Prof. Dr. H. Brenner **Osnabrück WS 2017/2018**

Algebraische Kurven

Vorlesung 19

Restklassendarstellung für monomiale Kurven

Sei $M \subseteq \mathbb{N}$ ein numerisches Monoid, das von den teilerfremden natürlichen Zahlen $e_1, \ldots, e_n$ erzeugt werde. Die zugehörige Surjektion $\mathbb{N}^n \to M \subseteq \mathbb{N}$ führt zu einer Surjektion

$$K[X_1, \ldots, X_n] \longrightarrow K[M],\ X_i \longmapsto T^{e_i},$$

und einer abgeschlossenen Einbettung $C = K-\text{Spek}\ (K[M]) \hookrightarrow \mathbb{A}^n_K$. Durch welche Gleichungen lässt sich C beschreiben?

Satz 19.1. *Sei $M \subseteq \mathbb{N}$ ein durch teilerfremde Elemente $e_1, \ldots, e_n$ erzeugtes Untermonoid und sei $\mathbb{N}^n \to M$ die zugehörige surjektive Abbildung mit dem zugehörigen Restklassenhomomorphismus $\varphi\colon K[X_1, \ldots, X_n] \to K[M]$. Dann wird das Kernideal durch*

$$\ker \varphi = \left(\prod_{i \in I_1} X_i^{r_i} - \prod_{i \in I_2} X_i^{s_i} : I_1, I_2 \subseteq \{1, \ldots, n\} \text{ disjunkt }, \sum_{i \in I_1} r_i e_i = \sum_{i \in I_2} s_i e_i \right)$$

(mit $r_i, s_i \geq 1$) beschrieben.

Beweis. Dass die angegebenen Elemente zum Kernideal gehören folgt direkt aus

$$\varphi\left(\prod_{i \in I_1} X_i^{r_i} \right) = \prod_{i \in I_1} (t^{e_i})^{r_i} = t^{\sum_{i \in I_1} r_i e_i}.$$

Für die Umkehrung sei $F \in K[X_1, \ldots, X_n]$ ein Polynom mit $\varphi(F) = 0$. Wir schreiben

$$F = \sum_{\nu} a_\nu X^\nu$$

(mit $\nu = (\nu_1, \ldots, \nu_n)$). Daher ist

$$\varphi(F) = \sum_{\nu} a_\nu t^{\sum_{i=1}^n \nu_i e_i} = \sum_{k=0} \left(\sum_{\nu\colon \sum_{i=1}^n \nu_i e_i = k} a_\nu \right) t^k.$$

Da dieses Polynom gleich 0 ist müssen alle Koeffizienten 0 sein, d.h. zu jedem k gehört auch

$$F_k = \sum_{\nu\colon \sum_{i=1}^n \nu_i e_i = k} a_\nu X^\nu$$

zum Kern. Wir können also annehmen, dass in F nur Monome X^ν mit dem gleichem Wert $\sum_{i=1}^n \nu_i e_i = k$ vorkommen. Betrachten wir ein solches Monom

aus F, sagen wir X^ν (mit $a_\nu \neq 0$). Es muss in F mindestens noch ein weiteres Monom, sagen wir X^μ, vorkommen, da ein einzelnes Monom nicht auf 0 abgebildet wird. Wir schreiben

$$F \;=\; a_\nu(X^\nu - X^\mu) + (F - a_\nu X^\nu + a_\nu X^\mu)\,.$$

Im Summand rechts kommt X^ν nicht mehr vor, und es kommt auch kein neues Monom hinzu. In $X^\nu - X^\mu$ können wir diejenigen Variablen, die beidseitig auftreten, so weit ausklammern, dass sich ein Ausdruck der Form

$$X^\nu - X^\mu \;=\; X_1^{b_1} \cdots X_n^{b_n} \left(\prod_{i \in I_1} X_i^{r_i} - \prod_{i \in I_2} X_i^{s_i} \right)$$

mit disjunkten I_1 und I_2 und mit $\sum_{i\in I_1} e_i r_i \;=\; \sum_{i\in I_2} e_i s_i$ ergibt. Der linke Summand in obiger Beschreibung von F gehört also zu dem von den angegebenen Binomen erzeugten Ideal und wir können mit dem rechten Summand, in dem ein Monom weniger vorkommt, fortfahren. □

Die im vorstehenden Satz auftretenden Gleichungen nennmt man *binomiale Gleichungen*. Die einfachsten binomialen Gleichungen sind von der Bauart ($i \neq j$)

$$X_i^{e_j/\operatorname{ggT}(e_i,e_j)} \;=\; X_j^{e_i/\operatorname{ggT}(e_i,e_j)}.$$

Im Fall von ebenen monomialen Kurven ist das auch die einzige Gleichung.

Korollar 19.2. *Sei C die durch $t \mapsto (t^{e_1}, t^{e_2}) = (x, y)$ (mit e_1, e_2 teilerfremd) gegebene monomiale ebene Kurve. Dann ist*

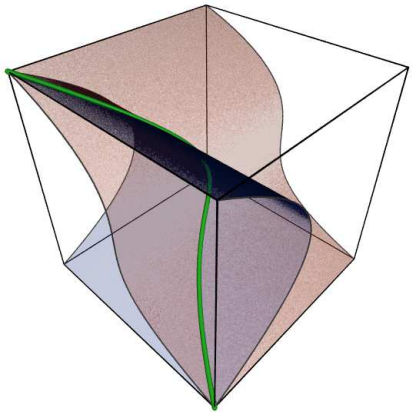
$$C \;=\; V(X^{e_2} - Y^{e_1}).$$

Beweis. Dies folgt sofort aus Satz 19.1. □

Bei monomialen Raumkurven lassen sich die beschreibenden Gleichungen auch noch einigermaßen einfach bestimmen, da man immer eine Variable isolieren kann.

Beispiel 19.3. Sei $C \subset \mathbb{A}^3_K$ die „gedrehte Kubik“, also das Bild der monomialen Abbildung, die durch $t \mapsto (t, t^2, t^3)$ gegeben ist. Diese Kurve ist isomorph zu einer affinen Geraden und insbesondere glatt. Das beschreibende Ideal ist nach Satz 19.1 gleich

$$\mathfrak{a} \;=\; (Y - X^2, Z - X^3, Y^3 - Z^2, Z - XY) \;=\; (Y - X^2, Z - X^3).$$



Die beiden letzten Idealerzeuger sind dabei überflüssig, da sie sich durch die beiden anderen ausdrücken lassen. Insgesamt ist also

$$C = V(Y - X^2, Z - X^3).$$

Die Bilder von C unter den drei verschiedenen Projektion sind

$$C_1 = V(Z^2 - Y^3),\ C_2 = V(Z - X^3),\ C_3 = V(Y - X^2)\,.$$

Dabei sind C_2 und C_3 isomorph zur affinen Geraden (als Graph einer Abbildung), während C_1 die singuläre Neilsche Parabel ist.

Beispiel 19.4. Sei C die durch

$$t \longmapsto (t^3, t^4, t^5) = (x, y, z)$$

gegebene monomiale Kurve. Für jede der drei Variablen müssen wir gemäß Satz 19.1 schauen, welche Potenzen davon, wenn man die t-Potenz substituiert, sich auch als Monom in den beiden anderen Variablen ausdrücken lassen.

Zunächst haben wir die Gleichungen, in denen jeweils nur zwei Variablen vorkommen. Das sind

$$Y^3 = X^4,\ Z^3 = X^5,\ Z^4 = Y^5\,.$$

Hier kann es, wie im ebenen Fall, immer nur eine Beziehung geben.

In den Relationen, wo alle drei Variablen beteiligt sind, kommt eine der Variablen allein vor. Starten wir mit X. Zunächst lassen sich X und X^2 nicht durch die anderen Variablen ausdrücken, dafür haben wir $X^3 = T^9 = YZ$. Eine andere (davon unabhängige) Kombination ist nicht möglich. Grundsätzlich impliziert eine mehrfache Darstellung $X^k = Y^iZ^j = Y^aZ^b$, dass man zwischen Potenzen von Y und von Z eine Beziehung hat, da man ja die kleineren Potenzen rauskürzen kann. Da wir alle Relationen mit nur zwei Variablen schon aufgelistet haben, liefert eine Potenz von X immer nur maximal eine neue Relation. Wir behaupten, dass wir für X alleinstehend schon fertig sind. Ist nämlich $X^k = Y^iZ^j$, so ist $k \geq 3$. Bei $i = 0$ oder $j = 0$

haben wir die Gleichungen schon aufgelistet. Sei also $i, j \geq 1$. Dann kann man aber mittels der Gleichung $X^3 = YZ$ die Exponenten in der Gleichung kleiner machen (indem man den Exponenten von X um 3 reduziert und die Exponenten von Y und von Z um 1).

Für Y hat man sofort die Gleichung $Y^2 = ZX$, mit der man wieder alle anderen Gleichungen reduzieren kann.

Für Z hat man $Z^2 = X^2Y$ und $Z^3 = XY^3$. Es gibt keine kleineren Monome in X und Y, die man als Potenz von Z ausdrücken kann. Daher kann man jede andere Relation mittels einer von diesen auf eine frühere zurückführen.

Insgesamt haben wir also für die Kurve C die Gleichungen

$$C = V(Y^3 - X^4, Z^3 - X^5, Z^4 - Y^5, X^3 - YZ, Y^2 - XZ, Z^2 - X^2Y, Z^3 - XY^3)$$

Ganzheit

DEFINITION 19.5. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ heißt eine Gleichung der Form

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1x + r_0 = 0,$$

wobei die Koeffizienten r_i, $i = 0, \ldots, n-1$, zu R gehören, eine *Ganzheitsgleichung* für x.

DEFINITION 19.6. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Ein Element $x \in S$ heißt *ganz* (über R), wenn x eine Ganzheitsgleichung mit Koeffizienten aus R erfüllt.

DEFINITION 19.7. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann nennt man die Menge der Elemente $x \in S$, die ganz über R sind, den *ganzen Abschluss* von R in S.

DEFINITION 19.8. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann heißt S *ganz* über R, wenn jedes Element $x \in S$ ganz über R ist.

S ist genau dann ganz über R, wenn der ganze Abschluss von R in S gleich S ist.

LEMMA 19.9. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ sind folgende Aussagen äquivalent.*

(1) *x ist ganz über R.*
(2) *Es gibt eine R-Unteralgebra T von S mit $x \in T$ und die ein endlicher R-Modul ist.*
(3) *Es gibt einen endlichen R-Untermodul M von S, der einen Nichtnullteiler aus S enthält, mit $xM \subseteq M$.*

Beweis. (1) $\Rightarrow$ (2). Wir betrachten die von den Potenzen von x erzeugte R-Unteralgebra $R[x]$ von S, die aus allen polynomialen Ausdrücken in x mit Koeffizienten aus R besteht. Aus einer Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1x + r_0 \;=\; 0$$

ergibt sich

$$x^n \;=\; -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \cdots - r_1x - r_0.$$

Man kann also x^n durch einen polynomialen Ausdruck von einem kleineren Grad ausdrücken. Durch Multiplikation dieser letzten Gleichung mit x^i kann man jede Potenz von x mit einem Exponenten $\geq n$ durch einen polynomialen Ausdruck von einem kleineren Grad ersetzen. Insgesamt kann man dann aber all diese Potenzen durch polynomiale Ausdrücke vom Grad $\leq n-1$ ersetzen. Damit ist

$$R[x] \;=\; R + Rx + Rx^2 + \cdots + Rx^{n-2} + Rx^{n-1}$$

und die Potenzen $x^0 = 1, x^1, x^2, \ldots, x^{n-1}$ bilden ein endliches Erzeugendensystem von $T = R[x]$.

(2) $\Rightarrow$ (3). Sei $x \in T \subseteq S$, T eine R-Unteralgebra, die als R-Modul endlich erzeugt sei. Dann ist $xT \subseteq T$, und T enthält den Nichtnullteiler 1.

(3) $\Rightarrow$ (1). Sei $M \subseteq S$ ein endlich erzeugter R-Untermodul mit $xM \subseteq M$. Seien $y_1, \ldots, y_n$ erzeugende Elemente von M. Dann ist insbesondere xy_i für jedes i eine R-Linearkombination der y_j, $j = 1, \ldots, n$. Dies bedeutet

$$xy_i \;=\; \sum_{j=1}^{n} r_{ij}y_j$$

mit $r_{ij} \in R$, oder, als Matrix geschrieben,

$$x \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix} \;=\; \begin{pmatrix} r_{1,1} & r_{1,2} & . & . & r_{1,n} \\ r_{2,1} & r_{2,2} & . & . & r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ r_{n,1} & r_{n,2} & . & . & r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix}.$$

Dies schreiben wir als

$$0 \;=\; \begin{pmatrix} x - r_{1,1} & -r_{1,2} & . & . & -r_{1,n} \\ -r_{2,1} & x - r_{2,2} & . & . & -r_{2,n} \\ . & . & . & . & . \\ . & . & . & . & . \\ -r_{n,1} & -r_{n,2} & . & . & x - r_{n,n} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ y_n \end{pmatrix}.$$

Nennen wir diese Matrix A (die Einträge sind aus S), und sei A^{adj} die adjungierte Matrix. Dann gilt $A^{adj}Ay = 0$ (y bezeichne den Vektor $(y_1, \ldots, y_n)$) und nach der Cramerschen Regel ist $A^{adj}A = (\det A)E_n$, also gilt $((\det A)E_n)y = 0$. Es ist also $(\det A)y_j = 0$ für alle j und damit $(\det A)z = 0$ für alle $z \in M$. Da M nach Voraussetzung einen Nichtnullteiler enthält, muss $\det A = 0$ sein.

Die Determinante ist aber ein normierter polynomialer Ausdruck in x vom Grad n, so dass eine Ganzheitsgleichung vorliegt. $\square$

KOROLLAR 19.10. *Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann ist der ganze Abschluss von R in S eine R-Unteralgebra von S.*

Beweis. Die Ganzheitsgleichungen $X - r$, $r \in R$, zeigen, dass jedes Element aus R ganz über R ist. Seien $x_1 \in S$ und $x_2 \in S$ ganz über R. Nach der Charakterisierung der Ganzheit gibt es endliche R-Unteralgebren $T_1, T_2 \subseteq S$ mit $x_1 \in T_1$ und $x_2 \in T_2$. Sei $y_1, \ldots, y_n$ ein R-Erzeugendensystem von T_1 und $z_1, \ldots, z_m$ ein R-Erzeugendensystem von T_2. Wir können annehmen, dass $y_1 = z_1 = 1$ ist. Betrachte den endlich erzeugten R-Modul

$$T \,=\, T_1 \cdot T_2 \,=\, \langle y_i z_j,\, i = 1, \ldots, n,\, j = 1, \ldots, m \rangle,$$

der offensichtlich $x_1 + x_2$ und $x_1 x_2$ (und 1) enthält. Dieser R-Modul T ist auch wieder eine R-Algebra, da für zwei beliebige Elemente gilt

$$\Big(\sum r_{ij} y_i z_j\Big) \Big(\sum s_{kl} y_k z_l\Big) \,=\, \sum r_{ij} s_{kl} y_i y_k z_j z_l,$$

und für die Produkte gilt $y_i y_k \in T_1$ und $z_j z_l \in T_2$, so dass diese Linearkombination zu T gehört. Dies zeigt, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Deshalb ist der ganze Abschluss ein Unterring von S, der R enthält. Also liegt eine R-Unteralgebra vor. $\square$

DEFINITION 19.11. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Man nennt R *ganz-abgeschlossen* in S, wenn der ganze Abschluss von R in S gleich R ist.

Abbildungsverzeichnis