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

21.Vorlesung

17 Juli 2017

§Idealnorm und Eigenschaften

Erinnerung: Sei $L/\mathbb{Q}$ ein Zahlkörper, $\mathcal{O}_L = \overline{\mathbb{Z}}^L$, $\mathcal{O}_L$ ist Dedekindring.

Definition 21.1
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, definiere
$N(\mathfrak{a}) := [\mathcal{O}_L : \mathfrak{a}] = |(\mathcal{O}_L, +)/(\mathfrak{a}, +)|$ (endlich oder ∞)

Satz 21.1 1. Sei $\mathfrak{b} \neq 0$, $\mathfrak{b} \lhd \mathcal{O}_L$, dann ist $N(\mathfrak{b}) < \infty$

2. $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ für $\neq 0$ Ideale $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$

Beweis. Wir zeigen (1) und daß

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

für $\mathfrak{p} \lhd \mathcal{O}_L$ ein Primideal.
(2. folgt aus $(**)$ wegen Primfaktorisierung von Idealen in Dedekindringen).
Zu 1.: Sei $0 \neq \alpha \in \mathfrak{b}$ und Ω die normale Hülle von $L/\mathbb{Q}$, $n := \deg L$ und $\sigma_1, \ldots, \sigma_n$ die n verschiedenen Einbettungen von L in Ω. Setze $0 \neq \alpha = \sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ und
$n_\alpha := N_{L/\mathbb{Q}}(\alpha) \underset{\text{Satz 11.4}}{=} \prod_{i=1}^n \sigma_i(\alpha) = \alpha \prod_{i=2}^n \sigma_i(\alpha)$.
(Bemerke, daß (Korollar 12.1) $n_\alpha \in \mathbb{Z}$, da $\alpha \in \mathcal{O}_L$), 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 $< n_\alpha >= \mathcal{O}_L n_\alpha \subseteq \mathfrak{b}$. (und wir haben 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, insbesondere ist $\mathcal{O}_L$ ein endlich erzeugter $\mathbb{Z}$-Modul und so ist auch $\mathcal{O}_L/ < n_\alpha >$. Außerdem ist $\mathcal{O}_L/ < n_\alpha >= (\mathcal{O}_L/ < n_\alpha)_{\text{tor}}$ ein Torsionsmodul (5. Vorlesung), und ein endlich erzeugter Torsionsmodul über $\mathbb{Z}$ ist endlich (folgt aus Struktursatz für endlich erzeugte Moduln über HIR in 6. Vorlesung). Insbesondere ist $\mathcal{O}_L/\mathfrak{b}$ auch endlich (als Bild von ψ).
Zu $(**)$: Wir zeigen, daß

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

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

(a) ist klar (3. Isomorphiesatz für Gruppen):
$\mathcal{O}_L/\mathfrak{ap} \to \mathcal{O}_L/\mathfrak{a}$, $x + \mathfrak{ap} \mapsto x + \mathfrak{a}$ ist ein surjektiver Homomorphismus von Gruppen mit Kern $\mathfrak{a}/\mathfrak{ap}$, also $\mathcal{O}_L/\mathfrak{a} \cong (\mathcal{O}_L/\mathfrak{ap})/(\mathfrak{a}/\mathfrak{ap})$, also ist $|\mathcal{O}_L/\mathfrak{a}| = \frac{|\mathcal{O}_L/\mathfrak{ap}|}{|\mathfrak{a}/\mathfrak{ap}|}$ (Lagrange).
Zu (b): Bemerke, daß $\mathfrak{ap} \subsetneq \mathfrak{a}$ (Eindeutigkeit der Primfaktorisierung).

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

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

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

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

Da $\mathfrak{ap} + < x > = \mathfrak{a}$, ist ψ surjektiv mit $\ker\psi \supseteq \mathfrak{p}$. Da $\mathfrak{p}$ maximal ist, und $\mathfrak{ap} \neq \mathfrak{a}, \ker\psi \neq \mathcal{O}_L$, folgt $\mathfrak{p} = \ker\psi$. D.h. $\mathcal{O}_L/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$

□

Als Nächstes wollen wir die folgende Proposition Zeigen:

Proposition 21.2
Sei $0 \neq \beta \in \mathcal{O}_L$. Es ist $\underbrace{N(< \beta >)}_{\in\mathbb{N}} = |\underbrace{N_{L/\mathbb{Q}}(\beta)}_{\in\mathbb{Z}}|$.

Bevor wir die Proposition 21.2 beweisen, brauchen wir :

Bemerkung (i) Sei N ein freier $\mathbb{Z}$-Modul vom Rang n und $M \leq N$ ein Untermodul (dann ist M frei vom Rang $\leq n$, da $\mathbb{Z}$ ein HIR ist).

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

Beweis von (i).

Behauptung 1: Sei $\{y_1, \ldots, y_m\}$ eine $\mathbb{Z}$-Basis für M. Schreibe $A := \begin{pmatrix} y_1 \\ \ldots \\ y_m \end{pmatrix}$, $y_j \in \mathbb{Z}^n$.

$A \in M_{m\times n}(\mathbb{Z})$

Nun zeigt ÜB, daß elementare Zeilen- und Spaltenumformungen eine Matrix B mit folgender Eigenschaft ergeben:

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

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

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

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 $v_z := (\underbrace{0, \ldots, 0}_{m}, \underbrace{z}_{\in\mathbb{Z}}, 0, \ldots, 0)$. Aus $z_1 \neq z_2$ folgt $v_{z_1} \neq v_{z_2}$ mod $\mathrm{Span}_{\mathbb{Z}}B$

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

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

$d_i \neq 0$, und

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

Wir berechnen

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

□

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

$A = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ für eine Basis $\{y_1, \ldots, y_n\} \subseteq M$ von M über $\mathbb{Z}$.

Um Proposition 21.2 zu beweisen, brauchen wir noch eine Berechnung:

Proposition 21.3
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. 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 (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:
$D(y_1, \ldots, y_n) \underset{14.Vor.}{=} \det A^2 D(e_1, \ldots, e_n) = \det A^2 D(\mathcal{O}_L/\mathbb{Z})$.
Andererseits folgt aus Bemerkung (ii), daß
$|\det A| = [\mathcal{O}_L : \mathfrak{a}]$.
Alles zusammen ergibt: $D(y_1, \ldots, y_n) = N(\mathfrak{a})^2 D(\mathcal{O}_L/\mathbb{Z})$ □

Beweis von Proposition 21.2. 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 21.3 folgern wir, daß
$D(\beta e_1, \ldots, \beta e_n) = D(\mathcal{O}_L/\mathbb{Z})N(< \beta >)^2$. Andererseits wissen wir, daß
$D(\beta e_1, \ldots, \beta e_n) = \det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j))$. Wir berechnen:
$\det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j)) = (\det((\sigma_i(\beta e_j))_{ij}))^2 = (\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}))^2$. Nun ist
$\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}) = \sigma_1(\beta) \ldots \sigma_n(\beta) \det(\sigma_i(e_j))_{ij} = N_{L/\mathbb{Q}}(\beta) \det(\sigma_i(e_j)_{ij})$. Alles zusammen ergibt:

$$D(\beta e_1, \ldots, \beta e_n) = (N_{L/\mathbb{Q}}(\beta))^2 (\det(\sigma_i(e_j))_{ij})^2 = (N_{L/\mathbb{Q}}(\beta))^2 D(e_1, \ldots, e_n) \underset{\text{Prop 21.3}}{=} N(< \beta >)^2 D(e_1, \ldots, e_n)$$

□