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

22.Vorlesung

20 Juli 2017

Ziel: Endlichkeit der Klassenzahl

Satz 22.1
Sei L ein Zahlkörper vom Grad n und $s \in \mathbb{N}$ fest. Dann ist $|\{I \mid I \lhd \mathcal{O}_L, N(I) = s\}| < \infty$

Beweis.

Behauptung 1: Sei $J \lhd \mathcal{O}_L$. Dann ist $N(J) \in J$.

Beweis. $N(J) = |\mathcal{O}_L/J| \Rightarrow \forall x \in \mathcal{O}_L, N(J)x \in J$. □

Behauptung 2: Seien $I, J \lhd \mathcal{O}_L, I \neq 0, J \neq 0$.
Es ist $I \subseteq J \Rightarrow IJ^{-1} \lhd \mathcal{O}_L$.

Beweis. $J^{-1} = (\mathcal{O}_L : J) = \{x \in L \mid xJ \subseteq \mathcal{O}_L\}$ □

Sei nun $J \lhd \mathcal{O}_L$ mit $N(J) = s$. Dann ist
$< s > \subseteq J$, also ist $< s > J^{-1} \lhd \mathcal{O}_L$. Setze $I := < s > J^{-1}$. Wir haben $< s > = IJ$. Die Eindeutigkeit der Primfaktorisierung zeigt, daß die Menge der Primideale, die in der Faktorisierung von J erscheinen, eine Untermenge von der Menge der Primideale, die in der Faktorisierung von $< s >$ erscheinen, ist. Außerdem: Wenn für $\mathfrak{p}$ Primideal $\mathfrak{p}^\nu$ in der Faktorisierung von J und P^μ in der Faktorisierung von $< s >$ erscheint $(\mu, \nu \in \mathbb{N})$, ist dann $\nu \leq \mu$.
Setze $\mu := v_\mathfrak{p}(< s >)$. Wir sehen also, daß es höchstens $\prod_{\mathfrak{p} \mid < s >}(v_\mathfrak{p}(< s >) + 1)$ Möglichkeiten für J gibt, insbesondere endlich viele. □

Satz 22.2 (Minkowski Schranke)
Sei $L/\mathbb{Q}$ ein Zahlkörper. Dann gibt es $c_L \in \mathbb{R}_+$, so daß: $\forall 0 \neq \mathfrak{a} \lhd \mathcal{O}_L \exists 0 \neq \alpha \in \mathfrak{a}$ mit

$$(\dagger) \qquad N(< \alpha >) \leq c_L N(\mathfrak{a})$$

Beweis. Später (siehe 23. Vorlesung). □

Korollar 22.3
Sei $L/\mathbb{Q}$ ein Zahlkörper. Es gilt:

$$\forall \bar{\mathfrak{q}} \in \mathcal{K}l(L) := \mathcal{K}l(\mathcal{O}_L) \quad \exists \mathfrak{a} \lhd \mathcal{O}_L, \text{ so daß } \bar{\mathfrak{a}} = \bar{\mathfrak{q}} \text{ und } N(\mathfrak{a}) \leq C_L$$

Erinnerung: $\mathcal{K}l(L) = \mathrm{Id}(\mathcal{O}_L)/H(\mathcal{O}_L) = \mathcal{K}l(\mathcal{O}_L)$ ist die Klassengruppe des Zahlkörpers L, wobei $\mathrm{Id}(\mathcal{O}_L) =$ die Gruppe der gebrochenen Ideale unf $H(\mathcal{O}_L) =$ die Untergruppe der gebrochenen Hauptideale.

Beweis. Sei $\bar{\mathfrak{q}} = \mathfrak{q}H(\mathcal{O}_L)$, $\mathfrak{q} \in \operatorname{Id}(\mathcal{O}_L) \Rightarrow \exists d \neq 0, d \in \mathcal{O}_L$ und $\mathfrak{b} \lhd \mathcal{O}_L$, so daß

$$(*) \qquad \mathfrak{q}^{-1} = \frac{1}{d}\mathfrak{b}$$

Satz 22.2 $\Rightarrow \exists \beta \in \mathfrak{b}$, so daß

$$(\dagger) \qquad |N_{L/\mathbb{Q}}(\beta)| \leq c_L N(\mathfrak{b})$$

Betrachte

$$(**) \qquad \mathfrak{a} := \beta\mathfrak{b}^{-1},$$

da $<\beta> \subseteq \mathfrak{b}$ gilt $\mathfrak{a} \lhd \mathcal{O}_L$. Also ist $\mathfrak{q} \overset{(*)}{=} d\mathfrak{b}^{-1} \overset{(**)}{=} d\beta^{-1}\mathfrak{a}$ d.h $\mathfrak{q}\mathfrak{a}^{-1} = \mathcal{O}_L(d\beta^{-1}) \in H(\mathcal{O}_L)$. Wir berechnen $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) \underset{(**)}{=} N(<\beta>) \underset{(\dagger)}{\leq} c_L N(\mathfrak{b})$, es folgt $N(\mathfrak{a}) \leq c_L$.

□

Erinnerung: $h_L := |\mathcal{K}l(L)|$ ist die Klassenzahl des Zahlkörpers L.

Satz 22.4 (Endlichkeit der Klassenzahl)
$\mathcal{K}l(L)$ ist endlich (d.h. $h_L \in \mathbb{N}$)

Beweis. Sei $\bar{\mathfrak{q}} \in \mathcal{K}l(L)$ und $\mathfrak{a} \lhd \mathcal{O}_L$ mit $N(\mathfrak{a}) \leq c_L$ und $\bar{\mathfrak{q}} = \bar{\mathfrak{a}}$. Dann ist $0 < N(\mathfrak{a}) \leq \lfloor c_L \rfloor$. Wir bekommen eine surjektive Abbildung von $\{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) \leq \lfloor c_L \rfloor\}$ nach $\mathcal{K}l(L)$ und $\{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) \leq \lfloor c_L \rfloor\} = \bigcup_{s=1}^{\lfloor c_L \rfloor}\{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) = s\}$ ist endlich wegen Satz 22.1 □

Wir wollen nun (†) beweisen. Dafür kehren wir zum Ansatz am Ende der 20. Vorlesung und definieren eine Abbildung $\sigma : L \to L_{\mathbb{R}}$ wie folgt: $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha))$.

Bemerkung
σ ist $\mathbb{Q}$-linear

Satz 22.5
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, dann ist $\sigma(\mathfrak{a})$ ein vollständiges Gitter.

Beweis. Sei $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_L$ eine Basis für $L/\mathbb{Q}$.

Behauptung: $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ ist eine Basis für $L_{\mathbb{R}}$ als $\mathbb{R}$-Vektorraum.

Beweis. Setze für $i = 1, \ldots, n$
$v_i := (\sigma_1(\alpha_i), \ldots, \sigma_s(\alpha_i);\ \operatorname{Re}\sigma_{s+1}(\alpha_i),\ \operatorname{Im}\sigma_{s+1}(\alpha_i), \ldots,\ \operatorname{Re}\sigma_{s+t}(\alpha_i),\ \operatorname{Im}\sigma_{s+t}(\alpha_i)) \in \mathbb{R}^{s+2t}$.
Vergleiche $A = \begin{pmatrix} v_1 \\ \ldots \\ v_n \end{pmatrix}$
mit $\mathcal{V}$(13. Vorlesung).

Erinnerung: $\mathcal{V} = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots\sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \ldots & \sigma_{s+t}(\alpha_1) & \overline{\sigma_{s+t}(\alpha_1)} \\ & \vdots & \vdots & & & & \\ \sigma_1(\alpha_n) & \ldots\sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \ldots & \sigma_{s+t}(\alpha_n) & \overline{\sigma_{s+t}(\alpha_n)} \end{pmatrix}$

In ÜB haben wir berechnet: $0 \neq (\det\mathcal{V})^2 = D(\alpha_1, \ldots, \alpha_n)$ (da $\{\alpha_1, \ldots, \alpha_n\}$ Basis ist). Aber man kann A durch elementare Spaltenumformungen aus $\mathcal{V}$ bekommen (siehe Berechnung weiter unten), also ist auch $\det A \neq 0$. □

Nun ist $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang n (21. Vorlesung), also wählen wir nun $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathfrak{a}$. Wir haben $\sigma(\mathfrak{a}) = \operatorname{Span}_{\mathbb{Z}}\{\sigma(\alpha_1, \ldots, \sigma(\alpha_n)\}$ (da σ $\mathbb{Q}$-linear ist) ein vollständiges Gitter.

□

Wir berechnen nun genau $\det A = ?$.

Erinnerung: Für $z \in \mathbb{C}$, $i = \sqrt{-1}$, $\operatorname{Re} z = \frac{z+\bar{z}}{2}$ und $\operatorname{Im} z = \frac{z-\bar{z}}{2i}$

Wir analysieren die Spaltenumformungen auf $\mathcal{V}$:

$$\begin{pmatrix} \dots & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \dots \\ & \vdots & \vdots & \\ \dots & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \dots \end{pmatrix} \xrightarrow{I+II} \begin{pmatrix} \dots & \operatorname{Re} \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \dots \\ & \vdots & \vdots & \\ \dots & \operatorname{Re} \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \dots \end{pmatrix}$$

wobei:
I: $(s+1)$-te Spalte von $\mathcal{V}$ wird mit $\frac{1}{2}$ multipliziert.
II: Addiere die $(s+2)$-te Spalte zur $(s+1)$-te Spalte.

$$\xrightarrow{III+IV} \begin{pmatrix} \dots & \operatorname{Re} \sigma_{s+1}(\alpha_1) & \operatorname{Im} \sigma_{s+1}(\alpha_1) & \dots \\ & \vdots & \vdots & \\ \dots & \operatorname{Re} \sigma_{s+1}(\alpha_n) & \operatorname{Im} \sigma_{s+1}(\alpha_n) & \dots \end{pmatrix}$$

Wobei :
III: $(s+2)$-te Spalte minus $(s+1)$-te Spalte.
IV: multipliziere mit i.
Wiederhole für $(s+3)$-te bis $(s+t)$-te Spalte, insgesamt t mal. Alles zusammen ergibt:
$\det A = (\frac{1}{2} i)^t \det \mathcal{V}$.

23