Addition ist.
(3) Was ist morgen plus morgen?
(4) Was ist übermorgen plus übermorgen?
(5) Was ist überübermorgen plus überüberübermorgen?

Aufgabe 12.9.*

Wir zählen

ich, Mama, Oma, Uroma, Ururoma, ...

(1) Was ist die Mama der Urururoma?
(2) Was ist die Uroma der Uroma?
(3) Was ist die Oma der Oma der Oma?
(4) Was ist das ich der Uroma der Ururoma?

Aufgabe 12.10.*

Es sei $(\mathbb{N}, 0, ')$ ein Dedekind-Peano-Modell der natürlichen Zahlen. Zeige, dass die Addition durch die Bedingungen

$$x + 0 = x \text{ für alle } x \in \mathbb{N} \text{ und } x + y' = (x + y)' \text{ für alle } x, y \in \mathbb{N}$$

eindeutig bestimmt ist.

Aufgabe 12.11. Zeige, dass die Addition auf den natürlichen Zahlen kommutativ und assoziativ ist und dass die Abziehregel (d.h., dass aus $n + k = m + k$ für ein k stets $n = m$ folgt) gilt.

Aufgabe 12.12. Es seien N_1 und N_2 Dedekind-Peano-Modelle der natürlichen Zahlen. Es sei

$$\varphi\colon\ N_1 \longrightarrow N_2$$

der eindeutig bestimmte Isomorphismus mit $\varphi(0_1) = 0_2$ und $\varphi(n') = (\varphi(n))'$ für alle $n \in N_1$. Zeige, dass φ die Addition respektiert, dass also

$$\varphi(m + n) = \varphi(m) + \varphi(n)$$

für alle $m, n \in N_1$ gilt.

Aufgabe 12.13. Wie verhält sich die über die Nachfolgerbeziehung eingeführte Addition auf den natürlichen Zahlen (das *Umlegungsmodell*) zu dem *Vereinigungsmodell*, dass die Summe $a+b$ zweier natürlichen Zahlen sich als Anzahl von Objekten (Äpfel) ergibt, wenn man eine Menge von a Objekten und eine Menge von (dazu disjunkten) b Objekten zusammenschmeißt.

Aufgabe 12.14. Begründe, dass die Addition von natürlichen Zahlen im Dezimalsystem (das *schriftliche Addieren*) das Umlegungsprinzip respektiert und auch die 0 richtig verarbeitet. Schließe daraus, dass die schriftliche Addition korrekt ist.

Aufgabe 12.15. Sei $(\mathbb{N}, 0, ')$ ein Dedekind-Peano-Modell der natürlichen Zahlen. Zeige, dass die Multiplikation durch die Bedingungen

$$x \cdot 0 = 0 \text{ für alle } x \in \mathbb{N} \text{ und } x \cdot y' = x \cdot y + x \text{ für alle } x, y \in \mathbb{N}$$

eindeutig bestimmt ist.

Aufgabe 12.16. Definiere auf einem Dedekind-Peano-Modell $(\mathbb{N}, 0, ')$ für die natürlichen Zahlen die Abbildung $Q\colon\ \mathbb{N} \to \mathbb{N}$ rekursiv durch die Bedingungen (die Addition sei mit den wesentlichen Eigenschaften etabliert)

$$Q(0) \ = \ 0$$

und

$$Q(n') \ = \ Q(n) + n + n + 1.$$

Zeige

$$Q(n) \ = \ n \cdot n.$$

Aufgabe 12.17.*

(1) Bestimme die kleinste natürliche Zahl, die größer als die ersten drei Quadratzahlen ist.
(2) Beschreibe die Bedingung (und zwar so, dass die Bedingung erkennbar ist) aus (1) durch einen prädikatenlogischen arithmetischen Ausdruck (also mit dem Symbolalphabet $+, \cdot, 0, 1$ und Variablen) in der einen freien Variablen x.
(3) Beschreibe das Ergebnis aus (1) durch einen einfachen prädikatenlogischen Ausdruck in der einen freien Variablen x.

Aufgabe 12.18. Wir definieren auf $\mathbb{N}_+$ eine neue Relation R durch folgende Vorschrift: Für zwei Zahlen $n, m \in \mathbb{N}_+$ mit $n = 2^k t$ und $m = 2^\ell u$ mit t, u ungerade sei

$$nRm \text{ falls } t < u \text{ gilt oder falls zugleich } t = u \text{ und } k \leq \ell \text{ gilt}$$

(rechts wird auf die natürliche Ordnung in $\mathbb{N}$ Bezug genommen).

(1) Zeige, dass R eine totale Ordnung auf $\mathbb{N}_+$ ergibt und beschreibe exemplarisch diese Ordnung.
(2) Zeige, dass es zu jedem $n \in \mathbb{N}_+$ ein wohldefiniertes Element $n^\star \in \mathbb{N}_+$, $n^\star \neq n$, derart gibt, dass $nRn^\star$ gilt und dass es zwischen n und $n^\star$ keine weiteren Elemente gibt (diese Formulierung ist zu präzisieren).
(3) Erfüllt die Menge $(\mathbb{N}_+, 1, \star)$ die Dedekind-Peano-Axiome?

Aufgabe 12.19. Betrachte die Produktmenge $\mathbb{N} \times \mathbb{N}$ mit der Nachfolgerfunktion

$$(a, b)' := (a, b')$$

und der sogenannten *lexikographische Ordnung*, für die

$$(a_1, b_1) \leq (a_2, b_2)$$

genau dann gilt, wenn $a_1 < a_2$ oder $a_1 = a_2$ und $b_1 \leq b_2$ ist. Zeige folgende Aussagen.

(1) Es handelt sich um eine totale Ordnung.
(2) Es ist
$$x' \geq x$$
für alle $x \in \mathbb{N} \times \mathbb{N}$.
(3) $(0, 0)$ ist das kleinste Element.
(4) Es liegt eine Wohlordnung (nach unten) vor.
(5) Diese Menge mit der Nachfolgerfunktion erfüllt nicht das Dedekind-Peano-Induktionsaxiom

Aufgabe 12.20. Es sei M die disjunkte Vereinigung aus $\mathbb{N}$ und aus $\mathbb{Z}$.[18] Wir definieren auf M eine Nachfolgerfunktion, die auf den beiden Bestandteilen durch den üblichen Nachfolger gegeben ist (also durch $+1$), und wir betrachten die $0 \in \mathbb{N}$ als die Null von M.

a) Zeige, dass M die ersten beiden Axiome aus den erststufigen Peano-Axiomen für die Nachfolgerfunktion erfüllt.

b) Zeige, dass es keine Addition auf M gibt, die mit den Additionen auf $\mathbb{N}$ und auf $\mathbb{Z}$ übereinstimmt und für die die Abziehregel gilt.

[18] Dabei muss man darauf achten, die Elemente aus $\mathbb{N}$ nicht mit denen aus $\mathbb{Z}_{\geq 0}$ zu verwechseln. Beispielsweise kann man die Elemente einerseits mit 5 und andererseits mit $5_{\mathbb{Z}}$ bezeichnen.

c) Gilt das erststufige Induktionsaxiom (formuliert für die Nachfolgerfunktion)?[19]

Aufgabe 12.21. Im Kalkül der Prädikatenlogik sei $\vdash \alpha \to \beta$ ableitbar. Zeige, dass dann auch

$$\vdash \exists x\alpha \to \exists x\beta$$

ableitbar ist.

Aufgabe 12.22. Zeige, dass in der Prädikatenlogik

$$\vdash \exists x\alpha \leftrightarrow \exists x\neg\neg\alpha$$

ableitbar ist.

12.2. **Aufgaben zum Abgeben.**

Aufgabe 12.23. (5 Punkte)

Sei $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ das Ziffernalphabet. Definiere die Teilmenge $N \subseteq A^*$, die aus den korrekt gebildeten Zifferndarstellungen einer natürlichen Zahl besteht. Definiere auf N eine Nachfolgerabbildung und zeige, dass N zu einem Dedekind-Peano-Modell wird. Worauf beruht die Gültigkeit der Dedekind-Peano-Axiome?

Aufgabe 12.24. (7 Punkte)

Sei $(\mathbb{N}, 0, ')$ ein Dedekind-Peano-Modell der natürlichen Zahlen mit der in Definition 12.7 festgelegten Multiplikation. Zeige die folgenden Aussagen.

(1)
$$0 \cdot n = 0 = n \cdot 0$$
für alle n.

(2)
$$1 \cdot n = n = n \cdot 1$$
für alle n, d.h. $1 = 0'$ ist das neutrale Element für die Multiplikation.

(3)
$$k' \cdot n = k \cdot n + n$$
für alle $n, k \in \mathbb{N}$.

(4) Die Multiplikation ist kommutativ.

(5) Die Multiplikation ist assoziativ.

(6) Aus einer Gleichung $n \cdot k = m \cdot k$ mit $k \neq 0$ folgt $n = m$ (*Kürzungsregel*).

[19] Diese Aufgabe ist wohl schwierig.

(7) Für beliebige $k, m, n \in \mathbb{N}$ gilt

$$k \cdot (m + n) = k \cdot m + k \cdot n$$

(Distributivgesetz).

Aufgabe 12.25. (3 Punkte)

Es seien N_1 und N_2 Dedekind-Peano-Modelle der natürlichen Zahlen. Es sei

$$\varphi\colon\ N_1 \longrightarrow N_2$$

der eindeutig bestimmte Isomorphismus mit $\varphi(0_1) = 0_2$ und $\varphi(n') = (\varphi(n))'$ für alle $n \in N_1$. Zeige, dass φ die Multiplikation respektiert, dass also

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

für alle $m, n \in N_1$ gilt.

Aufgabe 12.26. (3 Punkte)

Es sei $(N, 0, ')$ ein Dedekind-Peano-Modell der natürlichen Zahlen. Zeige, dass das erststufige Axiomenschema für die Induktion in N gilt.

13. Vorlesung - Peano-Arithmetik

13.1. **Erststufige Peano-Arithmetik - Folgerungen und Ableitungen.**

Die in der zweiten Stufe formulierten Dedekind-Peano-Axiome legen die natürlichen Zahlen bis auf Isomorphie fest, wie wir in der letzten Vorlesung gesehen haben. In dieser Vorlesung geben wir einen Einblick, welche wichtigen Eigenschaften der natürlichen Zahlen bereits aus den erststufigen Peano-Axiomen (formuliert mit der arithmetischen Symbolmenge $\{0, 1, +, \cdot\}$) folgen. Für Mengen, die diese Axiome erfüllen, führen wir einen eigenen Namen ein.

Definition 13.1. Eine Menge M mit zwei ausgezeichneten Elementen 0 und 1 und zwei Verknüpfungen $+$ und $\cdot$ heißt *Peano-Halbring*, wenn diese Strukturen die erststufigen Peano-Axiome erfüllen.

Neben der Menge der natürlichen Zahlen $\mathbb{N}$ gibt es weitere Peano-Halbringe, die allerdings nicht einfach zu konstruieren sind. Die Existenz solcher Modelle ergibt sich als Korollar aus dem Vollständigkeitssatz, siehe Aufgabe 15.11. Nach Aufgabe 13.33 enthält jeder Peano-Halbring ein Modell der natürlichen Zahlen als Teilmenge. Die Elemente dieser Teilmengen sind nicht mit erststufigen Ausdrücken, die aus den ersstufigen Peano-Axiomen folgen, von den anderen Elementen trennbar.

Wir ziehen einige Folgerungen aus den erststufigen Peano-Axiomen, und zwar argumentieren wir „mathematisch“ (also semantisch). D.h. wir zeigen für einen beliebigen Peano-Halbring (also ein mathematisches Objekt, das die Peano-Axiome erfüllt), dass gewisse Eigenschaften gelten müssen, so wie man aus den Gruppenaxiomen oder den Körperaxiomen gewisse Folgerungen zieht. In der Argumentation stellt man sich also einen Peano-Halbring vor, mit einer zugrunde liegenden Menge, einer Addition und einer Multiplikation u.s.w. Als Beweismittel sind nur die Axiome, die den Begriff eines Peano-Halbringes festlegen, erlaubt. Insbesondere darf man sich *nicht* auf das intendierte Modell, nämlich die natürlichen Zahlen, berufen, da es eben auch andere Peano-Halbringe gibt (obwohl deren Konstruktion schwierig ist). Die Situation ist vergleichbar zur schrittweisen axiomatischen Einführung der reellen Zahlen, wo es darum geht, Eigenschaften aus einer kleinen Menge aus Axiomen zu etablieren, ohne auf die reellen Zahlen selbst Bezug zu nehmen (ein großer Unterschied ist allerdings, dass die Konstruktion der natürlichen Zahlen einfach ist, die der reellen Zahlen aber nicht). Ein wichtiger Unterschied zu anderen mathematischen Konzepten ist, dass mit dem Induktionsschema die Peano-Axiome explizit auf prädikatenlogische Konstruktionen Bezug nehmen.

Wir werden später im Rahmen des Vollständigkeitssatzes sehen, dass die hier gezogenen Folgerungen auch aus den Peano-Axiomen ableitbar sind. Der formale Nachweis der Ableitbarkeit ist im Allgemeinen, verglichen mit einem „natürlichen Beweis“, deutlich umständlicher. Wir werden gelegentlich Ableitungsbeweise andeuten.

Die grundlegende allgemeine Struktur, die aus den Peano-Axiomen ableitbar ist, ist die eines kommutativen Halbringes (daher auch der Name Peano-Halbring).

Definition 13.2. Ein *kommutativer Halbring* R ist eine Menge mit zwei Verknüpfungen $+$ und $\cdot$ (genannt *Addition* und *Multiplikation*) und mit zwei ausgezeichneten Elementen 0 und 1 derart, dass folgende Bedingungen erfüllt sind:

(1) $(R, +, 0)$ ist ein kommutatives Monoid.
(2) $(R, \cdot, 1)$ ist ein kommutatives Monoid.
(3) Es gilt das *Distributivgesetz*, also

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

für alle $a, b, c \in R$.

Lemma 13.3. *Ein Peano-Halbring ist ein kommutativer Halbring.*

Beweis. Nur die Eigenschaft, dass 0 das neutrale Element (von rechts) der Addition ist, tritt unmittelbar in den Peano-Axiomen auf. Die (erststufig

formulierte) Eigenschaft $\forall x\,(0+x=x)$, also $0+x\;=\;x$ für alle $x\in M$[20] zeigen wir durch Induktion über x. Für $x\;=\;0$ ist dies klar. Sei die Aussage also für ein $x\in M$ bewiesen. Dann ist nach Axiom 12.10 (4) und der Induktionsvoraussetzung

$$0+(x+1)\;=\;(0+x)+1\;=\;x+1.$$

Wir zeigen zunächst, dass das vierte Axiom, also die Eigenschaft $x+(y+1)\;=\;(x+y)+1$, auch gilt, wenn man den ersten Summanden erhöht, also

$$(x+1)+y\;=\;(x+y)+1.$$

Dies zeigen wir (für jedes x) durch Induktion über y. Der Fall $y\;=\;0$ ist klar, da 0 neutrales Element ist. Der Übergang von y nach $y+1$ folgt aus

$$(x+1)+(y+1)\;=\;((x+1)+y)+1\;=\;((x+y)+1)+1\;=\;(x+(y+1))+1,$$

wobei wir das vierte Axiom und die Induktionsvoraussetzung angewendet haben.

Zum Nachweis der Kommutativität der Addition betrachten wir zu festem $y\in M$ die Eigenschaft, dass

$$x+y\;=\;y+x$$

für alle x ist. Dies wird erststufig durch

$$\forall x(x+y)=(y+x)$$

formalisiert, so dass wir also Induktion über y anwenden können. Wir müssen also zeigen, dass diese Eigenschaft für $y\;=\;0$ wahr ist (was stimmt, da 0 von beiden Seiten neutrales Element ist) und dass sie, wenn sie für ein y gilt, dann auch für $y+1$ gilt. Dies folgt aber aus

$$x+(y+1)\;=\;(x+y)+1\;=\;(y+x)+1\;=\;(y+1)+x,$$

wobei wir das Axiom 12.10 (4), die Induktionsvoraussetzung und einmal die Vorüberlegung angewendet haben. Für die weiteren Eigenschaften siehe Aufgabe 13.15, Aufgabe 13.16 und Aufgabe 13.34. □

Lemma 13.4. *In einem Peano-Halbring M gilt für jedes $x\in M$ die Eigenschaft: Entweder ist $x\;=\;0$ oder es gibt ein $u\in M$ mit $x\;=\;u+1$.*

Beweis. Beide Teilaussagen können wegen des ersten Peano-Axioms nicht zugleich wahr sein. Es geht also um die Aussage

$$\forall x\,((x=0)\vee(\exists u x=u+1))\;,$$

die wir durch Induktion beweisen. Der Induktionsanfang für $x\;=\;0$ ist durch den linken Bestandteil gesichert. Sei also die Aussage für ein gewisses x schon

[20] Wir bezeichnen hier und im Folgenden die Variable und das ihr in einer Belegung zugewiesene Element mit dem gleichen Symbol.

bewiesen, und sie ist für $x+1$ zu beweisen. Bei $x = 0$ ist $x+1 = 0+1$, so dass man $u = 0$ nehmen kann. Bei $x = u+1$ ist

$$x+1 = (u+1)+1$$

und somit kann man $u+1$ nehmen. □

Lemma 13.5. *In einem Peano-Halbring M gilt die folgende Abzieh- bzw. Kürzungsregel.*

(1) *Für alle $x, y, z \in M$ folgt aus $x+z = y+z$ die Gleichheit $x = y$.*
(2) *Für alle $x, y, z \in M$ mit $z \neq 0$ folgt aus $xz = yz$ die Gleichheit $x = y$.*

Beweis. Seien $x, y \in M$ fixiert. Wir betrachten die Aussage, dass für alle z die angegebene Eigenschaft gilt, also dass aus $x+z = y+z$ schon $x = y$ folgt. Diese Eigenschaft ist erststufig formulierbar. Sie gilt für $z = 0$ nach Axiom 12.10 (3). Nehmen wir an, sie gilt für ein bestimmtes, aber beliebiges z. Wir müssen die Aussage für $z+1$ zeigen. Es ist also

$$x+(z+1) = y+(z+1).$$

Aufgrund von Axiom 12.10 (4) gilt daher

$$(x+z)+1 = (y+z)+1$$

und nach Axiom 12.10 (2) folgt

$$x+z = y+z.$$

Die Induktionsvoraussetzung liefert

$$x = y.$$

Für die Kürzungsregel siehe Aufgabe 13.35. □

In jedem Peano-Halbring lässt sich durch

$$x \geq y \text{ genau dann, wenn es ein } z \text{ gibt mit } x = y+z$$

eine Relation definieren, die sich einfach als eine totale Ordnung nachweisen lässt. Wir schreiben $x = y$ als Abkürzung für $x \geq y$ und $x \neq y$.

Lemma 13.6. *In einem Peano-Halbring M ist $\geq$ eine totale Ordnung mit 0 als kleinstem Element. Für jedes $x \in M$, $x \neq 0$, ist*

$$x \geq 1.$$

Die Ordnung ist mit der Addition und der Multiplikation verträglich.

Beweis. Die Reflexivität folgt direkt aus Axiom 12.10 (3). Die Transitivität ergibt sich unmittelbar, da ja $x \geq y$ und $y \geq z$ bedeutet, dass es $u, v \in M$ mit $x = y+u$ und mit $y = z+v$ gibt, woraus sich

$$x = z+v+u,$$

also $x \geq z$ ergibt. Zum Beweis der Antisymmetrie sei $x \geq y$ und $y \geq x$, also $x = y + u$ und $y = x + v$ mit gewissen $u, v \in M$. Dann gilt auch

$$x = x + u + v.$$

Aus der Abziehregel folgt

$$0 = u + v.$$

Wären u, v nicht beide 0, so würde nach Lemma 13.4 beispielsweise $u = t+1$ gelten und damit

$$0 = (t + v) + 1,$$

ein Widerspruch zu Axiom 12.10 (1). Dass 0 das kleinste Element ist, folgt direkt aus Axiom 12.10 (3). Die Verträglichkeit mit der Addition ergibt sich direkt, die mit der Multiplikation folgt aus dem Distributivgesetz. Bei $x \neq 0$ ist $x = t+1$ nach der Vorgängereigenschaft und daher $x \geq 1$. Zum Nachweis der totalen Ordnung seien $x, y \in M$ gegeben. Wir beweisen die Eigenschaft, dass zu festem x für alle y die Eigenschaft $(x \geq y) \vee (y \geq x)$ gilt, durch Induktion über y. Bei $y = 0$ ist dies klar. Sei die Aussage nun für ein y bewiesen. Bei $y \geq x$ gilt erst recht $y+1 \geq x$. Sei also $x \geq y$, wobei wir uns direkt auf $x > y$ beschränken können. Dies bedeutet $x = y + u$ und $u \neq 0$ und somit $u \geq 1$. Also ist $x \geq y + 1$. □

Satz 13.7. *In einem Peano-Halbring M erfüllt $\geq$ das* Wohlordnungsprinzip für erststufige Ausdrücke*. D.h. für jeden Ausdruck $\alpha \in L^{\{0,1,+,\cdot\}}$ in der freien Variablen x gilt*

$$\exists x \alpha \to \exists y \left(\alpha \frac{y}{x} \wedge \forall x \left(\alpha \to x \geq y \right) \right) .$$

Beweis. Wir betrachten den Ausdruck

$$\forall u \left(\exists x \left(\alpha \wedge x \leq u \right) \to \exists y \left(\alpha \frac{y}{x} \wedge \forall x \left(\alpha \to x \geq y \right) \right) \right)$$

und wollen zeigen, dass er in jedem Peano-Halbring gilt. Dies zeigen wir unter Verwendung des Induktionsaxioms und fixieren einen Peano-Halbring M. Für $u = 0$ ist die Aussage richtig, da dann, falls der Vordersatz $\exists x \left(\alpha \wedge x \leq 0 \right)$ gilt, dann insbesondere $\alpha \frac{0}{x}$ in M gilt und man im Nachsatz

$$y = 0$$

nehmen kann, da ja 0 das kleinste Element ist. Zum Beweis des Induktionsschrittes müssen wir die Gültigkeit von

$$\forall u \left(\left(\exists x \left(\alpha \wedge x \leq u \right) \to \exists y \left(\alpha \frac{y}{x} \wedge \forall x \left(\alpha \to y \leq x \right) \right) \right) \to \left(\exists x \left(\alpha \wedge x \leq u + 1 \right) \to \exists y \left(\alpha \frac{y}{x} \wedge \forall x \left(\alpha \to x \geq y \right) \right) \right) \right)$$

zeigen. Sei also die Aussage für ein bestimmtes $u \in M$ (also der Vordersatz links) im Modell wahr. Wir müssen dann den Nachsatz, also die Aussage für $u + 1$ als wahr erweisen. Es gelte also

$$\exists x \left(\alpha \wedge x \leq u + 1 \right) .$$

Wenn sogar $\exists x\,(\alpha \wedge x \leq u)$ gilt, so sind wir nach Induktionsvoraussetzung fertig. Es gelte diese Aussage also nicht. Das bedeutet einerseits, dass der Ausdruck α für kein Element aus M gilt, das kleiner als oder gleich u ist, und andererseits, dass α gilt, wenn x durch $u+1$ interpretiert wird. Somit gilt der Ausdruck

$$\alpha\frac{u+1}{x} \wedge \forall x\,(\alpha \to x \geq u+1)$$

und damit

$$\exists y\left(\alpha\frac{y}{x} \wedge \forall x\,(\alpha \to x \geq y)\right).$$

□

Die Zahlentheorie beginnt mit der Division mit Rest.

Satz 13.8. *Sei M ein Peano-Halbring und $d \geq 1$. Dann gibt es zu jedem $m \in M$ eindeutig bestimmte $q, r \in M$ mit*[21] *r, $r < d$, und mit*

$$m = qd + r.$$

Beweis. Wir betrachten zum Nachweis der Existenz die erststufige Aussage

$$\forall d\,(d \geq 1 \to \exists q \exists r\,(m = dq + r \wedge r \leq d \wedge \neg r = d)),$$

die m als einzige freie Variable besitzt. Für $m = 0$ ist die Aussage mit $q = 0$ und

$$r = 0$$

richtig. Zum Beweis des Induktionsschritts sei

$$m = dq + r$$

mit den angegebenen Eigenschaften. Daher ist

$$m + 1 = dq + r + 1.$$

Wenn $r' = r + 1$ kleiner als d ist, so erfüllen q, r' die geforderten Eigenschaften. Bei $r + 1 \geq d$ muss $r + 1 = d$ gelten. Dann ist

$$m + 1 = dq + r + 1 = dq + d = d(q + 1),$$

so dass $q + 1, 0$ das Geforderte leisten. Für die Eindeutigkeit siehe Aufgabe 13.20. □

Mit der Division mit Rest kann man weitere, aus der elementaren Zahlentheorie bekannte Gesetzmäßigkeiten in jedem Peano-Halbring etablieren, wie die Existenz des größten gemeinsamen Teilers, des kleinsten gemeinsamen Vielfaches, u.s.w. Für die Teilbarkeitsbeziehung schreiben wir $a|b$. Gemeint ist damit, dass es ein Element c mit $b = ac$ gibt.

[21] Bei der üblichen Formulierung der Division mit Rest über $\mathbb{Z}$ schreibt man $0 \leq r < d$, doch ist dies hier überflüssig, da es keine negativen Zahlen in einem Peano-Halbring gibt.

Beispiel 13.9. Wir betrachten die Teilmenge

$$M \subseteq \mathbb{Z}[V]$$

des Polynomrings in der Variablen V über $\mathbb{Z}$, die aus dem Nullpolynom und allen Polynomen $P \in \mathbb{Z}[V]$ besteht, deren Leitkoeffizient zu $\mathbb{N}_+$ gehört. Die Menge M umfasst die natürlichen Zahlen (als Polynome vom Grad 0 mit nichtnegativem Leitkoeffizient) und sie ist abgeschlossen unter Addition und Multiplikation. Es gelten die erststufigen Peano-Axiome (1)-(6), wie man direkt sieht. Auch gilt die Vorgängereigenschaft, d.h. jedes von 0 verschiedene Element besitzt einen eindeutigen Vorgänger (dies ist der Grund, warum wir abgesehen für den Leitkoeffizienten auch negative Koeffizienten zulassen), siehe Aufgabe 13.30. Dagegen gilt das erststufige Induktionsschema nicht, und die natürlichen Zahlen lassen sich als Teilmenge von M erststufig charakterisieren. Zur Vereinfachung der folgenden Formulierung definieren wir die $\leq$-Relation durch

$$x \geq y \text{ genau dann, wenn } \exists z(x = y + z)\,,$$

dies ist eine totale Ordnung nach Aufgabe 14.25. Damit setzen wir

$$\alpha(x) = \forall m \forall d((m \leq x \wedge d \leq x \wedge d \geq 1) \to \exists q \exists r(m = qd + r \wedge r < d)).$$

Dies ist ein Ausdruck mit der einzigen freien Variablen x, der inhaltlich besagt, dass die Division mit Rest gilt, wenn die beteiligten Eingangsdaten m und d unterhalb von x liegen. Dieser Ausdruck gilt innerhalb der natürlichen Zahlen (also für $x \in \mathbb{N}$). Dagegen gilt sie in M nicht, und zwar gilt sie dort nur für die natürlichen Zahlen. Für ein Polynom x aus M vom Grad ≥ 1 kann man nämlich $m = x = a_s V^s + \cdots + a_1 V + a_0$ und für d eine Primzahl (aus $\mathbb{N}$) nehmen, die den Leitkoeffizienten a_s von m nicht teilt. Die Differenz zwischen x und einem jeden Vielfachen von d ist ein nichtkonstantes Polynom, daher gilt die Divsion mit Rest dafür nicht.

Wir betrachten nun die Induktionsversion dieser Aussage, also

$$\alpha\frac{0}{x} \wedge \forall x \left(\alpha \to \alpha\frac{x+1}{x}\right) \to \forall x \alpha\,.$$

Der Vordersatz gilt in M, da die beschriebene Eigenschaft genau für die natürlichen Zahlen und für alle anderen Elemente nicht gilt, und daher genau dann gilt, wenn sie auch für den Nachfolger gilt (die echten Polynome sind nicht als Nachfolger von natürlichen Zahlen erreichbar). Da der Nachsatz nicht gilt, ergibt sich, dass die Gesamtaussage nicht gilt.

13. Arbeitsblatt

13.1. Übungsaufgaben.

Aufgabe 13.1.*

Zeige, dass in einem kommutativen Halbring die Beziehung $0 \cdot 0 = 0$ gilt.

Aufgabe 13.2. Es sei R ein kommutativer Halbring. Zeige, dass

$$0 \cdot (1 + 1 + \cdots + 1) = 0$$

ist (mit einer beliebig langen Summe von Einsen).

Aufgabe 13.3.*

Man definiere auf der dreielementigen Menge $\{0, 1, u\}$ die Struktur eines kommutativen Halbringes, bei dem $0 \cdot u \neq 0$ gilt.

Aufgabe 13.4. Da man die natürlichen Zahlen zum Zählen von endlichen Mengen nimmt, es aber auch unendliche Mengen gibt, denkt sich Gabi Hochster, dass man die natürlichen Zahlen $\mathbb{N}$ um ein weiteres Symbol ∞ (sprich unendlich) erweitern sollte. Diese neue Menge bezeichnet sie mit $\mathbb{N}^\infty$. Sie möchte die Ordnungsstruktur, die Addition und die Multiplikation der natürlichen Zahlen auf ihre neue Menge ausdehnen, und zwar so, dass möglichst viele vertraute Rechengesetze erhalten bleiben.

(1) Wie legt Gabi die Ordnung fest?
(2) Wie legt sie die Nachfolgerabbildung fest? Gelten die Peano-Axiome?
(3) Wie legt sie die Addition fest? Sie möchte ja nur mit dem einzigen neuen Symbol ∞ arbeiten.
(4) Gilt mit dieser Addition die Abziehregel?
(5) Zuerst denkt sie an die Festlegung

$$0 \cdot \infty = 1,$$

doch dann stellt sie fest, dass sich das mit dem Distributivgesetz beißt. Warum?
(6) Gabi möchte nun, dass für die neue Menge die Eigenschaften aus Satz 8.13 (Grundkurs Mathematik (Osnabrück 2016-2017)) und aus Satz 9.4 (Grundkurs Mathematik (Osnabrück 2016-2017)) nach wie vor gelten. Wie legt sie die Verknüpfungen fest?
(7) Handelt es sich bei $\mathbb{N}^\infty$ mit den Festlegungen aus Teil (6) um einen kommutativen Halbring?
(8) Gilt die Kürzungsregel?

Aufgabe 13.5.*

Es sei $R = \mathfrak{P}(M)$ die Potenzmenge zu einer Menge M. Zeige, dass R mit der Vereinigung $\cup$ als Addition und der leeren Menge als 0 und mit dem Durchschnitt $\cap$ als Multiplikation und der Gesamtmenge M als 1 ein kommutativer Halbring ist.

Aufgabe 13.6. Sei R ein kommutativer Halbring und $f, a_i, b_j \in R$. Zeige die folgenden Gleichungen:

$$\sum_{i=0}^{n} a_i f^i + \sum_{j=0}^{m} b_j f^j = \sum_{k=0}^{\max(n,m)} (a_k + b_k) f^k$$

und

$$\left(\sum_{i=0}^{n} a_i f^i\right) \cdot \left(\sum_{j=0}^{m} b_j f^j\right) = \sum_{k=0}^{n+m} c_k f^k \text{ mit } c_k = \sum_{r=0}^{k} a_r b_{k-r}\,.$$

Aufgabe 13.7.*

Beweise das *allgemeine Distributivgesetz* für einen kommutativen Halbring.

Aufgabe 13.8.*

Beweise die folgende Form des allgemeinen Distributivgesetzes für einen kommutativen Halbring R durch Induktion über k, wobei der Fall $k = 2$ verwendet werden darf (dabei sind $n_1, \ldots, n_k$ natürliche Zahlen und $a_{j,i} \in R$).

$$\left(\sum_{i_1=1}^{n_1} a_{1,i_1}\right) \cdot \left(\sum_{i_2=1}^{n_2} a_{2,i_2}\right) \cdots \left(\sum_{i_k=1}^{n_k} a_{k,i_k}\right) = \sum_{(i_1,i_2,\ldots,i_k) \in \{1,\ldots,n_1\} \times \{1,\ldots,n_2\} \times \cdots \times \{1,\ldots,n_k\}} a_{1,i_1} \cdot a_{2,i_2} \cdots a_{k,i_k}.$$

Aufgabe 13.9. Zeige, dass in einem kommutativen Halbring durch

$$x \geq y \text{ genau dann, wenn } \exists z(x = y + z)$$

eine reflexive und transitive Relation gegeben ist. Zeige durch geeignete Beispiele, dass diese weder antisymmetrisch noch total sein muss.

In den folgenden Aufgaben besprechen wir Teilbarkeitskonzepte für einen kommutativen Halbring.

Eine Nichteinheit p in einem kommutativen Halbring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Diese Eigenschaft charakterisiert im Halbring $\mathbb{N}$ gerade die Primzahlen.

Eine Nichteinheit $p \neq 0$ in einem kommutativen Halbring R heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt es einen der Faktoren.

Aufgabe 13.10. Formalisiere in der (erststufigen) Sprache der kommutativen Halbringe die Konzepte Einheit, Teilt, irreduzibel, Primelement.

Aufgabe 13.11. Es sei R ein kommutativer Halbring, der die Kürzungsregel erfüllt. Zeige, dass ein Primelement stets irreduzibel ist.

Aufgabe 13.12. Zeige, dass für $\mathbb{N}$ die Konzepte Primelement und irreduzibel zusammenfallen.

Aufgabe 13.13. Man gebe Beispiele für kommutative Halbringe, in denen die Konzepte Primelement und irreduzibel auseinanderfallen.

Aufgabe 13.14. Gilt für die Vereinigung von Mengen die „Abziehregel“, d.h. kann man aus $A \cup C = B \cup C$ auf $A = B$ schließen?

Aufgabe 13.15. Zeige, dass in einem Peano-Halbring die Addition assoziativ ist.

Aufgabe 13.16. Zeige, dass in einem Peano-Halbring die Multiplikation kommutativ und assoziativ ist und dass 1 das neutrale Element ist.

Aufgabe 13.17.*

Man gebe ein Beispiel für einen kommutativen Halbring, der kein Peano-Halbring ist.

Aufgabe 13.18. Zeige, dass in einem Peano-Halbring die Ordnungsrelation mit der Addition und der Multiplikation verträglich ist.

Aufgabe 13.19. Zeige, dass in einem Peano-Halbring der Ausdruck

$$\forall x \forall y \, (x \leq y \wedge y \leq x + 1 \rightarrow (y = x \vee y = x + 1))$$

gilt.

Aufgabe 13.20.*

Zeige, dass in einem Peano-Halbring M zu $d \geq 1$ die Division mit Rest eindeutig ist.

Aufgabe 13.21. Zeige, dass in einem Peano-Halbring das *Lemma von Bezout* in der Form gilt, dass es zu zwei teilerfremden (das ist zu definieren) Elementen x, y Elemente a, b mit

$$ax = 1 + by$$

gibt.

Aufgabe 13.22. Zeige, dass in einer Struktur, die die Peano-Axiome für den Nachfolger erfüllt, die Aussage

$$\forall x \, (x = 0 \vee x = N0 \vee \exists y \, (NNy = x))$$

gilt.

Aufgabe 13.23.*

Zeige, dass die Vorgängereigenschaft

$$\forall x \, (x \neq 0 \to \exists y (x = Ny))$$

aus der Menge der Peano-Axiome für den Nachfolger folgt.

Aufgabe 13.24. Zeige, dass die Vorgängereigenschaft

$$\forall x \, (x \neq 0 \to \exists y (x = y + 1))$$

aus der Menge der erststufigen Peano-Axiome ableitbar ist.

Aufgabe 13.25. Zeige, dass die Division mit Rest aus der Menge der erststufigen Peano-Axiome ableitbar ist.

Aufgabe 13.26. Es sei M die disjunkte Vereinigung aus zwei Kopien von $\mathbb{N}$ zusammen mit dem ausgezeichneten Element $0 = 0_1$ (aus der ersten Kopie) und der Abbildung N, die auf beiden Kopien die übliche Nachfolgerabbildung ist. Welche der Peano-Axiome für den Nachfolger gelten für M, welche nicht?

Aufgabe 13.27. Es sei M die disjunkte Vereinigung aus $\mathbb{N}$ und aus $\mathbb{Z}$.[22] Wir definieren auf M eine Nachfolgerfunktion, die auf den beiden Bestandteilen durch den üblichen Nachfolger gegeben ist (also durch $+1$), und wir betrachten die $0 \in \mathbb{N}$ als die Null von M.

a) Zeige, dass M die ersten beiden Axiome aus den erststufigen Peano-Axiomen für die Nachfolgerfunktion erfüllt.

[22]Dabei muss man darauf achten, die Elemente aus $\mathbb{N}$ nicht mit denen aus $\mathbb{Z}_{\geq 0}$ zu verwechseln. Beispielsweise kann man die Elemente einerseits mit 5 und andererseits mit $5_{\mathbb{Z}}$ bezeichnen.

b) Zeige, dass es keine Addition auf M gibt, die mit den Additionen auf $\mathbb{N}$ und auf $\mathbb{Z}$ übereinstimmt und für die die Abziehregel gilt.

c) Gilt das erststufige Induktionsaxiom (formuliert für die Nachfolgerfunktion)?[23]

Aufgabe 13.28. Es sei

$$M = \mathbb{Q}_{\geq 0}$$

die Menge der nichtnegativen rationalen Zahlen mit der 0 und der Abbildung

$$N(x) = x + 1.$$

Welche der Peano-Axiome für den Nachfolger gelten für M, welche nicht?

Aufgabe 13.29.*

Es sei

$$M = \{0\} \cup \mathbb{Q}_{\geq 1}.$$

(1) Zeige, dass M ein kommutativer Halbring ist.
(2) Zeige, dass in M die Relationen

$$a \text{ teilt } b \text{ oder } a = 0$$

und

$$a \leq b \text{ oder } b = 0$$

zueinander äquivalent sind.
(3) Zeige, dass $\frac{6}{5}$ nicht irreduzibel in M ist.
(4) Zeige, dass es in M keine irreduziblen Elemente gibt.
(5) Es sei α die Aussage

$$x = 0 \vee \exists y(x = y + 1)\,.$$

Zeige, dass in M die Aussage

$$\alpha\frac{0}{x} \wedge \left(\alpha \to \alpha\frac{x+1}{x}\right)$$

wahr ist.
(6) Zeige, dass M kein Peano-Halbring ist.

Aufgabe 13.30. Zeige, dass in $M \subseteq \mathbb{Z}[V]$ aus Beispiel 13.9 jedes Element $\neq 0$ einen eindeutig bestimmten Vorgänger besitzt.

[23]Diese Aufgabe ist wohl schwierig.

Aufgabe 13.31. Zeige, dass in der arithmetischen Sprache erster Stufe mit den Konstanten $0, 1$, dem Nachfolgersymbol N und den zweistelligen Funktionssymbolen $+$ und $\cdot$ nur abzählbar viele Teilmengen von $\mathbb{N}$ „adressierbar“ sind und dass daher das zweitstufige Induktionsaxiom der Dedekind-Peano-Axiome nicht in dieser Sprache formulierbar ist.

Aufgabe 13.32. Zeige, dass man für jede Teilmenge $T \subseteq \mathbb{N}$ die arithmetische Sprache erster Stufe um ein einstelliges Relationssymbol R_T und die erststufigen Peano-Axiome um geeignete Axiome ergänzen kann, derart, dass diese neue Axiomatik in der Standardinterpretation $\mathbb{N}$ genau dann gilt, wenn R_T als T interpretiert wird. Man folgere daraus, dass mit überabzählbar vielen Relationssymbolen alle Teilmengen der natürlichen Zahlen „adressierbar“ sind.

(Dies bedeutet aber weder, dass für jede Struktur einer solchen Axiomatik jede Teilmenge adressierbar ist, noch, dass das zweitstufige Induktionsaxiom, das eine Aussage über alle Teilmengen macht, erststufig formulierbar ist).

13.2. **Aufgaben zum Abgeben.**

Aufgabe 13.33. (4 Punkte)

Es sei $\mathbb{N}$ ein Peano-Dedekind-Modell der natürlichen Zahlen und M ein Peano-Halbring. Zeige, dass es eine eindeutig bestimmte Abbildung

$$\varphi\colon\ \mathbb{N} \longrightarrow M$$

mit $\varphi(0) = 0$ und $\varphi(n') = \varphi(n) + 1$ gibt. Zeige ferner, dass φ injektiv ist und die Addition und die Multiplikation respektiert.

Aufgabe 13.34. (4 Punkte)

Zeige, dass in einem Peano-Halbring das Distributivgesetz gilt.

Aufgabe 13.35. (3 Punkte)

Zeige, dass in einem Peano-Halbring die Kürzungseigenschaft gilt, d.h. dass aus $xz = yz$ mit $z \neq 0$ die Gleichheit $x = y$ folgt.

Aufgabe 13.36. (4 Punkte)

Zeige, dass $\mathbb{R}_{\geq 0}$ mit $0, 1$ und der natürlichen Addition und Multiplikation die ersten sechs Peano-Axiome erfüllt, aber nicht das Induktionsaxiom.

13.3. **Die Aufgabe zum Aufgeben.**

Aufgabe 13.37. (5 Punkte)

Man gebe einen Ausdruck $\alpha \in L^{\mathrm{Ar}}$ aus der arithmetischen Sprache erster Stufe (also mit $0, 1, +, \cdot$) mit einer freien Variablen x an, der über den ganzen Zahlen $\mathbb{Z}$ folgende Eigenschaft besitzt: Es gilt

$$\mathbb{Z}\frac{m}{x} \vDash \alpha$$

genau dann, wenn $m \in \mathbb{N}$ ist (der Ausdruck gilt also genau für die natürlichen Zahlen).

14. Vorlesung - Satz von Henkin

14.1. **Die Korrektheit des Ableitungskalküls.**

Im Laufe der Einführung des syntaktischen Prädikatenkalküls haben wir gesehen, dass die in ihm ableitbaren Ausdrücke allgemeingültig sind, dass also sämtliche durch den Prädikatenkalkül generierten formalen Tautologien auch semantische Tautologien sind. Wir halten den sogenannten *Korrektheitssatz (für Tautologien)* fest.

Satz 14.1. *Es sei S ein Symbolalphabet und sei $\alpha \in L^S$ eine syntaktische Tautologie. Dann ist α auch eine semantische Tautologie.*

Beweis. Dies ergibt sich aus den einzelnen Korrektheitsüberlegungen im Anschluss an die Ableitungsregeln, siehe beispielsweise Lemma 11.4. □

Der entworfene Kalkül produziert also nur inhaltlich korrekte Ableitungen. Eine gleichwertige Variante davon bezieht sich auf die Ableitbarkeit und die Folgerung.

Satz 14.2. *Es sei S ein Symbolalphabet, Γ eine Menge an S-Ausdrücken und α ein weiterer S-Ausdruck. Dann folgt aus der Ableitungsbeziehung $\Gamma \vdash \alpha$ die Folgerungsbeziehung $\Gamma \vDash \alpha$.*

Beweis. Es sei $\Gamma \vdash \alpha$ vorausgesetzt. Dann gibt es endlich viele Ausdrücke $\alpha_1, \ldots, \alpha_n \in \Gamma$ derart, dass $\varphi = \alpha_1 \wedge \ldots \wedge \alpha_n \to \alpha$ eine formale Tautologie ist. Nach Satz 14.1 ist φ auch allgemeingültig. Es sei I eine Interpretation mit $I \vDash \Gamma$. Dann ist insbesondere $I \vDash \alpha_1 \wedge \ldots \wedge \alpha_n$ und wegen der Allgemeingültigkeit von φ gilt $I \vDash \varphi$. Also gilt auch $I \vDash \alpha$. □

Die Umkehrung dieser beiden Aussagen ist deutlich schwieriger: Es geht um die Frage, ob der Kalkül jeden allgemeingültigen Ausdruck formal ableiten kann, ob es also für jeden mathematischen Beweis eines Ausdrucks einer Sprache erster Stufe auch einen formalen Beweis gibt. Es ist die Frage, ob

der Kalkül *vollständig* ist. Dass dies der Fall ist, ist der Inhalt des *Vollständigkeitssatzes*, der auf Gödel zurückgeht und den wir in dieser und der nächsten Vorlesung beweisen werden. Der Beweis ist recht aufwändig, so dass wir kurz die Strategie erläutern, die in einer einfacheren Form schon im Beweis des Vollständigkeitssatzes für die Aussagenlogik verwendet wurde. Wir verwenden Kontraposition und zeigen, dass aus der Nichtableitbarkeit $\Gamma \nvdash \alpha$ die Nichtfolgerung $\Gamma \nvDash \alpha$ folgt. Ersteres bedeutet, dass $\Gamma \cup \{\neg\alpha\}$ widerspruchsfrei ist, und Letzteres bedeutet, dass $\Gamma \cup \{\neg\alpha\}$ erfüllbar ist. Wir zeigen daher allgemein, dass eine widerspruchsfreie Ausdrucksmenge erfüllbar ist. Dazu füllen wir eine widerspruchsfreie Ausdrucksmenge, analog zum aussagenlogischen Fall (siehe Lemma 5.17), zu einer maximal widerspruchsfreien Ausdrucksmenge auf. Wenn diese zusätzlich „Beispiele enthält“ (um das zu erreichen, muss man die Symbolmenge erweitern) so kann man auf der Sprache eine Äquivalenzrelation definieren, deren Äquivalenzklassen die Grundlage eines erfüllenden Modells bilden. Wir beginnen mit dem *Satz von Henkin*, der die Erfüllbarkeit im maximal widerspruchsfreien Fall mit Beispielen erledigt.

14.2. **Der Satz von Henkin.**

Definition 14.3. Eine Menge Γ an S-Ausdrücken (über einem Symbolalphabet S) heißt *maximal widerspruchsfrei*, wenn sie widerspruchsfrei ist und wenn jede Hinzunahme eines jeden Ausdrucks $\alpha \notin \Gamma$ die Menge widersprüchlich macht.

Definition 14.4. Man sagt, dass eine Menge Γ an S-Ausdrücken (über einem Symbolalphabet S) *Beispiele enthält*, wenn es für jeden Ausdruck der Form $\exists x\alpha$ einen S-Term t derart gibt, dass

$$\exists x\alpha \to \alpha\frac{t}{x}$$

zu Γ gehört.

Diese beiden Begriffe sind durch folgende Aussage motiviert.

Lemma 14.5. *Es sei S ein Symbolalphabet und I eine S-Interpretation auf einer Menge M, wobei die Terminterpretation surjektiv sei. Dann ist die Gültigkeitsmenge $\Gamma = I^{\vDash}$ maximal widerspruchsfrei und enthält Beispiele.*

Beweis. Zunächst ist $\Gamma = I^{\vDash}$ aufgrund des Korrektheitssatzes abgeschlossen unter Ableitungen. Für jeden S-Ausdruck α gilt die Alternative: Entweder $\alpha \in \Gamma$ oder $\neg\alpha \in \Gamma$. Insbesondere ist Γ widerspruchsfrei. Wenn $\alpha \notin \Gamma$ ist, so ist $\neg\alpha \in \Gamma$ und daher ist $\Gamma \cup \{\alpha\}$ widersprüchlich. Also ist Γ maximal widerspruchsfrei. Wir betrachten nun einen Ausdruck der Form $\alpha = \exists x\beta$. Wenn $\alpha \notin \Gamma$ gilt, so gilt $\exists x\beta \to \beta\frac{t}{x}$ in I für jeden Term t, da ja der Vordersatz nicht gilt. Wenn hingegen $\alpha \in \Gamma$ gilt, so gibt es aufgrund des semantischen Aufbaus der Gültigkeitbeziehung ein $m \in M$ derart, dass $I\frac{m}{x} \vDash \beta$ gilt. Wegen der vorausgesetzten Surjektivität der Belegung gibt es einen Term t, der

durch m interpretiert wird. Daher gilt nach dem Substitutionslemma $\beta\frac{t}{x}$ in I. Also gilt $\exists x\beta \to \beta\frac{t}{x}$ in I. □

Lemma 14.6. *Es sei Γ eine Menge an S-Ausdrücken (über einem Symbolalphabet S), die maximal widerspruchsfrei ist. Dann gelten folgende Eigenschaften.*

(1) *Für jeden Ausdruck α ist entweder $\alpha \in \Gamma$ oder $\neg\alpha \in \Gamma$.*
(2) *Aus $\Gamma \vdash \alpha$ folgt $\alpha \in \Gamma$, d.h. Γ ist abgeschlossen unter Ableitungen.*
(3) *Für Ausdrücke α, β ist $\alpha \wedge \beta \in \Gamma$ genau dann, wenn $\alpha \in \Gamma$ und $\beta \in \Gamma$ ist.*

Beweis. (1). Wegen der Widerspruchsfreiheit kann nicht sowohl α als auch $\neg\alpha$ zu Γ gehören. Wenn weder α noch $\neg\alpha$ zu Γ gehören, so ist entweder $\Gamma \cup \{\alpha\}$ oder $\Gamma \cup \{\neg\alpha\}$ widerspruchsfrei. Wären nämlich beide widersprüchlich, so würde für einen beliebigen Ausdruck β sowohl

$$\Gamma \cup \{\alpha\} \vdash \beta$$

als auch

$$\Gamma \cup \{\neg\alpha\} \vdash \beta$$

gelten. Dies bedeutet

$$\Gamma \vdash \alpha \to \beta$$

und

$$\Gamma \vdash \neg\alpha \to \beta\,,$$

woraus aufgrund der Fallunterscheidungsregel

$$\Gamma \vdash \beta$$

folgt. Dies bedeutet aber, dass Γ widersprüchlich ist. (2). Sei $\Gamma \vdash \alpha$. Nach (1) ist $\alpha \in \Gamma$ oder $\neg\alpha \in \Gamma$. Das zweite kann nicht sein, da sich daraus sofort ein Widerspruch ergeben würde. Also ist $\alpha \in \Gamma$. (3). Die Richtung von links nach rechts folgt aus (2). Seien also $\alpha, \beta \in \Gamma$. Da $\alpha \to (\beta \to \alpha \wedge \beta)$ nach Aufgabe 3.33 eine Tautologie ist, folgt $\alpha \wedge \beta \in \Gamma$ nach Teil (2). □

Wir werden nun umgekehrt zeigen, dass man zu einer jeden maximal widerspruchsfreien Ausdrucksmenge Γ, die Beispiele enthält, eine Interpretation konstruieren kann, deren Gültigkeitsmenge mit Γ übereinstimmt. Diese Konstruktion, die wir die *kanonische Termidentifizierung* nennen, geht folgendermaßen.

Konstruktion 14.7. Es sei Γ eine Menge an S-Ausdrücken (über einem Symbolalphabet S), die abgeschlossen unter Ableitungen ist. Dann definiert man auf der Menge aller S-Terme eine Äquivalenzrelation durch

$$t \sim s \text{ genau dann, wenn der Ausdruck } t = s \text{ zu } \Gamma \text{ gehört}\,.$$

Es sei M die Menge der Termklassen (also die Menge der Äquivalenzklassen zu dieser Äquivalenzrelation). Auf M definiert man für jedes n-stellige Relationssymbol R eine n-stellige Relation R^M durch

$R^M([t_1], [t_2], \ldots, [t_n])$ genau dann, wenn der Ausdruck $Rt_1t_2 \cdots t_n$ zu Γ gehört

und für jedes n-stellige Funktionssymbol f eine n-stellige Funktion f^M durch

$$f^M([t_1], [t_2], \ldots, [t_n]) := [ft_1t_2 \cdots t_n].$$

Konstanten werden als

$$c^M := [c]$$

interpretiert.

Wir müssen natürlich zunächst zeigen, dass wirklich eine Äquivalenzrelation vorliegt und dass die Relationen und Funktionen wohldefiniert sind.

Lemma 14.8. *Es sei Γ eine Menge an S-Ausdrücken (über einem Symbolalphabet S), die abgeschlossen unter Ableitungen ist. Dann liefert die in Konstruktion 14.7 beschriebene Konstruktion eine Äquivalenzrelation auf der Menge aller Terme und wohldefinierte Relationen bzw. Funktionen auf der Menge der Termklassen.*

Beweis. Eine Äquivalenzrelation liegt aufgrund von Axiom 10.5 (1) und Lemma 10.7 (1), (2) vor, da ja Γ nach Voraussetzung abgeschlossen unter Ableitungen ist und insbesondere alle syntaktischen Tautologien enthält.

Es sei M die Menge der Äquivalenzklassen, die wir in diesem Zusammenhang Termklassen nennen. Es sei R ein n-stelliges Relationssymbol. Es sei $([s_1], \ldots, [s_n])$ ein n-Tupel aus Termklassen, die einerseits durch das Termtupel $(s_1, \ldots, s_n)$ und andererseits durch das Termtupel $(t_1, \ldots, t_n)$ repräsentiert werde. Es gilt also $s_i \sim t_i$ bzw. $s_i = t_i \in \Gamma$. Wenn nun $Rs_1 \ldots s_n$ in Γ gilt, so folgt aus Lemma 10.7 (4) auch $Rt_1 \ldots t_n \in \Gamma$. Unter den gleichen Voraussetzungen folgt mit Lemma 10.7 (3) die Zugehörigkeit $fs_1 \ldots s_n = ft_1 \ldots t_n \in \Gamma$ und somit

$$[fs_1 \ldots s_n] = [ft_1 \ldots t_n],$$

also die Wohldefiniertheit der Funktion. □

Lemma 14.9. *Es sei Γ eine Menge an S-Ausdrücken (über einem Symbolalphabet S), die abgeschlossen unter Ableitungen ist. Dann gilt für die Interpretation (M, β), wobei M die in Konstruktion 14.7 beschriebene Menge aus Termklassen (mit der natürlichen Interpretation I von Konstanten, Funktionssymbolen und Relationssymbolen) und β die natürliche Belegung $\beta(x) = [x]$ für Variablen ist, die Beziehung*

$$I(t) = [t]$$

für alle Terme t.

Beweis. Wir führen Induktion über den Aufbau der Terme, wobei der Induktionsanfang unmittelbar durch die natürliche Belegung gesichert ist. Die Aussage gelte nun für Terme $t_1, \ldots, t_n$ und f sei ein n-stelliges Funktionssymbol. Dann ist

$$I(ft_1 \ldots t_n) = f^M(I(t_1), \ldots, I(t_n)) = f^M([t_1], \ldots, [t_n]) = [ft_1 \ldots t_n].$$

□

Die folgende Aussage heißt *Satz von Henkin*. Er wird durch Induktion über den sogenannten Rang eines Ausdrucks bewiesen. Dazu definieren wir.

Definition 14.10. Unter einem *atomaren Ausdruck* versteht man Ausdrücke der Form $s = t$, wobei s und t Terme sind, und der Form $Rt_1 \ldots t_n$, wobei R ein n-stelliges Relationssymbol ist und $t_1, \ldots, t_n$ Terme sind.

Definition 14.11. Es sei ein Alphabet einer Sprache erster Stufe gegeben. Dann definiert man für Ausdrücke $\alpha \in L^S$ den *Rang* ρ von α durch

(1) $\rho(\alpha) = 0$, falls α atomar ist.
(2) $\rho(\alpha) = \rho(\beta) + 1$, falls $\alpha = \neg(\beta)$ ist.
(3) $\rho(\alpha) = \rho(\beta) + \rho(\gamma) + 1$, falls $\alpha = (\beta) \circ (\gamma)$ mit $\circ = \wedge, \vee, \rightarrow, \leftrightarrow$ ist.
(4) $\rho(\alpha) = \rho(\beta) + 1$, falls $\alpha = \exists x\beta$ oder $\alpha = \forall x\beta$ ist.

Diese beiden Begriffe sind vor allem dann wichtig, wenn man eine Aussage über alle Ausdrücke induktiv beweisen möchte.

Satz 14.12. *Es sei* Γ *eine Menge an S-Ausdrücken (über einem Symbolalphabet S), die maximal widerspruchsfrei ist und Beispiele enthält. Dann ist die in Konstruktion 14.7 gegebene Interpretation ein Modell für* Γ*. Insbesondere ist* Γ *erfüllbar.*

Beweis. Es sei M das konstruierte Modell zu Γ und I die zugehörige Interpretation mit der natürlichen Belegung für die Variablen. Wir zeigen die Äquivalenz

$$\alpha \in \Gamma \text{ genau dann, wenn } I \vDash \alpha$$

für alle Ausdrücke α, durch Induktion über den Rang der Ausdrücke. Zum Induktionsanfang sei der Rang von α gleich 0, also α atomar. D.h. α ist entweder von der Form $s = t$ oder $Rt_1 \ldots t_n$. Im ersten Fall ist $s = t \in \Gamma$ äquivalent zu $s \sim t$ bzw. $[s] = [t]$ in M. Dies ist nach Lemma 14.9 äquivalent zu $I(s) = I(t)$ und das bedeutet $I \vDash s = t$.

Im zweiten Fall ist $Rt_1 \ldots t_n \in \Gamma$ - nach Konstruktion von M und R^M - äquivalent zu $R^M([t_1], \ldots, [t_n])$, und dies ist äquivalent zu $I \vDash Rt_1 \ldots t_n$.

Sei nun die Aussage für alle Ausdrücke vom Rang $\leq r$ bewiesen und sei α ein Ausdruck vom Rang $r + 1$. Wir betrachten die mögliche Struktur von α gemäß Definition 7.2. Bei

$$\alpha = \neg\beta$$

ergibt sich die Äquivalenz aus der Induktionsvoraussetzung (β hat kleineren Rang als α) und Lemma 14.6 (1). Bei

$$\alpha = \beta_1 \wedge \beta_2$$

besitzen die beiden Bestandteile kleineren Rang als α. Die Zugehörigkeit $\alpha \in \Gamma$ ist nach Lemma 14.6 (3) äquivalent zur gemeinsamen Zugehörigkeit $\beta_1, \beta_2 \in \Gamma$. Nach Induktionsvoraussetzung bedeutet dies $I \vDash \beta_1$ und $I \vDash \beta_2$. Dies bedeutet wiederum $I \vDash \beta_1 \wedge \beta_2$ aufgrund der Modellbeziehung. Bei

$$\alpha = \exists x \beta$$

besitzt wieder β einen kleineren Rang. Die Zugehörigkeit $\alpha \in \Gamma$ ist aufgrund der Eigenschaft, Beispiele zu enthalten und aufgrund von Axiom 11.1 äquivalent zur Existenz eines Terms t und der Zugehörigkeit $\beta\frac{t}{x} \in \Gamma$. Die Substitution von β nach $\beta\frac{t}{x}$ verändert nach Aufgabe 14.17 nicht den Rang. Wir können also auf $\beta\frac{t}{x}$ die Induktionsvoraussetzung anwenden und erhalten die Äquivalenz zu $I \vDash \beta\frac{t}{x}$. Nach dem Substitutionslemma ist dies äquivalent zu $I\frac{I(t)}{x} \vDash \beta$ bzw. $I\frac{[t]}{x} \vDash \beta$ wegen Lemma 14.9. Dies ist äquivalent zu $I \vDash \exists x \beta$ aufgrund der Modellbeziehung und der Surjektivität der Termabbildung. □

14. Arbeitsblatt

14.1. **Übungsaufgaben.**

Aufgabe 14.1. Es seien $S \subseteq S'$ Symbolalphabete und seien $L^S \subseteq L^{S'}$ die zugehörigen Sprachen Es sei $\Gamma \subseteq L^S$ eine Ausdrucksmenge.

(1) Γ sei widerspruchsfrei. Ist dann auch Γ, aufgefasst in $L^{S'}$, widerspruchsfrei?
(2) Γ sei maximal widerspruchsfrei. Ist dann auch Γ, aufgefasst in $L^{S'}$, maximal widerspruchsfrei?

Aufgabe 14.2. Zeige durch ein Beispiel, dass Lemma 14.5 ohne die Voraussetzung, dass eine surjektive Terminterpretation vorliegt, nicht gelten muss.

Aufgabe 14.3. Es sei S ein Symbolalphabet und I eine S-Interpretation auf einer Menge M mit der zugehörigen Terminterpretation. Zeige, dass man diese Terminterpretationsabbildung durch die Hinzunahme von Variablen (oder durch die Hinzunahme von Konstanten) surjektiv machen kann.

Aufgabe 14.4. Das Symbolalphabet S bestehe aus einer einzigen Variablen x und einem einzigen einstelligen Relationssymbol P. Zeige, dass zu einer Interpretation I die Gültigkeitsmenge $I^{\vDash} \subseteq L^S$ keine Beispiele enthalten muss.

Aufgabe 14.5.*

Es sei S ein Symbolalphabet und L^S die zugehörige Sprache und T die zugehörige Termmenge. Es sei $\Gamma \subseteq L^S$ eine Ausdrucksmenge.

(1) Zeige, dass durch

$s \cong_\Gamma t$ genau dann, wenn $I(s) = I(t)$ für jede Interpretation I mit $I \vDash \Gamma$

eine Äquivalenzrelation auf T definiert wird.

(2) Wenn man Γ vergrößert, werden dann die Äquivalenzklassen größer oder kleiner?

Aufgabe 14.6. Es sei S ein Symbolalphabet, T die zugehörige Termmenge und L^S die zugehörige Sprache. Es sei $\Gamma \subseteq L^S$ eine Ausdrucksmenge. Zeige, dass die Äquivalenzrelation $\sim_\Gamma$ aus Konstruktion 14.7 die semantische Äquivalenz $\cong_\Gamma$ aus Aufgabe 14.5 impliziert.

Aufgabe 14.7. Das Symbolalphabet S bestehe neben Variablen $x, y, z, \ldots$ aus einer Konstanten 0 und einem einstelligen Funktionssymbol f. Wir betrachten die Teilmengen

$$\Gamma_i \subseteq L^S$$

mit

$$\Gamma_1 = \{fff0 = 0\}^\vdash,$$

$$\Gamma_2 = \{fffx = x\}^\vdash,$$

$$\Gamma_3 = \{\forall x\,(fffx = x)\}^\vdash.$$

Es seien $\sim_i$ die zugehörigen Äquivalenzrelationen gemäß Konstruktion 14.7 auf der Termmenge.

(1) Gelten die Äquivalenzen

$$ffff0 \sim_1 f0,\ fffffff0 \sim_1 fff0,\ fffffffff0 \sim_1 fffffff0,\ ffffx \sim_1 fx?$$

(2) Gelten die Äquivalenzen

$$ffffx \sim_2 fx,\ ffffy \sim_2 fy,\ fffx \sim_2 y,\ ffffy \sim_3 fy\,?$$

(3) Welche Inklusionsbeziehungen bestehen zwischen $\Gamma_1, \Gamma_2, \Gamma_3$?

(4) Wie viele Termklassen gibt es zu $\sim_1, \sim_2, \sim_3$, wenn die Variablenmenge nur aus x besteht?

Aufgabe 14.8. Das Symbolalphabet S bestehe neben Variablen $x, y, z, \ldots$ aus einer Konstanten 0 und einem zweistelligen Funktionssymbol $+$. Es sei $\Gamma \subseteq L^S$ die Menge aller Ableitungen aus dem Axiomensystem

$$\forall x(x{+}0 = x),\ \forall x(0{+}x = x),\ \forall x\forall y\forall z((x{+}y){+}z) = x{+}(y{+}z)),\ \forall x(x{+}x = 0)\,.$$

Es sei $\sim$ die zugehörige Äquivalenzrelation gemäß Konstruktion 14.7. Zeige $x + y \sim y + x$ für jedes Variablenpaar x, y.

Aufgabe 14.9. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache. Zeige, dass zu

$$\Gamma = \emptyset$$

die in Konstruktion 14.7 eingeführte Äquivalenzrelation die Identität ist.

Aufgabe 14.10. Es sei $\Gamma \subseteq L^S$ eine widersprüchliche, unter Ableitungen abgeschlossene Teilmenge. Zeige, dass es nur eine Termklasse im Sinne von Konstruktion 14.7 gibt.

Aufgabe 14.11. Es sei $\Gamma \subseteq L^S$ eine unter Ableitungen abgeschlossene Teilmenge, die zu je zwei Termen s, t die Gleichheit $s = t$ enthalte. Wie viele Termklassen im Sinne von Konstruktion 14.7 gibt es? Ist Γ widersprüchlich?

Aufgabe 14.12. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache. Die Ausdrucksmenge Γ bestehe aus $x = y$, wobei x, y veschiedene Variablen seien. Zeige, dass zwei Terme s, t genau dann äquivalent im Sinne von Konstruktion 14.7 sind, wenn es eine Kette von Termen

$$t_0 = s, t_1, t_2, \ldots, t_{k-1}, t_k = t$$

derart gibt, dass beim Übergang von t_i nach t_{i+1} genau ein Vorkommen von x (bzw. y) in t_i durch y (bzw. x) ersetzt wird.

Aufgabe 14.13. Es sei V eine Variablenmenge und $\simeq$ eine Äquivalenzrelation auf V mit der Quotientenmenge $W = V/\simeq$. Es sei S ein erststufiges Symbolalphabet mit V als Variablenmenge und

$$\Gamma := \{x = y |\, x \simeq y\}^{\vdash}\,.$$

Es sei $\sim$ die zugehörige Äquivalenzrelation auf der Termmenge gemäß Konstruktion 14.7. Zeige, dass die Termklassenmenge zu Γ in kanonischer Weise mit der Termmenge zum Symbolalphabet S' in Bijektion steht, wobei S' aus S entsteht, indem man die Variablenmenge V durch W ersetzt.

In der folgenden Aufgabe sollen die Variablen $x_1, \ldots, x_n$ verschieden sein. Dennoch gibt es zwei Interpretationen für Teil (2), die aber inhaltlich äquivalent sind.

Aufgabe 14.14. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache. Es sei $\Gamma \subseteq L^S$ eine Ausdrucksmenge. Zu fixiertem $n \in \mathbb{N}_+$ sei F_n die Menge der n-stelligen Funktionssymbole. Zeige die folgenden Aussagen.

(1) Durch

$$f \cong g\,, \text{ falls } I(f) = I(g) \text{ für alle Interpretationen } I \text{ mit } I \vDash \Gamma$$

wird eine Äquivalenzrelation auf F_n definiert.

(2) Durch

$$f \sim g\,, \text{ falls } \Gamma \vdash \forall x_1 \forall x_2 \ldots \forall x_n f x_1 \ldots x_n = g x_1 \ldots x_n$$

wird eine Äquivalenzrelation auf F_n definiert.

(3) Die Äquivalenzrelation $\sim$ impliziert die Äquivalenzrelation $\cong$.

(4) Es sei $\sim$ die zu Γ gehörende formale Äquivalenzrelation auf der Termmenge im Sinne von Konstruktion 14.7. Dann gilt für Terme $s_1 \sim t_1, \ldots, s_n \sim t_n$ und Funktionssymbole $f, g \in F_n$ mit $f \sim g$ die Beziehung

$$f s_1 \ldots s_n \sim g t_1 \ldots t_n.$$

Aufgabe 14.15. Es sei $\alpha \in L^S$ ein atomarer Ausdruck, der zugleich eine Tautologie ist, also $\vdash \alpha$. Zeige, dass α gleich $s = s$ mit einem S-Term s ist.

Aufgabe 14.16. Bestimme den Rang der folgenden Ausdrücke.

(1) $a = fx$,
(2) $\exists x a = fx$,
(3) $(\neg Rxy \wedge ffx = c) \to (\exists x a = fx)$,
(4) $(\forall y Rxy) \to (\exists x a = fx)$.

Aufgabe 14.17. Zeige durch Induktion über den Aufbau der Ausdrücke, dass sich bei einer Termsubstitution der Rang eines Ausdrucks nicht ändert.

Aufgabe 14.18. Warum führt man im Beweis zum Satz von Henkin nicht Induktion über den Aufbau der Ausdrücke?

Aufgabe 14.19. Es sei M ein kommutativer Halbring. Zeige, dass es eine eindeutig bestimmte (kanonische) Abbildung

$$\varphi\colon \mathbb{N} \longrightarrow M$$

gibt, die sowohl die Addition als auch die Multiplikation respektiert.

Aufgabe 14.20. Es sei M ein Peano-Halbring und

$$\varphi\colon \mathbb{N} \longrightarrow M$$

die kanonische Abbildung. Zeige, dass φ injektiv ist.

Aufgabe 14.21. Sei $n \in \mathbb{N}_+$ und betrachte $M = \mathbb{Z}/(n)$ mit den natürlichen Operationen. Welche der Peano-Axiome gelten, welche nicht?

Aufgabe 14.22.*

Es sei M ein kommutativer Halbring und $x, y \in M$. Es sei

$$I := \{u \in M | \, \exists a \exists b \exists c \exists d \text{ mit } u + ax + by = cx + dy\}\,.$$

(1) Zeige, dass I die folgenden drei Eigenschaften erfüllt.
   (a) $0 \in I$.
   (b) Wenn $u, v \in I$ sind, so ist auch $u + v \in I$.
   (c) Wenn $u \in I$ und $r \in M$ ist, so ist auch $ru \in I$.
(2) M erfülle nun die Abziehregel. Zeige, dass aus $u, v \in I$ mit $u = v + z$ auch $z \in I$ folgt.

Die folgende Aufgabe gibt eine Version des Lemmas von Bezout für Peano-Halbringe.

Aufgabe 14.23. Es sei M ein Peano-Halbring und $x, y \in M$. Es sei

$$I := \{u \in M | \, \exists a \exists b \exists c \exists d \text{ mit } u + ax + by = cx + dy\}\,.$$

Zeige, dass es ein eindeutig bestimmtes $v \in M$ derart gibt, dass I aus sämtlichen Vielfachen von v besteht. Zeige, dass v der größte gemeinsame Teiler von x und y ist.

Aufgabe 14.24. Zeige, dass in einem Peano-Halbring M die Begriffe irreduzibel und prim zusammenfallen.

Aufgabe 14.25. Zeige, dass in $M \subseteq \mathbb{Z}[V]$ aus Beispiel 13.9 durch $x \geq y$, falls es ein $z \in M$ mit $x = y + z$ gibt, eine totale Ordnung gegeben ist.

14.2. **Aufgaben zum Abgeben.**

Aufgabe 14.26. (3 Punkte)

Es sei Γ eine Menge an S-Ausdrücken (über einem Symbolalphabet S), die folgende Eigenschaften erfüllt.

(1) Für jeden Ausdruck α ist $\alpha \in \Gamma$ oder $\neg\alpha \in \Gamma$.
(2) Aus $\Gamma \vdash \alpha$ folgt $\alpha \in \Gamma$, d.h. Γ ist abgeschlossen unter Ableitungen.
(3) Γ ist widerspruchsfrei.

Zeige, dass Γ maximal widerspruchsfrei ist.

Aufgabe 14.27. (4 Punkte)

Es sei S ein Symbolalphabet und L^S die zugehörige Sprache. Es seien s, t verschiedene Terme. Zeige, dass es eine S-Interpretation I mit

$$I(s) \neq I(t)$$

gibt.

Aufgabe 14.28. (5 Punkte)

Es sei $\Gamma \subseteq L^{\mathrm{Ar}}$ die Peano-Arithmetik, also die Menge aller aus den erststufigen Peano-Axiomen ableitbaren Ausdrücke. Zeige, dass jeder variablenfreie Term im Sinne von Konstruktion 14.7 äquivalent zu einem Term ist, bei dem das Multiplikationszeichen nicht mehr vorkommt.

Aufgabe 14.29. (8 (1+3+1+3) Punkte)

Es sei S ein Symbolalphabet und L^S die zugehörige Sprache. Es sei $\Gamma \subseteq L^S$ eine Ausdrucksmenge. Zu fixiertem $n \in \mathbb{N}_+$ sei R_n die Menge der n-stelligen Relationssymbole in S. Zeige die folgenden Aussagen.

(1) Durch

$$P \cong Q\,, \text{ falls } I(P) = I(Q) \text{ für alle Interpretationen } I \text{ mit } I \vDash \Gamma$$

wird eine Äquivalenzrelation auf R_n definiert.
(2) Durch

$$P \simeq Q\,, \text{ falls } \Gamma \vdash \forall x_1 \forall x_2 \ldots \forall x_n \, (Px_1 \ldots x_n \leftrightarrow Qx_1 \ldots x_n)$$

wird eine Äquivalenzrelation auf R_n definiert.
(3) Die Äquivalenzrelation $\simeq$ impliziert die Äquivalenzrelation $\cong$.

(4) Es sei $\sim$ die zu Γ gehörende Äquivalenzrelation auf der Termmenge im Sinne von Konstruktion 14.7. Dann gilt für Terme mit $s_1 \sim t_1, \ldots, s_n \sim t_n$ und Relationsssymbole $P, Q \in R_n$ mit $P \simeq Q$ die Beziehung

$$\Gamma \vdash Ps_1 \ldots s_n \leftrightarrow Qt_1 \ldots t_n \,.$$

Aufgabe 14.30. (2 Punkte)

Bestimme den Rang der folgenden Ausdrücke.

(1) $gxy = c$,
(2) $\forall xgcx = gxx$,
(3) $(\neg Pz \vee ggxyy = gcc) \to (\exists xPx)$,
(4) $(\forall yPy) \to (\neg\exists xgcx = gcgcx \wedge c = c)$.

15. Vorlesung - Der Vollständigkeitssatz

15.1. **Auffüllungsstrategien.**

Die weitere Strategie zum Beweis des Vollständigkeitssatzes ist nun, eine widerspruchsfreie Ausdrucksmenge zu einer maximal widerspruchsfreien Ausducksmenge, die Beispiele enthält, aufzufüllen, und so ein erfüllendes Modell mit Hilfe des Satzes von Henkin zu bekommen. Dabei betrachten wir zunächst das Problem, Beispiele hinzuzunehmen. Es sei Γ eine widerspruchsfreie Ausdrucksmenge über dem Alphabet S. Zu jedem Ausdruck α müssen wir einen Ausdruck der Form $\exists x\alpha \to \alpha\frac{t}{x}$ mit einem gewissen Term t hinzunehmen. Das Problem ist hierbei, dass bei ungeeigneter Wahl von t die Hinzunahme dieses Ausdrucks Γ widersprüchlich machen könnte. Es gibt keine Garantie, dass es überhaupt einen S-Term t gibt, mit dem man Γ widerspruchsfrei erweitern kann. Von daher wählt man eine andere Strategie, indem man simultan das Symbolalphabet erweitert und den hinzuzunehmenden Existenzausdruck mit einem neuen „unbelasteten“ Term ansetzt.

Lemma 15.1. *Es sei Γ eine widerspruchsfreie Menge an S-Ausdrücken (über einem Symbolalphabet S). Es sei z ein weiteres Variablensymbol, das nicht zu S gehört, und sei α ein S-Ausdruck. Dann ergibt die Hinzunahme von $\exists x\alpha \to \alpha\frac{z}{x}$ zu Γ eine ebenfalls widerspruchsfreie Ausdrucksmenge (über dem Symbolalphabet $S' = S \cup \{z\}$).*

Beweis. Nehmen wir an, dass $\Gamma' = \Gamma \cup \{\exists x\alpha \to \alpha\frac{z}{x}\}$ widersprüchlich ist. Dann kann man aus Γ' jeden Ausdruck ableiten. Es gilt also

$$\Gamma' \vdash \psi$$

und damit

$$\Gamma \vdash \left(\exists x\alpha \to \alpha\frac{z}{x}\right) \to \psi$$

für jeden Ausdruck ψ. Es gilt also insbesondere

$$\Gamma \vdash \neg\exists x\alpha \to \psi$$

und

$$\Gamma \vdash \alpha\frac{z}{x} \to \psi\,.$$

Wir nehmen nun zusätzlich an, dass z in ψ nicht vorkommt. Da z überhaupt nicht in den anderen Ausdrücken vorkommt, können wir mittels Axiom 11.2 (genauer wegen der in Aufgabe 11.20 besprochenen Variante) auf

$$\Gamma \vdash \exists x\alpha \to \psi\,.$$

schließen. Damit ergibt sich mit der Fallunterscheidungsregel

$$\Gamma \vdash \psi\,,$$

im Widerspruch zur Widerspruchsfreiheit von Γ. □

Lemma 15.2. *Es sei Γ eine widerspruchsfreie Menge an S-Ausdrücken (über einem Symbolalphabet S). Dann gibt es eine Symbolerweiterung $S^* \supseteq S$ und eine widerspruchsfreie S^*-Ausdrucksmenge $\Gamma^* \supseteq \Gamma$ derart, dass es zu jedem Ausdruck $\exists x\alpha \in L^S$ einen Term t (über S^*) derart gibt, dass*

$$\exists x\alpha \to \alpha\frac{t}{x} \in \Gamma^*$$

gilt.

Beweis. Die Menge S^* definieren wir als disjunkte Vereinigung

$$S^* \,=\, S \cup V,$$

wobei V eine Variablenmenge ist, die für jeden Ausdruck der Form $\exists x\alpha \in L^S$ genau eine (neue) Variable enthält, die wir mit $y_{\exists x\alpha}$ bezeichnen. Wir setzen

$$\Gamma^* \,=\, \Gamma \cup \left\{\exists x\alpha \to \alpha\frac{y_{\exists x\alpha}}{x} \,|\, \exists x\alpha \in L^S\right\}.$$

Daher ist $\Gamma \subseteq \Gamma^*$ und Γ^* enthält S-Beispiele. Es bleibt also die Widerspruchsfreiheit zu zeigen. Wäre Γ^* widerspruchsvoll, so wäre auch eine endliche Teilmenge davon widerspruchsvoll und insbesondere würde es Ausdrücke $\alpha_1, \ldots, \alpha_n \in L^S$ derart geben, dass

$$\Gamma \cup \{\exists x_1\alpha_1 \to \alpha_1\frac{y_{\exists x_1\alpha_1}}{x_1}\} \cup \ldots \cup \{\exists x_n\alpha_n \to \alpha_n\frac{y_{\exists x_n\alpha_n}}{x_n}\}$$

widersprüchlich ist (dabei können die x_i gleich oder verschieden sein). Da bei jeder Hinzunahme eine neue Variable $y_{\exists x_n\alpha_n}$ verwendet wird, können wir induktiv Lemma 15.1 anwenden und erhalten die Widersprüchlichkeit von Γ. □

Lemma 15.3. *Es sei Γ eine widerspruchsfreie Menge an S-Ausdrücken (über einem Symbolalphabet S). Dann gibt es eine aufsteigende Folge von Symbolmengen*

$$S_n \subseteq S_{n+1} \text{ mit } S_0 = S$$

und eine Folge von aufsteigenden S_n-Ausdrucksmengen

$$\Gamma_n \subseteq \Gamma_{n+1} \text{ mit } \Gamma_0 = \Gamma$$

derart, dass zum Symbolalphabet $S' = \bigcup_{n\in\mathbb{N}} S_n$ die S'-Ausdrucksmenge

$$\Gamma' = \bigcup_{n\in\mathbb{N}} \Gamma_n$$

widerspruchsfrei ist und Beispiele enthält.

Beweis. Wir konstruieren die Folgen S_n und Γ_n sukzessive mit der in Lemma 15.2 beschriebenen Methode durch

$$S_{n+1} = (S_n)^*$$

und

$$\Gamma_{n+1} = (\Gamma_n)^*.$$

Wäre Γ' widersprüchlich, so würde sich schon aus einer endlichen Teilmenge ein Widerspruch ergeben. Dann wäre schon eines der Γ_n widersprüchlich im Widerspruch zu Lemma 15.2. □

Wir wenden uns nun dem Problem zu, wie man eine widerspruchsfreie Ausdrucksmenge zu einer maximal widerspruchsfreien Menge ergänzen kann. Wie im entsprechenden Beweis der Aussagenlogik verwenden wir das Lemma von Zorn, wobei wir im abzählbaren Fall noch eine Beweisvariante angeben, die ohne das Lemma von Zorn auskommt.

Lemma 15.4. *Es sei Γ eine widerspruchsfreie Menge an S-Ausdrücken (über einem Symbolalphabet S). Dann gibt es eine maximal widerspruchsfreie S-Menge Γ' mit $\Gamma \subseteq \Gamma'$.*

Beweis. Wie betrachten die Menge

$$M = \{\Delta |\, \Gamma \subseteq \Delta \subseteq L^S, \, \Delta \text{ widerspruchsfreie Ausdrucksmenge}\}$$

aller widerspruchsfreien S-Ausdrucksmengen oberhalb von Γ. Es ist $\Gamma \in M$. Es sei $N \subseteq M$ eine nichtleere total geordnete Teilmenge. Die Vereinigung $\Delta' = \bigcup_{\Delta\in N} \Delta$ ist ebenfalls eine S-Ausdrucksmenge, die Γ umfasst. Sie ist auch widerspruchsfrei. Würde nämlich $\Delta' \vdash \neg\alpha \wedge \alpha$ gelten, so könnte man schon aus einer endlichen Teilmenge $T \subseteq \Delta'$ einen Widerspruch ableiten. Die Elemente aus T liegen jeweils in je einem $\Delta \in N$, und da diese eine Kette bilden, gibt es auch ein $\tilde{\Delta}$ mit $T \subseteq \tilde{\Delta}$, also wäre $\tilde{\Delta}$ widersprüchlich. Somit sind die Voraussetzungen im Lemma von Zorn erfüllt und daher gibt es eine maximale Menge Γ' in M. Diese ist offenbar maximal widerspruchsfrei. □

Wir besprechen eine Variante der vorstehenden Auffüllung für den Fall eines abzählbaren Symbolalphabets, die das Lemma von Zorn vermeidet und im Wesentlichen (siehe die Einschränkung weiter unten) konstruktiv ist. Man beachte, dass die oben durchgeführte Aufnahme von Beispielen bei einem

abzählbaren Ausgangsalphabet wieder abzählbare Symbolalphabete liefert und dies auch bei der abzählbaren Wiederholung dieses Prozesses wie in Lemma 15.3 der Fall ist.

Lemma 15.5. *Es sei Γ eine widerspruchsfreie Menge an S-Ausdrücken über einem abzählbaren Symbolalphabet S. Dann gibt es eine maximal widerspruchsfreie S-Menge Γ' mit $\Gamma \subseteq \Gamma'$, die man durch sukzessive Hinzunahme von einzelnen Ausdrücken erhalten kann.*

Beweis. Da S abzählbar ist, ist auch L^S abzählbar. Es sei α_n, $n \in \mathbb{N}$, eine Abzählung sämtlicher Ausdrücke aus L^S. Wir definieren induktiv eine aufsteigende Folge Γ_n von Ausdrucksmengen durch $\Gamma_0 = \Gamma$ und

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\alpha_{n+1}\}, & \text{falls dies widerspruchsfrei ist}, \\ \Gamma_n \text{ sonst}. \end{cases}$$

Wir setzen

$$\Gamma' = \bigcup_{n \in \mathbb{N}} \Gamma_n.$$

Diese Menge ist widerspruchsfrei, da andernfalls schon eines der Γ_n widersprüchlich wäre, was aufgrund der induktiven Definition nicht der Fall ist. Um zu zeigen, dass Γ' maximal widerspruchsfrei ist, sei $\alpha \notin \Gamma'$. Da α in der Abzählung der Ausdrücke vorkommt, ist $\alpha = \alpha_n$ für ein gewisses n. Im n-ten Konstruktionsschritt wurde α_n nicht hinzugenommen, sonst wäre $\alpha_n \in \Gamma_n \subseteq \Gamma'$. Also ist $\Gamma_{n-1} \cup \{\alpha_n\}$ widersprüchlich und damit ist auch $\Gamma' \cup \{\alpha\}$ widersprüchlich. □

Die vorstehende Variante sieht auf den ersten Blick konstruktiver aus, als sie ist. Das Problem ist die Entscheidung, ob $\Gamma_n \cup \{\alpha_{n+1}\}$ widerspruchsfrei ist. Dafür gibt es (anders als bei der Aussagenlogik) kein algorithmisches Verfahren.

15.2. **Der Vollständigkeitssatz.**

Die folgende Aussage ist der *Vollständigkeitssatz*.

Satz 15.6. *Es sei S ein Symbolalphabet, Γ eine Menge an S-Ausdrücken und α ein weiterer S-Ausdruck. Dann gilt $\Gamma \vDash \alpha$ genau dann, wenn $\Gamma \vdash \alpha$ gilt.*

Beweis. Die Richtung von rechts nach links ist der Korrektheitssatz. Sei umgekehrt $\Gamma \nvdash \alpha$. Um zu zeigen, dass auch $\Gamma \nvDash \alpha$ gilt, müssen wir ein Modell angeben, das Γ erfüllt, aber nicht α. Die Nichtableitbarkeit $\Gamma \nvdash \alpha$ bedeutet, dass $\Gamma \cup \{\neg\alpha\}$ widerspruchsfrei ist, und wir müssen zeigen, dass $\Gamma \cup \{\neg\alpha\}$ erfüllbar ist. Nach Lemma 15.3 gibt es eine widerspruchsfreie Erweiterung $S \subseteq S'$ des Symbolalphabets und eine Erweiterung Γ' von $\Gamma \cup \{\neg\alpha\}$, die Beispiele enthält. Nach Lemma 15.4 gibt es eine maximal widerspruchsfreie S'-Ausdrucksmenge $\Gamma'' \supseteq \Gamma'$. Diese enthält mit Γ' ebenfalls Beispiele. Nach

dem Satz von Henkin gibt es eine S'-Interpretation, die Γ'' erfüllt. Diese Interpretation erfüllt erst recht $\Gamma \cup \{\neg\alpha\}$. □

Für Tautologien ergibt sich der folgende Spezialfall.

Korollar 15.7. *Es sei S ein Symbolalphabet und $\alpha \in L^S$ ein S-Ausdruck. Dann ist α genau dann eine ableitbare Tautologie, wenn α allgemeingültig ist.*

Beweis. Dies folgt aus Satz 15.6 mit

$$\Gamma = \emptyset.$$

□

Korollar 15.8. *Es sei S ein Symbolalphabet und Γ eine Menge an S-Ausdrücken. Dann ist Γ genau dann widerspruchsfrei, wenn Γ erfüllbar ist.*

Beweis. In dieser Form haben wir den Vollständigkeitssatz bewiesen. Diese Aussage ergibt sich aber auch als Spezialfall von Satz 15.6, wenn man für α eine widersprüchliche Aussage ansetzt. □

Das folgende Korollar, der sogenannte *Endlichkeitssatz*, demonstriert, dass der Vollständigkeitssatz keineswegs selbstverständlich ist. Es sei eine Folgerungsbeziehung $\Gamma \vDash \alpha$ bewiesen, also gezeigt, dass jede Interpretation, die Γ erfüllt, auch α erfüllen muss. Dabei sei Γ unendlich, man denke etwa an ein unendliches Axiomenschema, wie es im Induktionsschema der erststufigen Peano-Arithmetik vorliegt. Ist es vorstellbar, dass in einem Beweis irgendwie auf all diese unendlich vielen Voraussetzungen Bezug genommen wird?

Korollar 15.9. *Es sei S ein Symbolalphabet, Γ eine Menge an S-Ausdrücken und α ein weiterer S-Ausdruck. Dann gilt $\Gamma \vDash \alpha$ genau dann, wenn es eine endliche Teilmenge $\Gamma_e \subseteq \Gamma$ gibt mit $\Gamma_e \vDash \alpha$.*

Beweis. Dies folgt direkt aus Satz 15.6, da die Endlichkeitsbeziehung für das Ableiten nach Definition gilt. □

Korollar 15.10. *Es sei S ein Symbolalphabet und Γ eine Menge an S-Ausdrücken. Es sei jede endliche Teilmenge $\Gamma_e \subseteq \Gamma$ erfüllbar. Dann ist Γ erfüllbar.*

Beweis. Dies folgt aus Korollar 15.8. Für die Widerspruchsfreiheit ist die Aussage klar, da eine Ableitung eines Widerspruchs nur Bezug auf endlich viele Voraussetzungen nimmt. □

Als ein weiteres Korollar zum Vollständigkeitssatz führen wir die Existenz von Peano-Halbringen an, die nicht archimedisch geordnet sind und daher nicht isomorph zum Standardmodell $\mathbb{N}$ sind. Die erststufigen Peano-Axiome charakterisieren also nicht die natürlichen Zahlen.

Korollar 15.11. *Es gibt Peano-Halbringe, die nicht zu* $\mathbb{N}$ *isomorph sind, also nicht die zweitstufigen Dedekind-Peano-Axiome erfüllen.*

Beweis. Siehe Aufgabe 15.11. □

15. Arbeitsblatt

15.1. **Übungsaufgaben.**

Aufgabe 15.1. Warum sind mathematische Beweise schwierig, obwohl sie (zumindest für erststufige Aussagen) aufgrund des Vollständigkeitssatzes mit einem sehr begrenzten und übersichtlichen formalen Regelwerk durchgeführt werden können?

Aufgabe 15.2. Diskutiere Metasprache und Objektsprache anhand der Formulierung „im Widerspruch zur Widerspruchsfreiheit“ aus dem Beweis zu Lemma 15.1.

Aufgabe 15.3. Es sei S ein Symbolalphabet (das mindestens eine Variable enthalte) einer Sprache erster Stufe und T die zugehörige Termmenge. Zeige, dass man T als Grundmenge einer Interpretation von S nehmen kann, indem man Variablen, Konstanten und Funktionssymbole „natürlich“ und Relationssymbole willkürlich interpretiert.

Aufgabe 15.4. Zeige, dass es eine widerspruchsfreie, unter Ableitungen abgeschlossene Ausdrucksmenge $\Gamma \subseteq L^S$ geben kann, wobei die Variablenmenge aus x_n, $n \in \mathbb{N}$, besteht, derart, dass es einen Ausdruck α mit $\exists x_0 \alpha \in \Gamma$ und $\neg\alpha\frac{x_n}{x_0} \in \Gamma$ für alle $n \in \mathbb{N}$ gibt.

Aufgabe 15.5. Es sei PA die Menge der aus den erststufigen Peano-Axiomen für die Addition und Multiplikation ableitbaren Ausdrücken. Es sei α der erststufige Ausdruck, der die Goldbach-Vermutung ausdrückt. Was kann man über die Widerspruchsfreiheit von $PA \cup \{\alpha\}$ bzw. von $PA \cup \{\neg\alpha\}$ sagen? Was bedeutet dies für das in Lemma 15.5 beschriebene Verfahren?

Aufgabe 15.6. Es sei $\Gamma \subseteq L^S$ eine Ausdrucksmenge, die über beliebig großen endlichen Grundmengen erfüllbar ist. Zeige, dass Γ auch über einer unendlichen Menge erfüllbar ist.

Aufgabe 15.7. Es sei S ein Symbolalphabet, das allein aus der einzigen Variablen x besteht. Zeige, dass die Menge aller S-Tautologien maximal widerspruchsfrei ist und Beispiele enthält.

Aufgabe 15.8. Es sei S ein Symbolalphabet, das nur aus Variablen besteht. Es sei

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

wobei x, y verschiedene Variablen seien, und sei

$$\Gamma = \Delta^{\vdash}.$$

Zeige, dass Γ maximal widerspruchsfrei ist und Beispiele enthält.

Aufgabe 15.9.*

Es sei S ein Symbolalphabet und $\Gamma \subseteq L^S$ eine Ausdrucksmenge. Begründe, warum man im Allgemeinen bei der Hinzunahme von Beispielen (innerhalb des Beweises des Vollständigkeitssatzes) nicht für alle Existenzaussagen $\exists x\alpha \in L^S$ mit einer einzigen neuen Variablen z arbeiten kann.

Aufgabe 15.10. Es sei S ein Symbolalphabet und $\Gamma \subseteq L^S$ eine Ausdrucksmenge. Zeige

$$\Gamma^{\vdash} = \bigcap_{I \vDash \Gamma} I^{\vDash}.$$

Aufgabe 15.11.*

Zeige, dass es einen Peano-Halbring M mit der Eigenschaft gibt, dass es darin ein Element $x \in M$ gibt, das größer als jede natürliche Zahl in M (also Zahlen der Form $1 + 1 + \cdots + 1$) ist.

Aufgabe 15.12. Man mache sich Gedanken zu den folgenden Zitaten aus Ludwig Wittgensteins Tractatus logico-philosophicus.

„6.2 Die Mathematik ist eine logische Methode. Die Sätze der Mathematik sind Gleichungen, also Scheinsätze. 6.21 Der Satz der Mathematik drückt keinen Gedanken aus“.

„6.22 Die Logik der Welt, die die Sätze der Logik in den Tautologien zeigen, zeigt die Mathematik in den Gleichungen“.

„6.2321 Und, dass die Sätze der Mathematik bewiesen werden können, heißt ja nichts anderes, als dass ihre Richtigkeit einzusehen ist, ohne dass das, was sie ausdrücken, selbst mit den Tatsachen auf seine Richtigkeit hin verglichen werden muss“.

„6.234 Die Mathematik ist eine Methode der Logik.

6.2341 Das Wesentliche der mathematischen Methode ist es, mit Gleichungen zu arbeiten. Auf dieser Methode beruht es nämlich, dass jeder Satz der Mathematik sich von selbst verstehen muss“.

„6.24 Die Methode der Mathematik, zu ihren Gleichungen zu kommen, ist die Substitutionsmethode“. (...)

15.2. **Aufgaben zum Abgeben.**

Aufgabe 15.13. (4 Punkte)

Es seien s, t nicht identische S-Terme. Zeige, dass es ein endliches S-Modell mit

$$I(s) \neq I(t)$$

gibt.

Aufgabe 15.14. (3 Punkte)

Man gebe ein Beispiel für eine widerspruchsfreie, unter Ableitungen abgeschlossene Ausdrucksmenge $\Gamma \subseteq L^S$ derart, dass für die konstruierte Interpretation I nicht $\Gamma \subseteq I^{\vdash}$ gilt.

Aufgabe 15.15. (4 Punkte)

Es sei $\Gamma \subseteq L^S$ eine abzählbare widerspruchsfreie Ausdrucksmenge. Zeige, dass Γ ein erfüllendes Modell mit abzählbar vielen Elementen besitzt.

Aufgabe 15.16. (4 Punkte)

Zeige, dass man die natürlichen Zahlen nicht erststufig festlegen kann.

16. Vorlesung - Elementare Äquivalenz I

16.1. S-**Homomorphismen und elementare Äquivalenz.**

In der Mathematik spielen strukturerhaltende Abbildungen eine herausragende Rolle. Eine erststufige Version dieses Konzeptes kommt in folgender Definition zum Ausdruck.

Definition 16.1. Es sei S ein erststufiges Symbolalphabet und M und N seien S-Strukturen. Eine Abbildung

$$\varphi\colon\ M \longrightarrow N$$

heißt S- *Homomorphismus* , wenn folgende Eigenschaften gelten.

(1) Für jede Konstante $c \in S$ ist
$$\varphi(c^M) = c^N.$$
(2) Für jedes n-stellige Funktionssymbol $f \in S$ ist
$$\varphi(f^M(m_1, \ldots, m_n)) = f^N(\varphi(m_1), \ldots, \varphi(m_n))$$
für alle $m_1, \ldots, m_n \in M$.
(3) Für jedes n-stellige Relationsymbol $R \in S$ impliziert die Gültigkeit von
$$R^M(m_1, \ldots, m_n)$$
die Gültigkeit von
$$R^N(\varphi(m_1), \ldots, \varphi(m_n)).$$

Die üblichen Begriffe der Mathematik, beispielsweise ein Gruppenhomomorphismus, ein Ringhomomorphismus, eine lineare Abbildung zwischen Vektorräumen, eine monotone Abbildung zwischen geordneten Mengen, fallen unter diesen abstrakten Homomorphiebegriff.

Definition 16.2. Es sei S ein erststufiges Symbolalphabet und M und N seien S-Strukturen. Eine bijektive Abbildung
$$\varphi\colon M \longrightarrow N$$
heißt S- *Isomorphismus* , wenn sowohl φ als auch die Umkehrabbildung φ^{-1} ein S-Homomorphismus ist.

Zwei S-Strukturen heißen *S-isomorph*, wenn es einen S-Isomorphismus zwischen ihnen gibt. Bei $M = N$ spricht man auch von einem *Automorphismus*.

Beispiel 16.3. Es sei S ein erststufiges Symbolalphabet, das nur aus einer Variablenmenge besteht, die Konstantenmenge und die Mengen der Funktionssymbole und der Relationssymbole seinen also leer. Dann ist jede (nichtleere) Menge M unmittelbar eine S-Struktur und jede Abbildung
$$\varphi\colon M \longrightarrow N$$
ist ein S-Homomorphismus. Insbesondere ist jede bijektive Abbildung
$$\varphi\colon M \longrightarrow N$$
ein S-Isomorphismus.

Bemerkung 16.4. Es sei S ein erststufiges Symbolalphabet und M und N seien S-Strukturen. Eine bijektive Abbildung
$$\varphi\colon M \longrightarrow N,$$
die ein S-Homomorphismus ist, muss kein S-Isomorphismus sein, da die Umkehrabbildung φ^{-1} im Allgemeinen kein Homomorphismus sein muss. Deshalb fordert man in der Definition eines Isomorphismus explizit die Homomorphie der Umkehrabbildung. Wenn allerdings das Symbolalphabet S keine Relationssymbole enthält, so ist die Umkehrabbildung automatisch

ein Homomorphismus, siehe Aufgabe 16.3. Ein Extremfall liegt, vor, wenn ein Relationssymbol R in M als die leere Relation interpretiert wird. Dann verhält sich $\varphi\colon M \to N$ bezüglich dieses Relationssymbols S-homomorph, unabhängig von der Interpretation von R auf N.

Wir haben in Satz 12.3 gesehen, dass je zwei Modelle der (allerdings nicht erststufig formulierten) Dedekind-Peano-Axiome zueinander isomorph sind. Dabei war 0 die einzige Konstante und die Nachfolgerabbildung die einzige (einstellige) Funktion. Auch zwei Modelle der reellen Zahlen sind isomorph, was schwieriger zu beweisen ist. Die zugehörigen Axiomensysteme legen also das intendierte Modell bis auf Isomorphie fest, und zwar ist sogar jeweils der Isomorphismus eindeutig bestimmt. Letzteres gilt beispielsweise für die komplexen Zahlen nicht. Die komplexen Zahlen können als algebraischer Abschluss von $\mathbb{R}$ eingeführt werden. Je zwei solche algebraische Abschlüsse sind untereinander isomorph, allerdings ist die Isomorphie nicht eindeutig bestimmt. Beispielsweise ist die komplexe Konjugation ein nichttrivialer Automorphismus auf $\mathbb{C}$.

Lemma 16.5. *Es sei S ein erststufiges Symbolalphabet, M und N seien S-Strukturen und*

$$\varphi\colon M \longrightarrow N$$

ein S-Homomorphismus. Es sei λ eine Variablenbelegung in M und $\varphi \circ \lambda$ die nach N übertragene Variablenbelegung. Es seien I und J die zugehörigen Interpretationen. Dann ist

$$\varphi(I(t)) = J(t)$$

für alle S-Terme t.

Beweis. Siehe Aufgabe 16.10. □

16.2. **Elementare Äquivalenz und Isomorphiesatz.**

Definition 16.6. Zwei S-Strukturen M und N über einem erststufigen Symbolalphabet S heißen *elementar äquivalent*, wenn jeder S-Satz, der in M gilt, auch in N gilt.

Dies bedeutet, dass in den beiden Strukturen überhaupt die gleichen Sätze gelten. Die folgende Aussage heißt *Isomorphiesatz* (oder *Isomorphielemma*).

Satz 16.7. *Es seien M und N isomorphe S-Strukturen über einem Symbolalphabet S. Dann sind M und N elementar äquivalent. Genauer: Zu einem Isomorphismus*

$$\varphi\colon M \longrightarrow N$$

und einer Variablenbelegung λ auf M und der zugehörigen Variablenbelegung $\varphi \circ \lambda$ auf N mit den zugehörigen Interpretationen I und J gilt für jeden S-Ausdruck α die Äquivalenz

$$I \vDash \alpha \text{ genau dann, wenn } J \vDash \alpha\,.$$

Beweis. Wir beweisen den Zusatz durch Induktion über den Aufbau der Ausdrücke, woraus sich dann die Hauptaussage, die unabhängig von Belegungen ist, ergibt. Es sei ein Isomorphismus

$$\varphi\colon\ M \longrightarrow N$$

fixiert. Nach Lemma 16.5 respektiert der Isomorphismus die Interpretation aller Terme. Da die Situation symmetrisch ist, müssen wir lediglich zeigen, dass aus der Gültigkeit von $I \vDash \alpha$ die Gültigkeit von $J \vDash \alpha$ folgt. Für einen Ausdruck der Form

$$s = t$$

mit Termen s, t bedeutet

$$I \vDash s = t$$

einfach

$$I(s) = I(t).$$

Daher ist

$$J(s) = \varphi(I(s)) = \varphi(I(t)) = J(t)$$

und somit

$$J \vDash s = t\,.$$

Für ein n-stelliges Relationssymbol R und n Terme $t_1, \ldots, t_n$ bedeutet

$$I \vDash Rt_1 \ldots t_n\,,$$

dass R^M auf $(I(t_1), \ldots, I(t_n))$ zutrifft. Dann trifft aufgrund der Homomorphie von φ auch R^N auf

$$(\varphi(I(t_1)), \ldots, \varphi(I(t_n))) = (J(t_1), \ldots, J(t_n))$$

zu. Also ist

$$J \vDash Rt_1 \ldots t_n\,.$$

Wir kommen zum Induktionsschluss. Bei $\alpha = \neg\beta$, $\alpha = \beta \wedge \gamma$ und $\alpha = \beta \to \gamma$ folgt die Aussage aus der Induktionsvoraussetzung, wobei man bei der Negation und der Implikation verwendet, dass eine Äquivalenz bewiesen wird.

Für eine Existenzaussage $\exists x\beta$ bedeutet

$$I \vDash \exists x\beta\,,$$

dass es ein $m \in M$ derart gibt, dass

$$I\frac{m}{x} \vDash \beta$$

gilt. Es sei

$$n = \varphi(m).$$

Nach der Induktionsvoraussetzung, angewendet auf β und die Interpretation $J\frac{n}{x}$, die zu $I\frac{m}{x}$ in der gleichen Beziehung steht wie J zu I (d.h. die Variablenbelegungen sind durch φ miteinander verbunden) gilt

$$J\frac{n}{x} \vDash \beta\,.$$

Dies impliziert

$$J \vDash \exists x \beta \,.$$

□

Für die meisten Axiomensysteme in der Mathematik gibt es natürlich verschiedene nicht isomorphe und im Allgemeinen auch nicht elementar äquivalente Modelle. Es gibt beispielsweise eine Vielzahl an Gruppen, die - nach Definition - alle die Gruppenaxiome erfüllen, die aber ansonsten wenig miteinander zu tun haben. Interessanter ist die Frage, ob es, wenn man ein Axiomensystem für ein bestimmtes intendiertes Modell aufstellt, es dieses bis auf Isomorphie festlegt (oder ob es nichtisomorphe Modelle gibt) oder ob es die Menge aller gültigen elementaren Aussagen vollständig festlegt, also ob alle im intendierten Modell gültigen Sätze aus dem Axiomensystem ableitbar sind.

16.3. **Elementare Äquivalenz für Elemente.**

Inwiefern kann man die einzelnen Elemente in einer gegebenen S-Struktur M mit der durch S gegebenen Sprache einzeln adressieren bzw. voneinander unterscheiden? Zur Präzisierung dieser Fragestellung dient das Konzept der elementaren Äquivalenz für Elemente.

Definition 16.8. Es sei S ein erststufiges Symbolalphabet und M eine S-Struktur. Wir nennen zwei Elemente $m, n \in M$ *elementar äquivalent*, wenn für jeden Ausdruck $\alpha \in L_1^S$ in der einen freien Variablen x und jede Variablenbelegung λ auf M die Beziehung

$$I\frac{m}{x} \vDash \alpha \text{ genau dann, wenn } I\frac{n}{x} \vDash \alpha$$

gilt.

Die elementare Äquivalenz drücken wir durch $m \sim n$ aus. Dabei handelt es sich offenbar um eine Äquivalenzrelation auf der Menge M. Wenn

$$\varphi\colon\ M \longrightarrow M$$

ein S-Isomorphismus (also ein Automorphismus) ist, der m auf n abbildet, so müssen die beiden Elemente elementar äquivalent sein, wie aus Satz 16.7 für eine beliebige Interpretation $\tilde{I}$ mit $I = \tilde{I}\frac{m}{x}$ und $J = \tilde{I}\frac{n}{x}$ folgt.

Beispiel 16.9. Es sei S ein Symbolalphabet, das neben Variablen aus einem einzigen einstelligen Funktionssymbol f besteht und es sei $M = \{1, \ldots, 6\}$ eine S-Struktur, wobei f als die Permutation π mit

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	4	6	2

interpretiert werde. Hier sind die Äquivalenzklassen zur elementaren Äquivalenz gleich der sogenannten Zykelzerlegung, nämlich gleich $\{1,3\}$, $\{2,5,6\}$ und $\{4\}$. Die Ordnung der Elemente kann man in der Sprache zu S ausdrücken und erhält dadurch trennende Ausdrücke, beispielsweise ist $fx = x$ ein Ausdruck in der einen freien Variablen x, der genau dann wahr wird, wenn x durch 4 belegt wird. Der Ausdruck

$$(ffx = x) \wedge \neg (fx = x)$$

ist ein Ausdruck, der genau dann wahr wird, wenn x durch 1 oder 3 belegt wird, u.s.w. Dass 1 oder 3 zueinander elementar äquivalent sind, sieht man am einfachsten, wenn man den Automorphismus betrachtet, der durch die Transposition $1 \leftrightarrow 3$ gegeben ist. Dieser ist nämlich ein S-Automorphismus und daher können wir des Isomorphiesatz anwenden.

Beispiel 16.10. Wenn man in der Definition 16.8 auch Ausdrücke in mehreren freien Variablen zulassen würde, so wären Elemente nur mit sich selbst äquivalent. Betrachten wir dazu den Ausdruck $x = y$, den wir α nennen, und zwei Elemente $m \neq n$ aus M. In der Interpretation I sei y durch m belegt. Dann gilt $I\frac{m}{x} \vDash \alpha$, denn dies bedeutet $m = m$, aber $I\frac{n}{x} \nvDash \alpha$, denn dies bedeuet $n = m$.

Für eine Konstante in $c \in S$, die in M als das Element $m = c^M$ interpretiert wird, ist die zugehörige Äquivalenzklasse einelementig: Sie wird durch den Ausdruck $x = c$ in der einen freien Variablen x charakterisiert, der offenbar nur bei der Belegung von x durch m wahr wird. Wir fragen uns, ob es für jede Äquivalenzklasse zur elementaren Äquivalenz einen solchen *charakterisierenden Ausdruck* (oder *trennenden Ausdruck*) in einer freien Variablen gibt.

Lemma 16.11. *Es sei S ein Symbolalphabet erster Stufe und M eine S-Struktur mit der Eigenschaft, dass es in M nur endlich viele Klassen zur elementaren Äquivalenz gibt. Dann gibt es zu jeder Äquivalenzklasse $[m] \subseteq M$ einen S-Ausdruck $\alpha_{[m]}$ in einer freien Variablen x, der die Klasse $[m]$ beschreibt, für den also*

$$n \in [m] \text{ genau dann, wenn } I\frac{n}{x} \vDash \alpha_{[m]}$$

gilt.

Beweis. Es seien $M_1, \ldots, M_k$ die Äquivalenzklassen der elementaren Äquivalenzrelation und sei $m_i \in M_i$ ein fest gewählter Repräsentant. Wir zeigen, dass es für M_1 einen solchen trennenden Ausdruck gibt. Zu jedem $i = 2, \ldots, k$ gibt es einen Ausdruck β_i in der freien Variablen x mit $I\frac{m_1}{x} \vDash \beta_i$, aber $I\frac{m_i}{x} \nvDash \beta_i$, da ja m_1 und m_i nicht elementar äquivalent sind. Wir können annehmen, dass die relevante Variable in jedem dieser Ausdrücke die gleiche ist. Der konjugierte Ausdruck

$$\alpha_1 = \beta_2 \wedge \ldots \wedge \beta_k$$

ist in einer Interpretation (zur S-Struktur M) genau dann wahr, wenn die Variable x durch ein Element aus M_1 belegt wird. □

Beispiel 16.12. Für das Symbolalphabet $\{0,'\}$ und die natürlichen Zahlen $\mathbb{N}$ mit der kanonischen Interpretation sind sämtliche Klassen zur elementaren Äquivalenz einelementig und können auch durch Ausdrücke charakterisiert werden, und zwar wird die Zahl n durch den Ausdruck $x = 0''^{\cdots'}$ mit n Strichen eindeutig beschrieben.

Beispiel 16.13. Es sei S das Symbolalphabet, das außer Variablen für jedes $k \in \mathbb{N}_+$ ein einstelliges Relationssymbol R_k enthält, und es sei

$$\alpha_k \;=\; R_k x.$$

Wir betrachten die Menge $M = \mathbb{N}_+$, wobei wir das Relationssymbol R_k durch

$$R_k^M(n) \text{ genau dann, wenn } n \text{ ein Vielfaches von } k \text{ ist}$$

interpretieren. Zwei Elemente $m \neq n \in \mathbb{N}$ können dann nicht elementar äquivalent sein, da sie sich nicht gegenseitig teilen können und daher beispielsweise $R_m^M(m)$, also $I\frac{m}{x} \vDash \alpha_m$, aber nicht $R_m^M(n)$, also $I\frac{n}{x} \vDash \neg\alpha_m$, gilt. Die Äquivalenzklassen sind also einelementig. Es ist aber nicht möglich, diese Klassen durch einen Ausdruck in dieser Sprache zu charakterisieren, da die Gültigkeitsmengen zu jedem Ausdruck entweder leer sind oder unendlich viele Elemente enthalten, siehe Aufgabe 16.22.

Lemma 16.14. *Es sei S ein Symbolalphabet erster Stufe und M eine S-Struktur. Für jede elementare Äquivalenzklasse $[m] \subseteq M$ gebe es einen S-Ausdruck $\alpha_{[m]}$ in einer freien Variablen x, der die Klasse $[m]$ beschreibt, für den also*

$$n \in [m] \text{ genau dann, wenn } I\frac{n}{x} \vDash \alpha_{[m]}$$

gilt. Dann gelten folgende Aussagen.

(1) *Für jedes k-stellige Relationssymbol R ist R^M auf den Äquivalenzklassen wohldefiniert.*
(2) *Für jedes k-stellige Funktionssymbol f ist f^M auf den Äquivalenzklassen wohldefiniert (und zwar in dem Sinn, dass aus $m_1 \sim m_1', \ldots, m_k \sim m_k'$ die elementare Äquivalenz*

$$f^M(m_1, \ldots, m_k) \;\sim\; f^M(m_1', \ldots, m_k')$$

folgt).

Beweis. (1). Es sei R ein k-stelliges Relationssymbol. Für ein k-Tupel $(m_1, \ldots, m_k)$ aus M mit $(m_1, \ldots, m_k) \in R^M$ und ein weiteres dazu elementaräquivalentes Tupel $(n_1, \ldots, n_k)$ (es gelte also $m_1 \sim n_1$, $m_2 \sim n_2, \ldots, m_k \sim n_k$) müssen wir $(n_1, \ldots, n_k) \in R^M$ zeigen. Es seien $\alpha_1, \ldots, \alpha_k$ Ausdrücke in

der einen freien (untereinander verschiedenen) Variablen x_i, die die Äquivalenzklassen zu m_i bzw. n_i charakterisieren. Es gilt

$$I \vDash \exists x_1 \ldots \exists x_k \, (\alpha_1 \wedge \ldots \wedge \alpha_k \to Rx_1 \ldots x_k) \ ,$$

wie ja die Belegung von x_j durch m_j zeigt. Ebenso gilt

$$I\frac{m_1}{x_1} \vDash \exists x_2 \ldots \exists x_k \, (\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_k \to Rx_1x_2 \ldots x_k) \ ,$$

wie die entsprechende Belegung zeigt. Dies ist jetzt ein Ausdruck in der einen freien Variablen x_1. Wenn man x_1 statt mit m_1 durch ein anderes elementar äquivalentes Element n_1 belegt, so erhält man nach Definition der elementaren Äquivalenz

$$I\frac{n_1}{x_1} \vDash \exists x_2 \ldots \exists x_k \, (\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_k \to Rx_1x_2 \ldots x_k)$$

und damit

$$I \vDash \forall x_1 \exists x_2 \ldots \exists x_k \, (\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_k \to Rx_1x_2 \ldots x_k) \ .$$

Somit hat man den ersten Existenzquantor durch einen Allquantor ersetzt. In dieser Weise fährt man mit den anderen Existenzquantoren fort und erhält schließlich

$$I \vDash \forall x_1 \forall x_2 \ldots \forall x_k \, (\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_k \to Rx_1x_2 \ldots x_k) \ .$$

Einsetzen von n_j für x_j liefert also, da ja α_j auf n_j zutrifft,

$$I\frac{n_1, \ldots, n_k}{x_1, \ldots, x_k} \vDash Rx_1x_2 \ldots x_k$$

und somit $(n_1, \ldots, n_k) \in R^M$.

(2). Die Aussage für Funktionssymbole wird ähnlich bewiesen, siehe Aufgabe 16.27. □

16. Arbeitsblatt

16.1. **Übungsaufgaben.**

Aufgabe 16.1. Es sei S ein erststufiges Symbolalphabet und L, M, N seien S-Strukturen. Zeige folgende Aussagen.

(1) Die Identität
$$\mathrm{Id}_M \colon M \longrightarrow M$$
ist ein Isomorphismus.

(2) Zu einem Isomorphismus
$$\varphi \colon M \longrightarrow N$$
ist die Umkehrabbildung
$$\varphi^{-1} \colon N \longrightarrow M$$
ein Isomorphismus.

(3) Es seien

$$\psi\colon\ L \longrightarrow M$$

und

$$\varphi\colon\ M \longrightarrow N$$

Homomorphismen (Isomorphismen). Dann ist auch die Hintereinanderschaltung $\varphi \circ \psi$ ein Homomorphismus (Isomorphismus).

Aufgabe 16.2. Zeige, dass die Begriffe Gruppenhomomorphismus, Ringhomomorphismus, monotone Abbildung zwischen geordneten Mengen und lineare Abbildung unter den abstrakten Homomorphiebegriff (über welchem erststufigen Symbolalphabet S?) fallen.

Aufgabe 16.3. Es sei S ein erststufiges Symbolalphabet, das keine Relationssymbole enthalte. Zeige, dass ein bijektiver S-Homomorphismus zwischen zwei S-Strukturen bereits ein S-Isomorphismus ist.

Die nächste Aufgabe verwendet die folgende Definition.

Es seien $(M_1, \leq_1)$ und $(M_2, \leq_2)$ zwei Mengen, auf denen jeweils eine Ordnung definiert ist. Eine Abbildung

$$F\colon\ M_1 \longrightarrow M_2,\ x \longmapsto F(x),$$

heißt *ordnungstreu* (oder *monoton*), wenn für alle $x, x' \in M_1$ mit $x \leq_1 x'$ stets auch $F(x) \leq_2 F(x')$ gilt.

Aufgabe 16.4. Es sei $(M, \leq)$ eine geordnete Menge und $\mathfrak{P}(M)$ die Potenzmenge von M. Zeige, dass die Abbildung

$$M \longrightarrow \mathfrak{P}(M),\ x \longmapsto \{y \in M \mid y \leq x\},$$

ordnungstreu und injektiv ist, wobei die Potenzmenge mit der Inklusion versehen ist.

Aufgabe 16.5. Es sei M die Menge aller unendlichen Teilmengen von $\mathbb{N}_+$, versehen mit der Inklusion als Ordnung, und es sei $[0, 1[$ das rechtsseitig offene reelle Einheitsintervall mit der Kleinergleich-Relation als Ordnung. Zeige, dass die Abbildung

$$\Psi\colon\ M \longrightarrow [0, 1[,\ T \longmapsto \sum_{n \notin T} \left(\frac{1}{2}\right)^n,$$

eine bijektive, ordnungstreue Abbildung ist, deren Umkehrabbildung nicht ordnungstreu ist.

Warum beschränkt man sich auf unendliche Teilmengen? Wie sehen die „transportierten Ordnungen“ aus?

Aufgabe 16.6. Es sei S ein Symbolalphabet, das neben Variablen aus einem einzigen einstelligen Relationssymbol besteht. Was bedeutet ein S-Homomorphismus? Welche mathematische Signifikanz hat dieser Begriff?

Aufgabe 16.7. Es sei S ein Symbolalphabet, das neben Variablen aus einem einzigen einstelligen Funktionssymbol besteht. Was bedeutet ein S-Homomorphismus? Welche mathematische Signifikanz hat dieser Begriff?

Aufgabe 16.8. Es sei S ein Symbolalphabet erster Stufe. Definiere eine S-„Unterstruktur“ in einer S-Struktur M.

Aufgabe 16.9.*

Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Es sei I eine S-Interpretation mit der Grundmenge N und es sei $\Gamma := I^{\vDash}$ mit der zugehörigen Äquivalenzrelation $\sim$ auf der Termmenge T.

(1) Zeige, dass $s \sim t$ genau dann gilt, wenn $I(s) = I(t)$ gilt.
(2) Zeige, dass es eine injektive Abbildung
$$\psi\colon T/\sim \longrightarrow N$$
mit
$$\psi([t]) = I(t)$$
gibt.
(3) Zeige, dass ψ ein S-Homomorphismus ist, wenn die Quotientenmenge $T/\sim$ mit der kanonischen S-Struktur versehen wird.
(4) Es sei J die kanonische Interpretation auf $T/\sim$. Es sei vorausgesetzt, dass die Terminterpretation für N surjektiv sei. Zeige, dass $I \vDash \alpha$ genau dann gilt, wenn $J \vDash \alpha$ gilt.

Aufgabe 16.10. Es sei S ein erststufiges Symbolalphabet, M und N seien S-Strukturen und
$$\varphi\colon M \longrightarrow N$$
ein Homomorphismus. Es sei λ eine Variablenbelegung in M und $\varphi \circ \lambda$ die nach N übertragene Variablenbelegung. Es seien I und J die zugehörigen Interpretationen. Zeige, dass
$$\varphi(I(t)) = J(t)$$
für alle S-Terme t gilt.

Unter einem *Automorphismus* einer S-Struktur M versteht man einen Isomorphismus von M nach M. Man spricht von der *S-Automorphismengruppe* von M, geschrieben $S - \mathrm{Aut}\ M$.

Aufgabe 16.11. Es sei S ein erststufiges Symbolalphabet und M sei eine S-Struktur. Zeige, dass die Menge der S-Automorphismen auf M eine Gruppe bildet.

Aufgabe 16.12. Es sei $S = \{0, +\}$ und $\mathbb{Z}$ sei versehen mit der natürlichen S-Interpretation. Bestimme die S-Automorphismengruppe von $\mathbb{Z}$.

Aufgabe 16.13. Es sei S ein erststufiges Symbolalphabet und M eine S-Struktur. Zeige, dass die elementare Äquivalenz von Elementen $m, n \in M$ eine Äquivalenzrelation auf M ist.

Aufgabe 16.14. In einer Wohngemeinschaft wohnen Albert, Beowulf, Clara, Dora, Emil und Gundula. Dabei können Albert und Beowulf kochen, die anderen vier nicht. Emil findet Beowulf doof, Dora findet Albert und Clara doof, Clara und Gundula finden beide ebenfalls den Albert doof. Charakterisiere jede Person durch einen sprachlichen Ausdruck, in dem nur auf die Kochfähigkeit und das Dooffinden Bezug genommen wird.

Aufgabe 16.15.*

In einer Wohngemeinschaft leben die Personen A, B, C, D, E. Wir betrachten die folgenden Relationen:

(1) Txy bedeutet, dass x und y manchmal miteinander Tennis spielen,
(2) $Sxyz$ bedeutet, dass x, y und z manchmal miteinander Skat spielen,
(3) $Kxyzw$ bedeutet, dass x, y, z und w manchmal miteinander Doppelkopf spielen.

In der WG gilt

$$TDE, SABC, SABE, KACED\,.$$

(1) Charakterisiere umgangssprachlich die Person D allein unter Bezugnahme auf die gegebenen Spielrelationen.
(2) Charakterisiere umgangssprachlich die Person C allein unter Bezugnahme auf die gegebenen Spielrelationen.
(3) Charakterisiere prädikatenlogisch durch einen Ausdruck mit der einzigen freien Variablen x und den Relationssymbolen T, S, K die Person A.
(4) Charakterisiere prädikatenlogisch durch einen Ausdruck mit der einzigen freien Variablen x und den Relationssymbolen T, S, K die Person B.
(5) Charakterisiere prädikatenlogisch durch einen Ausdruck mit der einzigen freien Variablen x und den Relationssymbolen T, S, K die Person E.

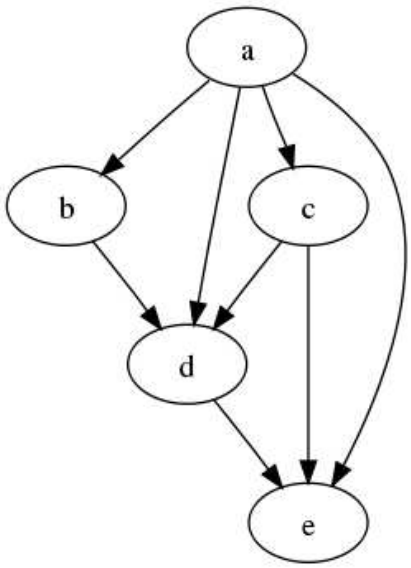
Aufgabe 16.16. Es sei S ein erststufiges Symbolalphabet, das nur aus einer Variablenmenge besteht, die Konstantenmenge und die Mengen der Funktionssymbole und der Relationssymbole seien also leer. Zeige, dass je zwei Elemente $m, n \in M$ elementar äquivalent sind.

Aufgabe 16.17. Es sei S ein Symbolalphabet, das neben Variablen aus einem einzigen einstelligen Funktionssymbol f besteht und es sei $M = \{1, \ldots, 8\}$ eine S-Struktur, wobei f als die Permutation π mit

x	1	2	3	4	5	6	7	8
$\pi(x)$	2	5	6	8	4	3	1	7

interpretiert werde. Bestimme die elementar äquivalenten Elemente von M.

Aufgabe 16.18.*



Charakterisiere den Punkt d im skizzierten Graphen mit einem Ausdruck in einer freien Variablen x über dem Symbolalphabet, das neben Variablen aus einem einzigen zweistelligen Relationssymbol R besteht, das im angegebenen Modell durch einen Pfeil wiedergegeben wird.

Aufgabe 16.19. Wir betrachten das Symbolalphabet $S = \{+, 0\}$ mit der natürlichen Interpretation auf $\mathbb{N}$. Zeige, dass jedes Element nur zu sich selbst elementar äquivalent ist.

Aufgabe 16.20. Es seien die Symbolalphabete $S = \{+, 0\}$, $T = \{+, 0, 1\}$, und $R = \{0, 1, +, \cdot\}$ gegeben, die wir auf $\mathbb{Z}$ natürlich interpretieren. Bestimme zu diesen Symbolalphabeten jeweils die Äquivalenzklassen zur elementaren Äquivalenz.

Aufgabe 16.21. Bestimme die Äquivalenzklassen zur elementaren Äquivalenz in der zyklischen Gruppe $\mathbb{Z}/(4)$ zum Symbolalphabet $S = \{0, +\}$.

Aufgabe 16.22. Bestimme die Äquivalenzklassen zur elementaren Äquivalenz in der Gruppe $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ zum Symbolalphabet $S = \{0, +\}$.

Aufgabe 16.23. Es sei S das Symbolalphabet, das außer Variablen für jedes $k \in \mathbb{N}_+$ ein einstelliges Relationssymbol R_k enthält. Wir betrachten die Menge $M = \mathbb{N}_+$, wobei wir das Relationssymbol R_k durch

$$R_k^M(n) \text{ genau dann, wenn } n \text{ ein Vielfaches von } k \text{ ist}$$

interpretieren. Es sei $\alpha \in L^S$ ein Ausdruck in einer freien Variablen x, wobei in α die Relationssymbole $R_{k_1}, \ldots, R_{k_m}$ vorkommen mögen. Es sei k das kleinste gemeinsame Vielfache von $k_1, \ldots, k_m$. Zeige, dass

$$M\frac{n}{x} \vDash \alpha$$

genau dann gilt, wenn

$$M\frac{n+k}{x} \vDash \alpha$$

gilt.

Aufgabe 16.24. Es sei S das Symbolalphabet, das neben Variablen aus einem zweistelligen Relationssymbol G besteht und es sei

$$\Gamma = \{\forall x \forall y\, (Gxy \to \neg Gyx)\}.$$

Zeige, dass eine vierelementige S-Struktur, die Γ erfüllt, äquivalent zur Gewinnstruktur in einer Vorgruppe bei einer Fußballweltmeisterschaft ist.

(Bemerkung: Eine zweistellige Relation wird oft durch ein Pfeildiagramm veranschaulicht.)

Aufgabe 16.25. Es sei S das Symbolalphabet, das neben Variablen aus einem zweistelligen Relationssymbol G besteht und es sei

$$M = \{\text{Bra}, \text{Kam}, \text{Kro}, \text{Mex}\}$$

die S-Struktur, bei der $G(m, n)$ als m gewinnt gegen n (bei der Fußballweltmeisterschaft 2014) interpretiert wird. Bestimme die Äquivalenzklassen zur elementaren Äquivalenz, trennende Ausdrücke und die Automorphismengruppe.

Aufgabe 16.26. Es sei S das Symbolalphabet, das neben Variablen aus einem zweistelligen Relationssymbol G besteht. Wir betrachten Modelle, die aus einer vierelementigen Menge M mit einer zweistelligen (Gewinn)-relation G^M bestehen und die die Aussage $\forall x \forall y \, (Gxy \to \neg Gyx)$ erfüllen. Zeige, dass zwei verschiedene Elemente $m, n \in M$ zueinander elementar äquivalent sein können, obwohl $G^M(m, n)$ gilt (m und n spielen also nicht unentschieden).

Aufgabe 16.27. Ein Turnier werde im KO-System mit 2^n Mannschaften ausgetragen, jedes Spiel endet also mit einem Gewinner und einem Verlierer und der Verlierer scheidet direkt aus (es gebe kein Spiel um Platz drei oder ähnliches). Das Turnier sei vorbei. Zeige, dass man jede Mannschaft in der Prädikatenlogik allein mit der Gewinnrelation adressieren kann (je zwei Mannschaften sind also nicht elementar äquivalent).

Aufgabe 16.28. Es sei S ein Symbolalphabet erster Stufe und M eine S-Struktur. Für jede elementare Äquivalenzklasse $[m] \subseteq M$ gebe es einen S-Ausdruck $\alpha_{[m]}$ in einer freien Variablen x, der die Klasse $[m]$ beschreibt. Zeige, dass für jedes k-stellige Funktionssymbol f aus $m_1 \sim m_1', \ldots, m_k \sim m_k'$ die elementare Äquivalenz $f^M(m_1, \ldots, m_k) \sim f^M(m_1', \ldots, m_k')$ folgt.

Aufgabe 16.29. Es sei S ein Symbolalphabet erster Stufe und M eine S-Struktur. Für jede elementare Äquivalenzklasse $[m] \subseteq M$ gebe es einen S-Ausdruck $\alpha_{[m]}$ in einer freien Variablen x, der die Klasse $[m]$ beschreibt. Zeige, dass für ein k-stelliges Funktionssymbol f aus $m_1 \sim m_1', \ldots, m_k \sim m_k'$ nicht die Gleichheit $f^M(m_1, \ldots, m_k) = f^M(m_1', \ldots, m_k')$ folgen muss.

16.2. **Aufgaben zum Abgeben.**

Aufgabe 16.30. (4 Punkte)

Es seien $\Gamma \subseteq \Gamma' \subseteq L^S$ widerspruchsfreie Ausdrucksmengen, die unter Ableitungen abgeschlossen seien, und seien M bzw. M' die gemäß der Konstruktion zugehörigen Modelle. Zeige, dass es einen S-Homomorphismus

$$M \longrightarrow M'$$

gibt.

Aufgabe 16.31. (2 Punkte)

Es sei S ein Symbolalphabet, das neben Variablen aus einem einzigen einstelligen Funktionssymbol f besteht und es sei $M = \{1, \ldots, 10\}$ eine S-Struktur, wobei f als die Permutation π mit

x	1	2	3	4	5	6	7	8	9	10
$\pi(x)$	5	10	8	4	3	6	9	1	7	2

interpretiert werde. Bestimme die elementar äquivalenten Elemente von M.

Aufgabe 16.32. (4 Punkte)

Es sei S das Symbolalphabet, das neben Variablen aus einem zweistelligen Relationssymbol G besteht und es sei

$$M = \{\text{Deu}, \text{Gha}, \text{Por}, \text{USA}\}$$

die S-Struktur, bei der $G(m,n)$ als m gewinnt gegen n (bei der Fußballweltmeisterschaft 2014) interpretiert wird. Bestimme die Äquivalenzklassen zur elementaren Äquivalenz, trennende Ausdrücke und die Automorphismengruppe.

Aufgabe 16.33. (8 Punkte)

Klassifiziere (bis auf Isomorphie) die möglichen Gewinnstrukturen bei einer Vierergruppe (wie bei einer Fußballweltmeisterschaft).

(Bemerkung: Es wird also eine vollständige Liste aller möglichen Isomorphietypen verlangt. Die Liste muss systematisch sein und die Vollständigkeit begründet werden.)

Aufgabe 16.34. (2 Punkte)

Es sei S ein erststufiges Symbolalphabet und M, N seien S-isomorphe S-Strukturen. Zeige, dass die zugehörigen Automorphismengruppen $\text{Aut}_S\, M$ und $\text{Aut}_S\, N$ isomorph sind.

Aufgabe 16.35. (3 Punkte)

Bestimme die Äquivalenzklassen zur elementaren Äquivalenz in der zyklischen Gruppe $\mathbb{Z}/(8)$ zum Symbolalphabet $S = \{0, +\}$.

17. Vorlesung - Elementare Äquivalenz II

17.1. Isomorphie und elementare Äquivalenz im endlichen Fall.

Wir möchten zeigen, dass bei endlichen Mengen die elementare Äquivalenz den Isomorphietyp bereits festlegt. Wir besprechen zunächst einige typische Beispiele, die als Orientierung für den komplexen Beweis dienen sollen.

Beispiel 17.1. Es sei S ein Symbolalphabet, das ausschließlich aus (abzählbar unendlich vielen) Variablen bestehe. Zwei endliche S-Mengen M und N sind genau dann elementar äquivalent, wenn sie die gleiche Anzahl an Elementen haben, denn die Elementanzahl kann man durch einen erststufigen Ausdruck aus L^S ausdrücken. In diesem Fall gibt es eine Bijektion zwischen M und N und diese ist ein S-Isomorphismus.

Beispiel 17.2. Das Symbolalphabet S bestehe (neben Variablen) aus einem einstelligen Funktionssymbol f. Die Ausdrucksmenge Γ bestehe aus einem Satz, der inhaltlich besagt, dass eine erfüllende Menge genau n Elemente besitzen muss, und einen Satz, der besagt, dass die Funktion bijektiv ist. Ein Modell für Γ ist also eine n-elementige Menge M zusammen mit einer fixierten Permutation

$$f^M\colon\ M \longrightarrow M$$

auf dieser Menge. Eine Teilmenge $T \subseteq M$ der Form

$$T = \{m, f(m), f^2(m), \ldots, f^{k-1}(m)\}$$

mit $f^k(m) = m$ und mit $f^i(m) \neq m$ für alle i, $1 \leq i \leq k-1$, nennt man Zykel zu f der Länge k. Die Menge M ist die disjunkte Vereinigung von Zykeln unterschiedlicher Länge. Zwei Elemente $m, n \in M$ sind genau dann elementar äquivalent, wenn sie beide in einem gleichlangen (aber nicht unbedingt im gleichen) Zykel liegen: Einerseits lässt sich die Zykellänge k erststufig formalisieren, etwa durch

$$f^k x = x \wedge f^{k-1}x \neq x \wedge \ldots \wedge fx \neq x\,,$$

wobei die Potenzen ausgeschrieben werden müssen. Andererseits kann man einfach Automorphismen angeben, indem man aus jedem Zykel Z_j ein Element m_j auswählt und dieses auf ein beliebiges Element $n_j = \psi(m_j)$ eines Zykels gleicher Länge schickt, wobei jeder Zykel genau einmal getroffen wird. Durch

$$\psi(f^i(m_j)) := f^i(\psi(m_j))$$

erhält man einen wohldefinierten Automorphismus. Insbesondere kann man einen Automorphismus konstruieren, der m auf n abbildet. Wenn man m auf n (elementar äquivalent zu m) abbilden möchte, so ist dadurch schon bestimmt, wohin man die Elemente aus dem Zyklel zu m abbilden muss. Es muss nämlich $\psi(fm) = f\psi(m)$, $\psi(ffm) = ff\psi(m)$, u.s.w. gelten.

Beispiel 17.3. Wir betrachten das Symbolalphabet S, das neben Variablen aus einer Konstanten 0 und einem zweistelligen Funktionssymbol + besteht. Wir betrachten die Gruppe $\mathbb{Z}/(8)$ mit der natürlichen S-Struktur. Die elementaren Äquivalenzklassen sind durch die Ordnung der Elemente gegeben. Die Klassen sind

$$\{\{0\}, \{4\}, \{2,6\}, \{1,3,5,7\}\}\,.$$

Bei einen S-Automorphismus auf $\mathbb{Z}/(8)$ müssen die einelementigen Klassen auf sich selbst abgebildet werden, bei den anderen hat man gewisse Freiheiten. Allerdings gibt es Abhängigkeiten zwischen den Wahlmöglichkeiten auf

den größeren Klassen. Wenn man 2 auf 6 abbilden möchte, so muss man zunächst 6 auf 2 abbilden. Wenn man diese partielle Abbildung

$$\{0,2,4,6\} \longrightarrow \{0,1,2,3,4,5,6,7,8\}$$

fortsetzen möchte, so muss man beispielsweise 3 wegen $3+3=6 \mapsto 2$ auf 1 oder auf 5 abbilden, die Werte 3 oder 7 sind ausgeschlossen.

Beispiel 17.4. Es sei S ein Symbolalphabet und M eine S-Struktur mit der Eigenschaft, dass jede Äquivalenzklasse zur elementaren Äquivalenz einelementig sei. Wenn N eine weitere, zu M elementar äquivalente S-Struktur ist, so hat auch diese einelementige Äquivalenzklassen. Die einzige Möglichkeit für einen S-Isomorphismus $M \to N$ ist dann, ein Element m auf das einzige Element $n \in N$ abzubilden, das den entsprechenden charakteristischen Ausdruck erfüllt. Es muss dann allerdings begründet werden, dass es sich wirklich um einen Homomorphismus handelt.

Aus den Überlegungen der letzten Vorlesung erhalten wir das folgende Resultat. Im Beweis arbeiten wir mit folgender Definition.

Definition 17.5. Es sei S ein erststufiges Symbolalphabet umd M eine S-Struktur. Eine Teilmenge $T \subseteq M$ heißt *funktional abgeschlossen* (oder eine S- *Unterstruktur*), wenn für jede Konstante $c \in S$ das Element c^M zu T gehört und für jedes k-stellige Funktionssymbol f und beliebige Elemente $m_1, \ldots, m_k \in T$ auch $f^M(m_1, \ldots, m_k)$ zu T gehört.

Unter einem *formal-zusammengesetzten Funktionssymbol* (oder *Funktionssymbolbaum*) versteht man die Elemente der folgenden rekursiv festgelegten Menge (innerhalb der Menge von Stammbäumen).

(1) Jedes Funktionssymbol (einschließlich der Konstanten) gehört dazu.
(2) Wenn f ein k-stelliges Funktionssymbol ist und $F_1, \ldots, F_k$ formal-zusammengesetzteFunktionssymbole, so ist auch der Stammbaum (nicht die Symbolkette) $fF_1 \ldots F_k$ ein formal-zusammengesetztes Funktionssymbol.

Bei einer Interpretation mit Grundmenge M wird ein formal-zusammengeetztes Funktionssymbol F als Hintereinanderschaltung der beteiligten Abbildungen interpretiert, wofür wir wieder F^M schreiben. Eine funktional abgeschlossene Menge ist auch unter jeder formal-zusammengesetzten Funktion abgeschlossen, siehe Aufgabe 17.8 und zu einer Startmenge $U \subseteq M$ besteht die kleinste funktional abgeschlossene Teilmenge, die U enthält, genau aus den Werten der formal-zusammengesetzten Funktionen mit Argumenten aus U. (die *funktionale Hülle* von U). Wenn man mit einem Element m startet, und nur ein einstelliges Funktionssymbol zur Verfügugn hat, so besteht die funktionale Hülle einfach aus $m, f(m), f(f(m)), f(f(f(m))), ...$

Satz 17.6. *Es sei S ein Symbolalphabet und es seien M und N S-Strukturen, wobei M endlich sei. Dann sind M und N genau dann elementar äquivalent, wenn sie zueinander isomorph sind.*

Beweis. Dass eine Isomorphie elementare Äquivalenz impliziert, wurde in Satz 16.7 bewiesen. Für die Umkehrung seien also die beiden Strukturen elementar äquivalent, und M habe r Elemente. Dann gilt in M die Aussage

$$\exists x_1 \exists x_2 \ldots \exists x_r (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \ldots \wedge x_1 \neq x_r \wedge x_2 \neq x_3 \wedge \ldots \wedge x_2 \neq x_r \wedge \ldots \wedge x_{r-1} \neq x_r)$$

und die entsprechende Aussage für $r+1$ gilt nicht. Aufgrund der elementaren Äquivalenz gilt diese Aussage (bzw. die entsprechende Aussage) auch (nicht) in N. D.h. N ist ebenfalls endlich mit r Elementen.

Wir konstruieren nun sukzessive Teilmengen $S_j \subset S_{j+1} \subseteq M$, wobei die S_j funktional abgeschlossen sind, und Abbildungen

$$\psi_j \colon S_j \longrightarrow N$$

mit $\psi_{j+1}|_{S_j} = \psi_j$ und derart, dass die ψ_j für jedes j Isomorphismen zwischen S_j und $T_j = \operatorname{bild} \psi_j$ sind.

Wir wählen $m_1 \in M$ beliebig und setzen S_1 als die kleinste, funktional abgeschlossene Teilmenge in M an, die m_1 enthält. Nach Lemma 16.11 gibt es einen Ausdruck α in einer freien Variablen, der die elementare Äquivalenzklasse $[m_1]$ beschreibt. Wir wählen ein Element $n_1 \in N$ aus der α entsprechenden Äquivalenzklasse in N (und diese ist nicht leer wegen der elementaren Äquivalenz zwischen M und N) und setzen

$$\psi_1(m_1) := n_1.$$

Für jedes formal-zusammengesetzte Funktionssymbol F definieren wir

$$\psi_1(F^M(m_1)) := F^N(\psi_1(m_1)) = F^N(n_1).$$

Diese Abbildung ist wohldefiniert. Ist nämlich

$$m = F^M(m_1) = G^M(m_1),$$

so gilt in M

$$\forall x \, (\alpha \to F(x) = G(x)) \, ,$$

da dies für m_1 gilt und daher auch für alle dazu elementar äquivalenten Elemente, und da für die dazu nicht elementar äquivalenten Elemente der Vordersatz nicht gilt. Diese Aussage gilt dann auch bei Interpretation über N. Daher ist

$$F^N(n_1) = G^N(n_1).$$

Wir müssen zeigen, dass ein Homomorphismus vorliegt. Die Verträglichkeit mit den Funktionssymbolen folgt unmittelbar aus der Definition der Abbildung. Ferner wird jedes Element zu einem Element aus der entsprechenden

Äquivalenzklasse abgebildet. Nach (dem Beweis zu) Lemma 16.14 und wegen der elementaren Äquivalenz berücksichtigt ψ daher die Relationen. Dies gilt in beide Richtungen, d.h. eine Relation trifft auf ein Tupel genau dann zu, wenn dies auf das Bildtupel zutrifft. Die Abbildung ist injektiv: Zu zwei Elementen $m, m' \in S_1$ gibt es zusammengesetzte Funktionssymbole F und G mit $m = F^M(m_1)$ und $m' = G^M(m_1)$ Bei $m \neq m'$ gilt

$$\models \forall x \, (\alpha \to Fx \neq Gx) \ ,$$

da dies bei Interpretation von x durch m_1 gilt, und diese Aussage gilt auch in N. Die Abbildung ist surjektiv auf das Bild, also liegt wegen der Äquivalenz bei den Relationen insgesamt ein Isomorphismus vor.

Es seien nun S_j und ψ_j schon konstruiert und $S_j \neq M$. Wir wählen $m_{j+1} \in M \setminus S_j$ und betrachten die funktionale Hülle von $S_j \cup \{m_{j+1}\}$. Wir betrachten die Menge aller Tupel $(\beta, m_1, \ldots, m_k)$, wobei $\beta \in L^S$ ein Ausdruck in den freien Variablen $x_1, \ldots, x_k$ und y ist und wobei $m_1, \ldots, m_k \in S_j$ (das müssen nicht die in der Konstruktion der ψ_j gewählten Elemente sein) mit der Eigenschaft, dass

$$I\frac{m_1, \ldots, m_k}{x_1, \ldots, x_k}\frac{m_{j+1}}{y} \models \beta$$

gilt. Dabei sei I eine fixierte Interpretation auf M und J entsprechend eine Interpretation auf N. Es gilt dann insbesondere

$$I\frac{m_1, \ldots, m_k}{x_1, \ldots, x_k} \models \exists y \beta \, .$$

Daher gilt nach Satz 16.7 (angewendet auf den Isomorphismus ψ_j mit $n_i = \psi_j(m_i)$) auch

$$J\frac{n_1, \ldots, n_k}{x_1, \ldots, x_k} \models \exists y \beta \, ,$$

und insbesondere gibt es ein (zunächst von β abhängiges) $n \in N$ mit

$$J\frac{n_1, \ldots, n_k}{x_1, \ldots, x_k}\frac{n}{y} \models \beta \, .$$

Dann gibt es auch ein $n \in N$, das man für alle β nehmen kann. Für jedes einzelne β ist nämlich die erfüllende Elementmenge nicht leer, und wenn der Durchschnitt über alle β leer wäre, dann schon für eine endliche Teilmenge und dann auch für die endliche Konjunktion darüber. Sei n_{j+1} ein solches Element. Wir setzen nun

$$\psi_{j+1}(m_{j+1}) := n_{j+1}$$

und definieren

$$\psi_{j+1}(F^M(m_1, \ldots, m_k, m_{j+1})) := F^N(n_1, \ldots, n_k, n_{j+1})$$

für jedes $k+1$-stellige formal zusammengesetzte Funktionssymbol F. Die Wohldefiniertheit von ψ_{j+1}, die Verträglichkeit mit den Funktionssymbolen und mit den Relationssymbolen (in beide Richtungen) sowie die Bijektivität und damit die Isomorphieeigenschaft folgt wie oben.

Da M endlich ist, erhalten wir, wenn wir diesen Konstruktionsschritt iterieren, insgesamt eine injektive Abbildung

$$\psi\colon\ M \longrightarrow N.$$

Da M und N gleich viele Elemente besitzen, ist diese auch surjektiv und insgesamt erhalten wir einen Isomorphismus. □

Das im Beweis beschriebene Verfahren zur Konsrtuktion eines Isomorphismus ist grundsätzlich konstruktiv.

17.2. **Nichtstandardmodelle.**

Definition 17.7. Es sei M eine fixierte S-Struktur (das *Standardmodell*) über einem Symbolalphabet S. Dann nennt man eine weitere S-Struktur M', die zu M elementar äquivalent, aber nicht zu M S-isomorph ist, ein *Nichtstandardmodell* von M.

Bemerkung 17.8. So formuliert ist diese Definition für jedes Modell M anwendbar. Man verwendet sie aber eigentlich nur dann, wenn ein wohlbestimmtes „prominentes“ Modell M ausgezeichnet ist. Das Standardmodell ist dann in der Regel durch den Kontext festgelegt. Im zahlentheoretischen Kontext ist $\mathbb{N}$ das Standardmodell, die entsprechenden Nichtstandardmodelle heißen *Nichtstandardmodelle der Arithmetik*, die Untersuchung solcher Modelle heißt *Nichtstandardarithmetik*. Im analytschen Kontext sind die reellen Zahlen das Standardmodell, die entsprechenden Nichtstandardmodelle heißen *Nichtstandardmodelle der reellen Zahlen*; man spricht von *Nichtstandardanalysis*.

Es ist keineswegs selbstverständlich, dass es Nichtstandardmodelle gibt. Dies ergibt sich, und zwar ganz allgemein für jede unendliche Struktur, aus einer Reihe von Überlegungen, die an den Vollständigkeitssatz anschließen. Ein wesentlicher Punkt ist dabei, dass man zwar die Unendlichkeit eines Modells durch ein erststufiges Axiomenschema beschreiben kann, nicht aber erststufig verschiedene Mächtigkeiten unterscheiden kann. Zu $n \in \mathbb{N}$ beschreibt die Aussage

$$\alpha_n \ = \ \exists x_1 \ldots \exists x_n \left(\wedge_{i\neq j}(x_i \neq x_j)\right),$$

dass es mindestens n verschiedene Elemente gibt (d.h. diese Aussage ist interpretiert in einem Modell M genau dann richtig, wenn M mindestens n Elemente besitzt). Die Ausdrucksmenge

$$\Gamma_\infty \ = \ \{\alpha_n |\, n \in \mathbb{N}\}$$

beschreibt daher die Unendlichkeit einer Menge. Aufgabe 15.16 zeigt, dass es Nichtstandardmodelle der Arithmetik gibt (siehe auch Korollar 15.11) und Aufgabe 15.15 zeigt (das Argument werden wir gleich wiederholen), dass es abzählbare Modelle gibt, die zu den reellen Zahlen elementar äquivalent sind. Man spricht von reell-abgeschlossenen Körpern.

17.3. **Reell-abgeschlossene Körper.**

Beispiel 17.9. Die Symbolmenge S bestehe aus $0, 1, +, \cdot$ (und abzählbar unendlich vielen Variablen), die in den reellen Zahlen $\mathbb{R}$ in natürlicher Weise interpretiert werden. Die Ausdrucksmenge

$$\Gamma = \mathbb{R}^{\vDash}$$

ist somit widerspruchsfrei. Der Beweis zu Lemma 15.3 zeigt, dass es dann eine abzählbare Symbolerweiterung $S' \supseteq S$ und eine S'-Ausdrucksmenge Γ' gibt, die Beispiele enthält (es ist nicht selbstverständlich, ob Γ selbst Beispiele enthält. Da es überabzählbar viele reelle Zahl gibt, liegt nicht jede reelle Zahl im Bild der Terminterpretation, so dass man Lemma 14.5 nicht anwenden kann), und die nach Lemma 15.4 zu einer maximal widerspruchsfreien Ausdrucksmenge ergänzt werden kann. Nach dem Satz von Henkin gibt es ein erfüllendes Modell, das aus Identifizieren von Termen entsteht. Da die Termmenge abzählbar ist, ist auch dieses Modell abzählbar. Es gibt daher ein abzählbares Nichtstandardmodell der reellen Zahlen.

Die Menge der rationalen Zahlen bilden einen abzählbaren angeordneten Körper, aber kein Nichtstandardmodell der reellen Zahlen, da ja beispielsweise die Aussage $\exists x(x^2 = 2)$ in $\mathbb{R}$ gilt, aber nicht in $\mathbb{Q}$. Wichtige erststufige Aussagen, die in $\mathbb{R}$ und damit auch in jedem Nichtstandardmodell gelten, fassen wir in folgender Proposition zusammen.

Proposition 17.10. *Für die reellen Zahlen gelten folgende Aussagen über dem Symbolalphabet*[24] $S = \{0, 1, +, \cdot, x_n, n \in \mathbb{N}\}$

(1) *Die Axiome eines*[25] *angeordneten Körpers.*
(2) *Für jedes ungerade $n \in \mathbb{N}$ gilt*

$$\forall c_0 \forall c_1 \ldots \forall c_n \left((c_n \neq 0) \to \exists x \left(c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0 \right) \right) .$$

(3) *Für jedes gerade $n \in \mathbb{N}$ gilt*

$$\forall x \left(\exists y \left((y^n = x) \vee (y^n = -x) \right) \right) .$$

(4) *Für jeden S-Ausdruck α in einer freien Variablen x gilt*

$$\exists x \alpha \wedge \exists b \forall x \left(\alpha \to x \leq b \right) \to \exists s \left(\forall x \left(\alpha \to x \leq s \right) \right.$$
$$\left. \wedge \forall c \forall x \left(\alpha \to x \leq c \right) \to s \leq c \right) .$$

[24] Um die Lesbarkeit zu erhöhen benutzen wir auch andere Variablennamen.

[25] Die Beziehung $u \geq v$ wird durch $\exists t(t^2 = u - v)$ erklärt. Alternativ kann man die Symbolmenge um $\geq$ ergänzen.

(5) *Für jeden S-Ausdruck α in einer freien Variablen x gilt*

$$\Big(\exists x\alpha \wedge \exists x\neg\alpha \wedge \forall x\forall y\left(x \leq y \to \left(\alpha\frac{y}{x} \to \alpha\right)\right) \\ \wedge\forall x\forall y\left(y \leq x \to \left(\neg\alpha\frac{y}{x} \to \neg\alpha\right)\right)\Big) \to \exists s\left(\forall x\left(\alpha \to x \leq s\right)\right. \\ \left.\wedge\forall x\left(\neg\alpha \to x \geq s\right)\right).$$

Beweis. (1) ist in der Axiomatik der reellen Zahlen enthalten. (2) folgt aus dem Zwischenwertsatz, der Stetigkeit von Polynomen und dem Verhalten von Polynomen von ungeradem Grad gegen $\pm\infty$. (3) folgt aus wiederholter Anwendung von Satz 7.4 (Analysis (Osnabrück 2014-2016)) und Teil (2). (4) ist eine Formulierung von Satz 7.5 (Analysis (Osnabrück 2014-2016)) für solche Teilmengen, die in der ersten Stufe beschrieben werden können. (5) folgt aus dem Dedekindschen Schnittaxiom. □

Diese Eigenschaften (insbesondere die beiden letzten) sind ein erststufiger Ersatz für die Vollständigkeit (ähnlich wie das Axiomenschema der Induktion in den erststufigen Peano-Axiomen ein Ersatz für die zweitstufige Induktion der Dedekind-Peano Axiome ist). Das Archimedes-Axiom, also dass es zu jeder reellen Zahl $x \in \mathbb{R}$ eine natürliche Zahl $n \geq x$ gibt, lässt sich nicht erststufig charakterisieren, da dies für die natürlichen Zahlen nicht möglich ist. Wir betrachten zu $n \in \mathbb{N}$ den Ausdruck

$$p_n = \exists x\left(x \geq n\right),$$

wobei n durch die n-fache Addition der 1 mit sich selbst repräsentiert wird. Eine Aussage wie „$\exists x\forall n(x \geq n)$“, was nichtarchimedisch bedeutet (n soll hier eine natürliche Zahl sein), ist nicht erststufig formulierbar.

Beispiel 17.11. Die Symbolalphabet S bestehe aus den Zeichen $0, 1, +, \cdot$ (und abzählbar unendlich vielen Variablen), die in den reellen Zahlen $\mathbb{R}$ in natürlicher Weise interpretiert werden. Die Ausdrucksmenge

$$\Gamma = \mathbb{R}^{\models}$$

ist somit widerspruchsfrei. Wir betrachten für $n \in \mathbb{N}$ den Ausdruck

$$\beta_n = x \geq n.$$

Es sei Γ' die Vereinigung von Γ mit $\{\beta_n | \, n \in \mathbb{N}\}$. Jede endliche Teilmenge von Γ' ist erfüllbar (nämlich in $\mathbb{R}$), also ist nach Korollar 15.10 auch Γ' erfüllbar. Es gibt also eine S-Struktur M, in der alle erststufigen Sätze von $\mathbb{R}$ gelten und auch alle $x \geq n$ bei geeigneter Belegung gelten, d.h. es gibt ein Element $m \in M$, das jenseits jeder natürlichen Zahl liegt. Insbesondere ist M ein nicht-archimedisch angeordneter Körper.

Definition 17.12. Ein angeordneter Körper K heißt *reell-abgeschlossen*, wenn folgende Eigenschaften gelten.

(1) Jedes nichtnegative Element aus K besitzt eine Quadratwurzel in K.

(2) Jedes Polynom $P \in K[X]$ mit ungeradem Grad besitzt in K eine Nullstelle.

Man kann zeigen, dass ein reell-abgeschlossener Körper K elementar äquivalent zu den reellen Zahlen ist und insbesondere die oben angeführten Eigenschaften besitzt. Eine wichtige Eigenschaft ist ferner, dass $K[\mathrm{i}]$ algebraisch abgeschlossen ist (d.h. durch Hinzunahme eines Elementes i mit $\mathrm{i}^2 = -1$ wird der Körper algebraisch abgeschlossen). Ein (abzählbares Modell) eines reell-abgeschlossenen Körpers sind die reellen algebraischen Zahlen, also alle reellen Zahlen, die Nullstelle eines Polynoms mit rationalen Koeffizienten sind. Dies ist zugleich der kleinste reell-abgeschlossene Körper. Da die Zahlen π und e transzendent sind, folgt, dass diese Zahlen nicht erststufig charakterisierbar sind. Eine Besonderheit der Theorie der reell-abgeschlossenen Körper ist, dass es dafür eine Entscheidungsprozedur gibt, d.h. es gibt einen maschinell durchführbaren Algorithmus, die *Quantorenelimination*, der für jeden Ausdruck α über der erststufigen Sprache zur Symbolmenge $\{0, 1, +, \cdot, \geq\}$ entscheidet, ob α aus den Axiomen ableitbar ist (äquivalent, in jedem reell-abgeschlossenen Körper gilt) oder nicht. Es gibt also prinzipiell keine erststufig formulierbaren „substantiellen Probleme“ für die reellen Zahlen.

17. Arbeitsblatt

17.1. **Übungsaufgaben.**

Aufgabe 17.1. Bestimme die funktionale Hülle zu einem Element $x \in M$, wobei auf M eine Permutation π fixiert sei.

Aufgabe 17.2. Es sei S ein Symbolalphabet, das neben Variablen aus einer Konstanten e und einem einzigen zweistelligen Funktionssymbol f bestehe. Es sei G eine endliche Gruppe, wobei e als neutrales Element und f als die Verknüpfung interpretiert werde. Zeige, dass die funktionale Hülle zu einem Element $g \in G$ mit der von g erzeugten Untergruppe übereinstimmt.

Aufgabe 17.3. Erstelle Funktionssymbolstammbäume, die den arithmetischen Ausdrücken

$$(x + y)z,\ xz + yz,\ x^3 + yz^2$$

entsprechen.

Aufgabe 17.4. Definiere einen Isomorphismus auf $\{1, 2, \ldots, 10\}$ zur Permutation

x	1	2	3	4	5	6	7	8	9	10
$\pi(x)$	4	9	3	10	8	5	2	6	7	1

anhand von Satz 17.6, wobei im ersten Schritt 4 auf 6 abgebildet werden soll.

Aufgabe 17.5. Bestimme die Automorphismengruppe zu einer fixierten Permutation π auf einer endlichen Menge M.

Aufgabe 17.6. Es sei $M = \mathbb{Z}/(12)$, aufgefasst als Gruppe. Definiere entlang von Satz 17.6 einen Isomorphismus

$$\varphi\colon\ \mathbb{Z}/(12) \longrightarrow \mathbb{Z}/(12),$$

startend mit $S_1 = \{0\}$ und weiter mit S_2, wobei S_2 die funktionale Hülle von 0 und $m_2 = 3$ sei, und n_2 als 9 gewählt wird, etc. Welche Wahlmöglichkeiten hat man für $\varphi_3(m_3)$ mit $m_3 = 1$?

Aufgabe 17.7. Definiere die Stelligkeit für ein formal-zusammengesetztes Funktionssymbol.

Aufgabe 17.8. Zeige, dass eine funktional abgeschlossene Teilmenge $T \subseteq M$ einer S-Struktur M auch unter jedem formal-zusammengesetzten Funktionssymbol abgeschlossen ist.

Aufgabe 17.9. Wir betrachten das Symbolalphabet S, welches neben Variablen aus $0, 1, +, \cdot$ besteht, mit der Standardinterpretation auf $\mathbb{R}$. Bestimme die funktionale Hülle der einzelnen Elemente $1, 3\sqrt{7}, e, \pi$. Welche sind untereinander S-isomorph, welche nicht?

Aufgabe 17.10. Es sei $S = \{0, 1, +, \cdot\}$. Zeige, dass die Automorphismengruppen der S-Strukturen $\mathbb{Q}$ und $\mathbb{R}$ jeweils trivial sind.

Aufgabe 17.11. Es sei $S = \{0, 1, +, \cdot\}$ die Symbolmenge eines Körpers. Zeige, dass es einen Unterkörper $K \subseteq \mathbb{R}$ derart gibt, dass $S - \mathrm{Aut}\ K$ nicht trivial ist.

Aufgabe 17.12. Es sei $S = \{0, 1, +, \cdot, \geq\}$ die Symbolmenge eines angeordneten Körpers. Zeige, dass für jeden Unterkörper $K \subseteq \mathbb{R}$ die Automorphismengruppe $S - \operatorname{Aut} K$ trivial ist.

Aufgabe 17.13. Es sei $S = \{0, 1, +, \cdot, \geq\}$ die Symbolmenge eines angeordneten Körpers. Zeige, dass es einen angeordneten Körper K derart gibt, dass $S - \operatorname{Aut} K$ nicht trivial ist.

Aufgabe 17.14.*

Es sei

$$S = \{0, 1, +, \cdot, \geq$$

das Symbolalphabet für einen angeordneten Körper und es sei $\mathbb{R}$ die S-Struktur mit der Standardinterpretation.

(1) Zeige, dass die Äquivalenzklassen zur elementaren Äquivalenz einelementig sind.
(2) Zeige, dass es für die Elemente im Allgemeinen keinen charakterisierenden Ausdruck gibt.

Aufgabe 17.15. Wir betrachten die beiden folgenden Punktkonfigurationen im $\mathbb{R}^2$,

$$M = \{(0,0), (0,1), (1,0), (2,0)\} \text{ und } N = \{(0,0), (0,1), (1,0), (3,0)\}.$$

Zeige, dass es keine lineare Abbildung

$$\varphi\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

gibt, die M in N überführt. Widerspricht dies Satz 17.6?

Aufgabe 17.16. Es sei f ein zweistelliges Funktionssymbol und g ein einstelliges Funktionssymbol. Man mache sich klar, dass die Symbolkette $fggg$ in zweifacher Weise als formal-zusammengesetztes Funktionssymbol gelesen werden kann.

Aufgabe 17.17. Es sei S ein erststufiges Symbolalphabet, M eine S-Struktur und $T \subseteq M$ eine Teilmenge. Zeige, dass die (rekursiv definierte) funktionale Hülle von T gleich dem Durchschnitt über alle funktional abgeschlossenen Teilmengen $N \subseteq M$ ist, die T umfassen.

In der Mathematik interessiert man sich nicht nur für die von einer Teilmenge einer Struktur erzeugte funktionale Hülle, sondern auch für Unterstrukturen, in denen zusätzlich noch die gleichen Gesetzmäßigkeiten (ausgedrückt durch ein Axiomensystem Γ) wie in der Struktur gelten, beispielsweise die von einer Teilmenge erzeugten Untergruppen, Unterringe, Unterkörper, Untervektorräume. Diese von einer Teilmenge erzeugten $S-\Gamma$-Strukturen kann man oft, wenn es sie überhaupt gibt, als Durchschnitt über alle $S-\Gamma$-Unterstrukturen erhalten, die die Teilmenge umfassen.

Aufgabe 17.18. Wir betrachten die Gruppe $(\mathbb{Z}, 0, +)$. Bestimme die funktionale Hülle von $T = \{15, 20\}$ (hier spricht man vom erzeugten Untermonoid) und die von T erzeugte Untergruppe.

Aufgabe 17.19. Das Symbolalphabet S bestehe neben Variablen aus einem einstelligen Funktionssymbol f und es sei $\Gamma = \{\alpha\}$ mit $\alpha = \forall x \exists y(fy = x)$. Es sei $M = \mathbb{Z}$, wobei f als $+2$ interpretiert wird mit der einzigen Ausnahme

$$f(x) = \begin{cases} x+1, \text{ falls } x \geq 0\,, \\ 0, \text{ falls } x = -1\,, \\ x+2, \text{ falls } x \leq -2\,. \end{cases}$$

a) Zeige, dass Γ von M erfüllt wird.

b) Bestimme die funktionale Hülle von $\{0\}$.

c) Zeige, dass die funktionale Hülle von $\{0\}$ nicht Γ erfüllt.

d) Man gebe zwei funktional abgeschlossene, Γ-erfüllende und 0 enthaltende Teilmengen $T_1, T_2 \subseteq \mathbb{Z}$ an, deren Durchschnitt $T_1 \cap T_2$ nicht Γ erfüllt.

Zu einer S-Struktur M und einer S-Unterstruktur $N \subseteq M$ versteht man unter der relativen *S-Automorphismengruppe* von M bezüglich N die Menge der S-Automorphismen auf M, die die Elemente aus N in sich überführen. Sie wird mit $S - \mathrm{Aut}_N\ M$ bezeichnet.

Aufgabe 17.20. Es sei S ein Symbolalphabet, M eine S-Struktur und $N \subseteq M$ eine S-Unterstruktur. Zeige, dass die relative Automorphismengruppe $S - \mathrm{Aut}_N\ M$ eine Untergruppe der Automorphismengruppe $S - \mathrm{Aut}\ M$ ist.

Aufgabe 17.21. Interpretiere die Galoisgruppe zu einer Körpererweiterung $K \subseteq L$ als eine relative Automorphismengruppe zu einem geeigneten Symbolalphabet. Welche Rolle spielen dabei die Körperaxiome?

Aufgabe 17.22. Es sei S ein Symbolalphabet, M eine S-Struktur und $N \subseteq M$ eine S-Unterstruktur. Zeige, dass man durch eine Symbolmengenerweiterung $S \subseteq S'$, wobei nur Konstanten hinzugenommen werden, erreichen kann, dass die relative Automorphismengruppe $S - \mathrm{Aut}_N\, M$ der S'-Automorphismengruppe $S' - \mathrm{Aut}\, M$ entspricht (dazu muss insbesondere S' auf M und N interpretiert werden).

Wir erinnern an die Definition eines algebraisch abgeschlossenen Körpers. Die komplexen Zahlen $\mathbb{C}$ sind algebraisch abgeschlossen (Fundamentalsatz der Algebra), die reellen Zahlen $\mathbb{R}$ nicht.

Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nichtkonstante Polynom $F \in K[X]$ eine Nullstelle in K besitzt.

Aufgabe 17.23. Definiere über der Symbolmenge $\{0, 1, +, \cdot\}$ einen algebraisch abgeschlossenen Körper mit Hilfe eines Axiomenschemas.

17.2. **Aufgaben zum Abgeben.**

Aufgabe 17.24. (3 Punkte)

Es sei S ein Symbolmenge und M eine endliche S-Struktur. Zeige, dass zwei Elemente $m, n \in M$ genau dann elementar äquivalent sind, wenn es einen S-Automorphismus

$$\varphi\colon\ M \longrightarrow M$$

mit $\varphi(m) = n$ gibt.

Aufgabe 17.25. (4 Punkte)

Zeige, dass ein angeordneter Körper, der die Supremumseigenschaft für erststufige Ausdrücke besitzt, reell-abgeschlossen ist.

Verwende, dass Polynomfunktionen auf einem angeordneten Körper stetig sind.

Aufgabe 17.26. (4 Punkte)

Es sei S das Symbolalphabet, das neben Variablen aus einem zweistelligen Relationssymbol G besteht. Wir betrachten vierelementige S-Strukturen, die $\forall x \forall y\, (Gxy \to \neg Gyx)$ erfüllen (also WM-Fußballgruppen, wobei $G(m, n)$ als m gewinnt gegen n interpretiert wird). Erstelle Aussagen $\alpha_0, \alpha_1, \ldots, \alpha_9$ in einer freien Variablen x derart, dass

$$M\frac{m}{x} \vDash \alpha_k$$

bedeutet, dass m in der Abschlusstabelle k Punkte hat.

Aufgabe 17.27. (3 Punkte)

Man gebe ein Beispiel für zwei (abstrakte) WM-Fußballgruppen, die die gleiche Abschlusspunktetabelle besitzen, aber nicht isomorph sind.

18. Vorlesung - Registermaschinen

Wir kehren nun zur Ausgangsfrage dieses Kurses zurück, ob es eine Maschine geben kann, die mathematische Probleme (etwa aus der Zahlentheorie) löst. In den vorhergehenden Vorlesungen haben wir eine formale Sprache entwickelt, in der man solche nichttrivialen Probleme präzise formulieren kann. Ferner haben wir gesehen, wie ein formaler Beweis (eine Ableitung im Prädikatenkalkül) in dieser Sprache aussieht, und dass es nach dem Vollständigkeitssatz für jeden mathematisch beweisbaren Ausdruck der Sprache auch einen formalen Beweis gibt.

In dem vorgestellten Ableitungskalkül der Prädikatenlogik sind die Starttautologien und die Ableitungsregeln übersichtlich strukturiert. Zwar nehmen die Starttautologien häufig Bezug auf beliebige Ausdrücke (und Variablen) der Sprache, doch da die Ausdrücke prinzipiell auflistbar sind, gilt dies auch für die Starttautologien. Daher kann man sich auch einen Algorithmus vorstellen, der nach und nach alle formalen Beweise und somit auch alle formal-beweisbaren Ausdrücke ausgibt. Ein andersgelagertes Problem ist die Fragestellung, ob es ein Entscheidungsverfahren für die Prädikatenlogik gibt, ob es also ein algorithmisches Verfahren gibt, dass zu einem gegebenen Ausdruck überprüfen kann, ob es dafür einen formalen Beweis gibt oder nicht.

Wenn wir bisher von Algorithmen gesprochen haben, so haben wir dabei immer an intuitiv durchführbare Algorithmen gedacht, ohne ein konkretes Durchführungsmodell vor Augen zu haben. In dieser Vorlesung stellen wir die Arbeitsweise einer konkreten algorithmischen Maschine vor, der Registermaschine, die wir von nun an als mechanische Realisierung unserer intuitiven Vorstellung von Algorithmen auffassen wollen.

18.1. **Registermaschinen.**

Es gibt verschiedene Möglichkeiten, eine deterministisch arbeitende Maschine zu modellieren. Wir arbeiten hier mit Registermaschinen, da diese einem wirklichen Computer ziemlich nahe kommen und daher etwas vertrauter sind als Turingmaschinen oder rekursive Funktionen (wobei letztere vom mathematischen Standpunkt her eleganter sind).

Statue von Alan Turing (1912-1954).

Definition 18.1. Unter einer *Registermaschine* versteht man eine endliche Folge von Registern $R_1, R_2, \ldots, R_m$ (oder Speichern), deren Inhalt jeweils eine natürliche Zahl ist, die durch eine endliche (eventuell leere) Folge von Strichen repräsentiert wird.

Ein *Programm für eine Registermaschine* ist eine endliche durchnummerierte Folge von Befehlen $B_1, B_2, \ldots, B_h$, wobei es für die einzelnen Befehle B_j die folgenden Möglichkeiten gibt.

(1) $i+$ (erhöhe den Inhalt des Registers R_i um 1, d.h. um einen Strich).
(2) $i-$ (reduziere den Inhalt des Registers R_i um 1, d.h. ziehe einen Strich ab; wenn der Inhalt leer ist, so lasse ihn leer).
(3) $C(ij)$ (wenn das i-te Register leer ist, so gehe zum Befehl B_j, andernfalls zum nächsten Befehl).
(4) Drucke (drucke den Inhalt des ersten Registers).
(5) Halte an.

Dabei muss $i \leq m$ für alle in einer Programmzeile adressierten Register und $j \leq h$ für alle adressierten Befehlszeilen gelten. Die letzte Befehlszeile B_h ist ein Haltebefehl und sonst gibt es keinen Haltebefehl.

Die beiden ersten Befehle nennt man *Inkrementierung* bzw. *Dekrementierung*. Der dritte Befehl ist der *Abfragebefehl* oder die (bedingte) *Sprunganweisung*. Es folgen *Druckbefehl* und *Haltebefehl*.

Ein Programm für eine Registermaschine arbeitet die Befehle der Reihe nach ab und zwar unter den jeweiligen zum Bearbeitungszeitpunkt vorgefundenen Registerbelegungen. Wenn die aktuelle Programmzeile ein bedingter Sprungbefehl $C(ij)$ ist, so wird, falls die Bedingung zu diesem Zeitpunkt erfüllt ist (also falls das Register R_i leer ist), zur Programmzeile B_j gewechselt. Wenn die Endzeile B_h, also der Haltebefehl erreicht wird, so ist die Bearbeitung beendet.

Die Belegung (oder der Inhalt) des Registers R_i, die sich im Laufe des Programmdurchlaufs mehrfach ändern kann, werden wir häufig mit r_i bezeichnen. Dies ist stets eine natürliche Zahl. Wenn das Register R_i leer ist, so ist sein Inhalt $r_i = 0$.

Die Möglichkeiten einer Registermaschine scheinen auf den ersten Blick recht bescheiden zu sein. Man sieht aber recht schnell, dass man aus diesen wenigen Befehlen Programmabschnitte zusammensetzen kann, die zunehmend komplexere Befehle ausführen. Komplexe Befehle, von denen schon gezeigt wurde, dass sie sich mit Hilfe der Grundbefehle realisieren lassen, werden ohne weiteren Kommentar weiterverwendet.

Man sagt, dass ein Programm *korrekt* ist, wenn es das tut, was es tun soll. Wenn beispielsweise gesagt wird, dass ein Programm zwei Zahlen addiert, so wird die Korrektheit dadurch bewiesen, dass man eben durch Analyse des Programmcodes nachweist, dass bei beliebiger Belegung der beiden Register, deren Inhalte addiert werden sollen, das Programm schließlich anhält und in ein weiteres Register wirklich die Summe der beiden Zahlen gespeichert ist. Ein Korrektheitsnachweis ist häufig eine mühevolle Kleinarbeit mit aufwändigen Fallunterscheidungen, in den natürlich auch mathematische Überlegungen eingehen, wie z.B. bei der Addition die Eigenschaft, dass $s+t = s+(t-1)+1$ ist, was einen induktiven Korrektheitsbeweis ermöglicht. Wir werden diese Korrektheitsüberlegungen häufig abkürzen.

18.2. **Programmbeispiele.**

Wir beschreiben nun einige Programme bzw. Programmabschnitte für Registermaschinen. Wenn man Programme aus schon entwickelten Programmabschnitten zusammensetzt, so ändern sich natürlich die absoluten Befehlsnummern im Programm, was wir aber ignorieren werden.

Beispiel 18.2. Einen unbedingten Sprung (ein „Go to-Befehl“) zu einer bestimmten Programmzeile, der also nicht von einer Abfrage abhängt, kann man dadurch realisieren, dass man ein neues Register R_k hinzunimmt, das von keiner anderen Programmzeile adressiert wird und dessen Inhalt auf 0 gesetzt wird. Dann bewirkt der Befehl $C(kj)$, dass zur j-ten Programmzeile gewechselt wird, da der Inhalt des Registers R_k im gesamten Programmverlauf gleich 0 bleibt.

Beispiel 18.3. Ein Programm soll sämtliche natürlichen Zahlen der Reihe nach ausdrucken. Dazu brauchen wir eine Registermaschine mit zwei Registern R_1 und R_2, die zum Start beide leer sind. Das zweite Register bleibt unverändert und wird nur für den unbedingten Sprungbefehl verwendet. Die Haltezeile wird nie erreicht.

(1) Drucke
(2) 1+
(3) Gehe zu 1

(4) Halte an

Beispiel 18.4. Das Register R_i soll geleert werden. Dies geschieht durch das folgende Programm.

(1) $C(i, 4)$
(2) $i-$
(3) Gehe zu 1
(4) Halte an

Bemerkung 18.5. Wir erlauben, dass bei einer Registermaschine die Anfangsbelegung der Register von außen festgelegt wird. Man könnte aber auch festlegen, dass die Anfangsbelegung stets die Nullbelegung ist, ohne die Berechnungsmöglichkeiten der Registermaschine einzuschränken. Dann kann man die eigentlich gewünschte Anfangsbelegung dadurch erreichen, dass man dem Programm ein „Belegungsprogramm“ voranstellt, das den einzelnen Registern R_i durch die s_i Befehle $i+, \ldots, i+$ die gewünschte Belegung s_i zuweist.

Man könnte auch erstmal ein „Entleerungsprogramm“ vorschalten, das alle Register leert und daran anschließend die Belegung durchführt, doch muss man für den Entleerungsvorgang, der nach Beispiel 18.4 einen unbedingten Sprungbefehl verwendet, zumindest ein leeres Register zur Verfügung haben.

Wenn der Registerinhalt r_i um eine natürliche Zahl k erhöht werden soll, also k-fach direkt hintereinander inkrementiert werden soll, so schreiben wir dafür auch $i + \cdots +$ mit k Pluszeichen.

Beispiel 18.6. Es soll mit einer Registermaschine festgestellt werden, ob der Inhalt r_i des Registers R_i größer oder gleich dem Inhalt r_j des Registers R_j ist. Dazu reserviert man das leere Register R_k (i, j, k seien paarweise verschieden) und baut einen Programmabschnitt der folgenden Art.

(1) $C(j, 6)$
(2) $j-$
(3) $C(i, 7)$
(4) $i-$
(5) Gehe zu 1
(6) $k+$
(7) Halte an

Wenn dieser Programmabschnitt abgelaufen ist, so steht im Register R_k der Wert $r_k = 1$ oder $r_k = 0$, je nachdem, ob $r_i \geq r_j$ ist oder nicht, und zwar unabhängig davon, ob man damit die Eingangsdaten oder Zwischendaten, wenn das Programm den ersten Befehl abarbeitet, meint. Die Korrektheit dieses Programms beruht darauf, dass $r \geq s$ genau dann gilt, wenn $r - 1 \geq s - 1$ ist. Dies ermöglicht einen Induktionsbeweis.

Beispiel 18.7. Wir wollen überprüfen, ob die Inhalte von zwei Registern R_i und R_j übereinstimmen. Dazu kann man das Programm aus Beispiel 18.6 einfach abändern zu

(1) $C(j, 6)$
(2) $j-$
(3) $C(i, 9)$
(4) $i-$
(5) Gehe zu 1
(6) $C(i, 8)$
(7) Gehe zu 9
(8) $k+$
(9) Halte an

Bei Gleichheit erhält man $r_k = 1$, bei Ungleichheit $r_k = 0$.

In den obigen beiden Beispielen wurde die Antwort im Register R_k (in der Form 0 oder 1 abgespeichert). Der Druckbefehl nimmt aber immer Bezug auf R_1. Daher ist es nötig, Registerinhalte in andere Register zu verschieben.

Beispiel 18.8. Wir wollen den Registerinhalt r_i des Registers R_i in das Register R_j übertragen (unabhängig von dessen Inhalt). Dies leistet das folgende Programm.

(1) Leere R_j
(2) $C(i, 6)$
(3) $i-$
(4) $j+$
(5) Gehe zu 2
(6) Halte an

Bei diesem Programm wird im Laufe der Durchführung das Ausgangsregister der Übertragung leer gemacht. Dies ist nicht immer erwünscht, häufig möchte man den Inhalt eines Registers kopieren und sich den Inhalt zugleich merken.

Beispiel 18.9. Wir wollen den Registerinhalt r_i des Registers R_i in das Register R_j übertragen (unabhängig von dessen Inhalt), ohne R_i zu leeren. Dazu brauchen wir ein drittes Register R_k und das folgende Programm.

(1) Leere R_j
(2) Leere R_k
(3) $C(i, 8)$
(4) $i-$
(5) $j+$
(6) $k+$
(7) Gehe zu 3
(8) Übertrage den Inhalt von R_k nach R_i
(9) Halte an

Hier wird zwar im Laufe des Programms der Inhalt von R_i verändert, zum Schluss wird der ursprüngliche Inhalt aber wieder hergestellt.

Beispiel 18.10. Die zwei Registerinhalte r_i (von R_i) und r_j (von R_j) sollen addiert werden, wobei die Summe zum Schluss in R_k stehen soll (es seien i, j, k paarweise verschieden). Dies leistet das folgende Programm.

(1) Leere R_k
(2) Übertrage r_i nach R_k
(3) $C(j, 7)$
(4) $j-$
(5) $k+$
(6) Gehe zu 3
(7) Halte an

Mit der Addition und der Kopie von Inhalten kann man auch den Inhalt eines Registers zu ein anderes Register dazuaddieren. Dies kann man natürlich auch einfach direkt realisieren.

Beispiel 18.11. Die beiden Registerinhalte r_i (von R_i) und r_j (von R_j) sollen multipliziert werden, wobei das Produkt zum Schluss in R_k stehen soll (es seien i, j, k paarweise verschieden). Dies leistet das folgende Programm mit dem Hilfsregister R_ℓ.

(1) Leere R_k
(2) Übertrage den Inhalt von R_i nach R_ℓ ohne R_i zu leeren
(3) $C(j, 7)$
(4) Addiere den Inhalt von R_ℓ zu R_k hinzu
(5) $j-$
(6) Gehe zu 2
(7) Halte an

Die Korrektheit dieses Programms beruht auf $r \cdot s = (r-1)s + s$; für das Produkt rs muss man r-mal s mit sich selbst addieren.

Beispiel 18.12. Es soll überprüft werden, ob der Registerinhalt r_t (von R_t) den Registerinhalt r_j (von R_j) teilt. Falls ja soll das Programm 1 ausgeben, andernfalls 0. Dies leistet das folgende Programm mit den Hilfsregistern R_k und R_ℓ (für Teilprogramme braucht man noch weitere Hilfsregister). Das Ausgaberegister R_1 soll zu Beginn leer sein.

(1) Leere R_ℓ
(2) Berechne $r_t \cdot r_\ell$ und schreibe das Ergebnis in R_k (ohne r_t, r_ℓ zu verändern)
(3) Bei $r_k > r_j$ gehe zu 8
(4) Bei $r_k = r_j$ gehe zu 7
(5) $\ell+$
(6) Gehe zu 2
(7) 1+
(8) Drucke
(9) Halte an

Beispiel 18.13. Es soll überprüft werden, ob der Registerinhalt r_j (von R_j) eine Primzahl ist. Falls ja soll das Programm 1 ausgeben, andernfalls 0. Dies leistet das folgende Programm mit dem Hilfsregister R_t (für Teilprogramme braucht man noch weitere Hilfsregister). Das Ausgaberegister R_1 soll zu Beginn leer sein.

(1) Leere R_t
(2) $t+$
(3) $t+$
(4) Wenn $r_t = r_j$, so gehe zu 8
(5) Wenn $r_t \geq r_j$, so gehe zu 9[26]
(6) Wenn r_j von r_t geteilt wird, so gehe zu 9
(7) Gehe zu 3
(8) $1+$
(9) Drucke
(10) Halte an

Beispiel 18.14. Es sollen die geraden Zahlen ≥ 4 daraufhin überprüft werden, ob sie die Eigenschaft in der Goldbachvermutung erfüllen, also ob sie die Summe von zwei Primzahlen sind. Das Programm soll die Ausgabe 0 machen, falls ein Gegenbeispiel gefunden wurde. Dies leistet das folgende Programm mit den Registern R_n, R_k und R_i, die alle zu Beginn auf 0 gesetzt seien. Auch das Ausgaberegister R_1 soll zu Beginn leer sein. Wir testen ab 6, um uns auf ungerade Primzahlen als Summanden beschränken zu können.

(1) $n++++$
(2) $n++$
(3) Leere R_k
(4) $k+$
(5) $k++$
(6) Wenn $r_k \geq r_n$, so gehe zu 12
(7) Wenn r_k eine Primzahl ist, so gehe zu 9
(8) Gehe zu 5
(9) Berechne $r_n - r_k$, schreibe das Ergebnis in R_i
(10) Wenn r_i eine Primzahl ist, so gehe zu 2
(11) Gehe zu 5
(12) Drucke
(13) Halte an

18. Arbeitsblatt

18.1. **Übungsaufgaben.**

[26]Die Programmzeile (5) ist nur für $r_j = 0, 1$ von Bedeutung.

Aufgabe 18.1. Entwerfe ein Programm für eine Registermaschine, das nach und nach alle Quadratzahlen ausdruckt.

Aufgabe 18.2.*

Erstelle ein Programm für eine Registermaschine, das abwechselnd 1 und 0 ausdruckt, das mit sechs Befehlszeilen auskommt und lediglich einen Sprungbefehl verwendet.

Aufgabe 18.3.*

Erstelle ein Programm für eine Registermaschine, das abwechselnd 1 und 0 ausdruckt, das mit sechs Befehlszeilen auskommt und lediglich einen Druckbefehl verwendet.

Aufgabe 18.4. Entwerfe ein Programm für eine Registermaschine, die für $r_i \geq r_j$ die Differenz $r_i - r_j$ von zwei Registerinhalten berechnet.

Aufgabe 18.5. Entwerfe ein Programm für eine Registermaschine, das entscheidet, ob der Registerinhalt r_i des Registers R_i die echte Potenz einer natürlichen Zahl ist.

Aufgabe 18.6. Sei $b \in \mathbb{N}_+$. Entwerfe ein Programm für eine Registermaschine, das bei der Eingabe von $(r_1, \ldots, r_k)$ in den ersten k Registern die Zahl $\sum_{i=1}^{k} r_i b^i$ berechnet, ausdruckt und anhält.

Aufgabe 18.7. Sei $b \in \mathbb{N}_{\geq 2}$. Entwerfe ein Programm für eine Registermaschine, das bei Eingabe von z im ersten Register die b-adische Ziffernentwicklung $z = \sum_{i=0}^{k} s_i b^i$ (mit $0 \leq r_i \leq b-1$) berechnet, nach und nach die Ziffern s_i (beginnend mit $i = 0$) ausdruckt und schließlich anhält.

Aufgabe 18.8. Sei $b \in \mathbb{N}_{\geq 2}$. Entwerfe ein Programm für eine Registermaschine, das zur Eingabe von z im ersten Register die b-adische Ziffernentwicklung $z = \sum_{i=1}^{k} s_i b^i$ (mit $0 \leq r_i \leq b-1$) berechnet, nach und nach die Exponenten i und die zugehörigen Ziffern s_i (beginnend mit k und s_k) ausdruckt und schließlich anhält.

Aufgabe 18.9. Entwerfe ein möglichst kurzes (also mit möglichst wenigen Befehlszeilen) Programm für eine Registermaschine, das bei leerer Startbelegung anhält und zum Schluss die Zahl 20 im ersten Register hat.

Aufgabe 18.10. Entwerfe ein Programm für eine Registermaschine, das bei Eingabe einer natürlichen Zahlen n im Register R_1 die Fakultät $n!$ in R_1 ausgibt.

Aufgabe 18.11. Entwerfe ein Programm für eine Registermaschine, das bei Eingabe von zwei natürlichen Zahlen n und k in den Registern R_2, R_3 den Binomialkoeffizienten $\binom{n}{k}$ in R_1 ausgibt.

Aufgabe 18.12. Entwerfe ein Programm für eine Registermaschine, das bei Eingabe von zwei natürlichen Zahlen a und b in den Registern R_2, R_3 den euklidischen Algorithmus durchführt und das Ergebnis, also den größten gemeinsamen Teiler von a und b, in R_1 ausgibt.

Aufgabe 18.13. Es sei P ein Programm für eine Registermaschine, es sei eine feste Anfangsbelegung gegeben und es sei vorausgesetzt, dass das Programm, angesetzt auf diese Anfangsbelegung, irgendwann anhält. Zeige, dass man den Ablauf des Programms, also die schrittweise Abfolge der Veränderungen der Registerinhalte, auch durch ein Programm realisieren kann, bei dem der Sprungbefehl nicht verwendet wird. Wozu braucht es dann eigentlich den Sprungbefehl?

Aufgabe 18.14. Zeige, dass es kein Programm für eine Registermaschine gibt, das bei jeder Anfangsbelegung sämtliche Register leert.

Aufgabe 18.15. Beschreibe ein Verfahren, das alle prädikatenlogischen Ausdrücke ausgibt (dabei sei vorausgesetzt, dass die Variablen, die Konstanten, die Relationssymbole und die Funktionssymbole in einer aufgezählten Form vorliegen).

Aufgabe 18.16. Entwerfe ein Programm für eine Registermaschine, das bei Eingabe einer natürlichen Zahlen n im Register R_1 den Collatz-Algorithmus durchführt, dabei die sukzessiven Werte ausdruckt und insbesondere anhält, wenn der Wert 1 erreicht wird.

Aufgabe 18.17. Welches Bildungsgesetz liegt der Folge

$$1, 11, 21, 1211, 111221, 312211, \ldots$$

zugrunde?

(Es wird behauptet, dass diese Aufgabe für Grundschulkinder sehr einfach und für Mathematiker sehr schwierig ist.)

18.2. **Aufgaben zum Abgeben.**

Aufgabe 18.18. (3 Punkte)

Entwerfe ein Programm für eine Registermaschine, das nach und nach alle Primzahlen ausdruckt.

Aufgabe 18.19. (5 Punkte)

Entwerfe ein Programm für eine Registermaschine, das nach und nach alle Glieder der in Aufgabe 18.17 beschriebenen Folge ausdruckt.

Aufgabe 18.20. (3 Punkte)

Entwerfe ein Programm für eine Registermaschine, das die Potenz $r_i^{r_j}$ berechnet (und ausgibt), wobei r_i bzw. r_j die Registerinhalte der Register R_i, R_j, $i \neq j$, sind.

Aufgabe 18.21. (3 Punkte)

Entwerfe ein Programm für eine Registermaschine, das nach und nach alle Mersenne-Primzahlen ausdruckt.

Aufgabe 18.22. (4 Punkte)

Entwerfe ein möglichst kurzes (also mit möglichst wenigen Befehlszeilen) Programm für eine Registermaschine, das bei leerer Startbelegung anhält und zum Schluss die Zahl 100 im ersten Register hat.

Punkte gibt es nur für ziemlich kurze Programme. Für den Kurs-Rekord gibt es drei Extrapunkte.

19. Vorlesung - Das Halteproblem

19.1. **Entscheidbarkeit und Berechenbarkeit.**

In der letzten Vorlesung haben wir verschiedene mathematische Operationen (wie Addition und Multiplikation) durch Registerprogramme berechnet und ebenso mathematische Prädikate (etwa das Prädikat, eine Primzahl zu sein) durch Registerprogramme charakterisiert. Die Fähigkeit eines Registerprogramms, bestimmte Funktionen bzw. Prädikate zu berechnen bzw. zu charakterisieren, führt zu den folgenden Begriffen.

Definition 19.1. Eine k-stellige Funktion

$$F\colon \mathbb{N}^k \longrightarrow \mathbb{N}$$

heißt *R- berechenbar* (oder *Register-berechenbar*), wenn es ein Programm P für eine Registermaschine gibt, die bei jeder Eingabe $(r_1, \ldots, r_k)$ (in den ersten k Registern) anhält und $F(r_1, \ldots, r_k)$ als (einzige) Ausgabe besitzt.

Definition 19.2. Es sei $T \subseteq \mathbb{N}$ eine Teilmenge der natürlichen Zahlen. Man sagt, dass diese Menge *R- entscheidbar* (oder *Register-entscheidbar*) ist, wenn es ein Programm P für eine Registermaschine gibt, die bei jeder Eingabe anhält und für die die Äquivalenz

$$n \in T \text{ genau dann, wenn } P(n) \text{ die Ausgabe } 0 \text{ besitzt}$$

gilt.

Eine Teilmenge $T \subseteq \mathbb{N}$ ist genau dann R-entscheidbar, wenn die zugehörige Indikatorfunktion R-berechenbar ist.

19.2. **Die Churchsche These.**

Wir haben in der letzten Vorlesung für einige recht einfache Probleme Registerprogramme angegeben, die diese Aufgabe lösen. Diese Beispiele vermitteln eine erste Vorstellung davon, was alles mit Registermaschinen berechnet werden kann. Zur Tragweite von algorithmischer Berechenbarkeit überhaupt ist die sogenannte *Churchsche These* von Bedeutung.

Bemerkung 19.3. Die *Churchsche These* (nach Alonzo Church, manchmal auch *Church-Turing-These*) behauptet, dass die intuitiv berechenbaren Funktionen (bzw. die intuitiv entscheidbaren Prädikate) mit den Registerberechenbaren Funktionen übereinstimmt. Da es sich bei „intuitiv berechenbar“ um einen nicht präzisen Begriff handelt, lässt sich diese These nicht beweisen. Sie ist dennoch weitgehend akzeptiert, wobei die folgenden Gründe angeführt werden.

• Alle Präzisierungen des Berechenbarkeitsbegriffs, nämlich durch Registermaschine, Turingmaschine, μ-rekursive Funktionen, λ-Kalkül, führen zu einer übereinstimmenden Klasse von berechenbaren Funktionen. Dies beruht darauf, dass man diese algorithmischen Verfahren wechselseitig simulieren kann.

• Konkrete, intuitiv berechenbare Funktionen lassen sich stets durch ein Registerprogramm realisieren.

In der Praxis ist die Churchsche These vor allem eine Erleichterung, da man aufgrund eines häufig naheliegenden intuitiven Algorithmus auf die Existenz eines Registerprogramms schließen kann, und so die oft mühevolle „Programmier-Arbeit“ umgeht.

19.3. **Das Halteproblem.**

Nicht jedes Programm hält an. Ein einfaches Beispiel mit zwei Registern R_1, R_2 und leerer Belegung für R_2 ist

(1) 1+
(2) $C(2,1)$
(3) Halte an

Im Allgemeinen wird es sehr schnell schwierig, zu einem gegebenen konkreten Programm zur Eingabe $r_1 = 0$ zu entscheiden, ob es den Haltebefehl schließlich erreicht oder nicht. Ebenso ist es schwierig zu entscheiden, für welche Eingabedaten in R_1 (den *Input*) das konkrete Programm stoppt. Wenn man das Programm bei einer bestimmten Eingabe laufen lässt und es nach einer gewissen Zeit anhält, so kann man dies natürlich unmittelbar als einen Beweis für die Halteeigenschaft des Programms verstehen. Wenn das Programm nicht die Halteeigenschaft hat, so kann man dies aus dem Programmablauf nicht erschließen. Das Programm läuft einfach weiter und man weiß nicht, ob es einfach noch nicht angehalten hat oder ob es niemals anhalten wird. Mit einer aufwändigen Analyse des Programms wird man im Allgemeinen erkennen können, ob das Programm anhält oder nicht.

Ein qualitativ anderes Problem ist allerdings die Frage, ob es ein Verfahren gibt, mit dem man für jedes Programm (bzw. jedes Programm und jede Eingabe) entscheiden kann, ob es anhält oder nicht.

Hier deutet sich eine selbstbezügliche Fragestellung an: Gibt es ein Programm, das Aussagen über alle Programme machen kann? Welche Aussage macht dann dieses Programm über sich selbst?

Um einen solchen Ansatz präzise machen zu können, müssen wir Programme als Eingabe für ein Programm interpretieren können. Das Programm einer Registermaschine erlaubt nur die Eingabe einer Zahl. Daher müssen wir ein Programm durch eine Zahl kodieren. Dies geschieht in zwei Schritten.

Zuerst führen wir für die erlaubten Befehle abkürzende Schreibweisen ein. Wir arbeiten mit dem Alphabet

$$\prime - \ I\, D\, C\, P\, H\,,$$

Die einzelnen Befehle werden folgendermaßen notiert

(1) Inkrementierung von R_i
$I\prime\prime\cdots\prime$ (mit i Strichen).
(2) Dekrementierung von R_i
$D\prime\prime\cdots\prime$ (mit i Strichen).
(3) Sprunganweisung $C(i,j)$
$C\prime\prime\cdots\prime,\prime\prime\cdots\prime$ (mit i Strichen vor dem Komma und j Strichen nach dem Komma).
(4) Druckanweisung: P.

(5) Halteanweisung: H.

Das Symbol $\prime$ wird also benutzt, um sowohl die Registernummern als auch die Zeilennummern (in der Sprunganweisung) auszudrücken. Da in jeder Befehlszeile eines konkreten Programmes konkrete Register bzw. Zeilen adressiert werden, stehen da jeweils natürliche Zahlen (keine Variablen), die problemlos durch eine Strichfolge ausgedrückt werden können.

Ein Programm, das aus den durchnummerierten Befehlszeilen $B_1, B_2, \ldots, B_h$ besteht, wird dann insgesamt durch die Zeichenfolge

$$b_1 - b_2 - \ldots - b_h$$

wiedergegeben, wobei b_j die soeben angeführte Kodierung der j-ten Befehlszeile ist. Das Zeichen $-$ wird also verwendet, um die Zeilen voneinander zu trennen. Das Mitschleppen der Zeilennummern ist nicht nötig, da sich die Nummer aus der Reihenfolge rekonstruieren lässt.

Das oben angegebene Programm hätte demnach die symbolische Kodierung

$$I\prime - C\prime\prime, \prime - H$$

In einem zweiten Schritt ersetzen wir diese symbolische Kodierung durch eine numerische Kodierung. Dafür gibt es verschiedene Möglichkeiten. Da unser Alphabet, mit dem wir jedes Programm schreiben können, 8 Symbole verwendet, liegt eine Repräsentierung im Achtersystem nahe. Da die 0 als Anfangsnummer etwas problematisch ist, arbeiten wir lieber im Neunersystem (man kann die folgenden Zahlen genauso gut im Zehnersystem auffassen) und ordnen den Symbolen von oben in der obigen Reihenfolge die Ziffern

$$1, 2, 3, 4, 5, 6, 7, 8$$

zu. Das Programm von oben wird dann zur Ziffernfolge

$$3125118127\,.$$

Die einem jeden Programm P auf diese Weise zugeordnete Zahl (also der Zahlwert, nicht die Ziffernfolge) nennen wir $c(P)$. Man spricht von der *Gödelnummer* des Programms.

Bemerkung 19.4. Es ist algorithmisch überprüfbar, ob eine als Strichfolge gegebene natürliche Zahl ein Code für ein Registerprogramm ist. Dazu muss zuerst die Zahl in ihre Ziffernentwicklung (im Neunersystem) übersetzt werden. Da der Trennstrich, der die einzelnen Befehle trennt, durch eine bestimmte Ziffer codiert wird, muss die Ziffernfolge zwischen zwei Trennstrichziffern einen Befehl codieren. Die syntaktische Korrektheit dieser einzelnen Befehlsziffernfolgen muss dann der Reihe nach überprüft werden. Dazu muss man für jeden der Einzelbefehle einen Algorithmus entwerfen. Wenn beispielsweise die Anfangsziffer einer Befehlsziffernfolge eine 3 (also ein I) ist, so muss es sich um einen Inkrementierungsbefehl handeln und alle nachfolgenden Ziffern (bis zum nächsten Trennstrich) müssen eine 1 sein.

Für ein Registerprogramm P und eine natürliche Zahl n verstehen wir unter $P(n)$ das Programm angesetzt auf n im ersten Register (und leeren anderen Registern).

Lemma 19.5. *Die Menge*

$$\{n \in \mathbb{N} |\, n \textit{ ist die Nummer eines Registerprogramms } P \textit{ und } P(n) \textit{ hält an}\}$$

ist nicht R-entscheidbar.

Beweis. Wir nehmen an, dass es ein Programm U gibt, das diese Menge entscheidet (der erste Teilaspekt, ob es sich überhaupt um ein valides Programm handelt, ist entscheidbar). Wir ändern dieses Programm zu einem Programm U' ab, indem wir den letzten Befehl von U (also den Haltebefehl) durch den Programmabschnitt (mit der relativen Nummerierung und einem neuen Register R_i)

(1) $C(1,3)$
(2) Gehe zu 5
(3) $i+$
(4) $C(1,3)$
(5) Halte an

ersetzen. Dies bedeutet, dass das Programm U' genau dann in eine Endlosschleife hineinkommt und nicht anhält, wenn das Programm U die Ausgabe 0 hat. Daher gilt die Äquivalenz, dass ein Programm P bei Eingabe der eigenen Programmnummer $c(P)$ genau dann anhält, wenn U' bei Eingabe der Programmnummer $c(P)$ von P nicht anhält. Diese Äquivalenz ergibt bei Anwendung auf das Programm $P = U'$ einen Widerspruch. □

Satz 19.6. *Die Menge*

$$\{n \in \mathbb{N} |\, n \textit{ ist die Nummer eines Registerprogramms } P \textit{ und } P(0) \textit{ hält an}\}$$

ist nicht R-entscheidbar.

Beweis. Wir nehmen an, dass es ein Registerprogramm V gibt, dass die in Frage stehende Menge entscheidet, also stets anhält und angesetzt auf eine Zahl n genau dann die Ausgabe 0 liefert, wenn $n = c(P)$ für ein Programm P ist (also wenn n die Programmnummer eines Registerprogramms ist) und wenn dieses Programm P, angesetzt auf 0, anhält. Wir entwickeln aus V ein Programm U, das genau dann die Ausgabe 0 hat, wenn $n = c(P)$ für ein Programm P ist und wenn P, angesetzt auf n, anhält. Dies ergibt einen Widerspruch zu Lemma 19.5.

Dazu wird U folgendermaßen konstruiert: Wenn n keine Programmnummer ist, so hält das Programm U mit der Ausgabe 1 an (hier gibt es also keinen Unterschied zu V). Wenn $n = c(P)$ eine Programmnummer ist, so wird das Programm P' aufgestellt, das dem Programm P die n-fache Inkrementierung des ersten Registers voranstellt und dessen (in einem bedingten Sprungbefehl

in einer Befehlszeile) adressierte Befehlszeilennummern sich um n erhöhen. Für die Programmnummer $n' = c(P')$ wird nun mittels V überprüft, welche Ausgabe P', angesetzt auf 0, besitzt. Aufgrund der Konstruktion von P' besitzt P' bei Eingabe 0 die Ausgabe 0 genau dann, wenn P bei Eingabe von n die Ausgabe 0 besitzt. □

19.4. **Aufzählbarkeit von Programmen.**

Wir führen einen weiteren Berechenbarkeitsbegriff ein.

Definition 19.7. Es sei $T \subseteq \mathbb{N}$ eine Teilmenge der natürlichen Zahlen. Man sagt, dass diese Menge *R- aufzählbar* (oder *Register-aufzählbar*) ist, wenn es ein Programm P für eine Registermaschine gibt, die bei Eingabe von 0 nach und nach genau die Zahlen aus T ausdruckt (dabei dürfen Zahlen aus T auch mehrfach ausgedruckt werden).

Zwischen Entscheidbarkeit und Aufzählbarkeit besteht der folgende Zusammenhang.

Lemma 19.8. *Es sei $T \subseteq \mathbb{N}$ eine Teilmenge der natürlichen Zahlen. Dann ist T genau dann R-entscheidbar, wenn sowohl T als auch das Komplement $\mathbb{N} \setminus T$ R-aufzählbar ist.*

Beweis. Wenn P ein Programm ist, das T entscheidet, so kann man einfach ein T aufzählendes Programm konstruieren. Man lässt der Reihe nach jede natürliche Zahl mittels P auf ihre Zugehörigkeit zu T überprüfen und druckt sie aus, falls sie dazu gehört (dazu muss man den Haltebefehl von P zu einer Druckausgabe modifizieren). Entsprechend konstruiert man ein Aufzählungsprogramm für das Komplement.

Es seien nun T als auch $\mathbb{N} \setminus T$ aufzählbar, und es seien P und Q Programme, die dies leisten. Dann liefert die folgende Kombination der beiden Programme ein Entscheidungsverfahren: Man schreibt die Programme P und Q hintereinander (wobei man natürlich die adressierten Register und Programmzeilen umnummerieren muss) und lässt sie abwechselnd bis zu einer Druckausgabe laufen. Sobald eine Druckausgabe eines Programmteils mit der zu überprüfenden Zahl n übereinstimmt, weiß man, ob n zu T gehört oder nicht. Da n entweder zu T oder zum Komplement gehört, muss einer dieser Fälle eintreten. □

Lemma 19.9. *Die Menge der Programmnummern von Registerprogrammen, die angesetzt auf 0 anhalten, ist R-aufzählbar.*

Beweis. Die Idee für ein algorithmisches Aufzählverfahren geht so: Zu jeder natürlichen Zahl n berechnet man sämtliche Programme P mit $c(P) \leq n$. Jedes dieser Programme lässt man, angesetzt auf 0, n Schritte (also n Befehlszeilenwechsel) lang laufen. Wenn P anhält, so druckt man $c(P)$ aus. Wenn all diese Programme n Schritte gelaufen sind, so erhöht man auf $n+1$.

Da ein jedes anhaltendes Programm nach einer gewissen Laufzeit ℓ anhält, wird es bei $n = \max(c(P), \ell)$ als anhaltendes Programm erfasst. □

Aus Satz 19.6 und Lemma 19.9 folgt insbesondere, dass die nicht haltenden Programme nicht aufzählbar sind.

19. Arbeitsblatt

19.1. **Übungsaufgaben.**

Aufgabe 19.1. Bestimme die symbolische und die numerische Kodierung des folgenden Programms für eine Registermaschine.

1. 3+
2. 2−
3. $C(2, 4)$
4. $C(3, 1)$
5. Drucke
6. Halte an .

Wir nennen ein Registerprogramm *Zustands-periodisch*, wenn zwei identische Zustände (d.h. identische Inhalte in allen Registern und identische Befehlszeilennummern) zu unterschiedlichen Zeitpunkten im Programmablauf eingenommen werden (bei leerer Anfangsbelegung).

Aufgabe 19.2. Man gebe ein Beispiel für ein Zustands-periodisches Programm.

Aufgabe 19.3. Seien $T, S \subseteq \mathbb{N}$ entscheidbare Mengen. Zeige, dass dann auch die Vereinigung $T \cup S$, der Durchschnitt $T \cap S$ und auch das Komplement $\mathbb{N} \setminus T$ entscheidbar sind.

Aufgabe 19.4. Zeige, dass es nur abzählbar viele entscheidbare Teilmengen von $\mathbb{N}$ gibt.

Aufgabe 19.5. Sei $\alpha \in L^{\mathrm{Ar}}$ ein Ausdruck in der Sprache der Arithmetik (mit den Konstanten $0, 1$, den Funktionssymbolen $+, \cdot$ und dem Relationssymbol $\geq$), der keine Quantoren enthält und nur eine einzige Variable x.

Zeige: Die Menge T aller $n \in \mathbb{N}$ die α erfüllen, d.h.

$$T = \left\{ n \in \mathbb{N} | \, \mathbb{N} \frac{n}{x} \vDash \alpha \right\},$$

ist entscheidbar.

In den folgende Aufgaben verwenden wir den Begriff der Aufzählbarkeit nicht nur für Teilmengen $T \subseteq \mathbb{N}$, sondern auch für Teilmengen aus L^S.

Aufgabe 19.6. Es sei S ein Symbolalphabet mit einer R-Aufzählung der in S vorkommenden Variablen, Konstanten und Funktionssymbole. Zeige, dass es auch eine R-Aufzählung der S-Terme gibt.

Aufgabe 19.7. Es sei S ein Symbolalphabet mit einer R-Aufzählung der in S vorkommenden Variablen, Konstanten, Funktionssymbole und Relationssymbole. Zeige, dass es auch eine R-Aufzählung der S-Ausdrücke gibt.

Aufgabe 19.8. Es sei S ein Symbolalphabet mit einer R-Aufzählung der in S vorkommenden Variablen, Konstanten, Funktionssymbole und Relationssymbole. Zeige, dass es auch eine R-Aufzählung der S-Tautologien gibt.

Aufgabe 19.9.*

Die Registerabteilung des VW-Konzerns hat - ohne Wissen des Vorstandes und am Aufsichtsrat vorbei - in jedes real existierende Registerprogramm P an einer willkürlich gewählten Stelle die aufeinanderfolgenden Befehlszeilen eingebaut (und dabei die Zeilennummern und die Sprungbefehlsnummern angepasst, k ist die Nummer eines in P nicht verwendeten Registers und h' ist die neue Haltebefehlsnummer)

$$k+$$

$$k+$$

$$\text{Drucke}$$

$$C(k, h') \, .$$

(1) Ändert sich durch diese Manipulation die Halteeigenschaft des Programms?

(2) Ändert sich durch diese Manipulation die Programmabbildung?
(3) Nachdem der Skandal herauskommt und die Öffentlichkeit eine Erklärung fordert, diskutieren Vorstand, Aufsichtsrat und Abteilungsleiter die folgenden möglichen Stellungsnahmen für die anstehende Pressekonferenz:
a) Man wollte Speicherplatz sparen.
b) Man wollte aus Werbezwecken erreichen, dass jedes Registerprogramm mindestens einmal „VW“ ausdruckt.
c) Man wollte einen Beitrag zur Entschleunigung leisten, indem man manche Programme etwas langsamer macht.
d) Man wollte einen Beitrag zur Entschleunigung leisten, indem man alle Programme etwas langsamer macht.
Welche dieser Erklärungen passen inhaltlich zu den Manipulationen?

Aufgabe 19.10. Entwerfe ein Programm für eine Registermaschine, das genau dann anhält, wenn die Goldbachsche Vermutung falsch ist.

Aufgabe 19.11. Zeige, dass das in Aufgabe 18.16 entworfene Programm für eine Registermaschine bei Eingabe einer natürlichen Zahlen n im Register R_1 genau dann nicht anhält, wenn die Zahl n eine negative Antwort zum Collatz-Problem liefert.

19.2. **Aufgaben zum Abgeben.**

Aufgabe 19.12. (4 Punkte)

Zeige, dass ein nicht anhaltendes, Register-beschränktes Programm (d.h. es gibt eine Schranke $S \in \mathbb{N}$, die die Registerinhalte zu keinem Zeitpunkt des Programmablaufes überschreiten) Zustands-periodisch ist.

Aufgabe 19.13. (4 Punkte)

Man gebe ein Beispiel für ein nicht anhaltendes Registerprogramm, das keine Periodizität im Ablauf der Befehlsnummern besitzt.

Aufgabe 19.14. (2 Punkte)

Zeige, dass jede endliche Teilmenge $T \subseteq \mathbb{N}$ der natürlichen Zahlen entscheidbar ist.

Aufgabe 19.15. (3 Punkte)

Seien $A, B \subseteq \mathbb{N}$ Teilmengen, deren symmetrische Differenz $A \triangle B$ endlich sei. Zeige, dass A genau dann aufzählbar bzw. entscheidbar ist, wenn B aufzählbar bzw. entscheidbar ist.

Aufgabe 19.16. (3 Punkte)

Sei $T \subseteq \mathbb{N}$ eine Teilmenge der natürlichen Zahlen. Es gebe ein Programm für eine Registermaschine, das die Elemente von T in aufsteigender Reihenfolge ausgibt. Zeige, dass T entscheidbar ist.

20. Vorlesung - Arithmetische Repräsentierungen

20.1. **Arithmetische Repräsentierbarkeit.**

Wir möchten die Wirkungsweise von Registerprogrammen arithmetisch repräsentieren, um so aus der Unentscheidbarkeit des Halteproblems auf die Unentscheidbarkeit der Arithmetik zu schließen. Im Folgenden arbeiten wir mit dem arithmetischen Alphabet $\mathrm{Ar} = \{0, 1, +, \cdot\}$ und der Standardinterpretation in $\mathbb{N}$.

Definition 20.1. Eine Abbildung

$$F\colon \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

heißt *arithmetisch repräsentierbar*, wenn es einen L^{Ar}-Ausdruck ψ in $r + s$ freien Variablen derart gibt, dass für alle $(r + s)$-Tupel $(n_1, \ldots, n_{r+s}) \in \mathbb{N}^{r+s}$ die Äquivalenz $F(n_1, \ldots, n_r) = (n_{r+1}, \ldots, n_{r+s})$ genau dann, wenn $\mathbb{N} \vDash \psi(n_1, \ldots, n_{r+s})$ gilt.

Definition 20.2. Eine Relation $R \subseteq \mathbb{N}^r$ heißt *arithmetisch repräsentierbar*, wenn es einen L^{Ar}-Ausdruck ψ in r freien Variablen derart gibt, dass für alle r-Tupel $(n_1, \ldots, n_r) \in \mathbb{N}^r$ die Äquivalenz $(n_1, \ldots, n_r) \in R$ genau dann, wenn $\mathbb{N} \vDash \psi(n_1, \ldots, n_r)$ gilt.

Die Schreibweise $\psi(n_1, \ldots, n_{r+s})$ bedeutet, dass die $r + s$ nicht namentlich aufgeführten freien Variablen durch die $n_1, \ldots, n_{r+s}$ ersetzt werden, wobei die natürlichen Zahlen n_j als Terme durch die n_j-fache Summe $1+\cdots+1$ (streng genommen mit einer fixierten Klammerung) wiedergegeben werden. Da die repräsentierenden Ausdrücke genau $r+s$ bzw. r freie Variablen besitzen, entsteht durch Substitution der freien Variablen durch die Terme eine Aussage ohne freie Variablen. Diese sind bei Interpretation über den natürlichen Zahlen wahr oder falsch. Aufgrund des Substitutionslemmas ist die Gültigkeit $\mathbb{N} \vDash \psi(n_1, \ldots, n_{r+s})$ äquivalent zur Gültigkeit $\mathbb{N}^{\frac{n_1,\ldots,n_{r+s}}{x_1,\ldots,x_{r+s}}} \vDash \psi$. Polynomfunktionen

$$\mathbb{N}^r \longrightarrow \mathbb{N}$$

mit natürlichzahligen Koeffizienten sind unmittelbar arithmetisch präsentierbar, siehe Aufgabe 20.5.

Wir wollen zeigen, dass Registerprogramme, oder besser gesagt die durch ein Registerprogramm festgelegte Programmabbildung, arithmetisch repräsentierbar sind.

20.2. **Registerprogramme als Abbildungen.**

Wir möchten ein Registerprogramm P, das aus h Programmzeilen besteht und m Register anspricht, als eine Abbildung auffassen. Die Wirkungsweise einer jeden Programmzeile hängt dabei nur von den Belegungen der Register zu dem Zeitpunkt ab, an dem diese Zeile aufgerufen wird. Sie ist geschichtsunabhängig, d.h. unabhängig von dem bisherigen Verlauf des Programmes. Man kann daher ein Programm vollständig durch die Abbildung

$$\begin{aligned}\varphi : \{1,2,\ldots,h\} \times \mathbb{N}^m &\longrightarrow \{1,2,\ldots,h\} \times \mathbb{N}^m \\ (\ell, n_1, \ldots, n_m) &\longmapsto \varphi(\ell, n_1, \ldots, n_m),\end{aligned}$$

erfassen. Diese Abbildung nennen wir die *Programmabbildung* $\varphi = \varphi_P$. Dabei steht ℓ für die Programmzeilennummer und n_j steht für den Inhalt des Registers R_j (von denen es ja m Stück gibt). Dem Tupel $(\ell, n_1, \ldots, n_m)$ wird dasjenige Tupel $\varphi(\ell, n_1, \ldots, n_m)$ zugeordnet, das bei Abruf des in der ℓ-ten Programmzeile stehenden Befehls B_ℓ bei der Registerbelegung $(n_1, \ldots, n_m)$ entsteht. Die Abbildung φ besteht dabei aus den $m+1$ Komponentenfunktionen $\varphi_0, \varphi_1, \ldots, \varphi_m$, wobei φ_0 die Wirkungsweise auf die Programmzeilennummer und die φ_j, $1 \leq j \leq m$, die Wirkungsweise auf das j-te Register beschreibt. Die Wirkung der einzelnen Befehle sieht folgendermaßen aus.

Bei $B_\ell = i+$ ist

$$\varphi(\ell, n_1, \ldots, n_m) = (\ell+1, n_1, \ldots, n_{i-1}, n_i + 1, n_{i+1}, \ldots, n_m).$$

Bei $B_\ell = i-$ ist

$$\varphi(\ell, n_1, \ldots, n_m) = (\ell+1, n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_m)$$

bei $n_i \geq 1$ und

$$\varphi(\ell, n_1, \ldots, n_m) = (\ell+1, n_1, \ldots, n_{i-1}, n_i, n_{i+1}, \ldots, n_m)$$

bei $n_i = 0$. Bei $B_\ell = C(ij)$ ist

$$\varphi(\ell, n_1, \ldots, n_m) = \begin{cases} (j, n_1, \ldots, n_m), \text{ falls } n_i = 0\,, \\ (\ell+1, n_1, \ldots, n_m) \text{ sonst}\,. \end{cases}$$

Bei $B_\ell = H$ (also bei $\ell = h$) ist

$$\varphi(h, n_1, \ldots, n_m) = (h, n_1, \ldots, n_m),$$

die Abbildung wirkt dort also wie die Identität. Der Druckbefehl ist für den Programmablauf nicht relevant und wird hier ignoriert.

In manchen Situationen möchte man eine auf ganz $\mathbb{N} \times \mathbb{N}^m$ definierte Programmabbildung haben. Um dies zu erreichen setzt man für $\ell > h$ einfach

$$\varphi(\ell, n_1, \ldots, n_m) = (\ell, n_1, \ldots, n_m).$$

20.3. **Repräsentierbarkeit der Registerbefehle.**

Ein Registerprogramm kann also in eine Abbildung übersetzt werden, die die Wirkungsweise des Programms widerspiegelt. Die dabei auftretenden Abbildungen sind prinzipiell einfach beschreibbar, auch wenn dafür eine lange Abbildungsdefinition und tief verschachtelte Fallunterscheidungen nötig sind.

Der Ablauf eines Programms P zur Anfangseingabe (Anfangskonfiguration) $e = (1, e_1, \ldots, e_m)$ (die Anfangszeile besitzt die Zeilennummer 1!) wird durch die Hintereinanderschaltung der Programmabbildung $\varphi = \varphi_P$ mit sich selbst beschrieben. Nach dem ersten Programmschritt, bei dem der Befehl in der ersten Programmzeile aufgerufen wird, erhält man die Folgekonfiguration $\varphi(e)$. Die nullte Komponente von $\varphi(e)$ gibt an, mit welcher Programmzeile weitergearbeitet wird. Dies ist aber alles in φ kodiert, so dass das Ergebnis nach dem nächsten Schritt einfach $\varphi(\varphi(e))$ ist. Das Ergebnis nach dem s-ten Rechenschritt (Befehlszeilenwechsel) ist also

$$\varphi(\ldots(\varphi(\varphi(e)))\ldots),$$

wobei s-mal φ angewendet wird. Dafür schreiben wir auch $\varphi^s(e)$. Die aktuelle Zeilennummer ist dabei stets als nullte Komponente von $\varphi^s(e)$ ablesbar, wofür wir $(\varphi^s(e))_0$ schreiben.

Wie wirkt sich nun die Eigenschaft eines Programms, anzuhalten oder nicht, auf diese Iterationen von φ aus? Das Programm hält genau dann an, wenn es bei Eingabe von e ein s mit $(\varphi^s(e))_0 = h$ gibt.

Wir möchten die Wirkungsweise von Programmen in der Sprache der Arithmetik selbst repräsentieren, um dort das Halteproblem (und seine Unentscheidbarkeit) nachbilden zu können. Dafür müssen wir zunächst die einzelnen Programmschritte arithmetisch erfassen.

Definition 20.3. Den Programmzeilen $B_1, \ldots, B_h$ eines Registerprogramms mit m Registern werden die folgenden arithmetischen Ausdrücke $A_1, \ldots, A_h$ in den freien Variablen $z, r_1, \ldots, r_m, z', r'_1, \ldots, r'_m$ zugeordnet.

(1) Bei $B_\ell = i+$ setzt man

$$A_\ell := (z = \ell) \to (z' = z + 1) \wedge (r'_1 = r_1) \wedge \ldots \wedge (r'_{i-1} = r_{i-1}) \wedge (r'_i = r_i + 1) \\ \wedge (r'_{i+1} = r_{i+1}) \wedge \ldots \wedge (r'_m = r_m).$$

(2) Bei $B_\ell = i-$ setzt man

$$A_\ell := (z = \ell) \to (z' = z + 1) \wedge (r_1' = r_1) \wedge \ldots \wedge (r_{i-1}' = r_{i-1}) \\ \wedge ((r_i = 0) \to (r_i' = r_i)) \wedge (\neg(r_i = 0) \to (r_i' + 1 = r_i)) \\ \wedge (r_{i+1}' = r_{i+1}) \wedge \ldots \wedge (r_m' = r_m).$$

(3) Bei $B_\ell = C(ij)$ setzt man

$$A_\ell := (z = \ell) \to ((r_i = 0) \to (z' = j)) \wedge (\neg(r_i = 0) \to (z' = z + 1)) \\ \wedge (r_1' = r_1) \wedge \ldots \wedge (r_m' = r_m).$$

(4) Bei $B_\ell = B_h = H$ setzt man

$$A_h := (z = h) \to (z' = z) \wedge (r_1' = r_1) \wedge \ldots \wedge (r_m' = r_m)\,.$$

Hierbei werden die natürlichen Zahlen ℓ und j in den arithmetischen Ausdrücken durch die entsprechenden Summen $1 + \cdots + 1$ repräsentiert, die Abfrage am i-ten Register schlägt sich in der Variablenbezeichnung nieder.

Wie bei der Programmabbildung ist es sinnvoll, für alle Programmzeilennummern (also auch für $\ell > h$) einen arithmetischen Ausdruck zu haben. Dazu setzen wir

$$A_{h+1} := (z \geq h + 1) \to (z' = z) \wedge (r_1' = r_1) \wedge \ldots \wedge (r_m' = r_m)$$

(wobei $z \geq h+1$ eine Abkürzung ist). Zu einem gegebenen Programm bestehend aus den Programmzeilen $B_1, \ldots, B_h$ betrachtet man die Konjunktion der soeben eingeführten zugehörigen arithmetischen Repräsentierungen, also $A_P = A_1 \wedge A_2 \wedge \ldots \wedge A_h \wedge A_{h+1}$. Dieser Ausdruck repräsentiert die Programmabbildung.

Lemma 20.4. *Es sei P ein Registerprogramm mit den Programmzeilen B_1, $\ldots, B_h$ und m Registern mit den zugehörigen arithmetischen Ausdrücken $A_1, \ldots, A_h$ in den freien Variablen $z, r_1, \ldots, r_m, z', r_1', \ldots, r_m'$. Es sei $A_P = A_1 \wedge \ldots \wedge A_h \wedge A_{h+1}$. Dann ist A_P eine arithmetische Repräsentierung der Programmabbildung φ_P.*

Beweis. Die Variablen z, z', r_j, r_j' seien durch die natürlichen Zahlen ℓ, ℓ', n_j, n_j' belegt. Wir müssen zeigen, dass die Gleichheit

$$\varphi_P(\ell, n_1, \ldots, n_m) = (\ell', n_1', \ldots, n_m')$$

genau dann gilt, wenn

$$\mathbb{N} \vDash A_P(\ell, \ell', n_1, \ldots, n_m, n_1', \ldots, n_m')$$

gilt. Der Ausdruck A_P gilt genau dann, wenn sämtliche Ausdrücke A_1, A_2, $\ldots, A_h, A_{h+1}$ gelten. Es sei ℓ fixiert. Dann gelten sämtliche A_k, $k \neq \ell$, automatisch, da für diese Ausdrücke der Vordersatz nicht gilt. Die Gültigkeit von A_P bei dieser Belegung bedeutet also, dass der Nachsatz in A_ℓ gelten muss.

Sowohl $\varphi(\ell, -)$ als auch der Nachsatz von A_ℓ drücken die Wirkungsweise des Befehls B_ℓ aus, daher gilt die Abbildungsgleichheit genau dann, wenn A_ℓ wahr ist. □

20.4. **Die β-Funktion.**

Das Halteproblem führte zu der Existenzaussage, dass es eine Iteration der Programmabbildung gibt, für die die 0-te Komponente gleich der Haltezeilennummer ist. Die arithmetische Repräsentierung dieser Existenzaussage bedarf einiger Vorbereitungen.

Eine natürliche Zahl n lässt sich bekanntlich im Zehnersystem als

$$n = a_0 1 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k$$

schreiben, wobei die a_i zwischen 0 und 9 liegen. Umgekehrt definiert eine endliche Ziffernfolge $(a_0, a_1, \ldots, a_k)$ (bzw. in alltäglicher Schreibweise $a_k a_{k-1} \ldots a_1 a_0$) eine natürliche Zahl. Anstatt der Basis 10 kann man jede natürliche Zahl $p \geq 2$ als Basis nehmen (für viele Zwecke ist auch die Basis 1 erlaubt, eine Zahl n wird dann einfach durch das n-fache Hintereinanderschreiben der 1 repräsentiert). Man spricht dann von der p-adischen Entwicklung (oder Darstellung) der Zahl. Die p-adische Entwicklung einer natürlichen Zahl ist eindeutig.

Sei $p \geq 2$ fixiert. Wie berechnet man die Ziffernfolge einer gegebenen Zahl n? Zuerst betrachten wir die Ziffer (die Einerziffer) $a_0(n) = a(n, 0)$. Es gilt die rekursive Beziehung

$$a(n,0) = \begin{cases} n, \text{falls } n < p\,, \\ a(n-p,0) \text{ sonst}\,. \end{cases}$$

Dies beruht einfach darauf, dass bei $n \geq p$ das Abziehen von p die Ziffer zu p^0 nicht ändert. Man beachte, dass sowohl die Abfrage, die die Fallunterscheidung in dieser Definition konstituiert, als auch die Subtraktion im Fall 2 mit einer Registermaschine durchführbar sind, und dass dadurch eine R-berechenbare Funktion vorliegt.

Auch die Definition der anderen Ziffern geschieht rekursiv. Wenn man von n die (schon berechnete) Ziffer zu p^0 abzieht, so erhält man eine durch p teilbare Zahl. Zwischen der Ziffernentwicklung von n und von $m = \frac{n-a(n,0)}{p}$ besteht ein direkter Zusammenhang, die Ziffer a_{i+1} von n ist einfach die Ziffer a_i von m. Daher ist für $i \geq 0$

$$a(n,i+1) = \begin{cases} 0, \text{falls } n < p^{i+1}\,, \\ a\left(\frac{n-a(n,0)}{p}, i\right) \text{ sonst}\,. \end{cases}$$

Damit ist die Berechnung der $(i+1)$-ten Ziffer auf die Berechnung der i-ten Ziffer einer kleineren Zahl rekursiv zurückgeführt. Die Bedingung in der Abfrage und die Subtraktion und die Division in der Definition sind durch eine Registermaschine durchführbar. Diese Funktionsvorschrift berechnet nicht

nur die „benötigten“ Ziffern, sondern auch alle höheren, wobei natürlich für alle unbenötigten 0 herauskommt.

Wir führen nun die β-Funktion ein. Der Hauptzweck dieser Funktion soll sein, endliche Folgen von natürlichen Zahlen unterschiedlicher Länge durch drei Zahlen zu kodieren. Die Grundidee ist, dies über die p-adische Entwicklung zu tun, wobei die drei Eingabezahlen einen Zahlwert, eine Basis und eine Ziffernstelle repräsentieren, und die Ausgabe die Ziffernfolge ist. Zugleich soll diese Funktion arithmetisch repräsentierbar sein, so dass die folgende Funktion etwas komplizierter aussieht. Wir folgen weitgehend dem Zugang von Ebbinghaus, Flum, Thomas.

Definition 20.5. Unter der β- *Funktion* versteht man die Abbildung

$$\mathbb{N}^3 \longrightarrow \mathbb{N},\ (p,n,i) \longmapsto \beta(p,n,i),$$

die folgendermaßen festgelegt ist. $\beta(p,n,i)$ ist die kleinste Zahl $a \in \mathbb{N}$, die die Bedingung erfüllt, dass es natürliche Zahlen b_0, b_1, b_2 gibt, die die folgenden Eigenschaften erfüllen:

(1) $n = b_0 + b_1\left((i+1) + ap + b_2p^2\right)$.
(2) $a < p$.
(3) $b_0 < b_1$.
(4) b_1 ist eine Quadratzahl.
(5) Alle Teiler $d \neq 1$ von b_1 sind ein Vielfaches von p.

Wenn kein solches a existiert, so ist $\beta(p,n,i) = 0$.

Zunächst ist klar, dass diese Funktion arithmetisch repräsentierbar ist. Wenn p eine Primzahl ist, so bedeutet Teil (5), dass b_1 eine Primzahlpotenz ist, und Teil (4), dass der Exponent geradzahlig ist. Das folgende Lemma sichert die gewünschte Eigenschaft der β-Funktion, nämlich die Eigenschaft, endliche Folgen zu repräsentieren.

Lemma 20.6. *Zu jeder endlichen Folge $(a_0,\ldots,a_s)$ aus $\mathbb{N}$ gibt es natürliche Zahlen p,n derart, dass $\beta(p,n,i) = a_i$ für $i \leq s$ ist.*

Beweis. Es sei die endliche Folge $(a_0,a_1,\ldots,a_s)$ vorgegeben. Wir wählen eine Primzahl p, die größer als alle a_i und größer als $s+1$ ist. Es sei

$$\begin{aligned} n &:= 1\cdot p^0 + a_0p^1 + 2p^2 + a_1p^3 + \cdots + (s+1)p^{2s} + a_sp^{2s+1} \\ &= \sum_{i=0}^{s} a_ip^{2i+1} + \sum_{i=0}^{s}(i+1)p^{2i} \\ &= \sum_{i=0}^{s}(i+1+a_ip)p^{2i}. \end{aligned}$$

Die vorgegebene Folge ist also die Folge der Ziffern der ungeraden Stellen in der p-adischen Ziffernentwicklung von n. Wir behaupten $\beta(p,n,k) = a_k$ für

$k \leq s$. Zunächst erfüllt a_k die in der Definition der β-Funktion formulierten Eigenschaften, und zwar mit

$$b_0 = 1p^0 + a_0p^1 + 2p^2 + a_1p^3 + \cdots + kp^{2k-2} + a_{k-1}p^{2k-1},$$
$$b_1 = p^{2k},$$
$$b_2 = (k+2) + a_{k+1}p + (k+3)p^2 + \cdots + (s+1)p^{2(s-k)-2} + a_sp^{2(s-k)-1}.$$

Die erste Eigenschaft ergibt sich aus

$$\begin{aligned} n &= \sum_{i=0}^{s} a_ip^{2i+1} + \sum_{i=0}^{s}(i+1)p^{2i} \\ &= \sum_{i=0}^{k-1} a_ip^{2i+1} + \sum_{i=0}^{k-1}(i+1)p^{2i} + \sum_{i=k}^{s} a_ip^{2i+1} + \sum_{i=k}^{s}(i+1)p^{2i} \\ &= b_0 + p^{2k}\left(\sum_{i=0}^{s-k} a_{k+i}p^{2i+1} + \sum_{i=0}^{s-k}(k+i+1)p^{2i}\right) \\ &= b_0 + p^{2k}\left(k+1+a_kp + \sum_{i=1}^{s-k} a_{k+i}p^{2i+1} + \sum_{i=1}^{s-k}(k+i+1)p^{2i}\right) \\ &= b_0 + b_1\left(k+1+a_kp+b_2p^2\right), \end{aligned}$$

die anderen sind klar. Wenn umgekehrt ein a die Bedingungen erfüllt (mit c_0, c_1, c_2), wobei $c_1 = p^{2\ell}$ ist, so ist

$$\begin{aligned} n &= b_0 + (k+1)p^{2k} + a_kp^{2k+1} + b_2p^{2k+2} \\ &= c_0 + (k+1)p^{2\ell} + ap^{2\ell+1} + c_2p^{2\ell+2}. \end{aligned}$$

Da die p-adische Entwicklung von n eindeutig ist, folgen daraus und aus den weiteren Bedingungen die Gleichheiten $\ell = k$ und $a = a_k$. □

20. Arbeitsblatt

20.1. **Übungsaufgaben.**

Aufgabe 20.1. Zeige, dass die folgenden Teilmengen T der natürlichen Zahlen arithmetisch repräsentierbar sind.

(1) Eine konkrete endliche Menge $\{n_1, \ldots, n_k\}$.
(2) Die Menge aller Vielfachen von 5.
(3) Die Menge der Primzahlen.
(4) Die Menge der Quadratzahlen.
(5) Die Menge der Zahlen, in deren Primfaktorzerlegung jeder Exponent maximal 1 ist.

Aufgabe 20.2. Zeige, dass die folgenden Abbildungen $\varphi\colon \mathbb{N}^r \to \mathbb{N}$ arithmetisch repräsentierbar sind.

(1) Die Addition

$$\mathbb{N}^2 \longrightarrow \mathbb{N},\ (x,y) \longmapsto x+y.$$

(2) Die Multiplikation

$$\mathbb{N}^2 \longrightarrow \mathbb{N},\ (x,y) \longmapsto x \cdot y.$$

(3) Die eingeschränkte Subtraktion

$$\mathbb{N}^2 \longrightarrow \mathbb{N},\ (x,y) \longmapsto \max(x-y,0),$$

die bei $y > x$ den Wert 0 besitzt.

(4) Die Restfunktion

$$\mathbb{N}^2 \longrightarrow \mathbb{N},\ (n,t) \longmapsto r(n,t),$$

die den Rest (zwischen 0 und $t-1$) bei Division von n durch t angibt.

Aufgabe 20.3. Es sei

$$f\colon\ \mathbb{N} \longrightarrow \mathbb{N}$$

eine Polynomfunktion mit $f(n) = a_d n^d + a_{d-1}n^{d-1} + \cdots + a_1 n + a_0$ mit Koeffizienten $a_i \in \mathbb{N}$. Zeige, dass f durch den Ausdruck $y = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ arithmetisch repräsentiert wird.

Aufgabe 20.4. Zeige, dass eine lineare Abbildung

$$F\colon\ \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

arithmetisch repräsentierbar ist.

Aufgabe 20.5. Zeige, dass eine polynomiale Abbildung (mit Koeffizienten aus $\mathbb{N}$)

$$F\colon\ \mathbb{N}^r \longrightarrow \mathbb{N},\ (x_1,\ldots,x_n) \longmapsto F(x_1,\ldots,x_n),$$

arithmetisch repräsentierbar ist.

Aufgabe 20.6.* Zeige, dass die Abbildung

$$f\colon\ \mathbb{N}^3 \longrightarrow \mathbb{N},\ (x,y,z) \longmapsto xy^2 - z^2 + 2z^3,$$

(wohldefiniert und) arithmetisch repräsentierbar ist.

Aufgabe 20.7. Zeige, dass die Abbildung

$$F\colon \mathbb{N} \longrightarrow \mathbb{N}$$

mit

$$F(n) = \begin{cases} \sqrt{n}\,, \text{ falls } \sqrt{n} \in \mathbb{N}\,, \\ 0 \text{ sonst}\,, \end{cases}$$

arithmetisch repräsentierbar ist.

Aufgabe 20.8. Es sei

$$\varphi\colon \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

eine Abbildung und $\Gamma \subseteq \mathbb{N}^r \times \mathbb{N}^s$ der zugehörige Graph, also die Menge

$$\Gamma = \{(n_1, \ldots, n_{r+s}) | \, \varphi(n_1, \ldots, n_r) = (n_{r+1}, \ldots, n_{r+s})\}\,.$$

Zeige, dass φ genau dann arithmetisch repräsentierbar ist, wenn Γ (als Relation) arithmetisch repräsentierbar ist.

Aufgabe 20.9. Es sei

$$\varphi\colon \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

eine arithmetisch repräsentierbare Abbildung. Zeige, dass zu jedem Punkt $P \in \mathbb{N}^s$ die Faser

$$\varphi^{-1}(P) \subseteq \mathbb{N}^r$$

arithmetisch repräsentierbar ist.

Aufgabe 20.10. Es sei

$$\varphi\colon \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

eine arithmetisch repräsentierbare Abbildung und es sei $T \subseteq \mathbb{N}^s$ eine arithmetisch repräsentierbare Relation. Zeige, dass das Urbild

$$\varphi^{-1}(T) \subseteq \mathbb{N}^r$$

arithmetisch repräsentierbar ist.

Aufgabe 20.11. Wir betrachten das Registerprogramm mit drei Registern (bei leerem dritten Register berechnet es die Summe der ersten beiden Registerinhalte)

(1) $C(2,5)$
(2) $1+$
(3) $2-$
(4) $C(3,1)$
(5) Halte an

a) Erstelle die Programmabbildung für dieses Programm.

b) Welche Beziehung besteht zwischen der Programmabbildung und der Additionsabbildung

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},\ (x, y) \longmapsto x + y?$$

c) Erstelle eine arithmetische Repräsentierung für dieses Programm.

Aufgabe 20.12. Zeige explizit, dass die in Vorlesung 18 besprochenen Registerprogramme (also ihre zugehörigen Programmabbildungen) arithmetisch repräsentierbar sind.

20.2. **Aufgaben zum Abgeben.**

Aufgabe 20.13. (2 Punkte)

Es sei

$$\varphi\colon\ \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

eine Abbildung. Zeige, dass φ genau dann arithmetisch repräsentierbar ist, wenn sämtliche Komponentenfunktionen φ_i, $1 \leq i \leq s$, arithmetisch repräsentierbar sind.

Aufgabe 20.14. (4 Punkte)

Zeige, dass die Abbildung

$$F\colon\ \mathbb{N} \times \mathbb{N}_+ \longrightarrow \mathbb{N},\ (x, y) \longmapsto \left\lfloor \frac{x}{y} \right\rfloor,$$

arithmetisch repräsentierbar ist.

Aufgabe 20.15. (5 Punkte)

Zeige, dass die β-Funktion arithmetisch repräsentierbar ist.

Aufgabe 20.16. (2 Punkte)

Zeige, dass es nur abzählbar viele arithmetisch repräsentierbare Relationen gibt.

21. Vorlesung - Die Unentscheidbarkeit der Arithmetik

> Für uns gibt es kein Ignorabimus, und meiner Meinung nach auch für die Naturwissenschaft überhaupt nicht. Statt des törichten Ignorabimus heiße im Gegenteil unsere Losung: Wir müssen wissen, wir werden wissen.
>
> David Hilbert

Zuletzt haben wir gezeigt, wir man die Programmabbildung zu einem Registerprogamm arithmetisch repräsentieren kann. Die Programmabbildung enthält zwar die volle Information über das Programm, doch die Frage, wie man die Eigenschaft, ob ein Programm anhält oder nicht, arithmetisch repräsentiert, ist damit noch nicht beantwortet, sondern bedarf weiterer Überlegungen.

21.1. **Repräsentierbarkeit der Halteeigenschaft.**

Ein Durchlauf eines Registerprogramms P (das auf m Register Bezug nimmt) bis zum Rechenschritt t wird am einfachsten durch die Folge der Programmkonfigurationen K_s, $1 \leq s \leq t$, dokumentiert, wobei jede Programmkonfiguration K_s aus der Nummer der im Rechenschritt s abzuarbeitenden Programmzeile und der Folge der Registerinhalte (zu diesem Zeitpunkt) besteht. Wenn man diese Konfigurationen einfach hintereinander schreibt, so erhält man eine Folge von $t(m+1)$ Zahlen. Wenn umgekehrt eine solche Zahlenfolge gegeben ist, so kann man einfach überprüfen, ob sie den Durchlauf des Programms bis zum Schritt t korrekt dokumentiert. Man muss sicherstellen, dass sich jeder Abschnitt $(s+1)(m+1)+1, \ldots, (s+1)(m+1)+m+1$ aus dem Vorgängerabschnitt $s(m+1)+1, \ldots, s(m+1)+m+1$ ergibt, wenn die Programmzeile $s(m+1)+1$ angewendet wird (der Abschnitt muss also durch die Programmabbildung aus dem Vorgängerabschnitt hervorgehen).

Lemma 21.1. *Für ein Programm P für eine Registermaschine gibt es einen arithmetischen Ausdruck ψ_P, der genau dann (bei der Standardinterpretation in den natürlichen Zahlen) gilt, wenn das Programm anhält. Genauer gesagt: Wenn das Programm h Programmzeilen besitzt und m Register verwendet, so gibt es einen arithmetischen Ausdruck ψ_P in $2m$ freien Variablen derart, dass*

$$\mathbb{N} \vDash \psi_P(e_1, \ldots, e_m, a_1, \ldots, a_m)$$

genau dann gilt, wenn das Programm bei Eingabe von $(1, e_1, \ldots, e_m)$ nach endlich vielen Schritten bei der Konfiguration $(h, a_1, \ldots, a_m)$ anlangt (und insbesondere anhält).

Beweis. Es sei A_P der das Programm repräsentierende Ausdruck im Sinne von Lemma 20.4 in den Variablen $r_0, \ldots, r_m, r'_0, \ldots, r'_m$ (zur Notationsvereinfachung schreiben wir also r_0 statt z und r'_0 statt z'.). Es sei ϑ der Ausdruck (in den vier freien Variablen p, n, i, r), der die β-Funktion arithmetisch repräsentiert. Der Ausdruck

$$\vartheta(p, n, i, r)$$

ist also genau dann wahr in $\mathbb{N}$, wenn[27] $\beta(p, n, i) = r$ ist. Diese Beziehung verwenden wir für $i = s(m+1) + j$ (bzw. $i = (s+1)(m+1) + j$) und $r = r_j$ (bzw. $r = r'_j$) und $j = 0, \ldots, m$. Daher ist der Ausdruck (in den freien Variablen p, n, s, r_j, r'_j)

$$\begin{aligned} T(p, n, s) :=& \vartheta(p, n, s(m+1), r_0) \wedge \ldots \wedge \vartheta(p, n, s(m+1) + m, r_m) \wedge \\ & \vartheta(p, n, (s+1)(m+1), r'_0) \wedge \ldots \wedge \vartheta(p, n, (s+1)(m+1) + m, r'_m) \end{aligned}$$

bei Interpretation in $\mathbb{N}$ genau dann wahr, wenn die β-Funktion $\beta(p, n, -)$ für die $m+1$ aufeinander folgenden Zahlen (eingesetzt in die dritte Komponente der β-Funktion) $s(m+1), s(m+1)+1, \ldots, s(m+1)+m$ gleich $r_0, r_1, \ldots, r_m$ und für die $m+1$ aufeinander folgenden Zahlen $(s+1)(m+1), (s+1)(m+1)+1, \ldots, (s+1)(m+1)+m$ gleich $r'_0, r'_1, \ldots, r'_m$ ist. An der mit $s(m+1)+j$ bezeichneten Stelle in $T(p, n, s)$ steht die $(m+1)$-fache Addition der Variablen s mit sich selbst plus die j-fache Addition der 1.

Mit diesem Ausdruck soll der Konfigurationsübergang beim s-ten Rechenschritt beschrieben werden. Da man die Registerbelegung beim s-ten Rechenschritt nicht von vornherein kennt, muss man den Übergang mit Allquantoren ansetzen. Der Ausdruck

$$E(p, n, s) := \forall r_0 \forall r_1 \ldots \forall r_m \forall r'_0 \forall r'_1 \ldots \forall r'_m (T(p, n, s) \to A_P)$$

besagt, dass der durch p, n, s über die β-Funktion kodierte Konfigurationsübergang durch das Programm bewirkt wird.

In analoger Weise ist der Ausdruck (in den $m+2$ freien Variablen $p, n, x_1, \ldots, x_m$)

$$D(p, n)(x_1, \ldots, x_m) := \vartheta(p, n, 0, 1) \wedge \vartheta(p, n, 1, x_1) \wedge \ldots \wedge \vartheta(p, n, m, x_m)$$

(bei inhaltlicher Interpretation) genau dann wahr, wenn $\beta(p, n, 0) = 1$ und $\beta(p, n, j) = x_j$ für $j = 1, \ldots, m$ ist, und der Ausdruck (in den $m+3$ freien Variablen $p, n, t, y_1, \ldots, y_m$)

$$\begin{aligned} F(p, n, t)(y_1, \ldots, y_m) :=& \vartheta(p, n, t(m+1), h) \wedge \vartheta(p, n, t(m+1)+1, y_1) \wedge \\ & \ldots \wedge \vartheta(p, n, t(m+1)+m, y_m) \end{aligned}$$

$\beta(p, n, t(m+1)) = h$ und $\beta(p, n, t(m+1)+j) = y_j$ für $j = 1, \ldots, m$ ist.

[27] Wir verwenden hier für die Termvariablen und mögliche Einsetzungen die gleichen Buchstaben.

Somit besagt der Ausdruck

$$\psi_P = \exists p \exists n \exists t \, (D(p,n)(x_1,\ldots,x_m) \wedge \forall s(1 \leq s < t \rightarrow E(p,n,s)) \\ \wedge F(p,n,t)(y_1,\ldots,y_m)) \,,$$

dass das Programm mit der Startkonfiguration $(1, x_1, \ldots, x_m)$ anhält und dabei die Konfiguration $(h, y_1, \ldots, y_m)$ erreicht. □

21.2. **Die Unentscheidbarkeit der Arithmetik.**

Die Idee des folgenden Beweises beruht darauf, dass man, wie wir in der letzten Vorlesung gezeigt haben, die Arbeitsweise von Registerprogrammen mit arithmetischen Ausdrücken repräsentieren und damit die Unentscheidbarkeit des Halteproblems arithmetisch modellieren kann.

Satz 21.2. *Die Menge der wahren arithmetischen Ausdrücke (ohne freie Variablen) ist nicht R-entscheidbar. D.h. es gibt kein R-Entscheidungsverfahren, mit dem man von einem beliebigen vorgegebenen Ausdruck $\alpha \in L_0^{\mathrm{Ar}}$ der arithmetischen Sprache bestimmen kann, ob er (in der Standardinterpretation $\mathbb{N}$) wahr oder falsch ist.*

Beweis. Nach Lemma 21.1 gibt es zu jedem Programm P (mit h Befehlen und m Registern) einen arithmetischen Ausdruck ψ_P in $2m$ freien Variablen $x_1, \ldots, x_m, y_1, \ldots, y_m$, der bei der Belegung mit $e_1, \ldots, e_m, a_1, \ldots, a_m \in \mathbb{N}$ genau dann wahr ist, wenn das Programm, angesetzt auf $(1, e_1, \ldots, e_m)$, schließlich mit der Konfiguration $(h, a_1, \ldots, a_m)$ anhält. Der Ausdruck

$$\varphi_P \;=\; \psi_P(0, 0, \ldots, 0, y_1, \ldots, y_m)$$

besagt daher, dass das Programm bei Nulleingabe mit der Registerbelegung $(y_1, \ldots, y_m)$ anhält und der Ausdruck (ohne freie Variablen)

$$\theta_P \;=\; \exists y_1 \exists y_2 \ldots \exists y_m \varphi_P$$

besagt, dass das Programm überhaupt anhält. Es gilt also

$$\mathbb{N} \vDash \theta_P$$

genau dann, wenn P bei Nulleingabe anhält. Man beachte, dass die Abbildung, die einem jeden Programm P dieses θ_P zuordnet, effektiv durch eine Registermaschine durchführbar ist.

Wenn es ein Entscheidungsverfahren für arithmetische Sätze geben würde, so könnte man insbesondere auch die Richtigkeit von $\mathbb{N} \vDash \theta_P$ entscheiden. Doch dann würde es ein Entscheidungsverfahren für das Halteproblem im Widerspruch zu Satz 19.6 geben. □

21.3. **Folgerungen aus der Unentscheidbarkeit.**

Wir werden aus der Unentscheidbarkeit weitere Folgerungen über die Aufzählbarkeit und die Axiomatisierbarkeit der Arithmetik in der ersten Stufe ziehen. Dazu werden wir diese Begriffe allgemein für sogenannte Theorien einführen.

Definition 21.3. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Teilmenge $T \subseteq L_0^S$ heißt *Theorie*, wenn T abgeschlossen unter der Ableitungsbeziehung ist, d.h. wenn aus $T \vdash \alpha$ für $\alpha \in L_0^S$ bereits $\alpha \in T$ folgt.

Zu jeder Ausdrucksmenge Γ ist die Menge $\Gamma^\vdash$ der aus Γ ableitbaren Sätze eine Theorie. Häufig wählt man „kleine“ und „handhabbare“ Mengen, um übersichtliche Theorien zu erhalten. Mengen, die eine Theorie erzeugen, heißen auch *Axiomensysteme* für diese Theorie. Es ist im Allgemeinen schwierig zu entscheiden, ob ein bestimmter Satz aus einem Axiomensystem ableitbar ist, also zu der entsprechenden Theorie gehört.

Wenn I eine Interpretation einer Sprache erster Stufe ist, so ist $I_0^\models$, also die Menge der in dem Modell gültigen Sätze, ebenfalls eine Theorie. Dies folgt direkt aus der Korrektheit des Ableitungskalküls. So ist $\mathbb{N}_0^\models$ eine Theorie zur Sprache L_0^{Ar}, die alle bei der Standardinterpretation gültigen Sätze beinhaltet.

Die Menge aller aus den erststufigen Peano-Axiomen ableitbaren Sätze bildet die *Peano-Arithmetik*, die wir hier PA nennen. Es ist $\mathrm{PA} \subseteq \mathbb{N}_0^\models$.

Die Gesamtmenge L_0^S ist natürlich ebenfalls abgeschlossen unter der Ableitungsbeziehung. Sie ist widersprüchlich im Sinne der folgenden Definition.

Definition 21.4. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^S$ heißt *widersprüchlich*, wenn es einen Satz $\alpha \in L_0^S$ mit $\alpha \in T$ und $\neg\alpha \in T$ gibt.

Lemma 21.5. *Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe, wobei die Sprache zumindest eine Variable besitzen möge. Es sei $T \subseteq L_0^S$ eine Theorie. Dann ist T genau dann widersprüchlich, wenn $T = L_0^S$ ist.*

Beweis. Siehe Aufgabe 21.4. □

Man interessiert sich natürlich hauptsächlich für widerspruchsfreie (also nicht widersprüchliche) Theorien.

Definition 21.6. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie T heißt *vollständig*, wenn für jeden Satz $\alpha \in L_0^S$ gilt $\alpha \in T$ oder $\neg\alpha \in T$.

Dabei ist grundsätzlich auch erlaubt, dass sowohl α als auch $\neg\alpha$ zu T gehört, doch liegt dann bereits eine widersprüchliche Theorie vor. Zu einer Interpretation I einer Sprache erster Stufe ist die Gültigkeitsmenge $I_0^{\models}$ eine widerspruchsfreie vollständige Theorie. Dies ergibt sich aus dem rekursiven Aufbau der Gültigkeitsbeziehung (die beinhaltet, dass wir das Tertium non datur anerkennen - sonst wäre eine mathematische Argumentation nicht möglich).

Definition 21.7. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^S$ heißt *endlich axiomatisierbar*, wenn es endlich viele Sätze $\alpha_1, \ldots, \alpha_n \in L_0^S$ mit[28] $T = \{\alpha_1, \ldots, \alpha_n\}^{\vdash}$ gibt.

Das ist häufig zu viel verlangt, wie die erststufige Peano-Arithmetik zeigt (zumindest haben wir sie nicht durch ein endliches Axiomensystem eingeführt). Eine schwächere Variante wird in der folgenden Definition beschrieben.

Definition 21.8. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^S$ heißt *aufzählbar axiomatisierbar*, wenn es eine R-aufzählbare Satzmenge $\Gamma \subseteq L_0^S$ mit $T = \Gamma^{\vdash}$ gibt.

Lemma 21.9. *Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine aufzählbar axiomatisierbare Theorie $T \subseteq L_0^S$ ist R-aufzählbar.*

Beweis. Es sei Γ eine R-aufzählbare Satzmenge, die T axiomatisiert, und es sei α_n, $n \in \mathbb{N}_+$, eine R-Aufzählung von Γ. Es sei β_n, $n \in \mathbb{N}_+$, eine R-Aufzählung der prädikatenlogischen Tautologien aus L^S. Wenn ein Satz γ aus Γ ableitbar ist, so gibt es eine endliche Auswahl $\alpha_1, \ldots, \alpha_n$ aus Γ (bzw. aus der gewählten Aufzählung) derart, dass

$$\vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \gamma$$

eine prädikatenlogische Tautologie ist. Daher leistet das folgende Verfahren, bei dem n wächst, das Gewünschte: Für jedes n notiert man die Tautologien $\beta_1, \ldots, \beta_n$ in der Form

$$\beta_i = \delta_1 \wedge \ldots \wedge \delta_s \to \epsilon.$$

Wenn β_i überhaupt diese Form besitzt, so ist diese eindeutig betimmt. Danach überprüft man für jedes $i \leq n$, ob alle $\delta_1, \ldots, \delta_s$ zu $\{\alpha_1, \ldots, \alpha_n\}$ gehören. Falls ja, und wenn ϵ ein Satz ist, so wird ϵ notiert. Danach geht man zum nächsten i. Wenn man $i = n$, erreicht hat, so geht man zu $n+1$, wobei man aber wieder bei $i = 1$ anfängt. □

Satz 21.10. *Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Jede aufzählbare (oder aufzählbar axiomatisierbare), widerspruchsfreie und vollständige Theorie $T \subseteq L_0^S$ ist entscheidbar.*

[28] Das Ableitungssymbol schränken wir hier auf die Sätze ein, eigentlich müssten wir $T = \{\alpha_1, \ldots, \alpha_n\}^{\vdash} \cap L_0^S$ schreiben.

Beweis. Nach Lemma 21.9 bedeutet die aufzählbare Axiomatisierbarkeit, dass schon die Theorie selbst aufzählbar ist. Sei also T aufzählbar, vollständig und widerspruchsfrei, und sei α_n, $n \in \mathbb{N}_+$, eine Aufzählung von T. Es sei $\beta \in L_0^S$ ein Satz. Wegen der Widerspruchsfreiheit und der Vollständigkeit gilt entweder $\beta \in T$ oder $\neg\beta \in T$. Daher kommt entweder β oder $\neg\beta$ in der Aufzählung von T vor. Bei $\alpha_n = \beta$ ist $\beta \in T$ und bei $\alpha_n = \neg\beta$ ist $\beta \notin T$. □

Bemerkung 21.11. Eine widersprüchliche Theorie ist natürlich aufzählbar, vollständig und entscheidbar, da sie jeden Satz enthält. Ohne die Voraussetzung der Widerspruchsfreiheit ist aber das Argument im Beweis zu Satz 21.10 nicht durchführbar. Wenn in einer Aufzählung einer Theorie eine widersprüchliche Aussage auftritt, so ist die Theorie natürlich widersprüchlich. Wenn aber bis zu einem bestimmten Zeitpunkt keine widersprüchliche Aussage auftritt, so lässt sich nicht entscheiden, ob dies an der Widerspruchsfreiheit der Theorie oder der Art der Aufzählung liegt. Wenn also in der Aufzählung $\neg\beta$ vorkommt, so kann man daraus nicht ohne die Bedingung der Widerspruchsfreiheit auf $\beta \notin T$ schließen.

Satz 21.12. *Die Menge der wahren arithmetischen Ausdrücke ist nicht R-aufzählbar. D.h. es gibt kein R-Verfahren, das alle in $\mathbb{N}$ wahren Sätze der arithmetischen Sprache auflistet.*

Beweis. Dies folgt direkt aus Satz 21.10 und aus Satz 21.2. □

Korollar 21.13. *Die (erststufige) Peano-Arithmetik ist unvollständig.*

Beweis. Wegen $PA \subseteq \mathbb{N}^{\vdash}$ würde die Vollständigkeit hier die Gleichheit bedeuten. Da die Peano-Arithmetik R-aufzählbar ist, würde aus Satz 21.10 die Entscheidbarkeit folgen im Widerspruch zu Satz 21.2. □

Die Lücke zwischen PA und $\mathbb{N}_0^{\vdash}$ kann man nicht systematisch auffüllen, da man das vorstehende Argument auf jede aufzählbar-axiomatisierbare Theorie T mit $PA \subseteq T \subseteq \mathbb{N}_0^{\vdash}$ anwenden kann.

21. Arbeitsblatt

21.1. **Übungsaufgaben.**

Aufgabe 21.1. Beschreibe für die in Vorlesung 18 besprochenen Registerprogramme die Konfigurationsfolge bei Nulleingabe.

Aufgabe 21.2. Erstelle für das Registerprogramm (mit keinem Register und leerer Anfangsbelegung)

(1) Halte an

den zugehörigen arithmetischen Ausdruck, der die Anhalteeigenschaft beschreibt.

Aufgabe 21.3. Erstelle für das Registerprogramm (mit zwei Registern R_1, R_2 und leerer Anfangsbelegung)

(1) 1+
(2) 2−
(3) Halte an

den zugehörigen arithmetischen Ausdruck, der die Anhalteeigenschaft beschreibt.

Aufgabe 21.4. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe, wobei die Sprache zumindest eine Variable besitzen möge. Es sei $T \subseteq L_0^S$ eine Theorie. Zeige, dass T genau dann widersprüchlich ist, wenn $T = L_0^S$ ist.

Aufgabe 21.5. Kann es ein Entscheidungsverfahren für mathematisch relevante Untertheorien $T \subseteq L_0^{\mathrm{Ar}}$ geben?

Aufgabe 21.6. Kann es ein Entscheidungsverfahren für die Symbolalphabete $\{0, 1, +\}$ bzw. $\{0, 1, \cdot\}$ (jeweils mit Variablen) geben? Wo geht bei der Arithmetisierung der Registerprogramme die Addition und wo die Multiplikation ein?

Aufgabe 21.7. Gibt es offene zahlentheoretische Probleme, die ohne Bezug auf die Addition oder ohne Bezug auf die Multiplikation formuliert werden können?

Aufgabe 21.8. Kann es mathematische Probleme innerhalb entscheidbarer Theorien geben?

Aufgabe 21.9. Zeige, dass eine endlich axiomatisierbare Theorie auch durch einen einzigen Ausdruck axiomatisierbar ist.

Aufgabe 21.10. Es sei $T \subseteq L^S$ eine aufzählbar axiomatisierbare Theorie und $\alpha_1, \ldots, \alpha_n \in L^S$. Zeige, dass dann auch

$$T' = (T \cup \{\alpha_1, \ldots, \alpha_n\})^{\vdash}$$

aufzählbar axiomatisierbar ist.

Aufgabe 21.11. Es seien $T_1, T_2 \subseteq L^S$ aufzählbar axiomatisierbare Theorien. Zeige, dass dann auch $(T_1 \cup T_2)^{\vdash}$ aufzählbar ist.

Aufgabe 21.12.*

Zeige, dass die erststufige Peano-Arithmetik PA eine vollständige widerspruchsfreie erststufige Erweiterung M, also $PA \subseteq M \subseteq L_0^{\mathrm{Ar}}$, besitzt, die von $\mathbb{N}_0^{\models}$ verschieden ist.

Aufgabe 21.13. Entwerfe ein R-Entscheidungsverfahren dafür, ob die Goldbach-Vermutung aus der erststufigen Peano-Arithmetik ableitbar ist.

Tipp: Verwende Aufgabe 19.10, Aufgabe 21.15 und Lemma 21.9.

21.2. **Aufgaben zum Abgeben.**

Aufgabe 21.14. (4 Punkte)

Erstelle für das Registerprogramm (mit zwei Registern R_1, R_2 und leerer Anfangsbelegung)

(1) 1+
(2) $C(2,1)$
(3) Halte an

den zugehörigen arithmetischen Ausdruck, der die Anhalteeigenschaft beschreibt.

Aufgabe 21.15. (3 Punkte)

Begründe, dass die (durch die erststufigen Peano-Axiome definierte) Peano-Arithmetik aufzählbar-axiomatisierbar ist.

Aufgabe 21.16. (3 Punkte)

Zeige, dass es zwischen der erststufigen Peano-Arithmetik und der Standardarithmetik unendlich viele Theorien gibt.

22. Vorlesung - Der Fixpunktsatz

22.1. **Repräsentierbarkeit in einer Theorie.**

Wir haben schon in der zwanzigsten Vorlesung davon gesprochen, wann eine arithmetische r-stellige Relation R (bzw. Funktion) in $\mathbb{N}$ arithmetisch repräsentierbar ist, wann es also einen arithmetischen Ausdruck ψ mit r freien Variablen derart gibt, dass dieser Ausdruck für jede Belegung genau

dann wahr wird, wenn die Relation auf das Belegungstupel zutrifft. Da $\mathbb{N}^{\vDash}$ vollständig ist, ergibt sich daraus die Äquivalenz, dass $(n_1, \ldots, n_r) \notin R$ äquivalent zur Nichtgültigkeit $\mathbb{N} \nvDash \psi(n_1, \ldots, n_r)$ und somit auch zur Gültigkeit der Negation $\mathbb{N} \vDash \neg\psi(n_1, \ldots, n_r)$ ist. Bei nichtvollständigen Ausdrucksmengen bzw. Theorien wollen wir auch von Repräsentierungen sprechen, wobei wir diese zweite Eigenschaft explizit fordern müssen.

Definition 22.1. Es sei Γ eine Menge von arithmetischen Ausdrücken. Eine Relation $T \subseteq \mathbb{N}^r$ heißt *repräsentierbar* in Γ, wenn es einen L^{Ar}-Ausdruck ψ in r freien Variablen derart gibt, dass für alle r-Tupel $(n_1, \ldots, n_r) \in \mathbb{N}^r$ die beiden Eigenschaften

(1) Wenn $(n_1, \ldots, n_r) \in T$, so ist $\Gamma \vdash \psi(n_1, \ldots, n_r)$,
(2) Wenn $(n_1, \ldots, n_r) \notin T$, so ist $\Gamma \vdash \neg\psi(n_1, \ldots, n_r)$,

gelten.

Definition 22.2. Es sei Γ eine Menge von arithmetischen Ausdrücken. Eine Funktion

$$F\colon\ \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

heißt *repräsentierbar* in Γ, wenn es einen L^{Ar}-Ausdruck ψ in $r + s$ freien Variablen derart gibt, dass für alle $(r + s)$-Tupel $(n_1, \ldots, n_{r+s}) \in \mathbb{N}^{r+s}$ die folgenden Eigenschaften

(1) Wenn $F(n_1, \ldots, n_r) = (n_{r+1}, \ldots, n_{r+s})$, so ist $\Gamma \vdash \psi(n_1, \ldots, n_{r+s})$,
(2) Wenn $F(n_1, \ldots, n_r) \neq (n_{r+1}, \ldots, n_{r+s})$, so ist $\Gamma \vdash \neg\psi(n_1, \ldots, n_{r+s})$,
(3) $\Gamma \vdash \exists! x_{r+1} \ldots \exists! x_{r+s} \psi(n_1, \ldots, n_r, x_{r+1}, \ldots, x_{r+s})$,

gelten.

Die dritte Eigenschaft besagt, dass die Theorie beweisen kann, dass es sich um eine Funktion handelt. Diese Eigenschaft folgt nicht aus den beiden ersten Eigenschaften. Der Ausdruck $\exists! z\alpha$ bedeutet die eindeutige Existenz und ist eine Abkürzung für $\exists z\,(\alpha(z) \wedge \forall y\,(\alpha(y) \to y = z))$. Hierbei ersetzen wir die freie Variable von α durch z bzw. durch y.

Gelegentlich werden wir mit dem folgenden schwächeren Repräsentierungsbegriff für Relationen arbeiten.

Definition 22.3. Es sei Γ eine Menge von arithmetischen Ausdrücken. Eine Relation $T \subseteq \mathbb{N}^r$ heißt *schwach repräsentierbar* in Γ, wenn es einen L^{Ar}-Ausdruck ψ in r freien Variablen derart gibt, dass für alle r-Tupel $(n_1, \ldots, n_r) \in \mathbb{N}^r$ die Äquivalenz

$$(n_1, \ldots, n_r) \in T \text{ genau dann, wenn } \Gamma \vdash \psi(n_1, \ldots, n_r)$$

gilt.

Im widerspruchsfreien Fall folgt aus der obigen (starken) Repräsentierung für eine Relation auch die schwache Repräsentierung.

Definition 22.4. Es sei Γ eine Menge von arithmetischen Ausdrücken. Man sagt, dass Γ *Repräsentierungen erlaubt*, wenn Γ jede R-berechenbare Relation und jede R-berechenbare Funktion repräsentiert.

Korollar 22.5. *Die natürliche Arithmetik, also die Menge der in* $\mathbb{N}$ *wahren Ausdrücke* $\mathbb{N}^{\vDash}$*, erlaubt Repräsentierungen.*

Beweis. Es sei $T \subseteq \mathbb{N}^r$ eine R-entscheidbare Relation und es sei P ein Registerprogramm mit den Registern $R_0, R_1, \ldots, R_m$ das diese Relation entscheidet. Aufgrund von Lemma 21.1 gibt es einen arithmetischen Ausdruck ψ_P in $2m$ freien Variablen, der den Programmablauf arithmetisch modelliert. Es gilt also $(n_1, \ldots, n_r) \in T$ genau dann, wenn P, angesetzt auf $(n_1, \ldots, n_r)$ (strenggenommen angesetzt auf $(1, n_1, \ldots, n_r, 0, \ldots, 0)$, wenn man die vollständige Registerbelegung angibt) anhält mit der Ausgabe 0 (d.h. $(h, 0, n'_2, \ldots, n'_m)$; andernfalls wird mit der Ausgabe 1 angehalten), genau dann, wenn $\mathbb{N} \vDash \psi_P(n_1, \ldots, n_r, 0, \ldots, 0, 0, n'_2, \ldots, n'_m)$ gilt.

Wegen der Vollständigkeit von $\mathbb{N}$ bedeutet dies, dass

$$\theta_P \;=\; \exists y_2 \ldots \exists y_m \psi_P(x_1, \ldots, x_r, 0, \ldots, 0, 0, y_2, \ldots, y_m)$$

die Relation repräsentiert. Es sei

$$F\colon\ \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

eine R-berechenbare Abbildung und es sei P ein Registerprogramm, dass F berechnet. Aufgrund von Lemma 21.1 gibt es einen arithmetischen Ausdruck ψ_P in $2m$ freien Variablen, der den Programmablauf arithmetisch modelliert. D.h. für jedes $(r+s)$-Tupel $n_1, \ldots, n_{r+s}$ gilt

$$F(n_1, \ldots, n_r) \;=\; (n_{r+1}, \ldots, n_{r+s})$$

genau dann, wenn das Programm P bei jeder Eingabe anhält und angesetzt auf $(n_1, \ldots, n_r)$ (in den ersten r Registern, die Eingabe ist also $(1, n_1, \ldots, n_r, 0, \ldots, 0)$) die Ausgabe $(n_{r+1}, \ldots, n_{r+s})$ (also $(h, n_{r+1}, \ldots, n_{r+s}, \ell_{m+s+1}, \ldots, \ell_{2m})$) besitzt, genau dann, wenn

$$\mathbb{N} \vDash \psi(n_1, \ldots, n_r, 0, \ldots, 0, n_{r+1}, \ldots, n_{r+s}, \ell_{m+s+1}, \ldots, \ell_{2m})$$

gilt. Von daher ist der Ausdruck (in den freien Variablen $x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+s}$)

$$\Theta \;=\; \exists z_{m+s+1} \ldots \exists z_{2m} \Psi(x_1, \ldots, x_r, 0, \ldots, 0, x_{r+1}, \ldots, x_{r+s}, z_{m+s+1}, \ldots, z_{2m})$$

Da eine Funktion vorliegt und $\mathbb{N}^{\vDash}$ vollständig ist, gilt auch

$$\mathbb{N} \vDash \exists! x_{r+1} \ldots \exists! x_{r+s} \Theta(n_1, \ldots, n_r, x_{r+1}, \ldots, x_{r+s})\,.$$

□

Bemerkung 22.6. Man kann zeigen, dass auch die erststufige Peano-Arithmetik Repräsentierungen erlaubt. Dazu muss man zeigen, dass die in der Definition 20.3 und in Lemma 21.1 konstruierten Ausdrücke, die die Wirkungsweise von Registerprogrammen beschreiben, nicht nur in $\mathbb{N}$ gelten, sondern

aus den erststufigen Peano-Axiomen ableitbar sind. Es ist noch nicht einmal selbstverständlich, dass die Addition der natürlichen Zahlen in der Peano-Arithmetik repräsentierbar ist, obwohl dafür direkt das Additionssymbol zur Verfügung steht, siehe Aufgabe 22.18.

22.2. **Der Fixpunktsatz.**

Schon beim Halteproblem haben wir die Programmcodes durch eine natürliche Zahl effektiv repräsentiert, was uns ermöglichte, in ein Programm die eigene Programmnummer einzusetzen und so eine Selbstbezüglichkeit abzubilden, die zur Unlösbarkeit des Halteproblems führte. Ähnliches haben wir mit der Arithmetik vor, wobei die arithmetische Sprache durch die Symbole $0, 1, +, \cdot$ gegeben sei.

Den Ausdrücken der Sprache ordnen wir eine natürliche Zahl, ihre sogenannte *Gödelnummer* zu. Die Gödelnummer eines Ausdrucks α bezeichnen wir mit $GN(\alpha)$. Wichtig ist dabei nicht die konkrete Gestalt, sondern allein ihre Effektivität in dem Sinne, dass diese Zuordnung durch eine Registermaschine ausführbar sein muss. Bei einem endlichen Alphabet ist die einfachste Möglichkeit, die Symbole mit Ziffern durchzunummerieren und die Ausdrücke durch die Hintereinanderschreibung der Ziffern in einem hinreichend großen Ziffernsystem zu realisieren. Da wir die Anzahl der Variablen nicht beschränken wollen, ist dies nicht direkt durchführbar. Im Falle von Programmen konnten wir die Register, deren Anzahl ebenfalls nicht beschränkt war, durch $R\prime\prime\ldots\prime$ benennen. Es ist auch möglich, in einem Zwischenschritt die Variablen $x_1, x_2, x_3 \ldots$ mit $x, x\prime, x\prime\prime, \ldots$ zu benennen und so ein endliches Alphabet zu erhalten. Eine andere Möglichkeit besteht darin, abzählbar unendlich viele Symbole mit den natürlichen Zahlen durchzunummerieren und einen Ausdruck der Form $s_{i_1} s_{i_2} \ldots s_{i_n}$ (i_j sei die Nummer des j-ten Symbols im Ausdruck) durch das Produkt $p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}$ wiederzugeben, wobei die $p_1, p_2, p_3, \ldots$ die Folge der Primzahlen sei.

Beispiel 22.7. Zu einer Ausdrucksmenge Γ kann man die Menge

$$\{GN(\alpha) |\, \Gamma \vdash \alpha\}$$

betrachten, also die Menge der Gödelnummern von Ausdrücken, die aus Γ ableitbar sind. Dies ist eine Teilmenge der natürlichen Zahlen, daher kann man auf diese Menge den Begriff der Repräsentierbarkeit anwenden. Eine natürliche Frage ist, ob diese Menge in Γ selbst repräsentierbar ist und welche Konsequenzen das hat.

Wir legen im Folgenden eine algorithmische Gödelisierung zu Grunde. Der folgende Satz heißt Gödelscher Fixpunktsatz.

Satz 22.8. *Es sei $\Gamma \subseteq L^{\mathrm{Ar}}$ eine Menge von arithmetischen Ausdrücken, die Repräsentierungen erlaube. Dann gibt es zu jedem $\alpha \in L_1^{\mathrm{Ar}}$ einen Satz $q \in L_0^{\mathrm{Ar}}$ mit*

$$\Gamma \vdash q \longleftrightarrow \alpha(GN(q)) \,.$$

Beweis. Wir betrachten die Abbildung

$$F\colon\ \mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N},\ (m,n)\longmapsto F(m,n),$$

die durch

$$F(m,n)\ :=\ \begin{cases} GN(\alpha(n)), & \text{falls } m \text{ die } GN \text{ eines } \alpha\in L_1^{\mathrm{Ar}} \text{ ist}\,,\\ 0 \text{ sonst}\,, \end{cases}$$

festgelegt ist. Bei der Berechnung von F wird also zuerst geschaut, ob das erste Argument, also m, die Gödelnummer eines arithmetischen Ausdrucks mit genau einer freien Variablen ist. Falls nicht, so ist $F(m,n)\ =\ 0$, unabhängig von n. Falls ja, so ist also $m\ =\ GN(\alpha)$ mit $\alpha\in L_1^{\mathrm{Ar}}$. In diesem Ausdruck wird dann die einzige freie Variable durch das zweite Argument der Abbildung, also n, ersetzt, wobei man einen Satz $\alpha(n)$ erhält. Dessen Gödelnummer ist nach Definition der Wert der Abbildung $F(m,n)$. In diesem Fall ist also $F(m,n)\ =\ GN(\alpha(n))$. Diese Erläuterungen zeigen zugleich, dass F berechenbar ist.Da Γ nach Voraussetzung Repräsentierungen erlaubt, gibt es einen Ausdruck $\varphi(x,y,z)$ mit drei freien Variablen, der diese Abbildung repräsentiert. D.h. es gilt für jede Belegung der Variablen mit natürlichen Zahlen m,n,k die Beziehungen (wir können annehmen, dass Γ widerspruchsfrei ist, da andernfalls das Resultat trivial ist)

$$F(m,n)=k \text{ genau dann, wenn } \Gamma\vdash\varphi(m,n,k)\,,$$

$$F(m,n)\neq k \text{ genau dann, wenn } \Gamma\vdash\neg\varphi(m,n,k)$$

und (für jede Belegung m,n für x und y)

$$\Gamma\vdash\exists!z\varphi(m,n,z)\,.$$

Den Fixpunkt zu einem vorgegebenen $\alpha\in L_1^{\mathrm{Ar}}$ erhalten wir nun durch eine trickreiche Anwendung von φ. Wir setzen

$$s\ :=\ \forall z\,(\varphi(x,x,z)\to\alpha(z))\,.$$

Der Ausdruck s besitzt die Gödelnummer $GN(s)$. Wir behaupten nun, dass der Satz

$$q\ :=\ s\frac{GN(s)}{x}\ =\forall z(\varphi(GN(s),GN(s),z)\to\alpha(z))$$

die zu beweisende Ableitungsbeziehung $\Gamma\vdash q\leftrightarrow\alpha(GN(q))$ erfüllt. Der Ausdruck s besitzt die einzige freie Variable x, daher gilt

$$F(GN(s),GN(s))\ =\ GN\left(s\frac{GN(s)}{x}\right)\ =\ GN(q).$$

Aufgrund der Repräsentierungseigenschaft ist daher

$$\Gamma\vdash\varphi(GN(s),GN(s),GN(q))\,.$$

Aus der Allaussage q erhält man durch Spezialisierung (man ersetzt die Variable z durch den Term $GN(q)$)

$$\vdash q\to(\varphi(GN(s),GN(s),GN(q))\to\alpha(GN(q)))\,.$$

Da das Antezedens der rechten Implikation aus Γ ableitbar ist, folgt

$$\Gamma \vdash q \to \alpha(GN(q)) .$$

Dies besagt also die Ableitbarkeit der Hinrichtung. Die aufgrund der Repräsentierbarkeit oben angeführte eindeutige Existenzaussage führt zu

$$\Gamma \vdash \forall z \, (\varphi(GN(s), GN(s), z) \to (z = GN(q))) \ .$$

Durch Substitution ergibt sich

$$\vdash (z = GN(q)) \to (\alpha(GN(q)) \to \alpha(z))$$

und somit nach einer prädikatenlogischen Umformulierung

$$\Gamma \vdash \forall z \, (\varphi(GN(s), GN(s), z) \wedge \alpha(GN(q)) \to \alpha(z)) \ .$$

Da hierbei $\alpha(GN(q))$ keine freie Variablen besitzt, ist auch

$$\Gamma \vdash \alpha(GN(q)) \to (\forall z(\varphi(GN(s), GN(s), z) \to \alpha(z))) \ ,$$

und das Sukzedens ist gerade q, so dass auch die Rückrichtung ableitbar ist. □

22. Arbeitsblatt

22.1. **Übungsaufgaben.**

Aufgabe 22.1. Zeige, dass für $\Gamma = \mathbb{N}^{\models}$ die beiden Repräsentierungskonzepte zusammenfallen.

Aufgabe 22.2. Es sei

$$T = \mathbb{N}2 \subseteq \mathbb{N}$$

die Menge der geraden natürlichen Zahlen. Es sei Γ die Ausdrucksmenge, die besagt, dass $+$ eine assoziative, kommutative Verknüpfung mit 0 als neutralem Element ist. Es sei

$$\psi = \exists y(x = y + y).$$

Zeige, dass T durch ψ in Γ schwach repräsentiert wird, aber nicht stark.

Aufgabe 22.3. Es sei

$$T = \mathbb{N}2 \subseteq \mathbb{N}$$

die Menge der geraden natürlichen Zahlen. Es sei Γ die Ausdrucksmenge, die besagt, dass $+$ eine assoziative, kommutative Verknüpfung mit 0 als neutralem Element ist. Es sei

$$\varphi = \exists y(x = y + y) \to \forall z \neg (x + 1 = z + z)$$

und

$$\Delta = \Gamma \cup \{\varphi\}.$$

Es sei

$$\psi \;=\; \exists y(x = y + y).$$

Zeige, dass T durch ψ in Δ repräsentiert wird.

Aufgabe 22.4. Zeige, dass eine widersprüchliche Ausdrucksmenge $\Gamma \subseteq L^{\mathrm{Ar}}$ Repräsentierungen erlaubt.

Aufgabe 22.5. Es sei $\Gamma \subseteq L^{\mathrm{ar}}$ eine Ausdrucksmenge, die Repräsentierungen erlaube. Zeige, dass jede größere Ausdrucksmenge $\Gamma' \supseteq \Gamma$ ebenfalls Repräsentierungen erlaubt.

Aufgabe 22.6. Zeige, dass die Gleichheit von natürlichen Zahlen (also die Diagonalrelation in $\mathbb{N}^2$) durch den Ausdruck $x = y$ in der erststufigen Peano-Arithmetik repräsentierbar ist.

Aufgabe 22.7. Es sei $\Gamma \subseteq L^{\mathrm{Ar}}$ das Axiomensystem eines kommutativen Halbringes. Zeige, dass die Gleichheit von natürlichen Zahlen (also die Diagonalrelation in $\mathbb{N}^2$) durch den Ausdruck $x = y$ in Γ nicht repräsentiert wird.

Aufgabe 22.8. Es sei $\Gamma \subseteq L^{\mathrm{Ar}}$ das Axiomensystem eines kommutativen Halbringes. Zeige, dass Γ keine Repräsentierungen erlaubt.

Insbesondere erlauben die erststufigen Peano-Axiome ohne das Induktionsschema keine Repräsentierungen.

Aufgabe 22.9. Sei $k \in \mathbb{N}$ und sei

$$\alpha \;:=\; \exists y(y + \cdots + y = x),$$

wobei k-mal der Summand y vorkommt. Zeige, dass $\mathbb{N}k \subseteq \mathbb{N}$, also die Menge der Vielfachen von k, in der erststufigen Peano-Arithmetik durch α repräsentiert wird.

Aufgabe 22.10. Zeige, dass die Menge der Quadratzahlen in der erststufigen Peano-Arithmetik repräsentiert werden kann.

Aufgabe 22.11. Es sei $\Gamma \subseteq L^{\mathrm{ar}}$ eine widerspruchsfreie und R-entscheidbare Ausdrucksmenge.

a) Zeige, dass jede in Γ repräsentierbare Relation $R \subseteq \mathbb{N}^r$ R-entscheidbar ist.

b) Zeige, dass jede in Γ repräsentierbare Abbildung

$$\varphi\colon\ \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

R-berechenbar ist.

Aufgabe 22.12.*

Es sei $\Gamma \subseteq L^{\mathrm{Ar}}$ eine arithmetische Ausdrucksmenge ohne freie Variablen und $R \subseteq \mathbb{N}$ eine Relation. Es seien $\alpha, \beta \in L^{\mathrm{Ar}}$ Ausdrücke in einer freien Variablen x. Zeige, dass aus

$$\Gamma \vdash \alpha \leftrightarrow \beta$$

folgt, dass α in Γ die Relation R genau dann repräsentiert, wenn β in Γ die Relation R repräsentiert.

Aufgabe 22.13.*

Es sei $\Gamma \subseteq L^{\mathrm{Ar}}$ eine arithmetische Ausdrucksmenge und $R \subseteq \mathbb{N}$ eine Relation. Es seien $\alpha, \beta \in L^{\mathrm{Ar}}$ Ausdrücke in einer freien Variablen x. Zeige, dass aus

$$\Gamma \vdash \alpha \leftrightarrow \beta$$

nicht folgt, dass α in Γ die Relation R genau dann repräsentiert, wenn β in Γ die Relation R repräsentiert.

Aufgabe 22.14. Es sei $s_1, s_2, s_3, \ldots$ eine Aufzählung einer abzählbar-unendlichen Symbolmengen. Berechne die zu Wörtern über diesem Alphabet zugehörige Zahl im Sinne der Primzahlkodierung und umgekehrt.

(1) $s_1 s_2 s_1 s_3 s_3 s_2$,
(2) $s_{13} s_{12} s_1 s_4 s_4 s_4$,
(3) $s_2 s_2 s_2 s_2 s_2 s_2$,
(4) $2^1 3^3 5^{17} 7^1$,
(5) $2^1 3^1 5^1 7^1 11^1$,
(6) $2^3 3^3 5^3 7^3 11^3$,
(7) 1728.

Aufgabe 22.15. Es sei $n \in \mathbb{N}$ eine fixierte natürliche Zahl und

$$\alpha(x) := x = n,$$

wobei n durch die n-fache Summe der 1 mit sich selbst realisiert werde. Zeige direkt, dass es Sätze $p, q \in L_0^{\mathrm{Ar}}$ mit

$$\vdash \alpha(GN(p)) \leftrightarrow p$$

und mit

$$\vdash \neg\alpha(GN(q)) \leftrightarrow q$$

gibt.

22.2. **Aufgaben zum Abgeben.**

Aufgabe 22.16. (4 Punkte)

Zeige, dass die Menge der Primzahlen in der erststufigen Peano-Arithmetik repräsentiert werden kann.

Aufgabe 22.17. (4 Punkte)

Es sei $s_1, s_2, s_3, \ldots$ eine Aufzählung einer abzählbar-unendlichen Symbolmengen. Berechne die zu Wörtern über diesem Alphabet zugehörige Zahl im Sinne der Primzahlkodierung und umgekehrt.

(1) $s_3 s_2 s_1 s_1 s_2 s_3$,
(2) $s_{20} s_{17} s_1 s_4 s_{19}$,
(3) $2^1 3^2 5^3 7^4 11^5$,
(4) $10!$.

Aufgabe 22.18. (4 Punkte)

Zeige, dass in der erststufigen Peano-Arithmetik die Addition von natürlichen Zahlen repräsentierbar ist.

Aufgabe 22.19. (6 Punkte)

Es sei

$$f\colon \mathbb{N} \longrightarrow \mathbb{N}$$

eine Polynomfunktion mit $f(n) = a_d n^d + a_{d-1} n^{d-1} + \cdots + a_1 n + a_0$ mit Koeffizienten $a_i \in \mathbb{N}$. Zeige, dass f durch den Ausdruck $y = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ in der erststufigen Peano-Arithmetik repräsentiert wird.

23. Vorlesung - Die Unvollständigkeitssätze

23.1. **Der erste Gödelsche Unvollständigkeitssatz.**

Wir haben gesehen, dass die Unentscheidbarkeit des Halteproblems über die arithmetische Repräsentierbarkeit von Registerprogrammen zur Unentscheidbarkeit der Arithmetik führt. Beim Beweis des ersten Gödelschen Unvollständigkeitssatzes arbeitet man mit einem Fixpunkt zu einem negierten Ableitungsprädikat, um eine „paradoxe“ Situation zu erhalten. Ein Ableitungsprädikat (zu einer Ausdrucksmenge Γ) $a(x)$ in einer freien Variablen soll die Eigenschaft haben, dass für jeden Satz $s \in L_0^{\mathrm{Ar}}$ die Ableitungsbeziehung $\Gamma \vdash s$ genau dann gilt, wenn $\Gamma \vdash a(GN(s))$ gilt. Man sagt, dass $a(x)$ die Ableitungseigenschaft *schwach repräsentiert*. Ein solches Ableitungsprädikat muss es im Allgemeinen nicht geben. Anders formuliert bedeutet diese Eigenschaft, dass die einstellige Relation

$$\{n \in \mathbb{N} |\, n \text{ ist Gödelnummer eines aus } \Gamma \text{ ableitbaren Satzes}\} \subseteq \mathbb{N}$$

in Γ schwach repräsentiert wird. Dass diese Teilmenge (stark) repräsentierbar ist, ist, wenn man die Widerspruchsfreiheit von Γ voraussetzt, stärker. Aus $\Gamma \vdash s$ ergibt sich nämlich direkt die Hinrichtung $\Gamma \vdash a(GN(s))$, und wenn $\Gamma \vdash s$ nicht wahr ist, so bedeutet dies im Falle der Repräsentierbarkeit, dass $\Gamma \vdash \neg a(GN(s))$ gilt, woraus bei widerspruchsfreiem Γ die Nichtableitbarkeit von $a(GN(s))$ folgt.

Im folgenden *Unvollständigkeitslemma* gehört die Existenz eines (schwach) repräsentierenden Ableitungsprädikates zur Voraussetzung.

Lemma 23.1. *Es sei Γ eine widerspruchsfreie, arithmetische Ausdrucksmenge, die Repräsentierungen erlaube. Die Ableitungsmenge $\Gamma^{\vdash}$ (also die Menge der zugehörigen Gödelnummern) sei schwach repräsentierbar in Γ. Dann gibt es einen arithmetischen Satz $q \in L_0^{\mathrm{Ar}}$ derart, dass weder q noch seine Negation $\neg q$ aus Γ ableitbar ist. Die Ableitungsmenge $\Gamma^{\vdash}$ ist also nicht vollständig.*

Beweis. Aus der Repräsentierbarkeit von $\Gamma^{\vdash}$ folgt, dass es einen arithmetischen Ausdruck in einer freien Variablen gibt, sagen wir $a(x)$, mit der Eigenschaft, dass

$$\Gamma \vdash s$$

genau dann gilt, wenn

$$\Gamma \vdash a(GN(s))$$

gilt. Wir betrachten die Negation $\beta = \neg a$. Nach Satz 22.8 gibt es für β einen Fixpunkt, also einen Satz q mit

$$\Gamma \vdash q \longleftrightarrow \beta(GN(q))$$

bzw.

$$\Gamma \vdash q \longleftrightarrow \neg a(GN(q))\,.$$

Sowohl aus $\Gamma \vdash q$ als auch aus $\Gamma \vdash \neg q$ ergibt sich dann direkt ein ableitbarer Widerspruch, was der Widerspruchsfreiheit des Systems widerspricht. $\square$

Man beachte, dass die Repräsentierbarkeit der Ableitungsmenge hier eine explizite Voraussetzung ist, die nicht aus der allgemein vorausgesetzten Eigenschaft, Repräsentierungen zu erlauben, folgt. Letztere bezieht sich nur auf rekursive (entscheidbare) Relationen und Funktionen, es wird aber nicht vorausgesetzt, dass Γ selbst oder $\Gamma^{\vdash}$ rekursiv ist.

Bemerkung 23.2. Was passiert mit den Voraussetzungen in Lemma 23.1, wenn man den Satz q (oder seine Negation) einfach zu Γ hinzunimmt? Zunächst führt die Hinzunahme von q noch von $\neg q$ zu einem widersprüchlichen System. Im Beweis haben wir die Annahme $\Gamma \vdash q$ (bzw. $\Gamma \vdash \neg q$) zu einem Widerspruch geführt, das bedeutet aber nicht $\Gamma' = \Gamma \cup \{q\} \vdash p \wedge \neg p$. Ein Problem ist hierbei, dass die neue Ableitungsmenge $(\Gamma \cup \{q\})^{\vdash}$ nicht mehr repräsentierbar in $\Gamma \cup \{q\}$ sein muss. Vor allem aber ist sie keinesfalls mit dem alten Ableitungsausdruck $a(x)$ repräsentierbar, sondern, wenn überhaupt, mit einem neuen $a'(x)$. Für dieses gibt es dann wieder einen neuen Fixpunkt q'. Es gibt keine rekursive Strategie, Γ zu einer vollständigen Theorie aufzufüllen.

Kurt Gödel (1906-1978) bewies im Alter von 24 Jahren seine Unvollständigkeitssätze.

Die folgende Aussage heißt *erster Gödelscher Unvollständigkeitssatz.*

Satz 23.3. *Es sei $\Gamma \subseteq L^{\mathrm{Ar}}$ eine arithmetische Ausdrucksmenge, die widerspruchsfrei und aufzählbar sei und Repräsentierungen erlaube. Dann ist $\Gamma^{\vdash}$ unvollständig. Es gibt also einen arithmetischen Satz, für den weder $\Gamma \vdash q$ noch $\Gamma \vdash \neg q$ gilt.*

Beweis. Wir nehmen an, dass $\Gamma^{\vdash}$ vollständig ist. Da Γ aufzählbar ist, ist $\Gamma^{\vdash}$ nach Lemma 21.9 aufzählbar und nach Satz 21.10 auch entscheidbar. Da Γ Repräsentierungen erlaubt, ist insbesondere $\Gamma^{\vdash}$ repräsentierbar. Daher sind

die Voraussetzungen von Lemma 23.1 erfüllt und es ergibt sich ein Widerspruch zur angenommenen Vollständigkeit. □

Korollar 23.4. *Es sei* $\Gamma \subseteq L^{\mathrm{Ar}}$ *eine arithmetische korrekte Ausdrucksmenge, die aufzählbar sei und Repräsentierungen erlaube. Dann gibt es einen in (der Standardinterpretation)* $\mathbb{N}$ *wahren Satz, der nicht zu* $\Gamma^{\vdash}$ *gehört, der also nicht aus* Γ *formal ableitbar ist.*

Beweis. Die Korrektheit bedeutet, dass $\Gamma^{\vdash} \subseteq \mathbb{N}^{\models}$ gilt. Dies sichert zugleich die Widerspruchsfreiheit von Γ. Gemäß Satz 23.3 gibt es einen Satz q, der weder selbst noch seine Negation $\neg q$ aus Γ ableitbar ist. Da aber $\mathbb{N}^{\models}$ vollständig ist, muss entweder q oder $\neg q$ in $\mathbb{N}$ wahr sein. □

Diese Aussage ist für die erststufige Peano-Arithmetik und jedes größere aufzählbare widerspruchsfreie System anwendbar, wobei wir aber die Eigenschaft der Peano-Arithmetik, Repräsentierungen zu erlauben, nicht bewiesen haben.

23.2. **Der zweite Gödelsche Unvollständigkeitssatz.**

Wenn die Ableitungsrelation $\Gamma^{\vdash}$ repräsentierbar ist und der zugehörige repräsentierende arithmetische Ausdruck a bekannt ist, so ist auch der im Beweis zu Lemma 23.1 verwendete Ausdruck q, (also der Fixpunkt zu $\neg a(x)$) prinzipiell bekannt, da der Fixpunktsatz konstruktiv ist. Im Beweis des ersten Gödelschen Unvollständigkeitssatz war ein solches Ableitungsprädikat a aber nur aufgrund der angenommenen Vollständigkeit vorhanden, die dann zum Widerspruch geführt wurde. Aus diesen Überlegungen ergibt sich weder die Existenz eines Ableitungsprädikates noch die eines Fixpunktes zum negierten Ableitungsprädikat.

Der zweite Gödelsche Unvollständigkeitssatz gibt hingegen explizit einen Satz an, der weder selbst noch seine Negation beweisbar ist, und zwar einen Satz von großer inhaltlicher Bedeutung: Es geht um den Satz, der die Widerspruchsfreiheit des gegebenen Systems behauptet.

Betrachten wir zunächst eine beliebige korrekte arithmetische Theorie $T \subseteq L_0^{\mathrm{Ar}}$, also eine deduktiv abgeschlossene Satzmenge, die bei der Standardinterpretation in $\mathbb{N}$ nur wahre Sätze ergibt (dazu genügt es wegen der Korrektheit des Ableitungskalküls, dass sämtliche Sätze aus einem Axiomensystem Γ für T (also $T = \Gamma^{\vdash}$) in $\mathbb{N}$ wahr sind). Da $\mathbb{N}^{\models}$, wie jede Gültigkeitsmenge eines Modells, vollständig und widerspruchsfrei ist, ist auch T (als Teilmenge von $\mathbb{N}^{\models}$) widerspruchsfrei. Daher gehört zu T kein Satz der Form $p \wedge \neg p$ und auch nicht der Satz $\neg(0 = 0)$ (da ja die Identität $0 = 0$ dazugehört). Eine andere Frage ist es, ob das System bzw. die Theorie oder das Axiomensystem diese Unableitbarkeit eines widersprüchlichen Satzes auch „weiß“.

Schon im Unvollständigkeitslemma und im ersten Gödelschen Unvollständigkeitssatz kam wesentlich ein Ableitungsprädikat a vor. Dieses hatte die Eigenschaft

$$\Gamma \vdash s \text{ genau dann, wenn } \Gamma \vdash a(GN(s)) \,,$$

allerdings unter der Bedingung, dass $\Gamma^{\vdash}$ entscheidbar und damit in Γ (das Repräsentierungen erlaube) repräsentierbar ist. Aus der Entscheidbarkeit von Γ folgt zwar die Aufzählbarkeit von $\Gamma^{\vdash}$, und daraus, wenn $\Gamma^{\vdash}$ zusätzlich vollständig ist, auch die Entscheidbarkeit von $\Gamma^{\vdash}$, sonst aber nicht. Diese Überlegung haben wir schon in umgekehrter Richtung angewendet, indem wir aus der Unentscheidbarkeit der Arithmetik auf die Unvollständigkeit der Peano-Arithmetik geschlossen haben (siehe Korollar 21.13). Es ist also keineswegs selbstverständlich, dass es ein sinnvolles entscheidbares Ableitungsprädikat gibt.

Allerdings ist ein schwächeres Ableitungsprädikat entscheidbar und damit repräsentierbar, nämlich die folgende zweistellige Ableitungsrelation. Dazu sei die Gödelisierung auf endliche Folgen von Ausdrücken (die mögliche Ableitungsketten repräsentieren mögen) ausgedehnt. Wir betrachten dann das zweistellige Prädikat $A \subseteq \mathbb{N} \times \mathbb{N}$ (eigentlich $A_\Gamma(x, y)$, da diese Teilmenge von Γ abhängt), mit der Eigenschaft, dass $(m, n) \in A$ genau dann gilt, wenn m die Gödelnummer einer korrekten Ableitung im Prädikatenkalkül aus Γ ist, deren letzter Ausdruck (also der in der Ableitung bewiesene Ausdruck) die Gödelnummer n besitzt. Diese Relation ist unter der Voraussetzung, dass Γ entscheidbar ist, selbst entscheidbar. Man kann ja zum ersten Eintrag m die Ableitung rekonstruieren, ihre Korrektheit im Prädikatenkalkül überprüfen und aufgrund der Entscheidbarkeit von Γ feststellen, ob nur Ausdrücke aus Γ als Voraussetzungen verwendet wurden. Wenn Γ Repräsentierungen erlaubt, so gibt es einen arithmetischen Ausdruck mit zwei freien Variablen, sagen wir $\delta(x, y)$ (eigentlich $\delta_\Gamma(x, y)$, da dieser Ausdruck von Γ abhängt), der für jede Belegung $(m, n) \in \mathbb{N}^2$ genau dann aus Γ ableitbar ist, wenn (m, n) zu A gehört, wenn also m einen Beweis aus Γ für die Aussage zu n kodiert.

Wie formuliert man die Eigenschaft, dass es einen prädikatenlogischen Beweis aus Γ für die Aussage zu n gibt? Dies ist äquivalent dazu, dass es ein $m \in \mathbb{N}$ gibt, das einen Beweis dafür kodiert, dass es also ein $m \in \mathbb{N}$ mit $(m, n) \in A$ gibt, was aufgrund der Repräsentierbarkeit wiederum zu $\Gamma \vdash \delta(m, n)$ äquivalent ist. Dies impliziert $\Gamma \vdash \exists x \delta(x, n)$. Hierbei gilt sogar die Umkehrung, da $\Gamma \vdash \exists x \delta(x, n)$ die Gültigkeit $\mathbb{N} \vDash \exists x \delta(x, n)$ bedeutet, was die Existenz einer natürlichen Zahl m mit $\mathbb{N} \vDash \delta(m, n)$ bedeutet. Wäre $(m, n) \notin A$, so würde sich über die starke Repräsentierbarkeit $\Gamma \vdash \neg\delta(m, n)$ ergeben und damit der Widerspruch $\mathbb{N} \vDash \neg\delta(m, n)$.

Wie formuliert man die Eigenschaft, dass es keinen prädikatenlogischen Beweis aus Γ für die Aussage zu n gibt? Innerhalb der natürlichen Zahlen ist dies äquivalent dazu, dass für alle $m \in \mathbb{N}$ die Beziehung $A(m, n)$ *nicht* gilt,

was wiederum zu

$$\mathbb{N} \vDash \forall x \neg \delta(x, n)$$

äquivalent ist. Dies muss aber *nicht* zu $\Gamma \vdash \forall x \neg \delta(x, n)$ äquivalent sein.

Definition 23.5. Es sei Γ eine korrekte aufzählbare arithmetische Ausdrucksmenge, die Repräsentierungen erlaube. Es sei $\delta_\Gamma(x, y)$ der L^{Ar}-Ausdruck, der in Γ die zweistellige Ableitungsrelation $A \subseteq \mathbb{N}^2$ repräsentiert. Dann setzt man

$$\alpha(y) \; = \; \exists x(\delta_\Gamma(x, y))$$

und nennt dies das (einstellige) *Ableitungsprädikat.*

Lemma 23.6. *Es sei Γ eine korrekte aufzählbare arithmetische Ausdrucksmenge, die Repräsentierungen erlaube, es sei $\alpha(x)$ das zugehörige (einstellige) Ableitungsprädikat und es sei q ein Fixpunkt zum negierten Ableitungsprädikat, also*

$$\Gamma \vdash q \leftrightarrow \neg \alpha(GN(q)) \, .$$

Dann ist q aus Γ nicht ableitbar.

Beweis. Wir nehmen $\Gamma \vdash q$ an. Dies bedeutet, dass es eine korrekte Ableitung von q aus Γ gibt. Diese Ableitung wird durch eine Zahl m kodiert und somit ist $(m, GN(q)) \in A$. Daher gilt

$$\Gamma \vdash \delta(m, GN(q)) \, ,$$

da ja δ das zweistellige Ableitungsprädikat repräsentiert. Aufgrund der Existenzeinführung im Sukzedens ist auch

$$\Gamma \vdash \exists x \delta(x, GN(q)) \, ,$$

also $\Gamma \vdash \alpha(GN(q))$. Die Kontraposition der Fixpunkteigenschaft ergibt somit

$$\Gamma \vdash \neg q \, ,$$

so dass ein Widerspruch vorliegt. □

Bemerkung 23.7. Das Beweisprädikat $\alpha(y)$ besitzt, wenn Γ die Peano-Arithmetik umfasst, einige ausdruckstarke Eigenschaften, die auch in Γ ableitbar sind. Der Beweis von diesen Eigenschaften ist aufwändig, da sie nicht abstrakt aus der Repräsentierbarkeit folgen, sondern im Beweiskalkül erarbeitet werden müssen. Wichtige Eigenschaften sind (Γ sei entscheidbar und enthalte die Peano-Arithmetik).

- Wenn $\Gamma \vdash s$, so ist $\Gamma \vdash \alpha(GN(s))$ für jeden Ausdruck $s \in L^{\mathrm{Ar}}$.
- Für je zwei Ausdrücke $s, t \in L^{\mathrm{Ar}}$ ist $\Gamma \vdash \alpha(GN(s \to t)) \to (\alpha(GN(s)) \to \alpha(GN(t)))$.
- Für jeden Ausdruck $s \in L^{\mathrm{Ar}}$ ist $\Gamma \vdash \alpha(GN(s)) \to \alpha(GN(\alpha(GN(s))))$.

Diese und ähnliche Gesetzmäßigkeiten sind der Ausgangspunkt der *Beweisbarkeitslogik*, die in der Sprache der Modallogik beweistheoretische Fragestellungen untersucht.

Die aufgelisteten Eigenschaften sind für ein Ableitungsprädikat natürlich wünschenswert; der naive Wunsch $\vdash s \leftrightarrow \alpha(GN(s))$ ist nicht realisierbar, da er in Verbindung mit dem Satz q von oben (der Fixpunkt zur Negation $\neg\alpha(GN(s))$) sofort einen internen Widerspruch ergibt. Die Verbindung der „positiven“ Eigenschaften des Ableitungsprädikates mit dem „paradoxen“ q aus dem Fixpunktsatz liefert einen Beweis für den zweiten Unvollständigkeitssatz. Dazu braucht man nicht die volle Liste von oben, sondern es genügt zu wissen, dass die in Lemma 23.6 auf Grundlage der Widerspruchsfreiheit von Γ gezeigte Unableitbarkeit von q aus Γ sich in der Peano-Arithmetik selbst nachvollziehen lässt. D.h. es gilt

$$PA \vdash WF(\Gamma) \longrightarrow \neg\alpha(GN(q))$$

Dabei realisieren wir die Widerspruchsfreiheit $WF(\Gamma)$ intern durch die Unableitbarkeit des weiter oben schon erwähnten widersprüchlichen Satzes $r = \neg(0 = 0)$, also durch

$$WF(\Gamma) \;=\; \neg\alpha(GN(r)) \;=\; \forall x \neg\delta(x, GN(r)).$$

Die soeben erwähnte Aussage, dass die Widerspruchsfreiheit die Nichtableitbarkeit von q impliziert, kann man auch aus den in Bemerkung 23.7 angeführten Eigenschaften des Ableitungsprädikats erhalten, siehe Aufgabe 23.17.

Die folgende Aussage heißt *Zweiter Gödelscher Unvollständigkeitssatz*.

Satz 23.8. *Es sei Γ eine arithmetische Ausdrucksmenge, die widerspruchsfrei und entscheidbar sei*[29] *und die Peano-Arithmetik umfasse. Dann ist die Widerspruchsfreiheit $WF(\Gamma)$ nicht aus Γ ableitbar, d.h. es ist*

$$\Gamma \nvdash WF(\Gamma)\,.$$

Beweis. Es sei q ein Fixpunkt zum negierten Ableitungsprädikat. Aus der Annahme $\Gamma \vdash WF(\Gamma)$ folgt wegen

$$PA \vdash WF(\Gamma) \longrightarrow \neg\alpha(GN(q))$$

(was wir allerdings nicht bewiesen haben) direkt

$$\Gamma \vdash \neg\alpha(GN(q))\,.$$

Aus der Fixpunkteigenschaft von q folgt somit $\Gamma \vdash q$, was aber in dem widerspruchsfreien System Γ nach Lemma 23.6 nicht sein kann. □

[29] D.h. Γ ist entscheidbar, die Ableitungsmenge $\Gamma^{\vdash}$ muss nicht entscheidbar sein.

23. Arbeitsblatt

23.1. Übungsaufgaben.

Aufgabe 23.1. Epimenides der Kreter sagte: „Alle Kreter sind Lügner“. Ist diese Aussage ein Widerspruch?

Aufgabe 23.2. Eine Person sagt: „Ich lüge (jetzt)“. Kann das wahr sein?

Aufgabe 23.3. In der *Russellsche Antinomie* wird die Definition

$$M = \{N | \, N \text{ ist eine Menge, die sich nicht selbst enthält}\}$$

betrachtet. Kann M eine Menge sein?

Aufgabe 23.4. Betrachte die Aussage: „Der Barbier von Sevilla rasiert alle Männer, die sich nicht selbst rasieren“. Rasiert er sich selbst?

Aufgabe 23.5.*

Es sei M eine beliebige Menge. Zeige, dass es keine surjektive Abbildung von M in die Potenzmenge $\mathfrak{P}(M)$ geben kann.

Aufgabe 23.6. Die Klasse 8c hat an jedem Wochentag eine Stunde mathematische Logik. Der Lehrer sagt am Freitag: „nächste Woche werden wir eine Klassenarbeit schreiben, und das wird eine Überraschung sein“. Begründe, dass der Lehrer lügt.

Aufgabe 23.7. Das Brennersche Putzparadoxon besagt: „Immer wenn ich putze, sieht es danach so aus, wie bei einer durchschnittlichen Hausfrau vor dem Putzen“. Ist dies ein Widerspruch, eine Antinomie, ein Paradoxon, oder einfach nur mangelndes Talent?

Aufgabe 23.8. Eine natürliche Zahl heißt *besonders*, wenn sie eine für sie spezifische, benennbare Eigenschaft erfüllt. Die 0 ist als neutrales Element der Addition und die 1 ist als neutrales Element der Multiplikation besonders. Die 2 ist die erste Primzahl, die 3 ist die kleinste ungerade Primzahl, die 4 ist die erste echte Quadratzahl, die 5 ist die Anzahl der Finger einer Hand, die 6 ist die kleinste aus verschiedenen Faktoren zusammengesetzte Zahl, die 7 ist die Anzahl der Zwerge im Märchen, u.s.w., diese Zahlen sind also alle besonders. Gibt es eine Zahl, die nicht besonders ist?

Aufgabe 23.9. Es sei Γ eine korrekte entscheidbare arithmetische Ausdrucksmenge, die die Peano-Arithmetik umfasse. Es sei $\alpha(x)$ das zugehörige Ableitungsprädikat. Zeige aus den in Bemerkung 23.7 aufgeführten Eigenschaften für einen Fixpunkt q mit

$$\Gamma \vdash \neg\alpha(GN(q)) \leftrightarrow q\,,$$

dass weder $\Gamma \vdash q$ noch $\Gamma \vdash \neg q$ gilt.

Aufgabe 23.10. Es sei Γ eine korrekte entscheidbare arithmetische Ausdrucksmenge, die die Peano-Arithmetik umfasse. Es sei $\alpha(x)$ das zugehörige Beweisbarkeitsprädikat und es sei q ein Fixpunkt zum negierten Ableitungsprädikat, also

$$\Gamma \vdash \neg\alpha(GN(q)) \leftrightarrow q\,.$$

(1) Welche Eigenschaften aus Bemerkung 23.7 gelten in $\mathbb{N}$?
(2) Gilt
$$\neg\alpha(GN(q)) \leftrightarrow q$$
in $\mathbb{N}$?
(3) Welche der Ausdrücke $q, \neg q, \alpha(GN(q)), \neg\alpha(GN(q))$ gelten in $\mathbb{N}$?

Aufgabe 23.11. Es sei Γ eine arithmetische Ausdrucksmenge und α ein einstelliges Prädikat mit

$$\Gamma \vdash \alpha(n)$$

für alle $n \in \mathbb{N}$. Zeige, dass es einen Satz q mit

$$\Gamma \vdash \alpha(GN(q)) \leftrightarrow q$$

gibt.

Aufgabe 23.12. Es sei Γ eine arithmetische Ausdrucksmenge und α ein einstelliges Prädikat mit

$$\Gamma \vdash \neg\alpha(n)$$

für alle $n \in \mathbb{N}$. Zeige, dass es einen Satz q mit

$$\Gamma \vdash \alpha(GN(q)) \leftrightarrow q$$

gibt.

Aufgabe 23.13. Wir setzen

$$\alpha(x) \;:=\; \exists y\,(x = y + y)$$

und es sei die Gödelisierung mit Primzahlen vorausgesetzt. Zeige (ohne den Fixpunktsatz zu verwenden), dass es einen Satz $q \in L_0^{\mathrm{Ar}}$ mit

$$PA \vdash \alpha(GN(q)) \leftrightarrow q$$

gibt.

Aufgabe 23.14. Es sei k eine fixierte positive natürliche Zahl und es sei

$$\alpha(x) := \exists y\,(x = ky)\,,$$

wobei ky als die k-fache Addition von y mit sich selbst realisiert werde. Es sei die Gödelisierung mit Primzahlen vorausgesetzt. Zeige (ohne den Fixpunktsatz zu verwenden), dass es einen Satz $q \in L_0^{\mathrm{Ar}}$ mit

$$PA \vdash \alpha(GN(q)) \leftrightarrow q$$

gibt.

23.2. **Aufgaben zum Abgeben.**

Aufgabe 23.15. (4 Punkte)

Es seien $n_1, \ldots, n_r$ natürliche Zahlen und sei

$$\alpha(x) := (x = n_1) \wedge \ldots \wedge (x = n_r)\,,$$

wobei n_j durch die n_j-fache Summe der 1 mit sich selbst realisiert werde. Zeige, dass es Sätze $p, q \in L_0^{\mathrm{Ar}}$ mit

$$\vdash \alpha(GN(p)) \leftrightarrow p$$

und mit

$$\vdash \neg\alpha(GN(q)) \leftrightarrow q$$

gibt.

Aufgabe 23.16. (3 Punkte)

Folgere aus dem ersten Gödelschen Unvollständigkeitssatz die Unentscheidbarkeit der Arithmetik.

Aufgabe 23.17. (6 Punkte)

Es sei Γ eine korrekte entscheidbare arithmetische Ausdrucksmenge, die die Peano-Arithmetik umfasse. Es sei $\alpha(x)$ das Ableitungsprädikat zu Γ und es sei q ein Fixpunkt zum negierten Ableitungsprädikat, also

$$\Gamma \vdash \neg\alpha(GN(q)) \leftrightarrow q\,.$$

Zeige, dass aus den in Bemerkung 23.7 angeführten Eigenschaften man

$$\Gamma \vdash \neg\alpha(GN(p \wedge \neg p)) \to \neg\alpha(GN(q))$$

erhalten kann, wobei p ein beliebiger Ausdruck ist.

Aufgabe 23.18. (4 Punkte)

Es sei Γ eine korrekte entscheidbare arithmetische Ausdrucksmenge, die die Peano-Arithmetik umfasse. Es sei $\alpha(x)$ das zugehörige Beweisbarkeitsprädikat und es sei q ein Fixpunkt zum negierten Ableitungsprädikat, also

$$\Gamma \vdash \neg\alpha(GN(q)) \leftrightarrow q\,.$$

Zu einem beliebigen Ausdruck p betrachten wir $\neg\alpha(GN(p \wedge \neg p))$. Welche der Ausdrücke

$$\neg\alpha(GN(p \wedge \neg p)),\ \neg\alpha(GN(q)),\ \neg\alpha(GN(p \wedge \neg p)) \to \neg\alpha(GN(q))$$

gelten in $\mathbb{N}$?

Aufgabe 23.19. (4 (2+2) Punkte)

Es sei Γ eine arithmetische Ausdrucksmenge und α ein einstelliges Prädikat.

(1) Es gelte

$$\Gamma \vdash \alpha(n)$$

für endlich viele $n \in \mathbb{N}$ und für alle übrigen natürlichen Zahlen gelte

$$\Gamma \vdash \neg\alpha(n)\,.$$

Zeige, dass es einen Satz q mit

$$\Gamma \vdash \alpha(GN(q)) \leftrightarrow q$$

gibt.

(2) Es gelte

$$\Gamma \vdash \neg\alpha(n)$$

für endlich viele $n \in \mathbb{N}$ und für alle übrigen natürlichen Zahlen gelte

$$\Gamma \vdash \alpha(n)\,.$$

Zeige, dass es einen Satz q mit

$$\Gamma \vdash \alpha(GN(q)) \leftrightarrow q$$

gibt.

24. Vorlesung - Modallogik I

Aristoteles (384-322 v.u.Z) ist der Begründer der Modallogik. Das achte Kapitel seiner ersten Analytik leitet die modallogische Problematik ein: „Da das einfache Sein und das nothwendige Sein und das statthafte Sein verschieden sind (denn Vieles ist zwar, aber nicht aus Nothwendigkeit und Anderes ist weder aus Nothwendigkeit, noch ist es überhaupt, aber das Sein desselben ist statthaft), so erhellt, dass auch die aus diesen unterschiedenen Arten zu sein gebildeten Schlüsse von einander verschieden sein werden, und zwar auch dann, wenn die beiden Vordersätze in einem Schlüsse nicht gleichartig lauten, sondern der eine das nothwendige, der andere das einfache Sein oder das blos statthafte Sein ausdrückt.“

24.1. **Modallogik.**

Die *Modallogik* beschäftigt sich mit der Logik der Notwendigkeit und Möglichkeit und allgemeiner mit Modalitäten von Aussagen. Sie baut auf der Aussagenlogik auf. Während diese die logische Abhängigkeit von mittels aussagenlogischer Junktoren definierten Ausdrücken in den Aussagenvariablen studiert, und für eine Aussagenvariable nur die beiden Wahrheitswerte wahr oder falsch kennt, erlaubt die Modallogik, auch modalisierte Aussagenvariablen zu untersuchen. Modalisierte Aussagen kommen häufig vor, typische Beispiele sind:

(1) p gilt notwendigerweise.
(2) Es ist moralisch geboten, dass p gilt.
(3) Ich möchte, dass p gilt.
(4) Ich weiß, dass p gilt.
(5) p ist beweisbar.

(6) p gilt überall (in allen Fällen, in allen Welten).

Die Negationen dieser Aussagen sind (es ist nicht der Fall, dass ...)

(1) p gilt nicht notwendigerweise.
(2) Es ist moralisch nicht geboten, dass p gilt.
(3) Ich möchte nicht, dass p gilt (im Sinne von, es ist mir egal).
(4) Ich weiß nicht, ob p gilt.
(5) p ist nicht beweisbar.
(6) p gilt nicht überall (nicht in allen Fällen, nicht in allen Welten).

Man kann aber auch die gleiche Modalität auf die Negation zu p anwenden, das ergibt.

(1) $\neg p$ gilt notwendigerweise.
(2) Es ist moralisch geboten, dass $\neg p$ gilt (also p ist moralisch verwerflich/verboten).
(3) Ich möchte, dass $\neg p$ gilt.
(4) Ich weiß, dass $\neg p$ gilt.
(5) $\neg p$ ist beweisbar.
(6) $\neg p$ gilt überall (in allen Fällen, in allen Welten), also p gilt nirgendwo.

Diesen Aussagen können wiederum als Ganzes negiert werden.

(1) Es ist nicht der Fall, dass $\neg p$ notwendigerweise gilt.
(2) Es ist nicht moralisch geboten, dass $\neg p$ gilt.
(3) Ich möchte nicht, dass $\neg p$ gilt.
(4) Ich weiß nicht, dass $\neg p$ gilt.
(5) $\neg p$ ist nicht beweisbar.
(6) $\neg p$ gilt nicht überall (nicht in allen Fällen).

Davon sind die folgenden Aussagen Paraphrasierungen.

(1) p gilt möglicherweise.
(2) p ist (moralisch) erlaubt.
(3) Ich kann p akzeptieren.
(4) Ich kann von meinem Wissen her nicht ausschließen, dass p gilt (p ist denkbar).
(5) p ist nicht ausschließbar.
(6) Es gibt Fälle bzw. Welten, wo p gilt.

Wenn man die zu Beginn genannten Modalitäten mit $\Box p$ (Notwendigkeit) bezeichnet, so haben wir nach $\Box p$ die Varianten $\neg\Box p$, $\Box\neg p$, $\neg\Box\neg p$ aufgelistet, und die letzte Variante konnten wir durch eine neue Modalität (Möglichkeit) ausdrücken, nämlich

$$\Diamond p \Leftrightarrow \neg\Box\neg p\,.$$

Möglich bedeutet also, dass das Gegenteil nicht notwendig ist, erlaubt bedeutet, dass das Gegenteil nicht verpflichtend ist, u.s.w. Diese Äquivalenz wird

etwas weniger verschachtelt, wenn man sie als

$$\neg\Diamond p \Leftrightarrow \Box\neg p$$

schreibt. Dass etwas nicht erlaubt ist bedeutet, dass das Gegenteil davon verpflichtend ist. In der formalen Modallogik untersucht man strukturelle Gesetzmäßigkeiten von Aussagen, die durch einen Operator $\Box$ modalisiert werden können. Philosophisch relevante Interpretationen sind die Notwendigkeitslogik, die Deontik (Moral, Recht), epistemische Logik (Wissen), Beweisbarkeitslogik. In der letzten Vorlesung haben wir in Bemerkung 23.7 für das einstellige Ableitungsprädikat einige strukturelle Eigenschaft formuliert. Wenn man dabei $\alpha(GN(s))$ als „s ist beweisbar“ liest und als $\Box s$ schreibt, wobei s nicht weiter hinterfragt wird und als Aussagenvariable aufgefasst wird, so kann man diese Eigenschaften modallogisch untersuchen.

24.2. **Die formale Sprache der Modallogik.**

Definition 24.1. Zu einer Menge von Aussagenvariablen $p_i, i \in I$, besteht die *modallogische Sprache* aus diesen Aussagenvariablen, aus allen rekursivkonstruierbaren aussagenlogischen Verknüpfungen und aus allen rekursivkonstruierbaren Ausdrücken der Form $\Box(\alpha)$.

Wie im aussagelogischen Kontext arbeiten wir mit $\neg, \wedge, \rightarrow$, wobei wir auch die Symbole $\vee$ und $\leftrightarrow$ in ihrer üblichen Bedeutung als Abkürzungen verwenden. Wir verzichten auch auf Klammern, um die Lesbarkeit der Ausdrücke zu erhöhen. Ein weiteres wichtiges sekundäres Symbol ist $\Diamond$. Es wird als

$$\Diamond\alpha \leftrightarrow \neg\Box(\neg\alpha)$$

eingeführt. Wir lesen $\Box\alpha$ als „α ist notwendig“ und $\Diamond\alpha$ als „α ist möglich“.

Definition 24.2. Eine unter aussagenlogischen Ableitungen abgeschlossene Teilmenge der modallogischen Sprache heißt (formale) *Modallogik*.

24.3. **Das System K.**

Definition 24.3. Eine Modallogik heißt eine K- *Modallogik* , wenn das Axiomenschema

$$\vdash \Box(\alpha \rightarrow \beta) \rightarrow (\Box\alpha \rightarrow \Box\beta)$$

für beliebige Ausdrücke α, β und die Ableitungsregel *Nezessisierungsregel*

aus $\vdash \alpha$ folgt $\vdash \Box\alpha$

für alle α gilt.

Das Axiomenschema K ist äquivalent zum Axiomenschema

$$\Diamond\gamma \rightarrow (\Diamond\neg\alpha \vee \Diamond(\alpha \wedge \gamma)),$$

siehe Aufgabe 24.2.

Definition 24.4. Man sagt, dass ein modallogischer Ausdruck α aus dem K-System *ableitbar* ist, wenn sich α aus aussagenlogischen Tautologien und aus Instanzen des K-Axioms mit Hilfe des Modus Ponens oder der Nezessisierungsregel ergibt. Dafür schreibt man

$$\vdash \alpha\,.$$

Lemma 24.5. *In einer K-Modallogik sind folgende Aussagen ableitbar.*

(1) *Aus*

$$\vdash \alpha \to \beta$$

folgt

$$\vdash \Box\alpha \to \Box\beta\,.$$

(2) *Aus*

$$\vdash \alpha \to \beta$$

folgt

$$\vdash \Diamond\alpha \to \Diamond\beta\,.$$

(3)

$$\vdash \Box(\alpha \wedge \beta) \to \Box\alpha\,.$$

(4)

$$\vdash \Box\alpha \wedge \Box\beta \to \Box(\alpha \wedge \beta)$$

(5)

$$\vdash \Box\neg\neg\alpha \leftrightarrow \Box\alpha\,.$$

Beweis. (1). Nach der Nezessisierungsregel gilt

$$\vdash \Box(\alpha \to \beta)$$

und nach dem K-Axiom gilt

$$\vdash \Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)\ .$$

Durch Modus Ponens ergibt sich

$$\vdash \Box\alpha \to \Box\beta\,.$$

(2). Aus

$$\vdash \alpha \to \beta$$

folgt durch Kontraposition zunächst

$$\vdash \neg\beta \to \neg\alpha$$

und daraus nach Teil (1)

$$\vdash \Box\neg\beta \to \Box\neg\alpha$$

Erneutes kontraponieren ergibt

$$\vdash \neg\Box\neg\alpha \to \neg\Box\neg\beta\,,$$

was

$$\vdash \Diamond\alpha \to \Diamond\beta$$

bedeutet.

(3). Aus der aussagenlogischen Tautologie

$$\vdash \alpha \wedge \beta \to \alpha$$

ergibt sich aus (1) direkt

$$\vdash \Box(\alpha \wedge \beta) \to \Box\alpha\,.$$

(4). Aus der aussagenlogischen Tautologie

$$\vdash \alpha \to (\beta \to \alpha \wedge \beta)$$

ergibt sich mit (1) zunächst

$$\vdash \Box\alpha \to \Box(\beta \to \alpha \wedge \beta)\,.$$

Aufgrund des K-Axioms gilt

$$\vdash \Box(\beta \to \alpha \wedge \beta) \to (\Box\beta \to \Box(\alpha \wedge \beta))\,.$$

Der Kettenschluss liefert

$$\vdash \Box\alpha \to (\Box\beta \to \Box(\alpha \wedge \beta))\,,$$

was aussagenlogisch äquivalent zu

$$\vdash \Box\alpha \wedge \Box\beta \to \Box(\alpha \wedge \beta)$$

ist.

(5) ergibt sich aus der aussagenlogischen Tautologie

$$\vdash \alpha \leftrightarrow \neg\neg\alpha$$

und Teil (1). □

Die erste der eben bewiesenen Eigenschaften der K-Modallogik bedeutet insbesondere, dass man in der Reichweite eines Notwendigkeitsoperators einen Ausdruck durcj einen jeden aussagenlogisch äquivalenten Ausdruck ersetzen kann.

24.4. **Einige modallogische Axiomenschemata.**

Wir besprechen einige modallogischen Axiomenschemata, die über das K-System hinausgehen. Die inhaltliche Relevanz der Systeme ist sehr unterschiedlich.

Definition 24.6. Das modallogische Axiomenschema

$$\Box\alpha$$

nennt man *Leerheitsaxiom.*

Dies ergibt keine interessante Modallogik, da einfach jede Aussage der Form $\Box\alpha$ gilt, auch dann, wenn α eine Kontradiktion ist, und jede Aussage der Form $\Diamond\alpha$ nicht gilt.

Definition 24.7. Das modallogische Axiomenschema

$$\Box\alpha \to \Diamond\alpha$$

nennt man *Möglichkeitsaxiom*.

Dies bedeutet also $\Diamond\alpha \vee \Diamond\neg\alpha$, es muss also die Aussage oder ihre Negation möglich sein, oder beides. Man spricht auch vom *Seriellitätsaxiom* oder *D*-Axiom. Die Bezeichnung *D* kommt von deontisch. Was verpflichtend ist, sollte insbesondere erlaubt sein.

Definition 24.8. Das modallogische Axiomenschema

$$\Diamond\alpha \to \Box\alpha$$

nennt man *Phantasiearmutsaxiom*.

Das Möglichkeitsaxiom bedeutet, dass es mindestens eine Vorstellungswelt gibt und das Phantasiearmutsaxiom bedeutet, dass es höchstens eine Vorstellungswelt gibt. Solche Charakterisierungen werden wir später im Rahmen der semantischen Interpretation mit gerichteten Graphen präzisieren.

Definition 24.9. Das modallogische Axiomenschema

$$\Diamond\alpha \leftrightarrow \Box\alpha$$

nennt man *Ideologieaxiom*.

In einer Ideologie stellt man sich genau eine Welt vor, die im Allgemeinen mit der Realität nichts zu tun hat.

Lemma 24.10. *Für eine K-Modallogik sind die folgenden Eigenschaften äquivalent.*

(1) *Es gilt das Phantasiearmutsaxiom.*
(2) *Es gilt die Umkehrung des K-Axioms, also*
$$\vdash (\Box\alpha \to \Box\beta) \to \Box(\alpha \to \beta)\,.$$
(3) *Es gilt das Axiomenschema*
$$\vdash \Diamond\alpha \wedge \Diamond\beta \to \Diamond(\alpha \wedge \beta)\,.$$

Beweis. Von (1) nach (2). Aus den aussagenlogischen Tautologien

$$\beta \to (\alpha \to \beta)$$

und

$$\neg\alpha \to (\alpha \to \beta)$$

ergeben sich mit Lemma 24.5 (1) die Ableitungen

$$\Box\beta \to \Box(\alpha \to \beta)$$

und

$$\Box\neg\alpha \to \Box(\alpha \to \beta)\,.$$

Das Phantasiearmutsaxiom liefert

$$\vdash \Diamond\neg\alpha \to \Box\neg\alpha$$

und über den Kettenschluss

$$\vdash \Diamond\neg\alpha \to \Box(\alpha \to \beta)\,.$$

Daher gilt

$$\vdash (\Diamond\neg\alpha \vee \Box\beta) \to \Box(\alpha \to \beta)\,,$$

was eben

$$\vdash (\Box\alpha \to \Box\beta) \to \Box(\alpha \to \beta)$$

bedeutet.

Von (2) nach (1). Aus der aussagenlogischen Tautologie

$$\vdash (\alpha \to \neg\alpha) \to \neg\alpha$$

ergibt sich mit Lemma 24.5 (1) direkt

$$\vdash \Box(\alpha \to \neg\alpha) \to \Box\neg\alpha\,.$$

Die Umkehrung des K-Axioms mit $\beta = \neg\alpha$ liefert

$$\vdash (\Box\alpha \to \Box\neg\alpha) \to \Box(\alpha \to \neg\alpha)\,.$$

Eine einfache aussagenlogische Überlegung zeigt

$$\vdash \Diamond\neg\alpha \to (\Box\alpha \to \Box\neg\alpha)\,.$$

Der doppelte Kettenschluss liefert

$$\vdash \Diamond\neg\alpha \to \Box\neg\alpha\,.$$

Da diese Beziehung für jedes $\neg\alpha$ gilt, gilt es nach Lemma 24.5 (5) überhaupt für jede Aussage.

Aus (1) folgt (3). Das K-Axiom liefert

$$\vdash \Box(\alpha \to \neg\beta) \to (\Box\alpha \to \Box\neg\beta)$$

und das Phantasiearmutsaxiom liefert

$$\vdash \Diamond\alpha \to \Box\alpha\,.$$

Dies zusammen ergibt

$$\vdash \Box(\alpha \to \neg\beta) \to (\Diamond\alpha \to \Box\neg\beta)\,.$$

Wir schreiben dies als

$$\vdash \Box(\neg\alpha \vee \neg\beta) \to (\neg\Diamond\alpha \vee \Box\neg\beta)\,.$$

Durch Kontraposition bedeutet dies

$$\vdash (\Diamond\alpha \wedge \neg\Box\neg\beta) \to \Diamond(\alpha \wedge \beta)\,.$$

Von (3) nach (1). Wir betrachten den Spezialfall

$$\vdash \Diamond\alpha \wedge \Diamond\neg\alpha \to \Diamond(\alpha \wedge \neg\alpha)\,.$$

Durch Kontraposition ist dies

$$\vdash \Box\neg(\alpha \wedge \neg\alpha) \rightarrow \neg(\Diamond\alpha \wedge \Diamond\neg\alpha)$$

und durch eine aussagenlogische Umstellung

$$\vdash \Box(\neg\alpha \vee \alpha) \rightarrow (\neg\Diamond\alpha \vee \neg\Diamond\neg\alpha)\,.$$

Aus der aussagenlogischen Tautologie

$$\vdash \neg\alpha \vee \alpha$$

folgt mit der Nezessisierungsregel

$$\vdash \Box(\neg\alpha \vee \alpha)$$

und somit

$$\vdash \neg\Diamond\alpha \vee \neg\Diamond\neg\alpha\,.$$

Dies bedeutet

$$\vdash \Diamond\alpha \rightarrow \Box\alpha\,.$$

□

24. Arbeitsblatt

24.1. **Übungsaufgaben.**

Aufgabe 24.1. Überprüfe, um die folgenden Wörter korrekt gebildete (einschließlich Klammerung) modallogische Ausdrücke sind.

(1) $\Box((p) \wedge (q))$,
(2) $(p) \rightarrow \Box(q)$,
(3) $(p) \rightarrow (\Box(q))$,
(4) $(\Diamond(p)) \rightarrow ((\Box(q)) \rightarrow (r))$.

Aufgabe 24.2. Zeige, dass das K-Axiom äquivalent zu

$$\vdash \Diamond\alpha \rightarrow (\Diamond\neg\beta \vee \Diamond(\alpha \wedge \beta))$$

ist.

Aufgabe 24.3. Formuliere die in Bemerkung 23.7 aufgeführten Eigenschaften für das Ableitungsprädikat in der Sprache der Modallogik.

Aufgabe 24.4.*

Zeige, dass im K-System der Ausdruck

$$\Box(\alpha \rightarrow \beta) \rightarrow (\Diamond\alpha \rightarrow \Diamond\beta)$$

ableitbar ist.

Aufgabe 24.5. Wir betrachten eine formale Modallogik, die durch das Axiomenschema

$$\vdash \Box\alpha \leftrightarrow \neg\alpha$$

gegeben sei.

(1) Erfüllt diese Modallogik das Axiomenschema K?
(2) Erfüllt diese Modallogik die Nezessisierungsregel?
(3) Erfüllt diese Modallogik das Ideologieaxiom?

Aufgabe 24.6. Es sei $p_i \quad i \in I$, eine Familie von Aussagenvariablen und sei L die zugehörige modallogische Sprache. Es sei S ein prädikatenlogisches Symbolalphabet, das unter anderem Konstanten c_i, $i \in I$, und eine fixierte Variable x enthalte.

(1) Definiere eine natürliche injektive Abbildung

$$\Psi\colon\ L \longrightarrow L^S,$$

bei der p_i auf $x = c_i$ und $\Box\alpha$ auf $\forall x\Psi(\alpha)$ abgebildet wird.
(2) Was ist $\Psi(\Diamond\alpha)$?
(3) Zeige, dass zu jeder in der K-Modallogik ableitbaren modallogischen Aussage α auch $\Psi(\alpha)$ im Prädikatenkalkül ableitbar ist.

Aufgabe 24.7.

(1) Zeige, dass in einer K-Modallogik das Axiomenschema

$$\Diamond(\alpha \wedge \beta) \to \Diamond\alpha \wedge \Diamond\beta$$

gilt.
(2) Zeige, dass in einer K-Modallogik das Axiomenschema

$$\Diamond\alpha \wedge \Diamond\beta \to \Diamond(\alpha \wedge \beta)$$

nicht gelten muss.

Aufgabe 24.8.

(1) Zeige, dass in einer K-Modallogik das Axiomenschema

$$\Diamond\alpha \vee \Diamond\beta \to \Diamond(\alpha \vee \beta)$$

gilt.
(2) Zeige, dass in einer K-Modallogik das Axiomenschema

$$\Diamond(\alpha \vee \beta) \to \Diamond\alpha \vee \Diamond\beta$$

nicht gelten muss.

Zur folgenden Aufgabe vergleiche auch Aufgabe 8.23.

Aufgabe 24.9. Zeige, dass in einer K-Modallogik das Axiomenschema

$$\Diamond(\alpha \to \beta) \to (\Diamond\alpha \to \Diamond\beta)$$

nicht gelten muss.

24.2. **Aufgaben zum Abgeben.**

Aufgabe 24.10. (2 Punkte)

Überprüfe, um die folgenden Wörter korrekt gebildete (einschließlich Klammerung) modallogische Ausdrücke sind.

(1) $\Box((p) \wedge (q)$,
(2) $(p) \to \Diamond((q) \vee (r))$,
(3) $(\Box(\Box((p)))) \to (\Box(q))$,
(4) $((\Diamond(p)) \to ((\Box(q)) \to (r)))$.

Aufgabe 24.11. (2 Punkte)

Zeige, dass in einer K-Modallogik

$$\vdash \Diamond\neg\neg\alpha \leftrightarrow \neg\neg\Diamond\alpha$$

ableitbar ist.

Aufgabe 24.12. (2 Punkte)

Zeige, dass die K-Modallogik widerspruchsfrei ist.

25. Vorlesung - Modallogik II

25.1. **Weitere Axiomenschemata.**

Definition 25.1. Das modallogische Axiomenschema

$$\Box\alpha \to \alpha$$

nennt man *Reflexivitätsaxiom*.

Durch das Reflexivitätsaxiom wird die eigene Welt bei Möglichkeitsüberlegungen mitberücksichtigt.

Definition 25.2. Das modallogische Axiomenschema

$$\alpha \to \Box\alpha$$

nennt man *Autismusaxiom*.

Durch das Autismusaxiom werden andere Welten bei Möglichkeitsüberlegungen nicht berücksichtigt, eventuell noch nicht einmal die eigene Welt. Wenn das Leerheitsaxiom gilt, so auch das Autismusaxiom.

Definition 25.3. Das modallogische Axiomenschema

$$\alpha \leftrightarrow \Box\alpha$$

nennt man *Fatalismusaxiom*.

In diesem Fall gilt auch

$$\alpha \leftrightarrow \Diamond\alpha$$

und damit auch

$$\Box\alpha \leftrightarrow \Diamond\alpha\,.$$

Es gilt als auch das Ideologieaxiom. Im Fatalismus wird die Realität zur Ideologie gemacht.

Die folgenden Axiomenschemata sind sinnvoller, die Bezeichnungen werden sich später erklären, wenn wir die semantische Interpretation zur Verfügung haben.

Definition 25.4. Das modallogische Axiomenschema

$$\alpha \to \Box\Diamond\alpha$$

nennt man *Symmetrieaxiom*.

Definition 25.5. Das modallogische Axiomenschema

$$\Box\alpha \to \Box\Box\alpha$$

nennt man *Transitivitätsaxiom*.

Definition 25.6. Das modallogische Axiomenschema

$$\Diamond\alpha \to \Box\Diamond\alpha$$

nennt man *euklidisches Axiom* (oder Axiom 5).

Lemma 25.7. *In einem modallogischen K-System, in dem das Symmetrieaxiom und das euklidische Axiom gelten, gilt auch das Transitivitätsaxiom.*

Beweis. Es sei S das in Frage stehende System. Eine spezielle Instanz des Symmetrieaxioms liefert

$$S \vdash \Box\alpha \to \Box\Diamond\Box\alpha\,.$$

Eine Umformulierung des euklidischen Axioms ist

$$S \vdash \Diamond\Box\alpha \to \Box\alpha\,.$$

Mit Lemma 24.5 (1) folgt daraus

$$S \vdash \Box\Diamond\Box\alpha \to \Box\Box\alpha$$

und insgesamt mit dem Kettenschluss

$$S \vdash \Box\alpha \to \Box\Box\alpha\,.$$

□

25.2. **Paradoxe Axiome.**

Einen modallogischen Ausdruck nennen wir *paradox*, wenn er, wenn man alle darin auftretenden $\Box$ (und somit auch alle $\Diamond$) weglässt, ein aussagenlogischer Widerspruch ergibt. Ein modallogisches Axiomenschema heißt paradox, wenn es davon eine paradoxe Instanz gibt.

Definition 25.8. Das modallogische Axiomenschema

$$\Box\alpha \leftrightarrow \neg\alpha$$

nennt man *Antiaxiom*.

Wenn das Antiaxiom gilt, so ist auch

$$\Diamond\alpha \leftrightarrow \neg\Box\neg\alpha \leftrightarrow \neg\neg\neg\alpha \leftrightarrow \neg\alpha \leftrightarrow \Box\alpha\,,$$

das Antiaxiom ist also ideologisch. In einer K-Modallogik führt das Antiaxiom zu einem Widerspruch, da ja dann zu einer aussagenlogischen Tautologie α wegen der Nezessisierungsregel auch $\Box\alpha$ und somit der Widerspruch $\neg\alpha$ gilt. Wenn man dagegen das Antiaxiom auf Aussagenvariablen beschränkt, also

$$\Box p \leftrightarrow \neg p$$

betrachtet, so ergibt sich ein sinnvolles K-System.

Definition 25.9. Das modallogische Axiomenschema

$$\Box(\Box\alpha \to \alpha) \to \Box\alpha$$

nennt man *Löb-Axiom*.

Bemerkung 25.10. Für das Ableitungsprädikat

$$\alpha(y) \;=\; \exists x(\delta_\Gamma(x, y))$$

zu einer die Peano-Arithmetik umfassenden entscheidbaren Satzmenge Γ gilt neben den in Bemerkung 23.7 angeführten Eigenschaften auch der Satz von Löb, nämlich

$$\alpha(GN(\alpha(GN(s)) \to s)) \to \alpha(GN(s))\,.$$

Wenn man

$$\Box s \;=\; \alpha(GN(s))$$

setzt, so kann man dies als

$$\Box(\Box s \to s) \to \Box s$$

schreiben, es liegt also genau das Löb-Axiom vor (daher der Name des Axioms). Unter der modallogischen *Beweisbarkeitslogik* versteht man die K-Modallogik, die durch das Löb-Axiom gegeben ist (das Transitivitätsaxiom lässt sich daraus ableiten). Es handelt sich um eine paradoxe Modallogik, in der man die Unvollständigkeit nachbbilden kann.

Es sei $\bot = p \wedge \neg p$ (gesprochen Falsum) eine Abkürzung für einen Widerspruch. Im Kontext der Beweisbarkeitslogik bedeutet dann $\neg\Box\bot$ die Nichtableitbarkeit eines Widerspruchs, also die Widerspruchsfreiheit des Systems. Aus dem Löb-Axiom (also der K-Modallogik L, die durch das Löbaxiom gegeben ist) lässt sich ableiten, dass diese Widerspruchsfreiheit ein Fixpunkt der Nichtableitbarkeit ist, d.h. es gilt

$$L \vdash \neg\Box\neg\Box\bot \leftrightarrow \neg\Box\bot\,,$$

siehe Aufgabe 25.6. Dies bedeutet insbesondere, dass weder $\Box\bot$ noch $\neg\Box\bot$ aus L ableitbar ist (die Widerspruchsfreiheit des Systems ergibt sich aus Satz 26.10 (6)). Insbesondere ist dieses Ableitungssystem unvollständig, was dem ersten Gödelschen Fixpunktsatz entspricht. Darüber hinaus ist die letzte Unableitbarkeit gerade die Aussage des zweiten Gödelschen Fixpunktsatzes, den man also so modallogisch nachbilden kann (die Hauptarbeit liegt aber darin, zu zeigen, dass das arithmetische Ableitungsprädikat das Löb-Axiom erfüllt).

25.3. **Einige klassische modallogische Systeme.**

Definition 25.11. Das modallogische K-System, in dem das Möglichkeitsaxiom gilt, heißt *D- System* .

Definition 25.12. Das modallogische K-System, in dem das Reflexionsaxiom gilt, heißt *T- System* .

Lemma 25.13. *Im modallogischen T-System gelten die folgenden Aussagen. Es ist*

$$T \vdash \alpha \to \Diamond\alpha\,.$$

Insbesondere ist

$$T \vdash \Box\alpha \to \Diamond\alpha$$

und damit ist ein T-System auch ein D-System.

Beweis. Die Kontraposition des Reflexivitätsaxioms ergibt direkt

$$T \vdash \neg\alpha \to \neg\Box\alpha\,,$$

also

$$T \vdash \neg\alpha \to \Diamond\neg\alpha\,.$$

Da dies für alle α gilt, gilt nach Lemma 24.5 (5) auch

$$T \vdash \alpha \to \Diamond\alpha\,.$$

Der Zusatz folgt aus

$$T \vdash \Box\alpha \to \alpha \text{ und } T \vdash \alpha \to \Diamond\alpha\,.$$

□

Definition 25.14. Das modallogische K-System, in dem das Reflexionsaxiom und das Symmetrieaxiom gilt, heißt *B- System* .

Definition 25.15. Das modallogische K-System, in dem das Reflexionsaxiom und das Transitivitätsaxiom gilt, heißt $S4$- *System* .

Definition 25.16. Das modallogische K-System, in dem das Reflexionsaxiom, das Symmetrieaxiom und das Transitivitätsaxiom gilt, heißt $S5$- *System* .

Lemma 25.17. *Für ein modallogisches K-System S sind folgende Aussagen äquivalent.*

(1) *Es gilt das Reflexivitätsaxiom und das euklidische Axiom*
(2) *Es gilt das Möglichkeitsaxiom, das Symmetrieaxiom und das Transitivitätsaxiom*
(3) *Es handelt sich um das $S5$-System.*

Beweis. Aus (1) folgt (2). Es sei Γ_1 das modallogische System, das durch die Gültigkeit von Reflexivitätsaxiom und euklidischem Axiom festgelegt ist. Nach Lemma 25.13 gilt mit dem Reflexivitätsaxiom auch das Möglichkeitsaxiom. Durch das Reflexivitätsaxiom gilt

$$\Gamma_1 \vdash \alpha \to \Diamond\alpha$$

und mit dem euklidischen Axiom gilt

$$\Gamma_1 \vdash \Diamond\alpha \to \Box\Diamond\alpha\,,$$

was mit dem Kettenschluss

$$\Gamma_1 \vdash \alpha \to \Box\Diamond\alpha\,,$$

also die Symmetrie ergibt. Aus dem euklidischen Axiom und der Symmetrie ergibt sich nach Lemma 25.7 auch die Transitivität.

Aus (2) folgt (3). Sei Γ_2 die Vereinigung aus dem Möglichkeitsaxiom, dem Symmetrieaxiom und dem Transitivitätsaxiom. Das Symmetrieaxiom ergibt

$$\Gamma_2 \vdash \alpha \to \Box\Diamond\alpha\,,$$

das Möglichkeitsaxiom liefert

$$\Gamma_2 \vdash \Box\Diamond\alpha \to \Diamond\Diamond\alpha$$

und das Transitivitätsaxiom liefert

$$\Gamma_2 \vdash \Diamond\Diamond\alpha \to \Diamond\alpha\,.$$

Der Kettenschluss darauf angewendet liefert

$$\Gamma_2 \vdash \alpha \to \Diamond\alpha\,,$$

also das Reflexivitätsaxiom.

Aus (3) folgt (1). Aus dem Transitivitätsaxiom

$$S_5 \vdash \Box\alpha \to \Box\Box\alpha$$

ergibt sich mit Lemma 24.5 (2)

$$S_5 \vdash \Diamond\Box\alpha \to \Diamond\Box\Box\alpha\,.$$

Aufgrund des Symmetrieaxioms gilt

$$S_5 \vdash \Diamond\Box\beta \to \beta\,.$$

Angewendet auf $\beta = \Box\alpha$ ergibt dies

$$S_5 \vdash \Diamond\Box\alpha \to \Box\alpha\,.$$

Dies ist gleichwertig zum euklidischen Axiom. □

Lemma 25.18. *In einem modallogischen K-System, in dem das Löb-Axiom gilt, gilt auch das Transitivitätsaxiom.*

Beweis. Wir wenden das Löb-Axiom auf den Ausdruck $\Box\alpha \wedge \alpha$ an und erhalten (L steht für dieses modallogische System)

$$L \vdash \Box(\Box(\Box\alpha \wedge \alpha) \to (\Box\alpha \wedge \alpha)) \to \Box(\Box\alpha \wedge \alpha)\,.$$

Wegen Lemma 24.5 (3) ist

$$\vdash \Box(\Box\alpha \wedge \alpha) \to \Box\Box\alpha$$

und

$$\vdash \Box(\Box\alpha \wedge \alpha) \to \Box\alpha\,.$$

Wegen der zuletzt angeführten Ableitung erhält man

$$\vdash \alpha \to (\Box(\Box\alpha \wedge \alpha) \to (\Box\alpha \wedge \alpha))$$

und daraus mit Lemma 24.5 (1) auch

$$\vdash \Box\alpha \to \Box((\Box(\Box\alpha \wedge \alpha) \to (\Box\alpha \wedge \alpha)))\,.$$

Ein zweifacher Kettenschluss liefert

$$L \vdash \Box\alpha \to \Box\Box\alpha\,.$$

□

25.4. **Gerichtete Graphen.**

Für die Modelltheorie der Modallogik benötigen wir gerichtete Graphen. Dies ist mathematisch betrachtet einfach eine zweistellige Relation auf einer Menge.

Definition 25.19. Ein *gerichteter Graph* ist eine Menge M versehen mit einer fixierten Relation $R \subseteq M \times M$.

Die Menge der Punkte $x \in M$ nennt man auch die Knoten des Graphen und man sagt, dass ein Pfeil von x nach y geht, wenn $(x, y) \in R$ ist. In dieser Weise werden gerichtete Graphen veranschaulicht. Einen Pfeil von einem Knoten zu sich selbst heißt *Schleife*.

Im Kontext von Ordnungsrelationen und Äquivalenzrelationen haben wir schon die Eigenschaften reflexiv, symmetrisch, transitiv kennengelernt. Einen symmetrischen gerichteten Graphen nennt man auch einen *ungerichteten*

Graphen. In diesem Fall nennt man einen verbindenden Pfeil eine Kante. Wir besprechen einige weitere Begrifflichkeiten und Eigenschaften.

Definition 25.20. Es sei (M, R) ein gerichteter Graph. Zu einer Teilmenge $T \subseteq M$ nennt man

$$\operatorname{Vorg}(T) = \{x \in M | \text{ es gibt } y \in T \text{ mit } xRy\}$$

die *Vorgängermenge* zu T.

Definition 25.21. Es sei (M, R) ein gerichteter Graph. Zu einer Teilmenge $T \subseteq M$ nennt man

$$\operatorname{Nachf}(T) = \{z \in M | \text{ es gibt } y \in T \text{ mit } yRz\}$$

die *Nachfolgermenge* zu T.

Ein Knoten ohne Nachfolger, also ohne abgehenden Pfeil (also auch keine Schleife), heißt *Sackgasse*.

Definition 25.22. Eine Relation auf einer Menge M heißt *euklidisch*, wenn zu $x, y, z \in M$ mit xRy und xRz stets yRz gilt.

25. Arbeitsblatt

25.1. Übungsaufgaben.

Aufgabe 25.1. Zeige, dass in einem K-System, in dem das Axiomenschema

$$\Box\alpha \to \Box\neg\alpha$$

gilt, bereits das Leerheitsaxiom gilt.

Aufgabe 25.2. Zeige die Äquivalenz (innerhalb der K-Modallogik) der folgenden modallogischen Axiomenschemata.

(1) Das Reflexivitätsaxiom ist äquivalent zu
$$\alpha \to \Diamond\alpha\,.$$
(2) Das Symmetrieaxiom ist äquivalent zu
$$\Diamond\Box\alpha \to \alpha\,.$$
(3) Das Transitivitätsaxiom ist äquivalent zu
$$\Diamond\Diamond\alpha \to \Diamond\alpha\,.$$
(4) Das euklidische Axiom ist äquivalent zu
$$\Diamond\Box\alpha \to \Box\alpha\,.$$

Zur folgenden Aufgabe vergleiche auch Aufgabe 23.17.

Aufgabe 25.3.*

Es sei M ein K-modallogisches System, in dem zusätzlich das Transitivitätsaxiom gelte. Ferner sei s ein modallogischer Ausdruck, für den

$$M \vdash \neg\Box s \leftrightarrow s$$

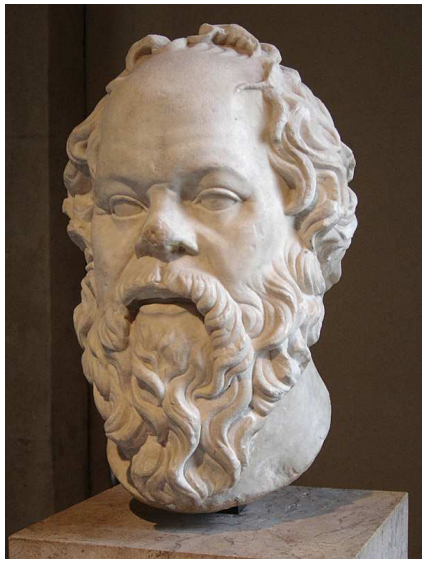
gelte. Zeige für einen beliebigen Ausdruck p die Ableitbarkeit

$$M \vdash \neg\Box(p \wedge \neg p) \rightarrow \neg\Box s\,.$$

Aufgabe 25.4. Zeige, dass das Löb-Axiom äquivalent zu

$$\vdash \Diamond\alpha \rightarrow \Diamond(\alpha \wedge \neg\Diamond\alpha)$$

ist.



Die Aussage „ich weiß, dass ich nichts weiß“ wird Sokrates zugeschrieben. In einer epistemischen K-Modallogik folgt daraus, dass Sokrates alles weiß.

Aufgabe 25.5.*

Wir interpretieren den Satz von Sokrates, „Ich weiß, dass ich nichts weiß“, als modallogisches Axiomenschema

$$\Box\neg\Box\alpha\,.$$

Zeige die folgenden Aussagen.

(1) Dieses Axiomenschema ist paradox.
(2) Dieses Axiomenschema ist innerhalb der K-Modallogik äquivalent zu

$$\Box\Diamond\alpha\,.$$

(3) Dieses Axiomenschema ist innerhalb der K-Modallogik äquivalent zu

$$\Box\alpha\,,$$

also zum Leerheitsaxiom.

Aufgabe 25.6.*

Es sei Γ die durch das Löb-Axiom gegebene K-Modallogik, also die Beweisbarkeitslogik. Wir setzen

$$\bot \,:=\, p \wedge \neg p$$

(als Abkürzung für einen Widerspruch). Zeige, dass

$$\Gamma \vdash \neg\Box\neg\Box\bot \leftrightarrow \neg\Box\bot$$

ableitbar ist.

Aufgabe 25.7. Es sei Γ eine Menge von modallogischen Ausdrücken, die allesamt nicht paradox seien und es sei

$$\Gamma \vdash \alpha$$

eine Ableitung. Zeige, dass α ebenfalls nicht paradox ist.

Aufgabe 25.8. Welche modallogischen Axiomenschemata gelten in der Prädikatenlogik, wenn man den Notwendigkeitsoperator $\Box$ als $\forall x$ mit einer fixierten Variablen x interpretiert?

Aufgabe 25.9. Zeige, dass ein gerichteter Graph, der sowohl euklidisch als auch symmetrisch ist, auch transitiv ist.

Aufgabe 25.10. Zeige, dass ein gerichteter Graph (M, R) genau dann reflexiv ist, wenn für die Nachfolgermengen zu jeder Teilmenge $T \subseteq M$ die Beziehung

$$T \,\subseteq\, \mathrm{Nachf}\,(T)$$

gilt.

Auf einer Menge M nennt man eine Abbildung

$$\mathfrak{P}\,(M) \longrightarrow \mathfrak{P}\,(M),\, T \longmapsto \overline{T},$$

einen *Hüllenoperator*, wenn die folgende Eigenschaften für alles Teilmengen $S, T \subseteq M$ gelten.

(1)

$$T \,\subseteq\, \overline{T}.$$

(2) Mit

$$S \subseteq T$$

ist auch

$$\overline{S} \subseteq \overline{T}.$$

(3)

$$\overline{\overline{T}} = \overline{T}.$$

Aufgabe 25.11. Es sei (M, R) ein gerichteter Graph. Welche der Eigenschaften eines Hüllenoperators erfüllt die Abbildung

$$\mathfrak{P}(M) \longrightarrow \mathfrak{P}(M),\ T \longmapsto \text{Nachf}(T),$$

welche nicht?

Auf einer Menge M nennt man eine Abbildung

$$\mathfrak{P}(M) \longrightarrow \mathfrak{P}(M),\ T \longmapsto \overline{T},$$

einen *topologischen Hüllenoperator*, wenn die folgenden Eigenschaften für alle Teilmengen $S, T \subseteq M$ gelten.

(1)

$$T \subseteq \overline{T}.$$

(2)

$$\overline{S \cup T} = \overline{S} \cup \overline{T}.$$

(3)

$$\overline{\emptyset} = \emptyset.$$

(4)

$$\overline{\overline{T}} = \overline{T}.$$

Aufgabe 25.12. Zeige die folgenden Aussagen.

(1) Es sei M ein topologischer Raum. Dann ist die Zuordnung

$$\mathfrak{P}(M) \longrightarrow \mathfrak{P}(M),\ T \longmapsto \overline{T} := \bigcap_{T \subseteq A,\, A \text{ abgeschlossen}} A,$$

die also einer Teilmenge ihren Abschluss (oder ihre abgeschlossene Hülle) zuordnet, ein topologischer Hüllenoperator.

(2) Auf M sei ein topologischer Hüllenoperator gegeben. Dann erhält man eine Topologie auf M, indem man die Teilmengen mit $A = \overline{A}$ als abgeschlossen erklärt.

Aufgabe 25.13. Es sei (M, R) ein gerichteter Graph. Wie kann man graphentheoretisch charakterisieren, dass die Abbildung

$$\mathfrak{P}(M) \longrightarrow \mathfrak{P}(M),\ T \longmapsto \text{Nachf}(T),$$

ein topologischer Hüllenoperator ist?

25.2. **Aufgaben zum Abgeben.**

Aufgabe 25.14. (4 Punkte)

Zeige, dass das modallogische Leerheitsaxiom das Autismusaxiom und dass das Autismusaxiom das Phantasiearmutsaxiom impliziert. Zeige ferner, dass diese Implikationen nicht umkehrbar sind.

Aufgabe 25.15. (2 Punkte)

Zeige, dass eine fatalistische K-Modallogik, die einen paradoxen Ausdruck enthält, bereits widersprüchlich ist.

Aufgabe 25.16. (2 Punkte)

Zeige, dass das Löb-Axiom paradox ist.

Aufgabe 25.17. (4 Punkte)

Zeige, dass für einen gerichteten Graphen (M, R) die folgenden Eigenschaften äquivalent sind.

(1) (M, R) ist reflexiv und euklidisch.
(2) (M, R) ist symmetrisch, transitiv und sackgassenfrei.
(3) (M, R) ist eine Äquivalenzrelation

Aufgabe 25.18. (2 Punkte)

Zeige, dass ein gerichteter Graph (M, R) genau dann transitiv ist, wenn für die Nachfolgermengen zu jeder Teilmenge $T \subseteq M$ die Beziehung

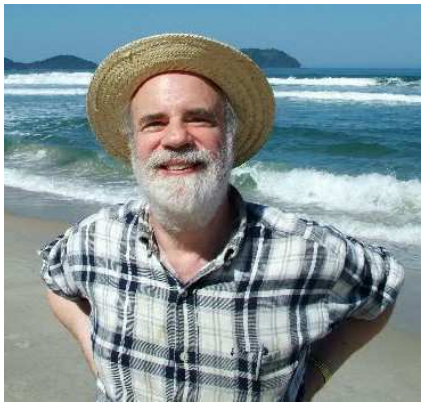
$$\text{Nachf}(\text{Nachf}(T)) \subseteq \text{Nachf}(T)$$

gilt.

26. Vorlesung - Semantik der Modallogik

26.1. **Semantik der Modallogik.**

Von Gottfried Wilhelm Leibniz stammt die Idee, Notwendigkeiten über mögliche Welten zu verstehen.



Saul Kripke schuf die formale Modelltheorie für die Modallogik.

Wir besprechen nun die Semantik der Modallogik, die mit gerichteten Graphen arbeitet, die die Idee von erreichbaren Welten modellieren.

Definition 26.1. Unter einem *modallogischen Modell* versteht man einen gerichteten Graphen (M, R) zusammen mit einer Wahrheitsbelegung μ für die Aussagenvariablen für jeden Knotenpunkt $w \in M$.

Die Knotenpunkte des gerichteten Graphen nennt man in diesem Zusammenhang auch *Welten* oder Weltpunkte. Die von einer Welt x aus verbundenen Welten y, also die mit xRy, nennt man die von x aus erreichbaren Welten, die Relation R heißt auch *Erreichbarkeitsrelation*. Durch die übliche Interpretation die aussagenlogischen Junktoren erhält man in jedem Weltpunkt eine Belegung für alle aussagenlogischen Ausdrücke in den gegebenen Aussagenvariablen. Darauf aufbauend kann man auch jedem modallogischen Ausdruck an jedem Knotenpunkt einen Wahrheitswert zuordnen, und zwar in folgender Weise.

Definition 26.2. In einem modallogischen Modell (M, R, μ) (mit einer punktweisen Wahrheitsbelegung μ) definiert man die Gültigkeit von modallogischen Ausdrücken induktiv wie folgt: Sei der modallogische Ausdruck α schon für jeden Weltpunkt definiert. Dann setzt man für einen jeden Weltpunkt $w \in M$

$$w \vDash \Box\alpha$$

genau dann, wenn in jeder von w aus erreichbaren Welt v die Beziehung

$$v \vDash \alpha$$

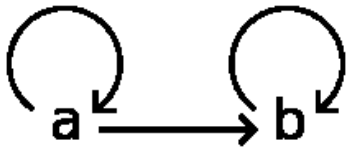
gilt.

Beispiel 26.3. Wir arbeiten mit den Aussagenvariablen p, q, r. Im Weltpunkt a gelte

$$a \vDash p, q, \neg r$$

und im Weltpunkt b gelte

$$b \vDash p, \neg q, r\,.$$



Daraus kann man die Gültigkeit von aussagenlogischen Ausdrücken jeweils erschließen, beispielsweise gilt

$$a \vDash p \wedge \neg r$$

oder

$$b \vDash \neg q \to r\,.$$

Für modallogische Ausdrücke muss man den gerichteten Graphen berücksichtigen, wobei man induktiv über die Anzahl der Boxen vorgeht. Es geht also zunächst um Ausdrücke der Form $\Box\alpha$, wobei α ein rein aussagenlogischer Ausdruck ist (also ohne jede Box). Die Gültigkeit von $\Box\alpha$ in einem Weltpunkt bedeutet, dass in jedem von diesem Weltpunkt aus erreichbaren Weltpunkt α gilt. Somit gilt beispielsweise

$$a \vDash \Box p$$

und

$$a \vDash \neg\Box q$$

und

$$a \vDash \Box(q \vee r)\,,$$

ferner

$$b \vDash \Box p$$

und

$$b \vDash \Box\neg q\,.$$

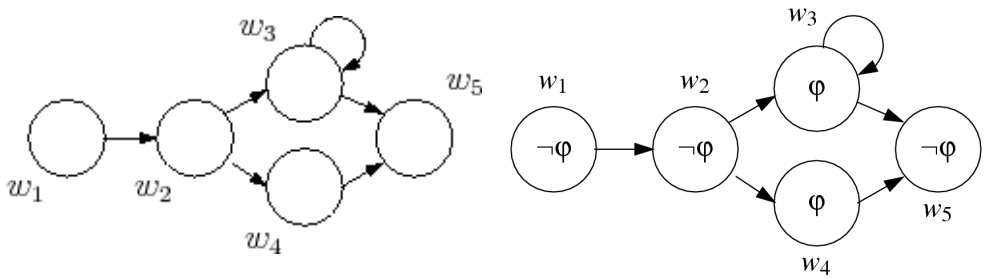
Damit kann man dann in jedem Punkt aussagenlogisch den Wahrheitswert von jeder modallogischen Aussage bestimmen, in der die Box nur einfach (also ohne Verschachtelungen) auftritt, beispielsweise

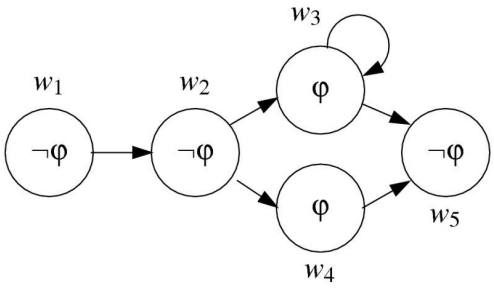
$$a \vDash \Box p \wedge \neg r \wedge \neg\Box\neg r\,.$$

Unter Berücksichtigung des gerichteten Graphen kann man dann auch den Wahrheitswert für jeden modallogischen Ausdruck mit modallogischer Verschachtelungstiefe ≤ 2 bestimmen, also etwa

$$a \vDash \Box\Box p\,,$$

u.s.w.





$\mathcal{M}, w_1 \models \neg\varphi$
$\mathcal{M}, w_1 \models \Box\Box\varphi$
$\mathcal{M}, w_2 \models \Box\varphi$
$\mathcal{M}, w_3 \models \Diamond\varphi$
$\mathcal{M}, w_5 \models \Box\varphi$
$\mathcal{M}, w_5 \models \Box\neg\varphi$

Definition 26.4. Man sagt, dass ein modallogischer Ausdruck α in einem modallogischen Modell (M, R, μ) *gilt*, geschrieben

$$(M, R, \mu) \vDash \alpha\,,$$

wenn

$$w \vDash \alpha$$

für alle $w \in M$ gilt.

Lemma 26.5. (1) *Die aussagenlogischen Tautologien der modallogischen Sprache gelten in jedem modallogischen Modell.*

(2) *In jedem modallogischen Modell* (M, R, β) *gilt das* K*-Axiom, also*

$$M \vDash \Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)\,.$$

(3) *Die in einem (jeden) modallogischen Modell gültigen Ausdrücke sind abgeschlossen unter dem Modus Ponens.*

(4) *Wenn ein modallogischer Ausdruck* α *in einem (jedem) modallogischen Modell gilt, so gilt auch* $\Box\alpha$ *in diesem (jedem) modallogischen Modell.*

Beweis. (1) und (3) sind klar, da die Gültigkeit in einem Knoten die aussagenlogischen Gesetze respektiert. (2). Sei $w \in M$ und

$$w \vDash \Box(\alpha \to \beta)$$

und

$$w \vDash \Box\alpha\,.$$

Dann gilt in jeder von w aus erreichbaren Welt v

$$v \vDash \alpha \to \beta \text{ und } v \vDash \alpha$$

und damit

$$v \vDash \beta\,.$$

Also ist

$$w \vDash \Box\beta\,.$$

(4). Wenn $(M, R, \mu) \vDash \alpha$ in einem modallogischen Modell (M, R, μ) gilt, so gilt für jede Welt $w \in M$ auch $w \vDash \alpha$. Wegen dieser allgemeinen Gültigkeit gilt auch $v \vDash \alpha$ für jede von w aus erreichbare Welt und damit $w \vDash \Box\alpha$. Dies gilt in jedem Punkt dieses Modells. □

Definition 26.6. Man sagt, dass eine Menge Γ von modallogischen Ausdrücken in einem modallogischen Modell (M, R, μ) *gilt*, geschrieben

$$(M, R, \mu) \vDash \Gamma\,,$$

wenn

$$(M, R, \mu) \vDash \alpha$$

für alle $\alpha \in \Gamma$ gilt.

Definition 26.7. Man sagt, dass ein *modallogischer Ausdruck* α in einem gerichteten Graphen (M, R) *gilt*, geschrieben

$$(M, R) \vDash \alpha\,,$$

wenn für jede Wahrheitsbelegung μ

$$(M, R, \mu) \vDash \alpha$$

gilt.

Definition 26.8. Es sei Γ eine Menge von modallogischen Ausdrücken und α ein modallogischer Ausdruck. Man sagt, dass α aus Γ *folgt*, geschrieben $\Gamma \vDash \alpha$, wenn für jedes modallogische Modell (M, R, μ) mit

$$(M, R, \mu) \vDash \Gamma$$

auch

$$(M, R, \mu) \vDash \alpha$$

gilt.

Für $\Gamma = \emptyset$ ergeben sich die modallogisch allgemeingültigen Ausdrücke. Aufgrund von Lemma 26.5 gehören alle in der K-Modallogik ableitbaren Ausdrücke dazu. Wie in der Aussagenlogik und der Prädikatenlogik ist also der Ableitungskalkül korrekt und es erhebt sich die Frage, ob er auch vollständig ist.

Lemma 26.9. *Es sei Γ ein K-modallogisches System und α ein modallogischer Ausdruck. Es gelte*

$$\Gamma \vdash \alpha\,.$$

Dann ist auch

$$\Gamma \vDash \alpha\,.$$

Beweis. Dies folgt aus Lemma 26.5. □

Diese Aussage erlaubt es insbesondere, zu zeigen, dass aus einem gegebenen modallogischen Axiomensystem Γ ein gewisser modallogischer Ausdruck α nicht ableitbar, indem man ein modallogisches Modell (M, R, μ) angibt, in dem Γ gilt, aber α nicht.

26.2. **Semantik der einzelnen modallogischen Systeme.**

Der durch die K-Modallogik gegebene axiomatische Rahmen gilt in jedem gerichteten Graphen, aufgefasst als modallogisches Modell. Wir fragen uns, wie speziellere modallogische Axiome mit Eigenschaften von gerichteten Graphen zusammenhängen. Der folgende Satz liefert eine Übersetzung zwischen diesen beiden Konzepten.

Satz 26.10.
(1) *In einem gerichteten Graphen (M, R) gilt das Möglichkeitsaxiom genau dann, wenn jeder Punkt $w \in M$ einen Nachfolger besitzt.*
(2) *In einem gerichteten Graphen (M, R) gilt das Reflexivitätsaxiom genau dann, wenn R reflexiv ist.*
(3) *In einem gerichteten Graphen (M, R) gilt das Symmetrieaxiom genau dann, wenn R symmetrisch ist.*
(4) *In einem gerichteten Graphen (M, R) gilt das Transitivitätsaxiom genau dann, wenn R transitiv ist.*
(5) *In einem gerichteten Graphen (M, R) gilt das euklidische Axiom genau dann, wenn R euklidisch ist.*

(6) *In einem gerichteten Graphen (M, R) gilt das Löb-Axiom genau dann, wenn R transitiv ist und es in M keine unendlichen Ketten gibt.*

Beweis. (1). Es sei (M, R) gegeben. Sei zunächst vorausgesetzt, dass in R jedes Element einen Nachfolger besitzt und sei

$$w \vDash \Box\alpha$$

für eine Welt $w \in M$. Es sei $v \in M$ mit wRv. Dann ist

$$v \vDash \alpha$$

und somit

$$w \vDash \Diamond\alpha\,,$$

also

$$w \vDash \Box\alpha \to \Diamond\alpha\,.$$

Sei umgekehrt angenommen, dass M eine Sackgassenwelt w besitzt. Dann ist für eine beliebige Aussagenvariable p

$$w \vDash \Box p\,,$$

aber

$$w \nvDash \Diamond p\,,$$

und das Möglichkeitsaxiom kann nicht gelten.

(2). Es sei (M, R) gegeben. Sei zunächst R reflexiv und sei

$$w \vDash \Box\alpha\,.$$

Wegen wRw ist insbesondere

$$w \vDash \alpha\,.$$

Wenn R nicht reflexiv ist, so sei $w \in M$ und wRw gelte nicht. Es sei μ die Belegung, bei der

$$w \vDash p$$

gelte, aber in allen anderen Welten $v \vDash \neg p$. Dann ist

$$w \vDash \neg\Diamond p\,,$$

und somit ist

$$w \nvDash p \to \Diamond p\,.$$

(3). Es sei (M, R) gegeben. Sei zunächst R symmetrisch und sei

$$w \vDash \alpha\,.$$

Es sei eine von w aus erreichbare Welt v gegeben, also wRv. Wegen der Symmetrie ist auch vRw und somit ist

$$v \vDash \Diamond\alpha\,.$$

Also ist

$$w \vdash \Box\Diamond\alpha\,.$$

Wenn R hingegen nicht symmetrisch ist, so seien $w, v \in M$ Welten mit wRv, aber nicht vRw. Es sei p eine Aussagenvariable und es sei μ die Belegung, bei der

$$w \vDash p$$

gelte und so, dass in allen von v aus erreichbaren Welten $z \vDash \neg p$ gelte. Dann ist

$$v \vDash \neg\Diamond p\,,$$

und somit ist

$$w \nvDash \Box\Diamond p\,,$$

also

$$w \nvDash p \to \Box\Diamond p\,.$$

(4). Es sei (M, R) gegeben. Sei zunächst R transitiv und sei

$$w \vDash \Box\alpha\,.$$

Es sei wRv und vRz und somit

$$z \vDash \alpha\,.$$

Also ist

$$v \vDash \Box\alpha\,.$$

und damit

$$w \vDash \Box\Box\alpha\,.$$

Es sei nun R nicht transitiv und seien $w, v, z \in M$ Punkte mit wRv, vRz, aber nicht wRz. Es sei p eine Aussagenvariable und sei μ die Belegung, bei der p in allen von w aus erreichbaren Welten gelte, in allen anderen Welten nicht. Dann ist

$$w \vDash \Box p$$

und

$$v \nvDash \Box p\,,$$

da ja $z \nvDash p$, und somit ist

$$w \nvDash \Box\Box p\,,$$

also

$$w \nvDash \Box p \to \Box\Box p\,.$$

(5). Es sei (M, R) gegeben. Sei zunächst R euklidisch und sei

$$w \vDash \Diamond\alpha\,.$$

Somit gibt es eine Welt v mit wRv und mit

$$v \vDash \alpha\,.$$

Es sei z eine Welt mit wRz. Nach der euklidischen Eigenschaft ist dann auch zRv, daher ist

$$z \vDash \Diamond\alpha\,.$$

Somit ist

$$w \vDash \Box\Diamond\alpha\,.$$

Es sei nun R nicht euklidisch und seien $w, v, z \in M$ Punkte mit wRv, wRz, aber nicht vRz. Es sei p eine Aussagenvariable und sei μ die Belegung, bei der $\neg p$ in allen von v aus erreichbaren Welten gelte, in allen anderen Welten nicht. Dann ist

$$v \vDash p$$

und somit

$$w \vDash \Diamond p\,.$$

In z gilt hingegen $\Box\neg p$, also

$$z \vDash \neg\Diamond p\,.$$

Somit gilt

$$w \vDash \neg\Box\Diamond p$$

und damit

$$w \nvDash \Diamond p \to \Box\Diamond p\,.$$

(6). Wir arbeiten mit der Kontraposition des Löb-Axioms, also mit

$$\Diamond\alpha \to \Diamond(\alpha \wedge \neg\Diamond\alpha)\,.$$

Sei zunächst vorausgesetzt, dass (M, R) die graphentheoretischen Eigenschaften besitzt. Sei $w \in W$ und

$$w \vDash \Diamond\alpha\,.$$

Dann gibt es eine Welt $v \in M$ mit wRv und mit

$$v \vDash \alpha\,.$$

Wir betrachten Ketten $vRv_2, v_2Rv_3, \ldots$ mit $v_i \vDash \alpha$. Da es keine unendliche Kette gibt, bricht eine solche Kette ab, sagen wir in v_n. In v_n gilt dann

$$v_n \vDash \alpha \wedge \neg\Diamond\alpha\,.$$

Wegen der Transitivität ist v_n von w aus erreichbar und somit ist

$$w \vDash \Diamond(\alpha \wedge \neg\Diamond\alpha)\,.$$

Sei nun vorausgesetzt, dass (M, R) nicht die Eigenschaften erfüllt. Wenn R nicht transitiv ist, so ist nach Lemma 25.18 in Verbindung mit Lemma 26.9 die Gültigkeit des Löb-Axioms ausgeschlossen. Es sei also eine unendlich lange Kette der Form w_nRw_{n+1} gegeben. Wir belegen $w_n \vDash p$ für alle $n \in \mathbb{N}$ und $v \vDash \neg p$ für alle anderen Welten. Dann gilt

$$w_0 \vDash \Diamond p \wedge \neg\Diamond(p \wedge \neg\Diamond p)\,,$$

da außerhalb der Kette stets $\neg p$ gilt und innerhalb der Kette stets $\Diamond p$ gilt. □

Bemerkung 26.11. Ein Modell des Löb-Axioms ist insbesondere frei von Schleifen, d.h. es ist reflexivitätsfrei, es gilt also nie wRw. Eine solche Schleife würde ja direkt eine unendliche Kette produzieren. Der gerichtete Graph

$$w_n, n \in \mathbb{N}\,,$$

mit der durch $w_n R w_m$, falls $n < m$ gegebenen Relation und der Belegung $w_n \vDash p$ für alle $n \in \mathbb{N}$ zeigt, dass das Löb-Axiom (in der Form $\Diamond p \to \Diamond(p \wedge \neg\Diamond p)$ bei einer unendlichen transitiven Kette ohne Schleifen nicht gelten muss.

Beispiel 26.12. Wir betrachten für $n \in \mathbb{N}_+$ die modallogische Ausdrucksmenge, die durch

$$\alpha_n = \Diamond(p_1 \wedge \ldots \wedge p_{n-1} \wedge \neg p_n)$$

gegeben ist. Da sich die Ausdrücke, die innerhalb des $\Diamond$-Operators von α_n stehen, gegenseitig ausschließen, bruacht man zur Realisierung von $\alpha_1 \wedge \ldots \wedge \alpha_n$ mindestens n Punkte. Daher ist

$$\Gamma = \{\alpha_n | \, n \in \mathbb{N}_+\}$$

nicht durch einen endlichen gerichteten Graphen erfüllbar. Die Ausdrucksmenge ist problemlos durch einen unendlichen gerichteten Graphen erfüllbar: Von einer Grundwelt W_0 aus sind die unendlich vielen Welten W_n, $n \in \mathbb{N}_+$, erreichbar, und in W_n gilt $p_1 \wedge \ldots \wedge p_{n-1} \wedge \neg p_n$ (die Wahrheitsbelegung ist ansonsten unerheblich).

26. Arbeitsblatt

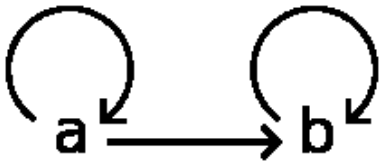
26.1. **Übungsaufgaben.**

Aufgabe 26.1. Für die Aussagenvariablen p, q, r gelte

$$a \vDash \neg p, q, r \text{ und } b \vDash \neg p, \neg q, r\,.$$

Bestimme in beiden Weltpunkten die Wahrheitswerte von

(1) $p \to \Box r$,
(2) $\Box q \to (\Box p \to \Box(r \wedge p))$,
(3) $(p \vee \Box\Box r) \to \Diamond r$,
(4) $\Diamond\Box\neg q \to (\Box\Diamond r \vee \neg p)$.



Aufgabe 26.2. Definiere die modallogische Verschachtelungstiefe für modallogische Ausdrücke.

Aufgabe 26.3. Zeige, dass bei einer Belegung der Aussagenvariablen durch die Definition 26.2 der Wahrheitswert für jeden modallogischen Ausdruck in jedem Punkt eines modallogischen Modelles eindeutig festgelegt ist.

Aufgabe 26.4. Es sei (M, R) der trivale Graph in dem Sinne, dass M einpunktig ist und dieser Punkt mit sich in Relation steht. Zeige, dass

$$(M, R) \vDash \alpha$$

genau dann bei jeder Belegung gilt, wenn α nicht paradox ist.

Aufgabe 26.5. Zeige durch Angabe eines modallogischen Modelles, dass im K-System der Ausdruck

$$\Box(p \vee q) \to \Box p \vee \Box q$$

nicht ableitbar ist.

Aufgabe 26.6. Zeige durch Angabe eines modallogischen Modelles, dass im K-System der Ausdruck

$$(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$$

nicht ableitbar ist. Insbesondere lässt sich also Lemma 24.5 (1) nicht internalisieren.

Aufgabe 26.7. Zeige durch Angabe eines modallogischen Modelles, dass im K-System der Ausdruck

$$(\Box\alpha \to \Box\beta) \to (\Diamond\alpha \to \Diamond\beta)$$

nicht ableitbar ist.

Aufgabe 26.8. Zeige durch Angabe eines modallogischen Modelles, dass im K-System der Ausdruck

$$(\Box\alpha \to \Box\beta) \to (\alpha \to \beta)$$

nicht ableitbar ist.

Aufgabe 26.9. Zeige durch Angabe eines modallogischen Modelles, dass im K-System der Ausdruck

$$\Box(\alpha \to \beta) \to (\alpha \to \beta)$$

nicht ableitbar ist.

Aufgabe 26.10. Zeige durch Angabe eines modallogischen Modelles, dass das System S4 nicht äquivalent zum System S5 ist.

Aufgabe 26.11. Seien $r \in \mathbb{N}$. Charakterisiere das modallogische Axiomenschema

$$\vdash \alpha \leftrightarrow \Diamond^r \alpha$$

graphentheoretisch.

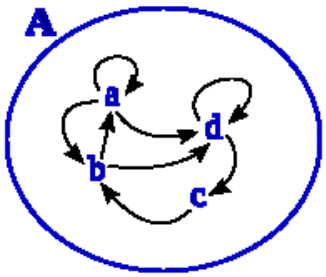
Aufgabe 26.12. Seien $r, s \in \mathbb{N}$. Charakterisiere das modallogische Axiomenschema

$$\vdash \Diamond^r \alpha \to \Diamond^s \alpha$$

graphentheoretisch.

26.2. **Aufgaben zum Abgeben.**

Aufgabe 26.13. (6 Punkte)



Für die Aussagenvariablen p, q, r gelte

$$a \vDash \neg p, q, \neg r\,, b \vDash \neg p, \neg q, r\,, c \vDash \neg p, \neg q, r\,, d \vDash p, q, r\,.$$

Bestimme in den vier Weltpunkten die Wahrheitswerte von

(1) $\Diamond q \to (\Box p \to \Box(r \wedge p))$,
(2) $(p \vee \Box\Box\neg r) \to \Diamond(\neg p \to r)$,
(3) $\Box\Diamond\Box\neg q \to (\Box\Diamond r \vee \neg p)$.

Aufgabe 26.14. (2 Punkte)

Zeige durch Angabe eines modallogischen Modelles, dass im K-System der Ausdruck

$$(\alpha \to \beta) \to (\Diamond\alpha \to \Diamond\beta)$$

nicht ableitbar ist.

Aufgabe 26.15. (5 Punkte)

Zeige die folgenden modelltheoretischen Charakterisierungen für modallogische Axiomenschemata.

(1) In einem gerichteten Graphen (M, R) gilt das Leerheitsaxiom genau dann, wenn die Relation R leer ist (wenn es also gar keine Pfeile gibt).
(2) In einem gerichteten Graphen (M, R) gilt das Autismusaxiom genau dann, wenn R nur aus Schleifen besteht.
(3) In einem gerichteten Graphen (M, R) gilt das Fatalismusaxiom genau dann, wenn R genau aus allen Schleifen besteht.
(4) In einem gerichteten Graphen (M, R) gilt das Phantasiearmutsaxiom genau dann, wenn von jedem Punkt höchstens ein Pfeil ausgeht.
(5) In einem gerichteten Graphen (M, R) gilt das Ideologieaxiom genau dann, wenn von jedem Punkt genau ein Pfeil ausgeht.

27. Vorlesung - Vollständigkeit der Modallogik

27.1. **Maximal widerspruchsfreie modallogische Ausdrucksmengen.**

Wir wollen die Vollständigkeit der modallogischen Modelle zeigen, d.h. die Beziehung, dass wenn aus einer modallogischen Ausdrucksmenge Γ die Gültigkeit von α folgt, dass dann α bereits aus Γ modallogisch ableitbar ist. Die Ausdrucksmenge umfasst dabei stets das System K und unter modallogisch ableitbar meint man ableitbar mit Hilfe von Modus Ponens und der Nezessisierungsregel. Dies muss hier betont werden, da es auf der Modellseite in natürlicher Weise Ausdrucksmengen gibt, die unter der Nezessisierungsregel abgeschlossen sind, und solche, die es nicht sind.

In einer K-Modallogik Γ gelten das modallogische Distributionsaxiom, die aussagenlogischen Tautologien und weitere, für Γ spezifische Ausdrücke. Ferner ist Γ abgeschlossenen unter dem Modus Ponens und der Nezessisierungsregel. In einem modallogischen Modell (M, R, μ), das Γ erfüllt, gilt Γ in jedem Weltpunkt $w \in M$, also

$$(M, R, \mu, w) \vDash \Gamma\,.$$

Die Gültigkeitsmenge in einem Weltpunkt ist unter aussagenlogischen Operationen und insbesondere unter dem Modus Ponens abgeschlossen. Dagegen ist die Gültigkeitsmenge in einem Weltpunkt *nicht* unter der Nezessisierungsregel abgeschlossen. Im allgemeinen muss es zu einem modallogischen System überhaupt keine vollständige widerspruchsfreie Erweiterung geben, die der Nezessisierungsregel genügt, siehe Aufgabe 27.6.

Von daher verstehen wir unter einer widerspruchsfreien Teilmenge innerhalb einer modallogischen Sprache L eine Teilmenge $W \subseteq L$, die die K-Modallogik umfasst und die unter Modus Ponens abgeschlossen ist und keinen (aussagenlogischen) Widerspruch enthält. Maximal widerspruchsfrei bedeutet wieder,

dass aus jeder echten Erweiterung ein Widerspruch aussagenlogisch ableitbar ist. Zu jeder Welt $w \in M$ in einem beliebigen modallogischen Modell (M, R, μ) von K ist die Gültigkeitsmenge $(M, R, \mu, w)^{\vdash}$ eine solche Teilmenge.

Lemma 27.1. *Es sei Γ eine modallogische Ausdrucksmenge, die aussagenlogisch widerspruchsfrei sei. Dann gibt es eine maximal widerspruchsfreie Ausdrucksmenge $\Gamma \subseteq \tilde{\Gamma}$.*

Beweis. Dies ist eine rein aussagenlogische Aussage, die im Prinzip aus Lemma 5.17 folgt. Allerdings ist hier durch die Anwesenheit von $\Box$ die Sprache etwas anders. Für diesen Zweck kann man modalisierte Aussagen einfach als neue Aussagenvariablen auffassen. Man kann auch direkt das Lemma von Zorn in der jetzigen Situation anwenden. Oder man kann im abzählbaren Fall wie folgt schließen: Mit I ist auch die modallogische Sprache überhaupt abzählbar. Wir betrachten eine Abzählung α_n, $n \in \mathbb{N}_+$, der modallogischen Ausdrücken und definieren

$$\Gamma_{n+1} = \Gamma_n \cup \{\alpha_{n+1}\},$$

falls dies widerspruchsfrei ist, und ansonsten durch

$$\Gamma_{n+1} = \Gamma_n \cup \{\neg\alpha_{n+1}\}.$$

Die Vereinigung $\tilde{\Gamma}$ ist dann maximal widerspruchsfrei. $\square$

27.2. **Das universelle modallogische Modell.**

In einer jeden Welt in einem modallogischen Modell (M, R, ν) ist die Gültigkeitsmenge maximal widerspruchsfrei. Für zwei Welten $w, v \in M$ gilt dabei

$$\text{Wenn } wRv, \text{ dann } (v \vDash \alpha \Rightarrow w \vDash \Diamond\alpha) .$$

Die rechte Seite kann man also als eine notwendige Bedingung dafür ansehen, dass v von w aus erreichbar ist. Im universellen modallogischen Modell definiert man die Erreichbarkeitsrelation durch diese notwendige Bedingung.

Konstruktion 27.2. Es sei p_i, $i \in I$, eine Menge von Aussagenvariablen und L die zugehörige modallogische Sprache. Es sei U die Menge aller K umfassenden, (aussagenlogisch) maximal widerspruchsfreien Teilmengen

$$W \subseteq L.$$

Auf U definieren wir eine Erreichbarkeitsrelation R durch

$$WRV \text{ genau dann, wenn für jedes } \alpha \in L \text{ mit } \alpha \in V \text{ die Beziehung } \Diamond\alpha \in W \text{ gilt.}$$

Wir nennen U versehen mit dieser Relation und der durch $W \vdash p$, wenn $p \in W$, festgelegten Belegung ν das *universelle modallogische Modell*.

Wir identifizieren also Welten mit der Menge der in ihnen gültigen modallogischen Aussagen. Wenn R eine Erreichbarkeitsrelation sein soll, so muss diese Beziehung gelten. Die rechte Seite ist dabei eine Implikation, keine Äquivalenz; es wird nicht gefordert, dass aus $\Diamond\alpha \in W$ auch $\alpha \in V$ folgt.

Konstruktion 27.3. Es sei p_i, $i \in I$, eine Menge von Aussagenvariablen und L die zugehörige modallogische Sprache. Es sei $\Gamma \subseteq L$ eine K-modallogische Ausdrucksmenge. Es sei U_Γ die Menge aller Γ umfassenden, (aussagenlogisch) maximal widerspruchsfreien Teilmengen

$$W \subseteq L.$$

Auf U_Γ definieren wir eine Erreichbarkeitsrelation R durch

WRV genau dann, wenn für jedes $\alpha \in L$ mit $\alpha \in V$ die Beziehung $\Diamond\alpha \in W$ gilt.

Wir nennen U_Γ versehen mit dieser Relation und der durch $W \vdash p$, wenn $p \in W$, festgelegten Belegung ν das Γ-*universelle modallogische Modell*.

Die Relation und die Belegung im Γ-universellen modallogischen Modell stimmen mit dem universellen Modell überein, es hndelt sich also um einen Teilgraphen. Es ist unser Ziel zu zeigen, dass im Γ-universellen modallogischen Modell (U, R, μ, W) genau die Ausdrücke aus W gelten.

Lemma 27.4. *Es sei Γ ein K-modallogisches System und α ein modallogischer Ausdruck. Dann folgt aus*

$$\Gamma \vdash \alpha$$

die Beziehung

$$\Box\Gamma \vdash \Box\alpha\,,$$

wobei

$$\Box\Gamma = \{\Box\beta |\, \beta \in \Gamma\}\,.$$

Beweis. Die Ableitbarkeit bedeutet, dass es Ausdrücke $\beta_1, \ldots, \beta_n \in \Gamma$ mit

$$\vdash \beta_1 \wedge \ldots \wedge \beta_n \to \alpha$$

gibt. Nach Lemma 24.5 (1) ist

$$\vdash \Box(\beta_1 \wedge \ldots \wedge \beta_n) \to \Box\alpha\,.$$

Aus Lemma 24.5 (4) folgt durch Induktion sofort

$$\vdash \Box\beta_1 \wedge \ldots \wedge \Box\beta_n \to \Box(\beta_1 \wedge \ldots \wedge \beta_n)$$

und somit mit dem Kettenschluss

$$\vdash \Box\beta_1 \wedge \ldots \wedge \Box\beta_n \to \Box\alpha\,.$$

Dies bedeutet

$$\Box\beta_1, \ldots, \Box\beta_n \vdash \Box\alpha\,.$$

□

Lemma 27.5. *Es sei p_i, $i \in I$, eine Menge von Aussagenvariablen und L die zugehörige modallogische Sprache. Es sei $\Gamma \subseteq L$ ein K-modallogisches System, es sei $W \subset L$ eine maximal widerspruchsfreie Γ-Teilmenge und es sei $\alpha \in L$ ein modallogischer Ausdruck mit $\Diamond\alpha \in W$. Dann gibt es eine maximal widerspruchsfreie Γ-Teilmenge $V \subset L$ mit $\alpha \in V$ und mit WRV im Sinne des Γ-universellen modallogischen Modells.*

Beweis. Wir betrachten die Menge

$$V' = \{\beta | \, \Box\beta \in W\} \cup \{\alpha\}\,,$$

die Γ umfasst, da Γ unter der Nezessisierungsregel abgeschlossen ist. Wir behaupten, dass diese Menge widerspruchsfrei ist. Andernfalls würde es endliche viele $\beta_1, \ldots, \beta_n$ mit $\Box\beta_i \in W$ geben mit

$$\vdash \beta_1 \wedge \ldots \wedge \beta_n \to (\alpha \to (p \wedge \neg p))\,.$$

Dies schreiben wir als

$$\vdash \beta_1 \wedge \ldots \wedge \beta_n \to (\neg(p \wedge \neg p) \to \neg\alpha)\,.$$

Nach Lemma 27.4 ist dann auch

$$\vdash \Box\beta_1 \wedge \ldots \wedge \Box\beta_n \to \Box(\neg(p \wedge \neg p) \to \neg\alpha)\,.$$

Wegen des K-Axioms ist

$$\vdash \Box(\neg(p \wedge \neg p) \to \neg\alpha) \to (\Box\neg(p \wedge \neg p) \to \Box\neg\alpha)$$

und somit

$$\vdash \Box\beta_1 \wedge \ldots \wedge \Box\beta_n \to (\Box(p \vee \neg p) \to \Box\neg\alpha)\,.$$

Da der Vordersatz zu W gehört, und W abgeschlossen unter Implikationen ist, ist auch

$$\Box(p \vee \neg p) \to \Box\neg\alpha \in W\,.$$

Da $p \vee \neg p$ eine Tautologie ist und wegen der Nezessisierungsregel (die ja für Tautologien gilt) ergibt sich

$$\Box\neg\alpha \in W\,,$$

was ein Widerspruch zu $\Diamond\alpha \in W$ angesichts der Widerspruchsfreiheit von W ist.

Somit ist V' widerspruchsfrei. Sei $V' \subseteq V$ eine maximal widerspruchsfreie Teilmenge von L, die es nach Lemma 27.1 gibt. Sei $\beta \in V$. Dann ist $\Diamond\beta \in W$. Andernfalls wäre nämlich wegen der Maximalität (von W) $\Box\neg\beta \in W$, doch dann wäre $\neg\beta \in V' \subseteq V$. Es gilt also WRV. □

Lemma 27.6. *Es sei Γ ein K-modallogisches System. Dann gilt im Γ-universellen modallogischen Modell für jede Welt und jeden modallogischen Ausdruck α die Beziehung*

$$W \vDash \alpha \text{ genau dann, wenn } \alpha \in W\,.$$

Beweis. Wir führen Induktion über den Aufbau der modallogischen Sprache, und zwar gleichzeitig für alle Welten. Für Aussagenvariablen gilt die Behauptung unmittelbar aufgrund der festgelegten Belegung. Die Äquivalenz ist auch unter aussagenlogischen Konstruktionen abgeschlossen, da die W unter K-Ableitungen abgeschlossen sind. Es bleibt noch zu zeigen, dass sich die Äquivalenz bei modallogischen Operationen erhält, wobei wir mit dem Möglichkeitsoperator $\Diamond$ arbeiten. Sei also $\Diamond\alpha$ gegeben, wobei die Äquivalenz für α und für alle Welten gelte. Wenn $W \vDash \Diamond\alpha$ gilt, so gibt es eine Welt $V \in U_\Gamma$ mit WRV und $V \vDash \alpha$. Aufgrund der Induktionsvoraussetzung gilt $\alpha \in V$. Wegen der Definition der Erreichbarkeitsrelation bedeutet dies insbesondere $\Diamond\alpha \in W$. Sei umgekehrt $\Diamond\alpha \in W$. Dann folgt aus Lemma 27.5 die Existenz einer von W aus erreichbaren Γ-Welt V mit $\alpha \in V$, also nach Induktionsvoraussetzung $V \vDash \alpha$ und somit $W \vDash \Diamond\alpha$. □

27.3. **Die Vollständigkeit der Modallogik.**

Satz 27.7. *Es sei Γ ein K-modallogisches System und sei α ein modallogischer Ausdruck. Dann ist*

$$\Gamma \vdash \alpha$$

genau dann, wenn

$$\Gamma \vDash \alpha\,.$$

Beweis. Die Hinrichtung ergibt sich aus Lemma 26.9. Für die Rückrichtung nehmen wir

$$\Gamma \nvdash \alpha$$

an. Dann ist

$$\Gamma' \,=\, \Gamma \cup \{\neg\alpha\}$$

(aussagenlogisch) nicht widersprüchlich und wir müssen zeigen, dass Γ' durch ein Γ-modallogisches Modell erfüllbar ist. Wir betrachten dazu das Γ-universelle modallogische Modell (U_Γ, R, ν), in dem Γ (in jedem Weltpunkt) gilt. Nach Lemma 27.1 gibt es eine maximal widerspruchsfreien Γ'-Ausdrucksmenge $\tilde{\Gamma}$, die wir als Welt $W = \tilde{\Gamma}$ in U_Γ betrachten können. Nach Lemma 27.6 gilt $W \vDash \tilde{\Gamma}$, was insbesondere die Gültigkeit von $\Gamma \cup \{\neg\alpha\}$ in W zeigt. □

Bemerkung 27.8. Es sei betont, dass der Vollständigkeitssatz sich auf die Folgerung bezieht, die unter Bezug auf Modelle formuliert wird, nicht auf Rahmen. Typischerweise ist eine modallogische Ausdrucksmenge in gewissen Rahmen bei jeder Belegung gültig, aber auch noch in weiteren Rahmen bei gewissen Belegungen. Ein semantischer Beweis für die Ableitbarkeit kann also im Allgemeinen nicht allein mit Eigenschaften von gerichteten Graphen arbeiten, sondern muss auch Variablenbelegungen mitberücksichtigen.

27. Arbeitsblatt

27.1. Übungsaufgaben.

Aufgabe 27.1. Zeige, dass eine K-Modallogik, in der das Möglichkeitsaxiom und das Löb-Axiom gelten, bereits widersprüchlich ist.

Aufgabe 27.2. Zeige, dass das universelle modallogische Modell zu einer einzigen Aussagenvariable p bereits unendlich ist.

Aufgabe 27.3. Es sei T eine maximal widerspruchsfreie modallogische Ausdrucksmenge. Zeige, dass T vollständig ist, dass also für jedes $\alpha \in L$ die Alternative „Entweder $\alpha \in T$ oder $\neg\alpha \in T$“ gilt.

Aufgabe 27.4. Es sei T eine maximal widerspruchsfreie modallogische Ausdrucksmenge, die die K-Modallogik umfasse und in der die Nezessisierungsregel gelte. Zeige, dass in T entweder das Leerheitsaxiom oder das Fatalismusaxiom gilt.

Aufgabe 27.5. Es sei T eine maximal widerspruchsfreie modallogische Ausdrucksmenge, die die K-Modallogik umfasse und in der es einen paradoxen Ausdruck gebe. Zeige, dass T nicht unter der Nezessisierungsregel abgeschlossen ist.

Die folgende Aufgabe kann man wegen Aufgabe 25.6 insbesondere auf die Beweisbarkeitslogik anwenden.

Aufgabe 27.6. Wir setzen

$$\bot := p \wedge \neg p.$$

Es sei Γ eine K-Modallogik, in der

$$\Gamma \vdash \Box\bot \leftrightarrow \Box\neg\Box\bot$$

ableitbar ist. Zeige, dass es keine widerspruchsfreie Erweiterung

$$\Gamma \subseteq \tilde{\Gamma}$$

gibt, die aussagenlogisch und unter der Nezessierungsregel abgeschlossen ist.

Aufgabe 27.7. Es sei $K = K^{\vdash}$ die K-Modallogik und sei U das universelle modallogische Modell. Zeige

$$K = \bigcap_{W \in U} W.$$

Aufgabe 27.8. Ist das universelle modallogische Modell symmetrisch, reflexiv, transitiv? Ist das universell symmetrische modallogische Modell reflexiv?

Aufgabe 27.9. Es sei (U, R, ν) das universelle modallogische Modell. Kann man auf (U, R) auch eine andere Wahrheitsbelegung definieren?

27.2. **Aufgaben zum Abgeben.**

Aufgabe 27.10. (2 Punkte)

Man gebe ein Beispiel für ein modallogisches Modell (M, R, ν), eine Welt $w \in M$ und einen modallogischen Ausdruck $\alpha \to \beta$ mit

$$(M, R, \nu, w) \vDash \alpha \to \beta\,,$$

aber

$$(M, R, \nu, w) \nvDash \Box\alpha \to \Box\beta\,.$$

Aufgabe 27.11. (3 Punkte)

Es sei (M, S, μ) ein modallogisches Modell und (U, R, ν) das universelle modallogische Modell. Zeige, dass durch

$$M \longrightarrow U,\ w \longmapsto (M, S, \mu, w)^{\vDash},$$

eine Abbildung definiert ist, die ein Homomorphismus (bezüglich der zweistelligen Relationen S und R) ist.

Aufgabe 27.12. (4 Punkte)

Es sei (M, R, μ) ein modallogisches Modell für die $S5$-Modallogik. Zeige, dass für zueinander erreichbare Welten $v, w \in M$ die Gültigkeitsmengen verschieden sein können, dass aber für jeden Ausdruck $(M, R, \mu, v) \vDash \Box\alpha$ genau dann gilt, wenn $(M, R, \mu, w) \vDash \Box\alpha$ gilt.

Aufgabe 27.13. (2 Punkte)

Es sei Γ eine modallogische Ausdrucksmenge und α ein modallogischer Ausdruck. Es sei $\Gamma \vDash \alpha$. Zeige, dass es eine endliche Teilmenge $\Gamma_e \subseteq \Gamma$ mit $\Gamma_e \vDash \alpha$ gibt.

Aufgabe 27.14. (3 Punkte)

Zeige, dass in der K-Modallogik das Schema

$$\Box\alpha \wedge \Diamond\beta \to \Diamond\alpha$$

ableitbar ist.

Aufgabe 27.15. (2 Punkte)

In einem K-modallogischen System S gelte das Axiomenschema

$$\alpha \to \Diamond\Box\alpha\,.$$

Zeige, dass man in S das Möglichkeitsaxiom

$$\Box\alpha \to \Diamond\alpha$$

ableiten kann.

Aufgabe 27.16. (3 Punkte)

Charakterisiere die modallogischen Rahmen, in denen (bei jeder Wahrheitsbelegung) das Axiomenschema

$$\alpha \to \Diamond\Box\alpha$$

gilt.

Aufgabe 27.17. (3 Punkte)

Zeige, dass aus dem K-modallogischen Axiomenschema

$$\alpha \to \Diamond\Box\alpha$$

nicht das Axiomenschema

$$\alpha \to \Box\Diamond\alpha$$

ableitbar ist.

In dieser Woche können Sie noch Aufgaben aus dem Kurs, die sie noch nicht oder nicht mit voler Punktzahl bearbeitet haben, nachreichen.

Anhang A: Bildlizenzen

Die Bilder dieses Textes stammen aus Commons (also http://commons.wikimedia.org), und stehen unter unterschiedlichen Lizenzen, die zwar alle die Verwendung hier erlauben, aber unterschiedliche Bedingungen an die Verwendung und Weitergabe stellen. Es folgt eine Auflistung der verwendeten Bilder dieses Textes (nach der Seitenzahl geordnet, von links nach rechts, von oben nach unten) zusammen mit ihren Quellen, Urhebern (Autoren) und Lizenzen. Dabei ist *Quelle* so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/File:

unmittelbar davor setzt, die entsprechende Datei auf Commons ergibt. *Autor* benennt den Urheber des Werkes, falls dieser bekannt ist. *Benutzer* meint den Hochlader der Datei; wenn keine weitere Information über den Autor vorliegt, so gilt der Benutzer als Urheber. Die Angabe des Benutzernamen ist so zu verstehen, dass sich, wenn man

http://commons.wikimedia.org/wiki/User:

unmittelbar davor setzt, die Benutzerseite ergibt. Wenn das Bild ursprünglich in einem anderen Wikimedia-Projekt hochgeladen wurde, so wird die Domäne (bspw. *de.wikipedia.org*) explizit angegeben.

Die *Lizenz* ist die auf der Dateiseite auf Commons angegebene Lizenz. Dabei bedeuten

- GFDL: Gnu Free Documentation License (siehe den angehängten Text, falls diese Lizenz vorkommt)
- CC-BY-SA-2.5 (3.0): Creative Commons Attribution ShareAlike 2.5 (oder 3.0)
- PD: gemeinfrei (public domain)

Abbildungsverzeichnis

Quelle = Marin Mersenne.jpeg , Autor = Benutzer Maksim auf Commons, Lizenz = PD 13

Quelle = Andrew wiles1-3.jpg , Autor = C. J. Mozzochi, Princeton N.J (= Benutzer Nyks auf Commons), Lizenz = freie Verwendung, copyright C. J. Mozzochi, Princeton N.J. 15

Quelle = Ramon Llull.jpg , Autor = Benutzer Pil56 auf Commons, Lizenz = gemeinfrei 18

Quelle = Gottfried Wilhelm Leibniz c1700.jpg , Autor = Johann Friedrich Wentzel d. Ä. (= Benutzer AndreasPraefcke auf Commons), Lizenz = PD 18

Quelle = Gartentoreverbindung.png , Autor = Benutzer Bocardodarapti auf Commons, Lizenz = CC-by-sa 4.0 19

Quelle = Goldbach-1000.png , Autor = Benutzer Mucfish auf Commons, Lizenz = PD 21

Quelle = DNA structure and bases FR.svg , Autor = Benutzer Dosto auf Commons, Lizenz = CC-by-sa 2.5 28

Quelle = Abstammungsbaum.png , Autor = Benutzer Funnyflowerpot auf Commons, Lizenz = CC-by-sa 4.0 33

Quelle = Rechtecke.png , Autor = Benutzer Mgausman auf Commons, Lizenz = CC-by-sa 3.0 36

Quelle = Termstammbaum.png , Autor = Benutzer Funnyflowerpot auf Commons, Lizenz = CC-by-sa 4.0 82

Quelle = Uni Freiburg - Philosophen 4.jpg , Autor = Cipri Adolf Bermann (= Benutzer Michael Sch. auf Commons), Lizenz = CC-BY-SA-2.5 83

Quelle = Dedekind.jpeg , Autor = Benutzer auf Commons, Lizenz = PD 149

Quelle = Giuseppe Peano.jpg , Autor = Benutzer Kalki auf Commons, Lizenz = PD? 149

Quelle = NachfolgermitSchleife.png , Autor = Benutzer Mgausmann auf Commons, Lizenz = CC-by-sa 4.0 156

Quelle = Tred-G.svg , Autor = Benutzer Dmitry Dzhus auf Commons, Lizenz = gemeinfrei 203

Quelle = Alan Turing cropped.jpg , Autor = Jon Callas (= Benutzer Compro auf Commons), Lizenz = CC by sa 2.0 220

Quelle = 1925 kurt gödel.png , Autor = Benutzer Kl833x9 auf Commons, Lizenz = PD 264

Quelle = Aristotle Altemps Inv8575.jpg , Autor = Benutzer Jastrow auf Commons, Lizenz = gemeinfrei 273

Quelle = Socrates Louvre.jpg , Autor = Benutzer Sting auf Commons, Lizenz = CC-by-sa 2.5 289

Quelle = Gottfried Wilhelm von Leibniz.jpg , Autor = Christoph Bernhard Francke (= Benutzer Andrejj auf Commons), Lizenz = 293

Quelle = Kripke.JPG , Autor = Benutzer Oursipan auf Commons, Lizenz = gemeinfrei 293

Quelle = Baby Category 2.svg , Autor = Benutzer Melikamp auf Commons, Lizenz = CC-by-sa 3.0 294

Quelle = Kripke frame.png , Autor = Benutzer Eusebius auf Commons, Lizenz = CC-by-sa 3.0 295

Quelle = Kripke model.png , Autor = Benutzer Eusebius auf Commons, Lizenz = CC-by-sa 3.0 295

Quelle = Frames.png , Autor = Benutzer Eusebius auf Commons, Lizenz = CC-by-sa 3.0 295

Quelle = Baby Category 2.svg , Autor = Benutzer Melikamp auf Commons, Lizenz = CC-by-sa 3.0 301

Quelle = Relación binaria 01.svg , Autor = Benutzer HiTe auf Commons, Lizenz = gemeinfrei 303