# Dirichlet's unit theorem:

Recall that for $D \in \mathbb{Z}$ a fundamental discriminant, $K = \mathbb{Q}(\sqrt{D})$, we know

$$\mathcal{O}_K^\times \text{ is } \begin{cases} \text{finite, if } D<0 & \text{norm is pos. definite} \\ \mathbb{Z} \text{ or } \mathbb{Z} \oplus \mathbb{Z}/_{2\mathbb{Z}} \text{ if } D>0 \end{cases} = \underbrace{\mu_K}_{\text{finite}} \oplus \mathbb{Z}^{r_1+r_2-1}.$$

Theorem (Dirichlet)

Let $K/\mathbb{Q}$ a #-field. Then $\mathcal{O}_K^\times$ is of finite type. More precisely,

$$\mathcal{O}_K^\times \cong \mu_K \oplus \mathbb{Z}^{r_1+r_2-1},$$

where $\mu_K$ is a finite group, namely the roots of unity in $K$.

Strategy: Let $r = r_1 + r_2$ and consider

$$H(\mathbb{R}) = \{(x_1, \dots, x_r) : \sum_{i=1}^r x_i = 0\}.$$

We will construct a group hom $F: \mathcal{O}_K^\times \longrightarrow H(\mathbb{R})$ such that

- $\ker F = \mu_K$
- $F(\mathcal{O}_K^\times) \subseteq H(\mathbb{R})$ is a lattice.

## The logarithmic embedding

We define $\mathrm{Log}: K_\infty^\times \longrightarrow \mathbb{R}^r$

$$(z_1,\dots,z_r) \longmapsto (\log|z_1|,\dots,\log|z_{r_1}|, 2\log|z_{r_1+1}|,\dots, 2\log|z_2|)$$

Properties: (i) Log is gp-hom.

(ii) $\ker \mathrm{Log} \cong \{\pm 1\}^{r_1} \oplus (S^1)^{r_2}$ is compact.

### Definition

The ~~logarithmic embedding~~ (of $K^\times$) is the map $\mathrm{Log}_\infty := \mathrm{Log} \circ \sigma_\infty$.

inappropriate, as ker non-trivial

### Proposition

- $\ker(\mathrm{Log}_\infty|_{\mathcal{O}_K^\times})$ is finite,
- $\mathrm{Log}_\infty(\mathcal{O}_K^\times)$ is a discrete subgroup of $H(\mathbb{R})$

Notation: $T \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^r, \mathbb{R})$ denotes $x \longmapsto T(x) = \sum_{i=1}^{r} x_i$, i.e., $H(\mathbb{R}) = \ker T$.

Pf: (i) $\mathrm{Log}_\infty(\mathcal{O}_K^\times) \subseteq H(\mathbb{R})$: Let $z \in \mathcal{O}_K^\times$, then

$$0 = \log|\underbrace{\mathrm{Nr}(z)}_{=\pm 1}| = \sum_{i=1}^{d} \log|\sigma_i(z)| = \sum_{i=1}^{r_1} \log|\sigma_i(z)| + \sum_{i=1}^{r_2} 2\log|\sigma_i(z)| = T(\mathrm{Log}_\infty(z)).$$

(ii) $\mathrm{Log}_\infty(\mathcal{O}_K^\times)$ is discrete + finiteness of kernel of $\mathrm{Log}_\infty|_{\mathcal{O}_K^\times}$: Exercise.

Corollary:

$\mathrm{Log}_\infty(\mathcal{O}_K^\times)$ is a free $\mathbb{Z}$-module of rank $r' < r$. In particular, $\mathcal{O}_K^\times$ is of finite type.

Proof: $\operatorname{rank} \mathrm{Log}_\infty(\mathcal{O}_K^\times) \leq \dim H(\mathbb{R})$ (by discreteness) $= r-1$.

Moreover, $\mathcal{O}_K^\times / \ker \mathrm{Log}_\infty|_{\mathcal{O}_K^\times} \cong \mathrm{Log}_\infty(\mathcal{O}_K^\times)$ is of finite type and $\ker \mathrm{Log}_\infty|_{\mathcal{O}_K^\times}$ finite

$\Rightarrow \mathcal{O}_K^\times$ is f.t.

$\boxtimes$

**Prop.** $\ker(\mathrm{Log}_\infty|_{\mathcal{O}_K^\times}) = \mathcal{O}_{K,\mathrm{tors}}^\times = \{z\in\mathcal{O}_K^\times : \exists m\in\mathbb{N}\ z^m=1\}$

$= \{z\in K : z \text{ is a root of unity}\} =: \mu_K \subseteq \mathcal{O}_K$

**Proof:** (i) $\mathcal{O}_{K,\mathrm{tors}}^\times = \mu_K$:

"$\subseteq$" Clear

"$\supseteq$" $z\in\mu_K \Rightarrow \exists\, m\in\mathbb{N}$ s.t. $z^m-1=0 \Rightarrow z\in\mathcal{O}_K$. Similarly, $z^{-m}-1 = -z^{-m}(z^m-1)=0$

$\Rightarrow z\in\mathcal{O}_K^\times$.

NTS: $z\in\mu_K \Rightarrow z^{-1}\in\mathcal{O}_K$

(ii) $\ker(\mathrm{Log}_\infty|_{\mathcal{O}_K^\times}) = \mathcal{O}_{K,\mathrm{tors}}^\times$:

"$\supseteq$" $\mathrm{Log}_\infty(\mathcal{O}_{K,\mathrm{tors}}^\times) \subseteq \mathrm{Log}_\infty(\mathcal{O}_K^\times)_{\mathrm{tors}} = \{0\}$.

"$\subseteq$" We know that $H = \ker(\mathrm{Log}_\infty|_{\mathcal{O}_K^\times})$ is finite; cf. Sheet 12. Thus $H < K^\times$ is a finite subgroup. Let $h\in H$, then $h^{|H|} = 1_K$, thus $h\in\mu_K \overset{(i)}{=} \mathcal{O}_{K,\mathrm{tors}}^\times$.

$\blacksquare$

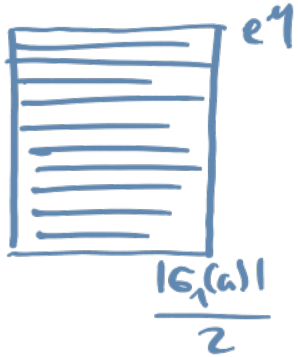
## Determining the rank of $\mathcal{O}_K^\times$ for real quadratic $K$:

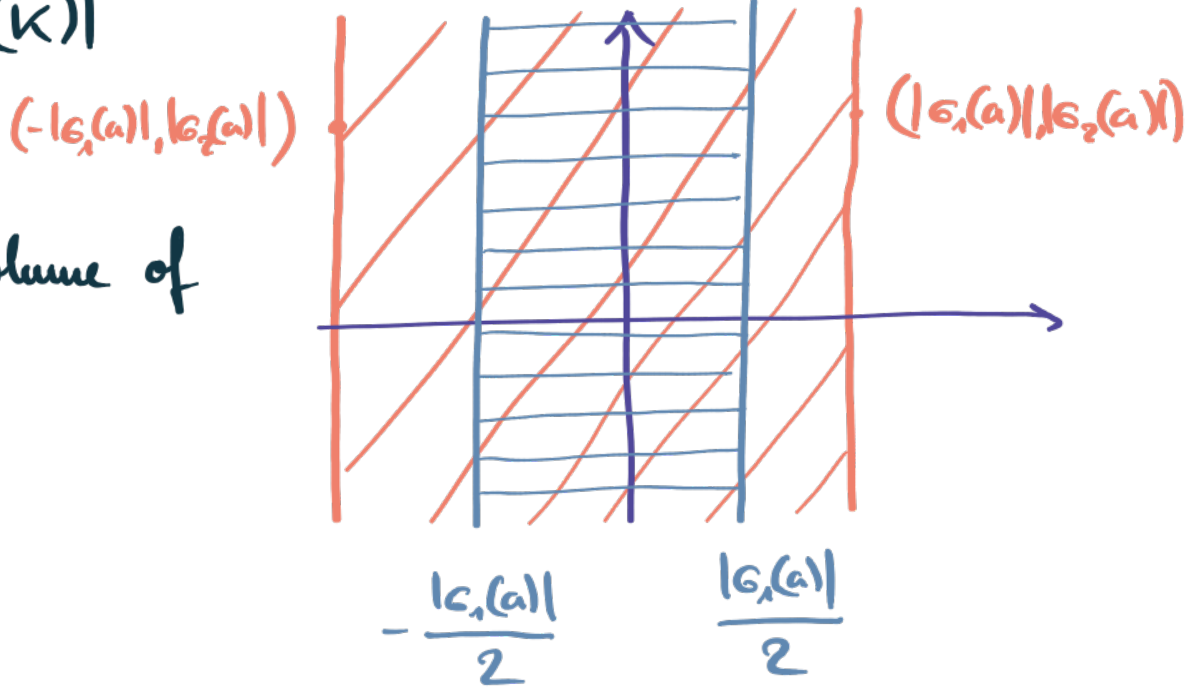
Step 1: For all $a \in \mathcal{O}_K - \{0\}$ there is $b \in \mathcal{O}_K - \{0\}$ s.t.

$$\text{(i)} \; |Nr_{K/\mathbb{Q}}(b)| \le 2\,|disc(K)|$$

$$\text{(ii)} \; |\sigma_1(b)| \le \frac{|\sigma_1(a)|}{2}$$

Proof via Minkowski's theorem: the volume of




goes to $\infty$ as $y \to \infty$.

Choose $y$ s.t. $|\sigma_1(a)| e^y = 4\,|disc(K)|^{1/2}$.

Minkowski's first theorem yields $b \in \mathcal{O}_K - \{0\}$ s.t. $|\sigma_1(b)| \le \frac{|\sigma_1(a)|}{2}$. Moreover,

$$|Nr(b)| = |\sigma_1(b)|\,|\sigma_2(b)| \le \frac{|\sigma_1(a)|}{2} e^y = 2\,|disc(K)|^{\frac{1}{2}}.$$

**Step 2:** Finding an element in $\mathcal{O}_K^\times - \mu_K$ (which is all we need since $r-1=1$)

Start with any element $a \in \mathcal{O}_K - \{0\}$ and produce a sequence $a_1, a_2, \ldots \in \mathcal{O}_K - \{0\}$ s.t. $|N_r(a_i)| \leq 2|\mathrm{disc}(K)|^{\frac{1}{2}}$ and $|\sigma_1(a_i)| \geq \frac{|\sigma_1(a_{i+1})|}{2}$.

The sequence of ideals $a_i\mathcal{O}_K$ all have norm $\ll 1$. As there are only finitely many such ideals, there are $i<j$ s.t. $a_i\mathcal{O}_K = a_j\mathcal{O}_K$. Hence $\frac{a_j}{a_i}$ is a unit such that

$$\left|\sigma_1\left(\frac{a_j}{a_i}\right)\right| = \frac{|\sigma_1(a_j)|}{|\sigma_1(a_i)|} = \frac{|\sigma_1(a_j)|}{|\sigma_1(a_i)|} \leq \frac{\frac{1}{2}|\sigma_1(a_i)|}{|\sigma_1(a_i)|} < 1$$

and therefore $\frac{a_i}{a_j} \notin \mu_K$.

## Determining the rank of $\mathcal{O}_K^\times$ in general:

**Proposition:** (We possibly need more than one element)

Suppose $u_1, \dots, u_r \in \mathcal{O}_K^\times$ s.t. for all $1 \leq k, i \leq r$ we have

$$i \neq k \Rightarrow \mathrm{Log}_\infty(u_k)_i < 0.$$

Then $(\mathrm{Log}_\infty(u_k))_{1 \leq k \leq r}$ contains a linearly independent subset of cardinality $r-1$.

**Note:** Assuming the proposition, it remains to prove that such a tuple $(u_1, \dots, u_{r-1})$ exists.

**Proof of proposition:** We have to show that for any $L \in H(\mathbb{R})^*$ there is $k$ s.t. $L(\mathrm{Log}_\infty(u_k)) \neq 0$.

Let $L \in H(\mathbb{R})^*$ non-zero. Then there are $\lambda_1, \dots, \lambda_{r-1} \in \mathbb{R}$ s.t. for all $v = (v_1, \dots, v_r) \in H(\mathbb{R})$

$$L(v) = \sum_{i=1}^{r-1} \lambda_i v_i .$$

Suppose $|\lambda_k| = \max_i |\lambda_i|$ and assume $\lambda_k > 0$. Then

$$L(\mathrm{Log}_\infty(u_k)) = \lambda_k \sum_{i=1}^{r-1} \mathrm{Log}_\infty(u_k)_i + \underbrace{\sum_{i=1}^{r-1} (\lambda_i - \lambda_k) \mathrm{Log}_\infty(u_k)_i}_{\geq 0 \ (i \neq k \Rightarrow \mathrm{Log}_\infty(u_k)_i < 0)} \geq -\lambda_k \mathrm{Log}_\infty(u_k)_r \overset{1 \leq k \leq r-1}{>} 0 .$$

So $L \neq 0$ on $\mathrm{Log}_\infty(\mathcal{O}_K^\times)$.

If $\lambda_k < 0$, the same argument shows that $-L \neq 0$ on $\mathrm{Log}_\infty(\mathcal{O}_K^\times)$. ∎

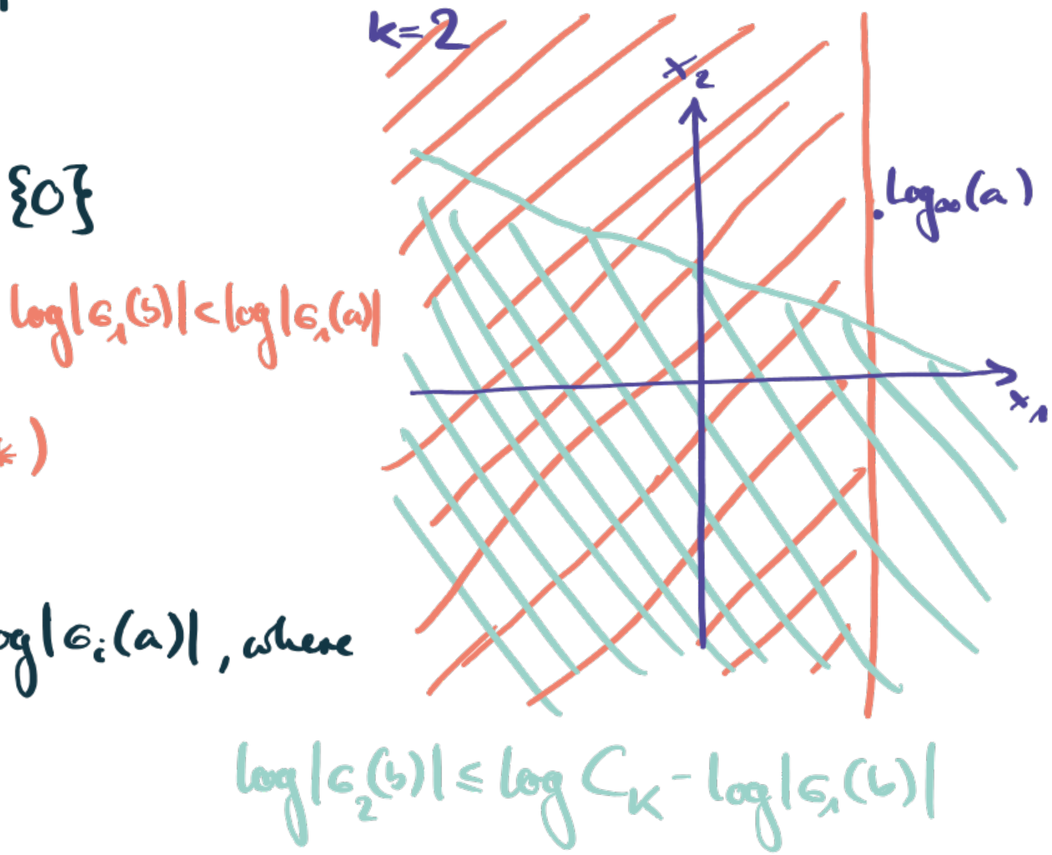
It remains to prove the existence of such a tuple.
The proof relies on the following lemma.

**Lemma:**

$\exists C_K > 0\ \forall k \leq r\ \forall a \in \mathcal{O}_K - \{0\}\ \exists b \in \mathcal{O}_K - \{0\}$

(i) $|Nr_{K|\mathbb{Q}}(b)| \leq C_K$

(ii) $\forall i \neq k\ \ \mathrm{Log}_\infty(a)_i > \mathrm{Log}_\infty(b)_i$ $\quad (*)$




Proof: Fix $k \leq r$. Let $\alpha_i = \mathrm{Log}_\infty(a)_i$. Then $\alpha_i = d_i \log|\sigma_i(a)|$, where

$$d_i = \begin{cases} 1 & \text{if } i \leq r_1, \\ 2 & \text{else.} \end{cases}$$

In this notation, $|Nr_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{r} |\sigma_i(a)|^{d_i} = \exp\left(\sum_{i=1}^{r} \alpha_i\right)$.

We will use Minkowski II: We choose a convex, symmetric neighbourhood $\mathcal{U}$ in $K_\infty$ of $0$ s.t. in the $i \neq k$ directions any pt. satisfies $(*)$, i.e.,

$$|z_i| < |\sigma_i(a)|$$

and in the $k$-direction we choose it large s.t. $\mathcal{U} \cap \sigma_\infty(\mathcal{O}_K) \neq \{0\}$.

Given $y \in \mathbb{R}$, let

$$B_k(y) = \left\{ z \in K_\infty : \begin{array}{ll} d_i \log|z_i| \leq \underset{\frac{d_i}{2}\log|\sigma_i(a)|}{\frac{\alpha_i}{2}} & \text{if } i \neq k, \\ d_k \log|z_i| \leq \frac{d_k y}{2} & \text{else}. \end{array} \right\} = \left\{ z \in K_\infty : \begin{array}{l} |z_i| \leq |\sigma_i(a)|^{\frac{1}{2}} \\ |z_k| \leq e^{y/2} \end{array} \right\}$$

Then

$$\mathrm{vol}(B_k(y)) = C(r_1, d) \exp\left(\frac{1}{2}\left(d_k y + \sum_{i \neq k} \alpha_i\right)\right) \begin{array}{l} \xrightarrow{y \to \infty} \infty \\ \xrightarrow{y \to -\infty} 0 \end{array}.$$

Choose $y$ s.t. $\mathrm{vol}(B_k(y)) = 2^d \operatorname{covol}(\mathcal{O}_K)$. Then we find $b \in \mathcal{O}_K - \{0\}$ such that $\sigma_\infty(b) \in B_k(y)$ and thus $b$ satisfies $(*)$.

Moreover,

$$|\mathrm{Nr}(b)| = \exp\left(\sum_i \mathrm{Log}_\infty(b)_i\right) \leq \exp\left(\frac{1}{2}\left(d_k y + \sum_{i \neq k} \alpha_i\right)\right) = \frac{2^d \operatorname{covol}(\mathcal{O}_K)}{C(r_1, d)} =: C_K.$$

$\blacksquare$

**Corollary:**

$\forall 1 \leq k \leq r\ \exists u_k \in \mathcal{O}_K^\times$ s.t.

$$i \neq k \Rightarrow \mathrm{Log}_\infty(u)_i < 0$$

**Proof:** Let $(a_n)_{n\in\mathbb{N}}$ s.t. (i) $a_n \in \mathcal{O}_K - \{0\}$,

(ii) $|\mathrm{Nr}_{K|\mathbb{Q}}(a_n)| \leq C_K$

(iii) $\forall n \in \mathbb{N}\ \forall i \neq k\ \ \mathrm{Log}(a_n)_i > \mathrm{Log}(a_{n+1})_i$

Let $\underline{a}_n = \mathcal{O}_K \cdot a_n \lhd \mathcal{O}_K$. Then $\mathrm{Nr}(\underline{a}_n) \leq C_K$, thus $\exists n > m$ s.t. $\underline{a}_n = \underline{a}_m$, i.e.,

$$a_n = u a_m \quad \text{for some } u \in \mathcal{O}_K^\times.$$

$$\Rightarrow \forall i \neq k \qquad \mathrm{Log}_\infty(u)_i = \mathrm{Log}_\infty(a_n)_i - \mathrm{Log}_\infty(a_m)_i < 0.$$

**Definition:** An $(r-1)$-tuple $(\varepsilon_1, \dots, \varepsilon_{r-1}) \in (\mathcal{O}_K^\times)^{r-1}$ s.t.

$$\mathcal{E} = (\mathrm{Log}_\infty(\varepsilon_1), \dots, \mathrm{Log}_\infty(\varepsilon_{r-1}))$$

is a $\mathbb{Z}$-basis of $\mathrm{Log}_\infty(\mathcal{O}_K^\times)$ is called a system of fundamental units.

The regulator of $K$ (or $\mathcal{O}_K$) is $\mathrm{reg}(K) = \mathrm{covol}(\mathrm{Log}_\infty(\mathcal{O}_K^\times))$.

defined using inner product on $H(\mathbb{R})$ induces from $\mathbb{R}^r$.

# The class number formula



## Theorem

Let $K/\mathbb{Q}$ a #-field, $[K:\mathbb{Q}] = d = r_1 + 2r_2$. Then

$$\left|\left\{ \mathfrak{a} \trianglelefteq \mathcal{O}_K : \mathrm{Nr}(\mathfrak{a}) \leq X \right\}\right| = \frac{2^{r_1}(2\pi)^{r_2} h(K) \operatorname{reg}(K)}{\omega_K |\mathrm{disc}(K)|^{1/2}} X + O_K\left(X^{1-\frac{1}{d}}\right),$$

where $h(K) = |\mathrm{Cl}(K)|$, $\omega_K = |\mu_K|$.

## Corollary:

Let $K/\mathbb{Q}$ imaginary, quadratic of discriminant $D \ll -1$. Then

$$h(K) = \lim_{X \to \infty} \frac{\sqrt{-D}}{\pi} \frac{\left|\left\{ \mathfrak{a} \trianglelefteq \mathcal{O}_K : \mathrm{Nr}(\mathfrak{a}) \leq X \right\}\right|}{X}.$$