Reminder:

Fix an odd prime ℓ and set $K := \mathbb{Q}(\mu_\ell)$ and $\zeta := e^{\frac{2\pi i}{\ell}}$.

Definition 3.7.1: The *Legendre symbol* of an integer a with respect to ℓ is

$$\left(\frac{a}{\ell}\right) := \begin{cases} 0 & \text{if } a \equiv 0 \bmod (\ell), \\ +1 & \text{if } a \equiv b^2 \bmod (\ell) \text{ for some } b \in \mathbb{Z} \setminus \ell\mathbb{Z}, \\ -1 & \text{otherwise.} \end{cases}$$

Definition 3.7.3: The *Gauss sum* associated to the prime ℓ is $g_\ell := \sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right) \cdot \zeta^a$.

Proposition 3.7.4: The Gauss sum satisfies $g_\ell^2 = \ell^* := (-1)^{\frac{\ell-1}{2}} \ell$.

Proposition 3.7.6: For any distinct odd primes ℓ, p we have $(\frac{\ell^*}{p}) = (\frac{p}{\ell})$.

Proof: $g_\ell^p = g_\ell \cdot (g_\ell^2)^{\frac{p-1}{2}} = g_\ell \cdot (\ell^*)^{\frac{p-1}{2}} \equiv g_\ell \cdot \left(\frac{\ell^*}{p}\right) \mod p\mathcal{O}_K$.

$$g_\ell^p = \Big(\sum_{a\in\mathbb{F}_\ell^\times} \left(\tfrac{a}{\ell}\right) \zeta^a\Big)^p \equiv \sum_{a\in\mathbb{F}_\ell^\times} \left(\tfrac{a}{\ell}\right) \zeta^{ap} = \sum_{b\in\mathbb{F}_\ell^\times} \left(\tfrac{b p^{-1}}{\ell}\right) \cdot \zeta^b = \left(\tfrac{p^{-1}}{\ell}\right) \cdot \sum_{b\in\mathbb{F}_\ell^\times} \left(\tfrac{b}{\ell}\right) \cdot \zeta^b$$

$$= \left(\tfrac{p}{\ell}\right) \cdot g_\ell .$$

Multiply by g_ℓ $\Rightarrow$ $\ell^* \left(\frac{\ell^*}{p}\right) = g_\ell^2 \cdot \left(\frac{\ell^*}{p}\right) \equiv g_\ell^2 \cdot \left(\frac{p}{\ell}\right) = \ell^* \cdot \left(\frac{p}{\ell}\right) \mod p\mathcal{O}_K$

ℓ^*, p coprime $\Rightarrow$ $\left(\frac{\ell^*}{p}\right) \equiv \left(\frac{p}{\ell}\right) \mod p\mathcal{O}_K$.

$\in \{\pm 1\}$ $\Rightarrow$ and $(p\mathcal{O}_K \cap \mathbb{Z}) = (p\mathbb{Z})$.

$p \geq 3$ $\Rightarrow$ $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$.

qed.

Theorem 3.7.7: *(Gauss Quadratic Reciprocity Law)*

✓ (a) For any distinct odd primes ℓ, p we have $\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{(p-1)(\ell-1)}{4}}$.

✓ (b) For any odd prime ℓ we have $\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}}$. *(First supplement)*

✓ (c) For any odd prime ℓ we have $\left(\frac{2}{\ell}\right) = (-1)^{\frac{\ell^2-1}{8}}$. *(Second supplement)*

Proof (a): $\ell = (-1)^{\frac{\ell-1}{2}} \cdot \ell^*$

$$\Rightarrow \left(\frac{\ell}{p}\right)\cdot\left(\frac{p}{\ell}\right) = \left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}} \cdot \underbrace{\left(\frac{\ell^*}{p}\right)\cdot\left(\frac{p}{\ell}\right)}_{1} = \left((-1)^{\frac{p-1}{2}}\right)^{\frac{\ell-1}{2}}.$$

qed

(b) Exercise.

Example:

$$\left(\frac{127}{163}\right) = (-1)^{63\cdot 81}\cdot\left(\frac{163}{127}\right) = -\left(\frac{36}{127}\right) = -\left(\frac{6^2}{127}\right) = -1.$$

$$\left(\frac{892}{997}\right) = \left(\frac{2^2\cdot 223}{997}\right) = \left(\frac{223}{997}\right) = (-1)^{111\cdot 498}\cdot\left(\frac{997}{223}\right) = +\left(\frac{105}{223}\right) =$$

$$= \left(\frac{3}{223}\right)\cdot\left(\frac{5}{223}\right)\cdot\left(\frac{7}{223}\right) = \underbrace{(-1)^{1\cdot 111}}_{-1}\cdot\left(\frac{223}{3}\right)\cdot\underbrace{(-1)^{2\cdot 111}}_{+1}\cdot\left(\frac{223}{5}\right)\cdot\underbrace{(-1)^{3\cdot 111}}_{-1}\cdot\left(\frac{223}{7}\right)$$

$$= +\underbrace{\left(\frac{1}{3}\right)}_{1}\cdot\left(\frac{3}{5}\right)\cdot\left(\frac{-1}{7}\right) = \underbrace{(-1)^{1\cdot 2}}_{+1}\cdot\left(\frac{5}{3}\right)\cdot\underbrace{(-1)^{3}}_{-1} = -\underbrace{\left(\frac{2}{3}\right)}_{-1} = 1$$

$892 = 2\cdot 446$
$= 4\cdot 223$

$997 - 892 = 105$

Nachtrag: 364^2 \equiv 892 \bmod 997

4 Additive Minkowski theory

Reminder:

Fix a finite extension $K/\mathbb{Q}$ of degree n. Abbreviate $\Sigma := \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ and set

$$\begin{aligned} r &:= \text{ the number of } \sigma \in \Sigma \text{ with } \sigma(K) \subset \mathbb{R}, \\ s &:= \text{ the number of } \sigma \in \Sigma \text{ with } \sigma(K) \not\subset \mathbb{R}, \text{ up to complex conjugation.} \end{aligned}$$

Proposition 3.4.1: We have $r + 2s = n$.

Proposition 3.4.2: We have ring isomorphisms

$$\begin{array}{ccc} K \otimes_{\mathbb{Q}} \mathbb{C} & \xrightarrow{\sim} & K_{\mathbb{C}} := \prod_{\sigma \in \Sigma} \mathbb{C}, \\ \cup & & \cup \\ K \otimes_{\mathbb{Q}} \mathbb{R} & \xrightarrow{\sim} & K_{\mathbb{R}} := \left\{ (z_\sigma)_\sigma \in K_{\mathbb{C}} \,\middle|\, \forall \sigma \in \Sigma \colon z_{\bar{\sigma}} = \bar{z}_\sigma \right\}. \\ x \otimes z & \longmapsto & (\sigma(x) z)_\sigma . \end{array}$$

The map $x \mapsto x \otimes 1$ induces an embdding $j \colon K \hookrightarrow K_{\mathbb{R}}$.

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

Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings and $\sigma_{r+1}, \ldots, \sigma_n$ the non-real embeddings such that $\bar{\sigma}_{r+j} = \bar{\sigma}_{r+j+s}$ for all $1 \leqslant j \leqslant s$.

Proposition 3.4.4: We have an isomorphism of $\mathbb{R}$-vector spaces

$$K_{\mathbb{R}} \xrightarrow{\sim} \mathbb{R}^n, \quad (z_\sigma)_\sigma \longmapsto \big(z_{\sigma_1}, \ldots, z_{\sigma_r}, \mathrm{Re}\, z_{\sigma_{r+1}}, \ldots, \mathrm{Re}\, z_{\sigma_{r+s}}, \mathrm{Im}\, z_{\sigma_{r+1}}, \ldots, \mathrm{Im}\, z_{\sigma_{r+s}}\big).$$

4.1 Euclidean embedding

We endow $K_\mathbb{C} := \mathbb{C}^\Sigma$ with the standard hermitian scalar product

$$\big\langle (z_\sigma)_\sigma, (w_\sigma)_\sigma \big\rangle := \sum_{\sigma\in\Sigma} \bar{z}_\sigma w_\sigma.$$

Proposition 4.1.1: Its restriction to $K_\mathbb{R} \times K_\mathbb{R}$ has values in $\mathbb{R}$ and turns $K_\mathbb{R}$ into a euclidean vector space.

Proof: $(z_\sigma)_\sigma, (w_\sigma)_\sigma \in K_\mathbb{R} \Rightarrow z_{\bar\sigma} = \overline{z_\sigma}$ and $w_{\bar\sigma} = \overline{w_\sigma}$.

$$\Rightarrow \overline{\sum_{\sigma\in\Sigma} \bar{z}_\sigma \cdot w_\sigma} = \sum_{\sigma\in\Sigma} z_\sigma \cdot \overline{w_\sigma} = \sum_{\tau\in\Sigma} z_{\bar\tau} \cdot \overline{w_{\bar\tau}} = \sum_{\tau\in\Sigma} \bar{z}_\tau \cdot w_\tau \quad \text{qed.}$$

Proposition 4.1.2: Under the isomorphism of Proposition 3.4.4 this scalar product on $K_\mathbb{R}$ corresponds to the following scalar product on $\mathbb{R}^n$:

$$\big\langle (x_j)_j, (y_j)_j \big\rangle := \sum_{i=1}^{r} x_j y_j + \sum_{i=r+1}^{n} 2x_j y_j.$$

Proof left to the conscientious reader!

4.2 Lattice bounds

$j(x) = (\sigma_i(x))_i$

Proposition 4.2.1: For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we have

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

Proof: $a_1, \dots, a_n$ $\mathbb{Z}$-basis of $\mathfrak{a}$

$T = (\sigma_i(a_j))_{i,j=1}^n$

$\det(T)^2 = \operatorname{disc}(\mathfrak{a})$

$\Gamma := j(\mathfrak{a})$ has $\mathbb{Z}$-basis $j(a_1), \dots, j(a_n)$

$\operatorname{vol}(K_{\mathbb{R}}/j(\mathfrak{a}))^2 = \det(\langle j(a_i), j(a_k)\rangle)_{i,k=1}^n$

$= \det(\overline{T} \cdot T^T) = |\det(T)|^2$

$\operatorname{vol} = |\det(T)| = \sqrt{\operatorname{disc}(\mathfrak{a})}$

$\mathfrak{a} \subset \mathfrak{b} \Rightarrow \operatorname{disc}(\mathfrak{b}) \cdot [\mathfrak{b} : \mathfrak{a}]^2 = \operatorname{disc}(\mathfrak{a}) = \operatorname{disc}(\mathfrak{b}) \cdot \frac{\operatorname{Nm}(\mathfrak{a})^2}{\operatorname{Nm}(\mathfrak{b})^2}$ $\Rightarrow \operatorname{disc}(\mathfrak{a}) = \operatorname{disc}(\mathcal{O}_K) \cdot \operatorname{Nm}(\mathfrak{a})^2.$

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

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

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

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