Random walks on Arakelov class groups

Boer, K. de

4. Random Walks on Arakelov Ray Class Groups

4.1. Summary

The Arakelov class group.

The Arakelov class group (denoted Pic^0_K) is a combination of the unit torus $T = \mathrm{Log}\, K^0_{\mathbb{R}}/\,\mathrm{Log}(\mathcal{O}_K^\times)$ and the class group Cl_K. The exponent 0 in $K^0_{\mathbb{R}}$ refers to elements of algebraic norm 1 (i.e., modulo renormalization), while the subscript $\mathbb{R}$ indicates that we are working in the tensor product of K with $\mathbb{R}$ over $\mathbb{Q}$. By 'a combination' we mean that there is a short exact sequence

$$0 \longrightarrow T \longrightarrow \mathrm{Pic}^0_K \longrightarrow \mathrm{Cl}_K \longrightarrow 0.$$

That is, T is (isomorphic to) a subgroup of Pic^0_K, and Cl_K is isomorphic to the quotient $\mathrm{Pic}^0_K\,/T$. Summarizing, the Arakelov class group is an abelian group which combines an uncountable but compact part T and a finite part Cl_K; topologically, it should be thought of as $|\mathrm{Cl}_K|$ many disconnected copies of the torus T.

The Arakelov ray class group.

In this chapter we actually consider a more general group, an Arakelov analogue of the finite *ideal ray class group* $\mathrm{Cl}^{\mathfrak{m}}_K = \mathcal{I}^{\mathfrak{m}}_K/\mathrm{Princ}^{\mathfrak{m}}_K$; which is the

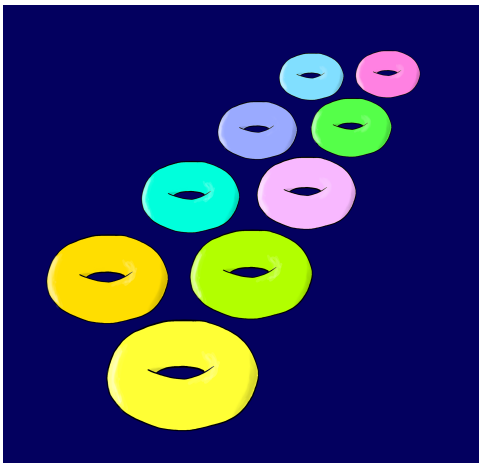

Figure 4.1.: The Arakelov class group can be thought of as $|\mathrm{Cl}_K|$ copies of the logarithmic unit torus.

reason why it is named the Arakelov *ray* class group. It is defined likewise via an exact sequence,

$$0 \longrightarrow T^{\mathfrak{m}} \longrightarrow \mathrm{Pic}^0_{K^{\mathfrak{m}}} \longrightarrow \mathrm{Cl}^{\mathfrak{m}}_K \longrightarrow 0,$$

where $T^{\mathfrak{m}} = \operatorname{Log} K^0_{\mathbb{R}} / \operatorname{Log}(\mathcal{O}_K^{\times} \cap K^{\mathfrak{m},1})$. Here, $K^{\mathfrak{m},1}$ is called the *ray* of $\mathfrak{m}$, the multiplicative subgroup of K^* generated by elements that are congruent to 1 modulo $\mathfrak{m}$. This Arakelov ray class group has essentially the same structure as the 'normal' Arakelov class group (which can be recovered by taking $\mathfrak{m} = \mathcal{O}_K$), in the sense that it can also be thought of as $|\mathrm{Cl}^{\mathfrak{m}}_K|$ many disconnected copies of the (larger) torus $T^{\mathfrak{m}}$.

Random walks on the Arakelov ray class group.

In this chapter we study the process of a random walk on this Arakelov ray class group, which can be described best by using the correspondence with Arakelov ray class group elements with *ideal lattices*. This random walk process consists of multiplying the input ideal lattice by a certain number of random prime ideals of bounded norm, followed by a slight disturbance of

the geometry of the ideal lattice. The end distribution over $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ is called the *random walk distribution*.

The main question to be solved is for which choice of parameters this random walk distribution is close to the uniform distribution. These parameters involve the maximum norm of the prime ideals, the number of prime ideals to multiply with and the magnitude of the geometrical disturbance.

Fourier analysis on the Arakelov ray class group.

Because the Arakelov ray class group is abelian and compact, this question is tackled by resorting to Fourier analysis: uniformity is demonstrated by showing that all the Fourier coefficients of the distribution resulting from the random walk tend to 0 except for the coefficient associated with the trivial character.

This argument can be roughly described as follows. The act of multiplying by random prime ideals can be described by a so-called Hecke operator, a linear Hermitian operator that has the characters of $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ as eigenfunctions. Assuming the Extended Riemann Hypothesis, one can show that all eigenvalues of the non-trivial eigenfunctions are bounded sufficiently below one, except for specific 'high-frequency eigenfunctions'. Choosing an initial distribution (the 'geometrical disturbance') that lacks those high-frequency eigenfunctions, e.g., a Gaussian, applying the Hecke operator sufficiently many times yields a near-uniform distribution (see Figure 4.7).

The preciseness of this argument allows us to very tightly estimate bounds for all parameters involved in order to achieve a nearly uniformly random final distribution.

4.2. Introduction

One of the more important concepts that occurs in complexity theory, number theory and modern cryptography is that of a *structured lattice*. The

most elementary examples of such structured lattices are *ideal lattices*, which are derived from ideals of a number field. It is a well-known fact among number theorists that the set of all ideal lattices up to K-linear isometry (or, equivalently, Hermitian line bundles) associated with a fixed number field K forms a compact abelian group, the *Arakelov class group* Pic_K^0 (e.g. [Sch08]). The motivation for studying this particular Arakelov class group in this thesis came from two directions.

The first direction relates to number theory and involves a computational problem related to the density of prime ideals. Namely: for a given ideal $\mathfrak{a}$ of $\mathcal{O}_K$, find an element $\alpha \in \mathfrak{a}$ with a predescribed bounded length such that $(\alpha)/\mathfrak{a}$ is a prime ideal. The most straightforward way to obtain such an element without class group computations is by *randomly* sampling an element α in the intersection of the ideal $\mathfrak{a}$ with a large box, and just simply *hope* that the ideal $(\alpha)/\mathfrak{a}$ is prime. For a fixed ideal $\mathfrak{a}$ we cannot prove that this approach is efficient, but for an ideal lattice $\mathfrak{a}$ that is *uniformly randomly distributed* in the Arakelov class group Pic_K^0 we can actually reasonably lower bound the success probability of this approach (see Chapter 6). The remaining question is: can we efficiently transform a fixed ideal $\mathfrak{a}$ into a random ideal in the Arakelov class group without changing too much of its properties?

The second direction relates more to complexity theory and cryptography, and involves the computational hardness of the *Hermite Shortest Vector Problem* on ideal lattices of a fixed number field. An interesting question here is, for a fixed number field K, whether there are ideal lattices that are significantly harder to solve Hermite-SVP in than for other ideal lattices. A natural way to approach this question is by comparing the hardness of Hermite-SVP on a fixed ideal lattice with the hardness of Hermite-SVP on an *average* ideal lattice, i.e., an ideal lattice uniformly distributed on the Arakelov class group. In Chapter 5 the random walk theorem of the current chapter will be applied in order to 'randomize' a fixed ideal lattice to a uniformly random ideal lattice *without disturbing its geometrical structure too much*.

These two research directions both have an underlying question that regards

randomization of ideal lattices in the Arakelov class group, but in such a way that it does not change the nature of these ideal lattices too much. In this chapter we propose an approach to do so by means of a *random walk*, a technique that has already been deployed in various areas of mathematics. In the field of algebraic geometry, for example, one can show by a random walk technique via isogenies on elliptic curves [JMV09] (and more general abelian varieties [JW15]) that the discrete logarithm problem in a randomly chosen elliptic curve is as hard as in any other in the same isogeny class. The random walk approach on the Arakelov class group, as treated in this chapter, is heavily inspired by these results.

Related work

We note that recent works [PHS19; Lee+19] were already implicitly relying on Arakelov theory. More specifically, the lattice given in Section 3.1 of [PHS19] is precisely the lattice of slightly more general Arakelov class relations between the appropriate set of degree-zero Arakelov divisors. In fact, by extending our theorem to Arakelov divisors that include (complex) phases in the infinite places, one can obtain upper bounds for the covering radius of the relation lattices, at least for sufficiently large factor bases. With more effort one may be able to eliminate Heuristic 4 from [PHS19] or Heuristic 1 of [Lee+19].

Applications

One application of the random walk theorem concerns a worst-case to average-case reduction, as treated in Chapter 5. By uniformizing over the Arakelov class group, one can 'randomize' an input lattice to a uniformly random lattice, without changing the geometry of the initial lattice too much. By using the efficient machinery of random walks, one can then obtain a worst-case to average-case reduction for Hermite-SVP with only a small loss in the quality of the output.

Another direct application of the random walk theorem concerns *ideal sampling* and is the the object of Chapter 6. Namely, we note that many algorithms [BF14; Bia+17; BP17] rely on finding elements α in an ideal $\mathfrak{a}$ such that $\alpha\mathfrak{a}^{-1}$ is easy to factor (e.g. prime, near-prime, or B-smooth). Such algorithms are analyzed only heuristically, by treating $\alpha\mathfrak{a}^{-1}$ as a uniformly sampled ideal, and applying know results on the density of prime or smooth ideals. The random walk theorem of this chapter allows to adjust this strategy and make the reasoning rigorous, see Chapter 6. This particular application allows to develop an efficient algorithm that computes the power residue symbol, which is the object of Chapter 7.

The result

In this chapter we show a new versatile tool: we prove that, subject to the Riemann Hypothesis for Hecke L-functions, certain random walks on the Arakelov class group have a rapid mixing property.

The random walk used in the result of this chapter can be seen as a combination of two different random walks, namely a discrete one and a continuous one. This is due to the fact that the Arakelov class group is topologically a disjoint union of (hyper)tori; the discrete walk 'jumps' from one torus to the other (see Figure 4.2), whereas the continuous walk crawls on the surface of one torus. These two different shapes of the random walk have an intuitive interpretation for ideal lattices associated with the Arakelov class group. Namely, the discrete walk corresponds to taking a random sub-ideal lattice of a given ideal lattice, also known as *sparsification*, whereas the continuous walk corresponds to *disturbing* the ideal lattice by multiplying each coordinate by a scalar.

Both the continuous and the discrete part of the random walk change the original nature of an input ideal lattice; the longer the random walk on an ideal lattice, the more disturbed this ideal lattice becomes. In the two research directions sketched earlier in this introduction, it was of fundamental importance that the final randomized ideal lattice does not *differ too much* from the input ideal lattice, but is nevertheless uniformly randomly

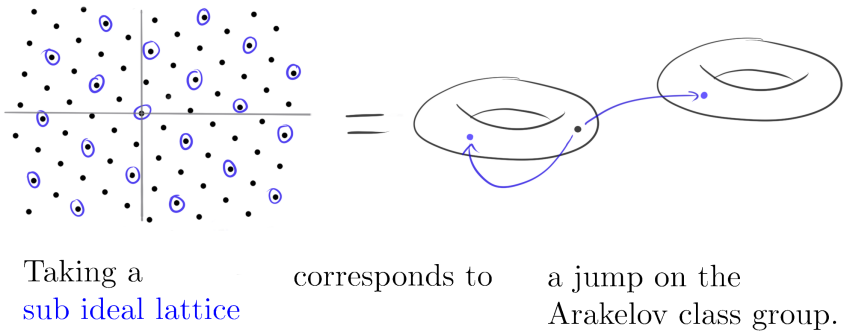

Figure 4.2.: The discrete walk on the Arakelov class group mostly jumps from one torus to another – but it is also possible that it jumps to another distant place on the same torus.

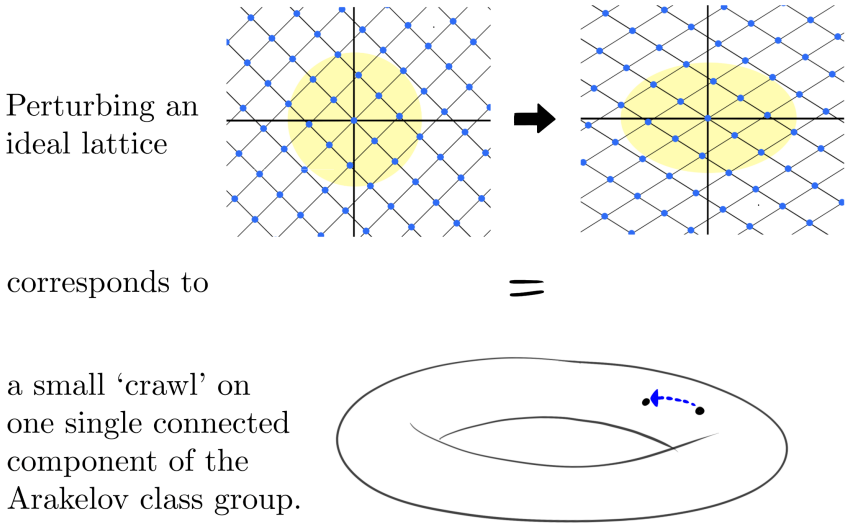

Figure 4.3.: The continuous walk on the Arakelov class group stays within the same torus and within a short distance of the initial point

distributed in the Arakelov class group. In other words, one would like to have an *as short as possible* random walk that still achieves uniformity in the Arakelov class group. Therefore, the study in this chapter boils down to the following succinct question.

How fast does a random walk in the Arakelov class group converge to the uniform distribution?

Concretely, the discrete walk involves so-called *finite places* and happens by multiplying the input Arakelov class by N random prime ideals the set $\mathcal{P}$ of all prime ideals with norm bounded by B. Contrarily, the continuous walk involves the *infinite places* and happens by applying a Gaussian noise of deviation s to the input Arakelov class. Noting that the Gaussian noise of deviation s roughly covers a surface of $s^{\mathfrak{r}}$ (where $\mathfrak{r}$ is the rank of the unit group of K) and assuming that the $|\mathcal{P}|^N$ discrete jumps are sufficiently equidistributed, we can heuristically expect the random walk to yield a uniform distribution whenever $s^{\mathfrak{r}} \cdot |\mathcal{P}|^N \approx |\mathrm{Pic}^0_K|$, where $|\mathrm{Pic}^0_K|$ is the total surface of the Arakelov class group Pic^0_K (see Figure 4.4). In fact, one can argue that this is the best situation that one can expect, due to the absence of overlapping Gaussians. This intuitive reasoning therefore can be considered as a *combined lower bound* on the parameters s, N and $|\mathcal{P}|$.

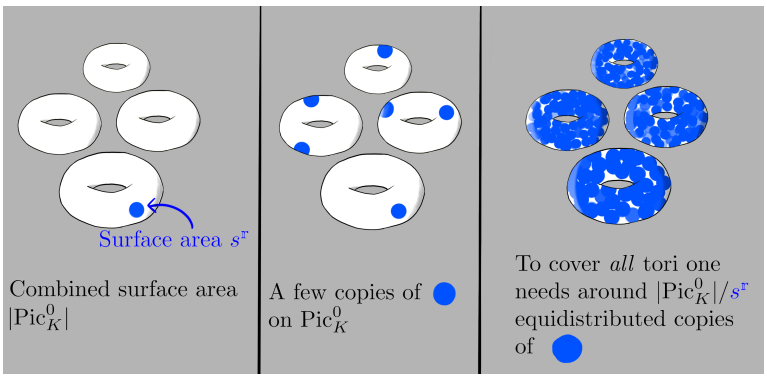

Figure 4.4.: To cover the entire Arakelov class group Pic^0_K with Gaussians of surface area roughly $s^{\mathfrak{r}}$, we need around $|\mathrm{Pic}^0_K|/s^{\mathfrak{r}}$ equidistributed copies of that Gaussian distribution.

In this work we show that the reality does not deviate much from this optimal intuitive combined lower bound on these parameters (see Theorem 4.3), assuming the Riemann Hypothesis for Hecke L-functions. The need for this specific hypothesis is not surprising: the heuristic argument assumes a reasonably controllable equidistribution of prime ideals in the Arakelov class group. For such an equidistribution of prime ideals to be within useful bounds, one often needs some form of the Riemann Hypothesis.

The actual proof that a random walk procedure yields a uniform distribution on the Arakelov class group happens by means of harmonic analysis; due to the fact that the Arakelov class group is compact and abelian, one can apply Fourier theory.

For an intuition for this proof it is convenient to consider the continuous walk before the discrete walk, i.e., we assume that we start with a reasonably narrow Gaussian distribution on one connected component of the Arakelov class group. The discrete walk, i.e., act of multiplying by a random bounded prime ideal, can be seen as a Hermitian operator on distributions on the Arakelov class group, called the *Hecke operator*. One can show that the eigenfunctions of this operator are precisely the *characters* on the Arakelov class group. Furthermore, all low-frequency characters have eigenvalues whose absolute value is sufficiently below one, except the unit character, which is kept intact under this Hecke operator. As Gaussian distributions only have a negligible contribution from high-frequency characters, applying the Hecke operator sufficiently often on this Gaussian suppresses all characters except the unit character, thus yielding an almost uniform distribution.

In this chapter we consider a slight generalization of the Arakelov class group, called the Arakelov *ray* class group with respect to a modulus ideal $\mathfrak{m} \subseteq \mathcal{O}_K$. This Arakelov ray class group is essentially an Arakelov class group where we 'leave out' the primes dividing the ideal $\mathfrak{m}$ and where the principal divisors must equal 1 modulo $\mathfrak{m}$. This generalization is needed in Chapter 7, in which we show that the power residue symbol can be computed within zero-error probabilistic polynomial time. To recover the ordinary Arakelov class group, one just puts $\mathfrak{m} = \mathcal{O}_K$.

4.3. Random Walk Theorem for the Arakelov Ray Class Group

In this section, we prove Theorem 4.3, on random walks on the Arakelov ray class group. Starting with a point in the hyperplane $H \subseteq \mathrm{Div}^0_{K^{\mathfrak{m}}}$, sampled according to a Gaussian distribution, we prove that multiplying this point sufficiently often by small random prime ideals yields a random ray divisor that is very close to uniformly distributed in the Arakelov ray class group (i.e., modulo principal ray divisors). The proof of Theorem 4.3 requires various techniques, extensively treated in Sections 4.3.2 to 4.3.7, and summarized in the following.

Hecke operators. The most important tool for proving Theorem 4.3 is that of a Hecke operator, whose definition and properties are covered in Section 4.3.2. This specific kind of operator acts on the space of probability distributions on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$, and has the virtue of having the characters of $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ as eigenfunctions.

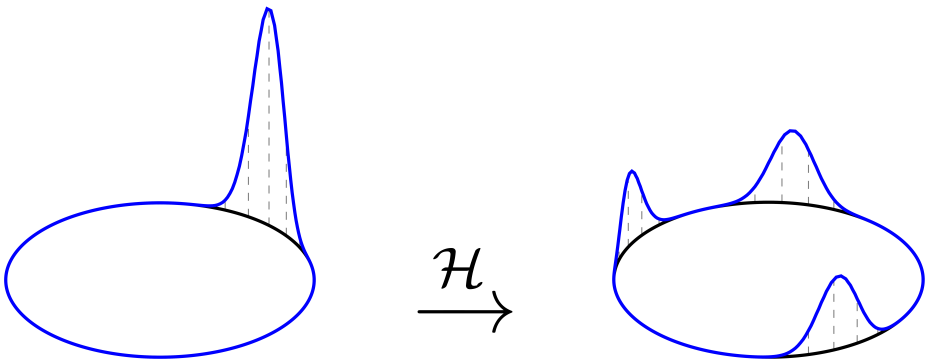

Figure 4.5.: On distributions on the Arakelov class group (here portrayed as a single circle) the Hecke operator has the effect of taking multiple shifts of the distribution and taking the average of those. In the pictured example, the Hecke operator maps the input Gaussian distribution on the circle to a distribution consisting of the average of three shifts of this Gaussian distribution.

Eigenvalues of Hecke operators. The aim of the proof is showing that applying this Hecke operator repeatedly on an appropriate initial distribution yields the uniform distribution on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$. The impact of consecutive applications of the Hecke operator can be studied by considering the eigenvalues of its eigenfunctions (which are the characters of $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$). Classical results from analytic number theory show that the eigenvalues of these characters are (in absolute value) sufficiently smaller than 1, whenever the so-called analytic conductor of the corresponding character is not too large. An exception is the unit character, which is fixed under each Hecke operation. This classical result and how to apply it in our specific setting is covered in Section 4.3.3.

The analytic conductor. The Hecke operator thus quickly 'damps out' all characters with small analytic conductor (except the unit character). In Section 4.3.4, we examine which quantities of a character of $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ define the analytic conductor. It turns out that this analytic conductor is closely related to how the character acts on the hypertorus $T^{\mathfrak{m}}$ defined by the log ray unit lattice. The higher the frequency of this character on the hypertorus, the larger the analytic conductor. This frequency can be measured by the norm of the uniquely associated dual log ray unit lattice point of the character. In fact, we establish a bound on the analytic conductor of a character in terms of the norm of its associated dual lattice point.

Fourier analysis on the hypertorus $T^{\mathfrak{m}}$. To summarize, low-frequency (non-trivial) characters on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ (i.e., with small analytic conductor) are quickly damped out by the action of the Hecke character, whereas for high-frequency characters we do not have good guarantees on the speed at which they damp out. To resolve this issue, we choose an initial distribution whose character decomposition has only a negligible portion of high-frequency oscillatory characters. An initial distribution that nicely satisfies this condition is the Gaussian distribution (on the hypertorus). To examine the exact amplitudes of the occurring characters of this Gaussian distribution, we need Fourier analysis on this hypertorus, as covered in Section 4.3.5.

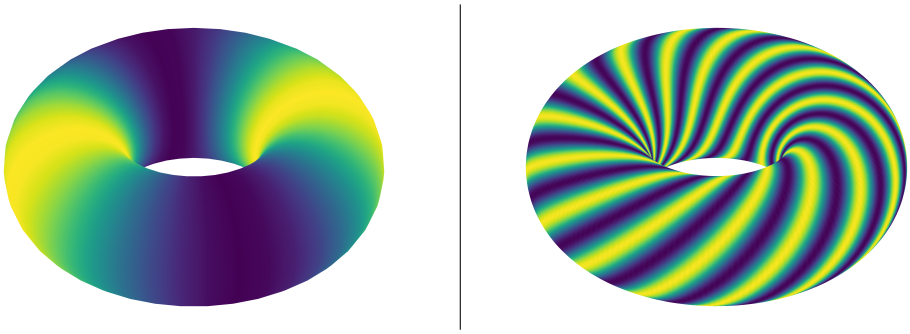

Figure 4.6.: On the left, a character with a low frequency on the hypertorus $T^{\mathfrak{m}}$ is pictured. Contrarily, on the right one can see a character that has a rather high frequency on the hypertorus. As a result, the character of the left image has a *lower analytic conductor* than the character on the right image.

Splitting up the character decomposition. In this part of the proof, which is covered in Section 4.3.6, we write the Gaussian distribution into its character decomposition, where we separate the high-frequency characters, the low-frequency character and the unit character. Applying the Hecke operator often enough, damps out the low-frequency ones, and as the high-frequency characters were only negligibly present anyway, one is left with (almost only) the unit character. This corresponds to a uniform distribution.

Conclusion. By assembling all technical results and choosing appropriate parameters, we arrive at the main theorem, which is stated and proved in Section 4.3.7.

4.3.1. Main result

Definition 4.1 (Random Walk Distribution in $\mathrm{Div}^0_{K^{\mathfrak{m}}}$)**.** *For a number field K, we denote by $\mathcal{W}_{\mathrm{Div}^0_{K^{\mathfrak{m}}}}(B, N, s)$ the distribution on $\mathrm{Div}^0_{K^{\mathfrak{m}}}$ that is obtained by the following random walk procedure.*

Sample $x \in H \subseteq \log K_{\mathbb{R}}$ according to a centered Gaussian distribution with standard deviation s. Subsequently, sample N ideals $\mathfrak{p}_j$ uniformly from the

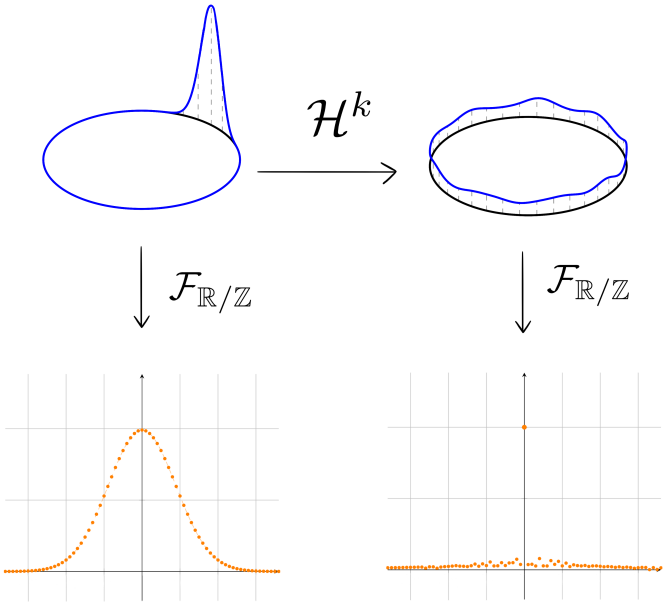

Figure 4.7.: The main theorem of this chapter is proven by resorting to Fourier analysis. The initial distribution (a Gaussian distribution in this example) on the Arakelov ray class group can be decomposed into a sum of characters. The Hecke operator $\mathcal{H}$ has a diminishing effect on non-unit characters. Therefore, applying it sufficiently many times results in a distribution that is almost uniform.

set of all prime ideals coprime with $\mathfrak{m}$ *with norm bounded by* B*. Finally, output* $x + \sum_{j=1}^{N} d^0(\mathfrak{p}_j)$*, where* $x \in \mathrm{Div}^0_{K^\mathfrak{m}}$ *is understood via the injection* $H \hookrightarrow \mathrm{Div}^0_{K^\mathfrak{m}}$*.*

Definition 4.2 (Random Walk Distribution in $\mathrm{Pic}^0_{K^\mathfrak{m}}$)**.** *By* $\mathcal{W}_{\mathrm{Pic}^0_{K^\mathfrak{m}}}(B, N, s)$*, we denote the distribution on the Arakelov class group obtained by sampling* $\mathbf{a}$ *from* $\mathcal{W}_{\mathrm{Div}^0_{K^\mathfrak{m}}}(B, N, s)$ *and taking the Arakelov ray class* $[\mathbf{a}] \in \mathrm{Pic}^0_{K^\mathfrak{m}}$*.*

Theorem 4.3 (Random Walks on the Arakelov Ray Class Group, ERH)**.** *Let* $\varepsilon > 0$ *and* $s > 0$ *be any positive real numbers and let* $k \in \mathbb{R}_{>0}$ *be a positive real number as well. Putting* $\tilde{s} = \min(\sqrt{2} \cdot s, 1/\eta_1(\Lambda^*_{K^\mathfrak{m},1}))$*, there exists a*

bound $B = \widetilde{O}(n^{2k}[n^2(\log\log(1/\varepsilon))^2 + n^2(\log(1/\tilde{s}))^2 + (\log(|\Delta_K|\mathcal{N}(\mathfrak{m})))^2])$ *such that for any integer*

$$N \geq \left\lceil \frac{1}{2k\log n} \cdot (\mathfrak{r} \cdot \log(1/\tilde{s}) + \log|\mathrm{Pic}^0_{K^\mathfrak{m}}| + 2\log(1/\varepsilon) + 2) \right\rceil, \tag{4.46}$$

the random walk distribution $\mathcal{W}_{\mathrm{Pic}^0_{K^\mathfrak{m}}}(B, N, s)$ *is* ε*-close to uniform in* $L_1(\mathrm{Pic}^0_{K^\mathfrak{m}})$*, i.e.,*

$$\left\| \mathcal{W}_{\mathrm{Pic}^0_{K^\mathfrak{m}}}(B, N, s) - \mathcal{U}(\mathrm{Pic}^0_{K^\mathfrak{m}}) \right\|_1 \leq \varepsilon.$$

4.3.2. Hecke Operators

A key tool to analyze random walks on $\mathrm{Pic}^0_{K^\mathfrak{m}}$ are Hecke operators, which allow to transform a given distribution into a new distribution obtained by adding one random step. This particular Hecke operator, though mainly interpreted as an operator on distributions, can in fact be applied on any function on $\mathrm{Pic}^0_{K^\mathfrak{m}}$.

Definition 4.4 (The Hecke operator)**.** *Let* $\mathcal{P}$ *be a finite subset of prime ideals of the number field* K *not dividing the modulus* $\mathfrak{m}$*, and let* $\mathrm{Pic}^0_{K^\mathfrak{m}}$ *be the Arakelov ray class group with respect to this modulus* $\mathfrak{m} \subseteq \mathcal{O}_K$*. Then we define the* Hecke operator $\mathcal{H}_\mathcal{P} : L^2(\mathrm{Pic}^0_{K^\mathfrak{m}}) \to L^2(\mathrm{Pic}^0_{K^\mathfrak{m}})$ *by the following rule:*

$$H_\mathcal{P}(f)(x) := \frac{1}{|\mathcal{P}|} \sum_{\mathfrak{p}\in\mathcal{P}} f(x - [d^0(\mathfrak{p})])$$

Concretely, the Hecke operator on the Arakelov ray class group $\mathrm{Pic}^0_{K^\mathfrak{m}}$ sends a distribution over $\mathrm{Pic}^0_{K^\mathfrak{m}}$ to an *average of shifts* of this distribution, see Figure 4.5.

Lemma 4.5 (Eigenfunctions of the Hecke operator)**.** *The Hecke operator* $\mathcal{H}_\mathcal{P} : L^2(\mathrm{Pic}^0_{K^\mathfrak{m}}) \to L^2(\mathrm{Pic}^0_{K^\mathfrak{m}})$ *has the characters* $\chi \in \widehat{\mathrm{Pic}^0_{K^\mathfrak{m}}}$ *as eigenfunctions, with eigenvalues* $\lambda_\chi = \frac{1}{|\mathcal{P}|}\sum_{\mathfrak{p}\in\mathcal{P}} \overline{\chi}([d^0(\mathfrak{p})])$*, i.e.,*

$$\mathcal{H}_\mathcal{P}(\chi) = \lambda_\chi \chi.$$

Proof. Let $\chi \in \widehat{\mathrm{Pic}^0_{K\mathfrak{m}}}$ be a character on $\mathrm{Pic}^0_{K\mathfrak{m}}$. We have

$$\begin{aligned}\mathcal{H}_{\mathcal{P}}(\chi)(x) &= \frac{1}{|\mathcal{P}|}\sum_{\mathfrak{p}\in\mathcal{P}} \chi(x - [d^0(\mathfrak{p})]) \\ &= \frac{1}{|\mathcal{P}|}\sum_{\mathfrak{p}\in\mathcal{P}} \chi(x)\overline{\chi}([d^0(\mathfrak{p})]) = \left(\frac{1}{|\mathcal{P}|}\sum_{\mathfrak{p}\in\mathcal{P}} \overline{\chi}([d^0(\mathfrak{p})])\right)\cdot\chi(x).\end{aligned}$$

So $\mathcal{H}_{\mathcal{P}}(\chi) = \lambda_\chi \chi$ with $\lambda_\chi = \frac{1}{|\mathcal{P}|}\sum_{\mathfrak{p}\in\mathcal{P}} \overline{\chi}([d^0(\mathfrak{p})])$. □

Note that $H_{\mathcal{P}}(\mathbf{1}) = \mathbf{1}$, for the trivial character $\mathbf{1} \in \widehat{\mathrm{Pic}^0_{K\mathfrak{m}}}$, so $\lambda_{\mathbf{1}} = 1$. For any other character χ it is evident from the above that $|\lambda_\chi| \leq 1$.

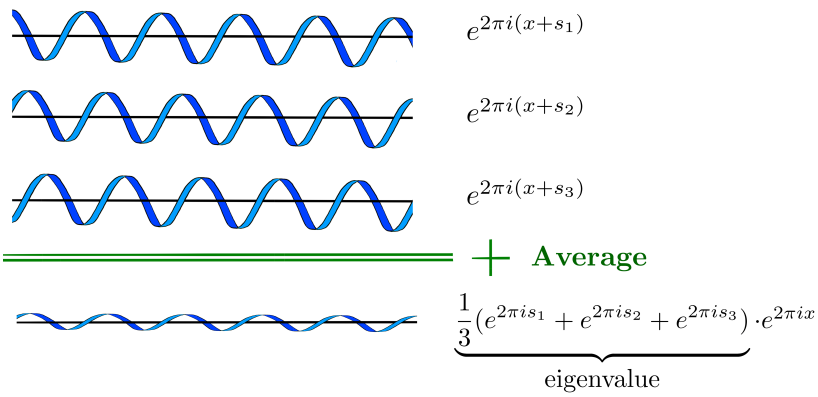

Figure 4.8.: Taking the average of shifted complex exponential functions yields a 'flattened' complex exponential function. Hence those complex exponentials (i.e., characters) are eigenfunctions of the Hecke operator, having eigen values in absolute value bounded by one.

4.3.3. Bounds on Eigenvalues of Hecke Operators

In the remaining part of this chapter we consider the Hecke operator whose prime set $\mathcal{P}$ consists of *all* primes with norm bounded by B that are not dividing the modulus $\mathfrak{m}$. Assuming the Extended Riemann Hypothesis for

Hecke L-functions (see Definition 2.10) and using classical results from analytic number theory, one can show that the eigenvalues of these specific Hecke operators tend to zero if B grows to infinity for non-trivial characters. More specifically, omitting quantities like the conductor and the discriminant for the moment, one can show that the eigenvalues of the non-trivial characters of these Hecke operators are essentially bounded by $O(B^{-1/2})$ in a non-uniform way.

Proposition 4.6 (Bound on the eigenvalues of the Hecke operator, ERH)**.** *Let $\mathcal{P}$ be the set of all primes of K not dividing $\mathfrak{m}$ and with norm bounded by $B \in \mathbb{N}$. Then, assuming the extended Riemann hypothesis (Definition 2.10), the eigenvalue λ_χ of any non-constant eigenfunction $\chi \in \widehat{\mathrm{Pic}^0_{K^{\mathfrak{m},1}}}$ of the Hecke operator satisfies*

$$\lambda_\chi = O\left(\frac{\log(B)\log(B^n \cdot |\Delta_K| \cdot \mathcal{N}(\mathfrak{m}) \cdot \mathfrak{q}_\infty(\chi))}{B^{1/2}}\right),$$

provided that $B \geq \max((12\log|\Delta_K| + 8n + 28)^4, 3 \cdot 10^{11}, 16 \cdot \omega(\mathfrak{m})^2)$, where $\mathfrak{q}_\infty(\chi)$ is the infinite part of the analytic conductor of the character χ, as in Definition 4.12 (cf. [IKS04, Eq. (5.6)]) and $\omega(\mathfrak{m})$ is the number of different prime ideal divisors of $\mathfrak{m}$.

Notation 4.7. *We denote by $\mathcal{M} : \mathcal{I}_K \to \mathbb{R}_{>0}$ the von Mangoldt function for number fields K. The value $\mathcal{M}(\mathfrak{a})$ equals $\log(\mathcal{N}(\mathfrak{p}))$ whenever $\mathfrak{a}$ is a power of a prime ideal $\mathfrak{p}$ and zero otherwise. We also define the function $\widetilde{\mathcal{M}} : \mathcal{I}_K \to \mathbb{R}_{>0}$, for which $\widetilde{\mathcal{M}}(\mathfrak{a}) = \log(\mathcal{N}(\mathfrak{a}))$ whenever $\mathcal{N}(\mathfrak{a})$ is prime and zero otherwise.*

In order to apply analytic number-theoretic results, we need to eliminate the non-split primes of the number field from the character sums arising in the eigenvalues of the Hecke operator. This happens in the following lemma, whose proof follows exactly the outline of [Wes18, Cor. 2.3.5].

Lemma 4.8. *For any character $\chi : \mathcal{I}_K^{\mathfrak{m}} \to \mathbb{C}$, we have*

$$\sum_{\substack{\mathcal{N}(\mathfrak{a}) \leq B \\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \chi(\mathfrak{a})\mathcal{M}(\mathfrak{a}) - \sum_{\substack{\mathcal{N}(\mathfrak{a}) \leq B \\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \chi(\mathfrak{a})\widetilde{\mathcal{M}}(\mathfrak{a}) = O(n\sqrt{B}) \tag{4.47}$$

where the sums are over all integral ideals coprime to the modulus $\mathfrak{m}$ *and with norm bounded by* B*.*

Proof. Any nonzero entry $\chi(\mathfrak{a})[\mathcal{M}(\mathfrak{a}) - \widetilde{\mathcal{M}}(\mathfrak{a})]$ arises from an ideal $\mathfrak{a}$ that is a power of a prime ideal and that does not have prime norm. As there are at most $n = [K : \mathbb{Q}]$ prime ideals above each prime number, we see that the left side of Equation (4.47) must be bounded by

$$\begin{aligned} n \sum_{\substack{p^\ell \leq B \\ \ell \geq 2}} \ln(p) &\leq n \sum_{\substack{p \leq \sqrt{B} \\ 2 \leq \ell \leq \frac{\ln B}{\ln p}}} \ln(p) \\ &\leq n \sum_{p \leq \sqrt{B}} \ln p \frac{\ln B}{\ln p} = n \cdot \pi(B^{1/2}) \cdot \ln B = O(n \cdot B^{1/2}), \end{aligned}$$

where π is the prime counting function over $\mathbb{Z}$ and where the last bound is obtained by the prime number theorem (see Theorem 2.12). □

Proof of Proposition 4.6. Assuming the Extended Riemann Hypothesis, we have the following classical analytic result[1] [IKS04, Thm. 5.15] for any non-trivial character $\chi \in \widehat{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}$.

[1] Any character on the Arakelov ray class group can be seen as a Hecke character, by projecting the idèle class group to the Arakelov ray class group. Since characters χ on the Arakelov ray class group are defined on $\mathcal{I}_K^{\mathfrak{m}}$, the conductor $\mathfrak{f}_\chi$ divides $\mathfrak{m}$. The analytic conductor $\mathfrak{q}(\chi)$ is then equal to $|\Delta_K| \cdot \mathcal{N}(\mathfrak{f}_\chi) \cdot \mathfrak{q}_\infty(\chi) \leq |\Delta_K| \cdot \mathcal{N}(\mathfrak{m}) \cdot \mathfrak{q}_\infty(\chi)$, where Δ_K is the discriminant of the number field K and $\mathfrak{q}_\infty(\chi)$ is the infinite part of the analytic conductor; see, for example, [IKS04, p. 129 & Eq. (5.7)].

The phrasing of the theorem in Iwaniec & Kowalski [IKS04, Thm. 5.15] involves the function $\psi(f, x) = \sum_{n \leq x} \Lambda_f(n)$, defined in [IKS04, Eq. (5.46), p. 110], where $\Lambda_f(n)$ is supported only on prime powers and arises from $-L'(f,s)/L(f,s) = \sum_{n \geq 1} \Lambda_f(n) n^{-s}$ [IKS04, Eq. (5.25), p. 102]. In our case, $f = \chi$ is a Hecke character with conductor $\mathfrak{m}$, which means that the associated L-function avoids $\mathfrak{m}$: $L(s, \chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} (1 - \chi(\mathfrak{p}) \mathcal{N}(\mathfrak{p})^{-s})^{-1}$ (see [Lan12, Ch. XIV, §8, p. 299]). By taking the logarithmic derivative of $L(\chi, s)$ one obtains that $\Lambda_\chi(n) = \sum_{\substack{\mathcal{N}(\mathfrak{a}) = n \\ \mathfrak{a} + \mathfrak{m} = \mathcal{O}_K}} \chi(\mathfrak{a}) \mathcal{M}(\mathfrak{a})$, where $\mathcal{M}$ is the van Mangoldt function as in Notation 4.7. The same theorem [IKS04, Thm. 5.15] involves a number r indicating the order of the pole of zero at $s = 1$ of the respective L-function. In the case of non-trivial Hecke characters χ this order r is zero, see [IKS04, Ch. 5, p. 94 and p. 129] or [Lan12, Ch. XV, §4, Thm. 2].

$$\sum_{\substack{\mathcal{N}(\mathfrak{a})\leq B\\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \mathcal{M}(\mathfrak{a})\chi(\mathfrak{a}) = O(B^{1/2}\log(B)\log(B^n\cdot|\Delta_K|\cdot\mathcal{N}(\mathfrak{m})\cdot\mathfrak{q}_\infty(\chi))),$$

where $\mathfrak{q}_\infty(\chi)$ is the infinite part of the analytic conductor of χ, and where $\mathcal{M}$ is the von Mangoldt function for the number field K (see Notation 4.7). In this expression, and in all subsequent expressions in this proof, the summation is over integral ideals $\mathfrak{a}$ *coprime* with the modulus $\mathfrak{m}$, as indicated by the phrase '$\mathfrak{a}+\mathfrak{m}=\mathcal{O}_K$'.

According to Lemma 4.8, the sums

$$\sum_{\substack{\mathcal{N}(\mathfrak{a})\leq B\\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \chi(\mathfrak{a})\widetilde{\mathcal{M}}(\mathfrak{a}) \quad\text{and}\quad \sum_{\substack{\mathcal{N}(\mathfrak{a})\leq B\\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \chi(\mathfrak{a})\mathcal{M}(\mathfrak{a})$$

(over integral ideals coprime with $\mathfrak{m}$) differ by at most $O(nB^{1/2})$, and therefore

$$\begin{aligned} A(B) := \sum_{2\leq j\leq B} a_j &= \sum_{\substack{\mathcal{N}(\mathfrak{a})\leq B\\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \chi(\mathfrak{a})\widetilde{\mathcal{M}}(\mathfrak{a}) \\ &= O(B^{1/2}\log(B)\log(B^n\cdot|\Delta_K|\cdot\mathcal{N}(\mathfrak{m})\cdot\mathfrak{q}_\infty(\chi))), \end{aligned}$$

where $a_n = \sum_{\substack{\mathcal{N}(\mathfrak{a})=n\\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \chi(\mathfrak{a})\widetilde{\mathcal{M}}(n)$ and where $\widetilde{\mathcal{M}}(n) = \log n$ whenever n is prime and zero otherwise. Using the Abel partial summation formula, and temporarily denoting $C = |\Delta_K|\cdot\mathcal{N}(\mathfrak{m})\cdot\mathfrak{q}_\infty(\chi)$ for the sake of brevity, we deduce

$$\begin{aligned} \sum_{\substack{\mathcal{N}(\mathfrak{a})\leq B\\ \mathfrak{a}+\mathfrak{m}=\mathcal{O}_K}} \chi(\mathfrak{p}) = \sum_{n\leq B} a_n\frac{1}{\log n} &= \frac{A(B)}{\log B} + \int_2^B A(t)\frac{dt}{t\log^2(t)} \\ &= O(B^{1/2}\log(B^n\cdot C)) + O\left(\int_2^B \frac{\log(t^n\cdot C)}{\log(t)t^{1/2}}dt\right) \\ &= O(B^{1/2}\log(B^n\cdot \underbrace{|\Delta_K|\cdot\mathcal{N}(\mathfrak{m})\cdot\mathfrak{q}_\infty(\chi)}_{C})) \end{aligned} \tag{4.48}$$

where the last equality uses the fact that

$$\int_2^B \frac{\log(t^n \cdot C)}{\log(t) t^{1/2}} dt \leq \log(B^n \cdot C)/\log(2) \int_2^B t^{-1/2} dt = O(B^{1/2} \cdot \log(B^n \cdot C)).$$

As the composition $\chi \circ [d^0(\cdot)] : \mathcal{I}_K^{\mathfrak{m}} \to \mathbb{C}$ is a Hecke character on ideals coprime to $\mathfrak{m}$, and $|\mathcal{P}| = \Theta(B/\log(B))$ (see[2] Lemma 2.13), we apply Equation (4.48) to obtain

$$\begin{aligned}\lambda_\chi &= \frac{1}{|\mathcal{P}|} \sum_{\mathfrak{p} \in \mathcal{P}} \overline{\chi}(d^0(\mathfrak{p})) = \frac{1}{|\mathcal{P}|} O(B^{1/2} \log(B^n \cdot |\Delta_K| \cdot \mathcal{N}(\mathfrak{m}) \cdot \mathfrak{q}_\infty(\chi))) \\ &= O\Big(B^{-1/2} \log(B) \log(B^n \cdot |\Delta_K| \cdot \mathcal{N}(\mathfrak{m}) \cdot \mathfrak{q}_\infty(\chi))\Big)\end{aligned}$$

which finishes the proof. □

4.3.4. The Infinite Analytic Conductor

In the bounds of Section 4.3.3, the infinite analytic conductor $\mathfrak{q}_\infty(\chi)$ of a character $\chi : \mathrm{Pic}^0_{K^{\mathfrak{m}}} \to \mathbb{C}$ plays a large role. In this section, we show that this infinite analytic conductor $\mathfrak{q}_\infty(\chi)$ is closely related to the dual logarithmic ray unit lattice point $\ell^* \in \Lambda^*_{K^{\mathfrak{m},1}} = \mathrm{Log}(\mathcal{O}^\times_{K^{\mathfrak{m},1}})^*$ that is uniquely associated with the character $\chi|_{T^{\mathfrak{m}}} : T^{\mathfrak{m}} \to \mathbb{C}$. We analyze the infinite analytic conductor of a character $\chi : \mathrm{Pic}^0_{K^{\mathfrak{m}}} \to \mathbb{C}$ using the following facts:

- *Any Arakelov ray class group* $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ *is a quotient group of the degree-zero idèle class group* $\mathcal{C}^0_K$. We will prove that there is a canonical projection $\mathcal{C}^0_K \to \mathrm{Pic}^0_{K^{\mathfrak{m}}}$ for all integral moduli $\mathfrak{m} \in \mathcal{I}_K$. This immediately has as a consequence that any character $\mathrm{Pic}^0_{K^{\mathfrak{m}}} \to \mathbb{C}$ yields an induced character on the idèle class group $\mathcal{C}^0_K$ by precomposition with this projection. Summarizing: Any character on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ is a Hecke character.
- *There is a canonical map* $K^0_{\mathbb{R}} \to \mathcal{C}^0_K$*, so any Hecke character* $\chi : \mathcal{C}^0_K \to \mathbb{C}$ *induces a derived character* $K^0_{\mathbb{R}} \to \mathcal{C}^0_K \xrightarrow{\chi} \mathbb{C}$. Characters on the group $K^0_{\mathbb{R}}$ are known to have a very specific shape, which can be described

[2] For this to be true, the lower bound on $B \geq \max((12 \log|\Delta_K| + 8n + 28)^4, 3 \cdot 10^{11}, 16 \cdot \omega(\mathfrak{m})^2)$ is needed, see Lemma 2.13.

in terms of an $2(n_{\mathbb{C}} + n_{\mathbb{R}})$-dimensional real vector. The entries of this specific vector are called the *local parameters at infinity* of the Hecke character χ.

- *Hecke characters derived from a character on the Arakelov ray class group* $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ *have local parameters at infinity that are closely related to the dual lattice of the logarithmic ray unit lattice* $\Lambda_{K^{\mathfrak{m},1}} = \mathrm{Log}(\mathcal{O}^{\times}_{K^{\mathfrak{m},1}}) = \mathrm{Log}(\mathcal{O}^{\times}_K \cap K^{\mathfrak{m},1})$. It turns out that a character on the Arakelov ray class group $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ induces a character on $K^0_{\mathbb{R}}$ that does not depend on the *phases* of the complex numbers involved, i.e., it solely depends on the absolute values of the entries in $K^0_{\mathbb{R}}$. This means that the induced character on $K^0_{\mathbb{R}}$ factors through the logarithmic image of the absolute values of $K^0_{\mathbb{R}}/\mathcal{O}^{\times}_K$, which equals $H/\Lambda_{K^{\mathfrak{m},1}} = T^{\mathfrak{m}}$. Characters on this *ray unit torus* $T^{\mathfrak{m}}$ are uniquely described by a dual logarithmic unit lattice point $\ell^* \in \Lambda^*_{K^{\mathfrak{m},1}}$.
- *The infinite analytic conductor* $\mathfrak{q}_\infty$ *is just a specific product of the local parameters of* χ *over all infinite places* ν. More specifically, we have

$$\mathfrak{q}_\infty(\chi) = \prod_{\nu \text{ real}} (3 + ||n_\nu| + i\phi_\nu|) \cdot \prod_{\nu \text{ complex}} (3 + |n_\nu + i\phi_\nu|)(3 + ||n_\nu| + i\phi_\nu + 1|).$$

  Via this formula, one can relate the size of the infinite analytic conductor $\mathfrak{q}_\infty(\chi)$ with the length of the dual logarithmic ray unit lattice.

In the following text we will elaborate on these four facts, for each fact a paragraph.

The Arakelov ray class group $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ is a quotient group of $\mathcal{C}^0_K$

Let $\mathcal{J}_{K^{\mathfrak{m}}} \subseteq \mathcal{J}_K$ be the subgroup of idèles that satisfy $a_\nu \equiv 1$ modulo $\mathfrak{p}_\nu^{\mathrm{ord}_\nu(\mathfrak{m})}$ for any place ν with $\mathfrak{p}_\nu \mid \mathfrak{m}$. More precisely,

$$\mathcal{J}_{K^{\mathfrak{m}}} = \{(a_\nu)_\nu \in \mathcal{J}_K \mid a_\nu \in 1 + \mathfrak{p}_\nu^{\mathrm{ord}_{\mathfrak{p}_\nu}(\mathfrak{m})} \text{ for all places } \nu \text{ with } \mathfrak{p}_\nu \mid \mathfrak{m}\}$$

Via the inclusion $\mathcal{J}_{K^{\mathfrak{m}}} \subseteq \mathcal{J}_K$, we have the isomorphism $\mathcal{J}_{K^{\mathfrak{m}}}/K^{\mathfrak{m},1} \xrightarrow{\sim} \mathcal{J}_K/K^*$ [Lan12, Ch. VII, §3]. The following map is surjective and has $K^{\mathfrak{m},1}$

in its kernel, which proves that the group $\mathrm{Pic}_{K^{\mathfrak{m}}}$ is a quotient group of $\mathcal{J}_{K^{\mathfrak{m}}}/K^{\mathfrak{m},1}$ and therefore of $\mathcal{J}_K/K^*$ as well.

$$\mathcal{J}_{K^{\mathfrak{m}}} \to \mathrm{Pic}_{K^{\mathfrak{m}}}, (a_\nu)_\nu \longmapsto \sum_{\nu \nmid \infty} \mathrm{ord}_{\mathfrak{p}_\nu}(a_\nu) \cdot (\!|\mathfrak{p}_\nu|\!) + \sum_{\nu|\infty} [K_\nu : \mathbb{R}] \cdot \log|a_\nu| \cdot (\!|\nu|\!).$$

Here, we mean by $\nu|\infty$ that ν is a infinite place (i.e., associated with an embedding $K \hookrightarrow \mathbb{C}$) and by $\nu \nmid \infty$ that ν is a finite place (i.e., associated with a prime ideal $\mathfrak{p}$). The degree maps $\deg : \mathcal{J}_K \to \mathbb{R}_{>0}, (a_\nu)_\nu \mapsto \prod_\nu |a_\nu|_\nu$ and $\deg : \mathrm{Pic}_{K^{\mathfrak{m}}} \to \mathbb{R}_{>0}, \sum_{\mathfrak{p}\nmid\mathfrak{m}} n_{\mathfrak{p}}(\!|\mathfrak{p}|\!) + \sum_{\nu|\infty} x_\nu (\!|\nu|\!) \longmapsto \prod_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{N}(\mathfrak{p})^{n_{\mathfrak{p}}} \prod_\nu e^{-x_\nu}$ are compatible with each other, which implies an induced surjective map $\mathcal{C}_K^0 \to \mathrm{Pic}_{K^{\mathfrak{m}}}^0$, proving that the Arakelov class group is a quotient of the degree zero idèle class group.

Any Hecke character $\chi : \mathcal{C}_K^0 \to \mathbb{C}$ induces a derived character on $K_{\mathbb{R}}^0$.

Let $\chi : \mathcal{C}_K^0 \to \mathbb{C}$ be a Hecke character. Recall that $K_{\mathbb{R}}^0 \simeq \{(x_\nu)_\nu \in K_{\mathbb{R}} \mid \prod_\nu |x_\nu|_\nu = 1\}$ (see Equation (2.10)), which embeds canonically into $\mathcal{J}_K^0$; we have the injection

$$K_{\mathbb{R}}^0 \hookrightarrow \mathcal{J}_K^0, \quad (x_\sigma)_\sigma \longmapsto (a_\nu)_{\nu_\sigma} \quad \text{where} \quad a_\nu = \begin{cases} x_\nu & \text{for } \nu \mid \infty \\ 1 & \text{for } \nu \nmid \infty \end{cases}.$$

So any character $\chi : \mathcal{C}_K^0 \to \mathbb{C}$ induces a character on $K_{\mathbb{R}}^0$ by precomposition with $K_{\mathbb{R}}^0 \to \mathcal{J}_K^0 \to \mathcal{C}_K^0 = \mathcal{J}_K^0/K^*$, which will be denoted by $\chi|_{K_{\mathbb{R}}^0}$. It is a well-known fact that any character on $K_{\mathbb{R}}^0$ is of the following shape, and is uniquely determined in that way (see [NS13, Ch. XII, Prop. 6.7]):

$$\chi : K_{\mathbb{R}}^0 \to S^1, (x_\nu)_\nu \longmapsto \prod_{\nu|\infty} \left(\frac{x_\nu}{|x_\nu|}\right)^{n_\nu} e^{i\cdot[K_\nu:\mathbb{R}]\cdot\phi_\nu\cdot\log|x_\nu|}, \tag{4.49}$$

with $n_\nu \in \mathbb{Z}$ if ν is complex, and $n_\nu \in \{0,1\}$ if ν is real and $\phi_\nu \in \mathbb{R}$. Note that $[K_\nu : \mathbb{R}] = 1$ if ν is real and $[K_\nu : \mathbb{R}] = 2$ if ν is a complex embedding.

Definition 4.9. *Let $\chi : \mathcal{C}_K^0 \to \mathbb{C}$ be a Hecke character and let $\chi|_{K_{\mathbb{R}}^0} : K_{\mathbb{R}}^0 \to \mathbb{C}$ be the induced character by precomposing with the map $K_{\mathbb{R}}^0 \to \mathcal{C}_K^0$. Then*

$(n_\nu)_\nu \in \mathbb{Z}^{n_\mathbb{C}} \times \{0,1\}^{n_\mathbb{R}}$ *and* $(\phi_\nu)_\nu \in \mathbb{R}^{n_\mathbb{C}+n_\mathbb{R}}$ *for* $\nu \mid \infty$ *that occur when writing* $\chi|_{K^0_\mathbb{R}}$ *in the shape of Equation* (4.49)*, are called the* local parameters at infinity of χ.

The local parameters at infinity of a Hecke character on the Arakelov ray class group $\mathrm{Pic}^0_{K^\mathfrak{m}}$ can be seen as a scaled point on the dual logarithmic ray unit lattice $\Lambda^*_{K^{\mathfrak{m},1}}$

For any character $\chi : \mathrm{Pic}^0_{K^\mathfrak{m}} \to \mathbb{C}$, we thus have an derived character $\chi|_{K^0_\mathbb{R}}$ on $K^0_\mathbb{R}$ as follows.

$$K^0_\mathbb{R} \to \mathcal{C}^0_K \to \mathrm{Pic}^0_{K^\mathfrak{m}} \xrightarrow{\chi} \mathbb{C}.$$

Of this derived character $\chi|_{K^0_\mathbb{R}}$ we would like to study the local parameters as in Equation (4.49). The combined map $K^0_\mathbb{R} \to \mathcal{C}^0_K \to \mathrm{Pic}^0_{K^\mathfrak{m}}$ can be described by the following rule:

$$K^0_\mathbb{R} \to \mathrm{Pic}^0_{K^\mathfrak{m}},\ (x_\nu)_\nu \longmapsto \sum_{\nu|\infty} [K_\nu : \mathbb{R}] \cdot \log|x_\nu| \cdot (\!|\nu|\!) \mod K^{\mathfrak{m},1}$$

So the derived character $\chi|_{K^0_\mathbb{R}} : K^0_\mathbb{R} \to \mathrm{Pic}^0_{K^\mathfrak{m}} \to \mathbb{C}$ cannot depend on the phases of $(x_\nu)_\nu \in K^0_\mathbb{R}$, which means that $n_\nu = 0$ in Equation (4.49) for all $\nu \mid \infty$ for such $\chi \in \mathrm{Pic}^0_{K^\mathfrak{m}}$. Also, by the fact that $\mathrm{Pic}^0_{K^\mathfrak{m}} = \mathrm{Div}^0_{K^\mathfrak{m}} / K^{\mathfrak{m},1}$, we have that $\mathcal{O}^\times_K \cap K^{\mathfrak{m},1} = \mathcal{O}^\times_{K^{\mathfrak{m},1}} \subseteq K^0_\mathbb{R}$ must lie in the kernel of $\chi|_{K^0_\mathbb{R}}$.

Summarizing, for characters $\chi : \mathrm{Pic}^0_{K^\mathfrak{m}} \to \mathbb{C}$, we have

$$\chi|_{K^0_\mathbb{R}}((x_\nu)_\nu) = \prod_{\nu|\infty} e^{i\cdot[K_\nu:\mathbb{R}]\cdot\phi_\nu\cdot\log|x_\nu|} = \exp\left(i \sum_{\sigma:K\to\mathbb{C}} \phi_{\nu_\sigma} \cdot \log|\sigma(x)|\right)$$

and $\chi|_{K^0_\mathbb{R}}(\mathcal{O}^\times_{K^{\mathfrak{m},1}}) = 1$. In above expression, the sum is over all embeddings $\sigma : K \to \mathbb{C}$, and ν_σ is the place ν uniquely associated with the embedding σ. This means that the following inner product satisfies

$$\left\langle \frac{1}{2\pi}(\phi_{\nu_\sigma})_\sigma, (\log|\sigma(\eta)|)_\sigma \right\rangle = \frac{1}{2\pi} \sum_{\sigma:K\to\mathbb{C}} \phi_{\nu_\sigma} \cdot \log|\sigma(\eta)| \in \mathbb{Z} \text{ for all } \eta \in \mathcal{O}^\times_{K^{\mathfrak{m},1}}.$$

Recalling that $\Lambda_{K^{\mathfrak{m},1}} = \mathrm{Log}(\mathcal{O}^\times_{K^{\mathfrak{m},1}}) = \mathrm{Log}(\mathcal{O}^\times_K \cap K^{\mathfrak{m},1})$, this is equivalent to $(\phi_{\nu_\sigma})_\sigma \in 2\pi\Lambda^*_{K^{\mathfrak{m},1}}$; i.e., the local parameters $(\phi_{\nu_\sigma})_\sigma$ are equal to 2π times

a dual logarithmic ray unit lattice point in $\Lambda^*_{K^{\mathfrak{m}},1}$. Thus we proved the following lemma.

Lemma 4.10 (Local parameters of a Hecke character on the Arakelov ray class group $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$)**.** *Let $\chi : \mathrm{Pic}^0_{K^{\mathfrak{m}}} \to \mathbb{C}$ be a character on the Arakelov ray class group. Then the local parameters at infinity of χ as in Definition 4.9, satisfy*

- *$n_\nu = 0$ for all $\nu \mid \infty$.*
- *There exists a dual logarithmic ray unit lattice point $\ell^* \in \Lambda^*_{K^{\mathfrak{m}},1}$ such that $\phi_\nu = \ell^*_{\sigma_\nu}$.*

Corollary 4.11. *Let $\chi : \mathrm{Pic}^0_{K^{\mathfrak{m}}} \to \mathbb{C}$ be a character on the Arakelov ray class group. Then, there exists a $\ell^* \in \Lambda^*_{K^{\mathfrak{m}},1} \subseteq H$ such that*

$$\chi|_{K^0_{\mathbb{R}}}((x_\nu)_\nu) = \exp\left(2\pi i \cdot \langle \ell^*, (x_{\nu_\sigma})_\sigma \rangle\right).$$

The converse is also true. For every $\ell^* \in \Lambda^*_{K^{\mathfrak{m}},1}$ there exists a character $\chi : \mathrm{Pic}^0_{K^{\mathfrak{m}}} \to \mathbb{C}$ such that

$$\chi|_{K^0_{\mathbb{R}}}((x_\nu)_\nu) = \exp\left(2\pi i \cdot \langle \ell^*, (x_{\nu_\sigma})_\sigma \rangle\right). \tag{4.50}$$

Proof. The first claim directly follows from Lemma 4.10. The second claim can be verified by the fact that one can construct a character $\chi : \mathrm{Pic}^0_{K^{\mathfrak{m}}} \to T^{\mathfrak{m}} \to \mathbb{C}$ that factors through the ray unit torus by the canonical quotient map $\mathrm{Pic}^0_{K^{\mathfrak{m}}} \to T^{\mathfrak{m}}$ of Figure 2.8. On this ray unit torus $T^{\mathfrak{m}}$ it has the values induced by Equation (4.50). In fact, by multiplying this character by other characters $\chi' \in \mathrm{Pic}^0_{K^{\mathfrak{m}}}$ for which $\chi'|_{T^{\mathfrak{m}}}$ is trivial, one obtains *all* characters on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ satisfying Equation (4.50). □

The infinite analytic conductor is a product of local parameters

Definition 4.12 (Infinite analytic conductor of a Hecke character)**.** *Let $\chi \in \widehat{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}$ be a character with local parameters at infinity n_ν and ϕ_ν as in*

Definition 4.9, where ν ranges over the infinite places of K. Then, we define the infinite part of the analytic conductor to be

$$\mathfrak{q}_\infty(\chi) = \prod_{\nu \text{ real}} (3+||n_\nu|+i\phi_\nu|) \prod_{\nu \text{ complex}} (3+|n_\nu+i\phi_\nu|)(3+||n_\nu|+i\phi_\nu+1|) \tag{4.51}$$

Remark 4.13. *The above definition of the infinite analytic conductor is obtained from [IKS04, p. 95, Eq. (5.6) with $s = 0$], where it is described in a slightly different form. In [IKS04], the functional equation lacks the complex L-functions $L_\mathbb{C}$. Instead, those are replaced by $L_\mathbb{R}(s)L_\mathbb{R}(s+1) = L_\mathbb{C}(s)$ (see [NS13, Ch. 7, Prop. 4.3(iv)]. This means that the local parameters $\kappa_\sigma, \kappa_{\bar\sigma}$ as in [IKS04, p. 93, Eq. (5.3)] must equal $k_\nu, k_\nu + 1$ for the embeddings $\{\sigma, \bar\sigma\}$ associated with the complex place ν (cf. [IKS04, p. 125]).*

Lemma 4.14. *Let $\mathfrak{q}_\infty(\chi)$ be the infinite part of the analytic conductor of the character $\chi \in \widehat{\mathrm{Pic}^0_{K^\mathfrak{m}}}$, and let $\ell^* \in \Lambda^*_{K^\mathfrak{m},1}$ be such that $\chi|_{T^\mathfrak{m}} = \chi_{\ell^*}$, where $\Lambda^*_{K^\mathfrak{m},1}$ is the dual lattice of the logarithmic ray unit lattice. Then we have*

$$\mathfrak{q}_\infty(\chi) \leq \left(4 + 2\pi \left\|\ell^*\right\| / \sqrt{n}\right)^n$$

Proof. Let $|\ell^*|$ denote the vector ℓ^* where all entries are replaced by their absolute value. Then, by applying subsequently the triangle inequality, the norm inequality between $\|\cdot\|_1$ and $\|\cdot\|_2$ and the arithmetic-geometric mean inequality, one obtains

$$\begin{aligned} 4\sqrt{n} + 2\pi \left\|\ell^*\right\|_2 &\geq \left\|\mathbf{4} + 2\pi|\ell^*|\right\|_2 \geq \frac{1}{\sqrt{n}}\left\|\mathbf{4} + 2\pi|\ell^*|\right\|_1 \\ &\geq \sqrt{n}\left(\prod_\sigma (4 + 2\pi|\ell^*_\sigma|)\right)^{1/n} \geq \sqrt{n}\cdot \mathfrak{q}_\infty(\chi)^{1/n}. \end{aligned}$$

Dividing by $\sqrt{n}$ and raising to the power n yields the claim. The last inequality follows just from Equation (4.51), in which $n_\nu = 0$ for all infinite ν. □

4.3.5. Fourier Analysis on the Ray Unit Torus

Definition 4.15. *Let $H \subseteq \operatorname{Log} K_{\mathbb{R}}$ be the ambient vector space of the log ray unit lattice $\Lambda_{K^{\mathfrak{m},1}} = \operatorname{Log}(\mathcal{O}^{\times}_{K^{\mathfrak{m},1}})$, where $\mathcal{O}^{\times}_{K^{\mathfrak{m},1}} = \mathcal{O}^{\times}_K \cap K^{\mathfrak{m},1}$. Recall the Gaussian function $\rho_s : H \to \mathbb{R}, x \mapsto e^{-\pi \|x\|^2/s^2}$. Denoting $T^{\mathfrak{m}} = H/\Lambda_{K^{\mathfrak{m},1}}$, we put $\rho_s|^{T^{\mathfrak{m}}} : T^{\mathfrak{m}} \to \mathbb{R}, x \mapsto \sum_{\ell \in \Lambda_{K^{\mathfrak{m},1}}} \rho_s(x+\ell)$.*

As we have (see Lemma A.3) $\|s^{-\mathfrak{r}}\rho_s\|_{H,1} = \int_H s^{-\mathfrak{r}}\rho_s(x)dx = 1$, and

$$\left\| s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}} \right\|_{T^{\mathfrak{m}},1} = \int_{T^{\mathfrak{m}}} s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}}(x)dx = 1,$$

both functions $s^{-\mathfrak{r}}\rho_s$ and $s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}}$ can be seen as probability distributions on their respective domains $\mathbb{R}^m$ and $T^{\mathfrak{m}}$.

Lemma 4.16 (Fourier coefficients of the periodized Gaussian)**.** *The periodized Gaussian function $s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}} \in L^2(T^{\mathfrak{m}})$ satisfies*

$$s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}} = \sum_{\ell^* \in \Lambda^*_{K^{\mathfrak{m},1}}} a_{\ell^*}\chi_{\ell^*} \tag{4.52}$$

where $a_{\ell^*} = \frac{1}{\operatorname{Vol}(T^{\mathfrak{m}})}\rho_{1/s}(\ell^*)$, where $\Lambda^*_{K^{\mathfrak{m},1}}$ is the dual lattice of the log unit lattice $\Lambda_{K^{\mathfrak{m},1}}$, and where $\chi_{\ell^*}(x) = e^{-2\pi i\langle x,\ell^*\rangle}$.

Proof. We have $\left\langle \chi_{\ell_1^*}, \chi_{\ell_2^*} \right\rangle = \operatorname{Vol}(T^{\mathfrak{m}}) \cdot \delta_{\ell_1^*,\ell_2^*}$, where δ is the Kronecker delta function, i.e., $\delta_{\ell_1^*,\ell_2^*}$ equals one if $\ell_1^* = \ell_2^*$ and zero otherwise. Identifying $\widehat{T^{\mathfrak{m}}}$ and $\Lambda^*_{K^{\mathfrak{m},1}}$ via the map $\chi_{\ell^*} \mapsto \ell^*$, taking a fundamental domain F of $\Lambda_{K^{\mathfrak{m},1}}$ and spelling out the definition of $\rho_s|^{T^{\mathfrak{m}}}$, we obtain, for all $\ell^* \in \Lambda^*_{K^{\mathfrak{m},1}}$,

$$\begin{aligned}
a_{\ell^*} &= \frac{1}{\operatorname{Vol}(T^{\mathfrak{m}})}\left\langle s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}}, \chi_{\ell^*} \right\rangle \\
&= \frac{1}{\operatorname{Vol}(T^{\mathfrak{m}})}\int_{x\in F}\sum_{\ell\in\Lambda_{K^{\mathfrak{m},1}}} s^{-\mathfrak{r}}\rho_s(x+\ell)\overline{\chi_{\ell^*}(x)}dx \\
&= \frac{1}{\operatorname{Vol}(T^{\mathfrak{m}})}\int_{x\in H} s^{-\mathfrak{r}}\rho_s(x)\overline{\chi_{\ell^*}(x)}dx = \frac{1}{\operatorname{Vol}(T^{\mathfrak{m}})}\mathcal{F}_H\{s^{-\mathfrak{r}}\rho_s\}(\ell^*) \\
&= \frac{1}{\operatorname{Vol}(T^{\mathfrak{m}})}\rho_{1/s}(\ell^*).
\end{aligned}$$

The last equality can be derived from the properties of the Gaussian function in Lemma 2.23. □

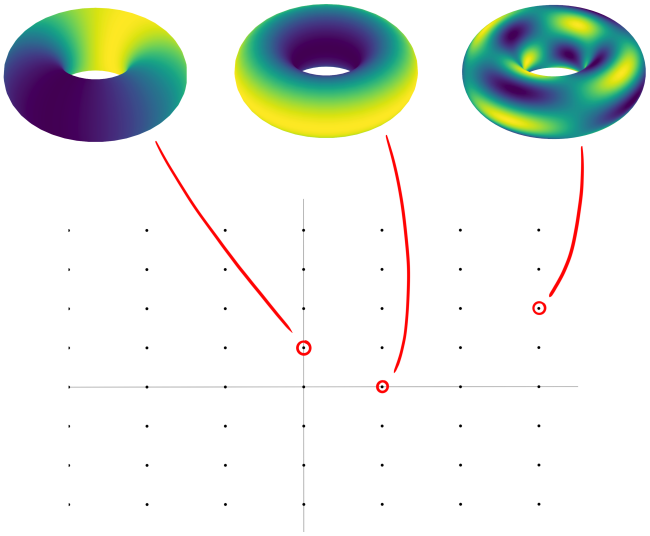

Figure 4.9.: In this picture three examples of characters ('eigenfunctions') on the ray unit torus are portrayed, together with their associated lattice points in the dual ray unit lattice at the bottom. In this particular example, one can see that characters that only depend on one rotational axis (the left two examples) have an associated dual lattice point on the x-axis or the y-axis. The 'mixed' character is associated with a dual lattice point that has both a non-zero x and y component.

4.3.6. Splitting up the Character Decomposition

Decomposing into characters on $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$

In Equation (4.52), the distribution $s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}}$ is decomposed into characters on the unit torus $T^{\mathfrak{m}}$. In order to apply the analytic bound on the eigenvalues of the Hecke operator as in Proposition 4.6, we need to decompose this distribution into characters on the *Arakelov ray class group* $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ instead.

To do so, we use the identity

$$\chi_{\ell^*} = \frac{1}{|\mathrm{Cl}_K^{\mathfrak{m}}|} \sum_{\substack{\chi' \in \widehat{\mathrm{Pic}^0_{K^{\mathfrak{m}}}} \\ \chi'|_{T^{\mathfrak{m}}} = \chi_{\ell^*}}} \chi', \tag{4.53}$$

which holds for any $\ell^* \in \Lambda^*_{K^{\mathfrak{m}},1}$, where $|\,\mathrm{Cl}_K^{\mathfrak{m}}\,|$ is the cardinality of the ray class group. Equation (4.53) is an identity of functions on the Arakelov ray class group $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$, where χ_{ℓ^*} is defined to be zero everywhere, except on the torus $T^{\mathfrak{m}} \subseteq \mathrm{Pic}^0_{K^{\mathfrak{m}}}$, the original domain of the function χ_{ℓ^*}. In this identity, χ' ranges over all characters $\chi' \in \widehat{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}$ which are identical to χ_{ℓ^*} when restricted to the unit group torus $T^{\mathfrak{m}}$. These characters χ' are called the *extensions* of the character χ_{ℓ^*} with respect to $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$, and it can be shown that for each $\ell^* \in \Lambda^*_{K^{\mathfrak{m}},1}$ there are exactly $|\,\mathrm{Cl}_K^{\mathfrak{m}}\,|$ such extensions (see [DE16, Cor. 3.6.2]).

The identity in Equation (4.53) follows essentially from the same argument that is used to prove general character orthogonality properties (see [Ser77, §2.3]).

Splitting up the character decomposition in a low-frequency and a high-frequency part

By above reasoning, we can rewrite Equation (4.52) in Lemma 4.16 into

$$s^{-\mathrm{r}} \rho_s|^{T^{\mathfrak{m}}} = \frac{1}{|\mathrm{Pic}^0_{K^{\mathfrak{m}}}|} \sum_{\chi_{\ell^*} \in \widehat{T^{\mathfrak{m}}}} \rho_{1/s}(\ell^*) \sum_{\chi'|_{T^{\mathfrak{m}}} = \chi_{\ell^*}} \chi', \tag{4.54}$$

where we used the identity $|\mathrm{Cl}_K^{\mathfrak{m}}|\,\mathrm{Vol}(T^{\mathfrak{m}}) = |\mathrm{Pic}^0_{K^{\mathfrak{m}}}|$. We will now split up this character decomposition into three parts: the 'trivial part', a 'low-frequency part' and a 'high-frequency part'.

The trivial part consists just of the unit character $\mathbf{1} = \mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}$. The low-frequency part consists of those (non-unit) characters $\chi' \in \widehat{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}$ that are extensions of a character $\chi_{\ell^*} \in \widehat{T^{\mathfrak{m}}}$ where $\ell^* \in \Lambda_{K^{\mathfrak{m}},1}$ has a small norm, say, $\|\ell^*\| < r$. Oppositely, the high-frequency part consists of those characters

that are extensions of some $\chi_{\ell^*} \in \hat{T}$ for which $\|\ell^*\| \geq r$. Here, $r \in \mathbb{R}_{>0}$ can in principle be chosen arbitrarily.

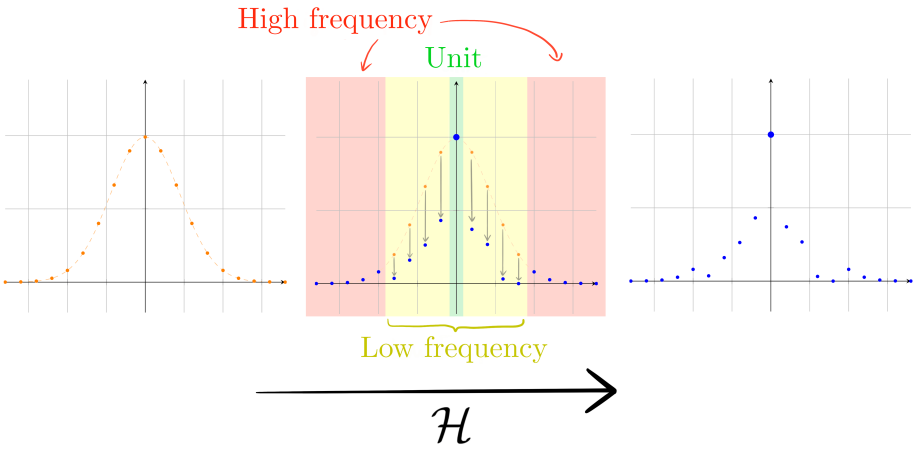

Figure 4.10.: Under assumption of the Extended Riemann Hypothesis, **low-frequency characters** diminish under the Hecke operator, whereas for high-frequency characters no such guarantee exists. By taking an initial distribution that has already almost no high-frequency content, like the Gaussian distribution, one can show that applying repeatedly the Hecke operator to such distribution yields an almost-uniform distribution.

$$|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| \cdot s^{-\mathbb{r}} \cdot \rho_s|^{T^{\mathfrak{m}}} = \underbrace{\mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}}_{\text{Unit character}} + \underbrace{\sum_{\substack{\chi_{\ell^*} \in \widehat{T^{\mathfrak{m}}} \\ \|\ell^*\| < r}} \rho_{1/s}(\ell^*) \sum_{\substack{\chi' |_{T^{\mathfrak{m}}} = \chi_{\ell^*} \\ \chi' \neq \mathbf{1}}} \chi'}_{\text{Low frequency characters}} + \underbrace{\sum_{\substack{\chi_{\ell^*} \in \widehat{T^{\mathfrak{m}}} \\ \|\ell^*\| \geq r}} \rho_{1/s}(\ell^*) \sum_{\chi' |_{T^{\mathfrak{m}}} = \chi_{\ell^*}} \chi'}_{\text{High frequency characters}}, \quad (4.55)$$

Bounding the parts of the character decomposition

Theorem 4.17 (ERH)**.** *Let $\mathcal{P}$ be the set of all prime ideals of a number field K coprime with $\mathfrak{m}$ and with norm at most B, and let $\mathcal{H} = \mathcal{H}_{\mathcal{P}}$ the Hecke operator (see Definition 4.4) for this set of primes. Then, assuming*

the Extended Riemann Hypothesis (see Definition 2.10), and for all $r, s > 0$ with $rs > \sqrt{\frac{\mathfrak{r}}{4\pi}}$, we have

$$\left\| \mathcal{H}^N(s^{-n}\rho_s|^{T^{\mathfrak{m}}}) - \frac{1}{|\mathrm{Pic}^0_{K^{\mathfrak{m}}}|}\mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}} \right\|^2 \leq \frac{\rho_{\frac{1}{\sqrt{2}s}}(\Lambda^*_{K^{\mathfrak{m}},1})}{\mathrm{Vol}(T^{\mathfrak{m}})}\left(c^{2N} + \beta^{(\mathfrak{r})}_{\sqrt{2}rs}\right) \quad (4.56)$$

with $c = O\left(\frac{\log(B)\log(B^n\cdot|\Delta_K|\cdot\mathcal{N}(\mathfrak{m})\cdot(4+2\pi r/\sqrt{n})^n)}{B^{1/2}}\right)$.

Proof. The Hecke operator $\mathcal{H} = \mathcal{H}_{\mathcal{P}}$ is a linear operator satisfying $\mathcal{H}(\mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}) = \mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}$ and $\mathcal{H}(\chi') = \lambda_{\chi'}\chi'$. Therefore, by applying the Hecke operator N times on Equation (4.55), we obtain

$$\begin{aligned} |\mathrm{Pic}^0_{K^{\mathfrak{m}}}| \cdot \mathcal{H}^N(s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}}) = \mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}} &+ \sum_{\substack{\chi_{\ell^*}\in\widehat{T^{\mathfrak{m}}} \\ \|\ell^*\|<r}} \rho_{1/s}(\ell^*) \sum_{\substack{\chi'|_{T^{\mathfrak{m}}}=\chi_{\ell^*} \\ \chi'\neq\mathbf{1}}} \lambda^N_{\chi'}\chi' \\ &+ \sum_{\substack{\chi_{\ell^*}\in\widehat{T^{\mathfrak{m}}} \\ \|\ell^*\|\geq r}} \rho_{1/s}(\ell^*) \sum_{\chi'|_{T^{\mathfrak{m}}}=\chi_{\ell^*}} \lambda^N_{\chi'}\chi', \quad (4.57) \end{aligned}$$

Therefore, by Parseval's theorem (see Equation (2.17)),

$$\left\| |\mathrm{Pic}^0_{K^{\mathfrak{m}}}| \cdot \mathcal{H}^N(s^{-\mathfrak{r}}\rho_s|^{T^{\mathfrak{m}}}) - \mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}} \right\|^2 = \underbrace{\sum_{\substack{\chi_{\ell^*}\in\widehat{T^{\mathfrak{m}}} \\ \|\ell^*\|<r}} \rho^2_{1/s}(\ell^*) \sum_{\substack{\chi'|_{T^{\mathfrak{m}}}=\chi_{\ell^*} \\ \chi'\neq\mathbf{1}}} |\lambda_{\chi'}|^{2N}}_{\text{Low frequency}} \quad (4.58)$$

$$+ \underbrace{\sum_{\substack{\chi_{\ell^*}\in\widehat{T^{\mathfrak{m}}} \\ \|\ell^*\|\geq r}} \rho^2_{1/s}(\ell^*) \sum_{\chi'|_{T^{\mathfrak{m}}}=\chi_{\ell^*}} |\lambda_{\chi'}|^{2N}}_{\text{High frequency}}. \quad (4.59)$$

We will bound the parts Equation (4.58) and Equation (4.59) separately, starting with the share of the latter, the high-frequency characters. By construction, $|\lambda_{\chi'}| \leq 1$ for all $\chi' \in \mathrm{Pic}^0_{K^{\mathfrak{m}}}$ (see Lemma 4.5). Combining this with the identity $\rho^2_{1/s} = \rho_{\frac{1}{\sqrt{2}s}}$ and the fact that there are exactly $|\mathrm{Cl}^{\mathfrak{m}}_K|$

character extensions to $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$ for each $\chi_{\ell^*} \in \widehat{T^{\mathfrak{m}}}$ (see [DE16, Cor. 3.6.2]), we have

$$\sum_{\substack{\chi_{\ell^*} \in \widehat{T^{\mathfrak{m}}} \\ \|\ell^*\| \geq r}} \rho^2_{1/s}(\ell^*) \sum_{\chi' | _{T^{\mathfrak{m}}} = \chi_{\ell^*}} |\lambda_{\chi'}|^{2N} \leq |\mathrm{Cl}^{\mathfrak{m}}_K| \sum_{\substack{\ell^* \in \Lambda^*_{K^{\mathfrak{m}},1} \\ \|\ell^*\| \geq r}} \rho_{\frac{1}{\sqrt{2}s}}(\ell^*)$$
$$\leq |\mathrm{Cl}^{\mathfrak{m}}_K| \cdot \beta^{(\mathbb{r})}_{\sqrt{2}rs} \cdot \rho_{\frac{1}{\sqrt{2}s}}(\Lambda^*_{K^{\mathfrak{m}},1}), \tag{4.60}$$

where the last inequality follows from Banaszczyk's tail bound (Lemma 2.25) and the assumption that $rs > \sqrt{\mathbb{r}/(4\pi)}$.

To bound the share of the low-frequency characters, we need to bound the absolute value of the eigenvalues $\lambda_{\chi'}$ of the low-frequency characters. Invoking the results from analytic number theory in Proposition 4.6 (thus assuming the Extended Riemann Hypothesis) we obtain $|\lambda_{\chi'}| \leq O\left(\frac{\log(B)\log(B^n \cdot |\Delta_K| \cdot \mathcal{N}(\mathfrak{m}) \cdot \mathfrak{q}_\infty(\chi'))}{B^{1/2}}\right)$. But since these characters have a 'low frequency', their analytic conductor $\mathfrak{q}_\infty(\chi')$ is bounded. More precisely, we have, by Lemma 4.14, that $\mathfrak{q}_\infty(\chi') \leq (4 + 2\pi r/\sqrt{n})^n$ for any $\chi' \in \mathrm{Pic}^0_{K^{\mathfrak{m}}}$ such that $\chi'|_{T^{\mathfrak{m}}} = \chi_{\ell^*}$ for some $\ell^* \in \Lambda^*_{K^{\mathfrak{m}},1}$ with $\|\ell^*\| < r$. Therefore, $|\lambda_{\chi'}| \leq c = O\left(\frac{\log(B)\log(B^n \cdot |\Delta_K| \cdot \mathcal{N}(\mathfrak{m}) \cdot (4+2\pi r/\sqrt{n})^n)}{B^{1/2}}\right)$. So, using again the identity $\rho^2_{1/s} = \rho_{\frac{1}{\sqrt{2}s}}$, and the fact that each χ_{ℓ^*} has $|\mathrm{Cl}^{\mathfrak{m}}_K|$ character extensions to $\mathrm{Pic}^0_{K^{\mathfrak{m}}}$, we have

$$\sum_{\|\ell^*\| \leq r} \rho^2_{1/s}(\ell^*) \underbrace{\sum_{\chi' | _{T^{\mathfrak{m}}} = \chi_{\ell^*}} |\lambda_{\chi'}|^{2N}}_{\leq |\mathrm{Cl}^{\mathfrak{m}}_K| \cdot c^{2N}} \leq |\mathrm{Cl}^{\mathfrak{m}}_K| \cdot c^{2N} \cdot \rho_{\frac{1}{\sqrt{2}s}}(\Lambda^*_{K^{\mathfrak{m}},1}) \tag{4.61}$$

We obtain the result by combining Equations (4.60) and (4.61), dividing by $|\mathrm{Pic}^0_{K^{\mathfrak{m}}}|$ and using the identity $|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| = |\mathrm{Cl}^{\mathfrak{m}}_K| \operatorname{Vol}(T^{\mathfrak{m}})$. □

4.3.7. Conclusion

Theorem 4.18. *Let $\varepsilon > 0$ and $s > 0$ be any positive real numbers and let $k \in \mathbb{R}_{>0}$ be a positive real number as well. Let $C \subseteq \Lambda_{K^{\mathfrak{m}},1}$ a sublattice of the logarithmic ray unit lattice of the number field K. Putting*

$\tilde{s} = \min(\sqrt{2}\cdot s, 1/\eta_1(C^*))$, *there exists a bound* $B = \widetilde{O}(n^{2k}[n^2(\log\log(1/\varepsilon))^2 + n^2(\log(1/\tilde{s}))^2 + n^2\log([\Lambda_{K^{\mathfrak{m},1}} : C])^2 + (\log(|\Delta_K|\mathcal{N}(\mathfrak{m})))^2])$ *such that for any integer*

$$N \geq \left\lceil \frac{1}{2k\log n} \cdot (\mathbb{r}\cdot\log(1/\tilde{s}) + \log|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| + 2\log(1/\varepsilon) + \log[\Lambda_{K^{\mathfrak{m},1}} : C] + 2)\right\rceil, \quad (4.62)$$

the random walk distribution $\mathcal{W}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}(B, N, s)$ *is* ε*-close to uniform in* $L_1(\mathrm{Pic}^0_{K^{\mathfrak{m}}})$*, i.e.,*

$$\left\|\mathcal{W}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}(B, N, s) - \mathcal{U}(\mathrm{Pic}^0_{K^{\mathfrak{m}}})\right\|_1 \leq \varepsilon.$$

Proof. Let $1 > \varepsilon > 0$, $s > 0$ and $k \in \mathbb{R}_{>0}$ be given. Let $C \subseteq \Lambda_{K^{\mathfrak{m},1}} = \mathrm{Log}(\mathcal{O}_K^\times \cap K^{\mathfrak{m},1})$ be a sublattice of the logarithmic ray unit lattice of index $[\Lambda_{K^{\mathfrak{m},1}} : C]$. Since, by construction, $1/\tilde{s} \geq \eta_1(C^*)$ and $1/\tilde{s} \geq 1/(\sqrt{2}s)$, and since $\Lambda^*_{K^{\mathfrak{m},1}} \subseteq C^*$, we have

$$\begin{aligned}\rho_{\frac{1}{\sqrt{2}s}}(\Lambda^*_{K^{\mathfrak{m},1}}) &\leq \rho_{\frac{1}{\sqrt{2}s}}(C^*) \leq \rho_{1/\tilde{s}}(C^*) \leq 2\cdot\det(C)/\tilde{s}^{\mathbb{r}} \\ &\leq 2\cdot[\Lambda_{K^{\mathfrak{m},1}} : C]\cdot\mathrm{Vol}(T^{\mathfrak{m}})/\tilde{s}^{\mathbb{r}} \end{aligned} \quad (4.63)$$

Using this inequality and Hölder's inequality (i.e., $\|f\cdot 1\|_1 \leq \|f\|_2\|1\|_2$), noting that $\|1_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}\|_2^2 = |\mathrm{Pic}^0_{K^{\mathfrak{m}}}|$ and applying Theorem 4.17 and Equation (4.63), we obtain, for each $r > \sqrt{\mathbb{r}}/(\sqrt{2}s)$,

$$\begin{aligned}&\left\|\mathcal{W}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}(B, N, s) - \mathcal{U}(\mathrm{Pic}^0_{K^{\mathfrak{m}}})\right\|_1^2 \\ &\leq |\mathrm{Pic}^0_{K^{\mathfrak{m}}}|\cdot\left\|\mathcal{H}^N(s^{-\mathbb{r}}\rho_s|^{T^{\mathfrak{m}}}) - \frac{1}{|\mathrm{Pic}^0_{K^{\mathfrak{m}}}|}\mathbf{1}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}\right\|_2^2 \\ &\leq |\mathrm{Cl}^{\mathfrak{m}}_K|\cdot\rho_{\frac{1}{\sqrt{2}s}}(\Lambda^*_{K^{\mathfrak{m},1}})\cdot(c^{2N} + \beta^{(\mathbb{r})}_{\sqrt{2}rs}) \\ &\leq |\mathrm{Cl}^{\mathfrak{m}}_K|\cdot 2\cdot\mathrm{Vol}(T^{\mathfrak{m}})\cdot[\Lambda_{K^{\mathfrak{m},1}} : C]\cdot\tilde{s}^{-\mathbb{r}}\cdot(c^{2N} + \beta^{(\mathbb{r})}_{\sqrt{2}rs}) \\ &\leq 2\cdot|\mathrm{Pic}^0_{K^{\mathfrak{m}}}|\cdot[\Lambda_{K^{\mathfrak{m},1}} : C]\cdot\tilde{s}^{-\mathbb{r}}\cdot(c^{2N} + \beta^{(\mathbb{r})}_{\sqrt{2}rs}). \end{aligned} \quad (4.64)$$

Here, $c = O\left(\frac{\log(B)\log(B^n\cdot|\Delta_K|\cdot\mathcal{N}(\mathfrak{m})\cdot(4+2\pi r/\sqrt{n})^n)}{B^{1/2}}\right)$, as in Theorem 4.17. We proceed by bounding the two summands in Equation (4.64) separately.

- By putting[3] r equal to the maximum of $\sqrt{\mathbb{r}}/(\sqrt{2}s)$ and
$$\frac{1}{\sqrt{2}s} \cdot \sqrt{2 + \mathbb{r}\log(1/\tilde{s}) + 2\log(1/\varepsilon) + \log|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| + \log[\Lambda_{K^{\mathfrak{m},1}} : C]}$$
we deduce that $2 \cdot |\mathrm{Pic}^0_{K^{\mathfrak{m}}}| \cdot [\Lambda_{K^{\mathfrak{m},1}} : C] \cdot \tilde{s}^{-\mathbb{r}} \cdot \beta^{(\mathbb{r})}_{\sqrt{2}rs} \leq \varepsilon^2/2$.
- Subsequently, choose[4] a $B = \tilde{O}(n^{2k}[\log(|\Delta_K|\mathcal{N}(\mathfrak{m}))^2 + n^2\log(r)^2])$, i.e.,
$$B = \tilde{O}\Big(n^{2k} \cdot \big[\log(|\Delta_K|\mathcal{N}(\mathfrak{m}))^2 + n^2\log(1/\tilde{s})^2 + n^2\log(\log(1/\varepsilon))^2 + n^2\log([\Lambda_{K^{\mathfrak{m},1}} : C])^2\big]\Big)$$
such that $c \leq 1/n^k$, where $c = O\left(\frac{\log(B)\log(B^n \cdot |\Delta_K| \cdot \mathcal{N}(\mathfrak{m}) \cdot (4+2\pi r/\sqrt{n})^n)}{B^{1/2}}\right)$ as in Theorem 4.17. Finally, taking any integer $N \geq \frac{1}{k\log n} \cdot (\frac{\mathbb{r}}{2} \cdot \log(1/\tilde{s}) + 2\log(1/\varepsilon) + \frac{1}{2}\log|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| + \log[\Lambda_{K^{\mathfrak{m},1}} : C] + 1)$ and noting that $c^{\frac{1}{k\log n}} \leq 1/e$, we deduce that $2 \cdot |\mathrm{Pic}^0_{K^{\mathfrak{m}}}| \cdot [\Lambda_{K^{\mathfrak{m},1}} : C] \cdot \tilde{s}^{-\mathbb{r}} \cdot c^{2N} \leq \varepsilon^2/2$.

Combining, we can bound the right-hand side of Equation (4.64) by ε^2. Taking square roots gives the final result. □

Remark 4.19. *Consider the base case $\mathfrak{m} = \mathcal{O}_K$. The occurrence of the sublattice $C \subseteq \Lambda_K$ of the log unit lattice in Theorem 4.18 might appear strange at first sight — indeed, just taking $C = \Lambda_K$ would make the result less complex and seemingly about equally powerful.*

We chose to phrase Theorem 4.18 in this way, because, in some number fields, certain subgroups of the unit group are better understood than the full unit group itself. For cyclotomic number fields, for example, the structure of the subgroup of the cyclotomic units *is simpler than that of the full unit group. Due to this simpler structure, we can achieve a tighter bound on $\eta_1(C^*)^{\mathbb{r}} \cdot [\Lambda_K : C]$ than we have on $\eta_1(\Lambda_K)$ (where C is here chosen to be the logarithmic image of the cyclotomic units).*

[3] We use the bound $\beta^{(\mathbb{r})}_{\alpha} \leq e^{-\alpha^2}$ for $\alpha \geq \sqrt{\mathbb{r}}$

[4] In this bound on B one would expect an additional $\log\log|\mathrm{Pic}^0_{K^{\mathfrak{m}}}|$. But as it is bounded by $\log(\log(|\Delta_K|\mathcal{N}(\mathfrak{m})))$ (see Lemma 2.17), it can be put in the hidden polylogarithmic factors.

Such a tight upper bound on the product $\eta_1(C^*)^{\mathbb{r}} \cdot [\Lambda_K : C]$ is important. This product does namely not only have a large influence on the complexity, but also has a significant leverage on $B^{N/n}$, the quality loss in the shortest-vector problem *of the reduction in Chapter 5.*

By taking $C = \Lambda_{K^{\mathfrak{m}}}$ in Theorem 4.18, we obtain the main theorem.

Theorem 4.3 (Random Walks on the Arakelov Ray Class Group, ERH)**.** *Let $\varepsilon > 0$ and $s > 0$ be any positive real numbers and let $k \in \mathbb{R}_{>0}$ be a positive real number as well. Putting $\tilde{s} = \min(\sqrt{2} \cdot s, 1/\eta_1(\Lambda^*_{K^{\mathfrak{m},1}}))$, there exists a bound $B = \widetilde{O}(n^{2k}[n^2(\log\log(1/\varepsilon))^2 + n^2(\log(1/\tilde{s}))^2 + (\log(|\Delta_K|\mathcal{N}(\mathfrak{m})))^2])$ such that for any integer*

$$N \geq \left\lceil \frac{1}{2k \log n} \cdot (\mathbb{r} \cdot \log(1/\tilde{s}) + \log|\mathrm{Pic}^0_{K^{\mathfrak{m}}}| + 2\log(1/\varepsilon) + 2) \right\rceil, \tag{4.46}$$

the random walk distribution $\mathcal{W}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}(B, N, s)$ is ε-close to uniform in $L_1(\mathrm{Pic}^0_{K^{\mathfrak{m}}})$, i.e.,

$$\left\| \mathcal{W}_{\mathrm{Pic}^0_{K^{\mathfrak{m}}}}(B, N, s) - \mathcal{U}(\mathrm{Pic}^0_{K^{\mathfrak{m}}}) \right\|_1 \leq \varepsilon.$$

Remark 4.20. *Consider again the base case $\mathfrak{m} = \mathcal{O}_K$. The running time of the random walk as in Theorem 4.18 depends on quite a subtle way on the Gaussian spread s of the continuous walk. Roughly said, one can distinguish three regions; $s < 1/\eta_1(\Lambda^*_K)$, $1/\eta_1(\Lambda^*_K) \leq s < \eta_1(\Lambda_K)$ and $\eta_1(\Lambda_K) \leq s$, see also Figure 4.11.*

(i) If $s < 1/\eta_1(\Lambda^*_K)$, the Gaussian is narrow compared to the unit group torus T. Each Gaussian covers a volume of around $s^{\mathbb{r}}$ in the Arakelov class group, which has volume $|\mathrm{Pic}^0_K|$. It is then intuitively clear that around $O(|\mathrm{Pic}^0_K|/s^{\mathbb{r}})$ reasonably equidistributed duplicates of that Gaussian spot are needed to cover the entire Arakelov class group, i.e., to get a nearly uniform distribution. As the duplicates grow exponentially per random walk step, one expects to need $O(\log|\mathrm{Pic}^0_K| + \mathbb{r}\log(s^{-1}))$ random walk steps. So in this particular case, the inverse $1/s$ of the Gaussian spread s has a significant influence on the running time.

(ii) *If* $1/\eta_1(\Lambda_K^*) \leq s < \eta_1(\Lambda_K)$*, the Gaussian spread is already so large that it has already some overlap on the unit torus. So it is then to be expected that the running time of the random walk does not so much depend on this Gaussian spread per se, but rather on the structure of the log unit lattice. If there is a significant gap between* $1/\eta_1(\Lambda_K^*) \approx 1/\lambda_{\mathbb{r}}(\Lambda_K^*) \approx \lambda_1(\Lambda_K)$ *and* $\eta_1(\Lambda_K) \approx \lambda_{\mathbb{r}}(\Lambda_K)$*, one can deduce that this log unit lattice must be quite 'distorted'.*

(iii) *If* $\eta_1(\Lambda_K) \leq s$*, the Gaussian is already so wide that it covers the entire unit group torus (the connected component of the unit in* Pic_K^0*). Then neither the Gaussian spread* s *nor the log unit lattice* Λ_K *have then any influence on the running time: For such large* s *one can simply replace* $\log(1/\tilde{s})$ *by* 0 *and* $\mathrm{Vol}(\mathrm{Pic}_K^0)$ *by* h_K *in Theorem 4.18. Not surprisingly, one then recovers the 'rapid mixing theorem' for ideal class groups by Jetchev and Wesolowski [JW15]. Additionally, by letting* k *tend to zero (i.e., allowing for an infinite number of steps* N*) one obtains that the prime ideals of norm below* $B = \widetilde{O}(\log(|\Delta_K|)^2)$ *generate the ideal class group, a fact better known as* Bach's bound *[Bac90].*

For the case $\mathfrak{m} \neq \mathcal{O}_K$*, the same reasoning applies, but with the ray unit torus* $T^{\mathfrak{m}}$ *instead.*

Applications of the Random Walk theorem in the subsequent chapters

The genericness of the random walk theorem (Theorem 4.18) allows it to be used for many applications. In this thesis, we specialize the parameters for two cases.

The first case concerns the worst-case to average-case reduction for Hermite-SVP on ideal lattices, the topic of Chapter 5. In that chapter we apply Theorem 4.18 for general number fields and cyclotomic fields separately (see Proposition 5.10). In this specialization of the random walk theorem we aim at an as low as possible value for $B^{N/n}$, as this is the loss in shortness quality in the worst-case to average-case reduction. The cyclotomic field gets a special treatment because one can obtain sharper bounds in that case,

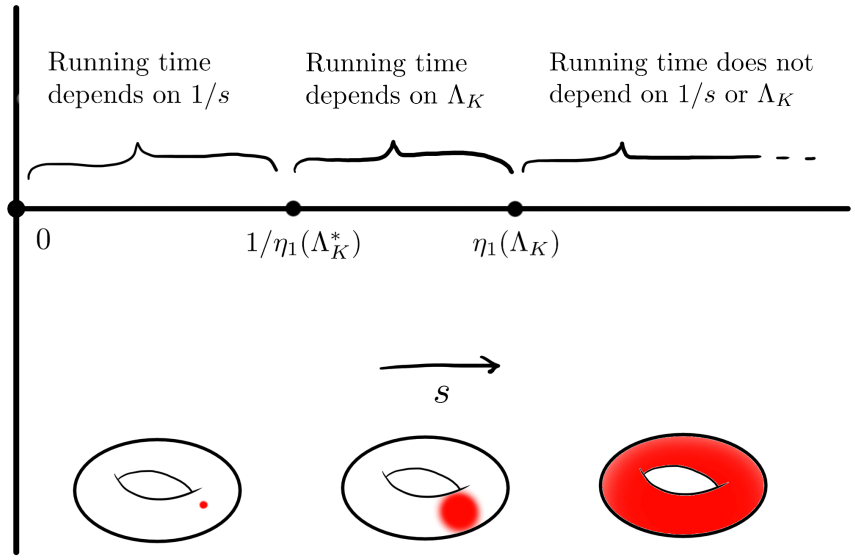

Figure 4.11.: The larger the Gaussian deviation s is, the less influence it has on the running time of the random walk.

assuming that the class number of the maximal totally real subfield of the cyclotomic field remains reasonably small, asymptotically. This is due to the occurrence of the *cyclotomic units* in cyclotomic fields, a subgroup of the unit group with particularly nice properties.

The second case concerns ideal sampling, the main topic of Chapter 6. In that chapter we show that a specific way of sampling in an ideal resembles sampling in a ideal that is a result of a random walk on the Arakelov class group. It applies Theorem 4.18 to show that this latter result of a random walk is close to uniformly distributed. In those cases one can apply ideal density results to lower bound the probability that the relative ideal (the sampled element divided by the input ideal) lies in a certain ideal set. In this application there is not really a restriction on any parameter, apart that those need to be small enough for the sampling algorithm to be efficient. In Theorem 6.3 of Chapter 6 we made some parameter choices (e.g., $s \approx 1/n^2$) to make the computation less involved and making the sampling in the

distorted box feasible; also the specialized theorem in this chapter is slightly aimed at a small B, the bound on the norm of the prime ideals. For the ideal sampling result this is not required; one can append these parameters as one wishes, provided that the sampling in the distorted box can still be done efficiently (or is at least non-vacuous) and taking care that the prime ideals involved (this depends on the parameter B) do not get too large to be feasible.