Diophantine Approximation and Diophantine Equations

Amalia Pizarro Madariaga

amalia.pizarro@uv.cl

Instituto de Matemáticas
Universidad de Valparaíso

CIMPA School Serre's big image theorem for Galois representations associated to elliptic curves

Motivation

The end of the proof of Serre's theorem on the image of the Galois representations attached to elliptic curves rests on the following result:

Let K be a number field, Δ a nonzero element of K, S a finite set of places of K including the archimedean places and O_S the ring of S–integers in K. Then there are only finitely many U, V in O_S satisfying $U^3 - 27V^2 = \Delta$.

We start by reducing the proof to the finiteness of the S-unit equation $u + v = 1$ with u, v units in the ring O_S.

Number Fields and Ring of Integers

- A field K is an **algebraic number field** if is a finite extension of $\mathbb{Q}$.
- An element α in a number field will be called **algebraic integer** if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
- We denote by $\mathcal{O}_K$ the ring of algebraic integers in the number field K.
- $\mathcal{O}_K$ is a Dedekind domain.
- A **fractional ideal** of is a subset $\mathfrak{a}$ of such that $\mathfrak{a} \neq 0$ and there is $\alpha \in K$ with $\alpha\mathfrak{a}$ is an ideal of $\mathcal{O}_K$.
- the inverse of a fractional ideal $\mathfrak{a}$ of O_K is defined by

$$\mathfrak{a}^{-1} := \{\alpha \in K : \alpha\mathfrak{a} \subseteq O_K\}$$

Fractional Ideals

Theorem

Let $\mathcal{P}\left(O_K\right)$ be the collection of non-zero prime ideals of O_K.

(i) The fractional ideals of O_K form an abelian group with product and inverse as defined above, and with unit element $O_K = (1)$.

(ii) Every fractional ideal $\mathfrak{a}$ of O_K can be written in a unique way as a product of powers of prime ideals

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}(O_K)} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})},$$

where the exponents $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$ are integers, at most finitely many of which are non-zero.

(iii) A fractional ideal $\mathfrak{a}$ of O_K is contained in O_K if and only if $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ for every $\mathfrak{p} \in \mathcal{P}\left(O_K\right)$.

Discrete Valuation

For $\mathfrak{p} \in \mathcal{P}(O_K)$ we define

$$\mathrm{ord}_{\mathfrak{p}}(x) := \mathrm{ord}_{\mathfrak{p}}((x)) \quad \text{if } x \in K^*, \quad \mathrm{ord}_{\mathfrak{p}}(0) := \infty$$

It gives a surjective map $\mathrm{ord}_{\mathfrak{p}} : K \to \mathbb{Z} \cup \{\infty\}$ such that for $x, y \in K$:

- $\mathrm{ord}_{\mathfrak{p}}(xy) = \mathrm{ord}_{\mathfrak{p}}(x) + \mathrm{ord}_{\mathfrak{p}}(y);$
- $\mathrm{ord}_{\mathfrak{p}}(x + y) \geq \min\left(\mathrm{ord}_{\mathfrak{p}}(x), \mathrm{ord}_{\mathfrak{p}}(y)\right),$
- $\mathrm{ord}_{\mathfrak{p}}(x) = \infty \text{ if and only if } , x = 0.$

Therefore, $\mathrm{ord}_{\mathfrak{p}}$ defines a **discrete valuation** on K.

Discrete Valuation

(i) Let $\mathfrak{a}$ be a fractional ideal of O_K. Then

$$x \in \mathfrak{a} \Longleftrightarrow \mathrm{ord}_{\mathfrak{p}}(x) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \text{ for all } \mathfrak{p} \in \mathcal{P}\left(O_K\right).$$

In particular,

$$x \in O_K \Longleftrightarrow \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \in \mathcal{P}\left(O_K\right)$$

(ii) Let $\mathfrak{a}$ be the fractional ideal of O_K generated by a set $\mathcal{S}$. Then

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = \min\left\{\mathrm{ord}_{\mathfrak{p}}(\alpha) : \alpha \in \mathcal{S}\right\} \qquad \text{for } \mathfrak{p} \in \mathcal{P}\left(O_K\right)$$

Discriminant and Class Group

- O_K is free of rank $[K:\mathbb{Q}]\mathbb{Z}$-module. Let $\{\omega_1,\ldots,\omega_d\}$ be a $\mathbb{Z}$-basis of O_K, we define the discriminant of K and σ_1,σ_n the embeddings, we define the discriminant of K by

$$D_K := D_{K/\mathbb{Q}}(\omega_1,\ldots,\omega_d) = \left(\det\left(\sigma_i\omega_j\right)_{i,j}\right)^2.$$

- Let $I(O_K)$ the group of fractional ideals of O_K and $P(O_K)$ the subgroup of principal fractional ideals of O_K. The quotient group

$$\mathrm{Cl}(O_K) = I(O_K)/P(O_K)$$

is called the class group of K.
The class group $\mathrm{Cl}(O_K)$ is finite.

Group of units

- If $r = r_1 + r_2 - 1$. Then

$$O_K^* \cong W_K \times \mathbb{Z}^r,$$

where W_K is the multiplicative group pf roots of unity in K. In fact, there are $\varepsilon_1, \ldots, \varepsilon_r \in O_K^*$ such that every $\varepsilon \in O_K^*$ can be expressed uniquely as

$$\varepsilon = \zeta \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r}$$

where ζ is a root of unity in K and $b_1, \ldots b_r$ are integers. A set of units $\{\varepsilon_1, \ldots, \varepsilon_r\}$ as above is called a fundamental system of units for K.

- We define the **regulator** of K by

$$R_K := \mid \det \left(e_j \log \left| \varepsilon_i^{(j)} \right| \right)_{i,j=1,\ldots,r} \mid .$$

Absolute Values

Let K be an infinite field.

- An **absolute value** on K is a function $|\cdot|: K \to \mathbb{R}_{\geq 0}$ such that:
  - $|xy| = |x| \cdot |y|$ for all $x, y \in K$;
  - There is $C \geq 1$ such that $|x+y| \leq C \cdot \max(|x|, |y|)$ for all $x, y \in K$;
  - $|x| = 0$ if and only if $x = 0$.
- Two absolute values $|\cdot|_1, |\cdot|_2$ on K are called **equivalent** if there is $c > 0$ such that $|x|_2 = |x|_1^c$ for all $x \in K$.
- An absolute value $|\cdot|$ on K is called **non-archimedean** if it satisfies the ultrametric inequality

$$|x+y| \leq \max(|x|, |y|) \quad \text{for } x, y \in K$$

  and **archimedean** if it does not satisfy this inequality.

Valuations

- A **valuation** on K is a function $v : K \to \mathbb{R} \cup \{\infty\}$
  - $v(0) = \infty$,
  - $v(x) \in \mathbb{R} \quad$ for $x \in K^*$,
  - $v(xy) = v(x) + v(y), \quad$ for $x, y \in K$.
  - $v(x + y) \geq \min(v(x), v(y)) \quad$ for $x, y \in K$.
- A **discrete valuation** on K is a valuation v on K for which $v\left(K^*\right) = \mathbb{Z}$.
- $(K, |\cdot|)$ is **complete** if every Cauchy sequence of $(K, |\cdot|)$ converges.

Absolute Values on a Number Field

- A **real place** of K is a set $\{\sigma\}$ where $\sigma : K \hookrightarrow \mathbb{R}$ is a real embedding of K.
- A complex place of K is a pair $\{\sigma, \bar{\sigma}\}$ of conjugate complex embeddings $K \hookrightarrow \mathbb{C}$.
- An **infinite place** is a real or complex place.
- A **finite place** of K is a non-zero prime ideal of O_K.
- M_K^∞: set of infinite places of K
- M_K^0: set of finite places of K
- M_K: set of all places of K, i.e., $M_K := M_K^\infty \cup M_K^0$.

Absolute Values on a number Field

For every place $v \in M_K$ we have an absolute value $|\cdot|_v$ on K, given by:

$$|\alpha|_v := |\sigma(\alpha)| \quad \text{if } v = \{\sigma\} \text{ is real;}$$
$$|\alpha|_v := |\sigma(\alpha)|^2 = |\bar{\sigma}(\alpha)|^2 \quad \text{if } v = \{\sigma, \bar{\sigma}\} \text{ is complex;}$$
$$|a|_v := N_K(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(a)} \quad \text{if } v = \mathfrak{p} \text{ is a prime ideal of } O_K,$$

Let K_v be the completion of K with respect to $|\cdot|_v$. Then: $K_v = \mathbb{R}$ if v is real, $K_v = \mathbb{C}$ if v is complex, while K_v is a finite extension of $\mathbb{Q}_p$ if $v = \mathfrak{p}$ is a prime ideal of O_K.
Product Formula over K,

$$\prod_{v \in M_K} |\alpha|_v = 1 \quad \text{for } \alpha \in K^*.$$