GEOMETRIE DER ZAHLEN UND ENDLICHKEIT DER KLASSENZAHL

MARCEL PIRRON

In diesem Abschnitt zeigen wir, dass die definierte Klassengruppe Cl_K für einen Zahlkörper K stets endlich ist und skizzieren den Dirichletschen Einheitensatz, um die Einheiten von $\mathcal{O}_K$ näher zu bestimmen. Unsere Untersuchungen werden uns über die *Geometrie der Zahlen* führen, eine auf Hermann Minkowski zurückgehende Theorie, in der die Elemente der Zahlkörper als Punkte in einem Vektorraum angesehen werden. Diese Betrachtungsweise haben wir bereits bei den Gaussschen Zahlen gesehen, wobei wir die Inklusion $\mathbb{Z}[i] \subseteq \mathbb{C}$ ausnutzten und $\mathbb{Z}[i]$ als Gitter in der komplexen Ebene interpretiert haben.

1. Gitter

Die Protagonisten dieses Abschnittes werden die Gitter sein. Sie stellen eine Verallgemeinerung der eben angesprochenen Idee dar.

Definition 1. *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und seien $v_1, \dots, v_m \in V$ linear unabhängig. Das **Gitter** in V zur **Basis** $(v_1, \dots, v_m)$ ist die Menge*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m.$$

Ferner nennen wir die Menge

$$\Phi = \left\{ \sum_{i=1}^{m} x_i v_i \mid x_i \in \mathbb{R} \cap [0,1) \right\}$$

*eine **Grundmasche** des Gitters. Ein Gitter heisst **vollständig**, wenn $m = n$ ist.*

Bemerkung 2. In einem vollständigen Gitter überdecken die Verschiebungen $\Phi + \gamma, \gamma \in \Gamma$ den gesamten Raum V.

Diese Definition liefert eine klare geometrische Charakterisierung der Gitter. Es ist klar, dass beispielsweise $\mathbb{Z}[i]$ ein Gitter ist. Jeder Untervektorraum enthält generell eine Vielzahl von Gittern. Man erhält diese, wenn man eine Basis wählt und nur Linearkombinationen mit ganzzahligen Koeffizienten betrachtet. Diese erste Definition bezieht sich also noch auf die Wahl linear unabhängiger Vektoren. Wir erstreben nun eine äquivalente Definition, die frei von einer solchen Wahl ist. Dazu bemerken wir zunächst, dass ein Gitter eine endlich erzeugte Untergruppe von V ist. Mit der endlich erzeugten Untergruppe $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$ ist aber auch schnell ein Beispiel gefunden, welches zeigt, dass diese Eigenschaft die Gitter noch nicht eindeutig charakterisieren kann. Die Hinzunahme einer weiteren Eigenschaft stellt sich jedoch als ausreichend heraus.

Satz 3. *Eine Untergruppe $\Gamma \subseteq V$ ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis. Es ist klar, dass ein Gitter eine diskrete Untergruppe ist. Sei also nun Γ eine diskrete Untergruppe von V und $V_0 := \langle \Gamma \rangle$ der von Γ erzeugte Unterraum. Dann können wir eine Basis von V_0 aus Vektoren $u_1, \dots, u_m \in \Gamma$ bilden und das vollständige Gitter

$$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subseteq \Gamma$$

von V_0 betrachten. Falls der Index $q := [\Gamma : \Gamma_0]$ endlich ist, so ist $q\Gamma \subseteq \Gamma_0$ und

$$\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}\left(\frac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\frac{1}{q}u_m\right).$$

Aus dem Hauptsatz über endlich erzeugte abelsche Gruppen folgt nun unmittelbar, dass Vektoren $v_1, \dots, v_r$ mit $r \leqslant m$ existieren, so dass $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r$. Da $v_1, \dots, v_r$ den m-dimensionalen Vektorraum V_0 aufspannen, sind diese linear unabhängig und es folgt, dass Γ ein Gitter ist.

Es verbleibt $q < \infty$ zu zeigen. Hierzu wählen wir einen Repräsentanten $\gamma_i \in \Gamma$ zu jeder Nebenklasse in Γ/Γ_0. Da Γ_0 vollständig in V_0 ist, überdecken die Verschiebungen der Grundmasche Φ_0

den ganzen Raum V_0. Für jedes γ_i finden wir also ein $\mu_i \in \Phi_0$ und $\gamma_{0i} \in \Gamma_0$, so dass $\gamma_i = \mu_i + \gamma_{0i}$. Die $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ bilden eine diskrete Teilmenge der Gruppe Γ und liegen in der beschränkten Menge Φ_0, womit ihre Anzahl endlich sein muss. Damit ist auch die Anzahl der Nebenklassen begrenzt. □

Bemerkung 4. Nebenbei haben wir auch gezeigt, dass die 0 ein Häufungspunkt von $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ ist. Dies folgt auch aus dem Dirichlet Lemma, welches bei der Pell Gleichung besprochen wurde.

Uns geht es nun darum, den Minkowskischen Gitterpunktsatz zu beweisen. Dieser wird für unsere Anwendungen in der Zahlentheorie von grosser Bedeutung sein. Dafür setzen wir von hier an vorraus, dass V ein euklidischer Vektorraum ist. Insbesondere soll $\dim(V) := n < \infty$ sein und es soll ein Skalarprodukt auf V geben. So können wir auf V einen Volumenbegriff wie folgt definieren: Ist Q ein Würfel, der von einer Orthonormalbasis $e_1, \dots, e_n$ aufgespannt wird, so setzen wir $\mathrm{vol}(Q) := 1$. Für n linear unabhängige Vektoren $v_1, \dots, v_n$ erhält das Parallelpiped

$$\Phi = \left\{ \sum_{i=1}^{n} x_i v_i \mid x_i \in \mathbb{R} \cap [0,1) \right\}$$

im Anschluss das Volumen $\mathrm{vol}(\Phi) := |\det(A)|$, wobei A die Übergangsmatrix von der Basis $e_1, \dots, e_n$ zu $v_1, \dots, v_n$ ist. Φ ist auch als Grundmasche des Gitters Γ zur Basis $v_1, \dots, v_n$ anzusehen und wir definieren

$$\mathrm{vol}(\Gamma) := \mathrm{vol}(\Phi).$$

Bemerkung 5. Das Gittervolumen ist basisunabhängig, da die Basiswechselmatrix zwischen zwei Gitterbasen ganzzahlige Koeffizenten hat und invertierbar ist. Somit hat sie Determinante ± 1 und lässt das Volumen unverändert.

Wir errinern letzlich noch an zwei Definitionen, ehe wir endlich den Gitterpunktsatz formulieren können. Eine Teilmenge $X \subseteq V$ heisst *zentralsymmetrisch*, falls für alle $x \in X$ auch $-x \in X$ ist und sie heisst *konvex*, wenn sie für alle Punkte $x, y \in X$ auch die Strecke $\{ty + (1-t)x \mid 0 \leqslant t \leqslant 1\}$ enthält.

Satz 6. *Sei Γ ein vollständiges Gitter in V und X eine zentralsymmetrische und konvexe Teilmenge von V. Falls*

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma),$$

so enthält X mindestens einen von Null verschiedenen Gitterpunkt.

Beweis. Es ist ausreichend zu zeigen, dass zwei verschiedene Gitterpunkte $\gamma_1, \gamma_2 \in \Gamma$ existieren, so dass

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \varnothing.$$

Dann lässt sich nämlich ein Punkt aus diesem Durchschnitt wählen

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2, \quad x_1, x_2 \in X,$$

so dass der Gitterpunkt

$$\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$$

nun gleichzeitig der Mittelpunkt der Strecke von x_2 nach $-x_1$ und somit in $X \cap \Gamma$ ist.

Wären nun die Mengen $\frac{1}{2}X + \gamma, \gamma \in \Gamma$ paarweise disjunkt, so wären auch die Durchschnitte mit einer Grundmasche $\Phi \cap \left(\frac{1}{2}X + \gamma\right)$ disjunkt und es wäre

$$\mathrm{vol}(\Phi) \geqslant \sum_{\gamma \in \Gamma} \mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right).$$

Durch Translation mit $-\gamma$ erhalten wir aus $\Phi \cap \left(\frac{1}{2}X + \gamma\right)$ die Menge $(\Phi - \gamma) \cap \frac{1}{2}X$ von gleichem Volumen. Da die $\Phi - \gamma, \gamma \in \Gamma$ den ganzen Raum V, und insbesondere auch $\frac{1}{2}X$ überdecken, würden

wir im Gegensatz zur Vorraussetzung

$$\mathrm{vol}(\Phi) \geqslant \sum_{\gamma\in\Gamma} \mathrm{vol}\left((\Phi-\gamma)\cap\frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{vol}(X)$$

erhalten. □

2. Geometrie der Zahlen

Um den Bezug zur Zahlentheorie herzustellen, wollen wir in diesem Abschnitt einem algebraischem Zahlkörper ein Gitter in einem geeigneten euklidischem Raum zuweisen. Wir betrachten also einen algebraischen Zahlkörper K vom Grad n und setzen $T := \mathrm{Hom}(K,\mathbb{C})$ für die Menge der **Einbettungen** von K in $\mathbb{C}$. Ferner definieren wir noch die Abbildung

$$j : K \to K_{\mathbb{C}} := \prod_{\tau\in T}\mathbb{C}, \quad a \mapsto (\tau a)_{\tau\in T}.$$

Es gibt insgesammt n Einbettungen, wovon r bereits reell sind $\rho_1,\dots,\rho_r : K \to \mathbb{R}$. Die anderen nicht-reelen gruppieren sich zu s Paaren $\sigma_1,\overline{\sigma}_1,\dots,\sigma_s,\overline{\sigma}_s : K \to \mathbb{C}$, so dass $n = r+2s$.

Die komplexe Konjugation lässt sich nicht nur auf die Koordinaten von $\prod_{\tau\in T}\mathbb{C}$ anwenden, sondern liefert für jedes τ auch eine konjugierte Abbildung durch $\overline{\tau}z = \overline{\tau z}$. Zusammengenommen ergibt sich die Involution

$$F : K_{\mathbb{C}} \to K_{\mathbb{C}}, \quad z = (z_\tau)_{\tau\in T} \mapsto (\overline{z}_{\overline{\tau}})_{\tau\in T}.$$

Bemerkung 7. Für das Skalarprodukt auf $K_{\mathbb{C}}$ gilt $\langle Fx, Fy\rangle = \overline{\langle x,y\rangle}$.

Die unter F invarianten Punkte von $K_{\mathbb{C}}$ bezeichnen wir mit $K_{\mathbb{R}}$. Dies sind genau die Punkte (z_τ) mit $z_\tau = \overline{z}_{\overline{\tau}}$ beziehungsweise $\overline{z}_\tau = z_{\overline{\tau}}$. Aus $\overline{\tau}a = \overline{\tau a}$ mit $a \in K$ folgt somit $F(ja) = ja$ und wir können j als eine Abbildung $j : K \to K_{\mathbb{R}}$ ansehen. Zudem ergibt die Einschränkung des Standardskalarprodukts von $K_{\mathbb{C}}$ auf den $\mathbb{R}$-Vektorraum $K_{\mathbb{R}}$ ein reelles Skalarprodukt. Denn für $x,y \in K_{\mathbb{R}}$ ist $\langle x,y\rangle \in \mathbb{R}$, was aus Bemerkung 7 folgt, ausserdem folgen $\langle x,y\rangle = \overline{\langle x,y\rangle} = \langle y,x\rangle$ und $\langle x,x\rangle > 0$ aus den Eigenschaften des komplexen Skalarprodukts.

Eine konkrete Beschreibung von $K_{\mathbb{R}}$ liefert nun der folgende

Satz 8. *Wir erhalten einen Isomorphismus*

$$f : K_{\mathbb{R}} \to \prod_{\tau\in T}\mathbb{R} = \mathbb{R}^{r+2s}$$

durch die Zuordnung $(z_\tau) \mapsto (x_\tau)$ *mit*

$$x_\rho = z_\rho, \quad x_\sigma = \mathrm{Re}(z_\sigma), \quad x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma).$$

Das eingeschränkte Standardskalarprodukt wird hierdurch in das folgende Skalarprodukt überführt

$$(x,y) = \sum_{\tau\in T}\alpha_\tau x_\tau y_\tau,$$

wobei α_τ *gleich* 1 *ist, falls* τ *reell und gleich* 2 *ist, falls* τ *komplex ist.*

Beweis. Aus der vorangegangenen Diskussion ergibt sich die explizite Beschreibung von

$$K_{\mathbb{R}} = \{(z_\tau)_{\tau\in T} \in \prod_{\tau\in T}\mathbb{C} \mid z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z}_\sigma\},$$

woraus unmittelbar die gewünschte Isomorphie folgt. Seien nun $z = (z_\tau)_{\tau\in T} = (x_\tau + iy_\tau), z' = (z'_\tau)_{\tau\in T} = (x'_\tau + iy'_\tau) \in K_{\mathbb{R}}$. Dann ist $z_\rho\overline{z}'_\rho = x_\rho x'_\rho$ und

$$z_\sigma\overline{z}'_\sigma + z_{\overline{\sigma}}\overline{z}'_{\overline{\sigma}} = z_\sigma\overline{z}'_\sigma + \overline{z}_\sigma z'_\sigma = 2\mathrm{Re}(z_\sigma\overline{z}'_\sigma) = 2(x_\sigma x'_\sigma + x_{\overline{\sigma}}x'_{\overline{\sigma}}).$$

Die Anwendung des Isomorphismus' liefert die Behauptung über Skalarprodukte. □

Bemerkung 9. Das kanonische Volumen wird durch das Skalarprodukt von $K_{\mathbb{R}}$ auf $\mathbb{R}^{r+2s}$ übertragen. Mit dem üblichen Lebesgue-Mass steht es in folgendem Zusammenhang

$$\mathrm{vol}_{\mathrm{kanonisch}}(X) = 2^s\mathrm{vol}_{\mathrm{Lebesgue}}(f(X)).$$

Wir können nun die Verbindung zu den Idealen schlagen.

Satz 10. *Ist $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}_K$, so ist $\Gamma = j\mathfrak{a}$ ein vollständiges Gitter in $K_\mathbb{R}$ mit dem Grundmaschenvolumen*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}]$$

Da der Satz auf weiteren nicht behandelten Resultaten aufbaut, geben wir hierzu keinen Beweis an. Dieser findet sich aber in [1, 1.5]. Zusammen mit dem Minkowskischen Gitterpunktsatz ergibt sich nun dennoch das folgende wichtige Resultat.

Theorem 11. *Sei $\mathfrak{a} \neq 0$ ein ganzes Ideal von K, und seien $c_\tau > 0$ für alle $\tau \in T$ reelle Zahlen mit $c_\tau = c_{\overline{\tau}}$ und*

$$\prod_{\tau \in T} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}].$$

Dann existiert ein $a \in \mathfrak{a}, a \neq 0$ mit

$$|\tau a| < c_\tau$$

für alle $\tau \in T$.

Beweis. Die Menge $X = \{(z_\tau)_{\tau \in T} \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Ihr kanonisches Volumen ist das 2^s-fache des Inhalts von

$$f(X) = \{(x_\tau)_{\tau \in T} \in \prod_{\tau \in T} \mathbb{R} \mid |x_\rho| < c_\rho, x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2\}.$$

Also

$$\mathrm{vol}(X) = 2^s \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s}\pi^s \prod_{\tau \in T} c_\tau.$$

Nach Vorraussetzung und mit dem vorrangegangenem Satz erhalten wir

$$\mathrm{vol}(X) > 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}] = 2^n \mathrm{vol}(\Gamma).$$

Es sind somit die Vorraussetzungen des Minkowskischen Gitterpunktsatz' erfüllt. X enthält also mindestens einen Gitterpunkt ja mit $a \neq 0, a \in \mathfrak{a}$. Die Aussage folgt nun aus der Definition von X. □

3. Endlichkeit der Klassenzahl

Wir sind nun in der Lage zu zeigen, dass die Idealklassengruppe $Cl_K = J_K/P_K$ für algebraische Zahlkörper K endlich ist. Wir nennen diese Ordnung im übrigen die **Klassenzahl** $h_K := [J_K : P_K]$. Auch $[\mathcal{O}_K : \mathfrak{a}]$ ist für Ideale $\mathfrak{a} \neq 0$ endlich und somit können wir die **Absolutnorm** von $\mathfrak{a}$

$$\mathfrak{N}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$$

definieren.

Bemerkung 12. Ein Hauptideal (α) von $\mathcal{O}_K$ hat Absolutnorm $\mathfrak{N}((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$. Hiervon leitet sich auch der Name der Absolutnorm ab.

Es ergibt sich der folgende

Satz 13. *Ist $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ die Primzerlegung des Ideals $\mathfrak{a} \neq 0$, so gilt*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}$$

Beweis. Nach dem chinesischen Restsatz ist

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}.$$

Es reicht also aus, Primidealpotenzen $\mathfrak{p}^\nu$ zu betrachten. In

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$$

ist $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ wegen der Eindeutigkeit der Primzerlegung und jeder Quotient $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist ein $\mathcal{O}_K/\mathfrak{p}$ Vektorraum der Dimension 1. Es ist also $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K\ \mathfrak{p}$ und somit

$$\mathfrak{N}(\mathfrak{p}^\nu) = [\mathcal{O}_K : \mathfrak{p}^\nu] = [\mathcal{O}_K : \mathfrak{p}] \cdot [\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu] = \mathfrak{N}(\mathfrak{p})^\nu$$

□

Wir erhalten dadruch die Multiplikativität der Absolutnorm

$$\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}).$$

Diese lässt sich daher zu einem Homomorphismus auf allen gebrochenen Idealen $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$ fortsetzen

$$\mathfrak{N} : J_K \to \mathbb{R}_{>0}$$

Um die Endlichkeit der Klassenzahl zu beweisen, benötigen wir letztlich noch das folgende Lemma. Im Anschluss gehen wir direkt zum Beweis über die Klassenzahl über.

Lemma 14. *In jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}_K$ gibt es ein $a \in \mathfrak{a}, a \neq 0$ mit*

$$|N_{K|\mathbb{Q}}(a)| \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

Beweis. Für $\varepsilon > 0$ wählen wir reelle Zahlen $c_\tau > 0$ für alle $\tau \in T$, so dass $c_\tau = c_{\overline{\tau}}$ und

$$\prod_{\tau \in T} c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Aus Theorem 11 ergibt sich die Existenz eines Elements $a \in \mathfrak{a}, a \neq 0$ mit $|\tau a| < c_\tau$, also

$$|N_{K|\mathbb{Q}}(a)| = \prod_{\tau \in T} |\tau a| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Die linke Seite ist stets eine natürliche Zahl, woraus sich nun auch die Existenz eines $a \in \mathfrak{a}, a \neq 0$ mit

$$|N_{K|\mathbb{Q}}(a)| \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a})$$

ergibt. □

Theorem 15. *Die Klassenzahl eines algebraischen Zahlkörpers ist endlich.*

Beweis. Sei $\mathfrak{p} \neq 0$ ein Primideal von $\mathcal{O}_K$ und $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, so ist $\mathcal{O}_K/\mathfrak{p}$ eine endliche Erweiterung von $\mathbb{Z}/p\mathbb{Z}$ von Grad $f \geqslant 1$ und es ist

$$\mathfrak{N}(\mathfrak{p}) = p^f.$$

Für ein ausgewähltes p gibt es nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ wegen $\mathfrak{p}|(p)$. Daher gibt es nur endlich viele Primideale $\mathfrak{p}$ mit Absolutnorm kleiner einer gegebenen Schranke. Da jedes ganze Ideal $\mathfrak{a}$ eindeutig in Primideale zerlegt werden kann und die Absolutnorm multiplikativ ist, gibt es überhaupt nur endlich viele Ideale $\mathfrak{a}$ mit beschränkter Absolutnorm $\mathfrak{N}(\mathfrak{a}) \leqslant M$.

Es reicht daher aus, für jede Klasse $[a] \in Cl_K$ ein ganzes Ideal $\mathfrak{a}_1$ mit

$$\mathfrak{N}(\mathfrak{a}_1) \leqslant M := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

zu finden. Sei dazu $\mathfrak{a} \in [a]$ beliebig und $\gamma \in \mathcal{O}_K, \gamma \neq 0$ mit $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Mit Lemma 14 erhalten wir ein $\alpha \in \mathfrak{b}, \alpha \neq 0$ mit

$$|N_{K|\mathbb{Q}}(\alpha)| \cdot \mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}((\alpha)\mathfrak{b}^{-1}) = \mathfrak{N}(\alpha\mathfrak{b}^{-1}) \leqslant M.$$

Demnach hat das Ideal $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [a]$ die gewünschte Eigenschaft. □

4. Der Dirichletsche Einheitensatz

Zuletzt stellen wir noch eine weitere Anwendung der Gitter vor - den Dirichletschen Einheitensatz. Dieser erlaubt es, die Gruppe $\mathcal{O}_K^\times$ näher zu bestimmen. Wir werden seinen Beweis allerdings nur skizzenhaft besprechen können. Eine vollständige Behandlung findet sich in [1, 1.7].

Theorem 16. *Die Einheitengruppe $\mathcal{O}_K^\times$ von $\mathcal{O}_K$ ist das direkte Produkt der endlichen zyklischen Untergruppe der Einheitswurzeln $\mu(K)$ von K und einer freien abelschen Gruppe vom Rang $r+s-1$.*

Es gibt also **Grundeinheiten** $\varepsilon_1, \ldots, \varepsilon_t, t = r + s - 1$, so dass sich jede weitere Einheit ε als ein Produkt

$$\varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$$

mit einer Einheitswurzel ζ schreiben lässt. Wir werden im folgenden den Beweis der Aussage skizzieren.

Beweis. Wir nummerieren die Einbettungen, wobei wir diesmal aus jedem Paar komplexer Einbettungen genau eine auswählen $\tau_1, \ldots, \tau_{r+s} : K \to \mathbb{C}$. Zum Beweis studiert man die Abbildung

$$\lambda : \mathcal{O}^\times \to \mathbb{R}^{r+s}, \quad \varepsilon \mapsto (\log |\tau_j \varepsilon|^{\alpha_j})_{1 \leqslant j \leqslant r+s},$$

wobei α_j wieder gleich 1 oder 2 ist, je nachdem, ob τ_j reell oder komplex ist.

Nun zeigt man, dass für den Gruppenhomomorphismus λ gilt $\mathrm{Kern}(\lambda) = \mu(K)$. Da $\zeta \in \mu_K$ endliche Ordnung hat, wird ζ durch jede Einbettung auf eine Zahl vom Betrag 1 abgebildet und liegt somit im Kern von λ. Falls andererseits $\varepsilon \in \mathcal{O}_K^\times$ liegt, so ist $|\tau_j \varepsilon| = 1$ für alle Einbettungen. Der Kern von λ bildet also einen beschränkten Bereich in $K_\mathbb{R}$. Gleichzeitig ist $j\varepsilon$ ein Punkt des Gitters $j\mathcal{O}_K$. Daraus folgt, dass $\mathrm{Kern}(\lambda)$ eine endliche Untergruppe von $K^\times$ ist und daher aus lauter Einheitswurzeln besteht.

Als nächstes betrachtet man den $t = r + s - 1$-dimensionalen Unterraum $H = \{x \in \mathbb{R}^{r+s} \mid \sum_{j=1}^{r+s} x_j = 0\}$ und zeigt, dass $\Gamma = \lambda(\mathcal{O}_K^\times)$ ein vollständiges Gitter in H, also isomorph zu $\mathbb{Z}^{r+s-1}$ ist. Man wählt dann eine $\mathbb{Z}$-Basis $v_1, \ldots, v_t$ der freien abelschen Gruppe Γ. Seien $\varepsilon_1, \ldots, \varepsilon_t \in \mathcal{O}_K^\times$ Urbilder der jeweiligen v_i. Dann wird die durch die ε_i erzeugte Untergruppe A durch λ isomorph auf Γ abgebildet. Es gilt somit $\mu(K) \cap A = \{1\}$ und daher $\mathcal{O}_K^\times = \mu(K) \times A$. □

References

[1] J. Neukirch, *Algebraische Zahlentheorie.* Springer-Verlag, Berlin, 1992

Email address: pirronm@student.ethz.ch