Random walks on Arakelov class groups

Boer, K. de

2. Preliminaries

2.1. General Notation

We denote by $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ the natural numbers, the integers, the rationals, the real numbers and the complex numbers respectively. All logarithms are in base e. For a rational number $p/q \in \mathbb{Q}$ with p and q coprime, we let $\mathrm{size}(p/q)$ refer to $\log|p| + \log|q|$. We extend this definition to vectors and matrices of rational numbers, by taking the sum of the sizes of all the coefficients.

Vectors $\mathbf{v} \in V$ are denoted in boldface and are to be interpreted column-wise unless stated otherwise. In the case of a vector in a (quantum) Hilbert space $\mathcal{H}$, we sometimes deviate from this notation and use the bra-ket notation as well; $|\mathbf{v}\rangle$ for primal vectors and $\langle\mathbf{v}|$ for dual vectors. An inner product of $\langle\mathbf{w}|$ and $|\mathbf{v}\rangle$ is then denoted $\langle\mathbf{w}|\mathbf{v}\rangle$, and the notation for the tensor product $|\mathbf{w}\rangle \otimes |\mathbf{v}\rangle$ of two vectors in a Hilbert space is generally suppressed, i.e., we denote $|\mathbf{w}\rangle|\mathbf{v}\rangle$ instead.

2.2. Fourier Theory

We start with a brief introduction to Fourier analysis over arbitrary locally compact abelian groups. This general treatment allows us to then apply the general principles to the different groups that play a role in this thesis, especially in Chapter 3. For the reader that is unfamiliar with such a general treatment, it is useful — and almost sufficient — to think of $\mathbb{R}$, of $\mathbb{T} = \mathbb{R}/\mathbb{Z}$,

and a finite group. For more details and for the proofs we refer to Deitmar's book on this subject [DE16].

2.2.1. Groups

Here and below we consider a *locally compact abelian* group G. Such a group admits a *Haar measure* μ that is unique up to a normalization factor. The crucial property of such a Haar measure is that it is invariant under the group action. Simple examples are $G = \mathbb{R}$ with μ the Lebesgue measure λ, or a finite group G with μ the counting measure $\#$.

The *dual group* $\hat{G}$, consisting of the continuous[1] group homomorphisms χ from G into S^1, the multiplicative group of complex numbers of absolute value 1, is again a locally compact abelian group. As we shall see soon, for a fixed choice of the normalization factor of the Haar measure μ for G, there is a natural choice for the normalization factor of the Haar measure $\hat{\mu}$ for $\hat{G}$.

Examples of locally compact abelian groups that play an important role in this dissertation are: the m-dimensional real vector space $\mathbb{R}^m$; the m-fold torus $\mathbb{T}^m := \mathbb{R}^m/\mathbb{Z}^m$ and more generally $\mathbb{R}^m/\Lambda$ for an arbitrary lattice Λ in $\mathbb{R}^m$; and the finite 'discretized torus' group $\mathbb{D}^m := \frac{1}{q}\mathbb{Z}^m/\mathbb{Z}^m \subset \mathbb{T}^m$ (which is isomorphic to $\mathbb{Z}^m/q\mathbb{Z}^m$) for a positive integer q. Figure 2.1 below shows the corresponding dual groups as well as the respective (dual) Haar measures as used in Chapter 3 of this thesis.

In some cases it will be useful to identify the quotient groups $\mathbb{T}^m = \mathbb{R}^m/\mathbb{Z}^m$ and $\mathbb{D}^m = \frac{1}{q}\mathbb{Z}^m/\mathbb{Z}^m$ with the respective representing sets

$$\mathbb{T}^m_{\text{rep}} := [-\tfrac{1}{2}, \tfrac{1}{2})^m \subset \mathbb{R}^m \qquad \text{and} \qquad \mathbb{D}^m_{\text{rep}} := \tfrac{1}{q}\mathbb{Z}^m \cap \mathbb{T}^m_{\text{rep}}\,,$$

and similarly $\hat{\mathbb{D}}^m \simeq \mathbb{Z}^m/q\mathbb{Z}^m$ with

$$\hat{\mathbb{D}}^m_{\text{rep}} := [q]^m_c := \mathbb{Z}^m \cap [-\tfrac{q}{2}, \tfrac{q}{2})^m\,.$$

[1] Discrete (and in particular, finite) groups have the discrete topology, implying that the continuity constraint for characters on these groups is void.

Group		**Dual group**	
G	μ	$\hat{G}$	$\hat{\mu}$
$\mathbb{R}^m$	λ	$\hat{\mathbb{R}}^m \simeq \mathbb{R}^m$	λ
$\mathbb{T}^m := \mathbb{R}^m/\mathbb{Z}^m$	λ	$\hat{\mathbb{T}}^m \simeq \mathbb{Z}^m$	$\#$
$\mathbb{D}^m := \frac{1}{q}\mathbb{Z}^m/\mathbb{Z}^m$	$\frac{1}{q^m}\#$	$\hat{\mathbb{D}}^m \simeq \mathbb{Z}^m/q\mathbb{Z}^m$	$\#$
$\mathbb{R}^m/\Lambda$	$\frac{1}{\det(\Lambda)}\lambda$	$\widehat{(\mathbb{R}^m/\Lambda)} \simeq \Lambda^*$	$\#$

Figure 2.1.: Some groups G and their respective dual groups $\hat{G}$, plus the considered (dual) Haar measures μ and $\hat{\mu}$. Here, λ denotes the Lebesgue measure and $\#$ the counting measure. Furthermore, Λ^* is the *dual lattice* of Λ, see Section 2.5.1.

It will be useful to understand that if $H \subset G$ is a closed subgroup then G/H and H have dual groups that satisfy the following natural isomorphisms.

$$\widehat{G/H} \simeq H^\perp := \{\chi \in \hat{G} \mid \chi(h) = 1 \text{ for all } h \in H\} \subset \hat{G} \quad \text{and} \quad \hat{H} \simeq \hat{G}/H^\perp.$$

As we shall see soon, for any choice of the Haar measure μ_H for H there is a natural choice for the Haar measure $\mu_{G/H}$ for G/H, and vice versa.

2.2.2. Norms and Fourier Transforms

Let G be as above with a fixed choice for the Haar measure μ. For any $p \in [1, \infty]$, $L_p(G)$ denotes the metric vector space of measurable functions $f : G \to \mathbb{C}$ with finite norm $\|f\|_p$ (modulo the functions with norm zero[2]), where

$$\|f\|_p^p := \int_{g \in G} |f(g)|^p d\mu \qquad \text{for } p < \infty,$$

and

$$\|f\|_\infty := \operatorname*{ess\,sup}_{g \in G} |f(g)|,$$

[2]This in order to make $\|\cdot\|_p$ a metric: $\|f\|_p = 0$ implies $f = 0$ in that case.

the essential supremum of $|f|$. We write $\|f\|_{p,G}$ if we want to make G explicit. For any function $f \in L^1(G)$, the *Fourier transform* of f is the function

$$\mathcal{F}_G\{f\} : \hat{G} \to \mathbb{C},\ \chi \mapsto \int_{g\in G} f(g)\bar{\chi}(g)d\mu\,,$$

also denoted by $\hat{f}$ when G is clear from the context. The Fourier transform of $f \in L^1(G)$ is continuous, but not necessarily in $L^1(\hat{G})$.

For example, for the group $\mathbb{D}^m := \frac{1}{q}\mathbb{Z}^m/\mathbb{Z}^m$ with the Haar measure as fixed in Figure 2.1, the L_2-norm and the Fourier transform are respectively given by

$$\|f\|_2^2 = \frac{1}{q^m}\sum_{x\in\mathbb{D}^m} |f(x)|^2 \qquad \text{and} \qquad \mathcal{F}\{f\}(y) = \frac{1}{q^m}\sum_{x\in\mathbb{D}^m} f(x)e^{-2\pi i\langle x,y\rangle}\,.$$

We note that we use a different convention on the scaling than what is common in the context of the quantum Fourier transform. Namely, in most literature (e.g., [NC11, §5.1]), the standard quantum Fourier transform uses a scaling of $q^{-m/2}$, for sake of preserving the L_2-norm and symmetry; here, we use the scaling q^{-m} one way, and a unit scaling the other way.

Given the Haar measure μ for G, there exists a unique *dual* Haar measure $\hat{\mu}$ for $\hat{G}$ with the property that, for any $f \in L^1(G)$, if $\hat{f} = \mathcal{F}_G\{f\} \in L^1(\hat{G})$, then $f = \mathcal{F}_G^{-1}\{\hat{f}\}$, where

$$\mathcal{F}_G^{-1}\{\hat{f}\} : G \to \mathbb{C},\ g \mapsto \int_{\chi\in\hat{G}} \hat{f}(\chi)\chi(g)d\hat{\mu}$$

is the *inverse Fourier transform*. From now on it is always understood that the Haar measure of the dual group is chosen to be the dual of the Haar measure of the primal group. With this choice, we also have the following well known fact [DE16, Thm. 3.4.8].

Theorem 2.1 (Plancherel's Identity)**.** *For all $f \in L^1(G) \cap L^2(G)$,*

$$\|f\|_{2,G} = \|\mathcal{F}_G\{f\}\|_{2,\hat{G}}\,.$$

Finally, we recall the *convolution theorem*, which states that $\widehat{fg} = \hat{f} \star \hat{g} = \int_{x \in G} \hat{f}(x)\hat{g}(\cdot - x)d\mu(x)$ for all functions $f, g \in L^1(G)$ that have Fourier transforms $\hat{f}, \hat{g} \in L^1(G)$. This extends to functions $f \in L^1(G/H)$ and $g \in L^1(G)$, with f understood as an H-periodic function on G. Tailored to $G = \mathbb{R}^m$ and $H = \Lambda$, where $\mathbb{R}^m/\Lambda$ has dual group Λ^*, it then states that, for all $y \in \mathbb{R}^m$,

$$\begin{aligned} \mathcal{F}_{\mathbb{R}^m}\{fg\}(y) &= \mathcal{F}_{\mathbb{R}^m/\Lambda}\{f\} \star \mathcal{F}_{\mathbb{R}^m}\{g\}(y) \\ &= \sum_{\ell^* \in \Lambda^*} \mathcal{F}_{\mathbb{R}^m/\Lambda}\{f\}(\ell^*)\, \mathcal{F}_{\mathbb{R}^m}\{g\}(y - \ell^*). \end{aligned} \tag{2.4}$$

2.2.3. The Poisson Summation Formula

Poisson summation formula is well-known for the group $G = \mathbb{R}$, where it states that $\sum_{k \in \mathbb{Z}} \hat{f}(k) = \sum_{x \in \mathbb{Z}} f(x)$. In the case $G = \mathbb{Z}/N\mathbb{Z}$, it reads

$$\sum_{i=0}^{N/s} \hat{f}(is) = \sum_{j=1}^{s} f(j\tfrac{N}{s})$$

for any integer s that divides N. In order to formulate the Poisson summation formula for an arbitrary locally compact abelian group G, we need to introduce the notion of *restriction* and *periodization* of functions (see Figures 2.2 and 2.3).

Definition 2.2 (Restriction)**.** *Let $H \subseteq G$ be a subset or a subgroup. For any continuous function $f : G \to \mathbb{C}$ we define $f\big|_H : H \to \mathbb{C}, h \mapsto f(h)$.*

Definition 2.3 (Periodization)**.** *Let H be a closed subgroup of G with Haar measure μ_H. For any function $f \in L^1(G)$, we define*

$$f|^{G/H} : G/H \to \mathbb{C},\ g + H \mapsto \int_{h \in H} f(g + h)d\mu_H\,.$$

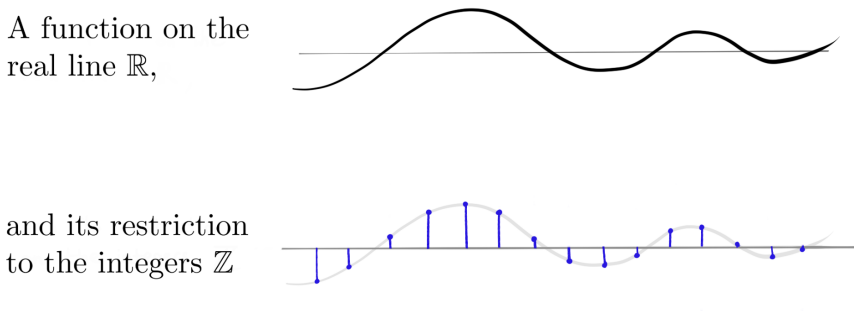


Figure 2.2.: A function on the real line and its restriction on the integers.

For any closed subgroup H of G with respective choices of Haar measures μ and μ_H, there exists a unique Haar measure $\mu_{G/H}$ for G/H such that the *quotient integral formula*

$$\int_{G/H} \left(\int_H f(g+h) d\mu_H(h) \right) d\mu_{G/H}(g+H) = \int_G f(g) d\mu(g)$$

holds for any continuous function $f : G \to \mathbb{C}$ with compact support (see [DE16, Sec. 1.5]).

With this choice of Haar measure for G/H, and with the dual measures for the respective dual groups, we are ready to state the general form of the Poisson summation formula (obtained from [DE16, Sec. 3.6], see also Figure 2.5).

Theorem 2.4 (Poisson Summation Formula)**.** *For continuous $f \in L^1(G)$,*

$$\mathcal{F}_H\{f|_H\} = \mathcal{F}_G\{f\}|^{\hat{H}} \quad \text{and} \quad \mathcal{F}_{G/H}\{f|^{G/H}\} = \mathcal{F}_G\{f\}|_{\widehat{G/H}}.$$

Applied to $G = \mathbb{R}^m$ and $H = \mathbb{Z}^m$, so that $G/H = \mathbb{R}^m/\mathbb{Z}^m = \mathbb{T}^m$ and $\widehat{G/H} \simeq \mathbb{Z}^m$; and applied to $G = \mathbb{T}^m$ and $H = \mathbb{D}^m$ below, we obtain the following.

Corollary 2.5. *For continuous $h \in L^1(\mathbb{R}^m)$, we have*

$$\mathcal{F}_{\mathbb{T}^m}\{h|^{\mathbb{T}^m}\} = \mathcal{F}_{\mathbb{R}^m}\{h\}|_{\mathbb{Z}^m}.$$

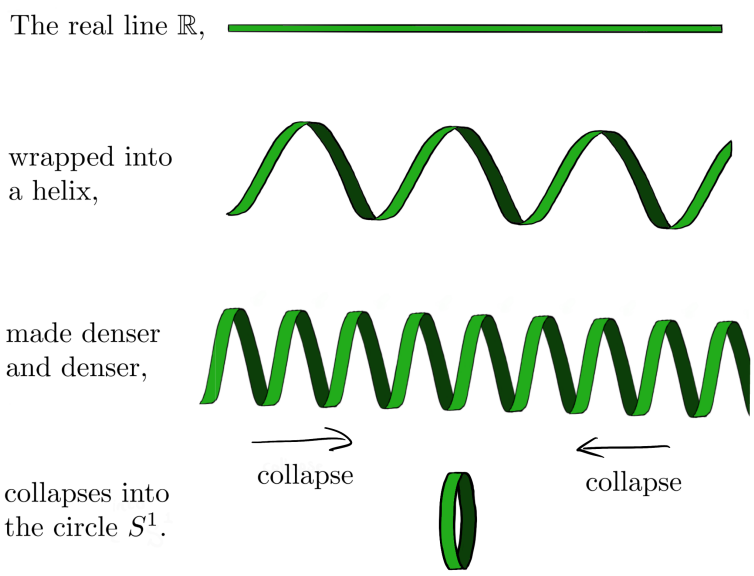


Figure 2.3.: The periodization of a function is a consequence of folding the space of its domain, i.e., taking the topological quotient space. In this example, the real line $\mathbb{R}$ is folded into a circle.

Corollary 2.6. *For continuous $t \in L^1(\mathbb{T}^m)$, we have*

$$\mathcal{F}_{\mathbb{D}^m}\left\{t|_{\mathbb{D}^m}\right\} = \mathcal{F}_{\mathbb{T}^m}\{t\}|^{\hat{\mathbb{D}}^m}.$$

Remark 2.7. *The Poisson summation formula can be used to show that a 'wide' periodized Gaussian on the circle is close to a constant function, see Figure 2.7. The wider a Gaussian function, the narrower the Gaussian function of its Fourier transform is. Taking the restriction of such a 'narrow' Gaussian function to the integers $\mathbb{Z}$ results in a spectrum heavily concentrated on zero, which corresponds to a* constant *function, as can be seen in the bottom example of Figure 2.7. Also note that for the 'narrower' Gaussian function on the circle, both the Gaussian on the circle as the restricted Fourier transform on $\mathbb{Z}$ resemble much more a 'real' Gaussian function. In short, the narrower the Gaussian on the circle, the more Gaussian properties*

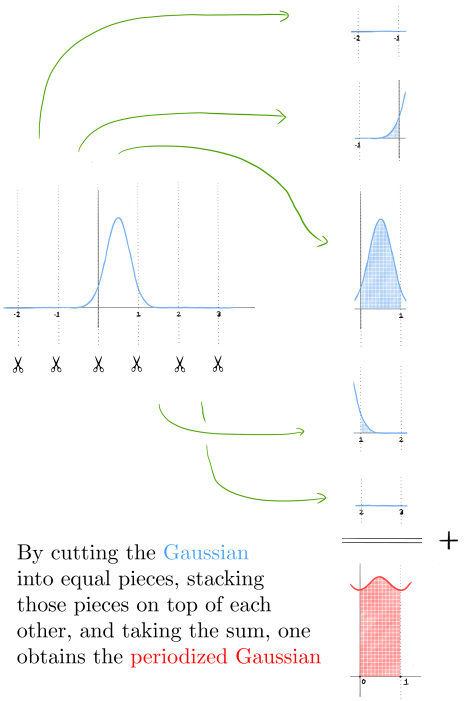


Figure 2.4.: An example of the periodization of a Gaussian on the real line, with respect to the subgroup $\mathbb{Z} \subseteq \mathbb{R}$. This leads to a *periodized* Gaussian on the circle $\mathbb{R}/\mathbb{Z} \simeq S^1$.

is has; the wider the Gaussian on the circle, the more 'constant' properties it has.

2.2.4. The Fourier Transform of Vector-valued Functions

The Fourier transform as discussed above generalizes to vector-valued functions $\mathbf{f} : G \to \mathbb{C}^N$ simply by applying $\mathcal{F}$ to the N coordinate functions, resulting in a function $\mathcal{F}\{\mathbf{f}\} : \hat{G} \to \mathbb{C}^N$. By fixing an orthonormal basis, this extends to functions $\mathbf{f} : G \to \mathcal{H}$ for an arbitrary finite-dimensional complex Hilbert space, where, by linearity of the Fourier transform, $\mathcal{F}\{\mathbf{f}\} : \hat{G} \to \mathcal{H}$ is independent of the choice of the basis.

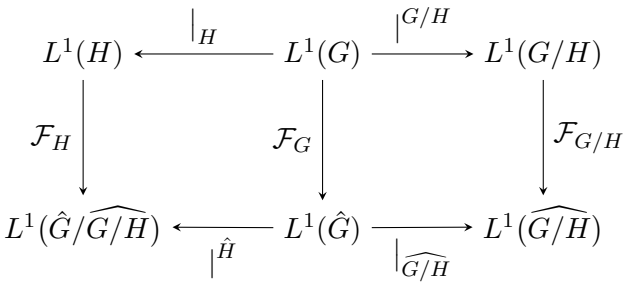


Figure 2.5.: Informal illustration of Theorem 2.4 by means of a diagram that commutes whenever the maps are well defined.

The norm $\|\cdot\|_{2,G}$ on functions $G \to \mathbb{C}$ generalizes to vector-valued functions $\mathbf{f} : G \to \mathcal{H}$, as well, by defining $\|\mathbf{f}\|_{2,G}$ to be the norm of the scalar function $x \mapsto \|\mathbf{f}(x)\|_{\mathcal{H}} = \sqrt{\langle \mathbf{f}(x) | \mathbf{f}(x) \rangle}$. The vectorial Fourier transforms and norms are compatible with each other, in the sense that Plancherel's identity (see Theorem 2.1) still holds; that is,

$$\|\mathbf{f}\|_{2,G} = \|\mathcal{F}_G\{\mathbf{f}\}\|_{2,\hat{G}}. \tag{2.5}$$

Also the Poisson summation formula (see Theorem 2.4) is still valid, as well as the convolution theorem whenever one of the functions in the product is scalar:

$$\mathcal{F}_G\{\mathbf{f}g\} = \mathcal{F}_G\{\mathbf{f}\} \star \mathcal{F}_G\{g\}. \tag{2.6}$$

An important example is the case $\mathbf{f} : \mathbb{R}^m/\Lambda \to \mathcal{H}$. Spelling out the above, we get

$$\begin{aligned} \mathcal{F}_{\mathbb{R}^m/\Lambda}\{\mathbf{f}\} :& \Lambda^* \to \mathcal{H}, \\ & \ell^* \mapsto |c_{\ell^*}\rangle := \frac{1}{\det \Lambda} \int_{x \in \mathbb{R}^m/\Lambda} |\mathbf{f}(x)\rangle e^{-2\pi i \langle x, \ell^* \rangle} dx, \end{aligned} \tag{2.7}$$

where the vectors $|c_{\ell^*}\rangle$ are also referred to as the *(vectorial) Fourier coefficients* of $\mathbf{f}$. The Parseval-Plancherel identity [DE16, Thm. 3.4.8] then becomes

$$\sum_{\ell^* \in \Lambda^*} \langle c_{\ell^*} | c_{\ell^*} \rangle = \|\mathbf{f}\|^2_{\mathbb{R}^m/\Lambda} := \frac{1}{\det \Lambda} \int_{x \in \mathbb{R}^m/\Lambda} \langle \mathbf{f}(x) | \mathbf{f}(x) \rangle dx. \tag{2.8}$$

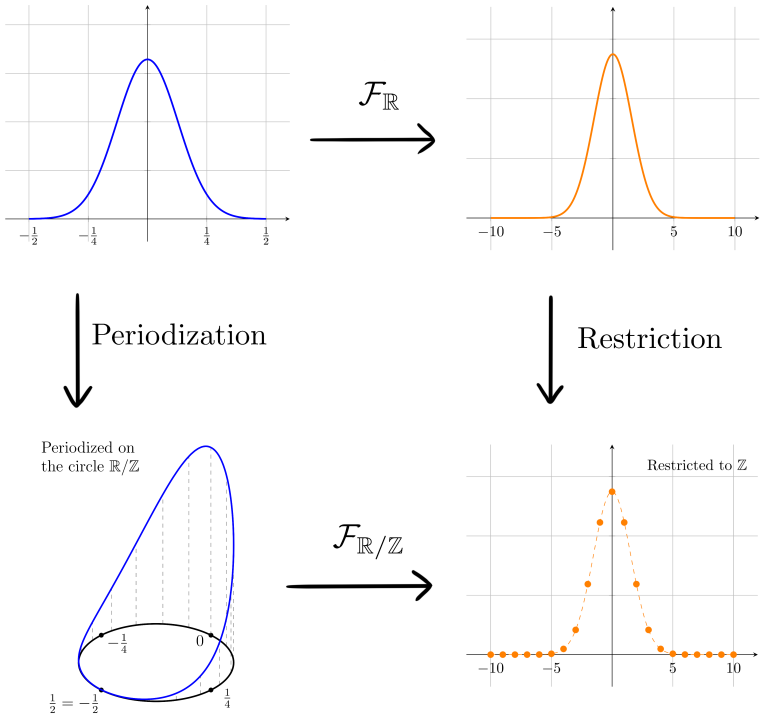


Figure 2.6.: A graphical depiction of the Poisson summation formula as described in Theorem 2.4, applied to a Gaussian function. First periodizing a function and then applying the Fourier transform gives the same result as first applying the Fourier transform and then restricting the function. As a result, the Fourier transform of a *periodized* Gaussian is a *discrete* Gaussian.

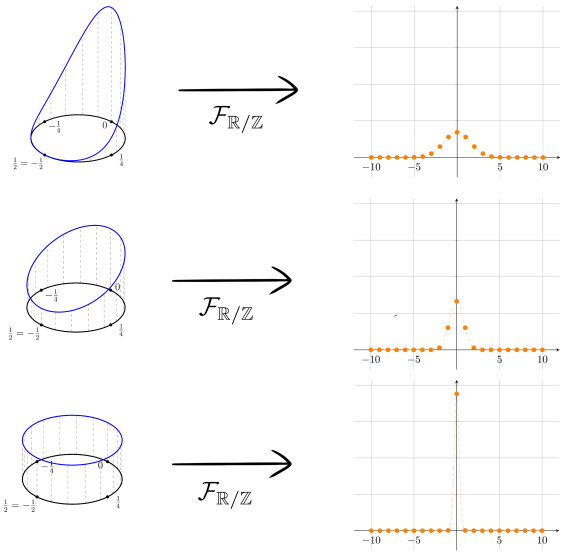


Figure 2.7.: The narrower the Gaussian on the circle, the more it looks like a Gaussian; the wider the Gaussian on the circle, the closer to constant it is.

The convolution theorem, as in Equation (2.6) and Equation (2.4), in this case, becomes,

$$\begin{aligned}\mathcal{F}_{\mathbb{R}^m}\{\mathbf{f}g\} &= \mathcal{F}_{\mathbb{R}^m/\Lambda}\{\mathbf{f}\} \star \mathcal{F}_{\mathbb{R}^m}\{g\} \\ &= \sum_{\ell^* \in \Lambda^*} \mathcal{F}_{\mathbb{R}^m/\Lambda}\{\mathbf{f}\} \cdot \mathcal{F}_{\mathbb{R}^m}\{g\}(\,\cdot - \ell^*). \end{aligned} \tag{2.9}$$

2.2.5. Trigonometric Approximation

As another application of the Poisson summation formula, we derive a relation between the Lipschitz constant of a function on $\mathbb{T}^m = \mathbb{R}^m/\mathbb{Z}^m$ and the 'error of discretization' in the Fourier transform when restricting the function to $\mathbb{D}^m$.

Theorem 2.8. *For any Lipschitz function* $\mathbf{h} : \mathbb{T}^m \to \mathcal{H}$ *(where* $\mathcal{H}$ *is a Hilbert space) with Lipschitz constant* $\mathrm{Lip}(\mathbf{h})$*, and any subset* $C \subseteq \hat{\mathbb{D}}^m$*, we*

have

$$\left| \|1_C \cdot \mathcal{F}_{\mathbb{D}^m}\{\mathbf{h}\}\|_{\hat{\mathbb{D}}^m} - \|1_C \cdot \mathcal{F}_{\mathbb{T}^m}\{\mathbf{h}\}\|_{\mathbb{Z}^m} \right| \leq \frac{4\pi\sqrt{m} \cdot \mathrm{Lip}(\mathbf{h})}{q}.$$

Here and below, we slightly abuse notation and use 1_C as indicator function acting on $\hat{\mathbb{D}}^m$ and on $\mathbb{Z}^m$, justified by identifying $\hat{\mathbb{D}}^m$ with $\hat{\mathbb{D}}^m_{\mathrm{rep}} = [q]^m_c \subset \mathbb{Z}^m$. Also, we write $\mathcal{F}_{\mathbb{D}^m}\{\mathbf{h}\}$ instead of $\mathcal{F}_{\mathbb{D}^m}\{\mathbf{h}|_{\mathbb{D}^m}\}$, taking it as understood that $\mathbf{h}$ is restricted to $\mathbb{D}^m$ when applying $\mathcal{F}_{\mathbb{D}^m}$.

Proof. Using a result of Yudin ([Yud76, Example I after Thm. 2], see also[3] Appendix A.4), there exists a trigonometric approximation $\mathbf{t}$ of $\mathbf{h}$, i.e. a function $\mathbf{t} : \mathbb{T}^m \to \mathbb{C}$ with $\hat{\mathbf{t}}(x) := \mathcal{F}_{\mathbb{T}^m}\{\mathbf{t}\}(x) = 0$ for all $x \in \mathbb{Z}^m \backslash [q]^m_c$ so that $\|\mathbf{h} - \mathbf{t}\|_\infty \leq \pi\sqrt{m} \cdot \mathrm{Lip}(\mathbf{h})/q$. Recalling that $\hat{\mathbb{D}}^m \simeq \mathbb{Z}^m/q\mathbb{Z}^m$, the fact that $\hat{\mathbf{t}} : \mathbb{Z}^m \to \mathbb{C}$ vanishes outside of $[q]^m_c$ implies for all $x \in [q]^m_c$ that

$$\hat{\mathbf{t}}(x) = \sum_{d \in q\mathbb{Z}^m} \hat{\mathbf{t}}(x+d) = \hat{\mathbf{t}}|^{\hat{\mathbb{D}}^m}(x) = \mathcal{F}_{\mathbb{D}^m}\{\mathbf{t}\}(x),$$

where the last equality holds by Corollary 2.6 (and our convention of omitting the restriction to $\mathbb{D}^m$). In particular, we have $\|1_C \cdot \mathcal{F}_{\mathbb{D}^m}\{\mathbf{t}\}\|_{2,\hat{\mathbb{D}}^m} = \|1_C \cdot \mathcal{F}_{\mathbb{T}^m}\{\mathbf{t}\}\|_{2,\mathbb{Z}^m}$. Therefore, by the (reverse) triangle inequality and the linearity of the Fourier transform, one obtains

$$\begin{aligned}&\left| \|1_C \cdot \mathcal{F}_{\mathbb{D}^m}\{\mathbf{h}\}\|_{\hat{\mathbb{D}}^m} - \|1_C \cdot \mathcal{F}_{\mathbb{T}^m}\{\mathbf{h}\}\|_{\mathbb{Z}^m} \right| \\ &\qquad \leq \|1_C \cdot \mathcal{F}_{\mathbb{D}^m}\{\mathbf{h}-\mathbf{t}\}\|_{\hat{\mathbb{D}}^m} + \|1_C \cdot \mathcal{F}_{\mathbb{T}^m}\{\mathbf{h}-\mathbf{t}\}\|_{\mathbb{Z}^m}.\end{aligned}$$

We now observe that

$$\begin{aligned}\|1_C \cdot \mathcal{F}_G\{\mathbf{h}-\mathbf{t}\}\|_{2,\hat{G}} \leq \|\mathcal{F}_G\{\mathbf{h}-\mathbf{t}\}\|_{2,\hat{G}} = \|\mathbf{h}-\mathbf{t}\|_{2,G} \leq \sqrt{\mu(G)}\|\mathbf{h}-\mathbf{t}\|_\infty \\ \leq \sqrt{\mu(G)} \cdot \pi\sqrt{m}\,\mathrm{Lip}(\mathbf{h})/q,\end{aligned}$$

where $\mu(G) = \int_G d\mu$ denotes the total measure of G. We conclude by noting that $\mu(G) = 1$ for both groups at hand $G = \mathbb{D}^m$ and $G = \mathbb{T}^m$. □

[3] In Appendix A.4, we provide a slight generalization of Yudin's paper [Yud76] to functions with vectorial output. In principle the bound of Theorem 2.8 can also derived without this generalization, but at the cost of an undesirable extra factor $\dim \mathcal{H} = 2^n$.

2.3. Number Theory

2.3.1. Algebraic Number Theory

In this thesis is assumed that the reader is somewhat familiar with the main concepts of algebraic number theory. In this section, we very briefly introduce definitions and notions required for this thesis. For a more elaborate explanation, I would suggest Neukirch's textbook [NS13].

Throughout this thesis, we use a fixed number field K of degree $n \geq 3$ over $\mathbb{Q}$, having ring of integers $\mathcal{O}_K$, discriminant Δ_K, regulator R_K, class number h_K and group of roots of unity μ_K. Elements of the number field K are generally denoted by lowercase Greek letters, α, β, γ, etc. Minkowski's theorem [Min67, p. 261–264] states[4] that $\log|\Delta_K| \geq \log(2) \cdot n$. The number field K has n field embeddings into $\mathbb{C}$, which are divided in $n_{\mathbb{R}}$ real embeddings and $n_{\mathbb{C}}$ conjugate pairs of complex embeddings, i.e., $n = n_{\mathbb{R}} + 2n_{\mathbb{C}}$. These embeddings combined yield the so-called Minkowski embedding $K \to K_{\mathbb{R}} \subseteq \bigoplus_{\sigma:K\hookrightarrow\mathbb{C}} \mathbb{C}$, $\alpha \mapsto (\sigma(\alpha))_\sigma$, where

$$K_{\mathbb{R}} = \left\{ x \in \bigoplus_{\sigma:K\hookrightarrow\mathbb{C}} \mathbb{C} \;\middle|\; x_{\overline{\sigma}} = \overline{x_\sigma} \right\}.$$

Here, $\overline{\sigma}$ equals the conjugate embedding of σ whenever σ is a complex embedding and it is just σ itself whenever it is a real embedding. Note that we index the components of the vectors in $K_{\mathbb{R}}$ by the embeddings of K. Embeddings up to conjugation are called infinite places, denoted by ν. With any embedding σ we denote by ν_σ the associated place; and for any place ν we choose a fixed embedding σ_ν. There are also *finite* places ν, which are in one-to-one correspondence with the prime ideals of $\mathcal{O}_K$. For finite places $\nu \nmid \infty$ we denote by $\mathfrak{p}_\nu \in \mathcal{I}_K$ their associated prime ideal, for infinite places $\nu \mid \infty$ we denote by σ_ν their (chosen) associated embedding.

Composing the Minkowski embedding by the component-wise logarithm of

[4] By Minkowski's theorem, we have $|\Delta_K|^{1/n} \geq \pi/4 \cdot \frac{n^2}{(n!)^{2/n}} \geq 2$ for $n \geq 3$.

the entries' absolute values yields the logarithmic map, denoted by Log.

$$\mathrm{Log} : K^* \to \mathrm{Log}\, K_{\mathbb{R}} \subseteq \bigoplus_{\sigma : K \hookrightarrow \mathbb{C}} \mathbb{R}, \ \alpha \mapsto (\log |\sigma(\alpha)|)_\sigma.$$

The multiplicative group of integral units $\mathcal{O}_K^\times$ under the logarithmic map forms a lattice, namely the lattice $\Lambda_K = \mathrm{Log}(\mathcal{O}_K^\times) \subseteq \mathrm{Log}\, K_{\mathbb{R}}$ (see Section 2.5.1 for the preliminaries on lattices). This so-called logarithmic unit lattice has rank $\mathbb{r} = n_{\mathbb{R}} + n_{\mathbb{C}} - 1$, is orthogonal to the all-one vector $(1)_\sigma$, and has covolume $\mathrm{Vol}(\Lambda_K) = \sqrt{n} \cdot 2^{-n_{\mathbb{C}}/2} \cdot R_K$, where the $2^{-n_{\mathbb{C}}/2}$ factor is due to the specific embedding we use (see Lemma A.2). We denote by $H = \mathrm{Span}(\Lambda_K)$ the hyperplane of dimension $\mathbb{r}$, which can also be defined as the subspace $\mathrm{Log}(K_{\mathbb{R}}^0)$ of $\mathrm{Log}\, K_{\mathbb{R}}$, where

$$K_{\mathbb{R}}^0 = \{x \in K_{\mathbb{R}} \mid \prod_{\sigma : K \hookrightarrow \mathbb{C}} |x_\sigma| = 1\}.$$

In other words, $H = \log K_{\mathbb{R}}^0$ is the subspace of $\mathrm{Log}\, K_{\mathbb{R}}$ orthogonal to the all-one vector $(1)_\sigma$. We denote by $T = H/\Lambda_K$ the hypertorus defined by the logarithmic unit lattice Λ_K. Note that $K_{\mathbb{R}} \simeq \prod_\nu K_\nu$, where ν ranges over all infinite places of K, and $K_\nu = \mathbb{C}$ of $\mathbb{R}$ depending on whether ν is complex or real respectively. In some cases it is more convenient to use this particular viewpoint of $K_{\mathbb{R}}$. Note that $K_{\mathbb{R}}^0$ can then be identified with

$$K_{\mathbb{R}}^0 = \{x \in \prod_{\nu|\infty} K_\nu \mid \prod_{\nu|\infty} |x_\nu|_{\mathbb{C}}^{[K_\nu:\mathbb{R}]} = 1\}. \tag{2.10}$$

Note that we take the usual complex absolute value here, which is raised to the power two whenever $K_\nu = \mathbb{C}$ and to the power one otherwise.

Fractional ideals of the number field K are denoted by $\mathfrak{a}, \mathfrak{b}, \ldots$, but the symbols $\mathfrak{p}, \mathfrak{q}$ are generally reserved for integral prime ideals of $\mathcal{O}_K$. Also, the symbol $\mathfrak{m}$ is reserved for the modulus ideal $\mathfrak{m} \subseteq \mathcal{O}_K$, a notion from class field theory. One can think of the primes dividing $\mathfrak{m}$ as the primes 'to avoid'. For $\mathfrak{a} \in \mathcal{I}_K$, we denote $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = \max\{k \mid \mathfrak{p}^k \text{ divides } \mathfrak{a}\}$ for the $\mathfrak{p}$-valuation of the ideal $\mathfrak{a}$; this can be generalized for elements $\alpha \in K^*$ by considering the principal ideal generated by that element. The group of fractional ideals of K is denoted by $\mathcal{I}_K$; the group of fractional ideals coprime with $\mathfrak{m}$ is

denoted by $\mathcal{I}_K^{\mathfrak{m}}$. Principal ideals with generator $\alpha \in K^*$ are usually denoted by (α). We denote by $K^{\mathfrak{m},1} = \langle \alpha \in \mathcal{O}_K \mid \alpha \equiv 1 \bmod \mathfrak{m} \rangle$ the *ray* modulo $\mathfrak{m}$, i.e., the multiplicative subgroup of K^* generated by elements in $\mathcal{O}_K$ that are one modulo $\mathfrak{m}$. In many texts the modulus can also include infinite primes (i.e., embeddings into $\mathbb{C}$); not in this thesis.

For any integral ideal $\mathfrak{a}$, we define the norm $\mathcal{N}(\mathfrak{a})$ of $\mathfrak{a}$ to be the number $|\mathcal{O}_K/\mathfrak{a}|$; this norm then generalizes to fractional ideals and elements as well. The class group of $\mathcal{O}_K$, denoted by Cl_K, is the quotient of the group $\mathcal{I}_K$ by the subgroup of principal ideals $\mathrm{Princ}_K := \{(\alpha) \in \mathcal{I}_K \mid \alpha \in K\}$. For any fractional ideal $\mathfrak{a}$, we denote the ideal class of $\mathfrak{a}$ in Cl_K by $[\mathfrak{a}]$.

In some parts of this thesis we need the notion of the *idèle group* $\mathcal{J}_K$, which is a topological group defined by the restricted topological product of the completions of the number field K over all places $\prod_\nu K_\nu^*$ where the restriction is with respect to the unit groups $\mathcal{O}_\nu^\times \subseteq K_\nu^*$. For a modulus $\mathfrak{m}$, the idèle group modulo $\mathfrak{m}$, $\mathcal{J}_{K^{\mathfrak{m}}}$, is defined similarly, by just leaving out the completions whose place are associated with a prime dividing $\mathfrak{m}$. For any modulus $\mathfrak{m}$, the ray $K^{\mathfrak{m},1}$ embeds diagonally into $\mathcal{J}_{K^{\mathfrak{m}}}$, by $\alpha \longmapsto (\alpha_\nu)_\nu \in \mathcal{J}_{K^{\mathfrak{m}}}$. Each component of this diagonal map is just the embedding of the completion $K \to K_\nu$. The quotient of the idèle group (modulo $\mathfrak{m}$) and the ray is called the *idèle class group* $\mathcal{C}_K$, which can be shown to be the same for any modulus $\mathfrak{m}$ (see [Lan12, Ch. VII, §4]).

In this thesis, extra attention is paid to the cyclotomic number fields $K = \mathbb{Q}(\zeta_m)$, for which one can sometimes phrase sharper results due to the fact thats these fields have more structure. The result in Chapter 5 tailored to cyclotomic fields relies on the size of the class group $h_K^+ = |\mathrm{Cl}_{K^+}|$ of the maximum real subfield $K^+ = \mathbb{Q}(\zeta_m + \bar{\zeta}_m)$ of K, which is conjectured to be rather small [Mil15; BPR04]. In Chapter 5, we make the mild assumption that $h_K^+ \leq (\log n)^{O(n)}$, where $n = [K : \mathbb{Q}] = \phi(m)$.

An important identity that will play a large role throughout this thesis is the *class number formula*, which relates multiple number-theoretic quantities with the residue at $s = 1$ of the Dedekind zeta function $\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{\mathcal{N}(\mathfrak{a})^s}$.

$$\rho_K = \lim_{s\to 1}(s-1)\zeta_K(s)\frac{2^{n_{\mathbb{R}}}\cdot(2\pi)^{n_{\mathbb{C}}}\cdot R_K\cdot h_K}{|\mu_K|\cdot\sqrt{|\Delta_K|}}. \tag{2.11}$$

2.3.2. The Extended Riemann Hypothesis

Almost all results in this paper rely heavily on the *Extended Riemann Hypothesis* (in the subsequent part of this paper abbreviated by ERH), which refers to the Riemann Hypothesis extended to Hecke L-functions (see [IKS04, §5.7]). All statements that mention (ERH), such as Theorem 4.3, assume the Extended Riemann Hypothesis.

Definition 2.9 (Hecke L-function)**.** *Let K be a number field and let $\chi : \mathcal{J}_{K^{\mathfrak{m}}}/K^{\mathfrak{m},1} \to S^1$ be a Hecke character on the idèle class group $\mathcal{C}_K = \mathcal{J}_{K^{\mathfrak{m}}}/K^{\mathfrak{m},1}$ of K (see [NS13, Ch. VI and Ch. VII, §6] and Section 4.3.4) defined modulo its conductor $\mathfrak{m}$. Then we define*

$$L(\chi, s) = \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K \\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s}$$

to be the associated Hecke L-function, where the sum ranges over all integral ideals of the maximal order $\mathcal{O}_K$ of K, coprime with the modulus $\mathfrak{m}$ (see, for example [Neu85, Ch. V, Def. 3.1]).

Definition 2.10 (Extended Riemann Hypothesis)**.** *For all number fields K and all Hecke characters χ, all zeroes of the Hecke L-functions that are in the critical strip $0 < Re(s) < 1$, satisfy $Re(s) = 1/2$. I.e., for all number fields K, Hecke characters χ and all complex numbers $s \in \mathbb{C}$,*

$$[L(\chi, s) = 0 \text{ and } Re(s) \in (0,1)] \implies Re(s) = 1/2.$$

Remark 2.11. *Most of the results in this thesis are phrased in terms of a* fixed *number field K. In such a case it is of course not needed to assume the Extended Riemann Hypothesis for* all *number fields; it suffices*

to assume the Extended Riemann Hypothesis for Hecke L-functions arising from Hecke-characters for the fixed number field K.

So, if a theorem in this thesis regards only a single number field K, and it assumes the Extended Riemann Hypothesis, one may weaken this hypothesis to the Extended Riemann Hypothesis 'tailored to K'.

2.3.3. Prime Densities

In multiple parts of this paper, we need an estimate on the number of prime ideals with bounded norm. This is achieved in the following theorem, obtained from Bach and Shallit's book [BS96, Thm. 8.7.4].

Theorem 2.12 (ERH)**.** *Let $\pi_K(x)$ be the number of prime ideals of K of norm $\leq x$. Then, assuming the Extended Riemann Hypothesis, there exists an absolute constant C (i.e., independent of K and x) such that, for all $x \geq 2$,*

$$|\pi_K(x) - \mathrm{li}(x)| \leq C \cdot \sqrt{x}\,(n \log x + \log|\Delta_K|)\,,$$

where $\mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t} \sim \frac{x}{\ln x}$.

In certain cases, we prefer a more explicit variant of this theorem that is due to Grenié and Molteni [GM15, Cor. 1.4].

Lemma 2.13 (ERH)**.** *Let $\mathfrak{m} \subseteq \mathcal{O}_K$ be an ideal modulus and denote*

$$\pi_K^{\mathfrak{m}}(x) = |\{\mathfrak{p} \in \mathcal{I}_K^{\mathfrak{m}} \mid \mathfrak{p} \text{ prime and } \mathcal{N}(\mathfrak{p}) \leq x\}|$$

for the number of prime ideals not dividing $\mathfrak{m}$ and having norm bounded by $x \in \mathbb{R}$. Let $\omega(\mathfrak{m})$ denote the number of different prime ideal divisors of $\mathfrak{m}$.

Then, for all $x \geq \max((12\log|\Delta_K| + 8n + 28)^4, 3 \cdot 10^{11}, 16 \cdot \omega(\mathfrak{m})^2)$, we have

$$\pi_K^{\mathfrak{m}}(x) \geq \frac{x}{4 \ln x}.$$

Proof. Denote $\pi_K(x) = |\{\mathfrak{p} \in \mathcal{I}_K \mid \mathfrak{p} \text{ prime and } \mathcal{N}(\mathfrak{p}) \leq x\}|$, i.e., whenever $\mathfrak{m} = \mathcal{O}_K$. We will prove the statement for this specific case first. By simplifying an explicit result of Grenié and Molteni [GM15, Cor. 1.4], we obtain, under the Extended Riemann Hypothesis[5],

$$\left|\pi_K(x) - \pi_K(3) - \int_3^x \frac{du}{\log u}\right| \leq \sqrt{x}[6\log|\Delta_K| + 4n\log x + 14].$$

Therefore, we have

$$\begin{aligned}\pi_K(x) &\geq \int_3^x \frac{du}{\log u} - \sqrt{x}[6\log|\Delta_K| + 4n\log x + 14] \\ &\geq \frac{x}{\ln x} - \sqrt{x}\ln(x)[6\log|\Delta_K| + 4n + 14] \\ &= \frac{x}{\ln x}\left(1 - \frac{\ln(x)^2(6\log|\Delta_K| + 4n + 14)}{\sqrt{x}}\right) \geq \frac{x}{2\ln x}\end{aligned}$$

where the first inequality follows from omitting $\pi_K(3)$ and the second inequality from $\int_3^x \frac{du}{\ln u} \geq \frac{x}{\ln x}$ and from the assumption that $x > 2^4 \cdot (6\log|\Delta_K| + 4n+14)^4$ and $x > 3\cdot 10^{11}$. Note that with such x, we have $\ln(x)^2/\sqrt{x} < x^{-1/4}$, so that $\frac{\ln(x)^2(6\log|\Delta_K|+4n+14)}{\sqrt{x}} < 1/2$.

For the general case of $\mathfrak{m} \neq \mathcal{O}_K$, we need to avoid $\mathfrak{m}$; so writing $\omega(\mathfrak{m})$ for the number of different prime ideals dividing $\mathfrak{m}$, we obtain

$$\pi_K^{\mathfrak{m}}(x) \geq \pi_K(x) - \omega(\mathfrak{m}) \geq \frac{x}{2\ln x}\left(1 - \frac{2\cdot\omega(\mathfrak{m})\cdot\ln x}{x}\right) \geq \frac{x}{4\ln x}.$$

Where the last inequality can be deduced as follows. Since $x > 3\cdot 10^{11}$, surely $\frac{\ln x}{x} \leq x^{-1/2} \leq (4\cdot\omega(\mathfrak{m}))^{-1}$ and therefore $\frac{2\cdot\omega(\mathfrak{m})\cdot\ln x}{x} \leq 1/2$. This proves the claim. □

Lemma 2.14 (Sampling of prime ideals, ERH)**.** *Let a basis of $\mathcal{O}_K$ be known and let $\mathcal{P} = \{\mathfrak{p}$ prime ideal of $K \mid \mathcal{N}(\mathfrak{p}) \leq B\}$ be the set of prime ideals of norm bounded by $B \geq \max((12\log|\Delta_K| + 8n + 28)^4, 3\cdot 10^{11})$. Then one can sample uniformly from $\mathcal{P}$ in expected time $O(n^3\log^2 B)$.*

[5] In the paper of Grenié and Molteni [GM15, Cor. 1.4], only the Dedekind zeta function $\zeta_K(s) = \sum_{\mathfrak{a}} \mathcal{N}(\mathfrak{a})^{-s}$ needs to satisfy the condition that all of its non-trivial zeroes lie at the vertical line $\Re(s) = 1/2$.

Proof. The sampling algorithm can be described as follows. Sample an integer uniformly in $[0, B]$ and check if it is a prime. If it is, factor the obtained prime p in $\mathcal{O}_K$ and list the different prime ideal factors $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ that have norm bounded by B. Choose one $\mathfrak{p}_i$ uniformly as random in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ and output it with probability k/n. Otherwise, output 'failure'.

Let $\mathfrak{q} \in \mathcal{P}$ be arbitrary, and let $\mathcal{N}(\mathfrak{q}) = q^j$ with q prime. Then, the probability of sampling $\mathfrak{q}$ equals $\frac{1}{nB}$, namely $\frac{1}{n}$ times the probability of sampling q. Therefore, the probability of sampling successfully (i.e., no failure) equals $\frac{|\mathcal{P}|}{nB} \geq \frac{1}{2n \log B}$, since $|\mathcal{P}| \geq \frac{B}{2 \log B}$, by Lemma 2.13.

The most costly part of the algorithm is the factorization of a rational prime $p \leq B$ into prime ideals of $\mathcal{O}_K$. This can be performed using the Kummer-Dedekind algorithm, which essentially amounts to factoring a degree n polynomial modulo p. Using Shoup's algorithm [Sho95] (which has complexity $O(n^2 + n \log p)$ [GP01, §4.1]) yields the complexity claim. □

2.4. Arakelov Theory

2.4.1. The Arakelov Ray Divisor Group

The *Arakelov ray divisor group* with respect to a modulus $\mathfrak{m} \subseteq \mathcal{O}_K$ is the group

$$\mathrm{Div}_{K^{\mathfrak{m}}} = \bigoplus_{\mathfrak{p} \nmid \mathfrak{m}} \mathbb{Z} \times \bigoplus_{\nu} \mathbb{R}$$

where $\mathfrak{p}$ ranges over the set of all prime ideals of $\mathcal{O}_K$ that do not divide the modulus $\mathfrak{m}$, and ν over the set of infinite primes (embeddings into the complex numbers up to possible conjugation). For readers that are not yet familiar with Arakelov ray divisor groups is might be insightful to first consider the ordinary Arakelov divisor group, which is obtained by putting $\mathfrak{m} = \mathcal{O}_K$.

We write an arbitrary element in $\mathrm{Div}_{K^{\mathfrak{m}}}$ as

$$\mathbf{a} = \sum_{\mathfrak{p} \nmid \mathfrak{m}} n_{\mathfrak{p}} \cdot (\!|\mathfrak{p}|\!) + \sum_{\nu} x_{\nu} \cdot (\!|\nu|\!),$$

with only finitely many non-zero $n_\mathfrak{p}$. We will consistently use the symbols $\mathbf{a}, \mathbf{b}, \mathbf{e}, \ldots$ for Arakelov ray divisors. Denoting $\mathrm{ord}_\mathfrak{p}$ for the valuation at the prime $\mathfrak{p}$, there is a canonical homomorphism

$$(\!|\cdot|\!) : K^{\mathfrak{m},1} \to \mathrm{Div}_{K^\mathfrak{m}}, \quad \alpha \longmapsto \sum_{\mathfrak{p} \nmid \mathfrak{m}} \mathrm{ord}_\mathfrak{p}(\alpha)(\!|\mathfrak{p}|\!) - \sum_\nu \log|\sigma_\nu(\alpha)| \cdot (\!|\nu|\!).$$

The divisors of the form $(\!|\alpha|\!)$ for $\alpha \in K^{\mathfrak{m},1}$ are called *principal ray divisors*. Here, $K^{\mathfrak{m},1} = \langle \alpha \in \mathcal{O}_K \mid \alpha \equiv 1 \bmod \mathfrak{m} \rangle$ is the multiplicative subgroup of K^* generated by elements equivalent to one modulo $\mathfrak{m}$. We will also make use of the notation $K^\mathfrak{m} = \langle \alpha \in \mathcal{O}_K \mid \alpha \bmod \mathfrak{m} \in (\mathcal{O}_K/\mathfrak{m})^* \rangle$, the multiplicative subgroup of K^* generated by elements coprime to $\mathfrak{m}$. Note that $K^{\mathfrak{m},1} \subseteq K^\mathfrak{m}$.

Just as the ideal ray class group is the group of ideals coprime with $\mathfrak{m}$ quotiented by the 'ray' $K^{\mathfrak{m},1}$, the *Picard ray group* is the group of Arakelov ray divisors quotiented by the group of principal ray Arakelov divisors. In other words, the Picard ray group $\mathrm{Pic}_{K^\mathfrak{m}}$ is defined by the following exact sequence, where $\mu_{K^{\mathfrak{m},1}} = \mu_K \cap K^{\mathfrak{m},1}$, the roots of unity in the ray.

$$0 \to \mu_{K^{\mathfrak{m},1}} \to K^{\mathfrak{m},1} \xrightarrow{(\!|\cdot|\!)} \mathrm{Div}_{K^\mathfrak{m}} \to \mathrm{Pic}_{K^\mathfrak{m}} \to 0.$$

For any Arakelov ray divisor $\mathbf{a} = \sum_{\mathfrak{p} \nmid \mathfrak{m}} n_\mathfrak{p} \cdot (\!|\mathfrak{p}|\!) + \sum_\nu x_\nu \cdot (\!|\nu|\!)$, we denote its class in the Picard ray group $\mathrm{Pic}_{K^\mathfrak{m}}$ by $[\mathbf{a}]$; in the same fashion that $[\mathfrak{a}]$ denotes the ideal class of the ideal $\mathfrak{a}$.

2.4.2. The Arakelov Ray Class Group

Despite the Arakelov ray divisor group and Picard ray group being interesting groups, it is for our purposes more useful to consider the *degree-zero* subgroups of these groups. The degree map is defined as follows:

$$\begin{aligned} &\deg : \mathrm{Div}_{K^\mathfrak{m}} \to \mathbb{R}, \\ &\sum_{\mathfrak{p} \nmid \mathfrak{m}} n_\mathfrak{p} \cdot (\!|\mathfrak{p}|\!) + \sum_\nu x_\nu \cdot (\!|\nu|\!) \mapsto \sum_{\mathfrak{p} \nmid \mathfrak{m}} n_\mathfrak{p} \cdot \log(\mathcal{N}(\mathfrak{p})) + \sum_{\nu \text{ real}} x_\nu + \sum_{\nu \text{ complex}} 2 \cdot x_\nu. \end{aligned} \tag{2.12}$$

The degree map sends principal ray divisors $(\!|\alpha|\!)$ for $\alpha \in K^{\mathfrak{m},1}$ to zero; therefore, the degree map is properly defined on $\mathrm{Pic}_{K^{\mathfrak{m}}}$, as well. We subsequently define the *degree-zero Arakelov ray divisor group* $\mathrm{Div}^0_{K^{\mathfrak{m}}} = \{\mathbf{a} \in \mathrm{Div}_{K^{\mathfrak{m}}} \mid \deg(\mathbf{a}) = 0\}$ and the *Arakelov ray class group* $\mathrm{Pic}^0_{K^{\mathfrak{m}}} = \{[\mathbf{a}] \in \mathrm{Pic}_{K^{\mathfrak{m}}} \mid \deg([\mathbf{a}]) = 0\}$. In other words, the group consisting of the degree zero Picard ray classes is called the Arakelov ray class group.

Any Arakelov ray divisor $\mathbf{a} \in \mathrm{Div}^0_{K^{\mathfrak{m}}}$ can be decomposed in a finite and an infinite part, $\mathbf{a} = \mathbf{a}_{\mathrm{f}} + \mathbf{a}_\infty$.

$$\mathbf{a} = \underbrace{\sum_{\mathfrak{p} \nmid \mathfrak{m}} n_{\mathfrak{p}} \cdot (\!|\mathfrak{p}|\!)}_{\mathbf{a}_{\mathrm{f}}} + \underbrace{\sum_{\nu} x_\nu \cdot (\!|\nu|\!)}_{\mathbf{a}_\infty} \tag{2.13}$$

The finite part $\mathbf{a}_{\mathrm{f}}$, that consists of a formal integer sum of prime ideals, can be uniquely associated with an ideal in $\mathcal{I}_K^{\mathfrak{m}}$, i.e., we have

$$\mathrm{Exp}(\cdot_{\mathrm{f}}) : \mathrm{Div}^0_{K^{\mathfrak{m}}} \to \mathcal{I}_K^{\mathfrak{m}}, \quad \mathbf{a} \mapsto \mathrm{Exp}(\mathbf{a}_{\mathrm{f}}) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \mathfrak{p}^{n_{\mathfrak{p}}},$$

where we use the exponential function Exp to denote the map sending $\sum_{\mathfrak{p} \mid \mathfrak{m}} n_{\mathfrak{p}} (\!|\mathfrak{p}|\!)$ to $\prod_{\mathfrak{p} \nmid \mathfrak{m}} \mathfrak{p}^{n_{\mathfrak{p}}}$. This map $\mathrm{Exp}(\cdot_{\mathrm{f}}) : \mathrm{Div}^0_{K^{\mathfrak{m}}} \to \mathcal{I}_K^{\mathfrak{m}}$ has the hyperplane H as kernel via the inclusion $H \hookrightarrow \mathrm{Div}^0_{K^{\mathfrak{m}}}$ and admits a section $d^0 : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Div}^0_{K^{\mathfrak{m}}}$, defined by the following rule.

$$d^0 : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Div}^0_{K^{\mathfrak{m}}}, \ \mathfrak{a} \longmapsto \sum_{\mathfrak{p} \nmid \mathfrak{m}} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \cdot (\!|\mathfrak{p}|\!) - \frac{\log(\mathcal{N}(\mathfrak{a}))}{n} \sum_{\nu} (\!|\nu|\!). \tag{2.14}$$

Occasionally, we also use the non-normalized version of d^0, called $d : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Div}_{K^{\mathfrak{m}}}$, which maps into $\mathrm{Div}_{K^{\mathfrak{m}}}$ instead.

$$d : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Div}_{K^{\mathfrak{m}}}, \ \mathfrak{a} \longmapsto \sum_{\mathfrak{p} \nmid \mathfrak{m}} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \cdot (\!|\mathfrak{p}|\!).$$

The infinite part $\mathbf{a}_\infty$ of $\mathbf{a}$ consists of a formal real sum of infinite places, which can be mapped into $K_{\mathbb{R}}$,

$$\mathrm{Exp}(\cdot_\infty) : \mathrm{Div}^0_{K^{\mathfrak{m}}} \to K_{\mathbb{R}}, \quad \mathbf{a} \mapsto \mathrm{Exp}(\mathbf{a}_\infty) = (e^{x_{\nu\sigma}})_\sigma \in K_{\mathbb{R}}.$$

2.4.3. Relation with Other Number-theoretic Groups

The groups and their relations treated above fit nicely in the diagram of exact sequences given in Figure 2.8, where the middle row sequence splits with the section d^0. In this diagram we use the notations $\mathcal{O}_{K^{\mathfrak{m},1}}^{\times} = \mathcal{O}_K^{\times} \cap K^{\mathfrak{m},1}$, $\mu_{K^{\mathfrak{m},1}} = \mu_K \cap K^{\mathfrak{m},1}$ and $\mathrm{Princ}_K^{\mathfrak{m}} = \{(\alpha) \mid \alpha \in K^{\mathfrak{m},1}\} \subseteq \mathcal{I}_K^{\mathfrak{m}}$. The group $\mathrm{Cl}_K^{\mathfrak{m}}$ is called the ideal ray class group with respect to $\mathfrak{m}$ and is defined by the exact sequence involved; the group $T^{\mathfrak{m}} = H/\Lambda_{K^{\mathfrak{m},1}}$ is the 'logarithmic ray unit torus', with $\Lambda_{K^{\mathfrak{m},1}} = \mathrm{Log}(\mathcal{O}_{K^{\mathfrak{m},1}}^{\times}) = \{(\log|\sigma(\eta)|)_\sigma \mid \eta \in \mathcal{O}_{K^{\mathfrak{m},1}}^{\times}\}$.

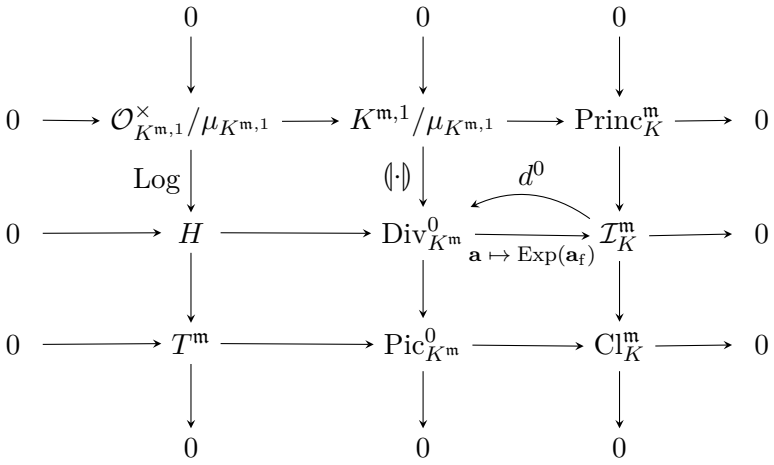


Figure 2.8.: A commutative diagram of short exact sequences involving the Arakelov ray class group.

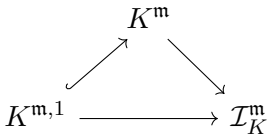
The (ray) unit groups $\mathcal{O}_K, \mathcal{O}_{K^{\mathfrak{m},1}}^{\times}$, the (ray) class groups $\mathrm{Cl}_K, \mathrm{Cl}_K^{\mathfrak{m}}$, and the ray groups $K^{\mathfrak{m},1}$ and $K^{\mathfrak{m}}$ are tightly related by an exact sequence. With this exact sequence one can relate the (relative) cardinalities of these groups.

Lemma 2.15. *Let K be a number field and let $\mathfrak{m} \subseteq \mathcal{O}_K$ be any modulus. Then we have the following exact sequence of groups*

$$0 \to \mathcal{O}_{K^{\mathfrak{m},1}}^{\times} \to \mathcal{O}_K^{\times} \to K^{\mathfrak{m}}/K^{\mathfrak{m},1} \to \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}_K \to 0.$$

In particular, $|\mathcal{O}_K^{\times}/\mathcal{O}_{K^{\mathfrak{m},1}}^{\times}| \cdot |\mathrm{Cl}_K^{\mathfrak{m}}| = \phi(\mathfrak{m}) \cdot |\mathrm{Cl}_K|$, where $\phi(\mathfrak{m}) = |K^{\mathfrak{m}}/K^{\mathfrak{m},1}|$ $= |(\mathcal{O}_K/\mathfrak{m})^*|$.

Proof. By considering the kernel-cokernel exact sequence (see Figure A.1) of the commutative triangle



one obtains the exact sequence

$$0 \to \mathcal{O}_{K^{\mathfrak{m},1}}^{\times} \to \mathcal{O}_K^{\times} \to K^{\mathfrak{m}}/K^{\mathfrak{m},1} \to \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}_K \to 0,$$

where we use the fact that $\mathcal{I}_K^{\mathfrak{m}}/K^{\mathfrak{m}} \simeq \mathrm{Cl}_K$ by the approximation theorem [Chi08, Ch. 3, Thm. 1.1]. In particular, one can 'compress' this sequence to an exact sequence of finite groups

$$0 \to \mathcal{O}_K^{\times}/\mathcal{O}_{K^{\mathfrak{m},1}}^{\times} \to K^{\mathfrak{m}}/K^{\mathfrak{m},1} \to \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}_K \to 0,$$

yielding $|\mathcal{O}_K^{\times}/\mathcal{O}_{K^{\mathfrak{m},1}}^{\times}| \cdot |\,\mathrm{Cl}_K^{\mathfrak{m}}\,| = |K^{\mathfrak{m}}/K^{\mathfrak{m},1}| \cdot |\,\mathrm{Cl}_K\,|$. The isomorphism between $K^{\mathfrak{m}}/K^{\mathfrak{m},1}$ and $(\mathcal{O}_K/\mathfrak{m})^*$ follows from the following short exact sequence, where the map $K^{\mathfrak{m}} \to (\mathcal{O}_K/\mathfrak{m})^*$ sends $\kappa/\kappa' \in K^{\mathfrak{m}}$ to $(\kappa \bmod \mathfrak{m}) \cdot (\kappa' \bmod \mathfrak{m})^{-1} \in (\mathcal{O}_K/\mathfrak{m})^*$.

$$0 \to K^{\mathfrak{m},1} \to K^{\mathfrak{m}} \to (\mathcal{O}_K/\mathfrak{m})^* \to 0$$

□

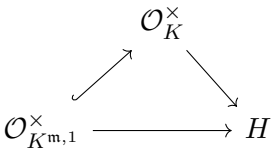
One would expect that the ray unit torus $T^{\mathfrak{m}} = H/\operatorname{Log}(\mathcal{O}_{K^{\mathfrak{m},1}}^{\times})$ and the unit torus $T = H/\operatorname{Log}(\mathcal{O}_K^{\times})$ differ in volume by $|\mathcal{O}_K^{\times}/\mathcal{O}_{K^{\mathfrak{m},1}}^{\times}|$. This is true, up to a correction for whenever the modulus $\mathfrak{m}$ causes $K^{\mathfrak{m},1}$ to have less roots of unity. This happens whenever $\zeta \not\equiv 1$ modulo $\mathfrak{m}$ for some root of unity $\zeta \in K$.

Lemma 2.16. *Let K be a number field and let $H = \log K_{\mathbb{R}}^0$ be the hyperplane where the log unit lattice $\Lambda_K = \operatorname{Log}(\mathcal{O}_K^{\times})$ and the log ray unit lattice $\Lambda_{K^{\mathfrak{m}}} = \operatorname{Log}(\mathcal{O}_{K^{\mathfrak{m},1}}^{\times})$ live in. Then we have the following exact sequence*

$$0 \to \mu_{K^{\mathfrak{m},1}} \to \mu_K \to \mathcal{O}_K^{\times}/\mathcal{O}_{K^{\mathfrak{m},1}}^{\times} \to T^{\mathfrak{m}} \to T \to 0.$$

In particular, $|\mu_{K^{\mathfrak{m},1}}| \cdot |\mathcal{O}_K^{\times}/\mathcal{O}_{K^{\mathfrak{m},1}}^{\times}| = |\mu_K| \cdot \operatorname{Vol}(T^{\mathfrak{m}})/\operatorname{Vol}(T)$.

Proof. Applying the kernel-cokernel exact sequence to the following diagram yields the result.



□

2.4.4. The Volume of the Arakelov Ray Class Group

It will be proven useful to show that the volume of the Arakelov ray class group roughly follows the square root of the field discriminant times $\phi(\mathfrak{m}) = |(\mathcal{O}_K/\mathfrak{m})^*|$.

Lemma 2.17 (Volume of $\mathrm{Pic}^0_{K^\mathfrak{m}}$)**.** *For $n = [K : \mathbb{Q}] > 1$, we have*

$$\begin{aligned} |\mathrm{Pic}^0_{K^\mathfrak{m}}| &= |\,\mathrm{Cl}_K^\mathfrak{m}\,| \cdot \mathrm{Vol}(T^\mathfrak{m}) = \frac{|\mu_{K^{\mathfrak{m},1}}|}{|\mu_K|} \cdot \phi(\mathfrak{m}) \cdot h_K \cdot \mathrm{Vol}(T) \\ &= \frac{|\mu_{K^{\mathfrak{m},1}}|}{|\mu_K|} \cdot \phi(\mathfrak{m}) h_K R_K \sqrt{n} 2^{-n_\mathbb{C}/2}, \end{aligned} \tag{2.15}$$

and

$$\log|\mathrm{Pic}^0_{K^\mathfrak{m}}| \leq \log \phi(\mathfrak{m}) + n\left(\frac{1}{2}\log(|\Delta_K|^{1/n}) + \log\log(|\Delta_K|^{1/n}) + 1\right),$$

where $\phi(\mathfrak{m}) = |(\mathcal{O}_K/\mathfrak{m})^*|$. A simpler, derived bound is

$$\log(\mathrm{Vol}(\mathrm{Pic}^0_{K^\mathfrak{m}})) \leq \log \mathcal{N}(\mathfrak{m}) + \log|\Delta_K|. \tag{2.16}$$

Proof. The first identity involving the volume of the Arakelov ray class group follows from the exact sequence in Figure 2.8. The second one can be deduced from the identities $|\,\mathrm{Cl}_K^\mathfrak{m}\,| \cdot [\mathcal{O}_K : \mathcal{O}_{K^{\mathfrak{m},1}}^\times] = \phi(\mathfrak{m}) \cdot h_K$ and $\mathrm{Vol}(T^\mathfrak{m}) = \mathrm{Vol}(T) \cdot [\mathcal{O}_K^\times : \mathcal{O}_{K^{\mathfrak{m},1}}^\times] \cdot |\mu_{K^{\mathfrak{m},1}}|/|\mu_K|$ (see Lemmas 2.15 and 2.16). The third one follows from the volume computation of T in Lemma A.2.

The bound on the logarithm is obtained by using $\frac{|\mu_{K^{\mathfrak{m}},1}|}{|\mu_K|} \leq 1$, applying the class number formula [NS13, VII.§5, Cor. 5.11] and Louboutin's bound [Lou00] on the residue ρ_K of the Dedekind zeta function at $s = 1$:

$$\begin{aligned}|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| &\leq \phi(\mathfrak{m}) h_K R_K \sqrt{n} 2^{-n_{\mathbb{C}}/2} = \frac{\phi(\mathfrak{m})\rho_K \sqrt{|\Delta_K|} \cdot |\mu_K| \cdot \sqrt{n}}{2^{n_{\mathbb{R}}}(2\sqrt{2}\pi)^{n_{\mathbb{C}}}} \\ &\leq \phi(\mathfrak{m}) \cdot \sqrt{|\Delta_K|} \cdot \rho_K \leq \phi(\mathfrak{m})\sqrt{|\Delta_K|} \left(\frac{e \log |\Delta_K|}{2(n-1)}\right)^{n-1} \\ &\leq \phi(\mathfrak{m})\sqrt{|\Delta_K|} \left(\frac{e \log |\Delta_K|}{n}\right)^{n},\end{aligned}$$

For the bound on the logarithm, we write

$$n \log(e \log |\Delta_K|/n) = n \log \log(|\Delta_K|^{1/n}) + n.$$

For the simpler bound in Equation (2.16) we use the fact that $\frac{e \log |x|}{|x|} \leq 1$ for all $x \in \mathbb{R}$. Therefore,

$$\frac{e \log \left(|\Delta_K|^{\frac{1}{2(n-1)}}\right)}{|\Delta_K|^{\frac{1}{2(n-1)}}} \leq 1,$$

and thus $\left(\frac{e \log |\Delta_K|}{2(n-1)}\right)^{n-1} \leq \sqrt{|\Delta_K|}$. □

We let $\mathcal{U}(\mathrm{Pic}^0_{K^{\mathfrak{m}}}) = \frac{1}{|\mathrm{Pic}^0_{K^{\mathfrak{m}}}|} \cdot \mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}$ denote the uniform distribution over the Arakelov ray class group.

Fourier theory over the Arakelov ray class group

As the Arakelov ray class group $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ is a compact abelian group, every function in[6] $L_2(\mathrm{Pic}^0_{K^{\mathfrak{m}}}) = \{f : \mathrm{Pic}^0_{K^{\mathfrak{m}}} \to \mathbb{C} \mid \int_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}} |f|^2 < \infty\}$ can be

[6]The measure on the Arakelov class group is unique up to scaling – it is the Haar measure. By fixing the volume of $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ as in Lemma 2.17, we fix this scaling as well. We use then *this* particular scaling of the Haar measure for the integrals over the Arakelov class group.

uniquely decomposed into a character sum

$$f = \sum_{\chi \in \widehat{\mathrm{Pic}^0_{K\mathfrak{m}}}} a_\chi \cdot \chi,$$

with $a_\chi \in \mathbb{C}$. In the proof of Theorem 4.3, we will make use of Parseval's identity [DE16, Thm. 3.4.8] (see also Theorem 2.1) in the following form.

$$\int_{\mathrm{Pic}^0_{K\mathfrak{m}}} |f|^2 = \|f\|_2^2 = \frac{1}{|\mathrm{Pic}^0_{K\mathfrak{m}}|} \sum_{\chi \in \widehat{\mathrm{Pic}^0_{K\mathfrak{m}}}} |a_\chi|^2 \tag{2.17}$$

2.4.5. An Example of an Arakelov Class Group

We compute the Arakelov class group of a totally real cubic field. Let $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathbb{C}$ is defined by the polynomial

$$f(x) = x^3 - x^2 - 9x + 10. \tag{2.18}$$

Computing the ring of integers

The discriminant of this polynomial equals $\Delta(f) = 1957 = 19 \cdot 103 > 0$. Because this is square free, the ring of integers of K equals $\mathcal{O}_K = \mathbb{Z}[\alpha]$, and $\Delta_K = 1957$. Since the discriminant is positive, the cubic field must be totally real, by Brill's theorem. The Minkowski bound can then be computed as $M_K = \sqrt{|\Delta_K|} \cdot \frac{3!}{3^3} \approx 9.83$.

Computations in the class group

The class group is therefore generated by the primes with norm at most 9.83, which are the four prime ideals $\mathfrak{p}_2, \mathfrak{q}_2, \mathfrak{p}_5, \mathfrak{q}_5$. This can be seen by factoring the polynomial $f(x)$ modulo $\mathbb{F}_p$ for $p = 2, 3, 5, 7$; noting that $f \mod 3$ and $f \mod 7$ are irreducible, and $f(x) \equiv x(x^2 + x + 1) \mod 2$ and $f(x) \equiv x(x^2 + 4x + 1) \mod 5$. We have $(2) = \mathfrak{p}_2\mathfrak{q}_2$ and $(5) = \mathfrak{p}_5\mathfrak{q}_5$, so, for the class group it is enough to consider only $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_5 = (5, \alpha)$.

Additionally, we have $(\alpha) = \mathfrak{p}_2\mathfrak{p}_5$ and $(\alpha - 2) = \mathfrak{p}_2^2$ This can be seen by computing the norms of α and $\alpha - 2$, which equal $f(0) = 10$ and $f(2) = -4$ respectively. Since $(\alpha - 2) \subseteq (2, \alpha) = \mathfrak{p}_2$ we must have $(\alpha - 2) = \mathfrak{p}_2^2$. Combining these relations yields that the class group is generated by $\mathfrak{p}_2$ and is either trivial or of order 2. We will show that the latter is the case; for that we need the fundamental units.

Computing units and (a multiple of) the regulator

The elements $\alpha - 1$ and $\alpha - 3$ are units in $\mathcal{O}_K$, since $\mathcal{N}(\alpha - 1) = f(1) = 1$ and $\mathcal{N}(\alpha - 3) = f(3) = 1$. Under the Minkowski embedding, the element α sends to $(-3.04096, 1.12946, 2.9115)$, and 1 to $(1, 1, 1)$. Therefore, the images under the Minkowski embedding of $\alpha - 1$ and $\alpha - 3$ are respectively $\approx (-4.04096, 0.12946, 1.9115)$ and $\approx (-6.04096, -1.87054, -0.0885)$. Taking the Logarithmic image of the absolute values yields $\mathrm{Log}(\alpha - 1) = (1.40, -2.04, 0.64)$ and $\mathrm{Log}(\alpha - 3) = (1.80, 0.63, -2.42)$. Putting these vectors into a matrix, one obtains

$$B = \begin{bmatrix} 1.40 & -2.04 & 0.64 \\ 1.80 & 0.63 & -2.42 \end{bmatrix}, \tag{2.19}$$

of which the absolute determinant of any 2×2 minor equals 4.554, which must be an approximation of a multiple of the regulator R_K. So surely, $R_K \leq 4.554$.

Computing an approximation of the Dedekind residue

Computing an approximation of the residue of the Dedekind zeta function $\rho_K = \lim_{s \to 1}(s - 1)\zeta_K(s)$ by means of a truncated combined Euler product, we obtain

$$\rho_K \approx \frac{\prod_{p<100}(1 - 1/p)}{\prod_{\mathcal{N}(\mathfrak{p})<100}(1 - 1/\mathcal{N}(\mathfrak{p}))} = 0.827.$$

By the class number formula (see Equation (2.11)), we have that

$$R_K h_K = \frac{\rho_K \cdot \sqrt{|\Delta_K|} \cdot |\mu_K|}{2^{n_{\mathbb{R}}} \cdot (2\pi)^{n_{\mathbb{C}}}} \approx \frac{0.827 \cdot 44.24 \cdot 2}{2^3 \cdot (2\pi)^0} = 9.15$$

Since $h_K \in \{1, 2\}$ and $R_K \leq 4.554$, we must have $h_K = 2$ and $R_K \approx 4.554$.

Assembling the Arakelov class group from the unit group and the class group

We have that $H = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$ equals the hyperplane where the logarithmic unit lattice lives in, and the log unit lattice equals $\Lambda_K = \mathcal{L}(B)$, where $\mathcal{L}(B)$ is the lattice generated by the rows of the matrix in Equation (2.19). The log unit torus is then equal to $T = H/\mathcal{L}(B)$.

The Arakelov class group Pic^0_K of the cubic field K then has two connected components, one consisting of T, and one consisting of $T + [d^0(\mathfrak{p}_2)]$ (see Equation (2.14)). The maps of the exact sequence

$$0 \to T \to \mathrm{Pic}^0_K \to \mathrm{Cl}_K \to 0$$

just consist of inclusion $T \hookrightarrow \mathrm{Pic}^0_K$ and projection $\mathrm{Pic}^0_K \to \mathrm{Cl}_K$, where $T \subseteq \mathrm{Pic}^0_K$ sends to the trivial ideal class, and $T + [d^0(\mathfrak{p}_2)]$ sends to $[\mathfrak{p}_2] \in \mathrm{Cl}_K$.

Computing elements in the Arakelov class group

We will compute the positions of $[d^0(\mathfrak{p}_5)]$, $[d^0(\mathfrak{q}_2)]$ and $[d^0(\mathfrak{p}_{17})]$ in the Arakelov class group, where $\mathfrak{p}_5 = (5, \alpha)$, $\mathfrak{q}_2 = (2, \alpha^2 + \alpha + 1)$ and $\mathfrak{p}_{17} = (17, \alpha + 1)$. This accounts to computing the discrete logarithm in the ideal class group and reducing modulo the logarithmic unit lattice.

As we have $\mathfrak{p}_5\mathfrak{p}_2 = (\alpha)$ and $\mathfrak{p}_2^2 = (\alpha - 2)$, we compute $\mathfrak{p}_5 = (\alpha)\mathfrak{p}_2^{-1} = (\alpha) \cdot (\alpha - 2)^{-1} \cdot \mathfrak{p}_2$. In terms of divisors, we have

$$(\!|\frac{\alpha}{\alpha - 2}|\!) = (\!|\mathfrak{p}_5|\!) - (\!|\mathfrak{p}_2|\!) - \mathrm{Log}(\alpha/(\alpha - 2)),$$

where we use the abbreviation $\mathrm{Log}(\beta) = \sum_\nu \log|\sigma_\nu(\beta)| \cdot (\!|\nu|\!)$. So,

$$\begin{aligned} d^0(\mathfrak{p}_5) &= (\!|\mathfrak{p}_5|\!) - \tfrac{1}{3} \cdot \mathrm{Log}(5) = (\!|\mathfrak{p}_2|\!) + (\!|\frac{\alpha}{\alpha - 2}|\!) + \mathrm{Log}(\frac{\alpha}{\alpha - 2}) - \tfrac{1}{3} \cdot \mathrm{Log}(5). \\ &= d^0(\mathfrak{p}_2) + (\!|\frac{\alpha}{\alpha - 2}|\!) + \tfrac{1}{3} \cdot \mathrm{Log}(2/5) + \mathrm{Log}(\frac{\alpha}{\alpha - 2}). \end{aligned}$$

Taking Arakelov classes, thus letting vanish the part $(\!|\alpha/(\alpha-2)|\!)$ (as it is a principal divisor), we obtain that

$$\begin{aligned}[d^0(\mathfrak{p}_5)] &= [d^0(\mathfrak{p}_2)] + \tfrac{1}{3}\cdot \mathrm{Log}(2/5) + \mathrm{Log}(\alpha/(\alpha-2)) \\ &\approx [d^0(\mathfrak{p}_2)] + (-0.81, -0.05, 0.86) \\ &\approx [d^0(\mathfrak{p}_2)] + (2.39, -1.46, -0.92) \in [d^0(\mathfrak{p}_2)] + T\end{aligned}$$

where the last computation just adds both rows of the logarithmic unit matrix from Equation (2.19) (in order to get in a fixed fundamental domain). A similar computation for $\mathfrak{q}_2$, satisfying $\mathfrak{p}_2\mathfrak{q}_2 = (2)$, gives $(\!|2/(\alpha-2)|\!) = (\!|\mathfrak{q}_2|\!) - (\!|\mathfrak{p}_2|\!) + \mathrm{Log}(2/(\alpha-2))$, and therefore

$$\begin{aligned}[d^0(\mathfrak{q}_2)] &= [d^0(\mathfrak{p}_2)] - \tfrac{1}{3}\,\mathrm{Log}(2) + \mathrm{Log}(2/(\alpha-2)) \\ &\approx [d^0(\mathfrak{p}_2)] + (-1.15, 0.60, 0.55) \\ &\approx [d^0(\mathfrak{p}_2)] + (2.05, -0.81, -1.23) \in [d^0(\mathfrak{p}_2)] + T.\end{aligned}$$

where, again, the last computation adds both rows of the logarithmic unit matrix from Equation (2.19). For $\mathfrak{p}_{17} = (17, \alpha+1)$, compute the norm of $\alpha+1$ to see that it equals 17, therefore, $(\!|\alpha+1|\!) = (\!|\mathfrak{p}_{17}|\!) - \mathrm{Log}(\alpha+1)$. This implies

$$\begin{aligned}[d^0(\mathfrak{p}_{17})] = -\tfrac{1}{3}\,\mathrm{Log}(17) + \mathrm{Log}(\alpha+1) &\approx (-0.23, -0.19, 0.42) \\ &\approx (1.57, 0.44, -2.00) \in T\end{aligned}$$

where the last computation adds the last row of the logarithmic unit matrix from Equation (2.19).

The Arakelov classes of the primes $\mathfrak{q}_2$, $\mathfrak{p}_5$ and $\mathfrak{p}_{17}$ are portrayed in Figures 2.9 and 2.10, in which the full Arakelov class group of $K = \mathbb{Q}(\alpha)$ is displayed. In Figure 2.9, the primes are visualized in a two-dimensional fundamental domain (a disjoint union of two parallelograms) whereas in Figure 2.10 the toroidal nature of the Arakelov class group is exemplified.

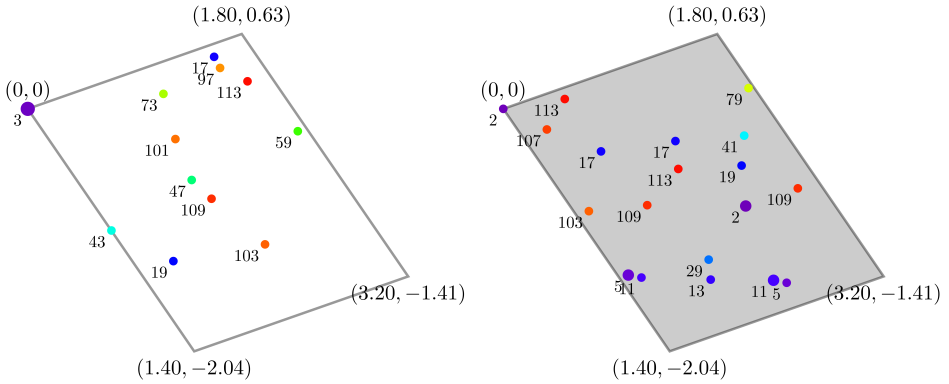


Figure 2.9.: In this picture, the Arakelov class group of $K = \mathbb{Q}(\alpha)$ is portrayed, where $\alpha \in \mathbb{C}$ is defined by the polynomial $f(x) = x^3 - x^2 - 9x + 10$. Due to the fact that the class group has order 2 and the unit group is free of rank 2, the Arakelov class group can be portrayed as a disjoint union of two parallelograms, serving as a fundamental domain. The connected component of the unit $[\mathcal{O}_K]$ is the white parallelogram on the left-hand side; the gray parallelogram is associated with the non-trivial ideal class group element. Prime ideals up to norm 113 are displayed as points, where the color hue varies with the size of the associated prime number, and the size of the point with the residue class degree of the prime ideal. The prime ideal $\mathfrak{q}_2 = (2, \alpha^2 + \alpha + 1)$ of residue class degree 2 can be seen in the gray parallelogram as the rather large dot labeled with '2'. The prime ideal $\mathfrak{p}_5 = (5, \alpha)$ is located at the right bottom of the gray parallelogram, as a purple point. The prime ideal $\mathfrak{p}_{17} = (17, \alpha + 1)$ is principal and it is therefore located in the white parallelogram, at the top right corner, as a blue point.

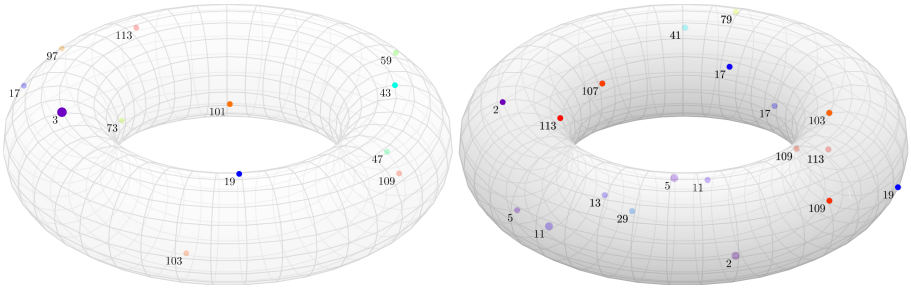


Figure 2.10.: This picture shows the Arakelov class group of the same number field K as in Figure 2.9. One obtains this image by 'gluing' the gray parallelogram into a gray torus and the white parallelogram into a white torus from Figure 2.9. The prime ideals with norms up to 113 are displayed accordingly. Note that the location of the smaller prime ideals seem to be skewed on the gray torus; but as the norms increase, the division among the two tori, but also on the tori seem to get more and more uniform. This phenomenon can be seen as a manifestation of the random walk theorem, which states that from a certain lower bound on the norms, prime ideals become more and more uniformly located on these tori; assuming the extended Riemann hypothesis (see Theorem 4.3).

2.5. Lattices

2.5.1. General Lattices

A lattice Λ is a discrete subgroup of a real vector space. In the following, we assume that this real vector space has dimension m and that the lattice is full-rank, i.e., $\mathrm{span}(\Lambda)$ equals the whole real space. A lattice can be represented by a basis $B = (\mathbf{b}_1, \cdots, \mathbf{b}_m)$ such that $\Lambda = \{\sum_i x_i \mathbf{b}_i \,,\, x_i \in \mathbb{Z}\}$. Important notions in lattice theory are the covolume $\mathrm{Vol}(\Lambda)$, which equals the volume of the hypertorus $\mathrm{span}(\Lambda)/\Lambda$ (alternatively, $\mathrm{Vol}(\Lambda)$ is the absolute determinant of any basis of Λ); the first minimum $\lambda_1(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} \|v\|$; and the last minimum $\lambda_m(\Lambda)$, which equals the minimal radius $r > 0$ such that $\{v \in \Lambda \mid \|v\| \leq r\}$ is of full rank m. The equivalent notions with respect to the maximum norm $\|\cdot\|_\infty$ instead of the Euclidean norm are denoted by $\lambda_1^{(\infty)}(\Lambda)$ and $\lambda_m^{(\infty)}(\Lambda)$. We will also use the following notation for the covering radius; $\mathrm{cov}_2(\Lambda)$ (and $\mathrm{cov}_\infty(\Lambda)$ for the maximum norm analogue), which is the minimum $r > 0$ such that any element $x \in \mathrm{span}(\Lambda)$ is at most r-close to a lattice point.

For any (full-rank) lattice $\Lambda \subseteq \mathbb{R}^m$ we denote by $\Lambda^* = \{v \in \mathbb{R}^m \mid \langle v, \ell \rangle \in \mathbb{Z} \text{ for all } \ell \in \Lambda\}$ the *dual lattice* of Λ. It is a lattice of full rank and, furthermore, for any basis B of Λ holds that $D = (B^T)^{-1}$ is a basis of Λ^*.

We will be interested into the following algorithmic problem over lattices.

Definition 2.18 (γ-Hermite Shortest Vector Problem)**.** *Given as input a basis of a rank m lattice Λ, the problem γ-Hermite-SVP consists in computing a non-zero vector $v \in \Lambda$ such that*

$$\|v\| \leq \gamma \cdot \mathrm{Vol}(\Lambda)^{1/m}.$$

2.5.2. Divisors and Ideal Lattices

It will be proven useful to view both ideals and Arakelov divisors as lattices in the real vector space $K_\mathbb{R}$, where $K_\mathbb{R}$ has its (Euclidean or maximum)

norm inherited from the complex vector space it lives in. Explicitly, the Euclidean and maximum norm of $\alpha \in K$ are respectively defined by the rules $\|\alpha\|_2^2 = \sum_\sigma |\sigma(\alpha)|^2$ and $\|\alpha\|_\infty = \max_\sigma |\sigma(\alpha)|$, where σ ranges over all embeddings $K \to \mathbb{C}$. By default, $\|\alpha\|$ refers to the Euclidean norm $\|\alpha\|_2$.

For any ideal $\mathfrak{a}$ of K, we define the associated lattice $\mathfrak{a} \subseteq K_\mathbb{R}$ to be the image of $\mathfrak{a} \subseteq K$ under the Minkowski embedding, which is clearly a discrete subgroup of $K_\mathbb{R}$. By slightly abusing the notation we both denote the ideal and the associated lattice with the same symbol $\mathfrak{a}$. In particular, $\mathcal{O}_K$ is a lattice and we will always assume throughout this thesis (except stated otherwise) that we know a $\mathbb{Z}$-basis $(\mathbf{b}_1, \cdots, \mathbf{b}_n)$ of $\mathcal{O}_K$. For Arakelov divisors $\mathbf{a} = \sum_\mathfrak{p} n_\mathfrak{p} \cdot (\!|\mathfrak{p}|\!) + \sum_\nu x_\nu \cdot (\!|\nu|\!)$, the associated lattice is defined as follows.

$$\mathrm{Exp}(\mathbf{a}) = \left\{ (e^{x_{\nu_\sigma}} \cdot \sigma(\alpha))_\sigma \mid \alpha \in \prod \mathfrak{p}^{n_\mathfrak{p}} \right\} = \mathrm{diag}\left((e^{x_{\nu_\sigma}})_\sigma\right) \cdot \prod \mathfrak{p}^{n_\mathfrak{p}} \subseteq K_\mathbb{R},$$

where diag denotes a diagonal matrix. We have $\mathrm{Vol}(\mathfrak{a}) = \sqrt{|\Delta_K|}\,\mathcal{N}(\mathfrak{a})$ for ideals $\mathfrak{a} \in \mathcal{I}_K$ and, for Arakelov divisors $\mathbf{a} \in \mathrm{Div}_K$,

$$\mathrm{Vol}(\mathrm{Exp}(\mathbf{a})) = \sqrt{|\Delta_K|} \cdot \prod_\sigma e^{x_{\nu_\sigma}} \cdot \mathcal{N}(\prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}) = \sqrt{|\Delta_K|} \cdot e^{\deg(\mathbf{a})}.$$

The associated lattice $\mathrm{Exp}(\mathbf{a})$ of a divisor is of a special kind, which we call *ideal lattices*, as in the following definition.

Definition 2.19 (Ideal lattices)**.** *Let K be a number field with ring of integers $\mathcal{O}_K$. An ideal lattice of K is a $\mathcal{O}_K$-module $I \subseteq K_\mathbb{R}$, with the additional requirement that there exists an $x \in K_\mathbb{R} \backslash \{0\}$ such that $xI \subseteq \mathcal{O}_K$. We denote the group of ideal lattices by* IdLat_K*.*

Note that the lattices $\mathfrak{a}$ for $\mathfrak{a} \in \mathcal{I}_K$ are special cases of ideal lattices, which we will call *fractional ideal lattices*. Since the Minkowski embedding is injective, the Minkowski embedding provides a bijection between the set of fractional ideals and the set of fractional ideal lattices.

The set IdLat_K of ideal lattices forms a group; the product of two ideal lattices $I = x\mathfrak{a}$ and $J = y\mathfrak{b}$ is defined by the rule $I \cdot J = xy\mathfrak{a}\mathfrak{b}$. It is clear that $\mathcal{O}_K \subseteq K_\mathbb{R}$ is the unit ideal lattice and $x^{-1}\mathfrak{a}^{-1}$ is the inverse ideal lattice of $x\mathfrak{a}$.

The map $\mathrm{Exp}(\cdot) : \mathrm{Div}_K^0 \to \mathrm{IdLat}_K, \mathbf{a} \mapsto \mathrm{Exp}(\mathbf{a})$ sends an Arakelov divisor to an ideal lattice. The image under this map is the following subgroup of IdLat_K.

$$\mathrm{IdLat}_K^0 = \{x\mathfrak{a} \mid \mathcal{N}(\mathfrak{a}) \prod_\sigma x_\sigma = 1 \text{ and } x_\sigma > 0 \text{ for all } \sigma\}.$$

Definition 2.20 (Isometry of ideal lattices)**.** *For two ideal lattices $L, L' \in \mathrm{IdLat}_K^0$, we say that L and L' are K-isometric, denoted by $L \sim L'$, when there exists $(\xi_\sigma) \in K_\mathbb{R}$ with $|\xi_\sigma| = 1$ such that $(\xi_\sigma)_\sigma \cdot L = L'$.*

In other words, we consider two ideal lattices to be K-isometric if they only differ in component-wise complex phase. Being K-isometric is an equivalence relation on IdLat_K^0 that is compatible with the group operation.

Relation between ideal lattices and Arakelov classes

Denoting $\mathrm{Iso_K}$ for the subgroup $\{L \in \mathrm{IdLat}_K^0 \mid L \sim \mathcal{O}_K\} \subset \mathrm{IdLat}_K^0$, we have the following result.

Lemma 2.21 (Arakelov classes are ideal lattices up to isometry)**.** *Denoting $P : \mathrm{IdLat}_K^0 \to \mathrm{Pic}_K^0$ for the map $x\mathfrak{a} \longmapsto \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(\mathfrak{a})[\mathfrak{p}] + \sum_\nu \log(x_{\sigma_\nu})[\nu]$ modulo principal divisors, we have the following exact sequence.*

$$0 \to \mathrm{Iso_K} \to \mathrm{IdLat}_K^0 \xrightarrow{P} \mathrm{Pic}_K^0 \to 0.$$

Proof. This is a well-known fact (e.g., [Sch08]), but we give a proof for completeness. It suffices to show that P is a well-defined surjective homomorphism and its kernel is $\mathrm{Iso_K}$. In order to be well-defined, P must satisfy $P(x\mathfrak{a}) = P(x'\mathfrak{a}')$ whenever $x\mathfrak{a} = x'\mathfrak{a}'$. Assuming the latter, we obtain $x^{-1}x'\mathcal{O}_K = (\mathfrak{a}')^{-1}\mathfrak{a} = \alpha\mathcal{O}_K$, for some $\alpha \in K^*$, as the module is a free $\mathcal{O}_K$-module. This implies that $(x^{-1}x')_\sigma = \sigma(\eta\alpha)$ for all embeddings $\sigma : K \to \mathbb{C}$, for some unit $\eta \in \mathcal{O}_K^\times$. Therefore, we have, $P(x\mathfrak{a}) - P(x'\mathfrak{a}') = \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(\alpha)[\mathfrak{p}] + \sum_\nu \log((x_{\sigma_\nu})^{-1}x'_{\sigma_\nu})[\nu] = (\!|\eta\alpha|\!)$; i.e., their difference is a principal divisor, meaning that their image in Pic_K^0 is the same.

One can check that P is a homomorphism, and its surjectivity can be proven by constructing an ideal lattice in the pre-image of a representative divisor $\mathbf{a} = \sum_{\mathfrak{p}} n_{\mathfrak{p}}[\mathfrak{p}] + \sum_{\nu} x_{\nu}[\nu] \in \mathrm{Div}_K^0$ of an Arakelov class $[\mathbf{a}]$, e.g., $(e^{x_{\nu_\sigma}})_\sigma \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$.

We finish the proof by showing that the kernel of P indeed equals $\mathrm{Iso_K}$. Suppose $x\mathfrak{a} \in \ker(P)$, i.e., $P(x\mathfrak{a}) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})[\mathfrak{p}] + \sum_{\nu} \log(x_{\sigma_\nu})[\nu] = (\!(\alpha)\!)$ is a principal divisor. This means that $\mathfrak{a} = \alpha\mathcal{O}_K$ and $x = (|\sigma(\alpha)|^{-1})_\sigma$, i.e., $x\mathfrak{a} = (|\sigma(\alpha)|^{-1})_\sigma \alpha\mathcal{O}_K = \left(\frac{\sigma(\alpha)}{|\sigma(\alpha)|}\right)_\sigma \cdot \mathcal{O}_K$, so $x\mathfrak{a} \sim \mathcal{O}_K$, implying $x\mathfrak{a} \in \mathrm{Iso_K}$. This shows that $\ker P \subseteq \mathrm{Iso_K}$. The reverse inclusion starts with the observation that $x\mathfrak{a} \sim \mathcal{O}_K$ directly implies that $\mathfrak{a} = \alpha\mathcal{O}_K$ is principal, by the fact that $x\mathfrak{a}$ is a free $\mathcal{O}_K$-module. So, $(x_\sigma\sigma(\alpha))_\sigma \cdot \mathcal{O}_K = x\alpha\mathcal{O}_K = (\xi_\sigma)_\sigma \cdot \mathcal{O}_K$ for some $(\xi_\sigma)_\sigma \in K_{\mathbb{R}}$ with $|\xi_\sigma| = 1$. Therefore, $|x_\sigma\sigma(\eta\alpha)| = |\xi_\sigma| = 1$, i.e., $|x_\sigma| = |\sigma(\eta\alpha)|^{-1}$ for some unit $\eta \in \mathcal{O}_K^\times$. From here one can directly conclude that $P(x\mathfrak{a}) = P((|\sigma(\eta\alpha)|^{-1})_\sigma \alpha\mathcal{O}_K) = (\!(\eta\alpha)\!)$, a principal divisor. □

Bounds on invariants of ideal lattices

Denote $\Gamma(\Lambda) = \lambda_n(\Lambda)/\lambda_1(\Lambda)$, and define, for a fixed number field K:

$$\Gamma_K = \sup_{\mathbf{a} \in \mathrm{Div}_K} \Gamma(\mathrm{Exp}(\mathbf{a})) \tag{2.20}$$

Recall the notion of the covering radius; $\mathrm{cov}_2(\Lambda)$ (and $\mathrm{cov}_\infty(\Lambda)$ for the maximum norm), which is the minimum $r > 0$ such that any element $x \in \mathrm{span}(\Lambda)$ is at most r-close to a lattice point. For ideal lattices, we then do have the following useful bounds, which are used often throughout this thesis.

Lemma 2.22. *For any modulus $\mathfrak{m} \subseteq \mathcal{O}_K$ and any divisor $\mathbf{a} \in \mathrm{Div}_{K^{\mathfrak{m}}}$,*

(i) $\Gamma_K \leq \lambda_n^{(\infty)}(\mathcal{O}_K) \leq |\Delta_K|^{1/n}$;
(ii) *For cyclotomic number fields K,* $\Gamma_K = 1$;
(iii) $\lambda_n(\mathrm{Exp}(\mathbf{a})) \leq \sqrt{n} \cdot \Gamma_K \cdot \mathrm{Vol}(\mathrm{Exp}(\mathbf{a}))^{1/n}$;
(iv) $\mathrm{cov}_\infty(\mathrm{Exp}(\mathbf{a})) \leq \mathrm{cov}_2(\mathrm{Exp}(\mathbf{a})) \leq n/2 \cdot \Gamma_K \cdot \mathrm{Vol}(\mathrm{Exp}(\mathbf{a}))^{1/n}$.

Proof. The bound $\lambda_n^{(\infty)}(\mathcal{O}_K) \leq |\Delta_K|^{1/n}$ can be proven by means of the techniques of [Bha+20, Thm. 3.1], as is done in Theorem A.4 of Appendix A.1. To obtain the bound $\Gamma_K \leq \lambda_n^{(\infty)}(\mathcal{O}_K)$, pick an arbitrary divisor $\mathbf{a} \in \mathrm{Div}_{K^{\mathfrak{m}}}$ and choose a shortest element $x\alpha \in \mathrm{Exp}(\mathbf{a})$ with $x = \mathrm{Exp}(\mathbf{a}_\infty)$ and $\alpha \in \mathrm{Exp}(\mathbf{a}_{\mathrm{f}}) \in \mathcal{I}_K^{\mathfrak{m}}$. That means $\|x\alpha\| = \lambda_1(\mathrm{Exp}(\mathbf{a}))$. Then $\mathrm{Exp}(\mathbf{a}) \supset x \cdot (\alpha)$, and therefore

$$\lambda_n(\mathrm{Exp}(\mathbf{a})) \leq \lambda_n(x \cdot (\alpha)) \leq \|x\alpha\|_2 \cdot \lambda_n^{(\infty)}(\mathcal{O}_K) = \lambda_1(\mathrm{Exp}(\mathbf{a})) \cdot \lambda_n^{(\infty)}(\mathcal{O}_K),$$

which proves part (i). Part (ii) follows from part (i) and the fact that $\|\zeta\| = \|1\|$ for roots of unity $\zeta \in K$. Part (iii) is essentially Minkowski's bound $\lambda_1(\mathrm{Exp}(\mathbf{a})) \leq \sqrt{n}\,\mathrm{Vol}(\mathrm{Exp}(\mathbf{a}))^{1/n}$ combined with the definition of Γ_K. The last item follows from the fact that $\mathrm{cov}_2(\Lambda) \leq \sqrt{n}/2 \cdot \lambda_n(\Lambda)$ [Mic]. □

2.5.3. The Gaussian Function and Smoothing Errors

Let n be a fixed positive integer. For any parameter $s > 0$, we consider the n-dimensional *Gaussian function*

$$\rho_s^{(n)} : \mathbb{R}^n \to \mathbb{C}\,,\ x \mapsto e^{-\frac{\pi\|x\|^2}{s^2}}\,,$$

(where we drop the (n) whenever it is clear from the context), which is well known to have the following basic properties.

Lemma 2.23. *For all $s > 0$, $n \in \mathbb{N}$ and $x, y \in \mathbb{R}^n$, we have $\int_{z\in\mathbb{R}^n} \rho_s(z)dz = s^n$, $\mathcal{F}_{\mathbb{R}^n}\{\rho_s\} = \int_{y\in\mathbb{R}^n} \rho_s(y)e^{-2\pi i\langle y,\cdot\rangle}dy = s^n\rho_{1/s}$, $\rho_s(x)^2 = \rho_{s/\sqrt{2}}(x)$. and $\sqrt{\rho_s(x)\rho_s(y)} = \rho_{2s}(x+y)\rho_{2s}(x-y)$.*

Remark 2.24. *From these properties it follows that the the L_2-norm of $x \mapsto s^{m/2} \cdot \sqrt{\rho_{1/s}(x)}$ equals 1, i.e., $\|s^{m/2} \cdot \sqrt{\rho_{1/s}(x)}\|_{\mathbb{R}^m}^2 = 1$.*

The following two results (and the variations we discuss below) will play an important role and will be used several times in this paper: *Banaszczyk's*

bound, originating from [Ban93], and the *smoothing parameter*, as introduced by Micciancio and Regev [MR07]. They allow us to control

$$\rho_s(X) := \sum_{x \in X} \rho_s(x)\,,$$

for certain discrete subsets $X \subseteq \mathbb{R}^m$. For ease of notation, we let

$$\beta_z^{(n)} := \left(\frac{2\pi e z^2}{n}\right)^{n/2} e^{-\pi z^2}\,,$$

which decays super-exponentially in z (for fixed n). In particular, we have $\beta_t^{(n)} \leq e^{-t^2}$ for all $t \geq \sqrt{n}$. The following formulation of Banaszczyk's lemma is obtained from [MS18, Eq. (1.1)].

Lemma 2.25 (Banaszczyk's Bound)**.** *Whenever* $r/s \geq \sqrt{\frac{n}{2\pi}}$,

$$\rho_s((\Lambda + t) \setminus \mathcal{B}_r) \leq \beta_{r/s}^{(n)} \cdot \rho_s(\Lambda)\,,$$

where $\mathcal{B}_r = \mathcal{B}_r(0) = \{x \in \mathbb{R}^n \mid \|x\|_2 < r\}$.

Definition 2.26 (Smoothing parameter)**.** *Given an* $\varepsilon > 0$ *and a lattice* Λ*, the* smoothing parameter $\eta_\varepsilon(\Lambda)$ *is the smallest real number* $s > 0$ *such that* $\rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \varepsilon$*. Here,* Λ^* *is the dual lattice of* Λ*.*

Lemma 2.27 (Smoothing Error)**.** *Let* $\Lambda \in \mathbb{R}^n$ *be a full rank lattice, and let* $s \geq \eta_\varepsilon(\Lambda)$*. Then, for any* $t \in \mathbb{R}^n$*,*

$$(1-\varepsilon)\frac{s^n}{\det \Lambda} \leq \rho_s(\Lambda + t) \leq (1+\varepsilon)\frac{s^n}{\det \Lambda}\,. \tag{2.21}$$

We have the following two useful upper bounds for full-rank n-dimensional lattices Λ [MR07, Lm. 3.2 and 3.3]: $\eta_\varepsilon(\Lambda) \leq \sqrt{\log(2n(1+1/\varepsilon))} \cdot \lambda_n(\Lambda)$ for all $\varepsilon > 0$ and $\eta_1(\Lambda) \leq \eta_{2^{-n}}(\Lambda) \leq \sqrt{n}/\lambda_1(\Lambda^*) \leq \sqrt{n} \cdot \lambda_n(\Lambda)$. The latter leads to the following corollary.

Corollary 2.28. *Let L be an ideal lattice in* IdLat_K*. Let $t \in \mathbb{R}^n$ be arbitrary and $s \geq n \cdot \lambda_n(\mathcal{O}_K) \cdot \mathrm{Vol}(L)^{1/n}$. Then it holds that*

$$\left| \frac{\rho_s(L-t) \cdot \mathrm{Vol}(L)}{s^n} - 1 \right| \leq 2^{-n}, \tag{2.22}$$

Proof. By the assumption on s and by Lemma 2.22, we have $s \geq n \cdot \lambda_n(\mathcal{O}_K) \cdot \mathrm{Vol}(L)^{1/n} \geq \sqrt{n} \cdot \lambda_n(L) \geq \eta_{2^{-n}}(\Lambda)$. The result follows then from Lemma 2.31. □

Alternative descriptions of the smoothing bound

Imitating techniques from Micciancio and Regev [MR07, Lm. 3.2], we have:

Lemma 2.29. *Let $s \geq \frac{\sqrt{m}}{\lambda_1(\Lambda^*)}$. Then $\rho_{1/s}(\Lambda^* \backslash 0) \leq 2 \cdot \beta_{s\lambda_1(\Lambda^*)}$.*

As a direct corollary, we have the following result.

Corollary 2.30. *Let $s \geq 2\sqrt{m}$, and let $x \in \mathbb{R}^m$ with $\|x\|_\infty \leq 1/2$. Then*

$$\rho_{1/s}(\mathbb{Z}^m \backslash \{0\} + x) \leq 2 \cdot \beta_{s/2}.$$

Proof. We have $\rho_{1/s}(\mathbb{Z}^m \backslash \{0\} + x) \leq \rho_{1/s}((\mathbb{Z}^m + x) \backslash \mathcal{B}_{\frac{1}{2}}) \leq \beta_{s/2} \cdot \rho_{1/s}(\mathbb{Z}^m)$, where the second inequality follows from Lemma 2.25. Using Lemma 2.29 to argue that $\rho_{1/s}(\mathbb{Z}^m) = 1 + \rho_{1/s}(\mathbb{Z}^m \backslash 0) \leq 1 + 2 \cdot \beta_s \leq 2$ then proves the claim. □

The following lemma, which combines [MR07, Lm. 4.1] and [MR07, Lm. 3.2], controls the fluctuation of the sum $\rho_s(\Lambda + t)$ for varying $t \in \mathbb{R}^m$.

Lemma 2.31 (Smoothing Error)**.** *Let $\Lambda \in \mathbb{R}^m$ be a full rank lattice, and let $s \geq \sqrt{m}/\lambda_1(\Lambda^*)$. Then, for any $t \in \mathbb{R}^m$,*

$$(1 - 2 \cdot \beta_{s\lambda_1(\Lambda^*)}) \frac{s^m}{\det \Lambda} \leq \rho_s(\Lambda + t) \leq (1 + 2 \cdot \beta_{s\lambda_1(\Lambda^*)}) \frac{s^m}{\det \Lambda}. \tag{2.23}$$

Corollary 2.32. *For $s \geq \frac{\sqrt{m}}{\lambda_1(\Lambda^*)}$ and for any $t \in \mathbb{R}^m$, we have $\rho_s(\Lambda + t) \leq 2\frac{s^m}{\det \Lambda}$.*

Proof. Using Lemma 2.31 and noticing $2 \cdot \beta_{s\lambda_1(\Lambda^*)} \leq 2 \cdot \beta_{\sqrt{m}} \leq 1$ yields the result. □

2.5.4. Gaussian Distributions

In this work, both discrete and continuous Gaussian distributions play a major role. We denote both of these distributions with $\mathcal{G}_{X,s,c}$, where the subscript X is a metric space which supports the distribution and thus indicates whether the Gaussian is discrete or continuous. More concretely, for discrete spaces X like lattices, $\mathcal{G}_{X,s}$ a discrete Gaussian, whereas for continuous spaces it is a continuous Gaussian. For the cases of a vector space and a lattice, the definition is spelled out below.

Continuous Gaussian distribution. For a real vector space H of dimension n, a parameter $s > 0$ and a center $c \in H$, we write $\mathcal{G}_{H,s,c}$ the continuous Gaussian distribution over H with density function $\rho_s(x - c)/s^n$ for all $x \in H$. When the center c is 0, we simplify the notation as $\mathcal{G}_{H,s}$.

Discrete Gaussian distributions. For any lattice $L \subset \mathbb{R}^n$, we define the discrete Gaussian distribution over L of standard deviation $s > 0$ and center $c \in \mathbb{R}^n$ by

$$\forall x \in L\,,\ \mathcal{G}_{L,s,c} = \frac{\rho_s(x - c)}{\rho_s(L - c)}.$$

When the center c is 0, we simplify the notation as $\mathcal{G}_{L,s}$.

2.6. The Lipschitz Condition

Theorem 2.33 (Rademacher's theorem)**.** *A Lipschitz function $\mathbf{f} : \mathbb{R}^m/\Lambda \to \mathcal{H}$ has weak partial derivatives $\partial_{x_j}\mathbf{f} : \mathbb{R}^m/\Lambda \to \mathcal{H}$ lying in $L_2(\mathbb{R}^m/\Lambda)$. In*

particular,

$$\sum_{j=1}^{m} \|\partial_{x_j} \mathbf{f}\|^2_{\mathbb{R}^m/\Lambda} \leq \mathrm{Lip}(\mathbf{f})^2.$$

Proof. Combining the proof of [Hei04, Thm. 4.1 and 4.9] and [Vil85, Thm. 2] on measures of compact sets, we obtain this result. □

Corollary 2.34. *Let $\mathbf{f} : \mathbb{R}^m/\Lambda \to \mathcal{H}$ be a Lipschitz-continuous function, and denote by $|c_{\ell^*}\rangle$ the vectorial Fourier coefficients of $\mathbf{f}$. Then,*

$$\sum_{\substack{\ell^* \in \Lambda^* \\ \|\ell^*\| \geq B}} \langle c_{\ell^*} | c_{\ell^*} \rangle \leq \frac{\mathrm{Lip}(\mathbf{f})^2}{4\pi^2 B^2}\,.$$

Proof. Since $\mathbf{f}$ is Lipschitz, we can apply Theorem 2.33. Furthermore, the identity $|\mathbf{f}(x)\rangle = \sum_{\ell^* \in \Lambda^*} |c_{\ell^*}\rangle e^{2\pi i \langle x, \ell^* \rangle}$ implies that

$$|\partial_{x_j} \mathbf{f}(x)\rangle = 2\pi i \sum_{\ell^* \in \Lambda^*} \ell^*_j |c_{\ell^*}\rangle e^{2\pi i \langle x, \ell^* \rangle}$$

almost everywhere ([Wer07, Lm. V.2.11] or [RA08, Lm. 2.16]). Finally, given that $\sum_{j=1}^m \|\partial_{x_j} \mathbf{f}\|^2_{\mathbb{R}^m/\Lambda} \leq \mathrm{Lip}(\mathbf{f})^2$, Plancherel's identity implies that

$$\begin{aligned}
\mathrm{Lip}(\mathbf{f})^2 &\geq \sum_{j=1}^{m} \|\partial_{x_j} \mathbf{f}\|^2_{\mathbb{R}^m/\Lambda} = 4\pi^2 \sum_{\ell^* \in \Lambda^*} \|\ell^*\|_2^2 \cdot \langle c_{\ell^*} | c_{\ell^*} \rangle \\
&\geq 4\pi^2 \sum_{\substack{\ell^* \in \Lambda^* \\ \|\ell^*\|_2 \geq B}} \|\ell^*\|_2^2 \cdot \langle c_{\ell^*} | c_{\ell^*} \rangle \geq 4B^2\pi^2 \sum_{\substack{\ell^* \in \Lambda^* \\ \|\ell^*\|_2 \geq B}} \langle c_{\ell^*} | c_{\ell^*} \rangle\,,
\end{aligned}$$

from which the claim follows. □