

Algebraische Zahlentheorie

SS 2013

- Kuhlmann -

23. Vorlesung am 11.07.2013

Sei $L/\mathbb{Q}$ Zahlkörper vom Grad n . Ansatz wie in der 22. Vor.
Wir wollen nun das Gitter $\mathcal{O}(\alpha) \subseteq L_{\mathbb{R}}$ studieren.

Bemerkung 1 Sei $\Gamma \subseteq \mathbb{R}^n$ vollständiges Gitter
mit Basis $\{v_1, \dots, v_n\}$ und F.P. T_{Γ} .

$$\text{Es ist: } v(T_{\Gamma}) = \left| \det \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right|$$

üA **ÜB 12.**

Wir können Bemerkung 1 anwenden mit $\Gamma = \mathcal{O}(\alpha)$;

Wir berechnen:

$$v(T_{\mathcal{O}(\alpha)}) = |\det A| = \left| \left(\frac{1}{2} (i) \right)^t \det V \right|$$

Andererseits ist

$$\left(\det V \right)^2 \underset{\text{Auf 7.1}}{=} D(d_1, \dots, d_n) \underset[21. \text{ Vor}]{\overset{\text{Prop 3}}{=}} N(\alpha)^2 D(\mathcal{O}_L/\mathbb{Z}).$$

Alles zusammen ergibt:

$$v(T_{\mathcal{O}(\alpha)}) = 2^{-t} N(\alpha) \sqrt{D(\mathcal{O}_L/\mathbb{Z})}$$

Bemerkung 2. Sei $\tau \in \mathbb{R}_+$ und setze

$$X_\tau := \left\{ (x_1, \dots, x_s; z_1, \dots, z_t) \in L_{\mathbb{R}} \mid \sum_{i=1}^s |x_i| + 2 \sum_{j=1}^t |z_j| < \tau \right\}.$$

Dann ist X_τ beschränkt, konvex, symmetrisch, und

$$v(X_\tau) = 2^s \left(\frac{\pi}{2}\right)^t \frac{\tau^n}{n!}.$$

ÜA ÜB 12.

18

Wir können nun zeigen eine genauere Aussage

über die Minkowski Schranke (Satz 2 22. Vor)

Satz 1 (Explizite Minkowski Schranke).

Sei $0 \neq \alpha \in \mathcal{O}_L$, $\exists 0 \neq \alpha \in \mathcal{O}_L$ so dass

$$|N_{L/\mathbb{Q}}(\alpha)| \leq \underbrace{\left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{D(\mathcal{O}_L/\mathbb{Z})}}_{:= C_L} N(\alpha)$$

Beweis: Wir wollen Minkowski's Satz anwenden auf (Satz 4 20. Vor)

$\Gamma := b(\alpha)$ und $X_\tau \in L_{\mathbb{R}}$ für geeignetes τ .

Wir bemerken jetzt schon:

Wenn ① $v(X_\tau) > 2^n v(T_{b(\alpha)})$ dann

② $\exists d \neq 0, d \in \alpha$ s.d. $b(d) \in X_\tau$, d.h.

s.d. $(b_1(d), \dots, b_s(d); b_{s+1}(d), \dots, b_{s+t}(d)) \in X_\tau$,

$$\text{d.h. } \sum_{i=1}^s |b_i(d)| + 2 \sum_{j=1}^t |b_{s+j}(d)| < \tau \quad (*)$$

Erinnerung: AGU

Seien $a_1, \dots, a_m \in \mathbb{R}_+$, $m \in \mathbb{N}$. Es ist:

$$\left(\prod_{i=1}^m a_i \right)^{1/m} \leq \frac{1}{m} \left(\sum_{i=1}^m a_i \right)$$

Setze $a_j := |b_j(d)|$ $j=1, \dots, s$ und

$a_{s+1} = a_{s+2} = |b_{s+1}(d)|$ und

$\vdots$

$a_{s+2t-1} = a_{s+2t} = |b_{s+t}(d)|$.

$= a_{m-1}$

$= a_m$

(*) bedeutet: $\sum_{l=1}^m a_l < \tau$. Die AGU impliziert

nun daß

$$n (a_1 \dots a_n)^{1/n} < \tau \text{ i.e.}$$

$$\prod_{i=1}^n a_i < \frac{\tau^n}{n^n}; \text{ d. h.}$$

$$|N_{L/Q}(\alpha)| = \prod_{i=1}^n a_i < \frac{\tau^n}{n^n}$$

Begründung:

$$\prod_{i=1}^s a_i = \prod_{i=1}^s |b_i(\alpha)| \prod_{j=1}^t |b_{s+j}(\alpha)|^2$$

Andererseits ist:

$$|b_{s+j}(\alpha)|^2 = |b_{s+j}(\alpha)| \cdot \overline{|b_{s+j}(\alpha)|},$$

$$\begin{aligned} \text{so daß } \prod_{i=1}^s a_i &= \left| \prod_{i=1}^s b_i(\alpha) \prod_{j=1}^t b_{s+j}(\alpha) \overline{b_{s+j}(\alpha)} \right| \\ &= \left| \prod_{i=1}^s b_i(\alpha) \prod_{j=1}^t b_{s+j}(\alpha) \prod_{j=1}^t \overline{b_{s+j}(\alpha)} \right| \\ &= |N_{L/Q}(\alpha)| \end{aligned}$$

weil $b_1, \dots, b_s, b_{s+1}, \overline{b_{s+1}}, \dots, b_{s+t}, \overline{b_{s+t}}$

alle Einbettungen über $\mathbb{Q}$ von L in $\mathbb{C}$ sind.]

Zusammenfassung:

① Ist $N(X_\tau) > 2^n N(T_0(\alpha))$ dann

② $\exists 0 \neq \alpha \in \mathfrak{a}$ s.d. $|N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n}$

oder

① Ist $2^s (\pi/2)^t \frac{\tau^n}{n!} > 2^n 2^{-t} N(\alpha) \sqrt{D(\mathcal{O}_L/\mathbb{Z})}$

dann ② gilt. Wir analysieren die Bedingung

① nun genauer:

$$\textcircled{1} \Leftrightarrow \tau^n > n! 2^{-s} 2^n 2^{-t} 2^t \pi^{-t} N(\alpha) \sqrt{D(\mathcal{O}_L/\mathbb{Z})}$$

$$\text{d.h. } \tau^n > n! 2^{n-s} \pi^{-t} N(\alpha) \sqrt{D(\mathcal{O}_L/\mathbb{Z})}$$

$$\text{d.h. } \tau^n > n! 2^{2t} \pi^{-t} N(\alpha) \sqrt{D(\mathcal{O}_L/\mathbb{Z})}$$

→ Wir haben bewiesen:

$$\text{Ist } \tau^n > n! \left(\frac{4}{\pi}\right)^t N(\alpha) \sqrt{D(\mathcal{O}_L/\mathbb{Z})} \quad \textcircled{1}$$

$$\text{dann } \exists 0 \neq \alpha \in \mathfrak{a} \text{ mit } |N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n} \quad \textcircled{2}.$$

Für jedes τ wie in ① definiere

$$A_\tau := \left\{ 0 \neq \alpha \in \mathfrak{a} \mid |N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n} \right\}$$

Dann ist $A_\tau \neq \emptyset$, $|A_\tau| < \infty [da \alpha \in X_\tau \cap \mathfrak{a}]$,

$$\tau_1 < \tau_2 \Rightarrow A_{\tau_1} \subseteq A_{\tau_2}.$$

Aus diesen Eigenschaften folgern wir daß

$\bigcap A_\tau \neq \emptyset$: Sei τ_0 so daß $|A_{\tau_0}| \leq |A_\tau|$ für
 $\{\tau \text{ erfüllt } \textcircled{1}\}$ alle τ die $\textcircled{1}$ erfüllen. Dann ist
 $\bigcap A_\tau = A_{\tau_0} \neq \emptyset$. $\square$

Sei nun $\alpha \in \bigcap A_\tau$. Wir behaupten daß

$$|N_{L/\mathbb{Q}}(\alpha)| \leq C_L N(\alpha).$$

da $0 \neq \alpha \in \bigcap A_\tau$ ist gilt

$$|N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n} \quad \forall \tau \text{ die } \textcircled{1} \text{ erfüllen.}$$

Es folgt:

$$|N_{L/\mathbb{Q}}(\alpha)| \leq \inf_{\{\tau \text{ erfüllt } \textcircled{1}\}} \left\{ \frac{\tau^n}{n^n} \right\} = \frac{1}{n^n} \inf_{\{\tau \text{ erfüllt } \textcircled{1}\}} \tau^n.$$

$$\text{Nun ist } \inf_{\{\tau \text{ erfüllt } \textcircled{1}\}} \tau^n = n! \left(\frac{4}{\pi} \right)^t N(\alpha) \sqrt{D(\mathcal{O}_L/\mathbb{Z})}. \quad \square$$