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

24.Vorlesung

24 Juli 2017

§Die Einheitsgruppe $\mathcal{O}_L^\times$

Ansatz wie in den 22. und 23. Vorlesungen.

Satz 24.1 (Dirichletsche Einheitssatz)
$\mathcal{O}_L^\times$ ist eine endlich erzeugte abelsche Gruppe mit freiem Rang $s+t-1$.

Beweis. Später. □

Bemerkung
Aus D.E.S können wir folgern, daß

(i) $\mathcal{O}_L^\times = F \times (\mathcal{O}_L^\times)_{\text{tor}}$, F freie abelsche Gruppe vom Rang $s+t-1$ (siehe Satz 5.4)

(ii) $\mu(L) := (\mathcal{O}_L^\times)_{\text{tor}} = \{x \neq 0, x \in \mathcal{O}_L, \exists \mu \in \mathbb{N}, x^\mu = 1\}$ besteht aus Einheitswurzeln in $\mathcal{O}_L^\times$, d.h. $\mu(L)$:=die Gruppe der Einheitswurzeln in L.

(iii) $\mathcal{O}_L^\times$ ist endlich erzeugt⇒ $(\mathcal{O}_L^\times)_{\text{tor}}$ ist endlich erzeugt, also ist $(\mathcal{O}_L^\times)_{\text{tor}}$ eine endliche Gruppe. Andererseits ist eine endliche Untergruppe von $L^\times$ zyklisch (siehe B3), insbesondere ist $(\mathcal{O}_L^\times)_{\text{tor}}$ eine endliche zyklische Gruppe mit Erzeuger eine Einheitswurzel $\mu \in L^\times$.

Für den Beweis von D.E.S brauchen wir zwei Schlüßelergebnisse:

Lemma 24.2
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. „⇒“

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

„⇐“ 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 24.3
Seien $m, M \in \mathbb{N}$ fest. Es ist: Die Menge der komplexen algebraischen Zahlen $A_{m,M} = \{\alpha \in \mathcal{O}_{\mathbb{C}} \mid \deg \text{ MinPol}_{\mathbb{Z}}(\alpha) \leq m$ und $|\alpha'| \leq M$ für alle konjugierte α' zu $\alpha\}$ ist endlich.

Beweis. α ist ganz über $\mathbb{Z}$. Es genügt zu zeigen: es gibt nur endlich viele normierte irreduzible Polynome in $\mathbb{Z}[X]$, die als $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ fungieren können (für solche $\alpha \in A_{m,M}$). Nun ist deg $\mathrm{MinPol}_{\mathbb{Z}}(\alpha) \leq m$. Wir behaupten: die Koeffiziente sind auch beschränkt, d.h $\exists M_m \in \mathbb{N}$, so daß alle Koeffiziente im Absolutbetrag $< M_m$ sind. In der Tat sind die Koeffiziente elementare symmetrische Funktionen in den Nullstellen, und die Nullstellen sind im Absolutbetrag $\leq M$ per Annahme. Genauer erklärt, sei z.B. $\mathrm{MinPol}_{\mathbb{Z}}(\alpha) = x^m + z_{m-1}x^{m-1} + \cdots + z_0$, $z_i \in \mathbb{Z}$ mit Nullstellen $\alpha_1, \ldots, \alpha_m$. Es ist

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

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

$$\vdots$$

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

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

□

Korollar 24.4
Sei $\alpha \in \mathbb{C}$ eine ganze algebraische Zahl, so daß $|\alpha'| = 1$ für alle α' zu α konjugiert (d.h. für alle Nullstellen α' von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$). Dann gibt es $\mu \in \mathbb{N}$, so daß $\alpha^\mu = 1$ (d.h.: α ist eine Einheitswurzel).

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

Wir können nun direkt zeigen, daß:

Korollar 24.5
$\mu(L) = (\mathcal{O}_L^\times)_{\mathrm{tor}}$ ist endlich.
(Vergleiche mit Bemerkung (iii))

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

Ansatz weiterhin wie in der 22. und 23. Vorlesung. Für den Beweis von D.E.S brauchen wir außerdem noch eine „Hilfsabbildung“ $\lambda : L^\times \to \mathbb{R}^{s+t}$
$\alpha \mapsto (\log|\sigma_1(\alpha)|, \ldots \log|\sigma_s(\alpha)|, \log|\sigma_{s+1}(\alpha)|, \log|\sigma_{s+2}(\alpha)|, \ldots, \log|\sigma_{s+t}(\alpha)|)$
λ ist ein Homomorphismus (der multiplikativen Gruppe $L^\times$ auf die additive Gruppe $\mathbb{R}^s \times \mathbb{R}^t$). Bemerke, daß

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

und umgekehrt auch: 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 die Untermenge von $\mathbb{R}^s \times \mathbb{R}^t$: $H := \{x \in \mathbb{R}^s \times \mathbb{R}^t \mid \sum_{i=1}^{s} x_i + 2\sum_{j=1}^{t} x_{s+j} = 0\}$. Eigentlich ist H ein Unterraum der Dimension $s + t - 1$ (Lösungsraum von einem homogenen Gleichungssystem mit einer Gleichung und in $s + t$ Unbekannten). Mit dieser Notation gilt: $\mathcal{O}_L^\times = \{\alpha \in \mathcal{O}_L \mid \lambda(\alpha) \in H\}$.

Proposition 24.6
$\lambda(\mathcal{O}_L^\times)$ ist ein Gitter in $\mathbb{R}^{s+t}$

Beweis. Später □

Korollar 24.7
$\mathcal{O}_L^\times$ 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:

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

Wir haben gezeigt: $\ker\lambda = \mu(L)$ ist eine endliche Gruppe. Zusammenfassend:

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

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.

Beweis von Proposition 24.6. z.z.: $\lambda(\mathcal{O}_L^\times)$ ist diskret. Dafür genügt es zu zeigen, dass:
$\forall c \in \mathbb{R}_+$ existieren endlich viele $\alpha \in \mathcal{O}_L^\times$ mit $|\log|\sigma_l(\alpha)|| \leq c \quad \forall l = 1,\dots,s+t$. Aber
$\log|\sigma_l(\alpha)| \leq c \Leftrightarrow |\sigma_l(\alpha)| \leq \exp c$. Also $\alpha \in \mathcal{O}_L^\times$ mit $|\log|\sigma_l(\alpha)|| \leq c \Rightarrow \alpha \in \underbrace{A_{n,\lceil\exp c\rceil}}_{\text{endlich wegen Prop.24.3}}$

□