B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

26.Vorlesung

20. Juli 2021

In diesem Skript werden wir die erste Ungleichung für Satz 25.1 zeigen (siehe Korollar 26.6). Dafür werden wir einige technische Lemmata beweisen und die Hilfsabbildung λ einführen. Wir werden, oft stillschweigend, die Ergebnisse vom Kapitel 6 aufrufen.

Ansatz und Notation wie im Skript 25. Für den Beweis von D.E.S brauchen wir zwei Schlüßelergebnisse. Lemma 26.1 ist eine Verallgemeinerung von [Skript 2 ; Behauptung (6) S. 3].

Lemma 26.1
Sei $\alpha \in L$. Dann ist $\alpha \in \mathcal{O}_L^\times \Leftrightarrow \alpha \in \mathcal{O}_L$ und $N_{L/\mathbb{Q}}(\alpha) = \pm 1$.

Beweis. „$\Rightarrow$“

$$\begin{aligned} \alpha \in \mathcal{O}_L^\times &\Rightarrow \beta = \alpha^{-1} \in \mathcal{O}_L \\ &\Rightarrow N_{L/\mathbb{Q}}(\alpha\beta) = \underbrace{N_{L/\mathbb{Q}}(\alpha)}_{\in\mathbb{Z}} \underbrace{N_{L/\mathbb{Q}}(\beta)}_{\in\mathbb{Z}} = 1 \\ &\Rightarrow N_{L/\mathbb{Q}}(\alpha) = \pm 1 \end{aligned}$$

„$\Leftarrow$“ Es ist: $\prod_{i=1}^n \sigma_i(\alpha) = \alpha \prod_{i=2}^n \sigma_i(\alpha) = \pm 1$ also $\alpha^{-1} = \pm \prod_{i=2}^n \sigma_i(\alpha)$, also ist α^{-1} ganz über $\mathbb{Z}$, außerdem ist $\alpha^{-1} \in L$. Also $\alpha^{-1} \in \mathcal{O}_L$ □

Proposition 26.2
Seien $m, M \in \mathbb{N}$ fest. Es ist: Die Menge der ganzen komplexen algebraischen Zahlen

$$A_{m,M} = \{\alpha \in \mathcal{O}_{\mathbb{C}} \mid \deg \ \mathrm{MinPol}_{\mathbb{Z}}(\alpha) \leq m \text{ und } |\alpha'| \leq M \text{ für alle konjugierte } \alpha' \text{ zu } \alpha\}$$

ist endlich.

Beweis. Sei $\alpha \in A_{m,M}$ (d.h. für alle Nullstellen α' von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ gilt $|\alpha'| \leq M$).

• Es genügt zu zeigen: für $\alpha \in A_{m,M}$ gibt es nur endlich viele normierte irreduzible Polynome in $\mathbb{Z}[x]$, die als $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ fungieren können.

• Wir behaupten: die Koeffiziente von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ sind auch beschränkt, d.h $\exists M_m \in \mathbb{N}$, so daß alle Koeffiziente von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ im Absolutbetrag $< M_m$ sind.

• *Beweis der Behauptung:* die Behauptung gilt weil einerseits sind die Koeffiziente elementare symmetrische Funktionen in den Nullstellen (ÜB), und andererseits sind die Nullstellen im Absolutbetrag $\leq M$ per Annahme. Genauer erklärt, sei

$$\mathrm{MinPol}_{\mathbb{Z}}(\alpha) = x^m + z_{m-1}x^{m-1} + \cdots + z_0, z_i \in \mathbb{Z} \text{ mit Nullstellen } \alpha_1, \ldots, \alpha_m \, .$$

Wir berechnen

$z_{m-1} = -\sum_{i=1}^{m} \alpha_i \Rightarrow |z_{m-1}| \leq \sum_{i=1}^{m} |\alpha_i| \leq mM = \binom{m}{1} M$

$z_{m-2} = \sum_{i<j} \alpha_i \alpha_j \Rightarrow |z_{m-2}| \leq \sum_{i<j} |\alpha_i \alpha_j| \leq \binom{m}{2} M^2$

$\vdots$

$z_{m-k} = (-1)^k \sum \alpha_{i_1} \dots \alpha_{i_k} \Rightarrow |z_{m-k}| \leq \sum |\alpha_{i_1} \dots \alpha_{i_k}| \leq \binom{m}{k} M^k \,.$ □

• Schließlich, da $\mathbb{Z}^m$ ein Gitter ist, und jedes normierte irreduzible Polynom in $\mathbb{Z}[x]$ vom deg $\leq m$ als Vektor in $\mathbb{Z}^m$ aufgefasst werden kann (als Vektor der Koeffiziente), ist der Durchschnitt mit der beschränkten Menge endlich wie behauptet. □

Korollar 26.3
Sei $\alpha \in \mathbb{C}$ eine ganze algebraische Zahl, so daß $|\alpha'| = 1$ für alle konjugierte α' zu α. Dann ist α ist eine Einheitswurzel, d.h. es gibt $\mu \in \mathbb{N}$, so daß $\alpha^\mu = 1$.

Beweis. Sei $m := \deg \text{ MinPol}_{\mathbb{Q}}(\alpha)$. Bemerke, daß die Menge $\{1, \alpha, \alpha^2, \dots\} \subseteq A_{m,1}$, also ist sie endlich, d.h. es gibt l, k mit $\alpha^l = \alpha^k$ oder $\alpha^{l-k} = 1$. □

Bemerkung 25.1 (iii) können wir hier nochmal direkt zeigen:

Korollar 26.4
$\mu(L) = (\mathcal{O}_L^\times)_{\text{tor}}$ ist endlich.

Beweis. Setze $n = \deg L/\mathbb{Q}$, $N = 1$. Es ist $\mu(L) \subseteq A_{n,1}$. □

Für den Beweis von D.E.S brauchen wir außerdem noch diese „Hilfsabbildung“ λ (Ansatz weiterhin wie im Skript 22 - 24):

$$\lambda : L^\times \to \mathbb{R}^{s+t} \,;\, \alpha \mapsto (\log|\sigma_1(\alpha)|, \dots \log|\sigma_s(\alpha)|, \log|\sigma_{s+1}(\alpha)|, \log|\sigma_{s+2}(\alpha)|, \dots, \log|\sigma_{s+t}(\alpha)|)$$

- λ ist ein Homomorphismus von der multiplikativen Gruppe $L^\times$ auf die additive Gruppe $\mathbb{R}^s \times \mathbb{R}^t$.
- Bemerke, daß

$$\begin{aligned} \alpha \in \mathcal{O}_L^\times &\Rightarrow |N_{L/\mathbb{Q}}(\alpha)| = 1 \\ &\Rightarrow \prod_{i=1}^{s} |\sigma_i(\alpha)| \prod_{j=1}^{t} |\sigma_{s+j}(\alpha)|^2 = 1 \\ (*) \qquad &\Rightarrow \sum_{i=1}^{s} \log|\sigma_i(\alpha)| + 2\sum_{j=1}^{t} \log|\sigma_{s+j}(\alpha)| = 0 \end{aligned}$$

- umgekehrt: für $\alpha \in \mathcal{O}_L$, $(*) \Rightarrow N_{L/\mathbb{Q}}(\alpha) = \pm 1$ also $\alpha \in \mathcal{O}_L^\times$, d.h.:
- $\forall \alpha \in \mathcal{O}_L, \alpha \in \mathcal{O}_L^\times \Leftrightarrow (*)$ gilt für α.
- Betrachte diese Untermenge von $\mathbb{R}^s \times \mathbb{R}^t$:

$$H := \{x \in \mathbb{R}^s \times \mathbb{R}^t \mid \sum_{i=1}^{s} x_i + 2\sum_{j=1}^{t} x_{s+j} = 0\} \,.$$

Also ist H der Lösungsraum von einem homogenen Gleichungssystem mit einer Gleichung und in $s+t$ Unbekannten, H ist ein Unterraum der Dimension $s+t-1$.

- Mit dieser Notation gilt: $\mathcal{O}_L^\times = \{\alpha \in \mathcal{O}_L \mid \lambda(\alpha) \in H\}$.

Proposition 26.5
$\lambda(\mathcal{O}_L^\times)$ ist ein Gitter in $\mathbb{R}^{s+t}$

Beweis. Wir zeigen: $\lambda(\mathcal{O}_L^\times)$ ist diskret. Dafür genügt es zu zeigen, dass:

$$\forall c \in \mathbb{R}_+ \; \exists \text{ nur endlich viele } \alpha \in \mathcal{O}_L^\times \text{ wofür gilt } |\log|\sigma_l(\alpha)|| \leq c \quad \forall l = 1, \ldots, s+t\,.$$

Nun ist

$$\log|\sigma_l(\alpha)| \leq c \Leftrightarrow |\sigma_l(\alpha)| \leq \exp c\,.$$

Also

$$\alpha \in \mathcal{O}_L^\times \text{ mit } |\log|\sigma_l(\alpha)|| \leq c \quad \forall l = 1, \ldots, s+t \Rightarrow \alpha \in A_{n,\lceil \exp c \rceil}\,.$$

Aber $A_{n,\lceil \exp c \rceil}$ ist eine endliche Menge wegen Prop.26.2.

□

Korollar 26.6
$\mathcal{O}_L^\times$ ist endlich erzeugt mit freiem Rang $\leq s+t-1$

Beweis. $\lambda(\mathcal{O}_L^\times)$ ist ein Gitter $\subseteq H$, also ist $\lambda(\mathcal{O}_L^\times)$ eine freie abelsche Gruppe vom Rang $\leq s+t-1$. Betrachte: $\lambda_{|\mathcal{O}_L^\times} : \mathcal{O}_L^\times \to H$ und berechne dessen Kern:

$$\begin{aligned}
\alpha \in \ker\lambda &\Leftrightarrow \log|\sigma_l(\alpha)| = 0 \quad \forall l = 1, \ldots, s+t \\
&\Leftrightarrow |\sigma_l(\alpha)| = 1 \quad \forall l = 1, \ldots, s+t \\
&\Leftrightarrow |\alpha'| = 1 \text{ für alle konjugierte } \alpha' \text{ zu } \alpha \\
&\Leftrightarrow \alpha \text{ ist Einheitswurzel} \Leftrightarrow \alpha \in \mu(L)
\end{aligned}$$

Es folgt (Korollar 26.3 und 26.4) daß $\ker\lambda = \mu(L)$ eine endliche Gruppe ist.
Zusammenfassend:

$$\begin{array}{rccc}
\lambda: & \mathcal{O}_L^\times & \to & \lambda(\mathcal{O}_L^\times) \\
& \mathcal{O}_L^\times / \underbrace{\mu(L)}_{\text{endlich}} & \cong & \underbrace{\lambda(\mathcal{O}_L^\times)}_{\text{endlich erzeugt}}
\end{array} \quad \Rightarrow \mathcal{O}_L^\times \text{ ist eine endlich erzeugte abelsche Gruppe.}$$

Ferner ist $\mu(L) = (\mathcal{O}_L^\times)_{\text{tor}}$ und der freie Rang von $\mathcal{O}_L^\times$ ist dann
$\dim_{\mathbb{Z}}(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)_{\text{tor}}) = \dim_{\mathbb{Z}}\lambda(\mathcal{O}_L^\times) \leq s+t-1$.

□

Bemerkung
Um D.E.S vollständig zu zeigen, müssen wir nur noch beweisen, daß $\lambda(\mathcal{O}_L^\times)$ ein vollständiges Gitter in H ist.