Explicit Methods in Algebraic Number Theory

Amalia Pizarro Madariaga
Instituto de Matemáticas
Universidad de Valparaíso, Chile
amalia.pizarro@uv.cl

1 Lecture 4 and 5

1.1 Dirichlet's Unit Theorem

Theorem 1.1. *Let K be a number field of degree n over $\mathbb{Q}$ with r_1 and r_2 the number of real and nonreal embedding over $\mathbb{C}$. Then there exist fundamental units $\varepsilon_1, \ldots \varepsilon_r$, with $r = r_1 + r_2 - 1$, such that every $\varepsilon \in \mathcal{O}_K^*$ can be written in a unique way by*

$$\varepsilon = \zeta \varepsilon_1^{n_1} \cdot \varepsilon_r^{n_r}, \; n_i \in \mathbb{Z},$$

where ζ is a root of unity in $\mathcal{O}_K$. More precisely, if W_K is the group of root of unity in $\mathcal{O}_K^*$, then W_K is finite, cyclic and $\mathcal{O}_K^* \cong W_K \times \mathbb{Z}^r$.

Imaginary Quadratic Fields

- $d \equiv 2, 3 \pmod 4$.
  In this case, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $a + b\sqrt{d} \in \mathcal{O}_K^*$ if and only if $a^2 - b^2 d = 1$.

  If $b = 0$, then $a = \pm 1$ and $\mathcal{O}_K^* \cong \{\pm 1\} \cong \mathbb{Z}_2$.

  If $b \neq 0$, then $a^2 - b^2 d \geq -d$ and $-d \leq -1$. If $d = -1$, $a^2 - b^2 d = a^2 + b^2 = 1$, then $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. Therefore, $\mathcal{O}_K^* \cong \{\pm 1, \pm i\} \cong \mathbb{Z}_4$.

- $d \equiv 1 \pmod 4$.
  In this case, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_K^*$ if and only if $a^2 - b^2 d = 4$.

  If $-d \geq 4$, then $b = 0$ and $a = \pm 2$, so $\mathcal{O}_K^* \cong \mathbb{Z}_2$.

  If $d = -3$, $a^2 - b^2 d = a^2 + 3b^2 = 4$, then $a = \pm 2$ and $b = 0$ or $a = \pm 1$ and $b = \pm 1$, so $\mathcal{O}_K^* \cong \{\pm \zeta_3, \pm \zeta_3^2, \pm 1\} \cong \mathbb{Z}_6$.

Remark 1. *$\mathcal{O}_K^*$ is finite if and only if $K = \mathbb{Q}$ or K is an imaginary quadratic field.*

Real Quadratic Fields $K \subset \mathbb{R}$ and $r_1 = 2$, so $W_K = \{\pm 1\}$ and $\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}$. Characterization of the fundamental unit:

- $d \equiv 2, 3 \pmod 4$.
  If $b = min\{\widetilde{b} : d\widetilde{b}^2 \pm 1 = a^2 : \text{ for some } a > 0\}$, then $a + b\sqrt{d}$ is a fundamental unit. (Exercise)

- $d \equiv 1 \pmod 4$.
  If $b = min\{\widetilde{b} : d\widetilde{b}^2 \pm 4 = a^2 : \text{ for some } a > 0\}$, then $a + b\sqrt{d}$ is a fundamental unit. (Exercise)

Example 1. *$\mathbb{Q}(\sqrt{3})$: $min\{\widetilde{b} : d\widetilde{b}^2 \pm 1 = a^2 :$ for some $a > 0\} = 1$ and $a = 2$, then $2 + \sqrt{2}$ is a fundamental unit.*

A different way to find fundamental units is by continued fractions.

Theorem 1.2. *Let n be the period of the continued fraction of $\sqrt{d}$ with d square free and let $C_k = p_k/q_k$ be the k-th convergent. If $d \equiv 2, 3 \pmod 4$, then $p_{n-1} + q_{n-1}\sqrt{d}$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$.*

Example 2. *In $\mathbb{Q}(\sqrt{6})$, we have that $\sqrt{6} = [2; \overline{2, 4}]$ (exercise). Then, $C_1 = \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = 2 + \frac{1}{2} = \frac{5}{2}$ and $5 + 2\sqrt{6}$ is a fundamental unit.*

1.2 Analytic Class Number Formula II

$$L(X_K, 1) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{|W_K|\sqrt{|D_K|}}.$$

Theorem 1.3. *Let K be a quadratic number field with discriminant D_K, then*

$$L(X_K, 1) = \begin{cases} \dfrac{-1}{\sqrt{D_K}} \displaystyle\sum_{r=1}^{D_K} \left(\frac{D_K}{r}\right) \log\left(\sin\frac{\pi r}{D_K}\right), & D_K > 0 \\ \dfrac{-\pi}{|D_K|^{3/2}} \displaystyle\sum_{r=1}^{|D_K|-1} \left(\frac{D_K}{r}\right) r, & D_K < 0 \end{cases}$$

Imaginary Quadratic Number Fields:

$$L(X_K, 1) = \frac{(2\pi)h_K}{|W_K|\sqrt{|D_K|}}.$$

Real Quadratic Number Fields:

$$L(X_K, 1) = \frac{2h_K \log\varepsilon}{\sqrt{D_K}},$$

where ε a fundamental unit.