# Application of Automorphic Forms to Lattice Problems

Samed Düzlü Juliane Krämer
Universität Regensburg
{samed.duzlu, juliane.kraemer}@ur.de

June 9, 2022

**Abstract**

In this paper, we propose a new approach to the study of lattice problems used in cryptography. We specifically focus on module lattices of a fixed rank over some number field. An essential question is the hardness of certain computational problems on such module lattices, as the additional structure may allow exploitation. The fundamental insight is the fact that the collection of those lattices are quotients of algebraic manifolds by arithmetic subgroups. Functions on these spaces are studied in mathematics as part of number theory. In particular, those form a module over the Hecke algebra associated with the general linear group. We use results on these function spaces to define a class of distributions on the space of lattices. Using the Hecke algebra, we define Hecke operators associated with collections of prime ideals of the number field and show a criterion on distributions to converge to the uniform distribution, if the Hecke operators are applied to the chosen distribution. Our approach is motivated by the work of de Boer, Ducas, Pellet-Mary, and Wesolowski (CRYPTO'20) on self-reduction of ideal lattices via Arakelov divisors.

**Keywords.** lattice-based cryptography – module lattices – automorphic representations – algebraic groups

## 1 Introduction

In recent years, lattice-based cryptography is viewed as one of the most promising candidates for cryptographic schemes that are assumed to be secure against attacks by quantum computers. Lattice-based cryptography is built on hardness assumptions of lattice problems. The learning with errors (LWE) problem is the most prominent problem which is used directly to build cryptographic protocols. The well-studied shortest vector problem (SVP) is often used to relate the hardness of LWE to a lattice problem that is known to be hard. Indeed, SVP, the problem of finding nonzero vectors which are shortest up to a constant, is NP hard [MG02; Mic01]. For efficiency reasons, many schemes are based on structured lattices in the sense that the lattices admit the structure of a module over the ring of integers of specifically chosen number fields, e.g., [Alk+16; Alk+20; Bos+18; Duc+18; Pre+20], see [Nae+20] for an unstructured version. The transition towards structured lattices appeared in two steps. First the lattices have been chosen to be fractional ideals of a number field, viewed as lattice in a Euclidean space by means of the Minkowski embedding, so-called ideal lattices [LPR10; LPR13]. No efficient algorithms are known thus far that exploit this additional structure. Hence, it is assumed that schemes based on this construction are as secure as their unstructured counterparts [Pei14; SS11]. See also [CDW17; DPW19; PHS19] for potential weaknesses due to quantum computing. Despite the security assumptions for ideal lattices, in a second step, some schemes started to use higher rank versions of ideal lattices, i.e., module lattices [LS15]. These form a middle ground between ideal lattices and unstructured lattices, as they are algebraically structured, but the structure is more complex than the structure of ideal lattices. Hence, cryptographic schemes based on module lattices are almost as efficient and at least as secure as the ideal lattice variants. As the use of structured lattices has become

standard in lattice-based cryptography, their in-depth analysis is crucial.

This work is mainly motivated by [Boe+20], which shows a worst-case to average-case reduction for ideal lattices. Below, we summarize their approach and describe how the steps there are reproduced for module lattices of higher rank. Two major distinctions in our approach is that for higher rank module lattices, the notion of Arakelov divisors is replaced by adèles and Fourier analysis is substituted by the notion of automorphic forms.

**Contribution.** We show that for a fixed number field, the collection of module lattices of a fixed rank $m$ admits a geometric structure as a quotient of a product of copies of $\mathrm{GL}_m$ over real and complex numbers. We present an approach to analyze the space of square-integrable functions and more precisely automorphic forms, which we view as distributions on the space of lattices. Specifically, we introduce a class of such distributions which we call cuspidal distributions. We expect that proper worst-case distributions on the space of lattices can be found among cuspidal distributions. Using the theory of automorphic forms, we construct certain Hecke operators attached to prime ideals of the given number field. Further, we show a convergence of cuspidal distributions towards the uniform distribution under applying the previously defined Hecke operators. As the mathematical foundations stem from the theory of automorphic forms, we use the approach previously defined to define a new, general class of structured lattices which we call $\mathcal{G}$-structured lattices associated with algebraic groups.

**Outline.** In Section 1.1 we continue with a brief summary of the approach of [Boe+20] to their worst-case to average-case reduction of ideal-SVP. We introduce the motivation to our approach with a step-by-step analysis of the path we follow in Section 1.2. Specifically, we explain the ideas behind the choices we make. In Section 2, we introduce notations and the basic tools from algebraic number theory which are used later. In particular, we introduce norms on number fields, completions, and the adèles of a number field. Section 3 establishes the connection between module lattices of a fixed rank and so-called adèlic points of $\mathrm{GL}_m$. In particular, the collection of such module lattices admits a geometric structure. In Section 4, we introduce a class of functions on the space of module lattices, namely automorphic forms and more specifically, cusp forms. We mention decomposition results which allow us to analyze cusp forms in terms of representation theory. We develop the background to the extent required for our purposes. In particular, the Hecke algebra is introduced, which is the source of Hecke operators we use in the criterion for a worst-case to average-case convergence. In Section 5, we define a subclass of automorphic forms which we call cuspidal distributions. We provide a convergence criterion for cuspidal distributions to converge to the average-case distribution that mimics the results of [Boe+20]. In Section 6 we introduce the lattices with $\mathcal{G}$-structure and give basic examples and a first application.

In Appendix A, we review the basic setup of [Boe+20] from the viewpoint of adèles as taken in this work. After giving an adèlic description of the space of ideal lattices, we review their worst-case distribution in terms of Hecke characters. In Appendix B, we cover more details of representation theory that allows to construct certain cuspidal automorphic representations. We show how one can use these to construct a cuspidal distribution on lattices of rank 2 using the case of ideal lattices.

This paper uses many results from algebraic number theory and representation theory. We recall many definitions and results that are necessary if they have not been used in the cryptographic literature, even if they are standard in the related fields of mathematics.

## 1.1 Summary of Results for Ideal Lattices

We briefly recall the approach in [Boe+20], which we follow in two main aspects with a shift of perspective. A transfer of their results to our framework is sketched in Appendix A.

**Geometry of Ideal Lattices.** Let $k$ denote a number field with ring of integers $\mathcal{O}_k$. A first step is to note that the set of ideal lattices can be identified with the Arakelov class group, which geometrically is given as

$$\mathrm{Pic}_k \coloneqq \coprod_{\mathrm{Cl}_k} \Lambda_k \backslash \mathbb{R}^r = (\Lambda_k \backslash \mathbb{R}^r)^{h_k},$$

with $r$ being the number of real and complex embeddings of $k$ up to conjugation, $\Lambda_k$ is the logarithm of the units $\mathcal{O}_k^\times$, and $\mathrm{Cl}_k$ and $h_k$ are the class group and class number of $k$, respectively. Algebraically, the set of ideal lattices forms a group, called Arakelov class group, which is an extension of $\Lambda_k \backslash \mathbb{R}^r$ by the class group $\mathrm{Cl}_k$. By Dirichlet's unit theorem, the unit lattice $\Lambda_k$ has rank $r-1$ and lies in the trace 0 subgroup $H \cong \mathbb{R}^{r-1}$. The ideal lattices that correspond to

$$\mathrm{Pic}_k^0 \coloneqq \coprod_{\mathrm{Cl}_k} \Lambda_k \backslash H$$

are lattices with norm 1, see Appendix A or [Boe+20] for a rigorous definition. This is the degree 0 subgroup of the Arakelov class group. By the fundamental fact that this space is a compact group, it admits a uniform distribution which corresponds to choosing uniformly random ideal lattices.

**Worst-case Distribution.** With the geometric perspective in hand, in [Boe+20] a worst-case distribution is defined by means of the usual Gaussian distribution on $H$, which is pushed down to the quotient $\Lambda_k \backslash H$ and extended by 0 to the whole $\mathrm{Pic}_k^0$ (i.e., the connected components different from $1 \in \mathrm{Cl}_k$). A class of Hecke operators on the space of square-integrable functions on $\mathrm{Pic}_k^0$ is defined in terms of a finite set of (finite) primes of $k$. These are translation operators at each prime, averaged over the set of chosen primes. They move the support of the worst-case distribution inside $\mathrm{Pic}_k^0$ so quickly that the sequence formed by iteratively applying them to the worst-case distribution converges to the uniform distribution. A technical but crucial feature is that characters of $\mathrm{Pic}_k^0$ are eigenfunctions of these operators. This property allows the analysis of the behavior of the worst-case distribution under the operators in terms of their Fourier series decomposition. The worst-case to average-case convergence is analyzed in terms of the Fourier series. Subject to the generalized Riemann hypothesis this convergence is the main result of [Boe+20]. Using this result, they show that, up to a change of constant, the worst-case SVP is as hard as the average-case SVP.

## 1.2 Summary of Our Framework

In this work, we attach a geometric structure to the set of module lattices of a fixed rank, which in rank 1 is equivalent to the approach in [Boe+20]. Instead of Arakelov theory, we use adèles, which are one of the basic constructions in algebraic number theory; see Remark 3.3.5 for a more detailed comparison. It turns out that the space of lattices of a fixed rank $m$ is quite similar to $\mathrm{Pic}_k$ in ideal lattices, i.e., the rank 1 case, namely,

$$\coprod_{\alpha \in \mathrm{Cl}_k} \Gamma_\alpha \backslash \mathrm{GL}_m(\mathbb{R})^{r_1} \times \mathrm{GL}_m(\mathbb{C})^{r_2},$$

where $r_1$ and $r_2$ are the number of real and complex embeddings of $k$, up to conjugation, respectively, and $\Gamma_\alpha$ is a discrete (arithmetic) subgroup of $\mathrm{GL}_m(\mathbb{R})^{r_1} \times \mathrm{GL}_m(\mathbb{C})^{r_2}$. The analogue of $\mathrm{Pic}_k^0$ is a norm 1 subspace of the above space, which we denote $\mathrm{Lat}_m^1(k)$. Of course, for $m > 1$, $\mathrm{Lat}_m^1(k)$ does *not* acquire a group structure from $\mathrm{GL}_m$, but still is a symmetric space as it admits a transitive group action by $\mathrm{GL}_m(\mathbb{R})^{r_1} \times \mathrm{GL}_m(\mathbb{C})^{r_2}$. Therefore, $\mathrm{Lat}_m^1(k)$ admits a right-invariant (with respect to the action of $\mathrm{GL}_m(\mathbb{R})^{r_1} \times \mathrm{GL}_m(\mathbb{C})^{r_2}$) measure, which is unique up to scaling. A well-known result tells that the volume of $\mathrm{Lat}_m^1(k)$ with respect to this invariant measure is finite, see Proposition 3.2.3. In particular, the unique normalized invariant measure takes the role of a uniform distribution on the space of module lattices of rank $m$.

The next step is to define a worst-case distribution as in our approach we want to mimic [Boe+20]. However, the goal of finding suitable worst-case distributions becomes nontrivial for two reasons. First, the space of module lattices for $m > 1$ is not a torus as it is for $m = 1$. Thus, we cannot define a Gaussian distribution in a straightforward manner. Second, even if we find a suitable function which geometrically mimics the properties of the worst-case distribution in rank 1, there is no general tool, which allows to decompose a function into basic components, as does Fourier analysis in rank 1. We take the following approach.

**Functions as Distributions.** We are looking for distributions in the space of functions on the space of lattices. From an abstract viewpoint, the space of distributions is strictly larger than the usual function spaces, e.g., Dirac's $\delta$-distributions are not represented by functions. In fact, $\delta$-distributions are perfect worst-case distributions. However, applying Hecke operators as in [Boe+20] to the $\delta$-distribution will result in distributions with discrete spectrum, which cannot converge to the uniform distribution.

With this assumption, the functions we consider should satisfy certain properties. Namely, it should be square-integrable, smooth, symmetric, and decay quickly outside of a central point. This motivates the second assumption to look into the space of automorphic forms and more specifically, cusp forms.

**Decomposition of Automorphic Forms and Cusp Forms.** The space of $\mathrm{L}^2$-functions on $\mathrm{Lat}_m^1(k)$ is subject of the study of automorphic forms in algebraic number theory and representation theory. For $m > 1$, the space of square-integrable functions admits a decomposition

$$\mathrm{L}^2(\mathrm{Lat}_m^1(k)) = \mathrm{L}_0^2(\mathrm{Lat}_m^1(k)) \times \mathrm{L}_{\mathrm{fin}}^2(\mathrm{Lat}_m^1(k)) \times \mathrm{L}_{\mathrm{Eis}}^2(\mathrm{Lat}_m^1(k)),$$

where $\mathrm{L}_0^2(\mathrm{Lat}_m^1(k))$ are cusp forms, $\mathrm{L}_{\mathrm{fin}}^2(\mathrm{Lat}_m^1(k))$ are constant functions, and $\mathrm{L}_{\mathrm{Eis}}^2(\mathrm{Lat}_m^1(k))$ are Eisenstein series. The subspace of cusp forms and constant functions can be analyzed in terms of representation theory. Moreover, in the case $m = 1$, all square-integrable functions lie in this subspace. Accordingly, we believe that a worst-case distribution for rank $m > 1$ ought to be in the space of cusp forms and constant functions.

The space of cusp forms itself decomposes into a (Hilbert space) direct sum of cusp forms with central character. Each of these terms again splits into irreducible components, which are the basic building blocks of the space of cusp forms, in the same manner as how characters are the basic functions in Fourier analysis. This is also a generalization of the classical theory of modular forms, which is the case of base field $\mathbb{Q}$ and rank $m = 2$. The decomposition then corresponds to cusp forms which are simultaneous eigenfunctions of Hecke operators, cf. [Kud03] for the connection between modular forms and automorphic forms for $\mathrm{GL}_2$ over $\mathbb{Q}$.

**Worst-Case to Average-Case Convergence.** Keeping the previous ideas in mind, we define a class of *cuspidal distributions* in the space of automorphic forms. These contain the uniform distribution and as described above, it can be seen as a source for worst-case distributions. For general cuspidal distributions, we give a criterion for the convergence to the uniform distribution. This is done in terms of the decomposition of cuspidal distributions into irreducible cusp forms plus a constant. As the cusp forms are eigenfunctions of Hecke operators, the condition is mainly a question of convergence of the coefficient series.

**Lattices with $\mathcal{G}$-Structure.** From a theoretical perspective, our approach is not restricted to the case of module lattices. Motivated by the theory of automorphic forms for a more general class of groups, we introduce a new concept of lattices with $\mathcal{G}$-structure. These lattices are defined in terms of an affine algebraic group over $\mathcal{O}_k$ with a (faithful) representation. We exemplify the definitions with commonly used types of structured lattices as well as of lattices with $\mathcal{G}$-structure for the symplectic group, which correspond to symplectic lattices. Further, we display how lattices defined in terms

of cyclic algebras as in [GLV19] are encapsulated by the given definition. The Jacquet–Langlands correspondence of the theory of automorphic forms allows us to transfer cuspidal distributions on rank 2 module lattices to cyclic lattices in [GLV19], for the case of quaternion algebras.

### 1.3 Related Work

Since [BGV12; LS15], module lattices are studied for their applications in cryptography. In [LS15] a worst-case to average-case reduction was proven that reduced worst-case instances of module-LWE to average-case instances. This result opened the door for the application of module lattices to replace unstructured or ideal lattices. More recently, a different type of self-reduction of SVP on module lattices was shown in [Lee+19; MS20], where SVP of module lattices is reduced to module lattices of a smaller rank, where the rank of the latter divides the rank of the former. Both are generalizations of the LLL algorithm [LLL82].

## 2 Preliminaries

Let $k$ be an algebraic number field of degree $n$, of signature $(r_1, r_2)$, and set $r = r_1 + r_2$. That is there are $r_1$ distinct *real embeddings* of $k$ into $\mathbb{R}$ and up to conjugation $r_2$ *complex embeddings* into $\mathbb{C}$ whose image does not lie in $\mathbb{R}$. We denote by $\mathcal{O}_k$ the ring of integers of $k$. Further, $\mathrm{Cl}_k$ denotes the class group of $k$ and $h_k$ the class number, i.e., the number of elements of the class group.

We will write $\mathbb{G}_m$ for the algebraic group of multiplicative units over $k$, that is, for any $k$-algebra $A$, $\mathbb{G}_m(A) = A^\times$ is the group of invertible elements in $A$. Here, $A$ is assumed to be commutative with unit, but we will be concerned with non-commutative non-unital algebras in Section 4. More generally, $\mathrm{GL}_m$ denotes the algebraic group of invertible $m$-by-$m$ matrices over $k$. Again, for any $A$, $\mathrm{GL}_m(A)$ is the group of $m$-by-$m$ matrices with entries in $A$, whose determinant is in $\mathbb{G}_m(A)$. For slightly more on algebraic groups, see Section 6.

### 2.1 Norms on a number field

In this subsection we briefly recall the notion of norms on a number field and state their characterization in terms of Ostrowski's Theorem. We exclude the trivial norm in the definition by requiring norms to be nonzero.

**Definition 2.1.1.** A *norm on* $k$ is a nonzero map $|\_|\colon k \to \mathbb{R}_{\geqslant 0}$ such that the following hold

- $|x| = x \iff x = 0$
- $|xy| = |x||y|$
- $|x + y| \leqslant |x| + |y|$.

Two norms $|\_|_1$ and $|\_|_2$ are *equivalent*, if there exists constants $c > 0$ such that for all $x$

$$|x|_1 \leqslant |x|_2^c.$$

We refer to [Neu99, II, Definition 3.2, Proposition 3.3] for a topological definition and their equivalence. There are two distinct classes of norms which we will exemplify now.

**Example 2.1.2** (Archimedean Norms)**.** Let $\sigma\colon k \hookrightarrow \mathbb{C}$ be an embedding of $k$, possibly with image in $\mathbb{R}$. Then a norm on $\mathbb{C}$ induces a norm on $k$ by restriction, i.e., $|x|_\sigma \coloneqq |\sigma(x)|$. For the purpose of standardizing, we choose the usual absolute value, if the embedding is real, while for a complex embedding $\sigma$ we set

$$|x|_\sigma \coloneqq \sigma(x)\overline{\sigma}(x) = \sigma(x)\overline{\sigma(x)}.$$

This differs from the usual norm on $\mathbb{C}$ by a square. The reason for this choice will become more apparent in the Product Formula 2.1.7.

**Example 2.1.3** (Non-Archimedean Norms)**.** For any nonzero element $x \in k$ the fractional ideal which it generates can be decomposed uniquely into a product of maximal ideals as

$$(x) = \prod_{\mathfrak{q}} \mathfrak{q}^{\nu_{\mathfrak{q}}(x)},$$

where for almost all $\mathfrak{q}$ the exponents are 0, so that the product is actually finite. For any nonzero prime ideal $\mathfrak{p}$ we define a valuation function

$$\nu_{\mathfrak{p}} \colon k^{\times} \to \mathbb{Z};\ x \mapsto \nu_{\mathfrak{p}}(x).$$

For any number $0 < u < 1$ we set

$$|\_|_{\mathfrak{p}} \colon k^{\times} \to \mathbb{R}_{>0};\ |x|_{\mathfrak{p}} = u^{\nu_{\mathfrak{p}}(x)}.$$

Extending this function to $k$ by setting $|0| := 0$ defines a norm called $\mathfrak{p}$-adic norm. Up to equivalence of norms, this construction is independent of $u$. For distinct primes $\mathfrak{p} \neq \mathfrak{q}$ the norms are inequivalent. This follows from the existence of elements $x$ which are contained in $\mathfrak{p}$ but not in $\mathfrak{q}$. Thus, $|x|_{\mathfrak{p}} < 1$ while $|x|_{\mathfrak{q}} = 1$, which implies that the sequence $x^n$ converges to 0 in the $\mathfrak{p}$-adic norm, but not in the $\mathfrak{q}$-adic. Again, we fix standard choices for the constants $u$. Namely, for a prime $\mathfrak{p}$, the intersection $\mathfrak{p} \cap \mathbb{Z} = (p)$ is an ideal generated by a prime element in the classical sense, with $p$ positive. Taking quotients induces an extension

$$\mathbb{Z}/p \subseteq \mathcal{O}_k/\mathfrak{p}$$

of finite fields. Let $f_{\mathfrak{p}}$ denote the degree of this extension (the *inertia index*). The standard choice of $u$ for $|\_|_{\mathfrak{p}}$ is $p^{-f_{\mathfrak{p}}}$. As for the choices of Archimedean norms 2.1.2, the reason for the choice will become clear in the Product Formula 2.1.7.

We want to note that the non-Archimedean norms are inherently different from the Archimedean norms, as they satisfy a *strong triangle inequality*.

**Lemma 2.1.4.** *Let $|\_|$ be a non-Archimedean norm as in Example 2.1.3. Then*

$$|x + y| \leqslant \max\{|x|, |y|\} \tag{2.1}$$

*for any $x, y$.*

For a proof, we refer to [Neu99], although, this follows easily from the analogous statement for the valuation $\nu_{\mathfrak{p}}$ (where max turns to min, and the sign changes), which is an immediate consequence of the definitions. Of course, this strong triangle inequality does not hold in the Archimedean cases, e.g., $2 = |2| > |1| = 1$, and similarly in the complex case (where $|2| = 4$). The strong triangle inequality is usually taken as the definition of a non-Archimedean norm.

**Definition 2.1.5.** A norm $|\_|$ on $k$ is *non-Archimedean*, if it satisfies the strong triangle inequality (2.1). Otherwise, $|\_|$ is *Archimedean*.

Note that Archimedean is defined to be not non-Archimedean. A characterization can be given in terms of the norm restricted to $\mathbb{Z}$. In fact, a norm $|\_|$ is Archimedean, if and only if $\mathbb{Z}$ is unbounded with respect to $|\_|$. The next result classifies all absolute values on a number field.

**Theorem 2.1.6** (Ostrowski)**.** *Up to equivalence, the norms on $k$ are*

- *Archimedean norms as in Example 2.1.2*
- *Non-Archimedean norms as in Example 2.1.3*

For a proof, see [Neu99, Chapter II].

The equivalence classes of norms on $k$ are called places of $k$. The set of all places will be denoted $\mathcal{P}_k$. A place is called *finite*, if it corresponds to a non-Archimedean absolute value. On the other hand, *infinite* places are the Archimedean ones. We stress that finite places are in natural one-to-one correspondence with (nonzero) primes of $\mathcal{O}_k$; while the infinite places correspond bijectively to embeddings into real and complex numbers up to conjugation. We will write $\nu \mid \infty$, if $\nu$ is an infinite place, and $\nu \nmid \infty$, if $\nu$ is a finite place.

**Theorem 2.1.7** (Product Formula)**.** *Let $0 \neq \lambda \in k$ be a nonzero element. Then $\prod_\nu |\lambda|_\nu = 1$ where the product is taken over all places of $k$.*

The Product Formula is one motivation for the normalizations we chose. However, they are quite natural from a measure theoretic perspective as one can find in [Wei95]. Note that the possibly infinite product is finite. In fact, $\nu_\mathfrak{p}(\lambda) \neq 0$, only if $\mathfrak{p}$ appears in the prime decomposition of $\lambda$, which consists of only finitely many factors.

### 2.1.1 Completions

It turns out that a norm $\nu$ on $k$ is never complete in the sense that Cauchy sequences with respect to $\nu$, do not necessarily converge in $k$.

**Example 2.1.8** (Archimedean Case)**.** Let us consider $\mathbb{Q}$ with respect to the standard (Archimedean) absolute value. The sequence of $(x_n)$, where the $n$-th term is $\sqrt{2}$ chopped after $n$ decimal places, is a Cauchy sequence with respect to the Archimedean norm. However, there is no $x \in \mathbb{Q}$ such that $(x_n) \xrightarrow{n\to\infty} x$. In fact, such an $x$ would satisfy $x^2 = 2$ which does not exist in $\mathbb{Q}$.

**Example 2.1.9** (Non-Archimedean Case)**.** We confine ourselves with the following fact. The $p$-adic integers $\mathbb{Q}_p$ contain $p$-th roots of unity, while $\mathbb{Q}$ does not contain any roots of unity except $\pm 1$. The existence in $\mathbb{Q}_p$ follows from Hensel's Lemma ([Neu99, pp. II, 4.6]) which cannot hold for $\mathbb{Q}$. It is possible to construct explicitly sequences that do not converge in $k$ as well.

The process of completion deals with this failure. For any norm $\nu$, there exists a field extension $k_\nu$ of $k$, together with a norm $\hat{\nu}$ that extends $\nu$ to $k_\nu$, such that $(k_\nu, \hat{\nu})$ is complete, and for every other field extension $K/k$ and extension $\nu_K$ of $\nu$ to $K$ such that $(K, \nu_K)$ is complete, there exists a unique homomorphism $k_\nu \to K$ such that $\nu_K$ extends $\hat{\nu}$. We do not need details of the construction but instead give the resulting completions in the two cases.

### 2.1.2 Completion at Archimedean Places

Let $\sigma$ be an Archimedean place corresponding to a real or complex embedding. As $\mathbb{R}$ and $\mathbb{C}$ are complete, we know that the completion $k_\sigma$ of $k$ with respect to $\sigma$ needs to be contained in $\mathbb{R}$ or $\mathbb{C}$, respectively. Using that $\mathbb{R}$ is by definition the completion of $\mathbb{Q}$ with respect to its Archimedean place, it is easy to see that $\mathbb{R}$ or $\mathbb{C}$ are in fact the completions of $k$ with respect to $\sigma$.

Let us define

$$k_\infty := \prod_{\sigma|\infty} k_\sigma.$$

It carries a norm defined by $\sum_\sigma |\_|_\sigma$. This space is equivalent to $k_\mathbb{R}$ in Minkowski theory. As in the theory of adèles, the perspective is taken on places rather than embeddings, we prefer $k_\infty$. Note that by an equivalence between $k_\infty$ and $k_\mathbb{R}$ we mean an isometry, however compatible choices need to be made at each place.

### 2.1.3 Completion at Non-Archimedean Places

As non-Archimedean norms are not used often in cryptography, we briefly recall the construction of the completions. Let us begin with $p$-adic integers $\mathbb{Z}_p$ and generalize from there. Note that unfortunately, $\mathbb{Z}_p$ is overloaded and can have totally distinct meanings. We will stick to the usual convention in algebraic number theory and denote by $\mathbb{Z}_p$ the $p$-adic integers, and write $\mathbb{Z}/p$ for the quotient modulo $p$. We sincerely hope that this will not cause confusion.

**Example 2.1.10.** Let $p$ be an integer prime. Then $\mathbb{Z}_p$ is the ring

$$\varprojlim_n \mathbb{Z}/p^n := \{x = (x_n) \in \prod_{n>0} \mathbb{Z}/p^n \mid \quad x_{n+1} \equiv x_n \mod p^n \text{ for all } n\}$$

with componentwise addition and multiplication. It is a closed subset of $\prod_{n>0} \mathbb{Z}/p^n$ where each factor has the discrete topology. Then, by Tychonoff's compactness theorem, it follows that $\mathbb{Z}_p$ is compact. There is a natural *injective* ring homomorphism $\mathbb{Z} \to \mathbb{Z}_p$. Moreover, $\mathbb{Z}_p$ is a local principal ideal domain with the unique nonzero prime ideal $(p)$. Such rings are called *discrete valuation rings*. Any other ideal of $\mathbb{Z}_p$ can be written as $(p^n)$ for some $n$. The field of fractions is denoted $\mathbb{Q}_p$, the $p$-adic numbers. It is the completion of $\mathbb{Q}$ with respect to the $p$-adic norm. Details can be found in [Neu99, Chapter II]. In particular, a representation of $p$-adic numbers as power series with coefficients in $0, \dots, p-1$ might be interesting for application purposes, although as in decimal representation of real numbers, arithmetic on such series is difficult due to carries.

Returning to the case of $k$, let $\mathfrak{p}$ be a finite place by which we also denote the corresponding prime ideal of $\mathcal{O}_k$. Let $p$ be the integer prime lying under $\mathfrak{p}$, i.e., $(p) = \mathfrak{p} \cap \mathbb{Z}$. Then set $\mathcal{O}_\mathfrak{p} \coloneqq \mathbb{Z}_p \otimes_\mathbb{Z} \mathcal{O}_k$. This is a ring which contains $\mathcal{O}_k$ as a subring. The properties for $\mathbb{Z}_p$ mentioned in Example 2.1.10 hold for $\mathcal{O}_\mathfrak{p}$. Note that this is different when comparing $\mathbb{Z}$ and $\mathcal{O}_k$, as e.g., $\mathcal{O}_k$ is not a PID in general. In particular, $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring with unique maximal ideal $\mathfrak{p}$. This is a slightly abusive notation as $\mathfrak{p}$ now denotes the place of $k$, an ideal of $\mathcal{O}_k$, and the unique maximal ideal of $\mathcal{O}_\mathfrak{p}$. This will however not cause any problem and they uniquely correspond to each other. The field of fractions $k_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ contains $k$. The norm on $k_\mathfrak{p}$ is defined via a (discrete) valuation as in Example 2.1.3. More precisely, let $t$ be a generator of the maximal ideal $\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$, commonly called *uniformizer* or *uniformizing element*. Then any element $\lambda \in k_\mathfrak{p}^\times$ can be written *uniquely* as $\lambda = ut^n$ with $u \in \mathcal{O}_\mathfrak{p}^\times$ and $n \in \mathbb{Z}$. The value $n$ is independent of the choice of $t$ and thus we can define

$$\nu_\mathfrak{p} \colon k_\mathfrak{p}^\times \to \mathbb{Z}; \;\; \lambda \mapsto n, \text{ if } \lambda = ut^n \text{ with } u \in \mathcal{O}_\mathfrak{p}^\times.$$

Then the $\mathfrak{p}$-adic norm on $k_\mathfrak{p}$ is defined as

$$|\_|_\mathfrak{p} \colon k_\mathfrak{p} \to \mathbb{R}_{\geqslant 0}; \;\; \lambda \mapsto p^{-f_\mathfrak{p}\, \nu_\mathfrak{p}(\lambda)}$$

where $|0|_\mathfrak{p}$ is understood to be 0. The ring $\mathcal{O}_\mathfrak{p}$ and its maximal ideal $\mathfrak{p}$ can be recovered as the sets

$$\mathcal{O}_\mathfrak{p} = \{\lambda \in k_\mathfrak{p} \mid \; |\lambda|_\mathfrak{p} \leqslant 1\}$$

and

$$\mathfrak{p} = \{\lambda \in k_\mathfrak{p} \mid \; |\lambda|_\mathfrak{p} < 1\}.$$

The unit group $\mathcal{O}_\mathfrak{p}^\times$ is open and closed, hence compact.

## 2.2 Adèles

The completions of $k$ introduced in the previous section constitute the factors of the adèles, which we are going to introduce here.

**Definition 2.2.1.** The adèle ring $\mathbb{A}_k$ of $k$ is the restricted product of $k_\nu$ with respect to $\mathcal{O}_\mathfrak{p}$ at all finite places.

This means that $\mathbb{A}_k \subseteq \prod_\nu k_\nu$ with $x = (x_\nu)_\nu \in \mathbb{A}_k$, if and only if $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ for all but finitely many finite places $\nu_\mathfrak{p}$. Recall that we wrote $k_\infty$ for the product of $k_\sigma$ with $\sigma \mid \infty$. The analogue for finite places is the ring $\mathbb{A}_{k,f}$ which is the restricted product of $k_\mathfrak{p}$ with respect to $\mathcal{O}_\mathfrak{p}$, taken over all finite places $\mathfrak{p}$. Again, this means that $x = (x_\mathfrak{p})_\mathfrak{p} \in \mathbb{A}_{k,f}$, if and only $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$. It then follows that $\mathbb{A}_k = k_\infty \times \mathbb{A}_{k,f}$. The ring of adèles gets a topology as follows. First, the infinite component $k_\infty$ carries a natural topology as described in Section 2.1.2. The finite part $\mathbb{A}_{k,f}$ is given the topology determined by enforcing $\widehat{\mathcal{O}}_k \coloneqq \prod_\mathfrak{p} \mathcal{O}_\mathfrak{p}$ to be open. Note that this is *not* the topology induced from the product of the $k_\mathfrak{p}$. The field $k$ is itself a subring of $\mathbb{A}_k$ via the diagonal embedding $k \hookrightarrow \mathbb{A}_k, \lambda \mapsto (\lambda)_\nu$.

**Theorem 2.2.2.** *With the diagonal embedding, $k$ is a discrete, cocompact subring.*

This theorem has important consequences in the Fourier analysis of number fields, which dates back to the thesis of Tate [Tat67]. Similar to the situation of lattices in Euclidean space, the Pontryagin dual of $k$ is $k\backslash\mathbb{A}_k$. More details can be found in Tate's thesis [Tat67] itself, as well as [RV99; Wei95].

Another important fact about the ring of adèles is that it satisfies an approximation theorem in the following sense. A proof can be found, for example, in [RV99, Chapter 5].

**Theorem 2.2.3.** *The subgroup $k$ of $\mathbb{A}_k$ is dense.*

A variant for $\mathrm{SL}_2$ will be used implicitly in Section 3.2 where we describe the geometry of the space of module lattices.

**Idèles.** The idèles of $k$ are defined to be $\mathbb{I}_k = \mathbb{G}_m(\mathbb{A}_k)$, i.e., invertible elements in $\mathbb{A}_k$. This group can be described explicitly as $x = (x_\nu)_\nu \in \mathbb{A}_k$ with $x_\nu \neq 0$ for all $\nu$ and $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$ for all but finitely many $\mathfrak{p} \nmid \infty$. It becomes a topological group by means of the embedding

$$\mathbb{G}_m(\mathbb{A}_k) \to \mathbb{A}_k^2;\ x \mapsto (x, x^{-1}).$$

Similar to adèles, we regard $k^\times$ as a subgroup of $\mathbb{G}_m(\mathbb{A}_k)$ via the diagonal embedding.

**Theorem 2.2.4.** *The group $k^\times$ of units is discrete in $\mathbb{G}_{\mathrm{m}}(\mathbb{A}_k)$.*

So far, the situation for the multiplicative group looks quite similar, however, the approximation theorem does not hold and the $k^\times$ is not cocompact in $\mathbb{G}_m(\mathbb{A}_k)$. A reason can be seen from the adèlic norm

$$|\_|\colon \mathbb{G}_m(\mathbb{A}_k) \to \mathbb{R}_{>0},\ x \mapsto \prod_\nu |x_\nu|_\nu.$$

Note that the condition that $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$ for all but finitely many $\mathfrak{p}$ ensures that all but finitely many factors are 1, so that this product is always well-defined. The norm map defines a group homomorphism. In fact, each factor is multiplicative, and the unit 1 has norm 1 in all places. We define the component norms

$$|\_|_\infty\colon k_\infty^\times \to \mathbb{R}_{>0},\ x \mapsto \prod_{\sigma|\infty} |x_\sigma|_\sigma$$

and

$$|\_|_f\colon \mathbb{G}_m(\mathbb{A}_{k,f}) \to \mathbb{R}_{>0},\ x \mapsto \prod_{\mathfrak{p}\nmid\infty} |x_\mathfrak{p}|_\mathfrak{p}.$$

The adèlic norm map is surjective, as it is so when restricting to any infinite place. As a consequence of the Product Formula 2.1.7 we have the following.

**Corollary 2.2.5.** *For $\lambda \in k^\times$ we have $|\lambda| = 1$.*

Here we regard $\lambda$ as an element of $\mathbb{G}_m(\mathbb{A}_k)$ via the diagonal embedding. In particular, the norm factors through $k^\times\backslash\mathbb{G}_m(\mathbb{A}_k)$ which shows that this quotient cannot be compact. This however, can be compensated in some sense. Let $\mathbb{G}_m(\mathbb{A}_k)^1$ denote the elements $x$ of $\mathbb{G}_m(\mathbb{A}_k)$ with $|x| = 1$.

**Theorem 2.2.6.** *The group $k^\times\backslash\mathbb{G}_{\mathrm{m}}^1(\mathbb{A}_k)$ is compact. More precisely, it is a disjoint union of $h_k$ many copies of $\Lambda_k\backslash\mathbb{R}^{r-1}$, where $\Lambda_k$ denotes the unit lattice in Minkowski theory.*

We do not go into the proof here. In the next section, we will consider the more general case where $\mathbb{G}_m$ is replaced by $\mathrm{GL}_m$. The present case is recovered by taking $m = 1$. The connection with the class group can be seen in terms of the finite idèles. Let $U_f := \mathbb{G}_m(\widehat{\mathcal{O}}_k) = \prod_\mathfrak{p} \mathbb{G}_m(\mathcal{O}_\mathfrak{p})$, where the product is taken over finite places of $k$.

**Proposition 2.2.7.** *The map*

$$\mathbb{G}_m(k)\backslash\mathbb{G}_m(\mathbb{A}_{k,f})/U_f \xrightarrow{\sim} \mathrm{Cl}_k;\ x = (x_\mathfrak{p}) \mapsto [I_x]$$

*where $I_x = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(x_\mathfrak{p})}$ is a fractional ideal, defines an isomorphism.*

*Proof.* It is easy to see that the above map is well-defined. Consider the map

$$\mathrm{I}_k \to \mathbb{G}_m(\mathbb{A}_{k,f});\ I \mapsto (t_{\mathfrak{p}}^{\nu_{\mathfrak{p}}(I)}),$$

where $t_{\mathfrak{p}}$ are uniformizers. It can be seen easily that this map induces a well-defined map $\mathrm{Cl}_k \to \mathbb{G}_m(k)\backslash\mathbb{G}_m(\mathbb{A}_{k,f})/U_f$, and the maps are mutually inverse. □

# 3 The space of module lattices

In this section, we redefine module lattices over the base field $k$ and attach to the set of module lattices of fixed rank a geometric structure. We set $G$ to be the algebraic group $\mathrm{GL}_m$.

## 3.1 Module lattices

Our definition mimics the notion of ideal lattices as defined in [Boe+20]. We proceed in two steps, first, we define rank $m$ analogues of fractional ideals, then we add a twist by $k_\infty$-automorphisms of $k_\infty^m$.

**Definition 3.1.1.** An $\mathcal{O}_k$-lattice is an $\mathcal{O}_k$-submodule $M \subseteq k^m$ of rank $m$.

This notion corresponds to *complete* lattices. Given an $\mathcal{O}_k$-lattice $M$ in $k^m$, we can view it as a subset of $k_\infty^m$ via the diagonal embedding. As such, $M$ defines a complete lattice in the usual sense, when we attach to $k_\infty$ the inner product and norm induced by its natural product structure. Let $\mathrm{Lat}_m^f(k)$ denote the set of $\mathcal{O}_k$-lattices of rank $m$.

We define $G_\infty$ to be $G(k_\infty) = \mathrm{GL}_m(k_\infty)$. This group comes with a natural product structure inherited from $k_\infty$. Namely, it decomposes as $G_\infty = \prod_{\sigma|\infty} G_\sigma$ with $G_\sigma = \mathrm{GL}_m(k_\sigma)$.

**Definition 3.1.2.** A *module lattice* of rank $m$ over $k$ is a lattice $\Lambda \subseteq k_\infty^m$ such that there exist an $\mathcal{O}_k$-lattice $M$ in $k^m$ and an element $g \in G_\infty$ such that $\Lambda = gM$.

We denote the set of module lattices of rank $m$ over $k$ by $\mathrm{Lat}_m(k)$. It can be described in terms of $\mathrm{Lat}_m^f(k)$ and $G_\infty$ as follows.

**Proposition 3.1.3.** *There is a canonical bijection*

$$G(k)\backslash\left(G_\infty \times \mathrm{Lat}_m^f(k)\right) \simeq \mathrm{Lat}_m(k);\ \ (g, M) \mapsto g^{-1}M.$$

We introduce the inverse for compatibility reasons, as will be seen later. Moreover, $G(k)$ acts on $G_\infty \times \mathrm{Lat}_m^f(k)$ by $\lambda.(g, M) = (\lambda g, \lambda M)$.

*Proof.* It is easy to see that the association $(g, M) \mapsto g^{-1}M$ is $G(k)$-equivariant, hence, the map on the quotient is well-defined. The surjectivity of the map is a basic consequence of the definition of module lattices. Suppose $(g, M)$ and $(h, N)$ are two pairs with $g^{-1}M = h^{-1}N$. Then $hg^{-1}M = N$, i.e., $hg^{-1}$ defines an isomorphism $\lambda\colon M \to N$ of $\mathcal{O}_k$-modules. Tensoring with $k$ over $\mathcal{O}_k$, $\lambda$ defines an isomorphism $k^m \to k^m$. In other words, $\lambda \in G(k)$ and it satisfies $\lambda M = N$, and $\lambda g = h$, so that $(g, M) = (h, N)$ modulo $G(k)$. □

As a consequence of the previous proposition, we will often write pairs $(g, M)$ for the module lattice $g^{-1}M$ associated with that pair.

Let $K_f$ be the subgroup $\mathrm{GL}_m(\widehat{\mathcal{O}}_k)$ of $G(\mathbb{A}_{k,f})$. It is a compact and open subgroup and decomposes into an infinite product $\prod_{\mathfrak{p}\nmid\infty} K_{\mathfrak{p}}$, with $K_{\mathfrak{p}} = \mathrm{GL}_m(\mathcal{O}_{\mathfrak{p}})$. Each factor $K_{\mathfrak{p}}$ itself is a compact open subgroup of $\mathrm{GL}_m(k_{\mathfrak{p}})$.

The next theorem can be found in [Bor63] and [Wei95, Theorem V.2.2]. We will use this description to define the geometric structure on the set of module lattices over $k$. Later, we will give a more effective description of the geometric object and the set of module lattices.

**Theorem 3.1.4.** *There exists a bijection*

$$\mathrm{Lat}_m(k) \xrightarrow{\sim} G(k)\backslash G(\mathbb{A}_k)/K_f;\ \ (g, M) \mapsto (g, (g_{M,\mathfrak{p}})_{\mathfrak{p}}).$$

*Here* $g_{M,\mathfrak{p}} \in G(k_{\mathfrak{p}})$ *with* $g_{M,\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}^m = M \otimes_{\mathcal{O}_k} \mathcal{O}_{\mathfrak{p}}$.

*Sketch of the proof.* Let us first explain the components at each finite place $\mathfrak{p}$. By scalar extension, the inclusion $M \subseteq k^m$ becomes $M \otimes_{\mathcal{O}_k} \mathcal{O}_{\mathfrak{p}} \subseteq k_{\mathfrak{p}}^m$. As $\mathcal{O}_{\mathfrak{p}}$ is a principal ideal domain, $M \otimes_{\mathcal{O}_k} \mathcal{O}_{\mathfrak{p}}$ is free. Hence, there exists an invertible matrix $g_{M,\mathfrak{p}} \in G(k_{\mathfrak{p}})$ such that $g_{M,\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}^m = M \otimes_{\mathcal{O}_k} \mathcal{O}_{\mathfrak{p}}$. The choice is unique, up to an automorphism of $\mathcal{O}_{\mathfrak{p}}^m$, i.e., up to $K_{\mathfrak{p}}$. Thus, the element $(g_{M,\mathfrak{p}})_{\mathfrak{p}} \in G(\mathbb{A}_{k,f})$ is unique up to $K_f$. In particular, the map is independent of the choice we made.

We need to ensure that with $\lambda \in G(k)$, the images of $(g, M)$ and $(\lambda g, \lambda M)$ coincide. At the infinite component $G_\infty$, the terms are $g$ and $\lambda g$, respectively. Let $\mathfrak{p}$ be any finite place, and $g_{M,\mathfrak{p}}$ the component of the image of $(g, M)$ at $\mathfrak{p}$. Then $\lambda g_{M,\mathfrak{p}}$ has to satisfy $\lambda g_{M,\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}^m = \lambda M \otimes_{\mathcal{O}_k} \mathcal{O}_{\mathfrak{p}}$, which clearly holds.

So far we have shown that the map is well-defined. For the remaining assertions we refer to the sources above. □

## 3.2 Geometry on the space of module lattices

In this subsection, we will give a more precise description of the geometric structure of the space of lattices. It turns out that the space is disconnected with connected components naturally identified with the class group of $k$. As in Proposition 2.2.7 we identify $\mathrm{Cl}_k = \mathbb{G}_m(k)\backslash\mathbb{G}_m(\mathbb{A}_{k,f})/U_f$.

**Lemma 3.2.1.** *The determinant* $\det\colon G(\mathbb{A}_{k,f}) \to \mathbb{G}_m(\mathbb{A}_{k,f})$ *induces a surjective map*

$$G(k)\backslash G(\mathbb{A}_{k,f})/K_f \twoheadrightarrow \mathrm{Cl}_k.$$

*Proof.* First note that the map is well-defined as the determinant maps $G(k)$ and $K_f$ to $\mathbb{G}_m(k)$ and $U_f$, respectively. The surjectivity is inherited from the surjectivity on $G(\mathbb{A}_{k,f})$. □

Forgetting the infinite component extends the determinant to a surjective map

$$G(k)\backslash G(\mathbb{A}_k)/K_f \twoheadrightarrow G(k)\backslash G(\mathbb{A}_{k,f})/K_f \twoheadrightarrow \mathrm{Cl}_k.$$

The connected components of $G(k)\backslash G(\mathbb{A}_k)/K_f$ are the fibers of this map, see Proposition 3.2.2 below.

We define $G_\infty^+$ to be the connected component of the identity of $G_\infty$. It consists of all elements $g = (g_\sigma)_{\sigma|\infty}$ with $\det(g_\sigma) > 0$ for all real places $\sigma$. Further, set $G(k)_+ = G(k) \cap G_\infty^+$.

**Proposition 3.2.2.** *Let* $\mathcal{C} \subseteq G(\mathbb{A}_{k,f})$ *be a full set of representatives of* $\mathrm{Cl}_k$. *Let* $\Gamma_g = gK_fg^{-1} \cap G(k)_+$ *for* $g \in \mathcal{C}$. *Then there is an isomorphism (homeomorphism)*

$$G(k)\backslash G(\mathbb{A}_k)/K_f \simeq \coprod_{g\in\mathcal{C}} \Gamma_g\backslash G_\infty^+.$$

*Sketch of the proof.* Define the map

$$\Gamma_g\backslash G_\infty^+ \to G(k)\backslash G(\mathbb{A}_k)/K_f;\ \ [x] \mapsto [g, x]$$

with image in the subspace of those elements in $G(k)\backslash G(\mathbb{A}_k)/K_f$ whose ideal class is the same as the class of $g$. That this is well-defined and injective is easy. The disjoint union of the $\Gamma_g\backslash G_\infty^+$ taken over $\mathcal{C}$ surjects onto the right hand side, so that we have the desired bijection. We refer to [Mil05] for further details, including the topological assertion, specifically, Lemma 5.13 and the references therein. □

For any $g \in \mathcal{C}$, the subgroup $\Gamma_g$ of $G_\infty^+$ is discrete. The quotient $\Gamma_g \backslash G_\infty^+$ admits a structure of a smooth manifold.

**Norm 1 group.** The space of lattices comes with a $G(\mathbb{A}_k)$-invariant measure induced from the Haar measure on $G(\mathbb{A}_k)$. Unfortunately, the invariant measure is not finite. We will describe an analogue of the norm 1 subgroup in the 1-dimensional case. In general, this will have a finite volume, but be non-compact for $m > 1$.

Consider $\Delta \colon \mathbb{R}_{>0} \to G_\infty$ given by

$$x \mapsto (\mathrm{diag}(x^{\frac{1}{mn}}))_\sigma.$$

Recall that $G = \mathrm{GL}_m$ and $n$ is the degree of extension of $k$ over $\mathbb{Q}$. By $\mathrm{diag}(z)$ we mean the scalar matrix associated with an element $z \in \mathbb{R}$. We stress that $\Delta(x)$ is constant at all infinite places. By definition, $\det(\Delta(x)) = (x^{\frac{1}{n}})_\sigma \in k_\infty^\times$. Hence, its norm is $|\det(\Delta(x))|_\infty = x$. Let $Z^1 \coloneqq Z_m^1 \coloneqq \mathrm{im}(\Delta)$.

**Proposition 3.2.3.** *There is a finite $G(\mathbb{A}_k)$-invariant measure on $G(k)Z^1\backslash G(\mathbb{A}_k)$, which induces a finite $G(\mathbb{A}_k)$-invariant measure on $G(k)Z^1\backslash G(\mathbb{A}_k)/K_f$. Further, there is a canonical identification*

$$G(k)Z^1\backslash G(\mathbb{A}_k)/K_f \simeq \coprod_{g\in\mathcal{C}} \Gamma_g Z^1 \backslash G_\infty^+.$$

*Proof.* The identification is an immediate consequence of Proposition 3.2.2 by noting that $Z^1$ acts equivariantly. The existence of such an invariant measure is a classical theorem in measure theory. Its finiteness is shown in [Bor63]. See also [Gar18] for the case $m = 2$. □

Invariant measures are only unique up to scaling, but we will always work implicitly with the normalized measure, i.e., the unique invariant measure such that the measure of $G(k)Z^1\backslash G(\mathbb{A}_k)/K_f$ is 1. In [Boe+20], the measure is chosen to be the induced measure from the Lebesgue measure on the real space, which explains the additional factor $\mathrm{vol}(\mathrm{Pic})^{-1}$ there.

The space $G(k)Z^1\backslash G(\mathbb{A}_k)/K_f$ can be identified with a subspace of $G(k)\backslash G(\mathbb{A}_k)/K_f$, which we want to describe now. Define $G(\mathbb{A}_k)^1$ to be the subgroup of $g$ such that the adèlic norm

$$|g| \coloneqq |\det(g)| = \prod_\nu |\det(g_\nu)|_\nu$$

is 1. By the Product Formula 2.1.7, $G(k) \subseteq G(\mathbb{A}_k)^1$. Further, it is easy to see that $K_f \subseteq G(\mathbb{A}_k)^1$.

**Lemma 3.2.4.** *The composition*

$$G(k)\backslash G(\mathbb{A}_k)^1/K_f \hookrightarrow G(k)\backslash G(\mathbb{A}_k)/K_f \twoheadrightarrow G(k)Z^1\backslash G(\mathbb{A}_k)/K_f$$

*is a bijection.*

*Proof.* Suppose $g, h \in G(\mathbb{A}_k)^1$, define the same class in $G(k)Z^1\backslash G(\mathbb{A}_k)/K_f$. Then there exist $x \in \mathbb{R}_{>0}$, $\gamma \in G(k)$ and $\xi \in K_f$, such that $g = \Delta(x)\gamma h \xi$. Noting that $|g|, |h|, |\gamma|, |\xi| = 1$, it must necessarily hold that $\Delta(x)$ has norm 1, and hence $x = 1$. Thus we have injectivity.

Let $g \in G(\mathbb{A}_k)$ be arbitrary. Then $|\Delta(x)g| = |\Delta(x)|_\infty |g|$. For $x \coloneqq |g|^{-1}$ it holds that $|\Delta(x)|_\infty = |g|^{-1}$, so that $\Delta(x)g \in G(\mathbb{A}_k)^1$ whose class in $G(k)Z^1\backslash G(\mathbb{A}_k)/K_f$ coincides with the class of $g$. □

On the level of module lattices the Propositions 3.2.2 and 3.2.3 yield the following.

**Corollary 3.2.5.** *There is a bijection*

$$Z^1\backslash \mathrm{Lat}_m(k) \xrightarrow{\sim} G(k)Z^1\backslash G(\mathbb{A}_k)/K_f \simeq G(k)\backslash G(\mathbb{A}_k)^1/K_f.$$

The lattices in $Z^1\backslash \mathrm{Lat}_m(k)$ will be called *norm 1 module lattices*.

**Determinant of modules.** As in Lemma 3.2.4, we want to describe a subset of $\mathrm{Lat}_m(k)$ that represents the norm 1 elements in $G(k)\backslash G(\mathbb{A}_k)^1/K_f$. First, we need the notion of determinant of $\mathcal{O}_k$-lattices.

Let $M$ be an $\mathcal{O}_k$-lattice of rank $m$. If $M$ is free, then $M = g\mathcal{O}_k^m$ for some $g \in G(k)$ and we define $\det(M)$ to be the fractional ideal of $\mathcal{O}_k$ generated by $\det(g)$. Note that this is independent of the choice of $g$ as any other basis would differ by $\gamma \in \mathrm{GL}_m(\mathcal{O}_k)$, hence the fractional ideal does not change. In general, $M$ will not be free, but for each $\mathfrak{p}$, the localization $M_\mathfrak{p}$ is a free $\mathcal{O}_{k,\mathfrak{p}}$-module. Thus we can associate with each $\mathfrak{p}$ the multiplicity $\nu_\mathfrak{p}(M) \coloneqq \nu_\mathfrak{p}(\det(g_\mathfrak{p}))$ where $g_\mathfrak{p}\mathcal{O}_{k,\mathfrak{p}}^m = M_\mathfrak{p}$. Then we set $\det(M) \coloneqq \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(M)}$. If $M$ is free, the two definitions coincide. The ideal class defined by $\det(M)$ will be called *determinant class* and if it does not cause confusion, we will denote it again by $\det(M)$. By construction we have the following compatibility result of the two notions of determinants.

**Proposition 3.2.6.** *Let $M$ be an $\mathcal{O}_k$-lattice of rank $m$. Let $(g_\mathfrak{p})_\mathfrak{p}$ be the element in $G(\mathbb{A}_{k,f})/K_f$ associated with $M$. Then, $\nu_\mathfrak{p}(\det(M)) = \nu_\mathfrak{p}(\det(g_\mathfrak{p}))$, as elements in the fractional ideals $\mathrm{I}_k \simeq \mathbb{G}_m(\mathbb{A}_{k,f})/U_f$. In particular, the determinant class of $M$ and the ideal class defined by $(\det(g_\mathfrak{p}))$ coincide.*

Recall from Theorem 3.1.4 that we associate with a pair $(g, M) \in \mathrm{Lat}_m(k)$ the element $(g, (g_\mathfrak{p})_\mathfrak{p}) \in G(k)\backslash G(\mathbb{A}_k)/K_f$. The proposition is then trivial by construction.

**Corollary 3.2.7.** *Under the identification of $\mathrm{Lat}_m(k)$ with $G(k)\backslash G(\mathbb{A}_k)/K_f$, the norm 1 lattices correspond to pairs $(g, M)$ such that $|\det(g)|_\infty |\det(M)|_f = 1$.*

The norm of $\det(g)$ is the product of the norms of its infinite components. Similarly, the norm of $\det(M)$ is the product of all norms at all finite places.

*Proof.* Clearly, if the image of $(g, M)$ can be represented by $x \in G(\mathbb{A}_k)^1$ with $x_\infty = g$ and $x_\mathfrak{p}\mathcal{O}_\mathfrak{p}^m = M \otimes_{\mathcal{O}_k} \mathcal{O}_\mathfrak{p}$, then $1 = |x| = |\det(g)|_\infty |\det(M)|_f$. Conversely, the last equation shows that $(g, M)$ can be represented by $x \in G(\mathbb{A}_k)^1$. □

Let $\mathrm{Lat}_m^1(k)$ denote the subset of module lattices over $k$ which correspond to the norm 1 space. For an arbitrary $\mathcal{O}_k$-lattice $M$, it is easy to see that $g \in G_\infty$ exists such that $|\det(g)|_\infty |\det(M)|_f = 1$, e.g., $g = \Delta(|\det(M)|_f^{-1})$. In this way, $\mathcal{O}_k$-lattices are represented in the space of norm 1 module lattices.

**Concrete description.** Lastly, we want to give a more concrete description of the correspondence between module lattices and the space described above. Up to determining the class group, this gives a rather simple identification that does not use adèles. We recall from $K$-theory the following basic result, as can be found in [Ros94].

**Proposition 3.2.8.** *Any $\mathcal{O}_k$-lattice is up to isomorphism uniquely determined by its rank and determinant class. The association*

$$M \mapsto (\det(M), \mathrm{rk}(M))$$

*from $\mathcal{O}_k$-lattices to $\mathrm{Cl}_k \times \mathbb{Z}$ defines an isomorphism*

$$\mathrm{K}^0(\mathcal{O}_k) \simeq \mathrm{Cl}_k \times \mathbb{Z}.$$

**Corollary 3.2.9.** *Let $M, N$ be $\mathcal{O}_k$-lattices of rank $m$. Then $M \cong N$, if and only if their determinant classes coincide. In this case, there exists $\lambda \in G(k)$ with $\lambda M = N$.*

With this result in hand, we can easily describe the association between the set of module lattices over $k$ of a fixed rank $m$ with the space defined in Proposition 3.2.2. We implicitly use Theorem 3.1.4 to associate with an element of $G(\mathbb{A}_{k,f})$ an $\mathcal{O}_k$-lattice. In applications, we may assume that the representatives of any ideal class $I$ is given by the lattice $I \oplus k^{m-1}$. By Proposition 3.2.8, these cover all possible classes.

**Proposition 3.2.10.** *Let $\mathcal{C} \subseteq G(\mathbb{A}_{k,f})$ be a set of representatives of* $\mathrm{Cl}_k$*. Then any module lattice $(g, M)$ can be written as $(h, \gamma)$, where $\gamma \in \mathcal{C}$ represents the ideal class of* $\det(M)$ *and $h \in \Gamma_\gamma \backslash G_\infty^+$. Conversely, any element $h \in \Gamma_\gamma \backslash G_\infty^+$ with $\gamma \in \mathcal{C}$ can be associated with the module lattice $(h, \gamma)$. Together, these define a bijection*

$$\mathrm{Lat}_m(k) \xrightarrow{\simeq} \coprod_{\gamma \in \mathcal{C}} \Gamma_\gamma \backslash G_\infty^+.$$

*Proof.* First, suppose $\gamma$ represents the determinant class of $M$. Let $N_\gamma$ denote the $\mathcal{O}_k$-lattice of rank $m$ associated with $\gamma$. Then $N_\gamma$ and $M$ are isomorphic by the previous corollary, hence let $\lambda \in G(k)$ with $\lambda M = N_\gamma$. For the module lattices, we have

$$g^{-1}M = g^{-1}\lambda^{-1}\lambda M = (\lambda g)^{-1} N_\gamma.$$

Hence, the pair $(\lambda g, N_\gamma)$ represents the same module lattice as $(g, M)$. Suppose $\mu \in G(k)$ defines another isomorphism $\mu M = N_\gamma$. Then

$$(\mu g, N_\gamma) = (\lambda g, N_\gamma)$$

which implies that $g^{-1}\mu^{-1}N_\gamma = g^{-1}\lambda^{-1}N_\gamma$, or multiplying by $g$ and $\lambda$, that $\lambda\mu^{-1}N_\gamma = N_\gamma$. On adèles, this means that $\lambda\mu^{-1}\gamma \in \gamma K_f$, or $\lambda\mu^{-1} \in \gamma K_f \gamma^{-1}$. Thus $\lambda\mu^{-1} \in G(k) \cap \gamma K_f \gamma^{-1} = \Gamma_\gamma$.

Conversely, given $h \in \Gamma_\gamma \backslash G_\infty^+$ the lattice $(h, N_\gamma)$ does not depend on the class of $h$ modulo $\Gamma_\gamma$ as any element of $\Gamma_\gamma$ preserves $N_\gamma$. □

*Remark* 3.2.11. The determinant of an $\mathcal{O}_k$-lattice can be computed effectively. In fact, in [Coh00], it is shown how to find a basis $(v_1, \ldots, v_m)$ and fractional ideals $I_1, \ldots, I_m$ such that $M = \bigoplus_i v_i I_i$. Then the determinant class of $M$ is just $\prod_i I_i$. Assuming the generalized Riemann hypothesis, there is a polynomial time quantum algorithm for computing the class group of a given number field, see [BS16].

## 3.3 Module lattices up to isometry

Often, questions about lattices are independent of its isometry class. For example, the minimal length of nonzero vectors coincide in $\Lambda$ and $g\Lambda$, when $g$ is an isometry. In our present case, the notion of isometry is most useful, when adopted to the particular structure of the Euclidean space in question. This is done in terms of maximal compact subgroups.

For $\sigma \mid \infty$, let $K_\sigma \subseteq G(k_\sigma)$ be a maximal compact subgroup. These are not unique, but any two are conjugate, hence isomorphic. Up to isomorphism, $K_\sigma$ is $\mathrm{O}_m(\mathbb{R})$ if $\sigma$ is real, and $\mathrm{U}(m)$ if $\sigma$ is complex. Recall here, that $\mathrm{O}_m(\mathbb{R})$ are the linear transformations which preserve the standard inner product of $\mathbb{R}^m$, while $U(m)$ are the $\mathbb{C}$-linear transformations that preserve the standard Hermitian inner product (sesqui-linear form) on $\mathbb{C}^m$. We define $K_\infty \coloneqq \prod_\sigma K_\sigma$. Then $K_\infty$ itself is a maximal compact subgroup of $G_\infty$.

**Definition 3.3.1.** Let $\Lambda, \Lambda' \in \mathrm{Lat}_m(k)$ be two module lattices over $k$ of rank $m$. Then $\Lambda$ and $\Lambda'$ are *isometric*, if there exists $x \in K_\infty$ with $\Lambda = x\Lambda'$. The isometry classes of module lattices over $k$ of rank $m$ is denoted $\mathrm{IsomLat}_m(k)$.

Let $K \coloneqq K_f K_\infty$. The following is an immediate consequence of Theorem 3.1.4.

**Corollary 3.3.2.** *There is a bijection*

$$\mathrm{IsomLat}_m(k) \xrightarrow{\sim} G(k) \backslash G(\mathbb{A}_k) / K.$$

Further, Proposition 3.2.2 yields the following.

**Corollary 3.3.3.** *There is bijection*

$$\mathrm{IsomLat}_m(k) \xrightarrow{\sim} \coprod_{g \in \mathcal{C}} \Gamma_g \backslash G_\infty^+ / K_\infty^+,$$

*where $K_\infty^+$ is the connected component of the identity of $K_\infty$.*

It is easy to see that as a subgroup of $G(\mathbb{A}_k)$, $K_\infty$ lies in $G(\mathbb{A}_k)^1$. In fact, the norm of the determinant of any element in $K_\sigma$ is 1, and so is their product. Similarly, if $(g, M)$ is a norm 1 lattice then so is $(gk, M)$ for $k \in K_\infty$. Note that the associated lattice $g^{-1}M$ is changed by $k^{-1} \in K_\infty$. Hence, we can deduce the following.

**Corollary 3.3.4.** *There is a bijection*

$$\mathrm{IsomLat}_m^1(k) \xrightarrow{\sim} G(k) \backslash G(\mathbb{A}_k)^1 / K.$$

In this section, the reason to use adèles has not yet become apparent. In fact, the geometric description of isometry classes of module lattices can be done in terms of Arakelov theory as sketched in the next remark. The adèlic viewpoint will be used in the next sections, when we define and analyze certain spaces of functions on the space of lattices.

*Remark* 3.3.5. Another approach to module lattices can be adopted in terms of basic Arakelov theory or metrized $\mathcal{O}_k$-modules, as in [Neu99]. Briefly, the action of $G_\infty$ on $\mathcal{O}_k$-lattices is replaced. Instead, on $M$ one attaches a Hermitian structure on each $M_\sigma := M \otimes_{\mathcal{O}_k, \sigma} \mathbb{C}$, where $\mathbb{C}$ is a $\mathcal{O}_k$-module via the infinite place $\sigma$. Such a Hermitian structure is defined in terms of a Hermitian matrix $H_\sigma \in G(k_\sigma)$. In our presentation, the Hermitian structure can be recovered by pulling back the canonical Hermitian structure along $g_\sigma$, for a pair $(g, M)$. This amounts to the same as defining the new Hermitian structure to be $g_\sigma^* g_\sigma$, where * is complex conjugation and transpose. The converse holds only partially for lattices up to isometry. Up to $K_\sigma$, $g_\sigma$ can be recovered from a Hermitian form. This gives another, familiar interpretation of lattices. Instead of changing the lattice, we change the geometry of the real space it generates.

# 4 Automorphic Forms and Representation Theory

In this section, we introduce the notion of automorphic forms and cuspidal automorphic forms for $\mathrm{GL}_m$ with focus on $\mathrm{GL}_2$. In a narrow sense, automorphic forms define a class of functions on the space of module lattices, which can be analyzed in terms of the group structure of $\mathrm{GL}_m$. They have nice properties, satisfying many differential equations and being square-integrable, which makes them a good source of potential worst-case distributions. This fact is the main motivation to consider automorphic forms in the context of lattice-based cryptography.

This section is a recollection of the theory of automorphic forms, which is included for making this article accessible to non-experts. Unless it makes definitions much easier, we will not restrict to $m = 2$, and in fact, many results have analogues for $\mathrm{GL}_m$ replaced by any reductive algebraic group. This is partly our motivation for introducing further classes of structured lattices in Section 6. In this section, we begin with introducing the notion of automorphic forms and cuspidal automorphic forms, and state first decomposition results. Both admit the structure of a module over a large algebra, the so-called Hecke algebra. We introduce the Hecke algebra by looking separately into the case of Archimedean and non-Archimedean places. Using the Hecke algebra, the space of cuspidal automorphic forms is treated as a representation theoretic object. As such, cuspidal automorphic forms decompose into irreducible components. A specific class of cuspidal automorphic forms of spherical cuspidal representations will be particularly interesting. Our main sources are [BH06; Bum97; CKM04; Gar18].

## 4.1 Automorphic forms

As before, let $G$ denote the group $\mathrm{GL}_m$ over $k$, where we do not yet specify $m$. The groups $G_\infty$ and $K_\infty$ as well as their components $G_\sigma$ and $K_\sigma$ are defined as in the previous section. Similarly, $K_f$ is a maximal compact open subgroup of $G(\mathbb{A}_{k,f})$ and $K_\mathfrak{p}$ its components for $\mathfrak{p} \nmid \infty$. We will write $K = K_f K_\infty$ as before.

Recall that $G_\infty$ is a Lie group. The group $G(\mathbb{A}_{k,f})$ is a totally disconnected topological group and the notion of smooth function on $G(\mathbb{A}_{k,f})$ in the classical sense does not behave well. This is resolved by requesting functions to be locally constant. More precisely, we define the following as in [BJ79, Section 4.1].

**Definition 4.1.1.** A function $\varphi\colon G(\mathbb{A}_k) \to \mathbb{C}$ is *smooth*, if it is smooth in the $G_\infty$-component, when the $G(\mathbb{A}_{k,f})$-component is fixed, and locally constant in the $G(\mathbb{A}_{k,f})$-component, when the $G_\infty$-component is fixed.

The set of smooth $\mathbb{C}$-valued functions on $G(\mathbb{A}_k)$ will be denoted as usual as $C^\infty(G(\mathbb{A}_k), \mathbb{C})$ or just $C^\infty(G(\mathbb{A}_k))$.

Before we can define automorphic forms, we need further notation. The Lie algebra of $G_\infty$ will be denoted $\mathfrak{g}_\infty$. It splits into components corresponding to the infinite places as $\mathfrak{g}_\infty = \prod_{\sigma|\infty} \mathfrak{g}_\sigma$. The Lie algebra $\mathfrak{g}_\infty$ acts on smooth functions $C^\infty(G(\mathbb{A}_k))$ as right-invariant differential operators. This action extends to an action of the universal enveloping algebra $\mathcal{U}(\mathfrak{g}_\infty)$ of $\mathfrak{g}_\infty$, which then restricts to its center $\mathcal{Z}_\infty$. There is an abundance of good sources for these notions, for example [Kna02].

**Definition 4.1.2.** A *$K$-finite automorphic form* is a smooth function $\varphi\colon G(\mathbb{A}_k) \to \mathbb{C}$, such that

1. if $\gamma \in G(k)$, $g \in G(\mathbb{A}_k)$ then $\varphi(\gamma g) = \varphi(g)$,
2. $\langle \varphi(gk) \mid k \in K \rangle$ is finite dimensional,
3. there exists an ideal $\vartheta \subseteq \mathcal{Z}_\infty$ of cofinite dimension, such that $X.\varphi = 0$ for all $X \in \vartheta$,
4. for any norm $|\_|$ on $G(\mathbb{A}_k)$, there exist $r, C > 0$ such that for all $g \in G(\mathbb{A}_k)$,

$$|\varphi(g)| \leqslant C|g|^r.$$

The space of $K$-finite automorphic forms will be denoted $\mathcal{A}(G)$. We briefly explain the conditions.

*Remark* 4.1.3. The first condition is called *automorphy*. The second is $K$-finiteness, which is the source for the name of this type of automorphic forms. It entails that the action of $K$ by right-translation stays in a finite dimensional subspace, which is desirable from representation theoretic viewpoint. The representation defined by $K$-finite automorphic form defines will be *admissible*, as we will explain below. See also the next remark for a connection to module lattices. By condition 3 an automorphic form satisfies many differential equations. This makes automorphic forms *highly symmetric* functions and motivates why we look into automorphic forms from application perspective, see Section 5.1. The last condition is called *moderate growth* and ensures that automorphic forms with central character will be square-integrable modulo center, as will be explained below.

*Remark* 4.1.4. A special form of $K$-finiteness is $K$-invariance, i.e., $\varphi$ satisfies $\varphi(gk) = \varphi(g)$ for all $g \in G(\mathbb{A}_k)$, $k \in K$. A $K$-invariant automorphic form in particular defines a smooth map

$$\varphi\colon G(k)\backslash G(\mathbb{A}_k)/K \to \mathbb{C},$$

i.e., a smooth function on the space of isometry classes of module lattices over $k$. Similarly, $K_f$-invariant automorphic forms define functions on the space of module lattices over $k$.

Let $\chi$ denote a character of $\mathbb{G}_m(\mathbb{A}_k)$, by which we mean a continuous group homomorphism $\mathbb{G}_m(\mathbb{A}_k) \to S^1 \subseteq \mathbb{C}^\times$. Note that $\mathbb{G}_m(\mathbb{A}_k) = Z(G) \coloneqq Z(G(\mathbb{A}_k))$ as scalar matrices. A $K$-finite automorphic form $\varphi$ has *central character* $\chi$, if

$$\varphi(zg) = \chi(z)\varphi(g) \tag{4.1}$$

whenever $z \in Z(G) = Z(G(\mathbb{A}_k))$. We will write $\mathcal{A}(G, \chi)$ for the space of $K$-finite automorphic forms with central character $\chi$. More generally, any measurable function on $G(\mathbb{A}_k)$ has central character $\chi$, if Equation (4.1) holds. As $|\chi(z)| = 1$ for any $z$, the following is well-defined.

**Definition 4.1.5.** An $\mathrm{L}^2$-*automorphic form* with central character $\chi$ is a measurable function $\varphi\colon G(\mathbb{A}_k) \to \mathbb{C}$ which is left $G(k)$-invariant, has central character $\chi$, and

$$\int_{Z(G)G(k)\backslash G(\mathbb{A}_k)} |\varphi(g)|^2 dg < \infty.$$

The space of $\mathrm{L}^2$-automorphic forms with central character $\chi$ is denoted $\mathrm{L}^2(G(k)\backslash G(\mathbb{A}_k), \chi)$ or just $\mathrm{L}^2(\chi)$. We can also restrict to functions that are invariant under $Z^1$ as in Proposition 3.2.3. These are square-integrable functions $\mathrm{L}^2(Z^1G(k)\backslash G(\mathbb{A}_k))$. As $Z^1G(k)\backslash G(\mathbb{A}_k)$ has finite volume by Proposition 3.2.3 again, the condition on a function of this space to be square-integrable is rather mild.

**Proposition 4.1.6.** *There is a decomposition*

$$\mathrm{L}^2(Z^1G(k)\backslash G(\mathbb{A}_k)) = \widehat{\bigoplus_{\chi}} \mathrm{L}^2(\chi)$$

*where the sum runs over characters of $\mathbb{G}_m(\mathbb{A}_k)$ that are trivial on the ray $(x, \dots, x) \in k_\infty^\times$, for $x \in \mathbb{R}_{>0}$. The decomposition is orthogonal with respect to the $\mathrm{L}^2$ inner product.*

We refer to [Gar18, Section 2.5] for a proof. Later, we will see further decompositions for the space of cusp forms.

**Cusp forms.** From now on, we restrict to the case $m = 2$, although, many definitions and results require only small changes. A $K$-finite automorphic form $\varphi$ is a cusp form, if for all $g \in G(\mathbb{A}_k)$

$$\int_{k \setminus \mathbb{A}_k} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) dx = 0. \tag{4.2}$$

The integral is always defined as by Theorem 2.2.2, $k \setminus \mathbb{A}_k$ is compact. The space of $K$-finite cusp forms is denoted $\mathcal{A}_0(G)$. For a fixed central character $\chi$, $\mathcal{A}_0(G, \chi)$ or simply $\mathcal{A}_0(\chi)$ denotes the cusp forms, which have $\chi$ as their central character. There is a geometric reasoning for this definition, which we recall briefly from the classic theory of modular forms.

*Remark* 4.1.7. Let $\mathfrak{h}$ denote the upper half space in the complex plane. For an arithmetic subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, the modular space $\Gamma\backslash\mathfrak{h}$ is a (in general) non-compact hyperbolic manifold. In the non-compact case, it admits a canonical compactification which is a Riemann surface. The points that need to be added are finite and discrete, so-called cusps. A modular form in classical sense is assumed to be holomorphic at the cusps, which is a condition on the Fourier series expansion about each cusp, namely, that it has only nonnegative terms. A cusp form is moreover assumed to *vanish at the cusps*, i.e., that the constant term is 0. There is a by-now classic translation of the theory of modular forms to the adèlic perspective, in which cusps are described in terms of subgroups of $\mathrm{GL}_2(\mathbb{A}_k)$ of the form

$$\left\{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right\}.$$

The above condition entails that *the Fourier coefficient vanishes*. The analogy to Fourier coefficients is inherent in Whittaker models, see [CKM04]. For the relationship between the classic and adèlic approaches is treated in [CKM04; Kud03].

The definition of $L^2$-cusp forms goes similar in fashion. An $L^2$-automorphic form $\varphi$ is a cusp form, if Equation (4.2) holds for almost all $g \in G(\mathbb{A}_k)$. The space of $L^2$-cusp forms with central character $\chi$ will be denoted $L_0^2(\chi)$. It holds that

$$\mathcal{A}_0(\chi) \subseteq L_0^2(\chi).$$

In fact, $\mathcal{A}_0(\chi)$ is the space of $K$-finite and smooth vectors in $L_0^2(\chi)$, see [CKM04]. In Remark 4.2.2 we will briefly explain $K$-finite and smooth vectors.

The space of automorphic forms or cusp forms can be analyzed in terms of representation theory. In the next section, we will introduce the Hecke algebras, which are the basic tool for analyzing the space of automorphic forms and cusp forms. In particular, they contain the Hecke operators which will be part of our criterion for a worst-case to average-case convergence.

## 4.2 Representation Theory

We introduce some backgrounds in representation theory of $G(\mathbb{A}_k)$. As the group $G(\mathbb{A}_k)$ decomposes into pieces $G_\nu$ for the places $\nu$ of $k$, up to basic restrictions, the theory of modules over $G(\mathbb{A}_k)$ of can be studied in terms of these $G_\nu$. We consider separately the case of Archimedean and non-Archimedean places, with a stronger focus on the non-Archimedean places, as they are the source of the Hecke operators we are interested in. We begin with a brief overview of the Archimedean case.

**Archimedean Case.** Let $\nu$ be an Archimedean place. For convenience, let $G = G_\nu$ for this paragraph and similarly, $K = K_\nu$ the maximal compact subgroup, and $\mathfrak{g} = \mathfrak{g}_\nu$ the Lie algebra. The Lie algebra of $K$ is denoted $\mathfrak{k}$ and is a subalgebra of $\mathfrak{g}$.

As $G$ is non-compact and non-commutative, the analysis of $G$-modules is more involved than e.g. for compact abelian groups. Therefore, we introduce the notion of $(\mathfrak{g}, K)$-modules, which encapture the interesting representations of $G$ for the purpose of automorphic forms. There is another approach using left and right $K$-invariant distributions on $G$ with support in $K$, which is equivalent to the notion of $(\mathfrak{g}, K)$-modules. For that approach, see [CKM04; Gel75; JL70].

**Definition 4.2.1.** A $(\mathfrak{g}, K)$-module is a complex vector space $V$, together with a Lie algebra representation $\mathfrak{g} \to \mathrm{End}(V)$ and an action $K \to \mathrm{GL}(V)$, such that

- $V$ decomposes into finite dimensional $K$-invariant subspaces,
- for any $Y \in \mathfrak{k}$, $v \in V$
$$\frac{d}{dt} \exp(tY)|_{t=0} .v = Y.v$$
- for any $k \in K$, $X \in \mathfrak{g}$, and $v \in V$,
$$k.(X.(k^{-1}.v)) = (\mathrm{ad}_k X).v.$$

In the definition, we write $X.v$ for the endomorphism associated with $X \in \mathfrak{g}$ applied to $v$, and similarly for $k.v$ for $k \in K$. The first condition makes $(\mathfrak{g}, K)$-modules technically simple. The second and third conditions are compatibility assumptions on the actions of $\mathfrak{g}$ and $K$. The exponential map for Lie algebras is a mapping from the Lie algebra of a group to the Lie group itself. The second condition says that the Lie algebra action is an extension of the Lie group action. The adjoint ad is a representation of $G$ on its Lie algebra. For $\mathrm{GL}_m$, the action is given by conjugation which is the reason for the last condition.

*Remark* 4.2.2. Let $V$ be a Hilbert space on which $G$ acts continuously. Then there exists a subspace $V^\infty$ of $V$, on which $G$ acts smoothly and which is dense in $V$. The elements are called smooth vectors and are defined by the condition that

$$\frac{d}{dt} \exp(tX)|_{t=0} .v$$

is defined for all $X \in \mathfrak{g}$. By definition, the $G$-action induces a $\mathfrak{g}$-action on $V^\infty$. Further, the subspace of $K$-finite vectors $V^K$ consisting of all $v \in V$ such that $K.v$ spans a finite dimensional subspace. It can be shown that $K$-finite vectors are smooth and $V^K$ is dense in $V$. Moreover, the action of $\mathfrak{g}$ preserves $K$-finiteness, and in fact, the two actions of $\mathfrak{g}$ and $K$ are compatible in the sense of Definition 4.2.1. Thus, to any continuous $G$-representation on a Hilbert space, we can naturally associate a $(\mathfrak{g}, K)$-module.

**Definition 4.2.3.** A $(\mathfrak{g}, K)$-module $V$ is *admissible*, if every $K$-isotypic component is finite dimensional.

Let us recall the notion of $K$-isotypic component. Let $\sigma$ be an irreducible finite dimensional representation of $K$. Then the $K$-isotypic component $V_\sigma$ of $V$ associated with $\sigma$ is the union of all irreducible submodules of $V$ isomorphic to $\sigma$. Admissibility is another condition that makes $(\mathfrak{g}, K)$-modules well-defined.

**Non-Archimedean Case.** Now, let $\nu$ be a non-Archimedean place. Let us again set $G = G_\nu$ and $K = K_\nu$ as a maximal compact open subgroup. In contrast to the Archimedean case, here we can work with $G$-representations. The notion of smoothness is the abstract counterpart of smooth functions as in Definition 4.1.1.

**Definition 4.2.4.** A $G$-module $V$ is *smooth*, if for every $v \in V$ there exists a compact open subgroup $U$ of $G$ such that $x.v = v$ for all $x \in U$.

For a compact open subgroup $U$ of $G$, let $V^U$ denote the $U$-fixed vectors of $V$. Then the smoothness of $V$ amounts to saying that $V = \bigcup_U V^U$, where the union is taken over all compact open subgroups. Similar to Remark 4.2.2, we can associate a smooth representation to an arbitrary representation $V$, by setting $V^\infty = \bigcup_U V^U$. Note that the $G$-action preserves invariance under some compact open subgroup. In fact, if $v$ is fixed by $U$, then $gv$ is fixed by $gUg^{-1}$. Hence, $V^\infty$ is indeed a smooth $G$-module.

For any isomorphism class $\rho$ of irreducible finite dimensional representations of $K$, let $V^\rho$ denote the $\rho$-isotypic component of $V$. We write $\widehat{K}$ for isomorphism classes of finite dimensional irreducible $K$-modules. The next theorem shows that smooth representations can be analyzed in terms of representations of $K$. A proof can be found in [BH06, Proposition 2.3].

**Theorem 4.2.5.** *Let $V$ be a smooth $G$-module. Then $V = \bigoplus_{\rho \in \widehat{K}} V^\rho$.*

Schur's Lemma holds in the context of smooth representations so that we have the following consequence.

**Corollary 4.2.6.** *Let $V$ be an irreducible smooth representation of $G$. Let $Z$ denote the center of $G$. Then there exists a character $\chi\colon Z \to \mathbb{C}^\times$ such that $z.v = \chi(z).v$ for all $z \in Z$.*

We refer to [BH06, 2.6 Corollary 1] for a proof. See also [Bum97, Proposition 4.2.4] and the discussion thereafter. Again, we have a notion of admissibility, as follows.

**Definition 4.2.7.** A smooth representation $V$ of $G$ is *admissible*, if for every compact open subgroup $U$ of $G$, the space of $U$-fixed vectors $V^U$ is finite dimensional.

As in representation theory of finite groups, there is a $\mathbb{C}$-algebra $\mathcal{H}(G)$ such that there is a natural correspondence between $G$-representations and $\mathcal{H}(G)$-modules. For finite groups, this algebra is the group algebra. In the present case, we introduce the Hecke algebra as follows.

The group $G$ admits a left-invariant Haar measure $\mu_G$, which we normalize by the condition $\mu_G(K) = 1$. Let $\mathcal{H}(G) \coloneqq C_c^\infty(G; \mathbb{C})$ denote the $\mathbb{C}$-algebra of locally constant functions with compact support, where multiplication given by convolution

$$\varphi \star \psi(x) = \int_G \varphi(y)\psi(y^{-1}x) d\mu_G(y),$$

for $\varphi, \psi \in \mathcal{H}(G)$. Unless $G$ is compact, $\mathcal{H}(G)$ does not have a unit. Intuitively, a unit would require to have support all over $G$, which cannot exist in the set of compactly supported functions if $G$ is non-compact. However, $\mathcal{H}(G)$ has many idempotents, i.e., elements $\xi$ with $\xi \star \xi = \xi$. In fact, suppose $U$ is any compact open subset, and $\chi_U$ is the characteristic function associated with $U$. That is, $\chi_U$ takes the value 1 on $U$ and 0 anywhere else. Then $\xi_U := \frac{1}{\mu_G(U)}\chi_U$ can be easily computed to be idempotent. Idempotents of this form are called *fundamental idempotents*.

Let $M$ be a $\mathcal{H}(G)$ module. Then we will write $\varphi \star m$ for the action of $\varphi \in \mathcal{H}(G)$ on $m \in M$, as in [BH06]. A $\mathcal{H}(G)$-module is smooth, if for every $m \in M$ there exists $\varphi \in \mathcal{H}(G)$ such that $\varphi \star m = m$.

**Theorem 4.2.8.** *There is a natural correspondence between $G$-modules and $\mathcal{H}(G)$-modules. A $G$-module is smooth, if and only if the corresponding $\mathcal{H}(G)$-module is smooth.*

Again, we refer to [BH06] for a proof. We finish with a final definition of modules which have $K$-invariant elements. These will form the collection of automorphic forms that define functions on the space of lattices.

**Definition 4.2.9.** Let $M$ be an irreducible $\mathcal{H}(G)$-module. A *spherical vector* is an element $m \in M$ such that $\xi_K \star m = \lambda m$ for $\lambda \in \mathbb{C}^\times$. An irreducible representation is *spherical*, if it contains a spherical vector.

For $G = \mathrm{GL}_2$ spherical vectors, if exist, are unique up to scaling, cf. Appendix B.1.

## 4.3 Automorphic Representations

In this section we use the tools introduced in the previous subsection to analyze the space of automorphic forms. The case of $\mathrm{L}^2$-automorphic forms is easier, as $G(\mathbb{A}_k)$ acts on this space via right translation, for any fixed central character. The same is not true for $K$-finite automorphic forms, as $K$-finiteness is not preserved by right-translation. The problem occurs only at the infinite places, where $K_\infty$-finiteness is not necessarily preserved. Therefore, one substitutes the right-translation action by $G_\infty$ with a $(\mathfrak{g}_\infty, K_\infty)$-module structure, as defined in Section 4.2. The necessity of the Hecke algebras at finite places comes from the operators we define from elements in the Hecke algebra. The results stated here can be found in [CKM04, Lecture 3] and the references there.

**Archimedean Hecke algebra.** The space of $K$-finite automorphic forms carries the structure of a $\mathfrak{g}_\infty$-module via differential operators. The $\mathfrak{g}_\infty$-action preserves $\mathcal{Z}$-finiteness, as the operators commute. Moreover, $K_\infty$ acts via right-translation. In contrast to right-translation by $G_\infty$, this preserves $K$-finiteness, by definition. These actions are compatible in the sense of Definition 4.2.1, so that $\mathcal{A}(G)$ becomes a $(\mathfrak{g}_\infty, K_\infty)$-module.

**Theorem 4.3.1.** *Let $\varphi \in \mathcal{A}(G)$. The $(\mathfrak{g}_\infty, K_\infty)$-module generated by $\varphi$ is admissible.*

**Non-Archimedean Hecke algebra.** In the previous section we defined Hecke algebras for each finite place $\mathfrak{p}$, separately. The finite part of the global Hecke algebra is defined as a restricted tensor product of those. The restrictedness is a finiteness condition similar to the condition for adèles. More precisely, we fix $K_\mathfrak{p}$, for each finite place $\mathfrak{p}$, to be the maximal compact open subgroup $\mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$. To $K_\mathfrak{p}$ we associate the fundamental idempotent $\xi_\mathfrak{p} := \xi_{K_\mathfrak{p}}$ as in Section 4.2. The *finite Hecke algebra* $\mathcal{H}_f$ is the restricted tensor product

$$\bigotimes_{\mathfrak{p}}{}' \mathcal{H}_\mathfrak{p},$$

where a tensor belongs to $\mathcal{H}_f$, if at all but finitely many places, the tensor is given by $\xi_\mathfrak{p}$. An $\mathcal{H}_f$-module $M$ is *admissible* if and only if there is a compact open $U_\mathfrak{p}$ for each $\mathfrak{p} \nmid \infty$, almost all $U_\mathfrak{p}$ being $K_\mathfrak{p}$, such that for $\xi := \otimes_\mathfrak{p} \xi_{U_\mathfrak{p}}$, the space $\xi M$ is finite dimensional.

**Example 4.3.2.** A basic construction of admissible $\mathcal{H}_f$-modules is as follows. For each $\mathfrak{p}$ let $V_\mathfrak{p}$ be an admissible $\mathcal{H}_\mathfrak{p}$-module, which is spherical for all but finitely many $\mathfrak{p}$. The restricted tensor product $V := \bigotimes'_\mathfrak{p} V_\mathfrak{p}$ is defined to be the subspace generated by tensors which are spherical in all but finitely many factors. Then $V$ is admissible. Combining Theorem 4.3.3 and Theorem 4.3.5 below, we will see that this construction covers automorphic representations.

The finite Hecke algebra acts on $\mathcal{A}(G)$ and $\mathrm{L}^2(\chi)$ for a fixed central character $\chi$, via convolution

$$R(\xi)\varphi(x) = \int_{G(\mathbb{A}_{k,f})} \varphi(xy)\xi(y)dy.$$

It is easy to see that $\mathcal{H}_f$ preserves $K$-finite automorphic forms.

**Theorem 4.3.3.** *Let $\varphi \in \mathcal{A}(G)$ or $\varphi \in \mathrm{L}^2(\chi)$. Then the $\mathcal{H}_f$-module generated by $\varphi$ is admissible.*

**Global Hecke algebra.** We define $\mathcal{H}$ as a symbol and say that $V$ is an $\mathcal{H}$-module, if it is a $\mathcal{H}_f$-module and a $(\mathfrak{g}_\infty, K_\infty)$-module such that the two actions commute. Any $\mathcal{H}$-module $M$ decomposes into a tensor product of an $\mathcal{H}_f$-module $M_f$ and $(\mathfrak{g}_\infty, K_\infty)$-module $M_\infty$. An $\mathcal{H}$-module $M$ is admissible, if $M_f$ is admissible as an $\mathcal{H}_f$-module, and $M_\infty$ is admissible as a $(\mathfrak{g}_\infty, K_\infty)$-module.

**Definition 4.3.4.** An *automorphic representation* is an $\mathcal{H}$-module $V$ that is isomorphic to an irreducible subquotient of $\mathcal{A}(G)$.

Most importantly for automorphic forms, we have a decomposition result by Flath, [Fla79].

**Theorem 4.3.5.** *Let $(\pi, V)$ be an irreducible admissible $\mathcal{H}$-module. Then there exist irreducible admissible $\mathcal{H}_\mathfrak{p}$-modules $\pi_\mathfrak{p}$ for all $\mathfrak{p} \nmid \infty$ which are spherical for all but finitely many $\mathfrak{p}$, and irreducible admissible $(\mathfrak{g}_\sigma, K_\sigma)$-modules $\pi_\sigma$ for all $\sigma \mid \infty$, such that*

$$\pi = \bigotimes_\nu{}' \pi_\nu$$

*where $\nu$ runs over all places.*

Together with Theorem 4.3.3, we conclude that from a theoretic perspective, the analysis of automorphic representations reduces to the analysis of admissible representations of $G(k_\nu)$ for all places $\nu$ of $k$. In the case of $G = \mathrm{GL}_2$, we give an outline in Appendix B.

There is a further notion of automorphic representations related to $\mathrm{L}^2$-automorphic forms. It has the advantage of being a $G(\mathbb{A}_k)$-module without utilizing the Hecke algebra introduced above.

**Definition 4.3.6.** An $\mathrm{L}^2$-*automorphic representation* is an irreducible submodule of the $G(\mathbb{A}_k)$-module $\mathrm{L}^2(\chi)$, for some central character $\chi$.

**Theorem 4.3.7.** *Let $\pi$ be an $\mathrm{L}^2$-automorphic representation. Then there exist irreducible unitary $G(k_\nu)$-modules $\pi_\nu$ such that $\pi = \widehat{\bigotimes}_\nu{}' \pi_\nu$.*

Here, the restricted tensor product is completed in the sense of tensor products of Hilbert spaces. As we do not need further details, we refer to [GGP90].

**Cuspidal automorphic representations.** It can be easily checked that the action of the Hecke algebra $\mathcal{H}$ on $K$-finite automorphic forms preserve cusp forms and central characters. Thus $\mathcal{A}_0(G)$ is always a submodule of $\mathcal{A}(G)$, and further $\mathcal{A}_0(G, \chi)$ is a submodule of $\mathcal{A}(G, \chi)$, for a central character $\chi$.

**Definition 4.3.8.** A $K$-finite *cuspidal automorphic representation* with central character $\chi$ is an irreducible submodule of $\mathcal{A}_0(G, \chi)$.

We will use the term *cuspidal representation* for a $K$-finite cuspidal automorphic representation for some central character. A main feature is a decomposition result on the space of cusp forms with a fixed central character, which goes as follows.

**Theorem 4.3.9.** *The space $\mathcal{A}_0(G,\chi)$ decomposes into a direct sum of irreducible $\mathcal{H}$-modules $\pi$ as*

$$\mathcal{A}_0(G,\chi) \simeq \bigoplus m_\pi \pi.$$

Here $m_\pi$ are nonnegative integers, the multiplicities of $\pi$. For $G = \mathrm{GL}_m$, one can show that $m_\pi = 1$.

**Theorem 4.3.10.** *Let $\pi$ and $\pi'$ be cuspidal representations with central character $\chi$. Suppose $\pi_\nu \cong \pi'_\nu$ for all but finitely many $\nu$ including all infinite places. Then $\pi = \pi'$ in $\mathrm{L}^2_0(\chi)$. In particular, $m_\pi = 1$.*

This theorem is called the *strong multiplicity one* theorem and is proved in [Cas73; JL70]. Finally, we want to mention that the complement of the cusp forms in $\mathrm{L}^2(\chi)$ can be described explicitly.

*Remark* 4.3.11. The space $\mathrm{L}^2(\chi)$ decomposes into an orthogonal direct sum

$$\mathrm{L}^2_0(\chi) \oplus \mathrm{L}^2_{\mathrm{Eis}}(\chi),$$

see [Gar18]. The term $\mathrm{L}^2_{\mathrm{Eis}}(\chi)$ is the space of Eisenstein series with central character $\chi$. As mentioned earlier, we believe that it is natural to look for worst-case distributions in the space of cusp forms. Still, Eisenstein functions might be worth to be considered in this regard, or more generally, for potential applications of automorphic forms to the cryptographic use of lattices.

# 5 Worst-Case to Average-Case Convergence

In this section, we want to specify our general notion of cuspidal distributions on the space of lattices and define a collection of Hecke operators associated with ideals of $\mathcal{O}_k$. For a chosen finite set $S$ of primes of $\mathcal{O}_k$, we consider the product $H_S$ of these Hecke operators, which is again an element of the finite Hecke algebra of $\mathrm{GL}_2$.

For a choice of a finite set $S$ of primes of $\mathcal{O}_k$, we give a condition on a cuspidal distribution $\rho$ that ensure that the sequence $H_S^n \rho$ converges to the uniform distribution, which is the analogue of the main theorem of [Boe+20], except that we do not specify a worst-case distribution.

## 5.1 Worst-Case Distributions

Let $G = \mathrm{GL}_2$. In Section 3 we have identified the space $\mathrm{IsomLat}_2^1(k)$ of isometry classes of norm 1 module lattices of rank 2 over $k$ with the space

$$G(k)Z^1 \backslash G(\mathbb{A}_k)/K$$

where $K = K_f K_\infty$ as before.

We expect a worst-case distribution to be a square-integrable map

$$\mathrm{IsomLat}_2^1(k) \to \mathbb{C}$$

whose support is concentrated about the identity lattice which corresponds to $1 \in G(\mathbb{A}_k)$. It should satisfy further symmetry properties reflecting the geometry of $\mathrm{IsomLat}_2^1(k)$. More precisely, the space $\mathrm{IsomLat}_2^1(k)$ carries the structure of a hyperbolic manifold, which in particular defines a metric $d$ on the connected component of the identity. Then, one expects that if $d(x,1) = d(y,1)$ for $x, y$ in the identity component, then a worst-case distribution should take the same values on $x$ and $y$.

Here, we define the notion of cuspidal distributions. These are contained in the space of $K$-finite automorphic forms. The above conditions are partially satisfied by definition for $K$-finite automorphic forms, cf. Remark 5.3.3.

**Definition 5.1.1.** A *cuspidal distribution* on the space of isometry classes of norm 1 module lattices of rank 2 over $k$ is defined to be an element of

$$\mathbb{C} \oplus \mathcal{A}_0(G)^K.$$

Here, $\mathbb{C}$ is for constant functions on $\mathrm{IsomLat}_2^1(k)$, which are determined by the single value $\lambda \in \mathbb{C}$, and $\mathcal{A}_0(G)^K$ is the space of $K$-invariant cuspidal automorphic forms. Note that the term cuspidal distribution does *not* mean that the form is a cusp form, but only a cusp form up to a constant.

*Remark* 5.1.2. In [Boe+20], the worst-case distribution has been chosen as a Gaussian on the torus $\mathrm{IsomLat}_1^1(k) = \mathrm{Pic}^1(k)$. This worst-case distribution admits a Fourier decomposition with a constant term, and a series over nontrivial characters. We view cuspidal automorphic forms as the generalization of characters in the rank 1 case, so that in the present case, we define a cuspidal distribution to have a constant term plus a series in cuspidal representations. The restriction to $K$-invariant forms ensures that the distribution is well-defined on the space of isometry classes of norm 1 module lattices, cf. Corollary 3.3.2.

**Proposition 5.1.3.** *Let $\varphi$ be a cuspidal distribution. Then, $\varphi$ can be written as*

$$\lambda + \sum_{\pi} \varphi_\pi$$

*where the sum runs over all spherical cuspidal automorphic representations $\pi$ and $\varphi_\pi$ are spherical vectors of $\pi$, and $\lambda \in \mathbb{C}$.*

*Proof.* By definition $\varphi$ is of the form $\lambda + \varphi_0$, with $\lambda \in \mathbb{C}$, $\varphi_0 \in \mathcal{A}_0(G)^K$. The decomposition $\mathcal{A}_0(G) = \bigoplus_\pi \pi$ in Theorem 4.3.9 yields a decomposition

$$\mathcal{A}_0(G)^K = \bigoplus_{\pi} \varphi_\pi \mathbb{C},$$

where the sum runs over spherical cuspidal representations and $\varphi_\pi$ are spherical vectors. □

*Remark* 5.1.4. The average-case distribution is merely the constant function 1, which corresponds to the normalized invariant measure we introduced earlier.

## 5.2 Hecke Operators

In this section, we introduce specific Hecke operators associated with ideals of $\mathcal{O}_k$ and analyze their action on spherical vectors. We begin with prime ideals first, and extend the definition to arbitrary ideals by using their decomposition.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_k$ and $t_\mathfrak{p}$ a uniformizer of $\mathcal{O}_\mathfrak{p}$. Let $\alpha_\mathfrak{p} \coloneqq \begin{pmatrix} t_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix}$. Then $U_\mathfrak{p} \coloneqq K_\mathfrak{p} \alpha_\mathfrak{p} K_\mathfrak{p}$ is a compact open subset of $G(k_\mathfrak{p})$, so that there is a fundamental idempotent $H_\mathfrak{p}$ associated with $U_\mathfrak{p}$. By the definition of the action of the Hecke algebra, it is clear that $H_\mathfrak{p}$ preserves constant functions. For spherical cusp forms, we have the following.

**Lemma 5.2.1.** *Let $\pi$ be a spherical cuspidal automorphic representation and $\varphi$ a spherical vector in $\pi$. Then $\varphi$ is an eigenvector of $H_\mathfrak{p}$. If $\pi_\mathfrak{p}$ is the factor at $\mathfrak{p}$ (according to Theorem 4.3.5), and the subgroups*

$$\left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \right\} \text{ and } \left\{ \begin{pmatrix} 1 & 0 \\ 0 & y \end{pmatrix} \right\}$$

*act via characters $\chi_1$ and $\chi_2$, then $\chi_1$ and $\chi_2$ are unramified and*

$$H_\mathfrak{p} \varphi = |t_\mathfrak{p}|_\mathfrak{p}^{-1/2} \left( \chi_1(t_\mathfrak{p}) + \chi_2(t_\mathfrak{p}) \right) \varphi.$$

Unramified for characters $\chi_1, \chi_2$ means that they are $U_f$-invariant, hence the values $\chi_1(t_\mathfrak{p})$ and $\chi_2(t_\mathfrak{p})$ are independent of the choice of $t_\mathfrak{p}$. That $\chi_1$ and $\chi_2$ are unramified is a consequence of the classification of admissible $G(k_\mathfrak{p})$-modules, particularly the spherical representations, see Appendix B.1 for an outline and references. The remaining claims can be found in [Bum97, Section 4.6] using an explicit description of the spherical representations.

Let $I$ be a nonzero ideal of $\mathcal{O}_k$ and $I = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$ its prime decomposition. Then we define $H_I \coloneqq \otimes H_\mathfrak{p}^{\nu_\mathfrak{p}}$. Note that $\nu_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$, so that by $H_\mathfrak{p}^0$ we mean the fundamental idempotent associated with the fixed maximal compact open subgroup $K_\mathfrak{p}$. We consider $H_I$ as an element of the global Hecke algebra $\mathcal{H}$, which acts trivially on the infinite component.

### 5.3 Convergence Criterion

Let $\varphi = \lambda + \sum_\pi \varphi_\pi$ be a cuspidal distribution on the space of isometry classes of norm 1 module lattices of rank 2 over $k$. Let $I \subseteq \mathcal{O}_k$ be a nonzero ideal, with prime decomposition as before. Then we have the following convergence criterion.

**Proposition 5.3.1.** *Let*

$$a_N \coloneqq \left( \prod_{\mathfrak{p} \mid I} |t_\mathfrak{p}|_\mathfrak{p}^{-\nu_\mathfrak{p} N/2} (\chi_{\pi,1}(t_\mathfrak{p}) + \chi_{\pi,2}(t_\mathfrak{p}))^{\nu_\mathfrak{p} N} \right)_N$$

*be viewed as a sequence in $\ell^2(\{\pi$ spherical cuspidal automorphic representations$\})$. Then, for $N \to \infty$, $H_I^N \varphi \to \lambda$, if $a_N \to 0$.*

*Proof.* The proposition is a formal consequence of the results mentioned previously. The space of cuspidal automorphic forms decomposes into a Hilbert space direct sum. A sequence in that space converges, if and only if the sequence of coefficients converge, hence the result. □

**Corollary 5.3.2.** *Let $\varphi = 1 + \sum_\pi \varphi_\pi$ be a cuspidal distribution and $a_N$ the $\ell^2$-sequence it induces. If $a_N \to 0$ as $N \to \infty$, then $H_I^N \varphi \to 1$. Hence, the cuspidal distribution converges to the average-case distribution.*

We have not made any concrete qualitative analysis of the cuspidal distributions here and we want make the following remark, which displays the difficulties in potential applications.

*Remark* 5.3.3. In practice, we can define worst-case distributions on the space of module lattices which intuitively satisfy properties that one expects of worst-case distributions. However, even if such worst-case distributions are cuspidal distributions, it is hard to find the decomposition into irreducible cusp forms as in Proposition 5.1.3. In the rank 1 case, this is easier thanks to Fourier analysis, which is not available in the present case. The problem falls into the field of non-abelian harmonic analysis. Conversely, it is possible to construct spherical cuspidal representations which can then be used to define a worst-case distribution which comes in a decomposed form by its construction. However, then it is difficult to make assertions on its quality as a worst-case distribution. We have outlined a construction of cuspidal automorphic representations with spherical vectors in Appendix B.3, and reviewed their potential application in the context of this section in Appendix B.4.

## 6 Lattices with $\mathcal{G}$-structure

In this section, we define a new notion of structured lattices. The structure is given by the choice of an algebraic group over the ring of integers of a number field together with a representation. Intuitively, the algebraic group is the additional structure, while the representation entails how the group acts on lattices. We will give a series of examples to show how lattices previously considered for cryptographic

applications fit into this notion. The motivation to consider this type of structured lattices is that the space of lattices with a fixed structure can be treated analogous to our approach in this article. This works particularly well, if the underlying group satisfies certain conditions.

We do not provide all mathematical details, as they would lead us to far astray. Specifically, we do not go into details on the theory of reductive groups, where the similarity to the case of $\mathrm{GL}_2$ is most apparent.

## 6.1 Affine algebraic groups

We begin with a brief introduction to the notion of affine algebraic groups. There are many sources on algebraic groups. We refer to [Wat79], where the general notion of affine group schemes over general base rings is introduced.

Let $k$ be a number field as before, and $\mathcal{O}_k$ its ring of integers. Until we consider central simple algebras, all algebras are assumed to be commutative with 1. We begin by introducing a few basic notions. An *algebraic group* over $\mathcal{O}_k$ is a rule $\mathcal{G}$ that associates to any $\mathcal{O}_k$-algebra $A$ a group $\mathcal{G}(A)$, and for every morphism $\varphi\colon A \to B$ of $\mathcal{O}_k$-algebras a group homomorphism $\mathcal{G}(\varphi)\colon \mathcal{G}(A) \to \mathcal{G}(B)$, subject to the conditions

- the identity $A \to A$ is associated with the identity $\mathcal{G}(A) \to \mathcal{G}(A)$,
- for two morphisms $\varphi\colon A \to B$ and $\psi\colon B \to C$ the diagram

$$\begin{array}{ccc} \mathcal{G}(A) & \xrightarrow{\quad\mathcal{G}(\psi\circ\varphi)\quad} & \mathcal{G}(C) \\ & {\scriptstyle\mathcal{G}(\varphi)}\searrow \quad \nearrow{\scriptstyle\mathcal{G}(\psi)} & \\ & \mathcal{G}(B) & \end{array}$$

  commutes.

The familiar reader will recognize that this is the functorial definition of an algebraic group. An *affine algebraic group* is an algebraic group $\mathcal{G}$ for which there exists an $\mathcal{O}_k$-algebra $S$ such that for any other $\mathcal{O}_k$-algebra $A$, there is a natural isomorphism

$$\mathcal{G}(A) \simeq \mathrm{Hom}_{\mathcal{O}_k}(S, A).$$

Here, natural isomorphism has a rigorous meaning, namely that the isomorphism is compatible with morphisms $A \to B$ between $\mathcal{O}_k$-algebras. If such an $S$ exists, it is unique up to isomorphism. An affine algebraic group is *of finite type*, if $S$ is an $\mathcal{O}_k$-algebra of finite type, i.e., there exists a surjective morphism

$$\mathcal{O}_k[t_1, \dots, t_m] \twoheadrightarrow S.$$

Of course, $\mathcal{O}_k$ in this definition can be replaced with any commutative unital ring. We give an example to illustrate this notion.

**Example 6.1.1.** The multiplicative group $\mathbb{G}_{m|\mathcal{O}_k}$ is defined by the association $A \mapsto A^\times$, for any $\mathcal{O}_k$-algebra $A$. Here, $A^\times$ is a group with respect to multiplication. The compatibility is easy to check so that $\mathbb{G}_{m|\mathcal{O}_k}$ defines an algebraic group over $\mathcal{O}_k$. For any $\mathcal{O}_k$-algebra $A$, $\mathrm{Hom}_{\mathcal{O}_k}(\mathcal{O}_k[t, t^{-1}], A) \simeq A^\times$. In fact, an $\mathcal{O}_k$-morphism from $\mathcal{O}_k[t, t^{-1}]$ to $A$ is determined uniquely by the image of $t$, which needs to be invertible in $A$. Conversely, for any invertible element $a \in A^\times$, $t \mapsto a$ defines such an $\mathcal{O}_k$-morphism. Thus, $\mathbb{G}_{m|\mathcal{O}_k}$ is an affine algebraic group represented by $\mathcal{O}_k[t, t^{-1}]$. It is of finite type, as $\mathcal{O}_k[x, y] \to \mathcal{O}_k[t, t^{-1}]$, defined by $x \mapsto t$, $y \mapsto t^{-1}$, is surjective. Similarly, one can see that $\mathrm{GL}_{m|\mathcal{O}_k}$ defines an affine algebraic group over $\mathcal{O}_k$ of finite type. It is the group that associates to an $\mathcal{O}_k$-algebra $A$ the group $\mathrm{GL}_m(A)$.

**Fibers of $\mathcal{G}$.** Let $\mathcal{G}$ be an (affine) algebraic group over $\mathcal{O}_k$ (of finite type). Given a $\mathcal{O}_k$-algebra $F$, we can define the *fiber* of $\mathcal{G}$ over $F$ by $G \coloneqq \mathcal{G} \otimes_{\mathcal{O}_k} F$, which is now an algebraic group over $F$ which takes an $F$-algebra $A$ to $\mathcal{G}(A)$. It inherits the notions affine and finite type, i.e., if $\mathcal{G}$ is affine, so is $G$, and similarly for finite type. The fiber over $k$ is called *generic fiber* of $\mathcal{G}$. Unfortunately, the motivation is somewhat hidden in the geometric viewpoint of algebraic groups which we do not explain here.

**Representations.** Let $\mathcal{G}$ be an affine algebraic group of finite type over $\mathcal{O}_k$. A *representation* of $\mathcal{G}$ is a morphism $\pi\colon \mathcal{G} \to \mathrm{GL}_{m|\mathcal{O}_k}$ of algebraic groups. That is, for any $\mathcal{O}_k$-algebra $A$, we get a group homomorphism

$$\pi_A\colon \mathcal{G}(A) \to \mathrm{GL}_m(A),$$

which again is assumed to be compatible in morphisms of $\mathcal{O}_k$-algebras. A representation is *faithful*, if for any $\mathcal{O}_k$-algebra $A$, the corresponding map $\pi_A$ is injective. Note that any single $A$ recovers the more familiar notion of representation, particularly, when $A$ is contained in the complex numbers.

There are trivial examples for representations in the above sense. For $\mathcal{G} = \mathrm{GL}_{m|\mathcal{O}_k}$, the identity representation associates to any $A$, the group homomorphism $\pi_A = \mathrm{id}_A$. If $\mathcal{G}$ is naturally a subgroup of $\mathrm{GL}_{m|\mathcal{O}_k}$, then the inclusion defines a representation.

**Example 6.1.2.** Consider the algebraic group $\mathrm{SL}_{m|\mathcal{O}_k}$ which associates to $A$ the group $\mathrm{SL}_m(A) = \{g \in \mathrm{GL}_m(A) \mid \det(g) = 1\}$. Clearly, for any $A$, $\mathrm{SL}_m(A)$ is a subgroup of $\mathrm{GL}_m(A)$. Thus, the inclusion is a representation.

We want to motivate the necessity of representations, which is also the key insight in the theory of module lattices.

*Remark* 6.1.3. Recall that any two lattices of a fixed rank are isomorphic as abstract groups, hence, in particular, so are their automorphism groups. The notion of module lattices is merely a systematic choice of lattices together with a subgroup of their automorphisms. This becomes apparent in Example 6.2.3 below and with our description in Proposition 3.2.2 of the space of module lattices of rank $m$ as

$$\mathrm{GL}_m(k)\backslash\mathrm{GL}_m(\mathbb{A}_k)/\mathrm{GL}_m(\widehat{\mathcal{O}}_k) \simeq \coprod_{g\in\mathcal{C}} \Gamma_g\backslash\mathrm{GL}_m(k_\infty)^+.$$

If we denote by $\mathcal{L}_x$ the lattice corresponding to $x$ in this space, we see that any $\gamma \in \Gamma_g$ defines an automorphism $\gamma\colon \mathcal{L}_x \to \mathcal{L}_x$. While the algebraic group itself does not provide information how to act on lattices, a choice of representation provides exactly this missing piece of information.

## 6.2 Lattices with $\mathcal{G}$-structure

Motivated by the previous remark we define $\mathcal{G}$-lattices as follows.

**Definition 6.2.1.** Let $\mathcal{G}$ be an affine algebraic group over $\mathcal{O}_k$ of finite type. Further, let $\pi$ be a (faithful) representation of $\mathcal{G}$ in $\mathrm{GL}_{m|\mathcal{O}_k}$. A *lattice with* $(\mathcal{G}, \pi)$-structure is an element of the image of the map

$$\mathcal{G}(k)\backslash\mathcal{G}(\mathbb{A}_k)/\mathcal{G}(\widehat{\mathcal{O}}_k) \xrightarrow{\pi} \mathrm{GL}_m(k)\backslash\mathrm{GL}_m(\mathbb{A}_k)/\mathrm{GL}_m(\widehat{\mathcal{O}}_k).$$

Of course, an element in the image of the above map is viewed as a lattice by means of Proposition 3.2.2. In particular, as in Remark 6.1.3 above, each lattice with $(\mathcal{G}, \pi)$-structure comes with a subgroup of their automorphism group. If $\pi$ is understood from the context, we will say a *lattice with $\mathcal{G}$-structure*. We show how this recovers the notions of lattices considered previously in cryptography.

**Example 6.2.2.** Let $\mathcal{G} \coloneqq \mathrm{GL}_{m|\mathcal{O}_k}$ Let $\pi = \mathrm{id}$ be the identity representation. Then by Proposition 3.2.2, lattices with $(\mathcal{G}, \pi)$-structure are the same as module lattices of rank $m$ over $k$ as in Definition 3.1.2.
For $k = \mathbb{Q}$ this also recovers $\mathbb{Z}$-lattices. In the context of Remark 6.1.3, for $\mathbb{Z}$-lattices, the full group of automorphisms is chosen.

The next example displays how module lattices over $\mathcal{O}_k$ can be viewed in terms of $\mathbb{Z}$-lattices. This resembles the fact that a module lattice is in particular a $\mathbb{Z}$-lattice.

**Example 6.2.3.** Let $\mathcal{H} := \mathrm{GL}_{m|\mathcal{O}_k}$ and $\mathcal{G}$ its *restriction of scalars* from $\mathcal{O}_k$ to $\mathbb{Z}$. That is, for a $\mathbb{Z}$-algebra $A$, $\mathcal{G}(A) := \mathrm{GL}_m(A \otimes_{\mathbb{Z}} \mathcal{O}_k)$. It can be shown that in the present case, this is again a finite type affine algebraic group over $\mathbb{Z}$. It satisfies the property

$$\mathrm{Hom}_{\mathbb{Z}}(\mathcal{G}, X) \simeq \mathrm{Hom}_{\mathcal{O}_k}(\mathcal{H}, X \otimes_{\mathbb{Z}} \mathcal{O}_k)$$

for any $\mathbb{Z}$-scheme $X$. By a choice of basis of $\mathcal{O}_k$ over $\mathbb{Z}$, one can see that $\mathcal{G}$ can be embedded into $\mathrm{GL}_{mn|\mathbb{Z}}$, where $n = [k\colon \mathbb{Q}]$. We view this as a faithful representation $\pi$. The space of lattices with $(\mathcal{G}, \pi)$-structure is

$$\mathcal{G}(\mathbb{Q})\backslash\mathcal{G}(\mathbb{A}_{\mathbb{Q}})/\mathcal{G}(\widehat{\mathbb{Z}}) = \mathrm{GL}_m(k)\backslash\mathrm{GL}_m(\mathbb{A}_k)/\mathrm{GL}_m(\widehat{\mathcal{O}}_k),$$

where we use the definition of restriction of scalars. The choice of basis, and with that $\pi$, defines an embedding of this space into

$$\mathrm{GL}_{mn}(\mathbb{Q})\backslash\mathrm{GL}_{mn}(\mathbb{A}_{\mathbb{Q}})/\mathrm{GL}_{mn}(\widehat{\mathbb{Z}}),$$

the space of $\mathbb{Z}$-lattices of rank $mn$. Note that two distinct choices of basis for $\mathcal{O}_k$ over $\mathbb{Z}$ yield conjugate embeddings into the space of $\mathbb{Z}$-lattices of rank $nm$.

## 6.3 Symplectic lattices

In the theory of (reductive) affine algebraic groups, symplectic groups take an important role as one of the so-called *classical groups*, see [Hum75]. We introduce them as they form an interesting class with potential implications to cryptography. Lattice reduction for symplectic lattices has been studied in [GHN06]. Symplectic structures have been used in [KEF19] for lattice reduction by introducing a symplectic structure on number fields. To avoid complications, we consider the base field $\mathbb{Q}$ only.

Let $\omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{GL}_{2m}(\mathbb{Z})$, where 1 represents the $m$-dimensional identity matrix. This defines a nondegenerate alternating form

$$\omega\colon k^{2m} \times k^{2m} \to k;\ (u, v) \mapsto u^t \omega v.$$

We define $\mathrm{Sp}_{2m}$ to be the algebraic group over $\mathbb{Q}$ that associates to a $\mathbb{Q}$-algebra $A$ the group

$$\mathrm{Sp}_{2m}(A) = \{g \in \mathrm{GL}_{2m}(A) \mid g^t \omega g = \omega\}.$$

Thus, points in $\mathrm{Sp}_{2m}$ preserve the form $\omega$. It is easy to see that this defines an affine algebraic group over $\mathbb{Q}$ of finite type. In fact, the equation $g^t \omega g = \omega$ defines polynomial equations in the coefficients of $g$, which need to be satisfied. It has a model over $\mathbb{Z}$, i.e., there exists an affine algebraic group $\underline{\mathrm{Sp}}_{2m}$ of finite type over $\mathbb{Z}$ with $\underline{\mathrm{Sp}}_{2m} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{Sp}_{2m}$. Further, $\underline{\mathrm{Sp}}_{2m}$ is naturally a subgroup of $\mathrm{GL}_{2m|\mathbb{Z}}$, which we view as faithful representation.

**Definition 6.3.1.** A *symplectic lattice* of rank $2m$ is a lattice with $\underline{\mathrm{Sp}}_{2m}$-structure.

Symplectic lattices are related to polarized abelian varieties over $\mathbb{C}$ and questions about such lattices can be rephrased in terms of questions on polarized abelian varieties. For example, see [Ber00].

## 6.4 Lattices in central simple algebras

Finally, we want to show that the lattices constructed in [GLV19] are structured lattices in sense of Definition 6.2.1. As we do not need the notion of cyclic lattices, which is introduced for efficiency reasons in [GLV19], we consider arbitrary central simple algebras. Recall that unless trivial, central simple algebras are *not* commutative. More details on central simple algebras can be found in [Mil20, Chapter IV] on Brauer Groups. We refer to [Voi21] for quaternion algebras.

Let $D$ be a central simple algebra over $k$ of dimension $m$. For simplicity we consider an order $\mathcal{O}_D$ of $D$ which is free over $\mathcal{O}_k$. We define the affine algebraic group $\mathcal{G}_D$ over $\mathcal{O}_k$ by the association

$$A \mapsto (A \otimes_{\mathcal{O}_k} \mathcal{O}_D)^\times$$

with $A$ commutative. Note the similarity to $\mathbb{G}_m$ in Example 6.1.1. The (right) translation action of $\mathcal{O}_D$ on itself yields a faithful representation of $\mathcal{O}_D$ in $\mathrm{M}_m(\mathcal{O}_k)$ by means of a choice of some basis of $\mathcal{O}_D$ over $\mathcal{O}_k$. This extends to a representation of $\mathcal{G}_D$. We define $\mathcal{O}_D$-lattices as lattices with $\mathcal{G}_D$-structure for the given representation.

Let us consider the case of quaternion algebras, i.e., a central simple algebra over $k$ of dimension 4. Quaternion algebras are close to $\mathrm{GL}_2$. In fact, $\mathrm{GL}_2$ is $\mathcal{G}_D$ for $D = \mathrm{M}_2(k)$. This is fundamentally reflected in the theory of automorphic representations for the groups $\mathcal{G}_D$ for arbitrary quaternion algebras and $\mathrm{GL}_2$, as we explain briefly.

First, there is a well-understood notion of automorphic forms over quaternion algebras over number fields, cf. [JL70, Chapter III]. It is said that $D$ is *split* or *unramified* at a place $\nu$ of $k$, if $D_\nu := D \otimes_k k_\nu$ is isomorphic to $\mathrm{M}_2(k_\nu)$, otherwise $D$ is ramified at $\nu$. It is known that $D$ is unramified at all but finitely many places. The Jacquet–Langlands correspondence, as can be found in [JL70] gives the aforementioned relationship in the theory of automorphic representations.

**Theorem 6.4.1.** *Let $\chi$ be a character of $\mathbb{G}_m(\mathbb{A}_k)$ and $D$ a quaternion algebra which is not $\mathrm{M}_2(k)$. Let $S$ be the nonempty set of places of $k$ at which $D$ ramifies. Then there is a one-to-one correspondence between*

- *automorphic representations $\pi = \otimes_\nu \pi_\nu$ of dimension $> 1$ of $G_D$ with central character $\chi$,*

*and*

- *cuspidal automorphic representations $\pi' = \otimes_\nu \pi'_\nu$ of $\mathrm{GL}_2$*

*such that $\pi'_\nu$ is a discrete series representation at all $\nu \in S$, and for all $\nu \notin S$, $\pi_\nu \simeq \pi'_\nu$.*

We do not explain discrete series representations here, see [Bum97; Gel75; JL70]. Analogous to our approach in Section 5, we may look for worst-case distributions on $\mathcal{G}_D$-structured lattices among automorphic forms.

**Reductive groups.** The theory of automorphic forms and representations works particularly analogous to $\mathrm{GL}_2$ as we covered in Section 4, if the group $G$ is reductive. The groups $\mathrm{Sp}_{2m}$ in Section 6.3 and $\mathcal{G}_D$ in Section 6.4 are examples of reductive groups. As reductive is a technical condition which we do not include more details here and refer to [Hum75; Wat79] for details.

## 6.5 LWE on $\mathcal{G}$-structured lattices

As a final remark, we want to mention two open questions regarding $\mathcal{G}$-structured lattices.

Firstly, our definition of $\mathcal{G}$-structured groups is quite abstract. It would be important for applications to spell out the definition for some choices of groups and give concrete descriptions of the corresponding lattices. E.g., this can be done for the symplectic lattices we defined above. In particular, this is required if the purpose of introducing additional structure is an increase of efficiency. Secondly, the classical reduction of the LWE problem to SVP has been treated separately for ideal and module lattices, and later for lattices over cyclic algebras. It might be possible to recover the proofs for $\mathcal{G}$-structured lattices for a certain class of groups.

# 7 Conclusion

The present work builds up a theoretical roadmap towards a worst-case to average-case reduction of computational problems on module lattices. This roadmap relies on the geometric structure of module lattices which is a consequence of the connection between module lattices and the general linear group. The description of the space of module lattices allows the study of functions on that space in terms of automorphic forms, which constitute our main technical tool for the analysis of distributions on the collection of module lattices. The space of automorphic forms admits a Hilbert space decomposition whose components can be understood in terms of basic building blocks. Our setup for a worst-case to average-case reduction is based on this insight; if the decomposition of a worst-case distribution into its basic building blocks has a specific form, then the convergence is only a question of convergence in terms of a coefficient sequence.

As a next step, it is necessary to find worst-case distributions according to our definition, which admit explicit descriptions as functions on the space of lattices, compare Appendix B. In fact, the problems here are two-fold. Given a smooth function on the space of lattices it is not known how to decompose it into irreducible components of the associated automorphic representation. On the other hand, a definition as in Appendix B does not yield an explicit function that can be used for applications. Both are mathematical problems that need effective versions of results in non-abelian harmonic analysis and representation theory. In the present work, we concentrated on the cuspidal part of functions on the space of lattices, though, in future work, one might consider Eisenstein series as well. Even further, we only touched upon the surface of the theory of automorphic forms which offers much deeper insights that might have an impact on lattice-based cryptography.

The $\mathcal{G}$-structured lattices we introduced here have not been considered in this generality yet. It might be interesting to analyze LWE on this type of lattices. Specifically, the classical security results of LWE as analyzed in [GLV19; LPR10; Reg05], may translate to conditions that are intrinsic to the underlying group structure.

**Acknowledgement.** This work was partially funded by the German Ministry of Education, Research and Technology in the context of the project Aquorypt (grant number 16KIS1022).

# References


[Alk+16] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. "Post-quantum Key Exchange - A New Hope". *USENIX Security 2016*. 2016, pp. 327–343 (cit. on p. 1).

[Alk+20] E. Alkim, P. S. L. M. Barreto, N. Bindel, J. Krämer, P. Longa, and J. E. Ricardini. "The Lattice-Based Digital Signature Scheme qTESLA". *ACNS 20, Part I*. Vol. 12146. 2020, pp. 441–460 (cit. on p. 1).

[Ber00] A.-M. Bergé. "Symplectic lattices". *Quadratic forms and their applications (Dublin, 1999)*. Vol. 272. 2000, pp. 9–22 (cit. on p. 28).

[BGV12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping". *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. 2012, pp. 309–325 (cit. on p. 5).

[BH06] C. J. Bushnell and G. Henniart. *The local Langlands conjecture for* GL(2). Vol. 335. 2006, pp. xii+347 (cit. on pp. 16, 19, 20).

[BJ79] A. Borel and H. Jacquet. "Automorphic forms and automorphic representations". *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*. 1979, pp. 189–207 (cit. on p. 16).

[Boe+20] K. de Boer, L. Ducas, A. Pellet-Mary, and B. Wesolowski. "Random self-reducibility of ideal-SVP via Arakelov random walks". *Advances in cryptology—CRYPTO 2020. Part II*. Vol. 12171. 2020, pp. 243–273 (cit. on pp. 2–4, 10, 12, 22, 23, 33–37).

[Bor63] A. Borel. "Some finiteness properties of adele groups over number fields". *Inst. Hautes Études Sci. Publ. Math.* 16 (1963), pp. 5–30 (cit. on pp. 11, 12).

[Bos+18] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM". *2018 IEEE European Symposium on Security and Privacy (EuroS P)*. 2018, pp. 353–367 (cit. on p. 1).

[BS16] J.-F. Biasse and F. Song. "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields". *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*. 2016, pp. 893–902 (cit. on p. 14).

[Bum97] D. Bump. *Automorphic forms and representations*. Vol. 55. 1997, pp. xiv+574 (cit. on pp. 16, 20, 24, 28, 37, 38).

[Cas73] W. Casselman. "On some results of Atkin and Lehner". *Math. Ann.* 201 (1973), pp. 301–314 (cit. on p. 22).

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. "Short Stickelberger class relations and application to ideal-SVP". *Advances in cryptology—EUROCRYPT 2017. Part I*. Vol. 10210. 2017, pp. 324–348 (cit. on p. 1).

[CKM04] J. W. Cogdell, H. H. Kim, and M. R. Murty. *Lectures on automorphic L-functions*. Vol. 20. 2004, pp. xii+283 (cit. on pp. 16, 18, 20).

[Coh00] H. Cohen. *Advanced topics in computational number theory*. Vol. 193. 2000, pp. xvi+578 (cit. on p. 14).

[DPW19] L. Ducas, M. Plançon, and B. Wesolowski. "On the shortness of vectors to be found by the ideal-SVP quantum algorithm". *Advances in cryptology—CRYPTO 2019. Part I*. Vol. 11692. 2019, pp. 322–351 (cit. on p. 1).

[Duc+18] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme". *IACR TCHES* 2018.1 (2018), pp. 238–268 (cit. on p. 1).

[Fla79] D. Flath. "Decomposition of representations into tensor products". *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*. 1979, pp. 179–183 (cit. on p. 21).

[Gar18] P. Garrett. *Modern analysis of automorphic forms by example. Vol. 1*. Vol. 173. 2018, pp. xxii+384 (cit. on pp. 12, 16, 17, 22).

[Gel75] S. S. Gelbart. *Automorphic forms on adèle groups*. 1975, pp. x+267 (cit. on pp. 18, 28, 41).
[GGP90] I. M. Gel'fand, M. I. Graev, and I. I. Pyatetskii-Shapiro. *Representation theory and automorphic functions*. Vol. 6. 1990, pp. xviii+426 (cit. on p. 22).
[GHN06] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen. "Symplectic lattice reduction and NTRU". *Advances in cryptology—EUROCRYPT 2006*. Vol. 4004. 2006, pp. 233–253 (cit. on p. 27).
[GLV19] C. Grover, C. Ling, and R. Vehkalahti. *Non-Commutative Ring Learning With Errors From Cyclic Algebras*. Cryptology ePrint Archive, Report 2019/680. 2019 (cit. on pp. 5, 28, 29).
[Hum75] J. E. Humphreys. *Linear algebraic groups*. 1975, pp. xiv+247 (cit. on pp. 27, 28).
[JL70] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). 1970, pp. vii+548 (cit. on pp. 18, 22, 28).
[KEF19] P. Kirchner, T. Espitau, and P.-A. Fouque. *Algebraic and Euclidean Lattices: Optimal Lattice Reduction and Beyond*. Cryptology ePrint Archive, Report 2019/1436. 2019 (cit. on p. 27).
[Kna02] A. W. Knapp. *Lie groups beyond an introduction*. Second. Vol. 140. 2002, pp. xviii+812 (cit. on p. 16).
[Kud03] S. S. Kudla. "From modular forms to automorphic representations". *An introduction to the Langlands program (Jerusalem, 2001)*. 2003, pp. 133–151 (cit. on pp. 4, 18).
[Lee+19] C. Lee, A. Pellet-Mary, D. Stehlé, and A. Wallet. "An LLL Algorithm for Module Lattices". *Advances in Cryptology – ASIACRYPT 2019*. Cham, 2019, pp. 59–90 (cit. on p. 5).
[LLL82] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. "Factoring polynomials with rational coefficients". *Math. Ann.* 261.4 (1982), pp. 515–534 (cit. on p. 5).
[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. "On ideal lattices and learning with errors over rings". *Advances in cryptology—EUROCRYPT 2010*. Vol. 6110. 2010, pp. 1–23 (cit. on pp. 1, 29).
[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev. "A toolkit for ring-LWE cryptography". *Advances in cryptology—EUROCRYPT 2013*. Vol. 7881. 2013, pp. 35–54 (cit. on p. 1).
[LS15] A. Langlois and D. Stehlé. "Worst-case to average-case reductions for module lattices". *Des. Codes Cryptogr.* 75.3 (2015), pp. 565–599 (cit. on pp. 1, 5).
[MG02] D. Micciancio and S. Goldwasser. *Complexity of lattice problems*. Vol. 671. 2002, pp. x+220 (cit. on p. 1).
[Mic01] D. Micciancio. "The Shortest Vector Problem is NP-hard to approximate to within some constant". *SIAM Journal on Computing* 30.6 (Mar. 2001), pp. 2008–2035 (cit. on p. 1).
[Mil05] J. S. Milne. "Introduction to Shimura varieties". *Harmonic analysis, the trace formula, and Shimura varieties*. Vol. 4. 2005, pp. 265–378 (cit. on p. 12).
[Mil20] J. Milne. *Class Field Theory (v4.03)*. 2020 (cit. on p. 28).
[MS20] T. Mukherjee and N. Stephens-Davidowitz. "Lattice reduction for modules, or how to reduce moduleSVP to moduleSVP". *Advances in cryptology—CRYPTO 2020. Part II*. Vol. 12171. 2020, pp. 213–242 (cit. on p. 5).
[Nae+20] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. *FrodoKEM*. Tech. rep. National Institute of Standards and Technology, 2020 (cit. on p. 1).
[Neu99] J. Neukirch. *Algebraic number theory*. Vol. 322. 1999, pp. xviii+571 (cit. on pp. 5–8, 15).
[Pei14] C. Peikert. "A decade of lattice cryptography". *Found. Trends Theor. Comput. Sci.* 10.4 (2014), pp. i–iii, 283–424 (cit. on p. 1).
[PHS19] A. Pellet-Mary, G. Hanrot, and D. Stehlé. "Approx-SVP in ideal lattices with pre-processing". *Advances in cryptology—EUROCRYPT 2019. Part II*. Vol. 11477. 2019, pp. 685–716 (cit. on p. 1).
[Pre+20] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. *FALCON*. Tech. rep. National Institute of Standards and Technology, 2020 (cit. on p. 1).

[Reg05] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography”. *STOC’05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. 2005, pp. 84–93 (cit. on p. 29).

[Ros94] J. Rosenberg. *Algebraic $K$-theory and its applications*. Vol. 147. 1994, pp. x+392 (cit. on p. 13).

[RV99] D. Ramakrishnan and R. J. Valenza. *Fourier analysis on number fields*. Vol. 186. 1999, pp. xxii+350 (cit. on p. 9).

[Ser79] J.-P. Serre. *Local fields*. Vol. 67. 1979, pp. viii+241 (cit. on p. 40).

[SS11] D. Stehlé and R. Steinfeld. “Making `NTRU` as secure as worst-case problems over ideal lattices”. *Advances in cryptology—EUROCRYPT 2011*. Vol. 6632. 2011, pp. 27–47 (cit. on p. 1).

[Tat67] J. T. Tate. “Fourier analysis in number fields, and Hecke’s zeta-functions”. *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*. 1967, pp. 305–347 (cit. on p. 9).

[Voi21] J. Voight. *Quaternion algebras*. Vol. 288. 2021, pp. xxiii+885 (cit. on p. 28).

[Wat79] W. C. Waterhouse. *Introduction to affine group schemes*. Vol. 66. 1979, pp. xi+164 (cit. on pp. 25, 28).

[Wei95] A. Weil. *Basic number theory*. 1995, pp. xviii+315 (cit. on pp. 7, 9, 11).

# A Rank 1 from adèlic perspective

In this appendix section we want to show how [Boe+20] can be understood in the terms of our present approach. In two sections, we explain first how ideal lattices can be viewed as adèle valued points of $\mathbb{G}_m$, i.e., as idèles, and translate the worst-case distribution in [Boe+20] to this framework in the second part.

The first section is closely related to Section 3 with the main distinction that the rank 1 case is less technical. We present the details for convenience. The reader who has not encountered the concept of adèles before can find a first impression how this terminology is applied. The second subsection is the rank 1 analogue of what we have developed through Sections 4 and 5. Again, the discussion is less technical here, as in dimension 1 the representation theory is easier and the well-known theory of Fourier analysis can be applied. We outline how the worst-case distribution in [Boe+20] can be viewed as a smooth function on the space of ideal lattices from the adèlic viewpoint, and show how the Hecke operators in [Boe+20] are related to Hecke operators in the sense of automorphic forms on $\mathbb{G}_m$. Finally, we describe briefly the representation theoretic assumption on the finite places.

## A.1 Ideal Lattices over $k$

In this section we define ideal lattices and relate them to idèles. We denote by $\mathrm{I}_k$ the set of $\mathcal{O}_k$-fractional ideals. If $I \subseteq k$ is such a fractional ideal, then we denote by $\mathcal{L}(I)$ its image under the diagonal embedding of $k$ into $k_\infty$.

**Definition A.1.1** (As in [Boe+20])**.** An $\mathcal{O}_k$*-ideal lattice* is an $\mathcal{O}_k$-submodule $M$ of $k_\infty$ of the form $M = g^{-1}\mathcal{L}(I)$ for a $g \in k_\infty^\times$ and a fractional ideal $I \in \mathrm{I}_k$. The set of ideal lattices is denoted $\mathrm{IdLat}(k)$ or $\mathrm{Lat}_1(k)$.

The inverse of $g$ in the definition is chosen for compatibility reasons only. The set of ideal lattices can be characterized as follows.

**Proposition A.1.2.** *There is a canonical surjective map $k_\infty^\times \times \mathrm{I}_k \twoheadrightarrow \mathrm{IdLat}(k)$ which factors to an isomorphism*

$$k^\times \backslash k_\infty^\times \times \mathrm{I}_k \xrightarrow{\simeq} \mathrm{IdLat}(k)$$

*where $k^\times$ acts on $k_\infty^\times \times \mathrm{I}_k$ via $\lambda.(g, I) = (\lambda g, \lambda I)$.*

*Proof.* We define the map by $(g, I) \mapsto g^{-1}I$. This is surjective by the definition of ideal lattices. For $\lambda \in k^\times$, $(\lambda g, \lambda I)$ maps to $g^{-1}I$ as $\lambda$ cancels out. Hence the map induces a surjective map from $k^\times \backslash k_\infty^\times \times \mathrm{I}_k$. Conversely, if two $(g, I)$ and $(h, J)$ define the same ideal lattice $g^{-1}I = h^{-1}J$, let $\lambda := hg^{-1}$. Then multiplication by $\lambda$ defines an isomorphism $I \to J$ of $\mathcal{O}_k$-modules, and by extension

$$k \simeq I \otimes_{\mathcal{O}_k} k \to J \otimes_{\mathcal{O}_k} k \simeq k.$$

Thus, $\lambda$ is an element of $\mathrm{GL}_1(k) = \mathbb{G}_m(k) = k^\times$. Moreover, it is trivial to check that $\lambda(g, I) = (h, J)$. □

Our goal is to relate $\mathrm{IdLat}(k)$ to $\mathbb{G}_m(\mathbb{A}_k)$. The previous proposition may be viewed as a first step in that direction. Considering the factorization $\mathbb{G}_m(\mathbb{A}_k) = k_\infty^\times \times \mathbb{G}_m(\mathbb{A}_{k,f})$ one expects a relationship between $\mathbb{G}_m(\mathbb{A}_{k,f})$ and $\mathrm{I}_k$. As before, let $U_f := \mathbb{G}_m(\widehat{\mathcal{O}}_k) = \widehat{\mathcal{O}}_k^\times$. Then, we have the following.

**Lemma A.1.3.** *There is a canonical isomorphism*

$$\Psi_1^f \colon \mathbb{G}_{\mathrm{m}}(\mathbb{A}_{k,\mathrm{f}})/U_f \longrightarrow \mathrm{I}_k;\ x \mapsto I_x := \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}(x_\mathfrak{p})}.$$

*Let $t_\mathfrak{p}$ be uniformizers of $\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$. Then the map*

$$\Phi_1^f \colon \mathrm{I}_k \longrightarrow \mathbb{G}_{\mathrm{m}}(\mathbb{A}_{k,\mathrm{f}})/U_f\ ;\ I \longmapsto (t_\mathfrak{p}^{\nu_\mathfrak{p}(I)})_\mathfrak{p}$$

*is an inverse.*

*Proof.* Note that $\Psi_1^f$ is well-defined, as if $(\xi_\mathfrak{p})_\mathfrak{p} \in U_f$, then $\nu_\mathfrak{p}(x_\mathfrak{p}\xi_\mathfrak{p}) = \nu_\mathfrak{p}(x_\mathfrak{p}) + \nu_\mathfrak{p}(\xi_\mathfrak{p}) = \nu_\mathfrak{p}(x_\mathfrak{p})$. That the two maps are mutually inverse is then obvious from the fact that $\nu_\mathfrak{p}(x_\mathfrak{p}) = \nu_\mathfrak{p}(I_x)$. □

Note moreover that $\Phi_1^f$ does not depend on the choice of $t_\mathfrak{p}$. In fact, any other choice would differ by $\xi_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$ for each $\mathfrak{p}$, hence $\xi = (\xi_\mathfrak{p}) \in U_f$.

**Corollary A.1.4.** *The class group of $k$ is isomorphic to $k^\times \backslash \mathbb{G}_\mathrm{m}(\mathbb{A}_{k,\mathrm{f}})/U_f$.*

*Proof.* One just needs to show that the maps $\Delta\colon k^\times \to \mathbb{G}_\mathrm{m}(\mathbb{A}_{k,\mathrm{f}})$ and $\mathrm{div}\colon k^\times \to \mathrm{I}_k$ are compatible with $\Psi_1^f$ in Lemma A.1.3. But this is clear. □

**Lemma A.1.5.** *The map $\Psi_1^f$ from Lemma A.1.3 induces a bijective map*

$$\widetilde{\Psi}_1\colon \mathbb{G}_m(\mathbb{A}_k)/U_f \longrightarrow k_\infty^\times \times \mathrm{I}_k$$

*which is $k^\times$-equivariant.*

*Proof.* The function $\widetilde{\Psi}_1$ is defined by mapping $(g,x) \in k_\infty^\times \times \mathbb{G}_m(\mathbb{A}_{k,f}) = \mathbb{G}_m(\mathbb{A}_k)$ to $(g, I_x)$, where $I_x = \Psi_1^f(x)$ as in Lemma A.1.3. It is clear that $\Phi_1^f$ induces an inverse to $\widetilde{\Psi}_1$. For $k^\times$-equivariance, let $\lambda \in k^\times$, and $(g,x) \in \mathbb{G}_m(\mathbb{A}_k)$. As $U_f$ only acts on $\mathbb{G}_m(\mathbb{A}_{k,f})$ we need to show $I_{\lambda x} = \lambda I_x$ as fractional ideals. But this is trivial from comparing their multiplicities at each prime. □

**Corollary A.1.6.** *There is a canonical isomorphism*

$$\Psi_1\colon k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)/U_f \xrightarrow{\simeq} \mathrm{IdLat}(k)$$

*induced from $\widetilde{\Psi}_1$ by taking quotients modulo $k^\times$.*

In Section 3 we have seen the analogue for $\mathbb{G}_m$ replaced by $\mathrm{GL}_m$.

**Norm 1 ideal lattices.** So far, we considered a quite general class of ideal lattices. However, this space is to large, in fact, $k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)/U_f$ is not compact, nor has it finite volume, compare Section 2.2 and the discussion about the diagonal embedding of $k^\times$ into the idèles there. One can remedy this problem as done in Section 2.2 for $\mathbb{G}_m(\mathbb{A}_k)$ by restricting to the norm 1 subgroup. There is a direct definition for ideal lattices.

**Definition A.1.7.** The *norm* of $(g,I) \in k_\infty^\times \times \mathrm{I}_k$ is defined as $\mathrm{N}(g,I) \coloneqq \mathrm{N}_{k/\mathbb{Q}}(I)|g|_\infty^{-1}$, where $|g|_\infty = \prod_\sigma |g_\sigma|_\sigma$.

We remark that in [Boe+20] there is a further condition that the infinite component consists of positive real entries.

**Lemma A.1.8.** *The norm on $k_\infty^\times \times \mathrm{I}_k$ induces a norm on $\mathrm{IdLat}(k)$, which is compatible with the norm on $\mathbb{G}_m(\mathbb{A}_k)$ up to inverse. More precisely, for any $(g,x) \in \mathbb{G}_m(\mathbb{A}_k)$ and $I = I_x$,*

$$|(g,x)| = \mathrm{N}(g,I)^{-1}.$$

*Proof.* Suppose $\lambda \in k^\times$ and $(g,I) \in k_\infty^\times \times \mathrm{I}_k$. Then we consider $\mathrm{N}(\lambda g, \lambda I) = \mathrm{N}_{k/\mathbb{Q}}(\lambda I)|\lambda g|_\infty^{-1}$. It holds true that $\mathrm{N}_{k/\mathbb{Q}}(\lambda I) = |\lambda|_f^{-1}\,\mathrm{N}_{k/\mathbb{Q}}(I)$. Moreover, the product formula 2.1.7 can be written as $|\lambda|_\infty|\lambda|_f = 1$, so that in conclusion, we have $\mathrm{N}(\lambda g, \lambda I) = \mathrm{N}(g,I)$, as we wanted. For the second claim we again note that for $(g,x) \in \mathbb{G}_m(\mathbb{A}_k)$, $|(g,x)| = |g|_\infty|x|_f$, so that it suffices to compare the factors separately. For $x$ note that the factor that a prime $\mathfrak{p}$ contributes to $|x|_f$ is $p^{-f_\mathfrak{p}\,\nu_\mathfrak{p}(x_\mathfrak{p})}$, while $\mathfrak{p}$ contributes to $\mathrm{N}_{k/\mathbb{Q}}(I_x)$

as factor $p^{f_\mathfrak{p}\,\nu_\mathfrak{p}(x_\mathfrak{p})}$. Hence, the claim follows for the finite part. For the infinite part, the inverse is by definition. □

We define the subgroup $\mathrm{IdLat}^1(k)$ of norm 1 ideal lattices over $k$ is defined as the set of $(g, I)$ with $\mathrm{N}(g, I) = 1$.

**Isometry classes of lattices.**

**Definition A.1.9.** Two $L, L' \in \mathrm{IdLat}^1(k)$ are *k-isometric* if there exists $x \in k_\infty$ with $|x_\sigma|_\sigma = 1$ for all $\sigma \mid \infty$, such that $xL = L'$. The set of classes of $k$-isometric lattices is denoted $\mathrm{IsomIdLat}^1_k$.

Note that $x \in k_\sigma$ for $\sigma \mid \infty$ satisfies $|x_\sigma|_\sigma = 1$, if and only if $x \in \pm 1$, in the case $\sigma$ is a real place, or $x \in S^1 \subseteq \mathbb{C}^\times$, if $\sigma$ is complex. These are the two maximal compact subgroups of $k_\sigma$. Let $U_\infty$ denote the product $\prod_{\sigma|\infty} U_\sigma$ with $U_\sigma = \pm 1$, if $\sigma$ real, and $U_\sigma = S^1$, if $\sigma$ is complex. Then we have the following.

**Theorem A.1.10.** *There is a canonical identification*

$$k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)^1 / U_f U_\infty \xrightarrow{\simeq} \mathrm{IsomIdLat}^1_k .$$

Together with the identification in [Boe+20] of $\mathrm{IsomIdLat}^1_k$ with the degree 0 part of the Arakelov Class Group, we see that this idèles recover the approach from Arakelov divisors. As in Section 3, we can describe the space of ideal lattices as follows.

**Theorem A.1.11.** *There is a natural identification*

$$k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)^1 / U_f U_\infty \xrightarrow{\simeq} \coprod_{\mathrm{Cl}_k} \mathcal{O}_k^\times \backslash k^1_\infty / U_\infty = \left(\mathcal{O}_k^\times \backslash k^1_\infty / U_\infty\right)^{h_k}.$$

*Remark* A.1.12. As $\mathbb{G}_m$ is abelian, we have a group structure on this space. A more natural form of Theorem A.1.11 is the following. The group $k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)^1 / U_f U_\infty$ is the extension of $\mathcal{O}_k^\times \backslash k^1_\infty / U_\infty$ by $\mathrm{Cl}_k$, that is, there exists a short exact sequence

$$0 \longrightarrow \mathcal{O}_k^\times \backslash k^1_\infty / U_\infty \longrightarrow k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)^1 / U_f U_\infty \xrightarrow{\det} \mathrm{Cl}_k \longrightarrow 0.$$

The det is the norm function on the finite component $\mathbb{G}_m(\mathbb{A}_{k,f})$. This is the adèlic version of the corresponding sequence in terms of the Arakelov class group in [Boe+20].

## A.2 Worst-Case to Average-Case Reduction in Rank 1

In this section, we recall the worst-case distribution in [Boe+20], and translate their definition to the adèlic approach for $\mathbb{G}_m$.

As before let $r$ denote the number of infinite places of $k$. Then there is a natural map $\ell\colon k_\infty^\times \to \bigotimes_\sigma \mathbb{R} \cong \mathbb{R}^r$ given by $(x_\sigma) \mapsto (\log|x_\sigma|)$, in which $\Lambda_k := \ell(\mathcal{O}_k^\times)$ defines a lattice.

**Lemma A.2.1.** *The map*

$$\ell\colon \mathcal{O}_k^\times \backslash k_\infty^\times / U_\infty \to \Lambda_k \backslash \mathbb{R}^r$$

*is an isomorphism.*

Under $\ell$, the norm 1 elements of $k_\infty^\times$ correspond to trace-zero elements $H_k$ of $\mathbb{R}^r$.

**Lemma A.2.2.** *The map*

$$\ell\colon \mathcal{O}_k^\times \backslash k^1_\infty / U_\infty \to \Lambda_k \backslash H_k$$

*is an isomorphism. In particular, $\Lambda_k$ is a complete lattice in $H_k$.*

This gives a new description of ideal lattices as follows.

**Corollary A.2.3.** *There is a natural one-to-one correspondence*

$$\mathrm{IsomIdLat}_k^1 \xrightarrow{\sim} \left(\Lambda_k \backslash H_k\right)^{h_k}.$$

In [Boe+20], they defined worst-case distributions on the space of ideal lattices as follows. On the connected component of the identity, one sets

$$\rho_s \colon \Lambda_k \backslash H_k \to \mathbb{R}_{>0};\ x \mapsto \sum_{y : \overline{y} = x} \exp(-\pi \|y\|^2 / s^2),$$

which is extended to $\left(\Lambda_k \backslash H_k\right)^{h_k}$ by 0. Let $\Lambda_k^\vee$ be the dual lattice of $\Lambda_k$ in $H_k$. That is, $\lambda \in \Lambda_k^\vee$, if and only if $\langle \lambda, x \rangle \in \mathbb{Z}$ for all $x \in \Lambda_k$. As shown in [Boe+20], one can use Fourier analysis to write

$$\rho_s = \sum_{\lambda \in \Lambda_k^\vee} a_\lambda \chi_\lambda \tag{A.1}$$

for certain $a_\lambda \in \mathbb{C}$, cf. [Boe+20, Lemma 3.15]. Note that we have a slightly different notation, the $a_\lambda$ differ by a scalar. By the identifications of Corollary A.2.3 and Proposition A.1.10, we can view characters on $\left(\Lambda_k \backslash H_k\right)^{h_k}$ as characters on

$$k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)^1 / U_f U_\infty.$$

These are unramified Hecke characters trivial on the ray $Z^1 \coloneqq \{(x, \dots, x) \mid x \in \mathbb{R}_{>0}\} \subseteq k_\infty^\times$. Similarly, we can express $\rho_s$ as a function on $k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)^1 / U_f U_\infty$, which admits a Fourier decomposition into the unramified $Z^1$-invariant Hecke characters of $k$. With slight abuse of notation,

$$\rho_s = \sum_\chi a_\chi \chi$$

where the sum runs over the unramified $Z^1$-invariant Hecke characters and if the restriction of $\chi$ to the connected component of the identity is given by $\chi_\lambda$ for some $\lambda \in \Lambda_k^\vee$, then $a_\chi = a_\lambda$.

**Hecke Algebra.** For any finite place $\mathfrak{p}$ of $k$, we define the Hecke algebra $\mathcal{H}_\mathfrak{p}$ at $\mathfrak{p}$ to be the space of locally constant functions with compact support on $k_\mathfrak{p}^\times$. It is an algebra with convolution of functions, however, it has no unit. For any compact open subset $U \subseteq k_\mathfrak{p}^\times$, there are idempotents $\xi_U = \frac{1}{\mathrm{vol}(U)} \chi_U$, where $\chi_U$ is the characteristic function of $U$. We set $H_\mathfrak{p}$ to be the idempotent associated with the compact open subset $t_\mathfrak{p} \mathcal{O}_\mathfrak{p}^\times$. The Hecke algebra acts on the space of $\mathrm{L}^2$ functions on $k^\times \backslash \mathbb{G}_m(\mathbb{A}_k)^1 / U_f U_\infty$ via convolution.

**Lemma A.2.4.** *Let $\chi$ be an unramified $Z^1$-invariant Hecke character. Then $\chi$ is an eigenvalue of the action of $H_\mathfrak{p}$.*

*Proof.* By definition,

$$\begin{aligned}
H_\mathfrak{p} \star \chi(x) &= \int_{k_\mathfrak{p}^\times} H_\mathfrak{p}(y) \chi(y^{-1} x) dy \\
&= \int_{k_\mathfrak{p}^\times} H_\mathfrak{p}(y) \chi(y^{-1}) \chi(x) dy \\
&= \left( \int_{k_\mathfrak{p}^\times} H_\mathfrak{p}(y) \chi(y^{-1}) dy \right) \chi(x) \\
&= \alpha_{\chi, \mathfrak{p}} \chi(x)
\end{aligned}$$

where $\alpha_{\chi,\mathfrak{p}} = \int_{k_\mathfrak{p}^\times} H_\mathfrak{p}(y) \chi(y^{-1}) dy$. □

Given a collection $S$ of primes of $\mathcal{O}_k$, we can define $H_S \coloneqq \otimes_{\mathfrak{p}\in S} H_{\mathfrak{p}}$. Then Lemma A.2.4 holds true for $H_S$.

We have described all the ingredients for the main result of [Boe+20], written in the language of adèles. The proof of the main result in the current approach is a direct consequence of the result in [Boe+20], as all parts transfer smoothly.

# B Construction of Cuspidal Automorphic Representations

In this section, we give a further outline of the notion of cuspidal representations. By Theorem 4.3.5, we know that a cuspidal representation is a tensor product of local representations. We describe the classes of representations that are interesting for the use in application as in Section 5. In particular, we will focus on the spherical representations at the non-Archimedean places. Afterwards, we will briefly recall how one can use a general construction due to Weil, to get cuspidal automorphic representations which are spherical at all finite places. This is only possible under certain assumptions on the number field, namely, that it admits an unramified degree 2 field extension. These cuspidal representations depend on such a choice of field extension $L/k$ and characters of the idèle class group of $L$. In particular, worst-case distributions of module lattices of rank 2 over $k$ can be defined in terms of worst-case distributions of ideal lattices over $L$. One of the main drawbacks of the construction from application perspective is that we have only know by abstract reasoning that the representation constructed is among cuspidal representations. However, we cannot give explicit description of e.g. the spherical vectors as functions on the space of lattices.

## B.1 Representations of $\mathrm{GL}_2$ over Non-Archimedean Fields

In this section, we give an overview of the characterization of irreducible admissible representations of $\mathrm{GL}_2$ over a non-Archimedean field. The most interesting for our purpose are spherical representations, which are infinite dimensional representations that contain a unique 1-dimensional $K$-subrepresentation. We will write $G$ for $\mathrm{GL}_2(F)$ for a non-Archimedean field $F$.

To begin with, all irreducible finite dimensional representations $(\pi, V)$ of $G$ have the property that there exists a quasi-character $\chi\colon F^\times \to \mathbb{C}^\times$ such that $\pi = \chi \circ \det$, see [Bum97]. Hence, irreducible finite dimensional representations are 1-dimensional.

We continue with infinite dimensional irreducible representations, which can be constructed as follows. First, we define certain subgroups of $G$, namely

$$T = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} \text{ and } A = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\},$$

and we set $B = TA$, the invertible upper triangular matrices. Here $*$ symbolizes any values in $F$ such that the resulting matrices are invertible. It is easy to see that $A \simeq F$ as additive group and $T \simeq (F^\times)^2$. For elements in $T$ we write $(a_1, a_2)$ as shorthand for the diagonal matrix with entries $a_1$ and $a_2$ on the diagonal.

The important fact in the representation theory of $G$ is that any irreducible admissible representation is found in induced representations from $B$ to $G$, which are trivial on $A$. More precisely, let $\chi_1, \chi_2\colon F^\times \to \mathbb{C}^\times$ be two quasi-characters. This defines a (normalized) representation $\pi$ of $T$ by

$$\pi(a_1, a_2) = |a_1|_F^{1/2}\ \chi_1(a_1)\ |a_2|_F^{-1/2}\ \chi_2(a_2).$$

which extends to $B$ by

$$\pi\left(\begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix}\right) = |a_1|_F^{1/2}\ \chi_1(a_1)\ |a_2|_F^{-1/2}\ \chi_2(a_2)$$

by ignoring $x$. We set

$$\mathrm{I}(\chi_1, \chi_2) = \mathrm{Ind}_B^G \pi,$$

i.e., $\mathrm{I}(\chi_1, \chi_2)$ consists of functions $f\colon G \to \mathbb{C}$ such that

$$f\left(\begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix} g\right) = |a_1|_F^{1/2}\ \chi_1(a_1)\ |a_2|_F^{-1/2}\ \chi_2(a_2)\ f(g)$$

for any $g \in G$, and $G$ acts on these functions by right translation.

**Proposition B.1.1.** *If $\chi_1\chi_2^{-1} \neq |\_|_F^{\pm 1}$, then $\mathrm{I}(\chi_1, \chi_2)$ is irreducible. If $\chi_1$ and $\chi_2$ are unramified, then $\mathrm{I}(\chi_1, \chi_2)$ contains a spherical vector, which is unique up to scaling.*

We only discuss the last part as this is important for our applications later. Recall that a quasi-character $\chi$ on $F^\times$ is unramified if its restriction $\chi|_{\mathcal{O}_F}$ is trivial. Further recall that over a non-Archimedean field $F$, $\mathrm{GL}_2$ has a *Iwasawa decomposition*

$$G = TK$$

where $K = \mathrm{GL}_2(\mathcal{O}_F)$. However, $K$ and $T$ intersect nontrivially. It thus follows that any $f \in \mathrm{I}(\chi_1, \chi_2)$ is determined by its values on $K$. Conversely, if $\chi_1$ and $\chi_2$ are unramified, forcing $f(k) = 1$ for all $k \in K$ is a well-defined element of $\mathrm{I}(\chi_1, \chi_2)$. Such a $K$-invariant element is called a *spherical vector* and a representation which admits a spherical vector is called *spherical representation*. This particular choice will be called the *normalized* spherical vector. We will construct cuspidal automorphic representations with spherical factors only. This is desirable from application side, as we want to have functions on the space of lattices, i.e., functions that are $K_\mathfrak{p}$-invariant, for each prime.

In the case when $\chi_1\chi_2^{-1} = |\_|_F^{\pm 1}$, the induced representation is not irreducible. Indeed, there is a character $\chi$ such that $\chi_i = \chi \otimes |\_|^{\pm 1/2}$ for both, $i = 1, 2$. Then $\chi \circ \det \in \mathrm{I}(\chi_1, \chi_2)$ is a $G$-invariant subrepresentation. The subquotient is again irreducible and called *Steinberg representation*. Note that for our construction later, we assume $\chi_i$ to be characters rather than merely quasi-characters. Under this assumption $\chi_1$ and $\chi_2$ cannot satisfy the property $\chi_1\chi_2^{-1} = |\_|_F^{\pm 1}$, so that the induced representation is always of the form given above. These results are well-known in the representation theory of $\mathrm{GL}_2$ over non-Archimedean fields. For example [Bum97, Chapter 4] builds up the theory from scratch.

The irreducible admissible representations of $G$ that do not fall into the classes we defined above, are called *supercuspidal*. As we mentioned, we are looking for spherical representations which cannot be supercuspidal. Therefore, we do not go into details of supercuspidal representations any further. Using the Weil representations it is possible to construct supercuspidal representations, see Subsection B.3.

## B.2 Representations of $\mathrm{GL}_2$ over Archimedean Fields

We continue with the classification of irreducible admissible representations of $\mathrm{GL}_2$ over Archimedean fields. As described earlier in Section 4.2, we use the notion of $(\mathfrak{g}, K)$-modules.

We will denote by $F$ an Archimedean field and $G = \mathrm{GL}_2(F)$. These can be constructed similar to the non-Archimedean case as induced representation of characters on the Borel subgroup of upper triangular matrices, up to normalization. However, it is possible to characterize irreducible admissible representations in terms of the following data.

- $K$-weights, i.e., the isotypic components that can appear in an irreducible admissible representation,
- the action of the center of $\mathcal{U}(\mathfrak{g})$.

This makes the classification of irreducible admissible representations of $G$ particularly coherent. Let us consider the two cases separately.

**Real case.** The real case seems less important for current cryptographic applications. Still, we recall the theory for completeness sake. Unfortunately, the real case comes with a slight complication in comparison to the complex case due to the fact that $G = \mathrm{GL}_2(\mathbb{R})$ is disconnected. In fact, the determinant maps $G$ onto $\mathbb{R}^\times$, and $G$ decomposes into the two connected components with positive and negative determinants. The subgroup of matrices with positive determinant is denoted $G^+$. The disconnectedness causes a problem as the Lie algebra only sees the connected component $G^+$ of the identity. One can deal with this by considering the maximal compact subgroup $\mathrm{O}_2(\mathbb{R})$ instead of $\mathrm{SO}_2(\mathbb{R})$, which keeps track of the second connected component. Then the $K$-isotypic classes may be replaced by $\mathrm{O}_2(\mathbb{R})$-isotypic components. Another way is to keep track of the action of a single, fixed element

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $T, A$ and $B$ be subgroups of $G$ as in Subsection B.1. Any two quasi-characters $\chi_1, \chi_2$ on $\mathbb{R}^\times$ define a representation $\pi$ on $B$ by

$$\pi\left(\begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix}\right) := \left|\frac{a_1}{a_2}\right|^{1/2} \chi_1(a_1)\chi_2(a_2).$$

Define

$$\pi(\chi_1, \chi_2) := \mathrm{Ind}_B^{G^+} \pi.$$

Thus, $\pi(\chi_1, \chi_2)$ consists of functions $\varphi$ on $G^+$ such that for $b = \begin{pmatrix} a_1 & x \\ 0 & a_2 \end{pmatrix}$ and $g \in G^+$,

$$\varphi(bg) = \left|\frac{a_1}{a_2}\right|^{1/2} \chi_1(a_1)\chi_2(a_2)\varphi(g).$$

The $(\mathfrak{g}, K)$-module defined by taking $K$-finite vectors is again denoted $\pi(\chi_1, \chi_2)$.

We consider the different cases for the choices of $\chi_i$, for which we need the classification of quasi-characters on $\mathbb{R}^\times$. A quasi-character $\chi$ is necessarily of the form

$$\chi(t) = |t|^s \operatorname{sgn}(t)^\varepsilon$$

with $s \in \mathbb{C}$ and $\varepsilon \in \{0, 1\}$. For $\chi_i$ let $s_i \in \mathbb{C}$ and $\varepsilon_i \in \{0, 1\}$ denote these parameters. Let $s = s_1 - s_2$, $\varepsilon = \varepsilon_1 - \varepsilon_2 \mod 2$. These are the corresponding parameters for $\chi_1/\chi_2$.

**Theorem B.2.1.** *Let $\chi_i$ and the parameters be as above.*

- *If $\chi_1/\chi_2$ is not of the form $|t|^k \operatorname{sgn}(t)$ for a nonzero integer $k$, then $\pi(\chi_1, \chi_2)$ is an irreducible admissible $(\mathfrak{g}, K)$-module,*
- *if $\chi_1/\chi_2$ is of the form $|t|^k \operatorname{sgn}(t)$ with $k$ a positive integer, then $\pi(\chi_1, \chi_2)$ has a unique invariant submodule $\pi^k(\chi_1, \chi_2)$ with finite-dimensional quotient $\pi^f(\chi_1, \chi_2)$,*
- *if $\chi_1/\chi_2$ is of the form $|t|^k \operatorname{sgn}(t)$ with $k$ a negative integer, then $\pi(\chi_1, \chi_2)$ contains a unique finite-dimensional submodule $\pi^f(\chi_1, \chi_2)$.*

**Complex case.** The complex case is quite similar, except that we do not have the complication with connected components as $\mathrm{GL}_2(\mathbb{C})$ is connected. Recall that any quasi-character on $\mathbb{C}^\times$ is of the form

$$\chi(t) = |t|^u t^v$$

for $u, v \in \mathbb{C}$. For $\chi_1, \chi_2$ such quasi-characters, we define $\pi(\chi_1, \chi_2)$ as the $(\mathfrak{g}, K)$-module of $K$-finite vectors in the induced representation $\mathrm{Ind}_B^G \pi$.

**Proposition B.2.2.** *Let $\chi_1, \chi_2$ as above with parameters $u_1, u_2, v_1, v_2 \in \mathbb{C}$. If $\chi_1/\chi_2 \neq z^p\overline{z}^q$ for integers $p, q$ with $pq > 0$, then $\pi(\chi_1, \chi_2)$ is irreducible. Any irreducible admissible $(\mathfrak{g}, K)$-module is isomorphic to one of this type.*

The last assertion is different in the complex case than in the real case, where the nontrivial subrepresentations of $\pi(\chi_1, \chi_2)$ are not isomorphic to $\pi(\mu_1, \mu_2)$, for other quasi-characters $\mu_1$ and $\mu_2$.

## B.3 Weil Representations

Finally, we want to give a construction of cuspidal automorphic representations. The construction due to Weil is particularly interesting for potential applications in lattice-based cryptography. In fact, Weil representations are constructed using characters of a degree 2 field extension of the base field. In this way, we can relate pieces of a worst-case distribution for rank 2 lattices over $k$ to the pieces of a worst-case distribution of rank 1 lattices over an extension $L/k$ of degree 2.

As we do not need the precise details of the construction, we will only give the results.

**Non-Archimedean Case.** Let $F$ be a non-Archimedean local field of characteristic zero, $L/F$ a degree 2 field extension. Let $q$ denote the norm map $L \to F$ viewed as quadratic form. Recall that $qL^\times \subseteq F^\times$ is an index 2 subgroup, cf. [Ser79, XIII, Proposition 9]. In particular, there is a unique character $\omega\colon F^\times/qL^\times \to \mathbb{C}^\times$.

**Proposition B.3.1.** *Let $\chi$ be a (quasi-)character of $L^\times$. Then, there exists an admissible representation $\pi_\chi$ of $\mathrm{GL}_2(F)$ associated with $\chi$, such that*

- *$\pi_\chi$ is supercuspidal, if $\chi$ does not factor through $q$,*
- *$\pi_\chi = \pi(\delta, \omega \otimes \delta)$ if $\chi$ factors through $q$ via $\delta\colon F^\times \to \mathbb{C}^\times$.*

In the second case, the representation $\pi(\delta, \omega \otimes \delta)$ is the induced representation defined in Section B.1.

**Archimedean Case.** In the Archimedean case, we only need to consider $F = \mathbb{R}$ as $\mathbb{C}$ has no degree 2 field extensions. Again this splits into the two cases, whether a quasi-character $\chi\colon \mathbb{C}^\times \to \mathbb{C}^\times$ factors through the norm or not. Any quasi-characters $\chi$ of $\mathbb{C}^\times$ can be written as

$$z \mapsto (z\overline{z})^u \left(\frac{z}{|z|}\right)^n$$

for $u \in \mathbb{C}$ and $n \in \mathbb{Z}$. This factors through the norm as a character $\delta$, if and only if $n = 0$. In that case $\pi_\chi$ is the principal series representation $\pi(\delta, \mathrm{sgn} \otimes \delta)$. In the case that $\chi$ does not factor through the norm, $\pi_\chi$ is the discrete series representation for the characters $\chi_1, \chi_2$ with the properties

$$\chi_1\chi_2(x) = |x|^{2u} x^n \,\mathrm{sgn}(x)$$
$$\chi_1/\chi_2(x) = x^n \,\mathrm{sgn}(x).$$

**Global Weil representation.** In the global case let $k$ be the base field, $L$ a degree 2 extension of $k$, and $\chi$ an idèlic quasi-character. For any place $\tau$ of $L$, there is the map

$$\iota_\tau\colon L_\tau^\times \to \mathbb{G}_m(\mathbb{A}_L);\ \lambda \mapsto (\ldots, 1, \lambda, 1, \ldots)$$

where $\lambda$ is mapped to the $\tau$-th entry. Then $\chi_\tau := \chi \circ \iota_\tau$ defines a *local* quasi-character on $L_\tau^\times$ and $\chi = \otimes_\tau \chi_\tau$. This is well-defined as for any idèle $x = (x_\tau)_\tau$, $x_\tau \in \mathcal{O}_\tau^\times$ and $\chi_\tau$ is unramified for all but finitely many $\tau$. The Weil representation $\pi_\chi$ associated with $L$ and $\chi$ is defined componentwise for each place $\nu$ of $k$.

- If $\nu$ is split, i.e., there exist places $\tau_1, \tau_2$ of $L$ lying over $\nu$, then $L_{\tau_1} = k_\nu = L_{\tau_2}$ and the characters $\chi_{\tau_i}$ can be viewed as characters on $k_\nu$. Then $\pi_{\chi,\nu} \coloneqq \pi(\chi_{\tau_1}, \chi_{\tau_2})$.
- If $\nu$ is non-split, i.e., there is a unique place $\tau$ of $L$ then $L_\tau$ is a degree 2 extension of $k_\nu$, which is separable as our base field has characteristic 0. Then $\pi_{\chi,\nu}$ is defined as the Weil representation in the local case for the field extension $L_\tau$ over $k_\nu$ and quasi-character $\chi_\tau$.

The representation $\pi_\chi$ is irreducible and admissible. The main result asserts that this defines a cuspidal automorphic representation under the following assumption. Let $\mathrm{N}\colon \mathbb{G}_m(\mathbb{A}_L) \to \mathbb{G}_m(\mathbb{A}_k)$ denote the idèlic norm given by $x = (x_\tau)_{\tau \in \mathcal{P}_L} \mapsto y$ with

$$y_\nu = \begin{cases} x_{\tau_1} x_{\tau_2} & \text{if } \nu \text{ is split, } \tau_1, \tau_2 \mid \nu, \\ \mathrm{N}_{\tau/\nu}(x_\tau) & \text{if } \nu \text{ is non-split, } \tau \mid \nu \end{cases} \qquad \text{for } \nu \in \mathcal{P}_k.$$

The condition for $\pi_\chi$ to be a cuspidal representation is, whether $\chi$ factors through N or not.

**Theorem B.3.2.** *Let $L$ be a degree 2 extension of $k$ and $\chi$ an idèlic quasi-character. Then $\pi_\chi$ is a cuspidal automorphic form, if $\chi$ does not factor through the norm N, i.e., there exists no idèlic quasi-character $\overline{\chi}$ of $k$, such that $\chi = \overline{\chi} \circ \mathrm{N}$.*

This is stated as Theorem 7.11 in [Gel75]. The proof is done by comparing the respective $L$-functions. Indeed, an irreducible admissible representation $\pi$ for $\mathrm{GL}_2(\mathbb{A}_k)$ is a cuspidal automorphic form if and only if its $L$-function is bounded on vertical stripes. This property is known for $L$-functions of Hecke characters of $L$ and it is shown in [Gel75] that the $L$-functions coincide locally for each place, where $\chi$ is viewed as an character of $k$ via the norm map N defined above.

## B.4 Constructing Worst-Case Distributions in Rank 2

In this section, we want to show, how Weil representations can be used to construct cuspidal distributions for module lattices of rank 2. By Definition 5.1.1, to define a cuspidal distribution, we need to construct a collection of spherical cuspidal representations. Our basic idea is to use characters that appear in the Fourier decomposition of the worst-case distribution on ideal lattices over an extension field $L$ of $k$ of degree 2. Not all those characters yield spherical cuspidal representations so that some restrictions are needed.

Let us fix an extension $L/k$ of degree 2 and an unramified Hecke character $\chi\colon L^\times \backslash \mathbb{G}_m(\mathbb{A}_L) \to S^1$. We assume that $\chi$ is trivial on $U_{L,\infty}$, i.e., that $\chi$ factors as $\chi\colon L^\times \backslash \mathbb{G}_m(\mathbb{A}_L)/U_L \to S^1$.

**Lemma B.4.1.** *Let $\pi$ be the Weil representation associated with $\chi$. Then, for any finite place $\mathfrak{p}$ of $k$, $\pi_\tau$ is a spherical representation.*

*Proof.* The assertion is clear when $\mathfrak{p}$ splits in $L$. Suppose $\mathfrak{p}$ does not split and let $\mathfrak{q} \mid \mathfrak{p}$. We show that in this case, $\chi_\mathfrak{q}$ factors through the norm $N_{\mathfrak{q}/\mathfrak{p}}$. Let $\theta$ be a uniformizer of $\mathcal{O}_\mathfrak{q}$. We have

$$1 = \nu_\mathfrak{q}(\theta) = \frac{1}{2}\nu_\mathfrak{p}(N_{\mathfrak{q}/\mathfrak{p}}\theta),$$

hence $\nu_\mathfrak{p}(N_{\mathfrak{q}/\mathfrak{p}}\theta) = 2$. Let $u \coloneqq \chi_\mathfrak{q}(\theta) \in S^1$ and $v_1, v_2 \in S^1$ the square roots of $u$. Then $\chi_\mathfrak{q}$ factors through the norm, via the unramified characters $\chi_{\mathfrak{p},i}$ defined by sending a uniformizer $t$ of $\mathcal{O}_\mathfrak{p}$ to $u_i$, for $i = 1, 2$, respectively. As $\chi_\mathfrak{q}$ factors through the norm, we conclude that $\pi_\mathfrak{p} = \pi(\chi_{\mathfrak{p},1}, \chi_{\mathfrak{p},2})$, which is spherical as $\chi_{\mathfrak{p},i}$ are unramified. □

One sees from the proof that at the finite non-split places, all characters necessarily factor through the norm. The same holds for infinite places, as we assume that $\chi$ is trivial on the maximal compact subgroups.

**Lemma B.4.2.** *Let $\nu$ be a place of $k$ which does not split in $L$ and let $\tau$ be the unique place of $L$ over $\nu$. Then $\chi_\tau$ factors through the norm $N_{\tau/\nu}$.*

*Proof.* The case of finite places is done in the proof of the previous lemma. We assume $\nu$ is an Archimedean place, and by the assumptions, we have that $k_\nu = \mathbb{R}$ and $k_\tau = \mathbb{C}$. In this case, $\chi_\tau(z) = |z|^{iu}$ for some $u \in \mathbb{R}$. By setting $\chi_\nu(x) = |x|^{iu}$, it is clear that $\chi_\nu$ defines a character on $\mathbb{R}^\times$ via which $\chi_\tau$ factors. Note that $\chi_\nu$ is invariant under $\pm 1$, hence factors via the absolute value $\mathbb{R} \to \mathbb{R}_{>0}$. □

The characters that do not factor through the norm are easily classified as follows.

**Lemma B.4.3.** *Let $\chi$ be an unramified Hecke character of $L$. Then $\chi$ does not factor through the norm of $L/k$, if there exists a place $\nu$ of $k$ which splits into $\tau_1, \tau_2$ in $L$, such that $\chi_{\tau_1} \neq \chi_{\tau_2}$.*

*Proof.* We have seen that at all non-split places, the characters necessarily factor through the norm. Hence, the existence of a split place is necessary. Let $\nu$ be such a split place and $\tau_1, \tau_2$ the places above $\nu$. Then, $k_\nu \simeq L_{\chi_i}$, for $i = 1, 2$. The norm map at $\nu$ is given by the multiplication $m \colon k_\nu^\times \times k_\nu^\times \to k_\nu^\times$. Suppose $\omega$ is a character on $k_\nu^\times$ such that $\chi_{\tau_1} \otimes \chi_{\tau_2} = \omega \circ m$. For any $x \in k_\nu^\times$, we have that

$$\begin{aligned}
\chi_{\tau_1}(x) &= \chi_{\tau_1} \otimes \chi_{\tau_2}(x \otimes 1) \\
&= \omega \circ m(x \otimes 1) \\
&= \omega \circ m(1 \otimes x) \\
&= \chi_{\tau_1} \otimes \chi_{\tau_2}(1 \otimes x) \\
&= \chi_{\tau_2}(x),
\end{aligned}$$

using that multiplication is symmetric, which proves the claim. □

We finish with the following final remark.

*Remark* B.4.4. To construct a good class of characters, we consider the complex places only, as they are surely split in any extension. Among the unramified Hecke characters of $L$, one only needs to characterize those, such that at some complex place, the two characters in the splitting part are distinct. The characters at infinity correspond to elements in the dual $\Lambda_L^\vee$ of the unit lattice $\Lambda_L$ associated with $L$. Let $\nu$ be a complex place with places $\tau_1, \tau_2$ above $\nu$. For a character associated with $\ell \in \Lambda_L^\vee$, it the $\tau_1$ and $\tau_2$ components are distinct, if $\ell_{\tau_1} \neq \ell_{\tau_2}$. Using this fact, we can use the collection of characters, for which there exists a complex place satisfying the above property. The resulting cuspidal representations have spherical vectors $\varphi_\chi$ by Lemmas B.4.1 and B.4.2. As mentioned before, this construction does not provide any intuitive reasoning why the resulting worst-case distribution is useful for applications. Further, the abstract construction does not yield a description of the worst-case distribution as a function on the space of lattices.