Algebraische Zahlentheorie
SS 2013
Kuhlmann

22. Vorlesung am 08.07.2013

Ziel: Endlichkeit der Klassenzahl S.4

Satz 1.
Sei L ein Zahlkörper vom Grad n, und sei $s \in \mathbb{N}$ fest. Dann ist

$$\left| \{ I \mid I \trianglelefteq O_L ;\ N(I) = s \} \right| < \infty .$$

Beweis: **Beh 1.** Sei $J \trianglelefteq O_L$. Dann ist $N(J) \in J$.
Bew: $N(J) = |O_L / J| \Rightarrow \forall x \in O_L : N(J).x \in J$ ∎

Beh 2: Seien $I, J \trianglelefteq O_L$ $\quad I \neq 0,\ J \neq 0$.
Es ist: $I \subseteq J \Rightarrow IJ^{-1} \trianglelefteq O_L$
Bew. $J^{-1} = (O_L : J) = \{ x \in L \mid xJ \subseteq O_L \}$. ∎

Sei nun $J \trianglelefteq O_L$ mit $N(J) = s$. Dann ist
$\langle s \rangle \subseteq J$, also ist $\langle s \rangle J^{-1} \trianglelefteq O_L$

Setze $I := \langle s \rangle J^{-1}$. Wir haben $\langle s \rangle = IJ$.

Die Eindeutigkeit der Primfaktorisierung zeigt

daß die Menge der Primidealen die in der Faktorisierung

von J erscheinen, ist eine Untermenge von der Menge der Primidealen die in der Faktorisierung von $\langle s \rangle$ erscheinen. Außerdem wenn für $\mathfrak{p}$ Primideal $\mathfrak{p}^\nu$ erscheint in der Faktorisierung von J $(\nu \in \mathbb{N})$ und $\mathfrak{p}^\mu$ " " " " " $\langle s \rangle$ $(\mu \in \mathbb{N})$ dann ist $\nu \leq \mu$.

Setze $\mu := \nu_{\mathfrak{p}}(\langle s \rangle)$.

Wir sehen also daß es höchstens

$$\prod_{\mathfrak{p} \mid \langle s \rangle} (\nu_{\mathfrak{p}}(\langle s \rangle) + 1)$$ Möglichkeiten

für J gibt, insbesondere endlich viele. ∎

Satz 2 (Minkowski Schranke).

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

$$N(\langle \alpha \rangle) \leq c_L N(\mathfrak{a}) \quad (\dagger)$$

Beweis: später. (siehe 23. Vorlesung).

Korollar 1 Sei $L/\mathbb{Q}$ ein Zahlkörper. Es gilt:

$$\forall\, \bar{q} \in Kl(L) := Kl(\mathcal{O}_L) \quad \exists\, \mathfrak{a} \lhd \mathcal{O}_L$$

so daß $\bar{\mathfrak{a}} = \bar{q}$ und $N(\mathfrak{a}) \leq C_L$.

[Erinnerung $Kl(L) = Id(\mathcal{O}_L)/H(\mathcal{O}_L) = Kl(\mathcal{O}_L)$

ist die Klassengruppe des Zahlkörpers L;

wobei $Id(\mathcal{O}_L) :=$ die Gruppe der gebr. Idealen

und $H(\mathcal{O}_L) :=$ " Untergruppe " " Hauptidealen.]

Beweis: Sei $\bar{q} = q \cdot H(\mathcal{O}_L)$, $q \in Id(\mathcal{O}_L) \Rightarrow$

$\exists\, d \neq 0$, $d \in \mathcal{O}_L$ und $\mathfrak{b} \lhd \mathcal{O}_L$ so daß

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

Satz (Minkowski Schranke) $\Rightarrow \exists\, \beta \in \mathfrak{b}$ so daß

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

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

da $\langle\beta\rangle \subseteq \mathfrak{b}$ gilt (Beh 2 S. 1) $\mathfrak{a} \lhd \mathcal{O}_L$.

Also ist $q \overset{(*)}{=} d\,\mathfrak{b}^{-1} \overset{(**)}{=} d\,\beta^{-1}\,\mathfrak{a}$

d.h. $q\,\mathfrak{a}^{-1} = \mathcal{O}_L(d\beta^{-1}) \in H(\mathcal{O}_L)$.

Wir berechnen:

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) \underset{(**)}{=} N(\langle\beta\rangle) \underset{(\dagger)}{\leq} C_L\, N(\mathfrak{b}),$$

es folgt: $N(\mathfrak{a}) \leq C_L$. ∎

Erinnerung: $h_L := |Kl(L)|$ ist die Klassenzahl des Zahlkörpers L.

Satz 3 (Endlichkeit der Klassenzahl):

$Kl(L)$ ist endlich (i.e. $h_L \in \mathbb{N}$).

Beweis. Sei $\bar{\mathfrak{q}} \in Kl(L)$ und $\mathfrak{a} \lhd \mathcal{O}_L$ mit

$$N(\mathfrak{a}) \leq C_L \quad \text{und} \quad \bar{\mathfrak{q}} = \bar{\mathfrak{a}}.$$

Dann ist $0 < N(\mathfrak{a}) \leq \lfloor C_L \rfloor$.

Wir bekommen eine ~~bije~~ surjektive Abbildung

von $\underbrace{\{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) \leq \lfloor C_L \rfloor\}}_{\lfloor C_L \rfloor} \longrightarrow\!\!\!\!\rightarrow Kl(L)$

und

$$= \bigcup_{s=1} \{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) = s\}$$ ist endlich wegen Satz 1. ∎

Wir wollen nun (†) beweisen. Dafür kehren wir zum Ansatz am Ende der 20. Vorlesung, und definieren eine Abbildung

$$\sigma : L \longrightarrow L_{\mathbb{R}} \quad \text{folgend}$$

$$\sigma(\alpha) := (\sigma_1(\alpha), \dots, \sigma_s(\alpha); \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha))$$

Bemerkung: σ ist $\mathbb{Q}$-linear.

Satz 4. Sei $0 \neq \mathfrak{a} \lhd O_L$, dann ist $\sigma(\mathfrak{a})$ ein vollständiges Gitter.

Beweis. Sei $\{\alpha_1, \dots, \alpha_n\} \subseteq O_L$ eine Basis für $L/\mathbb{Q}$.

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

Bew. Setze für $i = 1, \dots, n$

$$v_i := (\sigma_1(\alpha_i), \dots, \sigma_s(\alpha_i); \operatorname{Re}\sigma_{s+1}(\alpha_i), \operatorname{Im}\sigma_{s+1}(\alpha_i), \dots, \operatorname{Re}\sigma_{s+t}(\alpha_i), \operatorname{Im}\sigma_{s+t}(\alpha_i)) \in \mathbb{R}^{s+2t}$$

Vergleiche $A = \begin{pmatrix} v_1 \\ \hline \dots \\ \hline v_n \end{pmatrix}$ mit V (13. Vor S. 5 06.06.2013)

[Erinnerung: $v_{ij} = \sigma_i(\alpha_j)$, $i, j = 1, \dots, n$; i.e

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

In Auf. 7.1 haben wir berechnet:

$$0 \neq (\det V)^2 = D(\alpha_1, \dots, \alpha_n)$$

(da $\{\alpha_1, \dots, \alpha_n\}$ Basis ist)

Aber man kann A durch elementare Spaltenumformungen aus V bekommen (siehe Berechnung weiter unten)

also ist auch $\det A \neq 0$. ☐ Beh.

Nun ist $\mathfrak{a}$ freier $\mathbb{Z}$-Modul vom Rang n

(21. Vor) also wählen wir nun $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathfrak{a}$.

Wir haben

$\sigma(\mathfrak{a}) = \mathrm{Span}_{\mathbb{Z}}\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$ (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 V:

von V

$$\begin{pmatrix} \cdots & b_{s+1}(\alpha_1) & \overline{b_{s+1}(\alpha_1)} & \cdots \\ & & & \\ \cdots & b_{s+1}(\alpha_m) & b_{s+1}(\alpha_m) & \cdots \end{pmatrix} \xrightarrow{\text{I} + \text{II}} \begin{pmatrix} \cdots & \operatorname{Re} b_{s+1}(\alpha_1) & \overline{b_{s+1}(\alpha_1)} & \cdots \\ & & & \\ \cdots & \operatorname{Re} b_{s+1}(\alpha_m) & \overline{b_{s+1}(\alpha_m)} & \cdots \end{pmatrix}$$

wobei:

(I) ($s+1^{\text{te}}$ Spalte von V) wird mit $1/2$ multipliziert

(II) addiere hierzu die $s+2^{\text{te}}$ Spalte von V

$$\xrightarrow{\text{III} + \text{IV}} \begin{pmatrix} \cdots & \operatorname{Re} b_{s+1}(\alpha_1) & \operatorname{Im} b_{s+1}(\alpha_1) & \cdots \\ & \vdots & & \\ \cdots & \operatorname{Re} b_{s+1}(\alpha_m) & \operatorname{Im} b_{s+1}(\alpha_m) & \cdots \end{pmatrix}$$

nach A ...

wobei:

(III) $(s+2)^{\text{te}}$ Spalte minus $(s+1)^{\text{te}}$ Spalte

(IV) multipliziere mit i

Wiederhole für $(s+3)^{\text{te}}$ bis $(s+t)^{\text{te}}$ Spalte, insgesamt t mal.

Alles zusammen ergibt:

$$\det A = \left(\tfrac{1}{2} i\right)^t \det V$$ (Details prüfen!)