Vortrag 11: Der Satz von Mordell-Weil

Max Daniel

30. Januar 2013

Inhaltsverzeichnis

Einleitung

Sei E/K eine über einem Zahlkörper K definierte elliptische Kurve. Wir hatten gesehen, dass die K-rationalen Punkte $E(K)$ eine Untergruppe von E bilden. Wir wollen nun den *Satz von Mordell-Weil* beweisen, der besagt, dass $E(K)$ endlich erzeugt ist. Der Beweis verläuft über die *Abstiegsmethode*, ist also eine Anwendung des folgenden Satzes [Sil, S. 218, Thm. VIII.3.1], den wir in Vortrag 9 bewiesen hatten.

Satz 0.1. *Sei A eine abelsche Gruppe und $h\colon A \to \mathbb{R}$ eine Abbildung mit den folgenden Eigenschaften:*

(i) $\forall Q \in A\, \exists C_1 \in \mathbb{R}\, \forall P \in A : h(P+Q) \leq 2h(P) + C_1$

(ii) $\exists m \in \{2,3,4,\dots\}, C_2 \in \mathbb{R}\, \forall P \in A : h(mP) \geq m^2 h(P) - C_2$

(iii) $\forall C_3 \in \mathbb{R} : \{P \in A \mid h(P) \leq C_3\}$ *ist endlich*

Zusätzlich gebe es ein m, für das Bedingung (ii) erfüllt und A/mA endlich ist. Dann ist A endlich erzeugt.

Mit etwas Gruppenkohomologie und algebraischer Zahlentheorie hatten wir in Vortrag 9 bereits den sog. *schwachen* Satz von Mordell-Weil [Sil, S. 208, Thm. VIII.1.1] gezeigt:

Satz 0.2. *Für alle $m \in \{2,3,4,\dots\}$ ist $E(K)/mE(K)$ endlich.*

Zu zeigen bleibt also nur noch die Existenz einer Abbildung $h\colon E(K) \to \mathbb{R}$, die die Bedingungen aus Satz 0.1 erfüllt. Wir folgen hierbei Abschnitt VIII.6 von [Sil].

1 Höhenfunktionen auf elliptischen Kurven

Wir erinnern an die *absolute Höhenfunktion* $H\colon \bigcup_{N\in\mathbb{N}} \mathbb{P}^N(\overline{\mathbb{Q}}) \to \mathbb{R}$ aus Vortrag 10. Für unsere Zwecke ist die *absolute logarithmische Höhenfunktion* $h = \log \circ H$ besser geeignet.

Satz 1.1 (Eigenschaften der logarithmischen Höhe)**.** *(i)* $\forall P \in \mathbb{P}^N(\overline{\mathbb{Q}}) : h(P) \geq 0$

(ii) Sei $F\colon \mathbb{P}^N(\overline{\mathbb{Q}}) \to \mathbb{P}^M(\overline{\mathbb{Q}})$ *ein Morphismus von Grad* d*. Dann gibt es positive reelle Zahlen* C, C' *mit*

$$\forall P \in \mathbb{P}^N(\overline{\mathbb{Q}}) : Cdh(P) \leq h(F(P)) \leq C'dh(P).$$

(iii) Für ein Polynom $f(T) = \sum_{i=0}^{d} a_i T^i = a_d \prod_{i=j}^{d} (T - \alpha_j) \in \overline{\mathbb{Q}}[T]$ *gilt*

$$-d\log 2 + \sum_{j=1}^{d} h([\alpha_j, 1]) \leq h([a_d, \ldots, a_0]) \leq (d-1)\log 2 + \sum_{j=1}^{d} h([\alpha_j, 1]).$$

(iv) $\forall C \in \mathbb{R} : \{P \in \mathbb{P}^N(K) \mid h(P) \leq C\}$ *ist endlich*

Beweis. Vortrag 10 bzw. [Sil, S. 226, Prop. VIII.5.4(b)], [Sil, S. 227, Thm. VIII.5.6], [Sil, S. 230, Prop. VIII.5.9]. Man beachte, dass der Logarithmus bijektiv und monoton wachsend ist. □

Wir benutzen nun rationale Funktionen $f \in \overline{\mathbb{Q}}(E)$, um die logarithmische Höhe auf die elliptische Kurve E zurückzuziehen. Dazu betrachten wir solche f als Abbildungen

$$f\colon E(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}}), P \mapsto \begin{cases} [f(P), 1] & f \text{ definiert in } P \\ [1, 0] & P \text{ Pol von } f \end{cases}.$$

Da E nicht-singulär ist, ist dies sogar ein Morphismus, vgl. [Sil, S. 20, Ex. II.2.2].

Definition 1.2 (Höhe auf E)**.** Sei $f \in \overline{\mathbb{Q}}(E)$. Dann heißt

$$h_f\colon E(\overline{\mathbb{Q}}) \to \mathbb{R}, P \mapsto h(f(P))$$

Höhenfunktion auf E *bzgl.* f*.*

Bedingung (iii) aus Satz 0.1 bekommen wir leicht.

Satz 1.3. *Sei* $f \in K(E)$ *nichtkonstant. Dann ist für alle* $C_3 \in \mathbb{R}$ *die Menge*

$$\{P \in E(K) \mid h_f(P) \leq C_3\}$$

endlich.

Beweis. $f \in K(E)$ bildet $E(K)$ in $\mathbb{P}^1(K)$ ab. Für $C_3 \in \mathbb{R}$ ist

$$M = \{P \in \mathbb{P}^1(K) \mid h(P) \leq C_3\}$$

endlich nach 1.1(iv). Da eine nichtkonstante rationale Funktion nur endlich viele Null- und Polstellen hat, ist damit auch

$$\{P \in E(K) \mid h_f(P) \leq C_3\} = \bigcup_{P \in M} f^{-1}(\{P\})$$

endlich. □

Die Diskussion der ersten beiden Bedingungen aus 0.1 wird einige explizite Rechnungen nötig machen. Wir wählen also Weierstraß-Koordinaten $x, y \in K(E)$, d. h. (vgl. [Sil, S. 59, Prop. III.3.1])

$$[x, y, 1] \colon E \to \mathbb{P}^2$$

liefert einen Isomorphismus von E auf eine durch eine Weierstraß-Gleichung $y^2 = x^3 + Ax + B$ (beachte $\operatorname{char} K = 0$), $A, B \in K$, gegebene Kurve, wobei der ausgezeichnete Punkt $O \in E$ der einzige Pol von x ist und auf $[0, 1, 0]$ abgebildet wird. Wir erinnern außerdem an

$$[K(E) : K(x)] = [K(x, y) : K(x)] = 2 \qquad \text{[Sil, S. 61, Cor. III.3.1.1]}$$

und das folgende Resultat.

Lemma 1.4. *Für $f \in K(E)$ sind äquivalent:*

(a) f ist gerade, d. h. $\forall P \in E(K) : f(P) = f(-P)$.

(b) $f \in K(x)$

Beweis. Mithilfe von expliziten Formeln für das Gruppengesetz, vgl. [Sil, S. 54, Kor. III.2.3.1]. □

Wir zeigen nun, dass die Höhe h_x bzgl. der Weierstraß-Koordinate x „bis auf eine Konstante“ die Parallelogramm-Gleichung erfüllt. Damit verstehen wir den Zusammenhang zwischen der Höhe und dem Gruppengesetz der elliptischen Kurve hinreichend gut, um die Bedingungen (i) und (ii) einsehen zu können.

Definition 1.5. Seien $f, g \colon S \to \mathbb{R}$ auf einer beliebigen Menge definierte Abbildungen. Wir führen folgende Notation ein:

$$f = g + O(1) :\Leftrightarrow \exists C, C' \in \mathbb{R}\, \forall P \in S : C \leq f(P) - g(P) \leq C'$$

Dies definiert offenbar eine Äquivalenzrelation, insbesondere folgt aus $f = g + O(1)$ und $g = h + O(1)$, dass $f = h + O(1)$.

Lemma 1.6.

$$h_x(P+Q)+h_x(P-Q)=2h_x(P)+2h_x(Q)+O(1)$$

Hierbei sind beide Seiten als Abbildungen auf $E(\overline{\mathbb{Q}})\times E(\overline{\mathbb{Q}})$ zu betrachten, d. h. die zu $O(1)$ gehörigen Konstanten sind unabhängig von P,Q.

Beweis. Sei $G\colon E\times E\to E\times E, (P,Q)\mapsto (P+Q,P-Q)$. Wir werden werden die Existenz eines kommutativen Diagramms

$$\begin{array}{ccc} E\times E & \xrightarrow{\ G\ } & E\times E \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ \mathbb{P}^2 & \xrightarrow{\ g\ } & \mathbb{P}^2 \end{array}$$

zeigen, wobei

(1) $h(\sigma(P,Q))=h_x(P)+h_x(Q)+O(1)$, beide Seiten als auf $E\times E$ definierte Abbildungen zu verstehen.

(2) g ist ein Morphismus von Grad 2.

Hieraus folgt dann die Behauptung, denn:

$$\begin{array}{rcll} h_x(P+Q)+h_x(P-Q) & = & h(\sigma(G(P,Q))) + O(1) & (1) \\ & = & h(g(\sigma(P,Q))) + O(1) & \text{Diagramm kommutiert} \\ & = & 2h(\sigma(P,Q)) + O(1) & (2),\ 1.1(\text{ii}) \\ & = & 2h_x(P)+2h_x(Q) + O(1) & (1) \end{array}$$

Beweis von (1): σ sei die Abbildung, die das Diagramm

$$E\times E \xrightarrow[(x,x)]{} \mathbb{P}^1\times\mathbb{P}^1 \longrightarrow \mathbb{P}^2, \qquad E\times E \xrightarrow{\ \sigma\ } \mathbb{P}^2$$

mit $\mathbb{P}^1\times\mathbb{P}^1\to\mathbb{P}^2, ([\alpha_1,\beta_1],[\alpha_2,\beta_2])\mapsto[\beta_1\beta_2,\alpha_1\beta_2+\alpha_2\beta_1,\alpha_1\alpha_2]$ kommutativ macht.

Falls $P=O$ oder $Q=O$ kann man (1) direkt nachrechnen. Seien also P und Q von O verschieden und daher $x(P)=[\alpha_1,1]$, $x(Q)=[\alpha_2,1]$. Dann ist

$$\sigma(P,Q)=[1,\alpha_1+\alpha_2,\alpha_1\alpha_2],$$

weshalb (1) aus 1.1(iii) für das Polynom

$$T^2+(\alpha_1+\alpha_2)T+\alpha_1\alpha_2=(T+\alpha_1)(T+\alpha_2)$$

folgt.

Beweis von (2): Setze $g([t,u,v]) = [u^2 - 4tv, 2u(At+v) + 4Bt^2, (v-At)^2 - 4Btu] = [g_1, g_2, g_3]$. Da die g_i homogene Polynome in t, u, v von Grad 2 sind, definiert dies einen Morphismus von Grad 2, sofern g wohldefiniert ist; die Kommutativität des obigen Diagramms kann man dann unter Verwendung der expliziten Formeln für das Gruppengesetz auf Weierstraß-Kurven direkt nachrechnen. Es bleibt also nur noch zu zeigen:

$$g_1 = g_2 = g_3 = 0 \Rightarrow t = u = v = 0$$

Falls $t = 0$, so folgt $u = 0$ aus $g_1 = 0$ und dann $v = 0$ aus $g_3 = 0$. Falls $t \neq 0$, setze $x = \frac{u}{2t}$. Dann gilt:

$$\begin{aligned} g_1 = 0 &\Rightarrow x^2 = \frac{v}{t} \\ g_2 = 0 &\Rightarrow \psi(x) = 4x^3 + 4Ax + 4B = 0 \\ g_3 = 0 &\Rightarrow \phi(x) = x^4 - 2Ax^2 - 8Bx + A^2 = 0 \end{aligned}$$

Die Polynome $\psi(X), \phi(X)$ haben aber keine gemeinsamen Nullstellen, denn

$$(12X^2 + 16A)\phi(X) - (3X^3 - 5AX - 27B)\psi(X) = 4(4A^3 + 27B^2) = -\frac{\Delta}{4}$$

und die Diskriminante Δ ist nicht Null, da elliptische Kurven nicht-singulär sind. □

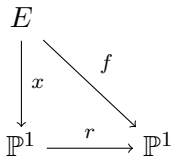
Da wir nur *eine* Höhenfunktion auf $E(K)$ mit den passenden Eigenschaften benötigen, reicht Lemma 1.6 für den Beweis des Satzes von Mordell-Weil bereits aus. Wir zeigen aber noch mehr.

Satz 1.7. *Seien $f, g \in K(E)$ gerade. Dann gilt:*

(i) Lemma 1.6 gilt auch mit h_f statt h_x.

(ii) $(\deg g)h_f = (\deg f)h_g + O(1)$

Beweis. Nach 1.4 gibt es $r(X) \in K(X) = K(\mathbb{P}^1)$ mit $f = r(x)$; in Termen von Morphismen kommutiert also das Diagramm



.

Also gilt $h_f = h_{r \circ x} \overset{1.1(ii)}{=} (\deg r)h_x + O(1)$ und aus der Multiplikativität des Grads erhalten wir $\deg f = (\deg x)(\deg r) = 2 \deg r$. Insgesamt folgt also

$$(*) \qquad h_f = \frac{1}{2}(\deg f)h_x + O(1),$$

weshalb sich (i) durch Multiplikation der Gleichung aus 1.6 mit $\frac{1}{2}(\deg f)$ ergibt. Ferner:

$$(\deg g)h_f \overset{(*)}{=} \frac{1}{2}(\deg f)(\deg g)h_x + O(1) \overset{(*)}{=} (\deg f)h_g + O(1)$$

□

Korollar 1.8. *Sei $f \in K(E)$ gerade. Dann gilt:*

(i) $\forall Q \in E(\overline{\mathbb{Q}})\, \exists C_1 \in \mathbb{R}\, \forall P \in E(\overline{\mathbb{Q}}) : h_f(P+Q) \leq 2h_f(P) + C_1$

(ii) $\forall m \in \mathbb{Z} : h_f \circ [m] = m^2 h_f + O(1)$

Beweis. (i) folgt unmittelbar aus 1.7(i) und 1.1(i). (ii) muss nur für $m \geq 0$ gezeigt werden, da f gerade ist; dies geschieht per Induktion. Für $m = 0$ folgt die behauptete Gleichung aus $h_f(O) = h([1,0]) = 0$, für $m = 1$ ist sie trivial. Wir folgern nun die Gültigkeit für $m+1$ aus der für m und $m-1$:

$$\begin{aligned} h_f([m+1]P) = h_f([m]P + P) &\overset{1.7(i)}{=} -h_f([m]P - P) + 2h_f([m]P) + 2h_f(P) + O(1) \\ &= -(m-1)^2 h_f(P) + 2m^2 h_f(P) + 2h_f(P) + O(1) \\ &= (m+1)^2 h_f(P) + O(1) \end{aligned}$$

□

Satz 1.9 (Mordell-Weil)**.** *$E(K)$ ist endlich erzeugt.*

Beweis. Nach dem Satz über die Abstiegsmethode 0.1 und dem schwachen Satz von Mordell-Weil 0.2 genügt es, ein $f \in \overline{\mathbb{Q}}(E)$ zu finden, für das die Höhenfunktion

$$h_f \colon E(K) \to \mathbb{R}$$

folgende Eigenschaften hat:

(i) $\forall Q \in E(K)\, \exists C_1 \in \mathbb{R}\, \forall P \in E(K) : h_f(P+Q) \leq 2h_f(P) + C_1$

(ii) $\exists m \in \{2,3,4,\dots\}, C_2 \in \mathbb{R}\, \forall P \in E(K) : h_f([m]P) \geq m^2 h_f(P) - C_2$

(iii) $\forall C_3 \in \mathbb{R} : \{P \in E(K) \mid h_f(P) \leq C_3\}$ ist endlich

Wir haben bereits gesehen, dass dies für $f = x$ der Fall ist, sogar für alle nichtkonstanten geraden $f \in K(E)$. Im Einzelnen folgt (i) aus 1.8(i), (ii) aus 1.8(ii) und (iii) aus 1.3. □

2 Ausblick

Nach dem Satz von Mordell-Weil und dem Hauptsatz für endlich erzeugte abelsche Gruppen ist

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$$

mit endlicher Torsions-Untergruppe $E(K)_{tors}$. Die Bestimmung der K-rationalen Torsionspunkte für eine feste elliptische Kurve E/K ist häufig vergleichsweise einfach möglich. Ist nämlich v eine nicht-archimedische Bewertung von K, für die E gute Reduktion hat, K_v die Komplettierung von K bzgl. v mit Restklassenkörper k_v, dann hat man für zu $\operatorname{char} k_v$ teilerfremde $m \in \mathbb{Z}$ eine Injektion

$$E(K_v)[m] \hookrightarrow \tilde{E}(k_v). \qquad \text{[Sil, S. 192, Prop. VII.3.1]}$$

Schwieriger ist die Frage, welche Torsionsgruppen für variierende elliptische Kurven auftreten können. Hierzu erwähnt [Sil, S. 242] die folgenden Resultate:

Satz 2.1 (Mazur)**.** *Sei $E/\mathbb{Q}$ eine über den rationalen Zahlen definierte elliptische Kurve. Dann ist $E(\mathbb{Q})_{tors}$ isomorph zu einer der folgenden 15 Gruppen:*

$$\begin{array}{rl} \mathbb{Z}/N\mathbb{Z} & , 1 \leq N \leq 10 \text{ oder } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & , 1 \leq N \leq 4 \end{array}$$

Alle diese Gruppen kommen vor.

Satz 2.2 (Merel)**.** *Sei $d \geq 1$. Dann gibt es $N(d) \in \mathbb{N}$, sodass für alle Zahlkörper K von Grad höchstens d über $\mathbb{Q}$ und alle über solchen K definierten elliptischen Kurven E/K gilt:*

$$|E(K)_{tors}| \leq N(d)$$

Abschließend noch eine Bemerkung zu Satz 1.7. Teil (i) besagt, dass für gerade $f \in K(E)$ die Höhe h_f „bis auf eine Konstante“ eine quadratische Form ist. Tatsächlich gibt es eine quadratische Form $\hat{h}$ auf $E(\overline{\mathbb{Q}})$ mit

$$(\deg f)\hat{h} = h_f + O(1)$$

für alle nichtkonstanten, geraden $f \in K(E)$. $\hat{h}$ heißt *kanonische Höhe* und kann zum Beispiel durch den Limes

$$\hat{h}(P) = \frac{1}{\deg f} \lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

definiert werden, wobei $f \in K(E)$ eine beliebige nichtkonstante gerade Funktion ist. Die Konvergenz sieht man mithilfe von 1.8(ii), die Unabhängigkeit von f mithilfe von 1.7(ii). Mehr zur kanonischen Höhe in [Sil, VIII.9].

Literatur

[Sil] J. H. Silverman. *The Arithmetic of Elliptic Curves: Second Edition.* Springer, 2009.