Algebraische Zahlentheorie

– SS 2013 – Kuhlmann –

– 25. Vorlesung am 18.07.2013 –

Ziel: Z.z.: $\lambda(\mathcal{O}_L^\times) \subseteq H$ ist vollständiges Gitter.
[Es genügt dafür $\varepsilon_1, \dots, \varepsilon_{s+t-1} \in \mathcal{O}_L^\times$ zu finden so daß $\{\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_{s+t-1})\} \subseteq H$ ist $\mathbb{R}$-linear unabhängig] Diese letzte Vorlesung hat als Hauptziel die folgende **Proposition 4** zu beweisen und daraus D.E.S zu folgern.

Proposition 4. $\exists\, \varepsilon_1, \dots, \exists\, \varepsilon_{s+t-1} \in \mathcal{O}_L^\times$ so daß $|\sigma_\ell(\varepsilon_k)| < 1$ für $\ell \neq k$, $\ell = 1, \dots, s+t$, $k = 1, \dots, s+t-1$.

Beweis: **später**

- Wir können nun schon (Aufgrund von **Proposition 4**) den Beweis für D.E.S fortsetzen.

Seien $\varepsilon_1, \dots, \varepsilon_{s+t-1}$ wie in Proposition 4. Wir zeigen daß
(✱) $\{\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_{s+t-1})\}$ linear unabhängig ist. Betrachte die Matrix A mit $k\ell$-te Eintrag

$$A_{k\ell} := \log |\sigma_\ell(\varepsilon_k)| \; ; \quad k = 1, \dots, s+t-1, \quad \ell = 1, \dots, s+t-1$$

Um (✱) zu beweisen genügt es z.z. daß A invertierbar ist. Durch elementare Spaltenumformungen (multipliziere die letzte $t-1$ Spalten mit 2) bekommen wir eine Matrix A' mit den folgenden **Eigenschaften**:

(i) $A'_{k\ell} < 0$ für $k \neq \ell$ $\quad [\,|\sigma_\ell(\varepsilon_k)| < 1 \Rightarrow \log|\sigma_\ell(\varepsilon_k)| < 0\,]$

(ii) $\sum_\ell A'_{k\ell} > 0$ $\quad [\,\sum_\ell A'_{k\ell} = \sum_{\ell=1}^{s} \log|\sigma_\ell(\varepsilon_k)| + 2\sum_{\ell=s+1}^{s+t-1} \log|\sigma_\ell(\varepsilon_k)|$

$= -2 \underbrace{\log | \sigma_{s+t}(\varepsilon_k)|}$ da $\chi(\varepsilon_k) \in H$.

Nun ist aber $\uparrow < 0$ also $-2 \log | \sigma_{s+t}(\varepsilon_k)| > 0$]

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

__Beweis__ ü A.

Damit ist D.E.S bewiesen.

Wir müssen nur noch Proposition 4 beweisen.
Ansatz wie in der 22. und 23. Vorlesungen.

__Bemerkungen__.

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

2. Für $x \in L_{\mathbb{R}}$ definiere die "Norm von x" folgend:
$$N(x) := \prod_{i=1}^{s} x_i \prod_{j=1}^{t} x_{s+j} \overline{x_{s+j}} = \prod_{i=1}^{s} x_i \prod_{j=1}^{t} |x_{s+j}|^2$$

[Bemerke daß
$$N_{L/\mathbb{Q}}(\alpha) = N(\sigma(\alpha)) \quad \forall \alpha \in L;$$ diese

begründet die Terminologie "Norm von x".]

Unsere **Hauptbehauptung** nun ist:
$\exists\, C > 0$ $C \in \mathbb{R}$ s.d. $\forall x \in L_{\mathbb{R}}$ mit $1/2 \leq |N(x)| \leq 1$
$\exists\, \varepsilon \in \mathcal{O}_L^\times$ s.d. $|x_\ell \sigma_\ell(\varepsilon)| < \varepsilon$ $\forall \ell = 1, \dots, s+t$

Bemerke daß: Hauptbehauptung $\Rightarrow$ Proposition 4:

Beweis: für jedes $k = 1, \dots, s+t-1$ 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 $\varepsilon_k \in \mathcal{O}_L^{\times}$

so daß $|x_l \, \sigma_l(\varepsilon_k)| < C \quad \forall l$.

Insbesondere wenn $l \neq k$ ist

$$|\sigma_l(\varepsilon_k)| < C / |x_l| < 1 \quad \text{wie erwünscht.} \; \blacksquare$$

Wir bemühen uns letzendlich 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 $\mathcal{O}_L \triangleleft \mathcal{O}_L$ ist wissen wir schon daß $\sigma(\mathcal{O}_L)$ ein vollständiges Gitter in $L_{\mathbb{R}}$ ist (siehe 22. Vor.), also daß $x\,\sigma(\mathcal{O}_L)$ vollständiges Gitter für $x = (1, \dots, 1)$.

Sei $\{\alpha_1, \dots, \alpha_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$ so $\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$ ist $\mathbb{R}$-linear unabhängig und

$$x\,\sigma(\mathcal{O}_L) = x\,\sigma(\alpha_1)\,\mathbb{Z} \oplus \dots \oplus x\,\sigma(\alpha_n)\,\mathbb{Z}$$

Wir zeigen: $\{x\,\sigma(\alpha_1), \dots, x\,\sigma(\alpha_n)\}$ ist $\mathbb{R}$-lin. unab.

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

$|\det(A)| = 2^{-t} \, |\det X|$ wobei X die

Matrix mit $i$te - Zeile gleich

$x_1 \sigma_1(\alpha_i) \ldots x_s \sigma_s(\alpha_i) \, x_{s+1} \sigma_{s+1}(\alpha_i) \, \overline{x_{s+1}} \, \overline{\sigma_{s+1}(\alpha_i)} \ldots$

Wir wollen also $\det X$ berechnen. Jede Spalte hat einen gemeinsamen Faktor, und zwar entweder x_j oder $\overline{x_j}$, wir sehen also daß

$$\det X = N(x) \, \det V \neq 0.$$

wobei wie immer $V_{ij} = \sigma_i(\alpha_j)$ $i = 1, \ldots, n$ $j = 1, \ldots, n$

Wir bekommen außerdem:

$$0 \neq |\det(A)| = 2^{-t} \, |N(x)| \sqrt{D(O_L/\mathbb{Z})}$$

(siehe 21. Vor).

Also ist $x\sigma(O_L)$ vollständiges Gitter und analogue Berechnungen wie in der 22. Vorlesung ergeben:

$$v(T_x) = |\det A| = 2^{-t} \, |N(x)| \sqrt{D(O_L/\mathbb{Z})}$$

(wobei $T_x := F.P$ von $x\sigma(O_L)$).

Insbesondere wenn $1/2 \leq |N(x)| \leq 1$ dann ist

$$v(T_x) \leq 2^{-t} \sqrt{D(O_L/\mathbb{Z})} \quad (**)$$

(Unabhängig von x !)

- Sei nun $X \subseteq L_{\mathbb{R}}$ konvex symmetrisch beschränkt s.d

$$v(X) > 2^n \, 2^{-t} \sqrt{D(\mathcal{O}_L/\mathbb{Z})}$$ (e.g $X = B_R(0)$ mit R groß genug)

- Sei $R \in \mathbb{R}_+$ s.d. $|N(y)| < R \quad \forall y \in X$.
- Minkowski und (**) ergeben: $\forall x \in L_{\mathbb{R}}$ mit $1/2 \leq |N(x)| \leq 1 \;\; \exists\, 0 \neq \alpha \in \mathcal{O}_L$ s.d $x\,\sigma(\alpha) \in X$ (***)

(Minkowski mit Gitter $x\sigma(\mathcal{O}_L)$ und X anwenden).

- Betrachte nun $\mathcal{I} := \{\alpha\mathcal{O}_L \triangleleft \mathcal{O}_L \,/\, \exists x \in L_{\mathbb{R}} : 1/2 \leq |N(x)| \leq 1$ und $x\sigma(\alpha) \in X\}$.

eine nichtleere wegen (***) Menge von Hauptidealen.

- Wir berechnen: $\alpha\mathcal{O}_L \in \mathcal{I} \Rightarrow \exists x \in L_{\mathbb{R}}$ s.d $1/2 \leq |N(x)| \leq 1$

$|N(x\,\sigma(\alpha))| < R \Rightarrow |N(x)||N(\sigma(\alpha))| < R \Rightarrow$

$$|N(\sigma(\alpha))| < R/_{1/2} = 2R$$

- 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; e.g

$$\mathcal{I} = \{\beta_1\mathcal{O}_L, \dots, \beta_m\mathcal{O}_L\} \qquad \beta_k \neq 0.$$

- Sei nun $x \in L_{\mathbb{R}}$ mit $1/2 \leq |N(x)| \leq 1$. (***) liefert $0 \neq \alpha \in \mathcal{O}_L$ s.d $\alpha\mathcal{O}_L \in \mathcal{I}$, d.h $\exists k$ s.d $\alpha\mathcal{O}_L = \beta_k\mathcal{O}_L$.
- Setze $\varepsilon = \alpha\beta_k^{-1}$. Dann ist $x\,\sigma(\varepsilon) = \underbrace{x\,\sigma(\alpha)}_{\in X}\,\sigma(\beta_k^{-1}) \in \sigma(\beta_k^{-1})X$.

- Wir haben gezeigt:

$\forall x \in L_{\mathbb{R}}$ mit $1/2 \leq |N(x)| \leq 1 \;\; \exists\, \varepsilon \in \mathcal{O}_L^\times$ s.d.

$$x\,\sigma(\varepsilon) \in \bigcup_{k=1}^{m} \sigma(\beta_k^{-1})X.$$

- Da X beschränkt ist, so ist $\sigma(\beta_k^{-1})X \quad \forall k = 1, \dots, m$.
- Es folgt: $\bigcup_{k=1}^{m} \sigma(\beta_k^{-1})X$ ist beschränkt.
- Endlich wählen wir eine Schranke C für diese beschränkte Menge.

■ Hauptbeh.

* * * ENDE * * *