$$\mathcal{O}_K/\mathfrak{p} \times \mathfrak{p}^i/\mathfrak{p}^{i+1} \longrightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1}$$
$$(x+\mathfrak{p},\ y+\mathfrak{p}^{i+1}) \longmapsto xy+\mathfrak{p}^{i+1}$$

$a+\mathfrak{p}^{i} \in \mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist Basis, denn

$$\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1}$$
$$x+\mathfrak{p} \longmapsto ax+\mathfrak{p}^{i+1}$$

ist VR-Iso.

Inj: klar, weil $a+\mathfrak{p}^{i+1} \neq 0 \in \mathfrak{p}^i/\mathfrak{p}^{i+1}$

Surj: Es ist $\mathfrak{p}^i \supset \underbrace{a\mathcal{O}_K+\mathfrak{p}^{i+1}}_{=:\mathfrak{b}} \supsetneq \mathfrak{p}^{i+1}$

$\Rightarrow \mathcal{O}_K \supset \mathfrak{b}\,\mathfrak{p}^{-i} \supsetneq \mathfrak{p}$

$\overset{\mathfrak{p}\text{ prim}}{\Rightarrow} \mathcal{O}_K = \mathfrak{b}\cdot\mathfrak{p}^{-i} \Rightarrow \mathfrak{b} = \mathfrak{p}^i$

$\Rightarrow$ Surj.

Also: $\#\,\mathfrak{p}^i/\mathfrak{p}^{i+1} = \#\,\mathcal{O}_K/\mathfrak{p} = N(\mathfrak{p})\ \forall i$

$\Rightarrow N(\mathfrak{p}^r) = [\mathcal{O}_K : \mathfrak{p}^r]$

$$= [\mathcal{O}_K:\mathfrak{p}][\mathfrak{p}:\mathfrak{p}^2]\cdots[\mathfrak{p}^{r-1}:\mathfrak{p}^r]$$
$$= N(\mathfrak{p})^r. \qquad \square$$

Kor 3: Für Ideale $\mathfrak{a},\mathfrak{b} \subset \mathcal{O}_K$ gilt $N(\mathfrak{a}\cdot\mathfrak{b}) = N(\mathfrak{a})\,N(\mathfrak{b})$.

Ist $\mathfrak{a} \subset K$ gebr. Ideal, so def. man die Norm wie folgt:

Schreibe $\mathfrak{a} = c^{-1} \cdot (c\mathfrak{a})$ mit $c \in \mathcal{O}_K$, so dass $c\mathfrak{a} \subset \mathcal{O}_K$ ganz.

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

Ist unabh. von Wahl von c.

Erhalten Hom

$$N : J_K \longrightarrow \mathbb{Q}^*$$

<u>Lemma 4</u>: Sei $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ Ideal. Es ex. $0 \neq a \in \mathfrak{a}$, mit

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

<u>Bew</u>: Sei $\varepsilon > 0$.
Wähle für $\sigma \in \mathrm{Hom}(K, \mathbb{C})$ Zahlen $c_\sigma \in \mathbb{R}_{>0}$ so dass $c_{\bar\sigma} = c_\sigma$ und

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

Nach §2, Satz 2, ex. $0 \neq a \in \mathfrak{a}$, so dass

$$|\sigma a| < c_\sigma \quad \forall \sigma.$$

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

Da $|N_{K/\mathbb{Q}}(a)| \in \mathbb{N}$ und da dies $\forall \varepsilon > 0$ gilt, muss $0 \neq a \in \mathfrak{a}$ ex. mit

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

<u>Satz 5</u>: Die Idealklassengruppe $Cl_K = J_K / P_K$ ist endl.

$h_K = \# Cl_K$ heißt Klassenzahl von K.

<u>Bew.</u>:

1) Sei $p \in \mathbb{N}$ PZ. Es ex nur endl viele Primideale $\mathfrak{p} \subset \mathcal{O}_K$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Denn: $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} \Rightarrow \mathfrak{p} \supset p\mathcal{O}_K$
$\Rightarrow \mathfrak{p} \mid p\mathcal{O}_K$

Aber $p\mathcal{O}_K$ hat nur endl viele Primidealteiler.

2) Sei $C > 0$. Es ex nur endl viele PI $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ mit $N(\mathfrak{p}) < C$.

Denn: $\mathfrak{p} \cap \mathbb{Z} \subset \mathbb{Z}$ Primideal
$\Rightarrow \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für ein PZ $p \in \mathbb{N}$.

$$\Rightarrow \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathcal{O}_K \\ \downarrow & & \downarrow \\ \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathcal{O}_K/\mathfrak{p} \end{array} \quad \text{kommutiert}$$

Untere Zeile ist Einr. endlicher Kp.

$\Rightarrow \# \mathcal{O}_K/\mathfrak{p} = p^f$, wobei $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] \in \mathbb{N}$

$N(\mathfrak{p}) < C \Rightarrow p^f < C \Rightarrow p < C$ und $f < \frac{\log C}{\log p}$.

$\Rightarrow$ Nur endl viele $\mathfrak{p}$.

3) Es ex nur endl viele Ideale $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ mit $N(\mathfrak{a}) < C$.

Dies folgt aus 2 und der eindeutigen PI-Zerl.

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{\nu_r}$$

$$\Rightarrow N(\mathfrak{a}) = N(\mathfrak{p}_1)^{\nu_1} \cdot \ldots \cdot N(\mathfrak{p}_r)^{\nu_r}.$$

4) Daher genügt es zz: Jede Idealklasse $\mathfrak{K} \in Cl_K$ enth. ganzes Ideal $\mathfrak{a} \in \mathfrak{K}$ mit

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

Dazu: Sei $\mathfrak{a}_0 \in \mathfrak{K}$ bel. und $0 \neq \gamma \in O_K$ so dass

$$\mathfrak{b} = \gamma \cdot \mathfrak{a}_0^{-1} \subset O_K.$$

Lem. 4 $\Rightarrow \exists\, 0 \neq \alpha \in \mathfrak{b}$ s.d.

$$N_{K/\mathbb{Q}}(\alpha) \le \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\, N(\mathfrak{b}) = M \cdot N(\mathfrak{b})$$

$\Rightarrow N_{K/\mathbb{Q}}(\alpha) \cdot N(\mathfrak{b})^{-1} \le M$

$\Rightarrow$ Das Ideal $\mathfrak{a} = \alpha \cdot \mathfrak{b}^{-1} = \alpha \gamma^{-1} \mathfrak{a}_0 \in \mathfrak{K}$ ist ganz

$(\alpha \in \mathfrak{b} \Rightarrow (\alpha) \subset \mathfrak{b} \Rightarrow \alpha \mathfrak{b}^{-1} \subset O_K)$

und $N(\mathfrak{a}) = N_{K/\mathbb{Q}}(\alpha) \cdot N(\mathfrak{b})^{-1} \le M$ □

Bsp: Für imaginär quadr. Zahlkörper gilt:

d_K	-3	-4	-7	-8	-11	-15	-19	-20	-23
h_K für $K = \mathbb{Q}(\sqrt{d_K})$	1	1	1	1	1	2	1	2	3

$h_K = 1$ für $d_K = -43, -67, -163$ und $h_K \sim \sqrt{|d_K|}$ (Siegel), vermut. (Heegner, Stark).

§4 Der Dirichletsche Einheitensatz

Sei $K|\mathbb{Q}$ Zahlkörper mit Ganzheitsring $\mathcal{O}_K$.

Ziel: Beschreibe $\mathcal{O}_K^*$.

• Enthält $\mu(K) :=$ Gruppe der Einheitswurzeln in K.

Betr.:

$$\begin{tikzcd}
K^* \arrow[r, "j"] \arrow[d, "N_{K|\mathbb{Q}}"'] & K_{\mathbb{R}}^* \arrow[r, "\ell"] \arrow[d, "N"] & \left(\prod_\tau \mathbb{R}\right)^+ = \{(x_\tau);\ x_\tau = x_{\bar\tau}\} \arrow[d, "Tr"] \\
\mathbb{Q}^* \arrow[r] & \mathbb{R}^* \arrow[r, "\log|\cdot|"] & \mathbb{R}
\end{tikzcd}$$

Sei $\mathcal{O}_K^* = \{\varepsilon \in \mathcal{O}_K;\ N_{K|\mathbb{Q}}(\varepsilon) = \pm 1\}$ Einheitengruppe von $\mathcal{O}_K$

$S = \{y \in K_{\mathbb{R}};\ N(y) = \pm 1\}$ Norm ± 1 Fläche

$H = \{x \in (\prod_\tau \mathbb{R})^+;\ Tr(x) = 0\}$ Spur 0 Hyperebene

Durch Einschränkung erhalten wir Hom.

$$\begin{tikzcd}
\mathcal{O}_K^* \arrow[r, "j"] \arrow[rr, bend right, "\lambda := \ell\circ j"'] & S \arrow[r, "\ell"] & H
\end{tikzcd}$$

Sei $\Gamma := \lambda(\mathcal{O}_K^*) \subset H$.

Lemma 1:
Die Sequenz

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

ist exakt.

Bew: ZZ: $\mu(K) = Ker(\lambda)$.

„$\subseteq$": Sei $\zeta \in \mu(K)$. Dann gilt $\forall\ \tau \in Hom(K, \mathbb{C})$, dass

$|\sigma(\xi)| = 1$

$\Rightarrow \log|\sigma(\xi)| = 0$

$\Rightarrow \xi \in \mathrm{Ker}(\lambda)$.

„$\supseteq$": Sei umgekehrt $\varepsilon \in \mathcal{O}_K^*$ mit $\lambda(\varepsilon) = 0$.

$\Rightarrow \ell(j(\varepsilon)) = 0$

$\Rightarrow |\sigma(\varepsilon)| = 1 \quad \forall \sigma \in \mathrm{Hom}(K, \mathbb{C})$

$\Rightarrow j(\varepsilon) = (\sigma\varepsilon)_\sigma$ liegt im (kompakten) „Einheitsquader" von $K_\mathbb{R}$.

Andererseits ist $j(\varepsilon)$ im Gitter $j(\mathcal{O}_K) \subset K_\mathbb{R}$ enthalten. Dies ist diskret.

$\Rightarrow$ Nur endlich viele $\varepsilon \in \mathcal{O}_K^*$ erfüllen dies.

$\Rightarrow \mathrm{Ker}(\lambda) \subset \mathcal{O}_K^*$ ist endliche Untergruppe

$\Rightarrow \mathrm{Ker}(\lambda)$ besteht aus Einheitswurzeln in K^*. □

Wir wollen nun Γ beschreiben.

<u>Lemma 2</u>: Sei $a \in \mathbb{Z}$. Bis auf Mult. mit Einheiten in $\mathcal{O}_K^*$ ex. nur endlich viele $\alpha \in \mathcal{O}_K$ mit $N_{K|\mathbb{Q}}(\alpha) = a$.

<u>Bew</u>: Klar für $a = 0$. Sei $a \neq 0$. In jeder Nebenklasse in $\mathcal{O}_K / a\mathcal{O}_K$ ex. bis auf Mult. mit $\mathcal{O}_K^*$ höchstens ein α mit $|N(\alpha)| = |a|$.

<u>Denn</u>: Sei $\beta = \alpha + a\gamma$, $\gamma \in \mathcal{O}_K$, ein zweites, so gilt

$$\frac{\alpha}{\beta} = \frac{\beta - a\gamma}{\beta} = 1 - \frac{a\gamma}{\beta} = 1 \pm \frac{N(\beta)}{\beta}\gamma \in \mathcal{O}_K$$

denn $N(\beta)/\beta \in \mathcal{O}_K$.

Genauso gilt $\frac{\beta}{\alpha} \in \mathcal{O}_K$.

$\Rightarrow \frac{\alpha}{\beta} \in \mathcal{O}_K^*$.

$\Rightarrow$ Bis auf Mult. mit Einheiten in $\mathcal{O}_K$ ex. höchstens $\# \mathcal{O}_K/\alpha\mathcal{O}_K = |N(\alpha)|$ Elemente in $\mathcal{O}_K$ der Norm a. □

<u>Satz</u> 3: Die Gruppe $\Gamma = \lambda(\mathcal{O}_K^*)$ ist ein vollst. Gitter im $(r+s-1)$-dim. Vektorraum H.

<u>Kor</u> 4: $\Gamma \cong \mathbb{Z}^{r+s-1}$.

<u>Bew</u> von Satz 3:

1. $\Gamma \subset H$ ist Gitter (d.h. diskrete Ug):

Haben

$$\begin{tikzcd}
\mathcal{O}_K^* \arrow[r] \arrow[d] & S \arrow[r] \arrow[d] & H \arrow[d] \\
K^* \arrow[r, "j"] \arrow[dr] & K_{\mathbb{R}}^* \arrow[r, "\ell"] \arrow[d] & (\prod_\sigma \mathbb{R})^+ \arrow[d] \\
& K_{\mathbb{C}}^* \arrow[r] & \prod_\sigma \mathbb{R}
\end{tikzcd}$$

Norm 1 Hyperfl.

Spur 0 Hyperfl.

(Die vertikalen Pfeile sind Inklusionen.)

Genügt z.z.: $\forall c > 0$ enthält der Quader $Q_c = \{(x_\sigma) \in \prod_\sigma \mathbb{R} : |x_\sigma| \le c\}$ nur endl. viele Punkte aus Γ.

Das Urbild von Q_c in $K_{\mathbb{C}}^*$ ist

$$\{(z_\sigma) \in \prod_\tau \mathbb{C}^* : e^{-c} \le |z_\tau| \le e^c \ \forall \tau\}$$

Diese kompakte Teilmenge enth. nur endl. viele Punkte aus $j(\mathcal{O}_K)$, da $j(\mathcal{O}_K) \subset K_{\mathbb{R}}$ diskret §2 Satz 1

($\Longleftrightarrow$ $j(\mathcal{O}_K) \subset K_{\mathbb{C}}$ " ".)

$\Longrightarrow$ $j(\mathcal{O}_K^*) \subset K_{\mathbb{C}}$ " .

2.) $\Gamma \subset H$ ist volles Gitter.

Benutze Kap 4, §1, Lemma 3.

(Ein Gitter $\Gamma \subset V$ ist voll $\Longleftrightarrow$ $\exists$ beschr. Teilmenge $M \subset V$ s.d. $\bigcup_{\gamma \in \Gamma} (\gamma + M) = V$.)

ZZ: $\exists$ beschr. Teilmenge $M \subset H$ s.d.

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma)$$

$\Longleftrightarrow$ $\exists$ beschr. Teilmenge $T \subset S$ s.d.

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} T j(\varepsilon).$$

Für $\sigma \in \mathrm{Hom}(K, \mathbb{C})$ sei

$c_\sigma > 0$ mit $c_\sigma = c_{\bar\sigma}$ und

$$C := \prod_\sigma c_\sigma > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

Sei $X = \{(z_\sigma) \in K_{\mathbb{R}} \,;\, |z_\sigma| < c_\sigma \ \forall \sigma\}$

Für $y = (y_\sigma) \in S$ gilt

$$X_y = \{(z_\sigma) \in K_{\mathbb{R}} \,;\, |z_\sigma| < c'_\sigma \ \forall \sigma\}$$

mit $c'_\sigma = c_\sigma |y_\sigma|$,

$c'_\sigma = c'_{\bar\sigma}$,

$\prod_\sigma c'_\sigma = C$ weil $\prod_\sigma |y_\sigma| = N(y) = 1$.

(*) Nach §2, Satz 2, ex. $0 \neq a \in \mathcal{O}_K$ mit

$$j(a) = (\sigma a)_\sigma \in Xy.$$

(**) Lemma 2 $\Rightarrow$

$$\{\alpha \in \mathcal{O}_K : |\underbrace{N_{K|\mathbb{Q}}(\alpha)}_{\in \mathbb{Z}}| \leq C\}/\mathcal{O}_K^*$$

ist endlich.

Seien $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K \setminus \{0\}$ ein Rep-System.

Def.: $T := S \cap \bigcup_{i=1}^{N} X(j\alpha_i)^{-1}$

hat die gewünschte Eigenschaft.

Denn: • $X \subset K_\mathbb{R}$ beschr.

$\Rightarrow X(j\alpha_i)^{-1}$ beschr.

$\Rightarrow T \subset S$ beschr.

• $S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} T(j\varepsilon)$, denn:

Sei $y \in S$.

(*) $\Rightarrow \exists\, 0 \neq a \in \mathcal{O}_K : j(a) \in Xy^{-1}$

$\Rightarrow j(a) = xy^{-1}$ für ein $x \in X$.

Es gilt

$|N_{K|\mathbb{Q}}(a)| = |N(xy^{-1})| = |N(x)| < \prod_\sigma c_\sigma = C$.

(**) $\Rightarrow$ Es ex. $i \in \{1, \dots, N\}$ und $\varepsilon \in \mathcal{O}_K^*$ s.d.

$$a = \varepsilon \alpha_i.$$

$\Rightarrow y = x j(a)^{-1} = x j(\varepsilon\alpha_i)^{-1}$

$\Rightarrow \underbrace{y j(\varepsilon)}_{\in S} = \underbrace{x(j\alpha_i)^{-1}}_{\in X(j\alpha_i)^{-1}}$

$\Rightarrow \gamma\, g^j(\varepsilon) \in \Gamma$

$\Rightarrow \gamma \in \Gamma_{g^j(\varepsilon)}$. $\square$

<u>Satz 5</u>: $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}$.

D.h. es ex. Einheiten $\varepsilon_1, \dots, \varepsilon_t$, $t = r+s-1$, so dass jedes $\varepsilon \in \mathcal{O}_K^*$ eine eind. Darst. der Form

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

($\zeta \in \mu(K)$, $\nu_i \in \mathbb{Z}$) hat.

$\varepsilon_1, \dots, \varepsilon_t$ heißen <u>Fundamentaleinheiten</u>.

<u>Bew</u>: Ex. Seq.

$$1 \to \mu(K) \to \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \to 0, \quad \Gamma \cong \mathbb{Z}^{r+s-1}$$

Sei $v_1, \dots, v_t$ $\mathbb{Z}$-Basis von Γ.
Seien $\varepsilon_1, \dots, \varepsilon_t \in \mathcal{O}_K^*$ mit

$$\lambda(\varepsilon_i) = v_i.$$

Sei $A \subset \mathcal{O}_K^*$ die von den ε_i erz. UG.
Dann ist $\lambda|_A : A \xrightarrow{\sim} \Gamma$ Iso.

$\Rightarrow$ $A \cap \mu(K) = \{1\}$ und

$$\mathcal{O}_K^* = \mu(K) \times A. \quad \square$$

$\Gamma = \lambda(\mathcal{O}_K^*) \subset H \cong \mathbb{R}^{r+s-1}$
ist vollst. Gitter.
H ist eukl. VR mit dem angeulr. Skalarprodukt vermöge

$$H \subset \left(\prod_\tau \mathbb{R}\right)^+$$

<u>Satz 6</u>: Das Volumen eines Fundamentalbereichs von $\Gamma \subset H$ ist

$$\mathrm{vol}(\Gamma) = \sqrt{r+s} \cdot R,$$

wobei R der <u>Regulator</u> von K ist. R ist def. als Betrag der Det einer $t \times t$-Untermatrix der $(t+1) \times t$ Matrix

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda_{t+1}(\varepsilon_1) & \cdots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}. \qquad \lambda : \mathcal{O}_K^\times \to H \subset \mathbb{R}^{r+s} = \mathbb{R}^{t+1}$$

<u>Bew</u>: Übung.