Definition 4.5. Eine Teilmenge $X \subset V$ heißt **zentralsymmetrisch**, wenn gilt:

$$x \in X \Rightarrow -x \in X,$$

und **konvex**, falls

$$x, y \in X \Rightarrow \{\lambda x + (1-\lambda)y \mid 0 \leq \lambda \leq 1\} \subset X.$$

Theorem 4.6 (Minkowskischer Gitterpunktsatz)**.** *Sei Γ ein vollständiges Gitter in einem euklidischen Vektorraum V und sei X eine (meßbare) zentralsymmetrische, konvexe Teilmenge in V. Gilt*

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

so enthält X mindestens einen von 0 verschiedenen Gitterpunkt $\gamma \in \Gamma$.

Beweis. Es g.z.z., dass $\gamma_1, \gamma_2 \in \Gamma$, $\gamma_1 \neq \gamma_2$, mit $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \varnothing$ existieren (nutze konvex + zentralsymmetrisch). Wären diese Teilmengen alle disjunkt, so gilt nach Schneiden mit der Grundmasche Φ:

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}(\Phi \cap (\tfrac{1}{2}X + \gamma)).$$

Nun induziert Translation mit $-\gamma$:

$$\mathrm{vol}(\Phi \cap (\frac{1}{2}X + \gamma)) = \mathrm{vol}((\Phi - \gamma) \cap \frac{1}{2}X),$$

und weil die $(\Phi - \gamma) \cap \frac{1}{2}X$ die Menge $\frac{1}{2}X$ disjunkt zerlegen, folgt

$$\begin{aligned} \mathrm{vol}(\Phi) &\geq \sum_{\gamma \in \Gamma} \mathrm{vol}((\Phi - \gamma) \cap \tfrac{1}{2}X) \\ &= \mathrm{vol}(\tfrac{1}{2}X) = \tfrac{1}{2^n}\mathrm{vol}(X), \end{aligned}$$

im Widerspruch zur Annahme. □

4.2 Minkowski-Theorie

(altmodisch: „Geometrie der Zahlen“)

Sei $K|\mathbb{Q}$ ein Zahlkörper, $n = [K : \mathbb{Q}]$. Dann gilt $\#\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = n$.

Ziel: Wir machen den n-dimensionalen $\mathbb{R}$-Vektorraum $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ zu einem euklidischen Vektorraum.

Zunächst erinnern wir an die lineare Unabhängigkeit von *Charakteren*: Sei G eine Gruppe und K ein Körper. Dann bezeichnet man einen Gruppenhomorphismus $G \to K^\times$ als K-wertigen Charakter der Gruppe G.

Die Menge der Abbildungen $\mathrm{Abb}(G, K)$ wird zum K-Vektorraum durch wertweise Addition und Skalarmultiplikation, d.h.

$$(a_1\phi_1 + a_2\phi_2)(g) := a_1\phi_1(g) + a_2\phi_2(g)$$

$\phi_1, \phi_2 \in \mathrm{Abb}(G, K),\ a_1, a_2 \in K,\ g \in G$. Über die (Mengen)abbildung $K^\times \hookrightarrow K$ können K-wertige Charaktere von G als Elemente des Vektorraums $\mathrm{Abb}(G, K)$ aufgefasst werden.

Satz 4.7. *Verschiedene Charaktere $\chi_1, \dots, \chi_n$ einer Gruppe G mit Werten in einen Körper K sind linear unabhängig als Elemente im K-Vektorraum* $\mathrm{Abb}(G, K)$.

Beweis. Siehe Algebra 1, 4.53 oder Bosch: „Algebra" §4.6. Satz 2. □

Sei nun $L|K$ und $M|K$ Körpererweiterungen. Die Menge $\mathrm{Hom}_K(L, M)$ (Körperhomorphismen) ist eine Teilmenge des K-Vektorraums $\mathrm{Hom}_{K\text{-VR}}(L, M)$ (K-Vektorraumhomomorphismen). Die K-Vektorraumstruktur setzt sich zu einer M-Vektorraumstruktur fort durch

$$(\alpha\phi)(x) = \alpha\phi(x), \quad \alpha \in M,\ x \in L,\ \phi \in \mathrm{Hom}_{K\text{-VR}}(L, M).$$

Auf diese Weise wird $\mathrm{Hom}_{K\text{-VR}}(L, M)$ ein M-Untervektorraum von $\mathrm{Abb}(L, M)$. Die Menge $\mathrm{Hom}_{K\text{-VR}}(L, M)$ der K-Vektorraumhomomorphismen von L nach M ist in natürlicher Weise ein K-Vektorraum. Die K-Vektorraumstruktur setzt sich zu einer M-Vektorraumstruktur fort durch

$$(\alpha\phi)(a) = \alpha\phi(a), \quad \alpha \in M,\ a \in L,\ \phi \in \mathrm{Hom}_K(L, M).$$

Auf diese Weise wird $\mathrm{Hom}_{K\text{-VR}}(L, M)$ ein M-Untervektorraum von $\mathrm{Abb}(L, M)$.

Satz 4.8 (Algebra 2, 4.54)**.** *Es ist* $\mathrm{Hom}_K(L, M)$ *eine linear unabhängige Menge von Vektoren im M-Vektorraum* $\mathrm{Hom}_{K\text{-VR}}(L, M) \subset \mathrm{Abb}(L, M)$.

Sei nun K wieder ein Zahlkörper, die Rolle von M wird durch den Körper $\mathbb{C}$ übernommen. Wir betrachten die $\mathbb{Q}$-Bilinearform

$$K \times \mathbb{C} \to \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \mathbb{C}, \qquad (x, \alpha) \mapsto ((\tau x) \cdot \alpha)_\tau.$$

Diese induziert

$$\phi : K \otimes_{\mathbb{Q}} \mathbb{C} \longrightarrow \prod_\tau \mathbb{C}, \quad x \otimes \alpha \longmapsto (\tau x \cdot \alpha)_\tau$$

Es ist ϕ bezüglich der natürlichen $\mathbb{C}$-Vektorraum-Strukturen von Quelle und Ziel ein $\mathbb{C}$-Vektorraumhomomorphismus.

Lemma 4.9. *Es ist*

$$\phi : K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \mathbb{C} \quad \cong \mathbb{C}^n$$

ein Isomorphismus von $\mathbb{C}$-Vektorräumen.

Beweis. Es gilt

$$\dim(\prod_{\tau} \mathbb{C}) = n \quad \text{und} \quad \dim_{\mathbb{C}}(K \otimes_{\mathbb{Q}} \mathbb{C}) = \dim_{\mathbb{Q}} K = n.$$

Daher genügt es zu zeigen, dass ϕ injektiv ist. Sei $x_1, \dots, x_n$ eine $\mathbb{Q}$-Basis von K. Nach Satz 4.8 sind die n Vektoren $(\tau x_1, \dots, \tau x_n)_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})}$ linear unabhängig im $\mathbb{C}^n$ (sonst gäbe es eine lineare Abhängigkeit der τ in $\mathrm{Hom}_{\mathbb{Q}\text{-VR}}(K, \mathbb{C})$). Also hat die Matrix

$$(\tau x_i)_{\substack{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}) \\ i=1,\dots,n}} \in M_{n,n}(\mathbb{C})$$

eine Determinante $\neq 0$, weshalb auch die Vektoren $(\tau x_i)_\tau$, $i = 1, \dots, n$, linear unabhängig im $\mathbb{C}^n$ sind. Nun ist $(x_1 \otimes 1, \dots, x_n \otimes 1)$ eine $\mathbb{C}$-Basis von $K_{\mathbb{C}}$ und da die Vektoren

$$\phi(x_i \otimes 1) = (\tau x_i)_\tau, \quad i = 1, \dots, n,$$

linear unabhängig sind, ist ϕ injektiv. □

Nun betrachten wir die komplexe Konjugation

$$F : \mathbb{C} \longrightarrow \mathbb{C},\ z \longmapsto \bar{z}, \quad \mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \langle F \rangle.$$

F induziert durch Wirkung auf der zweiten Komponente einen Automorphismus von $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$

$$F : K_{\mathbb{C}} \longrightarrow K_{\mathbb{C}}.$$

Lemma 4.10. *Bezüglich des natürlichen Isomorphismus $\phi : K_{\mathbb{C}} \cong \prod_{\tau} \mathbb{C}$ aus Lemma 4.9, ist $F \in \mathrm{Aut}(\prod_{\tau} \mathbb{C})$ gegeben durch*

$$F(z)_\tau = \bar{z}_{\bar{\tau}},$$

wobei $\overline{\tau} = F \circ \tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

Beweis. Klar nach Definition des natürlichen Isomorphismus ϕ. □

Lemma 4.11. *Die natürliche Inklusion $\mathbb{R} \hookrightarrow \mathbb{C}$ definiert eine natürliche Inklusion*

$$K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C},$$

deren Bild $K_{\mathbb{C}}^+ \subset K_{\mathbb{C}}$ genau aus den F-invarianten Elementen besteht.

Beweis. Wir betrachten den (üblichen) Isomorphismus

$$\mathbb{C} \cong \mathbb{R} \oplus \mathbb{R},\ z \longmapsto (\mathrm{Re}(z), \mathrm{Im}(z)).$$

Dies ist ein Isomorphismus von $\mathbb{R}$- und insbesondere von $\mathbb{Q}$-Vektorräumen. Daher gilt ($\otimes$ vertauscht mit $\oplus$)

$$\begin{aligned} &K \otimes_{\mathbb{Q}} \mathbb{C} \cong K \otimes_{\mathbb{Q}} \mathbb{R} \oplus K \otimes_{\mathbb{Q}} \mathbb{R} \\ &x \otimes z \longmapsto (x \otimes \mathrm{Re}(z),\ x \otimes \mathrm{Im}(z)). \end{aligned}$$

Auf der rechten Seite operiert F so:

- trivial auf der 1. Komponente.
- Multiplikation mit -1 auf der 2. Komponente.

$\Rightarrow$ die erste Komponente $= \mathrm{im}(K_{\mathbb{R}} \to K_{\mathbb{C}})$ besteht genau aus den F-invarianten Elementen. □

Wir erhalten hieraus das

Korollar 4.12. *Bezüglich der natürlichen Identifikation ϕ aus Lemma 4.9 und der Inklusion aus Lemma 4.11 gilt*

$$\begin{aligned} K_{\mathbb{R}} &\cong [\prod_{\tau} \mathbb{C}]^+ \\ &= \{z \in \prod_{\tau} \mathbb{C} \mid z_{\bar{\tau}} = \bar{z}_{\tau} \quad \forall\, \tau\}. \end{aligned}$$

Auf $K_{\mathbb{C}} \cong \prod_{\tau} \mathbb{C}$ haben wir das Standard-Hermitesche Skalarprodukt

$$\langle x, y\rangle = \sum_{\tau} x_{\tau}\bar{y}_{\tau}.$$

Lemma 4.13. *Dieses Skalarprodukt ist F-äquivariant, d.h. es gilt*

$$\langle Fx, Fy\rangle = F\langle x, y\rangle.$$

Beweis. Klar nach Einsetzen aller Definitionen. □

Nach Einschränkung auf $[\prod_{\tau} \mathbb{C}]^+ = K_{\mathbb{R}}$ erhalten wir daher eine symmetrische, positiv definite Bilinearform auf $K_{\mathbb{R}}$, d.h. $K_{\mathbb{R}}$ wird zum euklidischen Vektorraum.

Definition 4.14. Der so definierte euklidische Vektorraum $K_{\mathbb{R}} = [\prod_{\tau} \mathbb{C}]^+$ heißt **Minkowski-Raum** und sein Skalarprodukt die **kanonische Metrik**. Das assoziierte Maß heißt das **kanonische Maß** auf $K_{\mathbb{R}}$.

Auf $K_{\mathbb{C}}$ haben wir die natürliche („Spur")Abbildung

$$\mathrm{Sp} : \prod_{\tau} \mathbb{C} \longrightarrow \mathbb{C}, \quad z \longmapsto \sum_{\tau} z_{\tau}.$$

Sei $j : K \to K_{\mathbb{C}}$, $x \mapsto x \otimes 1 = (\tau x)_{\tau}$ die natürliche Inklusion. Nach Satz 3.17 gilt

$$\mathrm{Sp} \circ j(x) = \mathrm{Sp}_{K|\mathbb{Q}}(x).$$

Man rechnet leicht nach: $F \circ \mathrm{Sp} = \mathrm{Sp} \circ F$. Daher erhalten wir die Abbildung

$$\mathrm{Sp} : K_{\mathbb{R}} \to \mathbb{R}$$

und für die natürliche Inklusion $j : K \to K_{\mathbb{R}}$ gilt $\mathrm{Sp} \circ j(x) = \mathrm{Sp}_{K|\mathbb{Q}}(x)$ für $x \in K$.

Wir suchen nun eine Identifikation

$$K_{\mathbb{R}} \cong \mathbb{R}^n, \quad n = [K : \mathbb{Q}].$$

(jede $\mathbb{Q}$-Basis von K gibt uns eine solche, aber die wollen wir nicht). Wir unterteilen die Menge $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ in zwei Teilmengen. Die erste besteht aus

$$\rho_1, \ldots, \rho_{r_1} : K \longrightarrow \mathbb{R}$$

(alle die in $\mathbb{R}$ landen). Die anderen tauchen im Paaren auf:

$$\sigma_1, \bar{\sigma}_1, \ldots, \sigma_{r_2}, \bar{\sigma}_{r_2} : K \longrightarrow \mathbb{C}.$$

Wir haben also $r_1 + 2r_2 = n = [K : \mathbb{Q}]$. Der Buchstabe ρ bezeichne jetzt immer reelle Einbettungen. Aus jedem Paar konjugiert komplexer Einbettungen wählen wir uns willkürlich eine und bezeichnen diese stets mit σ. Wir erhalten (trivialerweise)

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

Satz 4.15. *Die Abbildung*

$$f : K_{\mathbb{R}} \longrightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^n,$$

die durch

$$(z)_{\tau} \in [\prod_{\tau} \mathbb{C}]^{+} \longmapsto (x)_{\tau} \in \prod_{\tau} \mathbb{R}$$

mit $x_{\rho} = z_{\rho}$, $x_{\sigma} = Re(z_{\sigma})$, $x_{\bar{\sigma}} = Im(z_{\sigma})$ gegeben ist, ist ein Isomorphismus. Es transformiert f die kanonische Metrik auf $K_{\mathbb{R}}$ in das Skalarprodukt

$$\langle x, y \rangle = \sum_{\tau} \varepsilon_{\tau} x_{\tau} y_{\tau},$$

wobei

$$\varepsilon_{\tau} = \begin{cases} 1 & \text{wenn } \tau \text{ reell} \\ 2 & \text{wenn } \tau \text{ komplex.} \end{cases}$$

Beweis. Offenbar ist f injektiv und daher ein Isomorphismus. Ist nun $(z)_\tau = (x)_\tau + i(y)_\tau \in [\prod_\tau \mathbb{C}]^+$, und $(z')_\tau = (x')_\tau + i(y')_\tau$, so gilt $z_\rho z'_\rho = x_\rho x'_\rho$ und wegen

$$y_\sigma = \mathrm{Im}(z_\sigma),\ y_{\bar\sigma} = \mathrm{Im}(z_{\bar\sigma}) = -\mathrm{Im}(z_\sigma) = -y_\sigma, \quad x_{\bar\sigma} = x_\sigma$$

erhält man

$$\begin{aligned} z_\sigma \bar z'_\sigma + z_{\bar\sigma} \bar z'_{\bar\sigma} &= (x_\sigma + iy_\sigma)(x'_\sigma - iy_\sigma) + (x_\sigma - iy_\sigma)(x'_\sigma + iy'_\sigma) \\ &= 2(x_\sigma x'_\sigma + y_\sigma y'_\sigma). \end{aligned}$$

□

Wir identifizieren nun $K_\mathbb{R}$ über f mit dem $\mathbb{R}^n$. Das kanonische Maß einer Teilmenge $X \subset K_\mathbb{R} \cong \mathbb{R}^n$ hängt mit dem Standard-Lebesgue-Maß durch die Regel

$$\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_2}\mathrm{vol}_{\mathrm{Lebesgue}}(f(X))$$

zusammen.

Satz 4.16. *Sei $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal. Das Bild $\Gamma = j(\mathfrak{a})$ unter der natürlichen Abbildung $j : K \to K_\mathbb{R}$ ist ein vollständiges Gitter in $K_\mathbb{R}$. Die Grundmasche hat den Inhalt*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

Beweis. Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ so dass $\Gamma = \mathbb{Z}j\alpha_1 + \cdots + \mathbb{Z}j\alpha_n$. Wir numerieren die Einbettungen $\tau : K \to \mathbb{C}$, $\tau_1, \ldots, \tau_n$, und bilden die Matrix $A = (\tau_k\alpha_\ell)$. Dann gilt nach Satz 3.73

$$\det(A)^2 = d(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})^2 \cdot d_K.$$

Außerdem gilt

$$\begin{aligned} (\langle j\alpha_k, j\alpha_\ell\rangle)_{k,\ell} &= (\sum_{i=1}^n \tau_i\alpha_k\bar\tau_i\alpha_\ell)_{k,\ell} \\ &= A \cdot \bar A^t. \end{aligned}$$

So erhält man

$$\mathrm{vol}(\Gamma) = |\det(\langle j\alpha_k, j\alpha_\ell\rangle)_{k,\ell}|^{1/2} = |\det A| = \sqrt{|d_K|} \cdot \mathfrak{N}(\mathfrak{a}).$$

Insbesondere gilt $\det A \neq 0$, weshalb $j\alpha_1, \ldots, j\alpha_n$ linear unabhängig, also Γ ein vollständiges Gitter ist. □

Theorem 4.17. *Sei $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal und seien $c_\tau > 0$, $\tau \in \mathrm{Hom}(K, \mathbb{C})$, reelle Zahlen mit $c_\tau = c_{\bar\tau}$ und*

$$\prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^{r_2} \cdot \mathfrak{N}(\mathfrak{a})\sqrt{|d_K|}.$$

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

$$|\tau a| < c_\tau \text{ für alle } \tau \in \mathrm{Hom}(K, \mathbb{C}).$$

Beweis. Die Menge $X := \{(z_\tau) \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Mit Hilfe der Abbildung $f : K_\mathbb{R} \xrightarrow{\sim} \prod_\tau \mathbb{R}$ aus Satz 4.15 ergibt sich

$$\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_2}\mathrm{vol}_{\mathrm{Lebesgue}}(f(X)).$$

Nun ist

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

(= Produkt von r_1 Intervallen und r_2 Kreisschreiben). Also gilt

$$\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_2}\prod_\rho(2c_\rho)\cdot\prod_\sigma(\pi c_\sigma^2) = 2^{r_1+r_2}\pi^{r_2}\prod_\tau c_\tau.$$

Der Grundmascheninhalt von $\Gamma = j\mathfrak{a}$ ist $\sqrt{|d_K|}\cdot\mathfrak{N}(\mathfrak{a})$. Also gilt

$$\begin{aligned}\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_1+r_2}\pi^{r_2}\prod_\tau c_\tau &> 2^{r_1+2r_2}\cdot\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|}\\ &= 2^n\mathrm{vol}(\Gamma).\end{aligned}$$

Nach dem Minkowskischen Gitterpunktsatz enthält X ein $\gamma \in \Gamma$, $\gamma \neq 0$. Nun ist per definitionem $\gamma = ja$ für ein $a \in \mathfrak{a}$, und dieses a ist das Gesuchte. □

4.3 Die Endlichkeit der Klassenzahl

Sei $K|\mathbb{Q}$ ein Zahlkörper. Wir setzen $J_K = J(\mathcal{O}_K)$, $P_K = P(\mathcal{O}_K)$, $Cl_K = J_K/P_K$. Wir nennen Cl_K die **Idealklassengruppe von K**. Unser Ziel ist der Beweis des folgenden Theorems.

Theorem 4.18. *Cl_K ist endlich.*

Definition 4.19. $h_K = \#Cl_K$ heißt die **Klassenzahl** von K.

Lemma 4.20. *In jedem Ideal $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ gibt es ein $0 \neq a \in \mathfrak{a}$ mit*

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

Beweis. Zu vorgegebenem $\varepsilon > 0$ wählen wir $c_\tau > 0$, $\tau \in \mathrm{Hom}(K,\mathbb{C})$, mit $c_\tau = c_{\bar\tau}$ und

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) + \varepsilon$$

und finden nach Theorem 4.17 ein $0 \neq a \in \mathfrak{a}$ mit $|\tau a| < c_\tau$ für alle τ, also

$$|N_{K|\mathbb{Q}}(a)| = \prod_\tau |\tau a| < \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Nun gilt $N_{K|\mathbb{Q}}(a) \in \mathbb{Z}$. Ist $\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) \notin \mathbb{Z}$, so erhält man (wähle $\varepsilon > 0$ hinreichend klein) die Ungleichung (sogar mit $<$). Gilt $\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) \in \mathbb{Z}$, so wählt man $\varepsilon < 1$, um die Ungleichung zu erhalten. □

Beweis von Theorem 4.18. Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Wegen

$$\mathfrak{N}(\mathfrak{p}) = \#(\mathcal{O}/\mathfrak{p}) \cdot 1 = 0 \in \mathcal{O}_K/\mathfrak{p}$$

gilt $\mathfrak{N}(\mathfrak{p}) \in \mathfrak{p} \cap \mathbb{Z}$. Daher gilt $\mathfrak{p} \cap \mathbb{Z} \neq 0$, also $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p und $\mathfrak{p} \mid p\mathcal{O}_K$. Außerdem ist $\mathcal{O}_K/\mathfrak{p}$ ein endlicher Körper der Charakteristik p, weshalb $\mathfrak{N}(\mathfrak{p}) = p^f$ für ein $f \in \mathbb{N}$ gilt. Da nun $p\mathcal{O}_K$ nur endlich viele Primteiler hat, gilt für jedes $N \in \mathbb{N}$, dass $\#\{\mathfrak{p} \subset \mathcal{O}_K \mid N(\mathfrak{p}) \leq N\} < \infty$.
Für beliebiges $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ gilt

$$\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_n^{v_n}, \quad \mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{v_1} \cdots N(\mathfrak{p}_n)^{v_n}$$

$\Rightarrow$ für jedes $N \in \mathbb{N}$ ist

$$\#\{\mathfrak{a} \subset \mathcal{O}_K \mid \mathfrak{N}(\mathfrak{a}) \leq N\} < \infty.$$

Daher folgt das Theorem aus dem folgenden Lemma. □

Lemma 4.21. *Jede Idealklasse enthält ein ganzes Ideal $\mathfrak{a} \subset \mathcal{O}_K$ mit*

$$\mathfrak{N}(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}.$$

Beweis. Sei $\mathfrak{a}_1 \subset K$ ein beliebiger Repräsentant einer Idealklasse und $0 \neq \gamma \in \mathcal{O}_K$ mit $\mathfrak{b} = \gamma\mathfrak{a}_1^{-1} \subset \mathcal{O}_K$. Nach Lemma 4.20 gibt es ein $\alpha \in \mathfrak{b}$, $\alpha \neq 0$, mit

$$|N_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} \mathfrak{N}(\mathfrak{b})\sqrt{|d_K|}\,.$$

Das ganze Ideal $\mathfrak{a} := \alpha\gamma^{-1}\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1}$ liegt in der gleichen Idealklasse wie $\mathfrak{a}_1$ und es gilt

$$\mathfrak{N}(\mathfrak{a}) = |\,N_{K|\mathbb{Q}}(\alpha)|N(\mathfrak{b})^{-1} \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}.$$ □

Bemerkung 4.22. Mit etwas mehr Aufwand kann die Schranke verbessert werden zu

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

Beispiele 4.23. 1.) $K = \mathbb{Q}(\sqrt{-3})$. Wir haben $r_1 = 0$, $r_2 = 1$, $d_K = -3$. Jede Idealklasse enthält ein ganzes Ideal der Norm $\leq \left(\frac{2}{\pi}\right)\sqrt{3} = 1,10\ldots$
Davon gibt es nur eines, nämlich $\mathcal{O}_K$ selbst $\Rightarrow h_K = 1$, $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ ist Hauptidealring.
Bemerkung: $\mathbb{Z}[\sqrt{-3}]$ ist kein Hauptidealring!

2) $K = \mathbb{Q}(\sqrt{-5})$. $r_1 = 0$, $r_2 = 1$, $d_K = -20$. Wir wissen schon, dass $\mathcal{O}_K$ *kein* Hauptidealring ist, also $h_K \geq 2$. Jede Idealklasse enthält ein ganzes Ideal der Norm $\leq \left(\frac{2}{\pi}\right)\sqrt{20} = 2,84\ldots$

$\mathfrak{N}(\mathfrak{a}) = 1 \Longleftrightarrow \mathfrak{a} = \mathcal{O}_K$

$\mathfrak{N}(\mathfrak{a}) = 2 \Longrightarrow \mathfrak{a} \mid (2)$. Wegen $(2) = \mathfrak{p}^2$ mit $\mathfrak{p} = (2, 1+\sqrt{-5})$ und $\mathfrak{N}(\mathfrak{p}) = 2$ folgt $\mathfrak{a} = \mathfrak{p} \Rightarrow h_K \leq 2$, also $h_K = 2$.

3) Wir betrachten für eine Primzahl $p > 2$ die Fermatgleichung $X^p + Y^p = Z^p$. Über $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ (Beweis später) können wir umformen

$$X^p = Z^p - Y^p = (Z-Y)(Z-\zeta_p Y)\dots(Z-\zeta_p^{p-1}Y).$$

Ist nun (x, y, z) eine nichttriviale (also $xyz \neq 0$) ganzzahlige Lösung, so erhalten wir eine Zerlegung von x^p, die man, wenn $\mathbb{Z}[\zeta_p]$ ein Hauptidealring ist (d.h. $h_{\mathbb{Q}(\zeta_p)} = 1$) zum Widerspruch führen kann. Nun gilt

$$h_{\mathbb{Q}(\zeta_p)} = 1 \Longleftrightarrow p \in \{3, 5, 7, 11, 13, 17, 19\}.$$

Kummer hat gezeigt, dass man die Bedingung $h_{\mathbb{Q}(\zeta_p)} = 1$ zu $p \nmid h_{\mathbb{Q}(\zeta_p)}$ abschwächen kann. Eine solche Primzahl heißt *reguläre Primzahl*. Die anderen Primzahlen heißen *irregulär*. Die irregulären Primzahlen < 100 sind $37, 59$ und 67.

Wie prüft man nun nach, ob p regulär ist?

Definition. Die rationale Zahl B_n in der Potenzreihenentwicklung

$$\frac{X}{e^X - 1} = \sum_{n=0}^{\infty} B_n \cdot \frac{X^n}{n!}$$

heißen **Bernoulli-Zahlen**.

Es gilt $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$ und allgemeiner $B_{2n+1} = 0$ für $n \geq 1$. Die nächsten geraden Werte sind: $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$. Nun gilt der

Satz (von Staudt-Clausen). *Für gerades positives n gilt*

$$B_n + \sum_{(p-1)\mid n} \frac{1}{p} \in \mathbb{Z}.$$

Insbesondere ist der Nenner von B_n (in gekürzter Schreibweise) genau durch die Primzahlen p mit $(p-1) \mid n$ teilbar.

Wir sehen:

- 2 und 3 teilen den Nenner stets.
- n gerade $n < p - 1 \Rightarrow$ der Nenner von B_n ist prim zu p.