Reminder:

Fix a finite extension $K/\mathbb{Q}$ of degree n. Write $r + 2s = n$ and let $\sigma_1, \dots, \sigma_r$ be the real embeddings and $\sigma_{r+1}, \dots, \sigma_n$ the non-real embeddings such that $\bar{\sigma}_{r+j} = \bar{\sigma}_{r+j+s}$ for all $1 \leqslant j \leqslant s$. Then

$$K \xhookrightarrow{j} K_{\mathbb{C}} \cong \mathbb{C}^n, \quad x \longmapsto \big(\sigma_1(x), \dots, \sigma_n(x)\big),$$

$$K \xhookrightarrow{j} K_{\mathbb{R}} \xrightarrow{\sim} \mathbb{R}^n, \quad x \longmapsto \big(\sigma_1(x), \dots, \sigma_r(x), \operatorname{Re}\sigma_{r+1}(x), \dots, \operatorname{Re}\sigma_{r+s}(x), \operatorname{Im}\sigma_{r+1}(x), \dots, \operatorname{Im}\sigma_{r+s}(x)\big).$$

Proposition 4.1.2: The standard scalar product on $K_{\mathbb{C}} \cong \mathbb{C}^n$ induces this scalar product on $\mathbb{R}^n$:

$$\boxed{\big\langle (x_i)_i, (y_i)_i \big\rangle := \sum_{i=1}^{r} x_i y_i + \sum_{i=r+1}^{n} 2x_i y_i.}$$

$2(x_i y_i + x_{i+s} y_{i+s})$

Note: For any $x \in K$ we get

$$\langle x, x\rangle = \sum_{i=1}^{n} \overline{\sigma_i(x)}\sigma_i(x) = \sum_{i=1}^{r} |\sigma_i(x)|^2 + \sum_{i=r+1}^{r+s} 2|\sigma_i(x)|^2.$$

Propositions 3.4.3 and 4.2.1: For every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the image $j(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$ with

$$\operatorname{vol}(K_{\mathbb{R}}/j(\mathfrak{a})) = \sqrt{\operatorname{disc}(\mathfrak{a})} = \operatorname{Nm}(\mathfrak{a}) \cdot \sqrt{|d_K|}.$$

Theorem 2.3.2: Let $X \subset V$ be a centrally symmetric convex subset which satisfies

$\Gamma < V$ complete lattice

$$\mathrm{vol}(X) \;>\; 2^{\dim(V)} \cdot \mathrm{vol}(V/\Gamma).$$

Then $X \cap \Gamma$ contains a non-zero element.

Theorem 4.2.2: Consider a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ and positive real numbers c_σ for all $\sigma \in \Sigma$ such that $c_{\bar\sigma} = c_\sigma$ and

$$\boxed{\prod_{\sigma\in\Sigma} c_\sigma \;>\; \left(\tfrac{2}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot \mathrm{Nm}(\mathfrak{a}).}$$

Then there exists an element $a \in \mathfrak{a} \smallsetminus \{0\}$ with the property

$$\forall \sigma \in \Sigma\colon\; |\sigma(a)| < c_\sigma.$$

Proof: $X := \left\{ (x_j)_j \;\middle|\; \begin{array}{l} \forall j = 1..r : |x_j| < c_{\sigma_j} \\ \forall j = 1...s : |x_{r+j} + i y_{r+s+j}| < c_{\sigma_{r+j}} \end{array} \right\}$

$\Rightarrow X \cap j(\mathfrak{a}) = \{ j(a) \mid a \in \mathfrak{a} \text{ and } : \forall \sigma \in \Sigma : |\sigma(a)| < c_\sigma \}$

$\mathrm{vol}(X) = \mathrm{vol}\left(\bigtimes_{j=1}^{r}]-c_{\sigma_j}, c_{\sigma_j}[\times \bigtimes_{j=1}^{s} B_{c_{\sigma_{r+j}}}(0) \right)$

$= \prod_{j=1}^{r} (2 c_{\sigma_j}) \cdot \prod_{j=1}^{s} (2 \cdot \pi \cdot c_{\sigma_{r+j}}^2) = 2^{r+s} \cdot \pi^s \cdot \prod_{\sigma\in\Sigma} c_\sigma$

$\leadsto \quad \mathrm{vol}(X) > 2^n \cdot \sqrt{|d_K|} \cdot N_m(\mathfrak{a}) \qquad n = r + 2s$

$$\iff \frac{\pi^s}{2^s} \cdot \prod_{\sigma \in \Sigma} c_\sigma > \sqrt{|d_K|} \cdot N_m(\mathfrak{a}).$$

$$\iff \prod_\sigma c_\sigma > \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot N_m(\mathfrak{a}). \qquad \underline{\text{qed}}.$$

4.3 Finiteness of the class group

Theorem 4.3.1: For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ there exists an element $a \in \mathfrak{a} \smallsetminus \{0\}$ with

$$|\mathrm{Nm}_{K/\mathbb{Q}}(a)| \leqslant \left(\tfrac{2}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot \mathrm{Nm}(\mathfrak{a}).$$

Proof: Choose $c_\sigma > 0$ with $c_\sigma = c_{\bar\sigma}$ and $\prod_\sigma c_\sigma = \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot \mathrm{Nm}(\mathfrak{a})$.

Then $\forall \varepsilon > 0 \; \exists a \in \mathfrak{a} \smallsetminus \{0\}: \; \forall \sigma: \; |\sigma(a)| < c_\sigma + \varepsilon$.

$\Rightarrow \; |\mathrm{Nm}_{K/\mathbb{Q}}(a)| < \prod_\sigma (c_\sigma + \varepsilon)$.

Let $\varepsilon \to 0$. qed.

Proposition 4.3.2: Every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subset \mathcal{O}_K$ with

$$\mathrm{Nm}(\mathfrak{a}) \leqslant \left(\tfrac{2}{\pi}\right)^s \cdot \sqrt{|d_K|}.$$

Proof: Take $\mathfrak{a}$ fractional ideal,

$a \in \mathfrak{a}^{-1} \setminus \{0\}$ with $|\mathrm{Nm}_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot \mathrm{Nm}(\mathfrak{a}^{-1})$.

$\Rightarrow$ $\mathrm{Nm}(a \cdot \mathfrak{a}) = \mathrm{Nm}((a)) \cdot \mathrm{Nm}(\mathfrak{a}) = |\mathrm{Nm}_{K/\mathbb{Q}}(a)| \cdot \mathrm{Nm}(\mathfrak{a}^{-1})^{-1}$

$\leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_K|}$.

$\mathcal{O}_K \supset a\mathfrak{a} \sim \mathfrak{a}$.

qed.

Theorem 4.3.3: The class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite.

Proof: There are only fin. many ideals $\mathfrak{a} < \mathcal{O}_K$ with $[\mathcal{O}_K : \mathfrak{a}] \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_K|}$

qed.

Example: The ideal class group of $K := \mathbb{Q}(\sqrt{-23}\,)$.

$\mathcal{O}_K = \mathbb{Z}\Big[\underbrace{\frac{1+\sqrt{-23}}{2}}_{\beta}\Big]$

$r = 0,\ s = 1$

$d_K = -23$

$\frac{2}{\pi}\cdot\sqrt{23} = 3.05.$

$\Rightarrow$ Enough to test $\mathrm{Nm}(\mathfrak{a}) \leq 3.$

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

$\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - X + 6)$

$2\beta - 1 = \sqrt{-23}$

$4\beta^2 - 4\beta + 1 = -23$

$4\beta^2 - 4\beta + 24 = 0$

$\beta^2 - \beta + 6 = 0$

$\mathrm{Nm}(\mathfrak{a}) = 1 \Rightarrow \boxed{\mathfrak{a} = (1)}$

$\mathrm{Nm}(\mathfrak{a}) = 2 \Rightarrow \mathfrak{a}$ prime ideal above $(2) \subset \mathbb{Z}$

$\mathcal{O}_K/(2) \cong \mathbb{Z}[X]/(X^2 + X + 6, 2)$

$= \mathbb{F}_2[X]/(X^2 \; X + 6)$

$= \mathbb{F}_2[X]/(X\cdot(X-1))$

$\cong \mathbb{F}_2 \times \mathbb{F}_2$

$\boxed{\mathfrak{a} = (2, \beta) \quad \text{or} \quad (2, \beta - 1)}$

$\mathrm{Nm}(\mathfrak{a}) = 3 \Rightarrow \mathfrak{a}$ above $(3) \subset \mathbb{Z}$

$\mathcal{O}_K/(3) = \mathbb{F}_3[X]/(X(X-1))$

$\boxed{\mathfrak{a} = (3, \beta), \quad (3, \beta - 1)}$

$(2, \beta)\cdot(2, \beta - 1) = (4, 2\beta, 2(\beta - 1), \beta(\beta - 1)) = (2, \beta^2 - \beta) = (2, -6) = (2).$

$(3, \beta)\cdot(3, \beta - 1) = (3).$

$$(2,\beta)^2 = (4, 2\beta, \beta^2) = (4, 2\beta, \beta-6) = (4, \beta+2)$$

$$6 = \beta - \beta^2 \Rightarrow (2)\cdot(3) = (\beta)\cdot(1-\beta)$$

$$(2,\beta)\cdot(3,\beta) = (6, 2\beta, 3\beta, \beta^2) = (\beta-\beta^2, \beta) = (\beta) \Rightarrow [(3,\beta)] = [(2,\beta-1)]$$

$$(2,\beta-1)\cdot(3,\beta-1) = (\beta-1). \Rightarrow [(3,\beta-1)] = [(2,\beta)].$$

$$(2,\beta)^3 = (2,\beta)(4,\beta+2) = (8, 4\beta, 2\beta+4, \beta^2+2\beta) = (8, 2\beta+4, \beta-6+2\beta)$$

$$= (8, 2\beta+4, 3\beta-6) = (8, 2\beta+4, \beta-10) = (8, 2\beta-4, \beta-2) = (8, \beta-2). = (\beta-2).$$

$$\boxed{(\beta-2)(\bar\beta-2) = (\beta-2)(1-\beta-2) = (\beta-2)(-\beta-1) = -\beta^2+2\beta-\beta+2 = -(\beta-6)+\beta+2 = 8}$$

If $(2,\beta) = (a+b\cdot\beta)$ with $a,b\in\mathbb{Z}$

$$\Rightarrow 2 = N((2,\beta)) = |N_{K/\mathbb{Q}}(a+b\beta)| = (a+b\beta)\cdot(a+b\bar\beta)$$

$$= \left|\left(a+\tfrac{b}{2}\right) + \tfrac{b}{2}\cdot\sqrt{-23}\right|^2$$

$$= \left(a+\tfrac{b}{2}\right)^2 + \left(\tfrac{b}{2}\right)^2\cdot 23.$$

$$\Rightarrow 8 = \underbrace{(2a+b)^2}_{\in\mathbb{Z}^2} + \underbrace{b^2}_{\in\mathbb{Z}^2}\cdot 23 \Rightarrow b=0 \Rightarrow 8 = (2a)^2 \Rightarrow ↯.$$

So $(2,\beta)$ is not principal.

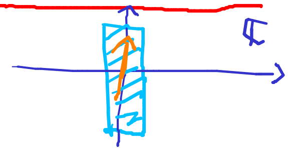
Conclusion: $Cl(\mathcal{O}_K)$ cyclic of order 3 with generator $[(2,\beta)]$.

up to $\cong$

d

4.4 Discriminant bounds

Theorem 4.4.1: For any n and c there exist at most finitely many number fields $K/\mathbb{Q}$ of degree n and with $|d_K| \leqslant c$.



Proof: Let K be such a field.

For $t>0$ set $Y_t := \left\{ (y_i) \in \mathbb{R}^n \;\middle|\; \begin{array}{ll} |y_{1+s}| < t & \text{if } \sigma_1 \text{ is nonreal} \\ |y_1| < t & \text{if } \sigma_1 \text{ is real} \\ |y_i| < \tfrac{1}{2} & \text{for all other } i \end{array} \right\}$

$\Rightarrow \operatorname{vol}(Y_t) = 2t \cdot 2^s$ because the scalar product is $|(y_i)|^2 = \sum_{i=1}^{n} y_i^2 + 2\sum_{i=r+1}^{n} y_i^2$.

Take $t := 2^{n-s} \cdot \sqrt{c} \Rightarrow \operatorname{vol}(Y_t) = 2^{n+1} \cdot \sqrt{c} > 2^n \cdot \sqrt{|d_K|} = 2^n \cdot \operatorname{covol}(j(\mathcal{O}_K))$

Minkowski $\Rightarrow \exists\, \alpha \in \mathcal{O}_K \setminus \{0\}$ with $j(\alpha) \in Y_t$.

i.e.:

σ_1 real $\Rightarrow |\sigma_1(\alpha)| < t$.	$|\sigma_1(\alpha)| < t$
σ_1 nonreal $\Rightarrow |\sigma_1(\alpha)|^2 < (t^2 + \frac{1}{4}) \cdot 2$	$|\sigma_1(\alpha)| < 2t$
$\sigma \neq \sigma_1, \bar\sigma_1$ real $\Rightarrow |\sigma(\alpha)| < 1/2$	$|\sigma(\alpha)| < 1$
$\sigma \neq \sigma_1, \bar\sigma_1$ nonreal $\Rightarrow |\sigma(\alpha)|^2 < \frac{1}{2} \cdot 2 = 1$	$|\sigma(\alpha)| < 1$

Also $\alpha \in \mathcal{O}_K \Rightarrow \operatorname{Nm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \setminus \{0\} \Rightarrow 1 \leq |\operatorname{Nm}_{K/\mathbb{Q}}(\alpha)| = \prod_{\sigma \in \Sigma} |\sigma(\alpha)|$.

So $|\sigma_1(\alpha)| > 1 > |\sigma(\alpha)|$ for all $\sigma \neq \sigma_1, \bar\sigma_1$.

$\Rightarrow$ particular $\sigma_1(\alpha) \neq \sigma(\alpha)$ for all $\sigma \neq \sigma_1, \bar\sigma_1$.

If σ_1 is nonreal, then $y_{1+s} = \operatorname{Im}(\sigma_1(\alpha))$ and $|\operatorname{Re}(\sigma_1(\alpha))| = |y_1| < \frac{1}{2} \Rightarrow y_{1+s} \neq 0$.

so $\forall \sigma \neq \sigma_1 : \sigma(a) \neq \sigma(a_1)$.

$\Rightarrow K = \mathbb{Q}(a)$.

$f(X) := \prod_{\sigma \in \Sigma_n} (X - \sigma(a))$ is the min. pol. of a over $\mathbb{Q}$.

$$= \sum_{j=0}^{n} a_j X^j \quad \text{with } a_j \in \mathbb{Z}.$$

and $|a_j| \leq \binom{n}{j} \cdot (2t)^{n-j}$.

$\Rightarrow$ fin. many possibilities for each a_j.

$\Rightarrow$. - - — — — - — f - .

. — — — - - K.

qed.