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

22.Vorlesung

06. Juli 2021

Wir betrachten den folgenden Ansatz: $L/\mathbb{Q}$ ein Zahlkörper von Grad n, $\mathcal{O}_L = \overline{\mathbb{Z}}^L$. Wir wissen, daß $L = Quot(\mathcal{O}_L)$ (Satz 9.5) und daß $\mathcal{O}_L$ ein Dedekindring ist (Satz 13.5). Wir verfolgen das folgende Ziel: Wir wollen den gebrochenen Idealen von $\mathcal{O}_L$ Gittern in $\mathbb{R}^n$ zuordnen. Wir werden dabei, oft stillschweigend, die Ergebnisse von [Algebra II; Kapitel 4] (insbesondere bezüglich der Klassengruppe) benutzen.

Erinnerung: • Sei θ ein primitives Element für L, i.e. $L = \mathbb{Q}(\theta)$ und seien $\sigma_1, \dots, \sigma_n$ die n verschiedenen Einbettungen von L in $\Omega := \mathbb{C}$.
• Ist $\sigma_i(\theta) \in \mathbb{R}$ (also $\sigma_j(L) \subseteq \mathbb{R}$), so heißt σ_j reell. Sonst heißt σ_j komplex.
In diesem Fall ist auch $\bar{\sigma}_j$ komplex.
• Sei $s := \sharp$reelle Einbettungen und $2t := \sharp$ komplexe Einbettungen. Es ist $n = s + 2t$, und

$$\sigma_1, \dots, \sigma_s \, ; \; \sigma_{s+1}, \bar{\sigma}_{s+1}, \; \cdots \; , \; \sigma_{s+t}, \bar{\sigma}_{s+t}$$

sind die n verschiedene Einbettungen.
• Setze $L_\mathbb{R} := \mathbb{R}^S \times \mathbb{C}^t = \mathbb{R}^S \times \mathbb{R}^{2t}$.

§Idealnorm und Eigenschaften

Definition 22.1
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, definiere
$N(\mathfrak{a}) := [\mathcal{O}_L : \mathfrak{a}] = |(\mathcal{O}_L, +)/(\mathfrak{a}, +)|$
($N(\mathfrak{a})$ ist a priori endlich oder ∞).

Satz 22.1
Seien $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$, $\mathfrak{a} \neq 0$, $\mathfrak{b} \neq 0$.

(1) Es ist $N(\mathfrak{b}) < \infty$

(2) $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$

Beweis. Wir zeigen (1) und daß

$$(**) \qquad N(\mathfrak{a}\mathfrak{p}) = N(\mathfrak{a})N(\mathfrak{p})$$

für $\mathfrak{p} \lhd \mathcal{O}_L$ ein Primideal. (2) folgt dann aus $(**)$ wegen Primfaktorisierung von Idealen in Dedekindringen.

Zu (1): Sei $0 \neq \alpha \in \mathfrak{b}$ und betrachte $\alpha := \sigma_1(\alpha)$ sowie $\sigma_2(\alpha)\ldots,\sigma_n(\alpha)$. Berechne:

$$n_\alpha := N_{L/\mathbb{Q}}(\alpha) \underset{\text{Satz 15.4}}{=} \prod_{i=1}^n \sigma_i(\alpha) = \alpha \prod_{i=2}^n \sigma_i(\alpha)\,.$$

• Da $\alpha \in \mathcal{O}_L$, ist $n_\alpha \in \mathbb{Z}$ (Korollar 15.2). Also ist $\prod_{i=2}^n \sigma_i(\alpha) = n_\alpha \alpha^{-1} \in L$. Außerdem sind alle $\sigma_i(\alpha)$ ganz über $\mathbb{Z}$, also ist $\prod_{i=2}^n \sigma_i(\alpha)$ ganz über $\mathbb{Z}$, und somit ist $\prod_{i=2}^n \sigma_i(\alpha) \in \mathcal{O}_L$.

• Nun ist $n_\alpha = \underbrace{\alpha}_{\in\mathfrak{b}} \underbrace{\prod_{i=2}^n \sigma_i(\alpha)}_{\in\mathcal{O}_L} \in \mathfrak{b}$ (weil $\mathfrak{b} \lhd \mathcal{O}_L$), also ist das Hauptideal $< n_\alpha >= \mathcal{O}_L n_\alpha \subseteq \mathfrak{b}$.

• Wir haben also einen surjektiven Homomorphismus $\psi : \mathcal{O}_L/ < n_\alpha > \to \mathcal{O}_L/\mathfrak{b}$.

• Nun ist $\mathcal{O}_L$ ein freier $\mathbb{Z}$-Modul vom Rang n (Satz 17.3), insbesondere ist $\mathcal{O}_L$ ein endlich erzeugter $\mathbb{Z}$-Modul. Also ist auch $\mathcal{O}_L/ < n_\alpha >$ endlich erzeugt.

• Da $n_\alpha \in \mathbb{Z}$ ist außerdem $\mathcal{O}_L/ < n_\alpha >= (\mathcal{O}_L/ < n_\alpha >)_{\text{tor}}$ ein Torsionsmodul (ÜA). Ein endlich erzeugter Torsionsmodul über $\mathbb{Z}$ ist endlich (folgt aus Struktursatz für endlich erzeugte Moduln über HIR). Insbesondere ist $\mathcal{O}_L/\mathfrak{b}$ auch endlich (als Bild von ψ).

Zu $(**)$: Dafür genügt es zu zeigen, daß

(a) $|\mathcal{O}_L/\mathfrak{a}\mathfrak{p}| = |\mathcal{O}_L/\mathfrak{a}||\mathfrak{a}/\mathfrak{a}\mathfrak{p}|$

und

(b) $|\mathfrak{a}/\mathfrak{a}\mathfrak{p}| = |\mathcal{O}_L/\mathfrak{p}|$

• Zu (a): $\mathcal{O}_L/\mathfrak{a}\mathfrak{p} \to \mathcal{O}_L/\mathfrak{a}$, $x + \mathfrak{a}\mathfrak{p} \mapsto x + \mathfrak{a}$ ist ein surjektiver Homomorphismus von Gruppen mit Kern $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$, also $\mathcal{O}_L/\mathfrak{a} \cong (\mathcal{O}_L/\mathfrak{a}\mathfrak{p})/(\mathfrak{a}/\mathfrak{a}\mathfrak{p})$, also ist $|\mathcal{O}_L/\mathfrak{a}| = \frac{|\mathcal{O}_L/\mathfrak{a}\mathfrak{p}|}{|\mathfrak{a}/\mathfrak{a}\mathfrak{p}|}$ (wegen Lagrange).

• Zu (b): Bemerke, daß $\mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a}$ (wegen Eindeutigkeit der Primfaktorisierung).

Behauptung: Sei $I \lhd \mathcal{O}_L$. Wenn $\mathfrak{a}\mathfrak{p} \subseteq I \subseteq \mathfrak{a}$, dann ist $I = \mathfrak{a}\mathfrak{p}$ oder $I = \mathfrak{a}$.

Beweis. $\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a}^{-1}I \subseteq \mathcal{O}_L$, d.h $\mathfrak{p} \subseteq \mathfrak{a}^{-1}I \subseteq \mathcal{O}_L$.
Nun $\mathfrak{p}$ maximal $\Rightarrow$ $\mathfrak{p} = \mathfrak{a}^{-1}I$ (in diesem Fall $\mathfrak{a}\mathfrak{p} = I$) oder $\mathcal{O}_L = \mathfrak{a}^{-1}I$ (in diesem Fall $\mathfrak{a} = I$). □

Wähle nun $x \in \mathfrak{a}$ so daß $x \notin \mathfrak{a}\mathfrak{p}$ und betrachte $\mathfrak{a}\mathfrak{p}+ < x >$. Wir haben $\mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a}\mathfrak{p}+ < x > \subseteq \mathfrak{a}$, also $\mathfrak{a}\mathfrak{p}+ < x >= \mathfrak{a}$. Wir definieren einen Homomorphismus

$$\begin{array}{rccl} \psi : & \mathcal{O}_L & \to & \mathfrak{a}/\mathfrak{a}\mathfrak{p} \\ & y & \mapsto & \underbrace{yx}_{\in\mathfrak{a}} + \mathfrak{a}\mathfrak{p} \end{array}$$

Da $\mathfrak{a}\mathfrak{p}+ < x >= \mathfrak{a}$, ist ψ surjektiv mit $\mathfrak{p} \subseteq \ker\psi \subseteq \mathcal{O}_L$, und da $\mathfrak{a}\mathfrak{p} \neq \mathfrak{a}$ ist $\ker\psi \neq \mathcal{O}_L$ (ÜA). Da $\mathfrak{p}$ maximal ist, folgt nun $\mathfrak{p} = \ker\psi$. Es folgt: $\mathcal{O}_L/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{p}$ □

Bevor wir die nächste Propositionen beweisen, fassen wir zusammen allgemeine ergänzende Bemerkungen:

Bemerkung 22.1 (i) Sei N ein freier $\mathbb{Z}$-Modul vom Rang n (i.e. $N \simeq \mathbb{Z}^n$) und $M \leq N$ ein Untermodul. Da $\mathbb{Z}$ ein HIR ist, wissen wir daß M frei vom Rang $m \leq n$ ist. Wir behaupten daß:

$$[N : M] < \infty \Leftrightarrow \dim_{\mathbb{Z}} M = n\,.$$

Beweis von (i).

Behauptung 1: Sei $\{y_1, \dots, y_m\} \subseteq \mathbb{Z}^n$ eine $\mathbb{Z}$-Basis für M. Betrachte die Matrix $A \in M_{m\times n}(\mathbb{Z})$ mit Zeilen $\{y_1, \dots, y_m\}$, also $A := \begin{pmatrix} y_1 \\ \dots \\ y_m \end{pmatrix}$.

Man kann zeigen, daß elementare Zeilen- und Spaltenumformungen eine Matrix $B \in M_{m\times n}(\mathbb{Z})$ mit folgender Eigenschaft ergeben:

$$\mathbb{Z}^n / \operatorname{Span}_{\mathbb{Z}}(B) \cong \mathbb{Z}^n / \operatorname{Span}_{\mathbb{Z}}(A) = \mathbb{Z}^n/M$$

(ÜA).

Behauptung 2: Zeilen-und Spaltenumformungen ergeben B der Form $B := \begin{pmatrix} d_1 & \dots & 0 & * \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & d_m & * \end{pmatrix}$

$d_i \in \mathbb{Z}, d_i \neq 0$ (da $\{y_1, \dots, y_m\}$ $\mathbb{Z}$-linear unabhängig sind) (ÜA).

• Mit Behauptung 1 und Behauptung 2 können wir nun die Äquivalenz in (i) zeigen:

„$\Rightarrow$“ wir nehmen an, $m < n$ und zeigen $[\mathbb{Z}^n : M] = \infty$.

Setze $v_z := (\underbrace{0, \dots, 0}_{m}, \underbrace{z}_{\in\mathbb{Z}}, 0, \dots, 0)$. Bemerke daß $v_z \notin \operatorname{Span}_{\mathbb{Z}} B$ wenn $z \neq 0$ (ÜA).

Aus $z_1 \neq z_2$ folgt also $v_{z_1} \neq v_{z_2} \mod \operatorname{Span}_{\mathbb{Z}} B$

(weil $v_{z_1} - v_{z_2} = v_{z_1 - z_2}, z = z_1 - z_2 \neq 0 \Rightarrow v_z \notin \operatorname{Span}_{\mathbb{Z}} B$).

„$\Leftarrow$“ Wir nehmen nun an, daß $\dim_{\mathbb{Z}} M = n$, d.h. $n = m$. Dann ist $B = \begin{pmatrix} d_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & d_n \end{pmatrix}$,

$d_i \neq 0$, und

$\mathbb{Z}^n / \operatorname{Span}_{\mathbb{Z}} B \cong \mathbb{Z}^n/M$.

Wir berechnen

$|\mathbb{Z}^n / \operatorname{Span}_{\mathbb{Z}} B| = |\mathbb{Z}/d_1\mathbb{Z} \bigoplus \dots \bigoplus \mathbb{Z}/d_n\mathbb{Z}| = \prod_{i=1}^n |d_i| < \infty$

□

(ii) Zusatz: Wir sehen außerdem, daß $n = m \Rightarrow |\mathbb{Z}^n/M| = |\det B| = |\det A|$, d.h
$n = m \Rightarrow [\mathbb{Z}^n : M] = |\det A|$.