$[K/\mathbb{Q}] = n$

$\Sigma = \mathrm{Hom}(K, \mathbb{C})$.

$\mathbb{C}^\times \cong S^1 \times \mathbb{R}$

5 Multiplicative Minkowski theory

5.1 Roots of unity

Lemma 5.1.1: We have a short exact sequence

$$1 \longrightarrow (S^1)^\Sigma \longrightarrow K_\mathbb{C}^\times = (\mathbb{C}^\times)^\Sigma \xrightarrow{\ \ell\ } \mathbb{R}^\Sigma \longrightarrow 0,$$
$$(z_\sigma)_\sigma \longmapsto (\log|z_\sigma|)_\sigma.$$

$$1 \to \ker \to \mathcal{O}_K^\times \longrightarrow \ell(\mathcal{O}_K^\times) \to 0$$

$\ker$ = finite.

$\ell(\mathcal{O}_K^\times) = \Gamma$ = torsion free

Set $\Gamma := \ell(\mathcal{O}_K^\times)$ and let $\mu(K)$ denote the group of elements of finite order in $K^\times$. This is $\subset \mathcal{O}_K^\times$

Proposition 5.1.2: The group $\mu(K)$ is a finite subgroup of $\mathcal{O}_K^\times$ and we have a short exact sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \longrightarrow \Gamma \longrightarrow 0.$$

Proof: $\mathcal{O}_K \subset K_\mathbb{C}^\times$ is discrete.

$\Rightarrow \ker(\ell|\mathcal{O}_K^\times)$ is discrete and compact $\Rightarrow$ finite.

qed.

Proposition 5.1.3: The group $\mu(K)$ is cyclic of even order.

Proof: $\mu(K) \ni \pm 1 \Rightarrow |\mu(K)| =: m$ even.

$\{\zeta \in \mathbb{C}^\times \mid \zeta^m = 1\}$ = cyclic of order m. qed.

Example 5.1.4: For any squarefree $d \in \mathbb{Z} \setminus \{1\}$ we have

$$\mu(\mathbb{Q}(\sqrt{d})) = \begin{cases} \text{cyclic of order 6 if } d = -3, \\ \text{cyclic of order 4 if } d = -1, \\ \text{cyclic of order 2 otherwise.} \end{cases}$$

$\mu(K)$ order m $\Rightarrow$ $\mathbb{Q}(\mu_m) \subset K$.

$[\mathbb{Q}(\mu_m)/\mathbb{Q}] = |(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$

$2 \mid m$

$\varphi(m) \leq 2 \Leftrightarrow m = 2, 4, 6.$

$\mathbb{Q}(\mu_6) = \mathbb{Q}(\sqrt{-3})$

$\frac{1+\sqrt{-3}}{2}$

$\mathbb{Q}(\mu_4) = \mathbb{Q}(i)$

5.2 Units

Lemma 5.2.1: The group Γ is a lattice in $\mathbb{R}^\Sigma$.

Proof: For any compact subset $X \subset \mathbb{R}^\Sigma$: $\ell^{-1}(X) \subset (\mathbb{C}^\times)^\Sigma$ is compact $\Rightarrow$ bounded in $\mathbb{C}^\Sigma$

$\Rightarrow \mathcal{O}_K^\times \cap \ell^{-1}(X) \subset \mathcal{O}_K \cap \ell^{-1}(X) =$ finite. So $\Gamma \cap X$ finite. qed.

Consider the homomorphisms

$$\begin{aligned} \mathrm{Nm}\colon \quad K_{\mathbb{C}}^\times = (\mathbb{C}^\times)^\Sigma &\longrightarrow \mathbb{C}^\times, \quad (z_\sigma)_\sigma \longmapsto \textstyle\prod_{\sigma\in\Sigma} z_\sigma \\ \mathrm{Tr}\colon \quad (\mathbb{R}^\times)^\Sigma &\longrightarrow \mathbb{R}, \quad (t_\sigma)_\sigma \longmapsto \textstyle\sum_{\sigma\in\Sigma} t_\sigma \end{aligned}$$

Lemma 5.2.2: We have a commutative diagram

$$\begin{tikzcd} & & & \Gamma \arrow[d, phantom, "\subset"] \\ \mathcal{O}_K^\times \arrow[r, hook] \arrow[d, "\mathrm{Nm}"'] \arrow[urrr, two heads, bend left] & K^\times \arrow[r, hook, "j"] \arrow[d, "\mathrm{Nm}"'] & (K_{\mathbb{C}})^\times \arrow[r, two heads, "\ell"] \arrow[d, "\mathrm{Nm}"'] & \mathbb{R}^\Sigma \arrow[d, "\mathrm{Tr}"'] \\ \{\pm 1\} \arrow[r, hook] & \mathbb{Q}^\times \arrow[r, hook] & \mathbb{C}^\times \arrow[r, two heads, "\log|\ |"] & \mathbb{R} \end{tikzcd}$$

$x \longmapsto (\sigma(x))_\sigma$

$\prod_{\sigma\in\Sigma} \sigma(x)$

$\log|\bar{\sigma}(x)| = \log|\sigma(x)|$

Consider the $\mathbb{R}$-subspaces

$$\begin{aligned} (\mathbb{R}^\Sigma)^+ &:= \left\{(t_\sigma)_\sigma \in \mathbb{R}^\Sigma \;\middle|\; \forall \sigma\colon t_{\bar\sigma} = t_\sigma\right\}, \\ H &:= \ker\big(\mathrm{Tr}\colon (\mathbb{R}^\Sigma)^+ \to \mathbb{R}\big). \end{aligned}$$

Lemma 5.2.3: We have $\Gamma \subset H$ and $\dim_\mathbb{R}(H) = r + s - 1$.

$$H = \left\{ (t_1, \ldots, t_r, t_{r+1}, \ldots, t_{r+s}, t_{r+1}, \ldots, t_{r+s}) \in \mathbb{R}^n \;\middle|\; \sum = 0 \right\}$$

zed.

5.3 Dirichlet's unit theorem

Theorem 5.3.1: The group Γ is a complete lattice in H.

Theorem 5.3.2: The group $\mathcal{O}_K^\times$ is isomorphic to $\mu(K) \times \mathbb{Z}^{r+s-1}$.

Caution 5.3.3: The isomorphism is uncanonical.

Proof: $1 \to \mu(K) \to \mathcal{O}_K^\times \to \Gamma \cong \mathbb{Z}^{r+s-1} \to 0$.

lift generators of Γ to $\varepsilon_1, \dots, \varepsilon_{r+s-1}$

$\Rightarrow \mathcal{O}_K^\times = \mu(K) \times \varepsilon_1^{\mathbb{Z}} \times \dots \times \varepsilon_{r+s-1}^{\mathbb{Z}}$. qed.

Corollary 5.3.4: The group $\mathcal{O}_K^\times$ is finite if and only if K is $\mathbb{Q}$ or imaginary quadratic.

Proof: $\mathcal{O}_K^\times$ finite $\Leftrightarrow$ $r+s-1=0$ $\Leftrightarrow$ $(r,s)=(1,0)$: $K=\mathbb{Q}$

$r+2s=n$ $\qquad (0,1)$: K imag. quadratic

Corollary 5.3.5: The group $\mathcal{O}_K^\times$ has $\mathbb{Z}$-rank 1 if and only if $(r,s) \in \{(2,0),(1,1),(0,2)\}$. In that case we have

$2 \qquad 3 \qquad 4$

K real quadratic

$$\mathcal{O}_K^\times = \mu(K) \times \varepsilon^{\mathbb{Z}}$$

for some unit ε of infinite order.

Definition 5.3.6: Any choice of such ε is then called a *fundamental unit.*

5.4 The real quadratic case

Suppose that $K = \mathbb{Q}(\sqrt{d})$ for a squarefree $d > 1$ and choose an embedding $K \hookrightarrow \mathbb{R}$.

Thm $\mathcal{O}_K^\times = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$.

Fact 5.4.1: There is a unique choice of fundamental unit $\varepsilon > 1$.

Proposition 5.4.2: If $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, then

(a) $\mathcal{O}_K^\times = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z},\ a^2 - b^2 d = \pm 1\}$.

(b) $\mathcal{O}_K^\times \cap \mathbb{R}^{>1} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z},\ a^2 - b^2 d = \pm 1,\ a, b > 0\}$.

(c) The fundamental unit $\varepsilon > 1$ is the element $a + b\sqrt{d} \in \mathcal{O}_K^\times \cap \mathbb{R}^{>1}$ as in (b) with the smallest value for a, or equivalently for b.

Prf:

(a) $a+b\sqrt{d} \in \mathcal{O}_K^\times \Rightarrow a-b\sqrt{d} \in \mathcal{O}_K^\times \Rightarrow a^2-b^2d = \mathrm{Nm}_{K/\mathbb{Q}}(a+b\sqrt{d}) \in \mathbb{Z}^\times = \{\pm 1\}$.

Conversely if $a^2-b^2d = \pm 1$ then $(a+b\sqrt{d})(a-b\sqrt{d}) \in \mathcal{O}_K^\times \Rightarrow a+b\sqrt{d} \in \mathcal{O}_K^\times$.

(b) $\varepsilon = a+b\sqrt{d} \in \mathcal{O}_K^\times \Rightarrow \{\pm\varepsilon^{\pm 1}\} = \{\pm a \pm b\sqrt{d} \mid \text{all signs}\}$

$\Rightarrow \varepsilon \geq 1 \Leftrightarrow a, b \geq 0$. If $b = 0$ then $a = \pm 1 \Rightarrow \varepsilon = \pm 1$.
If $a = 0$ then $-b^2 d = \pm 1 \Rightarrow$ ↯ because $d > 1$.

So $\varepsilon > 1 \Leftrightarrow a, b > 0$.

(c)

qed

$\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \supset \mathbb{Z}[\sqrt{d}]$ $\qquad$ $\mathbb{Z}[\sqrt{d}] \supset \mathbb{Z}[n\sqrt{d}]$.

Theorem 5.4.3: For any squarefree integer $d > 1$ there are infinitely many solutions $(a, b) \in \mathbb{Z}^2$ of the diophantine equation $a^2 - b^2 d = 1$.

Proof: $\varepsilon = a + b\sqrt{d} \in \mathcal{O}_K^\times$
$\boxed{\text{if } d \not\equiv 1 \, (4)}$ $\varepsilon > 1 \Rightarrow \forall k \geq 1$: $Nm(\varepsilon^{2k}) = Nm(\varepsilon)^{2k} = 1$.

Remark 5.4.4: The equation $a^2 - b^2 d = -1$ may or may not have a solution $(a, b) \in \mathbb{Z}^2$. But if it has a solution, it has infinitely many.

ε^{2k+1}

$D = \begin{cases} d & d \equiv 1 \, (4) \\ 4d & \text{else} \end{cases}$

$\Rightarrow D \geq 5$.

Proposition 5.4.5: The fundamental unit $\varepsilon > 1$ of K with discriminant D satisfies

$$\boxed{\varepsilon \;>\; \frac{\sqrt{D} + \sqrt{D-4}}{2} \;>\; 1.}$$

Consequently, if some unit of infinite order $u > 1$ is known, we have $u = \varepsilon^k$ for some $1 \leqslant k \leqslant \log(u)/\log((\sqrt{D} + \sqrt{D-4})/2)$ and one can efficiently find ε.

Proof: Let ε' be the galois conjugate of ε $\Rightarrow$ $\varepsilon > 1 > \varepsilon'$

& $K = \mathbb{Q}(\varepsilon) \Rightarrow \mathbb{Z}[\varepsilon] \subset \mathcal{O}_K \Rightarrow D = \operatorname{disc}(\mathcal{O}_K) \leq \operatorname{disc}(\mathbb{Z}[\varepsilon]) = |\varepsilon - \varepsilon'|^2$

$\Rightarrow \sqrt{D} \leq |\varepsilon - \varepsilon'| = \varepsilon - \varepsilon' \leq \varepsilon + \frac{1}{\varepsilon}$

$\varepsilon' = \frac{\pm 1}{\varepsilon}$

$\Rightarrow \varepsilon \cdot \sqrt{D} \leq \varepsilon^2 + 1$

$\Rightarrow \varepsilon^2 - \sqrt{D} \cdot \varepsilon + 1 \geq 0$

$\Leftrightarrow \underbrace{\Big(\varepsilon - \underbrace{\tfrac{\sqrt{D}+\sqrt{D-4}}{2}}_{>1}\Big)\Big(\underbrace{\varepsilon}_{>1} - \underbrace{\tfrac{\sqrt{D}-\sqrt{D-4}}{2}}_{<1}\Big)}_{} \geq 0$, $\quad \Big(\varepsilon - \tfrac{\sqrt{D}-\sqrt{D-4}}{2}\Big) > 0$

$\Leftrightarrow \varepsilon - \frac{\sqrt{D}+\sqrt{D-4}}{2} \geq 0$.

qed.

Remark 5.4.6: One can effectively find ε using continued fractions.

Example: Battle of Hastings: $13b^2+1=a^2 \iff a^2-13b^2=1$.

$K=\mathbb{Q}(\sqrt{13})$, $\mathcal{O}_K=\mathbb{Z}[\omega]$ with $\omega=\frac{1+\sqrt{13}}{2}$.

$\varepsilon := 1+\omega = \frac{3+\sqrt{13}}{2} \Rightarrow \mathrm{Nm}(\varepsilon) = \frac{3^2-13}{4} = -1$

$\Rightarrow \varepsilon^2 = \frac{9+6\sqrt{13}+13}{4} = \frac{11+3\sqrt{13}}{2} \notin \mathbb{Z}[\sqrt{13}]$

$\varepsilon^4 \notin \mathbb{Z}[\sqrt{13}]$

$\varepsilon^6 \in \mathbb{Z}[\sqrt{13}]$.

$\shortparallel$

$649+180\cdot\sqrt{13}$

$\Rightarrow \quad a+b\sqrt{d} = \varepsilon^{6k}$ for $k\geq 1$.

$\Rightarrow \quad a \geq 649 \Rightarrow a^2 \geq 649^2 \approx 421'200$

$\mathcal{O}_K^\times = \{\pm 1\}\times\varepsilon^{\mathbb{Z}}$

$\{u\in\mathcal{O}_K^\times \mid \mathrm{Nm}(u)=+1\}$
$=\{\pm 1\}\times\varepsilon^{2\mathbb{Z}}$.

$\{u\in\mathbb{Z}[\sqrt{13}]^\times \mid \mathrm{Nm}(u)=+1\}$
$=\{\pm 1\}\times\varepsilon^{6\mathbb{Z}}$.

Example: $K = \mathbb{Q}(\sqrt{3}) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$, $\varepsilon = 2+\sqrt{3}$ has $Nm(\varepsilon) = |(2+\sqrt{3})(2-\sqrt{3})| = 4-3 = 1$.

$$\Rightarrow \mathcal{O}_K^\times = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}.$$

$\mathbb{C} \supset L = \mathbb{Q}(\sqrt{3}, \sqrt{-2})$ has $(r,s) = (0,2) \Rightarrow \mathcal{O}_L^\times \cong \mu(L) \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z}$.

$\mu(L) = \{\pm 1\}$.

Write $\mathcal{O}_L^\times = \{\pm 1\} \times \delta^{\mathbb{Z}} \Rightarrow \varepsilon = \pm \delta^k$ for some $k \in \mathbb{Z} \setminus \{0\}$. WLOG $k > 0$.

$Gal(L/K) = \{id, \overline{}\} \Rightarrow \mathcal{O}_L^\times = \{\pm 1\} \times \bar{\delta}^{\mathbb{Z}} \Rightarrow \bar{\delta} = \pm \delta^{\pm 1}$.

$\Rightarrow \bar{\delta}^k = \pm (\delta^k)^{\pm 1}$

$\Rightarrow \varepsilon = \bar{\varepsilon} = \pm \varepsilon^{\pm 1}$

So $+1$

$\Rightarrow \bar{\delta} = \pm \delta \Rightarrow \bar{\delta}^2 = \delta^2 \Rightarrow \delta^2 \in K \Rightarrow \delta^2 \in \mathcal{O}_K^\times \Rightarrow k \leq 2$.

Test: $\sqrt{\pm \varepsilon} \in L$?

If $\delta \notin K$ then $\bar{\delta} = -\delta \Rightarrow \delta \in i\mathbb{R} \Rightarrow \delta^2 < 0 \Rightarrow \delta^2 = -\varepsilon$.

Test: $\sqrt{-\varepsilon} \in L$?

$\overline{\sqrt{-2}} = -\sqrt{-2} \longrightarrow \overline{(\delta \cdot \sqrt{-2})} = \delta \cdot \sqrt{-2} \Rightarrow \delta \cdot \sqrt{-2} = a + b\sqrt{3}$ $\quad a, b \in \mathbb{Q}$

integral $\quad a, b \in \mathbb{Z}$

$2(2+\sqrt{3}) = -2\varepsilon = -2\delta^2 = a^2 + 3b^2 + 2ab\sqrt{3}$ | $a = b = 1$ | $\delta = \frac{1+\sqrt{3}}{\sqrt{-2}}$ | Hence $[\mathcal{O}_L^\times : \mathcal{O}_K^\times] = 2$.

$= 4 + 2\sqrt{3}$