

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

## 24. Vorlesung

13. Juli 2021

*Sei  $L/\mathbb{Q}$  ein Zahlkörper mit  $[L : \mathbb{Q}] = n$ . Unser Ziel ist es Satz 23.4 (†) beweisen. Wir werden sogar eine explizite Minkowski Schranke  $c_L$  in Satz 24.2 angeben. Hier werden wir in Satz 24.1 wie angekündigt im Skript 22 den Idealen von  $\mathcal{O}_L$  Gittern in  $\mathbb{R}^n$  zuordnen. Dann werden wir genaue Volumen Berechnungen anstellen. Wir werden weiterhin, oft stillschweigend, die Notationen und Ergebnisse von [Algebra II], sowie die Eigenschaften der Norm und Diskriminante benutzen. Damit werden wir schließlich für den Beweis vom Satz 24.2 Minkowski's Satz 21.8 aufrufen können. Den Beweis von Satz 24.2 werden wir in Skript 25 ausführen.*

### Ansatz wie am Anfang der 22. Vorlesung (Erinnerung).

Wir definieren nun eine  $\mathbb{Q}$ -lineare Abbildung  $\sigma$  wie folgt:

$$\sigma : L \rightarrow L_{\mathbb{R}} ; \sigma(\alpha) := (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha)) .$$

Wir erinnern an die Notation:

(\*) Für  $z \in \mathbb{C}$  und  $i = \sqrt{-1}$ , ist  $\operatorname{Re} z = \frac{z+\bar{z}}{2}$  und  $\operatorname{Im} z = \frac{z-\bar{z}}{2i}$ .

### Satz 24.1

Sei  $0 \neq \mathfrak{a} \triangleleft \mathcal{O}_L$ , dann ist  $\sigma(\mathfrak{a})$  ein vollständiges Gitter.

*Beweis.* Sei  $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathcal{O}_L$  eine Basis für  $L/\mathbb{Q}$ .

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

*Beweis.* Setze für  $i = 1, \dots, n$

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

Nun definiere entsprechend die Matrix  $A := \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix}$ .

Andererseits erinnern wir an die Matrix (die wir schon im ÜB untersucht haben):

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

Da  $\{\alpha_1, \dots, \alpha_n\}$  Basis ist haben wir (wie wir im ÜB berechnet haben):

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

Wir vergleichen nun die Matrix  $A$  mit der Matrix  $\mathcal{V}$ : wir können  $A$  durch elementare Spaltenumformungen aus  $\mathcal{V}$  bekommen (siehe Berechnungsaufstellung in (\*\*)) weiter unten Seite 2), also ist auch  $\det A \neq 0$ .  $\square$

Nun ist  $\mathfrak{a}$  ein freier  $\mathbb{Z}$ -Modul vom Rang  $n$ , also wählen wir nun  $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathfrak{a}$  (Satz und Bemerkung 22.1). Also ist  $\sigma(\mathfrak{a}) = \text{Span}_{\mathbb{Z}}\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$  ein vollständiges Gitter.  $\square$

(\*\*) Wir skizzieren nun die Berechnung zwischen  $A$  und  $\mathcal{V}$ , beziehungsweise zwischen  $\det A$  und  $\det \mathcal{V}$  (bitte die Details prüfen).

Wir durchführen die folgende Spaltenumformungen auf  $\mathcal{V}$  (wofür wir (\*) ausnutzen):

$$\begin{pmatrix} \dots & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \dots \\ & \vdots & \vdots & \\ \dots & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \dots \end{pmatrix} \xrightarrow{I+II} \begin{pmatrix} \dots & \text{Re } \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \dots \\ & \vdots & \vdots & \\ \dots & \text{Re } \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \dots \end{pmatrix}$$

wobei I und II die folgende Umformungen sind:

- I:  $(s+1)$ -te Spalte von  $\mathcal{V}$  wird mit  $\frac{1}{2}$  multipliziert.
- II: Addiere die  $(s+2)$ -te Spalte zur  $(s+1)$ -te Spalte.

Dann

$$\xrightarrow{III+IV} \begin{pmatrix} \dots & \text{Re } \sigma_{s+1}(\alpha_1) & \text{Im } \sigma_{s+1}(\alpha_1) & \dots \\ & \vdots & \vdots & \\ \dots & \text{Re } \sigma_{s+1}(\alpha_n) & \text{Im } \sigma_{s+1}(\alpha_n) & \dots \end{pmatrix}$$

wobei III und IV die folgende Umformungen sind:

- III:  $(s+2)$ -te Spalte minus  $(s+1)$ -te Spalte.
- IV: multipliziere mit  $i$ .

Dann wiederhole für  $(s+3)$ -te bis  $(s+t)$ -te Spalte, insgesamt  $t$  mal. Alles zusammen ergibt:

$$\det A = \left(\frac{1}{2}i\right)^t \det \mathcal{V}.$$

Als nächstes wollen wir nun das Gitter  $\sigma(\mathfrak{a}) \subseteq L_{\mathbb{R}}$  und  $T_{\sigma(\mathfrak{a})}$  studieren. Wir brauchen einige Bemerkungen:

### Bemerkung 24.1

Sei  $\Gamma \subseteq \mathbb{R}^n$  ein vollständiges Gitter mit Basis  $\{v_1, \dots, v_n\}$  und f.P.  $T_{\Gamma}$ .

Es ist  $v(T_{\Gamma}) = \left| \det \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix} \right|$

*Beweis.* Siehe ÜB.  $\square$

**Bemerkung 24.2**

Wir wollen Bemerkung 24.1 anwenden mit  $\Gamma = \sigma(\mathfrak{a})$ . Wir berechnen:

$$v(T_{\sigma(\mathfrak{a})}) = |\det A| = \left| \left(\frac{1}{2}(i)\right)^t \det \mathcal{V} \right|.$$

Andererseits ist

$$(\det \mathcal{V})^2 \stackrel{\text{ÜB}}{=} D(\alpha_1, \dots, \alpha_n) \stackrel{\text{Prop. 23.1}}{=} N(\mathfrak{a})^2 D(\mathcal{O}_L/\mathbb{Z}).$$

Alles zusammen ergibt:

$$v(T_{\sigma(\mathfrak{a})}) = 2^{-t} N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}.$$

**Bemerkung 24.3**

Sei  $\tau \in \mathbb{R}_+$  und setze

$$X_\tau := \{(x_1, \dots, x_s, z_1, \dots, z_t) \in L_{\mathbb{R}} ; \sum_{i=1}^s |x_i| + 2 \sum_{j=1}^t |z_j| < \tau\}.$$

Dann ist  $X_\tau$  beschränkt, konvex, symmetrisch und

$$v(X_\tau) = 2^s \left(\frac{\pi}{2}\right)^t \frac{\tau^n}{n!}$$

*Beweis.* Siehe ÜB. □

**Erinnerung (AGU):** Seien  $a_1, \dots, a_n \in \mathbb{R}_+$ ,  $n \in \mathbb{N}$ . Es ist

$$\left(\prod_{i=1}^n a_i\right)^{\frac{1}{n}} \leq \frac{1}{n} \left(\sum_{i=1}^n a_i\right)$$

Wir können nun eine genauere Aussage über die Minkowski Schranke (Satz 23.4) schreiben.

**Satz 24.2** (Explizite Minkowski Schranke)

Sei  $L/\mathbb{Q}$  ein Zahlkörper mit  $[L:\mathbb{Q}] = n$ . Setze

$$c_L := \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}.$$

Dann gilt:

$$\forall 0 \neq \mathfrak{a} \triangleleft \mathcal{O}_L \exists 0 \neq \alpha \in \mathfrak{a}$$

so daß

$$|N_{L/\mathbb{Q}}(\alpha)| \leq c_L N(\mathfrak{a})$$

*Beweis.* Folgt im Skript 25. □