Algebraische Kurven - Vorlesung 11

Hilbertscher Nullstellensatz - geometrische Version

Wir wollen nun die geometrische Version des Hilbertschen Nullstellensatzes beweisen, der für den Fall eines algebraisch abgeschlossenen Körpers eine eindeutige Beziehung zwischen den affin-algebraischen Mengen im affinen Raum $\mathbb{A}_K^n$ und den Radikalidealen im Polynomring stiftet.

Satz 1. *((Hilbertscher Nullstellensatz (geometrische Version)))*

Sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge, die durch das Ideal $\mathfrak{a}$ beschrieben werde. Es sei $F \in K[X_1, \ldots, X_n]$ ein Polynom, das auf V verschwindet. Dann gehört F zum Radikal von $\mathfrak{a}$, d.h. es gibt ein $r \in \mathbb{N}$ mit $F^r \in \mathfrak{a}$.

Beweis. Angenommen, F gehöre nicht zum Radikal von $\mathfrak{a}$. Dann gibt es nach Satz 10.9 auch ein maximales Ideal $\mathfrak{m} \subset K[X_1, \ldots, X_n]$ mit $\mathfrak{a} \subseteq \mathfrak{m}$ und mit $F \notin \mathfrak{m}$. Nach Satz 10.10 ist

$$\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$$

für gewisse $a_1, \ldots, a_n \in K$. Die Eigenschaft $F \notin \mathfrak{m}$ bedeutet, dass F im zugehörigen Restekörper nicht 0 ist, und das bedeutet $F(a_1, \ldots, a_n) \neq 0$. Wegen $\mathfrak{a} \subseteq \mathfrak{m}$ ist aber $(a_1, \ldots, a_n)$ ein Punkt von V, so dass dort nach Voraussetzung F verschwindet. Das ist also ein Widerspruch. □

Satz 2. *((Radikale und affin-algebraische Mengen))*

Sei K ein algebraisch abgeschlossener Körper mit dem Polynomring $K[X_1, \ldots, X_n]$ und dem affinen Raum $\mathbb{A}_K^n$. Dann gibt es eine natürliche Korrespondenz zwischen affin-algebraischen Mengen in $\mathbb{A}_K^n$ und Radikalidealen in $K[X_1, \ldots, X_n]$. Dabei gehen Radikale auf ihre Nullstellengebilde und affin-algebraische Mengen auf ihre Verschwindungsideale.

Beweis. Sei $V \subseteq \mathbb{A}_K^n$ affin-algebraisch. Dann gilt $V = V(\operatorname{Id}(V))$ nach Lemma 3.7 (3). Für ein Radikal $I \subseteq K[X_1, \ldots, X_n]$ gilt die Inklusion $I \subseteq \operatorname{Id}(V(I))$ ebenfalls nach Lemma 3.7 (2). Die umgekehrte Inklusion, also $\operatorname{Id}(V(I)) \subseteq I$ ist der Inhalt des Hilbertschen Nullstellensatzes 11.1. □

Korollar 3. *Sei K ein algebraisch abgeschlossener Körper und seien $F_i \in K[X_1, \ldots, X_n]$, $i \in I$, Polynome mit*

$$\mathbb{A}_K^n = \bigcup_{i \in I} D(F_i) .$$

Dann erzeugen die F_i das Einheitsideal in $K[X_1, \ldots, X_n]$.

Beweis. Sei $\mathfrak{b}$ das von den F_i erzeugte Ideal. Die Voraussetzung besagt, dass

$$\bigcap_{i \in I} V(F_i) = V(\mathfrak{b})$$

leer ist. Dann ist $V(1) \subseteq V(\mathfrak{b})$, da ja $V(1)$ ebenfalls leer ist. Aus dem Hilbertschen Nullstellensatz 11.1 folgt, dass eine Potenz von 1, also 1 selbst, zu $\mathfrak{b}$ in $K[X_1, \ldots, X_n]$ gehört. D.h. dass $\mathfrak{b}$ das Einheitsideal ist. $\square$

Der Hilbertsche Nullstellensatz, wie wir ihn für den affinen Raum und den Polynomring formuliert haben, gilt entsprechend für jedes $V(\mathfrak{a})$ und den zugehörigen Restklassenring $K[X_1, \ldots, X_n]/\mathfrak{a}$.

Korollar 4. *Sei K ein algebraisch abgeschlossener Körper und sei $R = K[X_1, \ldots, X_n]/\mathfrak{a}$ eine endlich erzeugte K-Algebra mit Nullstellengebilde $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$. Es sei $\mathfrak{b}$ ein Ideal in R und $F \in R$ ein Element, das auf $V(\mathfrak{b}) \subseteq V$ verschwindet. Dann gibt es ein $r \in \mathbb{N}$ mit $F^r \in \mathfrak{b}$ in R.*

Beweis. Die Verschwindungsbedingung $V(\mathfrak{b}) \subseteq V(F)$ in $V = V(\mathfrak{a})$ besagt zurückübersetzt in den affinen Raum, dass dort $V(\mathfrak{a} + \mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b}) \subseteq V(F)$ gilt, wobei jetzt F ein repräsentierendes Polynom aus $K[X_1, \ldots, X_n]$ und $\mathfrak{b}$ das Urbildideal in $K[X_1, \ldots, X_n]$ sei. Nach dem Hilbertschen Nullstellensatz 11.1 gibt es ein $r \in \mathbb{N}$ mit $F^r \in \mathfrak{a} + \mathfrak{b}$. Dies bedeutet modulo $\mathfrak{a}$, dass in R die Beziehung $F^r \in \mathfrak{b}$ gilt. $\square$

Korollar 5. *Sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge, die durch das Ideal $\mathfrak{a}$ beschrieben werde. Es seien $F_i \in K[X_1, \ldots, X_n]$, $i \in I$, Polynome mit*

$$V = \bigcup_{i \in I} D(F_i) \, .$$

Dann erzeugen die F_i das Einheitsideal in $K[X_1, \ldots, X_n]/\mathfrak{a}$.

Beweis. Sei $\mathfrak{b}$ das von allen F_i, $i \in I$, erzeugte Ideal in $K[X_1, \ldots, X_n]/\mathfrak{a}$. Die Voraussetzung besagt, dass

$$V(\mathfrak{b}) = \bigcap_{i \in I} V(F_i)$$

(auf V) leer ist. Dann ist $V(1) \subseteq V(\mathfrak{b})$, da ja $V(1)$ ebenfalls leer ist. Aus dem Hilbertschen Nullstellensatz 11.4 folgt, dass eine Potenz von 1, also 1 selbst, zu $\mathfrak{b}$ in $K[X_1, \ldots, X_n]/\mathfrak{a}$ gehört. $\square$

Korollar 6. *Sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge, die durch das Ideal $\mathfrak{a}$ beschrieben werde. Es sei $F \in K[X_1, \ldots, X_n]$ ein Polynom, das auf V keine Nullstelle besitzt. Dann ist F im Restklassenring $K[X_1, \ldots, X_n]/\mathfrak{a}$ eine Einheit.*

Beweis. Dies ist ein Spezialfall von Korollar 11.5. $\square$

Korollar 7. *Sei K ein algebraisch abgeschlossener Körper und seien V_1 und V_2 zwei affin-algebraische Mengen in $\mathbb{A}_K^n$. Dann gilt*

$$\operatorname{Id}(V_1 \cap V_2) = \operatorname{rad}(\operatorname{Id}(V_1) + \operatorname{Id}(V_2)) \, .$$

Beweis. Sei $\mathfrak{a}_1 = \mathrm{Id}\,(V_1)$ und $\mathfrak{a}_2 = \mathrm{Id}\,(V_2)$. Die Aussage ergibt sich aus

$$\mathrm{rad}\,(\mathfrak{a}_1 + \mathfrak{a}_2) = \mathrm{Id}\,(V(\mathrm{rad}\,(\mathfrak{a}_1 + \mathfrak{a}_2))) = \mathrm{Id}\,(V(\mathfrak{a}_1 + \mathfrak{a}_2)) = \mathrm{Id}\,(V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2))\,,$$

wobei die erste Gleichung auf dem Hilbertschen Nullstellensatz 11.1 beruht. □

Auch diese Eigenschaften gelten nicht ohne die Voraussetzung algebraisch abgeschlossen, wie das folgende Beispiel zeigt.

Beispiel 8. Wir betrachten die beiden algebraischen Kurven

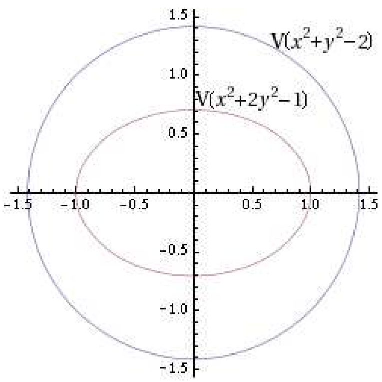
$$V_1 = V(X^2 + Y^2 - 2) \text{ und } V_2 = (X^2 + 2Y^2 - 1) \subseteq \mathbb{A}^2_K\,.$$

Bei $K = \mathbb{R}$ sind das beides irreduzible Quadriken. Der Durchschnitt wird beschrieben durch das Ideal

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

Da das Polynom $Y^2 + 1$ im Reellen keine Nullstelle hat, ist der Durchschnitt $V_1 \cap V_2 = \emptyset$ leer. Das Verschwindungsideal des (leeren) Durchschnittes ist natürlich das Einheitsideal, die Summe der beiden Verschwindungsideale ist aber nicht das Einheitsideal.

Es folgt, dass die Funktion $X^2 + 2Y^2 - 1$ auf $V(X^2 + Y^2 - 2)$ keine Nullstelle besitzt, also dort überall eine Einheit ist, aber dass sie keine Einheit im Koordinatenring $K[X,Y]/(X^2 + Y^2 - 2)$ ist.



Der Koordinatenring zu einer affin-algebraischen Menge

Sei $V \subseteq \mathbb{A}^n_K$ eine affin-algebraische Menge mit Verschwindungsideal $\mathrm{Id}\,(V)$. Ein Polynom $F \in K[X_1, \ldots, X_n]$ definiert eine Funktion auf dem affinen Raum und induziert damit eine Funktion auf der Teilmenge V.

$$\begin{tikzcd} \mathbb{A}^n_K \arrow[r, "F"] & K \\ V \arrow[u] \arrow[ur] & \end{tikzcd}$$

Dabei induziert ein Element aus dem Verschwindungsideal (nach Definition) die Nullfunktion auf V, und zwei Polynome $G, H \in K[X_1, \ldots, X_n]$, deren Differenz zum Verschwindungsideal gehören, induzieren auf V die gleiche Funktion. Es ist daher naheliegend, den Restklassenring $K[X_1, \ldots, X_n]/\operatorname{Id}(V)$ als Ring der polynomialen (oder algebraischen) Funktion auf V zu betrachten.

Definition 9. Zu einer affin-algebraischen Menge $V \subseteq \mathbb{A}_K^n$ mit Verschwindungsideal $\operatorname{Id}(V)$ nennt man

$$R(V) = K[X_1, \ldots, X_n]/\operatorname{Id}(V)$$

den *Koordinatenring*von V.

Dieser Begriff ist nicht völlig unproblematisch, insbesondere, wenn K nicht algebraisch abgeschlossen ist, siehe die Beispiele weiter unten. Wir erwähnen zunächst einige elementare Eigenschaften.

Proposition 10. *Sei $V \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge und sei $R = K[X_1, \ldots, X_n]/\operatorname{Id}(V)$ der zugehörige Koordinatenring. Dann gelten folgende Aussagen.*

(1) *R ist reduziert.*
(2) *$V = \emptyset$ genau dann, wenn R der Nullring ist.*
(3) *V ist irreduzibel genau dann, wenn R ein Integritätsbereich ist.*
(4) *V besteht aus einem einzigen Punkt genau dann, wenn $R = K$ ist.*
(5) *Ist K algebraisch abgeschlossen, und $V = V(\mathfrak{a})$, so ist $R = K[X_1, \ldots, X_n]/\operatorname{rad}(\mathfrak{a})$.*

Beweis. Es sei $I = \operatorname{Id}(V)$ das Verschwindungsideal zu V.

(1). Dies folgt aus Lemma 3.13 und Aufgabe 3.3.

(2). $V = \emptyset$ ist äquivalent zu $1 \in I$, und das ist äquivalent zu $R = 0$.

(3). Dies folgt aus Lemma 4.3 und Lemma (siehe die Übersicht zur Restklassenbildung).

(4). Sei $V = \{P\}$, $P = (a_1, \ldots, a_n)$. Dann ist $I = (X_1 - a_1, \ldots, X_n - a_n)$ und der Koordinatenring ist

$$K[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n) \cong K\,.$$

Umgekehrt, wenn der Koordinatenring K ist, so muss der zugehörige Restklassenhomomorphismus ein Einsetzungshomomorphismus $X_i \mapsto a_i$ sein, und das Verschwindungsideal zu V muss ein Punktideal sein, und es ist $P = (a_1, \ldots, a_n) \in V$. Wenn es noch einen weiteren Punkt $Q \in V$, $Q \neq P$, gibt, so hat man einen Widerspruch, da nicht alle $X_i - a_i$ in Q verschwinden.

(5). Bei K algebraisch abgeschlossen ist $\operatorname{Id}(V) = \operatorname{rad}(\mathfrak{a})$ nach dem Hilbertschen Nullstellensatz 11.1. □

Satz 11. *Sei K ein unendlicher Körper. Dann ist das Verschwindungsideal des affinen Raumes $\mathbb{A}_K^n$ das Nullideal und der zugehörige Koordinatenring ist der Polynomring $K[X_1, \ldots, X_n]$.*

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl der Variablen. Bei $n = 1$ folgt die Aussage daraus, dass ein Polynom vom Grad d maximal d Nullstellen besitzt. Zum Induktionsschritt sei $F \in K[X_1, \ldots, X_n]$ ein Polynom, das an allen Punkten von $\mathbb{A}_K^n = K^n$ verschwindet. Wir schreiben F als

$$F = P_d X_n^d + P_{d-1} X_n^d + \ldots + P_1 X_0 + P_0$$

mit Polynomen $P_d, \ldots, P_0 \in K[X_1, \ldots, X_{n-1}]$. Wir müssen zeigen, dass $F = 0$ ist, was äquivalent zu $P_i = 0$ ist für alle $i = 0, \ldots, d$. Sei also (ohne Einschränkung) angenommen, dass P_d nicht das Nullpolynom ist. Nach Induktionsvoraussetzung ist es dann auch nicht die Nullfunktion, d.h. es gibt einen Punkt $(a_1, \ldots, a_{n-1})$ mit $P_d(a_1, \ldots, a_{n-1}) \neq 0$. Damit ist $F(a_1, \ldots, a_{n-1})$ ein Polynom in der einen Variablen X_n vom Grad d und ist nach dem Fall einer Variablen nicht die Nullfunktion. □

Beispiel 12. Die Aussage 11.11 ist nicht richtig für endliche Körper. Für einen endlichen Körper besteht ein affiner Raum nur aus endlich vielen Punkten und es gibt viele Polynome, die auf all diesen Punkten verschwinden. Typische Beispiele werden gegeben durch die Polynome $X_i^q - X_i$, wobei q die Anzahl der Körperelemente bezeichne.

Beispiel 13. Sei $R = \mathbb{R}[X, Y]/(X^2 + Y^2)$. Da Quadrate im Reellen nie negativ sind, besteht die Nullstellenmenge des Polynoms $X^2 + Y^2$ einzig aus dem Nullpunkt, $V(X^2 + Y^2) = \{(0, 0)\}$. Das zugehörige Verschwindungsideal ist das maximale Ideal (X, Y), und der zugehörige Restklassenring (der Koordinatenring) ist dann $\mathbb{R}[X, Y]/(X, Y) \cong \mathbb{R}$. Der Koordinatenring kann also vom Restklassenring, mit dem man startet und dessen Ideal das Nullstellengebilde definiert, sehr verschieden sein.