Prof. Dr. H. Brenner **Osnabrück SS 2016**

Einführung in die mathematische Logik

Vorlesung 13

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 letzen Vorlesung gesehen haben. In dieser Vorlesung geben wie 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 15.7. Nach Aufgabe 13.16 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 $x \in M$[1] 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.

[1]Wir bezeichnen hier und im Folgenden die Variable und das ihr in einer Belegung zugewiesene Element mit dem gleichen Symbol.

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 13.1, Aufgabe 13.2 und Aufgabe 13.17. □

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 dem ersten Peano-Axiom nicht zugleich wahr sein. Es geht also um die Aussage

$$\forall x \left((x = 0) \vee (\exists u x = u + 1) \right) ,$$

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 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 13.18. □

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

$$\begin{aligned} \forall u \Big(\Big(\exists x \left(\alpha \wedge x \leq u \right) \to \exists y \left(\alpha \frac{y}{x} \wedge \forall x \left(\alpha \to y \leq x \right) \right) \Big) \to \\ \Big(\exists x \left(\alpha \wedge x \leq u + 1 \right) \to \exists y \left(\alpha \frac{y}{x} \wedge \forall x \left(\alpha \to x \geq y \right) \right) \Big) \Big) \end{aligned}$$

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 $\exists x \left(\alpha \wedge x \leq u \right)$ 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

$$\alpha \frac{u+1}{x} \wedge \forall x \left(\alpha \to x \geq u + 1 \right)$$

und damit

$$\exists y \left(\alpha \frac{y}{x} \wedge \forall x \left(\alpha \to x \geq y \right) \right) .$$

□

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[2] r, $r < d$, und mit*

$$m = qd + r.$$

[2]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.

Beweis. Wir betrachten 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. □

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.

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 Vorgänger (dies ist der Grund, warum wir abgesehen für den Leitkoeffizienten auch negative Koeffizienten zulassen). 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

$$x \geq y \text{ genau dann, wenn } \exists z(x = y + z)$$

und die Eigenschaft, ein größter gemeinsamer Teiler u von x und y zu sein, durch

$$(u|x) \wedge (u|y) \wedge ((v|x) \wedge (v|y) \to v|u)\ .$$

Damit setzen wir

$$\alpha(x) = \forall y((y \leq x) \to \forall u(u \text{ ist } \mathrm{GgT}(x, y) \to \exists a \exists b(ax + by = u))).$$

Dies ist ein Ausdruck mit der einzigen freien Variablen x, der inhaltlich besagt, dass für jedes Element y unterhalb von x der größte gemeinsame Teiler von x und y als Linearkombination aus x und y darstellbar ist. Dieser Ausdruck gilt innerhalb der natürlichen Zahlen (also für $x \in \mathbb{N}$), es handelt sich um das Lemma von Bezout. 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 für y eine Primzahl (aus $\mathbb{N}$) nehmen, die den Leitkoeffizienten von x nicht teilt. Wegen $x = (x - y) + y$ ist auch $y \leq x$. Der größte gemeinsame Teiler von x und y ist dann 1, doch die 1 ist nicht als Linearkombination von y und dem Polynom x darstellbar (wenn man modulo y geht, so verändert sich der Grad von x 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.