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

23.Vorlesung

08. Juli 2021

In diesem Skript ist der Ansatz weiterhin im Skript 22. Wir werden, oft stillschweigend, die Notationen und Ergebnisse von [Algebra II; Kapitel 4] (insbesondere bezüglich der Klassengruppe), sowie die Eigenschaften der Norm und Diskriminante (Skripte 15,16,17) benutzen. Wir werden zunächst in Propositionen 23.1 und 23.2 zwei weitere Schlüssel Eigenschaften von Idealnorm erklären. Dann werden wir Satz 23.3 beweisen. Um unser Hauptziel (Satz 23.6; Endlichkeit der Klassenzahl) zu erreichen werden wir Satz 23.4 (Minkowski Schranke) aussagen und gleich anwenden. Den Beweis vom Satz 23.4 werden wir erst im Skript 24 führen.

Proposition 23.1
Sei $L/\mathbb{Q}$ Zahlkörper vom Grad n, $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, $\{y_1, \ldots, y_n\}$ eine $\mathbb{Z}$-Basis für $\mathfrak{a}$. Es ist:

$$D(\mathcal{O}_L/\mathbb{Z})N(\mathfrak{a})^2 = D(y_1, \ldots, y_n)\,.$$

Beweis. Bemerke zunächst daß die Aussage sinnvoll ist: Wir wissen, daß $\mathcal{O}_L$ ein freier $\mathbb{Z}$-Modul vom Rang n ist, und außerdem, daß $[\mathcal{O}_L : \mathfrak{a}] < \infty$. Es folgt aus Bemerkung 22.1(i), daß $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang n ist.

• Sei $\{e_1, \ldots, e_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$ und $\{y_1, \ldots, y_n\}$ eine $\mathbb{Z}$-Basis für $\mathfrak{a}$. Schreibe
$y_i = \sum y_{ij}e_j, y_{ij} \in \mathbb{Z}$ und sei A die Matrix mit y_{ij} als ij-te Eintrag.

• Wir berechnen:
$D(y_1, \ldots, y_n) \underset{17.Vor.}{=} \det A^2 D(e_1, \ldots, e_n) = \det A^2 D(\mathcal{O}_L/\mathbb{Z})$.
Andererseits folgt aus Bemerkung 22.1 (ii), daß
$|\det A| = [\mathcal{O}_L : \mathfrak{a}]$.
Alles zusammen ergibt: $D(y_1, \ldots, y_n) = N(\mathfrak{a})^2 D(\mathcal{O}_L/\mathbb{Z})$ □

Proposition 23.2
Sei $0 \neq \beta \in \mathcal{O}_L$. Es ist $\underbrace{N(<\beta>)}_{\in\mathbb{N}} = |\underbrace{N_{L/\mathbb{Q}}(\beta)}_{\in\mathbb{Z}}|$.

Beweis. • Sei $\{e_1, \ldots, e_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$, dann ist $\{\beta e_1, \ldots, \beta e_n\}$ eine $\mathbb{Z}$-Basis für $<\beta>$.
• Aus Proposition 23.1 folgern wir, daß

$$D(\beta e_1, \ldots, \beta e_n) = D(\mathcal{O}_L/\mathbb{Z})N(<\beta>)^2\,.$$

Andererseits per Definition wissen wir, daß

$$D(\beta e_1, \ldots, \beta e_n) = \det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j))\,.$$

• Wir berechnen (ÜA, ÜB):

$$\det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j)) = (\det((\sigma_i(\beta e_j))_{ij}))^2 = (\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}))^2 .$$

• Nun ist (ÜA, Eigenschaften von Determinanten)

$$\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}) = \sigma_1(\beta)\dots\sigma_n(\beta)\det(\sigma_i(e_j)_{ij}) = N_{L/\mathbb{Q}}(\beta)\det(\sigma_i(e_j)_{ij}) .$$

Alles zusammen ergibt:

$$D(\beta e_1, \dots, \beta e_n) = (N_{L/\mathbb{Q}}(\beta))^2(\det(\sigma_i(e_j))_{ij})^2 = (N_{L/\mathbb{Q}}(\beta))^2 D(e_1, \dots, e_n) \underset{\text{Prop 23.1}}{=} N(<\beta>)^2 D(e_1, \dots, e_n)$$

□

Satz 23.3
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. $N(J) = |\mathcal{O}_L/J| \underset{\text{Lagrange}}{\Rightarrow} \forall x \in \mathcal{O}_L, N(J)x \in J$. Insbesondere gilt das für $x = 1$. □

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 $\mathfrak{p}^\mu$ 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 $\prod_{\mathfrak{p}|<s>}(v_\mathfrak{p}(< s >) + 1)$ Möglichkeiten für J gibt, insbesondere endlich viele. □

Satz 23.4 (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 24. Vorlesung). □

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 und $H(\mathcal{O}_L)$ = die Untergruppe der gebrochenen Hauptideale. $h_L := |\mathcal{K}l(L)|$ ist die Klassenzahl des Zahlkörpers L.

Korollar 23.5
Sei $L/\mathbb{Q}$ ein Zahlkörper und c_L wie in Satz 23.4. Es gilt:

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

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

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

Satz 23.4 $\Rightarrow \exists \beta \in \mathfrak{b}$, 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 (s. Beh. 2 S.2) $\mathfrak{a} \lhd \mathcal{O}_L$. Also ist

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

Das heißt:

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

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 $N(\mathfrak{a}) \leq c_L$.

□

Satz 23.6 (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 23.3 □