

Algebraische Zahlentheorie

Vorlesung 25

Zahlbereiche als Gitter

Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung vom Grad n . Gemäß Satz 7.12 gibt es n verschiedene Einbettungen von K in \mathbb{C} . Diese kann man zur komplexen Gesamteinbettung

$$\tau: K \longrightarrow \mathbb{C}^n$$

zusammenfassen. Insbesondere ist das Bild des Ganzheitsringes R unter dieser Abbildung interessant und erlaubt einen Zugang zu R , bei dem Methoden der diskreten Geometrie, der linearen Algebra, der Maßtheorie eingesetzt werden können. Nach Korollar 8.6 ist

$$R \cong \mathbb{Z}^n,$$

wobei die Standardbasis einer Ganzheitsbasis b_1, \dots, b_n von R entspricht. Diese legt die komplexe Ganzheitsmatrix

$$(\tau_j(b_k))_{1 \leq j, k \leq n}$$

fest. Sie definiert ein „komplexes Gitter“ im \mathbb{C}^n , das Quadrat ihrer Determinante ist nach Lemma 8.9 die Diskriminante, u.s.w. Allerdings entwickeln die angesprochenen Methoden ihre Schlagkraft deutlicher, wenn man zu der komplexen Gesamteinbettung eine reelle Version entwickelt.

Bei einer Einbettung

$$\sigma: K \longrightarrow \mathbb{C}$$

unterscheidet man, ob das Bild innerhalb der reellen Zahlen liegt oder nicht. Im ersten Fall spricht man von einer *reellen Einbettung*. Wenn σ keine reelle Einbettung ist, so spricht man von einer komplexen Einbettung, in diesem Sinn ist also eine reelle Einbettung nicht komplex. Zu einer komplexen Einbettung σ ist auch die konjugiert-komplexe Einbettung

$$\bar{\sigma}: K \xrightarrow{\sigma} \mathbb{C} \xrightarrow{\text{komplexe Konjugation}} \mathbb{C}$$

eine komplexe Einbettung, und zwar ist $\sigma \neq \bar{\sigma}$, denn sonst wäre σ eine reelle Einbettung. Komplexe Einbettungen treten also immer paarweise auf. Es sei r die Anzahl der reellen Einbettungen und $2s$ die Anzahl der komplexen Einbettungen, also s sei die Anzahl der Paare von komplexen Einbettungen. Dann gilt

$$n = r + 2s.$$

Häufig fixiert man zu jedem Paar von komplexen Einbettungen eine Einbettung davon, da sich die andere daraus direkt ablesen lässt. Die Wahl ist dabei

willkürlich. Alle numerisch möglichen Kombinationen von r und s treten auch auf.

Es seien ρ_i , $i = 1, \dots, r$ die reellen Einbettungen und σ_j , $j = 1, \dots, s$ Repräsentanten der Paare von komplexen Einbettungen. Dies definiert eine Gesamteinbettung

$$K \longrightarrow \mathbb{R}^r \times \mathbb{C}^s,$$

die wir die *reelle Gesamteinbettung* nennen. Wenn man einzelne komplexe Einbettungen durch ihre konjugierten Einbettungen ersetzt, so ergibt sich ein natürlicher \mathbb{R} -linearer Isomorphismus. Dabei gilt als reeller Vektorraum

$$\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^r \times \mathbb{R}^{2s} = \mathbb{R}^n,$$

d.h. die reelle Dimension des Einbettungsraumes stimmt mit dem Grad der Körpererweiterung überein. Zwischen der reellen Gesamteinbettung und der komplexen Gesamteinbettung besteht der Zusammenhang

$$\begin{array}{ccc} K & \xrightarrow{\tau^{\mathbb{R}}} & \mathbb{R}^r \times \mathbb{C}^s \\ \tau \searrow & & \downarrow \psi \\ & & \mathbb{C}^{r+2s}, \end{array}$$

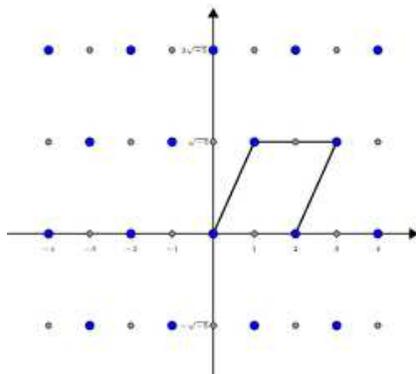
wobei ψ in den ersten r Komponenten die natürliche Einbettung $\mathbb{R} \subset \mathbb{C}$ und in den hinteren Komponenten die Abbildung $\mathbb{C} \rightarrow \mathbb{C} \times \mathbb{C}$, $z \mapsto (z, \bar{z})$, ist. Somit ist ψ eine \mathbb{R} -lineare Abbildung. Ein Element $b \in K$ wird unter der reellen Gesamteinbettung auf

$$\tau^{\mathbb{R}}(b) = \begin{pmatrix} \rho_1(b) \\ \vdots \\ \rho_r(b) \\ \operatorname{Re}(\sigma_1(b)) \\ \operatorname{Im}(\sigma_1(b)) \\ \vdots \\ \operatorname{Re}(\sigma_s(b)) \\ \operatorname{Im}(\sigma_s(b)) \end{pmatrix}$$

und unter der komplexen Gesamteinbettung auf

$$\tau(b) = \begin{pmatrix} \rho_1(b) \\ \vdots \\ \rho_r(b) \\ \sigma_1(b) \\ \bar{\sigma}_1(b) \\ \vdots \\ \sigma_s(b) \\ \bar{\sigma}_s(b) \end{pmatrix}$$

abgebildet.



Das Gitter zum Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ und zum Ideal $(2, 1 + \sqrt{-5})$ (blau, mit einer Grundmasche).

Die reelle Gesamtabbildung ist trivialerweise injektiv, da sie ja sogar in jeder einzelnen Komponente injektiv ist. Für die Gittertheorie der algebraischen Zahlen (Minkowski-Theorie) ist aber entscheidend, dass das Bild des Rings der ganzen Zahlen ein Gitter in diesem \mathbb{R}^n ist, also nicht in einem reellen Untervektorraum kleinerer Dimension liegt. Der Zahlbereich wird auf ein Gitter abgebildet, eine Ganzheitsbasis auf eine Gitterbasis.

DEFINITION 25.1. Es sei R ein Zahlbereich vom Grad n mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei

$$\tau^{\mathbb{R}}: R \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^r \times \mathbb{R}^{2s}$$

die reelle Gesamteinbettung. Es sei b_1, \dots, b_n eine Ganzheitsbasis von R . Dann nennt man die reelle $n \times n$ -Matrix

$$\left(\tau_j^{\mathbb{R}}(b_k) \right)_{1 \leq j, k \leq n}$$

die *reelle Ganzheitsmatrix* (zu dieser Basis).

Die reelle Ganzheitsmatrix steht mit der komplexen Ganzheitsmatrix in dem oben durch ψ beschriebenen Zusammenhang.

SATZ 25.2. *Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung vom Grad n mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei*

$$\tau^{\mathbb{R}}: K \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$$

die reelle Gesamteinbettung. Dann ist das Bild des Ganzheitsringes von K unter τ ein Gitter in \mathbb{R}^n

Beweis. Es sei b_1, \dots, b_n eine Ganzheitsbasis von R . Es ist zu zeigen, dass die $\tau^{\mathbb{R}}(b_k)$, $k = 1, \dots, n$, linear unabhängig sind. Über die \mathbb{R} -lineare Abbildung

$$\mathbb{R}^r \times \mathbb{R}^{2s} \longrightarrow \mathbb{C}^r \times \mathbb{C}^{2s}, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ u_1 \\ v_1 \\ \vdots \\ u_s \\ v_s \end{pmatrix} \longmapsto \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ u_1 + \mathrm{i}v_1 \\ u_1 - \mathrm{i}v_1 \\ \vdots \\ u_s + \mathrm{i}v_s \\ u_s - \mathrm{i}v_s \end{pmatrix},$$

erhält man aus der reellen Gesamteinbettung die komplexe Gesamteinbettung. Wären die Elemente \mathbb{R} -linear abhängig, so würde das auch für die Bilder unter der komplexen Gesamteinbettung gelten. Doch dies wäre ein Widerspruch zur Tatsache, dass die Diskriminante von b_1, \dots, b_n nicht 0 ist, siehe Lemma 8.3. \square

Wir werden dieses Gitter im \mathbb{R}^n zumeist mit Γ oder Γ_R oder Γ_K bezeichnen. Die reelle Gesamteinbettung liefert einen Gruppenisomorphismus $R \cong \Gamma \subseteq \mathbb{R}^n$.

BEISPIEL 25.3. Es sei $D < 0$ quadratfrei und A_D der zugehörige imaginär-quadratische Zahlbereich. Dann liefert eine fixierte Einbettung $A_D \subseteq \mathbb{Q}[\sqrt{D}] \subseteq \mathbb{C} \cong \mathbb{R}^2$ direkt eine Realisierung als Gitter im Sinne von Satz 25.2. Dem Element $q_1 + q_2\sqrt{D} = q_1 + q_2\sqrt{|D|}\mathrm{i}$ entspricht in der reellen Ebene das Element $\begin{pmatrix} q_1 \\ q_2\sqrt{-D} \end{pmatrix} = \begin{pmatrix} q_1 \\ q_2\sqrt{|D|} \end{pmatrix}$. Die Ganzheitsbasis $1, \sqrt{D}$ bei $D = 2, 3 \pmod{4}$ bzw. $1, \frac{1+\sqrt{D}}{2}$ bei $D = 1 \pmod{4}$ (vergleiche Satz 9.8) wird unter der reellen Gesamteinbettung auf die reelle Ganzheitsmatrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|D|} \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|D|}}{2} \end{pmatrix}$$

abgebildet.

BEISPIEL 25.4. Es sei $D \geq 2$ quadratfrei und $A_D \subseteq \mathbb{Q}[\sqrt{D}] = K$ der zugehörige reell-quadratische Zahlbereich. Es sei \sqrt{D} einerseits ein fixierte Quadratwurzel aus D in A_D und andererseits die positive reelle Quadratwurzel. Die Abbildung

$$K \longrightarrow \mathbb{R}^2, (q_1 + q_2\sqrt{D}) \longmapsto \begin{pmatrix} q_1 + q_2\sqrt{D} \\ q_1 - q_2\sqrt{D} \end{pmatrix},$$

ist dann die reelle Gesamteinbettung und liefert insbesondere eine explizite Realisierung von A_D als Gitter im Sinne von Satz 25.2. Das Gitter hängt wie die Ganzheitsbasis für A_D vom Rest von D modulo 4 ab, siehe Satz 9.8.

Die Ganzheitsbasis $1, \sqrt{D}$ bei $D = 2, 3 \pmod{4}$ bzw. $1, \frac{1+\sqrt{D}}{2}$ bei $D = 1 \pmod{4}$ (vergleiche Satz 9.8) wird unter der reellen Gesamteinbettung auf die reelle Ganzheitsmatrix

$$\begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}$$

abgebildet.

Wenn $\mathbb{Q} \subseteq K$ eine Galoiserweiterung mit einer fixierten reellen Einbettung ρ ist, so sind alle Einbettungen reell, und die gesamte Gitterabbildung wird durch

$$R \longrightarrow \mathbb{R}^n, f \longmapsto (\rho(\sigma(f)), \sigma \in \text{Gal}(K|\mathbb{Q}))$$

realisiert.

BEISPIEL 25.5. Die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}[X]/(X^3 - 3X + 1) = K$ ist eine Galoiserweiterung, wenn $\alpha \in \mathbb{R}$ eine Nullstelle von $X^3 - 3X + 1$, so sind auch $\beta = \alpha^2 - 2$ und $\gamma = -\alpha^2 - \alpha + 2$ Nullstellen, siehe Beispiel 11.2 (Körper- und Galoistheorie (Osnabrück 2018-2019)). Die Galoisgruppe permutiert diese Nullstellen. Der Automorphismus, der α auf $\alpha^2 - 2$ abbildet, schickt α^2 auf

$$(\alpha^2 - 2)^2 = \alpha^4 - 4\alpha^2 + 4 = 3\alpha^2 - \alpha - 4\alpha^2 + 4 = -\alpha^2 - \alpha + 4.$$

Wegen

$$R = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$$

wird die gesamte Gitterabbildung durch

$$R \cong \mathbb{Z}^3 \longrightarrow \mathbb{R}^3, a + b\alpha + c\alpha^2 \longmapsto \begin{pmatrix} a + b\alpha + c\alpha^2 \\ a + b(\alpha^2 - 2) + c(-\alpha^2 - \alpha + 4) \\ a + b(-\alpha^2 - \alpha + 2) + c(\alpha + 2) \end{pmatrix},$$

gegeben. Die Basis $1, \alpha, \alpha^2$ wird auf die Gitterbasis

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha \\ \alpha^2 - 2 \\ -\alpha^2 - \alpha + 4 \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ -\alpha^2 - \alpha + 4 \\ \alpha + 2 \end{pmatrix}$$

abgebildet.

Wenn man $1, \alpha, \beta$ als Ganzheitsbasis nimmt, so wird die Abbildung durch

$$R \cong \mathbb{Z}^3 \longrightarrow \mathbb{R}^3, a + b\alpha + d\beta \longmapsto \begin{pmatrix} a + b\alpha + d\beta \\ a + b\beta + d(-\alpha - \beta) \\ a + b(-\alpha - \beta) + d\alpha \end{pmatrix},$$

beschrieben. Diese Basis wird dann auf die Gitterbasis

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha \\ \beta \\ -\alpha - \beta \end{pmatrix}, \begin{pmatrix} \beta \\ -\alpha - \beta \\ \alpha \end{pmatrix}$$

abgebildet.

SATZ 25.6. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei \mathfrak{M} eine Grundmasche des Gitters Γ_R unter der reellen Gesamteinbettung*

$$\tau^{\mathbb{R}}: R \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^r \times \mathbb{R}^{2s}.$$

Dann ist das Volumen der Grundmasche bezüglich der euklidischen Standardmetrik des $\mathbb{R}^r \times \mathbb{R}^{2s}$ gleich

$$\text{Vol}(\mathfrak{M}) = \frac{1}{2^s} \sqrt{|\Delta_R|}.$$

Beweis. Wir haben die Zusammenstellung zu allen komplexen Einbettungen

$$\tau: R \longrightarrow \mathbb{C}^{r+2s}$$

und die reelle Gittereinbettung

$$\tau^{\mathbb{R}}: R \longrightarrow \mathbb{R}^r \times \mathbb{C}^s,$$

die durch die Einbettung

$$\mathbb{R}^r \times \mathbb{C}^s \longrightarrow \mathbb{C}^{r+2s}, (x_1, \dots, x_r; z_1, \dots, z_s) \longmapsto (x_1, \dots, x_r; z_1, \bar{z}_1, \dots, z_s, \bar{z}_s)$$

miteinander verbunden sind.

Zu einer \mathbb{Q} -Basis b_1, \dots, b_n von $Q(R)$ haben wir einerseits die reelle Ganzheitsmatrix

$$\begin{pmatrix} \rho_1(b_1) & \rho_1(b_2) & \dots & \dots & \rho_1(b_n) \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \rho_r(b_1) & \rho_r(b_2) & \dots & \dots & \rho_r(b_n) \\ \text{Re}(\sigma_1(b_1)) & \text{Re}(\sigma_1(b_2)) & \dots & \dots & \text{Re}(\sigma_1(b_n)) \\ \text{Im}(\sigma_1(b_1)) & \text{Im}(\sigma_1(b_2)) & \dots & \dots & \text{Im}(\sigma_1(b_n)) \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \text{Re}(\sigma_s(b_1)) & \text{Re}(\sigma_s(b_2)) & \dots & \dots & \text{Re}(\sigma_s(b_n)) \\ \text{Im}(\sigma_s(b_1)) & \text{Im}(\sigma_s(b_2)) & \dots & \dots & \text{Im}(\sigma_s(b_n)) \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|D|}}{2} \end{pmatrix}.$$

Deren Determinante, also bis auf das Vorzeichen der Flächeninhalt der Grundmasche des Gitters, ist

$$\det \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|D|} \end{pmatrix} = \sqrt{|D|}$$

bzw.

$$\det \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|D|}}{2} \end{pmatrix} = \frac{\sqrt{|D|}}{2}.$$

Die Diskriminante ist nach Lemma 9.9 gleich $4D$ bzw. D . In beiden Fällen erhält man also eine direkte Bestätigung von Satz 25.6.

BEISPIEL 25.8. Es sei $D > 2$ quadratfrei und A_D der zugehörige reell-quadratische Zahlbereich. Es gibt also zwei reelle Einbettungen und somit ist $s = 0$. Zur Ganzheitsbasis $1, \sqrt{D}$ bei $D \equiv 2, 3 \pmod{4}$ bzw. $1, \frac{1+\sqrt{D}}{2}$ bei $D \equiv 1 \pmod{4}$ gehört wie in Beispiel 25.4 berechnet die reelle Ganzheitsmatrix

$$\begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}$$

Deren Determinante ist

$$\det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} = -2\sqrt{D}$$

bzw.

$$\det \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix} = \frac{1-\sqrt{D}}{2} - \frac{1+\sqrt{D}}{2} = -\sqrt{D}.$$

Die Diskriminante ist nach Lemma 9.9 gleich $4D$ bzw. D . In beiden Fällen erhält man also wieder eine direkte Bestätigung von Satz 25.6.

SATZ 25.9. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei $\mathfrak{a} \subseteq R$ ein von 0 verschiedenes Ideal und es sei \mathfrak{N} eine Grundmasche des vollständigen Gitters $\tau^{\mathbb{R}}(\mathfrak{a})$. Dann ist das Volumen von \mathfrak{N} (bezüglich der euklidischen Standardmetrik des $\mathbb{R}^r \times \mathbb{R}^{2s}$) gleich*

$$\text{Vol}(\mathfrak{N}) = \frac{1}{2^s} \sqrt{|\Delta_R|} \cdot N(\mathfrak{a}).$$

Beweis. Das wird ähnlich wie Satz 25.6 bewiesen. □

Abbildungsverzeichnis

- Quelle = Wurzel5.png , Autor = Benutzer MGausmann auf Commons,
Lizenz = CC-by-sa 4.0 3
- Erläuterung: Die in diesem Text verwendeten Bilder stammen aus
Commons (also von <http://commons.wikimedia.org>) und haben eine
Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren
Dateinamen auf Commons angeführt zusammen mit ihrem Autor
bzw. Hochlader und der Lizenz. 9
- Lizenzklärung: Diese Seite wurde von Holger Brenner alias
Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und
unter die Lizenz CC-by-sa 3.0 gestellt. 9