aus $\mathcal{K}$ entfernen und in jeder verbleibenden Klausel gegebenenfalls das Literal $\neg x_{n+1}$ streichen. D.h.,

$$\mathcal{K}^+ := \{ K \setminus \{\neg x_{n+1}\} \mid K \in \mathcal{K},\ x_{n+1} \notin K \}.$$

Analog erhalten wir $\mathcal{K}^-$:

$$\mathcal{K}^- := \{ K \setminus \{x_{n+1}\} \mid K \in \mathcal{K},\ \neg x_{n+1} \notin K \}.$$

<u>Beh.:</u> $\mathcal{K}^+$ und $\mathcal{K}^-$ sind unerfüllbar.

<u>Bew. d. Beh.:</u>

<u>Annahme:</u> $\Phi_{\mathcal{K}^+}$ ist erfüllbar.

Dann existiert eine Belegung $\mathcal{B}$ der Variablen $x_1, x_2, \dots, x_n$, die $\Phi_{\mathcal{K}^+}$ erfüllt. Wir erweitern die Belegung $\mathcal{B}$ zu einer Belegung $\mathcal{B}'$ der Variablen $x_1, x_2, \dots, x_n, x_{n+1}$, indem wir der Variablen x_{n+1} den Wert wahr zuweisen. Dann erfüllt $\mathcal{B}'$ jede Klausel, die wir aus $\mathcal{K}$ entfernt haben $\Rightarrow$

$$\mathcal{B}' \models \Phi_{\mathcal{K}} \qquad \text{Widerspruch.}$$

Also war unsere Annahme falsch. D.h., $\Phi_{\mathcal{K}^+}$ ist unerfüllbar.

Genauso beweist man, dass $\Phi_{\mathcal{K}^-}$ unerfüllbar ist.

$\square$

Induktionsvoraussetzung $\Rightarrow$

$\square \in R^*(\mathcal{K}^+)$ und $\square \in R^*(\mathcal{K}^-)$.

$\Rightarrow$

Es existiert eine Folge $C_1, C_2, \dots, C_m$ von Klauseln, so dass

i) $C_m = \square$ und
ii) für $1 \leq i \leq m$ gilt $C_i \in \mathcal{K}^+$ oder es existieren $j, k < i$ mit C_i ist Resolvente von C_j und C_k.

Einige der Klauseln in obiger Folge können aus Klauseln in $\mathcal{K}$ durch Streichen von $\neg x_{n+1}$ entstanden sein.

Ist dies nicht der Fall, dann gilt:

$$C_1, C_2, \dots, C_m \in R^*(\mathcal{K}),$$

also $\square \in R^*(\mathcal{K})$.

Andernfalls erhalten wir durch Wiedereinfügen der gestrichenen Literalen $\neg x_{n+1}$ eine Folge von Klauseln $C_1', C_2', \dots, C_m'$, welche zeigt, dass

$$\{\neg x_{n+1}\} \in R^*(\mathcal{K}).$$

Analog impliziert $\square \in R^*(\mathcal{K}^-)$, dass

$$\square \in R^*(\mathcal{K}) \text{ oder } \{x_{n+1}\} \in R^*(\mathcal{K}).$$

Da $\square$ Resolvente der Klauseln $\{x_{n+1}\}, \{\neg x_{n+1}\}$ ist, impliziert $\{x_{n+1}\}, \{\neg x_{n+1}\} \in R^*(\mathcal{K})$ auch

$$\square \in R^*(\mathcal{K}).$$

■

Der Resolutionssatz kann nun verwendet werden um die Erfüllbarkeit eines aussagenlogischen Ausdruckes zu testen. Dies leistet folgender Algorithmus:

<u>Algorithmus</u> RESOLUTION

<u>Eingabe</u>: aussagelogischer Ausdruck ϕ

<u>Ausgabe</u>: $\begin{cases} \text{erfüllbar} & \text{falls } \phi \text{ erfüllbar} \\ \text{unerfüllbar} & \text{sonst.} \end{cases}$

<u>Methode</u>:

(1) Transformiere ϕ in einen Ausdruck ϕ' in KNF.

(2) Bilde die zu ϕ' korrespondierende Klauselmenge $\mathcal{K}_{\phi'}$.

(3) Konstruiere die Folge

$$R(\mathcal{K}_{\phi'}), R^2(\mathcal{K}_{\phi'}), \ldots$$

bis $R^k(\mathcal{K}_{\phi'}) = R^{k+1}(\mathcal{K}_{\phi'})$ für ein k.

(4) Falls $\square \in R^k(\mathcal{K}_{\phi'})$, dann

Ausgabe := unerfüllbar.

Andernfalls

Ausgabe := erfüllbar.

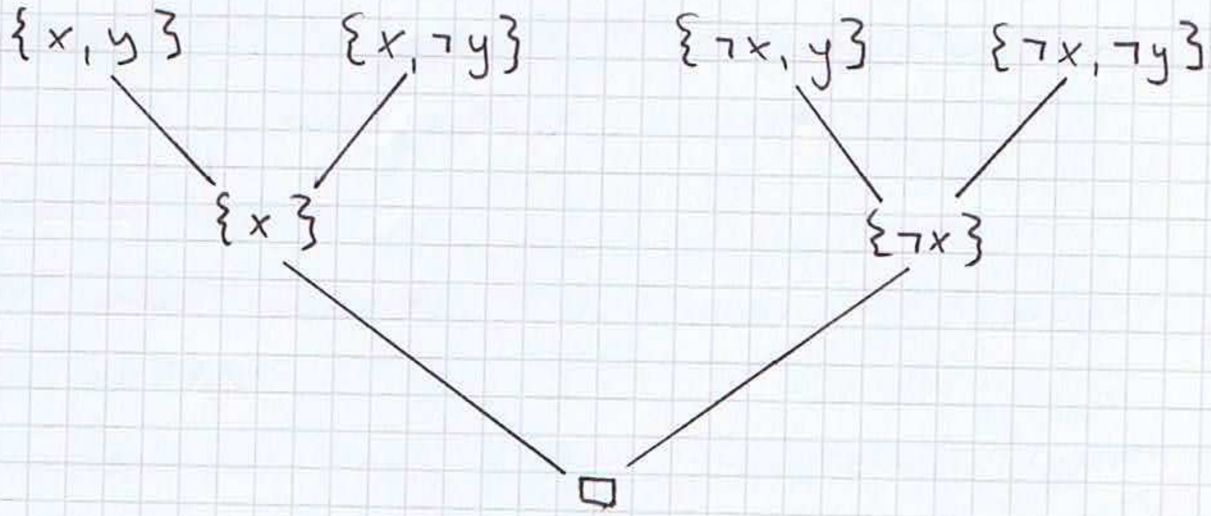
Obiger Algorithmus berechnet alle möglichen Resolventen.

<u>Frage:</u> Ist dies notwendig?

<u>Beobachtung:</u>
Jede Klausel in $R^*(\mathcal{K}_{\varphi'})$ hat einen "Stammbaum", der die Entstehung der Klausel widerspiegelt.

<u>Beispiel 2.5</u>

Betrachte $\mathcal{K} := \{\{x,y\},\{x,\neg y\},\{\neg x,y\},\{\neg x,\neg y\}\}$.
Folgender Baum zeigt die Unerfüllbarkeit von $\mathcal{K}$:



Die Klausel $\{y\}$, die Resolvente von $\{x,y\}$, $\{\neg x,y\}$ ist, wird nicht konstruiert. ■

<u>Idee:</u>
Anstatt alle möglichen Resolventen zu bilden genügt es, nur solche zu bilden, die zur Konstruktion der leeren Klausel benötigt werden.

Obige Idee legt folgende Definition nahe:

Eine Deduktion aus einer Klauselmenge $\mathcal{K}$ ist eine Folge $C_1, C_2, \ldots, C_m$ von Klauseln, so dass jedes C_i entweder eine Klausel in $\mathcal{K}$ oder eine Resolvente zweier Klauseln C_j und C_k für ein $j, k < i$ ist. Obige Deduktion ist dann eine Deduktion von C_m, der letzten Klausel in obiger Folge.

Der Resolutionssatz könnte wie folgt umformuliert werden:

Eine Menge von Klauseln ist genau dann unerfüllbar, wenn es eine Deduktion der leeren Klausel aus ihr gibt.

Diese Formulierung des Resolutionssatzes ist die Basis für viele Computerprogramme, die für aussagelogischen Ausdrücke entscheiden, ob diese erfüllbar sind.

Beispiel 2.6:

Betrachte $\mathcal{K} := \{\{x, y, \neg z\}, \{\neg x\}, \{x, y, z\}, \{x, \neg y\}\}$
Eine mögliche Deduktion von $\square$ aus $\mathcal{K}$ ist die folgende:

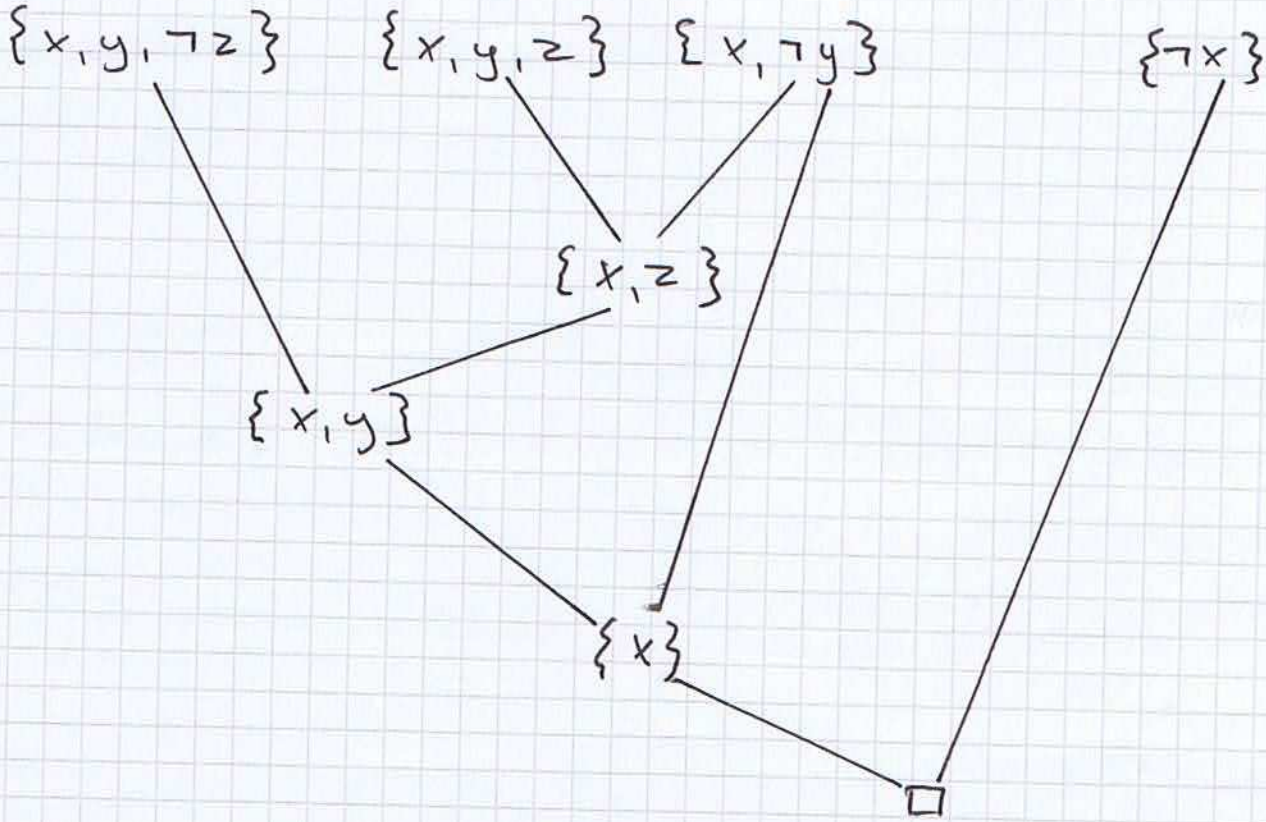
$K_1 = \{x, y, \neg z\}$ (Klausel aus $\mathcal{K}$)
$K_2 = \{x, y, z\}$ (Klausel aus $\mathcal{K}$)

$K_3 = \{x, \neg y\}$ (Klausel aus $\mathcal{K}$)
$K_4 = \{x, z\}$ (Resolvente von K_2, K_3)
$K_5 = \{x, y\}$ (Resolvente von K_1, K_4)
$K_6 = \{x\}$ (Resolvente von K_3, K_5)
$K_7 = \{\neg x\}$ (Klausel aus $\mathcal{K}$)
$K_8 = \square$ (Resolvente von K_6, K_7)

In obiger Deduktion wird die Klausel $\{x, \neg y\}$ zweimal verwendet. Es gibt eine kürzere Möglichkeit, aus $\mathcal{K}$ die leere Klausel $\square$ herzuleiten.

<u>Übung:</u>
Geben Sie eine kürzere Deduktion von $\square$ aus $\mathcal{K}$ an.

Folgender Graph veranschaulicht obige Deduktion



2.2 Die Prädikatenlogik

In der Aussagenlogik können ausschließlich Aussagen, die aus Booleschen Variablen und den aussagelogischen Verknüpfungen $\wedge, \vee, \neg$ bestehen, gebildet werden. Aussagen der Form

"Es gibt eine ganze Zahl x, die eine Primzahl ist."

oder

"Alle ganze Zahlen sind Primzahlen"

sind in der Aussagelogik nicht möglich.

Ziel:
Entwicklung einer Logik, in der auch komplexere mathematische Sachverhalte ausdrückbar sind.

Diese Logik heißt Prädikatenlogik oder auch Logik erster Stufe.

2.2.1 Die Syntax der Prädikatenlogik

Ein Vokabular (oder auch Signatur genannt) $\Sigma := (\Phi, \Pi, r)$ besteht aus

- einer abzählbaren Menge Φ von Funktionssymbolen,
- einer abzählbaren Menge Π von Relationssymbolen und

- einer Abbildung $r : \Phi \cup \Pi \to \mathbb{N}_0$, der sogenannten <u>Stelligkeitsfunktion</u>.

Dabei sind Φ und Π disjunkt. r ordnet jedem Symbol aus $\Phi \cup \Pi$ seine Stelligkeit zu. $f \in \Phi$ mit $r(f) = k$ heißt <u>k-stelliges Funktionssymbol</u> und $R \in \Pi$ mit $r(R) = k$ heißt <u>k-stelliges Relationssymbol</u>. Nullstellige Funktionssymbole heißen <u>Konstanten</u>. Relationssymbole sind niemals nullstellig. Bei uns wird Π stets die binäre <u>Gleichheitsrelation</u> $=$ enthalten.

$V := \{x, y, z, \ldots\}$ bezeichnet eine feste, abzählbare Menge von <u>Variablen</u>, die Werte aus dem zugrundeliegenden Universum annehmen können.

Wir definieren induktiv <u>Terme</u> über dem Vokabular Σ durch:

i) Jede Variable in V ist ein Term.
ii) Falls $f \in \Phi$ ein k-stelliges Funktionssymbol und $t_1, t_2, \ldots, t_k$ Terme sind, dann ist $f(t_1, t_2, \ldots, t_k)$ ein Term.

<u>Bemerkung</u>
Gemäß obiger Definition ist eine Konstante c ein Term. Nimm $k = 0$ und lasse in $c()$ die Klammern weg.

Ziel:

Definition von Ausdrücke über dem Vokabular Σ.

Seien $R \in \Pi$ ein k-stelliges Relationssymbol und $t_1, t_2, \ldots, t_k$ Terme. Dann ist $R(t_1, t_2, \ldots, t_k)$ ein <u>atomarer Ausdruck</u>. Wir definieren nun <u>prädikatenlogische Ausdrücke</u> induktiv durch:

i) Jeder atomarer Ausdruck ist ein prädikaten=logischer Ausdruck.

ii) Seien ϕ und ψ prädikatenlogische Ausdrücke. Dann sind $\neg\phi$, $(\phi \vee \psi)$ und $(\phi \wedge \psi)$ prädikatenlogische Ausdrücke.

iii) Seien ϕ ein prädikatenlogischer Ausdruck, $x \in V$ eine Variable und $\forall$ ein Zeichen mit der Bedeutung "für alle". Dann ist $(\forall x\, \phi)$ ein prädikatenlogisches Ausdruck.

iv) Dies sind alle prädikatenlogische Ausdrücke.

<u>Schreibweisen</u>:

- Genauso wie in der Aussagenlogik verwenden wir auch in der Prädikatenlogik die Schreibweisen $\rightarrow$ und $\leftrightarrow$
- Wir schreiben $(\exists x \phi)$ für $\neg(\forall x \neg\phi)$. Die Symbole $\forall$ und $\exists$ heißen <u>Quantoren</u>. $\forall$ ist der <u>Allquantor</u>, $\exists$ ist der <u>Existenzquantor</u>.
- Wenn dadurch keine Mehrdeutigkeit entsteht, lassen wir, wie in der Aussagenlogik, Klammerungen weg.

Will man konkrete Sachverhalte mit Hilfe der Prädikatenlogik ausdrücken, dann wählt man das zugrundeliegende Vokabular dementsprechend. Wir werden dies anhand von zwei Beispielen demonstrieren.

Beispiel 2.7

Zahlentheorie: Betrachte das Vokabular $\Sigma_N := (\Phi_N, \Pi_N, r_N)$, wobei

- $\Phi_N := \{0, \sigma, +, \times, \uparrow\}$

  0 ist eine Konstante und σ eine unäre Funktion (Nachfolgerfunktion). $+$ (Addition), $\times$ (Multiplikation) und $\uparrow$ (Exponentiation) sind binäre Funktionen.

- $\Pi_N := \{=, <\}$

  Beide Relationen $=$ und $<$ sind binär.

Ein Ausdruck über Σ_N ist z.B.:

$$\forall x < (+(x, \sigma(\sigma(0))), \sigma(\uparrow(x, \sigma(\sigma(0))))).$$

Üblicherweise werden derartige Ausdrücke vereinfacht, damit diese leichter zu lesen sind:

i) Verwendung von Infixnotation für Funktionen und Relationen. So schreibt man $(x \times 0)$ anstatt $\times(x, 0)$ oder auch $(y < y)$ anstatt

$<(y,y)$. Auch schreibt man 2 anstatt $\sigma(\sigma(0))$. Dies tut man für jede feste Anzahl der Anwendungen von σ auf 0:

$$5155 \text{ steht für } \underbrace{\sigma(\sigma(\sigma(\ldots(\sigma}_{5155 \text{ Anwendungen}}(0)\ldots))$$

Wenden wir diese Vereinfachungen auf obigen Ausdruck an, dann erhalten wir

$$\forall x\,((x+2) < \sigma((x \uparrow 2))).$$

Ein anderer Ausdruck über Σ_N ist z.B.:

$$((2 \times 3) + 3) = ((2 \uparrow 3) + 1).$$

Obige Ausdruck sind bis jetzt Zeichenfolgen ohne irgendeine mathematische Bedeutung.

$\Diamond$

Beispiel 2.8

Graphentheorie: Betrachte das Vokabular $\Sigma_G := (\Phi_G, \Pi_G, r_G)$, wobei

- $\Phi_G = \emptyset$, d.h., Σ_G enthält kein Funktionssymbol
- $\Pi_G = \{=, G\}$
  Beide Relationen $=$ und G sind binär.

Typische Ausdrücke über Σ_G sind z.B.:

$G(x,x)$

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

$\forall x(\forall y(G(x,y) \rightarrow G(y,x)))$

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

◊

Eine Variable kann mehrmals innerhalb des Textes eines Ausdruckes erscheinen. Zum Beispiel erschein x in $(\forall x(x+y>0)) \wedge (x>0)$ dreimal. Jedoch interpretiert man das x direkt nach $\forall$ als Teil des "Pakets" $\forall x$.

Ein Erscheinen einer Variablen x im Text eines Ausdruckes ϕ, das nicht direkt auf einen Quantor folgt, heißt ein <u>Vorkommen</u> von x in ϕ. Vorkommen einer Variablen kann <u>frei</u> oder <u>gebunden</u> sein. Intuitiv ist im obigen Ausdruck das Vorkommen von x in $x+y>0$ nicht frei, da es sich auf den Quantor $\forall x$ bezieht. Jedoch ist das zweite Vorkommen in $x>0$ frei. Demzufolge definieren wir:

Falls $\forall x \phi$ ein Ausdruck ist, dann heißt jedes Vorkommen von x in ϕ <u>gebunden</u>. Alle Vorkommen, die nicht gebunden sind, heißen <u>frei</u>.

Eine Variable, die ein freies Vorkommen in einem Ausdruck ϕ hat, ist eine <u>freie Variable</u> von ϕ (auch wenn dieselbe Variable andere gebundene Vorkommen in ϕ hat).

Ein Ausdruck ohne freie Variablen heißt Satz. Obiger Ausdruck ist kein Satz, da dieser zwei freie Variablen enthält. Dahingegen ist

$$\forall x (\forall y (\forall z (G(x,z) \wedge G(z,y)) \rightarrow G(x,y)))$$

ein Satz.

2.2.2 Strukturen und Modelle

Der Wahrheitswert eines prädikatenlogischen Ausdruckes ergibt sich aus den Werten seiner Bestandteile. Jedoch können in prädikatenlogischen Ausdrücken Variablen, Funktionen und Relationen komplexere Werte als wahr oder falsch annehmen. Das zu Belegungen analoge mathematische Objekt heißt Struktur.

Sei Σ ein fester Vokabular. Eine für Σ geeignete Struktur ist ein Paar $M := (U, \mu)$, wobei U eine beliebige aber nichtleere Menge, das sogenannte Universum von M, ist.
$\mu : V \cup \Phi \cup \Pi \rightarrow U$ ist eine Abbildung, die

- jeder Variablen $x \in V$ ein Element $x^M \in U$,
- jeder k-stelligen Funktion $f \in \Phi$ eine k-stellige Funktion $f^M : U^k \rightarrow k$ und
- jeder k-stelligen Relation $R \in \Pi$ eine k-stellige Relation $R^M \subseteq U^k$

zuordnet. Dabei wird der Gleichheitsrelation $=$ stets die Relation $=^M := \{ (u,u) \mid u \in U \}$ zugeordnet.

Bemerkung:
Falls $c \in \Phi$ eine Konstante ist, dann impliziert obige Definition, dass c^M ein Element von U ist.

Ziel:
Definition der Semantik eines Terms t in der Struktur M.

Wir definieren die Semantik von t induktiv.

i) Falls t eine Variable oder Konstante ist, dann ist t^M explizit durch M definiert.

ii) Falls $t = f(t_1, t_2, \dots, t_k)$ für eine k-stellige Funktion f, dann ist t^M definiert durch

$$f^M(t_1^M, t_2^M, \dots, t_k^M),$$

was ein Element des Universums U ist.

Sei ϕ ein Ausdruck über dem Vokabular Σ und M eine für Σ geeignete Struktur.

Ziel:
Definition, wann M den Ausdruck ϕ erfüllt (in Zeichen: $M \models \phi$).

Falls ϕ ein atomarer Ausdruck ist, d.h., $\phi = R(t_1, t_2, \dots, t_k)$, $R \in \Pi$ und $t_1, t_2, \dots, t_k$ sind Terme, dann erfüllt M den Ausdruck ϕ, falls $(t_1^M, t_2^M, \dots, t_k^M) \in R^M$.

Für nichtatomare Ausdrücke ϕ definieren wir die Erfüllbarkeit induktiv über den Aufbau von ϕ:

i) Falls $\phi = \neg \psi$, dann $M \models \phi$ falls $M \not\models \psi$.

ii) Falls $\phi = \psi_1 \vee \psi_2$, dann

$$M \models \phi \text{ falls } M \models \psi_1 \text{ oder } M \models \psi_2.$$

iii) Falls $\phi = \psi_1 \wedge \psi_2$, dann

$$M \models \phi \text{ falls } M \models \psi_1 \text{ und } M \models \psi_2.$$

$M_{x=u}$ bezeichnet diejenige Struktur, die wir aus M durch $x^{M_{x=u}} := u$ erhalten.

iv) Falls $\phi = \forall x \psi$, dann

$$M \models \phi \text{ falls } M_{x=u} \models \psi \text{ für alle } u \in U.$$

Folgendes Lemma zeigt, dass die Erfüllbarkeit eines Ausdruckes durch eine Struktur nicht von den Werten, die diese den nicht freien Variablen zuweist, abhängt.

<u>Lemma 2.4</u>

Seien ϕ ein Ausdruck über Σ und M und M' zwei für Σ geeignete Strukturen. Falls M und M' sich nur in Werten, die diese Variablen, die in ϕ nicht frei sind, zuweisen, unterscheiden, dann gilt genau dann $M \models \phi$ wenn $M' \models \phi$.

Beweis: (mittels Induktion über den Aufbau des Ausdruckes).

ϕ ist ein atomarer Ausdruck:

Dann sind alle Variablen in ϕ frei.

$\Rightarrow$

$$M = M'$$

Also gilt die Behauptung trivialerweise.

Annahme:

Die Behauptung gilt für die Ausdrücke ψ, ψ_1 und

$\phi = \neg \psi$:

Die freien Variablen in ϕ sind exakt dieselben wie in ψ. Also gilt

$$M \models \phi \iff M \not\models \psi \iff M' \not\models \psi \iff M' \models \phi.$$

$\phi = \psi_1 \wedge \psi_2$:

Die freien Variablen in ϕ ist die Vereinigung der freien Variablen in ψ_1 und in ψ_2.

Wenn M und M' sich nur bezüglich Werten, den diese nicht freien Variablen in ϕ zuweisen, unterscheiden, dann gilt dies auch bezüglich ψ_1 und ψ_2.

Induktionsannahme $\Rightarrow$

$$M \models \psi_i \iff M' \models \psi_i \quad \text{für } i = 1, 2$$

$\Rightarrow$

$$M \models \phi \Leftrightarrow (M \models \psi_1 \text{ und } M \models \psi_2)$$
$$\Leftrightarrow (M' \models \psi_1 \text{ und } M' \models \psi_2)$$
$$\Leftrightarrow M' \models \phi.$$

$\underline{\phi = \psi_1 \vee \psi_2}$:

analog Übung

$\underline{\phi = \forall x \psi}$:

Bis auf x sind die freien Variablen in ϕ exakt die freien Variablen in ψ. Die Variable x ist in ϕ gebunden. In ψ kann x frei sein oder nicht.

Definition $\Rightarrow$

$$M \models \phi \Leftrightarrow M_{x=u} \models \psi \text{ für alle } u \in U.$$

Induktionsannahme $\Rightarrow$

$$\left(M_{x=u} \models \psi \text{ für alle } u \in U \right)$$

$\Leftrightarrow \left((M_{x=u})' \models \psi \text{ für alle } u \in U \right)$ für alle Strukturen $(M_{x=u})'$, die sich nur bzgl. nicht-freie Variablen von ψ anders verhalten als $M_{x=u}$.

Im letzten Ausdruck variieren Werte der in ψ nichtfreie Variablen und Werte von x

$\Rightarrow$

Es variieren Werte der in ϕ nicht-freie Variablen

$\Rightarrow$

$M' \models \phi$ für alle M', die sich von M nur bezüglich in ϕ nicht freie Variablen unterscheiden.

<u>Beispiel 2.7</u> (Fortführung):

<u>Ziel</u>:

Definition einer für $\Sigma_N = (\Phi_N, \Pi_N, r_N)$ geeigneten Struktur $\mathcal{N} = (U, \mu)$.

- $U := \mathbb{N}_0$
- $\mu(0) = 0^{\mathcal{N}} := 0 \quad (\in \mathbb{N}_0)$
- $\mu(\sigma) := \sigma^{\mathcal{N}} : \mathbb{N}_0 \to \mathbb{N}_0$, wobei $\sigma^{\mathcal{N}}(n) := n+1$.
- $\mu(+)$ Addition
- $\mu(\times)$ Multiplikation
- $\mu(\uparrow)$ Exponentiation

- Für zwei Zahlen m und n gilt $m <^{\mathcal{N}} n$, falls m kleiner als n ist.
- μ bildet jede Variable auf die Zahl 0 ab.

<u>Beh. 1.</u>: $\mathcal{N} \models \forall x\,(x < x+1)$

<u>Bew.</u>:

Zum Beweis der Beh. 1 müssen wir unser Wissen bezüglich Eigenschaften von natürlichen Zahlen verwenden.

z.z. Für alle $n \in \mathbb{N}_0$ gilt $\mathcal{N}_{x=n} \models x < x+1$

D.h., wir müssen beweisen, dass für alle $n \in \mathbb{N}_0$

$$n <^{\mathcal{N}} n +^{\mathcal{N}} 1^{\mathcal{N}}.$$

Dies bedeutet $n < n+1$, was bekanntlich für jede ganze Zahl n gilt.

■

<u>Beh. 2</u>: $\mathcal{N} \not\models \forall x \exists y (x = y + y)$

<u>Bew.</u>:

Es gilt

$$\mathcal{N}_{x=1} \not\models \exists y (x = y + y)$$

oder äquivalent

$$\mathcal{N}_{x=1} \models \forall y \neg (x = y + y)$$

D.h., $1 \neq n + n$ für alle Zahlen n, was bekanntlich gilt.

■

◊

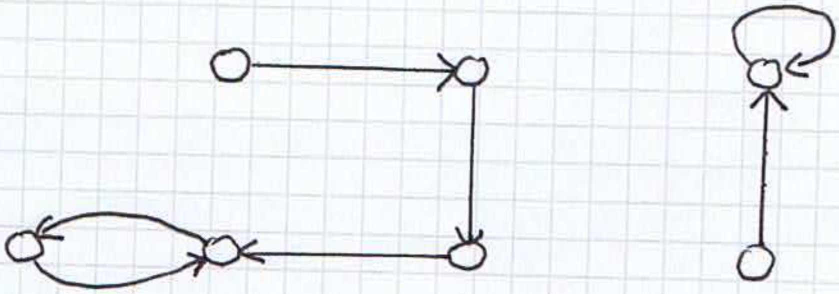
<u>Beispiel 2.8</u> (Fortführung)

Es gibt eine interessante Dualität zwischen Sätze und Strukturen. Eine Struktur erfüllt einen Satz oder erfüllt diesen nicht. Andererseits kann ein Satz als Beschreibung derjenigen Menge von Strukturen, die diesen erfüllen, angesehen werden. Wir illustrieren dies anhand des Vokabulars $\Sigma_G := (\Phi_G, \Pi_G, r_G)$.

Jede für Σ_G geeignete Struktur ist ein Graph. Wir betrachten nur endliche Graphen. Betrachte folgenden Satz:

$$\phi_1 := \left(\forall x \exists y\, G(x,y) \wedge \forall x \forall y \forall z ((G(x,y) \wedge G(x,z)) \rightarrow y = z)\right)$$

Folgende für Σ_G geeignete Struktur Γ erfüllt ϕ_1



Das Universum von Γ ist die Menge der sieben Knoten des Graphen im obigen Bild. Ferner gilt

$G^\Gamma(x,y)$, falls eine Kante von x nach y im obigen Graphen existiert.

Mittels Überprüfung überzeugt man sich, dass

$$\Gamma \models \phi_1.$$

<u>Frage:</u> Welche andere Graphen erfüllen ϕ_1?

<u>Übung:</u>
Zeigen Sie, dass genau diejenigen Graphen, deren Knoten alle den Ausgangsgrad eins haben, ϕ_1 erfüllen.

Somit erfüllen genau diejenigen Graphen, die eine <u>totale Funktion</u> repräsentieren ϕ_1.

Betrachte folgende Sätze:

$$\Phi_2 := \forall x(\forall y(\, G(x,y) \to G(y,x)))$$

$$\Phi_3 := \forall x(\forall y(\forall z\,(G(x,z) \wedge G(z,y)) \to G(x,y)))$$

Φ_2 erfüllen genau die Symmetrische und Φ_3 genau die transitive Graphen.

Lemma 2.4 besagt, dass die Tatsache, ob eine Struktur einen Ausdruck erfüllt oder nicht, nicht von denjenigen Werten abhängt, die die Struktur gebundenen oder im Ausdruck nicht vorkommenden Variablen zuordnet.

Wir sagen, dass eine Struktur für einen Ausdruck geeignet ist, wenn diese Struktur für alle im Ausdruck vorkommenden Funktionen, Relationen und freien Variablen definiert ist.

Eine für einen Ausdruck ϕ geeignete Struktur Γ heißt genau dann Modell für ϕ, wenn $\Gamma \models \phi$.

2.2.3 Gültige Ausdrücke

Ein Ausdruck ϕ heißt genau dann erfüllbar, wenn es ein Modell für ϕ gibt. ϕ heißt genau dann gültig, wenn jede für ϕ geeignete Struktur ein Modell für ϕ ist. Wenn ϕ gültig ist, dann schreiben wir $\models \phi$.

Lemma 2.5

Ein Ausdruck ist genau dann unerfüllbar, wenn seine Negation gültig ist.

Beweis:

Übung

∎

Frage: Was macht einen Ausdruck gültig?

Intuitiv ist ein Ausdruck aus grundlegenden Gründen, die etwas mit allgemeinen Eigenschaften von Funktionen, Gleichheit, Quantoren u.s.w. zu tun haben, gültig.

Ziel:

Herausarbeiten von solchen Basisgründen.

a) Aussagelogische Gültigkeit

Betrachten wir folgenden Ausdruck:

$$\phi := \forall x\, P(x) \;\vee\; \neg\forall x\, P(x).$$

ϕ hat die Form $\psi \vee \neg\psi$, wobei $\psi = \forall x\, P(x)$.

Wenn wir ψ als Boolesche Variable interpretieren, dann ist $\psi \vee \neg\psi$ eine Tautologie in der Aussagenlogik.

$\Rightarrow$

ϕ ist in der Prädikatenlogik ein gültiger Ausdruck.

Der Ausdruck

$$\big(G(x,y) \wedge G(y,x)\big) \rightarrow \big(G(y,x) \wedge G(x,y)\big)$$

ist gültig, da $\wedge$ kommutativ ist.

Obige prädikatenlogische Ausdrücke sind aus aus= sagelogischen Gründen gültig. Wir möchten diese Sichtweise verallgemeinern. Hierzu definieren wir für einen Ausdruck ϕ die Menge seiner Stammteilausdrücke $S(\phi)$:

i) ϕ atomarer Ausdruck oder $\phi = \forall x \psi$.
Dann besitzt ϕ genau einen Stammteil= ausdruck, nämlich sich selbst.

ii) $\phi = \neg\psi$.
Dann gilt $S(\phi) := S(\psi)$.

iii) $\phi = \psi_1 \vee \psi_2$ oder $\phi = \psi_1 \wedge \psi_2$.
Dann gilt $S(\phi) := S(\psi_1) \cup S(\psi_2)$.

Beispiel 2.9:

Betrachte

$$\phi := \forall x\, G(x,y) \wedge \exists x\, G(x,y) \wedge \big(G(z,x) \vee \forall x\, G(x,y)\big)$$

Zunächst expandieren wir

$$\exists x\, G(x,y) \text{ zu } \neg\forall x \neg G(x,y)$$

und erhalten dann

$$S(\phi) = \{ \forall x G(x,y),\ \forall x \neg G(x,y),\ G(z,x) \}$$

◊

Jeder prädikatenlogischer Ausdruck ϕ kann als aussagelogischer Ausdruck mit Stammteilausdrücke anstatt Booleschen Variablen interpretiert werden. Wir nennen dies die <u>aussagelogische Form</u> von ϕ.

<u>Beispiel 2.9</u> (Fortführung):

Die aussagenlogische Form von ϕ ist

$$x_1 \wedge (\neg x_2) \wedge (x_3 \vee x_1),$$

wobei $x_1 = \forall x G(x,y)$, $x_2 = \forall x \neg G(x,y)$ und $x_3 = G(z,x)$.

◆

<u>Lemma 2.6</u>

Wenn die aussagelogische Form eines prädikatenlogischen Ausdruckes ϕ eine Tautologie ist, dann ist ϕ gültig.

<u>Beweis</u>:

Sei M eine beliebige für ϕ geeignete Struktur. Jeder Stammteilausdruck von ϕ wird von M erfüllt oder nicht erfüllt. Dies definiert eine Belegung der Stammteilausdrücke von ϕ. Da die aussagenlogische Form von ϕ eine Tautologie ist, muss dies ϕ erfüllen.

■

Mit Hilfe der Aussagenlogik können nicht nur neue gültige Ausdrücke identifiziert sondern auch bekannte gültige Ausdrücke zu neuen kombiniert werden.

Wenn ϕ und ψ gültig sind, dann folgt hieraus die Gültigkeit von $\phi \wedge \psi$. Wenn ϕ und ϕ ψ gültig sind, dann ist auch ψ gültig.

<u>Lemma 2.7</u> (<u>Modus Ponens</u>):
Wenn ϕ und $\phi \rightarrow \psi$ gültig sind, dann ist auch ψ gültig.

b) <u>Gleichheit</u>

Ein Ausdruck kann auch aufgrund der Eigenschaften der Gleichheit gültig sein. So ist z.B. $x+1 = x+1$ gültig. Betrachte

$$\phi := x = 1 \rightarrow 1+1 = x+1.$$

Dieser Ausdruck ist unabhängig von der Semantik von 1 und + gültig. Wenn $x = 1$, dann führt jede Funktion, angewandt auf die Argumente $x, 1$ und auf $1, 1$ zum selben Resultat.

Dasselbe gilt für den Ausdruck

$$x = y \rightarrow (G(x,x) \rightarrow G(y,x)).$$

Falls $x = y$, dann impliziert $G(x,x)$ unabhängig von der Bedeutung von G auch $G(y,x)$.

Insgesamt gilt folgendes Lemma:

Lemma 2.8

Seien $t_1, t_2, \ldots, t_k, t_1', t_2', \ldots, t_k'$ Terme. Dann ist jeder der folgenden Ausdrücken gültig:

i) $t_1 = t_1$,

ii) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \ldots \wedge t_k = t_k') \rightarrow$
$$f(t_1, t_2, \ldots, t_k) = f(t_1', t_2', \ldots, t_k')$$ und

iii) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \ldots \wedge t_k = t_k') \rightarrow$
$$(R(t_1, t_2, \ldots, t_k) \rightarrow R(t_1', t_2', \ldots, t_k')).$$

c) Quantoren

Des Weiteren kann ein Ausdruck aufgrund der Bedeutung der Quantoren gültig sein. So ist z.B. der Ausdruck

$$G(x,1) \rightarrow \exists z\, G(x,z)$$

gültig. In jeder geeigneten Struktur impliziert im Falle, dass $G(x,1)$ gilt, dass es ein z gibt, so dass $G(x,z)$ gilt; nämlich $z = 1$.

Auch ist $\forall x\, G(x,y) \rightarrow G(z,y)$ gültig. Wenn es von jedem Knoten eine Kante zum Knoten y existiert, dann gibt es auch eine von z nach y.

Sein ϕ ein Ausdruck, x eine Variable und t ein Term. Die <u>Substitution von x durch t in ϕ</u> $\phi[x := t]$ ist derjenige Ausdruck, den wir aus ϕ nach Ersetzung von allen freien Vorkommen der Variablen durch den Term t erhalten.

<u>Beispiel 2.10</u>

Seien

$$\phi := (x=1) \to \exists x\,(x=y) \quad \text{und } t = y+1.$$

Dann erhalten wir

$$\phi[x:=t] = (y+1=1) \to \exists x\,(x=y) \quad \text{und}$$

$$\phi\,[y:=t] = (x=1) \to \exists\,(x=y+1).$$

$\Diamond$

Es gibt ein Problem mit obiger Definition falls t eine Variable, die an einer Position in der x vorkommt gebunden ist, enthält.

<u>Beispiel 2.10</u> (Fortführung)

Betrachte folgende Modifikation von ϕ:

$$\phi' := (x=1) \to \exists y\,(x=y)$$

Dann gilt:

$$\phi'[x:=t] = (y+1=1) \to \exists y\,(y+1=y),$$

was nicht unser Verständnis der Addition entspricht.

Um derartige Probleme zu vermeiden definieren wir, dass t genau dann <u>für x in ϕ substituierbar</u> ist, wenn es in t keine Variable y, die in einem Teilausdruck von ϕ der Form $\forall y \psi$ oder $\exists y \psi$ frei vorkommt, gibt.

Wir wenden die Notation $\phi[x:=t]$ nur dann verwenden, wenn t für x in ϕ substituierbar ist. Dies bedeutet, dass die Verwendung dieser Notation diese Annahme implizit enthält.

<u>Lemma 2.9</u>

Jeder Ausdruck der Form $\forall x \phi \to \phi[x:=t]$ ist gültig.

<u>Bemerkung:</u>

Lemma 2.9 impliziert, dass der Ausdruck $\phi[x:=t] \to \exists x \phi$ gültig ist.

<u>Lemma 2.10</u>

Falls ϕ gültig ist, dann ist auch $\forall x \phi$ gültig.

<u>Lemma 2.11</u>

Falls x nicht frei in ϕ vorkommt, dann ist der Ausdruck $\phi \to \forall x \phi$ gültig.

<u>Lemma 2.12</u>

Für alle ϕ und ψ ist der Ausdruck

$$(\forall x(\phi \to \psi)) \to ((\forall x \phi) \to (\forall x \psi))$$

gültig.

Übung:
Beweisen Sie die Lemmata 2.9 – 2.12.

d) Die Pränexnormalform

Mit Hilfe der Gültigkeit können wir Ausdrücke vereinfachen. Falls $\phi \Leftrightarrow \psi$ gültig ist, dann können wir in einem Ausdruck den Teilausdruck ϕ durch ψ ersetzen. Die sorgfältige Anwendung von solchen Ersetzungen führt zu einfacheren Ausdrücke. Falls $\phi \Leftrightarrow \psi$ gültig ist, dann schreiben wir $\phi \equiv \psi$, d.h. ϕ und ψ sind äquivalent.

Lemma 2.13
Seien ϕ und ψ beliebige prädikatenlogische Ausdrücke. Dann gilt:

i) $\forall x(\phi \wedge \psi) \equiv (\forall x \phi \wedge \forall x \psi)$.
ii) Falls x nicht frei in ψ vorkommt, dann
$\forall x(\phi \wedge \psi) \equiv (\forall x \phi \wedge \psi)$.
iii) Falls x nicht frei in ψ vorkommt, dann
$\forall x(\phi \vee \psi) \equiv (\forall x \phi \vee \psi)$.
iv) Falls y nicht in ϕ vorkommt, dann
$\forall x \phi \equiv \forall y \phi[x := y]$.

Beweis:

Übung

$\blacksquare$

Ein prädikatenlogischer Ausdruck ist in Pränexnormalform, falls er aus einer Folge von Quantoren gefolgt von einem Ausdruck ohne Quantoren besteht.

Ziel:

Umformung eines beliebigen prädikatenlogischen Ausdruckes in einen äquivalenten Ausdruck in Pränixnormalform.

Beispiel 2.11

Betrachte folgenden Ausdruck:

$$(\forall x (G(x,x) \wedge (\forall y\, G(x,y) \vee \exists y \neg G(y,y))) \wedge G(x,0).$$

Wir wenden zunächst Lemma 2.13 iv) an um verschiedene Variablennamen zur jeder Quantifizierung und jeder freien Variablen zuzuweisen.

$\rightsquigarrow$

$$(\forall x (G(x,x) \wedge (\forall y\, G(x,y) \vee \exists z \neg G(z,z))) \wedge G(w,0).$$

Unter Verwendung von Lemma 2.13 ii) bringen wir $\forall x$ nach draußen.

$\rightsquigarrow$

$$\forall x ((G(x,x) \wedge (\forall y\, G(x,y) \vee \exists z \quad G(z,z))) \wedge G(w,0)$$

Anwendung von Le. 2.13 iii) und dann ii) bringt

$\forall y$ nach draußen.

$\rightsquigarrow$

$$\forall x \forall y ((G(x,x) \wedge (G(x,y) \vee \exists z \neg G(z,z))) \wedge G(w,0))$$

Unter Anwendung der DeMorgan'schen Regeln machen wir $\exists z$ zu $\forall z$.

$\rightsquigarrow$

$$\forall x \forall y ((G(x,x) \wedge \neg(\neg G(x,y) \wedge \forall z\, G(z,z))) \wedge G(w,0)$$

Nun bringen wir $\forall z$ nach draußen:

$$\forall x \forall y ((G(x,x) \wedge \neg \forall z (\neg G(x,y) \wedge G(z,z))) \wedge G(w,0)$$

Das Ganze noch einmal:

$\rightsquigarrow$

$$\forall x \forall y (\neg(\neg G(x,x) \vee \forall z (\neg(G(x,y) \wedge G(z,z))) \wedge G(w,0)$$

$\rightsquigarrow$

$$\forall x \forall y (\neg \forall z (\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \wedge G(w,0)$$

DeMorgan $\rightsquigarrow$

$$\forall x \forall y \neg (\forall z (\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \vee \neg G(w,0)$$

$\rightsquigarrow$

$$\forall x \forall y \neg \forall z ((\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \vee \neg G(w,0)$$

Umformung von $\neg \forall z$ nach $\exists z$ $\rightsquigarrow$

$$\forall x \forall y \exists z \neg ((\neg G(x,x) \vee (\neg G(x,y) \wedge G(z,z))) \vee \neg G(w,0))$$

Der letzte Ausdruck ist in Pränexnormalform.

♦

Allgemein gilt der folgende Satz:

Satz 2.3

Jeder prädikatenlogischer Ausdruck kann in einen äquivalenten Ausdruck in Pränexnormalform transformiert werden.

Beweis:

Übung

■

2.2.4 Axiome und Beweise

Bisher haben wir die Syntax und die Semantik eines Systems, in dem wir mathematische Aussagen formulieren können, definiert. Was noch fehlt ist eine systematische Methode, mittels der wir beweisen können, dass eine Aussage wahr ist. Zunächst müssen wir definieren, was wir darunter verstehen, dass eine Aussage wahr ist. In der Prädikatenlogik können wir "Wahrheit" und Gültigkeit identifizieren. Dies bedeutet, dass wir dann eine systematische Methode benötigen, mittels der wir die Gültigkeit von Ausdrücken beweisen können. Hierzu konstruieren wir ein Beweissystem das auf den Basisgründen für die Gültigkeit und den Lemmata 2.7 - 2.12 aufbaut. Dieses wir auf Ausdrücken über einem festen Vokabular Σ anwendbar sein.

Unser Beweissystem baut auf einer aufzähl=bar unendlichen Menge von <u>logischen Axiomen</u> auf. Diese sind unsere <u>elementare gültige Ausdrücke</u>.

<u>Basisaxiome</u>:

AX 0: Alle Ausdrücke, deren aussagelogische Form eine Tautologie ist.

AX 1: Alle Ausdrücke, die eine der folgenden Formen haben ($k \in \mathbb{N}$):

a) $t = t$.

b) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \dots \wedge t_k = t_k') \rightarrow$
$f(t_1, t_2, \dots, t_k) = f(t_1', t_2', \dots, t_k')$

c) $(t_1 = t_1' \wedge t_2 = t_2' \wedge \dots \wedge t_k = t_k') \longrightarrow$
$(R(t_1, t_2, \dots, t_k) \rightarrow R(t_1', t_2', \dots, t_k'))$.

AX 2: Alle Ausdrücke der Form
$$\forall x \phi \rightarrow \phi[x := t].$$

AX 3: Alle Ausdrücke der Form
$$\phi \rightarrow \forall x \phi,$$
wobei x nicht frei in ϕ vorkommt.

AX 4: Alle Ausdrücke der Form
$$(\forall x (\phi \rightarrow \psi)) \rightarrow (\forall x \phi \rightarrow \forall x \psi).$$

AX 5: Alle Ausdrücke der Form $\forall x \phi$, wobei ϕ ein elementarer gültiger Ausdruck ist.

Unter Verwendung von Modus ponens (Lemma 27) kann unser Beweissystem neue (nicht=

elementare) gültige Ausdrücke generieren. Betrachten wir eine endliche Folge

$$S = \phi_1, \phi_2, \ldots, \phi_n$$

von prädikatenlogischen Ausdrücken, wobei für jeden Ausdruck ϕ_i, $1 \leq i \leq n$ in dieser Folge gilt:

a) $\phi_i \in \mathfrak{A}$, wobei $\mathfrak{A}$ die Menge der elementaren gültigen Ausdrücke ist

oder

b) es existieren unter $\phi_1, \phi_2, \ldots, \phi_{i-1}$ zwei Ausdrücke der Form ψ bzw. $\psi \to \phi_i$ (Anwendung von Modus ponens)

Dann ist S ein <u>Beweis</u> (oder auch <u>Ableitung</u>) des Ausdrucks ϕ_n. Der Ausdruck ϕ_n heißt dann <u>Satz der Prädikatenlogik</u> und wir schreiben $\vdash \phi_n$.

<u>Bemerkung:</u>

Wenn $\vdash \phi$, dann ist der Ausdruck ϕ gültig. Wenn $\models \phi$, dann ist der Ausdruck ϕ auch gültig. Jedoch muss nicht notwendigerweise ϕ aus den Axiomen ableitbar sein; d.h., es muss nicht notwendigerweise $\vdash \phi$ gelten.

Beispiel 2.12

- Die Reflexivität $x = x$ der Gleichheit ist ein Axiom.

- Die Symmetrie $x = y \to y = x$ der Gleichheit ist ein Satz der Prädikatenlogik. Diesen werden wir nun beweisen.

Betrachten wir folgende Folge von Ausdrücken:

$$S = \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5 \quad ,$$

wobei

$$\varphi_1 := (x = y \wedge x = x) \to (x = x \to y = x)$$
$$\varphi_2 := (x = x)$$
$$\varphi_3 := x = x \to ((x = y \wedge x = x) \to (x = x \to y = x)) \to (x = y \to y = x)$$
$$\varphi_4 := ((x = y \wedge x = x) \to (x = x \to y = x)) \to (x = y \to y = x)$$
$$\varphi_5 := (x = y \to y = x)$$

Wir werden nun zeigen, dass S ein Beweis des Ausdruckes $x = y \to y = x$ ist.

φ_1 ist ein Axiom der Gruppe AX 1 c), wobei

$k = 2$, R ist die Gleichheit, $t_1 = t_2 = t_2' = x$ und $t_1' = y$.

φ_2 ist ein Axiom der Gruppe AX 1 a).

ϕ_3 ist ein Axiom der Gruppe AXO
(überzeugen Sie sich).

ϕ_4 erhalten wir aus ϕ_2 und ϕ_3 mittels Modus ponens.

ϕ_5 erhalten wir aus ϕ_1 und ϕ_4 mittels Modus ponens.

Insgesamt haben wir $\vdash x = y \rightarrow y = x$ gezeigt.

◆

Sei Δ eine Menge von Ausdrücke und $\phi \notin \Delta$ ein weiterer Ausdruck. Φ ist genau dann eine <u>gültige Konsequenz von Δ</u>, wenn jede Struktur, die jeden Ausdruck in Δ erfüllt auch ϕ erfüllt. Wir schreiben dann $\Delta \models \phi$.

<u>Ziel</u>:
Verallgemeinerung des obigen Beweissystems.

Sei Δ eine Menge von Ausdrücken. Sei

$$S := \phi_1, \phi_2, \dots, \phi_n$$

eine Folge von Ausdrücken, wobei für jeden Ausdruck ϕ_i, $1 \leq i \leq n$ in dieser Folge gilt:

a) $\phi_i \in \mathfrak{A}$ oder
b) $\phi_i \in \Delta$ oder
c) es existieren unter $\phi_1, \phi_2, \dots, \phi_{i-1}$ zwei Ausdrücke der Form ψ bzw. $\psi \rightarrow \phi_i$ (Anwendung von Modus ponens)

Dann ist S ein Beweis (oder Ableitung) des Ausdruckes ϕ_n aus Δ. Der Ausdruck ϕ_n heißt dann Δ-Satz der Prädikatenlogik und wir schreiben $\Delta \vdash \phi_n$.

Bemerkung:
Beachte auch hier den Unterschied von $\Delta \vdash \phi$ und $\Delta \models \phi$.

Im obigen erweiterten Beweissystem heißen die Ausdrücke in Δ nichtlogische Ausdrücke des Beweissystems.

Ziel:
Herausarbeiten von drei Standardbeweismethoden der Mathematik.

Satz 2.4 (Deduktionstechnik)

Nehmen wir an, dass $\Delta \cup \{\phi\} \vdash \psi$. Dann gilt $\Delta \vdash \phi \to \psi$.

Beweis:
Betrachten wir einen Beweis $S = \phi_1, \phi_2, \dots, \phi_n$ von ψ aus $\Delta \cup \{\phi\}$. D.h., $\phi_n = \psi$.

Idee:
Beweis mittels Induktion über i, dass

$$\phi \to \phi_i \text{ aus } \Delta \text{ für } i = 1, 2, \dots, n.$$

Hieraus folgt dann wegen $\phi_n = \psi$ die Behauptung.

Durchführung:

$i = 1$:

Da $S = \phi_1, \phi_2, \ldots, \phi_n$ ein Beweis von ψ aus $\Delta \cup \{\phi\}$ ist, gilt $\phi_1 \in \mathfrak{A} \cup \Delta \cup \{\phi\}$.

Falls $\phi_1 = \phi$, dann ist $\phi \to \phi$ ein Axiom aus der Gruppe AX0 und somit ein Beweis für $\phi \to \phi$.

Falls $\phi_1 \in \mathfrak{A} \cup \Delta$, dann ist

$$\phi_1, \phi_1 \to (\phi \to \phi_1), \phi \to \phi_1$$

ein Beweis für $\phi \to \phi_1$ aus Δ, da

a) $\phi_1 \in \mathfrak{A} \cup \Delta$ gemäß Annahme,
b) $\phi_1 \to (\phi \to \phi_1)$ Axiom aus AX0 und
c) $\phi \to \phi_1$ aus den vorangegangenen Ausdrücken mittels modus ponens entsteht.

Annahme:
$1 \leq i < n$ und $\phi \to \phi_j$ für $1 \leq j \leq i$.

$i \leadsto i+1$:

Der Beweis für $\phi \to \phi_{i+1}$ enthält alle Beweise der Ausdrücke $\phi \to \phi_j$, $1 \leq j \leq i$ erweitert um einige neue Ausdrücke, die von ϕ_{i+1} abhängen. Bezüglich ϕ_{i+1} sind drei Fälle möglich:

1) $\phi_{i+1} = \phi$

Dann fügen wir $\phi \to \phi$, was ein Axiom aus AX0 ist, dem Beweis hinzu.

2) $\phi_{i+1} \in \mathfrak{A} \cup \Delta$

Dann erweitern wir den Beweis mit

$$\phi_{i+1},\ \phi_{i+1} \to (\phi \to \phi_{i+1}),\ \phi \to \phi_{i+1}$$

Dies ist ein Beweis für $\phi \to \phi_{i+1}$ aus Δ (Begründung s.o.).

3) ϕ_{i+1} erhält man in S aus einem ϕ_j und $\phi_j \to \phi_{i+1}$ mittels Modus ponens, wobei $j \leq i$.

Dann enthält unser Beweis bereits

$$\phi \to \phi_j \quad \text{und} \quad \phi \to (\phi_j \to \phi_{i+1}).$$

Wir erweitern unseren Beweis um die Ausdrücke

$$(\phi \to \phi_j) \to ((\phi \to (\phi_j \to \phi_{i+1})) \to (\phi \to \phi_{i+1})),$$
$$(\phi \to (\phi_j \to \phi_{i+1})) \to (\phi \to \phi_{i+1}) \quad \text{und}$$
$$\phi \to \phi_{i+1}$$

Der erste Ausdruck ist ein Axiom der Gruppe AX0. Die beiden anderen Ausdrücke entstehen mittels Modus ponens. (überzeugen Sie sich).

■

Bemerkung:

Nur im 3. Fall benötigen wir die Induktionsvoraus =

setzung.

Als nächstes betrachten wir den Widerspruchsbeweis. D.h., um ϕ zu beweisen nehmen wir $\neg\phi$ an und führen diese Annahme zu einem Widerspruch.

Formal kann ein Widerspruch durch einen Ausdruck

$$\psi \wedge \neg\psi ,$$

wobei ψ ein beliebiger Ausdruck ist, definiert werden.

Falls es einen Beweis von $\psi \wedge \neg\psi$ aus Δ gibt, dann gilt $\Delta \vdash \phi$ für alle Ausdrücke ϕ.

Übung:
Zeigen Sie, dass $\Delta \vdash \psi\wedge\neg\psi$ auch $\Delta \vdash \phi$ für jeden Ausdruck ϕ impliziert.

Falls $\Delta \vdash \phi$ für alle Ausdrücke ϕ, dann heißt Δ inkonsistent. Falls kein Widerspruch aus Δ bewiesen werden kann, dann heißt Δ konsistent.

Satz 2.5 (Widerspruchsbeweis)

Falls $\Delta \cup \{\neg\phi\}$ inkonsistent ist, dann gilt $\Delta \vdash \phi$.

Beweis:

Annahme: $\Delta \cup \{\neg\phi\}$ ist inkonsistent.

Dann gilt

$$\Delta \cup \{\neg\phi\} \vdash \phi$$

Satz 2.4 $\Rightarrow$

$$\Delta \vdash \neg\phi \rightarrow \phi$$

Wir erweitern den Beweis von $\neg\phi \rightarrow \phi$ aus Δ durch Hinzufügen der Folge

$$(\neg\phi \rightarrow \phi) \rightarrow \phi, \ \phi$$

Der erste Ausdruck ist ein Axiom der Gruppe AX0. Den zweiten Ausdruck erhalten wir mittels Modus ponens aus $\neg\phi \rightarrow \phi$ und dem ersten Ausdruck.

∎

Häufig nimmt man aus einer Menge ein beliebiges, aber festes Element und beweist für dieses eine Eigenschaft. Da dieses Element aus der Menge beliebig gewählt worden ist, schließt man nun daraus, dass jedes Element der Menge diese Eigenschaft besitzt. Diese Vorgehensweise heißt gerechtfertigte Verallgemeinerung.

Satz 2.6 (gerechtfertigte Verallgemeinerung)

Nehmen wir an, dass $\Delta \vdash \phi$ und x in keinem Ausdruck in Δ frei vorkommt. Dann gilt $\Delta \vdash \forall x\, \phi$.

Beweis:

Betrachten wir einen Beweis

$$S := \phi_1, \phi_2, \dots, \phi_n$$

von ϕ aus Δ (d.h., $\phi_n = \phi$).

Idee:

Beweise mittels Induktion über i, dass

$$\Delta \vdash \forall x\, \phi_i \quad \text{für } i = \;,\;, \dots, n.$$

Hieraus folgt dann wegen $\phi_n = \phi$ die Behauptung.

Durchführung:

$i = 1$:

Es gilt $\phi_1 \in \mathfrak{A} \cup \Delta$.

1) $\phi_1 \in \mathfrak{A}$

Dann ist auch $\forall x\, \phi_1 \in \mathfrak{A}$.

2) $\phi_1 \in \Delta$

Dann ist ϕ_1 ein nichtlogisches Axiom. Gemäß Voraussetzung kommt x nicht frei in ϕ_1 vor.

$\Rightarrow$

Die Folge $\phi_1,\ \overset{\text{AX3}}{\phi_1 \rightarrow \forall x\, \phi_1},\ \forall x\, \phi_1$ ist ein Beweis für $\forall x\, \phi_1$ aus Δ.

Annahme:

$1 \leq i < n$ und $\Delta \vdash \forall x\, \phi_j$ für $1 \leq j \leq i$.

$i \rightsquigarrow i+1$:

Der Beweis für $\forall x\, \phi_{i+1}$ enthält alle Beweise für die Ausdrücke $\forall x\, \phi_j$, $1 \leq j \leq i$, erweitert um einige neue Ausdrücke, die von ϕ_{i+1} abhängen. Bezüglich ϕ_{i+1} sind drei Fälle möglich:

1) $\phi_{i+1} \in \mathfrak{A}$.

Dann gilt auch $\forall x\, \phi_{i+1} \in \mathfrak{A}$ und wir fügen $\forall x\, \phi_{i+1}$ dem Beweis hinzu.

2) $\phi_{i+1} \in \Delta$.

Dann ist ϕ_{i+1} ein nichtlogisches Axiom. Gemäß Voraussetzung kommt x nicht frei in ϕ_{i+1} vor.

Wir erweitern unseren Beweis um die Ausdrücke

$$\phi_{i+1},\ (\underset{\Uparrow}{\overset{AX3}{}}\phi_{i+1} \to \forall x\, \phi_{i+1}),\ \forall x\, \phi_{i+1}$$

3) ϕ_{i+1} erhält man in S aus einem ϕ_j und $\phi_j \to \phi_{i+1}$ mittels Modus ponens, wobei $j \leq i$.

Induktionsannahme $\Rightarrow$

Unser Beweis enthält bereits

$\forall x \phi_j$ und $\forall x(\phi_j \to \phi_{i+1})$

Wir erweitern unseren Beweis um die Ausdrücke

$(\forall x(\phi_j \to \phi_{i+1})) \to (\forall x \phi_j \to \forall x \phi_{i+1}) \in AX$

$\forall x \phi_j \to \forall x \phi_{i+1}$ Modus ponens

$\forall x \phi_{i+1}$ Modus ponens.

■

Beispiel 2.13

a) Beh.: $\vdash \forall x \forall y \phi \to \forall y \forall x \phi$.

Bew.:

Sei $\phi_1 := \forall x \forall y \phi$.

Für die Anwendung der Deduktionstechnik nehmen wir an, dass die Voraussetzung des gewünschten Ausdrucks erfüllt ist. D.h., wir setzen

$\Delta := \{\phi_1\}$.

Wir erweitern die bisherige Folge ϕ_1 durch

$\phi_2 := \forall x \forall y \phi \to \forall y \phi \quad \in AX2$, da

$\forall x \forall y \to \forall y \phi[x \leftarrow x] \in AX2$

$\phi_3 := \forall y \phi \to \phi \quad \in AX2$

$\phi_4 := \forall y \phi$ Modus ponens

$\phi_5 := \phi$ Modus ponens

$\phi_6 := \forall x\, \phi$ gerechtfertigte Verallgemeinerung
(Beachte, dass x nicht in ϕ_1 frei vorkommt)

$\phi_7 := \forall y \forall x\, \phi$ gerechtfertigte Verallgemeinerung

Also haben wir gezeigt:

$$\emptyset \cup \{\forall x \forall y\, \phi\} \vdash \forall y \forall x\, \phi$$

$\overset{\Longrightarrow}{\text{Satz 2.4}}$ $\vdash \forall x \forall y\, \phi \rightarrow \forall y \forall x\, \phi.$

$\blacksquare$

b) <u>Beh.</u>: $\vdash \forall x\, \phi \rightarrow \exists x\, \phi$

<u>Bew.</u>: Setze $\phi_1 := \forall x\, \phi$ und $\Delta := \{\phi_1\}$.

Wir erweitern die Folge ϕ_1 durch

$\phi_2 := (\forall x\, \phi) \rightarrow \phi$ $\in AX2$

$\phi_3 := \phi$ Modus ponens

$\phi_4 := \forall x\, \neg\phi \rightarrow \neg\phi$ $\in AX2$

$\phi_5 := (\forall x \neg\phi \rightarrow \neg\phi) \rightarrow (\phi \rightarrow \exists x\, \phi)$ $\in AX0$
(Beachte, dass $\exists$ eine Abkürzung ist.)

$\phi_6 := \phi \rightarrow \exists x\, \phi$ Modus ponens

$\phi_7 := \exists x\, \phi$ Modus ponens

$\blacksquare$

c) Beh.: Seien ϕ und ψ zwei Ausdrücke, die bis auf folgenden Unterschied identisch sind:

ϕ hat genau an denjenigen Positionen freie Vorkommen von x in denen ψ freie Vorkommen von y hat. Dann gilt:

$$\vdash \forall x \phi \to \forall y \psi .$$

Bew.:

Setze $\phi_1 := \forall x \phi$ und $\Delta := \{\phi_1\}$.
Wir erweitern die Folge ϕ_1 durch:

$\phi_2 := \forall x \phi \to \psi \quad \in AX2$, da $\psi = \phi[x \leftarrow y]$.
$\phi_3 := \psi \quad$ Modus ponens
$\phi_4 := \forall y \psi \quad$ gerechtfertigte Verallgemeinerung
Beachte: y ist nicht frei in $\forall x \phi$.

Der nächste Satz zeigt, dass unser Beweissystem nur gültige Konsequenzen beweist.

Satz 2.7
Wenn $\Delta \vdash \phi$, dann $\Delta \models \phi$.

Beweis:

Übung