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

Stanley Li

May 20, 2023

Abstract

We give an outline of some algebraic number theory and describe the proof that the Dedekind zeta function has a meromorphic continuation to $\mathrm{Re}(s) > 1 - 1/n$, except for a simple pole at $s = 1$, whose residue consists of many fundamental invariants of the number field, and is referred to the analytic class number formula.

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, and this is a free $\mathbb{Z}$-module of rank n. 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

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

which is multiplicative, in essence due to the fact that $\mathcal{O}_K$ admits unique prime ideal factorisation.

We can view the number field geometrically through the embeddings $K \to \mathbb{C}$, by embedding K into the n-dimensional $\mathbb{R}$-vector space $K_{\mathbb{R}} := \{(z_\sigma)_\sigma \in \prod_{\sigma:K\to\mathbb{C}} \mathbb{C} \mid z_{\overline{\sigma}} = \overline{z}_\sigma\}$ by $x \mapsto (\sigma(x))_\sigma$. We identify $K_{\mathbb{R}}$ with $\mathbb{R}^r \times \mathbb{C}^s$ by choosing one embedding from each conjugate pair: writing the embeddings as $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$, our identification is exactly $(z_\sigma)_\sigma \leftrightarrow (z_{\sigma_i})_{i=1}^{r+s}$. Volumes in $K_{\mathbb{R}}$ are induced by the standard inner product on $\prod_{\sigma:K\to\mathbb{C}} \mathbb{C} \mid z_{\overline{\sigma}} = \mathbb{C}^n$, which yields the usual volume in the components corresponding to real embeddings $K \to \mathbb{R}$, but gives twice the volume in components corresponding to conjugate pairs: writing $z_j = x_j + y_j i$ for $j = 1, 2$, the inner product in these components is given by $\langle (z_1, \overline{z_1}), (z_2, \overline{z_2}) \rangle = z_1\overline{z_2} + \overline{z_1}z_2 = 2\mathrm{Re}(z_1\overline{z_2}) = 2(x_1y_1 + x_2y_2)$.

Under this embedding, the image of $\mathcal{O}_K$ is a *lattice* (i.e. finitely generated $\mathbb{Z}$-submodule) of rank n, and we can consider its *covolume*, which is the volume of a unit grid square with respect to a basis (well-defined as a change of basis matrix between $\mathbb{Z}$-bases has $|\det(M)| = 1$). Fixing a $\mathbb{Z}$-basis $e_1, \ldots, e_n$ of $\mathcal{O}_K$, this covolume is exactly the absolute determinant of the matrix M_K with components $(M_K)_{ij} = \sigma_i(e_j)$. The quantity $\Delta_K := \det(M_K)^2$ is the *discriminant* of K, which plays a role in the distribution of prime ideals on $\mathcal{O}_K$. We thus have $\mathrm{covol}(\mathcal{O}_K) = |\Delta_K|^{1/2}$. The image of an ideal $I \subseteq \mathcal{O}_K$ then has covolume $\mathrm{covol}(I) = [\mathcal{O}_K : I]\,\mathrm{covol}(\mathcal{O}_K) = N(I)\,|\Delta_K|^{1/2}$, corresponding to the size of the quotient $\mathcal{O}_K/I$.

Another important part of the structure of $\mathcal{O}_K$ is the *unit group* $\mathcal{O}_K^*$, which we can view the unit group geometrically by embedding K^* into $\mathbb{R}^{r+s}$. We do this 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

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

which is the logarithm taken pointwise to the image of z under our previous embedding, with identical coordinates removed). Under this map, the image of $\mathcal{O}_K^*$ is a rank $(r + s - 1)$ lattice in the *trace-zero hyperplane*

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

and with respect to a basis $x_1, \ldots, x_{r+s-1}$ for the image of $\mathcal{O}_K^*$, we can consider the volume of a $(r+s-1)$-dimensional "unit grid square" (of the form $\{a_1x_1 + \ldots + a_{r+s-1}x_{r+s-1} \mid 0 \leq a_i < 1\}$). We do this by taking the measure corresponding to any coordinate projection $\pi : \mathbb{R}^{r+s} \twoheadrightarrow \mathbb{R}^{r+s-1}$ by leaving out a single coordinate. This volume is independent of projection as the projection leaving out the i^{th} coordinate corresponds to the shear on $\mathbb{R}^{r+s}$ sending $x_i \mapsto x_1 + \ldots + x_n$ and fixing the other coordinates. This volume measures the density of the units in $\mathcal{O}_K$, and we define this to be the *regulator* R_K of K.

The image of $\mathcal{O}_K^*$ under the Log map is a $(r+s-1)$-dimensional lattice, and its restriction to $\text{Log}\,|_{\mathcal{O}_K^*}$ has kernel μ_K [[**Reference**]]. This gives us a structure theorem for the unit group $\mathcal{O}_K^*$, namely that it takes the form $\mathcal{O}_K^* = \mu_K \times U$ for some free $\mathbb{Z}$-module $U \subseteq \mathcal{O}_K^*$ of rank $r+s-1$.

1.1 The Dedekind zeta function

Having outlined the geometry and structure of a number field $K/\mathbb{Q}$, We can define our main object of interest, which we can view as a natural generalisation of the Riemann zeta function.

Definition 1 (Dedekind zeta function)**.** *Let K be a number field. The* Dedekind zeta function ζ_K *is defined (formally) as the sum*

$$\zeta_K(s) := \sum_{0 \neq I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s}$$

Taking $K = \mathbb{Q}$, we find $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ as usual. Rewriting this sum over the indices $N(I) = [\mathcal{O}_K : I]$, we have

$$\zeta_K(s) = \sum_{m=1}^{\infty} \frac{|\{I \subseteq \mathcal{O}_K \mid [\mathcal{O}_K : I] = m\}|}{m^s}$$

This is a series of the form $\sum_{m=1}^{\infty} a_m m^{-s}$ where a_m counts the number of ideals of norm m, and gives us an important relation between the ideals of $\mathcal{O}_K$ of bounded norm and the values of ζ_K. Our main result is then formulated as follows.

Theorem 1 (The analytic class number formula)**.** *Let K be a number field with degree $n = r+2s$. Then the Dedekind zeta function ζ_K is holomorphic on the half-plane $Re(s) > 1$, and admits a meromorphic continuation to $Re(s) > 1-1/n$, holomorphic everywhere except for a simple pole at $s = 1$ with residue*

$$\operatorname{Res}_{s=1} \zeta_K = \frac{2^r (2\pi)^s h_K R_K}{\omega_K \sqrt{|\Delta_K|}}$$

A slightly stronger statement holds, namely that ζ_K extends to a function holomorphic everywhere in $\mathbb{C} \setminus \{1\}$, with a simple pole at $s = 1$ [[**Reference**]].

Chapter 2

The analytic class number formula

[[Mention fixing notation?]]

We begin by establishing a connection between the asymptotic distribution of ideals of bounded norm and the convergence and poles of the Dedekind zeta function, and then estimate the number of ideals with bounded norm by point-counting.

2.1 Series and continuations

Before considering a general series of the form $\sum_{m=1}^{\infty} a_m m^{-s}$ first establish these convergence results for the Riemann zeta function $\zeta(s) = \sum_{m=1}^{\infty} m^{-s}$, which will correspond to the principal term in our asymptotic formula for the ideals of bounded norm, and the pole of ζ_K at $s = 1$.

Lemma 1. *The Riemann zeta function $\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s}$ defines a holomorphic function for $Re(s) > 1$, and admits a meromorphic continuation to $Re(s) > 0$ except for a pole at $s = 1$ of residue 1.*

Proof. For $\mathrm{Re}(s) > 1$ we have $\left|\frac{1}{m^s}\right| = \frac{1}{m^{\mathrm{Re}(s)}}$, so the series $\sum_{m=1}^{\infty} \frac{1}{m^s}$ converges absolutely. We note that

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m^s} + \sum_{m=1}^{\infty} \frac{(-1)^{m+1}+1}{m^s} = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m^s} + \sum_{m=1}^{\infty} \frac{2}{2^s m^s} = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m^s} + 2^{1-s}\zeta(s)$$

and so

$$\zeta(s) = \frac{1}{1-2^{1-s}} \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m^s} \tag{2.1}$$

and that

$$\sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m^s} = \sum_{m=1}^{\infty} \frac{1}{(2m-1)^s} - \sum_{m=1}^{\infty} \frac{1}{(2m)^s}$$

Applying the mean value theorem to x^{-s} on $(2n-1, 2n)$, we have $\left|\frac{d}{dx} x^{-s}\right| = \left|-sx^{-s-1}\right| = |s|\, x^{-\mathrm{Re}(s)-1}$, and so

$$\left|\frac{1}{(2n-1)^s} - \frac{1}{(2n)^s}\right| \le \frac{|s|}{(2n-1)^{\mathrm{Re}(s)+1}}$$

and so (2.1) converges for $\mathrm{Re}(s) > 0$, $s \neq 1$. To show $\zeta(s)$ has a simple pole at $s = 1$ and compute the residue we compute $\lim_{s \to 1^+} \zeta(s)$ as a real limit. For $s > 1$ we have

$$\frac{1}{s-1} = \int_1^\infty \frac{1}{t^s} dt < \sum_{m=1}^{\infty} \frac{1}{m^s} < 1 + \int_1^\infty \frac{1}{t^s} dt = \frac{s}{s-1}$$

and so multiplying by $s-1$, we have $\mathrm{Res}_{s=1} \zeta = \lim_{s \to 1^+} (s-1)\zeta(s) = 1$, and that $(s-1)^{-1}$ is the first term in the Laurent series expansion of ζ around 1. $\square$

The previous lemma suggests the asymptotic distribution of ideals of bounded norm should scale linearly, up to some error term. The following result describes how this error term relates to the convergence of our extension of ζ_K.

Lemma 2. *Let (a_m) be a sequence of complex numbers, $\sigma \in \mathbb{R}$ and suppose that $\sum_{m=1}^t a_m = O(t^\sigma)$. Then the series $\sum_{m=1}^\infty a_m m^{-s}$ defines a holomorphic function on Re$(s) > \sigma$.*

Proof. Let $\mathrm{Re}(s) > \sigma$. Applying Abel's theorem [[**reference apostol**]] to $f(x) = x^{-s}$ and $A(x) = \sum_{m \leq x} a_m$ on $[1/2, x]$ and noting that $A(x) = 0$ for $x < 1$, we find

$$\sum_{m \leq x} a_m m^{-s} = A(x)x^{-s} - (-s) \int_{1/2}^x \frac{A(t)}{t^{s+1}} dt = A(x)x^{-s} + s \int_1^x \frac{A(t)}{t^{s+1}} dt$$

We note that $|A(x)x^{-s}| = O(x^{\sigma - \mathrm{Re}(s)})$ and $\left|A(t)/t^{s+1}\right| = O(t^{\sigma - \mathrm{Re}(s) - 1})$ and $\sigma - \mathrm{Re}(s) - 1 < -1$. Thus the right-hand side converges as $x \to \infty$, and so $\sum_{m=1}^t a_m m^{-s}$ defines a holomorphic function on $\mathrm{Re}(s) > \sigma$. $\square$

Putting these two together, we have

Lemma 3. *Let (a_m) be a sequence of complex numbers such that*

$$\sum_{m=1}^{t} a_m = \rho t + O(t^\sigma)$$

for some $\sigma \in [0, 1)$. Then $\sum_{m=1}^\infty a_m m^{-s}$ defines a holomorphic function on Re$(s) > 1$, with a meromorphic extension to Re$(s) > \sigma$ holomorphic everywhere except for a simple pole at $s = 1$ of residue ρ.

Proof. Letting $b_m = a_m - \rho$ be the error term, with $\sum_{m=1}^t b_m = O(t^\sigma)$. Then

$$\sum_{m=1}^{\infty} a_m m^{-s} = \rho \sum_{m=1}^{\infty} m^{-s} + \sum_{m=1}^{\infty} b_m m^{-s} = \rho\zeta(s) + \sum_{m=1}^{\infty} b_m m^{-s}$$

The first term is holomorphic on $\mathrm{Re}(s) > 1$ with extension to $\mathrm{Re}(s) > 0$ holomorphic everywhere except for a pole at $s = 1$, and the second term is holomorphic everywhere on $\mathrm{Re}(s) > \sigma$. Thus as $0 \leq \sigma < 1$, their sum admits a meromorphic extension to $\mathrm{Re}(s) > \sigma$ with a simple pole at $s = 1$ of residue $\rho \cdot 1 + 0 = \rho$. $\square$

2.2 The distribution of ideals

Comparing Theorem 1 to Lemma 3, we may expect that the number of ideals of norm at most t is asymptotically

$$\left(\frac{2^r(2\pi)^s h_K R_K}{\omega_K \sqrt{|\Delta_K|}}\right) t + O(t^{1-1/n})$$

and to show this, we

Ideal result to prove

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

Theorem – integral ideals of bounded norm

Corollary – ACNF

REFERENCES - ANT stevenhagen

borevich shafarevich

andrew sutherland