

## Einführung in die mathematische Logik

### Vorlesung 22

#### 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  $\psi$  mit  $r$  freien Variablen derart gibt, dass dieser Ausdruck für jede Belegung genau dann wahr wird, wenn die Relation auf das Belegungstupel zutrifft. Da  $\mathbb{N}^{\mathbb{F}}$  vollständig ist, ergibt sich daraus die Äquivalenz, dass  $(n_1, \dots, n_r) \notin R$  äquivalent zur Nichtgültigkeit  $\mathbb{N} \not\models \psi(n_1, \dots, n_r)$  und somit auch zur Gültigkeit der Negation  $\mathbb{N} \models \neg\psi(n_1, \dots, n_r)$  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  $\Gamma$  eine Menge von arithmetischen Ausdrücken. Eine Relation  $T \subseteq \mathbb{N}^r$  heißt *repräsentierbar* in  $\Gamma$ , wenn es einen  $L^{\text{Ar}}$ -Ausdruck  $\psi$  in  $r$  freien Variablen derart gibt, dass für alle  $r$ -Tupel  $(n_1, \dots, n_r) \in \mathbb{N}^r$  die beiden Eigenschaften

- (1) Wenn  $(n_1, \dots, n_r) \in T$ , so ist  $\Gamma \vdash \psi(n_1, \dots, n_r)$ ,
- (2) Wenn  $(n_1, \dots, n_r) \notin T$ , so ist  $\Gamma \vdash \neg\psi(n_1, \dots, n_r)$ ,

gelten.

DEFINITION 22.2. Es sei  $\Gamma$  eine Menge von arithmetischen Ausdrücken. Eine Funktion

$$F: \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

heißt *repräsentierbar* in  $\Gamma$ , wenn es einen  $L^{\text{Ar}}$ -Ausdruck  $\psi$  in  $r + s$  freien Variablen derart gibt, dass für alle  $(r + s)$ -Tupel  $(n_1, \dots, n_{r+s}) \in \mathbb{N}^{r+s}$  die folgenden Eigenschaften

- (1) Wenn  $F(n_1, \dots, n_r) = (n_{r+1}, \dots, n_{r+s})$ , so ist  $\Gamma \vdash \psi(n_1, \dots, n_{r+s})$ ,
- (2) Wenn  $F(n_1, \dots, n_r) \neq (n_{r+1}, \dots, n_{r+s})$ , so ist  $\Gamma \vdash \neg\psi(n_1, \dots, n_{r+s})$ ,
- (3)  $\Gamma \vdash \exists!x_{r+1} \dots \exists!x_{r+s} \psi(n_1, \dots, n_r, x_{r+1}, \dots, x_{r+s})$ ,

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  $\exists z(\alpha(z) \wedge \forall y(\alpha(y) \rightarrow y = z))$ . Hierbei ersetzen wir die freie Variable von  $\alpha$  durch  $z$  bzw. durch  $y$ .

Gelegentlich werden wir mit dem folgenden schwächeren Repräsentierungsbegriff für Relationen arbeiten.

DEFINITION 22.3. Es sei  $\Gamma$  eine Menge von arithmetischen Ausdrücken. Eine Relation  $T \subseteq \mathbb{N}^r$  heißt *schwach repräsentierbar* in  $\Gamma$ , wenn es einen  $L^{\text{Ar}}$ -Ausdruck  $\psi$  in  $r$  freien Variablen derart gibt, dass für alle  $r$ -Tupel  $(n_1, \dots, n_r) \in \mathbb{N}^r$  die Äquivalenz

$$(n_1, \dots, n_r) \in T \text{ genau dann, wenn } \Gamma \vdash \psi(n_1, \dots, n_r)$$

gilt.

Im widerspruchsfreien Fall folgt aus der obigen (starken) Repräsentierung für eine Relation auch die schwache Repräsentierung.

DEFINITION 22.4. Es sei  $\Gamma$  eine Menge von arithmetischen Ausdrücken. Man sagt, dass  $\Gamma$  *Repräsentierungen erlaubt*, wenn  $\Gamma$  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  $\mathbb{N}^{\text{F}}$ , erlaubt Repräsentierungen.*

*Beweis.* Es sei  $T \subseteq \mathbb{N}^r$  eine  $R$ -entscheidbare Relation und es sei  $P$  ein Registerprogramm mit den Registern  $R_0, R_1, \dots, R_m$  das diese Relation entscheidet. Aufgrund von Lemma 21.1 gibt es einen arithmetischen Ausdruck  $\psi_P$  in  $2m$  freien Variablen, der den Programmablauf arithmetisch modelliert. Es gilt also  $(n_1, \dots, n_r) \in T$  genau dann, wenn  $P$ , angesetzt auf  $(n_1, \dots, n_r)$  (strenggenommen angesetzt auf  $(1, n_1, \dots, n_r, 0, \dots, 0)$ , wenn man die vollständige Registerbelegung angibt) anhält mit der Ausgabe 0 (d.h.  $(h, 0, n'_2, \dots, n'_m)$ ; andernfalls wird mit der Ausgabe 1 angehalten), genau dann, wenn  $\mathbb{N} \models \psi_P(n_1, \dots, n_r, 0, \dots, 0, 0, n'_2, \dots, n'_m)$  gilt.

Wegen der Vollständigkeit von  $\mathbb{N}$  bedeutet dies, dass

$$\theta_P = \exists y_2 \dots \exists y_m \psi_P(x_1, \dots, x_r, 0, \dots, 0, 0, y_2, \dots, y_m)$$

die Relation repräsentiert. Es sei

$$F: \mathbb{N}^r \longrightarrow \mathbb{N}^s$$

eine  $R$ -berechenbare Abbildung und es sei  $P$  ein Registerprogramm, das  $F$  berechnet. Aufgrund von Lemma 21.1 gibt es einen arithmetischen Ausdruck  $\psi_P$  in  $2m$  freien Variablen, der den Programmablauf arithmetisch modelliert. D.h. für jedes  $(r + s)$ -Tupel  $n_1, \dots, n_{r+s}$  gilt

$$F(n_1, \dots, n_r) = (n_{r+1}, \dots, n_{r+s})$$

genau dann, wenn das Programm  $P$  bei jeder Eingabe anhält und angesetzt auf  $(n_1, \dots, n_r)$  (in den ersten  $r$  Registern, die Eingabe ist also  $(1, n_1, \dots, n_r, 0, \dots, 0)$ ) die Ausgabe  $(n_{r+1}, \dots, n_{r+s})$  (also  $(h, n_{r+1}, \dots, n_{r+s}, \ell_{m+s+1}, \dots, \ell_{2m})$ ) besitzt, genau dann, wenn

$$\mathbb{N} \models \psi_P(n_1, \dots, n_r, 0, \dots, 0, n_{r+1}, \dots, n_{r+s}, \ell_{m+s+1}, \dots, \ell_{2m})$$

gilt. Von daher ist der Ausdruck (in den freien Variablen  $x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}$ )

$$\Theta = \exists z_{m+s+1} \dots \exists z_{2m} \Psi(x_1, \dots, x_r, 0, \dots, 0, x_{r+1}, \dots, x_{r+s}, z_{m+s+1}, \dots, z_{2m})$$

Da eine Funktion vorliegt und  $\mathbb{N}^\#$  vollständig ist, gilt auch

$$\mathbb{N} \models \exists! x_{r+1} \dots \exists! x_{r+s} \Theta(n_1, \dots, n_r, x_{r+1}, \dots, x_{r+s}).$$

□

**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.

## 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  $\alpha$  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 durchnummerieren 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  $R'' \dots l$  benennen. Es ist auch möglich, in einem Zwischenschritt die Variablen  $x_1, x_2, x_3 \dots$  mit  $x, x', x'', \dots$  zu benennen und so ein endliches Alphabet zu erhalten. Eine andere Möglichkeit besteht darin, abzählbar unendlich viele Symbole mit den natürlichen Zahlen durchnummerieren und einen Ausdruck der Form  $s_{i_1} s_{i_2} \dots s_{i_n}$  ( $i_j$  sei die Nummer des  $j$ -ten Symbols im Ausdruck) durch das Produkt  $p_1^{i_1} p_2^{i_2} \dots p_n^{i_n}$  wiederzugeben, wobei die  $p_1, p_2, p_3, \dots$  die Folge der Primzahlen sei.

BEISPIEL 22.7. Zu einer Ausdrucksmenge  $\Gamma$  kann man die Menge

$$\{GN(\alpha) \mid \Gamma \vdash \alpha\}$$

betrachten, also die Menge der Gödelnummern von Ausdrücken, die aus  $\Gamma$  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  $\Gamma$  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  $\Gamma \subseteq L^{\text{Ar}}$  eine Menge von arithmetischen Ausdrücken, die Repräsentierungen erlaube. Dann gibt es zu jedem  $\alpha \in L_1^{\text{Ar}}$  einen Satz  $q \in L_0^{\text{Ar}}$  mit*

$$\Gamma \vdash q \iff \alpha(GN(q)).$$

*Beweis.* Wir betrachten die Abbildung

$$F: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, (m, n) \longmapsto F(m, n),$$

die durch

$$F(m, n) := \begin{cases} GN(\alpha(n)), & \text{falls } m \text{ die } GN \text{ eines } \alpha \in L_1^{\text{Ar}} \text{ ist,} \\ 0 & \text{sonst,} \end{cases}$$

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  $\alpha \in L_1^{\text{Ar}}$ . 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  $\Gamma$  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  $\Gamma$  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  $\alpha \in L_1^{\text{Ar}}$  erhalten wir nun durch eine trickreiche Anwendung von  $\varphi$ . Wir setzen

$$s := \forall z (\varphi(x, x, z) \rightarrow \alpha(z)).$$

Der Ausdruck  $s$  besitzt die Gödelnummer  $GN(s)$ . Wir behaupten nun, dass der Satz

$$q := s \frac{GN(s)}{x} = \forall z (\varphi(GN(s), GN(s), z) \rightarrow \alpha(z))$$

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  $GN(q)$ )

$$\vdash q \rightarrow (\varphi(GN(s), GN(s), GN(q)) \rightarrow \alpha(GN(q))).$$

Da das Antezedens der rechten Implikation aus  $\Gamma$  ableitbar ist, folgt

$$\Gamma \vdash q \rightarrow \alpha(GN(q)).$$

Dies besagt also die Ableitbarkeit der Hinrichtung. Die aufgrund der Repräsentierbarkeit oben angeführte eindeutige Existenzaussage führt zu

$$\Gamma \vdash \forall z (\varphi(GN(s), GN(s), z) \rightarrow (z = GN(q))).$$

Durch Substitution ergibt sich

$$\vdash (z = GN(q)) \rightarrow (\alpha(GN(q)) \rightarrow \alpha(z))$$

und somit nach einer prädikatenlogischen Umformulierung

$$\Gamma \vdash \forall z (\varphi(GN(s), GN(s), z) \wedge \alpha(GN(q)) \rightarrow \alpha(z)).$$

Da hierbei  $\alpha(GN(q))$  keine freie Variablen besitzt, ist auch

$$\Gamma \vdash \alpha(GN(q)) \rightarrow (\forall z (\varphi(GN(s), GN(s), z) \rightarrow \alpha(z))),$$

und das Sukzedens ist gerade  $q$ , so dass auch die Rückrichtung ableitbar ist.  $\square$