10. Minkowskische Gitterpunkt-Theorie

10.1. Definition. Ein *Gitter* Λ im $\mathbb{R}^n$ (oder allgemeiner in einem n-dimensionalen reellen Vektorraum) ist eine additive Untergruppe der Gestalt

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \ldots + \mathbb{Z}\omega_n,$$

wobei $\omega_1, \omega_2, \ldots, \omega_n$ reell-linear unabhängige Vektoren sind. Diese Vektoren heißen dann eine $\mathbb{Z}$-Basis des Gitters. Ein weiteres n-tupel $\omega_1', \ldots, \omega_n'$ von Vektoren ist genau dann eine $\mathbb{Z}$-Basis desselben Gitters Λ, wenn es eine ganzzahlige $n \times n$-Matrix (c_{ij}) mit $\det(c_{ij}) = \pm 1$ gibt, so dass

$$\omega_i' = \sum_{j=1}^{n} c_{ij}\omega_j, \qquad i = 1, 2, \ldots, n.$$

Man zeigt: Eine additive Untergruppe $\Lambda \subset \mathbb{R}^n$ ist genau dann ein Gitter, wenn gilt:

(i) Λ ist eine diskrete Untergruppe des $\mathbb{R}^n$, d.h. es gibt eine Nullumgebung $U \subset \mathbb{R}^n$, so dass $\Lambda \cap U = \{0\}$.

(ii) Λ ist in keinem echten Untervektorraum $W \subsetneqq \mathbb{R}^n$ enthalten.

Ist $\Lambda = \sum_{\nu=1}^{n} \mathbb{Z}\omega_1 \subset \mathbb{R}^n$ ein Gitter, so heißt

$$\mathcal{P} := \{t_1\omega_1 + \ldots + t_n\omega_n : 0 \leqslant t_\nu \leqslant 1\}$$

Fundamental-Parallelotop oder auch *Grundmasche* des Gitters. Das Volumen des Fundamental-Parallelotops bzgl. der üblichen Euklidischen Metrik des $\mathbb{R}^n$ ist

$$\mathrm{Vol}(\mathcal{P}) = |\det(\omega_1, \ldots, \omega_n)|.$$

Bildet man das Fundamental-Paralletotop $\mathcal{P}'$ bzgl. einer anderen $\mathbb{Z}$-Basis $\omega_1', \ldots, \omega_n'$ des Gitters Λ, so ergibt sich, da die Transformations-Matrix zwischen den Basen die Determinante ± 1 hat, $\mathrm{Vol}(\mathcal{P}) = \mathrm{Vol}(\mathcal{P}')$. Dieser also nur vom Gitter abhängige Wert heißt auch das Volumen des Gitters, in Zeichen $\mathrm{Vol}(\Lambda) := \mathrm{Vol}(\mathcal{P})$.

10.2. Definition. Eine Teilmenge $B \subset \mathbb{R}^n$ heißt *konvex*, wenn mit je zwei Punkten $x, y \in B$ auch die ganze Verbindungs-Strecke

$$\{tx + (1-t)y : 0 \leqslant t \leqslant 1\}$$

in B liegt. B heißt *symmetrisch*, wenn aus $x \in B$ folgt, dass $-x \in B$.

10.3. Satz. *Sei $\Lambda \subset \mathbb{R}^n$ ein Gitter und $B \subset \mathbb{R}^n$ eine messbare, konvexe und symmetrische Teilmenge. Falls*

$$\mathrm{Vol}(B) > 2^n \mathrm{Vol}(\Lambda),$$

enthält B einen von 0 verschiedenen Gittervektor, d.h. $B \cap (\Lambda \smallsetminus \{0\}) \neq \emptyset$.

Zusatz. *Setzt man B zusätzlich als kompakt voraus, genügt als Voraussetzung über das Volumen schon $\mathrm{Vol}(B) \geqslant 2^n \mathrm{Vol}(\Lambda)$.*

Beweis. Sei P ein Fundamental-Parallelotop von Λ und $B_1 := \frac{1}{2}B$. Dann ist $\mathrm{Vol}(B_1) = 2^{-n}\mathrm{Vol}(B)$, also $\mathrm{Vol}(B_1) > \mathrm{Vol}(P)$. Da $\bigcup_{\lambda\in\Lambda}(\lambda + P) = \mathbb{R}^n$, gilt

$$\bigcup_{\lambda\in\Lambda} B_1 \cap (\lambda + P) = B_1 \qquad \Rightarrow \qquad \sum_{\lambda\in\Lambda} \mathrm{Vol}\left(B_1 \cap (\lambda + P)\right) = \mathrm{Vol}(B_1).$$

Andrerseits ist wegen der Translations-Invarianz des Volumens

$$\mathrm{Vol}((-\lambda + B_1) \cap P) = \mathrm{Vol}(B_1 \cap (\lambda + P)),$$

woraus folgt

$$\sum_{\lambda\in\Lambda} \mathrm{Vol}\left((\lambda + B_1) \cap P\right) = \mathrm{Vol}(B_1) > \mathrm{Vol}(P).$$

Wären alle $(\lambda + B_1) \cap P$ paarweise punktfremd, müsste gelten

$$\sum_{\lambda\in\Lambda} \mathrm{Vol}\left((\lambda + B_1) \cap P\right) \leqslant \mathrm{Vol}(P).$$

Da dies aber nicht der Fall ist, gibt es also Gittervektoren $\lambda_1 \neq \lambda_2$ mit

$$(\lambda_1 + B_1) \cap (\lambda_2 + B_1) \neq \emptyset.$$

Daher existieren Elemente $x, y \in B_1$, so dass

$$\lambda_1 + x = \lambda_2 + y \qquad \Rightarrow \qquad x - y = \lambda_2 - \lambda_1 =: \lambda \in \Lambda \smallsetminus \{0\}$$

Da B_1 symmetrisch ist, gilt auch $-y \in B_1$ und wegen der Konvexität folgt $\frac{1}{2}(x-y) \in B_1$. Da $B = 2 \cdot B_1$, folgt $x - y \in B$, d.h. $\lambda \in B$, q.e.d.

Zum Beweis des Zusatzes betrachte man für $\nu > 0$ die Mengen $B^{(\nu)} := (1 + \frac{1}{\nu})B$. Da $\mathrm{Vol}(B^{(\nu)}) > 2^n\mathrm{Vol}(\Lambda)$, gibt es einen Vektor $0 \neq \lambda_\nu \in B^{(\nu)} \cap \Lambda$. Eine Teilfolge λ_{ν_i} konvergiert dann gegen einen Vektor $0 \neq \lambda \in B \cap \Lambda$.

10.4. Einbettung von Zahlkörpern. Sei K ein algebraischer Zahlkörper vom Grad n. Dann gibt es insgesamt n Körper-Monomorphismen $\sigma_\nu : K \to \mathbb{C}$, d.h. Isomorphismen von K auf Unterkörper von $\mathbb{C}$. Ein solcher Isomorphismus heißt reell, falls

$\sigma_\nu(K) \subset \mathbb{R}$, andernfalls komplex. Die komplexen Isomorphismen treten stets paarweise auf, denn mit $\sigma : K \to \mathbb{C}$ ist auch $\overline{\sigma} : K \to \mathbb{C}$ ein Isomorphismus von K auf einen Unterkörper von $\mathbb{C}$. Sei r_1 die Anzahl der reellen und $2r_2$ die Anzahl der komplexen Isomorphismen; es gilt also $n = r_1 + 2r_2$. Man nennt (r_1, r_2) die Signatur des Zahlkörpers K. Wir numerieren die Isomorphismen so, dass $\sigma_1, \ldots, \sigma_{r_1}$ reell und $\sigma_{r_1+\nu}$ für $\nu = 1, \ldots, r_2$ untereinander nicht konjugierte komplexe Isomorphismen sind, sowie $\sigma_{r_1+r_2+\nu} = \overline{\sigma}_{r_1+\nu}$ für $\nu = 1, \ldots, r_2$. Wir definieren nun eine *kanonische Einbettung*

$$j \; : \; K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$$

durch

$$\begin{aligned} j(x) &:= (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+\nu}(x), \ldots, \sigma_{r_1+r_2}(x)) \\ &= (\sigma_1(x), \ldots, \sigma_{r_1}(x), \ldots, \mathsf{Re}(\sigma_{r_1+\nu}(x)), \mathsf{Im}(\sigma_{r_1+\nu}(x)), \ldots) \end{aligned}$$

10.5. Satz. *Sei K ein algebraischer Zahlkörper vom Grad n, Signatur (r_1, r_2) und Diskriminante $\Delta := \operatorname{discr}(K)$. Sei $j : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ die kanonische Einbettung. Dann gilt:*

a) *Das Bild $\Lambda := j(\mathfrak{O}_K) \subset \mathbb{R}^n$ des Ganzheitsrings ist ein Gitter mit*

$$\operatorname{Vol}(\Lambda) = 2^{-r_2}\sqrt{|\Delta|}.$$

b) *Sei $\mathfrak{a} \subset \mathfrak{O}_K$ ein Ideal. Dann is $\Gamma := j(\mathfrak{a})$ ein Gitter mit*

$$\operatorname{Vol}(\Gamma) = 2^{-r_2}\mathrm{N}(\mathfrak{a})\sqrt{|\Delta|}.$$

Beweis. Sei $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{O}_K$. Dann ist $\Lambda = \sum_{k=1}^n \mathbb{Z}j(\omega_k)$ mit

$$j(\omega_k) = (\sigma_1(\omega_k), \ldots, \sigma_{r_1}(\omega_k), \ldots, \mathsf{Re}(\sigma_{r_1+\nu}(\omega_k)), \mathsf{Im}(\sigma_{r_1+\nu}(\omega_k)), \ldots)$$

Damit gilt $\operatorname{Vol}(\Lambda) = |\det M_1|$, wobei M_1 die folgende $n \times n$-Matrix ist:

$$M_1 := \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \ldots & \mathsf{Re}(\sigma_{r_1+\nu}(\omega_1)) & \mathsf{Im}(\sigma_{r_1+\nu}(\omega_1)) & \ldots \\ \vdots & & \vdots & & \vdots & \vdots & \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \ldots & \mathsf{Re}(\sigma_{r_1+\nu}(\omega_n)) & \mathsf{Im}(\sigma_{r_1+\nu}(\omega_n)) & \ldots \end{pmatrix}$$

Andrerseits ist $|\Delta| = |\operatorname{discr}(\omega_1, \ldots, \omega_n)| = |\det M_2|^2$ mit der $n \times n$-Matrix

$$M_2 := \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \ldots & \sigma_{r_1+\nu}(\omega_1) & \overline{\sigma}_{r_1+\nu}(\omega_1) & \ldots \\ \vdots & & \vdots & & \vdots & \vdots & \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \ldots & \sigma_{r_1+\nu}(\omega_n) & \overline{\sigma}_{r_1+\nu}(\omega_n) & \ldots \end{pmatrix}$$

Durch Spalten-Umformungen sieht man, dass $|\det M_2| = 2^{r_2}|\det M_1|$. Daraus folgt die Behauptung a).

Teil b) folgt daraus, dass allgemein für ein Gitter Λ und ein Untergitter $\Lambda_1 \subset \Lambda$ gilt

$$\mathrm{Vol}(\Lambda_1) = \#(\Lambda/\Lambda_1) \cdot \mathrm{Vol}(\Lambda).$$

10.6. Hilfssatz. *Im $\mathbb{R}^n \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, $(n = r_1 + 2r_2)$, mit der üblichen Euklidischen Metrik sei*

$$B_t := \Big\{ x \in \mathbb{R}^n : \sum_{\mu=1}^{r_1} |x_\mu| + 2 \sum_{\nu=1}^{r_2} \big| x_{r_1+2\nu-1}^2 + x_{r_1+2\nu}^2 \big|^{1/2} \leqslant t \Big\}, \qquad t > 0.$$

Dann gilt

$$\mathrm{Vol}(B_t) = 2^{r_1} \Big(\frac{\pi}{2}\Big)^{r_2} \cdot \frac{t^n}{n!}.$$

Beweis. Es genügt, die Formel für $t = 1$ zu beweisen, da $\mathrm{Vol}(B_t) = \mathrm{Vol}(B_1)\, t^n$.

Für $(r_1, r_2) = (1, 0)$ ist B_1 das Intervall $[-1, 1] \subset \mathbb{R}$, also $\mathrm{Vol}(B_1) = 2$.

Für $(r_1, r_2) = (0, 1)$ ist B_1 eine Kreisscheibe vom Radius $1/2$ in $\mathbb{R}^2$, also $\mathrm{Vol}(B_1) = \pi/4$.

Den allgemeinen Fall beweist man durch vollständige Induktion unter Zuhilfenahme des Satzes von Fubini.

10.7. Satz. *Sei K ein algebraischer Zahlkörper vom Grad n, Signatur (r_1, r_2) und Diskriminante Δ. Sei $\mathfrak{a} \subset \mathfrak{O}_K$ ein ganzes Ideal $\neq (0)$. Dann gibt es ein Element $0 \neq \xi \in \mathfrak{a}$ mit*

$$|\mathrm{N}(\xi)| \leqslant \Big(\frac{4}{\pi}\Big)^{r_2} \frac{n!}{n^n} \mathrm{N}(\mathfrak{a}) \sqrt{|\Delta|}.$$

Beweis. Sei $j : K \to \mathbb{R}^n$ die kanonische Einbettung von K. Wir wenden Satz 10.3 auf das Gitter $\Gamma := j(\mathfrak{a})$ und die konvexe, symmetrische Menge B_t aus Hilfssatz 10.6 an, wobei t so bestimmt sei, dass

$$\mathrm{Vol}(B_t) = 2^n \mathrm{Vol}(\Gamma).$$

Dies bedeutet

$$2^{r_1} \Big(\frac{\pi}{2}\Big)^{r_2} \frac{t^n}{n!} = 2^n 2^{-r_2} \mathrm{N}(\mathfrak{a}) \sqrt{|\Delta|} \quad \Rightarrow \quad t^n = \Big(\frac{4}{\pi}\Big)^{r_2} n! \mathrm{N}(\mathfrak{a}) \sqrt{|\Delta|}$$

Nach Satz 10.3 existiert ein $\xi \in \mathfrak{a}$, $\xi \neq 0$, mit $j(\xi) \in B_t$. Es ist

$$j(\xi) = (x_1, \ldots, x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+2r_2}),$$

wobei

$$\begin{aligned} x_\mu &= \sigma_\mu(\xi) && \text{für } \mu = 1, \ldots, r_1 \qquad \text{und} \\ x_{r_1+2\nu-1} + i x_{r_1+2\nu} &= \sigma_{r_1+\nu}(\xi) && \text{für } \nu = 1, \ldots, r_2. \end{aligned}$$

Daraus folgt

$$|\mathrm{N}(\xi)| = |x_1| \cdot \ldots \cdot |x_{r_1}| \cdot |x_{r_1+1}^2 + x_{r_1+2}^2| \cdot \ldots \cdot |x_{r_1+2r_2-1}^2 + x_{r_1+2r_2}^2|.$$

Aus der Ungleichung zwischen geometrischem und arithmetischen Mittel ergibt sich nun

$$|\mathrm{N}(\xi)|^{1/n} \leqslant \frac{1}{n}\left(\sum_{\mu=1}^{r_1} |x_\mu| + 2\sum_{\nu=1}^{r_2} \left|x_{r_1+2\nu-1}^2 + x_{r_1+2\nu}^2\right|^{1/2}\right) \leqslant \frac{t}{n}, \qquad \text{also}$$

$$|\mathrm{N}(\xi)| \leqslant \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \mathrm{N}(\mathfrak{a})\sqrt{|\Delta|}, \qquad \text{q.e.d.}$$

10.8. Satz. *Sei K ein algebraischer Zahlkörper vom Grad n, Signatur (r_1, r_2) und Diskriminante Δ. Dann gibt es in jeder Idealklasse $\mathfrak{A}$ von K ein ganzes Ideal $\mathfrak{a} \subset \mathfrak{O}_K$ mit*

$$\mathrm{N}(\mathfrak{a}) \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\Delta|}.$$

Beweis. Sei $\mathfrak{b} \subset \mathfrak{O}_K$ ein ganzes Ideal, das zur Idealklasse $\mathfrak{A}^{-1}$ gehört. Nach Satz 10.7 gibt es ein Element $0 \neq \beta \in \mathfrak{b}$ mit

$$|\mathrm{N}(\beta)| \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \mathrm{N}(\mathfrak{b})\sqrt{|\Delta|}.$$

Da $(\beta) \subset \mathfrak{b}$, gibt es ein ganzes Ideal $\mathfrak{a} \subset \mathfrak{O}_K$ mit $(\beta) = \mathfrak{b}\mathfrak{a}$. Das Ideal $\mathfrak{a}$ gehört dann zur Idealklasse $\mathfrak{A}$ und es gilt $|\mathrm{N}(\beta)| = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$. Setzt man dies in die obige Ungleichung ein und kürzt durch $\mathrm{N}(\mathfrak{b})$, folgt die Behauptung des Satzes.

10.9. Satz. *Die Gruppe der Idealklassen eines algebraischen Zahlkörpers ist endlich.*

Dies folgt daraus, dass es nur endlich viele ganze Ideale mit vorgegebener Norm gibt.

Die Ordnung der Klassengruppe ist die sog. *Klassenzahl* des Zahlkörpers.

10.10. Beispiele.

a) $K = \mathbb{Q}(\sqrt[3]{2})$, $r_2 = 1$, $\Delta = -108$.

Jedes Ideal ist äquivalent zu einem ganzen Ideal $\mathfrak{a} \subset \mathfrak{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ mit

$$|\mathrm{N}(\mathfrak{a})| \leqslant \left(\frac{4}{\pi}\right) \frac{3!}{3^3}\sqrt{108} = 2.94\ldots$$

Da die Primzahl 2 in $\mathfrak{O}_K$ vollständig verzweigt ist, $(2) = (\sqrt[3]{2})^3$, gibt es ein einziges Ideal mit Norm 2, nämlich $(\sqrt[3]{2})$. Da dies ein Hauptideal ist, ist jedes Ideal ein Hauptideal, K hat also die Klassenzahl 1.

b) $K = \mathbb{Q}(e^{2\pi i/5})$, $r_2 = 2$, $\Delta = 5^3$.

Jedes Ideal ist äquivalent zu einem ganzen Ideal $\mathfrak{a}$ mit

$$|\mathrm{N}(\mathfrak{a})| \leqslant \left(\frac{4}{\pi}\right)^2 \frac{4!}{4^4}\sqrt{5^3} = 1.699\ldots$$

Jedes Ideal ist daher äquivalent zum Einheitsideal, also hat K die Klassenzahl 1.