Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 13

Wir entwickeln nun die allgemeine Theorie zu elliptischen Kurven über einem beliebigen Körper weiter, wobei die Situation über den komplexen Zahlen eine wichtige Orientierung liefert.

Morphismen zwischen Kurven

Wir untersuchen nun die Morphismen zwischen glatten projektiven Kurven genauer, insbesondere zwischen elliptischen Kurven, wobei wir insbesondere Satz 7.12 vertiefen werden. Als Hauptbeispiele sollte man eine rationale Funktion

$$f\colon \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K,$$

die durch die rationale Funktion $x = \frac{X}{Z}$ gegebene Projektion

$$E = V_+(Y^2Z - X^3 - aXZ^2 - bZ^3) \longrightarrow \mathbb{P}^1_K$$

einer elliptischen Kurve auf die projektive Gerade oder die durch die Verdoppelung gegebene Abbildung

$$[2]\colon E \longrightarrow E$$

(vergleiche Korollar 6.7) vor Augen haben. In positiver Charakteristik wird später der Frobenius eine ausgezeichnete Rolle spielen.

Definition 13.1. Es seien C und D irreduzible algebraische Kurven über einem algebraisch abgeschlossenen Körper K und sei

$$\varphi\colon C \longrightarrow D$$

eine endliche Abbildung. Dann nennt man den Grad der zugehörigen Körpererweiterung der Funktionenkörper $Q(D) \subseteq Q(C)$ den *Grad* von φ.

Satz 13.2. *Es seien C und D irreduzible glatte Kurven über einem algebraisch abgeschlossenen Körper K und sei*

$$\varphi\colon C \longrightarrow D$$

eine endliche Abbildung vom Grad n. Dann besteht für jeden Punkt $P \in D$ das Urbild $\varphi^{-1}(P)$ aus höchstens n Punkten. Wenn man die Punkte mit Multiplizitäten zählt, so handelt es sich jeweils um genau n Punkte.

Beweis. Wir können die affine Situation betrachten, es seien also R, S integre normale K-Algebren vom endlichen Typ der Dimension 1 und $R \subseteq S$ sei eine endliche Erweiterung. Es besitzt $Q(R) \subseteq Q(S)$ den Grad n. Der Punkt P entspreche dem maximalen Ideal $\mathfrak{p}$ von R. Aufgrund der Glattheit ist die

Lokalisierung $R_{\mathfrak{p}}$ ein diskreter Bewertungsring und daher ist $S_{\mathfrak{p}} = S \otimes_R R_{\mathfrak{p}} = S_{R \setminus \mathfrak{p}}$ eine freie (da torsionsfrei) $R_{\mathfrak{p}}$-Algebra von Rang n. Daher ist auch der Faserring über $\mathfrak{p}$, also

$$S \otimes_R \kappa(\mathfrak{p}) = S_{R \setminus \mathfrak{p}}/\mathfrak{p}S,$$

eine freie $\kappa(\mathfrak{p})$-Algebra vom Rang n, also ein $\kappa(\mathfrak{p})$-Vektorraum der Vektorraumdimension n. Die schematheoretische Faser hat also die Vektorraumdimension n (das ist mit Multiplizität) gemeint. Dieser Ring hat die Form $A_1 \times \cdots \times A_m$, wobei die A_j $\kappa(\mathfrak{p})$-Algebren mit einem einzigen maximalen Ideal sind. Daher ist $m \leq n$. □

Lemma 13.3. *Es sei K ein Körper,*

$$f = \frac{g}{h} \in K(X)$$

eine nichtkonstante rationale Funktion in gekürzter Darstellung. Dann ist der Grad der zugehörigen Körpererweiterung

$$K(U) \longrightarrow K(X),\, U \longmapsto f(X),$$

gleich dem Maximum der Grade von g und h.

Beweis. Wir geben einen geometrischen Beweis und können annehmen, dass K algebraisch abgeschlossen ist. Wir betrachten die zugehörige rationale Abbildung

$$\mathbb{A}^1_K \longrightarrow \mathbb{A}^1_K,\, x \longmapsto f(x),$$

die außerhalb der Nullstellen von h definiert ist. Es geht nach Satz 13.2 um die Anzahl der Fasern dieser Abbildung. Zu $a \in K$ ist die Faser durch $\left\{x \in K \mid \frac{g(x)}{h(x)} = a\right\}$ bzw. durch $\{x \in K \mid g(x) - ah(x)\} = 0$ charakterisiert. Dies ist (eventuell mit einzelnen Ausnahmen für a) eine polynomiale Bedingung für x, deren Grad das Maximum der Grade von g und h ist. □

Eine wichtige Frage ist, wie man die Punkte bestimmen kann, über denen es im Sinne von Satz 13.2 genau n Urbildpunkte gibt, ohne dass man Multiplizitäten berücksichtigen muss. In Charakteristik 0 ist dies das generische Verhalten.

Definition 13.4. Zu einem injektiven Ringhomomorphismus $R \subseteq S$ zwischen diskreten Bewertungsringen nennt man die Ordnung einer Ortsuniformisierenden von R in S die *Verzweigungsordnung* der Erweiterung.

Definition 13.5. Ein injektiver Ringhomomorphismus $R \subseteq S$ zwischen diskreten Bewertungsringen heißt *verzweigt*, wenn seine Verzweigungsordnung ≥ 2 ist.

Unverzweigt bedeutet also, dass eine Ortsuniformisierende auf eine Ortsuniformisierende abgebildet wird. Diese Konzepte werden insbesondere bei einem nichtkonstanten Morphismus $\varphi\colon C \to D$ zwischen glatten Kurven und

einem Punkt $Q \in C$ mit $\varphi(Q) = P$ auf den zugehörigen Ringhomomorphismus $\mathcal{O}_{D,P} \to \mathcal{O}_{C,Q}$ angewendet. In diesem Fall schreibt man $\operatorname{Verz}(Q|P)$ für die Verzweigungsordnung.

SATZ 13.6. *Es seien C und D irreduzible glatte Kurven über einem algebraisch abgeschlossenen Körper K und sei*

$$\varphi\colon C \longrightarrow D$$

eine endliche Abbildung vom Grad n. Dann sind für einen Punkt $P \in D$ mit lokalem Ring $\mathcal{O}_P$ die folgenden Aussagen äquivalent.

(1) *Die Faser über P besteht aus genau n Punkten.*
(2) *Die Faser über P ist reduziert.*
(3) *Für jeden Punkt $Q \in C$ oberhalb von P wird unter*
$$\mathcal{O}_P \longrightarrow \mathcal{O}_Q$$
eine Ortsuniformisierende auf eine Ortsuniformisierende abgebildet.
(4) *Es ist*
$$\left(\Omega_{C|D}\right)_Q = 0$$
für jeden Punkt $Q \in C$ oberhalb von P.

Beweis. Wir können direkt davon ausgehen, dass R und S glatte endlich erzeugte kommutative K-Algebren der Dimension 1 sind, dass $R \subseteq S$ eine endlich freie Ringerweiterung vom Rang n ist und dass P dem maximalen Ideal $\mathfrak{m}$ entspricht, $\mathcal{O}_P = R_{\mathfrak{m}}$. Es ist $R_{\mathfrak{m}} \to S_{R\setminus\mathfrak{m}}$ die lokalisierte Version der Abbildung und

$$K \cong R/\mathfrak{m} \longrightarrow S \otimes_R R/\mathfrak{m}$$

die Restklasssenversion. Dabei ist $S \otimes_R R/\mathfrak{m}$ eine endlichdimensionale K-Algebra der Vektorraumdimension n (und der Krulldimension 0) und besitzt die Form $A_1 \times \cdots \times A_m$ mit lokalen K-Algebren der Krulldimension 0. Da K algebraisch abgeschlossen ist, sind die Restklassenkörper von A_i gleich K und daher gibt es in der Faser genau dann n Punkte, wenn die Faser reduziert ist. Deshalb sind (1) und (2) äquivalent. Die Äquivalenz von (2) und (3) beruht auf Lemma 18.3 (Algebraische Zahlentheorie (Osnabrück 2020-2021)). Die Äquivalenz zwischen (3) und (4) ergibt sich aus Satz Anhang 2.2. □

DEFINITION 13.7. Es seien C und D irreduzible algebraische Kurven über einem algebraisch abgeschlossenen Körper K und sei

$$\varphi\colon C \longrightarrow D$$

eine endliche Abbildung. Man nennt φ *separabel*, wenn die zugehörige Körpererweiterung der Funktionenkörper $Q(D) \subseteq Q(C)$ separabel ist.

In Charakteristik 0 sind die endlichen Morphismen nach Bemerkung 13.4 (Körper- und Galoistheorie (Osnabrück 2018-2019)) stets separabel. Der Frobenius ist hingegen nicht separabel.

Satz 13.8. *Es seien C und D irreduzible Kurven über einem algebraisch abgeschlossenen Körper K und sei*

$$\varphi\colon\, C \longrightarrow D$$

eine separable endliche Abbildung vom Grad n. Dann besteht außerhalb einer endlichen Ausnahmemenge für jeden Punkt $P \in D$ das Urbild $\varphi^{-1}(P)$ aus genau n Punkten.

Beweis. Wir können direkt davon ausgehen, dass affine glatte Kurven vorliegen, da eine Kurve außerhalb einer endlichen Teilmenge stets glatt ist. Es sei $R \subseteq S$ der zugehörige endliche Ringhomomorphismus, wir arbeiten mit dem Modul der Kähler-Differentiale $\Omega_{S|R}$ und wenden Satz 13.2 an. Nach Voraussetzung ist die Körpererweiterung

$$Q(D) \,=\, Q(R) \,\subseteq\, Q(C) \,=\, Q(S)$$

separabel. Daher gilt

$$\Omega_{Q(S)|Q(R)} \,=\, 0$$

nach Satz Anhang 7.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)). Es ist $\Omega_{Q(S)|Q(R)}$ nach Lemma 18.6 (Bündel, Garben und Kohomologie (Osnabrück 2019-2020)) die Nenneraufnahme von $\Omega_{S|R}$ an $S \setminus \{0\}$ bzw. an $R \setminus \{0\}$. Da der Kählermodul nach Korollar 19.4 (Algebraische Zahlentheorie (Osnabrück 2020-2021)) endlich erzeugt ist, gibt es auch ein $f \in R$, $f \neq 0$, mit

$$\left(\Omega_{S|R}\right)_f \,=\, \Omega_{S_f|R_f} \,=\, 0.$$

In der abgeschlossenen Teilmenge $V(f)$, also außerhalb von $D(f)$, liegen nur endlich viele Punkte. Daher können wir die Aussage auf $D(f)$ beweisen. D.h. wir können von einer endlichen Erweiterung $R \subseteq S$ ausgehen, für die der Modul der Kähler-Differentiale überhaupt gleich 0 ist. Die Aussage ergibt sich dann aus Satz 13.6. □

Satz 13.9. *Es sei E eine elliptische Kurve über einem Körper K. Dann ist jeder Morphismus*

$$\mathbb{P}^1_K \longrightarrow E$$

konstant.

Beweis. Es sei K algebraisch abgeschlossen. Die elliptische Kurve E liege in der Legendre-Form

$$y^2 \,=\, x(x-1)(x-\lambda)$$

vor. Es sei der Morphismus

$$\mathbb{P}^1_K \longrightarrow E,\, t \longmapsto (\varphi(t),\, \psi(t))\,,$$

gegeben, der

$$\psi^2(t) \,=\, \varphi(t)(\varphi(t)-1)(\varphi(t)-\lambda)$$

erfüllt, wobei φ, ψ rationale Funktionen in t sind. Wir multiplizieren mit der dritten Potenz des Nenners von $\varphi = \frac{h}{g}$ und können dann von einer Gleichung der Form

$$\psi^2 g^3 = h(t)(h(t) - g(t))(h(t) - \lambda g(t))$$

mit teilerfremden Polynomen h, g in t ausgehen. Eine Nullstelle von g ist keine Nullstelle von h und damit auch keine Nullstelle von $h - g$ und $h - \lambda g$.

Es sei $\psi = \frac{r}{s}$ gekürzt. Da in der obigen Gleichung rechts ein Polynom steht, muss sich g^3 gegen s^2 wegkürzen. Somit ist $s = \alpha^3$ und $g = \beta\alpha^2$ mit Polynomen α, β. Da die Nullstellen von g rechts nicht auftreten, folgt $\beta = 1$. Es liegt also die Situation

$$r^2 = h(h - \alpha^2)(h - \lambda\alpha^2)$$

vor. Eine Nullstelle links besitzt eine gerade Nullstellenordnung. Die Faktoren rechts haben keine gemeinsame Nullstelle, deshalb tritt in ihnen auch jede Nullstelle mit einer geraden Nullstellenordnung auf und deshalb liegen vier Quadrate

$$\beta^2, \alpha^2, \beta^2 - \alpha^2, \beta^2 - \lambda\alpha^2$$

in $K[t]$ vor, die projektiv unabhängig voneinander sind. Aus Satz Anhang 3.2 folgt, dass es sich um Konstanten handelt. □

LEMMA 13.10. *Es seien E_1 und E_2 elliptische Kurven über einem Körper K. Es sei*

$$y^2 = x^3 + ax + b$$

die Gleichung von E_1 und

$$v^2 = u^3 + cu + d$$

die Gleichung von E_2. Dann ist durch

$$u = \varphi(x, y) = f(x) + g(x)y$$

und

$$v = \psi(x, y) = p(x) + q(x)y$$

mit $f, g, p, q \in K(x)$ genau dann ein Morphismus

$$E_1 \longrightarrow E_2$$

gegeben, wenn

$$p^2 + q^2\big(x^3 + ax + b\big) = f^3 + cf + 3fg^2(x^3 + ax + b) + d$$

und

$$2pq = g^3\big(x^3 + ax + b\big) + 3f^2 g + cg$$

gilt.

Beweis. Die Bedingung für einem Morphismus ist

$$\psi^2 \;=\; \varphi^3 + c\varphi + d,$$

also

$$(p+qy)^2 \;=\; (f+gy)^3 + c(f+gy) + d.$$

Dabei ist

$$\begin{array}{rcl}(p+qy)^2 & = & p^2 + q^2y^2 + 2pqy \\ & = & p^2 + q^2\big(x^3+xa+b\big) + 2pqy\end{array}$$

und

$$\begin{array}{rl} & (f+gy)^3 + c(f+gy) + d \\ = & f^3 + 3f^2gy + 3fg^2y^2 + g^3y^3 + cf + d + cgy \\ = & f^3 + 3fg^2\big(x^3+ax+b\big) + cf + d + \big(3f^2g + g^3\big(x^3+ax+b\big) + cg\big)y.\end{array}$$

Das Resultat folgt mit Koeffizientenvergleich. □

Bei der Verdoppelungsabbildung auf einer elliptischen Kurve in sich ist in der Notation von Lemma 13.10 $g = p = 0$, siehe Korollar 6.7. In diesem Fall vereinfachen sich die beiden Bedingungen zu der einen Bedingung

$$q^2(x^3+ax+b) \;=\; f^3 + af + b.$$

LEMMA 13.11. *Es seien E_1 und E_2 elliptische Kurven über einem Körper K. Es sei*

$$y^2 \;=\; x^3 + ax + b$$

die Gleichung von E_1 und

$$v^2 \;=\; u^3 + cu + d$$

die Gleichung von E_2. Es seien $f, q \in K(X)$ rationale Funktionen mit

$$q^2(x^3+ax+b) \;=\; f^3 + cf + d,$$

f nicht konstant, und sei

$$\theta\colon\; E_1 \longrightarrow E_2,\; (x,y) \longmapsto (f(x), q(x)y)$$

der zugehörige Morphismus im Sinne von Lemma 13.10. Dann ist der Grad von θ gleich dem Maximum des Grades von Zähler und Nenner von f in einer gekürzten Darstellung.

Beweis. Die zugehörige Abbildung der Funktionenkörper ist durch

$$\vartheta : Q(E_2) = K(U)[V]/\big(V^2 - U^3 - cU - d\big) \longrightarrow Q(E_1) = K(X)[Y]/\big(Y^2 - X^3 - aX - b\big)$$

mit $U \mapsto f(X)$ und $V \mapsto q(X)Y$ gegeben. Nach Definition ist der Grad der Kurvenabbildung der Grad dieser Körpererweiterung. Es liegt das kommutative Diagramm

$$\begin{array}{ccc} K(U) & \stackrel{U\mapsto f}{\longrightarrow} & K(X) \\ \downarrow & & \downarrow \\ K(U)[V]/(V^2-U^3-cU-d) & \stackrel{\vartheta}{\longrightarrow} & K(X)[Y]/(Y^2-X^3-aX-b) \end{array}$$

vor, wobei die vertikalen Einbettungen den Grad 2 haben. Aufgrund der Gradformel genügt es, den Grad der oberen Körpererweiterung zu bestimmen. Dieser ist das behauptete Maximum nach Lemma 13.3. $\square$

Abbildungsverzeichnis