Hilbert's Nullstellensatz

Yvan Ngumeteh Emma Ahrens

3. Mai 2018

1 Abstract

2 Einleitung

3 Hyperebenen

Satz 1 (Hilbert's Nullstellensatz für Hyperebenen)**.** *Sei k algebraisch abgeschlossen, $f \in k[X_1, \dots, X_n]$ nicht konstant und $\emptyset \neq H_f \subseteq k^n$ die korrespondierende Hyperebene. Wir können f schreiben als $f = f_1^{n_1} \cdots f_r^{n_r}$ mit $f_1, \dots, f_r$ irreduzibel und paarweise teilerfremd. Dann ist*

$$H_f = H_{f_1} \cup \cdots \cup H_{f_r} \text{ und } \mathbf{I}(H_f) = (f_1 \cdots f_r).$$

Insbesondere gilt, falls f irreduzibel ist, dass $\mathbf{I}(H_f) = (f)$.

4 Schwache Form

Definition 2 (Algebraische Elemente)**.** *Sei A eine k-Algebra. Dann heißt die Menge $a_1, \dots, a_m \in A$ algebraisch unabhängig, falls kein Polynom $0 \neq F \in k[X_1, \dots, X_m]$ existiert mit $F(a_1, \dots, a_m) = 0$.*

Im Folgenden sind A und B kommmutative Ringe mit Eins und $A \subseteq B$.

Definition 3 (Ganze Elemente)**.** *Wir nennen $b \in B$ ganz über A, wenn es Elemente $a_1, \dots, a_n \in A$ gibt mit*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

für ein $n \in \mathbb{N}$. Außerdem heißt B ganz über A, wenn jedes Element aus B ganz über A ist.

Lemma 4. *Sei $b \in B$. Dann ist äquivalent:*

1. *b ist ganz über A*
2. *Der von b erzeugte Teilring $A[b] \subseteq B$ ist ein endlich erzeugter A-Modul.*
3. *Es existiert ein Teilring $C \subseteq B$ mit $A[b] \subseteq C$ und C ist ein endlich erzeugter A-Modul.*

Beweis. ($1 \Rightarrow 2$): Es ist $A[b] = \{f(b) \mid f \in A[X]\}$ und da b ganz ist, existiert ein Polynom $0 \neq g \in A[X]$ mit $g(b) = 0$ und $Grad(g) = n \geq 1$. Da $A[X]$ ein euklidischer Ring ist, können wir jedes $f \in A[X]$ schreiben als $f = qg + r$ mit $q, r \in A[X]$ und $Grad(r) < n$. Also $f(b) = q(b) * g(b) + r(b) = r(b)$ und f ist eine A-Linearkombination von $1, b, b^2, \dots, b^{n-1}$, also ist $A[b]$ endlich erzeugt.
($2 \Rightarrow 3$): Setze $C := A[b]$, dann ist C ein Teilring von B und die Aussage folgt.
($3 \Rightarrow 1$): Seien $c_1, \dots, c_n \in C$ mit $C = \sum_{i=1}^n Ac_i$. Es gilt $b \in A[b] \subseteq C$, also auch $bc_i \in C$ und es existieren die $a_{ij} \in A$ mit $bc_i = \sum_{j=1}^n a_{ij}c_i$. Sei $A \in A^{n \times n}$ eine Matrix mit $(A)_{i,j} = a_{ij}$ für alle $i, j \in \underline{n}$ und $v \in A^n$ der Vektor mit $v_i = c_i$ wie oben. Dann entsprechen die obigen Gleichungen dem Gleichungssystem

$$Av = bv \Leftrightarrow (A - I_n)v = 0.$$

Die Cramersche Regel besagt, dass $v_i = \frac{Det((A-I_n)_i)}{Det(A-I_n)} \Leftrightarrow v_i Det(A-I_n) = Det((A-I_n)_i)$, wobei in die Matrix $(A-I_n)_i$ in unserem Fall nur Nullen in der i-ten Spalte stehen. Also gilt

$$Det((A-I_n)_i) = 0 \Rightarrow v_i Det(A-I_n) = 0.$$

Wir müssen noch zeigen, dass daraus $Det(A-I_n) = 0$ folgt, denn dann können wir die Determinante ausschreiben und $1, b, \ldots$ wird linear abhängig über A, also ist b ganz über A.
Es ist $1 \in C$, also existiert eine Linearkombination $1 = \sum_{i=1}^n a_i c_i \Leftrightarrow Det(M-I_n) = \sum_{i=1}^n a_i c_i Det(M-I_n) = 0$. Also gilt $Det(A-I_n) = 0$ und die Behauptung folgt. □

Korollar 5. *Seien A, B kommutative Ringe mit $A \subseteq B$.*

1. *Falls $B = A[b_1, \ldots, b_n]$, wobei jedes $b_i \in B$ ganz über $A[b_1, \ldots, b_{i-1}]$ ist, dann ist B endlich erzeugter A-Modul und ganz über A.*

2. *Die Menge $\overline{A}_B := \{b \in B \mid b \text{ ganz über } A\}$ ist ein Teilring von B und heißt ganzer Abschluss von A in B.*

3. *Sei $C \subseteq B$ ein Teilring mit $A \subseteq C$. Falls C ganz ist über A und B ganz ist über C, dann ist auch B ganz über A.*

4. *Falls B ein Körper ist und ganz über A, dann ist A auch ein Körper.*

Beweis.

1. Beweis durch Induktion über $n \in \mathbb{N}$.
   $n = 1$: Sei $B_n = B_1 = A[b_1]$ und b_1 ganz über A. Dann folgt mit Lemma 4, dass $A[b_1]$ ein endlich erzeugter A-Modul ist und $A[b_1]$ ganz über A ist.
   Angenommen die Behauptung gilt für ein beliebiges, aber festes $n \in \mathbb{N}$.
   $n \to n+1$: Sei $B_{n+1} = A[b_1, \ldots, b_{n+1}]$ und b_i ganz über B_{i-1} für jedes $i \in \underline{n+1}$. Nach Induktionsvoraussetzung wissen wir, dass B_n endlich erzeugter A-Modul und ganz über A ist. Außerdem ist b_{n+1} ganz über B_n und damit auch $B_n[b_{n+1}] \cong B_{n+1}$ endlich erzeugter A-Modul und TODO

2. Zu zeigen ist nach Untergruppenkriterium, dass für $b, b' \in \overline{A}_B$ auch $bb', b - b' \in \overline{A}_B$ und $1 \in \overline{A}_B$.
   Die 1 ist offensichtlich ganz über A, also gilt $1 \in \overline{A}_B$. Es sind b, b' ganz in A, also auch b' ganz in $A[b]$, also folgt mit (1), dass alle Elemente aus $A[b, b']$ ganz über A sind, also insbesondere bb' und $b - b'$. Also ist $\overline{A}_B$ ein Unterring von B.

3. B ist ganz über C, also gilt für ein $b \in B$, dass $b^m + c_{m-1}b^{m-1} + \ldots + c_0 = 0$ mit $m \geq 1, c_i \in C$. Da $c_0, \ldots, c_{m-1}$ ganz sind in A, ist (1) anwendbar und $A[c_0, \ldots, c_{m-1}]$ ist endlich erzeugter A-Modul und ganz über A. Außerdem ist b ganz über $A[c_0, \ldots, c_{m-1}]$ und mit nochmaliger Anwendung folgt, dass auch $C' := A[c_0, \ldots, c_{m-1}, b]$ endlich erzeugter A-Modul und ganz über A ist. Also $A[b] \subseteq C' \subseteq B$ und mit Lemma 4 folgt, dass b ganz ist über A.

4. A ist ein Ring, also müssen wir zeigen, dass $A* = A - \{0\}$ ist. Sei $a \in A \subseteq B$. Dann existiert $b \in B$ mit $ab = 1$. b ist ganz in A, also existieren $a_i \in A$ und $m \geq 1$ mit

$$\begin{aligned} & b^m + a_{m-1}b^{m-1} + \ldots + a_0 = 0 \\ \Leftrightarrow \quad & b^m a^{m-1} + a_{m-1}b^{m-1}a^{m-1} + \ldots + a_0 a^{m-1} = 0 \\ \Leftrightarrow \quad & b = -(a_{m-1}b^{m-1}a^{m-1} + \ldots + a_0 a^{m-1}) \in A. \end{aligned}$$

   Also ist A ein Körper.

□

Eine k-Algebra ist im Folgenden immer eine kommutative, assoziative k-Algebra mit Eins.

Satz 6 (Noetherscher Normalisierungssatz)**.** *Sei A eine endlich erzeugte k-Algebra. Dann existieren algebraisch unabhängige Elemente $a_1, \ldots, a_d \in A$, so dass A ganz ist über dem Teilring $k[a_1, \ldots, a_d]$.*

Satz 7 (Schwache Form von Hilbert's Nullstellensatz)**.** *Sei k algebraisch abgeschlossen. Dann sind die maximalen Ideale in $k[X_1, \ldots, X_n]$ genau die Ideale der Form $(X_1 - v_1, \ldots, X_n - v_n)$ mit $v_i \in k$. Allgemeiner gilt, falls A eine beliebige k-Algebra ist, dass $A/I \cong k$ für jedes maximale Ideal I in A.*

5 Normale Form

6 Starke Form

7 Anwendung