Algebraische Kurven
Vorlesung im Wintersemester
2001/2002

Michael Stoll

KAPITEL 1

Einführung

Ein Ziel dieser Vorlesung soll sein, zu erklären, wie man mit Hilfe von algebraischen Kurven über endlichen Körpern Codes konstruieren kann.

Eine algebraische Kurve ist (wie der Name nahelegt) zunächst einmal ein geometrisches Objekt. In der einfachsten Variante als *ebene affine algebraische Kurve* ist die Kurve C definiert durch eine Gleichung

$$F(X, Y) = 0\,,$$

wobei $F \in K[X, Y]$ ein Polynom in zwei Variablen mit Koeffizienten aus dem *Grundkörper* K ist und wir verlangen, dass F nicht konstant ist. Man sagt dann auch genauer, C sei über K definiert oder eine Kurve über K.

So eine Kurve hat *Punkte*, die durch die Lösungen der Gleichung gegeben sind. Genauer ist die Menge der *K-rationalen Punkte auf C* definiert als

$$C(K) = \{(\xi, \eta) \in K^2 \mid F(\xi, \eta) = 0\}\,;$$

allgemeiner setzt man für einen Erweiterungskörper L von K

$$C(L) = \{(\xi, \eta) \in L^2 \mid F(\xi, \eta) = 0\}\,.$$

(Menge der L-rationalen Punkte.)

Im allgemeinen ist eine Kurve nicht durch die Menge ihrer K-rationalen Punkte bestimmt (z.B. hat $X^2+Y^2+1 = 0$ keine reellen ($\mathbb{R}$-rationalen) Punkte, ist aber offensichtlich verschieden von $X^4 + Y^4 + 3 = 0$); das trifft jedoch zu, wenn K algebraisch abgeschlossen ist.

Wie in anderen Gebieten der Mathematik, z.B. der Analysis, wo man sich nicht nur für differenzierbare Mannigfaltigkeiten interessiert, sonder auch für die (differenzierbaren) Funktionen darauf, brauchen wir geeignete Funktionen auf unseren Kurven. Da wir hier Algebra betreiben, haben wir nur die vier Grundrechenarten zur Verfügung. Daher betrachten wir *Polynomfunktionen* und *rationale Funktionen*. Die Funktionen auf C, die durch Polynome beschrieben werden, bilden einen Ring

$$K[C] = K[X, Y]/(F) = K[x, y]\,,$$

den *affinen Koordinatenring* von C (dabei seien x und y die Bilder von X und Y in $K[C]$). Wenn $P = (\xi, \eta) \in L(C)$ ein Punkt auf C ist und $f \in K[C]$ eine Polynomfunktion, dann können wir f in P auswerten (schreibe $f = \phi(x, y)$ mit $\phi \in K[X, Y]$ und setze $f(P) = \phi(\xi, \eta) \in L$; das ist wohldefiniert, da $F(\xi, \eta) = 0$).

Wenn F irreduzibel ist, was wir von jetzt an voraussetzen wollen, dann ist (F) ein Primideal in $K[X, Y]$ und daher $K[C]$ ein Integritätsring. Als solcher besitzt

er einen Quotientenkörper $K(C)$, den *Funktionenkörper* von C. Er ist ein sogenannter algebraischer Funktionenkörper einer Variablen, d.h. er kann geschrieben werden als endliche Erweiterung des rationalen Funktionenkörpers $K(T)$. Umgekehrt ist jeder algebraische Funktionenkörper einer Variablen über einem perfekten Grundkörper K der Funktionenkörper einer ebenen affinen Kurve; die Kurvengleichung ergibt sich aus dem Minimalpolynom eines Erzeugers des Körpers über $K(T)$.

Nun gibt es eine ganze Menge Möglichkeiten, so einen Körper als endliche separable Erweiterung von $K(T)$ zu schreiben — meistens kann man für T ein beliebiges Element $\notin K$ wählen. Dementsprechend erhält man viele ebene affine Kurven. Diese Kurven sind jedoch alle *birational äquivalent*, d.h. es gibt zu einander inverse rationale Abbildungen zwischen ihnen (man kann die Koordinaten eines Punktes auf der einen Kurve rational durch die Koordinaten des entsprechenden Punktes auf der anderen Kurve ausdrücken und umgekehrt). Umgekehrt haben zwei birational äquivalente Kurven isomorphe Funktionenkörper. Das bedeutet: Die birationalen Äquivalenzklassen von algebraischen Kurven sind durch ihre Funktionenkörper klassifiziert.

Da man sich meistens für Kurven nur modulo birationaler Äquivalenz interessiert, kann man also genauso gut den Funktionenkörper betrachten, ein algebraisches statt eines geometrischen Objekts. Dabei stellt sich natürlich die Frage, was denn auf der algebraischen Seite den geometrischen Punkten entspricht.

Dazu müssen wir erst einmal definieren, wann eine rationale Funktion $f \in K(C)$ in einem Punkt $P \in C(L)$ definiert ist. Das ist dann der Fall, wenn wir f als Quotient $f = g/h$ mit $g, h \in K[C]$ schreiben können, so dass $h(P) \neq 0$ ist. In diesem Fall setzen wir natürlich $f(P) = g(P)/h(P) \in L$; das ist wieder wohldefiniert.

Die Menge aller $f \in K(C)$, die in einem gegebenen Punkt $P \in C(K)$ definiert sind, bildet einen Ring $\mathcal{O}_{C,P}$. Die Auswertung in P liefert einen surjektiven Ringhomomorphismus $\mathcal{O}_{C,P} \longrightarrow K$, dessen Kern das maximale Ideal $\mathfrak{m}_P = \{f \in \mathcal{O}_{C,P} \mid f(P) = 0\}$ ist. Dies ist das einzige maximale Ideal von $\mathcal{O}_{C,P}$, denn jedes $f \in \mathcal{O}_{C,P} \setminus \mathfrak{m}_P$ ist in $\mathcal{O}_{C,P}$ invertierbar (denn in diesem Fall gibt es eine Darstellung als Quotient, so dass weder Zähler noch Nenner in P verschwinden) — $\mathcal{O}_{C,P}$ ist ein *lokaler Ring*.

Wenn nun C zusätzlich in P *glatt* ist (das bedeutet, dass nicht beide partielle Ableitungen $\frac{\partial F}{\partial X}$ und $\frac{\partial F}{\partial Y}$ in P verschwinden), dann ist $\mathcal{O}_{C,P}$ sogar ein lokaler Hauptidealring, ein sogenannter *diskreter Bewertungsring*. Das bedeutet, dass es ein Element $t \in \mathcal{O}_{C,P}$ gibt, so dass sich jedes Element $f \in K(C)^\times$ eindeutig schreiben lässt als $f = ut^n$ mit $u \in \mathcal{O}_{C,P}^\times$ und $n \in \mathbb{Z}$. Der Exponent n hängt dabei nicht von der Wahl von t ab, definiert also eine nur von P abhängende surjektive Funktion $v_P : K(C)^\times \longrightarrow \mathbb{Z}$, die folgende Eigenschaften hat.

$$v_P(fg) = v_P(f) + v_P(g)\,, \quad v_P(f+g) \geq \min\{v_P(f), v_P(g)\}\,, \quad v_P|_{K^\times} = 0\,.$$

(Dabei setzt man noch $v_P(0) = \infty > n$ und $\infty + n = \infty$ für alle $n \in \mathbb{Z}$.) $v_P(f)$ lässt sich interpretieren als die Verschwindungsordnung von f in P (bzw. $-v_P(f)$ als die Ordnung des Pols von f in P, falls $v_P(f) < 0$ ist). Eine solche Funktion v heißt *diskrete Bewertung von* $K(C)/K$ und gehört stets zu einem

diskreten Bewertungsring $K \subset R \subset K(C)$; er ist gegeben durch $R = \{f \in K(C) \mid v(f) \geq 0\}$ und hat das maximale Ideal $\mathfrak{m} = \{f \in K(C) \mid v(f) > 0\}$.

Jedem glatten Punkt von C entspricht also eine diskrete Bewertung von $K(C)/K$. Wenn K algebraisch abgeschlossen ist, gilt umgekehrt: Jede diskrete Bewertung voon $K(C)/K$ gehört zu einem glatten Punkt auf einer zu C birational äquivalenten Kurve; bis auf endlich viele diskrete Bewertungen gehören sie alle zu einem glatten Punkt auf C. (Zu Punkten, in denen C nicht glatt ist, können mehrere diskrete Bewertungen gehören; außerdem gibt es diskrete Bewertungen, die keinen Punkten auf C entsprechen; sie gehören zu „Punkten im Undendlichen“ von C.)

Man kann also die Menge der diskreten Bewertungen von $K(C)/K$ als die Menge der glatten Punkte eines idealen Repräsentanten der birationalen Äquivalenzklasse von C auffassen, der sich „lokal“ (d.h. in der Nähe jedes beliebigen Punktes) durch eine ebene affine Kurve realisieren lässt. (Tatsächlich kann man diesen idealen Repräsentanten als glatte projektive Kurve in einem eventuell höherdimensionalen Raum realisieren.) Das ist ein Vorteil des Arbeitens auf der algebraischen Seite — man macht sich von den verschiedenen Modellen der Kurve unabhängig.

Als Beispiel betrachten wir die Gerade, gegeben z.B. durch die Gleichung $Y = 0$. Ihr Funktionenkörper ist $K(X)$, die (affinen) Punkte sind $(a, 0)$ mit $a \in K$. Der zugehörige diskrete Bewertungsring ist $\mathcal{O}_a = \{g/h \mid g, h \in K[X], h(a) \neq 0\}$. Es gibt aber noch einen weiteren diskreten Bewertungsring in $K(X)$, nämlich $\mathcal{O}_\infty = \{g/h \mid g, h \in K[X], h \neq 0, \deg h \geq \deg g\}$ mit zugehöriger Bewertung $v_\infty(g/h) = \deg h - \deg g$. Wenn K algebraisch abgeschlossen ist, dann sind $\mathcal{O}_a$, $a \in K$, und $\mathcal{O}_\infty$ alle diskreten Bewertungsringe $K \subset R \subset K(X)$. Der affinen Geraden fehlt also ein Punkt ∞; er kommt hinzu, wenn man die projektive Gerade betrachtet.

Wir werden daher ab jetzt die diskreten Bewertungen von $K(C)/K$ als die Punkte von C betrachten. Der Körper K sei im Folgenden als algebraisch abgeschlossen vorausgesetzt.

Nun ist es naheliegend zu überlegen, in wie weit es möglich ist, Funktionen in $K(C)$ zu konstruieren, die nur an vorgegebenen Stellen Pole vorgegebener Ordnung haben. Um dafür eine praktische Schreibweise zu haben, führt man die Gruppe der *Divisoren* auf C ein:

$$\mathrm{Div}(C) = \text{freie abelsche Gruppe über den Punkten von } C$$

Ein Divisor hat also die Form $D = \sum_P n_P \cdot P$, wo P die Punkte von C durchläuft und $n_P \in \mathbb{Z}$ ist mit $n_P = 0$ für alle bis auf endlich viele P. Wir schreiben auch $n_P = v_P(D)$. Der *Grad* von D ist definiert als $\deg D = \sum_P n_P \in \mathbb{Z}$; wir haben also einen surjektiven Homomorphismus $\deg : \mathrm{Div}(C) \longrightarrow \mathbb{Z}$. Jeder Funktion $f \in K(C)^\times$ können wir einen Divisor zuordnen,

$$\mathrm{div}(f) = \sum_P v_P(f) \cdot P\,.$$

Dafür gelten die grundlegenden Eigenschaften

$$\mathrm{div}(f) = 0 \iff f \in K^\times \quad \text{und} \quad \deg \mathrm{div}(f) = 0\,.$$

Wenn wir sagen, ein Divisor D sei $\geq D'$, falls die Ungleichung koeffizientenweise gilt, dann lässt sich die Bedingung an eine Funktion, höchstens Pole gewisser Ordnung in gewissen Punkten zu haben, durch eine Ungleichung für Divisoren formulieren. Wir definieren

$$L(D) = \{f \in K(C) \mid \operatorname{div}(f) + D \geq 0\}$$

(dabei gilt $\operatorname{div}(0) + D \geq 0$ per Konvention). Dann ist $L(D)$ ein endlich-dimensionaler K-Vektorraum und besteht aus den Funktionen, deren Polordnung in P höchstens $v_P(D)$ ist.

Nun will man natürlich wissen, wie groß $L(D)$ ist. Die Antwort wird gegeben durch den *Satz von Riemann-Roch*. Er besagt, dass es eine natürliche Zahl $g = g(C)$ gibt und einen Divisor $\kappa \in \operatorname{Div}(C)$, so dass für alle Divisoren D gilt

$$\dim L(D) = \deg D - g + 1 + \dim L(\kappa - D)\,.$$

Aus obigen grundlegenden Eigenschaften folgt außerdem $L(D) = 0$ falls $\deg D < 0$ und $L(0) = K$. Setzt man $D = 0$ im Satz von RR, dann bekommt man $\dim L(\kappa) = g$; setzt man $D = \kappa$, so sieht man $\deg \kappa = 2g - 2$. Also bekommt man das Korollar:

$$\dim L(D) \geq \deg D - g + 1$$

mit Gleichheit, wenn $\deg D \geq 2g + 1$. Es folgt, dass g eindeutig bestimmt ist; g heißt das *Geschlecht* von C. Ein Divisor κ wie oben heißt *kanonischer Divisor*. Hat man zwei kanonische Divisoren κ und κ', dann folgt (mit $D = \kappa'$ bzw. κ), dass $\dim L(\kappa - \kappa') = \dim L(\kappa' - \kappa) = 1$ ist. Daraus ergibt sich, dass $\kappa - \kappa' = \operatorname{div}(f)$ ist für ein $f \in K(C)^\times$ (nämlich jedes $f \neq 0$, so dass $f \in L(\kappa' - \kappa)$). Der kanonische Divisor ist also bis auf „lineare Äquivalenz“ eindeutig bestimmt. Wir werden ihn später als Divisor eines Differenzials auf der Kurve konstruieren.

Der Satz von Riemann-Roch ist ein zentrales Resultat der Theorie. Wir werden ihn in dieser Vorlesung aus Zeitgründen nicht beweisen, sondern versuchen, den Hintergrund zu erklären und Anwendungen zu besprechen.

Als Beispiel betrachten wir wieder die Gerade. Sie hat die Punkte P_a, $a \in K$ und ∞. Wenn wir uns einen Divisor $D = \sum_a n_a \cdot P_a + n_\infty \cdot \infty$ mit $n_a, n_\infty \geq 0$ vorgeben, dann haben wir

$$\begin{aligned} L(D) &= \{\phi/\psi \mid \phi, \psi \in K[X], \psi \text{ teilt } \prod_a (X-a)^{n_a}, \deg \phi \leq \deg \psi + n_\infty\} \\ &= \{\phi/\prod_a (X-a)^{n_a} \mid \deg \phi \leq \deg D\}\,, \end{aligned}$$

also $\dim L(D) = \deg D + 1$. Es folgt, dass die Gerade Geschlecht 0 hat und dass allgemein gilt $\dim L(D) = \max\{0, \deg D + 1\}$. Für κ kann man jeden Divisor vom Grad $-2 = 2g - 2$ nehmen.

Der Satz von Riemann-Roch verhilft uns nun auch dazu, brauchbare Codes zu kontruieren. Dazu betrachten wir eine Kurve über dem endlichen Körper $K = \mathbb{F}_q$. Wir wählen Punkte $P_1, \ldots, P_n \in C(\mathbb{F}_q)$ und einen Divisor D vom Grad N, in dem die Punkte P_j nicht vorkommen. Dann sind die Funktionen in $L(D)$ in den Punkten P_j definiert, und wir haben eine lineare Abbildung

$$\Phi : L(D) \longrightarrow \mathbb{F}_q^n\,, \qquad f \longmapsto (f(P_1), \ldots, f(P_n))\,.$$

Das Bild dieser Abbildung ist ein Code der Länge n. Wenn Φ injektiv ist, dann ist seine Dimension gerade $k = \dim L(D) \geq N-g+1$. Um eine Aussage über den Minimalabstand zu bekommen, überlegen wir, was passiert, wenn wir verlangen, dass f in mindestens $n-\delta$ der Punkte P_j verschwindet, sagen wir in $P_1, \ldots, P_{n-\delta}$. Dann muss $f \in L(D - P_1 - P_2 \cdots - P_{n-\delta})$ sein. Wenn also $n-\delta > N$ ist, dann ist der Grad des obigen Divisors negativ, und es folgt $f = 0$. Insbesondere (mit $\delta = 0$) folgt, dass Φ injektiv ist, solange $N < n$ ist. Das ergibt folgenden Satz:

Sei $0 \leq N < n$. Dann ist $\Phi(L(D))$ ein (n, k, d)-Code mit $k \geq N - g + 1$ und $d \geq n - N$.

Als Beispiel betrachten wir wieder die Gerade über $\mathbb{F}_q$. Als Punkte P_j nehmen wir die Punkte P_a, $a \in \mathbb{F}_q$, als Divisor nehmen wir $D = N \cdot \infty$. Dann haben wir $L(D) = \{f \in \mathbb{F}_q[X] \mid \deg f \leq N\}$, und der Code wird erzeugt von $(a^\nu)_{a \in \mathbb{F}_q}$ für $\nu = 0, 1, \ldots, N$. Dies ist ein $(q+1, N+1, q+1-N)$-Code.

Wenn man aber sehr lange Codes haben will (bei festen Körper $\mathbb{F}_q$), dann muss man Kurven mit hohem Geschlecht betrachten (denn $\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$). Die Codes, die man bekommt, haben die Eigenschaft $k/n + d/n \geq 1 - (g-1)/n$, und n kann maximal die Anzahl der $\mathbb{F}_q$-rationalen Punkte der Kurve sein. Um asymptotisch gute Codes zu bekommen, braucht man also Kurven, die relativ zu ihrem Geschlecht sehr viele rationale Punkte haben.

Aus $\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$ folgt $\limsup N/g \leq 2\sqrt{q}$. Tatsächlich gilt sogar die schärfere Schranke $\limsup N/g \leq \sqrt{q} + 1$. Für Quadrate q (d.h. $q = p^{2m}$) kann man hier sogar Gleichheit beweisen. Damit bekommt man für solche q mit $q \geq 49$ die bisher asymptotisch besten bekannten Codes.

KAPITEL 2

Diskrete Bewertungsringe

Da diskrete Bewertungsringe als Äquivalent der geometrischen Punkte einer Kurve eine große Rolle spielen werden, wollen wir uns zunächst etwas genauer mit ihnen befassen.

Zur Erinnerung: Ein *lokaler Ring* ist ein Ring, der genau ein maximales Ideal besitzt. Ein Ring R ist genau dann lokal mit maximalem Ideal $\mathfrak{m}$, wenn $R^\times = R \setminus \mathfrak{m}$.

DEFINITION 2.1. Ein lokaler Hauptidealring (das soll einschließen, dass der Ring ein Integritätsring ist), der kein Körper ist, heißt *Diskreter Bewertungring* oder kurz *DBR*.

Der folgende Satz charakterisiert diskrete Bewertungsringe durch ein paar andere Eigenschaften.

SATZ 2.2. *Sei R ein Integritätsring, aber kein Körper. Dann sind folgende Eigenschaften äquivalent.*

(1) *R ist ein DBR.*
(2) *R ist lokal und noethersch und das maximale Ideal $\mathfrak{m}$ ist ein Hauptideal.*
(3) *Es gibt $t \in R$, so dass jedes $z \in R \setminus \{0\}$ sich (eindeutig) schreiben lässt als $z = ut^n$ mit $u \in R^\times$ und $n \in \mathbb{N}$.*
(4) *R ist lokal und noethersch mit maximalem Ideal $\mathfrak{m}$ und $\mathfrak{m}/\mathfrak{m}^2$ ist ein eindimensionaler $R/\mathfrak{m}$-Vektorraum.*

BEWEIS: „1 $\Rightarrow$2“: Klar nach Definition.

„2 $\Rightarrow$3“: Sei $\mathfrak{m} = R \cdot t$. Sei $z \in R \setminus \{0\}$. Wir setzen $z_0 = z$ und konstruieren eine (evtl. abbrechende) Folge (z_n) in R wie folgt. Falls $z_n \in R^\times$, dann setzen wir $u = z_n$ und brechen ab. Sonst ist $z_n \in \mathfrak{m}$, also $z_n = z_{n+1}t$, was z_{n+1} definiert. Wenn die Konstruktion abbricht, dann ist offensichtlich $z = ut^n$ wie gewünscht. Es bleibt also zu zeigen, dass die Folge abbricht. Anderenfalls hätten wir aber die echt aufsteigende Kette von Idealen $Rz_0 \subsetneq Rz_1 \subsetneq Rz_2 \subsetneq \dots$ (denn aus $z_{n+1} \in Rz_n = Rz_{n+1}t$ würde $t \in R^\times$ folgen, ein Widerspruch). Das kann aber nicht sein, da R noethersch ist.

Die Eindeutigkeit der Darstellung folgt leicht.

„3 $\Rightarrow$1“: R ist offenbar lokal mit maximalem Ideal $R \cdot t$, da $R \setminus R \cdot t = R^\times$. Bleibt zu zeigen, dass R Hauptidealring ist. Sei also $0 \neq I \subset R$ ein Ideal. Setze $n = \min\{\nu \in \mathbb{N} \mid t^\nu in I\}$. Das ist wohldefiniert, da mit ut^n auch $t^n \in I$ liegt ($u \in R^\times$). Behauptung: $I = Rt^n$. Die Richtung „$\supset$“ ist klar, da $t^n \in I$ nach Definition. Die umgekehrte Richtung folgt wieder aus $ut^n \in I \Rightarrow t^n \in I$.

Für die Äquivalenz von 4 mit den anderen Eigenschaften braucht man das *Lemma von Nakayama*:

LEMMA 2.3. *Sei R ein noetherscher lokaler Ring mit maximalem Ideal $\mathfrak{m}$.*

(1) *Ist M ein endlich erzeugter R-Modul mit $M = \mathfrak{m} \cdot M$, so ist $M = 0$.*
(2) *Sind $N \subset M$ zwei R-Moduln mit M/N endlich erzeugt, dann impliziert $M = N + \mathfrak{m} \cdot M$, dass $M = N$ ist.*

BEWEIS: 1 Sei $M = \sum_{i=1}^{n} Rx_i$ mit n minimal. Falls $n = 0$, folgt $M = 0$, und wir sind fertig. Anderenfalls gilt wegen $M = \mathfrak{m} \cdot M$, dass $x_n = \sum_{i=1}^{n} m_i x_i$ mit $x_i \in \mathfrak{m}$. Also haben wir $(1 - m_n)x_n = \sum_{i=1}^{n-1} m_i x_i$. Da R lokal, ist $1 - m_n$ invertierbar, also folgt $x_n \in \sum_{i=1}^{n-1} Rx_i$, im Widerspruch zur Minimalität von n. Also muss $n = 0$ sein. Zum Beweis von 2 wende man Teil 1 auf den Modul M/N an. □

„2 ⇒4“: Sei $\mathfrak{m} = R \cdot t$. Dann ist $\mathfrak{m}/\mathfrak{m}^2 = (R/\mathfrak{m}) \cdot \bar{t}$, also höchstens eindimensional. Auf der anderen Seite ist $\mathfrak{m}/\mathfrak{m}^2 \neq 0$, das sonst nach dem Lemma von Nakayama $\mathfrak{m} = 0$ wäre; R ist aber kein Körper.

„4 ⇒2“: Nach Voraussetzung gibt es $t \in \mathfrak{m}$, so dass $\mathfrak{m}/\mathfrak{m}^2 = (R/\mathfrak{m}) \cdot \bar{t}$ ist. Das bedeutet $\mathfrak{m} = R \cdot t + \mathfrak{m}^2$. Nach dem Lemma von Nakayama folgt $\mathfrak{m} = R \cdot t$. □

LEMMA 2.4. *Sei R ein DBR mit Quotientenkörper K. Wenn R' ein Ring ist mit $R \subset R' \subset K$, dann ist $R' = R$ oder $R' = K$.*

BEWEIS: Angenommen, $R' \neq R$. Dann gibt es $x \in R' \setminus R$, und $x = ut^{-n}$ mit $u \in R^\times$, $n > 0$. Dann ist aber $t^{-1} = (u^{-1}t^{n-1}) \cdot x \in R'$, also $R' \supset R[t^{-1}] = K$. □

Eine wichtige Klasse von Beispielen erhält man aus folgendem Resultat. Zuvor eine Definition/Erinnerung.

DEFINITION 2.5. Sei R ein Integritätsring mit Quotientenkörper K, und sei $\mathfrak{p} \subset R$ ein Primideal. Dann heißt der Ring

$$R_{\mathfrak{p}} = \left\{ \frac{a}{b} \;\middle|\; a, b \in R, b \notin \mathfrak{p} \right\}$$

die *Lokalisierung* von R nach $\mathfrak{p}$.

$R_{\mathfrak{p}}$ ist ein lokaler Ring mit maximalem Ideal $R_{\mathfrak{p}} \cdot \mathfrak{p}$.

Mit dieser Konstruktion kann man aus Hauptidealringen diskrete Bewertungsringe erzeugen.

PROPOSITION 2.6. *Sei R ein Hauptidealring mit Quotientenkörper K. Dann ist für jedes maximale Ideal $\mathfrak{m} \neq 0$ von R die Lokalisierung $R_{\mathfrak{m}}$ ein DBR. Umgekehrt erhält man auf diese Weise alle DBR, die zwischen R und K liegen.*

BEWEIS: Da $\mathfrak{m} \neq 0$, ist $R_{\mathfrak{m}}$ kein Körper. Außerdem ist $R_{\mathfrak{m}}$ lokal, und das maximale Ideal $R_{\mathfrak{m}} \cdot \mathfrak{m}$ ist ein Hauptideal, da $\mathfrak{m}$ ein Hauptideal ist. Also ist $R_{\mathfrak{m}}$ ein DBR.

Umgekehrt sei $R \subset R' \subset K$ ein DBR mit maximalem Ideal $\mathfrak{m}'$. Sei $\mathfrak{m} = R \cap \mathfrak{m}'$. Dann ist $\mathfrak{m} \neq 0$, da sonst die zu R' gehörende Bewertung auf R und damit auf K trivial wäre. Weiterhin ist $\mathfrak{m}$ ein Primideal (als Urbild des Primideals $\mathfrak{m}'$ unter dem Ringhomomorphismus $R \hookrightarrow R'$), also maximal, da R ein Hauptidealring ist. Es folgt, dass $R_{\mathfrak{m}} \subset R'$, denn die Bewertung der Elemente in $R_{\mathfrak{m}}$ ist ≥ 0. Nach Lemma 2.4 ergibt sich $R' = R_{\mathfrak{m}}$, da $R_{\mathfrak{m}}$ ein DBR und $R' \neq K$ ist. □

Allgemein heißt ein Integritätsring R mit der Eigenschaft, dass für jedes Primideal $\mathfrak{p} \neq 0$ von R die Lokalisierung $R_\mathfrak{p}$ ein DBR ist, ein *Dedekind-Ring*. Beispiele sind der Ring der ganzen Zahlen in einem algebraischen Zahlkörper oder auch der affine Koordinatenring einer glatten ebenen affinen Kurve.

Beispiele 2.7.

(1) **Diskrete Bewertungsringe in $\mathbb{Q}$.** Jeder Ring $R \subset \mathbb{Q}$ enthält $\mathbb{Z}$, und $\mathbb{Z}$ ist ein Hauptidealring. Nach Prop. 2.6 sind die DBR in $\mathbb{Q}$ also gerade gegeben durch

$$\mathbb{Z}_{(p)} = \{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}\,.$$

(2) **Diskrete Bewertungsringe über K in $K(X)$.** Diese kommen in zwei Sorten. Entweder gilt $X \in R$ und damit $K[X] \subset R \subset K(X)$; dann ist

$$R = K[X]_{(f)} = \{a/b \mid a, b \in K[X], f \nmid b\}$$

für ein irreduzibles normiertes Polynom $f \in K[X]$. Falls K algebraisch abgeschlossen ist, dann ist $f = X - \alpha$ für ein $\alpha \in K$, und $f \nmid b$ ist äquivalent zu $f(\alpha) \neq 0$.

Oder $X \notin R$, dann muss $X^{-1} \in \mathfrak{m}$ sein, wo $\mathfrak{m}$ das maximale Ideal von R ist. Daraus folgt dann direkt

$$R = K[X^{-1}]_{(X^{-1})} = \{a/b \mid a, b \in K[X], b \neq 0, \deg(b) \geq \deg(a)\}\,.$$

(3) **Der Potenzreihenring.** Der Ring $K[\![T]\!]$ ist ebenfalls ein DBR, mit maximalem Ideal (T). Er ist wichtig, weil er in gewisser Weise universell ist:

Sei K ein Körper und $K \subset R$ ein DBR mit maximalem Ideal $\mathfrak{m}$, so dass die Komposition $K \hookrightarrow R \twoheadrightarrow R/\mathfrak{m}$ ein Isomorphismus ist. Sei t ein uniformisierendes Element von R. Dann gibt es eine eindeutig bestimmte Einbettung $\phi : R \hookrightarrow K[\![T]\!]$ (als K-Algebren), so dass $\phi(t) = T$.

Zum Beweis überlegt man sich, dass es zu jedem $z \in R$ eine Folge $\lambda_0, \lambda_1, \dots \in K$ gibt mit $z = \lambda_0 + \lambda_1 t + \dots + \lambda_{n-1} t^{n-1} + z_n t^n$ für alle $n \in \mathbb{N}$, wo $z_n \in R$. In der Tat — es gibt $\lambda_0 \in K$ mit $\lambda_0 \equiv z \bmod \mathfrak{m}$ nach Voraussetzung; also ist $z = \lambda_0 + z_1 t$; der Rest folgt mit Induktion. Die Einbettung ϕ ist dann gegeben durch $\phi(z) = \lambda_0 + \lambda_1 T + \dots$.

Dass ϕ injektiv ist, ergibt sich aus $\bigcap_n \mathfrak{m}^n = 0$, was wiederum aus dem Lemma von Nakayama folgt — setze $M = \bigcap_n \mathfrak{m}^n$, dann ist $M = \mathfrak{m} \cdot M$, also $M = 0$.

(4) **Ein lokaler Ring, der kein DBR ist.** Wir betrachten den Punkt $P = (0,0)$ auf der Kurve $C : Y^2 = X^2(X+1)$. Seien x und y die Bilder von X und Y in $K(C)$. Dann ist $z = x/y \notin \mathcal{O}_P$ — die Gleichung $YF(X,Y) = XG(X,Y) + (Y^2 - X^2(X+1))H(X,Y)$ in Polynomen $F, G, H \in K[X,Y]$ impliziert $F(0,0) = 0$ (setze $X = 0$ und teile durch Y), also gibt es keine Darstellung $z = G(x,y)/F(x,y)$ mit $F(0,0) \neq 0$. Ebenso zeigt man, dass $z^{-1} = y/x \notin \mathcal{O}_P$. Damit kann $\mathcal{O}_P$ kein DBR sein. Anschaulich hat C zwei „Äste“ durch P, auf denen z die Werte 1 und -1 annehmen möchte, deswegen kann man z (und ebenso z^{-1}) keinen Wert in P zuordnen. Tatsächlich gibt es zwei DBR oberhalb von $\mathcal{O}_P$, nämlich $\mathcal{O}_P[(z+1)^{-1}]$ und $\mathcal{O}_P[(z-1)^{-1}]$, die gerade diesen beiden Ästen in P entsprechen.

KAPITEL 3

Kurven und Funktionenkörper

Unser Ziel in diesem Kapitel ist es, die „Anti-Äquivalenz“ der Kategorien „Ebene affine Kurven mit rationalen Abbildungen“ und „Algebraische Funktionenkörper einer Variablen“ zu zeigen. Dazu müssen wir erst die relevanten Begriffe einführen.

Zunächst eine kurze Wiederholung einiger Begriffe aus der Einführung. K sei im folgenden ein Körper, den wir ab jetzt als *perfekt* voraussetzen (d.h. K hat Charakteristik 0, oder K hat Charakteristik $p > 0$, und die Abbildung $K \ni x \mapsto x^p \in K$ ist surjektiv. Das ist äquivalent dazu, dass jede endliche Erweiterung von K separabel ist).

Definition 3.1.

(1) Eine *ebene affine algebraische Kurve C über K* (meistens kurz „Kurve (über K)“ genannt) ist gegeben durch ein nicht-konstantes irreduzibles Polynom $F \in K[X, Y]$.
(2) Der *affine Koordinatenring* von C ist
$$K[C] = K[X, Y]/(F) =: K[x, y]\,,$$
wobei wir die Bilder von X und Y in $K[C]$ mit x und y bezeichnen.
(3) Der *Funktionenkörper $K(C)$* von C ist der Quotientenkörper $K(x, y)$ von $K[C]$. (Da F irreduzibel ist, ist (F) ein Primideal in $K[X, Y]$, also ist $K[C]$ ein Integritätsring und besitzt somit einen Quotientenkörper.)
(4) Die Elemente von $K(C)$ heißen *rationale Funktionen* auf C. $\phi \in K(C)$ heißt *konstant*, wenn ϕ über K algebraisch ist. Die Menge der konstanten Funktionen in $K(C)$ ist also der algebraische Abschluss von K in $K(C)$ und heißt der *Konstantenkörper* von $K(C)$.
(5) Ein Paar $(\xi, \eta) \in K^2$ heißt *K-rationaler Punkt* von C, wenn $F(\xi, \eta) = 0$. Die Menge der K-rationalen Punkte von C wird mit $C(K)$ bezeichnet. Analog für L-rationale Punkte, wenn L/K eine Körpererweiterung ist.
(6) $\phi \in K(C)$ heißt *definiert* in $P = (\xi, \eta) \in C(K)$, wenn es $G, H \in K[X, Y]$ gibt mit $\phi = G(x, y)/H(x, y)$ und $H(\xi, \eta) \neq 0$. In diesem Fall setzen wir $\phi(P) = G(\xi, \eta)/H(\xi, \eta) \in K$ (das ist wohldefiniert).
(7) Der *lokale Ring* von C in $P = (\xi, \eta) \in C(K)$ ist definiert durch
$$\mathcal{O}_P = \mathcal{O}_{C,P} = \{\phi \in K(C) \mid \phi \text{ definiert in } P\}\,.$$
Es gilt $\mathcal{O}_P = K[C]_{(x-\xi, y-\eta)}$ (Übung oder später).

Das folgende Lemma impliziert, dass eine rationale Funktion stets in allen Punkten einer Kurve bis auf endlich viele definiert ist.

Lemma 3.2. *Seien $G, H \in K[X, Y]$ teilerfremd. Dann ist die Menge*
$$M(G, H) = \{(\xi, \eta) \in K^2 \mid G(\xi, \eta) = H(\xi, \eta) = 0\}$$

endlich und enthalten in $\bar{K}^2$.

BEWEIS: Die Polynome sind auch in $K(X)[Y]$ teilerfremd, also gibt es $a, b \in K(X)$ mit $aG + bH = 1$. Nach Multiplikation mit einem gemeinsamen Nenner von a und b erhalten wir eine Gleichung $AG + BH = Q \in K[X]$ mit $Q \neq 0$. Es folgt, dass $Q(\xi) = 0$ sein muss für jedes $(\xi, \eta) \in M(G, H)$. Entsprechend gibt es ein Polynom $0 \neq R \in K[Y]$, so dass für jedes Element $(\xi, \eta) \in M(G, H)$ gilt $R(\eta) = 0$. Da Q bzw. R jeweils nur endlich viele Nullstellen haben, folgt die erste Behauptung. Die zweite Behauptung ist klar, da ξ und η Nullstellen eines Polynoms mit Koeffizienten in K sind. □

KOROLLAR 3.3. *Ist $\phi \in K(C)$, dann ist ϕ höchstens in endlich vielen Punkten von C nicht definiert.*

BEWEIS: Sei $\phi = G(x, y)/H(x, y)$ mit $G, H \in K[X, Y]$. Dann ist ϕ höchsten in den (ξ, η) nicht definiert, für die $H(\xi, \eta) = 0$ gilt. Diese Punkte liegen alle in $M(F, H)$, und diese Menge ist endlich, da F und H teilerfremd sind. Anderenfalls wäre F ein Teiler von H (denn F ist irreduzibel) und damit $H(x, y) = 0$ in $K[C]$, also würde ϕ gar nicht existieren. □

Als nächstes definieren wir, was eine rationale Abbildung zwischen zwei Kurven ist.

DEFINITION 3.4. Seien $C : F(X, Y) = 0$ und $D : G(X, Y) = 0$ zwei Kurven über K. Eine *rationale Abbildung* f von C nach D ist ein Paar $(\phi, \psi) \in K(C)^2$ mit $G(\phi, \psi) = 0$. f heißt *definiert* in $P \in K(C)$, falls ϕ und ψ in P definiert sind; dann setzen wir $f(P) = (\phi(P), \psi(P)) \in D(K)$.

f heißt *konstant*, wenn ϕ und ψ konstant sind.

Sind $C_j : F_j(X, Y) = 0$ $(j = 1, 2, 3)$ drei Kurven, und sind $f_1 : C_1 \longrightarrow C_2$ und $f_2 : C_2 \to C_3$ rationale Abbildungen, dann gibt es eine rationale Abbildung $f_2 \circ f_1 : C_1 \longrightarrow C_3$, die man wie folgt erhält. Wir schreiben die Komponenten (ϕ_2, ψ_2) von f_2 als Quotienten $\phi_2 = G_1(x_2, y_2)/H_1(x_2, y_2)$ und $\psi_2 = G_2(x_2, y_2)/H_2(x_2, y_2)$; dann ist

$$f_2 \circ f_1 = (G_1(\phi_1, \psi_1)/H_1(\phi_1, \psi_1), G_2(\phi_1, \psi_1)/H_2(\phi_1, \psi_1)),$$

wenn $f_1 = (\phi_1, \psi_1)$ ist. Es ist leicht zu sehen, dass dies wohldefiniert ist, und dass $(f_2 \circ f_1)(P) = f_2(f_1(P))$ ist, wann immer beide Seiten definiert sind. Außerdem ist diese Verknüpfung assoziativ.

Schließlich gibt es stets die identische rationale Abbildung id_C, die durch (x, y) gegeben ist. Es gilt $\mathrm{id}_C \circ f = f$ und $f \circ \mathrm{id}_C = f$ für alle passenden rationalen Abbildungen f.

Damit erhalten wir eine Kategorie, deren Objekte die ebenen affinen algebraischen Kurven über K sind, mit Morphismen, die durch rationale Abbildungen gegeben sind.

DEFINITION 3.5. Zwei Kurven C und D heißen *birational äquivalent*, wenn es rationale Abbildungen $f : C \to D$ und $g : D \to C$ gibt mit $f \circ g = \mathrm{id}_D$ und $g \circ f = \mathrm{id}_C$.

Wir wollen nun sehen, wie sich rationale Abbildungen in die Sprache der Funktionenkörper übersetzen.

PROPOSITION 3.6. *Seien C und D zwei Kurven über K. Dann haben wir eine Bijektion*

$$\begin{array}{rcl} \textit{nicht-konst. rationale Abb. } C \to D & \longleftrightarrow & K\textit{-Algebra-Homom. } K(D) \to K(C) \\ f = (\phi, \psi) & \longmapsto & (x \mapsto \phi, y \mapsto \psi) \\ (\varphi(x), \varphi(y)) & \longmapsfrom & \varphi \end{array}$$

BEWEIS: Sei D gegeben durch die Gleichung $G(X, Y) = 0$. Wir haben zu zeigen, dass die Abbildungen in beiden Richtungen wohldefiniert und zueinander invers sind. Zunächst zu „$\to$“. Es gibt sicher einen K-Algebra-Homomorphismus $\Phi : K[X, Y] \to K(C)$, der X auf ϕ und Y auf ψ abbildet. Nach Definition von rationalen Abbildungen gilt $G(\phi, \psi) = 0$, also bekommen wir einen wohldefinierten K-Algebra-Homomorphismus $K[D] = K[X, Y]/(G) \to K(C)$. Wir müssen noch zeigen, dass dieser injektiv ist; dann lässt er sich zu einem K-Algebra-Homomorphismus $K(D) \to K(C)$ fortsetzen. Dazu ist äquivalent, dass der Kern von Φ gerade (G) ist. Anderenfalls gäbe es ein zu G teilerfremdes Polynom $H \in K[X, Y]$ mit $H(\psi, \psi) = 0$. Aus dem Beweis von Lemma 3.2 folgt dann aber, dass ψ und ϕ algebraisch über K, also konstant sind, Widerspruch.

Jetzt zur Gegenrichtung „$\leftarrow$“. $\varphi(x)$ und $\varphi(y)$ sind natürlich in $K(C)$; es bleibt zu zeigen, dass $G(\varphi(x), \varphi(y)) = 0$ ist. Das folgt aber sofort aus $G(x, y) = 0$.

Dass $\leftarrow \circ \rightarrow$ die Identität ist, ist klar. Umgekehrt gilt das genauso (ein K-Algebra-Homomorphismus mit Quelle $K(D)$ ist ja durch seine Werte bei x und y festgelegt). □

KOROLLAR 3.7. *Zwei Kurven C und D über K sind genau dann birational äquivalent, wenn ihre Fuktionenkörper $K(C)$ und $K(D)$ isomorph sind (als K-Algebren).*

BEWEIS: Nach der vorstehenden Proposition übersetzt sich ein birationaler Isomorphismus in einen Isomorphismus der Funktionenkörper und umgekehrt. □

Das zeigt, dass man statt birationaler Äquivalenzklassen von Kurven ebenso gut die zugehörigen Funktionenkörper studieren kann. Dabei ist es nützlich, diese Körper rein algebraisch charakterisieren zu können.

DEFINITION 3.8. Ein *Algebraischer Funktionenkörper einer Variablen* über K ist ein Erweiterungskörper $\mathcal{K}/K$, so dass es $x \in \mathcal{K}$ gibt mit x transzendent über K und $\mathcal{K}/K(x)$ endlich und separabel.

BEMERKUNG 3.9. Meistens wird die Forderung nach der Separabilität weggelassen, so dass man eine endlich erzeugte Körpererweiterung vom Transzendenzgrad 1 hat. Für perfekte Körper K sind aber beide Definitionen äquivalent, wie man sich überlegen kann.

SATZ 3.10.

(1) *Sei C eine Kurve über K. Dann ist $K(C)$ ein algebraischer Funktionenkörper einer Variablen über K.*

(2) *Sei umgekehrt $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen. Dann gibt es eine Kurve C/K mit $\mathcal{K} = K(C)$.*

BEWEIS: (1). Sei $K(C) = K(x, y)$ wie üblich. Dann können nicht sowohl x als auch y algebraisch über K sein. Denn sonst müsste F sowohl ein Polynom in $K[X]$ (das Minimalpolynom von x) als auch ein Polynom in $K[Y]$ (das Minimalpolynom von y) teilen; dann wäre F aber konstant. Sei also ohne Einschränkung x/K transzendent. Wenn y/K algebraisch ist, dann ist F ein Polynom in Y alleine, und F ist separabel, da es irreduzibel und K perfekt ist. Damit ist $K(C)$ über $K(x) = K(X)$ separabel, da durch F gegeben.

Wenn y transzendent ist, dann ist wenigstens eine der (endlichen) Erweiterungen $K(C)/K(x)$ und $K(C)/K(y)$ separabel. Denn ist $K(C)/K(x)$ nicht separabel, dann ist $F \in K[X, Y^p]$ (wo p die Charakteristik von K ist), und ist $K(C)/K(y)$ nicht separabel, dann ist $F \in K[X^p, Y]$, Wenn beides eintritt, folgt $F \in K[X^p, Y^p]$, und da K perfekt ist, wäre F eine $p$te Potenz, also nicht irreduzibel.

(2). Sei $x \in \mathcal{K}$ transzendent über K mit $\mathcal{K}/K(x)$ separabel. Dann gibt es nach dem Satz vom Primitiven Element ein $y \in \mathcal{K}$, so dass $\mathcal{K} = K(x, y)$. Sei $F_0 \in K(x)[Y]$ das Minimalpolynom von y über $K(x)$. Wir können F_0 mit dem Hauptnenner der Koeffizienten multiplizieren und erhalten $F \in K[X, Y]$ mit $F(x, y) = 0$ und F irreduzibel. Es folgt $\mathcal{K} = K(C)$, wo C durch $F = 0$ gegeben ist. □

Wir können also sagen, dass die birationalen Äquivalenzklassen von Kurven über K genau den Isomorphieklassen von algebraischen Funktionenkörpern einer Variablen über K entsprechen.

Eine Kurve heißt *rational*, wenn ihr Funktionenkörper isomorph zum rationalen Funktionenkörper einer Variablen ist. Zum Beispiel ist die Gerade $Y = 0$ eine rationale Kurve. Man kann also auch sagen, dass eine Kurve genau dann rational ist, wenn sie birational äquivalent zur Geraden ist. Hier sind noch einige Beispiele für rationale Kurven.

BEISPIELE 3.11.

(1) **Graphen.** Jede Kurve der Form $C : G(X)Y = F(X)$ ist rational, denn $K(C) = K(X)$.
(2) **Der Kreis.** Sei $C : X^2 + Y^2 = 1$. Dann ist $K(C) \cong K(T)$ durch $(x, y) \mapsto (\frac{2T}{1+T^2}, \frac{1-T^2}{1+T^2})$ bzw. $T \mapsto (1 - y)/x$.
    In ähnlicher Weise kann man zeigen, dass jede Kurve, die durch ein Polynom F von (Gesamt-)Grad höchstens 2 gegeben ist und einen rationalen Punkt hat, rational ist.
(3) **Die Neilsche Parabel.** Sei $C : Y^2 = X^3$. Dan ist $K(C) \cong K(T)$ durch $(x, y) \mapsto (T^2, T^3)$ bzw. $T \mapsto y/x$.
(4) **Die Knotenparabel.** Sei $C : Y^2 = X^2(X + 1)$. Dann ist $K(C) \cong K(T)$ durch $(x, y) \mapsto (T^2 - 1, T(T^2 - 1))$ bzw. $T \mapsto y/x$.

Ein weiteres Beispiel zweier Kurven, die birational äquivalent sind, ist wie folgt.

BEISPIEL 3.12. K habe nicht die Charakteristik 2 oder 3, und sei $a \in K^\times$. Dann sind folgende Kurven birational äquivalent:

$$C : X^3 + Y^3 = a\,, \qquad D : Y^2 = X^3 - 432\,a^2\,.$$

Zueinander inverse rationale Abbildungen sind z.B. gegeben durch

$$\left(\frac{12a}{x+y}, \frac{36a(x-y)}{x+y}\right) \quad : \quad C \longrightarrow D \qquad \text{und}$$

$$\left(\frac{36a+y}{6x}, \frac{36a-y}{6x}\right) \quad : \quad D \longrightarrow C\,.$$

KAPITEL 4

Punkte und Diskrete Bewertungsringe

Unser Ziel in diesem Kapitel wird sein, uns zu überlegen, dass die K-rationalen Punkte auf einer glatten Kurve C gerade den diskreten Bewertungsringen R mit $K[C] \subset R \subset K(C)$ und Restklassenkörper K entsprechen. Falls K algebraisch abgeschlossen ist, dann kann die Bedingung an den Restklassenkörper sogar entfallen. Außerdem enthält man eine Bijektion zwischen den diskreten Bewertungsringen wie oben und den maximalen Idealen $\mathfrak{m}$ von $K[C]$ (mit $K[C]/\mathfrak{m} = K$).

1. Glatte Punkte

Dazu müssen wir aber zunächst definieren, wann eine Kurve „glatt“ heißen soll.

DEFINITION 4.1. Sei $C : F(X, Y) = 0$ eine Kurve über K, L/K eine Körpererweiterung und $P \in C(L)$.

(1) C heißt *glatt in* P, falls nicht beide partielle Ableitungen F_X und F_Y in P verschwinden (dabei ist $F_X = \partial F/\partial X$ etc.). Ist das der Fall, dann heißt die durch
$$F_X(P)\,(X - x(P)) + F_Y(P)\,(Y - y(P)) = 0$$
definierte Gerade (über L) die *Tangente* an C in P. Ein Punkt auf C, in dem C nicht glatt ist, heißt *singulärer Punkt* oder *Singularität* von C.
(2) C heißt (schlechthin) *glatt*, wenn C in allen Punkten $P \in C(\bar{K})$ glatt ist.

BEMERKUNG 4.2. Eine Kurve C hat stets nur endlich viele singuläre Punkte (über beliebigen Erweiterungskörpern), und diese sind alle in $C(\bar{K})$.

Zum Beweis bemerken wir zunächst, dass nicht beide partielle Ableitungen (als Polynome) verschwinden können, da F nicht konstant ist. Sei zum Beispiel $F_X \neq 0$. Dann sind F und F_X teilerfremd, da F irreduzibel ist und F_X einen kleineren Grad in X hat als F. Nach Lemma 3.2 folgt dann die Behauptung, da die singularen Punkte gemeinsame Nullstellen von F und F_X sind.

BEISPIELE 4.3.

(1) Die Gerade $aX+bY = c$ ($a, b, c \in K$, $(a, b) \neq (0, 0)$) ist glatt, da $F_X = a$, $F_Y = b$, und wenigstens eine der beiden Ableitungen konstant $\neq 0$ ist.
(2) Der Kreis $X^2+Y^2 = 1$ ist glatt, falls $\mathrm{char}(K) \neq 2$: $F_X = 2X$, $F_Y = 2Y$, und beide verschwinden nur in $(0, 0)$; dieser Punkt liegt aber nicht auf der Kurve.
(3) Die Neilsche Parabel $Y^2 = X^3$ ist singulär in $(0, 0)$.
(4) Das Gleiche gilt für die Knotenparabel $Y^2 = X^2(X + 1)$.

(5) Eine Kurve der Form $Y^2 = G(X)$ ist genau dann glatt, wenn $\mathrm{char}(K) \neq 2$ und G keine mehrfachen Nullstellen hat. (Für $\mathrm{char}(K) \neq 2$ haben wir $\eta^2 = G(\xi)$, $\eta = 0$, $G'(\xi) = 0$, also ist ξ mehrfache Nullstelle von G. In Charakteristik 2 ist jeder Punkt $(\xi, \eta) \in C$ mit $G'(\xi) = 0$ singulär.)

Jetzt werden wir den Zusammenhang zwischen glatten Punkten und diskreten Bewertungsringen erhellen.

PROPOSITION 4.4. *Sei C eine Kurve über K und $P \in C(K)$ ein Punkt.*

(1) $\mathcal{O}_p/\mathfrak{m}_P = K$.
(2) *C ist in P glatt* $\iff \dim_K \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$.
(3) *C ist in P glatt* $\iff$ *$\mathcal{O}_P$ ist diskreter Bewertungsring.*

BEWEIS: (1) Einerseits ist der Restklassenkörper $\mathcal{O}_P/\mathfrak{m}_P$ eine K-Algebra, andererseits ist $\mathcal{O}_P/\mathfrak{m}_P \subset K$, da $\mathfrak{m}_P$ der Kern des K-Algebra-Homomorphismus $\mathcal{O}_P \ni f \mapsto f(P) \in K$ ist. Also $K \subset \mathcal{O}_P/\mathfrak{m}_P \subset K$, und die Behauptung folgt.

(2) Nach einer eventuellen Verschiebung der Koordinaten können wir annehmen, dass $P = (0,0)$ ist. Wir schreiben $F(X,Y) = aX + bY + \dots$. Wenn C in P glatt ist, dann ist $a \neq 0$ oder $b \neq 0$, Sei zum Beispiel $b \neq 0$ (der andere Fall geht genauso). Dann ist $y \equiv -b^{-1}ax \bmod \mathfrak{m}_P^2$, also wird $\mathfrak{m}_P/\mathfrak{m}_P^2$ erzeugt von $x \bmod \mathfrak{m}_P^2$. Nach dem Lemma von Nakayama (Lemma 2.3) ist $\mathfrak{m}_P/\mathfrak{m}_P^2 \neq 0$ (da $\mathfrak{m}_P \neq 0$), also ist $\dim_K \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$.

Sei nun umgekehrt $\dim_K \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$. Der Quotient $\mathfrak{m}_P/\mathfrak{m}_P^2$ wird stets von den Restklassn von x und von y erzeugt. Wir haben also (z.B.) eine Relation $y \equiv \alpha x \bmod \mathfrak{m}_P^2$ mit $\alpha \in K$. Also gibt es Polynome $G, H \in K[X,Y]$ mit $G \in (X,Y)^2$ und $H \in (X,Y)$, so dass $y - \alpha x = G(x,y)/(1+H(x,y))$. Nach Multiplikation mit $1+H(x,y)$ und Reduktion modulo $(x,y)^2$ erhalten wir $Y - \alpha X \in (X,Y)^2 + (F)$. Wäre C in P nicht glatt, dann wäre $F \in (X,Y)^2$, und wir hätten $Y - \alpha X \in (X,Y)^2$, ein offensichtlicher Widerspruch.

(3) Das folgt unmittelbar aus Teil (2) mit Satz 2.2, da $\mathcal{O}_P$ stets lokal und noethersch ist. □

Als nächstes studieren wir die Beziehung zwischen rationalen Punkten und maximalen Idealen des Koordinatenrings.

PROPOSITION 4.5. *Sei C eine Kurve über K.*

(1) *Wir haben eine Bijektion*

$$C(K) \longleftrightarrow \{\mathfrak{m} \mid \mathfrak{m} \subset K[C] \text{ max. Ideal mit } K[C]/\mathfrak{m} = K\},$$

die gegeben ist durch $(\xi, \eta) \mapsto (x - \xi, y - \eta)$.
(2) *Sei $\mathfrak{m} \subset K[C]$ ein maximales Ideal. Dann ist $K[C]/\mathfrak{m}$ eine endliche Körpererweiterung von K.*

BEWEIS: (1) Sei $P = (\xi, \eta) \in C(K)$. Dann ist $\mathfrak{m} = \ker(K[C] \ni f \mapsto f(P) \in K)$ ein maximales Ideal in $K[C]$, denn $K \hookrightarrow K[C]/\mathfrak{m} \subset K$, also ist $K[C]/\mathfrak{m} = K$. Da $x(P) = \xi$, $y(P) = \eta$, sind $x - \xi, y - \eta \in \mathfrak{m}$, also ist $\mathfrak{m} = (x - \xi, y - \eta)$, denn letzteres Ideal ist maximal.

Sei umgekehrt $\mathfrak{m} \subset K[C]$ maximal mit $K[C]/\mathfrak{m} = K$. Seien $\xi, \eta \in K$ die Bilder von $x, y \in K[C]$ unter dem kanonischen Epimorphismus $K[C] \twoheadrightarrow K[C]/\mathfrak{m} = K$.

Dann folgt $F(\xi,\eta)=0$, da bereits $F(x,y)=0$ ist ($F(X,Y)=0$ sei wie üblich die C definierende Gleichung). Also ist $P=(\xi,\eta)\in C(K)$ und $\mathfrak{m}=(x-\xi,y-\eta)$.

(2) Wir nehmen zunächst an, F habe die Form

$$F(X,Y)=Y^n+F_{n-1}(X)Y^{n-1}+\cdots+F_1(X)Y+F_0(X)\,.$$

Dann ist $K[C]$ eine endliche Ringerweiterung von $K[x]=K[X]$, denn y ist ganz über $K[x]$. Sei nun $\mathfrak{m}\subset K[C]$ maximal, dann ist $\mathfrak{m}_0=\mathfrak{m}\cap K[x]$ ebenfalls ein maximales Ideal in $K[x]$ ($\mathfrak{m}_0$ ist jedenfalls ein Primideal; außerdem ist $\mathfrak{m}_0\neq 0$ (das gilt stets in ganzen Ringerweiterungen von Integritätsringen; zum Beweis betrachte $0\neq z\in\mathfrak{m}$, dann ist der konstante Koeffizient im Minimalpolynom von z ein Element $0\neq z_0\in\mathfrak{m}_0$), also ist $\mathfrak{m}_0$ maximal, da der Polynomring ein Hauptidealring ist). Wir wissen, dass $K[x]/\mathfrak{m}_0$ eine endliche Körpererweiterung von K ist. Außerdem ist $K[C]/\mathfrak{m}$ endlich erzeugt als $K[x]$-Modul (da $K[C]$ endlich erzeugt), also ein endlich-dimensionaler Vektorraum über $K[x]/\mathfrak{m}_0$. Insgesamt folgt, dass $K[C]/\mathfrak{m}$ auch endlich über K ist.

Sei nun allgemein

$$F(X,Y)=F_n(X)Y^n+F_{n-1}(X)Y^{n-1}+\cdots+F_0(X)\,.$$

Wir setzen $x=x'-y^{n+1}$; dann ist $K[C]=K[x',y]$, und wir haben $F'(x',y)=0$, wo F' gegeben ist durch

$$F'(X,Y)=F(X+Y^{n+1},Y)=F_n(X+Y^{n+1})Y^n+\cdots+F_0(X+Y^{n+1})\,.$$

Sei k die größte Zahl, so dass F_k maximalen Grad unter den F_j hat; der Grad sei m. Dann hat $F'(X,Y)$ die Form

$$F'(X,Y)=\alpha Y^{m(n+1)+k}+\text{Terme mit niedrigerem Grad in } Y$$

mit $\alpha\in K^\times$. Wir können F' ersetzen durch $\alpha^{-1}F'$; dann sind wir in der anfänglich betrachteten Situation. □

Bemerkung 4.6. Wir haben im Beweis von Teil (2) gezeigt, dass $K[C]$ stets eine endliche Ringerweiterung des Polynomrings ist. — Teil (2) der Proposition ist nichts anderes als der *Hilbertsche Nullstellensatz* für Kurven.

Korollar 4.7. *Sei C eine Kurve über einem algebraisch abgeschlossenen Körper K. Dann stehen die Punkte in $C(K)$ in Bijektion zu den maximalen Idealen von $K[C]$.*

Beweis: Nach Prop. 4.5, (1), müssen wir nur noch zeigen, dass für jedes maximale Ideal $\mathfrak{m}\subset K[C]$ gilt $K[C]/\mathfrak{m}=K$. Nach Prop. 4.5, (2), ist aber $K[C]/\mathfrak{m}$ eine endliche Erweiterung von K. Da K algebraisch abgeschlossen ist, gibt es keine nichttrivialen endlichen Erweiterungen, also ist tatsächlich $K[C]/\mathfrak{m}=K$. □

Wenn C eine glatte Kurve ist, dann können wir beide Beziehungen (glatte Punkte $\leftrightarrow$ Diskrete Bewertungsringe und Punkte $\leftrightarrow$ maximale Ideale) miteinander verbinden. Wir erhalten folgendes Resultat.

Satz 4.8. *Sei C eine glatte Kurve über K.*

(1) *Wir haben eine Bijektion*

$$\begin{aligned} C(K) &\longleftrightarrow \{DBR\ (R,\mathfrak{m}) \mid K[C] \subset R \subset K(C), R/\mathfrak{m} = K\} \\ P &\longmapsto (\mathcal{O}_P, \mathfrak{m}_P) \\ (x \bmod \mathfrak{m}, y \bmod \mathfrak{m}) &\longmapsto (R,\mathfrak{m})\,. \end{aligned}$$

(2) *Wenn K algebraisch abgeschlossen ist, dann haben wir die Bijektion*

$$C(K) \longleftrightarrow \{DBR\ (R,\mathfrak{m}) \mid K[C] \subset R \subset K(C)\}\,.$$

Beweis: (1) Die Abbidung von links nach rechts ist wohldefiniert nach Prop. 4.4. Die Abbildung von rechts nach links ist wohldefiniert, da $F(x,y) = 0$ (wie oben). Es bleibt zu zeigen, dass beide Abbildungen invers zueinander sind. Dass $(\mathcal{O}_P, \mathfrak{m}_P)$ wieder zurück auf $P \in C(K)$ abgebildet wird, ist klar. Sei umgekehrt $(R,\mathfrak{m})$ ein diskreter Bewertungsring wie in der rechten Seite und P der Punkt, auf den R abgebildet wird. Dann gilt $\mathcal{O}_P \subset R$: Sei $f \in \mathcal{O}_P$; wir können f schreiben als $G(x,y)/H(x,y)$, wobei $H(P) \neq 0$. Es folgt $H(x,y) \in R \setminus \mathfrak{m} = R^\times$ (Auswertung in P ist $R \twoheadrightarrow R/\mathfrak{m} = K$), also $f = G(x,y)/H(x,y) \in R$ (beachte, dass $G(x,y), H(x,y) \in K[C] \subset R$). Da $\mathcal{O}_P$ ein DBR mit dem selben Quotientenkörper wie R ist, folgt $\mathcal{O}_P = R$.

(2) Dafür ist nur zu zeigen, dass jeder DBR $K[C] \subset R \subset K(C)$ $R/\mathfrak{m} = K$ erfüllt. Sei dazu $\mathfrak{m}_0 = \mathfrak{m} \cap K[C]$; das ist ein maximales Ideal in $K[C]$ (da Primideal $\neq 0$). Nach Prop.4.5, (2), gehört $\mathfrak{m}_0$ zu einem Punkt $P \in C(K)$. Es folgt $K[C]_{\mathfrak{m}_0} = \mathcal{O}_P \subset R$ und daher wieder $\mathcal{O}_P = R$, so dass sich schließlich $R/\mathfrak{m} = \mathcal{O}_P/\mathfrak{m}_P = K$ ergibt. □

Der folgende Satz, den wir hier nicht beweisen wollen, zeigt, dass man auch umgekehrt jeden geeigneten diskreten Bewertungsring in einem algebraischen Funktionenkörper einer Variablen als lokalen Ring eines glatten Punktes einer Kurve realisieren kann.

Satz 4.9. *Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen und R ein diskreter Bewertungsring mit $K \subset R \subset \mathcal{K}$ und Quotientenkörper $\mathcal{K}$, so dass $R/\mathfrak{m} = K$ ist. Dann gibt es eine Kurve C über K und einen glatten Punkt $P \in C(K)$, so dass $K(C) = \mathcal{K}$ und $R = \mathcal{O}_P$.*

2. Primdivisoren

Man kann also für einen algebraischen Funktionenkörper einer Variablen $\mathcal{K}/K$ die Menge

$$\mathrm{PrD}(\mathcal{K}/K) = \{\mathrm{DBR}\ (R,\mathfrak{m}) \mid K \subset R \subset \mathcal{K}, \mathrm{Quot}(R) = \mathcal{K}\}$$

als die Menge der „Punkte“ einer zugehörigen glatten vollständigen Kurve betrachten, bzw.

$$\mathrm{PrD}(\mathcal{K}/K)(K) = \{(R,\mathfrak{m}) \in \mathrm{PrD}(\mathcal{K}/K) \mid R/\mathfrak{m} = K\}$$

als die Menge der rationalen „Punkte“.

Wir nennen die Elemente von $\mathrm{PrD}(\mathcal{K}/K)$ *Primdivisoren*. Wir werden einen Primdivisor meistens mit P (oder ähnlich) bezeichnen; der zugehörige diskrete Bewertungsring heißt dann $\mathcal{O}_P$, sein maximales Ideal $\mathfrak{m}_P$, der Restklassenkörper $K_P = \mathcal{O}_P/\mathfrak{m}_P$, ein uniformisierendes Element t_P und so weiter.

DEFINITION 4.10. Der *Grad* eines Primdivisors $P \in \mathrm{PrD}(\mathcal{K}/K)$ ist definiert als $\deg P = [K_P : K]$.

Die rationalen Primdivisoren sind also gerade die Primdivisoren vom Grad 1.

Wenn C eine Kurve über K ist, dann schreiben wir statt $\mathrm{PrD}(K(C)/K)$ auch $\mathcal{C}$ (und stellen uns $\mathcal{C}$ gewissermaßen als ein ideales Modell von C vor). Wir haben dann eine Inklusion

$$\{P \in C(K) \mid C \text{ glatt in } P\} \hookrightarrow \mathcal{C}(K)\,,$$

deren Bild nur endlich viele Elemente auslässt (Beweis als Übung). Es ist übrigens tatsächlich möglich, $\mathcal{C}$ als glatte *projektive* (nicht notwendig ebene) Kurve zu realisieren; dann haben alle „Punkte“ eine geometrische Entsprechung.

BEISPIEL 4.11. Sei G die Gerade; dann können wir $\mathcal{G}$ identifizieren mit

$$\{f \in K[x] \mid f \text{ normiert und irreduzibel}\} \cup \{\infty\}\,.$$

DEFINITION 4.12. Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen, $f \in \mathcal{K}$ und $P \in \mathrm{PrD}(\mathcal{K}/K)$.

(1) f heißt *defininiert* in P, falls $f \in \mathcal{O}_P$.
(2) In diesem Fall sei $f(P) \in K_P$ das Bild von f unter dem kanonischen Epimorphismus $\mathcal{O}_P \twoheadrightarrow \mathcal{O}_P/\mathfrak{m}_P = K_P$.

SATZ 4.13. *Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen. Dann gilt für $f \in \mathcal{K}$:*

$$f \textit{ überall definiert} \iff f \textit{ konstant}\,.$$

Anders ausgedrückt,

$$\bigcap_{P \in \mathrm{PrD}(\mathcal{K}/K)} \mathcal{O}_P = \tilde{K}\,.$$

BEWEIS: Wenn f konstant ist, dann ist f offensichtlich überall definiert. Für die umgekehrte Richtung nehmen wir zunächst an, dass $\mathcal{K} = K(x)$. In diesem Fall sieht man die Behauptung leicht direkt — schreibe $f = G(x)/H(x)$ in gekürzter Form; dann ist f nicht definiert in allen Punkten, die Teilern von H entsprechen, also ist $H = 1$ und f ein Polynom. Ein Polynom ist aber nur dann in ∞ definiert, wenn es konstant ist.

Im allgemeinen Fall wählen wir ein $x \in \mathcal{K}$, so dass $\mathcal{K}/K(x)$ endlich separabel ist. Wenn $f \in \mathcal{K}$ überall definiert ist, dann hat das Mininalpolynom von f über $K(x)$ Koeffizienten, die ebenfalls überall (in $K(x)$) definiert sind. Nach dem eben betrachteten Spezialfall sind die Koeffizienten konstant, also ist f algebraisch. □

Dieser wichtige Satz drückt die Vollständigkeit unseres idealen Modells aus — eine nicht-konstante Funktion muss irgendwo Pole haben; sie kann sie nicht im Unendlichen verstecken wie bei affinen Modellen.

3. Primdivisoren und rationale Abbildungen

Wir wollen nun die Situation betrachten, dass wir eine nicht-konstante rationale Abbildung $\phi : C \to D$ zwischen zwei Kurven haben. Wir möchten gerne eine zugehörige Abbildung $\phi : \mathcal{C} \to \mathcal{D}$ definieren und die Struktur ihrer Fasern studieren.

Wir erinnern uns, dass die Angabe einer rationalen Abbildung ϕ wie oben äquivalent ist zur Angabe einer Inklusion $\phi^* : K(D) \hookrightarrow K(C)$. Sei nun $Q \in \mathcal{C}$; dann ist also $\mathcal{O}_Q \subset K(C)$ ein diskreter Bewertungsring mit Quotientenkörper $K(C)$. Wir können den Ring $\mathcal{O}_Q \cap K(D) = (\phi^*)^{-1}(\mathcal{O}_Q)$ betrachten.

Im folgenden setzen wir voraus, dass die Körpererweiterung phi^* separabel ist.

LEMMA 4.14. *$\mathcal{O}_Q \cap K(D)$ ist ein diskreter Bewertungsring mit Quotientenkörper $K(D)$.*

BEWEIS: Sei $R = \mathcal{O}_Q \cap K(D)$. Zunächst ist leicht zu sehen, dass der Quotientenkörper von R gerade $K(D)$ ist: Sei $x \in K(D)$; dann kann man x schreiben als $x = y/z$ mit $y, z \in \mathcal{O}_Q$. Es gibt dann $z' \in \mathcal{O}_Q$, so dass $zz' \in K(D)$ (betrachte das Minimalpolynom von z). Nach Erweitern mit z' können wir also annehmen, dass $y, z \in \mathcal{O}_Q \cap K(D) = R$ sind.

Weiter ist R ein lokaler Ring mit maximalem Ideal $\mathfrak{m} = \mathfrak{m}_Q \cap K(D)$. Denn ist $r \in R \setminus \mathfrak{m} \subset \mathcal{O}_Q \setminus \mathfrak{m}_Q = \mathcal{O}_Q^\times$, dann ist $r^{-1} \in CO_Q \cap K(D) = R$.

Sei nun $w = \min\{v_Q(t) \mid t \in \mathfrak{m}\}$ und $t \in \mathfrak{m}$ mit $v_Q(t) = w$. Sei nun $t' \in \mathfrak{m}$. Dann ist $v_Q(t'/t) \geq 0$, also $t'/t \in \mathcal{O}_Q \cap K(D) = R$. Es folgt $\mathfrak{m} = Rt$, d.h., R ist ein diskreter Bewertungsring. □

Wir können also definieren:

DEFINITION 4.15. Sei $\phi : C \to D$ wie oben. Wir definieren $\phi : \mathcal{C} \to \mathcal{D}$ durch

$$\phi(Q) = P \iff (\phi^*)^{-1}(\mathcal{O}_Q) = \mathcal{O}_P \iff \phi^*(\mathcal{O}_P) \subset \mathcal{O}_Q\,.$$

Beide Bedingungen sind äquivalent, da aus der zweiten folgt $\mathcal{O}_P \subset (\phi^*)^{-1}(\mathcal{O}_Q)$, also Gleichheit wegen der Maximalität von diskreten Bewertungsringen. Nach dem Lemma ist $\phi(Q)$ wohldefiniert.

Folgende Proposition zeigt, dass $\phi : \mathcal{C} \to \mathcal{D}$ mit $\phi : C(K) \to D(K)$ kompatibel ist.

PROPOSITION 4.16. *In der betrachteten Situation gilt für $P \in C(K)$ glatt, dass $\phi(P) \in D(K)$ ebenfalls glatt ist. Außerdem ist $\phi(\tilde{P}) = \widetilde{\phi(P)}$, wenn $\tilde{P}$ den P entsprechenden Punkt in $\mathcal{C}(K)$ bezeichnet (ebenso für $D(K)$).*

BEWEIS: Wird nachgetragen. □

Für das Studium der Fasern von $\phi : \mathcal{C} \to \mathcal{D}$ benötigen wir ein algebraisches Resultat.

SATZ 4.17. *Sei $(R, \mathfrak{m})$ ein diskreter Bewertungsring mit Quotientenkörper K; sei weiter L/K eine endliche separable Körpererweiterung und S der ganze Abschluss von R in L. Dann ist S ein semilokaler Hauptidealring mit Quotientenkörper L.*

Dabei heißt ein Ring *semilokal*, wenn er nur endlich viele maximale Ideale besitzt.

Beweis: Dieser Satz ist im Grunde ein Spezialfall des allgemeineren Resultats, das in der obigen Situation sagt „R Dedekindring $\Longrightarrow$ S Dedekindring“ (vergleiche jedes Buch über ALgebraische Zahlentheorie), zusammen mit der Aussage, dass ein semilokaler Dedekindring ein Hauptidealring ist. (Ein *Dedekindring* ist ein noetherscher Integritätsring, dessen Primideale $\neq 0$ alle maximal sind und dessen Lokalisierung nach jedem maximalen Ideal ein Hauptidealring (also ein diskreter Bewertungsring) ist. Hauptidealringe sind zum Beispiel Dedekindringe.) Der folgende Beweis ist teilweise „selbstgestrickt“ und setzt voraus, dass der Restklassenkörper $R/\mathfrak{m}$ groß genug ist ($\#R/\mathfrak{m} \geq [L:K]$).

In einem ersten Schritt zeigen wir, dass S ein freier R-Modul vom Rang $n = [L:K]$ ist, mit $\dim_{R/\mathfrak{m}} S/\mathfrak{m}S = n$. Die meiste Arbeit steckt dabei im Beweis, dass S als R-Modul endlich erzeugt ist. Für diese Aussage wird nur benötigt, dass R ein noetherscher Integritätsring ist. Sei $b_1, \ldots, b_n$ eine K-Basis von L, bestehend aus Elementen von S (das ist möglich, da $L = S \otimes_R K$ ist, d.h., zu $0 \neq \alpha \in K$ gibt es $0 \neq rinR$ mit $r\alpha \in S$). Sei $\mathrm{Tr} = \mathrm{Tr}_{L/K}$ die Spur und $D = \det(\mathrm{Tr}(b_i b_j))_{i,j=1,\ldots,n}$ die *Diskriminante* der betrachteten Basis. Da L/K separabel ist, ist $D \neq 0$. Außerdem haben wir

$$\sum_{j=1}^{n} Rb_j \subset S \subset D^{-1} \sum_{j=1}^{n} Rb_j \,.$$

Die linke Inklusion ist klar; für die rechte sei $s \in S$; wir schreiben $s = \sum_{j=1}^{n} \sigma_j b_j$ mit $\sigma_j \in K$. Es gilt dann $R \ni \mathrm{Tr}(b_i s) = \sum_{j=1}^{n} \sigma_j \,\mathrm{Tr}(b_i b_j)$, woraus $D\sigma_j \in R$ folgt. Damit ist S ein Untermodul eines endlich erzeugten Moduls über dem noetherschen Ring R, also selbst endlich erzeugt. Da R ein Hauptidealring uns S ein Integritätsring ist, ist S ein torsionsfreier und damit freier R-Modul. Der Rang ist dann gleich der Dimension des K-Vektorraums $L = S \otimes_R K$, also n.

Jetzt zeigen wir, dass S nur endlich viele maximale Ideale hat. Jedes solche Ideal $\mathfrak{M}$ enthält $\mathfrak{m}S$ (denn $\mathfrak{M} \cap R$ ist ein maximales Ideal von R, also gleich $\mathfrak{m}$). Die maximalen Ideale von S entsprechen also den maximalen Idealen von $S/\mathfrak{m}S$; letzteres ist eine endlich-dimensionale $R/\mathfrak{m}$-Algebra. Sind $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$ verschiedene maximale Ideale, dann haben wir nach dem Chinesischen Restsatz einen surjektiven Homomorphismus

$$S/\mathfrak{m}S \twoheadrightarrow S/\bigcap_j \mathfrak{M}_j \xrightarrow{\cong} \prod_j S/\mathfrak{M}_j \,;$$

es folgt $\sum_{j=1}^{k} \dim_{R/\mathfrak{m}} S/\mathfrak{M}_j \leq \dim_{R/\mathfrak{m}} S/\mathfrak{m}S = n$. Insbesondere ist $k \leq n$.

Im letzten Schritt zeigen wir noch, dass S ein Hauptidealring ist. Unser Beweis setzt voraus, dass $\#R/\mathfrak{m} \geq n$ ist; das Resultat ist aber allgemein richtig. Wir zeigen, dass S ein euklidischer Ring ist bezüglich der Normfunktion

$$\nu : S \setminus \{0\} \longrightarrow \mathbb{N} \qquad s \longmapsto v_R(\mathrm{N}_{L/K}(s)) \,.$$

Seien also $a, b \in S$ mit $b \neq 0$; dann ist $\alpha = a/b \in L$. Wenn $\alpha \in S$, dann ist $a = \alpha \cdot b + 0$, und wir sind fertig. Sei also $\alpha \notin S$. Wir zeigen unten, dass es dann ein $c \in S$ gibt, so dass $v_R(\mathrm{N}_{L/K}(\alpha - c)) < 0$. Es folgt dann $a = c \cdot b + (\alpha - c)b$, wobei $r = (\alpha - c)b = a - bc \in S$ ist mit $\nu(r) = \mathrm{N}_{L/K}(\alpha - c) + \nu(b) < \nu(b)$. Damit ist S als euklidisch nachgewiesen.

Es bleibt noch zu zeigen, dass c wie oben angeben existiert. Sei dazu $f(X) = X^n + f_{n-1}X^{n-1} + \cdots + f_0$ das charakteristische Polynom von α über K. Da $\alpha \notin S$, ist wenigstens einer der Koeffizienten nicht in R, d.h., $w = \min\{v_R(f_j) \mid j = 0, \ldots, n-1\} < 0$. Sei nun t ein uniformisierendes Element von R; dann ist

$$\tilde{f}(X) = (t^{-w} f(X)) \bmod \mathfrak{m} \in R/\mathfrak{m}[X] \setminus \{0\}$$

ein Polynom vom Grad $< n$. Da $\#R/\mathfrak{m} \geq n$ nach Voraussetzung, gibt es $\bar{c} \in \mathbb{R}/\mathfrak{m}$ mit $\tilde{f}(\bar{c}) \neq 0$. Sei $c \in R$ ein Lift von $\bar{c}$. Dann hat das konstante Glied von $f(X+c)$ Bewertung $w < 0$; dieser Koeffizient ist aber gerade $\mathrm{N}_{L/K}(\alpha - c)$. □

Satz 4.18. *Die Situation sei wie im vorigen Satz. $t_1, \ldots, t_r$ seien Erzeuger der verschiedenen maximalen Ideale von S. Sei t ein uniformisierendes Element von R. Dann können wir schreiben*

$$t = u t_1^{e_1} \ldots t_r^{e_r}$$

mit $e_j \geq 1$ und $u \in S^\times$. Sei weiter

$$f_j = \dim_{R/Rt} S/St_j\,.$$

Dann gilt

$$n = [L : K] = \sum_{j=1}^{r} e_j f_j\,.$$

Beweis: Da S ein Hauptidealring ist und die t_j ein vollständiges System paarweie nicht-assozierter Primelemente bilden, lässt sich t eindeutig als Produkt in der angegebenen Form schreiben. Die Exponenten e_j sind positiv, da $t \in St_j$.

Wir wissen aus dem Beweis des vorigen Satzes, dass $\dim_{R/Rt} S/St = n$. Nach dem Chinesischen Restsatz ist $S/St \cong \prod_{j=!}^{r} S/St_j^{e_j}$, also gilt $n = \sum_{j=1}^{r} \dim_{R/Rt} S/St_j^{e_j}$.

Weiterhin haben wir folgende exakte Sequenz von R/Rt-Moduln für jedes $e \geq 1$:

$$0 \longrightarrow S/St_j^e \xrightarrow{\cdot t_j} S/St_j^{e+1} \longrightarrow S/St_j \longrightarrow 0\,.$$

Daraus folgt leicht mit Induktion, dass $\dim_{R/Rt} S/St_j^e = e \dim_{R/Rt} S/St_j = ef_j$ ist. Insgesamt ergibt sich die Behauptung. □

Korollar 4.19. *In obiger Situation gilt, dass die diskreten Bewertungsringe $\mathcal{O}$ mit $R \subset \mathcal{O} \subset L$ und $\mathrm{Quot}(\mathcal{O}) = L$ gerade Lokalisierungen $\mathcal{O}_j = S_{\mathfrak{M}_j}$ sind. Wir haben dann $e_j = v_{\mathcal{O}_j}(t)$ und $f_j = \dim_{R/Rt} \mathcal{O}_j/\mathfrak{M}_j\mathcal{O}_j$.*

Beweis: Das folgt aus Prop. 2.6. □

Wir wenden das nun an auf $\phi : \mathcal{C} \to \mathcal{D}$.

Definition 4.20. Sei ϕ wie oben, $Q \in \mathcal{C}$, $P \in \mathcal{D}$ mit $\phi(Q) = P$. Sei t_P ein uniformisierendes Element von $\mathcal{O}_P$. Dann heißt $e_{Q/P} = v_Q(\phi^*(t_P))$ der *Verzweigungsindex* und $f_{Q/P} = \dim_{K_P} K_Q$ der *Restklassengrad* von Q über P.

Wenn $e_{Q/P} > 1$ ist, dann sagen wir, dass ϕ in Q oder über P *verzweigt* ist. Wenn $e_{Q/P} = 1$ ist, dann heißt dementsprechend ϕ in Q *unverzweigt*. ϕ heißt über P unverzweigt, wenn ϕ in allen $Q \in \phi^{-1}(P)$ unverzweigt ist.

Unsere algebraischen Ergebnisse implizieren nun folgende Beschreibung der Faser $\phi^{-1}(P)$. Wir erinnern uns, dass der Grad $\deg \phi$ von ϕ definert ist als $\deg \phi = [K(C) : \phi^*(K(D))]$.

SATZ 4.21. *Sei $\phi : C \to D$ eine separable nicht-konstante rationale Abbildung, und sei $P \in \mathcal{D}$. Dann ist $\phi^{-1}(P) \subset \mathcal{C}$ endlich, und es gilt*

$$\sum_{Q \in \phi^{-1}(P)} e_{Q/P} f_{Q/P} = \deg \phi \,.$$

BEWEIS: Es gilt nach Definition, dass $Q \in \phi^{-1}(P)$ genau dann, wenn $\phi^*(\mathcal{O}_P) \subset \mathcal{O}_Q$. Die Behauptung folgt nun aus Kor. 4.19 und Sart 4.18. □

Das Resultat bleibt auch für nicht notwendig separable rationale Abbildungen richtig. Dazu überlegt man sich zunächst (leicht), dass für Primdivisoren $R \mapsto Q \mapsto P$ unter der Komposition zweier rationaler Abblidungen gilt

$$e_{R/P} = e_{R/Q} e_{Q/P} \quad \text{und} \quad f_{R/P} = f_{R/Q} f_{Q/P} \,.$$

Es genügt dann, den Satz für eine elementare inseparable Erweiterung der Funktionenkörper zu zeigen. Die hat stets die Form $\mathcal{K}^p \subset \mathcal{K}$ (mit $\mathcal{K}^p = \{\alpha^p : \alpha \in \mathcal{K}$, p die Charakteristik von K). Für $Q \mapsto P$ hat man dann $\mathcal{O}_Q = \{\alpha \in \mathcal{K} \mid \alpha^p \in \mathcal{O}_P\}$ und erhält, dass $\phi^{-1}(P)$ nur einen Punkt Q enthält mit $e_{Q/P} = p$, $f_{Q/P} = 1$ (wir verwenden hier, dass K perfekt ist).

Ein wichtiges Resultat in diesem Zusammenhang ist noch, dass eine separable rationale Abbildung nur in endlich vielen Punkten verzweigt ist.

SATZ 4.22. *Sei $\phi : C \to C'$ eine nicht-konstante separable rationale Abbildung. Dann ist ϕ nur in endlich vielen $Q \in \mathcal{C}$ verzweigt.*

BEWEIS: Wir identifizieren im Folgenden $K(C')$ mit seinem Bild unter ϕ^* in $K(C)$. Da $K(C)/K(C')$ nach Voraussetzung separabel ist, gibt es ein primitives Element $y \in K(C)$ (d.h. so dass $K(C) = K(C')(y)$). Sei $F(Y) \in K(C')[Y]$ das Minimalpolynom von y und δ die Diskriminante von F. Wieder wegen der Separabilität ist $\delta \in K(C')^\times$. δ ist außerdem gleich der Diskriminante der $K(C')$-Basis $1, y, \ldots, y^{\deg \phi - 1}$ von $K(C)$.

Wir behaupten nun, dass für alle $P \in \mathcal{C}'$, so dass y ganz ist über $\mathcal{O}_P$ und so dass $\delta \in \mathcal{O}_P^\times$ ist, ϕ über P unverzweigt ist. Daraus folgt die Behauptung, da nur endlich viele P eine der Bedingungen verletzen und die Faser $\phi^{-1}(P)$ endlich ist.

Zum Beweis der Behauptung betrachten wir S, den ganzen Abschluss von $\mathcal{O}_P$ in $K(C)$. Unsere Voraussetzungen implizieren dann, dass $S = \mathcal{O}_P[y]$ ist (denn wir haben $\mathcal{O}_P[y] \subset S \subset \delta^{-1}\mathcal{O}_P[y]$; vergleiche den Beweis von Satz 4.17). Es folgt $S = \mathcal{O}_P[Y]/(F)$ und damit $S/\mathfrak{m}_P S = K_P[Y]/(\bar{F})$, wobei $\bar{F}$ das Bild von F in $K_P[Y]$ ist (Reduktion koeffizientenweise). Wir wissen, dass die maximalen Ideale von S genau den $Q \in \phi^{-1}(P)$ entsprechen; außerdem stehen sie in Bijektion zu den maximalen Idealen des Quotientenrings $S/\mathfrak{m}_P S$. Nach dem Chinesischen Restsatz bekommt man eine Bijektion zwischen diesen maximalen Idealen und den irreduziblen Faktoren von $\bar{F}$: Sei $\bar{F} = \bar{F}_1 \ldots \bar{F}_r$ die Faktorisierung von $\bar{F}$; dann sind die maximalen Ideale von S gegeben durch $\mathfrak{M}_j = (\mathfrak{m}_P, F_j(y))$, wobei $F_j \in \mathcal{O}_P[Y]$ ein Polynom ist, das sich zu $\bar{F}_j$ reduziert. (Die $\bar{F}_j$ sind paarweise verschieden, da $\delta \in \mathcal{O}_P^\times$, also $\bar{\delta} \in K_P^\times$.) Für den Punkt $Q_j \in \mathcal{C}$, der zu $\mathfrak{M}_j$ gehört, hat man dann $f_{Q_j/P} = \deg \bar{F}_j$; damit bekommen wir

$$\deg \phi = \deg F = \sum_j f_{Q_j/P} = \sum_j e_{Q_j/P} f_{Q_j/P} \,,$$

was $e_{Q_j/P} = 1$ impliziert. □

KAPITEL 5

Divisoren und der Satz von Riemann-Roch

Divisoren sind zunächst ein nützliches Mittel, um Nullstellen und Pole rationaler Funktionen zu beschreiben. Formal definieren wir:

DEFINITION 5.1. Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen. Die *Divisorengruppe* von $\mathcal{K}/K$ ist die freie abelsche Gruppe über den Primdivisoren:

$$\mathrm{Div}(\mathcal{K}/K) = \bigoplus_{P \in \mathrm{PrD}(\mathcal{K}/K)} \mathbb{Z} \cdot P$$

Ein *Divisor* ist also eine endliche formale Linearkombination mit ganzzahligen Koeffizienten von Primdivisoren:

$$D = \sum_{P \in \mathrm{PrD}(\mathcal{K}/K)} n_P \cdot P$$

mit $n_P \in \mathbb{Z}$; alle bis auf endlich viele der n_P sind null. Wir schreiben auch $v_P(D) = n_P$.

Ist $\mathcal{K} = K(C)$, dann schreiben wir auch $\mathrm{Div}(C/K)$ für $\mathrm{Div}(K(C)/K)$.

Der Gradhomomorphismus $\deg : \mathrm{Div}(\mathcal{K}/K) \to \mathbb{Z}$ ist induziert von der Gradabbildung $\deg : \mathrm{PrD}(\mathcal{K}/K) \ni P \mapsto \deg P = \dim_K K_P$.

Wir schreiben $D \geq D'$, wenn $v_P(D) \geq v_P(D')$ gilt für alle P.

PROPOSITION 5.2. *Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen und $x \in \mathcal{K}^\times$. Dann hat x nur endlich viele Nullstellen und Pole. Genauer gilt für nicht-konstantes x*

$$\begin{aligned}\sum_{P \in \mathrm{PrD}(\mathcal{K}/K)} \max\{0, v_P(x)\} \deg P &= \sum_{P \in \mathrm{PrD}(\mathcal{K}/K)} \max\{0, -v_P(x)\} \deg P \\ &= [\mathcal{K} : K(x)] = \deg x\,.\end{aligned}$$

Richtig gezählt, gibt es also ebenso viele Nullstellen wie Polstellen.

BEWEIS: Ist x konstant, dann hat es weder Nullstellen noch Pole. Wir können also annehmen, dass x nicht konstant ist; dann ist $[\mathcal{K} : K(x)]$ endlich. Die Inklusion $K(x) \hookrightarrow \mathcal{K}$ kann aufgefasst werden als die zu einer rationalen Abbildung gehörende Inklusion ϕ^*, wobei ϕ eine rationale Abbildung von einer zu $\mathcal{K}$ gehörenden Kurve C auf die Gerade G ist. Für $P \in \mathrm{PrD}(\mathcal{K}/K)$ gilt dann:

$$\begin{aligned}x \text{ hat Nullstelle in } P &\iff \phi(P) = 0 \\ x \text{ hat Polstelle in } P &\iff \phi(P) = \infty\end{aligned}$$

Da $\phi^{-1}(0)$ und $\phi^{-1}(\infty)$ endlich sind, kann x nur endlich viele Null- und Polstellen besitzen. Genauer gilt für Nullstellen P von x, dass $v_P(x) = e_{P/0}$, denn x ist

uniformisierendes Element von $\mathcal{O}_0$. Ebenso gilt für Polstellen P von x, dass $v_P(x) = -e_{P/\infty}$, denn x^{-1} ist uniformisierendes Elment von $\mathcal{O}_\infty$. Daher ist

$$\sum_{P\in \mathrm{PrD}(\mathcal{K}/K)} \max\{0, v_P(x)\} \deg P = \sum_{P:x(P)=0} e_{P/0} f_{P/0} = \deg \phi = [\mathcal{K} : K(x)]\,;$$

ebenso sieht man die Formel für die Polordnungen. □

Aufgrund dieser Proposition ist folgende Definition sinnvoll.

Definition 5.3. Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen und $x \in \mathcal{K}^\times$. Dann ist der *Divisor von* x definiert als

$$\mathrm{div}(x) = \sum_{P\in \mathrm{PrD}(\mathcal{K}/K)} v_P(x) \cdot P \in \mathrm{Div}(\mathcal{K}/K)\,.$$

Es gilt stets $\deg \mathrm{div}(x) = 0$.

Die Operationen, Bilder und Urbilder von Primdivisoren unter rationalen Abbildungen zu nehmen, lassen sich zu Homomorphismen der Divisorengruppen fortsetzen.

Definition 5.4. Seien C und C' zwei Kurven über K. Wie üblich schreiben wir $\mathcal{C} = \mathrm{PrD}(C/K)$ und $\mathcal{C}' = \mathrm{PrD}(C'/K)$. Sei weiter $\phi : C \to C'$ eine nicht konstante rationale Abbildung. Dann definieren wir Homomorphismen (durch ihre Werte auf $\mathcal{C}$ bzw. $\mathcal{C}'$)

$$\begin{aligned} \phi_* &: \mathrm{Div}(C/K) \longrightarrow \mathrm{Div}(C'/K)\,, \quad Q \longmapsto f_{Q/\phi(Q)} \cdot \phi(Q) \\ \phi^* &: \mathrm{Div}(C'/K) \longrightarrow \mathrm{Div}(C/K)\,, \quad P \longmapsto \sum_{Q\in\phi^{-1}(P)} e_{Q/P} \cdot Q \end{aligned}$$

Dass diese Definitionen sinnvoll sind, zeigt folgende Proposition.

Proposition 5.5. *Wir behalten die Situation der vorstehenden Definition bei.*

(1) *Für alle* $D \in \mathrm{Div}(C'/K)$ *gilt* $\phi_*\phi^*(D) = (\deg\phi)D$ *und* $\deg\phi^*(D) = (\deg\phi)\deg D$.
(2) *Für* $f \in K(C')^\times$ *gilt* $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$.
(3) *Für* $f \in K(C)^\times$ *gilt* $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\mathrm{N}_{K(C)/K(C')}(f))$.

Beweis: (1) Es genügt, $D = P \in \mathcal{C}'$ zu betrachten. Dann haben wir $\phi_*\phi^*(P) = \phi_*(\sum_Q e_{Q/P} \cdot Q) = \sum_Q e_{Q/P} f_{Q/P} \cdot P = (\deg\phi) \cdot P$ nach Satz 4.21. Ebenso hat man $\deg\phi^*(P) = \sum_Q e_{Q/P} \deg Q = \sum_Q e_{Q/P} f_{Q/P} \deg P = (\deg\phi)\deg P$.
(2) Nach Definition gilt $v_Q(\phi^*(f)) = e_{Q/P} v_P(f)$, woraus die Behauptung folgt.
(3) Sei t_Q ein uniformisierendes Element für $\mathcal{O}_Q$, $Q \in \mathcal{C}$. Nach dem folgenden Lemma gilt $v_P(\mathrm{N}(t_Q)) = f_{Q/P}$. Daraus folgt die Behauptung. □

Lemma 5.6. *Sei R ein diskreter Bewertungsring mit Quotientenkörper K, L/K eine endliche Körpererweiterung und S ein diskreter Bewertungsring mit Quotientenkörper L, so dass $S \cap K = R$. Sei s ein uniformisierendes Element von S. Dann gilt $v_R(\mathrm{N}_{L/K}(s)) = [S/\mathfrak{m}_S : R/\mathfrak{m}_R]$.*

Beweis: Wird nachgetragen. □

Wenn wir x mit der rationalen Abbildung, die durch Auswerten von x gegeben ist, identifizieren, $x : C \to G$ (G ist die Gerade), dann haben wir einfach $\mathrm{div}(x) = x^*(\mathrm{div}(x_G)) = x^*(0 - \infty)$, was eine Kurzfassung des Beweises von Prop. 5.2 ist.

Die Divisoren von Funktionen, auch *Hauptdivisoren* genannt, spielen eine große Rolle. Sie bilden eine Untergruppe der Divisoren vom Grad 0. Daher kann man die entsprechende Kongruenzrelation betrachten.

DEFINITION 5.7. Sei C/K eine Kurve. Zwei Divisoren $D, D' \in \mathrm{Div}(C/K)$ heißen *linear äquivalent*, $D \sim D'$, wenn es eine Funktion $f \in \mathbb{C}(K)^\times$ gibt, so dass $D' = D + \mathrm{div}(f)$ ist.

Die linearen Äquivalenzklassen bilden eine Gruppe $\mathrm{Pic}(C/K)$, die *Picardgruppe* von C/K. Es gilt $\mathrm{Pic}(C/K) = \mathrm{Div}(C/K)/\{\mathrm{div}(f) : f \in \mathcal{K}^\times\}$.

Die Picardgruppe ist analog zur Idealklassengruppe eines algebraischen Zahlkörpers gebildet.

Nun werden wir unsere Divisoren benutzen, um Bedingungen an die (Null- und) Polstellen rationaler Funktionen zu stellen.

DEFINITION 5.8. Sei C/K eine Kurve und $D \in \mathrm{Div}(C/K)$ ein Divisor. Dann setzen wir

$$L(D) = \{f \in C(K)^\times \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

Um künftige Formulierungen zu vereinfachen, vereinbaren wir, dass die Aussage „$\mathrm{div}(0) + D \geq 0$“ stets wahr sein soll (obwohl sie eigentlich gar nicht sinnvoll ist; der Gedanke dabei ist, dass 0 in jedem Punkt eine Nullstelle beliebig großer Ordnung hat).

Wenn $D \geq 0$, also *effektiv* ist, dann sagt die Bedingung für $f \in L(D)$, dass f Pole höchstens in den Punkten haben darf, die in D vorkommen, und die Polordnung darf höchstens so groß sein wie der Koeffizient des jeweiligen Punktes.

SATZ 5.9. *$L(D)$ ist ein endlich-dimensionaler K-Vektorraum.*

BEWEIS: Es gilt $L(0) = \tilde{K}$, der Konstantenkörper, also gilt die Behauptung für $D = 0$. Wir zeigen nun für $D \in \mathrm{Div}(C/K)$ und $P \in \mathrm{PrD}(C/K)$, dass $L(D)$ endlich-dimensional ist genau dann, wenn $L(D + P)$ endlich-dimensional ist. Daraus folgt die Behauptung durch Induktion (etwa über die Summe der Absolutbeträge der Koeffizienten von D).

Wir haben eine exakte Sequenz

$$0 \longrightarrow L(D) \longrightarrow L(D + P) \longrightarrow K_P\,,$$

wobei die Abbildung $L(D) \to L(D+P)$ die Inklusion ist; die rechte Abbildung ist gegeben durch $f \mapsto (t_P^{-v_P(D+P)})(P)$, dabei ist t_P ein uniformisierendes Element bei P. Die Behauptung folgt, denn es gilt

$$\dim_K L(D) \leq \dim_K L(D + P) \leq \dim_K L(D) + \deg P\,.$$

□

Wenn man einen endlich-dimensionalen Vektorraum gefunden hat, stellt sich natürlich sofort die Frage nach der Dimension. Diese Frage wird durch den Satz

von Riemann-Roch beantwortet. Zuvor wollen wir uns jedoch noch ein paar einfache Beispiele ansehen.

Im Folgenden nehmen wir der Einfachheit halber an, dass $K = \tilde{K}$ ist, also dass K in $K(C)$ algebraisch abgeschlossen ist. (Sollte das nicht der Fall sein, ersetze man K durch $\tilde{K}$.)

LEMMA 5.10. *Sei wie stets C/K eine Kurve, und sei $D \in \mathrm{Div}(C/K)$.*

(1) $\deg D < 0 \Longrightarrow L(D) = 0$.
(2) *Sind D und D' linear äquivalent, so ist $L(D) \cong L(D')$.*
(3) *$L(D) \neq 0$ genau dann, wenn es einen zu D linear äquivalenten Divisor $D' \geq 0$ gibt.*
(4) *Wenn $\deg D = 0$ ist, dann ist $L(D) \neq 0$ genau dann, wenn D ein Hauptdivisor ist.*

BEWEIS: (1) Wäre $0 \neq f \in L(D)$, dann folgte $0 \leq \deg(\mathrm{div}(f) + D) = \deg D$.
(2) Sei $D' = D + \mathrm{div}(z)$. Dann ist ein Isomorphismus $L(D) \to L(D')$ gegeben durch $f \mapsto fz^{-1}$.
(3) Das folgt unmittelbar aus der Definition.
(4) Nach (3) muss D linear äquivalent zu 0 sein. □

Der Beweis von Satz 5.9 lässt vermuten, dass die Dimension von $L(D)$ etwa wie der Grad von D wächst. Dies ist tatsächlich der Fall, wie der Satz von Riemann-Roch zeigt.

SATZ 5.11 (Riemann-Roch). *Sei C/K eine Kurve. Dann gibt es eine ganze Zahl g und einen Divisor $W \in \mathrm{Div}(C/K)$, so dass für alle Divisoren $D \in \mathrm{Div}(C/K)$*

$$\dim_K L(D) = \deg D + 1 - g + \dim_K(W - D)\,.$$

Wir werden diesen wichtigen Satz hier nicht beweisen (Beweise sind in den einschlägigen Büchern zu finden), sondern uns auf Folgerungen daraus beschränken. Ein Divisor W wie im Satz heißt *kanonischer Divisor*.

PROPOSITION 5.12.

(1) *Die Zahl g ist nichtnegativ und eindeutig bestimmt.*
(2) *Der Divisor W ist bis auf lineare Äquivalenz eindeutig bestimmt.*
(3) *Es gilt $\dim_K L(W) = g$ und $\deg W = 2g - 2$.*

BEWEIS: (1) Für $\deg D > \deg W$ folgt $g = \deg D + 1 - \dim L(D)$, also ist g eindeutig bestimmt. Für $g \geq 0$ siehe Teil (3).
(3) Durch Einsetzen von $D = 0$ in den Satz von Riemann-Roch ergibt sich $\dim L(W) = g$. Es folgt $g \geq 0$. Wenn man nun $D = W$ einsetzt, bekommt man $\deg W = 2g - 2$.
(2) Sei W' ein weiterer kanonischer Divisor. Durch Einsetzen von $D = W'$ erhält man $\dim L(W - W') = 1$; außerdem $\deg(W - W') = 0$. Nach Lemma 5.10, Teil (4), folgt $W \sim W'$. □

Wir werden im nächsten Kapitel eine schöne Interpretation der *kanonischen Klasse* (lineare Äquivalenzklasse der kanonischen Divisoren) kennen lernen.

Jetzt wollen wir aber erst einmal sehen, wozu sich der Satz von Riemann-Roch verwenden lässt.

PROPOSITION 5.13. *Eine Kurve C über K ist genau dann rational (d.h., $K(C) \cong K(x)$), wenn sie Geschlecht null hat und einen K-rationalen Punkt besitzt.*

BEWEIS: Wenn die Kurve rational ist, dann hat sie offenbar rationale Punkte, und das Geschlecht ist null. Sei umgekehrt $g(C) = 0$ und $P \in \mathcal{C}(K)$ (oder $C(K)$). Nach dem Satz von Riemann-Roch ist $\dim L(P) = 2$, also gibt es eine nicht konstante Funktion $x \in L(P)$; dann ist aber $\deg x = \deg \operatorname{div}(x)_\infty = \deg P = 1$, also $K(C) = K(x)$. □

Was kann man über Kurven vom Geschlecht null sagen, wenn man nicht weiß, ob sie einen rationalen Punkt haben?

PROPOSITION 5.14. *Eine Kurve C vom Geschlecht null ist stets birational äquivalent zu einer Quadrik (d.h. einer Kurve, die durch ein Polynom vom Grad 2 definiert ist).*

BEWEIS: Sei W ein kanonischer Divisor, dann gilt $\deg(-W) = 2$, also ist $\dim L(-W) = 3$. Es gibt Funktionen $x, y \in L(-W)$, so dass $1, x, y$ eine Basis von $L(-W)$ ist. Weiter ist $\dim L(-2W) = 5$, aber wir haben sechs Elemente $1, x, y, x^2, xy, y^2 \in L(-2W)$. Es muss also ein Polynom F vom Grad 2 geben mit $F(x, y) = 0$. Es bleibt zu zeigen, dass $K(C) = K(x, y)$ ist. Es gilt $\deg x, \deg y \leq 2$, also sind $K(x), K(y)$ Unterkörper von $K(C)$ vom Grad ≤ 2. Wenn einer der beiden Grade schon 1 ist, sind wir fertig. Anderenfalls sind $K(x)$ und $K(y)$ verschieden (sonst wäre $y = a + bx$, da beide die gleichen Pole haben; $1, x, y$ sind aber linear unabhängig). Es folgt $K(x) \subsetneq K(x, y) \subset K(C)$ und damit $K(C) = K(x, y)$. □

Wie sieht es aus mit Kurven vom Geschlecht 1?

PROPOSITION 5.15. *Sei C/K eine Kurve vom Geschlecht 1 und $P \in \mathcal{C}(K)$ ein K-rationaler Punkt. Dann ist C birational äquivalent zu einer Kurve der Form*

$$E : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6 ,$$

wobei P dem Punkt im Unendlichen von E entspricht.

BEWEIS: Wir betrachten Vielfache von P. Nach dem Satz von Riemann-Roch gilt $\dim L(2P) = 2$, $\dim L(3P) = 3$, $\dim L(6P) = 6$. Sei $1, x$ eine Basis von $L(2P)$ und $y \in L(3P)$, so dass $1, x, y$ eine Basis von $L(3P)$ ist. Wir haben $\deg x = 2$ und $\deg y = 3$. Die sieben Elemente $1, x, y, x^2, xy, x^3, y^2 \in L(6P)$ müssen linear abhängig sein; also gibt es ein Polynom

$$F = Y^2 + a_1 XY + a_3 Y - a_0 X^3 - a_2 X^2 - a_4 X - a_6 \in K[X, Y]$$

mit $F(x, y) = 0$ und $a_0 \neq 0$. (Die Koeffizienten von Y^2 und X^3 müssen beide von 0 verschieden sein, da sonst alle Terme verschiedene Bewertung bei P hätten.) Wir können x und y ersetzen durch $a_0 x$ und $a_0^2 y$; dann bekommen wir $a_0 = 1$ in der neuen Gleichung. Wegen $[K(C) : K(x)] = 2$ und $[K(C) : K(y)] = 3$ folgt $K(C) = K(x, y)$. Der Punkt P wird auf den Punkt im Unendlichen von E abgebildet, da x und y in P Pole haben. □

Eine Kurve E wie oben heißt *Elliptische Kurve* (vergleiche meine Vorlesungen dazu). Das Besondere an elliptischen Kurven ist, dass ihre (rationalen) Punkte in natürlicher Weise eine Gruppe bilden. Das lässt sich mit dem Satz von Riemann-Roch recht einfach beweisen: Seien $P, Q \in \mathcal{E}(K)$, und sei $O \in \mathcal{E}(K)$ der Punkt

im Unendlichen. Nach dem Satz von Riemann-Roch ist $\dim L(P+Q-O)=1$, also gibt es genau einen effektiven Divisor, der linear äquivalent zu $P+Q-O$ ist; dieser Divisor hat Grad 1, ist also ein Punkt $R \in \mathcal{E}(K)$. Man setzt $R = P+Q$ und zeigt dann leicht, dass $\mathcal{E}(K)$ mit dieser Addition eine abelsche Gruppe bildet.

Kurven vom Geschlecht 1 ohne rationale Punkte können recht kompliziert sein. Die folgenden Aussagen seien als Übungsaufgaben empfohlen.

ÜBUNGSAUFGABEN 5.1.

(1) Sei C/K eine Kurve vom Geschlecht 1 mit einem Punkt $P \in \mathcal{C}$ vom Grad 2, und sei $\mathrm{char}(K) \neq 2$. Dann ist C birational äquivalent zu einer Kurve, gegeben durch eine Gleichung der Form
$$Y^2 = a\,X^4 + b\,X^3 + c\,X^2 + d\,X + e\,.$$
(2) Sei C/K eine Kurve vom Geschlecht 1 mit einem Punkt $P \in \mathcal{C}$ vom Grad 3. Dann ist C birational äquivalent zu einer Kurve, gegeben durch ein Polynom vom (Gesamt-)Grad 3.

Für Kurven vom Geschlecht 2 sieht es wieder etwas besser aus.

PROPOSITION 5.16. *Sei* $\mathrm{char}(K) \neq 2$ *und* C/K *eine Kurve vom Geschlecht* 2. *Dann ist* C *birational äquivalent zu einer Kurve der Form*
$$Y^2 = f_6\,X^6 + f_5\,X^5 + f_4\,X^4 + f_3\,X^3 + f_2\,X^2 + f_1\,X + f_0 = F(X)\,,$$
wobei $\deg F \geq 5$ *und* F *quadratfrei ist.*

BEWEIS: Sei W ein kanonischer Divisor; dann ist $\deg W = 2$ und $\dim L(W) = 2$. Es gibt also eine Funktion x, so dass $1, x$ eine Basis von $L(W)$ ist. Weiter ist $\dim L(3W) = 5$; sei y eine Funktion, so dass $1, x, x^2, x^3, y$ eine Basis von $L(3W)$ ist. Es gilt $\dim L(6W) = 11$, und in diesem Raum haben wir die 12 Elemente $1, x, \ldots, x^6, y, xy, x^2y, x^3y, y^2$, die also einer Relation genügen müssen. Der Koeffizient von y^2 darin kann nicht verschwinden, denn sonst wäre $y \in K(x)$, was nicht der Fall ist (denn y hat die selben Pole wie x^3, ist aber von $1, x, x^2, x^3$ linear unabhängig). Wenn wir y durch $y - H(x)$ ersetzen, wobei H ein Polynom vom Grad ≤ 3 ist, dann bekommen wir eine Gleichung der Form $y^2 = F(x)$ (das geht, wenn $\mathrm{char}(K) \neq 2$ ist). Wie schon früher haben wir $[K(C) : K(x)] = 2$ und $y \notin K(x)$, also ist $K(C) = K(x, y)$. Wäre F nicht quadratfrei oder $\deg F \leq 4$, dann bekäme man eine Gleichung $z^2 = G(x)$ mit $\deg G \leq 4$, woraus folgen würde, dass $z \in L(2W) = \langle 1, x, x^2 \rangle$ ist, also insbesondere $z \in K(x)$. Nun ist aber $z = y/(ax+b) \notin K(x)$, also ist diese Gleichung kleineren Grades nicht möglich. □

KAPITEL 6

Differenziale und der Satz von Riemann-Hurwitz

Wir haben gesehen, dass der kanonische Divisor W im Satz von Riemann-Roch bis auf lineare Äquivalenz eindeutig bestimmt ist. Das wirft die Frage auf, ob sich diese bedeutsame lineare Äquivalenzklasse auch direkter beschreiben lässt. Die Antwort ist Ja und wird gegeben durch die Differenziale auf der Kurve.

Um diese Differenziale einzuführen, brauchen wir ein wenig Algebra.

DEFINITION 6.1. Sei A eine K-Algebra und M ein A-Modul. Eine *K-Derivation* von A nach M ist eine K-lineare Abbildung $\delta : A \to M$, so dass $\delta(xy) = x\delta(y) + y\delta(x)$.

BEISPIEL 6.2. (Formale) Differenziation definiert eine K-Derivation $K[X] \to K[X]$ und auch $K(X) \to K(X)$.

DEFINITION 6.3. Sei A eine K-Algebra. Ein Paar (Ω, d), bestehend aus einem A-Modul Ω und einer K-Derivation $d : A \to \Omega$ heißt *universelle* K-Derivation von A, wenn es zu jeder K-Derivation $\delta : A \to M$ eine A-lineare Abbildung $\phi : \Omega \to M$ gibt, so dass $\delta = \phi \circ d$ ist. Ω heißt dann auch *Differnzialmodul* von A; seine Elemente heißen *K-Differenziale* von A.

Es ist klar, dass (Ω, d) (wenn existent) bis auf eindeutigen Isomorphismus bestimmt ist. Wir schreiben daher auch $\Omega_{A/K}$ für ein solches Ω. Die Existenz bekommt man leicht durch „brutale Gewalt“ — man nimmt den freien A-Modul über einer K-Basis von A (oder sogar über A selbst) und teilt alle geforderten Relationen heraus. Eine etwas elegantere Konstruktion ist wie folgt. Man setzt $\Omega_{A/K} = \ker(\mu : A \otimes_K A \to A)$, wo μ die Multiplikation ist ($\mu(a \otimes b) = ab$); dann ist $da = (1 \otimes a) - (a \otimes 1)$. Auf diese Weise bekommt man $\Omega_{A/K}$ nicht als Quotient, sondern als Untermodul von $A \otimes_K A$.

Es stellt sich nun die Frage nach der Struktur des A-Moduls $\Omega_{A/K}$.

BEISPIELE 6.4.

(1) Sei $A = K[X]$ der Polynomring. Dann ist $\Omega_{K[X]/K} = K[X] \cdot dX$, und $d(X^n) = nX^{n-1}\,dX$. Letztere Formel folgt aus den Eigenschaften einer K-Derivation. Man prüft leicht nach, dass die universelle Eigenschaft erfüllt ist.
(2) Sei A ein Integritätsring und $\mathcal{K}$ der Quotientenkörper von A. Dann ist $\Omega_{\mathcal{K}/K} = \mathcal{K} \otimes_A \Omega_{A/K}$. Denn wir müssen $d(a/b) = b^{-2}\,(b\,da - a\,db)$ haben, und das so fortgesetzte d ist immer noch eine K-Derivation.
(3) Sei $K \subset \mathcal{K}$ ein Körper und $\mathcal{L}/\mathcal{K}$ eine endliche separable Körpererweiterung. Dann ist $\Omega_{\mathcal{L}/K} = \mathcal{L} \otimes_{\mathcal{K}} \Omega_{\mathcal{K}/K}$. Denn sei $\alpha \in \mathcal{L}$ mit Minimalpolynom F über $\mathcal{K}$. Sei F_d das Polynom mit Koeffizienten in $\Omega_{\mathcal{K}/K}$, das aus F entsteht, indem man d auf die Koeffizienten anwendet. Aus $F(\alpha) = 0$

folgt $F'(\alpha)\,d\alpha + F_d(\alpha) = 0$, also muss $d\alpha = -F_d(\alpha)/F'(\alpha)$ sein. Dieser Ausdruck ist wohldefiniert, da F keine mehrfachen Nullstellen hat. Man prüft nach, dass das so fortgesetzte d eine universelle K-Derivation von $\mathcal{L}$ ist.

SATZ 6.5. *Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen. Dann ist $\Omega_{\mathcal{K}/K}$ ein eindimensionaler $\mathcal{K}$-Vektorraum.*

BEWEIS: Sei $x \in \mathcal{K}$, so dass $\mathcal{K}/K(x)$ endlich separabel ist. Nach Beispielen 6.4 ist dann

$$\Omega_{\mathcal{K}/K} = \mathcal{K} \otimes_{K(x)} (K(x) \otimes_{K[x]} K[x]\,dx) = \mathcal{K}\,dx\,.$$

□

Insbesondere sehen wir, dass für $x \in \mathcal{K}$ separierend (d.h., so dass $\mathcal{K}/K(x)$ endlich separabel ist) gilt, dass $dx \neq 0$ ist. Die Umkehrung gilt ebenfalls, denn wenn $\mathcal{K}/K(x)$ nicht endlich ist, so ist $x \in \tilde{K}$, und man sieht leicht $dx = 0$. Wenn $\mathcal{K}/K(x)$ endlich, aber nicht separabel ist, dann ist $x = y^p$ mit einem $y \in \mathcal{K}$ und daher $dx = py^{p-1}\,dy = 0$.

Wir werden nun zeigen, dass jedes uniformisierende Element eines Ringes $\mathcal{O}_P$ separierend ist. Dazu brauchen wir etwas Vorbereitung.

LEMMA 6.6. *Der algebraische Abschluss von $K(T)$ in $K(\!(T)\!)$ ist separabel.*

BEWEIS: Wir haben zu zeigen, dass jede über $K(T)$ algebraische Laurentreihe $x \in K(\!(T)\!)$ über $K(T)$ separabel ist. Sei dazu $Q(T,X) \in K(T)[X]$ das Minimalpolynom von x, und sei $n = \deg Q$. Sei weiter p die Charakteristik von K; wir können $p \neq 0$ annehmen, da die Behauptung sonst klar ist. Wir schreiben

$$Q(T,X) = Q_0(T^p,X) + T\,Q_1(T^p,X) + \cdots + T^{p-1}\,Q_{p-1}(T^p,X)$$

mit Polynomen $Q_j(T^p,X) \in K(T^p)[X]$; das geht, weil $1, T, \ldots, T^{p-1}$ eine $K(T^p)$-Basis von $K(T)$ ist. Es gilt dann $Q_0(T^p,X) = X^n +$ Terme niedrigeren Grades in X und $\deg Q_j \leq n-1$ für $j \geq 1$. Wenn nun x nicht separabel über $K(T)$ wäre, dann wäre $Q(T,X) = \tilde{Q}(T,X^p)$ mit einem Polynom $\tilde{Q} \in K(T)[X]$. Entsprechend ist dann $Q_j(T^p,X) = \tilde{Q}_j(T^p,X^p)$. Nun ist $x^p \in K(\!(T^p)\!)$, also

$$0 = Q(T,x) = \tilde{Q}(T,x^p) = \sum_{j=0}^{p-1} \tilde{Q}_j(T^p,x^p)T^j\,.$$

Da $\tilde{Q}_j(T^p,x^p) \in K(\!(T^p)\!)$ und $1, T, \ldots, T^{p-1}$ auch eine $K(\!(T^p)\!)$-Basis von $K(\!(T)\!)$ ist, folgt daraus $\tilde{Q}_0(T^p,x^p) = 0$. Da K perfekt ist, gibt es ein Polynom $\bar{Q} \in K(T)[X]$ mit $\tilde{Q}_0(T^p,X^p) = \bar{Q}(T,X)^p$. Es folgt $\bar{Q}(T,x) = 0$, aber $\deg \bar{Q} = n/p < \deg Q$, im Widerspruch dazu, dass Q das Minimalpolynom von x ist. Daher muss x doch separabel sein. □

PROPOSITION 6.7. *Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen, $P \in \mathrm{PrD}(\mathcal{K}/K)$ und t_P ein uniformisierendes Element von $\mathcal{O}_P$. Dann ist t_P separierend, d.h. $\mathcal{K}/K(t_P)$ ist endlich separabel. Insbesondere ist $dt \neq 0$.*

BEWEIS: t_P ist transzendent über K, also ist $\mathcal{K}/K(t_P)$ endlich. In Beispiel 2.7, (3), hatten wir gesehen, dass $\mathcal{O}_P \hookrightarrow K[\![T]\!]$ durch $t_P \mapsto T$. Daher können wir $\mathcal{K}$ als Quotientenkörper von $\mathcal{O}_P$ einbetten in $K(\!(T)\!)$. Da $\mathcal{K}/K(t_P)$ algebraisch ist,

ist das Bild von $\mathcal{K}$ in $K(\!(T)\!)$ ebenfalls algebraisch über $K(T)$. Nach dem vorigen Lemma ist $\mathcal{K}$ also separabel über $K(t_P)$. □

Daraus ergibt sich nun unmittelbar:

KOROLLAR 6.8. *Sei $\mathcal{K}/K$ ein algebraischer Funktionenkörper einer Variablen, $P \in \mathrm{PrD}(\mathcal{K}/K)$ und t_P ein uniformisierendes Element von $\mathcal{O}_P$. Dann gibt es zu jedem Differenzial $\omega \in \Omega_{\mathcal{K}/K}$ ein eindeutig bestimmtes $f \in \mathcal{K}$, so dass $\omega = f\,dt_P$.*

DEFINITION 6.9. In dieser Situation setzen wir $v_P(\omega) = v_P(f)$.

Dies ist wohldefiniert: Sei t' ein weiteres uniformisierendes Element; dann ist $t_P = ut'$ mit $u \in \mathcal{O}_P^\times$, also $dt_P = u\,dt' + t'\,du$. Damit ist $f' = f(u + t'\,du/dt')$. Es ist $du/dt' \in \mathcal{O}_P$ (wie man anhand der Potenzreihenentwicklung in t' leicht sieht), also $v_P(u + t'\,du/dt') = 0$.

Als nächstes wollen wir zeigen, dass diese Koeffizienten einen Divisor $\mathrm{div}(\omega)$ ergeben, d.h., dass nur endlich viele $v_P(\omega) \neq 0$ sind. Dazu müssen wir etwas weiter ausholen und erst einmal den Verzweigungsdivisor einer separablen rationalen Abbildung einführen.

Sei also $\phi : C \to C'$ eine separable nicht-konstante rationale Abbildung. Dann ist $f \mapsto d\phi^*(f) \in \Omega_{K(C)/K}$ eine K-Derivation von $K(C')$. Nach der universellen Eigenschaft des Differenzialmoduls gibt es also eine eindeutig bestimmte $K(C')$-lineare Abbildung $\phi^* : \Omega_{K(C')/K} \to \Omega_{K(C)/K}$, so dass $\phi^*(df) = d\phi^*(f)$ ist.

DEFINITION 6.10. Der *Verzweigungsdivisor* von ϕ ist

$$R_\phi = \sum_{Q \in \mathcal{C}} v_Q(\phi^*(dt_{\phi(Q)})) \cdot Q \in \mathrm{Div}(C/K)\,.$$

Dabei ist wie üblich $dt_{\phi(Q)}$ ein uniformisierendes Element von $\mathcal{O}_{\phi(Q)}$. (Der Buchstabe „R“ kommt vom englischen Wort *ramification* für Verzweigung.)

Der Koeffizient von Q in R_ϕ hängt nicht von der Wahl des uniformisierenden Elements ab, wie man leicht einsieht.

PROPOSITION 6.11. *Sei ϕ wie oben und p die Charakteristik von K. Sei weiter $Q \in \mathcal{C}$ und $P = \phi(Q) \in \mathcal{C}'$. Dann gilt*

$$p \nmid e_{Q/P} \quad \Longrightarrow \quad v_Q(R_\phi) = e_{Q/P} - 1\,.$$

Falls $p \mid e_{Q/P}$, dann ist $v_Q(R_\phi) \geq e_{Q/P}$. Insbesondere ist R_ϕ ein wohldefinierter Divisor.

BEWEIS: Es gilt $\phi^*(t_P) = u t_Q^{e_{Q/P}}$ mit $u \in \mathcal{O}_Q^\times$. Daraus folgt

$$\phi^*(dt_P) = d\phi^*(t_P) = \left(e_{Q/P}\, u t_Q^{e_{Q/P}-1} + t_Q^{e_{Q/P}} \frac{du}{dt_Q} \right) dt_Q\,.$$

Wir haben $v_Q(du/dt_Q) \geq 0$, also ist $v_Q(\phi^*(dt_P)) = e_{Q/P} - 1$, wenn $e_{Q/P} \neq 0$ in K, also $p \nmid e_{Q/P}$. Im anderen Fall gilt $v_Q(\phi^*(dt_P)) = e_{Q/P} + v_Q(du/dt_Q) \geq e_{Q/P}$. Nach Satz 4.22 sind alle bis auf endlich viele $e_{Q/P} = 1$; für diese Q ist dann $v_Q(R_\phi) = 0$. Also ist R_ϕ tatsächlich ein Divisor. □

BEMERKUNG 6.12. Im Fall $e_{Q/P} > 1$, $p \nmid e_{Q/P}$ spricht man auch von *zahmer* Verzweigung, während Q im Fall $p \mid e_{Q/P}$ *wild* verzweigt heißt.

LEMMA 6.13.

(1) *Für* $\mathcal{K} = K(x)$ *haben wir* $\operatorname{div}(dx) = -2 \cdot \infty$.
(2) *Sei* $\phi : C \to C'$ *separabel und* $\omega \in \Omega_{K(C')/K}$. *Wenn* $\operatorname{div}(\omega)$ *existiert, dann existiert auch* $\operatorname{div}(\phi^*\omega)$, *und es gilt*

$$\operatorname{div}(\phi^*\omega) = \phi^*(\operatorname{div}(\omega)) + R_\phi\,.$$

BEWEIS: (1) Sei $P \in \mathrm{PrD}(K(x)/K)\backslash\{\infty\}$. Dann gibt es ein irreduzibles Polynom $f(x) \in K[x]$, so dass $f(x) = t_P$ gewählt werden kann. Wir haben

$$v_P(dx) = v_P(dx/df(x)) = -v_P(f'(x)) = 0\,,$$

da $f(x) \nmid f'(x)$ (K ist perfekt). Für $P = \infty$ wählen wir $t_\infty = x^{-1}$; dann ist $v_\infty(dx) = v_\infty(dx/d(x^{-1})) = v_\infty(-x^2) = -2$.

(2) Es gilt für $Q \in \mathcal{C}$, $P = \phi(Q)$:

$$\begin{aligned} v_Q(\phi^*\omega) &= v_Q(\phi^*\omega/dt_Q) \\ &= v_Q(\phi^*(\omega/dt_P)) + v_Q(\phi^*(dt_P)/dt_Q) \\ &= e_{Q/P}\; v_P(\omega/dt_P) + v_Q(R_\phi) \\ &= v_Q(\phi^* \operatorname{div}(\omega)) + v_Q(R_\phi)\,. \end{aligned}$$

Daraus folgt die Behauptung. □

PROPOSITION 6.14. *Sei* $\omega \in \Omega_{\mathcal{K}/K} \setminus \{0\}$. *Dann ist* $\operatorname{div}(\omega) = \sum_{P \in \mathrm{PrD}(\mathcal{K}/K)} v_P(\omega) \cdot P$ *ein wohldefinierter Divisor.*

BEWEIS: Wir haben nur zu zeigen, dass $v_P(\omega) = 0$ ist für alle bis auf endlich viele P. Sei dazu $x \in \mathcal{K}$ separierend; dann ist $\omega = f\,dx$ mit $f \in \mathcal{K}^\times$ und $\operatorname{div}(\omega) = \operatorname{div}(f) + \operatorname{div}(dx)$. Es genügt also, die Behauptung für $\omega = dx$ zu zeigen. Sei $\phi^* : K(x) \hookrightarrow K(C)$ die Inklusion. Nach dem vorstehenden Lemma haben wir

$$\operatorname{div}(\omega) = \operatorname{div}(f) + \phi^* \operatorname{div}_{K(x)}(dx) + R_\phi = \operatorname{div}(f) - 2\phi^*(\infty) + R_\phi \in \operatorname{Div}(C/K)\,.$$

□

Wir können daher analog zu den L-Räumen auch Ω-Räume definieren.

DEFINITION 6.15. Sei $D \in \operatorname{Div}(\mathcal{K}/K)$. Dann definieren wir

$$\Omega(D) = \{\omega \in \Omega_{\mathcal{K}/K} \mid \operatorname{div}(\omega) \geq D\}\,.$$

$\omega \in \Omega_{\mathcal{K}/K}$ heißt *regulär* (oder auch *holomorph*), wenn $\operatorname{div}(\omega) \geq 0$ ist.

Die große Bedeutung der Differenziale für die algebraische Geometrie der Kurven beruht auf dem folgenden Resultat.

SATZ 6.16. *Die kanonischen Divisoren in* $\operatorname{Div}(\mathcal{K}/K)$ *sind genau die Differenzialdivisoren* $\operatorname{div}(\omega)$, $\omega \in \Omega_{\mathcal{K}/K} \setminus \{0\}$.

KOROLLAR 6.17.

(1) *Sei* $W = \operatorname{div}(\omega)$. *Wir haben einen Isomorphismus*

$$L(W - D) \longrightarrow \Omega(D)\,, \qquad f \longmapsto f\omega\,.$$

Insbesondere ist $\Omega(D)$ *ein endlich-dimensionaler* K*-Vektorraum.*

(2) *Der Satz von Riemann-Roch kann auch so formuliert werden:*

$$\dim_K L(D) = \deg D - g + 1 + \dim_K \Omega(D)\,.$$

(3) *Es gilt* $\dim_K \Omega(0) = g$*. Das Geschlecht ist also gerade die Anzahl der linear unabhängigen regulären Differenziale.*
(4) *Für* $0 \neq \omega \in \Omega_{\mathcal{K}/K}$ *gilt* $\deg \operatorname{div}(\omega) = 2g - 2$*.*

BEWEIS: (1) Das folgt unmittelbar aus den Definitionen.

(2) Das folgt aus (1), da $W = \operatorname{div}(\omega)$ für ein geeignetes ω.

(3) Wir haben $\dim \Omega(0) = \dim L(W) = g$.

(4) Wir haben $\deg \operatorname{div}(\omega) = \deg W = 2g - 2$. □

Die Aussage $\deg \operatorname{div}(\omega) = 2g-2$ liefert nun zusammen mit der Formel $\operatorname{div}(\phi^*\omega) = \phi^* \operatorname{div}(\omega) + R_\phi$ sofort den Satz von Riemann-Hurwitz, der eine Aussage darüber macht, wie bei einer rationalen Abbildung $\phi : C \to C'$ das Geschlecht von C, das Geschlecht von C', der Grad von ϕ und das Verzweigungsverhalten von ϕ miteinander zusammenhängen.

SATZ 6.18 (Riemann-Hurwitz). *Sei* $\phi : C \to C'$ *eine nicht konstante separable rationale Abbildung. Dann gilt für die Geschlechter* $g(C)$ *und* $g(C')$ *von* C *bzw.* C'

$$2g(C) - 2 = (\deg \phi)(2g(C') - 2) + \deg R_\phi\,.$$

BEWEIS: Sei $\omega' \in \Omega_{C'/K}$. Wir betrachten den Divisor von $\omega = \phi^*\omega'$. Es gilt

$$\begin{aligned} 2g(C) - 2 &= \deg \operatorname{div}(\omega) \\ &= \deg(\phi^* \operatorname{div}(\omega')) + \deg R_\phi \\ &= (\deg \phi) \deg \operatorname{div}(\omega') + \deg R_\phi \\ &= (\deg \phi)(2g(C') - 2) + \deg R_\phi\,. \end{aligned}$$

□

Daraus lassen sich einige interessante Schlüsse ziehen.

KOROLLAR 6.19.

(1) *Der Grad von* R_ϕ *ist gerade.*
(2) *Es gilt stets* $g(C) \geq g(C')$*.*
(3) *Gleichheit* $g(C) = g(C')$ *gilt genau in den folgenden Fällen:*
(a) $\deg \phi = 1$*, (b)* $g(C') = 0$ *und* $\deg R_\phi = 2(\deg \phi - 1)$*, (c)* $g(C') = 1$ *und* ϕ *ist unverzweigt (d.h.* $R_\phi = 0$*).*
(4) *Es gibt keine echte (d.h.* $\deg \phi > 1$*) unverzweigte Überlagerung (bzw. Erweiterung) der Geraden (bzw. von* $K(x)$*).*

BEWEIS: (1) Das folgt sofort aus der Formel im Satz von Riemann-Hurwitz.
(2) Das ist klar für $g(C') = 0$. Anderenfalls ist $g(C') - 1 \geq 0$, und wir haben die Ungleichung $g(C) - 1 \geq (\deg \phi)(g(C') - 1) \geq g(C') - 1$.
(3) Wenn $g(C) = g(C') = g$, dann lautet die Formel $\deg R_\phi = 2(1-g)(\deg \phi - 1)$. Ist $g \geq 2$ und $\deg \phi \geq 2$, dann ist die rechte Seite negativ, die linke aber nicht. Die verbleibenden Fälle führen gerade auf (a), (b), (c).
(4) Ist $g(C') = 0$, dann folgt $\deg R_\phi = 2(g(C) - 1 + \deg \phi) > 0$, falls $\deg \phi \geq 2$.
□

Aussage (4) ist analog zu der zahlentheoretischen Aussage, dass es keine unverzweigte Erweiterung von $\mathbb{Q}$ gibt (anders gesagt, keinen algebraischen Zahlkörper außer $\mathbb{Q}$, der Diskriminante 1 hat). In der Zahlentheorie wird diese Aussage aber mit ganz anderen Methoden bewiesen (Minkowski-Schranke). Überhaupt gibt es eine weit tragende Analogie zwischen algebrasicher Zahlentheorie (d.h. der Theorie der endlichen Erweiterungen von $\mathbb{Q}$) und algebraischer Geometrie von Kurven (d.h. der Theorie der endlichen Erweiterungen von $K(x)$). Viele Ergebnisse, die in der Zahlentheorie schwierige offene Probleme darstellen, haben im Fall der Funktionenkörper einfache Beweise. Der Hauptgrund dafür ist die Riemann-Hurwitz-Formel (oder allgemeiner, die Möglichkeit mit Differenzialen zu arbeiten); etwas Analoges existiert in der Zahlentheorie nicht.

Eine Anwendung

Wir wollen nun die Aussage $\dim \Omega(0) = g$ dazu benutzen, eine Art Formel für das Geschlecht für eine große Klasse von Kurven herzuleiten.

Der Einfachheit halber sei im Folgenden vorausgesetzt, dass der Körper K Charakteristik null hat. Wir führen zunächst einige Begriffe ein.

Definition 6.20. Sei $F \in K[X,Y] \setminus \{0\}$, $F = \sum_{i,j} a_{ij} X^i Y^j$.

(1) Das *Newton-Polygon* von F, $\mathrm{NP}(F)$, ist die konvexe Hülle der Menge $\{(i,j) \in \mathbb{Z}^2 \mid a_{ij} \neq 0\}$ der Gitterpunkte zu Monomen, die in F auftreten.
(2) Seien $a, b \in \mathbb{Z}$ teilerfremd. Wir sagen, $\mathrm{NP}(F)$ habe eine (a,b)-Kante, wenn es $m \in \mathbb{Z}$ gibt mit
$$\mathrm{NP}(F) \subset \{(\xi,\eta) \in \mathbb{R}^2 \mid a\xi + b\eta \leq m\}$$
und $\{(\xi,\eta) \in \mathrm{NP}(F) \mid a\xi + b\eta = m\}$ nicht nur aus höchstens einem Punkt besteht.
(3) Für eine (a,b)-Kante von $\mathrm{NP}(F)$ mit m wie oben setzen wir
$$F_{(a,b)}(u) = \sum_{i,j:ai+bj=m} a_{ij} u^{(bi-aj)/(a^2+b^2)-\gamma} \in K[u]\,,$$
wobei $\gamma = (bi_0 - aj_0)/(a^2+b^2)$ und $(i_0, j_0) \in \mathrm{NP}(F) \cap \mathbb{Z}^2$ der Punkt mit $ai_0 + bj_0 = m$ und $bi_0 - aj_0$ minimal ist. Dann ist $F_{(a,b)}(0) \neq 0$ und $\deg F_{(a,b)}(u) \geq 1$. Wir nennen $F_{(a,b)}$ das (a,b)-*Kantenpolynom* von F.

Nun können wir das Resultat formulieren.

Satz 6.21. *Sei $C : F(X,Y) = 0$ eine glatte Kurve mit der Eigenschaft, dass alle (a,b)-Kantenpolynome von F mit $a < 0$ oder $b < 0$ quadratfrei sind. Dann ist das Geschlecht von C gleich der Anzahl der Gitterpunkte im Inneren des Newtonpolygons von F.*

Der Beweis ergibt sich aus der Tatsache, dass $\dim \Omega(0) = g$ ist und aus der folgenden Proposition.

Proposition 6.22. *In der Situation des Satzes ist eine Basis des Raumes $\Omega(0)$ der regulären Differenziale auf C gegeben durch*
$$\{x^{i-1} y^{j-1} \omega_0 \mid (i,j) \in \mathrm{NP}(F)^0 \cap \mathbb{Z}^2\}\,.$$

Dabei ist

$$\omega_0 = \frac{dx}{F_Y(x,y)} = -\frac{dy}{F_X(x,y)}\,.$$

Hier bezeichnen F_X und F_Y die partiellen Ableitungen von F. Die Gleichheit der beiden Ausdrücke für ω_0 folgt aus

$$0 = dF(x,y) = F_X(x,y)\,dx + F_Y(x,y)\,dy\,.$$

Zum Beweis der Proposition müssen wir uns überlegen, was die Regularität eines Differenzials in den verschiedenen Punkten bedeutet. In einem ersten Schritt tun wir das für alle affinen Punkte (d.h. diejenigen Primdivisoren, deren lokale Ringe über dem affinen Koordinatenring $K[x,y]$ liegen).

LEMMA 6.23. *Ein Differenzial ω auf C ist genau dann regulär in allen affinen Punkten von C, wenn es von der Form $\omega = f\omega_0$ ist mit $f \in K[x,y]$.*

BEWEIS: Da $K[x,y]$ genau aus allen Funktionen besteht, die in allen affinen Punkten regulär (d.h. definiert) sind, ist die Behauptung äquivalent zu der Behauptung, dass für alle affinen P gilt $v_P(\omega_0) = 0$. Um das zu zeigen, verwenden wir, dass C in P glatt ist. Das bedeutet, dass wenigstens eine der beiden partiellen Ableitungen $F_X(x,y)$ und $F_Y(x,y)$ in P nicht verschwindet; sei zum Beispiel $F_Y(x,y)(P) \neq 0$, d.h. $v_P(F_Y(x,y)) = 0$. Wir behaupten, dass dann auch $v_P(dx) = 0$ ist. Sei dazu $t = t_P$ ein uniformisierendes Element bei P. Es gilt

$$F_X(x,y)(P)\frac{dx}{dt}(P) + F_Y(x,y)(P)\frac{dy}{dt}(P) = 0\,.$$

Wenn also dx/dt bei P verschwindet, dann auch dy/dt. Nun ist aber $t = T(x,y) \in K(x,y)$ eine rationale Funktion in x und y, also $1 = dt/dt = T_X(x,y)\,dx/dt + T_Y(x,y)\,dy/dt$. Da t in P regulär ist, sind T_X und T_Y ebenfalls in P definiert, und es würde folgen, dass 1 in P verschwindet. Folglich muss $v_P(dx) = 0$ sein, und damit ist auch $v_P(\omega_0) = 0$. □

Da C insbesondere in $(0,0)$ glatt ist, folgt, dass die inneren Punkte des unbeschränkten Polygons, das durch den Schnitt der Halbebenen $ax+by \geq m$ gegeben ist für alle (a,b)-Seiten von $\mathrm{NP}(F)$ mit $a,b \geq 0$, genau die inneren Punkte des ersten Quadranten sind. Die Aussage des Lemmas sagt also in etwa, dass die Bedingung, die von der linken unteren Ecke des Newtonpolygons kommt, gerade der Regularität in den affinen Punkten entspricht.

Wir müssen also jetzt die Punkte „im Unendlichen“ betrachten. Wir wollen die Menge dieser Primdivisoren (deren lokale Ringe also nicht über $K[x,y]$ liegen) mit $\mathcal{C}_\infty$ bezeichnen.

Sei außerdem $X \subset \mathbb{Z}^2 \times K[u]$ folgende Menge. Ein Paar $((a,b),H)$ gehört zu X, wenn

(i) $\mathrm{NP}(F)$ eine (a,b)-Seite hat und $a < 0$ oder $b < 0$ ist und
(ii) H ein irreduzibler Faktor von $F_{(a,b)}(u)$ ist.

LEMMA 6.24.

(1) *Es gibt eine surjektive Abbildung*

$$\phi : \mathcal{C}_\infty \longrightarrow X$$

mit folgenden Eigenschaften. Sei $\phi(P) = ((a,b),H)$. *Dann gilt* $v_P(x) = a$, $v_P(y) = b$ *und* $v_P(H(x^b y^{-a})) > 0$.

(2) *Sei* $\mathcal{C}_{(a,b)} \subset \mathcal{C}_\infty$ *die Teilmenge der Punkte, die in der ersten Komponente auf* (a,b) *abgebildet werden. Sei weiter* $G \in K[X,Y] \setminus \{0\}$ *und* $m_G = \min\{a\xi + b\eta \mid (\xi,\eta) \in \mathrm{NP}(G)\}$. *Wir definieren* $G_{(a,b)}(u)$ *wie oben, auch wenn* $\mathrm{NP}(G)$ *keine* (a,b)*-Kante haben sollte (dann ist* $G_{(a,b)}(u) \in K^\times$*). Wenn für alle* $P \in \mathcal{C}_{(a,b)}$ *gilt* $v_P(G(x,y)) > m_G$, *dann folgt* $F_{(a,b)}(u) \mid G_{(a,b)}(u)$ *(und insbesondere hat dann* $\mathrm{NP}(G)$ *eine* (a,b)*-Kante).*

Beweis: Sei $P \in \mathcal{C}_\infty$. Dann folgt $x^{-1} \in \mathcal{O}_P$ oder $y^{-1} \in \mathcal{O}_P$ (oder beides). Wenn wir also $v_P(x) = a'$, $v_P(y) = b'$ setzen, dann ist $a' < 0$ oder $b' < 0$. Sei weiter $\gamma = \mathrm{ggT}(a,b)$ und $a = a'/\gamma$, $b = b'/\gamma$. Es gibt Zahlen $r, s \in \mathbb{Z}$ mit $ra + sb = 1$. Wir setzen $u = x^b y^{-a}$ und $t = x^r y^s$; dann folgt $v_P(u) = 0$, $v_P(t) = \gamma$. Außerdem ist $x = u^s t^a$ und $y = u^{-r} t^b$, also $K(C) = K(x,y) = K(t,u)$. Wir können also F schreiben als $F(x,y) = t^m \tilde{F}(t,u)$ mit $\tilde{F} \in K[u,u^{-1}][t]$, wobei $m = \min\{a\xi + b\eta \mid (\xi,\eta) \in \mathrm{NP}(F)\}$ ist. Dabei ist $\tilde{F}(u,0) = u^w F_{(a,b)}(u)$ für ein $w \in \mathbb{Z}$.

Da $\tilde{F}(t,u) = 0$ ist, folgt $v_P(F_{(a,b)}(u)) > 0$ (denn die übrigen Terme in $\tilde{F}(t,u)$ haben positive Bewertung). Also gibt es genau einen irreduziblen Faktor H von $F_{(a,b)}$, so dass $v_P(H(u)) > 0$ ist. Wir definieren $\phi(P) = ((a,b),H)$.

Wir müssen noch zeigen, dass $(a,b) = (a',b')$, also dass $\gamma = 1$ ist. Dazu betrachten wir den Ring $R = K[u]_{(H)}[t]$ (seine Elemente können geschrieben werden in der Form $f(t,u)/g(u)$ mit Polynomen f und g, so dass g kein Vielfaches von H ist). Sein Quotientenkörper ist offensichtlich $K(C)$; also genügt es zu zeigen, dass $v_P(R \setminus \{0\}) = \gamma\mathbb{Z}_{\geq 0}$ ist.

Wir schreiben $F_{(a,b)}(u) = H(u)\tilde{H}(u)$. Da wir angenommen haben, dass $F_{(a,b)}$ quadratfrei ist, ist $\tilde{H}(u) \in R^\times$, und wir bekommen aus $\tilde{F}(t,u) = 0$ die Relation

$$H(u) = -\tilde{H}(u)^{-1} t \tilde{F}_1(t,u) \in t\,R\,;$$

dabei ist $\tilde{F}(t,u) = F_{(a,b)}(u) + t\tilde{F}_1(t,u)$. Sei nun $f \in R \setminus \{0\}$. Wir schreiben f in der Form $f = t^\nu f_1$ mit $f_1 \in R$ und ν maximal (das geht, da $v_P(f) \geq \gamma\nu$). Wir behaupten, dass dann $v_P(f) = \gamma\nu$ ist, woraus unsere Behauptung $\gamma = 1$ folgt. Wäre $v_P(f) > \gamma\nu$, dann hätten wir $v_P(f_1(t,u)) > 0$. In diesem Fall können wir schreiben

$$f_1(t,u) = H(u)f_2(u) + tf_3(t,u) = t(-\tilde{H}(u)^{-1}\tilde{F}_1(t,u)f_2(u) + f_3(t,u)) \in t\,R\,,$$

also war ν nicht maximal, im Widerspruch zu unserer Annahme.

Um den Beweis von Teil (1) abzuschließen. müssen wir noch zeigen, dass ϕ surjektiv ist. Das folgt daraus, dass es diskrete Bewertungsringe mit Quotientenkörper $K(C)$ gibt, die den diskreten Bewertungsring $K[u]_{(H)}$ enthalten. (Geometrisch interpretiert sind das die Punkte, die unter der der Inklusion $K(u) \to K(C)$ entsprechenden Abbildung $C \to$ Gerade auf den dem Polynom H entsprechenden Punkt abgebildet werden.)

Nun zu Teil (2). Wir können G schreiben als $G(x,y) = t^{m_G}\tilde{G}(t,u)$, so dass $\tilde{G}(0,u) = u^{w_G}G_{(a,b)}(u)$ (mit $w_G \in \mathbb{Z}$) ist. Sei $P \in \mathcal{C}_{(a,b)}$. Ist $v_P(G) > m_G$, so folgt $v_P(G_{(a,b)}(u)) > 0$, also wird $G_{(a,b)}$ von H geteilt, wenn $\phi(P) = ((a,b),H)$

ist. Nun gibt es aber zu jedem irreduziblen Faktor H von $F_{(a,b)}$ einen solchen Punkt P. Da $F_{(a,b)}$ nach Annahme quadratfrei ist, muss $G_{(a,b)}$ also von $F_{(a,b)}$ geteilt werden. □

Nun können wir die Bedingung dafür formulieren, dass ein Differenzial auf C regulär ist. Wir setzen $m_{(a,b)} = \min\{a\xi + b\eta \mid (\xi,\eta) \in \mathrm{NP}(F)\}$.

LEMMA 6.25. *Sei $\omega = f\omega_0$ ein Differenzial auf C. Dann ist ω regulär genau dann, wenn $f \in K[x,y]$ ist und $v_P(xyf) > m_{(a,b)}$ ist für alle $P \in \mathcal{C}_{(a.b)}$, wobei (a,b) alle Paare ganzer Zahlen durchläuft, so dass $\mathrm{NP}(F)$ eine (a,b)-Kante hat und $a < 0$ oder $b < 0$ ist.*

BEWEIS: Die erste Bedingung wurde in Lemma 6.23 beweisen. Die zweite Bedingung muss dann dazu äquivalent sein, dass ω in allen Punkte in $\mathcal{C}_\infty$ regulär ist. Sei also $P \in \mathcal{C}_{(a,b)} \subset \mathcal{C}_\infty$. Wir bestimmen $v_P(\omega_0)$. Sei beispielsweise $a < 0$. Dann folgt (da $\mathrm{char}(K) = 0$) $v_P(dx) = a - 1$. Weiterhin ist (wenn man $\tilde{F} \in K[U, U^{-1}, T]$ auffasst)

$$\begin{aligned} F_Y(x,y) &= \frac{\partial}{\partial Y}\left(T^m \tilde{F}(T,U)\right)(t,u) \\ &= \frac{m}{y} t^m \tilde{F}(t,u) + \frac{t^m}{y}\left(st\,\tilde{F}_T(t,u) - au\,\tilde{F}_U(t,u)\right) \\ &= 0 + \frac{t^m}{y}\left(-au^{w+1} F'_{(a,b)}(u) + t(\dots)\right), \end{aligned}$$

also (wiederum da $F_{(a,b)}$ quadratfrei ist) $v_P(F_Y(x,y)) = m - b$. Insgesamt haben wir $v_P(\omega_0) = a + b - m - 1$ und damit $v_P(\omega) = v_P(xyf) - (m+1)$. Also ist $v_P(\omega) \geq 0$ genau dann, wenn $v_P(xyf) > m$ ist. □

Ist $f = x^i y^j$ ein Monom, dann bedeuten die Bedingungen des Lemmas gerade, dass $(i+1, j+1)$ ein innerer Punkt von $\mathrm{NP}(F)$ ist. Die in Prop. 6.22 genannten Differenziale spannen also jedenfalls einen Unterraum von $\Omega(0)$ auf. Es bleibt zu zeigen, dass sie sogar den ganzen Raum aufspannen.

Sei also $\omega = f\omega_0 \in \Omega(0)$. Wir können eine geeignete Linearkombination der Basiselemente von ω abziehen, so dass in xyf nur noch Monome auftreten, die zu Gitterpunkten außerhalb des Inneren von $\mathrm{NP}(F)$ gehören. Wir betrachten so eine Darstellung (von $\bar{\omega} \in \Omega(0)/\langle B\rangle$, wobei B die in Prop. 6.22 angegebene Basis ist) $xyf = \sum_{i,j} b_{ij} x^i y^j$ mit

$$\mu = \sum_{(a,b)} \max\{0, \max\{m_{(a,b)} + 1 - ai - bj \mid b_{ij} \neq 0\}\}$$

minimal. Wir wollen zeigen, das $\mu = 0$ ist, denn dann folgt $f = 0$. Wir nehmen also an, dass $\mu > 0$ ist; sei etwa (a,b) mit $\mu_{(a,b)} = \max\{m_{(a,b)} + 1 - ai - bj \mid b_{ij} \neq 0\} > 0$. Nach Lemma 6.25 ist $v_P(xyf) < m_{(a,b)}$ für alle $P \in \mathcal{C}_{(a,b)}$. Nach Lemma 6.24, (2), folgt, dass $F_{(a,b)}$ das Kantenpolynom $f_{(a,b)}$ teilt: $f_{(a,b)}(u) = F_{(a,b)}(u)G(u)$ und daher mit $0 = \tilde{F}(t,u) = (u^w F_{(a,b)}(u) + t\tilde{F}_1(t,u))$ und einer

analogen Zerlegung von $f(x,y) = \tilde{f}(t,u)$:

$$\begin{aligned}\tilde{f}(t,u) &= t^{m_f+1}\tilde{f}_1(t,u) + t^{m_f}u^{w_f}f_{(a,b)}(u)\\ &= t^{m_f+1}\tilde{f}_1(t,u) + t^{m_f}u^{w_f}G(u)F_{(a,b)}(u)\\ &= t^{m_f+1}\tilde{f}_1(t,u) - t^{m_f}u^{w_f}G(u)\cdot tu^{-w}\tilde{F}_1(t,u)\\ &= t^{m_f+1}\tilde{f}_1(t,u) - t^{m_f+1}u_{w_f-w}G(u)\tilde{F}_1(t,u)\end{aligned}$$

Die Terme hierin (wenn wieder in x und y ausgedrückt) haben alle $m+1-ai-bj < \mu_{(a,b)}$, während sich die Werte für andere (a,b) nicht vergrößert haben. Also war μ nicht minimal, und die Proposition ist bewiesen.

Fortsetzung folgt!