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

Stanley Li

June 11, 2023

Abstract

We give an exposition of the analytic class number formula, usually stated as a theorem on the convergence, poles and residues of the Dedekind zeta function of a number field K. We describe how this relates to the asymptotic distribution of ideals of bounded index, and by viewing the number field geometrically, we deduce an asymptotic formula for the ideals of bounded index.

Contents

Chapter 1

Background

We briefly outline some of the basic objects in algebraic number theory, and a more thorough treatment is given in [2]. A *number field* K is a finite extension of $\mathbb{Q}$, and it has an associated *ring of integers* $\mathcal{O}_K \subseteq K$ which plays a similar role to $\mathbb{Z} \subseteq \mathbb{Q}$, and is explicitly the set of all algebraic integers (or roots of monic integer polynomials) in K, and a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

In terms of ideal theory, we have a generalised notion of an ideal allowing denominators, namely a *fractional ideal*, which is explicitly a non-zero $\mathcal{O}_K$-submodule $I \subseteq K$ so that $xI \subseteq \mathcal{O}_K$ for some non-zero $x \in \mathcal{O}_K$. Since the $\mathcal{O}_K$-submodules of $\mathcal{O}_K$ are exactly the ideals, we can view these as "ideals with denominators", and we refer to the usual non-zero ideals $I \subseteq \mathcal{O}_K$ as *integral ideals.* It turns out that every fractional ideal is invertible under the usual ideal multiplication (with identity $\mathcal{O}_K$), so these form an abelian group $\mathcal{I}(\mathcal{O}_K)$, generated by integral ideals and their inverses, with the principal fractional ideals $\mathcal{P}(\mathcal{O}_K) = \{x\mathcal{O}_K \mid x \in K^*\}$ as a subgroup. The quotient $\mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K)$ is the *class group* $\mathrm{cl}(K)$, and we have the following structure theorem for $\mathrm{cl}(K)$.

Theorem 1 (Finiteness of the class group)**.** *Let K be a number field. Then* $\mathrm{cl}(K)$ *is a finite abelian group.*

The *class number* h_K of K is then defined as the size of $\mathrm{cl}(K)$, and can be viewed as a measure of the failure of unique factorisation in $\mathcal{O}_K$.

In terms of numerics, for $x \in K$ we have the *field norm* $N(x) = \prod_{\sigma:K\to\mathbb{C}} \sigma(x)$, which is rational as it is a symmetric polynomial in the roots of the minimal polynomial of x, and its absolute value can be viewed as a notion of size for x. This is in contrast to the *ideal norm*, defined on integral ideals as the index $\mathrm{N}(I) = [\mathcal{O}_K : I]$. This norm is multiplicative for $I \subseteq \mathcal{O}_K$, and so we can extend this to $\mathcal{I}(\mathcal{O}_K)$ by writing any fractional ideal in the form IJ^{-1} for $I, J \subseteq \mathcal{O}_K$. These two notions of norm are compatible where they coincide, in the sense that $\mathrm{N}((x)) = |N(x)|$ for any $x \in K^*$.

We can view the number field geometrically through the embeddings $K \to \mathbb{C}$ (determined by the images of α for $K = \mathbb{Q}(\alpha)$), by embedding K into the n-dimensional $\mathbb{R}$-vector space

$$K_{\mathbb{R}} := \left\{ (z_\sigma)_\sigma \in \prod_{\sigma:K\to\mathbb{C}} \mathbb{C} \mid z_{\overline{\sigma}} = \overline{z}_\sigma \right\}$$

by $\iota : x \mapsto (\sigma(x))_\sigma$, and we have a corresponding group of units $K_{\mathbb{R}}^*$ under pointwise multiplication. We identify $K_{\mathbb{R}}$ with $\mathbb{R}^r \times \mathbb{C}^s$ (and thus $K_{\mathbb{R}}^*$ with $(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$) by choosing one embedding from each conjugate pair: writing the embeddings as $\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$, our identification is exactly $(z_\sigma)_\sigma \leftrightarrow (z_{\sigma_i})_{i=1}^{r+s}$. This also yields a *geometric norm* on $K_\mathbb{R}^*$ analogous to that of the field norm, by $\mathbf{N}((z_\sigma)_{\sigma:K\to\mathbb{C}}) = \prod_{\sigma:K\to\mathbb{C}} |z_\sigma|$, and this is compatible with the field norm by $\mathbf{N}(\iota(x)) = |N(x)|$.

The volumes in $K_\mathbb{R}$ are induced by the standard inner product on $\prod_{\sigma:K\to\mathbb{C}} \mathbb{C} = \mathbb{C}^n$, 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* or finitely generated $\mathbb{Z}$-submodule of maximal rank n in $K_\mathbb{R}$, and we can consider its *covolume*, which is the volume of a *fundamental parallelepiped*

$$\left\{ \sum_{j=1}^{n} a_j e_j \mid 0 \leq a_j < 1 \right\}$$

with respect to a basis $\{e_j\}_{j=1}^n$, well-defined as $\dim_\mathbb{Z}(\iota(\mathcal{O}_K)) = \dim_\mathbb{R}(K_\mathbb{R})$, and 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 square of this determinant is called the *discriminant* Δ_K *of* K, and equals the usual polynomial discriminant of the minimal polynomial of α when $\mathcal{O}_K = \mathbb{Z}[\alpha]$. The covolume of $\mathcal{O}_K$ is thus $|\Delta_K|^{1/2}$, and the image of an ideal $I \subseteq \mathcal{O}_K$ then has covolume $\mathrm{covol}(I) = [\mathcal{O}_K : I]\,\mathrm{covol}(\mathcal{O}_K) = N(I)\,|\Delta_K|^{1/2}$, that is, the covolume of $\mathcal{O}_K$ scaled by the index or ideal norm $N(I) = [\mathcal{O}_K : I]$.

We can also view the unit group geometrically by embedding K^* into $K_\mathbb{R}^* \cong (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$. We do this by choosing a single complex embedding from each conjugate pair and mapping $x \mapsto (\sigma(x))_\sigma$. We also have the logarithm map which sends each coordinate in $K_\mathbb{R}^*$ to its absolute logarithm, under identification with $(\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$

$$\begin{aligned} \mathrm{Log} : K_\mathbb{R}^* &\to \mathbb{R}^{r+s} \\ (x_1, \ldots, x_r, z_1, \ldots, z_s) &\mapsto (\log|x_1|, \ldots, \log|x_r|, 2\log|z_1|, \ldots, 2\log|z_s|) \end{aligned}$$

where the factors of 2 correspond to how $K_\mathbb{R}$ is embedded in $\mathbb{C}^n$. 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 we can consider its covolume. 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 inverse of the shear on $\mathbb{R}^{r+s}$ sending $x_i \mapsto x_1 + \ldots + x_n$ and fixing the other coordinates, which has determinant 1. This volume intuitively measures the density of the units in $\mathcal{O}_K$, and we define this to be the *regulator* R_K of K. We also have the following structure theorem for the unit group $\mathcal{O}_K^*$, based on the fact that the Log map sends $\mathcal{O}_K^*$ to a rank $(r+s-1)$ lattice in $\mathbb{R}_0^{r+s}$.

Theorem 2 (Dirichlet's unit theorem)**.** *Let K be a number field, and μ_K be the set of roots of unity in K. Then $\mathcal{O}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$.*

That is, the unit group splits into 2 parts: a free part, i.e. a free $\mathbb{Z}$-submodule U of $\mathcal{O}_K^*$ of rank $(r+s-1)$), and the roots of unity in K.

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*

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

Taking $K = \mathbb{Q}$, we find $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ as usual. Our main result is then formulated as follows.

Theorem 3 (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*

$$\mathrm{Res}_{s=1}\, \zeta_K = \frac{2^r(2\pi)^s h_K R_K}{\omega_K \left|\Delta_K\right|^{1/2}}$$

The statement of this theorem and formula may seem slightly out of the blue, though we can heuristically reason that this formula makes sense as follows. We will show soon that if $\sum_{m=1}^{t} a_m = \rho t + O(t^\sigma)$ for $0 \leq \sigma < 1$, then the associated series $\sum a_m m^{-s}$ converges on $\mathrm{Re}(s) > 1$, and admits a continuation to $\mathrm{Re}(s) > \sigma$ holomorphic everywhere except for a simple pole at 1 of residue ρ, corresponding to the behaviour of the Riemann zeta function. Rewriting the sum ζ_K over the indices $\mathrm{N}(I) = [\mathcal{O}_K : I]$, we have

$$\zeta_K(s) = \sum_{m=1}^{\infty} \frac{|\{I \subseteq \mathcal{O}_K \mid [\mathcal{O}_K : I] = m\}|}{m^s} \tag{1.1}$$

This is a series of the form $\sum_{m=1}^{\infty} a_m m^{-s}$ where a_m is exactly the number of ideals of norm m. We have a bijection between non-zero principal ideals of norm at most t and $\{\alpha \in \mathcal{O}_K \setminus \{0\} \mid |N(\alpha)| \leq t\} / \mathcal{O}_K^*$ as $(\alpha) = (\alpha')$ if and only if $\alpha/\alpha' \in \mathcal{O}_K^*$, and intuitively we should be able to approximate the number of points of a lattice Λ (such as $\mathcal{O}_K^* \subseteq \mathbb{R}_0^{r+s}$) in the set tS as $t \to \infty$ by $|tS \cap \Lambda| = \frac{\mu(S)}{\mathrm{covol}(\Lambda)} t^n + O(t^{n-1})$, where the $O(t^{n-1})$ error term represents points near the boundary of tS.

The number of principal ideals of norm at most 1 should then be the size of $S_1 \cap \mathcal{O}_K$ where S_1 is a reasonably shaped set so that every $x \in K_{\mathbb{R}}^*$ of norm $\mathbf{N}(x) \leq 1$ can be written uniquely as a product $x_1 x_2$ for $x_1 \in S_1$, $x_2 \in \mathcal{O}_K^*$. Since scaling uniformly by $t^{1/n}$ scales n-dimensional volume by t, the number of principal ideals of norm at most t should then be counted by a set of the form $t^{1/n} S \cap \Lambda$. We thus may expect the number of ideals of norm at most t to be asymptotically $\frac{\mu(S)}{\mathrm{covol}(\Lambda)} t + O(t^{1-1/n})$, which would establish the half-plane of convergence, and suggests the $\left|\Delta_K\right|^{1/2}$ factor in the denominator of the residue corresponds exactly to $\mathrm{covol}(\mathcal{O}_K)$.

The set $S_1 \subseteq K_{\mathbb{R}}^*$ can be viewed as a multiplicative complement of $\mathcal{O}_K^*$ in the "closed unit ball" $\mathcal{B} = \{x \in K_{\mathbb{R}}^* \mid \mathbf{N}(x) \leq 1\}$. When $\mathcal{O}_K^*$ is "larger" in K^*, S_1 should be smaller, and so the factor of R_K/ω_K should correspond to the unit group $\mathcal{O}_K^*$, with R_K corresponding to the density of the free part of the unit group in K (being the covolume of $\mathcal{O}_K^*$ in $\mathbb{R}_0^{r+s}$), and $1/\omega_K$ from the roots of unity. The set $\mathcal{B}$ has 2^r connected components (2 for each $\mathbb{R}^* = \mathbb{R}^- \sqcup \mathbb{R}^+$ component), and the factor of $(2\pi)^s$ can be viewed as encoding the range of possible arguments in each $\mathbb{C}^*$ component.

Chapter 2

The analytic class number formula

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 estimating using point-counting.

2.1 Series and continuations

Before considering more general series of the form $\sum_{m=1}^{\infty} a_m m^{-s}$ (such as the Dedekind zeta function), we first describe convergence results for the Riemann zeta function $\zeta(s) = \sum_{m=1}^{\infty} m^{-s}$, which will ultimately yield the pole and residue of ζ_K at $s = 1$. We have the following classical result:

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 $\mathbb{C} \setminus \{1\}$, with a simple pole at $s = 1$ of residue 1.*

A proof of this result can be found in Chapter 12 of [1]. The previous lemma in conjunction with Theorem 3 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 $\sum_{m \leq t} a_m = O(t^\sigma)$. 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 [1, Theorem 4.2] 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 uniformly locally on $\mathrm{Re}(s) > \sigma$ as $x \to \infty$, and so $\sum_{m=1}^{t} a_m m^{-s}$ defines a holomorphic function on $\mathrm{Re}(s) > \sigma$. □

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 $\sigma < 1$. 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 $\sum_{m \le t} b_m = O(t^\sigma)$. 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 $\sigma < 1$, their sum admits a meromorphic extension to $\mathrm{Re}(s) > \sigma$ with a simple pole at $s = 1$ of residue $\rho \operatorname{Res}_{s=1} \zeta + 0 = \rho$. □

Specialising the statement of the above lemma to the Dedekind zeta function $\zeta_K(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}$, the sum $\sum_{m \le t} a_m$ is exactly the number of ideals $I \subseteq \mathcal{O}_K$ with ideal norm at most t. The previous lemma says that if this sum scales linearly with some lower order error term, then it also determines the continuation of ζ_K to a slightly larger half-plane excluding $s = 1$, and the residue at 1. To reason about the convergence and poles of the Dedekind zeta function, we can thus instead reason about the distribution of ideals of bounded norm.

2.2 The distribution of ideals

Throughout this section, we take K to be a fixed number field with r real embeddings $K \hookrightarrow \mathbb{R}$ and $2s$ complex embeddings $K \hookrightarrow \mathbb{C}$, with degree $n = [K : \mathbb{Q}] = r + 2s$, class number h_K, regulator R_K, discriminant Δ_K, and ω_K roots of unity.

To reason about the convergence and residues of ζ_K, we use Lemma 3 and reinterpret principal ideals as points in some reasonable subset of $K_{\mathbb{R}}^*$. Comparing Theorem 3 to Lemma 3, we may expect that the number of ideals of norm at most t is asymptotically

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

To show this, we first count the number of principal ideals up to a certain bound, and then adapt our argument slightly for ideals in an arbitrary ideal class. We do this by choosing a set of reasonable shape $S \subseteq K_{\mathbb{R}}^*$ and the lattice $\mathcal{O}_K^* \subseteq K_{\mathbb{R}}^*$ so that for $t \to \infty$, the number of points in $tS \cap \mathcal{O}_K^*$ corresponds to the number of ideals of norm at most some function of t.

2.2.1 Lipschitz parametrisability

We quantify "a reasonable shape" for a set by saying that the boundary should be reasonable, which we take to mean that the boundary of our set should be parametrisable by finitely many Lipschitz functions from unit cubes.

Definition 2 (Lipschitz parametrisable)**.** *A subset B of a metric space X is m-Lipschitz parametrisable if it is the union of the images of finitely many Lipschitz functions $[0,1]^m \to B$*

For a set $S \subseteq K_{\mathbb{R}}$ with Lipschitz parametrisable boundary and a lattice Λ, we then have the following point-counting relation between the number of lattice points in the scaled sets tS and the volume of S. Here we measure the volume of S with respect to a scaled version of the Lebesgue measure on $\mathbb{R}^r \times \mathbb{C}^s \cong K_{\mathbb{R}}$, with the measure doubled in the $\mathbb{C}$ components, corresponding to our previous identification of $K_{\mathbb{R}}$ with a subset of $\mathbb{C}^n$.

Lemma 4. *Let $\Lambda \subseteq K_{\mathbb{R}}$ be a lattice, and $S \subseteq K_{\mathbb{R}}$ have $(n-1)$-Lipschitz parametrisable boundary ∂S. Then*

$$|tS \cap \Lambda| = \frac{\mu(S)}{\operatorname{covol}(\Lambda)} t^n + O(t^{n-1})$$

as $t \to \infty$.

That is, number of lattice points in tS grows like t^n multiplied by the ratio of volumes $\mu(S)/\operatorname{covol}(\Lambda)$ as t gets large. A proof of this result can be found as 19.5 and 19.6 in [3].

2.2.2 Integral ideals of bounded norm

We note first that as $\mathcal{O}_K$ is an integral domain, $\alpha, \alpha' \in \mathcal{O}_K$ generate the same principal ideal if and only if $\alpha/\alpha' \in \mathcal{O}_K^*$, and so $\{(\alpha) \subseteq \mathcal{O}_K \mid I \neq 0, N((\alpha)) \leq t\}$ has the same cardinality as the set

$$\{\alpha \in K^* \cap \mathcal{O}_K \mid N(\alpha) \leq t\} / \mathcal{O}_K^*$$

where the notation $/\mathcal{O}_K^*$ refers to the equivalence classes under the equivalence relation $\alpha \sim u\alpha$ for some $u \in \mathcal{O}_K^*$. Setting $K_{\mathbb{R},\leq t} := \{x \in K_{\mathbb{R}}^* \mid N(x) \leq t\}$, we can write $(K_{\mathbb{R},\leq t}^* \cap \mathcal{O}_K)/\mathcal{O}_K^*$ for the above set, where this intersection is taken in $K_{\mathbb{R}}^* \subseteq K_{\mathbb{R}}$ and partitioned into classes modulo $\mathcal{O}_K^*$. Writing $\mathbf{N}$ for the geometric norm on $K_{\mathbb{R}}^*$, we have $\log(\mathbf{N}(x)) = \sum_\sigma \log|x_\sigma|$, which is exactly the sum of coordinates of $\operatorname{Log}(x)$. The set $K_{\mathbb{R},1}^* = \{x \in K^* \mid \mathbf{N}(x) = 1\}$ is then exactly the preimage of the trace-zero hyperplane $\mathbb{R}_0^{r+s}$, and we have a projection onto $K_{\mathbb{R},1}^*$ given by

$$\begin{aligned} \nu : K_{\mathbb{R}}^* &\twoheadrightarrow K_{\mathbb{R},1}^* \\ x &\mapsto x\,\mathbf{N}(x)^{-1/n} \end{aligned}$$

well-defined as for $r \in \mathbb{R}^+$ we have $\mathbf{N}(rx) = \prod_\sigma (|x_\sigma|\, r) = r^n \prod_\sigma |x_\sigma| = r^n\, \mathbf{N}(x)$ and surjective as each $x \in K_{\mathbb{R},1}^*$ maps to itself.

By Theorem 2 (Dirichlet's unit theorem) we have $\mathcal{O}_K^* = \mu_K \times U$ for some free $\mathbb{Z}$-module $U \subseteq \mathcal{O}_K^*$ of rank $r+s-1$, and the restriction of the Log map to U is injective. It is thus easier to estimate $|(K_{\mathbb{R},\leq t^*} \cap \mathcal{O}_K)/U|$, and noting that the fibres of the natural map

$$(K_{\mathbb{R},\leq t^*} \cap \mathcal{O}_K)/U \twoheadrightarrow (K_{\mathbb{R},\leq t^*} \cap \mathcal{O}_K)/\mathcal{O}_K^*$$

have size $|\mu_K| = \omega_K$, we have $|(K_{\mathbb{R},\leq t^*} \cap \mathcal{O}_K)/U| = \omega_K\, |(K_{\mathbb{R},\leq t^*} \cap \mathcal{O}_K)/\mathcal{O}_K^*|$, so we can obtain an estimate for $|(K_{\mathbb{R},\leq t^*} \cap \mathcal{O}_K)/\mathcal{O}_K^*|$ on dividing by ω_K.

Fixing a fundamental domain D for the lattice $\operatorname{Log}(U) \subseteq \mathbb{R}_0^{r+s}$, as ν and Log are injective on U it follows that $S := (\operatorname{Log} \circ \nu)^{-1}(R)$ is a set of unique coset representatives for $K_{\mathbb{R}}^*/U$, and these now correspond ω_K-to-1 to principal fractional ideals (up to multiplication by a root of unity). Letting

$S_{\leq t} = \{x \in S \mid \mathbf{N}(x) \leq t\} \subseteq K_{\mathbb{R}}$, the finite set $S_{\leq t} \cap \mathcal{O}_K \subseteq K_{\mathbb{R}}$ then corresponds ω_K-to-1 to the principal ideals in $\mathcal{O}_K$ of norm at most t. We then have $S_{\leq t} = t^{1/n} S_{\leq 1}$, and to compute the volume of $S_{\leq t}$, we check that the set $S_{\leq 1}$ has $(n-1)$-Lipschitz parametrisable boundary.

We note the Log map has kernel given by points with each component having norm 1, explicitly $\{\pm 1\}^r \times (S^1)^s \subseteq (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \cong K_{\mathbb{R}}^*$. Thus we have a continuous group isomorphism

$$\begin{aligned} K_{\mathbb{R}}^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s &\to \mathbb{R}^{r+s} \times \{\pm 1\}^r \times (S^1)^s \\ x = (x_1, \dots, x_r, z_1, \dots, z_s) &\mapsto \left(\operatorname{Log}(x), \operatorname{sign}(x_1), \dots, \operatorname{sign}(x_r), \frac{z_1}{|z_1|}, \dots, \frac{z_s}{|z_s|} \right) \end{aligned} \tag{2.1}$$

Since $\mathbb{R}^* = \mathbb{R}^- \sqcup \mathbb{R}^+$, $S_{\leq 1}$ consists of 2^r connected components, corresponding to choices of signs in each component. We note each $x \in S_{\leq 1}$ is of the form $x = \mathbf{N}(x)^{1/n} x'$ for $\mathbf{N}(x') = 1$, $\mathbf{N}(x)^{1/n} \in (0, 1]$. We then note that the componentwise absolute values of a point in U are described uniquely by its image under the Log map, so each point in S is described uniquely by its image in D under the Log map and the arguments in each $\mathbb{C}$ component.

Denote by $S_{\leq 1}^a = S_{\leq 1} \cap \prod_{j=1}^r \mathbb{R}^{a_j}$ the connected component corresponding to the choice of signs $a = (a_1, \dots, a_r) \in \{-, +\}^r$. Fixing a basis $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ for U so that

$$D = \left\{ \sum_{j=1}^{r+s-1} b_j \operatorname{Log}(\varepsilon_j) \mid 0 \leq b_j < 1 \right\}$$

is the fundamental parallelepiped of $\{e_j\}_{j=1}^{r+s-1}$, we can parametrise $S_{\leq 1}^a$ in n components, by taking $r+s-1$ components in $[0, 1)$ encoding $x / \mathbf{N}(x)^{1/n}$ by its $\mathbb{R}$-coefficients when expressed in terms of $\operatorname{Log}(\varepsilon_1), \dots, \operatorname{Log}(\varepsilon_{r+s-1})$, s components in $[0, 1)$ encoding points in S^1 by argument, and 1 component for $\mathbf{N}(x)^{1/n}$. These yield a continuously differentiable (in particular Lipschitz) bijection $C = [0, 1)^{n-1} \times (0, 1] \subseteq [0, 1]^n \to S_{\leq 1}^a$: each map in the first set maps a point to its component in a basis, the second set consists of maps of the form $x \mapsto e^{2\pi i x}$, and the third is differentiable as the absolute value is differentiable away from 0. The boundary of C is then the Lipschitz parametrisable set $\partial[0, 1]^n$, and so the above bijection shows $S_{\leq 1}^a$ is parametrisable for each $a \in \{\pm 1\}^r$, and thus so is $S_{\leq 1}$.

Applying Lemma 4 to $\Lambda = \mathcal{O}_K$, $S = S_{\leq 1}$ and with $t^{1/n}$ in place of t yields

$$|S_{\leq t} \cap \mathcal{O}_K| = \frac{\mu(S_{\leq 1})}{\operatorname{covol}(\mathcal{O}_K)} (t^{1/n})^n + O((t^{1/n})^{n-1}) = \frac{\mu(S_{\leq 1})}{\operatorname{covol}(\mathcal{O}_K)} t + O\left(t^{1-1/n}\right) \tag{2.2}$$

and so it remains to compute $\mu(S_{\leq 1})$. Writing each $x \in S_{\leq 1}$ as $x = \mathbf{N}(x)^{1/n} \nu(x)$ for $\mathbf{N}(x) \in (0, 1]$, under the Log map (which is the first component of (2.1), $S_{\leq 1}$ is mapped by

$$\begin{aligned} S_{\leq 1} &\to D + (-\infty, 0] \left(\frac{1}{n}, \dots, \frac{1}{n}, \frac{2}{n}, \dots, \frac{2}{n} \right) \\ x = \nu(x) \, \mathbf{N}(x)^{1/n} &\mapsto \operatorname{Log}(\nu(x)) + \log(\mathbf{N}(x)) \left(\frac{1}{n}, \dots, \frac{1}{n}, \frac{2}{n}, \dots, \frac{2}{n} \right) \end{aligned}$$

To compute $S_{\leq 1}$ we integrate over each connected component $S_{\leq 1}^a$ for $a \in \{-, +\}^r$. We reindex each $\mathbb{R}^{a_i}$ component of $S_{\leq 1}^a$ by the maps

$$\begin{aligned} \mathbb{R}^{a_i} &\to \mathbb{R} \\ x_i &\mapsto \log |x_i| =: \ell_i \end{aligned}$$

or equivalently $x_i = a_i e^{\ell_i}$, and under this change of variables we have $dx_i = \left| a_i e^{\ell_i} \right| d\ell_i = e^{\ell_i} d\ell_i$. For each $\mathbb{C}^*$ component of $S_{\leq 1}^a$ we reindex by polar coordinates (with $e^{\ell/2}$ in place of r) by

$$\mathbb{C}^* \to \mathbb{R} \times [0, 2\pi)$$

$$z_j \mapsto (2\log|z_j|, \arg(z_j)) =: (\ell_{r+j}, \theta_j)$$

and noting that the standard measure on $\mathbb{C}^*$ (as a component on $K_{\mathbb{R}}^*$) is twice that of the usual measure on $\mathbb{C}^*$, reindexing yields $2dz_j = 2e^{\ell_{r+j}/2}d(e^{\ell_{r+j}/2})d\theta_j = e^{\ell_{r+j}}d\ell_{r+j}d\theta_j$. Overall we have

$$dx_1 \ldots dx_r dz_1 \ldots dz_s = e^{\ell_1+\ldots+\ell_{r+s}} d\ell_1 \ldots d\ell_{r+s} d\theta_1 \ldots d\theta_s$$

To simplify the exponent we change the last variable (fixing the other variables) to

$$t = \ell_1 + \ldots + \ell_{r+s} = \log|x_1| + \ldots + \log|x_r| + 2\log|z_1| + \ldots 2\log|z_s| = \log(\mathbf{N}(x))$$

We then have $dt = d\ell_{r+s}$, and letting $\pi : \mathbb{R}^{r+s} \twoheadrightarrow \mathbb{R}^{r+s-1}$ be the projection onto the first $r+s-1$ components and letting $\ell = (\ell_1, \ldots, \ell_{r+s-1})$ and $d\ell = d\ell_1 \ldots d\ell_{r+s-1}$, the Log map ultimately maps $S^a_{\leq 1}$ to $\pi(D) \times (-\infty, 0]$ under this reindexing, so we can write our change of variables as

$$\begin{aligned} S^a_{\leq 1} &\to \pi(D) \times (-\infty, 0] \times [0, 2\pi)^s \\ x = (x_1, \ldots, x_r, z_1, \ldots, z_s) &\mapsto (\pi(\mathrm{Log}(x)), \log(\mathbf{N}(x)), \arg(z_1), \ldots, \arg(z_s)) =: (\ell, t, \theta_1, \ldots, \theta_s) \\ dx_1 \ldots dx_r dz_1 \ldots dz_s &= e^t d\ell dt d\theta_1 \ldots d\theta_s \end{aligned}$$

Noting then that the regulator R_K is exactly the volume (or measure) of $\pi(D)$, we then have

$$\begin{aligned} \mu(S^a_{\leq 1}) &= \int_{S^a_{\leq 1}} dx_1 \ldots dx_r dz_1 \ldots dz_r \\ &= \left(\int_{\pi(D)} d\ell\right)\left(\int_{-\infty}^0 e^t dt\right)\left(\int_0^{2\pi} d\theta_1\right) \cdots \left(\int_0^{2\pi} d\theta_s\right) \\ &= R_K (2\pi)^s \end{aligned}$$

Since $S_{\leq 1} = \bigsqcup_{a \in \{-,+\}^r} S^a_{\leq 1}$ we then have

$$\mu(S_{\leq 1}) = \sum_{a \in \{-,+\}^r} \mu(S^a_{\leq 1}) = 2^r (2\pi)^s R_K$$

Dividing by ω_K to account for the ω_K-to-1 map $S_{\leq t} \cap \mathcal{O}_K \twoheadrightarrow (K^*_{\mathbb{R},\leq t} \cap \mathcal{O}_K)/\mathcal{O}_K$, we find that

$$|\{(\alpha) \subseteq \mathcal{O}_K \mid N(\alpha) \leq t\}| = \frac{2^r (2\pi)^s R_K}{\omega_K \operatorname{covol}(\mathcal{O}_K)} + O\left(t^{1-1/n}\right) \tag{2.3}$$

For an arbitrary ideal class $\gamma \in \mathrm{cl}(K)$, we aim to show note first that (2.3) generalises to any non-zero ideal $I \subseteq \mathcal{O}_K$ by replacing I with $\mathcal{O}_K$ and noting that $S_{\leq 1} \cap I$ counts the number of principal ideals $(\alpha) \subseteq I$, yielding

$$|\{(\alpha) \subseteq I \mid N(I) \leq t\}| = \left(\frac{2^r (2\pi)^s R_K}{\omega_K \operatorname{covol}(I)}\right) t + O(t^{1-1/n}) \tag{2.4}$$

Let $I_\gamma \subseteq \mathcal{O}_K$ be a representative for γ. Then for the inverse class $[I_\gamma^{-1}]$, we have a bijection given by multiplying by I_γ:

$$\left\{I \in [I_\gamma^{-1}] \mid I \subseteq \mathcal{O}_K, N(I) \leq t\right\} \xrightarrow{I \mapsto II_\gamma} \{(\alpha) \subseteq I_\gamma \mid N(\alpha) \leq tN(I_\gamma)\}$$

and so taking cardinalities, we find

$$\begin{aligned} \left|\left\{I \in [I_\gamma^{-1}] \mid I \subseteq \mathcal{O}_K, N(I) \leq t\right\}\right| &= \left(\frac{2^r (2\pi)^s R_K}{\omega_K \operatorname{covol}(I_\gamma)}\right) tN(I_\gamma) + O\left(t^{1-1/n}\right) \\ &= \left(\frac{2^r (2\pi)^s R_K}{\omega_K \operatorname{covol}(\mathcal{O}_K) N(I_\gamma)}\right) tN(I_\gamma) + O\left(t^{1-1/n}\right) \end{aligned}$$

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

which in particular is independent of the ideal class $\gamma \in \mathrm{cl}(K)$. Summing up over ideal classes yields

$$\begin{aligned} |\{I \subseteq \mathcal{O}_K \mid N(I) \leq t\}| &= \sum_{\gamma \in \mathrm{cl}(K)} \left|\{I \in [I_\gamma^{-1}] \mid I \subseteq \mathcal{O}_K, N(I) \leq t\}\right| \\ &= \left(\frac{2^r (2\pi)^s h_K R_K}{\omega_K \left|\Delta_K\right|^{1/2}} \right) t + O\left(t^{1-1/n}\right) \end{aligned}$$

We have thus proved the following theorem on the distribution of integral ideals of bounded norm.

Theorem 4. *Let K be a number field with r real and $2s$ complex embeddings. Then the number of ideals $I \subseteq \mathcal{O}_K$ of norm at most t is*

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

as $t \to \infty$, where h_K is the class number, R_K is the regulator, ω_K is the number of roots of unity in K and Δ_K is the discriminant of K.

Combining this with Lemma 3 and recalling that the sum of coefficients $a_1 + \ldots + a_t$ when writing $\zeta_K(s) = \sum a_m m^{-s}$ is the number of ideals of norm at most t, we have also proven Theorem 3, which we restate succinctly with the same setup as above.

Theorem 5 (Analytic class number formula)**.** *The Dedekind zeta function $\zeta_K(s) = \sum_{0 \neq I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s}$ is holomorphic on the half-plane $Re(s) > 1$, and admits a continuation to $Re(s) > 1 - 1/n$ holomorphic everywhere except for a simple pole at $s = 1$ with residue*

$$\mathrm{Res}_{s=1}\, \zeta_K = \frac{2^r (2\pi)^s h_K R_K}{\omega_K \left|\Delta_K\right|^{1/2}}$$

The simplest application of this formula is in computing (or approximating) these invariants of the number field K. We can approximate this residue to arbitrary precision as in [2, Chapter 6], and given all but one of these values, the above result allows us to compute the remaining value. This is particularly reliable when we look to compute h_K, which we can be relatively certain about as it only takes on integer values.

A simple example of this is in the case of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ where d is squarefree, where we can easily compute all quantities except for h_K. In these such fields there are no non-trivial units, and so the regulator R_K is just 1, corresponding to the empty product. Here K has $r = 0$ real embeddings and $s = 1$ conjugate pair of embeddings. The ring of integers $\mathcal{O}_K$ is given by

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}] & d \equiv 1, 2 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] & d \equiv 3 \mod 4 \end{cases}$$

with discriminant $-4d$ in the first case, and $-d$ in the second. The unit group of $\mathbb{Q}(\sqrt{-d})$ is generated by i when $d = -1$, $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ when $d = -3$, and -1 otherwise, so we have 4, 6 and 2 roots of unity in each of these cases. The process for computing the residue mentioned above reduces to looking at congruence conditions, and with sufficient precision we can compute the class number of any imaginary quadratic field in this way.

Chapter 3

References

1. Apostol, T., (1976), *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg
2. Stevenhagen, P., (2019), *Number rings*, online at *https://websites.math.leidenuniv.nl /algebra/ant.pdf*
3. Sutherland, A., (2016), *The analytic class number formula*, online at *https://math.mit.edu /classes/18.785/2017fa/LectureNotes19.pdf*