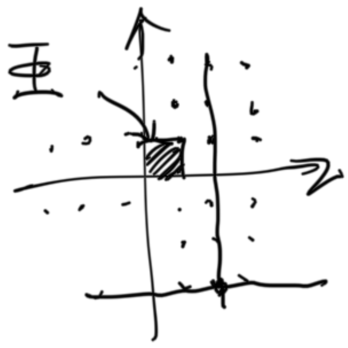
Geometrie der Zahlen

1) $h_K := |Cl_K| = |J_K / P_K|$

2) $\mathcal{O}_K^*$ näher bestimmen

$\mathbb{Z}[i] \subseteq \mathbb{C}$



1. Gitter

Def Sei V ein n-dim. VR und seien $v_1, \dots, v_m$. Dann nennen

$$\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$$

ein Gitter in V zur $(v_1, \dots, v_m)$.
Die Menge

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

Γ heisst vollständig falls $m = n$.

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

Bsp • $\mathbb{Z}[i] \subseteq \mathbb{C}$

- $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ ist kein Gitter $\subseteq \mathbb{R}$

<u>Satz</u> Eine UG $\Gamma \subseteq V$ ist ein Gitter genau dann, wenn sie diskret ist.

<u>Beweis</u> Sei also Γ eine diskrete UG von V und $V_0 := \langle \Gamma \rangle$. Dann wählen wir eine Basis $u_1, \dots, u_m \in \Gamma$ von V_0 und setzen

$$\Gamma_0 := \mathbb{Z}u_1 + \dots + \mathbb{Z}u_m \subseteq \Gamma.$$

Sei $q = [\Gamma : \Gamma_0] < \infty \Rightarrow q\Gamma \subseteq \Gamma_0$ bzw

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

Aus dem HAG folgt, dass $v_1, \dots, v_r$, $r \leq m$ existieren, so dass

$$\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_r$$

ein Gitter ist.

$\blacksquare$

Sei V ein eukl. VR. Wir definieren ein Volumen wie folgt:

1) Sei $B = (e_1, \dots, e_n)$ eine ONB von V und Q der von B aufgespannte Würfel:
$$\mathrm{vol}(Q) := 1$$
2) Sei $C = (v_1, \dots, v_n)$ und A die BWM von B zu C und
$$\Phi = \left\{ \sum_{i=1}^{n} x_i v_i \;\middle|\; x_i \in \mathbb{R} \cap [0,1) \right\}$$
Dann:
$$\mathrm{vol}(\Phi) := |\det(A)|$$

3) Sei Γ ein Gitter mit Grundmasche Φ

$$\operatorname{vol}(\Gamma) := \operatorname{vol}(\Phi)$$

Bem Das Gittervolumen ist basisunabhängig.

Errinnerung Wir nennen $K \subseteq V$

- zentralsymmetrisch, falls für alle $x \in K$ auch $-x \in K$
- konvex, falls für alle $x, y \in K$, $t \in [0,1]$ auch $ty + (1-t)x \in K$

Satz Sei Γ ein vollständiges Gitter in V und $K \subseteq V$ eine zentralsymmetrisch und konvexe Teilmenge. Falls

$$\operatorname{vol}(K) > 2^n \operatorname{vol}(\Gamma),$$

so enthält K mindestens einen von 0 versch. GP.

Beweis Es genügt zwei GP $\gamma_1, \gamma_2 \in \Gamma$, so dass

$$\left(\tfrac{1}{2}K + \gamma_1\right) \cap \left(\tfrac{1}{2}K + \gamma_2\right) \neq \emptyset.$$

Wir können dann einen Schnittpunkt finden

$$\tfrac{1}{2}x_1 + \gamma_1 = \tfrac{1}{2}x_2 + \gamma_2, \quad x_1, x_2 \in K$$

$$\Leftrightarrow \gamma = \underbrace{\gamma_1 - \gamma_2}_{\in \Gamma} = \underbrace{\frac{x_2 - x_1}{2}}_{\in K}$$

Wären die Mengen $(\tfrac{1}{2}K + \gamma)$, $\gamma \in \Gamma$ paarweise disjunkt, so wären auch die Durchschnitte $\Phi \cap (\tfrac{1}{2}K + \gamma)$ und es wäre

$$\operatorname{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \operatorname{vol}\left(\Phi \cap \left(\tfrac{1}{2}K + \gamma\right)\right)$$

Durch die Translationen und $-\gamma$

$(\Phi - \gamma) \cap \frac{1}{2}K$ erhalten wir Mengen vom selben Volumen.
Die Verschiebungen $\Phi - \gamma$, $\gamma \in \Gamma$ überdecken $\frac{1}{2}K$. Es folgt

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \tfrac{1}{2}K\right)$$

$$= \mathrm{vol}\left(\tfrac{1}{2}K\right) = \frac{1}{2^n}\mathrm{vol}(K).$$

$\square$

2. Geometrie der Zahlen

<u>Setting</u> · K ist ein algebraischer Zahlkörper vom Grad n.
· $\mathcal{O}_K$ sein Ganzheitsring
· $T := \mathrm{Hom}(K, \mathbb{C})$

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

Es gibt n Einbettungen.
Es gibt r reelle Einbettungen $\rho_1, \dots, \rho_r : K \to \mathbb{R}$
Die komplexen Einbettungen gruppieren sich zu s Paaren $\sigma_1, \overline{\sigma}_1, \dots, \sigma_s, \overline{\sigma}_s : K \to \mathbb{C}$.
$n = r + 2s$

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

<u>Bem</u> Für das Skalarprodukt auf $K_{\mathbb{C}}$ gilt
$\langle Fx, Fy \rangle = \overline{\langle x, y \rangle}$

<u>Def</u> $K_{\mathbb{R}} := \{ \underset{z=}{(z_\tau)_{\tau \in T}} \in K_{\mathbb{C}} \mid F(z) = z \}$

<u>Bem</u> $F(ja) = ja$
Wir können also j als Abbildung $j : K \to K_{\mathbb{R}}$ ansehen.

<u>Bem</u> Das Skalarprodukt eingeschränkt auf $K_{\mathbb{R}}$ ist ein reelles Skalarprodukt.

<u>Satz</u> Wir erhalten einen Isomorphismus

$$f : K_{\mathbb{R}} \to \mathbb{R}^{r+2s} = \prod \mathbb{R}$$

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

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

Das Skalarprodukt in $K_\mathbb{R}$ wird in ein Skalarprodukt

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

überführt, wobei $\alpha_\tau=1$, falls τ reell ist und $\alpha_\tau=2$, falls τ komplex ist.

<u>Beweis</u> Fall $z=(z_\tau)_{\tau\in T}\in K_\mathbb{R}$, dann muss

$$z_{\bar\tau}=\overline{z_\tau}$$

gelten. $\square$

<u>Bem</u> $\mathrm{vol}_{\text{kanonisch}}(X) = 2^s\,\mathrm{vol}_{\text{Lebesgue}}(f(X))$

<u>Satz</u> Ist $\underline{a}\neq 0$ ein Ideal von $\mathcal{O}_K$. Dann ist $\Gamma = j\underline{a}$ ein vollständiges Gitter in $K_\mathbb{R}$ mit dem Grundmaschenvolumen

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

<u>Beweis</u> Sei $\alpha_1,\dots,\alpha_n$ eine $\mathbb{Z}$-Basis von $\underline{a}$.

$$\Rightarrow \Gamma = j\underline{a} = \mathbb{Z} j\alpha_1+\dots+\mathbb{Z} j\alpha_n.$$

<u>Thm</u> Sei $\underline{a}\neq 0$ ein ganzes Ideal von K und sei $c_\tau>0$ für alle $\tau\in T$, $c_\tau=c_{\bar\tau}$ und

$$\prod_{\tau\in T} c_\tau > \left(\frac{2}{\pi}\right)^s \underbrace{\sqrt{|d_K|}\,[\mathcal{O}_K:\underline{a}]}_{\mathrm{vol}(\Gamma)}$$

Dann existiert ein $a\in\underline{a}$, $a\neq 0$, sodass

$$|\tau a|<c_\tau \quad \forall \tau\in T$$

<u>Beweis</u> Die $X=\{(z_\tau)_{\tau\in T}\in K_\mathbb{R} \mid |z_\tau|<c_\tau\}$ ist zentralsymmetrisch und konvex.

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

$$\mathrm{vol}(X) = 2^s\,\mathrm{vol}(f(X))$$

$$\Rightarrow \mathrm{vol}(K) = 2^s \mathrm{vol}_{Leb.}(f(K))$$
$$= 2^s \prod_\rho 2c_\rho \prod_\sigma (\pi c_\sigma^2)$$
$$= 2^{r+s} \pi^s \prod_{\tau \in T} c_\tau$$
$$> 2^{r+s} \pi^s \left(\frac{2}{\pi}\right)^s \mathrm{vol}(\Gamma)$$
$$= 2^n \mathrm{vol}(\Gamma)$$

Mit dem Gitterpunktsatz finden ein $a \in \underline{a}$, $a \neq 0$, so dass $ja \in \Gamma \cap K$. Die Aussage folgt aus der Def von K.

3. Endlichkeit der Klassenzahl

$$h_K := |Cl_K|$$

<u>Def</u> Sei $\underline{a} \neq 0$. Dann nennen wir

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

<u>Bem</u> Ein Hauptideal (α) von $\mathcal{O}_K$ hat die Absolutnorm $\underline{N}((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$.

<u>Satz</u> Die Absolutnorm ist multiplikativ

$$\underline{N}(\underline{a}\underline{b}) = \underline{N}(\underline{a}) \underline{N}(\underline{b})$$

<u>Lem</u> In jedem Ideal $\underline{a} \neq 0$ von $\mathcal{O}_K$ gibt es ein $a \in \underline{a}$, $a \neq 0$, so dass

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

<u>Beweis</u> Für $\varepsilon > 0$ wählen $c_\tau > 0$ mit $c_{\bar\tau} = c_\tau$ und

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

Mit dem Thm finden wir $a \in \underline{a}$, $a \neq 0$ mit $|\tau a| < c_\tau$.

$$|N_{K|\mathbb{Q}}(a)| = \prod |\tau a| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, \underline{N}(\underline{a}) + \varepsilon$$

Wir erhalten insbesondere ein $a \in \underline{a}, a \neq 0$ mit

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

□

Thm Die Klassenzahl für alg. Zahlkörper ist endlich.

Beweis Für $M > 0$ gibt es nur endlich viele Ideale $\underline{a}$ mit $\underline{N}(\underline{a}) \leq M$.

Sei $\mathfrak{p} \neq 0$ ein Primideal von $\mathcal{O}_K$, sodass $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Dann ist $\mathcal{O}_K/\mathfrak{p}$ eine endliche Erweiterung von $\mathbb{Z}/p\mathbb{Z}$ vom $f \geq 1$ und

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

Für ein festes $p \in \mathbb{Z}$ gibt es nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, wegen $\mathfrak{p} \mid (p)$.

$\Rightarrow$ Es gibt nur endlich viele Ideale $\underline{a}$ mit $\underline{N}(\underline{a}) \leq M$

Es reicht daher aus für jedes $[\underline{a}] \in Cl_K$ ein ganzes Ideal $\underline{a}_1$ zu finden mit

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

Sei $\underline{a} \in [\underline{a}]$, $\gamma \in \mathcal{O}_K, \gamma \neq 0$, so dass $\underline{b} = \gamma \underline{a}^{-1} \subseteq \mathcal{O}_K$. Das Lemma gibt uns ein $\alpha \in \underline{b}, \alpha \neq 0$ mit

$$M \geq |N_{K|\mathbb{Q}}(\alpha)|\, \underline{N}(\underline{b})^{-1} = \underline{N}((\alpha))\, \underline{N}(\underline{b})^{-1}$$
$$= \underline{N}(\alpha \underline{b}^{-1}).$$

Demnach hat $\alpha \underline{b}^{-1} = \alpha \gamma^{-1} \underline{a} \in [\underline{a}]$ die gewünschte Eigenschaft.

□