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

Elliptische Kurven

Vorlesung 22

Die Höhe unter Morphismen

SATZ 22.1. *Es sei*

$$\varphi\colon\ \mathbb{P}^1_{\overline{\mathbb{Q}}} \longrightarrow \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

ein Morphismus, der durch teilerfremde Polynome $f, g \in \overline{\mathbb{Q}}[X]$ gegeben ist. Es sei d das Maximum der Grade der Polynome. Dann gibt es eine positive Konstante C derart, dass die absolute Höhe die Abschätzung

$$H(\varphi(P)) \geq C \cdot H(P)^d$$

für jeden Punkt $P \in \mathbb{P}^1_{\overline{\mathbb{Q}}}$ erfüllt.

Beweis. In der homogenen Realisierung des Morphismus seien F_0, F_1 die teilerfremden homogenen Polynome vom Grad d in den Variablen X_0, X_1. Aufgrund der Teilerfremdheit erzeugen F_0 und F_1 in $\overline{\mathbb{Q}}[X,Y]$ das maximale Ideal bis auf das Radikal, d.h. es gibt mit dem Hilbertschen Nullstellensatz ein $e \geq d$ und Polynome $A_{ij} \in \overline{\mathbb{Q}}[X,Y]$ mit

$$X_0^e = A_{00}F_0 + A_{01}F_1$$

und

$$X_1^e = A_{10}F_0 + A_{11}F_1.$$

Hierbei können wir direkt A_{ij} als homogen vom Grad $e-d$ annehmen. Ferner können wir durch eine endliche Körpererweiterung annehmen, dass alle Polynome über K definiert sind.

Es sei $v \in M_K$ ein Betrag, wobei wir im nichtarchimedischen Fall $\delta = 0$ und im archimedischen Fall $\delta = 1$ setzen. Es sei $P = (x_0, x_1) \in \mathbb{P}^1_K$ ein Punkt. Es gilt dann

$$\begin{aligned} |x_0|_v^e &= |A_{00}(P)F_0(P) + A_{01}(P)F_1(P)|_v \\ &\leq 2^\delta \max\left(|A_{00}(P)F_0(P)|_v\,,\ |A_{01}(P)F_1(P)|_v\right) \\ &= 2^\delta \max\left(|A_{00}(P)|_v \cdot |F_0(P)|_v\,,\ |A_{01}(P)|_v \cdot |F_1(P)|_v\right) \\ &\leq 2^\delta \max\left(|A_{00}(P)|_v\,,\ |A_{01}(P)|_v\right) \cdot \max\left(|F_0(P)|_v\,,\ |F_1(P)|_v\right) \end{aligned}$$

und entsprechend für x_1^e, was wir zu

$$\max\left(|x_0|_v^e\,,\ |x_1|_v^e\right) \leq 2^\delta \max\left(|A_{ij}(P)|_v\,|ij\right) \cdot \max\left(|F_0(P)|_v\,,\ |F_1(P)|_v\right)$$

zusammenfassen.

Wir setzen

$$A_v = \max\left(|a|_v\,|a \text{ ist Koeffizient von einem } A_{ij}\right).$$

Da die A_{ij} alle den Grad $e-d$ besitzen, kommt in ihnen eine bestimmte Anzahl, sagen wir m an Monomen vor. Es gilt dann

$$\begin{aligned} |A_{ij}(P)|_v &\leq \left| \sum_\mu a_{ij,\mu} x_0^{\mu_0} x_1^{\mu_1} \right|_v \\ &\leq m^\delta \cdot \max\left(|a_{ij,\mu} x_0^{\mu_0} x_1^{\mu_1}|_v \,|\mu \right) \\ &\leq m^\delta \cdot A_v \cdot \max\left(\left|x_0^{e-d}\right|_v, \left|x_1^{e-d}\right|_v \right). \end{aligned}$$

Einsetzen der zweiten Abschätzung in die erste ergibt

$$\begin{aligned} \max\left(|x_0|_v^e, |x_1|_v^e\right) &\leq 2^\delta m^\delta \cdot A_v \cdot \max\left(\left|x_0^{e-d}\right|_v, \left|x_1^{e-d}\right|_v \right) \\ &\quad \cdot \max\left(|F_0(P)|_v, |F_1(P)|_v\right). \end{aligned}$$

Multiplikation mit der positiven Zahl $\max\left(|x_0|_v, |x_1|_v\right)^{d-e}$ ergibt die Abschätzungen

$$\max\left(|x_0|_v^d, |x_1|_v^d\right) \leq 2^\delta \cdot m^\delta \cdot A_v \cdot \max\left(|F_0(P)|_v, |F_1(P)|_v\right).$$

Es gibt nur endlich viele archimedische Beträge, für die nichtarchimedischen Beträge werden die Faktoren $2^\delta \cdot m^\delta$ zu 1 und bis auf endlich viele Beträge ist auch $A_v = 1$, da die Koeffizienten aller A_{ij} jeweils nur für endlich viele Beträge $\neq 1$ sind. Die Abschätzungen bleiben erhalten, wenn man die Potenzen zu den Exponenten n_v nimmt und man kann dann das Produkt über alle Beträge nehmen. Schließlich geht man durch Wurzelziehen zur absoluten Höhe über. □

Definition 22.2. Zu $P \in \mathbb{P}^m(\overline{\mathbb{Q}})$ nennt man

$$h(P) := \ln H(P),$$

wobei $H(P)$ die absolute Höhe von P bezeichnet, die *logarithmische Höhe* von P.

Für die logarithmische Höhe schreibt man also ein kleines h. Die Werte von h liegen in $\mathbb{R}_{\geq 0}$. Wegen der strengen Monotonie des natürlichen Logarithmus gilt Satz 20.10 entsprechend.

Die Höhenfunktion auf einer elliptischen Kurve

Es sei

$$E = V_+(F) = \mathbb{P}^2_K$$

eine über einem Zahlkörper K definierte elliptische Kurve, gegeben durch eine kurze Weierstraßgleichung $y^2 = x^3 + ax + b$. Wir wollen auf den Punkten von E eine Höhenfunktion definieren, die im Beweis des Satzes von Mordell-Weil helfen soll. Dazu muss sie gewisse Eigenschaften bezüglich der Addition erfüllen. Wir arbeiten (statt mit der durch die Einbettung gegebene Höhe) mit der Abbildung

$$E \longrightarrow \mathbb{P}^1_K,\ (x,y,z) \longmapsto (x,z).$$

Affin wird also ein Punkt (x,y) einfach auf x projiziert.

LEMMA 22.3. *Es sei E eine elliptische Kurve über einem Zahlkörper K und sei $P = (x,y,1) \in E$ ein fixierter Punkt aus $E(K)$. Dann gibt es eine Konstante C derart, dass für jeden Punkt $Q \in E(K)$ die absolute Höhe die Abschätzung*

$$H(P+Q) \leq C \cdot H(Q)^2$$

erfüllt.

Beweis. Wir können annehmen, dass die x-Koordinate von P gleich 0 ist, die Gleichung habe die Form

$$y^2 = x^3 + rx^2 + sx + t$$

(durch die Verschiebung können wir nicht davon ausgehend, dass $r = 0$ ist), es ist also $P(0,y_1,1) = $. Es sei $Q = (x_2,y_2,1) \in E(K)$, dessen Höhe ist also nach Definition die absolute Höhe von $(x_2,1)$. Es geht darum, eine Höhenabschätzung für x_3 zu zeigen, wobei

$$P+Q = (x_3,y_3,1)$$

ist. Die expliziten Formel für die Koordinaten der Summe liefern

$$\begin{aligned} x_3 &= \alpha^2 - r - x_2 \\ &= \left(\frac{y_2-y_1}{x_2}\right)^2 - r - x_2 \\ &= \frac{x_2^3 + rx_2^2 + sx_2 + t - 2y_1y_2 + y_1^2}{x_2^2} - r - x_2, \end{aligned}$$

siehe Aufgabe 6.20. Die Summanden im Bruch haben die Form x_2, r, sx_2^{-1}, cx_2^{-2} und $dy_2x_2^{-2}$, es ist ja y_1 fixiert. Die Höhe dieser ersten Terme kann man wegen Lemma 21.8 jeweils durch eine Konstante mal $H(x_2)^2$ nach oben abschätzen. Vom zuletzt genannten Term betrachten wir das Quadrat, also

$$\frac{y_2^2}{x_2^4} = \frac{x_2^3 + rx_2^2 + sx_2 + t}{x_2^4},$$

und es geht wieder darum, die Höhe dieser Summanden nach oben abzuschätzen. Da die Summanden bis auf Konstanten die Form x_2^i mit $i = -1,-2,-3,-4$ besitzen, haben wir insgesamt eine Abschätzung nach oben der Form $\leq C \cdot H(x_2)^4$. Durch Ziehen der Quadratwurzel erhalten wir wieder eine Abschätzung der gewünschten Form. □

De folgende Satz besagt, dass bei einer elliptischen Kurve über einem Zahlkörper die über die x-Projektion auf die projektive Gerade definierte logarithmische Höhe eine schwache Höhenfunktion ist.

SATZ 22.4. *Es sei E eine elliptische Kurve über einem Zahlkörper K mit einer Weierstraßgleichung*

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

und zugehöriger Projektion $E \to \mathbb{P}^1$. Dann erfüllt die zugehörige logarithmische Höhe die folgenden Eigenschaften.

(1) *Zu jedem Punkt $P \in E(K)$ gibt es eine Konstante C derart, dass für jeden Punkt $Q \in E(K)$ die Abschätzung*
$$h(P+Q) \leq 2h(Q) + C$$
erfüllt ist.

(2) *Es gibt eine Konstante D derart, dass für alle $P \in E(K)$ die Abschätzung*
$$h(2P) \geq 4h(P) - D$$
gilt.

(3) *Zu jeder Schranke S ist*
$$\{P \in E(K) \mid h(P) \leq S\}$$
endlich.

Beweis. (1) Das ist die logarithmische Version von Lemma 22.3.

(2) Dies folgt über den Logarithmus aus Satz 22.1 und der expliziten Formel für die x-Koordinate bei der Verdoppelung, siehe Korollar 6.7.

(3) Dies folgt aus Satz 21.10, da die Abbildung $E \to \mathbb{P}^1$ den Grad 2 besitzt.

□

Der Satz von Mordell-Weil

Satz 22.5. *Es sei E eine elliptische Kurve über einem Zahlkörper K. Dann ist $E(K)$ endlich erzeugt.*

Beweis. Dies folgt mit Lemma 20.3 (für $m = 2$) aus Satz 19.8 und aus Satz 22.4. □

Der Satz bedeutet also, dass die Gruppe $E(K)$ der K-rationalen Punkte die Form
$$E(K) \cong T \times \mathbb{Z}^r$$
besitzt, wobei T die endliche Torsionsuntergruppe und r der endliche Rang der elliptischen Kurve ist. Es ist im Allgemeinen schwierig, zu einer gegebenen elliptischen Kurve die Gruppenstruktur und insbesondere den Rang zu bestimmen. Wir erwähnen einige Beispiele.

Beispiel 22.6. Auf der durch $y^2 = x^3 - 2x$ gegebenen elliptischen Kurve gibt es über $\mathbb{Q}$ die beiden Torsionspunkte $(0,0)$, $\mathfrak{O}$. Daneben gibt es noch den Punkt $(-1,1)$, der den torsionsfreien Teil erzeugt. Die Gruppenstruktur ist
$$E(\mathbb{Q}) \cong \mathbb{Z}/(2) \times \mathbb{Z}$$

und $(-1, 1)$ ist ein Erzeuger der torsionsfreien Komponente.

Beispiel 22.7. Auf der durch $y^2 = x^3 + 17$ gegebenen elliptischen Kurve gibt es über $\mathbb{Q}$ die beiden unabhängigen Punkte $(-2, 3)$ und $(2, 5)$. Hier ist

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}$$

und die angegebenen Punkte sind Erzeuger, der Rang ist also 2.

Beispiel 22.8. Auf der durch $y^2 = x^3 - (2 \cdot 3 \cdot 11 \cdot 19)^2 x$ gegebenen elliptischen Kurve gibt es über $\mathbb{Q}$ neben den 2-Torsionspunkten, die den Nullstellen des kubischen Polynoms in x entsprechen (siehe Lemma 18.2 und Satz 25.7), die drei unabhängigen Punkte $(-98, 12376)$, $(1650, 43560)$ und $(109554, 36258840)$. Hier ist

$$E(\mathbb{Q}) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}^3,$$

der Rang ist also 3.

Bemerkung 22.9. Man vermutet, dass es keine allgemeine Schranke für den Rang einer elliptischen Kurve über $\mathbb{Q}$ gibt. Es ist aber schwierig, elliptische Kurven mit großen Rang anzugeben, der derzeitige Rekord liegt bei Rang 28.

Bemerkung 22.10. Der Satz von Mordell-Weil gilt auch für abelsche Varietäten über einem Zahlkörper K, d.h. auch in diesem Fall ist die Gruppe der K-rationalen Punkte $A(K)$ endlich erzeugt.

Auf der projektiven Geraden (Geschlecht 0), die ja die Vereinigung der affinen Geraden mit dem unendlich fernen Punkt ist, gibt es, egal über welchem Zahlkörper man sich bewegt, stets einen rationalen Punkt mehr als im Körper. Hier gibt es also keine interessanten Fragen über die Existenz oder die Verteilung von rationalen Punkten. Bei Geschlecht 1, also den elliptischen Kurven, wird die Frage nach den rationalen Punkten grob durch den Satz von Mordell-Weil beantwortet, auch wenn die Frage nach dem Rang in jedem Einzelfall schwierig bleibt. Im Fall von höherem Geschlecht hat Mordell vermutet, dass es da stets zur endlich viele rationale Punkte gibt. Dies wurde um 1983 von Gerd Faltings bewiesen. Der Beweis geht weit über diese Vorlesung hinaus, er benutzt aber wesentlich abelsche Varietäten.

Satz 22.11. *Es sei C eine projektive glatte Kurve vom Geschlecht $g(C) \geq 2$ über einem Zahlkörper K. Dann ist die Menge der K-rationalen Punkte $K(C)$ endlich.*

Dies kann man beispielsweise für jede glatte ebene Kurve vom Grad ≥ 4 anwenden.

Abbildungsverzeichnis