Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

25.Vorlesung

27 Juli 2017

Ziel: $\lambda(\mathcal{O}_L^\times) \subseteq H$ ist ein vollständiges Gitter. Es genügt dafür, $\epsilon_1, \ldots, \epsilon_{s+t-1} \in \mathcal{O}_L^\times$ zu finden, so daß $\{\lambda(\epsilon_1), \ldots, \lambda(\epsilon_{s+t-1})\} \subseteq H$ $\mathbb{R}$-linear unabhängig ist. Diese letzte Vorlesung hat als Hauptziel, die folgende Proposition 25.1 zu beweisen und daraus D.E.S zu folgern.

Proposition 25.1
$\exists \epsilon_1, \ldots, \epsilon_{s+t-1} \in \mathcal{O}_L^\times$, so daß $|\sigma_l(\epsilon_k)| < 1$ für $l \neq k, l = 1, \ldots, s+t, k = 1, \ldots, s+t-1$.

Beweis. Später. □

Wir können nun schon Aufgrund von Proposition 25.1 den Beweis für D.E.S fortsetzen. Seien $\epsilon_1, \ldots, \epsilon_{s+t-1}$ wie in Proposition 25.1. Wir zeigen:

$$(*) \qquad \{\lambda(\epsilon_1), \ldots, \lambda(\epsilon_{s+t-1})\} \text{ ist linear unabhängig.}$$

Betrachte die Matrix A mit (k,l)-tem Eintrag
$A_{k,l} := \log|\sigma_l(\epsilon_k)|$, $k = 1, \ldots, s+t-1$, $l = 1, \ldots, s+t-1$.
Um $(*)$ zu beweisen, genügt es zu zeigen, daß A invertierbar ist. Durch elementare Spaltenumformungen (multipliziere die letzte $t-1$ Spalten mit 2) bekommen wie eine Matrix A' mit den folgenden Eigenschaften:

(i) $A'_{kl} < 0$ für $k \neq l$ $(|\sigma_l(\epsilon_k)| < 1 \Rightarrow \log|\sigma_l(\epsilon_k)| < 0)$

(ii) $\sum_l A'_{kl} > 0$ $(\sum_l A'_{kl} = \sum_{l=1}^{s} \log|\sigma_l(\epsilon_k)| + 2\sum_{l=s+1}^{s+t-1} \log|\sigma_l(\epsilon_k)| = -2\log|\sigma_{s+t}(\epsilon_k)|$, da $\lambda(\epsilon_k) \in H$.

Nun ist aber $\log|\sigma_{s+t}(\epsilon_k)| < 0$, also $-2\log|\sigma_{s+t}(\epsilon_k)| > 0$.)

Hilfslemma
Sei A' eine $m \times m$ matrix, die die Eigenschaften (i)+(ii) erfüllt. Dann ist A' invertierbar.

Beweis. ÜA □

Damit ist D.E.S bewiesen.

Wir müßen nur noch Proposition 25.1 beweisen. Ansatz wie in der 22 und 23 Vorlesung.

Bemerkung 1. $L_\mathbb{R}$ ist nicht nur ein $\mathbb{R}$-Vektorraum, sondern eine $\mathbb{R}$-Algebra (mit Komponentenweise Multiplikation versehen).

2. Für $x \in L_\mathbb{R}$ definiere die "Norm von x" wie folgt:
$N(x) := \prod_{i=1}^{s} x_i \prod_{j=1}^{t} x_{s+j}\bar{x}_{s+j} = \prod_{i=1}^{s} x_i \prod_{j=1}^{t} |x_{s+j}|^2$.
(Bemerke, daß $N_{L/\mathbb{Q}}(\alpha) = N(\sigma(\alpha)) \forall \alpha \in L$, dies begründet die Terminologie "Norm von x".)

Unsere **Hauptbehauptung** nun ist: $\exists c > 0, c \in \mathbb{R}$ so daß $\forall x \in L_{\mathbb{R}}$ mit $\frac{1}{2} \leq |N(x)| \leq 1$, $\exists \epsilon \in \mathcal{O}_L^{\times}$, so daß $|x_l \sigma_l(\epsilon)| < \epsilon \quad \forall l = 1, \ldots, s+t$.

Bemerke, daß **Hauptbehauptung**$\Rightarrow$Proposition 25.1:

Beweis. für jedes $k = 1, \ldots, s+t-1$ wähle $x \in L_{\mathbb{R}}$ mit $|N(x)| = 1$ aber $|x_l| > c$ für $l \neq k$ (ausgleichen mit dem k-te Komponente). Unsere Hauptbehauptung liefert $\epsilon_k \in \mathcal{O}_L^{\times}$, so daß $|x_l \sigma_l(\epsilon_k)| < c \quad \forall l$. Insbesondere wenn $l \neq k$, ist $|\sigma_l(\epsilon_k)| < c/|x_l| < 1$ wie erwnüscht. $\square$

Wir bemühen uns letztendlich darum, die **Hauptbehauptung** zu beweisen. Wir werden dafür Minkowski's Satz anwenden.
Sei $x \in L_{\mathbb{R}}$ mit $N(x) \neq 0$. Wir zeigen zunächst, daß $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter in $L_{\mathbb{R}}$ ist. Bemerke: Da $\mathcal{O}_L \lhd \mathcal{O}_L$ ist, wissen wir schon, daß $\sigma(\mathcal{O}_L)$ ein vollständiges Gitter in $L_{\mathbb{R}}$ ist (siehe 22. Vorlesung), also daß $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter für $x = (1, \ldots, 1)$ ist.
Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$, also $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ ist $\mathbb{R}$-linear unabhängig und $x\sigma(\mathcal{O}_L) = x\sigma(\alpha_1)\mathbb{Z} \oplus \cdots \oplus x\sigma(\alpha_n)\mathbb{Z}$.
Wir zeigen: $\{x\sigma(\alpha_1), \ldots, x\sigma(\alpha_n)\}$ ist $\mathbb{R}$-linear unabhängig. Dafür betrachten wir wie immer die Matrix
$A = \begin{pmatrix} x\sigma(\alpha_1) \\ \vdots \\ x\sigma(\alpha_n) \end{pmatrix} \in \mathrm{Mat}_{n\times n}(\mathbb{R})$. Analogue Berechnungen wie früher zeigen, daß $|\det(A)| = 2^{-t}|\det \chi|$, wobei χ die Matrix mit i-te Zeile gleich

$$x_1\sigma_1(\alpha_i) \ldots x_s\sigma_s(\alpha_i) \quad x_{s+1}\sigma_{s+1}(\alpha_i) \quad \bar{x}_{s+1}\overline{\sigma_{s+1}(\alpha_i)} \ldots$$

ist. Wir wollen also $\det \chi$ berechnen. Jede Spalte hat einen gemeinsamen Faktor, und zwar entweder x_j oder $\bar{x}_j$, wir sehen also, daß $\det \chi = N(x) \det \mathcal{V}$, wobei wie immer $V_{ij} = \sigma_i(\alpha_j)$. Wir bekommen außerdem $0 \neq |\det(A)| = 2^{-t}|N(x)|\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ (siehe 21. Vorlesung). Also ist $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter und analogue Berechnungen wie in der 22. Vorlesung ergeben: $v(T_x) = |\det A| = 2^{-t}|N(x)|\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ (wobei $T_x :=$ f.P von $x\sigma(\mathcal{O}_L)$). Insbesondere wenn $\frac{1}{2} \leq |N(x)| \leq 1$, dann ist

$$(**) \qquad v(T_x) \leq 2^{-t}\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$$

(unabhängig von x)

- Sei nun $X \subseteq L_{\mathbb{R}}$ konvex symmetrisch beschränkt, so daß $v(X) > 2^n 2^{-t}\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ (z.B. $X = B_R(0)$ mit R groß genug)
- Sei $R \in \mathbb{R}_+$, so daß $|N(y)| < R \quad \forall y \in X$.
- Minkowski und $(**)$ ergeben:

$$(***) \qquad \forall x \in L_{\mathbb{R}} \text{ mit } \frac{1}{2} \leq |N(x)| \leq 1, \exists 0 \neq \alpha \in \mathcal{O}_L, \text{ so daß } x\sigma(\alpha) \in X$$

  (Minkowski mit Gitter $x\sigma(\mathcal{O}_L)$ und X anwenden)
- Betrachte nun $\mathcal{I} := \{\alpha\mathcal{O}_L \lhd \mathcal{O}_L \mid \exists x \in L_{\mathbb{R}}, \frac{1}{2} \leq |N(x)| \leq 1 \text{ und } x\sigma(\alpha) \in X\}$ ($\mathcal{I}$ ist wegen $(***)$ eine nicht leere Menge von Hauptidealen.)
- Wir berechnen: $\alpha\mathcal{O}_L \in \mathcal{I} \Rightarrow \exists x \in L_{\mathbb{R}}$, so daß $\frac{1}{2} \leq |N(x)| \leq 1$
  $|N(x\sigma(\alpha))| < R \Rightarrow |N(x)||N(\sigma(\alpha))| < R \Rightarrow |N(\sigma(\alpha))| < R/\frac{1}{2} = 2R$

- Wir haben berechnet : $\forall \alpha\mathcal{O}_L \in \mathcal{I}$ gilt $N(\alpha\mathcal{O}_L) < 2R$.
- Also ist $\mathcal{I}$ eine endliche Menge, d.h. $\mathcal{I} = \{\beta_1\mathcal{O}_L, \ldots, \beta_m\mathcal{O}_L\}$, $\beta_k \neq 0$.
- Sein nun $x \in L_{\mathbb{R}}$ mit $\frac{1}{2} \leq |N(x)| \leq 1$. $(***)$ liefert $0 \neq \alpha \in \mathcal{O}_L$, so daß $\alpha\mathcal{O}_L \in \mathcal{I}$, d.h. $\exists k$, so daß $\alpha\mathcal{O}_L = \beta_k\mathcal{O}_L$.
- Setze $\epsilon = \alpha\beta_k^{-1}$. Dann ist $x\sigma(\epsilon) = \underbrace{x\sigma(\alpha)}_{\in X}\sigma(\beta_k^{-1}) \in \sigma(\beta_k^{-1})X$.
- Wir haben gezeigt: $\forall x \in L_{\mathbb{R}}$ mit $\frac{1}{2} \leq |N(x)| \leq 1$, $\exists \epsilon \in \mathcal{O}_L^\times$, so daß $x\sigma(\epsilon) \in \bigcup_{k=1}^m \sigma(\beta_k^{-1})X$.
- Da X beschränkt ist, so ist $\sigma(\beta_k^{-1})X \quad \forall k = 1, \ldots, m$.
- Es folgt: $\bigcup_{k=1}^m \sigma(\beta_k^{-1})X$ ist beschränkt.
- Endlich wählen wir eine Schranke c für diese beschränkte Menge.