Algebraische Zahlentheorie

SS 2013

Kuhlmann

21. Vorlesung am 04.07.2013

§ Idealnorm und Eigenschaften.

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

Definition 1.

Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, definiere

$$N(\mathfrak{a}) := [\mathcal{O}_L : \mathfrak{a}] = \left| (\mathcal{O}_L, +) / (\mathfrak{a}, +) \right|$$

(endlich oder ∞).

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

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

für $\neq 0$ Ideale $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$

Beweis: wir zeigen (1) und daß

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

für $\mathfrak{p} \lhd \mathcal{O}_L$ Primideal

((2) folgt aus (**) dann wegen Primfaktorisierung von Idealen in Dedekindringe).

Zu (1): Sei $0 \neq \alpha \in \mathfrak{b}$ und Ω die Normalhülle von $L/\mathbb{Q}$, $n := \deg L$ und $\sigma_1, \ldots, \sigma_n$ die n

verschiedene Einbettungen von L in Ω.

Setze $0 \neq \alpha = \sigma_1(\alpha), \dots, \sigma_n(\alpha)$ und

$$n_\alpha := N_{L/\mathbb{Q}}(\alpha) \underset{\substack{\text{Satz 4} \\ \text{11. Vor}}}{=} \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \prod_{i=2}^{n} \sigma_i(\alpha)$$

[Bemerke daß (Kor 1. 12. Vor) $n_\alpha \in \mathbb{Z}$ 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 $\mathbb{Z}$,

so $\prod_{i=2}^{n} \sigma_i(\alpha)$ ist 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 $\langle n_\alpha \rangle = \mathcal{O}_L n_\alpha \subseteq \mathfrak{b}$.

[und wir haben einen surjektiven Homomorphismus

$\psi: \mathcal{O}_L / \langle n_\alpha \rangle \longrightarrow \mathcal{O}_L / \mathfrak{b}$].

Nun ist $\mathcal{O}_L$ freier $\mathbb{Z}$-Modul vom Rang n,

insbesondere ist $\mathcal{O}_L$ endl. erzeugt $\mathbb{Z}$-Modul

und so ist auch $\mathcal{O}_L / \langle n_a \rangle$.

Außerdem ist $\mathcal{O}_L / \langle n_a \rangle = \left(\mathcal{O}_L / \langle n_a \rangle \right)_{tor}$ ist Torsionsmodul (5. Vor), und ein endl. erz. Torsionsmodul über $\mathbb{Z}$ ist endlich (folgt aus Strukturssatz für endlich erzeugte Moduln über HIR 6. Vor). Insbesondere ist $\mathcal{O}_L / b$ auch endlich (als Bild von ψ). ∎ (1)

Zu (**): Wir zeigen daß

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

und

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

(dann hätten wir (**) etabliert).

ⓐ ist klar (3. Isomorphiesatz für Gruppen):

$$\mathcal{O}_L / a\mathfrak{p} \twoheadrightarrow \mathcal{O}_L / a \qquad x + a\mathfrak{p} \longmapsto x + a$$

ist surjektiver Homomorphismus von Gruppen mit Kernel $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$, so

$$\mathcal{O}_L/\mathfrak{a} \simeq \mathcal{O}_L/\mathfrak{a}\mathfrak{p} \;/\; \mathfrak{a}/\mathfrak{a}\mathfrak{p},$$

also ist $|\mathcal{O}_L/\mathfrak{a}| = \dfrac{|\mathcal{O}_L/\mathfrak{a}\mathfrak{p}|}{|\mathfrak{a}/\mathfrak{a}\mathfrak{p}|}$ (Lagrange). ■ (a)

Zu (b): Bemerke daß $\mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a}$

(Eindeutigkeit der Primfaktorisierung).

Beh: Seien $I \lhd \mathcal{O}_L$ s.d.

$\mathfrak{a}\mathfrak{p} \subseteq I \subseteq \mathfrak{a}$, dann ist

$I = \mathfrak{a}\mathfrak{p}$ oder $I = \mathfrak{a}$.

Bew der Beh:

$$\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{p} \subseteq \mathfrak{a}^{-1} I \subseteq \mathcal{O}_L$$

i.e $\mathfrak{p} \subseteq \mathfrak{a}^{-1} I \subseteq \mathcal{O}_L$,

$\mathfrak{p}$ maximal $\Rightarrow$ $\mathfrak{p} = \mathfrak{a}^{-1} I$ (i.e $\mathfrak{a}\mathfrak{p} = I$)
oder $\mathcal{O}_L = \mathfrak{a}^{-1} I$ (i.e $\mathfrak{a} = I$). □ Beh

Sei nun $x \in \mathfrak{a}$, $x \notin \mathfrak{a}\mathfrak{p}$ und betrachte

$\mathfrak{a}\mathfrak{p} + \langle x \rangle$. Wir haben

$$\mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a}\mathfrak{p} + \langle x \rangle \subseteq \mathfrak{a}$$

so $\mathfrak{a}\mathfrak{p} + \langle x \rangle = \mathfrak{a}$

Wir definieren einen Homomorphismus

$$\varphi : \mathcal{O}_L \longrightarrow \mathfrak{a}/\mathfrak{a}\mathfrak{p}$$

$$y \longmapsto \underbrace{yx}_{\in \mathfrak{a}} + \mathfrak{a}\mathfrak{p}$$

Da $\mathfrak{a}\mathfrak{p} + \langle x \rangle = \mathfrak{a}$ ist φ surjektiv

mit $\ker \varphi \supseteq \mathfrak{p}$. Da $\mathfrak{p}$ maximal ist,

und $\mathfrak{a}\mathfrak{p} \neq \mathfrak{a}$, $\ker \varphi \neq \mathcal{O}_L$,

folgt $\mathfrak{p} = \ker \varphi$.

D.h $\mathcal{O}_L/\mathfrak{p} \simeq \mathfrak{a}/\mathfrak{a}\mathfrak{p}$. □ (6). ■ Satz 1

Als nächstes wollen wir die folgende

Proposition zeigen:

Proposition 1. 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 1 beweisen brauchen wir

allgemeine Bemerkungen:

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

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

Beweis von (i): Bzl Sei $\{y_1, \dots, y_m\}$ $\mathbb{Z}$-Basis für M.

Schreibe $A := \begin{pmatrix} y_1 \\ \hline \cdots \\ \hline y_m \end{pmatrix}$ $y_j \in \mathbb{Z}^n$

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

Nun zeigen Auf 4.4 (a) und (b) daß elementare Zeilen und Spaltenumformungen

ergeben eine Matrix B mit der Eigenschaft daß

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

$$= \mathbb{Z}^n / M \,. \qquad \square \text{ Beh 1}$$

Beh 2: [Analog zu Aufg 4.4 (c)]:

Zeilen und Spaltenumformungen ergeben

B aus der Form $B = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & (*) \\ 0 & & d_m & \end{array}\right)$

$d_i \in \mathbb{Z}$, $d_i \neq 0$ (da $\{y_1, \dots, y_m\}$ $\mathbb{Z}$-lin. unab sind) $\square$ **Beh 2**

Mit **Beh 1** und **Beh 2** können wir nun die Äquivalenz $\Leftrightarrow$ in **(i)**:

"$\Rightarrow$" Wir nehmen an $m < n$ und zeigen $[\mathbb{Z}^n : M] = \infty$.

Setze $v_z := (0, \dots, 0, \underbrace{z}_{m}, \underbrace{0, \dots, 0}_{z \in \mathbb{Z}})$.

Aus $z_1 \neq z_2$ folgt $v_{z_1} \not\equiv v_{z_2} \bmod \operatorname{span}_{\mathbb{Z}} B$

(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 $\dim_{\mathbb{Z}} M = n$, i.e $n = m$.

Dann ist $B = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$ und $\mathbb{Z}^n / \operatorname{span}_{\mathbb{Z}} B \simeq \mathbb{Z}^n / M$

$d_i \neq 0$

Wir berechnen:

$$\left| \mathbb{Z}^n / \operatorname{span}_{\mathbb{Z}} B \right| = \left| \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_n\mathbb{Z} \right|$$

$$= \prod_{i=1}^{n} |d_i| < \infty. \qquad \blacksquare (i).$$

(ii) Wir sehen außerdem daß:

$$n = m \Rightarrow |\mathbb{Z}^n / M| = |\det B| = |\det A|$$

i.e $n = m \Rightarrow [\mathbb{Z}^n : M] = |\det A|$ wobei

$$A = \begin{pmatrix} y_1 \\ \hline \dots \\ \hline y_n \end{pmatrix}$$ für eine Basis $\{y_1, \dots, y_n\} \subseteq M$ für M über $\mathbb{Z}$. $\blacksquare$ (ii)

Um Proposition 1 zu beweisen brauchen wir noch eine Berechnung:

<u>Proposition 3</u>: Sei $L/\mathbb{Q}$ Zahlkörper von Grad n, $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, $\{y_1, \dots, y_n\}$ eine $\mathbb{Z}$-Basis für $\mathfrak{a}$.

Es ist : $D(\mathcal{O}_L/\mathbb{Z})\, N(\mathfrak{a})^2 = D(y_1, \dots, y_n)$

Beweis: Wir wissen daß $\mathcal{O}_L$ frei $\mathbb{Z}$-Modul vom Rang n ist, und außerdem daß $[\mathcal{O}_L : \mathfrak{a}] < \infty$.

Es folgt aus Bemerkungen (i) daß $\mathfrak{a}$ frei $\mathbb{Z}$-Modul vom Rang n ist.

Sei $\{e_1, \dots, e_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$ und
$\{y_1, \dots, y_n\}$ eine $\mathbb{Z}$-Basis für $\mathfrak{a}$

schreibe $y_i = \sum y_{ij} e_j \qquad y_{ij} \in \mathbb{Z}$

und sei A die Matrix mit y_{ij} als ij-te Eintrag, i.e $A_{ij} = y_{ij}$.

Wir berechnen :

$$D(y_1, \dots, y_n) \underset{\text{14. Vor.}}{=} \det A^2 \; D(e_1, \dots, e_n).$$

$$\underset{\text{S. 4}}{=} \det A^2 \; D(\mathcal{O}_L/\mathbb{Z})$$

Anderseits folgt aus Bemerkungen (ii) daß

$$|\det A| = [\mathcal{O}_L : \mathfrak{a}].$$

Alles zusammen ergibt:

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

Beweis von Proposition 1: Sei $\{e_1, \dots, e_n\}$ eine $\mathbb{Z}$-Basis für O_L, dann ist $\{\beta e_1, \dots, \beta e_n\}$ eine $\mathbb{Z}$-Basis für $\langle \beta \rangle$. Aus Proposition 3 folgern wir daß

$$D(\beta e_1, \dots, \beta e_m) = D(O_L / \mathbb{Z}) \, N(\langle \beta \rangle)^2.$$

Anderseits wissen wir daß

$$D(\beta e_1, \dots, \beta e_m) = \det \left(B_{L/\mathbb{Q}} (\beta e_i, \beta e_j) \right).$$

Wir berechnen:

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

$$= \left[\det \left((\sigma_i(\beta) \; \sigma_i(e_j))_{ij} \right) \right]^2$$

Nun ist

$$\det \left((\sigma_i(\beta) \sigma_i(e_j))_{ij} \right. = \sigma_1(\beta) \cdots \sigma_n(\beta) \det \left(\sigma_i(e_j)_{ij} \right.$$

$$= N_{L/\mathbb{Q}}(\beta) \det \left(\sigma_i(e_j)_{ij} \right).$$

Alles zusammen ergibt:

$$D(\beta e_1, \dots, \beta e_m) = \left(N_{L/\mathbb{Q}}(\beta) \right)^2 \left[\det \left(\sigma_i(e_j)_{ij} \right. \right]^2$$

$$= \left[N_{L/\mathbb{Q}}(\beta) \right]^2 D(e_1, \dots, e_n) \underset{\text{Prop 3}}{=} N(\langle \beta \rangle)^2 D(e_1, \dots, e_n). \blacksquare$$