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

Elliptische Kurven

Vorlesung 15

Der Vorschub eines Weildivisors

DEFINITION 15.1. Zu einem nichtkonstanten Morphismus

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

zwischen glatten Kurven über einem algebraisch abgeschlossenen Körper und einem Weildivisor $D = \sum_P n_P \cdot P$ auf C_1 nennt man

$$\varphi_* D := \sum_{P \in C_1} n_P \varphi(P) = \sum_{Q \in C_2} \left(\sum_{P \in \varphi^{-1}(Q)} n_P \right) Q$$

den *vorgeschobenen Weildivisor*.

Die entscheidende Eigenschaft ist, dass ein Punkt $P \in C_1$ auf den Punkt $\varphi(P) \in C_2$ abgebildet wird, dies legt den Gruppenhomomorphismus φ_* fest.

LEMMA 15.2. *Es sei $\varphi\colon C_1 \to C_2$ ein endlicher Morphismus vom Grad d zwischen irreduziblen, glatten Kurven. Dann gelten die folgenden Eigenschaften.*

(1) *Zu einem weiteren endlichen Morphismus $\psi\colon C_2 \to C_3$ ist $(\psi \circ \varphi)_* = \psi_* \circ \varphi_*$.*
(2) *Zu einem Divisor D auf C_1 ist*
$$\operatorname{Grad}(\varphi_* D) = \operatorname{Grad}(D).$$
(3) *Zu einem Weildivisor D auf C_2 ist*
$$\varphi_*(\varphi^*(D)) = d \cdot D.$$

Beweis. (1) ist klar, bei (2) und (3) genügt es, die Aussagen für einen einzelnen Punkt zu zeigen. (2) ist dann klar, (3) folgt aus Satz 13.2. □

LEMMA 15.3. *Es sei $\varphi\colon C_1 \to C_2$ ein endlicher Morphismus vom Grad d zwischen irreduziblen, glatten Kurven, die zugehörige Körpererweiterung der Funktionenkörper sei galoissch mit Galoisgruppe G.*

(1) *Zu einem Weildivisor D auf C_1 ist*
$$\varphi_*(D) = \varphi_*(\sigma_*(D))$$
für $\sigma \in G$.
(2) *Zu $g \in Q(C_2)$, $g \neq 0$, ist*
$$\varphi_* \operatorname{div}(g) = d \cdot \operatorname{div}(g)$$

(3) *Zu einem Hauptdivisor* $\operatorname{div}(f)$ *mit* $f \in Q(C_1)$, $f \neq 0$, *ist*

$$\varphi_*(\operatorname{div}(f)) = \operatorname{div}(N(f)),$$

wobei $N(f)$ *die Norm bezeichnet.*

Beweis. Wegen der Endlichkeit der Abbildung operiert die Galoisgruppe auf C_1, siehe Satz 21.2 (Algebraische Zahlentheorie (Osnabrück 2020-2021)). (1) folgt direkt aus der Funktorialität des Vorschubs. (2) ergibt sich unter Verwendung von Lemma 15.2 (3) und Satz 14.13 mit

$$\varphi_* \operatorname{div}(g) = \varphi_*\varphi^*(\operatorname{div}(g)) = d \cdot \operatorname{div}(g).$$

(3). Es ist

$$N(f) = \prod_{\sigma \in G} \sigma \circ f.$$

In der Divisorengruppe zu C_1 gilt

$$\operatorname{div}(N(f)) = \sum_{\sigma} \operatorname{div}(\sigma \circ f)$$

und daher ist nach (2) und (1)

$$d \cdot \operatorname{div}(N(f)) = \varphi_* \operatorname{div}(N(f)) = \sum_{\sigma} \varphi_* \operatorname{div}(\sigma \circ f) = d \cdot \varphi_* \operatorname{div}(f).$$

Da die Divisorengruppe torsionsfrei ist, folgt die Gleichheit. □

Lemma 15.4. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik p und sei $K \subseteq L$ eine Körpererweiterung des Transzendenzgrades 1 mit der zugehörigen glatten projektiven Kurve C_2 im Sinne von Satz 7.6. Das Element $a \in L$ besitze in L keine p-te Wurzel und sei $M = L[Y]/(Y^p - a)$ der dadurch gegebene Erweiterungskörper von L mit zugehöriger Kurve C_1 und dem zugehörigen endlichen Morphismus $\varphi\colon C_1 \to C_2$ im Sinne von Satz 7.12. Dann gilt für den Vorschub eines Hauptdivisors*

$$\varphi_*(\operatorname{div}(f)) = \operatorname{div}(f^p).$$

Beweis. Die Kurvenabbildung ist eine Bijektion mit Verzweigungsordnung p in jedem Punkt, die Erweiterung der diskreten Bewertungsringe ist durch $V \to V[X]/(X^p - b) = W$ mit einem $b \in V$ gegeben. Für eine Ortsuniformisierende $\pi_1 \in V$ ist $\pi_2 = u\pi_1^p$ mit einer Einheit u. Für $f \in W$ ist $f^p \in V$ und aus

$$f = v\pi_2^n$$

folgt direkt

$$f^p = v^p \pi_2^{pn} = v^p \pi_1^n,$$

die Ordnung von f oben stimmt also mit der Ordung von f^p unten überein. □

LEMMA 15.5. *Es sei $\varphi\colon C_1 \to C_2$ ein endlicher Morphismus vom Grad d zwischen irreduziblen, glatten Kurven. Dann werden unter dem Vorschub*

$$\varphi_*\colon \operatorname{Div}(C_1) \longrightarrow \operatorname{Div}(C_2),\ D \longmapsto \varphi_* D,$$

Hauptdivisoren auf Hauptdivisoren abgebildet. Insbesondere induziert der Morphismus einen Homomorphismus

$$\varphi_*\colon \operatorname{DKG}(C_1) \longrightarrow \operatorname{DKG}(C_2)$$

der Divisorenklassengruppen.

Beweis. Die Erweiterung der Funktionenkörper $\mathbb{Q}(C_2) \subseteq \mathbb{Q}(C_1)$ besitzt nach Lemma Anhang 7.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)) einen Zwischenkörper $\mathbb{Q}(C_2) \subseteq M \subseteq \mathbb{Q}(C_1)$ derart, dass $\mathbb{Q}(C_2) \subseteq M$ separabel und $M \subseteq \mathbb{Q}(C_1)$ rein-inseparabel ist. Dem entspricht gemäß Satz 7.12 eine Faktorisierung

$$C_1 \longrightarrow C \longrightarrow C_2\,.$$

Es genügt also, die Aussage für eine separable Kurvenabbildung und eine rein-inseparable Kurvenabbildung zu zeigen. Im zweiten Fall liegt eine Verknüpfung von Körpererweiterungen der in Lemma 15.4 beschriebenen Form vor, für diese wurde die Behauptung dort bewiesen.

Den separablen Fall kann man auf den Galoisfall zurückführen, der in Lemma 15.3 (3) behandelt wurde. Es sei $Q(C) \subseteq Q(C_1) \subseteq L$ insgesamt galoissch und $L = Q(C_0)$ mit einer weiteren Kurve C_0 endlich über C_1. Wir betrachten also die Situation

$$C_0 \xrightarrow{\psi} C_1 \xrightarrow{\theta} C\,.$$

Zu $D = \operatorname{div}(f)$ behaupten wir wieder

$$\theta_* D \;=\; \operatorname{div}\big(N_C^{C_1}(f)\big).$$

Es ist

$$\psi_*\psi^* \operatorname{div}(f) \;=\; \operatorname{Grad}(\psi) \cdot \operatorname{div}(f).$$

Nach Lemma 15.2 (3), Satz 14.13, Lemma 15.3 (3) und Gesetzen für die Norm ist

$$\begin{aligned}
\operatorname{Grad}(\psi) \cdot \theta_*(\operatorname{div}(f)) &= \theta_*(\operatorname{Grad}(\psi) \cdot \operatorname{div}(f)) \\
&= \theta_*(\psi_*\psi^* \operatorname{div}(f)) \\
&= (\theta_*\psi_*)(\operatorname{div}(f)) \\
&= \operatorname{div}\big(N_C^{C_0}(f)\big) \\
&= \operatorname{div}\big(N_C^{C_1}(f^{\operatorname{Grad}(\psi)})\big) \\
&= \operatorname{Grad}(\psi) \cdot \operatorname{div}\big(N_C^{C_1}(f)\big).
\end{aligned}$$

□

Weildivisoren auf elliptischen Kurven

LEMMA 15.6. *Es sei E eine elliptische Kurve über dem algebraisch abgeschlossenen Körper K mit dem Nullpunkt $\mathfrak{O} \in E$. Es seien $P_1, P_2 \in E$. Dann gibt es einen Punkt $A \in E$ derart, dass die Divisoren $P_1 + P_2$ und $\mathfrak{O} + A$ zueinander linear äquivalent sind.*

Beweis. Es sei $E = V_+(F) \subseteq \mathbb{P}^2_K$ mit F homogen vom Grad 3. Bei $P_1 \neq P_2$ betrachten wir die projektive Gerade $L \subseteq \mathbb{P}^2_K$ durch die beiden Punkte. Bei $P_1 = P_2$ betrachten wir die Tangente

$L \subseteq \mathbb{P}^2_K$ an den Punkt. Es wird L durch eine Linearform $\ell_1 \neq 0$ beschrieben. Der Weil-Divisor zu dieser Linearform ist $(\ell_1) = P_1 + P_2 + P_3$, da ja $E \cap L$ aus drei Punkten (mit Multiplizitäten) besteht. Die Punkte $P_3, \mathfrak{O}$ definieren in der gleichen Weise eine weitere Gerade und eine zugehörige Linearform ℓ_2 mit $(\ell_2) = P_3 + \mathfrak{O} + A$. Die Funktion $\frac{\ell_1}{\ell_2}$ ist eine rationale Funktion auf E und definiert den Hauptdivisor

$$\left(\frac{\ell_1}{\ell_2}\right) = P_1 + P_2 + P_3 - (P_3 + \mathfrak{O} + A) = P_1 + P_2 - \mathfrak{O} - A.$$

Damit ist $P_1 + P_2 = \mathfrak{O} + A$. □

SATZ 15.7. *Es sei E eine elliptische Kurve über dem algebraisch abgeschlossenen Körper K mit dem Nullpunkt $\mathfrak{O} \in E$. Dann ist die Abbildung*

$$E \longrightarrow \mathrm{DKG}_0(E),\ P \longmapsto P - \mathfrak{O},$$

ein Gruppenisomorphismus.

Beweis. Wir zeigen zuerst die Injektivität. Seien $P, Q \in E$ verschiedene Punkte. Wenn $P - \mathfrak{O}$ und $Q - \mathfrak{O}$ zueinander linear äquivalent sind, so sind auch P und Q zueinander linear äquivalent. Dann gibt es eine rationale Funktion f auf E mit $\mathrm{div}(f) = P - Q$. Wenn wir f als einen Morphismus nach $\mathbb{P}^1_K$ auffassen, so hat dieser nach Korollar 14.14 den Grad 1. Doch dann wäre die elliptische Kurve isomorph zu $\mathbb{P}^1_K$, was Satz 13.9 widerspricht.

Zum Nachweis der Surjektivität sei ein Divisor D vom Grad 0 gegeben, sagen wir $D = P_1 + P_2 + \cdots + P_n - Q_1 - Q_2 - \cdots - Q_n$, wobei Punkte mehrfach vorkommen können. Mit Hilfe von Lemma 15.6 kann man zeigen, dass dieser Divisor linear äquivalent zu

$$(n-1)\mathfrak{O} + A - ((n-1)\mathfrak{O} + B) = A - B.$$

Die Punkte A und $\mathfrak{O}$ definieren wie in Lemma 15.6 eine Gerade und einen dritten Schnittpunkt C. Ebenso definieren B und C eine Gerade und einen dritten Schnittpunkt D. Es ist dann

$$A - B \sim A - B + (B + C + D - A - \mathfrak{O} - C) = D - \mathfrak{O}.$$

Zum Nachweis der Homomorphie seien Punkte $P, Q \in E$ gegeben. Es sei L die durch P und Q gegebene Gerade mit der Linearform ℓ_1 und dem dritten

Schnittpunkt C und es sei L_2 die Gerade durch C und $\mathfrak{O}$ mit der Linearform ℓ_2 und dem dritten Schnittpunkt D. Nach Definition ist D gleich $P+Q$ in der Gruppenstruktur auf der elliptischen Kurve. In der Divisorenklassengruppe ist

$$\begin{aligned}[P]-[\mathfrak{O}]+[Q]-[\mathfrak{O}] &= [P]+[Q]-2[\mathfrak{O}] \\ &= [P]+[Q]-2[\mathfrak{O}]+[\mathfrak{O}]+[D]-[P]-[Q] \\ &= [D]-[\mathfrak{O}],\end{aligned}$$

es liegt also ein Gruppenhomomorphismus vor. □

Satz 15.8. *Es seien E_1, E_2 elliptische Kurven über einem Körper K und sei*

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

eine Isogenie. Dann ist φ ein Homomorphismus bezüglich der Gruppenstrukturen auf den Kurven.

Beweis. Wir können annehmen, dass K algebraisch abgeschlossen ist. Es liegt ein kommutatives Diagramm

$$\begin{array}{ccc} E_1 & \longrightarrow & \mathrm{DKG}_0(E_1) \\ \varphi\downarrow & & \downarrow\varphi_* \\ E_2 & \longrightarrow & \mathrm{DKG}_0(E_2) \end{array}$$

vor, da

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

ist. Die horizontalen Abbildungen sind nach Satz 15.7 Gruppenisomorphismen. Die vertikale Abbildung rechts ist nach Lemma 15.5 ein Gruppenhomomorphismus. Daher ist auch die vertikale Abbildung links ein Gruppenhomomorphismus. □

Unter étale kann man im folgenden Satz einfach überall unverzweigt verstehen.

Satz 15.9. *Es sei $\varphi\colon E_1 \to E_2$ eine separable Isogenie zwischen den elliptischen Kurven E_1 und E_2. Dann ist φ étale.*

Beweis. Aufgrund der Separabilität gibt es nach Satz 13.8 eine nichtleere offene affine Teilmenge $V \subseteq E_2$ derart, dass $\varphi^{-1}(V)$ auch affin ist und die eingeschränkte Abbildung

$$\varphi\colon \varphi^{-1}(V) \longrightarrow V$$

die Eigenschaft besitzt, dass der Kählermodul gleich 0 ist. Aus Satz 13.6 folgt somit, dass über einem jeden Punkt $Q \in V$ genau n Punkte liegen, wobei n den Grad der Kurvenabbildung bezeichnet. Es sei nun $Q' \in E_2$ ein beliebiger Punkt und sei $P' \in E_1$ ein Punkt oberhalb von Q'. Wir fixieren einen Punkt $P \in V$ und einen Punkt $Q \in E_1$ oberhalb von P. Wir betrachten die

Translation τ_1 auf E_1 von P nach P' und die Translation τ_2 auf E_2 von Q nach Q'. Nach Satz 15.8 gilt

$$\begin{aligned}\varphi(\tau_1(x)) &= \varphi(x+P'-P)\\ &= \varphi(x)+\varphi(P')-\varphi(P)\\ &= \varphi(x)+Q'-Q\\ &= \tau_2(\varphi(x)),\end{aligned}$$

d.h. das Diagramm

$$\begin{array}{ccc} E_1 & \xrightarrow{\tau_1} & E_1 \\ \varphi\downarrow & & \downarrow\varphi \\ E_2 & \xrightarrow{\tau_2} & E_2 \end{array}$$

kommutiert. D.h. durch τ_1 wird die Faser über Q isomorph in die Faser über Q' überführt und besteht auch aus genau n Punkten. □

KOROLLAR 15.10. *Es sei $\varphi\colon E_1 \to E_2$ eine separable Isogenie zwischen den elliptischen Kurven E_1 und E_2 über einem algebraisch abgeschlossenen Körper K. Dann ist*

$$\#\,(\ker\varphi) \;=\; \mathrm{Grad}\,(\varphi).$$

Beweis. Dies folgt aus Satz 15.9, da nach Satz 13.6 für einen étalen Morphismus zwischen glatten projektiven Kurven die Anzahl der Punkte in jeder Faser konstant gleich dem Grad ist. □

Abbildungsverzeichnis