Algebraische Kurven

Vorlesung 21

Diskrete Bewertungsringe

Wir setzen nun die lokale Untersuchung von algebraischen Kurven fort und werden im weiteren Verlauf verschiedene Charakterisierungen dafür finden, dass ein Punkt einer Kurve nichtsingulär (oder glatt) ist. Zu dem Punkt P auf der Kurve gehört der lokale Ring in P, der die Lokalisierung des affinen Koordinatenringes der Kurve am maximalen Ideal ist, das zu P gehört. Wenn $P = (a, b) \in C = V(F) \subset \mathbb{A}_K^2$ ist, so lässt sich der lokale Ring in doppelter Weise beschreiben, nämlich als

$$K[X,Y]_{(X-a,Y-b)}/(F) \cong (K[X,Y]/(F))_{\mathfrak{m}}$$

(dabei ist $\mathfrak{m}$ das maximale Ideal aufgefasst im Restklassenring). Dieser Ring beschreibt die wesentlichen algebraischen Eigenschaften des Punktes auf der Kurve. Wichtig ist zunächst der Begriff des diskreten Bewertungsringes.

Definition 21.1. Ein *diskreter Bewertungsring* R ist ein Hauptidealbereich mit der Eigenschaft, dass es bis auf Assoziiertheit genau ein Primelement in R gibt.

Lemma 21.2. *Ein diskreter Bewertungsring ist ein lokaler, noetherscher Hauptidealbereich mit genau zwei Primidealen, nämlich* 0 *und dem maximalen Ideal* $\mathfrak{m}$.

Beweis. Ein diskreter Bewertungsring ist kein Körper. In einem Hauptidealbereich, der kein Körper ist, wird jedes maximale Ideal von einen Primelement erzeugt, und die Primerzeuger zu verschiedenen maximalen Idealen können nicht assoziiert sein. Also gibt es genau ein maximales Ideal. Ebenso wird jedes von null verschiedene Primideal durch ein Primelement erzeugt, so dass es neben dem maximalen Ideal nur noch das Nullideal gibt. □

Beispiel 21.3. Es sei A ein Hauptidealbereich und $\mathfrak{m} \subseteq A$ ein maximales Ideal. Dieses ist ein Hauptideal und wird durch ein Primelement, sagen wir $\mathfrak{m} = (p)$, erzeugt. Die Lokalisierung

$$R = A_{\mathfrak{m}} = \left\{ \frac{f}{g} | \, f \in A, \, g \notin \mathfrak{m} \right\}$$

ist nach Satz 15.4 ein lokaler Ring mit dem maximalen Ideal $\mathfrak{m}A_{\mathfrak{m}}$, das ebenfalls von p erzeugt wird. Alle Primelemente $q \in A$, die nicht zu p assoziiert sind, werden in der Lokalisierung zu Einheiten. Daher gibt es in der Lokalisierung bis auf Assoziiertheit genau ein Primelement, und somit liegt ein diskreter Bewertungsring vor. Für $A = \mathbb{Z}$ und eine Primzahl p ist $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ der Unterring der rationalen Zahlen, deren Nenner kein Vielfaches von p sind.

DEFINITION 21.4. Zu einem Element $f \in R$, $f \neq 0$, in einem diskreten Bewertungsring mit Primelement p heißt die Zahl $n \in \mathbb{N}$ mit der Eigenschaft $f = up^n$, wobei u eine Einheit bezeichne, die *Ordnung* von f. Sie wird mit $\operatorname{ord}(f)$ bezeichnet.

Die Ordnung ist also nichts anderes als der Exponent zum (bis auf Assoziiertheit) einzigen Primelement in der Primfaktorzerlegung. Sie hat folgende Eigenschaften.

LEMMA 21.5. *Sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Dann hat die Ordnung*

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \operatorname{ord}(f),$$

folgende Eigenschaften.

(1) $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
(2) $\operatorname{ord}(f + g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$.
(3) $f \in \mathfrak{m}$ *genau dann, wenn* $\operatorname{ord}(f) \geq 1$.
(4) $f \in R^\times$ *genau dann, wenn* $\operatorname{ord}(f) = 0$.

Beweis. Siehe Aufgabe 21.5. □

Wir wollen eine wichtige Charakterisierung für diskrete Bewertungsringe beweisen, die insbesondere beinhaltet, dass ein normaler lokaler Integritätsbereich mit genau zwei Primidealen bereits ein diskreter Bewertungsring ist. Dazu benötigen wir einige Vorbereitungen.

LEMMA 21.6. *Sei R ein kommutativer Ring und sei $f \in R$ nicht nilpotent. Dann gibt es ein Primideal $\mathfrak{p}$ in R mit $f \notin \mathfrak{p}$.*

Beweis. Wir betrachten die Menge der Ideale

$$M = \{\mathfrak{a} \text{ Ideal} \mid f^r \notin \mathfrak{a} \text{ für alle } r\}\ .$$

Diese Menge ist nicht leer, da sie das Nullideal enthält. Ferner ist sie induktiv geordnet (bezüglich der Inklusion). Ist nämlich $\mathfrak{a}_i$ eine total geordnete Teilmenge, so ist deren Vereinigung ebenfalls ein Ideal, das keine Potenz von f enthält. Nach dem Lemma von Zorn gibt es daher maximale Elemente in M.

Wir behaupten, dass ein solches maximales Element $\mathfrak{p}$ ein Primideal ist. Sei dazu $g, h \in R$ und $gh \in \mathfrak{p}$, und sei $g, h \notin \mathfrak{p}$ angenommen. Dann hat man echte Inklusionen

$$\mathfrak{p} \subset \mathfrak{p} + (g), \mathfrak{p} + (h)\,.$$

Wegen der Maximalität können die beiden Ideale rechts nicht zu M gehören, und das bedeutet, dass es Exponenten $r, s \in \mathbb{N}$ gibt mit

$$f^r \in \mathfrak{p} + (g) \text{ und } f^s \in \mathfrak{p} + (h)\,.$$

Dann ergibt sich der Widerspruch

$$f^r f^s \in \mathfrak{p} + (gh) \subseteq \mathfrak{p}\,.$$

□

Lemma 21.7. *Sei R ein noetherscher lokaler kommutativer Ring. Es sei vorausgesetzt, dass das maximale Ideal $\mathfrak{m}$ das einzige Primideal von R ist. Dann gibt es einen Exponenten $n \in \mathbb{N}$ mit*

$$\mathfrak{m}^n = 0\,.$$

Beweis. Wir behaupten zunächst, dass jedes Element in R eine Einheit oder nilpotent ist. Sei hierzu $f \in R$ keine Einheit. Dann ist $f \in \mathfrak{m}$. Angenommen, f ist nicht nilpotent. Dann gibt es nach Lemma 21.6 ein Primideal $\mathfrak{p}$ mit $f \notin \mathfrak{p}$. Damit ergibt sich der Widerspruch $\mathfrak{p} \neq \mathfrak{m}$.

Es ist also jedes Element im maximalen Ideal nilpotent. Insbesondere gibt es für ein endliches Erzeugendensystem $f_1, \ldots, f_k$ von $\mathfrak{m}$ eine natürliche Zahl m mit $f_i^m = 0$ für alle $i = 1, \ldots, k$. Sei $n = km$. Dann ist ein beliebiges Element aus $\mathfrak{m}^n$ von der Gestalt

$$\left(\sum_{i=1}^k a_{i1} f_i\right) \left(\sum_{i=1}^k a_{i2} f_i\right) \cdots \left(\sum_{i=1}^k a_{in} f_i\right)\,.$$

Ausmultiplizieren ergibt eine Linearkombination mit Monomen $f_1^{r_1} \cdots f_k^{r_k}$ und $\sum_{i=1}^k r_i = n$, so dass ein f_i mit einem Exponenten $\geq n/k = m$ vorkommt. Daher ist das Produkt 0. □

Satz 21.8. *Sei R ein noetherscher lokaler Integritätsbereich mit der Eigenschaft, dass es genau zwei Primideale $0 \subset \mathfrak{m}$ gibt. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein diskreter Bewertungsring.*
(2) *R ist ein Hauptidealbereich.*
(3) *R ist faktoriell.*
(4) *R ist normal.*
(5) *$\mathfrak{m}$ ist ein Hauptideal.*

Beweis. (1) ⇒ (2) folgt direkt aus der Definition.

(2) ⇒ (3) folgt aus der allgemeinen Aussage, dass jeder Hauptidealbereich faktoriell ist.

(3) ⇒ (4) folgt aus Satz 20.3.

(4) ⇒ (5). Sei $f \in \mathfrak{m}$, $f \neq 0$. Dann ist $R/(f)$ ein noetherscher lokaler Ring mit nur einem Primideal (nämlich $\tilde{\mathfrak{m}} = \mathfrak{m}R/(f)$). Daher gibt es nach Satz

21.7 ein $n \in \mathbb{N}$ mit $\tilde{\mathfrak{m}}^n = 0$. Zurückübersetzt nach R heißt das, dass $\mathfrak{m}^n \subseteq (f)$ gilt. Wir wählen n minimal mit den Eigenschaften

$$\mathfrak{m}^n \subseteq (f) \text{ und } \mathfrak{m}^{n-1} \not\subseteq (f) .$$

Wähle $g \in \mathfrak{m}^{n-1}$ mit $g \notin (f)$ und betrachte

$$h := \frac{f}{g} \in Q(R) (\text{es ist } g \neq 0) .$$

Das Inverse, also $h^{-1} = \frac{g}{f}$, gehört nicht zu R, sonst wäre $g \in (f)$. Da R nach Voraussetzung normal ist, ist h^{-1} auch nicht ganz über R. Nach dem Modulkriterium Lemma 19.9 für die Ganzheit gilt insbesondere für das maximale Ideal $\mathfrak{m} \subset R$ die Beziehung

$$h^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$$

ist. Nach Wahl von g ist aber auch

$$h^{-1}\mathfrak{m} = \frac{g}{f}\mathfrak{m} \subseteq \frac{\mathfrak{m}^n}{f} \subseteq R .$$

Daher ist $h^{-1}\mathfrak{m}$ ein Ideal in R, das nicht im maximalen Ideal enthalten ist. Also ist $h^{-1}\mathfrak{m} = R$. Das heißt einerseits $h \in \mathfrak{m}$ und andererseits gilt für ein beliebiges $x \in \mathfrak{m}$ die Beziehung $h^{-1}x \in R$, also $x = h(h^{-1}x)$, also $x \in (h)$ und somit $(h) = \mathfrak{m}$.

(5) $\Rightarrow$ (1). Sei $\mathfrak{m} = (\pi)$. Dann ist π ein Primelement und zwar bis auf Assoziiertheit das einzige. Sei $f \in R$, $f \neq 0$ keine Einheit. Dann ist $f \in \mathfrak{m}$ und daher $f = \pi g_1$. Dann ist g_1 eine Einheit oder $g_1 \in \mathfrak{m}$. Im zweiten Fall ist wieder $g_1 = \pi g_2$ und $f = \pi^2 g_2$.

Wir behaupten, dass man $f = \pi^k u$ mit einer Einheit u schreiben kann. Andernfalls könnte man $f = \pi^n g_n$ mit beliebig großem n schreiben. Nach Satz 21.7 gibt es ein $m \in \mathbb{N}$ mit $(\pi^m) = \mathfrak{m}^m \subseteq (f)$. Bei $n \geq m+1$ ergibt sich $\pi^m = af = a\pi^{m+1}b$ und der Widerspruch $1 = ab\pi$.

Es lässt sich also jede Nichteinheit $\neq 0$ als Produkt einer Potenz des Primelements mit einer Einheit schreiben. Insbesondere ist R faktoriell. Für ein beliebiges Ideal $\mathfrak{a} = (f_1, \ldots, f_s)$ ist $f_i = \pi^{n_i} u_i$ mit Einheiten u_i. Dann sieht man leicht, dass $\mathfrak{a} = (\pi^n)$ ist mit $n = \min_i\{n_i\}$. □

Das Lemma von Nakayama

Nach dem vorangehenden Überlegungen liegt ein diskreter Bewertungsring genau dann vor, wenn der lokale Integritätsbereich die Eigenschaft hat, dass das maximale Ideal durch ein Element erzeugt wird. Es ist von daher naheliegend, generell die lokalen Ringe zu Punkten auf einer algebraischen Kurve dahingehend zu studieren, wie viele Erzeuger das maximale Ideal benötigt. Dies führt zum Begriff der Einbettungsdimension, den wir schon im Zusammenhang mit monomialen Kurven erwähnt haben. Diese Einbettungsdimension ist auch die Dimension des $R/\mathfrak{m}$-Vektorraumes $\mathfrak{m}/\mathfrak{m}^2$, für diesen Zusammenhang brauchen wir aber einige Vorbereitungen und insbesondere das *Lemma von Nakayama*.

Im Lemma von Nakayama wird folgende Konstruktion betrachtet: Zu einem R-Modul V, einem Untermodul $U \subseteq V$ und einem Ideal $I \subseteq R$ bezeichnet man mit IU den R-Untermodul von V, der von allen Elementen der Form fv, $f \in I$, $v \in U$, erzeugt wird (dies ist auch ein R-Untermodul von U). Ist U ebenfalls ein Ideal (also ein R-Untermodul von R)so fällt dieses Konzept mit dem Produkt von Idealen zusammen. Der Restklassenmodul V/IV ist dabei in natürlicher Weise nicht nur ein R-Modul, sondern auch ein R/I-Modul. Wenn I ein maximales Ideal ist, so bedeutet dies, dass der Restklassenmodul sogar ein Vektorraum über dem Restklassenkörper ist.

LEMMA 21.9. *Sei $(R, \mathfrak{m})$ ein lokaler Ring und sei V ein endlich erzeugter R-Modul. Es sei $\mathfrak{m}V = V$ vorausgesetzt. Dann ist $V = 0$.*

Beweis. Sei $v_1, \ldots, v_n$ ein Erzeugendensystem von V. Nach Voraussetzung gibt es wegen $v_i \in \mathfrak{m}V$ zu jedem v_i eine Darstellung

$$v_i = a_{i1}v_1 + \ldots + a_{in}v_n$$

mit $a_{ij} \in \mathfrak{m}$. Daraus ergibt sich für jedes i eine Darstellung

$$(1 - a_{ii})v_i = a_{i1}v_1 + \ldots + a_{i,i-1}v_{i-1} + a_{i,i+1}v_{i+1} + a_{in}v_n \,.$$

Da $a_{ii} \in \mathfrak{m}$ ist, ist der Koeffizient $1 - a_{ii}$ eine Einheit. Dies bedeutet aber, dass man nach v_i auflösen kann, so dass also v_i überflüssig ist. So kann man sukzessive auf alle Erzeuger verzichten, was bedeutet, dass der Nullmodul vorliegen muss. $\square$