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

Elliptische Kurven

Vorlesung 14

Isogenien

DEFINITION 14.1. Es seien E_1 und E_2 elliptische Kurven über einem Körper K. Eine *Isogenie* ist ein Morphismus

$$\varphi\colon\ E_1 \longrightarrow E_2$$

mit $\varphi(\mathfrak{O}_1) = \mathfrak{O}_2$.

Die konstante Abbildung mit dem Wert $\mathfrak{O}_2$ betrachten wir hier als eine Isogenie, die Konventionen sind unterschiedlich. Oft wird diese konstante Abbildung nicht als Isogenie angesehen und nur unsere nichtkonstanten Isogenien gelten als Isogenie. So oder so sind die nichtkonstanten Isogenien interessant.

Anders als in der Definition 10.5 von Isogenien zwischen komplexen Tori wird hier nicht verlangt, dass eine Isogenie ein Gruppenhomomorphismus ist. Allerdings werden wir in Satz 15.8 beweisen, dass die Isogenien im algebraischen Sinn stets Gruppenhomomorphismen sind.

Als eine nichtkonstante Abbildung zwischen projektiven Kurven ist nach Satz 7.11 eine nichtkonstante Isogenie eine surjektive endliche Abbildung von einem bestimmten Grad, und der Grad stimmt mit dem Grad der Körpererweiterung $Q(E_2) \subseteq Q(E_1)$ überein. Wir betrachten zunächst Isogenien auf einer elliptischen Kurve E, die unmittelbar mit der Gruppenstruktur auf E zusammenhängen. Zu jeder (additiv geschriebenen) kommutativen Gruppe G und jeder ganzen Zahl n ist durch

$$G \longrightarrow G,\ x \longmapsto nx,$$

ein Gruppenendomorphismus gegeben. Bei $n = 1$ ist dies die Identität, bei $n = -1$ die Negation und bei $n = 0$ die konstante Abbildung auf 0. Der Kern ist die Menge

$$\{x \in G \mid nx = 0\}$$

der *Torsionselemente* zur Ordnung n.

Bei einem komplexen Torus über den komplexen Zahlen $E = \mathbb{C}/\Gamma$ zu einem Gitter $\Gamma \subseteq \mathbb{C}$ und $n \in \mathbb{N}_+$ liegt die Untergitterbeziehung $n\Gamma \subseteq \Gamma$ und das kommutative Diagramm

$$\begin{array}{ccc} \mathbb{C} & \stackrel{n}{\longrightarrow} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Gamma & \stackrel{[n]}{\longrightarrow} & \mathbb{C}/\Gamma\ . \end{array}$$

von Gruppenhomomorphismen vor, vergleiche Lemma 10.6. Dabei ist die obere horizontale Abbildung bijektiv und die untere horizontale Abbildung surjektiv mit dem Kern

$$\left\{ i\frac{u}{n} + j\frac{v}{n} \mid i,j = 0,1,\ldots,n-1 \right\},$$

wenn u und v eine Basis des Gitters bezeichnet, siehe Lemma 10.6. Insbesondere besteht der Kern von $[n]$ aus n^2 Elementen. Allgemeiner besteht das Urbild unter $[n]$ zu $Q \in \mathbb{C}/\Gamma$ aus

$$\left\{ P + i\frac{u}{n} + j\frac{v}{n} \mid i,j = 0,1,\ldots,n-1 \right\}$$

wenn P ein Urbild ist. Insbesondere bestehen sämtliche Urbilder ebenfalls aus n^2 Elementen was bedeutet, dass der Grad dieser Abbildung gleich n^2 ist.

Nach Lemma 7.14 sind die Multiplikationen $[m]\colon E \to E$ Morphismen und damit Isogenien. Auch die Gradeigenschaft gilt über jedem Körper.

Satz 14.2. *Es sei E eine elliptische Kurve über einem Körper K und $m \in \mathbb{N}_+$. Dann ist der Grad der Multiplikationsabbildung*

$$[m]\colon E \longrightarrow E,\, P \longmapsto mP,$$

gleich m^2.

Beweis. Nach Korollar 6.8 wird die m-te Vervielfachung durch $(f_m, q_m y)$ mit rekursiv definierten rationalen Funktionen $f_m, q_m \in K(x)$ beschrieben. Mit erheblichem Aufwand kann man zeigen, dass der Grad des Zählers von f_m gleich m^2 und der Grad des Nenners kleiner ist. Dann kann man mit Lemma 13.11 schließen. □

Insbesondere sind die Multiplikationsabbildungen nicht konstant, wobei allerdings eventuell alle K-Punkte auf $\mathfrak{O}$ abgebildet werden können.

Lemma 14.3. *Es seien*

$$\varphi_1, \varphi_2\colon E_1 \longrightarrow E_2$$

Isogenien zwischen den elliptischen Kurven E_1 und E_2. Dann ist auch

$$\varphi_1 + \varphi_2\colon E_1 \longrightarrow E_2$$

eine Isogenie.

Beweis. Dies folgt aus

$$E_1 \stackrel{\varphi_1 \times \varphi_2}{\longrightarrow} E_2 \times E_2 \stackrel{+}{\longrightarrow} E_2\,.$$

da die Hintereinanderschaltung von Morphismen wieder ein Morphismus ist und $\mathfrak{O}_1$ insgesamt auf $\mathfrak{O}_2$ abgebildet wird. □

DEFINITION 14.4. Zu elliptischen Kurven E_1 und E_2 über einem Körper K bezeichnet

$$\mathrm{Hom}_K(E_1, E_2) = \{\varphi : E_1 \to E_2 \mid \varphi \text{ Isogenie } \}$$

die Gruppe der Isogenien von E_1 nach E_2 zusammen mit der konstanten Abbildung nach $\mathfrak{O}$.

DEFINITION 14.5. Zu einer elliptischen Kurve E über dem Körper K nennt man

$$\mathrm{End}(E) = \{f : E \to E \mid f \text{ Isogenie } \}$$

mit der Addition und der Hintereinanderschaltung von Isogenien den *Endomorphismenring* von E.

Es handelt sich in der Tat um einen Ring, wobei alle Eigenschaften bis auf die Distributivität klar sind. Diese wird sich aus Satz 15.8 ergeben, siehe Aufgabe 15.4. Der Endomorphismenring enthält die ganzen Zahlen als Unterring, und zwar entspricht der Zahl n die Multiplikationsabbildung mit n. Es ist eine wichtige Frage, wann es über diese Multiplikationsabbildungen hinaus weitere Isogenien gibt.

Weildivisoren

Wir haben in Beispiel 7.2 gesehen, dass es für eine rationale Funktion auf einer elliptischen Kurve keine eindeutige Darstellung als Bruch gibt. Dies hängt damit zusammen, dass der affine (und auch homogene) Koordinatenring der elliptischen Kurve nicht faktoriell ist. Ein Maß für die Nichtfaktorialität eines Ringes und einer Varietät wird durch die Divisorenklassengruppe beschrieben, die auch in der algebraischen Zahlentheorie eine wichtige Rolle spielt.

Eine rationale Funktion $\neq 0$ auf einer glatten Kurve C besitzt in jedem Punkt P eine Ordnung, die sich über die Ordnung im zugehörigen diskreten Bewertungsring $\mathcal{O}_P$ ergibt. Sie ist positiv, wenn dort eine Nullstelle vorliegt, und die negativ ist, wenn dort eine Polstelle vorliegt. Bis auf endlich viele Punkte ist die Ordnung gleich 0, das Null- und Polstellenverhalten einer Funktion wird also vollständig dadurch beschrieben, dass einer endlichen Punktemenge ganze Zahlen zugeordnet sind. Man kann sich umgekehrt fragen, ob eine solche Vorgabe durch eine rationale Funktion realisiert werden kann. Dies ist die Idee der Weildivisoren.

DEFINITION 14.6. Es sei C eine irreduzible glatte Kurve über einem algebraisch abgeschlossenen Körper K. Unter einem *Weildivisor* versteht man eine formale endliche Summe $D = \sum_{P \in C} n_P P$.

Die Menge der Weildivisoren bildet eine Gruppe.

DEFINITION 14.7. Es sei C eine irreduzible glatte Kurve über einem algebraisch abgeschlossenen Körper K und sei $f \in Q(C)$, $f \neq 0$, ein Element des

Funktionenkörpers. Man nennt $\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f) P$ den *Hauptdivisor* zu f.

DEFINITION 14.8. Zwei Divisoren D, E auf einer glatten Kurve C über einem algebraisch abgeschlossenen Körper K heißen *linear äquivalent*, wenn $D - E$ ein Hauptdivisor ist.

LEMMA 14.9. *Es sei C eine irreduzible glatte Kurve über einem algebraisch abgeschlossenen Körper K mit Funktionenkörper $Q(C)$. Dann ist die Zuordnung*

$$Q(C)^\times \longrightarrow \operatorname{Div}(C),\ f \longmapsto \operatorname{div}(f),$$

ein Gruppenhomomorphismus.

Beweis. Siehe Aufgabe 14.10. □

DEFINITION 14.10. Es sei C eine irreduzible glatte Kurve über einem algebraisch abgeschlossenen Körper K mit Funktionenkörper $Q(C)$. Dann nennt man die Restklassengruppe

$$\operatorname{DKG}(C) = \operatorname{Div}(C)/\operatorname{HDiv}(C)$$

die *Divisorenklassengruppe* von C.

DEFINITION 14.11. Es sei C eine glatte projektive Kurve über einem algebraisch abgeschlossenen Körper K. Zu einem Weildivisor $D = \sum_{P \in C} n_P P$ auf C ist der *Grad* als

$$\deg(D) := \sum_{P \in C} n_P$$

definiert.

Der Rückzug eines Weildivisors

DEFINITION 14.12. Zu einem nichtkonstanten Morphismus

$$\varphi\colon C_1 \longrightarrow C_2$$

zwischen glatten Kurven über einem algebraisch abgeschlossenen Körper und einem Weildivisor $D = \sum_P a_P \cdot P$ auf C_2 nennt man

$$\varphi^* D := \sum_{Q \in C_1} \operatorname{Verz}(Q|\varphi(Q)) a_{\varphi(Q)} \cdot Q$$

den *zurückgezogenen Weildivisor*.

Insbesondere gilt für einen Punkt $P \in C$

$$\varphi^* P = \sum_{Q \in \varphi^{-1}(P)} \operatorname{Verz}(Q|P) \cdot Q.$$

Die Abbildung

$$\varphi^*\colon \operatorname{Div}(C_2) \longrightarrow \operatorname{Div}(C_1)$$

ist ein Gruppenhomomorphismus.

SATZ 14.13. *Zu einem nichtkonstanten Morphismus*

$$\varphi\colon C_1 \longrightarrow C_2$$

zwischen irreduziblen glatten Kurven über einem algebraisch abgeschlossenen Körper und einem Hauptdivisor $D = \sum_P a_P \cdot P = \operatorname{div}(q)$ *auf* C_2 *mit* $q \in Q(C_2)$, $q \neq 0$, *stimmt der zurückgezogene Divisor* $\varphi^*(D)$ *mit dem Hauptdivisor zu* $q \in Q(C_1)$ *auf* C_1 *überein.*

Beweis. Wegen der Nichtkonstanz gehört zu φ eine Körpererweiterung

$$Q(C_2) \subseteq Q(C_1)$$

und zu jedem Punkt $Q \in C_1$ liegt ein kommutatives Diagramm

$$\begin{array}{ccc} \mathcal{O}_{C_2,\varphi(Q)} & \longrightarrow & \mathcal{O}_{C_1,Q} \\ \downarrow & & \downarrow \\ Q(C_2) & \longrightarrow & Q(C_1) \end{array}$$

von injektiven Ringhomomorphismen vor, wobei in der ersten Zeile diskrete Berwertungsringe stehen. Wenn

$$q = u\pi_2^n$$

mit einer Einheit $u \in \mathcal{O}_{C_2,\varphi(Q)}$ und einer Ortsuniformisierenden

$$\pi_2 \in \mathcal{O}_{C_2,\varphi(Q)}$$

gilt, so ist

$$q = u\pi_2^n = u\Big(u'\pi_1^{\operatorname{Verz}(Q|\varphi(Q))}\Big)^n = uu'\pi_1^{n\operatorname{Verz}(Q|\varphi(Q))}$$

mit einer Orstuniformisierenden π_1 von $\mathcal{O}_{C_1,Q}$, woraus die Aussage folgt. □

Die vorstehende Aussage sichert, dass

$$\varphi\colon C_1 \longrightarrow C_2$$

einen Gruppenhomomorphismus

$$\operatorname{DKG}(C_2) \longrightarrow \operatorname{DKG}(C_1)$$

induziert.

KOROLLAR 14.14. *Es sei* C *eine glatte irreduzible Kurve über einem algebraisch abgeschlossenen Körper* K *und sei* Q *der Funktionenkörper von* C. *Es sei* $q \in Q$, $q \notin K$, *und*

$$q\colon C \longrightarrow \mathbb{P}^1_K$$

der nach Lemma 7.13 zugehörige Morphismus zu einem Element $q \in Q$. *Dann gilt für den zurückgezogenen Divisor*

$$q^*((0) - (\infty)) = \operatorname{div}(q).$$

Beweis. Der Funktionenkörper der projektiven Geraden

$$\mathbb{P}^1_K = \operatorname{Proj}(K[X,Y])$$

ist $K(t)$ mit $t = \frac{Y}{X}$. Die Erweiterung der Funktionenkörper ist durch

$$K(t) \longrightarrow Q(C),\ t \longmapsto q,$$

gegeben. Der Hauptdivisor zu t auf $\mathbb{P}^1_K$ ist $(0) - (\infty) = (Y) - (X)$, wobei zwei Beschreibungsmöglichkeiten für die Punkte verwendet wurden. Daher folgt die Aussage aus Satz 14.13. □

Satz 14.15. *Es sei C eine glatte projektive Kurve über einem algebraisch abgeschlossenen Körper K. Dann ist der Grad eines Hauptdivisors gleich* 0.

Beweis. Für $q \neq 0$ konstant ist die Aussage klar. Sei also q nicht konstant. Wir betrachten den im Sinne von Lemma 7.13 zugehörigen endlichen Morphismus

$$q\colon\ C \longrightarrow \mathbb{P}^1_K$$

vom Grad n. Nach Korollar 14.14 ist

$$\operatorname{div}(q) = q^*((0) - (\infty)) = q^*(0) - q^*(\infty).$$

Nach Satz 13.2 besitzen die beiden schematheoretischen Fasern beide die K-Dimension n und diese ist die Gesamtmultiplizität der Faser. □

Die vorstehenden Resultate erlauben folgende Definition.

Definition 14.16. Es sei C eine glatte projektive Kurve über einem algebraisch abgeschlossenen Körper K. Man nennt

$$\mathrm{DKG}_0(C) = \operatorname{Div}_0(C)/\operatorname{HDiv}(C)$$

die *Divisorenklassengruppe vom Grad 0* zu C.

Abbildungsverzeichnis