The analytic class number formula and the distribution of ideals in a number field

Stanley Li

May 14, 2023

Abstract

Outline ACNF, show how distribution of ideals relates

Contents

Chapter 1

Background

Let $K/\mathbb{Q}$ be a finite extension of degree n, which we will refer to as a *number field*. Then K is of the form $\mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ by separability, and we can consider the embeddings $K \hookrightarrow \mathbb{C}$. These correspond to sending α to a root of its minimal polynomial in $\mathbb{C}$, and so come in conjugate pairs. Throughout this report, we write r for the number of embeddings with image in $\mathbb{R}$, and s for the number of conjugate pairs of complex embeddings, so that $n = r + 2s$.

To each such number field, we have a *ring of integers* $\mathcal{O}_K$ which plays a similar role to $\mathbb{Z} \subseteq \mathbb{Q}$, defined as the set (subring [[**reference??**]]) of $x \in K$ which are roots of monic integer polynomials. The ring of integers naturally corresponds to the number field K in that it is the maximal finitely-generated $\mathbb{Z}$-submodule of K, and the minimal subring of K admitting *unique prime ideal factorisation* (i.e. where every ideal splits as a product of prime ideals). [[**mention** $\mathrm{Frac}(\mathcal{O}_K) = K$**??**]]

In general, $\mathcal{O}_K$ does not admit unique prime factorisation, and we can quantify the failure of unique prime ideal factorisation in $\mathcal{O}_K$ by considering what proportion of ideals are principal (i.e. correspond to elements of $\mathcal{O}_K$). We do this by constructing a group of ideals under the usual multiplication.

Noting that the $\mathcal{O}_K$-submodules of $\mathcal{O}_K$ are exactly the ideals $I \subseteq \mathcal{O}_K$, we define a *fractional ideal* I to be a non-zero $\mathcal{O}_K$-submodule of K with $xI \subseteq \mathcal{O}_K$ for some $x \in \mathcal{O}_K$, so that the fractional ideals are of the form $\frac{1}{x}I$ for some $x \in \mathcal{O}_K$, $0 \neq I \subseteq \mathcal{O}_K$. In the case of $\mathcal{O}_K \subseteq K$, every fractional ideal I is *invertible* under ideal multiplication [[**Reference??**]], i.e. has a fractional ideal J with $IJ = JI = \mathcal{O}_K$, so the set of fractional ideals forms an abelian group $\mathcal{I}(\mathcal{O}_K)$. The principal fractional ideals $\mathcal{P}(\mathcal{O}_K) := \{\alpha\mathcal{O}_K \mid \alpha \in K^*\}$ are a subgroup of $\mathcal{I}(\mathcal{O}_K)$, and the failure of unique factorisation is described by the size of the quotient $\mathscr{C}(K) := \mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K)$, which we refer to as the *class group of* K. A large structure result states that the class group is finite for any number field K, and we refer to its size h_K as the *class number of* K.

The number field K has various notions of size for ideals and elements: for elements we have the *field norm*

$$\begin{aligned} N_{K/\mathbb{Q}} : K &\to \mathbb{Q} \\ \beta &\mapsto \prod_{\sigma: K \to \mathbb{C}} \sigma(\beta) \end{aligned}$$

This is well-defined since for any β, each $\sigma : \mathbb{Q}(\beta) \to \mathbb{C}$ has exactly $[K : \mathbb{Q}(\beta)]$ extensions, and so

$$N_{K/\mathbb{Q}}(\beta) = \left(\prod_{\sigma:\mathbb{Q}(\beta)\to\mathbb{C}} \sigma(\beta) \right)^{[K:\mathbb{Q}(\beta)]}$$

and this is rational as the product is $(-1)^{[\mathbb{Q}(\beta):\mathbb{Q}]}$ multiplied by the constant term of the minimal polynomial of β over $\mathbb{Q}$. We also have the *ideal norm* for ideals $0 \neq I \subseteq \mathcal{O}_K$, defined by

$$N(I) = [\mathcal{O}_K : I]$$

and this is multiplicative since $\mathcal{O}_K$ has unique factorisation.

Another important part of the structure of $\mathcal{O}_K$ is the *unit group* $\mathcal{O}_K^*$, which is dual to the ideal group in the sense that for non-zero principal ideals, $(\alpha) = (\alpha')$ if and only if $\alpha/\alpha' \in \mathcal{O}_K^*$. We can view the unit group geometrically by embedding K^* into $\mathbb{R}^{r+s}$ by choosing a single complex embedding from each conjugate pair, and noting the value of $[\mathbb{R}(\sigma(z)) : \mathbb{R}] \log |\sigma(z)|$ is the same under $\sigma \leftrightarrow \overline{\sigma}$, we can consider its image under the map

$$\begin{aligned} \mathrm{Log} : K^* &\to \mathbb{R}^{r+s} \\ z &\mapsto ([\mathbb{R}(\sigma(z)) : \mathbb{R}] \log |\sigma(z)|)_\sigma \end{aligned}$$

Under this map, the image of $\mathcal{O}_K^*$ is a lattice in the "trace-zero hyperplane"

$$\mathbb{R}_0^{r+s} := \left\{ (x_1, \ldots, x_{r+s}) \;\middle|\; \sum_{i=1}^{r+s} x_i = 0 \right\}$$

We also have a structure result for the unit group, which states that $\mathcal{O}_K^* = \mu_K \times U$, where μ_K is the group of roots of unity in K **(whose size we denote ω_K)**, and U is a free $\mathbb{Z}$-module of rank $r + s - 1$.

We can consider the ideals and the units ...

"Sizes of elements"

field norm N [in terms of embeddings]

The Dedekind zeta function (state both formulations - norms of ideals and number of ideals of each norm)

State the theorem

1.1 Geometry

Geometric interpretation $K \hookrightarrow K_{\mathbb{R}}$ (and volume), discriminant (of modules), lattices, covolume of $\mathcal{O}_K$ and ideals

Chapter 2

The analytic class number formula

2.1 Series and continuations

Lemma 1: (a_i) with $\sum a_i = O(t^\sigma)$

Lemma 1.5: Riemann zeta admits a meromorphic continuation to $\mathrm{Re}(s) > 0$, simple pole at $s = 1$ of residue 1.

Lemma 2: (a_i) with $\sum a_i = \rho t + O(t^\sigma)$, $\sigma \in [0, 1)$.

Motivation for why this is relevant

2.2 The distribution of ideals

Motivate by arguing for sufficiently nice boundary

2.2.1 Lipschitz parametrisability

Idea: count points in image of $\mathcal{O}_K$ under Log, but need nice boundary

Lemma + corollary on computing with $(n-1)$-Lipschitz parametrisable boundary.

2.2.2 Integral ideals of bounded norm

The long computation