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

Elliptische Kurven

Vorlesung 17

Das Geschlecht einer Kurve

In diesem Kurs arbeiten wir nahezu ausschließlich mit elliptischen Kurven in dem Sinne, dass wir darunter eine glatte kubische Kurve in der projektiven Ebene verstehen. Dies hat den Vorteil, dass wir mit einfachen Gleichungen arbeiten können, dass wir auf geometrisch nachvollziehbare Weise eine Gruppenstruktur erhalten, dass wir direkt Fragestellungen zu K-rationalen Punkten (insbesondere bei $K = \mathbb{Q}$ und endlichen Körpern, siehe auch die folgenden Vorlesungen), angehen können. Es gibt aber auch andere Möglichkeiten, eine elliptische Kurve zu definieren, die den Fokus auf andere Aspekte legen. In der komplexen Situation haben wir gesehen, dass die komplexe Tori eine bestimmte topologische Gestalt besitzen, nämlich eben Tori sind. Generell sind komplexe glatte projektive Kurven, aufgefasst als reell-zweidimensionale kompakte orientierte Mannigfaltigkeiten, topologisch betrachtet einfach Kugeloberflächenn, die man mit einer bestimmten Anzahl an Henkeln versehen hat. Diese Anzahl nennt man das *topologische Geschlecht* der Fläche bzw. der komplexen Kurve. Komplex-elliptische Kurven besitzen also das topologische Geschlecht 1. Es erhebt sich die Frage, ob man rein algebraisch das Geschlecht einer glatten projektiven Kurve definieren kann, welche Relevanz das besitzt und was dann Geschlecht 1 bedeutet. Wir werden hier, weitgehend ohne Beweise, zwei Möglichkeiten vorstellen, wie man das Geschlecht algebraisch definieren kann, und dabei erläutern, dass Geschlecht 1 genau den elliptischen Kurven entspricht.

Definition 17.1. Zu einer glatten projektiven Kurve C über einem algebraisch abgeschlossenen Körper K nennt man

$$g := \dim_K \left(H^0\big(C, \Omega_{C|K}\big) \right)$$

das *differentielle Geschlecht* der Kurve.

Beim differentiellen Geschlecht geht es also um die maximale Anzahl an linear unabhängigen globalen Differentialformen auf der Kurve. Auf einer Varietät bilden die Differentialformen eine Garbe, die globalen Differentialformen sind einfach die globalen Schnitte davor. Ohne den Garbenbegriff kann man das für eine Kurve C mit Funktionenkörper $Q(C)$ auch so formulieren: Es geht um die rationalen Differentialformen, also Elemente aus $\Omega_{Q(C)|K}$, die in jedem Punkt $P \in C$ zu $\Omega_{\mathcal{O}_{C,P}|K}$ gehören. Nach Lemma 16.5 ist das differentielle Geschlecht einer elliptischen Kurve gleich 1, die bis auf skalare Vielfache einzige globale Differentialform ist, wenn die Kurve in Weierstraß-Form $y^2 = x^3 + ax + b$ gegeben ist,

$$\frac{dy}{3x^2 + a} = \frac{dx}{2y}.$$

Auf der projektiven Geraden gibt es außer der 0 keine globalen Differentialformen, ihr differentielles Geschlecht ist also 0.

Da die Garbe $\Omega_{C|K}$ invertierbar ist, bedeutet differentielles Geschlecht 1 direkt, dass der zu einer nichttrivialen Differentialform $\omega \in H^0\big(C, \Omega_{C|K}\big)$ definierte Garbenhomomorphismus

$$\mathcal{O}_C \longrightarrow \Omega_{C|K}$$

sogar ein Isomorphismus ist, da dies eindimensional lokal stets gilt. In diesem Fall ist also die Garbe der Kähler-Differentiale, die man auch die *kanonische Garbe* nennt, isomorph zur Strukturgarbe.

Definition 17.2. Zu einer glatten projektiven Kurve C über einem algebraisch abgeschlossenen Körper K nennt man

$$g := \dim_K \left(H^1(C, \mathcal{O}_C)\right)$$

das *Geschlecht* der Kurve.

In Abgrenzung zum differentiellen Geschlecht spricht man auch vom kohomologischen Geschlecht. Die sogenannte Serre-Dualität besagt, dass beide Arten, das Geschlecht zu definieren, übereinstimmen. Es ist ein erheblicher Aufwand, Kohomologie von Garben auf Varietäten (und allgemeiner) zu definieren. Für eine projektive Kurve kann man Kohomologie für quasikohärente Garben über ?ech-Kohomologie direkt und effektiv einführen. Die Kurve C wird überdeckt durch zwei offene affine Teilmengen U und V, eine elliptische Kurve in Weierstraßform beispielsweise durch $D_+(Z)$ und $D_+(Y)$. Die erste Kohomologie (höhere Kohomologien gibt es im Kurvenfall nicht, die nullte Kohomologie ist die globale Auswertung) einer quasikohärenten Garbe $\mathcal{F}$ (dazu gehört die Strukturgarbe, die Garbe der Differentialformen, alle invertierbaren Garben) ist der Kokern der zusammengesetzten Restriktionsabbildung

$$H^0(U, \mathcal{F}) \oplus H^0(V, \mathcal{F}) \longrightarrow H^0(U \cap V, \mathcal{F}).$$

Die universellen Beschreibungen der Kohomologie sichern, dass das Ergebnis unabhängig von der gewählten Überdeckung ist. Für projektive Varietäten

sind sämtliche Kohomologien von quasikohärenten Moduln nach Satz 27.6 (Bündel, Garben und Kohomologie (Osnabrück 2019-2020)) endlichdimensional, was der Hauptgrund ist, warum man mit Kohomologie sinnvolle Invarianten definieren kann. Im Allgemeinen ist die Berechnung von Kohomologien schwierig, es gibt aber auch viele erfolgreiche Techniken. Ein wichtiger Satz bezieht sich auf ebene Kurven.

Satz 17.3. *Es sei $C = V_+(f) \subset \mathbb{P}^2_K$ eine ebene projektive Kurve über einem algebraisch abgeschlossenen Körper K vom Grad d. Dann ist*

$$\dim_K \left(H^1(C, \mathcal{O}_C) \right) = \frac{(d-1)(d-2)}{2}.$$

Insbesondere ergibt sich bei $d = 1, 2$ das Geschlecht 0, und in der Tag liegt hier jeweils eine projektive Gerade vor. Bei $d = 3$ ist das Geschlecht 1. Elliptische Kurven, definiert als glatte kubische Kurven, haben also das Geschlecht 1.

Bemerkung 17.4. Für eine ebene projektive Kurve vom Grad d lässt sich die Kohomologiegruppe zur Strukturgarbe explizit angeben. Wenn

$$C = V_+(F)$$

und F die Form Z^n + andere Terme besitzt, so ist

$$\begin{aligned} H^1(C, \mathcal{O}_C) &= \operatorname{Kokern} \left(((K[X,Y,Z]/(F))_X)_0 \oplus ((K[X,Y,Z]/(F))_Y)_0 \right. \\ &\quad \left. \longrightarrow ((K[X,Y,Z]/(F))_{XY})_0 \right). \end{aligned}$$

Dabei ist

$$R = K[X,Y,Z]/(F)$$

der homogene Koordinatenring der Kurve, wobei die Nenneraufnahme an X (bzw. Y bzw. XY) gemacht wird und davon die nullte homogene Komponente genommen wird. Bei F vom Grad 3 ist die Kohomologie gleich $K\frac{Z^2}{XY}$. Die Kohomologieklasse $\frac{Z^2}{XY}$ lässt sich nicht als Summe von Elementen aus $(R_X)_0$ und $(R_Y)_0$ ausdrücken. Dagegen ist beispielsweise in der Kohomologiegruppe unter Verwendung der Kurvengleichung

$$Z^3 = XG + YH$$

mit $G, H \in K[X,Y,Z]$ vom Grad 2

$$\begin{aligned} \frac{Z^3}{X^2Y} &= \frac{XG+YH}{X^2Y} \\ &= \frac{XG}{X^2Y} + \frac{YH}{X^2Y} \\ &= \frac{G}{XY} + \frac{H}{X^2} \\ &= \frac{aZ^2 + bX^2 + cY^2 + dXY + eXZ + fYZ}{XY} = \frac{aZ^2}{XY}, \end{aligned}$$

d.h. $\frac{Z^3}{X^2Y}$ ist ein Vielfaches von $\frac{Z^2}{XY}$.

Bei F vom Grad 4 wird die Kohomologie durch die Basiselemente

$$\frac{Z^2}{XY}, \frac{Z^3}{X^2Y}, \frac{Z^3}{XY^2}$$

erzeugt.

Bemerkung 17.5. Es seien F und G zwei Quadriken in vier Variablen, also homogene Polynome vom Grad 2. Jede definiert eine projektive Fläche

$$V_+(F), V_+(G) \subseteq \mathbb{P}^3_K$$

im projektiven Raum. Wenn die beiden Flächen keine Komponente gemeinsam haben, so ist ihr Durchschnitt

$$C = V_+(F,G) = V_+(F) \cap V_+(G)$$

eindimensional, also eine projektive Kurve, die im projektiven Raum liegt. Wenn beide Flächen irreduzibel sind, so bedeutet die Komponentenbedingung einfach, dass die Flächen verschieden sind. Die Kurve C kann wieder glatt sein oder Singularitäten besitzen, was wiederum angelehnt an den Satz über implizite Abbildungen durch ein Jacobikriterium definiert wird, siehe Definition .. Wenn nun der Durchschnitt C der beiden Quadriken glatt ist, so kann man relativ einfach zeigen, dass das Geschlecht dieser Raumkurve gleich 1. Völlig andere Fragen sind es, ob es für eine solche Kurve auch eine ebene kubische Realisierung gibt und ob es darauf eine Gruppenstruktur gibt.

In dieser Situation zeigt sich eine typische Strategie der algebraischen Geometrie. Zuerst ordnet man den irgendwie gegegeben geometrischen Objekten Invarianten zu. Diese sind zumeist kohomologischer Natur, entscheidend ist, dass diese dem Objekt intrinsisch zukommen und unabhängig von der gewählten Einbettung sind. Sodann fragt man sich in einem davon unabhängigen Schritt, welche Eigenschaften durch die Invarianten festgelegt sind und wie man Objekte mit fixierten Invarianten möglicht einfach realisieren kann.

Im Beispiel vom Durchschnitt von zwei Quadriken erhält man also, dass das kohomologische Geschlecht 1 ist (was man ebenso und unabhängig von der Serre-Dualität für das differentielle Geschlecht beweisen kann). Dann fragt man sich, welche Schlussfolgerungen für Kurven, die das Geschlecht 1 besitzen, erzielen kann. Hier ist insbesondere die Auswirkung des Geschlechtes auf die Anzahl von Schnitten von Geradenbündeln und auf die Divisorenklassegruppe der Kurve wichtig. In der Tat ergibt sich, dass man jede Kurve vom Geschlecht 1 kubisch realisieren kann und es darauf eine Gruppenstruktur gibt.

Der folgende Satz heißt Satz von Riemann-Roch. Es bezeichnet darin h^0 bzw. h^1 die Dimension der zugehörigen Kohomologiegruppen, der Grad einer invertierbaren Garbe ist der Grad der zugehörigen Weildivisorklasse.

Satz 17.6. *Es sei C eine irreduzible glatte projektive Kurve über einem algebraisch abgeschlossenen Körper K vom Geschlecht g und sei $\mathcal{L}$ eine invertierbare Garbe auf C. Dann ist*

$$h^0(C,\mathcal{L}) - h^1(C,\mathcal{L}) = \operatorname{Grad}(\mathcal{L}) + 1 - g.$$

Dieser Satz beherrscht die Frage, wie viele globale Schnitte eine invertierbare Garbe besitzt. Es gibt eine im Allgemeinen schwierige Beziehung zwischen einer geometrischen Realisierung (einer projektiven Einbettung) und dem Geschlecht. Eine invertierbare Garbe $\mathcal{L}$ auf einer Kurve C und ein System von globalen Schnitten (typischerweise eine Basis) $s_0, s_1, \ldots, s_n \in \Gamma(C,\mathcal{L}) = H^0(C,\mathcal{L})$ definiert einen Morphismus

$$C \longrightarrow \mathbb{P}^n_K.$$

Satz 17.7. *Es sei $\mathcal{L}$ eine invertierbare Garbe auf einer glatten projektiven Kurve C über einem algebraisch abgeschlossenen Körper K vom Geschlecht g. Es sei*

$$\operatorname{Grad}(\mathcal{L}) \geq 2g+1.$$

Dann definieren die globalen Schnitte von $\mathcal{L}$ eine abgeschlossene Einbettung

$$C \longrightarrow \mathbb{P}^N_K.$$

Definition 17.8. Eine glatte projektive Kurve C über einem algebraisch abgeschlossenen Körper K vom Geschlecht 1 nennt man *elliptische Kurve*.

Die erste Kohomologie $H^1(C,\mathcal{O}_C)$ muss also eindimensional sein. Eine glatte kubische Kurve besitzt nach Satz 17.3 das Geschlecht 1. Wenn man wie oben eine elliptische Kurve durch das Geschlecht definiert, so ist es keineswegs klar, dass sie eine kubische Realisierung besitzt. Beispielsweise besitzt wie in Bemerkung 17.5 erläutert der Durchschnitt im $\mathbb{P}^3_K$ von zwei Flächen vom Grad 2 im glatten Fall ebenfalls das Geschlecht 1, und diese geometrische Realisierung legt nicht nahe, dass es auch eine ebene kubische Realisierung gibt. Aus Satz 17.7 folgt für eine elliptische Kurve das folgende Einbettungsresultat.

Satz 17.9. *Es sei $\mathcal{L}$ eine invertierbare Garbe auf einer elliptischen Kurve über einem algebraisch abgeschlossenen Körper. Es sei* $\operatorname{Grad}(\mathcal{L}) = 3$. *Dann definieren die globalen Schnitte von $\mathcal{L}$ eine abgeschlossene Einbettung*

$$C \longrightarrow \mathbb{P}^2_K.$$

Das Bild ist eine kubische Kurve.

Beweis. Dass eine Einbettung ist ein Spezialfall von Satz 17.7. Es seien $r,s,t \in \Gamma(C,\mathcal{L})$ unabhängige Schnitte, die unter der Einbettung den Variablen x,y,z entsprechen. In $\Gamma(C,\mathcal{L}^2)$ gibt es die Schnitte $r^2, s^2, t^2, rs, rt, st$. Zwischen diesen besteht keine Relation, da andernfalls das Bild der Kurve eine quadratische Relation erfüllen würde, doch dann wäre sie eine projektive Gerade. In $\Gamma(C,\mathcal{L}^3)$ gibt es die Schnitte $r^3, s^3, t^3, rs^2, rt^2, rst, rs^2, rt^2, s^2t, st^2$.

Nach Satz 17.6 und Serre-Dualität ist der Raum aber neundimensional. Deshalb muss es eine lineare Relation zwischen diesen zehn Termen geben, und dies ist die kubische Relation, die das Bild der Kurve erfüllt. □

Satz 17.10. *Es sei K ein algebraisch abgeschlossener Körper und sei C eine irreduzible glatte projektive Kurve über K. Dann sind folgende Aussagen äquivalent.*

(1) *Das kohomolgische Geschlecht von C ist* 1.
(2) *Das differentielle Geschlecht von C ist* 1.
(3) *C besitzt eine Realisierung als glatte kubische Kurve.*
(4) *C besitzt die Struktur einer Gruppenvarietät.*

Beweis. Wir skizzieren die wesentlichen Argumente. Die Äquivalenz von (1) und (2) ist Serre-Dualität. Von (1) nach (3) ist Satz 17.9. Von (3) nach (4) ist Satz 6.3 und Satz 6.5. Von (4) nach (1). Hier zeigt man vergleichbar mit Korollar 16.8, dass das Tangentialbündel auf C trivial ist. □

Abbildungsverzeichnis