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

Elliptische Kurven

Vorlesung 19

In den folgenden Vorlesungen werden wir den Satz von Mordell-Weil beweisen, der besagt, dass zu einer elliptischen Kurve E über einem Zahlbereich K die Gruppe der K-rationalen Punkte $E(K)$ eine endlich erzeugte Gruppe ist. Wir zeigen zuerst den sogenannten schwachen Satz von Mordell-Weil, der die Endlichkeit der Restklassengruppe $E(K)/2E(K)$ besagt. Mittels Höhenfunktionen werden wir darauf die endliche Erzeugtheit zurückführen können. Zu diesem Zweck müssen wir Bewertungen und Beträge auf Zahlkörpern studieren und die dadurch gegebenen Höhenfunktionen auf dem projektiven Raum und auf elliptischen Kurven verstehen.

Der schwache Satz von Mordell-Weil

Zu einer (additiv geschriebenen) Gruppe G bezeichnet $2G$ die Untergruppe derjenigen Elemente, die das Doppelte eines Elementes sind, die also eine Halbierung besitzen. Im Folgenden wird die Restklassengruppe $G/2G$ eine wichtige Rolle spielen. Bei der multiplikativen Gruppe eines Körpers ist dies die Restklassengruppe $K^\times/(K^\times)^2$, also die Gruppe der Einheiten modulo der Quadrate.

Definition 19.1. Es sei

$$Y^2 = (X-\lambda_1)(X-\lambda_2)(X-\lambda_3)$$

die Gleichung einer elliptischen Kurve E in Zerlegungsform über einem Körper K mit $\lambda_1, \lambda_2, \lambda_3 \in K$. Wir definieren die Abbildung (und entsprechend φ_2, φ_3)

$$\varphi_1 \colon E(K) \longrightarrow K^\times/\left(K^\times\right)^2$$

durch

$$\varphi_1(P) = \begin{cases} 1, \text{ wenn } P = \mathfrak{O}, \\ (\lambda_1-\lambda_2)(\lambda_1-\lambda_3), \text{ wenn } P = (\lambda_1, 0)\,, \\ x-\lambda_1 \text{ sonst } (P=(x,y))\,. \end{cases}$$

Lemma 19.2. *Es sei*

$$Y^2 = (X-\lambda_1)(X-\lambda_2)(X-\lambda_3)$$

die Gleichung einer elliptischen Kurve E in Zerlegungsform über einem Körper K mit $\lambda_1, \lambda_2, \lambda_3 \in K$. Dann ist die Abbildung

$$\varphi_1 \colon E(K) \longrightarrow K^\times/\left(K^\times\right)^2$$

ein Gruppenhomomorphismus.

Beweis. Seien (x_1, y_1) und (x_2, y_2) Punkte auf $E(K)$ (für den unendlich fernen Punkt sind kleine Sonderüberlegungen nötig). Es sei $y = \alpha x + \beta$ eine Gleichung für die Verbindungsgerade zwischen den beiden Punkten bzw. der Tangente. Die Schnittpunkte dieser Geraden mit der Kurve sind durch die Bedingung

$$(\alpha x + \beta)^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$$

gegeben. Dies wird durch x_1 und x_2 und von der x-Koordinate des dritten Schnittpunktes und des Summenpunktes (x_3, y_3) erfüllt. Es ist also

$$(x - \lambda_1)(x - \lambda_2)(x - \lambda_3) - (\alpha x + \beta)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Wenn man darin $x = \lambda_1$ setzt, so erhält man

$$(\alpha\lambda_1 + \beta)^2 = (x_1 - \lambda_1)(x_2 - \lambda_1)(x_3 - \lambda_1),$$

also ist

$$x_3 - \lambda_1 = \frac{(\alpha\lambda_1 + \beta)^2}{(x_1 - \lambda_1)(x_2 - \lambda_1)} = (x_1 - \lambda_1)(x_2 - \lambda_1)$$

modulo der Quadrate. □

Satz 19.3. *Es sei*

$$Y^2 = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3)$$

die Gleichung einer elliptischen Kurve E in Zerlegungsform über einem Körper K mit $\lambda_1, \lambda_2, \lambda_3 \in K$. Dann ist ein Punkt $(x, y) \in E(K)$ genau dann ein Verdoppelungspunkt auf $E(K)$, also von der Form

$$(x, y) = 2(z, w) = (z, w) + (z, w)$$

mit $(z, w) \in E(K)$, wenn die drei Elemente $x - \lambda_1, x - \lambda_2, x - \lambda_3$ allesamt Quadrate in K sind.

Beweis. Es sei (x, y) ein fixierter Punkt der Kurve. Mit der verschobenen Variablen

$$X' = X - x$$

können wir die Gleichung als

$$Y^2 = (X' + x - \lambda_1)(X' + x - \lambda_2)(X' + x - \lambda_3)$$

schreiben mit den neuen Nullstellen $\lambda_i - x$ der rechten Seite. Die beiden als äquivalent nachzuweisenden Aussagen des Satzes ändern sich bei dieser Transformation nicht. Wir können also annehmen, dass $x = 0$ ist. Es ist somit zu zeigen, dass ein Punkt der Form $(0, y)$ genau dann eine Halbierung auf der elliptischen Kurve besitzt, wenn $-\lambda_1, -\lambda_2, -\lambda_3$ Quadrate in K sind.

Unter den Gruppenhomomorphismen $\varphi_1, \varphi_2, \varphi_3$ (siehe Lemma 19.2) wird der Punkt $(0, y)$ auf $(-\lambda_1, -\lambda_2, -\lambda_3)$ abgebildet. Wenn der Punkt eine Halbierung besitzt, so gilt dies auch für den Bildpunkt, und das heißt, dass diese drei Zahlen eine Quadratwurzel besitzen.

Es seien nun umgekehrt $-\lambda_1, -\lambda_2, -\lambda_3$ Quadrate in K und zwar sei

$$-\lambda_i = \mu_i^2.$$

Es ist dann $y = \pm\mu_1\mu_2\mu_2$, wir betrachten den positiven Fall, im negativen Fall kann man ein μ_i durch $-\mu_i$ ersetzen. Wir behaupten, dass der Punkt (w, z) mit

$$w = \mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3$$

und

$$z = -(\mu_1 + \mu_2 + \mu_3)w + \mu_1\mu_2\mu_3$$

ein Halbierungspunkt von $(0, y)$ ist. Dass dieser Punkt zur Kurve gehört wird in Aufgabe 18.9 gezeigt. Für die Gleichung $2(z, w) = (0, y)$ siehe Aufgabe 18.10. □

LEMMA 19.4. *Es sei R ein faktorieller Bereich, $K = Q(R)$ sein Quotientenkörper und sei*

$$Y^2 = (X - \lambda_1)(X - \lambda_2)(X - \lambda_3)$$

die Gleichung einer elliptischen Kurve E in Zerlegungsform über K mit $\lambda_1, \lambda_2, \lambda_3 \in R$. Es sei p ein Primelement von R, das keines der Elemente $\lambda_1 - \lambda_2$, $\lambda_1 - \lambda_3$, $\lambda_2 - \lambda_3$ teile. Es sei $P = (x, y) \in E(K)$ ein Punkt der Kurve. Dann ist die Ordnung von $x - \lambda_j$ in p gerade.

Beweis. Wir schreiben $\operatorname{ord}(f)$ für die Ordnung eines Elementes $f \in K$, $f \neq 0$, in p. Dies ist die Ordnung von f im diskreten Bewertungsring $R_{(p)}$ bzw. dessen Quotientenkörper (siehe Aufgabe 2.36 und Aufgabe 2.37). Aufgrund der Kurvengleichung gilt die Ordnungsbeziehung

$$\begin{aligned} 2\operatorname{ord}(y) &= \operatorname{ord}(y^2) \\ &= \operatorname{ord}((x - \lambda_1)(x - \lambda_2)(x - \lambda_3)) \\ &= \operatorname{ord}(x - \lambda_1) + \operatorname{ord}(x - \lambda_2) + \operatorname{ord}(x - \lambda_3). \end{aligned}$$

Es sei zuerst $\operatorname{ord}(x - \lambda_1) < 0$. Dann ist

$$\operatorname{ord}(x - \lambda_1) = \operatorname{ord}(x) = \operatorname{ord}(x - \lambda)$$

für überhaupt alle $\lambda \in R$. Somit ist

$$2\operatorname{ord}(y) = \operatorname{ord}(x - \lambda_1) + \operatorname{ord}(x - \lambda_2) + \operatorname{ord}(x - \lambda_3) = 3\operatorname{ord}(x - \lambda_1),$$

also sind die $\operatorname{ord}(x - \lambda_j)$ gerade. Wir können also

$$\operatorname{ord}(x - \lambda_1), \operatorname{ord}(x - \lambda_2), \operatorname{ord}(x - \lambda_3) \geq 0$$

annehmen. Aus $\operatorname{ord}(x - \lambda_1), \operatorname{ord}(x - \lambda_2) \geq 1$ würde

$$\operatorname{ord}(\lambda_2 - \lambda_1) = \operatorname{ord}(-(x - \lambda_2) + (x - \lambda_1)) \geq 1$$

folgen im Widerspruch dazu, dass p kein Teiler der Differenzen der Nullstellen ist. Also ist $\operatorname{ord}(x - \lambda_2), \operatorname{ord}(x - \lambda_3) = 0$. Dann ist aber

$$\begin{aligned} 2\operatorname{ord}(y) &= \operatorname{ord}(x - \lambda_1) + \operatorname{ord}(x - \lambda_2) + \operatorname{ord}(x - \lambda_3) \\ &= \operatorname{ord}(x - \lambda_1), \end{aligned}$$

also hat $x-\lambda_1$ wieder gerade Ordnung. □

Mit der Hilfe von Lemma 19.4 können wir im Zahlkörperfall das Bild von φ_j in $K^\times/(K^\times)^2$ besser eingrenzen. Hierfür sind zwei Hauptergebnisse zu der algebraischen Zahlentheorie entscheidend, nämlich die Endlichkeit der Klassengruppe und der Dirichletsche Einheitensatz.

LEMMA 19.5. *Es sei*

$$Y^2 = (X-\lambda_1)(X-\lambda_2)(X-\lambda_3)$$

die Gleichung einer elliptischen Kurve E in Zerlegungsform über einem Zahlkörper K mit $\lambda_1,\lambda_2,\lambda_3 \in K$. Dann gibt es einen faktoriellen Bereich $R \subseteq K$ mit den folgenden Eigenschaften.

(1) *Es ist $Q(R) = K$.*
(2) *Es ist $\lambda_1,\lambda_2,\lambda_3 \in R$.*
(3) *Die Einheitengruppe $R^\times$ ist endlich erzeugt.*
(4) *Zu jedem Punkt $P = (x,y) \in E(K)$ besitzt $\varphi_i(P) \in K^\times/(K^\times)^2$ eine Darstellung $\varphi_i(P) = u$ mit $u \in R^\times$.*

Beweis. Wir starten mit dem Ganzheitsring A von K, so dass (1) direkt erfüllt ist. Nach Satz 26.6 (Algebraische Zahlentheorie (Osnabrück 2020-2021)) ist die Klassengruppe von A endlich, deshalb gibt es eine Nenneraufnahme an einem Element f derart, dass A_f faktoriell ist. Durch eine weitere Nenneraufnahme am Hauptnenner der λ_i erreichen wir (2) und durch eine weitere Nenneraufnahme an einem Element erreichen wir, dass die Primteiler von $\lambda_i-\lambda_j$ für $i \neq j$ Einheiten im Ring werden. Diese Nenneraufnahme nennen wir R. Es ist

$$\varphi_j(P) = [u \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n}]$$

in $K^\times/(K^\times)^2$ mit $u \in R^\times$ und gewissen Primelementen aus R und Exponenten aus $\mathbb{Z}$. Nach Lemma 19.4 sind diese Exponenten aber gerade, also ist (4) erfüllt. Die Eigenschaft (3) folgt aus Satz 28.7 (Algebraische Zahlentheorie (Osnabrück 2020-2021)) in der Version Aufgabe 28.30 (Algebraische Zahlentheorie (Osnabrück 2020-2021)). □

LEMMA 19.6. *Es sei*

$$Y^2 = (X-\lambda_1)(X-\lambda_2)(X-\lambda_3)$$

die Gleichung einer elliptischen Kurve E in Zerlegungsform über einem Zahlkörper K mit $\lambda_1,\lambda_2,\lambda_3 \in K$. Dann besitzt die Abbildung

$$\varphi = (\varphi_1,\varphi_2,\varphi_3)\colon E(K) \longrightarrow K^\times/\left(K^\times\right)^2 \times K^\times/\left(K^\times\right)^2 \times K^\times/\left(K^\times\right)^2$$

mit φ_i wie in Definition 19.1 folgende Eigenschaften.

(1) *φ ist ein Gruppenhomomorphismus.*
(2) *Der Kern von φ ist $2E(K)$.*
(3) *Das Bild von φ ist endlich.*

Beweis. (1) Dies folgt aus Lemma 19.2.

(2) Es sei $P \in E(K)$. Bei $P = \mathfrak{O}$ sind beide Seiten der Aussage erfüllt. Sei also $P = (x,y)$. Nach Satz 19.3 ist P genau dann ein Verdoppelungspunkt auf der Kurve, wenn alle $x - \lambda_i$ Quadrate in K sind. Dies ist bei $x \neq \lambda_i$ direkt die Behauptung. Bei $x = \lambda_1$ ist

$$\varphi((\lambda_1, 0)) = ((\lambda_1 - \lambda_2)(\lambda_1 - \lambda_3),\, \lambda_1 - \lambda_2,\, \lambda_1 - \lambda_3)$$

und sowohl die Kernbedingung als auch die Halbierungsbedingung aus Satz 19.3 sind genau dann erfüllt, wenn $\lambda_1 - \lambda_2$ und $\lambda_1 - \lambda_3$ Quadrate sind.

(3) Nach Lemma 19.5 wird jedes Element des Bildes von einer endlich erzeugten Gruppe repräsentiert. Da $K^\times/(K^\times)^2$ eine Torsionsgruppe ist, ist das Bild endlich.

□

Lemma 19.7. *Es sei E eine elliptische Kurve über einem Körper K und es sei $K \subseteq L$ eine Galoiserweiterung. Es sei $E(L)/2E(L)$ endlich. Dann ist auch $E(K)/2E(K)$ endlich.*

Beweis. Wir zeigen, dass der Kern H der natürlichen Abbildung

$$E(K)/2E(K) \longrightarrow E(L)/2E(L)$$

endlich ist, woraus die Behauptung folgt. Es sei $\mathrm{Tor}_2(E(L))$ die Untergruppe der Torsionselemente zur Ordnung 2, die nach Korollar 18.4 endlich ist und es sei G die Galoisgruppe von L über K. Es sei $P \in H$, repräsentiert durch $P \in E(K)$. Nach Voraussetzung ist P in $E(L)$ das Doppelte eines Punktes $Q \in E(L)$. Wir wählen zu jedem P einen solchen Punkt Q und definieren damit die Abbildung

$$\theta_P \colon G \longrightarrow \mathrm{Tor}_2(E(L)),\ \varphi \longmapsto \varphi^*(Q) - Q,$$

wobei wir die zu φ gehörigen Automorphismen φ^* auf der Kurve betrachten, siehe Aufgabe 13.27. Wir behaupten, dass die Zuordnung

$$H \longrightarrow \mathrm{Abb}\,(G, \mathrm{Tor}_2(E(L))),\ P \longmapsto \theta_p,$$

injektiv ist. Seien also $P, P' \in H$, repräsentiert von $P, P' \in E(K)$ und mit Halbierungspunkten $Q, Q' \in E(L)$. Die Gleichheit $\theta_P = \theta_{P'}$ bedeutet

$$\varphi^*(Q) - Q = \varphi^*(Q') - Q'$$

für alle $\varphi \in G$. Dies bedeutet nach Aufgabe 13.28

$$\varphi^*(Q' - Q) = Q' - Q$$

für alle $\varphi \in G$. D.h., dass $Q' - Q$ invariant unter der Galoisgruppe ist und daher gemäß Aufgabe 13.25 zu $E(K)$ gehört. Also ist

$$P' - P = 2Q' - 2Q = 2(Q' - Q)$$

und somit ist $[P'] = [P]$ in $E(K)/2E(K)$. Wegen der Endlichkeit der Abbildungsmenge zwischen den endlichen Mengen G und $\mathrm{Tor}_2(E(L))$ ist auch $E(K)/2E(K)$ endlich. □

Louis Mordell (1888-1972)

Der folgende Satz heißt der schwache Satz von Mordell-Weil.

Satz 19.8. *Es sei E eine elliptische Kurve E über einem Zahlkörper K. Dann ist $E(K)/2E(K)$ endlich.*

Beweis. Es sei

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

eine kurze Weierstraßgleichung für E über K. Das Polynom x^3+ax+b besitzt in einer endlichen Galoiserweiterung (siehe Lemma 11.5 (Körper- und Galoistheorie (Osnabrück 2018-2019)) und Satz 16.6 (Körper- und Galoistheorie (Osnabrück 2018-2019))) $K \subseteq L$ drei Nullstellen. Nach Lemma 19.7 können wir die Endlichkeit über L nachweisen, d.h. wir können davon ausgehen, dass die Gleichung in der Form

$$y^2 = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

vorliegt. Den neuen Körper nennen wir wieder K. Nach Lemma 19.6 ist

$$E(K)/2E(K) \cong \mathrm{bild}\,\varphi$$

endlich. □

Abbildungsverzeichnis