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

# Elliptische Kurven

## Vorlesung 21

### Die Höhenfunktion auf dem projektiven Raum

Im projektiven Raum über einem Körper ist jeder Punkt gleichberechtigt, es gibt stets einen Automorphismus, der den einen Punkt in einen anderen Punkt überführt. Im projektiven Raum über $\overline{\mathbb{Q}}$ unterscheiden sich aber dennoch die Punkte hinsichtlich ihrer arithmetischen Eigenschaften oder arithmetischen Komplexität. Da ist zum einen die Frage, über welchem Körper ein Punkt definiert werden kann. Da es nur endlich viele Koordinaten gibt und diese algebraische Zahlen sind, gehört jeder Punkt $P = (x_0, x_1, \ldots, x_m) \in \mathbb{P}^m\big(\overline{\mathbb{Q}}\big)$ bereits zu $P \in \mathbb{P}^m(K)$ für eine endliche Erweiterung $\mathbb{Q} \subseteq K$, beispielsweise kann man

$$K = \mathbb{Q}(x_0, x_1, \ldots, x_m)$$

nehmen, was aber im Allgemeinen nicht der Körper von minimalen Grad sein muss, man denke an $\big(\sqrt{2}, \sqrt{2}, \ldots, \sqrt{2}\big)$, der bereits über $\mathbb{Q}$ definiert ist. Natürlich gibt es im projektiven Raum unendlich viele Punkte mit rationalen Koordinaten. Daher erhebt sich die Frage, wie man bei einem fixierten Zahlkörper die Punkte sinnvoll in zunehmend größere endliche Teilmengen anordnen kann. Es bezeichnet $|-|_v$, $v \in M_K$, die Standardbeträge eines Zahlkörpers $K$.

Definition 21.1. Es sei $K$ ein Zahlkörper und sei $P \in \mathbb{P}^m_K$ ein $K$-Punkt mit den homogenen Koordinaten $P = (x_0, x_1, \ldots, x_m)$. Dann versteht man unter der *Höhe* (über $K$) von $P$ die reelle Zahl

$$\begin{aligned} H_K(P) &:= \prod_{v \in M_K} \max\{|x_0|_v^{n_v}, |x_1|_v^{n_v}, \ldots, |x_m|_v^{n_v}\} \\ &= \prod_{v \in M_K} \max\{\|x_0\|_v, \|x_1\|_v, \ldots, \|x_m\|_v\}. \end{aligned}$$

Dieser Ausdruck existiert, da bis auf endlich viele Ausnahmen zu jedem nichtarchimedischen Betrag der Faktor gleich 1 ist. Durch die Potenz mit dem lokalen Grad $n_v$ als Exponenten wird aus dem Standardbetrag der natürliche Betrag, siehe Bemerkung 20.8.

Beispiel 21.2. Betrachten wir den rationalen Punkt $\big(8, \frac{7}{26}, \frac{4}{45}\big) \in \mathbb{P}^2_{\mathbb{Q}}$. Wir müssen für die verschiedenen Beträge das Maximum bestimmen und die Ergebnisse miteinander multiplizieren. Für den archimedischen Betrag $|-|_{\mathbb{R}}$ hat

man direkt 8, gehen wir also die Primzahlen durch. Dabei wird das Maximum des Betrages im Minimum der zugehörigen Bewertungsordnung angenommen. Die 2 kommt in der mittleren Koordinate mit Ordnung $-1$ vor, was zum maximalen 2-Betrag $2^1 = 2$ führt. Die 3 kommt in der dritten Koordinate mit Ordnung $-2$ vor, was zum maximalen 3-Betrag $3^2 = 9$ führt. Die 5 kommt in der dritten Koordinate mit Ordnung $-1$ vor, was zum maximalen 5-Betrag $5^1 = 5$ führt. Die 7 kommt in der zweiten Koordinate mit Ordnung 1 vor, was für diese Komponente zum 7-Betrag $7^{-1}$ führt, der aber irrelevant ist, da ja das Maximum mit 1 genommen wird. Schließlich kommt die 13 in der zweiten Koordinate mit Ordnung $-1$ vor, was zum maximalen 13-Betrag 13 führt, die anderen Beträge haben den Wert 1. Die Höhe des Punktes ist somit

$$8 \cdot 2 \cdot 9 \cdot 5 \cdot 13 \, .$$

Beispiel 21.3. In $\mathbb{P}^1(\mathbb{Q})$ besitzen die Punkte $(1,0), (0,1), (1,1), (1,-1)$ die Höhe 1. Wir beschränken uns nun auf Punkte der Form $(x,1)$ mit

$$x \, = \, \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n} \, = \, \pm \frac{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}{p_{k+1}^{-\alpha_{k+1}} \cdots p_n^{-\alpha_n}}$$

und $\alpha_i \in \mathbb{Z}$ ( $n \geq 1$, die Exponenten seien bis zum $k$-ten Term positiv, danach negativ). Ein solcher Punkt hat die Höhe

$$\begin{aligned} H_{\mathbb{Q}}(P) &= \max\{|x| \, , \, 1\} \cdot \max\{p_1^{-\alpha_1}, \, 1\} \cdots \max\{p_n^{-\alpha_n}, \, 1\} \\ &= \max\{|x| \, , \, 1\} \cdot p_{k+1}^{-\alpha_{k+1}} \cdots p_n^{-\alpha_n}, \end{aligned}$$

wobei alle Faktoren $\geq 1$ sind. Das hintere Produkt ist einfach der Nenner der rationalen Zahl $x$, die Höhe ist nach Aufgabe 21.2 eine natürliche Zahl. Bestimmen wir die Punkte $(x,1)$, deren Höhe gleich 2 ist. Ihre $x$-Koordinate ist $\pm 2$ oder $\pm \frac{1}{2}$. Die Punkte der Höhe 3 haben die $x$-Koordinate $\pm 3, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{3}{2}$. Die Punkte der Höhe 4 haben die $x$-Koordinate $\pm 4, \pm \frac{1}{4}, \pm \frac{3}{4}, \pm \frac{4}{3}$. Die Punkte der Höhe 5 haben die $x$-Koordinate $\pm 5, \pm \frac{1}{5}, \pm \frac{2}{5}, \pm \frac{3}{5}, \pm \frac{4}{5}, \pm \frac{5}{2}, \pm \frac{5}{3}, \pm \frac{5}{4}$, etc.

Lemma 21.4. *Es sei $K$ ein Zahlkörper und $\mathbb{P}_K^m$ der projektive Raum über $K$. Dann ist die Höhe eine wohldefinierte Funktion*

$$H_K \colon \, \mathbb{P}^m(K) \longrightarrow \mathbb{R}_{\geq 1}, \, P \longmapsto H_K(P).$$

*Beweis.* Es sei $P = (x_0, \, x_1, \, \ldots, \, x_m)$ und $c \in K^\times$. Aufgrund der Multiplikativität der Beträge ist

$$|cx_i|_v \, = \, |c|_v \, |x_i|_v$$

für jeden Betrag $v \in M_K$. Das überträgt sich auf die Maxima und auf die Potenzen derart, dass zwischen der mittels $(x_0, \, x_1, \, \ldots, \, x_m)$ und der mittels $(cx_0, \, cx_1, \, \ldots, \, cx_m)$ berechneten Höhe der Faktor $\prod_v |c|_v^{n_v}$ besteht. Dieser ist aber nach Satz Anhang 4.3 gleich 1. Da wir eine Koordinate gleich 1 setzen können, und die 1 unter sämtlichen Beträgen aus $M_K$ den Wert 1 besitzt, ist das Maximum jeweils $\geq 1$ und daher ist die Höhe $\geq 1$. $\square$

LEMMA 21.5. *Es sei $K$ ein Zahlkörper, $K \subseteq L$ eine endliche Körpererweiterung vom Grad $d$ und sei $P \in \mathbb{P}^m(K) \subseteq \mathbb{P}^m(L)$. Dann gilt für die Höhen die Beziehung*

$$H_L(P) = H_K(P)^d.$$

*Beweis.* Es sei

$$P = (x_0, x_1, \ldots, x_m) \in K^{m+1} \subseteq L^{m+1}.$$

Dann gilt für einen Betrag $w \in M_L$ die Einschränkung $|x|_w = |x|_v$ mit einem Betrag $v \in M_K$ und unter Verwendung von Satz Anhang 4.2 ergibt sich

$$\begin{aligned}
& H_L(P) \\
= & \prod_{w \in M_L} \max\{|x_0|_w^{n_w}, |x_1|_w^{n_w}, \ldots, |x_m|_w^{n_w}\} \\
= & \prod_{v \in M_K} \prod_{w \in M_L \text{ über } v} \max\{|x_0|_w^{n_w}, |x_1|_w^{n_w}, \ldots, |x_m|_w^{n_w}\} \\
= & \prod_{v \in M_K} \prod_{w \in M_L \text{ über } v} \max\{|x_0|_v^{n_w}, |x_1|_v^{n_w}, \ldots, |x_m|_v^{n_w}\} \\
= & \prod_{v \in M_K} \max\{\prod_{w \in M_L \text{ über } v} |x_0|_v^{n_w}, \prod_{w \in M_L \text{ über } v} |x_1|_v^{n_w}, \ldots, \prod_{w \in M_L \text{ über } v} |x_m|_v^{n_w}\} \\
= & \prod_{v \in M_K} \max\{|x_0|_v^{\sum_{w \in M_L \text{ über } v} n_w}, |x_1|_v^{\sum_{w \in M_L \text{ über } v} n_w}, \ldots, |x_m|_v^{\sum_{w \in M_L \text{ über } v} n_w}\} \\
= & \prod_{v \in M_K} \max\{|x_0|_v^{n_v d}, |x_1|_v^{n_v d}, \ldots, |x_m|_v^{n_v d}\} \\
= & H_K(P)^d.
\end{aligned}$$

□

Die im vorstehenden Lemma ausgedrückte Abhängigkeit vom Körper wird durch die folgende Definition überwunden.

DEFINITION 21.6. Es sei $P \in \mathbb{P}^m(\overline{\mathbb{Q}})$ und sei $K$ ein Zahlkörper, über den der Punkt $P$ definiert ist. Dann nennt man

$$H(P) := H_K(P)^{\frac{1}{\operatorname{grad}_{\mathbb{Q}} K}} = \sqrt[\operatorname{grad}_{\mathbb{Q}} K]{H_K(P)}$$

die *absolute Höhe* von $P$.

Wegen Lemma 21.5 und der Gradformel gilt für eine Körperkette $\mathbb{Q} \subseteq K \subseteq L$ und einen Punkt $P \in \mathbb{P}^m(K)$

$$\begin{aligned}
H(P) &= H_K(P)^{1/\operatorname{grad}_{\mathbb{Q}} K} \\
&= H_K(P)^{\operatorname{grad}_K L/(\operatorname{grad}_{\mathbb{Q}} K)(\operatorname{grad}_K L)} \\
&= \left(H_K(P)^{\operatorname{grad}_K L}\right)^{1/(\operatorname{grad}_{\mathbb{Q}} K)(\operatorname{grad}_K L)} \\
&= H_L(P)^{1/\operatorname{grad}_{\mathbb{Q}} L},
\end{aligned}$$

also ist die absolute Höhe in der Tat unabhängig vom Körper. Zur Berechnung der absoluten Höhe eines Punktes $P \in \mathbb{P}^m_{\overline{\mathbb{Q}}}$ wählt man eine beliebige endliche Körpererweiterung $\mathbb{Q} \subseteq K$, über den der Punkt definiert ist, und bestimmt

$$\begin{aligned} H(P) &= \prod_{v \in M_K} \max\{|x_0|_v^{n_v}, |x_1|_v^{n_v}, \ldots, |x_m|_v^{n_v}\}^{\frac{1}{\operatorname{grad}_{\mathbb{Q}} K}} \\ &= \prod_{v \in M_K} \max\{|x_0|_v^{\frac{n_v}{\operatorname{grad}_{\mathbb{Q}} K}}, |x_1|_v^{\frac{n_v}{\operatorname{grad}_{\mathbb{Q}} K}}, \ldots, |x_m|_v^{\frac{n_v}{\operatorname{grad}_{\mathbb{Q}} K}}\}. \end{aligned}$$

Beispiel 21.7. Wir betrachten in $\mathbb{P}^1(\mathbb{Q}[\sqrt[d]{2}])$ den Punkt $(\sqrt[d]{2}, 1)$. Der Grad der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[d]{2}])$ ist $d$. Für einen Betrag $|-|_v$ auf $\mathbb{Q}[\sqrt[d]{2}]$ oberhalb des archimedischen Absolutbetrages ist $|2|_v = 2$ und das ist auch die absolute Höhe (die man ja in diesem Fall direkt über $\mathbb{Q}$ ausrechnen kann). Die absolute Höhe von $(\sqrt[d]{2}, 1)$ ist $\sqrt[d]{2}$ wegen der Potenzierungseigenschaft, siehe Lemma 21.8 (1). Ohne Gradbeschränkung gibt es also unendlich viele Punkte in $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ mit einer absoluten Höhe $\leq 2$.

Lemma 21.8. *Die absolute Höhe besitzt auf*

$$\overline{\mathbb{Q}} = \mathbb{A}^1_{\overline{\mathbb{Q}}} \subseteq \mathbb{P}^1_{\overline{\mathbb{Q}}}$$

*(es wird also $x \in \overline{\mathbb{Q}}$ als $(x, 1) \in \mathbb{P}^1_{\overline{\mathbb{Q}}}$ aufgefasst) folgende Eigenschaften.*

(1) *Es ist $H(x^k) = H(x)^k$ für $k \in \mathbb{N}$.*
(2) *Es ist $H(xy) \leq H(x)H(y)$.*
(3) *Es ist $H(x+y) \leq H(x) + H(y)$.*
(4) *Es ist $H(x) = H(x^{-1})$ für $x \neq 0$.*

*Beweis.* Die Elemente seien jeweils aus einem Zahlkörper $K$ mit der Standardbetragsmenge $M_K$.

(1) Man macht für jeden Betrag $v \in M_K$ die Fallunterscheidung, ob

$$|x|_v \geq 1$$

ist oder nicht. Dies gilt dann auch für $\left|x^k\right|_v^{n_v}$ und für $\left|x^k\right|_v^{n_v/\operatorname{grad}_{\mathbb{Q}} K}$, woraus die Aussage folgt.

(2) Es sei $v$ ein Betrag. Bei $\max\{|x|_v^{n_v}, 1\}, \max\{|y|_v^{n_v}, 1\} \geq 1$ ist die Aussage klar, ebenso wenn die beiden $v$-Faktoren $\leq 1$ sind. Sei also $|x|_v^{n_v} > 1 > |y|_v^{n_v}$. Dann ist

$$\begin{aligned} \max\{|xy|_v^{n_v}, 1\} &= \max\{|x|_v^{n_v} |y|_v^{n_v}, 1\} \\ &\leq \max\{|x|_v^{n_v}, 1\} \\ &= |x|_v^{n_v} \\ &= |x|_v^{n_v} \cdot \max\{|y|_v^{n_v}, 1\} \\ &= \max\{|x|_v^{n_v}, 1\} \cdot \max\{|y|_v^{n_v}, 1\}. \end{aligned}$$

(3) Dies folgt durch eine Fallunterscheidung für die archimedischen und die nichtarchimedischen Beträge. Für die archimedischen Beträge verwendet man die Subadditivität des Potenzierens mit dem Exponenten

$$\alpha \;=\; \frac{n_v}{\operatorname{grad}_{\mathbb{Q}} K} \;\leq\; 1.$$

Eine Fallunterscheidung entlang dem Vergleich zu 1 ergibt

$$\begin{array}{rcl} \max\{|x+y|_v^{\alpha}, 1\} & \leq & \max\{|x|_v^{\alpha} + |y|_v^{\alpha}, 1\} \\ & \leq & \max\{|x|_v^{\alpha}, 1\} + \max\{|y|_v^{\alpha}, 1\}. \end{array}$$

(4) Wir vergleichen die Höhe bezüglich $K$. Nach Satz Anhang 4.3 ist

$$1 \;=\; \prod_v |x|_v^{n_v} \;=\; \prod_{v,\,|x|_v>1} |x|_v^{n_v} \cdot \prod_{v,\,|x|_v<1} |x|_v^{n_v}.$$

Somit ist

$$\begin{array}{rcl} H_K(x) & = & \displaystyle\prod_v \max\{|x|_v^{n_v}, 1\} \\ & = & \displaystyle\prod_{v,\,|x|_v>1} |x|_v^{n_v} \\ & = & \displaystyle\left( \prod_{v,\,|x|_v<1} |x|_v^{n_v} \right)^{-1} \\ & = & \displaystyle\left( \prod_{v,\,|x|_v<1} \left|x^{-1}\right|_v^{n_v} \right) \\ & = & \displaystyle\prod_{v,\,|x^{-1}|_v>1} \left|x^{-1}\right|_v^{n_v} \\ & = & \displaystyle\prod_v \max\{\left|x^{-1}\right|_v^{n_v}, 1\} \\ & = & H_K(x^{-1}). \end{array}$$

□

## Der Schrankensatz

LEMMA 21.9. *Es sei* $P = a_dT^d + \cdots + a_1T + a_0 \in \mathbb{Q}[T]$ *ein Polynom vom Grad* $d$ *mit einer Faktorzerlegung*

$$P \;=\; a_d(T-x_1)\cdots(T-x_d)$$

*mit* $x_j \in \overline{\mathbb{Q}}$. *Dann gelten für die absolute Höhe die Abschätzungen*

$$2^{-d}\prod_{j=1}^{d} H(x_j) \;\leq\; H(a_0,\ldots,a_d) \;\leq\; 2^{d-1}\prod_{j=1}^{d} H(x_j).$$

*Beweis.* Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

Der folgende Satz besagt, dass man mit Hilfe der absoluten Höhe und dem Grad der Körpererweiterung endliche Punktmengen beschreiben kann.

SATZ 21.10. *Zu jeder vorgegebenen Gradschranke $d \in \mathbb{N}_+$ und jeder Höhenschranke $S \in \mathbb{R}_+$ ist die Menge*

$$\left\{P \in \mathbb{P}^1(\overline{\mathbb{Q}}) \mid P \text{ besitzt Koordinaten in } K \text{ und } \operatorname{grad}_{\mathbb{Q}} K \leq d \text{ und } H(P) \leq S\right\}$$

*endlich.*

*Beweis.* Wir müssen nur Punkte der Form $(x,1)$ betrachten. Es seien die Schranken $d$ und $S$ fixiert und sei $(x,1)$ unterhalb der Schranke. D.h. dass $x$ in einer Körpererweiterung $\mathbb{Q} \subseteq K$ liegt, deren Grad $\leq d$ ist, und $H(x) \leq S$. Es sei $P = T^e + a_{e-1}T^{e-1} + \cdots + a_1T + a_0 \in \mathbb{Q}[T]$ das Minimalpolynom zu $x$, dessen Grad $e \leq d$ sei. Es liegt dann in $\overline{\mathbb{Q}}$ die Faktorzerlegung (mit $x_1 = x$)

$$P = (T - x_1)(T - x_2)\cdots(T - x_e)$$

vor. Nach Aufgabe 21.14 stimmt die Höhe der $x_i$ mit der Höhe von $x$ überein. Nach Lemma 21.9 ist

$$H(a_0, \ldots, a_{e-1}, 1) \leq 2^{e-1} \prod_{j=1}^{e} H(x_j) = 2^{e-1} H(x)^e \leq (2S)^d.$$

Nach Aufgabe 21.13 unterbieten nur endlich viele $\mathbb{Q}$-rationale Punkte $(a_0, \ldots, a_{e-1}, 1)$ eine vorgegebene Höhenschranke. Somit kommen nur endlich viele Polynome als Minimalpolynome in Frage und diese haben jeweils nur endlich viele Nullstellen. □

Der Satz gilt auch für höherdimensionale projektive Räume.

# Abbildungsverzeichnis