

Algebraische Kurven - Vorlesung 9

Noethersche Ringe

Unser Ziel ist es zu zeigen, dass wenn R ein noetherscher Ring ist, dann auch der Polynomring $R[X]$ ein noetherscher Ring ist (Hilbertscher Basissatz). Dies gilt dann auch für die Hinzunahme von mehreren (endlich vielen) Variablen und insbesondere für Polynomringe in endlich vielen Variablen über einem Körper. Wir erinnern an den Begriff des noetherschen Ringes.

Definition 1. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.



Emmy Noether (1882-1935)

Proposition 2. Für einen kommutativen Ring R sind folgende Aussagen äquivalent.

- (1) R ist noethersch.
- (2) Jede aufsteigende Idealkette

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

wird stationär, d.h. es gibt ein n mit $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$

Beweis. (1) \Rightarrow (2). Sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

eine aufsteigende Idealkette in R . Wir betrachten die Vereinigung $\mathfrak{a} = \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n$, die wieder ein Ideal in R ist. Da R noethersch ist, ist \mathfrak{a} endlich erzeugt, d.h. $\mathfrak{a} = (f_1, \dots, f_k)$. Da diese f_i in der Vereinigung der Ideale \mathfrak{a}_n liegen, und da die Ideale aufsteigend sind, muss es ein n geben derart, dass $f_1, \dots, f_k \in \mathfrak{a}_n$ liegt. Wegen

$$(f_1, \dots, f_k) \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+m} \subseteq \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n \subseteq (f_1, \dots, f_k)$$

für $m \geq 0$ muss hier Gleichheit gelten, so dass die Idealkette ab n stationär ist.

(2) \Rightarrow (1). Sei \mathfrak{a} ein Ideal in R . Wir nehmen an, \mathfrak{a} sei nicht endlich erzeugt, und konstruieren sukzessive eine unendliche echt aufsteigende Idealkette $\mathfrak{a}_n \subset \mathfrak{a}$, wobei die \mathfrak{a}_n alle endlich erzeugt sind. Sei dazu

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots \subset \mathfrak{a}_n \subset \mathfrak{a}$$

bereits konstruiert. Da \mathfrak{a}_n endlich erzeugt ist, aber \mathfrak{a} nicht, ist die Inklusion $\mathfrak{a}_n \subseteq \mathfrak{a}$ echt und es gibt ein Element

$$f_{n+1} \in \mathfrak{a}, f_{n+1} \notin \mathfrak{a}_n$$

Dann setzt das Ideal $\mathfrak{a}_{n+1} := \mathfrak{a}_n + (f_{n+1})$ die Idealkette echt aufsteigend fort. \square

Lemma 3. (*Restklassenringe noetherscher Ringe*)

Sei R ein noetherscher Ring. Dann ist auch jeder Restklassenring R/\mathfrak{b} noethersch.

Beweis. Sei $\mathfrak{a} \subseteq R/\mathfrak{b}$ ein Ideal und sei $\tilde{\mathfrak{a}} \subseteq R$ das Urbildideal davon. Dieses ist endlich erzeugt nach Voraussetzung, also $\tilde{\mathfrak{a}} = (f_1, \dots, f_n)$. Die Restklassen dieser Erzeuger, also $\bar{f}_1, \dots, \bar{f}_n$, bilden ein Idealerzeugendensystem von \mathfrak{a} : Für ein Element $\bar{g} \in \mathfrak{a}$ gilt ja $g = \sum_{i=1}^n r_i f_i$ in R und damit $\bar{g} = \sum_{i=1}^n \bar{r}_i \bar{f}_i$ in R/\mathfrak{b} . \square

Der Hilbertsche Basissatz

Wie viele grundlegende Aussagen der kommutativen Algebra geht der Hilbertsche Basissatz, dem wir uns jetzt zuwenden, auf David Hilbert zurück, genauer auf seine Arbeit von 1890, „Ueber die Theorie der algebraischen Formen“.



David Hilbert (1862-1943)

Satz 4. (*Hilbertscher Basissatz*)

Sei R ein noetherscher Ring. Dann ist auch der Polynomring $R[X]$ noethersch.

Beweis. Sei \mathfrak{b} ein Ideal im Polynomring $R[X]$. Zu $n \in \mathbb{N}$ definieren wir ein Ideal \mathfrak{a}_n in R durch

$$\mathfrak{a}_n = \{c \in R : \text{es gibt } F \in \mathfrak{b} \text{ mit } F = cX^n + c_{n-1}X^{n-1} + \dots + c_1X + c_0\}.$$

Die Menge \mathfrak{a}_n besteht also aus allen Leitkoeffizienten von Polynomen vom Grad n aus \mathfrak{b} . Es handelt sich dabei offensichtlich um Ideale in R (wobei wir hier 0 als Leitkoeffizient zulassen). Ferner ist $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$, da man ja ein Polynom F vom Grad n mit Leitkoeffizient c mit der Variablen X multiplizieren kann, um ein Polynom vom Grad $n+1$ zu erhalten, das wieder c als Leitkoeffizient besitzt. Da R noethersch ist, muss diese aufsteigende Idealkette stationär werden; sei n so, dass $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$ ist.

Zu jedem $i \leq n$ sei nun $\mathfrak{a}_i = (c_{i1}, \dots, c_{ik_i})$ ein endliches Erzeugendensystem, und es seien

$$F_{ij} = c_{ij}X^i + \text{Terme von kleinerem Grad}$$

zugehörige Polynome aus \mathfrak{b} (die es nach Definition der \mathfrak{a}_i geben muss).

Wir behaupten, dass \mathfrak{b} von allen $\{F_{ij} : 0 \leq i \leq n, 1 \leq j \leq k_i\}$ erzeugt wird. Dazu beweisen wir zu $G \in \mathfrak{b}$ durch Induktion über den Grad von G , dass es als Linearkombination mit diesen F_{ij} darstellbar ist. Für G konstant, also $G \in R$, ist dies klar. Sei nun der Grad von G gleich d und die Aussage sei für kleineren Grad bewiesen. Wir schreiben

$$G = cX^d + c_{d-1}X^{d-1} + \dots + c_1X + c_0.$$

Es ist $c \in \mathfrak{a}_d$ und damit kann man c schreiben als R -Linearkombination der c_{ij} , $0 \leq i \leq n$, $1 \leq j \leq k_i$. Bei $d \leq n$ kann man c sogar schreiben als R -Linearkombination der c_{dj} , $j = 1, \dots, k_d$, sagen wir $c = \sum_{j=1}^{k_d} r_j c_{dj}$. Dann ist $G - \sum_{j=1}^{k_d} r_j F_{dj} \in \mathfrak{b}$ und hat einen kleineren Grad, so dass man darauf die Induktionsvoraussetzung anwenden kann. Bei $d > n$ ist

$$c = \sum_{i=0, \dots, n, j=1, \dots, k_i} r_{ij} c_{ij}.$$

Damit gehört

$$G - \sum_{i=0, \dots, n, j=1, \dots, k_i} r_{ij} X^{d-i} F_{ij}$$

ebenfalls zu \mathfrak{b} und hat einen kleineren Grad, so dass man wieder die Induktionsvoraussetzung anwenden kann. \square

Korollar 5. *Sei R ein noetherscher Ring. Dann ist auch $R[X_1, \dots, X_n]$ noethersch.*

Beweis. Dies folgt durch induktive Anwendung des Hilbertschen Basissatzes auf die Kette

$$\begin{aligned} R \subset R[X_1] \subset (R[X_1])[X_2] &= R[X_1, X_2] \subset (R[X_1, X_2])[X_3] \\ &= R[X_1, X_2, X_3] \subset \dots \subset R[X_1, \dots, X_n]. \end{aligned}$$

\square

Korollar 6. *Sei K ein Körper. Dann ist $K[X_1, \dots, X_n]$ noethersch.*

Beweis. Dies ist ein Spezialfall von Korollar 9.5. \square

Der Hilbertsche Basissatz bedeutet insbesondere, dass jede abgeschlossene Untervarietät $V \subset \mathbb{A}_K^n$ in einem affinen Raum durch endlich viele Polynome beschrieben werden kann. Jedes algebraische Nullstellengebilde ist also bereits das Nullstellengebilde von endlich vielen Polynomen.

Korollar 7. *Sei $V \subseteq \mathbb{A}_K^n$ eine affin-algebraische Menge. Dann gibt es eine Abbildung*

$$\varphi : \mathbb{A}_K^n \rightarrow \mathbb{A}_K^m,$$

die komponentenweise durch Polynome $F_i \in K[X_1, \dots, X_n]$ gegeben ist, also $\varphi = (F_1, \dots, F_m)$, derart, dass V das Urbild des Nullpunktes $0 \in \mathbb{A}_K^m$ ist.

Beweis. Es sei \mathfrak{a} ein beschreibendes Ideal für V , also $V = V(\mathfrak{a})$. Nach dem Hilbertschen Basissatz gibt es $F_1, \dots, F_m \in K[X_1, \dots, X_n]$ mit $\mathfrak{a} = (F_1, \dots, F_m)$. Damit ist insbesondere

$$V = V(\mathfrak{a}) = V(F_1) \cap \dots \cap V(F_m).$$

Diese F_i kann man zu einer Abbildung

$$\varphi = (F_1, \dots, F_m) : \mathbb{A}_K^n \longrightarrow \mathbb{A}_K^m$$

zusammenfassen. Dann ist $\varphi(P) = 0$ genau dann, wenn alle Komponentenfunktionen null sind, und das ist genau dann der Fall, wenn $P \in V(F_i)$ ist für alle i . \square

Definition 8. Sei R ein kommutativer Ring. Eine R -Algebra A heißt *von endlichem Typ* (oder *endlich erzeugt*), wenn sie die Form

$$A = R[X_1, \dots, X_n]/\mathfrak{a}$$

besitzt.

Eine endlich erzeugte R -Algebra besitzt also eine Darstellung als Restklassenring einer Polynomalgebra über R in endlich vielen Variablen. Eine solche Darstellung ist keineswegs eindeutig.

Korollar 9. *Sei R ein noetherscher Ring. Dann ist jede R -Algebra von endlichem Typ ebenfalls noethersch. Insbesondere ist für einen Körper K jede K -Algebra von endlichem Typ noethersch.*

Beweis. Dies folgt aus Korollar 9.5 und aus Lemma 9.3. \square

Zerlegung in irreduzible Komponenten

Aus dem Hilbertschen Basissatz folgt, dass eine aufsteigende Idealkette

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$$

in $K[X_1, \dots, X_n]$ stationär werden muss. Dies hat für absteigende Ketten von affin-algebraischen Teilmengen in einem affinen Raum folgende Konsequenz:

Satz 10. *In einem affinen Raum \mathbb{A}_K^n wird jede absteigende Folge von abgeschlossenen Mengen*

$$V_1 \supseteq V_2 \supseteq \dots$$

stationär.

Beweis. Sei

$$V_1 \supseteq V_2 \supseteq \dots$$

eine absteigende Kette von affin-algebraischen Teilmengen im \mathbb{A}_K^n . Daraus folgt nach Lemma 3.6 $\text{Id}(V_i) \subseteq \text{Id}(V_{i+1})$ für die zugehörigen Verschwindungsideale. Nach Korollar 9.6 wird diese Idealkette stationär, sagen wir für $i \geq i_0$. Nach Lemma 3.7 ist $V_i = V(\text{Id}(V_i))$. Daraus folgt dann aber für $i \geq i_0$, dass

$$V_i = V(\text{Id}(V_i)) = V(\text{Id}(V_{i+1})) = V_{i+1},$$

so dass die absteigende Kette stationär werden muss. \square

Es ergibt sich daraus durch Übergang zu den Komplementen, dass jede aufsteigende Kette von Zariski-offenen Mengen in einem affinen Raum stationär wird. Eine solche Topologie nennt man auch *noethersch* (generell nennt man eine (partielle) Ordnung, für die jede aufsteigende Kette stationär wird, noethersch). Für einen noetherschen Raum gilt: jede nicht-leere Teilmenge von offenen Mengen (abgeschlossenen Mengen) besitzt ein maximales (minimales) Element. Dies kann man vorteilhaft als Beweisprinzip einsetzen (*Beweis durch noethersche Induktion*): Man möchte zeigen, dass eine gewisse Eigenschaft E für alle abgeschlossenen Teilmengen gilt, und man betrachtet die Menge derjenigen abgeschlossenen Teilmengen, die E nicht erfüllen. Man möchte zeigen, dass die Menge leer ist, und nimmt an, dass sie nicht leer ist. Dann besitzt sie auch ein minimales Element, und dies muss man dann zum Widerspruch führen. Die Gültigkeit dieses Beweisprinzips beruht darauf, dass man in einer nicht-leeren Menge ohne einem minimalen Element eine unendlich absteigende Kette konstruieren kann. Ein typisches Beispiel für dieses Beweisprinzip liefert der Beweis der folgenden Aussage.

Satz 11. *Sei $V \subset \mathbb{A}_K^n$ eine affin-algebraische Menge. Dann gibt es eine eindeutige Zerlegung*

$$V = V_1 \cup \dots \cup V_k$$

mit irreduziblen Mengen V_i mit $V_i \not\subseteq V_j$ für $i \neq j$.

Beweis. Die Existenz beweisen wir durch noethersche Induktion. Angenommen, nicht jede affin-algebraische Menge habe eine solche Zerlegung. Dann gibt es auch eine minimale Teilmenge, sagen wir V , ohne eine solche Zerlegung. V kann nicht irreduzibel sein, sondern es gibt eine nicht-triviale Darstellung $V = V_1 \cup V_2$. Da V_1 und V_2 echte Teilmengen von V sind, gibt es für diese beiden jeweils endliche Darstellungen als Vereinigung von irreduziblen Teilmengen. Diese beiden vereinigen sich zu einer Darstellung von V , was ein Widerspruch ist.

Zur Eindeutigkeit. Sei

$$V = V_1 \cup \dots \cup V_k = W_1 \cup \dots \cup W_m$$

zwei Zerlegungen in irreduzible Teilmengen (jeweils ohne Inklusionsbeziehung). Es ist

$$V_1 = V_1 \cap V = V_1 \cap (W_1 \cup \dots \cup W_m) = (V_1 \cap W_1) \cup \dots \cup (V_1 \cap W_m).$$

Da V_1 irreduzibel ist, muss $V_1 \subseteq W_j$ für ein j sein. Umgekehrt ist mit dem gleichen Argument $W_j \subseteq V_i$ für ein i , woraus $i = 1$ und $V_1 = W_j$ folgt. Ebenso findet sich V_2 etc. in der Zerlegung rechts wieder, so dass die Zerlegung eindeutig ist. \square

Moduln

Definition 12. Sei R ein kommutativer Ring und $M = (M, +, 0)$ eine kommutative Gruppe. Man nennt M einen R -Modul, wenn es eine Operation

$$R \times M \longrightarrow M, (r, v) \longmapsto rv = r \cdot v$$

gibt, die folgende Axiome erfüllt (dabei seien $r, s \in R$ und $u, v \in M$ beliebig):

- (1) $r(su) = (rs)u$,
- (2) $r(u + v) = (ru) + (rv)$,
- (3) $(r + s)u = (ru) + (su)$,
- (4) $1u = u$.

Definition 13. Sei R ein kommutativer Ring und M ein R -Modul. Eine Teilmenge $U \subseteq M$ heißt *Unterm modul*, wenn sie eine Untergruppe von M ist und wenn für jedes $u \in U$ und $r \in R$ gilt, dass auch $ru \in U$ ist.

Definition 14. Sei R ein kommutativer Ring und M ein R -Modul. Eine Teilmenge $v_i \in M, i \in I$, heißt *Erzeugendensystem* für M , wenn es für jedes Element $v \in M$ eine Darstellung

$$v = \sum_{i \in J} r_i v_i$$

gibt, wobei $J \subseteq I$ endlich ist und $r_i \in R$.

Definition 15. Sei R ein kommutativer Ring und M ein R -Modul. Der Modul M heißt *endlich erzeugt* oder *endlich*, wenn es ein endliches Erzeugendensystem $v_i, i \in I$, für ihn gibt (also mit einer endlicher Indexmenge).

Ein kommutativer Ring R selbst ist in natürlicher Weise ein R -Modul, wenn man die Ringmultiplikation als Skalarmultiplikation interpretiert. Die Ideale sind dann genau die R -Unterm oduln von R . Die Begriffe Ideal-Erzeugendensystem und Modul-Erzeugendensystem stimmen für Ideale überein.