Der Hilbertsche Nullstellensatz

Eine erste Frage, die man sich über den Zusammenhang zwischen einem Gleichungssystem und seiner Lösungsmenge stellen kann, ist die, ob es überhaupt Lösungen gibt. Im Falle einer Gleichung in einer Variablen sagt uns die Algebra, daß ein nichtkonstantes Polynom aus $k[X]$ zumindest in einem Erweiterungskörper von k eine Nullstelle haben muß; der sogenannte *Fundamentalsatz der Algebra* sagt uns speziell für $k = \mathbb{C}$, daß jedes nichtkonstante Polynom aus $\mathbb{C}[X]$ mindestens eine komplexe Nullstelle hat. Bei Gleichungssystemen kann es schon im linearen Fall vorkommen, daß ein System nichtkonstanter Polynome keine gemeinsame Nullstelle hat, beispielsweise im Falle der beiden Polynome $X + Y - 1$ und $2X + 2Y - 3$. In diesem Fall ist aber

$$2(X + Y - 1) - (2X + 2Y - 3) = 1 ,$$

das von den beiden Polynomen erzeugte Ideal enthält also die Eins und ist somit gleich dem gesamten Polynomring. Wie DAVID HILBERT 1893 gezeigt hat, ist dies für jedes Gleichungssystem, das auch über keinem Erweiterungskörper eine Lösung hat, der Fall:

Schwache Form des Hilbertschen Nullstellensatzes: k sei ein Körper und K ein algebraisch abgeschlossener Körper, der k enthält. Für ein echtes Ideal $I \lhd k[X_1, \ldots, X_n]$ ist $V_K(I) \neq \emptyset$.

Beweis: Nach dem HILBERTschen Basissatz hat jedes Ideal I ein endliches Erzeugendensystem $\{f_1, \ldots, f_m\}$. Wir betrachten das von den f_i erzeugte Ideal $\bar{I}$ in $K[X_1, \ldots, X_n]$. Da eine Basis des k-Vektorraums $k[X_1, \ldots, X_n]/I$ auch Basis des K-Vektorraums $K[X_1, \ldots, X_n]/\bar{I}$ ist, muß auch $\bar{I}$ ein echtes Ideal von $K[X_1, \ldots, X_n]$ sein und liegt somit in einem maximalen Ideal $\mathfrak{m} \lhd K[X_1, \ldots, K_n]$. Der Satz folgt somit aus der folgenden alternativen Version des HILBERTschen Nullstellensatzes, die auch den Namen „Nullstellensatz“ erklärt:

Satz: Die maximalen Ideale $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ sind genau die Ideale der Form

$$\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$$

mit $(x_1, \ldots, x_n) \in K^n$.

Beweis: $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$ ist der Kern der Abbildung

$$\begin{cases} K[X_1, \ldots, X_n] \to K \\ \qquad\qquad f \mapsto f(x_1, \ldots, x_n) \end{cases}.$$

Ist daher I ein Ideal, das $\mathfrak{m}$ echt enthält, so muß der Vektorraum $K[X_1, \ldots, X_n]/I$ isomorph sein zu einem echten Untervektorraum von $K[X_1, \ldots, X_n]/\mathfrak{m}$. Da letzterer nach dem Homomorphiesatz isomorph zum eindimensionalen Vektorraum K ist, muß dies der Nullraum sein. Somit ist $I = K[X_1, \ldots, X_m]$, d.h. $\mathfrak{m}$ ist ein maximales Ideal.

Umgekehrt sei $\mathfrak{m}$ ein maximales Ideal. Wenn wir zeigen können, daß es Elemente $x_1, \ldots, x_n$ gibt, für die $X_i - x_i$ in $\mathfrak{m}$ liegt, ist $(X_1 - x_1, \ldots, X_n - x_n) \subseteq \mathfrak{m}$, und da links ein maximales Ideal steht, müssen beide Seiten gleich sein.

Angenommen, es gibt ein $i \in \{1, \ldots, n\}$, für das $X_i - x$ für kein $x \in K$ im Ideal $\mathfrak{m}$ liegt. Wegen der Maximalität von $\mathfrak{m}$ ist dann

$$\mathfrak{m} + (X - x) = K[X_1, \ldots, X_n] \quad \text{für jedes } x \in K\,.$$

Somit gibt es für jedes $x \in K$ ein Polynom $f_x \in \mathfrak{m}$ sowie ein Polynom $h_x \in K[X_1, \ldots, X_n]$ derart, daß

$$f_x + h_x \cdot (X_i - x) = 1$$

ist. Da $1 \notin \mathfrak{m}$, ist dabei $h_x \neq 0$. Wir wählen für jedes $x \in K$ ein festes Polynom h_x (und damit auch f_x), das obige Gleichung erfüllt, und setzen $K_d = \{x \in K \,|\, \deg h_x = d\}$ für jedes $d \in \mathbb{N}_0$. Da K nach Voraussetzung überabzählbar viele Elemente enthält und K die Vereinigung der K_d ist, muß mindestens eine der Mengen K_d unendlich viele Elemente enthalten. (Nur an dieser Stelle des Beweises brauchen wir die Voraussetzung der Überabzählbarkeit.)

Wir wählen eine solche unendliche Menge K_d und betrachten den Vektorraum $K[X_1, \ldots, K_n]_d$ aller Polynome vom Grad höchstens d. Da es nur endlich viele Monome vom Grad höchstens d gibt, ist dies ein endlichdimensionaler K-Vektorraum. Wir wählen eine natürliche Zahl r, die größer ist als seine Dimension, und dazu r Elemente $x^{(1)}, \ldots, x^{(r)} \in K$ mit $h_{x^{(i)}} \in k[X_1, \ldots, X_n]_d$. Dazu muß es wegen

der linearen AbHängigkeit der $h_{x^{(i)}}$ Elemente $\lambda_1, \ldots, \lambda_r \in K$ geben, die nicht allesamt verschwinden, derart, daß

$$\lambda_1 h_{x^{(1)}} + \cdots + \lambda_r h_{x^{(r)}} = 0$$

ist.

Damit definieren wir ein Polynom

$$g = \sum_{j=1}^{r} \lambda_j \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) \in K[X_i]\,.$$

Dieses Polynom liegt auch in $\mathfrak{m}$, denn wegen

$$1 = f_{x^{(j)}} + h_{x^{(j)}}\left(X_i - x^{(j)}\right) \quad \text{für } j = 1, \ldots, r$$

ist

$$\begin{aligned} g &= \sum_{j=1}^{r} \lambda_j \left(f_{x^{(j)}} + h_{x^{(j)}}\left(X_i - x^{(j)}\right)\right) \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) \in K[X_i] \\ &= \sum_{j=1}^{r} \lambda_j f_{x^{(j)}} \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) + \left(\sum_{j=1}^{r} \lambda_j h_{x^{(j)}}\right) \prod_{\ell=1}^{n} \left(X_i - x^{(\ell)}\right) \\ &= \sum_{j=1}^{r} \lambda_j \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) f_{x^{(j)}} \in \mathfrak{m}\,, \end{aligned}$$

da $\sum\limits_{j=1}^{r} \lambda_j h_{x^{(j)}}$ verschwindet und alle $f_{x^{(j)}}$ in $\mathfrak{m}$ liegen.

g ist nicht das Nullpolynom, denn für jeden Index ν ist

$$g\left(x^{(\nu)}\right) = \sum_{j=1}^{r} \lambda_j \prod_{\ell \neq j} \left(x^{(\nu)} - x^{(\ell)}\right) = \lambda_\nu \prod_{\ell \neq \nu} \left(x^{(\nu)} - x^{(\ell)}\right)\,.$$

Da die $x^{(\ell)}$ paarweise verschieden sind und mindestens ein λ_ν nicht verschwindet, muß mindestens einer dieser Werte von Null verschieden sein.

g kann auch keine von Null verschiedene Konstante sein, denn g liegt im maximalen Ideal $\mathfrak{m}$, das als echtes Ideal keine von Null verschiedene Konstante enthalten kann. Somit hat g einen positiven Grad e

und zerfällt daher über dem algebraisch abgeschlossenen Körper K in Linearfaktoren:

$$g = c\,(X_i - z_1)\ldots(X_i - z_e) \;\text{ mit }\; c \in K \setminus \{0\},\; z_1, \ldots z_e \in k\,.$$

g liegt in $\mathfrak{m}$, aber nach Voraussetzung liegt keiner der Faktoren $X_i - z_j$ in $\mathfrak{m}$, und die Konstante $c \neq 0$ natürlich auch nicht. Dies ist ein Widerspruch, denn als maximales Ideal ist $\mathfrak{m}$ insbesondere ein Primideal, muß also mit jedem Produkt mindestens einen der Faktoren enthalten. ∎

Somit hat also jedes echte Ideal $I \lhd k[X_1, \ldots, X_n]$ zumindest in einem Erweiterungskörper K von k mindestens eine Nullstelle. Damit folgt umgekehrt

Satz: Das Gleichungssystem

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0$$

mit $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ ist genau dann in jedem Erweiterungskörper K von k unlösbar, wenn es Polynome $h_1, \ldots, h_m$ in $X_1, \ldots, X_n$ gibt, so daß $h_1 f_1 + \cdots + h_m f_m = 1$ ist.

Beweis: Im Falle der Unlösbarkeit ist das von $f_1, \ldots, f_m$ erzeugte Ideal der ganze Polynomring, enthält also insbesondere die Eins. Da

$$(f_1, \ldots, f_m) = \left\{ h_1 f_1 + \cdots + h_m f_m \;\middle|\; h_1, \ldots, h_m \in k[X_1, \ldots, X_n] \right\},$$

hat auch die Eins eine Darstellung der verlangten Form.

Ist umgekehrt $h_1 f_1 + \cdots + h_m f_m = 1$ für irgendwelche Polynome $h_1, \ldots, h_m$, so ist für jeden Erweiterungskörper K von k und jedes n-Tupel $(x_1, \ldots, x_n) \in K^n$

$$h_1(x_1, \ldots, x_n) f_1(x_1, \ldots, x_n) + \cdots + h_m(x_1, \ldots, x_n) f_m(x_1, \ldots, x_n) = 1\,,$$

so daß nicht alle $f_j(x_1, \ldots, x_n)$ verschwinden können. ∎

Wenn wir eine GRÖBNER-Basis eines Ideals I kennen, ist es einfach zu entscheiden, ob $I = k[X_1, \ldots, X_n]$ ist (oder äquivalent, ob $1 \in I$): Da der führende Term eines jeden Polynoms aus I durch den führenden Term eines Elements der GRÖBNER-Basis teilbar sein muß, enthält diese

im Falle eines Ideals, das die Eins enthält, ein Polynom, dessen führendes Monom die Eins ist. Da diese bezüglich jeder Monomordnung das kleinste Monom ist, muß somit die GRÖBNER-Basis eine Konstante enthalten. Die zugehörige minimale und erst recht die reduzierte GRÖBNER-Basis besteht in diesem Fall nur aus der Eins.

Die gerade bewiesene schwache Form des HILBERTschen Nullstellensatzes ist auch ein entscheidender Schritt auf dem Weg zu einem Kriterium. wann zwei Gleichungssysteme über jedem Erweiterungskörper des Grundkörpers die gleiche Lösungsmenge haben. Um den Beweis möglichst einfach zu halten, gehen wir hier von einem *überabzählbaren* algebraisch abgeschlossenen Erweiterungskörper aus; dann läßt sich der Beweis durch einen 1929 von J.L. RABINOWITSCH gefundenen Trick deutlich verkürzen. Die Voraussetzung der Überabzählbarkeit ist allerdings nicht wirklich notwendig; HILBERTs ursprünglicher Beweis von 1893 würde auch funktionieren für einen abzählbaren algebraisch abgeschlossenen Körper wie etwa den algebraischen Abschluß von $\mathbb{Q}$ oder eines endlichen Körpers $\mathbb{F}_p$. (Bei HILBERT ist natürlich noch nicht von algebraisch abgeschlossenen Körpern die Rede; selbst der Begriff des Körpers wurde erst 1910 von ERNST STEINITZ (1871–1928) eingeführt.)

Starke Form des Hilbertschen Nullstellensatzes: k sei ein beliebiger Körper und K ein überabzählbarer algebraisch abgeschlossener Erweiterungskörper von k. Falls für ein Ideal $I \lhd k[X_1, \ldots, X_n]$ ein Polynom $f \in k[X_1, \ldots, X_n]$ auf ganz $V_K(I)$ verschwindet, gibt es ein $q \in \mathbb{N}$, so daß f^q in I liegt.

Beweis: Wir erweitern den Polynomring $k[X_1, \ldots, X_n]$ mit einer neuen Variablen X_{n+1} zu $k[X_1, \ldots, X_{n+1}]$ und betrachten dort für ein Erzeugendensystem $\{f_1, \ldots, f_m\}$ von I das Gleichungssystem

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 1 - x_{n+1} f(x_1, \ldots, x_n) = 0 \,.$$

Für jeden Punkt $(x_1, \ldots, x_n, x_{n+1}) \in K^{n+1}$, für den die $f_j(x_1, \ldots, x_n)$ verschwinden, verschwindet nach Voraussetzung auch $f(x_1, \ldots, x_n)$, d.h.

$$1 - x_{n+1} f(x_1, \ldots, x_n) = 1 \,,$$

so daß das Gleichungssystem in keinem Erweiterungskörper K von k eine Lösung haben kann. Nach der gerade bewiesenen schwachen Form des HILBERTschen Nullstellensatzes gibt es daher Polynome $h_1, \ldots, h_{m+1} \in k[X_1, \ldots, X_{n+1}]$ derart, daß

$$h_1 f_1 + \cdots + h_m f_m + h_{m+1}(1 - X_{n+1} f) = 1$$

ist. Diese Gleichung bleibt gültig, wenn wir überall für X_{n+1} ein Polynom oder eine rationale Funktion in $X_1, \ldots, X_n$ einsetzen; wir setzen $X_{n+1} = 1/f$. Die h_j werden dann zu rationalen Funktionen in $X_1, \ldots, X_n$, wobei alle Nenner Potenzen von f sind. Ist f^q die höchste dieser Potenzen, so erhalten wir nach Multiplikation mit f^q eine Gleichung der Form

$$\widetilde{h}_1 f_1 + \cdots + \widetilde{h}_m f_m = f^q$$

mit $\widetilde{h}_j = f^q h_j\left(X_1, \ldots, X_n, 1/f\right) \in k[X_1, \ldots, X_n]$. Dies zeigt, daß f^q in $I = (f_1, \ldots, f_m)$ liegt.

∎

Definition: R sei ein Ring und $I \lhd R$ ein Ideal von R. Das *Radikal* von I ist die Menge $\sqrt{I} \underset{\text{def}}{=} \left\{ f \in R \;\middle|\; \exists q \in \mathbb{N} : f^q \in I \right\}$.

Das Radikal besteht also aus allen Ringelementen, die eine Potenz in I haben. Es ist selbst ein Ideal, denn sind $f, g \in \sqrt{I}$ zwei Elemente mit $f^p \in I$ und $g^q \in I$, so sind in

$$(f+g)^{p+q} = \sum_{\ell=0}^{p+q} \binom{p+q}{\ell} f^{p+q-\ell} g^{\ell}$$

die ersten q Summanden Vielfache von f^p, und die restlichen p sind Vielfache von g^q. Somit liegt jeder Summand in I, also auch die Summe. Für ein beliebiges $r \in R$ liegt natürlich auch rf in $\sqrt{I}$, denn seine q-te Potenz $(rf)^q = r^q f^q$ liegt in I, sobald f^q in I liegt.

Mit diesem neuen Begriff können wir den obigen Satz umformulieren:

Satz: Ein Polynom $f \in k[X_1, \ldots, X_n]$ verschwindet genau dann auf $V_K(I)$, wenn $f \in \sqrt{I}$.

∎

Anders ausgedrückt heißt dies

Satz: Für zwei Ideale $I, J \lhd k[X_1, \ldots, X_n]$ ist $V_K(I) = V_K(J)$ genau dann, wenn $\sqrt{I} = \sqrt{J}$ ist. ∎

Falls ein Ideal mit seinem Radikal übereinstimmt, enthält es *alle* Polynome, die auf $V_K(I)$ verschwinden; zwei Polynome nehmen genau dann in jedem Punkt von $V_K(I)$ denselben Wert an, wenn ihre Differenz in I liegt, wenn sie also modulo I dieselbe Restklasse definieren.

Wenn das Ideal I nicht mit seinem Radikal übereinstimmt, gilt zwar nicht mehr *genau dann,* aber wir können trotzdem die Elemente des Faktorvektorraums $A = k[X_1, \ldots, X_n]/I$ auffassen als Funktionen von $V_K(I)$ nach K: Für jede Restklasse und jeden Punkt aus $V_K(I)$ nehmen wir einfach irgendein Polynom aus der Restklasse und setzen die Koordinaten des Punkts ein. Da die Differenz zweier Polynome aus derselben Restklasse in I liegt, wird sie nach Einsetzen des Punktes zu Null, der Wert hängt also nicht ab von der Wahl des Polynoms. Auch Polynome aus $K[X_1, \ldots, X_n]$ definieren in dieser Weise Funktionen $V_K(I) \to K$; hinreichend (aber nicht notwendig) dafür, daß zwei Polynome dieselbe Funktion definieren ist, daß ihre Differenz im von I erzeugten Ideal $\bar{I} \lhd K[X_1, \ldots, X_n]$ liegt.

Im Falle von Polynomen einer Veränderlichen ist jedes Ideal von $k[X]$ ein Hauptideal, denn nach dem HILBERTschen Basissatz hat es ein endliches Erzeugendensystem $\{f_, \ldots, f_m\}$ und wird daher offensichtlich von $f = \mathrm{ggT}(f_1, \ldots, f_m)$ erzeugt. Ist $I = (f)$ mit einem Polynom $f \neq 0$ vom Grad d, so können wir die Restklassen repräsentieren durch die Polynome vom Grad höchstens $d - 1$, denn jedes Polynom $g \in k[X]$ hat dieselbe Restklasse wie sein Divisionsrest bei der Polynomdivision durch f. Somit ist $A = k[X]/I$ in diesem Fall ein d-dimensionaler Vektorraum. Da $V_K(I)$ gerade aus den Nullstellen von f in K besteht, von denen es höchstens d verschiedene gibt, liefert die Dimension von A eine obere Schranke für die Elementanzahl von $V_K(I)$; wenn wir die Nullstellen mit ihrer Vielfachheit zählen, ist die Dimension von A sogar *gleich* der Gesamtzahl der Nullstellen. Ähnliche Ergebnisse gelten auch für Systeme von Polynomgleichungen in mehreren Veränderlichen; teilweise werden wir sie in der nächsten Vorlesung kennen lernen.