Version vom 25. November 2013

Dieser Absatz ist mir einem Strich am rand markiert: damit werden in diesem Dokument die Prüfungsrelevanten Teile hervorgehoben.

1. Kurzwiederholung Vollständigkeitssatz

(1) **Richard Paradoxon:**

> Sei n die kleinste natürliche Zahl die nicht mit einem Satz mit weniger als tausend Buchstaben definiert werden kann.

Dieses Paradoxon weist schon auf einen wesentlichen Effekt der mathematischen Logik hin:

(2) **Haupt-Erkenntnis:** Um Begriffe wie Beweis, Definition etc zu untersuchen muss man sich auf eine (formale) Sprache festlegen, die sogenannte **Objektsprache**. (Als **Metasprache** wird dann üblicherweise die (formale oder informelle) Sprache bezeichnet in der man sich über die Objektsprache unterhält.)

Diese Festlegung einer Objektsprache ist immer und notwendigerweise eine Einschränkung: Es gibt keine universelle mathematische Sprache. (Im Unterschied zB zum universellen Berechenbarkeitsbegriff.)

Anders ausgedrückt: Eine Metasprache die "viel" über die Objektsprache ausdrücken kann (z.B. die Begriffe, die für das Richard Paradoxon verwendet werden) muss notwendigerweise stärker sein als die Objektsprache. Man kann aber auch manche Sätze über die Objektsprache in der Objektsprache selbst ausdrücken (wichtiges Beispiel: Beweisbarkeit in PA kann man in PA ausdrücken, was zum 2. Unvollständigkeitssatz führt).

Bem.:

- Das Richard Paradoxon deutet schon die Tarskische Unbeweisbarkeit der Wahrheit an: Es gibt kein Prädikat $\mathcal{W}$ mit $\mathcal{W}(\ulcorner\phi\urcorner) \leftrightarrow \phi$. Für die first order Logik werden wir das später beweisen.
- Wir werden uns mit "first order" Logik beschäftigen. Diese ist i.A. nicht nur theoretisch (wie oben angedeutet) sondern auch praktisch eine dramatische Einschränkung: Die Sprache der first order Gruppentheorie, $(\circ, ^{-1})$, beinhaltet fast gar nichts von Interesse aus der Gruppentheorie: Man kann nicht ausdrücken "die Gruppe (=das Universum) ist einfach" etc (und nicht einmal "die Gruppe (=das Universum) ist endlich").
- In der Praxis "stark genug" ist allerdings die first order Sprache der Zahlentheorie, $(0, 1, +, \times, <)$: Fast alle elementaren Sätze der Zahlentheorie lassen sich da ausdrücken (z.B.: Es gibt in unendlich viele Primzahlenzwillinge, in der Form von: Es gibt beliebig große Primzahlenzwillinge!)
- Später werden wir sehen dass die first order Sprache der Mengenlehre sehr wohl eine für praktische Belange universelle Sprache ist. (Aber der Undefinierbarkeit der Wahrheit / dem Richard Paradoxon kann man natürlich nicht entgehen.)

(3) Wir beschäftigen uns wie schon gesagt mit **first Order Logik**. Im weiteren wiederholen wir die Begriffe und Grund-Tatsachen (Ziegler 1-4). Zuerst ein paar **Synonyme:** (Z..Bezeichnungen aus Ziegler)

- Signatur = (Z) Sprache
- Symbol = (Z) Zeichen
- Atomformel = atomare Formel = (Z) Primformel
- Satz = (Z) Aussage, d.h. Formel ohne freie Variable
- konsistent = (Z) widerspruchsfrei

Später (im Kapitel 4) kommen dann noch dazu:

- (für Satzmengen) r.e. = (Z) axiomatisierbar
- PA = (Z) P, Peano Arithmetik
- PRA: primitiv rekursive Arithmetik
- (in PA) beweisbar totale Funktion = (Z) in L_1^P definierbare Funktion

(4) **Syntax:** Signatur=Sprache beinhaltet Konstanten- Funktions und Relations-symbole/Zeichen. Damit definiert man Term, Formel, Satz(=Aussage), (freie/gebundene) Variable.

Wir werden im Weiteren informelle Abkürzungen bzw Umschreibungen für Formeln verwenden (wie es ja auch im Ziegler gemacht wird).

(5) Es gibt zwei wichtige Fälle:
- **finitäre Fall:** Die Signatur ist endlich (oder unendlich aber "rekursiv repräsentiert", d.h. wie in Ziegler 14 gödelisiert)
- **allgemeiner Fall:** Die Signatur kann beliebig groß sein (auch überabzählbar) sein.

Der finitäre Fall ist für die mathematischen Grundlagen besonders wichtig: Statt über (unendliche, unklare) mathematische Strukturen zu sprechen, kann man endliche Zeichenketten verwenden und über Ableitungen solcher endlichen Zeichenketten sprechen. Das ergibt selbst für "Finitisten" Sinn, die die Existenz/die Sinnhaftigkeit der beschriebenen mathematischen Strukturen ablehnen. Für Finitisten ist also der finitäre Fall der Syntax und das Ableitungskalkül sinnvoll (aber i.A. nicht die Semantik; und auch nicht der allgemeine Fall der Syntax).

Im Ziegler wird der Vollständigkeitssatz für den finitären Fall bewiesen, er läßt sich aber auch für den allgemeinen Fall (mit minimalen Änderungen) beweisen.

(6) **Semantik:** Bringt die mathematischen Objekte in Bezug auf die formale Sprache.
- Wir definieren L-Struktur, Belegung, und Gültigkeit bezüglich einer Belegung $\mathcal{M} \vDash \phi[\beta]$. Wir zeige dass die Belegung nur relevant ist auf den Variablen die in ϕ frei vorkommen.
- Insbesondere: Ist ϕ Satz dann hängt die Gültigkeit nicht von β ab, und wir schreiben $\mathcal{M} \vDash \phi$.
- Notation: Wenn ϕ kein Satz ist, schreiben wir oft $\phi(x_1, \dots, x_n)$ um anzudeuten dass die freien Variablen von ϕ Teilmenge von $\{x_1, \dots, x_n\}$ sind; und statt $\mathcal{M} \vDash \phi[\beta]$ schreiben wir dann $M \vDash \phi(m_1, \dots, m_n)$ oder $M \vDash \phi[m_1, \dots, m_n]$, wobei $m_i = \beta(x_i)$.
- Notation: Wir unterscheiden üblicherweise notationell nicht zwischen Struktur $\mathcal{M} = (M, \dots)$ und Grundmenge M. (Ähnlich: die Gruppe $\mathbb{Q}$ wird ja oft als $\mathbb{Q}$ bezeichnet statt als $(\mathbb{Q}, +)$ etc.).
- Für eine Satzmenge T schreiben wir $\mathcal{M} \vDash T$ wenn $\mathcal{M} \vDash \phi$ für all $\phi \in T$. Wenn $\mathcal{M} \vDash T$, dann sagen wir auch $\mathcal{M}$ ist ein Modell von T.
  Bsp: Modelle der Gruppen Axiome sind genau die Gruppen.
- Bemerkung: Wir können also auf diese Weise eine Art "unendliche Konjunktion" ausdrücken; aber keine "unendliche Disjunktion". Die Aussage $\mathcal{M} \nvDash T$ ist im Allgemeinen nicht äquivalent zu $\mathcal{M} \vDash S$ für irgendein S. Um Gegensatz dazu ist natürlich $\mathcal{M} \nvDash \phi$ äquivalent zu $\mathcal{M} \vDash \neg\phi$.
  Klassisches Beispiel: Sei ϕ_n^* der Satz der besagt dass das Universum mindestens n Elemente hat: $\exists x_1, \dots, x_n : x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \dots \wedge x_{n-1} \neq x_n$.
  Sei T_∞ die Menge $\{\phi_1^*, \phi_2^*, \dots\}$. Dann besagt T_∞ dass das Universum unendlich ist (d.h.: $\mathcal{M} \vDash T_\infty$ gdw M unendlich). Es gibt aber keine Satzmenge S die besagt dass das Universum endlich ist (d.h.: $\mathcal{M} \vDash S$ gdw M endlich). Das ist eine Folgerung des Kompaktheitssatzes, siehe unten.
- Die Gültigkeit führt zum wichtigen Begriff der semantischen Folgerung: $T \vDash \phi$ heißt: $\mathcal{M} \vDash T$ impliziert $\mathcal{M} \vDash \phi$.
  Bsp: Gruppen Axiome $\vDash \phi$ heißt per Definition: ϕ gilt in allen Gruppen.
- T (bzw. ϕ) heißt erfüllbar, wenn es ein T-Modell gibt (bzw: ein $\{\phi\}$-Modell), sonst unerfüllbar. ϕ heißt allgemeingültig wenn T in jedem Modell gilt (d.h., wenn $\emptyset \vDash \phi$.)

(7) **Ableitungskalkül**.
- Ein Beweis (ohne nichtlogische Axiome) ist eine endliche Folge von Formeln, so dass jede Formel entweder ein logisches Axiom ist (Ziegler: B1-B3) oder sich aus Modus Ponens oder $\exists$-Einführung aus vorherigen Formeln ergibt (B4-B5).
- Eine Formel ϕ die in einem Beweis vorkommt heißt beweisbar, wir schreiben auch $\vdash \phi$.

- Die Beweisbarkeit aus einer Axiomenmenge (=Menge von Formeln) T kann man auf zwei Arten definieren:
  Version1 (Wie Ziegler Seite 20): $T \vdash \phi$ heißt: Es gibt $\psi_1, \dots, \psi_n$ aus T so dass $\vdash [(\psi_1 \wedge \dots \wedge \psi_n) \to \phi]$.
  Üblichere Version2: Ein "Beweis mit T als Axiomen" ist eine endliche Folge $s = (\phi_0, \dots, \phi_n)$ von Formeln in der jeder Eintrag ϕ_ℓ entweder logisches Axiom ist (B1–B3), oder $\phi_\ell \in T$ ("nichtlogisches Axiom") oder ϕ_ℓ geht aus vorhergehenden Elementen der Folge durch B4 oder B5 hervor. Dann wird $T \vdash \phi$ definiert als: Es gibt einen Beweis von ϕ mit T als Axiomen.
  Version1 und Version2 sind äquivalent. Ziegler benötigt das im Abschnitt 19, siehe Lemma 19.1. Beweis: Übung.
- Die drei wichtigen Eigenschaften des Kalküls sind:
  - Korrektheit: Nur allgemeingültige Sätze werden abgeleitet, $\vdash \varphi \to \vDash \varphi$; bzw. für eine Axiomenmenge T: $T \vdash \varphi \to T \vDash \varphi$.
  - Vollständigkeit: Alle allgemeingültigen Sätze werden abgeleitet: $\vDash \varphi \to \vdash \varphi$; bzw. für eine Axiomenmenge T: $T \vDash \varphi \to T \vdash \varphi$. (Siehe weiter unten.)
  - Im finitären Fall: Der Kalkül ist "mechanistisch". Genauer werden wir später sehen: Wenn T r.e. ist, dann ist $\{\varphi : T \vdash \varphi\}$ auch r.e.
- T heißt inkonsistent, wenn $T \vdash (\forall x\, x \neq x)$. (Äquivalent (Übung): wenn für alle ϕ gilt $T \vdash \phi$.)
  Im weiteren werden wir bei manchen Sätzen vielleicht manchmal vergessen zu erwähnen dass wir voraussetzen dass T konsistent ist.
- Wir werden später verwenden:
  (*) T ist konsistent genau dann wenn jede endliche Teilmenge von T konsistent ist.
  Beweis: Wenn T inkonsistent ist, dann gibt es einen T-Beweis eines Widerspruchs. Dieser Beweis verwendet aber nur endlich viele Formeln $\psi_1, \dots, \psi_n$ aus T. Sei $T' := \{\psi_1, \dots, \psi_n\}$. Dann ist T' eine endliche, inkonsistente Teilmenge von T.
- T heißt vollständig, wenn (T konsistent ist und) für jeden Satz ϕ gilt: $T \vdash \phi$ oder $T \vdash \neg\phi$.

(8) **Vollständigkeitssatz** $T \vdash \phi$ gdw $T \vDash \phi$. (Gilt nicht nur für den finitären Fall, sondern auch für den allgemeinen.)

- Intuitiv gesprochen: In Wirklichkeit interessiert man sich in der Mathematik für die Frage $\mathbb{N} \vDash \phi$. Diese Frage ist schwierig (und allenfalls auch "philosophisch" problematisch). Stattdessen kann man sich auf Axiome, zB PA, einigen, von denen man annimmt dass sie in $\mathbb{N}$ gelten. Nun kann man stattdessen fragen ob PA$\vDash \phi$ gilt. Auf den ersten Blick ist diese Frage noch viel komplizierte als $\mathbb{N} \vDash \phi$, weil man ja $\mathcal{M} \vDash \phi$ für alle PA-Strukturen $\mathcal{M}$ entscheiden/untersuchen muss, nicht nur für $\mathbb{N}$. Durch den Vollständigkeitssatz stellt sich aber heraus dass PA$\vDash \phi$ äquivalent zur "mechanischen" (r.e.) Frage PA$\vdash \phi$ ist.
- Man kann leicht zeigen dass folgende Aussage "äquivalent" ist zum Vollständigkeitssatz:
  Jede konsistente Theorie hat ein Modell.
  Diese Aussage wiederum zeigt man so:
  (a) Erweitere die konsistente L-Theorie T zu einer konsistenten $L \cup C$-Theorie T^+ die eine Henkintheorie ist.
  Der finitäre Fall ist im Ziegler bewiesen. Der Allgemeine Fall geht genauso, nur wird für überabzählbare Signatur L die Konstantenmenge C nicht mehr abzählbar sein sondern so groß wie L.
  (b) Vervollständige (bei gleicher Signatur $L \cup C$) die Theorie T^+ zu einer (immer noch konsistenten) Theorie T^*, die dann klarerweise immer noch eine Henkintheorie ist.

Der finitäre Fall ist im Ziegler bewiesen. (Bemerkung: Auch dieser Fall ist nicht "konstruktiv" im Sinne von rekursiv, weil nicht entscheidbar ist ob $T \vdash \varphi$ gilt oder nicht.)
Für den allgemeinen Fall braucht man erst mal das Auswahlaxiom, um alle Formeln der Signatur $L \cup C$ als $(\varphi_i : i \in \alpha)$ wohlzuordnen. Und satt der Induktion über $\mathbb{N}$ wie im finitären Fall muss man eine transfinite Induktion über α durchführen. Sonst ist der Beweis gleich.

(c) Zeige: Wenn T^* eine vollständige (konsistente) Henkintheorie ist, dann gibt es ein kanonisches "Termmodell" $\mathbb{M}$ von T^*: Das Universum M besteht aus den Äquivalenzklassen $[c]$ der Konstantensymbole, wobei c und d äquivalent sind wenn $c = d \in T^*$. Die Interpretation der Konstanten-, Funktions und Relationssymbole ist kanonisch.

(9) **Folgerungen**

- **Kompaktheitssatz:** Wenn jede endliche Teilmenge von T ein Modell hat, dann auch T.
  Beweis: "T ist erfüllbar" gdw (V.S.) "T ist konsistent" gdw (*) "jede endl TM von T ist konsistent" gdw (V.S.) "jede endl TM von T ist erfüllbar".
  Dabei verwenden wir den V.S. in der Form: erfüllbar ist dasselbe wie konsistent; und (*) aus Punkt 7.
- Das impliziert im weiteren dass first order alles mögliche nicht ausdrücken kann. Z.B.:
  - Es gibt keine Satzmenge S die Endlichkeit ausdrückt; d.h.: $\mathcal{M} \models S$ gdw $\mathcal{M}$ endlich.
    Beweis: Oben ist ϕ_n^* und T_∞ definiert. Sei S eine Satzmenge so dass es beliebig große endliche Modelle von S gibt. Sei $T := S \cup T_\infty$. Jede endliche Teilmenge von T ist also erfüllbar; damit ist auch T erfüllbar, d.h., S hat ein unendliches Modell.
  - Folgerung: "Das Universum ist unendlich" lässt sich zwar mit der Satzmenge T_∞, aber nicht mit endliche vielen Sätzen $\psi_1, \ldots, \psi_n$ ausdrücken.
    Beweis: Sonst würde ja $\neg(\psi_1 \wedge \cdots \wedge \psi_n)$ Endlichkeit ausdrücken.
  - Analog: "Das Universum ist eine endliche Gruppe" lässt sich mit einer unendlichen, aber nicht mit einer endlichen Satzmenge ausdrücken. "Das Universum ist eine endliche Gruppe" lässt sich gar nicht ausdrücken. (Das gilt nicht nur für Gruppen, sondern für jede Klasse von Strukturen die first order definierbar ist und beliebig große endliche Vertreter hat; z.B. Ringe, Körper, Ordnungen, etc)
  - Bemerkung: "Das Universum ist eine lineare Ordnung ohne Endpunkt" ist natürlich auch first order definierbar und hat nur unendliche Modelle; dasselbe gilt für PA, dichte lineare Ordnungen und hunderte weitere natürliche mathematische Satzmengen/Axiomensystemen. Genauso hat die (nicht sehr interessante) Satzmenge $\forall x, y : x = y$ bis auf Isomorphie nur ein Modell (mit einem Element).
- **Skolem Löwenheim:** Sei X eine beliebige unendliche Menge die zumindest so groß ist wie die Sprache L_0, und T_0 eine L_0-Theorie die ein unendliches Modell hat. Dann hat T_0 ein Modell mit genau soviel Elementen wie X.
  Beweis: Sei L die Sprache die entsteht wenn zu L_0 ein neues Konstantensymbol c_x für jedes $x \in X$ dazu fügt. Sei T die L-Theorie $T \cup \{c_x \neq c_y : x \neq y \in X\}$.
  Betrachte den Beweis des Vollständigkeitssatzes:
  Im Schritt 1 ist die Menge C genauso groß wie X. (Grund: Es gibt genauso viele L-Formeln (=endliche Zeichenfolgen) wie X, daher ist C_1 so groß wie X. Damit gibt es aber auch genauso viele $L \cup C_1$-Formeln wie X, d.h., C_2 ist so groß wie X. Damit ist aber auch $C := \bigcup_{i \in \mathbb{N}} C_i$ so groß wie X.)
  In Schritt 3 wird dann ein Modell konstruiert das höchstens so groß ist wie C, d.h. wie X. Weil aber in diesem Modell $c_x \neq c_y$ gilt für alle $x \neq y \in X$, ist die Größe genau die von X.

- **Folgerung:** Wenn L endlich oder abzählbar ist und T eine L-Theorie ist die ein unendliches Modell hat, dann hat T ein abzählbar unendliches Modell.
- **Folgerung:** Zu jeder Theorie T mit einem unendlichen Modell gibt es ein dazu nichtisomorphes Modell.
  Beweis: Sei $\mathbb{M}$ ein unendliches T-Modell, und X größer als $\mathbb{M}$ (X könnte z.B. die Potentzmenge von $\mathbb{M}$ sein). Dann gibt es ein Modell der Größe X, das daher nicht isomorph zu $\mathcal{M}$ sein kann.
- **Nonstandard Modelle:** Sei $L = (0, 1, +, \times, <)$, und sei T die Menge der Sätze die in $\mathbb{N}$ gelten. (Insbesondere ist also T konsistent und vollständig, und $\mathbb{N}$ ist ein abzählbares T-Modell.) Es gibt ein abzählbares T-Modell $\mathcal{M}$ das nicht isomorph zu $\mathbb{N}$ ist.
  Beweis: Sei $L' := L \cup \{c\}$ und $T' := T \cup \{1 < c, 1+1 < c, \dots\}$. Jede endliche Teilmenge von T ist erfüllbar (weil ja $\mathbb{N}$ mit geeigneter Interpretation von c ein Modell ist); daher ist T erfüllbar und hat nach Skolem-Löwenheim ein abzählbares Modell $\mathcal{M}$. Dieses Modell kann nicht isomorph zu $\mathbb{N}$ sein: Nehmen wir an $f : \mathcal{M} \to \mathbb{N}$ sei ein Isomorphismus. Sei $n := f(c^{\mathcal{M}})$. Es gilt also $1 + \dots + 1 = f(c^{\mathcal{M}})$ (n Einser), und daher ist $1^{\mathcal{M}} + \dots + 1^{\mathcal{M}} = c$. Das ist ein Widerspruch zu $1 + \dots + 1 < C \in T'$.

2. Kurzwiederholung Rekursionstheorie

(10) **Haupt-Erkenntnis:** Alle "vernünftigen" Computermodelle sind äquivalent.
Ein Computer hat:
- endliches (aber beliebig langes) Programm
  Bemerkung: Mit unendlich langen Programmen könnte man trivialerweise jede Funktion berechnen (unendliche Fallunterscheidung), dieser Begriff der Berechenbarkeit wäre nicht sinnvoll.
- Es steht potentiell unendlich viel Speicher und potentiell unendlich lange Zeit für eine Berechnung zur Verfügung (aber eine konkrete, erfolgreiche Berechnung verwendet immer nur endlich viel Speicher und endet nach endlicher Zeit).

Ziegler verwendet **Registermaschinen** als Computermodell (definiert auf Seite 60 und 61).

Jedes Computermodell führt zu einer Definition der Berechenbarkeit: Eine partielle Funktion $f : \mathbb{N}^n \to \mathbb{N}$ ist **berechenbar**, wenn es ein Programm $\mathcal{M}$ gibt dass f entspricht, d.h., $f = F^n_{\mathcal{M}}$ in der Notation Ziegler Seite 61. Insbesondere: f ist auf $\bar{x}$ definiert genau dann wenn die Maschine(=das Programm) $\mathcal{M}$ auf Input $\bar{x}$ terminiert (=hält).

Wie gesagt verwendet Ziegler Registermaschinen. Äquivalente Modelle sind die folgenden (d.h. sie führen zum selben Begriff der Berechenbarkeit. Manchmal werden sie auch "Turing-vollständig" genannt). Turingmaschinen, C++, Basic, Perl, Javascript, Java, Python, Prolog, List, und, für uns wichtiger, rekursive Funktionen.

(Bemerkung: Natürlich gibt es auch schwächere Modelle, zB endliche Automaten oder reguläre Grammatiken / regular expressions etc; oder (für uns wichtiger) die primitiv rekursiven Funktionen.)

(11) Wie schon erwähnt, es gibt auch eine andere Definition, die kein Computermodell verwendet: **rekursiv** (äquivalent zu berechenbar). Bei Ziegler siehe Seite 61,62. Ziegler definiert das nur für totale Funktionen, siehe aber die folgende Übung. Eine Teilmenge davon sind die **primitiv rekursiven** Funktionen (diese sind immer total).

Übung: Modifizieren Sie die Definitionen so, dass sie auch (sinnvoll!) für partielle Funktionen funktionieren. Die derart definierten Funktionen heißen auch **partiell rekursiv**. Eine weitere Übung: Beweise dass partiell rekursiv = berechenbar. (Verwende natürlich den Normalformensatz.)

(12) Ein ganz wesentlicher Punkt (allgemein in der math. Logik) ist die **Kodierung**: Ein Programm (=Source Code) ist eine Zeichenkette bzw eine endliche Folge von Befehlen. (Und es gibt nur endlich viele verschiedene Befehle). So ein source code entspricht auf

kanonischer Weise einer natürlichen Zahl (bei uns: Gödelisierung von Registermaschinen, Seite 69). Wir ordnen also jedem Programm $\mathcal{M}$ eine Gödelnummer $\ulcorner\mathcal{M}\urcorner \in \mathbb{N}$ zu.

Eine triviale Folgerung: Es gibt nur abzählbar viele berechenbare Funktionen. (Aber überabzählbar viele beliebige Funktionen, also muss es nicht-berechenbare Funktionen geben).

(13) Weitere **Haupt-Erkenntnis:** Es gibt ein universelles Programm $\mathcal{U}$, d.h., ein Programm das auf Input $(\ulcorner\mathcal{M}\urcorner, x)$ genau den output liefert den das Programm $\mathcal{M}$ auf Input x liefert (insbesondere: genau dann hält wenn das simulierte Programm hält). In anderen Worten: $F^2_{\mathcal{U}}(\ulcorner\mathcal{M}\urcorner, x) = F^1_{\mathcal{M}}(x)$.

Der Vollständigkeit halber: Das funktioniert natürlich auch für andere Input-Dimensionen: Es gibt für jede natürliche Zahl n ein universelles Programm $\mathcal{U}^n$, d.h., ein Programm das auf Input $(\ulcorner\mathcal{M}\urcorner, x_1, \ldots, x_n)$ genau den output liefert den das Programm $\mathcal{M}$ auf Input $(x_1, \ldots, x_n)$ liefert (insbesondere: genau dann hält wenn das simulierte Programm hält).

Im Ziegler ist das etwas versteckt, auf Seite 71:

$$\mathcal{U}(y, x_1, \ldots, x_n) := (\mu g\ T_n(y, x_1, \ldots, x_n, g))_0.$$

Die obige Behauptung ist dann genau Zieglers Formel (1).

Im Computeralltag entspricht ein universelles Programm einfach einem **Interpreter**: ein Programm, das einen beliebigen Sourcecode P und einen Inputwert x als Input nimmt, und als output $P(x)$ liefert.

Die wesentliche Eigenschaft die im Beweis verwendet wird: Die Eigenschaft *Das Programm m hält auf Input x nach t schritten mit output y* ist primitiv rekursiv (und entspricht in etwa der Funktion T_n auf Seite 71, wobei $t = (g)_1$ und $y = (g)_0$).

(14) Folgerungen der Existenz eines Universellen Programms:

- Unlösbarkeit des **Halteproblems**: Man kann kein Computerprogramm schreiben dass entscheidet ob das Programm $\mathcal{M}$ auf Input $\ulcorner\mathcal{M}\urcorner$ hält oder nicht. Definiere $\mathcal{H} := \{m : \mathcal{U}(m, m) \text{ ist definiert}\}$. Die Aussage ist also: $\mathcal{H}$ ist nicht rekursiv.
  Beweis: Versuche durch Diagonalisierung die Abzählbarkeit der berechenbaren Funktionen zu widerlegen. Durch das universelle Programm kann man diese Funktionen als $f_n = \mathcal{U}(n, \cdot)$ aufzählen, und effektiv die Funktion $g(n) = f_n(n)+1$ definieren (d.h., g ist berechenbar).
  Das ist soweit kein Widerspruch, da ja die f_n nur partielle Funktionen sind. (Es gilt also $g = f_m$, und $f_m(m) = g_m(m) = f_m(m) + 1$ sagt eben nur dass g auf input m nicht definiert ist. Kein Widerspruch.)
  Wäre aber Halteproblem rekursiv lösbar, könnte man mit einer Fallunterscheidung die rekursive Funktion g' definieren durch: $g'(n) = g(n)$ falls $g(n)$ hält und 0 sonst. Man kann leicht überprüfen dass dieses g' nun tatsächlich ein widersprüchlich ist.
- Die Notwendigkeit partieller Funktionen: man kann "Endlosschleifen" oder dergl nicht durch kluge Konzeption einer Programmiersprache vermeiden: Sonst wäre die obige Funktion g total und damit tatsächlich ein Widerspruch.
  Etwas formaler: Es kann keine "totale universelle Funktion" geben, d.h. eine rekursive, totale, zweistellige Funktion $\mathcal{U}^t$ so dass es für jede totale rekursive einstellige Funktion f einen Code m gibt mit $f(x) = \mathcal{U}^t(m, x)$ für alle x. Warum? Sonst konstruiere g wie oben, Widerspruch.

(15) Noch ein Wort zur **Kodierung** Wir haben uns in der Untersuchung auf Funktionen von $\mathbb{N}^n$ nach $\mathbb{N}$ beschränkt. Eine wichtige Erkenntnis: äquivalenter weise kann man endliche Zeichenketten, beliebig lange endliche Tupel von natürlichen Zahlen, rationale Zahlen etc verwenden (wobei man jeweils "vernünftige" Injektionen auf $\mathbb{N}$ verwendet, so genannte Kodierungen). Als Beispiel haben wir ja bereits gesehen dass man Source-Codes selbst als Inputs verwenden kann. (Ziegler: Gödelisierung von Registermaschinen, S 69). Später werden wir auch prädikatenlogische Formeln kodieren (Ziegler 14). Aber es gibt auch viele andere Beispiele von mathematischen Objekten, die man in natürlicher/kanonischer Weise als Zahlen kodieren kann und für die man daher einen natürlichen Begriff der (algorithmischen) Berechenbarkeit bzw. der (algorithmischen) Entscheidbarkeit hat.

Beispiele:

- Ganze Zahlen $\mathbb{Z}$, rationale Zahlen $\mathbb{Q}$. Natürlich ist dann zB Division in $\mathbb{Q}$ berechenbar etc.
- Polynome (in beliebig vielen Variablen) über $\mathbb{Z}$ oder $\mathbb{Q}$.
  Bemerkung: Man kann zeigen: Es ist entscheidbar ob ganzzahlige Polynome in einer Variable ganzzahlige Nullstellen haben (leicht). Es ist nicht entscheidbar ob ganzzahlige Polynome in 9 Variablen ganzzahlige Nullstellen haben. Das ist ein schwieriges Resultat (allgemeine Diophanitsche Gleichung, 10. Hilbertsches Problem, Satz von matijasevitch).
- Wörter (=Zeichenketten) in Gruppen mit abzählbar vielen Erzeugern. Bemerkung: Man kann zeigen: Es gibt eine Gruppe G die durch endlich viele Erzeuger und endlich viele Äquivalenzrelationen definiert ist und für die es keinen Algorithmus gibt der für ein Wort w entscheidet ob $w = e$ oder nicht. (Wortproblem in Gruppen).
- Wir haben schon erwähnt dass man first order Sätze ebenfalls kodieren kann. Zur Sprache $(+, \times, 0, 1, <)$ kann man zeigen: Es ist entscheidbar ob ein Satz ϕ dieser Sprache in $\mathbb{R}$ gilt oder nicht (Tarksi, quantorenelimination in reell abgeschlossenen Körpern). Es ist aber nicht entscheidbar ob ein Satz ϕ dieser Sprache in $\mathbb{N}$ gilt oder nicht (Unvollständigkeitssatz).
- Bemerkung: Viele weniger klar ist es wie man Begriffe der Berechenbarkeit über reelle Zahlen definieren kann.

Bemerkung (nicht notwendig zum Verständnis des Stoffes): Egal welche "vernünftige" Kodierung man verwendet, man kommt zum selben Begriff der Berechenbarkeit. Man kann aber natürlich auch unvernünftige Kodierungen definieren. Zum Beispiel: In Ziegler haben wir die "vernünftige" Kodierung $\mathcal{M} \mapsto \ulcorner \mathcal{M} \urcorner$ definiert. Sei nun $\phi(\mathcal{M})$ gleich $2^{\ulcorner \mathcal{M} \urcorner}$ falls $\mathcal{M} \in \mathcal{H}$ (der Haltemenge), und gleich $1 + 2^{\ulcorner \mathcal{M} \urcorner}$ sonst. Diese Kodierung ist nicht "vernünftig": Man sieht dem Code sofort an ob $\mathcal{M}$ auf Input $\ulcorner \mathcal{M} \urcorner$ hält oder nicht, d.h. in Bezug auf diese Kodierung ist das Halteproblem entscheidbar. (Und man sieht der Zieglerschen Definition der Kodierung sofort an dass sie "maschinell durchführbar" ist, die Kodierung ϕ aber nicht. Diese Aussage ist aber nur intuitiv und hat keinen formal exakten Inhalt, weil wir ja "maschinell durchführbar" eben offiziell nur für Funktionen von $\mathbb{N}^n$ nach $\mathbb{N}$ definiert haben.)

(16) Für Teilmengen A von $\mathbb{N}$ haben wir definiert: A ist rekursiv gdw die charakteristische Funktion (die ja total ist) rekursiv ist. Wir können auch χ'_A definieren als: $\chi'_A(n) = 0$ wenn $n \in A$ und undefiniert sonst. Dann gilt (**Übung**):

Die Folgenden sind äquivalent (und definieren "A ist r.e."):

(a) χ'_A ist partiell rekursiv.
(b) A ist der Definitionsbereich einer partiell rekursiven Funktion.
(c) A ist der Bildbereich einer partiell rekursiven Funktion.
(d) A ist leer oder der Bildbereich einer totalen rekursiven Funktion. (Ziegler Lem 13.1)
(e) A ist die Projektion einer rekursiven Teilmenge B von $\mathbb{N}^2$. (Das ist die offizielle Definition in Ziegler).
(f) A ist die Projektion einer primitiv rekursiven Teilmenge B von $\mathbb{N}^2$. (Hinweis: Normalformensatz.)

Die ersten beiden sagen: Es gibt ein Computerprogramm dass A "halb" entscheidet: Wenn $n \in A$ dann kann das Programm das beweisen, aber wenn nicht dann hält das Programm nicht. Die nächsten beiden besagen: Es gibt ein "unendlich lang laufendes Computerprogramm" das nach und nach genau die Elemente von A ausgibt/generiert.

Ziegler Lemma 13.5 ist wichtig (und intuitiv leicht einzusehen).

3. Ergänzungen Ziegler Kapitel 4

(17) Achtung: Q* besteht nicht nur (wie in Ziegler nach 17.1 auf Seite 80 angegeben) aus Q*1 - Q*3, sondern zusätzlich aus Q5.

(Wenn man will kann man Q5 aber auch als Fall $a = 0$ von Q*3 auffassen.)

(18) Bemerkung: Peano Arithmetik (bei Ziegler P genannt) wird oft auch mit PA bezeichnet. Die primitiv rekursive Arithmetik (Ziegler S 89) wird oft PRA genannt.

(19) Historische Bemerkung: Das ursprüngliche "Robinson's Q", das auch heute in vielen Lehrbüchern verwendet wird (und die unendliche Teiltheorie S) unterscheidet sich deutlich von Ziegler's (schwächerem) Q (und unendliche Teiltheorie Q^*). Für Ziegler's Version funktioniert aber alles ganz genauso (dafür braucht man den seltsamen Trick mit γ auf Seite 83; das kommt bei Robinson nicht vor).

(20) Eine "schwache" Grundform des (ersten) Gödelschen Unvollständigkeitssatzes ist:

Th($\mathbb{N}$) ist unentscheidbar,

oder äquivalent:

Es gibt keine r.e. (="axiomatisierbare" in Ziegler Notation) und vollständige Axiomatisierung von Th($\mathbb{N}$).

Im Kapitel 4 wird eine Reihe von verschiedenen Verallgemeinerungen bewiesen:

- (Abschnitt 16) Satz: Sei T eine Axiomenmenge die wahr ist, d.h., $T \subseteq \mathrm{Th}(\mathbb{N})$. Wenn T auch nur arithmetisch ist (viel schwächer als r.e.), dann ist T unvollständig.
- (Abschnitt 17): Es wird die (sehr schwache) endliche Theorie Q eingeführt.
  Satz: Wenn $T \cup$Q konsistent ist, dann ist (die Menge der Folgerungen aus) T unentscheidbar.
- Folgerung1: Wenn T r.e. und mit Q konsistent ist, dann ist T unvollständig (sonst wäre T ja entscheidbar).
  (Das ist "stärker" als der Satz aus Abschnitt 16, weil wir nicht "wahr" voraussetzen, aber "viel schwächer" weil wir r.e. statt arithmetisch voraussetzen.)
- Folgerung2: Die leere Theorie (die klarerweise mit Q konsistent ist) ist unentscheidbar. Die (r.e.) Menge $\{\phi : \vdash \phi\}$ ist also nicht rekursiv.
  Allgemeiner gilt (ohne Beweis, Beweis ist relativ einfach): Wenn die Signatur L (mindestens) ein (mindestens) zweistelliges Relationssymbol enthält, dann ist die Menge der allgemeingültigen L-Sätze nicht rekursiv.
- (Abschnitt 18): Es wird die viel stärkere Theorie PA (bei Ziegler: P) eingeführt (in der sich übrigens die allermeisten zahlentheoretischen Resultate beweisen lassen).
  Satz: Seit T r.e. und kompatibel mit PA. Dann ist "$T \vdash \phi$" und damit auch "Con(T)" first order in L_N formulierbar, aber $T \nvdash$Con(T) (vorausgesetzt T ist konsistent). Das ist der wichtige 2. Unvollständigkeitssatz, 19.4.

(21) Für den Beweis des 2. Unvollständigkeitssatzes wird das Diagonal-Lemma 17.8 bewiesen, aus dem noch ein zweites wichtiges Resultat folgt (Tarskis Undefinierbarkeit der Wahrheit, analog zu Folgerung 10.3):

- Sei T kompatibel mit Q (oder auch nur mit Q^*). Es gibt kein $W(x)$ so dass für alle Sätze ϕ gilt: $T \vdash W(\ulcorner\phi\urcorner) \leftrightarrow \phi$.
- Insbesondere gibt es kein $W(x)$ so dass für alle Sätze ϕ gilt: $\mathbb{N} \vDash W(\ulcorner\phi\urcorner) \leftrightarrow \phi$.

Beweis: Sei $W(x)$ gegeben. Wende den Fixpunktsatz 17.8 auf $\neg W(x)$ an. Das liefert ein ϕ mit $T \cup Q^* \vdash \phi \leftrightarrow \neg W(\ulcorner\phi\urcorner)$. Wenn also $T \vdash W(\ulcorner\phi\urcorner) \leftrightarrow \phi$, dann ist $T \cup Q^*$ inkonsistent.

(22) Ebenfalls wichtig ist Lemma 19.2: Es gibt eine Σ_1 Formel die ein Wahrheitsprädikat für Σ_1-Sätze ist.

Analog dazu (ohne Beweis): Es gibt eine Σ_n Formel die ein Wahrheitsprädikat für Σ_n-Sätze ist. Man kann auch leicht eine second-order Formel angeben die ein Wahrheitsprädikat für first order Formeln ist. Dieser Effekt wird sich auch in der Mengenlehre finden: Es gibt kein Wahrheitsprädikat; aber es gibt ein Σ_n-Wahrheitsprädikat für Σ_n-Formeln. Und in der Mengenlehre lässt sich "arithmetische Wahrheit" natürlich schon definieren...

(23) In Kapitel 4 werden verschiedene Begriffe der "definierbaren Funktion" verwendet. Die Unterschiede sind technisch wichtig (aber teilweise etwas subtile):

- Abschnitt 16: Definierbar.
  Eine Funktion f ist arithmetisch definierbar, wenn $x = f(y)$ (in $\mathbb{N}$) äquivalent ist zu einer Σ_1 Formel $\phi_f(y, x)$.
  Satz 17.3: Die rekursiven Funktionen sind (genau die) Σ_1-definierbar(en).

- Abschnitt 17: Repräsentierbar.
  Es wird gezeigt dass alle wahren Σ_1-Sätze in Q beweisbar sind. Wenn also f Σ_1-definierbar ist, dann gilt für alle a: $b = f(a)$ gdw $\mathrm{Q}^* \vdash \phi_f(b, a)$. Es gilt aber mehr: f ist in Q^* sogar (durch eine leicht andere Σ_1 Formel) repräsentierbar, d.h. zusätzlich gilt für alle a: $\mathrm{Q}^* \vdash \exists! y \phi_f(y, a)$. (Daraus folgt dann auch $\mathrm{Q}^* \vdash \neg\phi_f(c, a)$ für $c \neq f(a)$; aber Repräsentierbarkeit ist stärker als das: Für jedes (fixe, "standard") a gibt es beweisbar kein y außer $f(a)$ (auch kein nichtstandard-Element).
  Jede rekursive Funktion ist also in Q^* repräsentierbar.
- Abschnitt 18: Beweisbar total.
  Eine Funktion f sei durch die Formel $\phi(y, x)$ definiert. Dann ist f beweisbar total (in PA), wenn $\mathrm{PA} \vdash \forall x \exists! y \phi_f(y, x)$ (und zusätzlich $\mathrm{PA} \vdash \phi_f(f(a), a)$ für alle a, was im Fall einer Σ_1-Definition ϕ sowieso immer gilt).
  Ziegler nennt diese beweisbar totalen Funktionen "durch eine Σ_1^P-Funktion definierbar".
  Satz 18.3: Jede primitiv rekursive Funktion ist beweisbar total.
- Es ist nicht jede rekursive Funktion beweisbar total! Die Übung auf Seite 89 gibt ein Beispiel.

(24) Eine Bemerkung/Übung in Zushg mit obiger Folgerung2 (nicht LVA-Stoff): Folgerung2 besagt ja dass "ϕ ist allgemeingültig" r.e. aber nicht rekursiv ist; analog ist "ϕ ist unerfüllbar" r.e. aber nicht rekursiv (warum?); und "ϕ ist erfüllbar" ist nicht einmal r.e. (warum?).

Wir können nun definieren: "ϕ ist endlich allgemeingültig" heißt: ϕ gilt in jeder endlichen Struktur; "ϕ ist endlich erfüllbar" heißt: ϕ gilt in einer endlichen Struktur; und "ϕ ist endlich unerfüllbar" heißt: ϕ gilt in keiner endlichen Struktur.

Übung: Zeige (leicht): "ϕ ist endlich erfüllbar" ist r.e.; (schwer) "ϕ ist endlich unerfüllbar" bzw "ϕ ist endlich allgemeingültig" ist nicht r.e.

4. Σ_n Formeln

Version Z (analog zu Ziegler; für Arithmetik). Ziegler definiert (für die Arithmetik) auf Seite 81 Σ_1 Formeln, und auch "Σ_1 Formeln im engeren Sinn".

Auf ähnliche Weise kann man allgemein Σ_n-Formeln und Π_n-Formeln definieren: (Achtung: rein formal sind die so definierten Formeln weder dasselbe wie Zieglers Σ_1 noch wie Zieglers Σ_1 Formeln im engeren Sinn.)

- Wir gehen davon aus dass unsere Sprache das zweistellige Relationssymbol $<$ enthält.
- Ein beschränkter Quantor ist ein Quantor der Form $\forall x < y$ oder $\exists x < y$ (hier ist y eine Variable, kein Term).

  Dabei ist $(\forall x < y)\phi$ eine Abkürzung für: $\forall x(x < y \to \phi)$, und $(\exists x < y)\phi$ eine Abkürzung für: $\exists x(x < y \wedge \phi)$.

  Eine Formel heißt beschränkt, wenn sie nur beschränkte Quantoren enthält. Eine quantorenfreie Formel ist daher natürlich beschränkt.
- Σ_0 Formeln (oder äquivalent: Π_0 Formelen) sind beschränkte Formeln.
- Für $n > 0$ definieren wir Σ_n als Abschluss der Π_{n-1}-Formeln unter: $\wedge$, $\vee$, Existenz-Quantifikation $\exists$, und beschränkter Quantifikation $\exists x < y$ und $\exists y < x$.
- Π_n analog (beginnend mit Σ_{n-1} und mit $\forall$ statt $\exists$.

Diese Definition ist äquivalent zu Zieglers:

- Verallgemeinerte beschränkte Quantifikation ist Quantifikation der Form $\forall x < t$, für alle Terme t in denen x nicht vorkommt; bzw $\exists x < t$.

  Es gilt: Für $n \geq 1$ sind Σ_n (und Π_n) auch unter verallgemeinerter beschränkter Quantifikation abgeschlossen. Genauer: Sei $\phi\Sigma_n$. Dann ist $(\forall x < t)\phi$. logisch äquivalent zu einer Σ_n Formel. (Analog für Π_n oder für $(\exists x < t)\phi$.)

  Beweis: Für ϕ Σ_n ist $(\forall x < t)\phi$ ist äquivalent zu $(\exists v)(v = t \wedge (\forall x < v)\phi)$; für ϕ Π_n ist $(\exists x < t)\phi$ äquivalent zu $(\forall v)(v \neq t \vee (\exists x < v)\phi)$.

  Bemerkung: Für Σ_0 gilt das nicht: $\forall x < (y + y)\phi(x, p)$ ist i.A. zu keiner beschränkten Formel $\psi(y, p)$ äquivalent.

- Die obige Standard Definition von Σ_1 ist also äquivalent zu Zieglers Σ_1.
- Ziegler definiert auch "Σ_1 Formeln im engeren Sinn" und beweist dass sie (logisch) äquivalent sind zu Σ_1 Formeln. (Wenn man eine andere Sprache verwendet, muss man diese Definition natürlich modifizieren: Für jedes Funktionssymbol (inklusive Konstanten) muss man $f(x_1, \ldots, x_n) = y$ und für jedes Relationssymbol (und Gleichheit) sowohl $R(x_1, \ldots, x_n)$ als auch $\neg R(x_1, \ldots, x_n)$ dazufügen.

Diese Definitionen sind sehr vernünftig und nützlich (und notwendig wenn man mit schwachen Systemen wir Q arbeitet). Hier präsentieren wir noch eine andere Definition (Version B), die die Pränex Normalform benutzt und in der Praxis oft einfacher zu verwenden ist. Modulo PA sind diese Versionen äquivalent.

Im Folgenden bezeichnet "Σ_n" immer die gerade beschriebene Version; falls auf eine andere Version verweisen wird geschieht das z.B. durch "Version-Z Σ_1".

Version A: prenex Version, modulo quantorenfrei.

- ϕ ist in prenex Normalform, wenn in ϕ zuerst alle Quantoren vorkommen werden und dann ein quantorenfreier Rest ψ.
- Z.B. ist $\forall x \exists y (R(x) \wedge x < y)$ in prenex Normalform, aber $\forall x (R(x) \wedge \exists y x < y)$ nicht.
- Es gilt: Zu jeder Formel ϕ gibt es eine logisch äquivalente Formel ϕ' in prenex Normalform. (Das folgt aus dem Satz A1 unten.)
- Sei ϕ in prenex Normalform. Wir fassen alle aufeinander folgenden All-Quantoren zu einem "Block" zusammen, ebenso alle aufeinander folgenden Existenz-Quantoren. Sei n die Anzahl dieser Blöcke. Wenn der erste auftretende Quantor ein Existenz-Quantor ist, nennen wir die Formel Σ_n-Formel, sonst Π_n-Formel. (Quantorenfreie Formeln sind sowohl Σ_0 als auch Π_0.)
- Bsp: $\forall x \forall z \exists y (R(x) \wedge x < y)$ ist Π_2. $\exists x_1 \exists x_2 (x_3 = f(x_1, x_2))$ ist Σ_1.
- Satz A1:
  (1) Wenn ϕ Σ_n ist, dann ist $\exists x \phi$ Σ_n und $\forall x \phi$ Π_{n+1}.
  (2) Wenn ϕ Σ_n ist, dann ist $\neg\phi$ logisch äquivalent zu einer Π_n Formel.
  (3) Wenn ϕ_1 und ϕ_2 Σ_n sind, dann ist $\phi_1 \wedge \phi_2$ logisch äquivalent zu einer Σ_n Formel, und $\phi_1 \vee \phi_2$ auch.
  (4) Bemerkung: Wenn ϕ_1 Π_n ist und ϕ_2 Σ_n, dann ist $\phi_1 \to \phi_2$ äquivalent zu $\neg\phi_1 \vee \phi_2$ und daher Σ_n.
  (5) Natürlich gelten die Dualen Aussagen (mit Σ_n und Π_n bzw $\exists$ und $\forall$ vertauscht).

  Beweis:
  (1) ist eine triviale Folgerung der Definition.
  Für (2) wende wiederholt $(\neg\exists x\phi) \leftrightarrow (\forall x \neg\phi)$ (und die duale Aussage) an.
  Für (3): Seien ϕ_1 und ϕ_2 Σ_n, d.h.:

$$\phi_1 = \exists x_1^1 \ldots \exists x_{m_1}^1 \forall x_1^2 \ldots \forall x_{m_2}^2 \ldots \psi_1$$

  (mit ψ_1 quantorenfrei); und analog

$$\phi_2 = \exists y_1^1 \ldots \exists y_{k_1}^1 \forall y_1^2 \ldots \forall y_{k_2}^2 \ldots \psi_2;$$

  durch Umbenennung der Variablen können wir davon ausgehen dass keine gebundene Variable zugleich in ϕ_1 und ϕ_2 verwendet wird. Dann ist $\phi_1 \wedge \phi_2$ äquivalent zu:
  $\exists x_1^1 \ldots \exists x_{m_1}^1 \exists y_1^1 \ldots \exists y_{k_1}^1 \forall x_1^2 \ldots \forall x_{m_2}^2 \forall y_1^2 \ldots \forall y_{k_2}^2 \ldots \psi_1 \wedge \psi_2$. Anders gesagt: Da der Satz der gebundenen Variablen in ϕ_1 und der in ϕ_2 voneinander völlig unabhängig sind, kann man diese Quantoren in beliebiger Weise zueinander anordnen (aber intern darf man die Quantoren natürlich nicht beliebig umordnen: $\forall x_1 \exists x_2 \phi(x_1, x_2)$ ist etwas anderes als $\exists x_1 \forall x_2 \psi(x_1, x_2)$; aber $(\forall x_1 \exists x_2 \forall z)(\phi(x_1, x_2) \wedge \psi(z))$ ist dasselbe wie $(\forall z \forall x_1 \exists x_2)(\phi(x_1, x_2) \wedge \psi(z))$.)
  Der Fall $\vee$ ist analog.

Version B: Prenex modulo beschränkter Quantoren (Arithmetik).

- Wir gehen davon aus dass unsere Sprache das zweistellige Relationssymbol $<$ enthält, und definieren beschränkte Quantifikation und beschränkte Formel wie in Version Z.

- Wir definieren nun Σ_n und Π_n Formeln wie in Version A, nur diesmal fordern wir dass der "Rest" ψ beschränkt ist (statt "quantorenfrei" wie in Version A).
  Insbesondere heißt Σ_0 (und äquivalent: Π_0) jetzt also "beschränkt".
- Satz B1: Satz A1 (1)-(5) von oben gilt ganz analog. (Mit genau denselben Beweisen.)
- Wir nennen zwei Formeln ϕ und ψ PA-äquivalent, wenn PA$\vdash \phi \leftrightarrow \psi$. (Insbesondere gilt dann $\mathbb{N} \vDash \phi \leftrightarrow \psi$.)
- Lemma B1: $(\forall x_1, \dots, x_m)\phi$ ist PA-äquivalent zu $(\forall y)(\forall x_1 < y, \dots, x_m < y)\phi$.
  (Analog für $\exists$.)
  Beweis: "Links nach Rechts" ist allgemeingültig. "Rechts nach Links": Argumentiere in PA. Angenommen $\neg(\forall x_1, \dots, x_m)\phi$, d.h. es gibt $a_1, \dots, a_n$ mit $\neg\phi(a_1, \dots, a_n)$. Setze $y := S(a_1 + \dots + a_n)$. Dann $a_\ell < y$, und daher $\neg(\forall x_1 < y, \dots, x_m < y)\phi$.
- Lemma B2: $(\forall x < y)(\exists z)\phi$ is PA äquivalent zu $(\exists v)(\forall x < y)(\exists z < v)\phi$.
  Dual gilt dann natürlich auch (durch Negation):
  $(\exists x < y)(\forall z)\phi$ is PA äquivalent zu $(\forall v)(\exists x < y)(\forall z < v)\phi$.
  Beweis: "Rechts nach Links" ist allgemeingültig. "Links nach Rechts": Induktion in PA nach y: Für $y = 0$ ist Links und Rechts trivialerweise wahr. Der Lesbarkeit halber schreiben wir $\phi(x)$ und ignorieren die anderen freien Variablen die in ϕ vorkommen können. Wir setzen also voraus: (Induktionsannahme) $(\forall x < y)(\exists z)\phi(x)$ impliziert $(\exists v)(\forall x < y)(\exists z < v)\phi(x)$; und (Links für $y+1$): $(\forall x < S(y))(\exists z)\phi(x)$; und wir wollen zeigen: $(\exists v')(\forall x < S(y))(\exists z < v')\phi(x)$. Aber aus "Links" folgt $(\exists z)\phi(y)$; setze $v' := v + S(z)$.
- Wir können diese Lemma iterieren: $(\forall x < y)(\exists z_1, \dots, z_m)\phi$ ist PA äquivalent zu $(\exists v_1)(\forall x < y)(\exists z_2, \dots, z_m)(\exists z_1 < v_1)$ und daher zu $(\exists v_1)(\exists v_2)(\forall x < y)(\exists z_3, \dots, z_m)(\exists z_1 < v_1)(\exists z_2 < v_2)$ etc, und letztlich zu $(\exists v_1 \dots v_m)(\forall x < y)(\exists z_1 < v_1 \dots z_m < v_m)$.
- Man kann also beschränkte Quantoren mit unbeschränkten vertauschen. Es gilt daher:
  Satz B2: Wenn ϕ Σ_n ist, dann sind $(\forall x < y)\phi$ und $(\exists x < y)\phi$ PA-äquivalent zu Σ_n Formeln.
- Insbesondere ist Σ_n PA-äquivalent zu Version-Z Σ_n. (Durch Satz B1 und B2).
- Natürlich ist für $n \geq 1$ Σ_n (und Π_n) auch abgeschlossen (modulo PA) unter verallgemeinerten beschränkten Quantoren, siehe Version Z.

Version B, Variante Mengenlehre (wieder prenex modulo beschränkt).

- In der Sprache der Mengenlehre verwendet man das zweistellige Prädikat $\in$. Man kann nun dieses Prädikat statt $<$ verwenden, um beschränkte Quantifikation zu definieren.
- Völlig analog zur Sprache der Arithmetik definiert man so Version-B Σ_n Formeln in der Sprache der Mengenlehre.
- Die obigen Sätze gelten analog für diese Situation (ersetze PA durch ZFC, oder eine geeignete schwache Teiltheorie T von ZFC). Für die Abgeschlossenheit von Σ_n unter beschränkter Quantifikation (modulo T-Äquivalenz) muss T (für beliebige Formeln ϕ) beweisen können: $(\forall x \in A)(\exists y_1, \dots, y_n)\psi(x, y_1, \dots, y_n)$ impliziert $(\exists Z)(\forall x \in A)(\exists y_1 \in Z, \dots, y_n \in Z)\psi(x, y_1, \dots, y_n)$. Das folgt aus dem sogenannten Ersetzungsaxiom (plus entweder Auswahlaxiom oder Fundierungsaxiom+Potenzmengenaxiom).

Version C: Deskriptive Mengenlehre (kein LVA Stoff).

- Σ_n Formeln der Sprache der Arithmetik nennt man (vor allem aus Sicht der Mengentheorie) manchmal auch Σ^0_n (analog für Π). Das 0 bezieht sich darauf dass sich die (unbeschränkten) Quantoren auf $\mathbb{N}$ beziehen (in der Sprache der Arithmetik stellen wir uns ja normalerweise vor dass unsere Sprache die natürlichen Zahlen beschreibt, insbesondere dass wir über natürliche Zahlen quantifizieren). Wir beschreiben das im Folgenden eine Spur exakter:
- In der Sprache der Mengenlehre (genauer: in ZFC, das wir noch genau kennenlernen werden) kann man $\mathbb{N}$ definieren (Bem: in einem schwachen Sinn: natürlich gibt es nonstandard ZFC-Modelle deren $\mathbb{N}$ eine nonstandard Version der natürlichen Zahlen ist, oder sogar falsche Sätze wie z.B. $\neg$Con(ZFC) erfüllt.
  Dann kann man Quantifikation über $\mathbb{N}$ einfach als $\forall x \in \mathbb{N}$ bzw $\exists x \in \mathbb{N}$ ausdrücken.

Eine Σ_n^0-Formel ist dann einfach eine Version-B(Arithmetik)-Σ_n-Formel, bei der alle Quantoren durch Quantoren über $\mathbb{N}$ ersetzt werden. Eine Formel nennt man dann arithmetisch, wenn sie nur Quantoren über $\mathbb{N}$ enthält, d.h. äquivalent ist zu einer Σ_n^0-Formel für irgendein n.

- Analog kann man $\mathbb{R}$ (und Quantifikation darüber) definieren. Damit kann man dann Σ_n^1 Formeln definieren (ein Begriff der in der Deskriptiven Mengentheorie zentral ist): Eine (mengentheoretische) Formel ist Σ_n^1, wenn sie ähnlich zur Version-B Σ_n-Formel aufgebaut ist, nur lassen wir nur Quantifikation über $\mathbb{R}$ zu, und als "Rest" ψ eine beliebige arithmetische Formel (statt nur eine quantorenfreie wie in Version A oder eine beschränkte wie in Version B).
- In der Deskriptiven Mengenlehre zeigt man dann: Eine Teilmenge von $\mathbb{R}$ hat eine Σ_1^1 Definition (mit reellen Parametern) genau dann wenn sie stetiges Bild einer Borelmenge ist; eine Menge ist Borel genau dann wenn sie sowohl eine Σ_1^1 als auch eine Π_1^1-Definition hat (jeweils mit reellen Parametern); jede Σ_1^1 Menge ist Lebesque messbar; etc etc. Im Allgemeinen beginnen jenseits von Σ_1^1 massive Unvollständigkeitsphänomene. Es ist z.B. nicht entscheidbar (genauer: aus ZFC weder beweisbar noch widerlegbar) ob jede Σ_2^1 Menge Lebesque messbar ist.

5. Beweis-Details Ziegler Kapitel 4

Q* impliziert erste Folgerung (S 80). Achtung: Q* besteht nicht nur (wie in Ziegler angegeben) aus Q*1 - Q*3, sondern zusätzlich aus Q5.

(Wenn man will kann man das als Fall $a = 0$ von Q*3 auffassen.)

Detaillierter Beweis der ersten Folgerung.

Für $a < b$ folgt aus Q*3 dass $\Delta_a < \Delta_b$ beweisbar ist. Der Rest der Folgerung wird mit Induktion nach b (jeweils für alle a) bewiesen:

Für $b = 0$ folgt (aus Q5) $\neg\Delta_a < \Delta_0$ für alle a; für $a > 0$ folgt $\neg\Delta_a = \Delta_0$, weil ja $\Delta_0 < \Delta_a$ und daher andernfalls $\Delta_0 < \Delta_a = \Delta_0$ wäre, ein Widerspruch.

Wir nehmen also an dass die Aussagen für b (und für alle a) beweisbar sind, und betrachten den Fall $b + 1$.

Fixiere $a \not< b+1$, d.h. $a \geq b+1$. Insbesondere $a \neq 0$, $a \neq 1$, etc, bis $a \neq b$; und daher (Induktion) gilt dass $\Delta_a \neq \Delta_c$ beweisbar ist für $c = 0, \ldots, b$, und damit auch $\neg(\Delta_a = \Delta_0 \vee \cdots \vee \Delta_a = \Delta_b)$. Wir können nun (in Q*) argumentieren: Aus $\Delta_a < \Delta_{b+1}$ folgt (mit Q*3) der (gerade widerlegte Satz) $\Delta_a = \Delta_0 \vee \cdots \vee \Delta_a = \Delta_b$; und daher gilt $\neg\Delta_a < \Delta_{b+1}$.

Für $a \neq b+1$ ist $a < b+1$ oder $b+1 < a$ und damit ist $\Delta_a > \Delta_{b+1} \vee \Delta_a < \Delta_{b+1}$ auch beweisbar. Wir können also (in Q*) argumentieren: Aus $\Delta_a = \Delta_{b+1}$ folgt $\Delta_{b+1} < \Delta_{b+1}$, ein Widerspruch, also gilt $\Delta_a \neq \Delta_{b+1}$.

Lem 18.1(3): PA beweist die Kommutativität von +. Sie $\phi_1(x)$ die Formel $x+0 = x = 0+x$. Mit Induktion nach x kann man (in PA) den Satz $\psi_1 = \forall x \phi_1(x)$ beweisen:

$0 + 0 = 0$ (verwende Q1); Wir verwenden nun als Induktionsannahme $x + 0 = x = 0 + x$ und zeigen (in PA) $S(x) + 0 = S(x) = 0 + S(x)$:

$0 + S(x) = S(0 + x) = S(x) = S(x) + 0$ (verwende Q2, die Induktionsannahme, und Q1).

Sei $\phi_2(x)$ die Formel $(\forall y)S(y+x) = S(y)+x$. Wir beweisen mit Induktion über $\phi_2(x)$ den Satz $\psi_2 = \forall x \phi_2(x)$:

$S(y + 0) = S(y) = S(y) + 0$ (verwende zweimal Q1). Und $S(y + S(x)) = S(S(y + x)) = S(S(y) + x) = S(y) + S(x)$. (verwende Q2, die Induktionsannahme und nochmals Q2).

Sei $\phi_3(x)$ die Formel $(\forall y)x + y = y + x$. Wir beweisen mit Induktion $\forall x \phi_3(x)$, d.h. die Kommutativität von +:

Der Fall $x = 0$ ist ψ_1. Wir verwenden also als Induktionsannahme $(\forall y)x+y = y+x$ und wollen (in PA) zeigen dass $(\forall y)S(x)+y = y+S(x)$. Es gilt aber $y+S(x) = S(y+x) = S(x+y) = S(x)+y$ (benutze Q2, die Induktionsannahme und ψ_2).