NULLSTELLENSATZ

Anwendungen der Logik, SS 2008, Martin Goldstern

Galoisverbindungen

Sei X eine Menge von „Objekten“ (zB Punkten in $\mathbb{R}^n$), und E eine Menge von „Eigenschaften“ oder „Merkmalen“ (zB Hyperebenen im $\mathbb{R}^n$). Sei weiters $R \subseteq X \times E$ eine Relation (zB „Punkt x liegt in der Hyperebene e“.)
Für jede Menge $A \subseteq X$ definieren wir $A^\uparrow := \{e \in E : \forall x \in A\ (x,e) \in R\}$, und für jede Menge $B \subseteq E$ sei $B^\downarrow := \{x \in X : \forall e \in B\ (x,e) \in R\}$.
Man sieht leicht, dass $A \subseteq A^{\uparrow\downarrow}$ und $B \subseteq B^{\downarrow\uparrow}$ für alle A, B gilt.
Weiters gilt $A^{\uparrow\downarrow\uparrow} = A^\uparrow$ und die dazu duale Aussage. Die Elemente der Menge

$$\{B \subseteq E : B^{\downarrow\uparrow} = B\} = \{A^\uparrow : A \subseteq X\}$$

heißen die „Galois-abgeschlossenen“ Teilmengen von B; analog sind die Galois-abgeschlossenen Teilmengen von A definiert.
(Im Beispiel sind die Galois-abgeschlossenen Untermengen von X genau die affinen Unterräume von X.)
Oft ist es von Interesse, den Abschlussoperator $A \mapsto A^{\uparrow\downarrow}$ durch einen „Erzeugungsprozess“ zu charakterisieren, sozusagen „von unten“. (Im Beispiel: „erzeugter Unterraum“, durch gewisse Linearkombinationen.)

Oft ist es praktisch, eine Eigenschaft zur Verfügung zu haben, die von keinem $x \in X$ erfüllt wird.
Wenn $\perp$ so eine Eigenschaft ist, dann gilt offenbar

- $\perp \in B \ \Rightarrow\ B^\downarrow = \emptyset$
- $B^\downarrow = \emptyset \ \Leftrightarrow\ \perp \in B^{\downarrow\uparrow}$. (Wir nennen so ein B „unerfüllbar“ oder „inkonsistent“

Weitere Beispiele können Sie sich selbst überlegen:

(1) E = Menge aller aussagenlogischen Formeln, X = Menge aller Belegungen. $(x,e) \in R$ wenn die Belegung e die Formel x erfüllt.
(2) E = Menge aller Klauseln, X = Menge aller Belegungen.
(3) E = Menge aller geschlossenen prädikatenlogischen Formeln (für eine fixe Sprache L), X = Menge aller Strukturen für diese Sprache.[1]
(4) X = Menge aller Unterstrukturen einer festen Struktur S, E = Menge aller Automorphismen von S, $(x,e) \in R$ wenn der Automorphismus e auf der Unterstruktur x die Identität ist.
(5) $\cdots$

Ich überlasse es dem Leser, in jedem dieser Fälle die Relation R, die Operatoren $^{\downarrow\uparrow}$ und $^{\uparrow\downarrow}$ bzw die Galois-abgeschlossenen Mengen explizit zu beschreiben. (Hinweis: Vollständigkeitssatz, Resolutionsalgorithmus, klassische Galoistheorie.)

[1] Eigentlich eine Klasse. Betrachten wir lieber alle Strukturen auf einer festen Grundmenge.

Ein einfaches Beispiel: Lineare Gleichungen

In diesem Abschnitt betrachten wir nur Polynome vom Grad ≤ 1.
Betrachten wir zwei Polynome p_1, p_2, zB

$$\begin{aligned} p_1(x,y,z) &= 2x - y + 4z - 1 \\ p_2(x,y,z) &= 3x + y - 2z + 5 \end{aligned}$$

In der linearen Algebra lernen wir Methoden, um die folgende Fragen zu beantworten:

(1) Gibt es eine gemeinsame (reelle) Nullstelle der beiden Polynome?

Tatsächlich betrachtet man auch noch weiterführende Fragen, wie zB

(2) Wie sehen alle gemeinsamen Nullstellen der vorgegebenen Gleichungen aus?
(3) Wenn (x_0, y_0, z_0) eine gemeinsame Nullstelle ist, welche Gleichungen muss (x_0, y_0, z_0) sonst noch erfüllen, d.h. welche anderen Polynome „annullieren“ (x_0, y_0, z_0) sonst noch?

Es ist offensichtlich, dass jede Linearkombination der beiden Polynome

$$\lambda \cdot p_1(x,y,z) + \mu \cdot p_2(x,y,z) \qquad (\lambda, \mu \in \mathbb{R})$$

wiederum ein Polynom liefert, das jede Lösung des Systems $p_1 = 0 \wedge p_2 = 0$ annulliert; in der linearen Algebra zeigt man:

($**$) Die Menge all dieser Linearkombinationen ist bereits die Antwort auf Frage 3.

Wir schreiben $\mathrm{lin}(P)$ für die Menge aller Linearkombinationen einer Menge P von Polynomen.
Aus der Antwort auf Frage 3 kann man eine Antwort auf Frage 1 ableiten.

Die Antwort auf Frage 1 lautet:

- Wenn es eine Linearkombination $\lambda \cdot p_1 + \mu \cdot p_2$ gibt, die das konstante Polynom 1 ist, dann hat das System $p_1 = p_2 = 0$ offenbar keine Lösung.
- Wenn das System $p_1 = p_2 = 0$ keine Lösung hat, dann ist offenbar jede Lösung des Systems auch Nullstelle des konstanten Polynoms 1; nach dem Satz ($**$) ist dann $1 \in \mathrm{lin}(p_1, p_2)$.

In der Sprache der Galoisverbindungen, mit $X = \mathbb{R}^3$, $E =$ Polynome in $\mathbb{R}[x,y,z]$ vom Grad ≤ 1, und der Relation „ist Nullstelle von“ schreibt man die angeführten Sachverhalte so:
Die Frage 1 „Wann ist $P^{\downarrow} = \emptyset$?“ hat die Antwort „Genau dann, wenn $1 \in \mathrm{lin}(P)$.“

Die Frage 3 „Beschreibe $P^{\downarrow\uparrow}$ “ wird durch $P^{\downarrow\uparrow} = \mathrm{lin}(P)$“ beantwortet.
Oder: Eine Menge von Gleichungen ist genau dann abgeschlossen, wenn sie unter lin abgeschlossen ist.
(Wiederum sieht man leicht, dass Frage 1 ein Spezialfall von Frage 3 ist. $P^{\downarrow} = \emptyset$ ist nämlich trivialerweise äquivalent zu $1 \in P^{\downarrow\uparrow}$.)

Zwischenbemerkung aus logischer Sicht. Bemerkenswert ist hier die Struktur der Aussagen auf beiden Seiten der Äquivalenz. Auf der einen Seite steht ein Allsatz (bzw eine negierte Existenz, „es gibt keine Lösung“), auf der anderen ein Existenzsatz.
Daraus folgt, dass die Unlösbarkeit eines Gleichungssystems nicht vom Körper abhängt, über dem es betrachtet wird. Genauer:

> Seien $K \leq L$ Körper, und sei P ein System linearer Gleichungen mit Koeffizienten in K.
> Dann hat P in K genau dann eine Lösung, wenn es in L eine Lösung hat.

Wenn es nämlich eine Lösung in K gibt, dann klarerweise auch eine in L. Wenn es keine Lösung in K gibt, dann gibt es eine Linearkombination in K, die auf die Gleichung $1 = 0$ führt, also erst recht so eine Linearkombination in L.
Aus logischer Sicht sehen wir das so:

- Wenn ein reiner Allsatz in einer Struktur gilt, dann gilt er auch in allen Unterstrukturen. (ZB ist jede Untergruppe einer kommutativen Gruppe wieder kommutativ.) Wir sagen auch: Allsätze sind „abwärts-absolut“.
- Dual dazu: Wenn ein reiner Existenzsatz in einer Struktur gilt, dann auch in allen Oberstrukturen. Existenzsätze sind „aufwärts-absolut“.
- Wenn wir nun einen reinen Allsatz $\forall x\, \varphi$ haben, der in allen betrachteten Strukturen zu einem reinen Allsatz $\exists y\, \psi$ äquivalent ist, dann ist dieser Satz „absolut“, seine Wahrheit vererbt sich also sowohl auf Ober- wie auch auf Unterstrukturen.
  Dies ist einer der Gründe, warum Charakterisierungen der Form $\forall x(\cdots) \Leftrightarrow \exists y(\cdots)$ oft von besonderem Interesse sind.

Galoisverbindung Ideale–Varietäten. Sei I ein Ideal in einem beliebigen kommutativen Ring R. Wir definieren das „Radikal“ von I, $\sqrt{I}$, so:

$$\sqrt{I} := \{r \in R : \exists e \geq 0\, r^e \in I\}$$

Man sieht leicht, dass $\sqrt{I}$ ein Ideal ist, und $\sqrt{\sqrt{I}} = \sqrt{I}$ gilt.
Sei I eine Menge von Polynomen in $K[x_1, \ldots, x_n]$. Mit $V(I)$ oder $V_K(I)$ bezeichnen wir die zu I gehörige „Varietät“, die Menge aller Nullstellen von I:

$$I^{\downarrow} = V_K(I) := \{(a_1, \ldots, a_n) \in K^n : \forall p(x_1, \ldots, x_n) \in I\ p(a_1, \ldots, a_n) = 0\}$$

Für die einelementige Menge $I_1 := \{(x^2 + y^2 - 1)\}$ und die einelementige Menge $I_2 := \{(x^2 + y^2 - 1)^5\}$ gilt zum Beispiel $V(I_1) = V(I_2)$.
Umgekehrt definieren wir für jede Menge $A \subseteq K^n$ das zugehörige „Ideal“ aller Polynome, die auf A verschwinden:

$$A^{\uparrow} = J(A) := \{p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] : \forall (a_1, \ldots, a_n) \in A\ \ p(a_1, \ldots, a_n) = 0\}$$

$J(A)$ ist immer ein Ideal, und es gilt offensichtlich $\sqrt{J(A)} = J(A)$.
Für beliebige Ideale I gilt offensichtlich $I \subseteq J(V(I))$, daher auch $\sqrt{I} \subseteq J(V(I))$.

BEISPIEL. Sei I das von $\{(x^2+1)y^4\}$ erzeugte Ideal in $\mathbb{R}[x, y]$. Dann ist $V(I) = \{(a, b) \in \mathbb{R}^2 : b = 0\}$, und $J(V(I))$ ist das von y erzeugte Ideal, während $\sqrt{I}$ das von $(x^2 + 1)y$ erzeugte Ideal ist.

Der „logische“ Nullstellensatz

Wir verwenden die prädikatenlogische Sprache der Ringe mit 1, d.h. neben den üblichen logischen Symbolen wie $\neg, \vee, \wedge, \rightarrow, =, \forall, \exists$ verwenden wir die „nichtlogischen“ Symbole 0, 1 (Konstantensymbole) und $+$, $\cdot$ (Funktionssymbole). Wir verwenden hier Prädikatenlogik erster Stufe; das heißt, dass Quantoren sich immer nur auf Objekte der betrachteten Struktur beziehen, nicht etwa auf Teilmengen, Funktionen, etc.
Sei Σ die Theorie der algebraisch abgeschlossenen Körper. Neben den (endliche vielen) Körperaxiomen[2] enthält Σ also auch für jede natürliche Zahl $n \geq 1$ das Axiom $\forall x_1, \ldots, x_n \, \exists y \, y^n + x_1 y^{n-1} + \cdots + x_n = 0$.

Der „logische“ Nullstellensatz, syntaktisch. Sei $\varphi(x_1, \ldots, x_n)$ eine beliebige Formel mit n freien Variablen. Dann gibt es eine *quantorenfreie* Formel φ' mit den selben freien Variablen, die modulo Σ zu φ äquivalent ist, d.h.

$$\Sigma \models \forall x_1 \cdots \forall x_n \, [\varphi(\bar{x}) \leftrightarrow \varphi'(\bar{x})]$$

Anders ausgedrückt: In jedem algebraisch abgeschlossenen Körper K, und für alle Elemente $k_1, \ldots, k_n \in K$ gilt $\varphi(k_1, \ldots, k_n)$ genau dann, wenn $\varphi'(k_1, \ldots, k_n)$ gilt.
Weiters gilt, dass man ein effektives (wenn auch nicht effizientes) Verfahren angeben kann, um φ' aus φ zu konstruieren. Den Übergang von φ zu φ' nennt man *Quantorenelimination*

BEISPIELE: Die Formel $\exists x \, x^2 \cdot z = 1$ ist zu $z \neq 0$ äquivalent. Die Formel $\forall x \, \exists y \, x \cdot y = z + 1$ ist zu $z + 1 = 0$ äquivalent.
Eine scheinbare Verallgemeinerung[3] ist die folgende Variante: Sei K ein algebraisch abgeschlossener Körper, und sei $\varphi(x_1, \ldots, x_n)$ eine beliebige Formel mit n freien Variablen; anders als vorhin lassen wir nun neben 0 und 1 jedes Element von K als Konstantensymbol zu.
Dann gibt es eine *quantorenfreie* Formel φ' mit den selben freien Variablen und den selben Konstanten, die in K und in allen algebraisch abgeschlossenen Erweiterungskörpern von K zu φ äquivalent ist.

Der „logische“ Nullstellensatz, semantisch. Seien $K \leq L$ algebraisch abgeschlossene[4] Körper ($K \leq L$ bedeutet, dass L Erweiterungskörper von K ist). Dann ist K elementares Untermodell von L. Das heißt: Für jede Formel $\varphi(x_1, \ldots, x_n)$ und für alle $a_1, \ldots, a_n \in K$ gilt:

$$K \models \varphi(a_1, \ldots, a_n) \;\Leftrightarrow L \models \varphi(a_1, \ldots, a_n)$$

Insbesondere gilt:

---

[2] Wir setzen die Körperaxiome als bekannt voraus. Als Beispiel möge die Formel $\forall x \, (x \neq 0 \rightarrow \exists y \, (xy = 1))$ dienen.

[3] In Wirklichkeit ist diese Variante eine einfache Folgerung des Satzes.

[4] Der algebraische Abschluss ist hier wichtig. Zum Beispiel ist $\mathbb{R}$ kein elementares Untermodell von $\mathbb{C}$, da die Formel $\exists x \, x^2 + 1 = 0$ in $\mathbb{R}$ und $\mathbb{C}$ verschiedene Wahrheitswerte hat. Wenn allgemeiner K ein beliebiger Körper ist, in dem das Polynom $a_n x^n + \cdots + a_0$ keine Nullstelle hat, dann kann man einen Erweiterungskörper finden, in dem dieses Polynom schon eine Nullstelle hat; dieser ist dann keine elementare Erweiterung.

(∗) Wenn ein endliches System von Polynomgleichungen (also Gleichungen der Form $p(x_1, \ldots, x_n) = 0$, mit $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$) in L eine Lösung hat, dann bereits in K.
Statt eines Systems von Polynomgleichungen dürfen wir auch ein Gemisch von Gleichungen und Ungleichungen verwenden: $p_1(\vec{x}) = 0 \ \wedge \ p_2(\vec{x}) \neq 0 \ \wedge \ \cdots$

Die hier angegebene semantische Version des Satzes ist schwächer als die syntaktische, und lässt sich aus dieser leicht beweisen. Für quantorenfreie Formeln φ' ist nämlich die Äquivalenz $K \models \varphi \Leftrightarrow L \models \varphi'$ trivial, da sie direkt aus der Definition von $K \leq L$ folgt.

Beweis des „syntaktischen'" Nullstellensatzes

Polynomdivision. Sei K ein Körper (kommutativ, $0 \neq 1$), $K[y]$ der Polynomring. Polynome vom Grad n können wir in K durch ein $n+1$-Tupel von Koeffizienten beschreiben.
Für alle natürlichen Zahlen $k, n \geq 0$ geben wir (induktiv) eine Formel $T_{n,k}(\bar{a}; \bar{b})$ mit $(n+1)+(k+1)$ freien Variablen $\bar{a} = (a_0, \ldots, a_n)$, $\bar{b} = (b_0, \ldots, b_k)$ konstruieren, die aussagt, dass das durch $\bar{a}$ bestimmte Polynom $A(y) = a_0 + \cdots + a_n y^n$ das durch $\bar{b}$ bestimmte Polynom $B(y) = b_0 + \cdots + b_k y^k$ teilt:

$$K[y] \models a_0 + \cdots + a_n y^n | b_0 + \cdots + b_k y^k \quad \Leftrightarrow \quad K \models T_{n,k}(\bar{a}, \bar{b})$$

Man beachte, welche Rolle die Koeffizienten a_i und b_j spielen: aus *logischer* Sicht, also aus der Sicht der Formel $T_{n,k}$ sind a_i und b_j die freien Variablen, während die Variable y in der Formel gar nicht vorkommt. Aus *algebraischer* Sicht sind die a_i und b_j Konstante oder Parameter, während y die Unbekannte oder Unbestimmte ist.
Zum Beispiel ist das Polynom $a+by \in K[y]$ genau dann ein Teiler[5] des Polynoms $c + y$, wenn $bc = a \vee (b = 0 \wedge a \neq 0)$ gilt. Unsere noch zu findende Formel $T_{1,1}(a_0, a_1; b_0, b_1)$ wird also $T_{1,1}(a, b; c, 1) \Leftrightarrow bc = a \vee (b = 0 \wedge a \neq 0)$ erfüllen.

- Wir betrachten zunächst den Fall $k = 0$. Wann gilt $a_0 + \cdots + a_n y^n | b_0$? Dazu muss entweder $A(y)$ eine Konstante ($\neq 0$) sein, oder $B(y)$ das Nullpolynom:

  $$T_{n,0}(a_0, \ldots, a_n; b_0) := \ (b_0 = 0) \vee (a_1 = \cdots = a_n = 0 \wedge a_0 \neq 0)$$

- Nun betrachten wir den Fall $n = 0$. Dann ist $A(y)$ konstant, also gilt $A(y)|B(y)$ genau dann, wenn entweder $B(y)$ konstant 0 ist, oder $A(y)$ nicht konstant 0 ist.

  $$T_{0,k}(a_0, \bar{b}) := a_0 \neq 0 \vee (b_0 = \cdots = b_k = 0)$$

- Nun suchen wir eine Formel $T_{n+1,k+1}(a_0, \ldots, a_n, a_*; b_0, \ldots, b_k, b_*)$, die aussagen soll, dass $A(y) := a_0 + \cdots + a_n y^n + a_* y^{n+1}$ ein Teiler von $B(y) := b_0 + \cdots + b_k y^k + b_* y^{k+1}$ ist. Wenn einer der Führungskoeffizienten gleich 0 ist, dann können wir die Frage der Teilbarkeit auf ein gelöstes Problem

[5] Im Ring $K[y, a, b, c]$, wo y, a, b, c Unbestimmte sind, ist das Polynom $a + by$ kein Teiler des Polynoms $c + y$. Diese Teilbarkeit betrachten wir aber hier nicht, sondern immer nur Teilbarkeit in $K[y]$.

zurückführen ($T_{n,k+1}$ bzw $T_{n+1,k}$); nur wenn beide Führungskoeffizienten ungleich 0 sind, müssen wir uns etwas anderes überlegen ($T'_{n+1,k+1}$):

$$\begin{aligned} T_{n+1,k+1}(a_0,\dots,a_n,a_*;b_0,\dots,b_k,b_*) \quad := \quad & a_* = 0 \wedge T_{n,k+1}(\bar{a};\bar{b},b_*) \vee \\ & \vee\ b_* = 0 \wedge T_{n+1,k}(\bar{a},a_*;\bar{b}) \vee \\ & \vee\ a_* \neq 0 \wedge b_* \neq 0 \wedge T'_{n+1,k+1}(\bar{a},a_*,\bar{b},b_*) \end{aligned}$$

- Wenn $a_*, b_* \neq 0$, dann kann $A(y)|B(y)$ nur dann gelten, wenn $n \leq k$ ist. Für $n > k$ setzen wir also $T'_{n+1,k+1} := \bot$.
  Sei nun $n \leq k$. Dann gilt

$$A(y)|B(y) \ \Leftrightarrow\ A(y)|(a_* \cdot B(y)) \ \Leftrightarrow\ A(y)|\Big(a_* \cdot B(y) - b_* \cdot y^{k-n} \cdot A(y)\Big)$$

  Der Koeffizient von y^{k+1} im Polynom auf der rechten Seite ist nun $a_* \cdot b_* - b_* \cdot a_* = 0$, das Polynom $a^*B - b^*y^{n-k}A$ auf der rechten Seite hat also höchstens Grad k. Also definieren wir

$$T'_{n+1,k+1}(\bar{a},a_*;\bar{b},b_*) := T_{n+1,k}(\bar{a},a_*;b_0,\dots,b_{k-n-1},a_*b_{k-n}-b_*a_0,\dots,a_*b_k-b_*a_n)$$

Quantorenelimination

Wir werden zeigen, dass jede Formel $\varphi(x_1,\dots,x_n)$ von der Form

$$\varphi(\vec{x}) = \exists y\, \psi(\vec{x},y),$$

wobei ψ eine quantorenfreie Formel ist, selbst zu einer quantorenfreien Formel äquivalent ist (modulo der Theorie der algebraisch abgeschlossenen Körper), d.h. wir finden eine quantorenfreie Formel $\varphi'(\vec{x})$, sodass die Äquivalenz

$$\forall x_1, \cdots, \forall x_n\, (\varphi(\vec{x}) \leftrightarrow \varphi'(x))$$

in allen algebraisch abgeschlossenen Körpern gilt.
Dieses Lemma reicht erstens aus, um den Satz $(*)$ über die Lösbarkeit zu zeigen. Mit Induktion über den Aufbau einer Formel folgt aber daraus schon, dass *jede* Formel zu einer quantorenfreien äquivalent ist (modulo der Theorie der algebraisch abgeschlossenen Körper).

Wir betrachten eine Formel $\exists y\, \psi(\vec{x},y)$, wobei ψ quantorenfrei ist. Wir wollen eine äquivalente quantorenfreie Formel $\varphi'(\vec{x})$ finden.

Vereinfachung der Atomformeln. Die einfachsten quantorenfreien Formeln (mit freien Variablen unter $x_1,\dots,x_n,y$) sind die sogenannten „Atomformeln“, d.h. Formeln der Form $p = q$, wobei $p, q \in K[x_1,\dots,x_n,y]$. Der Einfachkeit halber ersetzen wir so eine Formel durch $p - q = 0$.

Keine Disjunktionen. Unter „Literalen“ verstehen wir Atomformeln und negierte Atomformeln. Jede quantorenfreie Formel ist offensichtlich äquivalent zu einer Disjunktion von Konjunktionen von Literalen. Eine Formel der Form $\exists x(K_1 \vee \cdots \vee K_i)$ ist logisch äquivalent zur Formel

$$(\exists x\, K_1) \vee \cdots \vee (\exists x\, K_i)$$

Daher genügt es, Elimination von Quantoren für Formeln der Form

$$\exists y\, (L_1 \wedge \cdots \wedge L_i)$$

zu betrachten, wobei jedes L_j ein Literal ist. Solche Formeln nennen wir im Folgenden *einfache Existenzformeln*. Wir werden diese Formel Schritt für Schritt in eine einfachere (äquivalente) Formel transformieren.
Jedes Literal ist eine Gleichung oder Ungleichung der Form $p(\vec{x}, y) = 0$ oder $p(\vec{x}, y) \neq 0$. $p(\vec{x}, y)$ ist formal ein Polynom in $K[x_1, \ldots, x_n, y]$, wir fassen es aber als Polynom in y auf, wobei die Koeffizienten in $K[x_1, \ldots, x_n]$ liegen. Mit „Grad“ meinen wir immer den Grad in Bezug auf y. Der Grad eines Literals ist der Grad des vorkommenden Polynoms; der Grad einer Konjunktion von Literalen ist die Summe der Einzelgrade.
Unser Reduktionsprozess wird Schritt für Schritt den Grad reduzieren. Anders ausgedrückt: Eine einfache Existenzformel vom Grad 0 ist offensichtlich zu einer quantorenfreien Formel äquivalent. Es genügt also, zu jeder einfachen Existenzformel vom Grad $n > 0$ eine äquivalente von kleinerem Grad[6] zu finden.
Es genügt sogar folgende schwächere Variante:

(!) Jede einfache Existenzformel vom Grad $n > 0$ ist äquivalent zu einer endlichen Disjunktion von einfachen Existenzformeln, die alle Grad $< n$ haben.

Wenn y in einem Literal, etwa in L_1, gar nicht vorkommt, d.h. wenn der Grad des entsprechenden Polynoms 0 ist, dann können wir dieses Literal aus dem Existenzquantor „herausziehen“:

$$\exists y(\ p_1(\vec{x}) = 0 \ \wedge\ p_2(\vec{x}, y) = 0 \ \wedge\ \cdots) \quad \Leftrightarrow \quad p_1(\vec{x}) = 0 \ \wedge\ \exists y(\ p_2(\vec{x}, y) = 0 \ \wedge\ \cdots)$$

Reduktion der Ungleichungen. Wir wollen nun zeigen, dass jede Formel $\exists y\, K$, wobei K eine Konjunktion von Literalen ist, äquivalent zu einer quantorenfreien Formel ist.
Die Konjunktion von zwei (oder mehreren) negierten Atomformeln lässt sich durch eine negierte Atomformel (von gleichem Grad) ersetzen:

$$p(\vec{x}, y) \neq 0 \wedge q(\vec{x}, y) \neq 0 \quad \Leftrightarrow \quad p(\vec{x}, y) \cdot q(\vec{x}, y) \neq 0$$

Daher dürfen wir annehmen, dass unsere Formel von der Form

$$\exists y\,(\, p_1(\vec{x}, y) = 0 \ \wedge\ \cdots\ \wedge\ p_i(\vec{x}, y) = 0 \ \wedge\ q(\vec{x}, y) \neq 0\,)$$

ist.
(Um die Notation zu vereinfachen, nehmen wir an, dass sowohl Gleichungen wie Ungleichungen vorkommen. Wenn keine Gleichungen oder keine Ungleichungen vorkommen, können wir einige der folgenden Schritte überspringen.)

Reduktion der Gleichungen. Wir wollen nun die Anzahl der vorkommenden Gleichungen auf höchstens eine reduzieren, d.h. wir wollen eine äquivalente Formel finden, in der nur eine einzige Gleichung und eine einzige Ungleichung vorkommt.
Betrachten wir zunächst den Spezialfall der folgenden Formel

$$\exists y(y^2 + by + c = 0 \ \wedge\ py^3 + qy^2 + ry + s = 0)$$

(wobei b, c, p, q, r, s Polynome in den Variablen $x_1, \ldots, x_n$ sind). Offensichtlich ist diese Formel zu

$$\exists y(y^2 + by + c = 0 \ \wedge\ (py^3 + qy^2 + ry + s) - py(y^2 + by + c) = 0)$$

[6]Formal wäre hier ein Beweis mit vollständiger Induktion zu führen.

äquivalent, somit zu

$$\exists y(y^2 + by + c = 0 \ \wedge \ (q - pb)y^2 + (r - pc)y + s = 0)$$

äquivalent, also einer Formel niedrigeren Grades.
Wir hatten hier einen Spezialfall betrachtet, in dem einer der Führungskoeffizienten gleich 1 ist. Um diese Reduktion auch im allgemeinen Fall durchführen zu können, scheint zunächst eine Division notwendig zu sein; in unserer Sprache gibt es aber kein Symbol für die Division. Eine Division kann man aber vermeiden, indem man beide Polynome mit dem Führungskoeffizienten des anderen multipliziert; dies ist aber nur dann eine Äquivalenzumformung, wenn diese Faktoren $\neq 0$ sind.
Wir wissen im allgemeinen Fall aber gar nicht, ob der Führungskoeffizient (ein Polynom in $\vec{x}$) überhaupt ungleich 0 ist; dies können wir aber durch eine Fallunterscheidung klären, die nicht von y abhängt. Betrachten wir also den etwas allgemeineren Spezialfall der folgenden Formel von Grad 5:

$$\varphi := \quad \exists y(ay^2 + by + c = 0 \ \wedge \ py^3 + qy^2 + ry + s = 0)$$

- Die Formel $a = 0 \ \wedge \ \varphi$ ist offensichtlich äquivalent zur Formel

  $$\varphi_1 := \quad a = 0 \ \wedge \ \exists y(by + c = 0 \ \wedge \ py^3 + qy^2 + ry + s = 0),$$

  die nur Grad 4 hat.
- Die Formel $a \neq 0 \ \wedge \ \varphi$ ist äquivalent zur Formel

  $$a \neq 0 \ \wedge \ \exists y(ay^2 + by + c = 0 \ \wedge \ a(py^3 + qy^2 + ry + s) = 0),$$

  und diese Formel können äquivalent zu

  $$a \neq 0 \ \wedge \ \exists y(ay^2 + by + c = 0 \ \wedge \ a(py^3 + qy^2 + ry + s) - py(ay^2 + by + c) = 0)$$

  umformen, die offensichtlich zu einer Formel φ_2 vom Grad 4 äquivalent ist.

Daher haben wir die Äquivalenz

$$\varphi \quad \Leftrightarrow \quad \varphi_1 \ \vee \ \varphi_2,$$

somit ist unsere Formel vom Grad 5 äquivalent zur Disjunktion von zwei Formeln vom Grad 4.

Eine ähnliche Reduktion des Grades können wir für beliebige einfache Existenzformeln durchführen, solange in ihnen mindestens 2 Gleichungen vorkommen.

Gleichungen vs Ungleichungen. Wir betrachten nun eine einfache Existenzformel φ der Form

$$\exists y \, (\, p(\vec{x}, y) = 0 \wedge q(\vec{x}, y) \neq 0 \,)$$

Bis jetzt haben wir für unsere Äquivalenzumformungen nur Körpereigenschaften verwendet. Nun verwenden wir erstmals die algebraische Abgeschlossenheit. In jedem algebraisch abgeschlossenen Körper K gilt nämlich für beliebige Polynome $p(y), q(y) \in K[y]$:

- Wenn $p(y)$ keine mehrfachen Nullstellen hat, dann kann man genau dann ein Element $b \in K$ mit der Eigenschaft

  $$p(b) = 0 \wedge q(b) \neq 0$$

finden, wenn $p(y)$ kein Teiler von $q(y)$ ist (im Ring $K[y]$).
(Beweis: Wegen der algebraischen Abgeschlossenheit zerfällt $p(y)$ in Linearfaktoren. Einer dieser Faktoren ist kein Teiler von $q(y)$; damit haben wir eine Nullstelle von p gefunden, die keine Nullstelle von q ist.)

- Sei k der Grad von p. Dann kann man genau dann ein Element $b \in K$ mit der Eigenschaft

$$p(b) = 0 \wedge q(b) \neq 0$$

finden, wenn $p(y)$ kein Teiler von $q(y)^k$ ist.
(Beweis: Ähnlich wie vorhin. Wenn jeder Linearfaktor $(y - b)$ von $p(x)$ ein Linearfaktor von $q(x)$ wäre, dann wäre auch für jede mehrfache (sagen wir ℓ-fache, $\ell \leq k$) Nullstelle b von p auch das Polynom $(y - b)^k$ ein Faktor von $q(y)^n$, somit erst recht das Polynom $(y-b)^\ell$. Daher wäre p ein Teiler von q^n.)

Somit ist die Aussage

$$\exists y \, (\, p(\vec{x}, y) = 0 \wedge q(\vec{x}, y) \neq 0 \,)$$

äquivalent zu einer der schon früher konstruierten quantorenfreien Formeln $T_{\cdot,\cdot}$.

Damit ist der „syntaktische“ Nullstellensatz bewiesen.

Algebraische Folgerungen

Der „schwache“ Nullstellensatz. Sei K algebraisch abgeschlossener Körper, und seien $p_1(x_1,\dots,x_n),\dots,p_k(x_1,\dots,x_n)$ Polynome in $K[x_1,\dots,x_n]$.
Angenommen, das von $p_1,\dots,p_k$ erzeugte Ideal ist echt (d.h. enthält nicht 1).
Dann gibt es eine gemeinsame Nullstelle, d.h. es gibt $\bar{a} = (a_1,\dots,a_n) \in K^n$, sodass für $i = 1,\dots,k$ die Gleichung $p_i(a_1,\dots,a_n) = 0$ erfüllt ist.
[Folgende Umkehrung ist offensichtlich: Wenn $1 \in \langle p_1,\dots,p_k\rangle$, dann gibt es keine gemeinsame Nullstelle.]

Beweis des schwachen Nullstellensatzes. Sei I das von den Polynomen erzeugte Ideal in $K[x_1,\dots,x_n]$. Es gibt ein maximales Ideal $M \supseteq I$. Dann ist $L := K[x_1,\dots,x_n]/M$ ein Körper, der K enthält.
Betrachten wir die Polynome $p_1(y_1,\dots,y_n),\dots,p_k(y_1,\dots,y_n) \in L[y_1,\dots,y_n]$.
Im Körper L haben diese Polynome eine gemeinsame Nullstelle, nämlich das n-Tupel $(x_1+M,\dots,x_n+M)$.
Sei nun $\bar{L}$ ein algebraisch abgeschlossener Erweiterungskörper von L.
Da es in $\bar{L}$ eine gemeinsame Nullstelle der Gleichungen $p_1 = 0,\dots,p_k = 0$ gibt, muss es (nach dem „logischen“ Nullstellensatz) auch in K so eine Lösung geben.

Der „große“ Nullstellensatz. Sei K ein algebraisch abgeschlossener Körper, $n \geq 1$. Sei $I \subseteq K[x_1,\dots,x_n]$ ein Ideal.
Dann ist $J(V(I)) = \sqrt{I}$.
Wenn I von den Polynomen $p_1,\dots,p_k \in K[x_1,\dots,x_n]$ erzeugt wird, dann besagt dieser Satz also:
Wenn p ein Polynom ist mit $p(a_1,\dots,a_n) = 0$ für jede Lösung des Systems
$p_1(\bar{a}) = 0,\dots,p_k(\bar{a}) = 0$,
dann muss entweder p selbst oder zumindest eine geeignete Potenz p^e, $e \geq 1$
im Ideal $\langle p_1,\dots,p_k\rangle$ liegen.

Aus dem „großen“ bekommt man leicht den „schwachen“ Nullstellensatz. Umgekehrt bekommt man mit „Rabinowitschs Trick“ aus dem schwachen auch den großen Nullstellensatz.
Sei nämlich I ein Ideal. Wir wollen $V(K(I)) = \sqrt{I}$ zeigen, genauer: die Inklusion $V(K(I)) \subseteq \sqrt{I}$.
Sei also $q(x_1,\dots,x_n)$ Polynom in $V(K(I))$.
Wir betrachten nun Polynome im Polynomring $K[x_1,\dots,x_n,y]$. Sei I' das Ideal, das von I zusammen mit dem Polynom $1 - y\cdot q(x_1,\dots,x_n)$ erzeugt wird. $K(I') = \emptyset$, denn wäre $(a_1,\dots,a_n,b)$ eine Nullstelle aller Polynome in I', dann wäre (wegen $q \in V(K(I))$) das Tupel $a_1,\dots,a_n$ Nullstelle von q, somit hätte das Polynom $1 - y\cdot q$ an der Stelle $(a_1,\dots,a_n,b)$ den Wert 1.
Wenn wir nun $y := 1/q$ setzten (und im Körper der rationalen Funktionen rechnen) bekommen wir nach Umformungen ein n mit $q^n \in I$.

Anmerkung: Solange wir nur an *Gleichungen* interessiert sind, kann man zeigen, dass dieser Satz auch für unendlich viele Gleichungen gilt, es gilt nämlich eine Art „Kompaktheitssatz“: Ein System von beliebig vielen Gleichungen $p(\vec{x}) = 0$ in endlich vielen Variablen lässt sich genau dann in K lösen, wenn sich jedes endliche Teilsystem in K lösen lässt. (Genau dann, wenn das von den Polynomen p erzeugte Ideal nicht die Konstante 1 enthält.)

Für Systeme von Ungleichungen gilt so ein Kompaktheitssatz nicht. Sei etwa K der Körper aller algebraischen Zahlen, dann kann man durch Aufzählung *aller* Polynome ein System von Ungleichungen in einer einzigen Variablen angeben, das nur von transzendenten Zahlen gelöst wird, also in K keine Lösung hat; jedes endliche Teilsystem hat aber eine Lösung in K.

Reell abgeschlossene Körper

Ein linear geordneter[7] Körper K heißt reell abgeschlossen, wenn in ihm jedes Polynom ungeraden Grades eine Nullstelle hat, und jedes positive Element eine Quadratwurzel[8]. (BEISPIELE: Der Körper der reellen Zahlen, oder der Körper aller algebraischen Zahlen, die reell sind. Man kann zeigen, dass für jeden reell abgeschlossenen Körper K der Körper $K(i)$ algebraisch abgeschlossen ist.)
Auch in reell abgeschlossenen Körpern lässt sich Quantorenelimination durchführen.

Der „logische" Nullstellensatz für reell abgeschlossene Körper. Sei $\varphi(x_1, \ldots, x_n)$ eine beliebige Formel mit n freien Variablen. Dann gibt es eine *quantorenfreie* Formel φ' mit den selben freien Variablen, die in allen reell abgeschlossenen Körpern zu φ äquivalent ist, d.h.:
In jedem reell abgeschlossenen Körper K, und für alle Elemente $k_1, \ldots, k_n \in K$ gilt $\varphi(k_1, \ldots, k_n)$ genau dann, wenn $\varphi'(k_1, \ldots, k_n)$ gilt.

Als Folgerung erhalten wir wiederum:

Seien $K \leq L$ reell abgeschlossene Körper. Dann ist K elementares Untermodell von L. Das heißt: Für jede Formel $\varphi(x_1, \ldots, x_n)$ und für alle $a_1, \ldots, a_n \in K$ gilt:

$$K \models \varphi(a_1, \ldots, a_n) \Leftrightarrow L \models \varphi(a_1, \ldots, a_n)$$

Insbesondere gilt: Ein System von Polynomgleichungen $p_1(\vec{x}) = 0, \ldots, p_k(\vec{x}) = 0$ ist in einem reell abgeschlossenen Körper genau dann lösbar, wenn es in einem reell abgeschlossenen Erweiterungskörper lösbar ist.

Formal reelle Körper. Man kann zeigen, dass in einem Körper die folgenden Aussagen äquivalent sind:

- Es gibt eine mit den Körperoperationen verträgliche lineare Ordnung.
- -1 lässt sich nicht als Summe von Quadraten darstellen.
- K ist Unterkörper eines reell abgeschlossenen Körpers.

Solche Körper nennt man „formal reell".
Als Folgerung des obigen Satzes erhält man:

> Ein System von Polynomgleichungen $p_1(\vec{x}) = 0, \ldots, p_k(\vec{x}) = 0$ ist in einem reell abgeschlossenen Körper genau dann lösbar, wenn es einen formal reellen Erweiterungskörper gibt, in dem dieses System lösbar ist.

Quellen

Die Sätze über Quantorenelimination stammen von Alfred Tarski aus den 1940er Jahren. Die hier präsentierte Version lehnt sich an die Darstellung im Buch von Kreisel und Krivine über Modelltheorie an.

---

[7] Hier wird verlangt, dass die lineare Ordnung mit den Körperoperationen verträglich ist: Summen und Produkte von positiven Elementen müssen positiv sein

[8] In reell abgeschlossenen Körpern gilt also $0 \leq x \Leftrightarrow \exists y\,(y^2 = x)$. Es ist Geschmackssache, ob man das Symbol $\leq$ nun als neues Relationssymbol in der „Sprache der reell abgeschlossenen Körper" betrachtet, oder $x \leq z$ es als Abkürzung für $\exists y\,(x + y^2 = z)$ ansieht.