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

Elliptische Kurven

Vorlesung 20

in dieser Vorlesung besprechen wir zwei esentliche Hilfsmittel zum Beweis des Satzes von Mordell-Weil, nämlich die sogenannten (schwachen) Höhenfunktionen auf einer kommutativen Gruppe, mit denen man die endliche Erzeugtheit der Gruppe nachweisen kann, und die Beträge auf Zahlkörpern, mit denen man auf dem projektiven Raum und dann auch auf elliptischen Kurven Höhenfunktionen konstruieren kann.

Höhenfunktionen auf einer Gruppe

DEFINITION 20.1. Es sei G eine kommutative Gruppe und sei

$$h\colon G \longrightarrow \mathbb{R}_{\geq 0}$$

eine Funktion. Wir nennen h eine *schwache Höhenfunktion*, wenn folgende Eigenschaften erfüllt sind.

(1) Zu $P \in G$ gibt es eine reelle Zahl S_1 derart, dass
$$h(P+Q) \leq 2h(Q) + S_1$$
für alle $Q \in G$ gilt.

(2) Es gibt eine natürliche Zahl $m \in \mathbb{N}_{\geq 2}$ und eine Konstante S_2 derart, dass
$$h(mP) \geq m^2 h(P) - S_2$$
für alle $P \in G$ gilt.

(3) Für jede Schranke S ist die Menge
$$\{x \in G \mid h(x) \leq S\}$$
endlich.

Wenn man die Rolle des m aus Teil (2) betonen möchte, so spricht man von einer schwachen Höhenfunktion für die m-Vervielfachung.

BEISPIEL 20.2. Auf dem $\mathbb{Z}^n$ induzierte jede Norm auf $\mathbb{R}^n$ über $h(P) = \|P\|^2$ eine schwache Höhenfunktion. Die Endlichkeitsbedingung (3) ist klar (man denke etwa an die Maximumsnorm). Die Dreiecksabschätzung ergibt

$$\begin{aligned} h(P+Q) &= \|P+Q\|^2 \\ &\leq (\|P\| + \|Q\|)^2 \\ &= \|P\|^2 + \|Q\|^2 + 2\|P\| \cdot \|Q\| \\ &= h(Q) + \|P\|^2 + 2\|P\| \cdot \|Q\| \\ &\leq 2h(Q) + S_1, \end{aligned}$$

wobei die letzte Abschätzung darauf beruht, dass bei fixiertem P bis auf endlich viele Ausnahmen $\|P\| \leq \frac{1}{2}\|Q\|$ gilt. In der Eigenschaft (2) gilt Gleichheit mit $S_2 = 0$,

LEMMA 20.3. *Es sei G eine kommutative Gruppe und sei $m \geq 2$ eine fixierte natürliche Zahl. Dann ist G genau dann endlich erzeugt, wenn G eine schwache Höhenfunktion für die m-Vervielfachung besitzt und die Restklassengruppe G/mG endlich ist.*

Beweis. Sei zunächst G endlich erzeugt. Dann ist nach dem Hauptsatz über endlich erzeugte abelsche Gruppen

$$G = \mathbb{Z}^r \times T$$

mit einer endlichen Torsionsgruppe T. Wir betrachten

$$\mathbb{Z}^r \times T \xrightarrow{p_1} \mathbb{Z}^r \hookrightarrow \mathbb{R}^r .$$

Dann ergibt jede Norm auf $\mathbb{R}^r$ im Quadrat genommen eine schwache Höhenfunktion auf G, siehe Beispiel 20.2. Ferner ist

$$G/mG = \mathbb{Z}^r \times T/m(\mathbb{Z}^r \times T) = (\mathbb{Z}/(m))^r \times T/mT$$

endlich.

Zum Beweis der Umkehrung sei eine schwache Höhenfunktion h gegeben und sei $A \subseteq G$ ein Repräsentantensystem für die nach Voraussetzung endliche Restklassengruppe G/mG. Zu jedem $a \in A$ gibt es eine reelle Zahl $S_1(a)$ derart, dass

$$h(-a+Q) \leq 2h(Q) + S_1(a)$$

für alle $Q \in G$. Wir setzen

$$S := S_2 + \max\{S_1(a),\, a \in A\},$$

wobei S_2 von der zweiten Eigenschaft einer schwachen Höhenfunktion herrührt. Zu jedem $P \in G$ gibt es ein $a \in A$ mit $[P] = [a]$ in G/mG, daher gibt es ein $P' \in G$ mit $P = mP' + a$ in G. Dabei gilt

$$\begin{aligned} h(P') &\leq \frac{1}{m^2}(h(mP') + S_2) \\ &= \frac{1}{m^2}(h(P-a) + S_2) \\ &\leq \frac{1}{m^2}(2h(P) + S(-a) + S_2) \\ &\leq \frac{1}{m^2}(2h(P) + S). \end{aligned}$$

Die Konstruktion

$$P = mP' + a$$

können wir iterieren, wir setzen $P_0 = P$,

$$\begin{aligned} P_0 &= mP_1 + a_1, \\ P_1 &= mP_2 + a_2, \end{aligned}$$

etc. Dabei gilt die rekursive Abschätzung

$$h(P_{n+1}) \leq \frac{1}{m^2}(2h(P_n)+S)$$

und somit unter Verwendung der geometrischen Reihe

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{S}{m^2}\left(1+\frac{2}{m^2}+\left(\frac{2}{m^2}\right)^2+\cdots+\left(\frac{2}{m^2}\right)^{n-1}\right) \\ &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{S}{m^2}\cdot\frac{m^2}{m^2-2} \\ &\leq \left(\frac{1}{2}\right)^n h(P) + \frac{S}{m^2-2}. \end{aligned}$$

Für n hinreichend groß ist somit

$$h(P_n) \leq 1+\frac{S}{2}.$$

Es ist daher

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} a_j$$

mit gewissen $a_j \in A$ und somit ist insgesamt die endliche Menge

$$A \cup \left\{ Q \in G \mid h(Q) \leq 1+\frac{S}{2} \right\}$$

ein Erzeugendensystem der Gruppe. □

Bewertungen und Beträge auf einem Zahlkörper

Definition 20.4. Es sei K ein Körper. Eine Funktion

$$|-| : K \longrightarrow \mathbb{R},\ f \longmapsto |f|$$

heißt *Betrag* (oder *Absolutbetrag*) auf K, wenn die folgenden Bedingungen erfüllt sind.

(1) Es ist $|f| \geq 0$ für alle f.
(2) Es ist $|f| = 0$ genau dann, wenn $f = 0$ ist.
(3) Es ist
$$|fg| = |f| \cdot |g|.$$
(4) Es ist
$$|f+g| \leq |f| + |g|.$$

Beispielsweise ist der übliche Betrag auf den rationalen oder reellen oder komplexen Zahlen ein Absolutbetrag in diesem Sinne.

Beispiel 20.5. Es sei K ein Zahlkörper und sei $K \to \mathbb{K}$ eine reelle oder komplexe Einbettung. Dann induziert der gewöhnliche Betrag einen Betrag auf K.

Zu einer komplexen Einbettung definiert dabei die konjugiert-komplexe Einbettung den gleichen Betrag auf K.

Mit der Festlegung

$$d(f,g) = |f-g|$$

wird ein Körper mit einem Betrag zu einem metrischen Raum, siehe Aufgabe 20.2.

Zu einem Primideal $\mathfrak{p}$ in einem Zahlbereich R zu einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ ist $R_{\mathfrak{p}}$ nach Korollar 22.18 (Zahlentheorie (Osnabrück 2016-2017)) ein diskreter Bewertungsring und die zugehörige Ordnung

$$K \setminus \{0\} \longrightarrow \mathbb{Z},\ f \longmapsto \operatorname{ord}_{\mathfrak{p}}(f),$$

besitzt die Eigenschaften

(1) $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
(2) $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$. Häufig setzt man

$$\operatorname{ord}(0) = \infty.$$

Lemma 20.6. *Es sei R ein Zahlbereich, $\mathfrak{p} \subseteq R$ ein maximales Ideal und $\operatorname{ord}(-)$ die zugehörige Bewertung auf $K = Q(R)$. Dann ist zu einer reellen Zahl $a > 1$ durch*

$$|f|_{\mathfrak{p}} := a^{-\operatorname{ord}(f)}$$

ein Betrag auf K gegeben (hierbei ist $a^{-\infty}$ als 0 zu interpretieren).

Beweis. Die drei ersten Eigenschaften eines Betrages folgen unmittelbar aus grundlegenden Gesetzen, siehe Lemma 27.8 (Grundkurs Mathematik (Osnabrück 2018-2019)) und Lemma 27.9 (Grundkurs Mathematik (Osnabrück 2018-2019)). Die Dreiecksabschätzung folgt aus

$$\begin{aligned} |f+g|_{\mathfrak{p}} &= a^{-\operatorname{ord}(f+g)} \\ &\leq a^{-\min(\operatorname{ord}(f),\operatorname{ord}(g))} \\ &= a^{\max(-\operatorname{ord}(f),-\operatorname{ord}(g))} \\ &= \max\left(a^{-\operatorname{ord}(f)}, a^{-\operatorname{ord}(g)}\right) \\ &\leq a^{-\operatorname{ord}(f)} + a^{-\operatorname{ord}(g)} \\ &= |f|_{\mathfrak{p}} + |g|_{\mathfrak{p}}. \end{aligned}$$

□

Definition 20.7. Ein Betrag

$$|-| : K \longrightarrow \mathbb{R}$$

auf einem Körper K heißt *archimedisch*, wenn die Menge $\mathbb{N}$ in K nicht beschränkt ist.

Ein Betrag ist genau dann nichtarchimedisch, wenn die Dreiecksabschäzung in der verschärften Form

$$|f+g| \leq \max(|f|, |g|)$$

gilt, siehe Aufgabe 20.9. In Lemma 20.6 wurde mitbewiesen, dass die Beträge, die von einer Bewertung herrühren, nichtarchimedisch sind.

Bemerkung 20.8. Die gewählte Basis a in Lemma 20.6 spielt dabei für die topologischen Eigenschaften des Betrags keine wesentliche Rolle. Um aber ein sinnvolles funktorielles (bezüglich von endlichen Körpererweiterungen) Verhalten zu erhalten, sind verschiedene Normierungen sinnvoll. Die wichtigsten Möglichkeiten sind die folgenden, wobei wir die Notation von Lemma 20.6 übernehmen und wobei $N(\mathfrak{p})$ die Norm von $\mathfrak{p}$ bezeichnet, also die Anzahl der Elemente im Restklassenkörper $R/\mathfrak{p}$.

(1)
$$|h|_{\mathfrak{p},\text{ nat}} := N(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(h)}.$$
Dies ist wohl der natürlichste Betrag.

(2)
$$|h|_{\mathfrak{p}} := N(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(h)/e(\mathfrak{p})f(\mathfrak{p})},$$
wobei $e = e(\mathfrak{p})$ den Verzweigungsindex und $f = f(\mathfrak{p})$ Trägheitsgrad von $\mathfrak{p}$ über $(p) = \mathbb{Z} \cap \mathfrak{p}$ bezeichnet. Diese Normierung besitzt den Vorteil, dass die Einschränkung dieses Betrages auf $\mathbb{Q}$ den nichtarchimedischen Standardbetrag
$$|h|_p = p^{-\operatorname{ord}_p(h)}$$
ergibt, es sich also um eine Ausdehnung eines rationalen Standardbetrages handelt. Mit $h = gp^\alpha$ in $\mathbb{Q}$, $\alpha \in \mathbb{Z}$, $\operatorname{ord}_p(g) = 0$, ist ja $\operatorname{ord}_{\mathfrak{p}}(p) = e$ und $N(\mathfrak{p}) = p^f$ und somit
$$\begin{aligned} |h|_{\mathfrak{p}} &:= N(\mathfrak{p})^{\frac{-\operatorname{ord}_{\mathfrak{p}}(gp^\alpha)}{ef}} \\ &= N(\mathfrak{p})^{\frac{-\alpha\operatorname{ord}_{\mathfrak{p}}(p)}{ef}} \\ &= \left(p^f\right)^{\frac{-\alpha e}{ef}} \\ &= p^{-\alpha}. \end{aligned}$$
Zwischen dem natürlichen Betrag aus (1) und dem Standardbetrag aus (2) besteht somit insbesondere der Zusammenhang
$$|h|_{\mathfrak{p}\text{ nat}} = |h|_{\mathfrak{p}}^{ef} = |h|_{\mathfrak{p}}^{n_{\mathfrak{p}}},$$
wobei wir eben
$$n_{\mathfrak{p}} = ef$$
setzen. Diese Zahl stimmt mit dem sogenannten lokalen Grad überein.

(3) Der absolute Betrag ist
$$|h|_{\mathfrak{p}\text{ abs}} := N(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(h)/\operatorname{grad}_{\mathbb{Q}} K}.$$
Diese Normierung berücksichtigt, dass über dem Primideal (p) aus $\mathbb{Z}$ in R mehrere Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ liegen, die jeweils zu Beträgen

in K Anlass geben und sich sozusagen der eine standardisierte Betrag $|-|_p$ auf mehrere Beträge verteilt. Nach Satz 20.4 (Algebraische Zahlentheorie (Osnabrück 2020-2021)) gilt dabei

$$\operatorname{grad}_{\mathbb{Q}} K = \sum_{j=1}^{k} e_j f_j.$$

Somit ist, wieder mit $h = gp^{\alpha}$ wie oben,

$$\begin{aligned}
\prod_{j=1}^{k} |h|_{\mathfrak{p}_j \text{ abs}} &= \prod_{j=1}^{k} N(\mathfrak{p}_j)^{\frac{-\operatorname{ord}_{\mathfrak{p}_j}(h)}{\operatorname{grad}_{\mathbb{Q}} K}} \\
&= \prod_{j=1}^{k} \left(p^{f_j}\right)^{\frac{-\operatorname{ord}_{\mathfrak{p}_j}(p^{\alpha})}{\operatorname{grad}_{\mathbb{Q}} K}} \\
&= \prod_{j=1}^{k} \left(p^{f_j}\right)^{\frac{-\alpha e_j}{\operatorname{grad}_{\mathbb{Q}} K}} \\
&= \prod_{j=1}^{k} p^{\frac{-\alpha e_j f_j}{\operatorname{grad}_{\mathbb{Q}} K}} \\
&= p^{\frac{-\alpha \sum_{j=1}^{k} e_j f_j}{\operatorname{grad}_{\mathbb{Q}} K}} \\
&= p^{-\alpha} \\
&= |h|_p .
\end{aligned}$$

Definition 20.9. Unter $M_{\mathbb{Q}}$ versteht man die Menge bestehend aus dem archimedischen Standardbetrag

$$|-| = |-|_{\infty}$$

und aus den Beträgen $|-|_p$ zu jeder Primzahl p, die durch

$$|f|_p := p^{-\operatorname{ord}_p(f)}$$

gegeben sind.

Definition 20.10. Es sei K ein Zahlkörper. Mit M_K bezeichnet man die Menge der Beträge auf K, deren Einschränkung auf $\mathbb{Q}$ mit einem rationalen Standardbetrag übereinstimmt.

Man spricht von den Standardbeträgen auf K. Die 1 hat unter jedem Standardbetrag den Wert 1. Das gleiche gilt für jede Einheit aus dem Ring der ganzen Zahlen zu K.

Definition 20.11. Zu einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ und einem Betrag $v \in M_K$ nennt man den Grad der Körpererweiterung der Komplettierungen $\mathbb{Q}_v \subseteq K_v$ den *lokalen Grad* in v.

Zu $v \in M_K$ schreibt man auch

$$\|-\|_v = |-|_v^{n_v},$$

wobei n_v den lokalen Grad bezeichnet. Für einen nichtarchimedischen Betrag zu einem Primideal $\mathfrak{p}$ (aus dem Zahlbereich R zu K) über (p) ist n_v das Produkt aus Trägheitsgrad, also dem Grad der Körpererweiterung

$$\mathbb{Z}/(p) \subseteq \kappa(\mathfrak{p})$$

und dem Verzweigungsindex von

$$\mathbb{Z}_{(p)} \subseteq R_{\mathfrak{p}}.$$

Bei einem archimedischen Betrag ist der lokale Grad 1 im reellen und 2 im komplexen Fall.

Abbildungsverzeichnis