Effective p-adic Ergodic Theory, Diophantine Approximation and Property (τ)

Constantin Kogler
Master Thesis
ETH Zürich

supervised by
Prof. Dr. Manfred Einsiedler

February 2020

Contents

Abstract

The principal aim of this thesis is to give an alternative proof of property (τ) for $\mathbb{Q}$-forms of SL_2, following ideas of [GGN]. One uses the circle method [HB96] to establish effective results on Diophantine approximation, which in turn imply a uniform effective mean ergodic theorem or equivalently a uniform spectral gap. We moreover give a comprehensive exposition of the involved methods from representation theory, ergodic theory and analytic number theory.

Introduction

The dynamics of homogeneous spaces has decisive influence in number theory. For instance, the reader may recall the work of Margulis [Mar] on Oppenheim's conjecture or the contribution of Einsiedler, Katok and Lindenstrauss [EKL06] on Littlewood's conjecture. On the other hand, number theoretic techniques have applications to dynamics as for example in the work of Einsiedler, Lindenstrauss, Michel and Venkatesh ([ELMV09], [ELMV11], [ELMV12]) or Einsiedler, Margulis, Mohammadi and Venkatesh ([EMV09],[EMMV19]).

This thesis is on the interface between ergodic theory and number theory. We apply effective p-adic ergodic theory to answer questions concerning Diophantine approximation. On the other hand, we use the circle method to establish results in Diophantine approximation, which in turn imply effective results in p-adic ergodic theory, culminating in an alternative proof of property (τ) for $\mathbb{Q}$-forms of SL_2. To summarize, the following diagram of ideas sketches the main themes of this thesis.

$$\begin{array}{c} \text{Property } (\tau) \\ \Updownarrow \\ \text{Uniform Effective } p\text{-adic Mean Ergodic Theorem} \\ \Updownarrow \\ \text{Uniform Diophantine Approixmation} \\ \Uparrow \\ \text{Circle Method} \end{array}$$

In order to contextualize this thesis, we briefly review the recent results of [EMMV19]. Namely, they proved an effective adelic equidistribution statement for semisimple algebraic groups over number fields by using property (τ). Moreover, their method gives an independent and dynamical proof of property (τ) for groups whose absolute rank is ≥ 2. For these groups one can use property (T) at suitable places to establish the latter effective equidistribution statement which then readily implies property (τ).

$$\begin{array}{c} \text{Property } (\tau) \\ \Updownarrow \\ \text{Uniform Effective Adelic Equidistribution Theorem} \\ \Uparrow \\ \text{Property } (T) \text{ for Groups with Absolute Rank} \geq 2. \end{array}$$

In the next paragraphs, we give a more detailed exposition of some central parts of this thesis. Let p be a prime number. A principal aim is to understand the density of $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ in $\mathrm{SL}_2(\mathbb{R})$. More precisely, we want to quantify how many prime powers of p are necessary to approximate a given element of $\mathrm{SL}_2(\mathbb{R})$

well. More generally, the same question can be raised for the ℓ-congruence subgroups $\Gamma_{p,\ell}$ of $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ for ℓ coprime to p.

The $|\cdot|_p$-norm on $\mathbb{Q}$ is defined for a rational number of the form $x = p^n \frac{a}{b} \in \mathbb{Q}$ for $n \in \mathbb{Z}$ and a, b coprime to p as $|x|_p = |p^n \frac{a}{b}|_p = p^{-n}$. In vague terms, $|\cdot|_p$ measures how often the prime number p appears in the denominator of x. We thus want to understand for an element $g \in \mathrm{SL}_2(\mathbb{R})$ how large all of the $|\cdot|_p$-norms of the coefficients of an element $\gamma \in \Gamma_{p,\ell}$ must be so that γ is very close to g.

At first sight, the question at hand seems unrelated to homogeneous dynamics. Nonetheless, if one enlarges the group $\mathrm{SL}_2(\mathbb{R})$ to the product group $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$, then $\Gamma_{p,\ell}$, viewed as a diagonally embedded subgroup of $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$, is a lattice. Using the latter setting, Diophantine approximation of $\Gamma_{p,\ell}$ in $\mathrm{SL}_2(\mathbb{R})$ can equivalently be formulated as a condition on the behavior of certain $\mathrm{SL}_2(\mathbb{Q}_p)$-orbits in the homogeneous space

$$(\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p))/\Gamma_{p,\ell}. \tag{0.1}$$

This homogeneous space is referred to as the p-adic extension of $\mathrm{SL}_2(\mathbb{R})/\Gamma_\ell$, where Γ_ℓ the ℓ-congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Property (τ) for SL_2 implies a uniform effective mixing rate for the collection of all $\mathrm{SL}_2(\mathbb{Q}_p)$-measure preserving systems of the form (0.1). This can be used to establish an effective mean ergodic theorem, which in turn implies a uniform rate of Diophantine approximation for all the congruence subgroups $\Gamma_{p,\ell}$. This is work by [GGN13].

Furthermore, given $x \in \mathrm{SL}_2(\mathbb{R})$ one can ask how many elements of $\gamma \in \Gamma_{p,\ell}$ are ε-close to x. Write for convenience $\Gamma = \Gamma_{p,\ell}$ and for $h > 0$ denote $\Gamma_h = \{\gamma \in \Gamma : ||\gamma||_p \leq h\}$ for $||\cdot||_p$ a suitable norm on $\mathrm{SL}_2(\mathbb{Q}_p)$. In particular, we aim towards effective estimates of

$$|\Gamma_h \cap B_\varepsilon(x)| \tag{0.2}$$

as $h \to \infty$. Such estimates can again be achieved by using the effective mean ergodic theorem. Remarkably so, the converse also holds. Namely, effective estimates of (0.2) imply a mean ergodic theorem which in turn also implies a uniform effective mixing rate. Thus, in order to give an independent proof of effective mixing for the dynamical systems in question, one needs an independent proof of (0.2).

This is precisely where the circle method comes into play. In fact, [HB96] gives results on the number of solutions of quadratic forms in four variables. The link to our current setting comes from noting that one can view the determinant on $\mathrm{M}_{2,2}(\mathbb{R}) \cong \mathbb{R}^4$ as a quadratic form in four variables. In this context, the quantity (0.2) can be expressed as the number of integer matrices with a congruence condition so that the determinant of the latter integer matrix is h^2. The results of [HB96] then lead to effective estimates of (0.2).

In order to prove property (τ) for $\mathbb{Q}$-forms of SL_2, the reader may observe that all of the above holds if $\mathrm{M}_{2,2}$ is replaced by a quaternion algebra B over $\mathbb{Q}$. Then SL_2 is replaced by the elements of unit norm of B. By using the norm quadratic form instead of the determinant, uniform effective estimates of (0.2) can again be established by [HB96].

We next comment on the organization of this thesis. In chapter 1, we discuss $\mathrm{SL}_2(\mathbb{Q}_p)$ and its p-adic extension. Moreover, quaternion algebras are discussed in sufficient detail. Chapters 2 and 3 are devoted to developing the necessary background from the theory of unitary representations. Then, in chapter 4, the results from chapters 2 and 3 are exploited in order to deduce effective ergodic theorems. In chapter 5 we apply the developed theory to deduce results on Diophantine approximation as in [GGN13]. In addition, following [GGN], we explain how results established by the circle method are used to deduce a spectral gap. Finally, chapters 6 and 7 are devoted to the circle method. In chapter 6 we expose the Hardy-Littlewood asymptotic formula for Waring's problem. Then, in chapter 7, we present the results by [HB96] and apply them to quaternion algebras.

Acknowledgments

First and foremost, I sincerely thank Manfred Einsiedler for suggesting the topic and for generosity with his time. I also want to take the opportunity to express my gratitude to him and his collaborator Tom Ward for their expository efforts from which I have profited during the last couple of years. Second, I thank Alex Gorodnik for making the unpublished preprint [GGN] available and for answering several questions related to it. Finally, I thank Ole Ossen for discussions concerning algebraic aspects of this thesis and Nicholas Dykeman for proofreading.

Constantin Kogler,
Zurich, February 2020

Notation and Conventions

Most of the below notations and convention will be introduced throughout this thesis, yet we assume it to be useful for the reader to collect them here.

We write $\ll$ or $\gg$ if two quantities are $\leq$ or $\geq$ up a constant, which might depend on some quantities that are usually indexed in $\ll$ or $\gg$. We also write $A \asymp B$ if $A \ll B \ll A$. If the quantity A is complex valued then the notation $A \ll B$ is a defined as $|A| \ll B$.

The notation $e(\alpha)$ is used for $e^{2\pi i\alpha}$. For $x \in \mathbb{R}$, we write $||x|| = \min_{z\in\mathbb{Z}} |x-z|$ and we denote by $[x]$ the integer part of x and by $\{x\}$ the fractional part.

By a group G we mean a locally compact, Hausdorff group and for convenience assume that G is σ-compact and metric. A left Haar measure is denoted by m_G and if we speak of a Haar measure, we refer to a left Haar measure. The corresponding L^p-space with respect to any Haar measure is written as $L^p(G)$. If $\Gamma < G$ is a lattice in G and $X = G/\Gamma$, then we denote by $L^p(X)$ the L^p-space on X with respect to the Haar probability measure on X induced by G.

A Hilbert space $\mathscr{H}$ is assumed be complex and separable, unless stated otherwise. A unitary representation $(\pi, \mathscr{H})$ of a group G is always continuous, i.e. $G \times \mathscr{H} \to \mathscr{H}$ is a continuous map. For $v, w \in \mathscr{H}$ we write $\varphi^{\pi}_{v,w}$ for the **matrix coefficient**, i.e. the function

$$\varphi^{\pi}_{v,w} : G \longrightarrow \mathbb{C}, \qquad g \longmapsto \langle \pi_g v, w\rangle.$$

The diagonal matrix coefficients $\varphi^{\pi}_{v,v}$ will also be written as φ^{π}_{v}. The space of all diagonal matrix coefficients of all unitary representations of G is denoted as $\mathscr{P}(G)$ and the reader may recall that $\mathscr{P}(G)$ is precisely the space of continuous positive definite functions on G.

We say that a unitary representation $(\pi, \mathscr{H})$ is **tempered** if it is weakly contained in the regular representation. For $(\pi, \mathscr{H})$ a unitary representation of G and $q \in [2, \infty]$, we say that $(\pi, \mathscr{H})$ is q-integrable if there exists a dense set of vectors $V \subset \mathscr{H}_G^{\perp}$ such for all $v, w \in V$ the matrix coefficients $\varphi^{\pi}_{v,w}$ satisfy $\varphi^{\pi}_{v,w} \in L^q(G)$. We define the **almost integrability exponent** $q(\pi) \in [2, \infty]$ as

$$q(\pi) = \inf\{q \in [2, \infty] \,:\, \pi \text{ is } q\text{-integrable}\}.$$

A **measure preserving system** or a G**-system** consists of a group G acting on a space X preserving a probability measure μ and is denoted as the triple (G, X, μ). To such a G-system one associates the **Koopman representation** on $L^2_\mu(X)$ given by

$$(\pi_g f)(x) = f(g^{-1}.x)$$

for $f \in L^2_\mu(X)$, $g \in G$ and $x \in X$. In this setting $L^2_0(X)$ denotes the subspace $\{f \in L^2_\mu(X) \,:\, \mu(f) = \int f \, d\mu = 0\}$.

An algebraic group G is assumed to be a simply connected, almost simple algebraic group over the rational numbers, unless stated otherwise. By using the font G we always mean a group object in the category schemes, whereas G is reserved for groups such as $\mathrm{G}(\mathbb{Q}_p)$ for p a place of $\mathbb{Q}$.

Denote by $\mathrm{B}_{a,b}$ the quaternion algebra associated to $a, b \in \mathbb{Q}^{\times}$. To be precise, if we write $\mathrm{B}_{a,b}$ we refer to the affine scheme $\mathbb{A}^4$ equipped with the corresponding algebra structure. For a quadratic form Q over $\mathbb{Q}$, we denote by O_Q and SO_Q the orthogonal respectively special orthogonal group scheme associated to Q.

For an algebraic group G as above, we write $G_\infty = \mathrm{G}(\mathbb{R})$ and for a prime p, $G_p = \mathrm{G}(\mathbb{Q}_p)$. The group G_p has an Iwasawa decomposition $G_p = K_p B_p$, where we assume that K_p is a maximal compact subgroup and B_p an associated minimal parabolic. We moreover assume that $\mathrm{G}(\mathbb{Z}_p) \subset K_p$ so that for almost all primes p, $\mathrm{G}(\mathbb{Z}_p) = K_p$.

We moreover denote by m_∞ the Haar measure on G_∞ which is normalized so that $m_\infty(\mathrm{G}(\mathbb{R})/\mathrm{G}(\mathbb{Z})) = 1$. For a prime p, we denote by m_p the Haar measure on G_p that satisfies $m_p(K_p) = 1$. For a place p of $\mathbb{Q}$, we denote by m_p^{Tam} the Tamagawa measure on $\mathrm{G}(\mathbb{Q}_p)$ induced by a fixed gauge form.

For such an algebraic group G, we denote by Γ_ℓ the ℓ-congruence subgroup of $\mathrm{G}(\mathbb{R})$. For p a prime number and ℓ a number coprime to p, we denote by $\Gamma_{p,\ell}$ the ℓ-congruence subgroup of $\mathrm{G}(\mathbb{Z}[\frac{1}{p}])$ and by $X_{p,\ell}$ the homogeneous space

$$(\mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p))\big/\Gamma_{p,\ell},$$

where $\Gamma_{p,\ell}$ is diagonally embedded. We denote by $\pi_{p,\ell}$ the unitary representation of $\mathrm{G}(\mathbb{Q}_p)$ on $L^2(X_{p,\ell})$ given by multiplication in the second coordinate.

Moreover, we write

$$X_{\mathbb{A}} = \mathrm{G}(\mathbb{A})\big/\mathrm{G}(\mathbb{Q})$$

and denote by π_p the corresponding representation of $\mathrm{G}(\mathbb{Q}_p)$ on $L^2(X_{\mathbb{A}})$.

1 The p-adic and the Adelic Extension

Before starting to develop the theory, we allude to a geometric view of the p-adic extension. The reader may recall that the transitive action of $\mathrm{SL}_2(\mathbb{R})$ on the upper half plane $\mathbb{H}$ by fractional linear transformations allows one to regard $\mathrm{SL}_2(\mathbb{R})$ as the unit tangent bundle of $\mathbb{H}$. Analogously, in intuitive terms, one could say that $\mathrm{SL}_2(\mathbb{Q}_p)$ is the *unit tangent bundle* of the $(p+1)$-regular tree. More precisely, the subgroup $\mathrm{SL}_2(\mathbb{Z}_p)$ is a maximal compact subgroup and the quotient $\mathrm{SL}_2(\mathbb{Q}_p)/\mathrm{SL}_2(\mathbb{Z}_p)$ has a structure closely related to a $(p+1)$-regular tree.[1]

Figure 1: $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$

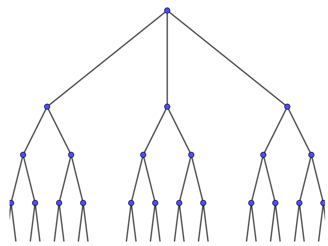

Figure 2: $\mathrm{SL}_2(\mathbb{Q}_2)/\mathrm{SL}_2(\mathbb{Z}_2)$

From this viewpoint, the product group $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$ can be visualized as a upper half plane where to each point one attaches a $(p+1)$-regular tree. The p-adic extension is then a finite volume folding of the latter space. Moreover, with this image in mind, the $\mathrm{SL}_2(\mathbb{Q}_p)$ action at a point corresponds to traveling further down along the tree-part of that point.

In this chapter, we first give a detailed exposition of properties of $\mathrm{SL}_2(\mathbb{Q}_p)$ and of the p-adic extension for SL_2. Then, in chapter 1.2, we treat general algebraic groups and discuss examples of particular importance. Finally, in chapter 1.3 the adeles are exposed as well as and the adelic points of algebraic groups.

1.1 The p-adic Extension of SL_2

Let p be a prime number and denote by $\mathbb{Q}_p$ the p-adic numbers, i.e. the completion of $\mathbb{Q}$ with respect to the p-norm $|\cdot|_p$. Recall that the p-adic integers are given by

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

The Lie group $\mathrm{SL}_2(\mathbb{R})$ is equipped with the norm

$$||g|| = ||g||_\infty = \max_{1 \leq i,j \leq 2} |g_{ij}|$$

with $g \in \mathrm{SL}_2(\mathbb{R})$ and for $g \in \mathrm{SL}_2(\mathbb{Q}_p)$ we set

$$||g|| = ||g||_p = \max_{1 \leq i,j \leq 2} |g_{ij}|_p.$$

Write $K_p = \mathrm{SL}_2(\mathbb{Z}_p)$.

[1] In fact the quotient $\mathrm{SL}_2(\mathbb{Q}_p)/\mathrm{SL}_2(\mathbb{Z}_p)$ can be viewed as the subtree of the $(p+1)$-regular tree consisting of all vertices of even distance of a fixed starting vertex.

Lemma 1.1. *The norm $||\cdot||$ on $\mathrm{SL}_2(\mathbb{Q}_p)$ is submultiplicative and bi-K_p-invariant.*

Proof. The first claim easily follows as the norm is non-archimedean. For the second claim we exploit the property that

$$|a+b|_p = \max\{|a|_p, |b|_p\} \tag{1.1}$$

if $|a|_p \neq |b|_p$. It suffices to prove left-K_p-invariance as this implies right-K_p-invariance by noticing $||g|| = ||g^{-1}||$ since $g \in \mathrm{SL}_2(\mathbb{Q}_p)$.

Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Q}_p)$ and $k = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in K_p$. Then either x or z must be an element of $\mathbb{Z}_p^\times$ as otherwise $\det(k) \neq 1$. In the following we assume $|a|_p = ||g||$ and $|x|_p = 1$ and omit the other cases as they are analogous. We calculate

$$kg = \begin{pmatrix} xa+yc & xb+yd \\ za+wc & zb+wd \end{pmatrix}.$$

If $|c|_p < |a|_p$ or $|y|_p < 1$, then by (1.1), one concludes $||kg|| = |a|_p = ||g||$. Thus we assume $|c|_p = |a|_p$ and $|y|_p = 1$. Then it follows that

$$1 = |1|_p = |xw - yz|_p \leq \max\{|xw|_p, |yz|_p\} = \max\{|w|_p, |z|_p\} \leq 1.$$

If either $|w|_p < 1$ or $|z|_p < 1$, then it again follows by (1.1) that $||kg|| = |a|_p = ||g||$. Thus it remains to deal with the case $1 = |x|_p = |y|_p = |z|_p = |w|_p$.

Write $a = p^n \mathbb{Z}_p^\times$ for $n \in \mathbb{Z}$. If $|xa+yc|_p = |a|_p = p^{-n}$, then we are done. Thus assume that this is not the case. Since clearly $|xa+yc|_p \leq |a|_p$, we can express $xa+yc$ as

$$xa + yc = h \in p^m \mathbb{Z}_p$$

for $m > n$. Using that $1 = xw - zy$ and $yc = h - xa$, it follows that

$$\begin{aligned} za + wc &= za + \left(\frac{1+zy}{x}\right) c \\ &= za + \frac{c}{x} + \frac{zyc}{x} \\ &= za + \frac{c}{x} + \frac{z(h-xa)}{x} \\ &= \frac{c}{x} + \frac{zh}{x}. \end{aligned}$$

Thus since $|x|_p = |z|_p = 1$,

$$|za+wc|_p = \left|\frac{c}{x} + \frac{zh}{x}\right|_p = \left|\frac{c}{x}\right|_p = |c|_p = |a|_p,$$

where we used (1.1) as $|\frac{zh}{x}|_p = |h|_p \leq p^{-m} < p^{-n} = |\frac{c}{x}|_p$. This finally shows $||kg|| = |a|_p = ||g||$. □

It will be useful to have two decompositions of the group $\mathrm{SL}_2(\mathbb{Q}_p)$. We further introduce the notation

$$A_p^+ = \left\{ \begin{pmatrix} p^n & 0 \\ 0 & p^{-n} \end{pmatrix} : n \in \mathbb{Z}_{\geq 0} \right\}$$

and

$$B_p = \{\text{upper trangular matrices in } \mathrm{SL}_2(\mathbb{Q}_p)\}.$$

Lemma 1.2. *(Iwasawa decomposition and Cartan Decomposition) We have an Iwasawa decomposition*

$$\mathrm{SL}_2(\mathbb{Q}_p) = K_p B_p$$

and a Cartan decomposition

$$\mathrm{SL}_2(\mathbb{Q}_p) = K_p A_p^+ K_p,$$

where the element of A_p^+ is uniquely determined by $g \in \mathrm{SL}_2(\mathbb{Q}_p)$.

Proof. Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Q}_p)$. For the Iwasawa decomposition assume first that $|a|_p \geq |c|_p$. As $\det(g) = 1$, $|a|_p > 0$ and so in particular $a \neq 0$. Then an Iwasawa decomposition is given as

$$g = \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in K_p B_p.$$

On the other hand if $|a|_p \leq |c|_p$ then

$$g = \begin{pmatrix} \frac{a}{c} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix} \in K_p B_p$$

is an Iwasawa decomposition.

To prove the Cartan decomposition, assume without loss of generality, upon left and right multiplication by the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, that

$$|a|_p = \max\{|a|_p, |b|_p, |c|_p, |d|_p\}.$$

Then as a has maximal p-norm, one can use matrices from K_p, which perform the operation of row and and column reduction, to turn g into a diagonal matrix. In particular, there are matrices $k_1, k_2 \in K_p$ so that

$$k_1 g k_2 = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Choose $m \in \mathbb{Z}$ so that $|a|_p = p^m$ and note

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} p^m & 0 \\ 0 & p^{-m} \end{pmatrix} \begin{pmatrix} \frac{a}{|a|_p} & 0 \\ 0 & \frac{|a|_p}{a} \end{pmatrix}.$$

Thus the Cartan decomposition follows from the observation

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} p^m & 0 \\ 0 & p^{-m} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p^{-m} & 0 \\ 0 & p^m \end{pmatrix}.$$

Finally, uniqueness of the element of A_p^+ follows by bi-K_p-invariance of the norm. $\square$

Lemma 1.3. *The subset $\mathrm{SL}_2(\mathbb{Z}_p) \subset \mathrm{SL}_2(\mathbb{Q}_p)$ is a maximal compact subgroup.*

Proof. The subgroup property follows as $|\cdot|_p$ is non-archimedean. In order to prove that $\mathrm{SL}_2(\mathbb{Z}_p)$ is maximal compact, consider a subgroup $H < \mathrm{SL}_2(\mathbb{Q}_p)$ with $\mathrm{SL}_2(\mathbb{Z}_p) \subsetneq H$. Then there is an element $h = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in H$ where at least one of the coefficients has p-norm > 1. By the Cartan decomposition, there are matrices $k_1, k_2 \in K$ with

$$\begin{pmatrix} p^m & 0 \\ 0 & p^{-m} \end{pmatrix} = k_1 h k_2 \in H$$

for $m \geq 1$. In particular H contains the matrices

$$\begin{pmatrix} p^{nm} & 0 \\ 0 & p^{-nm} \end{pmatrix}$$

for all $n \geq 1$ which implies that H is non-compact and $\mathrm{SL}_2(\mathbb{Z}_p)$ is maximal compact. □

Lemma 1.4. *The diagonally embedded subgroup* $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) < \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$ *is a lattice.*

Proof. We use that $\mathrm{SL}_2(\mathbb{Z}) < \mathrm{SL}_2(\mathbb{R})$ is a lattice. Hence there is some $\varepsilon > 0$ with $B_\varepsilon(e) \cap \mathrm{SL}_2(\mathbb{Z}) = \{e\}$, where we define

$$B_\varepsilon(e) = \{g \in \mathrm{SL}_2(\mathbb{R}) \,:\, ||g - e||_\infty < \varepsilon\}.$$

Observe that if $\gamma \in \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ satisfies $(\gamma, \gamma) \in B_\varepsilon(e) \times \mathrm{SL}_2(\mathbb{Z}_p)$, then $||\gamma||_p \leq 1$ yielding $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and hence in particular $\gamma = e$ by our choice of ε. This shows that $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) < \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$ is discrete. Moreover, the same argument can also be used to show that the orbit $(\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Z}_p))\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ is isomorphic to $(\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Z}_p))/\mathrm{SL}_2(\mathbb{Z})$, where the map is given by

$$(g_\infty, g_p)\mathrm{SL}_2(\mathbb{Z}[\tfrac{1}{p}]) \mapsto (g_\infty, g_p)\mathrm{SL}_2(\mathbb{Z}).$$

By this observation, in order to prove that $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ is a lattice, it suffices to show $\mathrm{SL}_2(\mathbb{Q}_p) = \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])\mathrm{SL}_2(\mathbb{Z}_p)$, which is clear as $\mathbb{Z}[\frac{1}{p}] \subset \mathbb{Q}_p$ is dense and $\mathrm{SL}_2(\mathbb{Z}_p)$ is an open subgroup. In particular, it follows that if $F \subset \mathrm{SL}_2(\mathbb{R})$ is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z}) < \mathrm{SL}_2(\mathbb{R})$, then $F \times \mathrm{SL}_2(\mathbb{Z}_p)$ is a surjective domain for $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) < \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$. □

As $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ is a lattice in $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$, we can equip the homogeneous space

$$X_p = (\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p))/\mathrm{SL}_2(\mathbb{Z}[\tfrac{1}{p}])$$

with a Haar probability measure m_{X_p}. The space X_p is referred to as the p-adic extension of $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$.

Multiplying on the left induces a natural action of $\mathrm{SL}_2(\mathbb{Q}_p)$ on X_p. More precisely, if $x = (g_\infty, g_p)\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) \in X$ and $g \in \mathrm{SL}_2(\mathbb{Q}_p)$ we set

$$g.x = (g_\infty, gg_p)\mathrm{SL}_2(\mathbb{Z}[\tfrac{1}{p}]).$$

Proposition 1.5. *The* $\mathrm{SL}_2(\mathbb{Q}_p)$ *action on* X_p *is ergodic.*

Proof. We write $u_\infty(x) = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ for $x \in \mathbb{R}$ and $u_p(x) = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ with $x \in \mathbb{Q}_p$. For $r \in \mathbb{Q}$ we denote $u(r) = u_\infty(r) \times u_p(r)$. We claim that

$$(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \times u_p(\mathbb{Q}_p)) \cdot u(\mathbb{Z}[\tfrac{1}{p}]) \subset u_\infty(\mathbb{R}) \times u_p(\mathbb{Q}_p)$$

is dense. To prove this, it suffices to show that for each tuple $(r_\infty, r_p) \in \mathbb{R} \times \mathbb{Q}_p$, there is $\gamma \in \mathbb{Z}[\frac{1}{p}]$ and $q \in \mathbb{Q}_p$ so that $|r_\infty - \gamma| \le p^{-n}$ and $|r_p - (\gamma + q)|_p \le p^{-n}$ for any n. As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we assume without loss of generality that $r_p = \frac{a}{b} \in \mathbb{Q}$. Then choose $m \in \mathbb{Z}$ so that $\gamma = \frac{m}{p^n}$ satisfies the former inequality. The latter inequality is then achieved by setting $q = -\frac{m}{p^n} + \frac{a}{b} + p^n \in \mathbb{Q} \subset \mathbb{Q}_p$. The same argument also works with matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$.

To prove ergodicity, consider a $\mathrm{SL}_2(\mathbb{Q}_p)$-invariant measurable function $f : X_p \to \mathbb{C}$. The function f lifts to an $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$-invariant function on $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$, which we again denote by f. As SL_2 is generated by $\{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)\}$, it follows by the above claim that f is invariant under a dense subset of $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$. Recalling that every Borel measurable function that is invariant under a dense subset is constant, the statement follows. □

If ℓ is an integer coprime to p we denote by $\Gamma_{p,\ell}$ the kernel of the homomorphism

$$\mathrm{SL}_2(\mathbb{Z}[\tfrac{1}{p}]) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

which is well defined as p is invertible in $\mathbb{Z}/\ell\mathbb{Z}$. We also denote by $\Gamma_{p,0} = \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$. As the group $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is finite, it follows by the first homomorphism theorem that $\Gamma_{p,\ell}$ is a finite index subgroup of $\Gamma_{p,0}$ and hence in particular a lattice of $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)$. We furthermore write

$$X_{p,\ell} = \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{Q}_p)/\Gamma_{p,\ell},$$

where again $\Gamma_{p,\ell}$ is diagonally embedded and $\mathrm{SL}_2(\mathbb{Q}_p)$ acts by left multiplication.

Corollary 1.6. *For ℓ coprime to p, the $\mathrm{SL}_2(\mathbb{Q}_p)$ action on $X_{p,\ell}$ is ergodic.*

Proof. We use the same notation as in Proposition 1.5, however denote

$$U_{p,\ell} = \{u(\tfrac{z}{p^n}) \text{ so that } z \in \mathbb{Z} \text{ with } z \equiv 0 \mod \ell \text{ and } n \ge 0\}.$$

As in Proposition 1.5, the statement follows if we show

$$(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \times u_p(\mathbb{Q}_p)) \cdot U_{p,\ell} \subset u_\infty(\mathbb{R}) \times u_p(\mathbb{Q}_p)$$

is dense, which follows by the same argument as in Proposition 1.5 since

$$\bigcup_{n \ge 1} \frac{1}{p^n} \{z \in \mathbb{Z} : z \not\equiv 0 \mod \ell\} \subset \mathbb{R}$$

is dense. □

Finally, we discuss integration over $\mathrm{SL}_2(\mathbb{Q}_p)$. We assume in the following that the unimodular Haar measure on $\mathrm{SL}_2(\mathbb{Q}_p)$ is normalized so that $m_{G_p}(K_p) = 1$. The aim is to prove the following result.

Proposition 1.7. *For all $f \in L^1(G_p)$,*

$$\int_{G_p} f \, dm_{G_p} = \int_{K_p} f(k) \, dm_{K_p}(k) + \sum_{n \ge 1} (p+1) p^{2n-1} \int_{K_p} \int_{K_p} f(k_1 \left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right) k_2) \, dm_{K_p}(k_1) dm_{K_p}(k_2).$$

In particular, if f is bi-K_p-invariant, i.e. $f(k_1 g k_2) = f(g)$ for all $k_1, k_2 \in K_p$ and $g \in G_p$, then

$$\int_{G_p} f \, dm_{G_p} = f(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) + \sum_{n \geq 1} (p+1) p^{2n+1} f(\left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right)).$$

The key to Proposition 1.7 is to understand how $K_p \left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right) K_p$ decomposes as a disjoint union of K_p-cosets. In particular, we prove the following proposition.

Proposition 1.8. *For $n \geq 1$, there exist elements $g_{n,\ell} \in G_p$ of norm p^n for $\ell = 1, \ldots (p+1)p^{2n-1}$ so that*

$$K_p \begin{pmatrix} p^n & 0 \\ 0 & p^{-n} \end{pmatrix} K_p = \bigsqcup_{\ell=1}^{(p+1)p^{2n-1}} K_p g_{n,\ell}.$$

In particular

$$m_{G_p} \left(K_p \begin{pmatrix} p^n & 0 \\ 0 & p^{-n} \end{pmatrix} K_p \right) = (p+1) p^{2n-1}.$$

As a first step, we treat the case $n = 1$.

Lemma 1.9. *It holds that*

$$\begin{aligned} K_p \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix} K_p = & \bigsqcup_{j=0}^{p^2-1} K_p \begin{pmatrix} p^{-1} & jp^{-1} \\ 0 & p \end{pmatrix} \\ & \sqcup \left(\bigsqcup_{j=1}^{p-1} K_p \begin{pmatrix} 1 & jp^{-1} \\ 0 & 1 \end{pmatrix} \right) \sqcup K_p \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}. \end{aligned}$$

In particular

$$m_{G_p} \left(K_p \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix} K_p \right) = (p+1)p.$$

Proof. To show that the union on the right hand side is indeed disjoint, assume first that there exist $j_1, j_2 \in \{0, \ldots, p^2 - 1\}$ so that

$$K_p \begin{pmatrix} p^{-1} & j_1 p^{-1} \\ 0 & p \end{pmatrix} = K_p \begin{pmatrix} p^{-1} & j_2 p^{-1} \\ 0 & p \end{pmatrix}.$$

Then in particular

$$\begin{aligned} \begin{pmatrix} p^{-1} & j_1 p^{-1} \\ 0 & p \end{pmatrix} \begin{pmatrix} p^{-1} & j_2 p^{-1} \\ 0 & p \end{pmatrix}^{-1} &= \begin{pmatrix} p^{-1} & j_1 p^{-1} \\ 0 & p \end{pmatrix} \begin{pmatrix} p & -j_2 p^{-1} \\ 0 & p^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & (j_1 - j_2) p^{-2} \\ 0 & 1 \end{pmatrix} \end{aligned}$$

is an element of K_p, which is the case if and only if $j_1 = j_2$. A similar argument applies to the other cases showing that indeed the union is disjoint.

The inclusion $\supset$ easily follows as for instance

$$\begin{pmatrix} p^{-1} & jp^{-1} \\ 0 & p \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \in K_p \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix} K_p.$$

It remains to show $\subset$. So let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K_p\left(\begin{smallmatrix} p & 0 \\ 0 & p^{-1} \end{smallmatrix}\right)K_p$ with $p = ||g|| = \max(|a|_p, |b|_p, |c|_p, |d|_p)$. Assume first that either a or c is an element of $p^{-1}\mathbb{Z}_p^\times$. We can assume without loss of generality upon left multiplication by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ that $a \in p^{-1}\mathbb{Z}_p$. Then

$$K_p g = K_p \begin{pmatrix} (ap)^{-1} & 0 \\ -cp & ap \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = K_p \begin{pmatrix} p^{-1} & b_1 \\ 0 & p \end{pmatrix}$$

for $b_1 = (ap)^{-1} b \in p^{-1}\mathbb{Z}_p$. Then choose $j \in \{0, \ldots p^2 - 1\}$ with $pb_1 \equiv j \bmod p^2$ implying

$$K_p \begin{pmatrix} p^{-1} & b_1 \\ 0 & p \end{pmatrix} = K_p \begin{pmatrix} 1 & \frac{-pb_1 + j}{p^2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p^{-1} & b_1 \\ 0 & p \end{pmatrix} = K_p \begin{pmatrix} p^{-1} & jp^{-1} \\ 0 & p \end{pmatrix}.$$

Next we assume that a or c is an element of $\mathbb{Z}_p^\times$ so we assume without loss of generality $a \in \mathbb{Z}_p^\times$. Thus we again have

$$K_p g = K_p \begin{pmatrix} a^{-1} & 0 \\ -\frac{c}{a} & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = K_p \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}$$

for $b_1 = a^{-1} b \in p^{-1}\mathbb{Z}_p$. This time we choose $pb_1 = j \bmod p$ for $j \in \{1, \ldots, p-1\}$, where we note that the case $j = 0$ is not possible as then $b_1 \in \mathbb{Z}_p$, which contradicts $||g|| = p$. Then as above,

$$K_p \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} = K_p \begin{pmatrix} 1 & \frac{-pb_1 + j}{p} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} = K_p \begin{pmatrix} 1 & jp^{-1} \\ 0 & 1 \end{pmatrix}.$$

Finally we treat the case where $a, c \in p\mathbb{Z}_p$. If $a, c \in p^2\mathbb{Z}_p$, then using $b, d \in p^{-1}\mathbb{Z}_p$ (which follows from $||g|| = p$) it follows $1 = \det(g) \in p\mathbb{Z}_p$, a contradiction. Thus we assume without loss of generality $a \in p\mathbb{Z}_p^\times$. Then for $b_1 = \frac{pb}{a}$,

$$\begin{aligned} K_p g &= K_p \begin{pmatrix} (\frac{a}{p})^{-1} & 0 \\ -\frac{c}{p} & \frac{a}{p} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = K_p \begin{pmatrix} p & b_1 \\ 0 & p^{-1} \end{pmatrix} \\ &= K_p \begin{pmatrix} 1 & -pb_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & b_1 \\ 0 & p^{-1} \end{pmatrix} = K_p \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}. \end{aligned}$$

□

Proof. (of Proposition 1.8) Precisely the same proof applies as the one of

Lemma 1.9. In fact, with exactly the same method one proves:

$$
\begin{aligned}
K_p \begin{pmatrix} p^n & 0 \\ 0 & p^{-n} \end{pmatrix} K_p = & \left(\bigsqcup_{j=0}^{p^{2n}-1} K_p \begin{pmatrix} p^{-n} & jp^{-n} \\ 0 & p^n \end{pmatrix} \right) \\
& \sqcup \left(\bigsqcup_{\substack{j=0 \\ p \nmid j}}^{p^{2n-1}-1} K_p \begin{pmatrix} p^{-(n-1)} & jp^{-n} \\ 0 & p^{n-1} \end{pmatrix} \right) \\
& \sqcup \left(\bigsqcup_{\substack{j=0 \\ p^2 \nmid j}}^{p^{2n-2}-1} K_p \begin{pmatrix} p^{-(n-2)} & jp^{-n} \\ 0 & p^{n-2} \end{pmatrix} \right) \sqcup \ldots \\
& \ldots \sqcup \left(\bigsqcup_{\substack{j=0 \\ p^n \nmid j}}^{p^n} K_p \begin{pmatrix} 1 & jp^{-n} \\ 0 & 1 \end{pmatrix} \right) \sqcup K_p \begin{pmatrix} p^n & 0 \\ 0 & p^{-n} \end{pmatrix}.
\end{aligned}
$$

In particular, the number of cosets of the above decomposition is

$$p^{2n} + p^{2n-1} - p^{2n-2} + p^{2n-2} - p^{2n-3} + \ldots + p^n - 1 + 1 = (p+1)p^{2n-1}.$$

□

Proof. (of Proposition 1.7) The proof is a straightforward consequence of Proposition 1.8. In fact for $f \in L^1(G)$,

$$
\begin{aligned}
\int f \, dm_{G_p} &= \sum_{n \geq 0} \int_{||g||=p^n} f \, dm_{G_p} \\
&= \int_{K_p} f(k) \, dm_{K_p}(k) + \sum_{n \geq 1} \int_{||g||=p^n} f \, dm_{G_p}.
\end{aligned}
$$

Thus we are reduced to treating the integral over $||g|| = p^n$ for a fixed n. Using unimodularity of G_p and our normalization of the Haar measure on K_p, we conclude,

$$
\begin{aligned}
\int_{||g||=p^n} f \, dm_{G_p} &= \int_{||g||=p^n} \int_{K_p} \int_{K_p} f(k_1 g k_2) \, dm_{G_p}(g) dm_{K_p}(k_1) dm_{K_p}(k_2) \\
&= \int_{||g||=p^n} \int_{K_p} \int_{K_p} f(k_1 \left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right) k_2) \, dm_{G_p}(g) dm_{K_p}(k_1) dm_{K_p}(k_2) \\
&= m_{G_p}(\{g \in G_p : ||g|| = p^n\}) \int_{K_p} \int_{K_p} f(k_1 \left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right) k_2) \, dm_{K_p}(k_1) dm_{K_p}(k_2) \\
&= (p+1)p^{2n-1} \int_{K_p} \int_{K_p} f(k_1 \left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right) k_2) \, dm_{K_p}(k_1) dm_{K_p}(k_2),
\end{aligned}
$$

where we used in the last line that $\{g \in G_p : ||g|| = p^n\} = K_p \left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right) K_p$ together with Proposition 1.8. □

1.2 Recollections from the Theory of Algebraic Groups

We first survey some definitions and results concerning algebraic groups and discuss some examples. Second, we generalize the discussion around the p-adic extension for SL_2 to general algebraic groups. We refer to [Spr98] and [PR94] for a detailed exposition of parts of the material discussed. Let F be a field.

Definition 1.10. An algebraic group G over F is called **almost simple**, if there are no non-trivial, connected, normal subgroups.

Definition 1.11. Two algebraic groups G_1 and G_2 over F are called **isogeneous** if there exists a surjective morphism defined over F of algebraic groups $\mathrm{G}_1 \to \mathrm{G}_2$ with finite kernel.

Definition 1.12. An algebraic group G over F is called **semisimple**, if one of the following two equivalent definitions hold:

1. There are no non-trivial connected, normal, solvable subgroups.
2. The group G is isogeneous to a direct product of almost simple algebraic groups over F.

Let G be a semisimple algebraic group over $\mathbb{Q}$. A further notion of importance is that of a **simply connected** group. In order to avoid introducing too much notation, we refer for the definition to [Spr98]. For our purposes it will be sufficient to note that G is simply connected if and only if $\mathrm{G}(\mathbb{C})$ is a simply connected complex Lie group.

Definition 1.13. Let G be a semisimple algebraic group over F. We say that G is **F-isotropic** if its F-rank is > 0, i.e. if G contains a non-trivial, F-split torus. The algebraic group G is called **F-anisotropic** if its F-rank is 0.

In the following we discuss an important example, which motivates the term isotropic. Let Q be a quadratic form over $\mathbb{Q}$ of degree n, i.e. a homogeneous polynomial $Q \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree 2. Let $q_{ij} \in \mathbb{Q}$ for $1 \leq i \leq j \leq n$ be the coefficients of Q, i.e.

$$Q(x) = \sum_{1 \leq i \leq j \leq n} q_{ij} x_i x_j$$

for $x = (x_1, \ldots, x_n) \in \mathbb{Q}^n$.

If we denote

$$A_Q = \frac{1}{2}\left(\begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ 0 & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & q_{nn} \end{pmatrix} + \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ 0 & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & q_{nn} \end{pmatrix}^T\right),$$

then we can write $Q(x) = x^T A_Q x$ for $x \in \mathbb{Q}^n$. We aim towards defining the special orthogonal group with respect to the quadratic form Q as an algebraic group such that

$$\begin{aligned} \mathrm{SO}_Q(\mathbb{Q}) &= \{g \in \mathrm{SL}_n(\mathbb{Q}) \,:\, Q(gx) = Q(x) \text{ for all } x \in \mathbb{Q}^n\} \\ &= \{g \in \mathrm{SL}_n(\mathbb{Q}) \,:\, g^T A_Q g = A_Q\}. \end{aligned}$$

Denote by $\{f_i, i \in I\}$ the polynomials in n^2-variables whose vanishing locus determines the equation $g^T A_Q g = A_Q$. Then we set

$$\mathrm{SO}_Q = \operatorname{Spec} \mathbb{Q}[X_1, \dots, X_{n^2}]/(\{\det -1, f_i : i \in I\}),$$

where $(\{\det -1, f_i : i \in I\})$ is the ideal generated by those polynomials. Moreover, we set

$$\mathrm{O}_Q = \operatorname{Spec} \mathbb{Q}[X_1, \dots, X_{n^2}]/(\{f_i : i \in I\}).$$

The opportunity is taken to clarify the difference between viewing SO_Q as an algebraic group over $\mathbb{Q}_p$ and to consider its $\mathbb{Q}_p$-points, where p is a place of $\mathbb{Q}$. To discuss a more general setting, let $X = \operatorname{Spec} R$ be an affine scheme over $\mathbb{Q}$ where R is a $\mathbb{Q}$-algebra. If we say that we view X over $\mathbb{Q}_p$, then we actually refer to the affine scheme

$$X = \operatorname{Spec} R \otimes_{\mathbb{Q}} \mathbb{Q}_p,$$

whereas the $\mathbb{Q}_p$ points are defined as

$$\begin{aligned} X(\mathbb{Q}_p) &= \{f : \operatorname{Spec} \mathbb{Q}_p \to \operatorname{Spec} R \otimes_{\mathbb{Q}} \mathbb{Q}_p \mid f \text{ is a morphism of affine schemes}\} \\ &= \{f : R \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathbb{Q}_p \mid f \text{ is a ring homomorphism}\}. \end{aligned}$$

Returning to our concrete case, the algebraic group SO_Q viewed over $\mathbb{Q}_p$ is the affine scheme

$$\operatorname{Spec} \mathbb{Q}_p[X_1, \dots, X_{n^2}]/(\{\det -1, f_i : i \in I\}),$$

which corresponds to viewing the quadratic form Q over $\mathbb{Q}_p$. Then

$$\begin{aligned} \mathrm{SO}_Q(\mathbb{Q}_p) &= \{\text{ring homomorphisms } \mathbb{Q}_p[X_1, \dots, X_{n^2}]/(\{\det -1, f_i : i \in I\}) \to \mathbb{Q}_p\} \\ &= \{g \in \mathrm{SL}_n(\mathbb{Q}_p) \,:\, g^T A_Q g = A_Q\}. \end{aligned}$$

Two quadratic forms Q_1 and Q_2 over $\mathbb{Q}$ are called **equivalent** if there is $C \in \mathrm{GL}_n(\mathbb{Q})$ so that $A_{Q_1} = C^T A_{Q_2} C$ or equivalently if $Q_1(v) = Q_2(Cv)$ for all $v \in \mathbb{Q}^n$. The quadratic forms Q_1 and Q_1 are **similar**, if they are equivalent up to a scalar non-zero multiple. Similarity of quadratic forms corresponds precisely to the property that SO_{Q_1} and SO_{Q_2} are isomorphic as algebraic groups, as can be shown using group cohomology (see Proposition 2.6 in chapter 2.2 of [PR94]). This observation allows us to find examples of algebraic groups that are isomorphic over $\mathbb{Q}_p$ but not over $\mathbb{Q}$ by considering two quadratic forms that are similar over $\mathbb{Q}_p$ yet not similar over $\mathbb{Q}$.

Recall that the quadratic form Q is said to be **isotropic** if there is a non-zero $v \in \mathbb{Q}^n$ so that $Q(v) = 0$. If there exists no such v, we call Q **anisotropic**. The following lemma motivates the term isotropic in the context of algebraic groups. We note that the proof of Lemma 1.14 can be extended to case of a quadratic form over any field with characteristic $\neq 2$.

Lemma 1.14. *The quadratic form Q is isotropic over $\mathbb{Q}$ if and only if SO_Q is a $\mathbb{Q}$-isotropic algebraic group.*

Proof. Assume that SO_Q is isotropic, i.e. there exists a non-trivial $\mathbb{Q}$-split torus $\mathrm{T} \subset \mathrm{SO}_Q$. Then we can find a non-trivial eigenvector $v \in \mathbb{Q}^n$ for T with a non-trivial character $\chi : \mathrm{T}(\mathbb{Q}) \to \mathbb{Q}^\times$. Thus for all $t \in \mathrm{T}(\mathbb{Q})$,

$$Q(v) = Q(tv) = Q(\chi(t)v) = \chi(t)^2 Q(v).$$

This implies $Q(v) = 0$ and Q is isotropic.

For the converse we recall that the quadratic forms $x^2 - y^2$ and xy are equivalent via the matrix

$$\begin{pmatrix} 1 & \frac{1}{4} \\ -1 & \frac{1}{4} \end{pmatrix}.$$

More generally, if Q is an isotropic quadratic form then we can replace it without loss of generality by $x_1x_2 + Q_0(x_3, \ldots, x_n)$ for Q_0 a quadratic form of degree $n - 2$. In this case

$$\mathrm{T} = \mathrm{diag}(*, *, 1, \ldots, 1) \subset \mathrm{SO}_Q \subset \mathrm{SL}_n$$

defines a non-trivial $\mathbb{Q}$-split torus. □

We next discuss ternary quadratic forms. For p a place of $\mathbb{Q}$ and $a, b, c \in \mathbb{Q}_p$, we denote by $\langle a, b, c\rangle$ the quadratic form $aX^2 + bY^2 + cZ^2$. Over $\mathbb{R}$, there are only two similarity classes of non-degenerate ternary quadratic forms. This follows as if Q is such a quadratic form, then as defined above A_Q is a symmetric matrix and hence there exists a matrix $B \in \mathrm{GL}_3(\mathbb{R})$ so that

$$B^T A_Q B = \begin{pmatrix} \alpha_1 & & \\ & \alpha_2 & \\ & & \alpha_3 \end{pmatrix}$$

for real numbers $\alpha_1 \geq \alpha_2 \geq \alpha_3$. If $C = \mathrm{diag}(\sqrt{|\alpha_1|}^{-1}, \sqrt{|\alpha_2|}^{-1}, \sqrt{|\alpha_3|}^{-1})$, then

$$C \begin{pmatrix} \alpha_1 & & \\ & \alpha_2 & \\ & & \alpha_3 \end{pmatrix} C^T$$

is equal to a matrix with only 1 and -1 on the diagonal. Thus the four triples $(1, 1, 1), (1, 1, -1), (1, -1, -1), (-1, -1, -1)$ classify the four equivalence classes of non-degenerate ternary quadratic form over $\mathbb{R}$. As the class $(1, 1, 1)$ is similar to $(-1, -1, -1)$ as well as $(1, 1, -1)$ is to $(1, -1, -1)$, it follows that there are two similarity classes of ternary quadratic forms over $\mathbb{R}$. The precisely same argument shows that there only one similarity class of ternary quadratic forms over $\mathbb{C}$.

Whereas in the real case a ternary quadratic form is determined by its signature, the situation is more subtle over the p-adic numbers. We review the discussion exposed in [Jer] or [Bay]. In analogy to the real case, however with an altered proof, one shows that each ternary quadratic form over $\mathbb{Q}_p$ is isomorphic to one of the form $\langle a, b, c\rangle$. However, we cannot proceed as before since square roots behave differently over the p-adic numbers.

Lemma 1.15. *Let p be a prime number. Then*

$$|\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2| = \begin{cases} 4 & \text{if } p \neq 2, \\ 8 & \text{if } p = 2. \end{cases}$$

Proof. This is Lemma 3.6 of [Jer]. We only discuss the case $p \neq 2$. Denote as usual $\mathbb{Z}_p^\times = \{z \in \mathbb{Z}_p : |z|_p = 1\}$. We first show $|\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2| = 2$. As $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$, we have a ring homomorphism

$$\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p.$$

Moreover, clearly $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$. We use Hensel's lemma. Let $x, z \in \mathbb{Z}_p^\times$ so that $z = x^2 \mod p$. Then consider the polynomial $f(X) = X^2 - z$ which satisfies $f(x) \equiv 0 \bmod p$ and $|f'(x)|_p = |2x|_p = 1$. Thus by Hensel's lemma, there is a root of f. This argument shows $|\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2| = |\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2| = 2$.

The claim of the lemma now follows as each p-adic number $x \in \mathbb{Q}_p^\times$ can be written uniquely in the form $x = zp^\ell$ for $z \in \mathbb{Z}_p^\times$ and $\ell \in \mathbb{Z}$. Thus $x^2 = z^2p^{2\ell}$ and so for $x \in \mathbb{Q}_p^\times$ to be a square of another number in $\mathbb{Q}_p^\times$, it has to hold that $z \in (\mathbb{Z}_p^\times)^2$ and that ℓ must be even. □

One then proves (cf. Proposition 3.13 of [Bay]), that over $\mathbb{Q}_p$ there exists precisely one anisotropic and one isotropic ternary quadratic form up to similarity. We won't give the details for this statement here, yet provide an example of an anisotropic ternary form, shedding some light on the proof of the latter statement.

Throughout the following we fix an odd prime p and an element $e \in \mathbb{Z}_p^\times \backslash (\mathbb{Z}_p^\times)^2$. We claim that the quadratic form $\langle 1, -e, -p\rangle$ is anisotropic over $\mathbb{Q}_p$. For a contradiction assume there exist $x, y, z \in \mathbb{Q}_p$ not all equal to zero that satisfy $x^2 - ey^2 - pz^2 = 0$. We assume without loss of generality that $x, y, z \in \mathbb{Z}_p$ and that at least one of them lies in $\mathbb{Z}_p^\times$. Reducing modulo p, we hence obtain $x^2 \equiv ey^2 \mod p$. If $y \in \mathbb{Z}_p^\times$, then as in the lemma above $e \in (\mathbb{Z}_p^\times)^2$, which is a contradiction. On the other hand, if $p|y$, then $p|x$ and hence $z \in \mathbb{Z}_p^\times$. It follows $p^{-1} = |pz^2|_p = |x^2 - ey^2|_p \le p^{-2}$, a contradiction. Thus indeed $\langle 1, -e, -p\rangle$ is anisotropic.

Relating to the above, we discuss quaternion algebras over $\mathbb{Q}$. Let a and b be two nonzero elements of $\mathbb{Q}$. Then we denote by

$$\mathrm{B}_{a,b}(\mathbb{Q}) = \{x_0 + x_1 i + x_2 j + x_3 k \ : \ x_0, x_1, x_2, x_3 \in \mathbb{Q}\}$$

the **quaternion algebra** over $\mathbb{Q}$ associated to a and b, where $1, i, j, k$ are variables that satisfy

$$i^2 = a, \quad j^2 = b \quad \text{and} \quad ij = k = -ji.$$

If $\alpha = x_0 + x_1 i + x_2 j + x_3 k$, then we define the conjugate of α as

$$\overline{\alpha} = x_0 - x_1 i - x_2 j - x_3 k$$

and the norm and trace of α as

$$\mathrm{Nr}(\alpha) = \alpha\overline{\alpha} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \quad \text{and} \quad \mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2x_0.$$

Observe that the norm satisfies $\mathrm{Nr}(\alpha\beta) = \mathrm{Nr}(\alpha)\mathrm{Nr}(\beta)$ for $\alpha, \beta \in \mathrm{B}_{a,b}(\mathbb{Q})$ and moreover, an element α is invertible if and only if $\mathrm{Nr}(\alpha) \neq 0$ and then

$$\alpha^{-1} = \frac{\overline{\alpha}}{\mathrm{Nr}(\alpha)} = \frac{\overline{\alpha}}{\alpha\overline{\alpha}}.$$

We want to consider $\mathrm{B}_{a,b}$ as an algebra object in category of affine schemes over $\mathbb{Q}$. In order to do so, we view $\mathrm{B}_{a,b}$ as the affine space $\mathbb{A}^4$ equipped with the morphisms of affine schemes which correspond to the algebra structure on $\mathrm{B}_{a,b}(\mathbb{Q})$.

If every non-zero element of $\mathrm{B}_{a,b}(\mathbb{Q})$ is invertible, we then say that $\mathrm{B}_{a,b}$ is a **division algebra** over $\mathbb{Q}$. For the next lemma, we note that we can also view the set of 2×2 matrices, $\mathrm{M}_{2,2}$ as an affine algebra scheme over $\mathbb{Q}$.

Lemma 1.16. *Let $a, b \in \mathbb{Q}^\times$. Then the following properties are equivalent:*

(i) $\mathrm{B}_{a,b}$ *is not a division algebra over* $\mathbb{Q}$.

(ii) The quadratic form $\langle 1, -a, -b, ab\rangle$ *is isotropic over* $\mathbb{Q}$.

(iii) The quadratic form $\langle -a, -b, ab\rangle$ *is isotropic over* $\mathbb{Q}$.

(iv) $\mathrm{B}_{a,b} \cong \mathrm{B}_{1,1} \cong \mathrm{M}_{2,2}$ *as algebra objects in the category of affine schemes over* $\mathbb{Q}$.

Proof. (i) and (ii) are equivalent as the quadratic form $\langle 1, -a, -b, ab\rangle$ is precisely the norm form on $\mathrm{B}_{a,b}(\mathbb{Q})$. For the equivalence of (ii) and (iii) we refer to [Bay] Theorem 2.33.

We next show that $\mathrm{B}_{1,1} \cong \mathrm{M}_{2,2}$. Consider the map

$$\Phi : \mathrm{B}_{1,1}(\mathbb{Q}) \longrightarrow \mathrm{M}_2(\mathbb{Q})$$

determined by

$$\Phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \Phi(i) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and

$$\Phi(j) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \Phi(k) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus for $x_0, x_1, x_2, x_3 \in \mathbb{Q}_p$,

$$\Phi(x_0 + x_1 i + x_2 j + x_3 k) = \begin{pmatrix} x_0 + x_1 & x_2 + x_3 \\ x_2 - x_3 & x_0 - x_1 \end{pmatrix}.$$

One checks that this defines a ring isomorphism with the property that for $\alpha = x_0 + x_1 i + x_2 j + x_3 k$,

$$\det(\Phi(\alpha)) = x_0^2 - x_1^2 - x_2^2 + x_3^2 = \mathrm{Nr}(\alpha).$$

This also shows that $\mathrm{B}_{1,1}$ is not a division algebra. Also (iv) implies (i) since $\mathrm{M}_{2,2}$ is not a division algebra.

Assume now that $\mathrm{B}_{a,b}$ is not a division algebra. Then choose a non-invertible and non-zero element $b \in \mathrm{B}_{a,b}(\mathbb{Q})$ and consider the proper left ideal $\mathfrak{a}$ generated by b. Then $\mathfrak{a}$ is a $\mathbb{Q}$-subspace of $\mathrm{B}_{a,b}(\mathbb{Q})$ and denote by m its $\mathbb{Q}$-dimension. Left multiplication of a fixed element in $\mathrm{B}_{a,b}(\mathbb{Q})$ gives rise to an algebra homomorphism

$$\mathrm{B}_{a,b}(\mathbb{Q}) \longrightarrow \mathrm{End}_{\mathbb{Q}}(\mathfrak{a}) \cong \mathrm{M}_{m,m}(\mathbb{Q}).$$

Observe that this algebra homomorphism is injective since $\mathrm{B}_{a,b}(\mathbb{Q})$ is a simple algebra, i.e. the only two-sided ideals are $\{0\}$ and $\mathrm{B}_{a,b}(\mathbb{Q})$. This shows $m \geq 2$ as $\dim_{\mathbb{Q}} \mathrm{B}_{a,b}(\mathbb{Q}) = 4$. The same argument applied to the non-trivial quotient algebra $\mathrm{B}_{a,b}(\mathbb{Q})/\mathfrak{a}$ shows $m \leq 2$. Hence the above map is an isomorphism. □

We denote by $\mathrm{B}^1_{a,b}$ the group scheme of norm one elements and by $\mathrm{B}^0_{a,b}(\mathbb{Q})$ the trace zero elements. Then the above lemma allows us to draw the following corollary.

Corollary 1.17. *Let $a, b \in \mathbb{Q}^\times$ and assume that $\mathrm{B}_{a,b}$ is not a division algebra. Then there exists an isomorphism of algebraic groups*

$$\mathrm{B}_{a,b}^{(1)} \longrightarrow \mathrm{SL}_2$$

over $\mathbb{Q}$.

Proof. This follows by Lemma 1.16 and its proof. □

To proceed, we consider the norm quadratic form on $\mathrm{B}_{a,b}^0(\mathbb{Q})$ with respect to the natural basis, arriving at the ternary quadratic form

$$Q_{a,b}(x,y,z) = -ax^2 - by^2 + abz^2.$$

Furthermore we discuss

$$\mathrm{PB}_{a,b}^\times = \mathrm{B}_{a,b}^\times / \mathbb{G}_m$$

the projective group of invertible quaternions so that for instance

$$\mathrm{PB}_{a,b}^\times(\mathbb{Q}) = \mathrm{B}_{a,b}^\times(\mathbb{Q})/\mathbb{Q}^\times.$$

Proposition 1.18. *There exists an isomorphism of algebraic groups over $\mathbb{Q}$,*

$$\mathrm{PB}_{a,b}^\times \longrightarrow \mathrm{SO}_{Q_{a,b}}$$

Proof. The idea is to view each element of $\mathrm{B}_{a,b}^\times$ as an element of the automorphism group of $\mathrm{B}_{a,b}^0$ preserving the quadratic form $Q_{a,b}$. For $\alpha \in \mathrm{B}_{a,b}^\times(\mathbb{Q})$ consider the automorphism

$$S_\alpha : \mathrm{B}_{a,b}(\mathbb{Q}) \longrightarrow \mathrm{B}_{a,b}(\mathbb{Q}), \qquad \beta \longmapsto \alpha\beta\alpha^{-1}.$$

As the norm is multiplicative, S_α preserves the norm. We claim that $S_\alpha(\mathrm{B}_{a,b}^0(\mathbb{Q})) = \mathrm{B}_{a,b}^0(\mathbb{Q})$. To see this let $\alpha = x_1 i + x_2 j + x_3 k \in \mathrm{B}_{a,b}^0(\mathbb{Q})$. By $\mathbb{Q}$-linearity of S_α it suffices to check that $\alpha i \overline{\alpha}$, $\alpha j \overline{\alpha}$ and $\alpha k \overline{\alpha}$ are all elements of $\mathrm{B}_{a,b}^0(\mathbb{Q})$. This follows as

$$\begin{aligned} k^2 &= -ijji = -ab, \\ ik &= iij = aj, \\ jk &= -jji = -bi, \\ ki &= -jii = -aj, \\ kj &= ijj = bi \end{aligned}$$

and

$$\begin{aligned} \alpha i \overline{\alpha} &= (x_0 + x_1 i + x_2 j + x_3 k) i (x_0 - x_1 i - x_2 j - x_3 k) \\ &= (x_0 i + x_1 i^2 + x_2 ji + x_3 ki)(x_0 - x_1 i - x_2 j - x_3 k) \\ &= (x_0 i + a x_1 - x_2 k - a x_3 j)(x_0 - x_1 i - x_2 j - x_3 k) \\ &= (-a x_0 x_1 + a x_0 x_1 - ab x_2 x_3 + ab x_2 x_3) + (\ldots) i + (\ldots) j + (\ldots) k \\ &= 0 + (\ldots) i + (\ldots) j + (\ldots) k \end{aligned}$$

showing $\alpha i\overline{\alpha} \in \mathrm{B}^0_{a,b}(\mathbb{Q})$. One analogously checks that $\alpha j\overline{\alpha}, \alpha k\overline{\alpha} \in \mathrm{B}^0_{a,b}(\mathbb{Q})$ which implies $S_\alpha(\mathrm{B}^0_{a,b}(\mathbb{Q})) \subset \mathrm{B}^0_{a,b}(\mathbb{Q})$. The claim follows as α is replaced by its inverse.

As S_α is $\mathbb{Q}$-linear, we can view it as a matrix by identifying $\mathrm{B}^0_{a,b}(\mathbb{Q})$ as the $\mathbb{Q}$-span of i, j, k. More precisely, if

$$\begin{aligned} S_\alpha(i) &= a_{11}i + a_{21}j + a_{31}k, \\ S_\alpha(j) &= a_{12}i + a_{22}j + a_{32}k, \\ S_\alpha(k) &= a_{13}i + a_{23}j + a_{33}k, \end{aligned}$$

then we view S_α as the matrix

$$M_{S_\alpha} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

As S_α preserves the norm, it follows

$$Q_{a,b}(S_\alpha(\beta)) = \mathrm{Nr}(S_\alpha(\beta)) = \mathrm{Nr}(\beta) = Q_{a,b}(\beta)$$

and thus

$$M_{S_\alpha} \in \mathrm{O}_{Q_{a,b}}(\mathbb{Q}).$$

Finally as $S_{\alpha_1\alpha_2} = S_{\alpha_1} \circ S_{\alpha_2}$ for all $\alpha_1, \alpha_2 \in \mathrm{B}^0_{a,b}(\mathbb{Q})$, we hence have arrived at a group homomorphism

$$\mathrm{B}^\times_{a,b}(\mathbb{Q}) \longrightarrow \mathrm{O}_{Q_{a,b}}(\mathbb{Q}), \qquad \alpha \longmapsto M_{S_\alpha},$$

which only depends on $[\alpha] \in \mathrm{PB}^\times_{a,b}$ and hence induces a group homomorphism

$$\mathrm{PB}^\times_{a,b}(\mathbb{Q}) \longrightarrow \mathrm{O}_{Q_{a,b}}(\mathbb{Q}), \qquad \alpha \longmapsto M_{S_\alpha}.$$

It remains to check that the map is onto $\mathrm{SO}_{Q_{a,b}}$, for which we refer to Lemma 2.4 of [Ber16]. In essence, the claim follows as $\mathrm{SO}_{Q_{a,b}}$ is generated by even reflections. □

Corollary 1.19. *For $a, b \in \mathbb{Q}^\times$, the algebraic group $\mathrm{B}^1_{a,b}$ is anisotropic over $\mathbb{Q}_p$ if and only if the quadratic form $Q_{a,b}$ is anisotropic over $\mathbb{Q}_p$.*

Proof. This follows directly from last proposition as $\mathrm{B}^1_{a,b}$ can be viewed as a double cover of $\mathrm{PB}^\times_{a,b}$. □

Definition 1.20. The algebraic groups $\mathrm{G} = \mathrm{B}^1_{a,b}$ for $a, b \in \mathbb{Q}^\times$ are called the **$\mathbb{Q}$-forms of** SL_2.

We return to the general case of a linear algebraic group $\mathrm{G} \subset \mathrm{GL}_n$ over F, yet restrict in the discussion below to the case where F is a local field of characteristic zero and $\mathrm{G} \subset \mathrm{GL}_n$ is semisimple. The theory reviewed in this paragraph can be found for instance in [BT72]. Denote the F-points as $G = \mathrm{G}(F)$. The group G has an **Iwasawa decomposition**, i.e. there exists a maximal compact subgroup $K \subset G$, and a corresponding minimal parabolic $B \subset G$ so that $G = KB$. If A is a suitable abelian subgroup we also have a Cartan decomposition

$$G = KAK$$

so that for all $a \in A$,

$$a^{-1} = k_1 a k_2, \tag{1.2}$$

for some $k_1, k_2 \in K$.

Lemma 1.21. *Let* $\mathrm{G} \subset \mathrm{GL}_n$ *be a semisimple algebraic group over* $\mathbb{Q}$ *and* p *a prime number. Then the diagonally embedded subgroup* $\mathrm{G}(\mathbb{Z}[\frac{1}{p}]) < \mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p)$ *is a lattice.*

Proof. As the class number of G is finite (see [PR94] chapter 5), there exist $x_1, \ldots, x_n \in \mathrm{G}(\mathbb{Q}_p)$ so that

$$\mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p) = \bigcup_{i=1}^{n} (\mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Z}_p)) x_i \mathrm{G}(\mathbb{Z}_p).$$

Denote $C = \bigcup_{i=1}^{r} \mathrm{G}(\mathbb{Z}_p) x_i \mathrm{G}(\mathbb{Z}_p)$ and observe that C is compact. Thus if $F \subset \mathrm{G}(\mathbb{R})$ is a fundamental domain for $\mathrm{G}(\mathbb{Z})$ then $F \times C$ is a finite volume surjective domain for $\mathrm{G}(\mathbb{Z}[\frac{1}{p}]) < \mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p)$. $\square$

In analogy to chapter 1.1, write

$$X_p = \mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p) / \mathrm{G}(\mathbb{Z}[\tfrac{1}{p}]),$$

equipped with the Haar probability measure m_{X_p}. Set $G_p = \mathrm{G}(\mathbb{Q}_p)$. Then G_p acts on X_p by left multiplication.

Proposition 1.22. *Let* $\mathrm{G} \subset \mathrm{GL}_n$ *be a simply connected, almost simple algebraic group over* $\mathbb{Q}$ *and* p *a prime number. The action of* G_p *on* X_p *is ergodic.*

Proof. The proof uses the property that such groups $\mathrm{G} \subset \mathrm{GL}_n$ are generated by unipotent subgroups. Then the same argument as in the proof of Proposition 1.5 applies. $\square$

As $\mathrm{G} \subset \mathrm{GL}_n$, we can again define the congruence subgroups $\Gamma_{p,\ell}$ for ℓ coprime to p as the kernel of the homomorphism

$$\mathrm{G}(\mathbb{Z}[\tfrac{1}{p}]) \longrightarrow \mathrm{G}(\mathbb{Z}/\ell\mathbb{Z})$$

and again write $\Gamma_{p,0} = \mathrm{G}(\mathbb{Z}[\frac{1}{p}])$. Then one deduces as in chapter 1.1, that $\Gamma_{p,\ell}$ is a lattice, diagonally embedded in $\mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p)$ and the $\mathrm{G}(\mathbb{Q}_p)$ action on

$$X_{p,\ell} = \mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p) / \Gamma_{p,\ell}$$

is ergodic.

The associated Koopman representation of the action of G_p on $X_{p,\ell}$ will be denoted throughout this thesis as $\pi_{p,\ell}$. In particular, for $f \in L^2(X_{p,\ell})$ we have

$$((\pi_{p,\ell})_g f)(x) = f(g^{-1}x),$$

where $g \in G_p$ and $x \in X_{p,\ell}$.

In the final part of this subchapter we discuss Tamagawa measures. Fix a rational invariant differential form on G of top degree (see [Wei82]). Such a form is called a gauge form. The gauge form defines Haar measures m_∞^{Tam} and m_p^{Tam} on $\mathrm{G}(\mathbb{R})$ and $\mathrm{G}(\mathbb{Q}_p)$. It is well known ([Kot88]), as G is simply connected, that

$$m_\infty^{\mathrm{Tam}}(\mathrm{G}(\mathbb{R})/\mathrm{G}(\mathbb{Z})) \prod_{p \text{ prime}} m_p^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)) = 1.$$

We next discuss a lemma from [BR95].

Lemma 1.23. *In the above setting, for any prime p,*

$$m_p^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)) = \lim_{k\to\infty} \frac{|\mathrm{G}(\mathbb{Z}/p^k\mathbb{Z})|}{p^{\dim(\mathrm{G})k}}$$

Proof. For simplicity we only treat the case where

$$\mathrm{G} = \operatorname{Spec} \mathbb{Q}[X_1, \dots, X_{n^2}]/(f_1, \dots, f_r)$$

for $f_1, \dots, f_r \in \mathbb{Z}[X_1, \dots, X_{x^2}]$ with the property

$$\operatorname{rank}((\partial_j f_i)_{ij}) = r.$$

As G is smooth,

$$\dim(G) = n^2 - \operatorname{rank}((\partial_j f_i)_{ij}).$$

Let ω be the fixed gauge form on G. Consider the smooth map $f : (f_1, \dots, f_r) : \mathbb{A}^{n^2} \to \mathbb{A}^r$. We denote by G_s the fiber $f^{-1}(s)$ for $s \in \mathbb{A}^r$ so that $\mathrm{G} = \mathrm{G}_0$. As $\operatorname{rank}((\partial_j f_i)_{ij}) = r$, the map f is smooth on $f^{-1}(U)$ for some Zariski open set U of $\mathbb{A}^r$. Fix a prime number p. As discussed in chapter 1 of [BR95], there exists a differential form ω_s on the fibers $\mathrm{G}_s = f^{-1}(s)$ inducing measures $m_{p,s}^{\mathrm{Tam}}$ so that

$$\int_{\mathbb{Q}_p^{n^2}} \phi(f(x))\psi(x)\, dx = \int_{\mathbb{Q}_p^r} \phi(s) \left(\int_{\mathrm{G}_s(\mathbb{Q}_p)} \psi \, dm_{p,s}^{\mathrm{Tam}} \right) ds,$$

where ψ and ρ are locally constant compactly supported functions.

Next fix $k > 0$ and set

$$C_k = p^k \mathbb{Z}_p^r \subset \mathbb{Q}_p^r \qquad \text{and} \qquad B = \mathbb{Z}_p^{n^2} \subset \mathbb{Q}_p^{n^2}.$$

Then $\operatorname{vol}(C_k) = p^{-kr}$. Let ψ be the characteristic function of the compact open subset B and ϕ the characteristic function of C_k. Observe that as $s \mapsto m_{p,s}^{\mathrm{Tam}}(\mathrm{G}_s(\mathbb{Z}_p))$ is continuous and since C_k is a sequence of neighborhoods decreasing to 0 in $\mathbb{Q}_p^r$, it follows that

$$\begin{aligned}\lim_{k\to\infty} \frac{1}{\operatorname{vol}(C_k)} \int_{C_k} m_{p,s}^{\mathrm{Tam}}(\mathrm{G}_s(\mathbb{Z}_p))\, ds &= \frac{1}{p^{-kr}} \int_{C_k} m_{p,s}^{\mathrm{Tam}}(\mathrm{G}_s(\mathbb{Z}_p))\, ds \\ &= m_{p,0}^{\mathrm{Tam}}(\mathrm{G}_0(\mathbb{Z}_p)) = m_p^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)).\end{aligned}$$

Thus upon dividing by p^{-kr} the lemma follows from the final claim that

$$\int_{C_k} m_{p,s}^{\mathrm{Tam}}(\mathrm{G}_s(\mathbb{Z}_p))\, ds = \frac{|\mathrm{G}(\mathbb{Z}/p^k\mathbb{Z})|}{p^{n^2 k}}.$$

To prove the claim, we first apply the above integration formula to conclude

$$\int_{C_k} m_{p,s}^{\mathrm{Tam}}(\mathrm{G}_s(\mathbb{Z}_p))\, ds = \int_{\mathbb{Z}_p^{n^2}} \chi_{p^k\mathbb{Z}_p^r}(f(x))\, dx.$$

Recall that the map $\mathbb{Z} \to \mathbb{Z}_p/p^k\mathbb{Z}_p$ that factors through the canonical injection $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ is surjective. In particular, for each element $x \in \mathbb{Z}_p^{n^2}$ there is a residue class $a \in (\mathbb{Z}/p^k\mathbb{Z})^{n^2}$ so that $x \in a + p^k\mathbb{Z}_p^{n^2}$. Moreover, the $p^k\mathbb{Z}_p^r$ residue class of the value $f(x)$ only depends on the value $f(a)$. As the volume of each residue class $a + p^k\mathbb{Z}_p^{n^2}$ is p^{n^2k}, we conclude

$$\begin{aligned}\int_{\mathbb{Z}_p^{n^2}} \chi_{p^k\mathbb{Z}_p^r}(f(x))\,dx &= \frac{1}{p^{n^2k}} \sum_{a\in(\mathbb{Z}/p^k\mathbb{Z})^{n^2}} \chi_{p^k\mathbb{Z}_p^r}(f(a)) \\ &= \frac{|\mathrm{G}(\mathbb{Z}/p^k\mathbb{Z})|}{p^{n^2k}}.\end{aligned}$$

□

Lemma 1.23 will be applied in chapter 5.5. Furthermore, we will also need in chapter 5.5 the following claim, for which we consider the concrete setting $\mathrm{G} = \mathrm{B}^1$, where B is a quaternion algebra over $\mathbb{Q}$. Fix a prime p and let $h = p^m$. Denote by

$$B_h = \{x \in \mathrm{B}(\mathbb{Q}_p) \,:\, \mathrm{Nr}(x) = 1, ||x||_p \le h\}$$

and by

$$B_h' = \{x \in \mathrm{B}(\mathbb{Z}_p) \,:\, \mathrm{Nr}(x) = h^2\}.$$

We will again use the measures $m_{p,s}^{\mathrm{Tam}}$, which were introduced in the proof of Lemma 1.23. In this concrete setting, the defining property of the measures $m_{p,s}^{\mathrm{Tam}}$ reads as

$$\int_{\mathbb{Q}_p^4} \phi(\mathrm{Nr}(x))\psi(x)\,dx = \int_{\mathbb{Q}_p\setminus\{0\}} \phi(s)\left(\int_{\mathrm{Nr}^{-1}(s)} \psi\,dm_{p,s}^{\mathrm{Tam}}\right) ds.$$

Denote by $F : \mathrm{B}(\mathbb{Q}_p) \to \mathrm{B}(\mathbb{Q}_p), x \mapsto h^{-1}x$ and note that F defines a bijection between B_h' and B_h. We aim to calculate $F_*(m_{p,s}^{\mathrm{Tam}})$. In order to do so, let ϕ and ψ be any locally constant functions with compact support. Then,

$$\begin{aligned}&\int_{\mathbb{Q}_p\setminus\{0\}} \phi(s)\left(\int_{\mathrm{Nr}^{-1}(s)} \psi\,dm_{p,s}^{\mathrm{Tam}}\right) ds \\ &= \int_{\mathbb{Q}_p^4} \phi(\mathrm{Nr}(x))\psi(x)\,dx \\ &= \int_{\mathbb{Q}_p^4} \phi(h^{-2}\mathrm{Nr}(x))\psi(h^{-1}x)|h|_p^{-4}\,dx \\ &= \int_{\mathbb{Q}_p\setminus\{0\}} \phi(h^{-2}s)\left(\int_{\mathrm{Nr}^{-1}(s)} \psi\circ F\,dm_{p,s}^{\mathrm{Tam}}\right)|h|_p^{-4}\,ds \\ &= \int_{\mathbb{Q}_p\setminus\{0\}} \phi(s)\left(\int_{\mathrm{Nr}^{-1}(h^2s)} \psi\circ F\,dm_{p,h^2s}^{\mathrm{Tam}}\right)|h|_p^{-2}\,ds \\ &= \int_{\mathbb{Q}_p\setminus\{0\}} \phi(s)\left(\int_{\mathrm{Nr}^{-1}(s)} \psi\,dF_*(m_{p,h^2s}^{\mathrm{Tam}})\right)|h|_p^{-2}\,ds,\end{aligned}$$

where we replaced in the third line x by $h^{-1}x$ and in the penultimate line s by $h^{-2}s$. We conclude for any $s \in \mathbb{Q}_p\setminus\{0\}$,

$$F_*(m_{p,s}^{\mathrm{Tam}}) = |h|_p^2 m_{p,h^{-2}s}^{\mathrm{Tam}}. \tag{1.3}$$

Lemma 1.24. *In the above setting,*

$$\lim_{k\to\infty} \frac{|\{x \in (\mathbb{Z}/p^k\mathbb{Z})^4 \,:\, \mathrm{Nr}(x) = h^2 \mod p^k\}|}{p^{3k}} = h^{-2} m_p^{\mathrm{Tam}}(B_h).$$

Proof. By equation (1.3),

$$\begin{aligned} m_p^{\mathrm{Tam}}(B_h) &= m_{p,e}^{\mathrm{Tam}}(B_h) = m_{p,h^{-2}h^2}^{\mathrm{Tam}}(B_h) \\ &= |h|_p^{-2} m_{p,h^2}^{\mathrm{Tam}}(F^{-1}(B_h)) = h^2 m_{p,h^2}^{\mathrm{Tam}}(B'_h). \end{aligned}$$

As in the proof of Lemma 1.23 one shows that

$$\int_{h^2+p^k\mathbb{Z}_p} m_{p,s}^{\mathrm{Tam}}(B'_h)\, ds = \frac{|\{x \in (\mathbb{Z}/p^k\mathbb{Z})^4 \,:\, \mathrm{Nr}(x) = h^2 \mod p^k\}|}{p^{4k}}.$$

The claim again follows since $s \mapsto m_{p,s}^{\mathrm{Tam}}(B'_h)$ is continuous and $h^2 + p^k\mathbb{Z}_p$ is a sequence of neighborhoods of h that converges to h as $k \to \infty$. Thus,

$$\lim_{k\to\infty} \frac{1}{p^{-k}} \int_{h^2+p^k\mathbb{Z}_p} m_{p,s}^{\mathrm{Tam}}(B'_h)\, ds = m_{p,h^2}^{\mathrm{Tam}}(B'_h) = h^{-2} m_p^{\mathrm{Tam}}(B_h).$$

□

1.3 Adeles and Adelic Points of Algebraic Groups over $\mathbb{Q}$

We follow in part the exposition given in chapter 3 of [GGPS].

Definition 1.25. The **adeles** of $\mathbb{Q}$ are the ring

$$\mathbb{A} = \{(a_\infty, a_2, a_3, \ldots) \,:\, a_\infty \in \mathbb{R}, a_p \in \mathbb{Q}_p \text{ and for almost all pimes } a_p \in \mathbb{Z}_p\}$$

equipped with componentwise addition and multiplication.

We discuss how to equip the adeles with a natural topology. First we consider the subring

$$\mathbb{A}^\circ = \mathbb{R} \times \prod_p \mathbb{Z}_p \subset \mathbb{A},$$

on which we consider the product topology so that a basis is given by

$$U \times \prod_p U_p$$

with $U \subset \mathbb{R}$ and $U_p \subset \mathbb{Z}_p$ open so that $U_p = \mathbb{Z}_p$ for almost all primes p. We furthermore require that $\mathbb{A}^\circ$ is open in $\mathbb{A}$. This yields that a basis for the topology on $\mathbb{A}$ is given by

$$a + \left(U \times \prod_p U_p\right) = (a_\infty + U) \times \prod_p (a_p + U_p),$$

with U and U_p as above and $a \in \mathbb{A}$.

Lemma 1.26. *The adeles are a locally compact, second countable Hausdorff topological ring.*

Proof. As $\mathbb{Z}_p$ is compact for all primes p, it follows from Tychonoff's Theorem that for each point $a \in \mathbb{A}$ the neighborhood

$$a \in [a_\infty - 1, a_\infty + 1] \times \prod_p a_j + \mathbb{Z}_p$$

is compact. As $\mathbb{R}$ and $\mathbb{Q}_p$ are second countable and Hausdorff, the adele ring also has these properties. It remains to check that addition and multiplication

$$+ : \mathbb{A} \times \mathbb{A} \to \mathbb{A}, \qquad \cdot : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$$

are continuous.

We first treat the addition map. As $\mathbb{A}$ is second countable, it suffices to show that if $a^n \to a$ and $b^n \to b$ in $\mathbb{A}$ then $a^n + b^n \to a + b$. Analyzing the topology on $\mathbb{A}$, it follows that the sequence

$$a^n = (a^n_\infty, a^n_2, a^n_3, \ldots)$$

converges to

$$a = (a_\infty, a_2, a_3, \ldots),$$

if and only if the sequence converges pointwise and there is some large N so that for all $n \geq N$ the difference $a_p - a^n_p$ is a p-adic integer for all primes p. In view of this observation, to prove $a^n + b^n \to a + b$ is straightforward. Pointwise convergence follows from continuity of addition in $\mathbb{R}$ and $\mathbb{Q}_p$. Choosing N large enough so that $a_p - a^n_p \in \mathbb{Z}_p$ and $b_p - b^n_p \in \mathbb{Z}_p$ for all $n \geq N$, we conclude

$$a_p + b_p - a^n_p + b^n_p = (a_p - a^n_p) + (b_p - b^n_p) \in \mathbb{Z}_p$$

for $n \geq N$.

To show continuity of multiplication, we first show that left multiplication

$$L_b : \mathbb{A} \to \mathbb{A}, \qquad a \mapsto ba$$

is continuous for any $b \in \mathbb{A}$. To see this let $a^n \to a$. We want to show that $ba^n \to ba$. Componentwise convergence again follows from continuity of multiplication in $\mathbb{Q}_p$. It remains to check that for large enough n and all p we have that

$$b_p a_p - b_p a^n_p = b_p(a_p - a^n_p)$$

is a p-adic integer. As $a_n \to a$ for $n \geq N_0$, the difference $a_p - a^n_p$ is a p-adic integer. By definition of the adeles, we can find P large enough so that for all $p \geq P$ the element $b_p \in \mathbb{Q}_p$ is a p-adic integer. Set next

$$c = \max_{2 \leq p \leq P} \left(\max\{1, |b_p|_p\}\right).$$

By componentwise convergence, we can find N_1 large enough with the property that for $n \geq N_1$ $|a_p - a^n_p|_p \leq c^{-1}$ and so $|b_p(a_p - a^n_p)| \leq 1$ for all $2 \leq p \leq P$. Choosing $n \geq \max\{N_0, N_1\}$,

$$b_p(a_p - a^n_p) \in \mathbb{Z}_p$$

for all primes p, proving $ba^n \to ba$.

One analogously shows that right multiplication is continuous. We are now in a suitable position to prove that $\cdot : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ is continuous. Namely, if $a^n \to a$ and $b^n \to b$, we want to show $a^n b^n \to ab$. Again, componentwise convergence is clear. So it remains to show that for large enough n,

$$\begin{aligned} ab - a^n b^n &= ab - ab^n + ab^n - a^n b^n = a(b - b^n) + (a - a^n)b^n \\ &= a(b - b^n) + (a - a^n)(b^n - b + b) \\ &= a(b - b^n) + (a - a^n)(b^n - b) + (a - a^n)b \end{aligned}$$

is a p-adic integer at every prime. For the left and right term in the last expression this follows as left and right multiplication are continuous. For the middle term one exploits that $\mathbb{Z}_p$ is closed under multiplication. $\square$

Viewing the adeles as an additive abelian group, the adeles have a Haar measure $\mu_{\mathbb{A}}$ on $\mathbb{A}$, which is given by restricting the product measure on $\mathbb{R} \times \prod_p \mathbb{Q}_p$. Moreover, we choose a normalization of the Haar measure giving unit volume to

$$[0,1] \times \prod_p \mathbb{Z}_p = \{a \in \mathbb{A} \,:\, a_\infty \in [0,1] \text{ and } |a_p|_p \leq 1 \text{ for all } p\}.$$

The rational numbers can be viewed as a subring of $\mathbb{A}$ via the embedding

$$\mathbb{Q} \hookrightarrow \mathbb{A}, \qquad q \mapsto (q, q, q, \ldots),$$

where one observes that this map is well defined as $|q|_p = 1$ for p large enough.

Proposition 1.27. *The rational numbers form a lattice in the ring of adeles.*

Proof. We first show that $\mathbb{Q}$ is a discrete subgroup. Assume for a contradiction that they are not discrete, i.e. there is a sequence of non-zero rational number $r_n = (r_n, r_n, r_n, \ldots)$ with $r_n \to 0$ in $\mathbb{A}$. For n large enough, r_n is a p-adic integer for all primes p. Hence r_n is an integer for large enough n but then r_n does not converge to 0.

Finally notice that

$$F = \{(a_\infty, a_2, a_3, \ldots) \,:\, 0 \leq a_\infty < 1 \text{ and } a_p \in \mathbb{Z}_p \text{ for all primes } p\}$$

is a fundamental domain for $\mathbb{A}/\mathbb{Q}$, which implies that $\mathbb{Q}$ is a lattice in $\mathbb{A}$ as F has volume 1. $\square$

Let $\mathrm{G} \subset \mathrm{GL}_n$ be an algebraic group over $\mathbb{Q}$. We define

$$\mathrm{G}(\mathbb{Z}_p) = \mathrm{G}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p),$$

where $\mathrm{GL}_n(\mathbb{Z}_p) = \{g \in \mathrm{M}_{n,n}(\mathbb{Q}_p) \,:\, g \text{ and } g^{-1} \in \mathrm{M}_{n,n}(\mathbb{Z}_p)\}$.

Definition 1.28. The **adelic points** $\mathrm{G}(\mathbb{A})$ of the algebraic group G are defined as the subgroup of

$$\mathrm{G}(\mathbb{R}) \times \prod_p \mathrm{G}(\mathbb{Q}_p)$$

given by

$$\mathrm{G}(\mathbb{A}) = \{(a_\infty, a_2, a_3, \ldots) \,:\, a_p \in \mathrm{G}(\mathbb{Z}_p) \text{ for almost all primes } p\},$$

equipped with componentwise multiplication.

Analogously to the case of p-adic numbers, we equip

$$\mathrm{G}(\mathbb{R}) \times \prod_p \mathrm{G}(\mathbb{Z}_p)$$

with the product topology and require that it is an open subset of $\mathrm{G}(\mathbb{A})$. Equivalently, a sequence of adelic points $g^n \in \mathrm{G}(\mathbb{A})$ converges to $g \in \mathrm{G}(\mathbb{A})$ if and only if we have componentwise convergence and there is some N large enough so that for all $n \geq N$ and primes p, the difference $g_p - g_p^n \in \mathrm{G}(\mathbb{Z}_p)$.

Lemma 1.29. *The adelic points* $\mathrm{G}(\mathbb{A})$ *form a locally compact, second countable Hausdorff topological group.*

Proof. Let $g \in \mathrm{G}(\mathbb{A})$ and let U_{g_∞} be a compact neighborhood of g_∞ in $\mathrm{G}(\mathbb{R})$. Then we have that by Tychonoff's Theorem

$$U_{g_\infty} \times \prod_p (g_p + \mathrm{G}(\mathbb{Z}_p))$$

is a compact neighborhood of g as $\mathrm{G}(\mathbb{Z}_p)$ is compact at every p. To see that $\mathrm{G}(\mathbb{A})$ is second countable and Hausdorff just note that $\mathrm{G}(\mathbb{R})$ and $\mathrm{G}(\mathbb{Q}_p)$ have these properties.

Finally, we check that the multiplication map is continuous. So let $g^n \to g$ and $h^n \to h$ be converging sequences of elements in $\mathrm{G}(\mathbb{A})$. Clearly, $g^n h^n$ converges to gh componentwise and so it remain to check that for large n the matrices

$$g_p h_p - g_p^n h_p^n$$

are in $\mathrm{Mat}_n(\mathbb{Z}_p)$ for all p. This simply follows as the adeles are a topological ring and hence for large enough n each matrix entry of $g_p h_p - g_p^n h_p^n$ is in $\mathbb{Z}_p$. $\square$

If $S \subset P$ is any set of places, then analogously to the adelic points, we can define G_S again as the restricted direct product equipped with the analogous topology. It hence follows that G_S is a locally compact, second countable Hausdorff topological group.

Returning to $\mathrm{G}(\mathbb{A})$, we note that it has a Haar measure. As before, there is an injection

$$\mathrm{G}(\mathbb{Q}) \hookrightarrow \mathrm{G}(\mathbb{A}), \qquad r \mapsto (r, r, r, \ldots),$$

so that $\mathrm{G}(\mathbb{Q})$ can be viewed as a subgroup of $\mathrm{G}(\mathbb{A})$.

Proposition 1.30. *If* G *is a semisimple algebraic group over* $\mathbb{Q}$*, the* $\mathbb{Q}$*-points* $\mathrm{G}(\mathbb{Q})$ *form a lattice in* $\mathrm{G}(\mathbb{A})$*.*

Proof. We first show that $\mathrm{G}(\mathbb{Q})$ is a discrete subgroup. Assume for a contradiction that this is not the case so that there is a sequence of non-identity rational matrices r^n converging to 1 in $\mathrm{G}(\mathbb{A})$. Then for large enough n, the rational matrix $1 - r_p^n$ is a $\mathbb{Z}_p$-matrix for every p and hence in particular a $\mathbb{Z}$-matrix. Thus for large n we have that $r_p^n \in 1 + \mathrm{Mat}_n(\mathbb{Z})$ and so in particular r^n is an integer matrix for n large enough. This contradicts the assumption that $r_n \to 0$.

To show that $\mathrm{G}(\mathbb{A})/\mathrm{G}(\mathbb{Q})$ has finite volume, we refer to [PR94] chapter 5.3. The proof uses that the class number of G is finite, i.e. that there are finitely many points $x_1, \ldots, x_n \in G_{P \setminus \{\infty\}}$ so that

$$\mathrm{G}(\mathbb{A}) = \bigcup_{i=1}^{n} \mathrm{G}(\mathbb{R}) x_i \mathrm{G}(\mathbb{Q}).$$

This statement easily implies the claim. Choose a fundamental domain F for $\mathrm{G}(\mathbb{Z}) < \mathrm{G}(\mathbb{R})$ and denote by $K = \prod_{p \in P\setminus\{\infty\}} \mathrm{G}(\mathbb{Z}_p)$. If we choose $C = \bigcup_{i=1}^{n} K x_i K$, it clearly follows that $F \cdot C$ is a surjective domain of finite volume for $\mathrm{G}(\mathbb{A})/\mathrm{G}(\mathbb{Q})$ and hence $\mathrm{G}(\mathbb{Q})$ is a lattice in $\mathrm{G}(\mathbb{A})$. $\square$

In analogy to the p-adic extension, we also study the adelic extension

$$X_{\mathbb{A}} = \mathrm{G}(\mathbb{A})\big/\mathrm{G}(\mathbb{Q}).$$

If S is a finite set of places, then G_S acts on $X_{\mathbb{A}}$ by left multiplication.

To prove ergodicity of the G_S action on $X_{\mathbb{A}}$, we need to assume that G is isotropic over S, as this has the following consequence.

Theorem 1.31. *Let* G *be a simply connected almost simple algebraic group over* $\mathbb{Q}$*. Let* p *be a prime number and assume that* G *is isotropic over* $\mathbb{Q}_p$*. Then*

(i) The product group $\mathrm{G}(\mathbb{Q}_p)\mathrm{G}(\mathbb{Q}) \subset \mathrm{G}(\mathbb{A})$ *is dense.*

(ii) The subgroup $\mathrm{G}(\mathbb{Z}[\frac{1}{p}]) \subset \mathrm{G}(\mathbb{R})$ *is dense.*

Proof. The first statement is the strong approximation property, we refer to chapter 7 of [PR94]. (ii) follows from (i) as we now show. Note that by (i), the diagonally embedded subgroup $\mathrm{G}(\mathbb{Q}) \subset G_{P\setminus\{p\}}$ is dense. Let $x \in \mathrm{G}(\mathbb{R})$. We consider the element $(x, 1, 1, \ldots) \in G_{P\setminus\{p\}}$. So for any $\varepsilon > 0$ we can find $\gamma \in \mathrm{G}(\mathbb{Q})$ so that x is arbitrarily close to γ in $\mathrm{G}(\mathbb{R})$ and $\gamma \in \mathrm{G}(\mathbb{Z}_q)$ for all primes $q \in P\setminus\{p\}$. Thus it follows that $\gamma \in \mathrm{G}(\mathbb{Z}[\frac{1}{p}])$, which then implies the claim. $\square$

Proposition 1.32. *Let* G *is a simply connected, almost simple algebraic group over* $\mathbb{Q}$*. Let* $S \subset P$ *be a finite set of places and assume that* G *is isotropic over* S*. Then the action of* G_S *on* $X_{\mathbb{A}}$ *is ergodic.*

Proof. By Theorem 1.31, this shows that $G_S\mathrm{G}(\mathbb{Q})$ is dense in $\mathrm{G}(\mathbb{A})$. Hence, as in the proof of Proposition 1.5, we consider a G_S invariant measurable function $f : X_{\mathbb{A}} \to \mathbb{C}$. This function lifts to a $\mathrm{G}(\mathbb{Q})$-invariant function on $f : \mathrm{G}(\mathbb{A}) \to \mathbb{C}$, which is hence constant. $\square$

We will denote by π_p the Koopman representation of the G_p action on $X_{\mathbb{A}}$. Thus for $f \in L^2(X_{\mathbb{A}})$ we have

$$((\pi_p)_g f)(x) = f(g^{-1}x),$$

where $g \in G_p$ and $x \in X_{\mathbb{A}}$.

2 Elements of the Theory of Unitary Representations

In this chapter we review some notions and results concerning unitary representations. Even though we aim towards applications in dynamics, we give a general and comprehensive exposition of the stated results, which the reader hopefully may find useful. As a good introductory reference for the theory of unitary representations we cite the upcoming book [EW], whose notation we mostly follow.

Throughout this chapter and even thesis, if we speak of a topological group G we will always refer to a locally compact, Hausdorff group and for convenience also assume that G is σ-compact and metric, even though these assumptions are not strictly necessary. Denote by m_G a left Haar measure on G and by $L^p(G)$ the corresponding L^p-space with respect to any Haar measure. The central object of study in this chapter are unitary representations $(\pi, \mathscr{H})$. The Hilbert space $\mathscr{H}$ is always assumed to be complex and separable unless stated otherwise. For $v, w \in \mathscr{H}$ we write $\varphi^{\pi}_{v,w}$ for the **matrix coefficient**, i.e. the function

$$\varphi^{\pi}_{v,w} : G \longrightarrow \mathbb{C}, \qquad g \longmapsto \langle \pi_g v, w \rangle.$$

The diagonal matrix coefficient $\varphi^{\pi}_{v,v}$ will also be written as φ^{π}_{v}. The space of all diagonal matrix coefficients of all unitary representations of G is denoted as $\mathscr{P}(G)$ and the reader may recall that $\mathscr{P}(G)$ is precisely the space of continuous positive definite functions on G.

2.1 Containment, Temperedness and the Fell Topology

The primary reference for this subchapter is chapter 4 of [EW]. Let $(\pi, \mathscr{H})$ be a unitary representation. Recall that, up to unitary isomorphism, the diagonal matrix coefficient of an element $v \in \mathscr{H}$ determines the cyclic subspace generated by v in $\mathscr{H}$. As each unitary representation can be written as a direct sum of cyclic subspaces, it follows that the matrix coefficients of $(\pi, \mathscr{H})$ determine the representation. The set of matrix coefficients $\mathscr{P}(G)$ is equipped with the topology of uniform convergence on compact sets. This viewpoint suggest that two unitary representations $(\pi, \mathscr{H}_1)$ and $(\rho, \mathscr{H}_2)$ are *close* to each other if some matrix coefficient of π can be approximated on some compact set with some accuracy by the matrix coefficients of ρ. The further development of these ideas leads to the Fell topology which will be discussed later.

In this context, one could say that a unitary representation $(\pi, \mathscr{H}_1)$ is *as close as possible* to another unitary representation $(\rho, \mathscr{H}_2)$ if all the matrix coefficients of π can be approximated by the matrix coefficients of ρ. This leads to the notion of **weak containment**.

Definition 2.1. Let $(\pi, \mathscr{H}_1)$ and $(\rho, \mathscr{H}_2)$ be unitary representations of G. We say that π is **weakly contained** in ρ and write $\pi \prec \rho$ if the following three equivalent (see chapter 4.3 of [EW]) conditions holds:

1. The diagonal matrix coefficients of π can be approximated by sums of diagonal matrix coefficients of ρ, i.e. for each $v \in \mathscr{H}_1$, compact subset

$K \subset G$ and $\varepsilon > 0$ there are elements $w_1, \ldots, w_n \in \mathscr{H}_2$ so that

$$\left|\left|\varphi_v^\pi - \sum_{i=1}^n \varphi_{w_i}^\rho\right|\right|_{K,\infty} < \varepsilon.$$

2. For every $v, w \in \mathscr{H}_1$, compact $K \subset G$ and $\varepsilon > 0$, there are $g_1, \ldots g_n, h_1, \ldots, h_n \in \mathscr{H}_2$ so that

$$\left|\left|\varphi_{v,w}^\pi - \sum_{i=1}^n \varphi_{g_i,h_i}^\rho\right|\right|_{K,\infty} < \varepsilon$$

with the additional constraint

$$\sum_{i=1}^n ||g_i||\,||h_i|| < ||v||\,||w||.$$

3. For all $f \in L^1(G)$,

$$||\pi(f)||_{\mathrm{op}} \leq ||\rho(f)||_{\mathrm{op}}.$$

Recall that we say that π is **contained** in ρ and write $\pi < \rho$ if there is a closed subspace $V \subset \mathscr{H}_2$ so that π and $\rho|_V$ are isomorphic unitary representations. This condition is equivalent to the property that the matrix coefficients of π are a subset of the matrix coefficients of ρ and hence indeed, weak containment is a generalization of containment. As the notion of weak containment is central to this thesis, we discuss some further properties and examples.

Proposition 2.2. *Let $(\pi, \mathscr{H}_1)$ and $(\rho, \mathscr{H}_2)$ be unitary representations of G and assume that $(\pi, \mathscr{H}_1)$ is irreducible. Then $\pi \prec \rho$ if and only if for any $v \in \mathscr{H}_1$, $K \subset G$ compact and $\varepsilon > 0$, there is $w \in \mathscr{H}_2$ with $||w|| = ||v||$ so that*

$$||\varphi_v^\pi - \varphi_w^\rho||_{K,\infty} < \varepsilon.$$

Proof. This is Proposition 4.8 of [EW]. □

We next give an equivalent condition for $1_G \prec \pi$, where 1_G is the trivial representation.

Definition 2.3. Let $(\pi, \mathscr{H})$ be a unitary representation of G. We say that π has **almost invariant unit vectors** if for every compact subset $K \subset G$ and $\varepsilon > 0$ there is a unit vector $v \in \mathscr{H}$ so that

$$||\pi_g v - v|| < \varepsilon$$

for all $g \in K$.

The next lemma reflects the fact that $1_G < \pi$ if and only if π has invariant vectors.

Lemma 2.4. *For a unitary representation $(\pi, \mathscr{H})$ of G the following properties are equivalent:*

1. *π has almost invariant unit vectors.*

2. $1_G \prec \pi$.

Proof. Assume that π has almost invariant unit vectors. To show $1_G \prec \pi$, it suffices to consider unit elements $\lambda \in \mathbb{C}$, i.e. so that $\varphi_\lambda^{1_G} = 1$. For each compact subset $K \subset G$ and $\varepsilon > 0$ there is some unit vector $v \in \mathscr{H}$ so that $||\pi_g v - v|| < \varepsilon$ for all $g \in K$. Thus we conclude

$$||\varphi_\lambda^{1_G} - \varphi_v^\pi||_{K,\infty} = ||1 - \varphi_v^\pi||_{K,\infty} = ||\langle \pi_g v - v, v\rangle||_{K,\infty} < \varepsilon,$$

which implies that $1_G \prec \pi$.

For the converse, assume $1_G \prec \pi$. Since 1_G is irreducible, using Proposition 2.2, for each unit vector $\lambda \in \mathbb{C}$, compact $K \subset G$ and $\varepsilon > 0$ there is a unit vector $v \in \mathscr{H}$ so that

$$||\varphi_\lambda^{1_G} - \varphi_v^\pi||_{K,\infty} = ||1 - \varphi_v^\pi||_{K,\infty} = ||1 - \langle \pi_g v, v\rangle||_{K,\infty} < \varepsilon.$$

Using that π_g is unitary it follows for all $g \in K$,

$$\begin{aligned} ||\pi_g v - v||^2 &= \langle \pi_g v - v, \pi_g v - v\rangle \\ &= 2(||v||^2 - \mathrm{Re}(\langle \pi_g v, v\rangle)) \\ &= 2(1 - \mathrm{Re}(\langle \pi_g v, v\rangle)) < 2\varepsilon. \end{aligned}$$

Thus for all $g \in K$,

$$||\pi_g v - v|| < \sqrt{2\varepsilon},$$

which implies the claim. □

Lemma 2.5. *Let $(\pi_n, \mathscr{H}_n)_{n\in\mathbb{N}}$ be a collection of unitary representations of G all weakly contained in the representation $(\rho, \mathscr{H})$. Then*

$$\bigoplus_{n\in\mathbb{N}} \pi_n \prec \rho.$$

Proof. Let $v = (v_n)_{n\in\mathbb{N}} \in \bigoplus_{n\in\mathbb{N}} \mathscr{H}_n$ so that

$$||v||^2 = \sum_{n\in\mathbb{N}} ||v_n||^2_{\mathscr{H}_n} \qquad \text{and} \qquad \varphi_v^\pi(g) = \sum_{n\in\mathbb{N}} \varphi_{v_n}^{\pi_n}(g)$$

for all $g \in G$. Let $K \subset G$ be a compact set and $\varepsilon > 0$. Choose N large enough so that

$$\sum_{n>N}^{\infty} ||v_n||^2_{\mathscr{H}_n} < \varepsilon.$$

Then for each v_n with $n \le N$ we choose a collection of vectors $w_{n,1}, \dots, w_{n,k(n)}$ so that

$$\left|\left| \varphi_{v_n}^{\pi_n} - \sum_{i=1}^{k(n)} \varphi_{w_{n,i}}^\rho \right|\right|_{K,\infty} < \frac{\varepsilon}{N}.$$

Thus we conclude

$$\begin{aligned} \left|\left| \varphi_v^\pi - \sum_{n\le N}\sum_{i=1}^{k(n)} \varphi_{w_{n,i}}^\rho \right|\right|_{K,\infty} &= \left|\left| \sum_{n>N} \varphi_{v_n}^{\pi_n} + \sum_{n\le N} \varphi_{v_n}^{\pi_n} - \sum_{n\le N}\sum_{i=1}^{k(n)} \varphi_{w_{n,i}}^\rho \right|\right|_{K,\infty} \\ &\le \varepsilon + \left|\left| \sum_{n\le N} \left(\varphi_{v_n}^{\pi_n} - \sum_{i=1}^{k(n)} \varphi_{w_{n,i}}^\rho \right) \right|\right|_{K,\infty} \\ &< \varepsilon + N\frac{\varepsilon}{N} \le 2\varepsilon, \end{aligned}$$

implying the claim. □

We next discuss weak containment for compact groups a bit further. Before stating the next result, we denote for a unitary representation $(\pi, \mathscr{H})$ by $(\pi^\infty, \mathscr{H}^\infty)$ the unitary representation

$$\bigoplus_{n\in\mathbb{N}} \mathscr{H}.$$

Proposition 2.6. *Let $(\pi_1, \mathscr{H}_1)$ and $(\pi_2, \mathscr{H}_2)$ be unitary representations of a compact group G. The following properties are equivalent:*

(i) $\pi_1 \prec \pi_2$.

(ii) *If $\sigma < \pi_1$ for an irreducible unitary representation $\sigma \in \widehat{G}$ then $\sigma < \pi_2$.*

(iii) $\pi_1 < \pi_2^\infty$.

In particular, if π_1 is irreducible, then $\pi_1 \prec \pi_2$ if and only if $\pi_1 < \pi_2$.

Proof. Assume (i) and let $\sigma < \pi_1$ for $\sigma \in \widehat{G}$. Since $\pi_1 \prec \pi_2$, it follows by transitivity of weak containment that $\sigma \prec \pi_2$. Let $v \in \mathscr{H}_\sigma$. Since σ is irreducible and G is compact, for each $n \in \mathbb{N}$ there is a vector $v_n \in \mathscr{H}_2$ with $||v|| = ||v_n||$ so that

$$||\varphi_v^\sigma - \varphi_{v_n}^{\pi_2}||_\infty < \frac{1}{n}.$$

By Banach-Alaoglu, there exists a weak*-limit $v^* \in \mathscr{H}_2$ of v_n. Then we have in particular pointwise convergence $\varphi_{v_n}^{\pi_2} \to \varphi_{v^*}^{\pi_2}$. Thus it follows that $\varphi_{v^*}^{\pi_2} = \varphi_v^\sigma$ and hence we conclude $\sigma < \pi_2$. Thus we have showed (ii). (ii) implies (iii) follows as every representation of a compact group G is a direct sum of irreducibles and each irreducible representation can appear at most a countable number of times since we require our Hilbert spaces to be separable. (iii) implies (ii) implies (i) is equally straightforward. □

Unitary representations that are weakly contained in the regular representation are called **tempered** and they will be of particular importance later on.

Lemma 2.7. *Every unitary representation of a compact group is tempered.*

Proof. Recall that every irreducible representation of a compact group is contained in the regular representation. Thus the claim follows by the last lemma as each unitary representation of a compact group is a direct sum of irreducible representations. □

We next discuss abelian groups. If $(\pi, \mathscr{H})$ is a unitary representation of the abelian group G, then one defines the **spectrum** $\sigma(\pi)$ as the support of any measure of maximal spectral type.

Lemma 2.8. *For an abelian group G, the following properties hold.*

(i) *If $(\pi, \mathscr{H}_1)$ and $(\rho, \mathscr{H}_2)$ are two unitary representations of G, then $\pi \prec \rho$ if and only if $\sigma(\pi) \subset \sigma(\rho)$.*

(ii) *Every character is weakly contained in the regular representation.*

(iii) Every unitary representation of G is tempered.

Proof. To prove (i), we first claim that for any $f \in L^1(G)$,

$$||\pi(f)||_{\mathrm{op}} = ||\check{f}||_{\sigma(\pi),\infty},$$

where $\check{f} \in L^\infty(\widehat{G})$ is defined as

$$\check{f}(\chi) = \int f\chi\, dm$$

for $\chi \in \widehat{G}$. We use the spectral theory for a vector of maximal spectral type $v_{\max}$ arriving at a commutative diagram:

$$\begin{array}{ccc} \langle v_{\max}\rangle_{\mathscr{H}} & \longrightarrow & L^2_{\mu_{v_{\max}}}(\widehat{G}) \\ {\scriptstyle \pi(f)}\Big\downarrow & & \Big\downarrow{\scriptstyle M_{\check{f}}} \\ \langle v_{\max}\rangle_{\mathscr{H}} & \longrightarrow & L^2_{\mu_{v_{\max}}}(\widehat{G}) \end{array}$$

As the operator $M_{\check{f}}$ has operator norm $||\check{f}||_{\sigma(\pi),\infty}$, the claim follows.

By the claim we conclude that if $\sigma(\pi) \subset \sigma(\rho)$, then for all $f \in L^1(G)$,

$$||\pi(f)||_{\mathrm{op}} = ||\check{f}||_{\sigma(\pi),\infty} \leq ||\check{f}||_{\sigma(\rho),\infty} = ||\rho(f)||_{\mathrm{op}},$$

which implies $\pi \prec \rho$. Conversely assume that $\pi \prec \rho$ but for a contradiction $\sigma(\pi) \not\subset \sigma(\rho)$. So choose $t_0 \in \sigma(\pi)\backslash\sigma(\rho)$ and by Urysohn's Lemma, a function $F \in C_c(U)$ so that $F(t_0) = 1$ but $F \equiv 0$ on $\sigma(\rho)$. As $\widehat{L^1(G)} \subset C_0(\widehat{G})$ is dense with respect to $||\cdot||_\infty$, there is a function $f \in L^1(G)$ so that

$$||\widehat{f} - F||_\infty < \frac{1}{2}.$$

Thus

$$||\pi(f)||_{\mathrm{op}} = ||\check{f}||_{\sigma(\pi),\infty} \geq |\check{f}(t_0) - F(t_0)| \geq \frac{1}{2}$$

and

$$||\rho(f)||_{\mathrm{op}} = ||\check{f} - F||_{\sigma(\rho),\infty} = ||\check{f} - F||_{\sigma(\rho),\infty} < \frac{1}{2},$$

contradicting $\pi \prec \rho$.

We give two proofs of (ii). Recall that by Plancharel's Formula, the regular representation is unitarily isomorphic to $L^2(\widehat{G})$ with the representation $(M_g f)(\chi) = \chi(g)f(\chi)$ for $f \in L^2(\widehat{G})$ and $\chi \in \widehat{G}$. Thus it suffices to show $\chi \prec L^2(\widehat{G})$. We first show $1_G \prec L^2(\widehat{G})$, so let $\varepsilon > 0$ and $K \subset G$ be compact. Let B_n be a sequence of open subsets of $\widehat{G}$ with $B_n \to \{e\}$ in $\widehat{G}$ and set $\psi_n = \frac{\chi_{B_n}}{\sqrt{m(B_n)}}$. Then for $\varepsilon > 0$ we choose n large enough so that for all $\chi \in B_n$ we have that $|\chi(g) - 1| < \varepsilon$ for all $g \in K$. Thus for all $g \in K$,

$$\begin{aligned} |1 - \varphi^M_{\psi_n}(g)| &= |1 - \langle M_g\psi_n, \psi_n\rangle| \\ &= \left|1 - \int_{\widehat{G}} \chi(g)\frac{\chi_{B_n}}{m(B_n)}\, \mathrm{dm}_{\widehat{G}}(\chi)\right| \\ &= \left|\int_{\widehat{G}} (1 - \chi(g))\frac{\chi_{B_n}}{m(B_n)}\, \mathrm{dm}_{\widehat{G}}(\chi)\right| < \varepsilon \end{aligned}$$

which shows that $1_G \prec L^2(\widehat{G})$. An analogous argument works for any character χ.

We give a second proof that $1_G \prec \lambda_G$ using that G is amenable. So for every compact $K \subset G$ and $\varepsilon > 0$ there is a compact set B with

$$\frac{m(B \triangle (k+B))}{m(B)} < \varepsilon$$

for all $k \in K$. We assume without loss of generality that K is symmetric. Consider the function $f_B = \frac{\chi_B}{m(B)}$ which satisfies $||f_B||_1 = 1$. Then for all $k \in K$,

$$||\lambda_G(k) f_B - f_B||_1 < \varepsilon.$$

Thus it follows that if we take the square root $h = \sqrt{f_B}$ so that $||h||_2 = 1$, then we have for all $k \in K$,

$$\begin{aligned}
|1 - \varphi^{\lambda}_{f_B}(k)|^2 &= |\langle \lambda_G(k)h - h, h\rangle|^2 \\
&\leq ||\lambda_G(k)h - h||_2^2 \\
&= \int |h(g+k) - h(g)|^2 \, dm_G(g) \\
&\leq \int |h(g+k)^2 - h(g)^2| \, dm_G(g) \\
&= \int |f_B(g+k) - f_B(g)| \, dm_G(g) \\
&= ||\lambda_G(k) f_B - f_B||_1 < \varepsilon,
\end{aligned}$$

where we used that $|a-b|^2 \leq |a^2 - b^2|$ for all real numbers $a, b \in \mathbb{R}$.

By (ii), $\sigma(\lambda_G) = \widehat{G}$ and thus (iii) follows from (i). $\square$

We return to considering a general topological group G. Another lemma that will turn out to be useful in chapter 4.2 is the next one, for which we introduce the following notion.

Definition 2.9. Let $(\pi, \mathscr{H})$ be a unitary representation of G. The support of π consists of all irreducible unitary representation weakly contained in π, i.e.

$$\operatorname{supp}(\pi) = \{\sigma \in \widehat{G} \, : \, \sigma \prec \pi\}.$$

Lemma 2.10. *Let $(\pi, \mathscr{H})$ be a unitary representation of G. Then the representation*

$$\sigma_{\operatorname{supp}(\pi)} = \bigoplus_{\sigma \in \operatorname{supp}(\pi)} \sigma$$

is weakly equivalent to π, i.e. $\pi \prec \sigma_{\operatorname{supp}(\pi)}$ and $\sigma_{\operatorname{supp}(\pi)} \prec \pi$. In particular, for all $f \in L^1(G)$,

$$||\pi(f)||_{\mathrm{op}} = \sup\{||\sigma(f)||_{\mathrm{op}} \, : \, \sigma \in \operatorname{supp}(\pi)\}.$$

Proof. It is clear that $\sigma_{\operatorname{supp}(\pi)} \prec \pi$, as for each $\sigma \in \operatorname{supp}(\pi)$ we have $\sigma \prec \pi$. The claim $\pi \prec \sigma_{\operatorname{supp}(\pi)}$ follows as the diagonal matrix coefficients of π can be approximated by diagonal matrix coefficients of irreducible unitary representation weakly contained in π, by Proposition 4.33 of [EW]. The last claim is immediate. $\square$

We point out that the representation $\sigma_{\mathrm{supp}(\pi)}$ from the last proposition does not need to be separable, which does not cause any problems.

We finally discuss a general criterion, which implies that a unitary representation is tempered. Namely, we say that a unitary representation $(\pi, \mathscr{H})$ of G is **almost square integrable** if there is a dense set $V \subset \mathscr{H}$ with the property that for all $v \in V$ the diagonal matrix coefficient φ_v^π is contained in $L^{2+\varepsilon}(G)$ for any $\varepsilon > 0$. A proof of the next theorem is exposed in [EW].

Theorem 2.11. *(Theorem 1 of [CHH88]) Every almost square integrable unitary representation is tempered.*

Corollary 2.12. *Let $(\pi, \mathscr{H})$ be a cyclic representation of G with generating vector v. Assume that the diagonal matrix coefficient φ_v^π is almost square integrable. Then $(\pi, \mathscr{H})$ is tempered.*

Proof. Using Theorem 2.11, it suffices to show that for all vectors of the form

$$w = \sum_{i=1}^n \alpha_i \pi_{g_i} v$$

for $\alpha_i \in \mathbb{C}$ and $g_i \in G$ we have that $\varphi_w^\pi \in L^{2+\varepsilon}(G)$ for all $\varepsilon > 0$. To see this note that

$$\varphi_w^\pi = \sum_{i,j=1}^n \alpha_i \overline{\alpha_j} \langle \pi_{g_i} v, \pi_{g_j} v \rangle = \sum_{i,j=1}^n \alpha_i \overline{\alpha_j} \varphi_v^\pi (g_j^{-1} g g_i).$$

Thus it suffices to show that for all $g_i, g_j \in G$, $||\varphi_v^\pi(g_j^{-1} \cdot g_i)||_{2+\varepsilon}$ is finite for all $\varepsilon > 0$. We calculate

$$\begin{aligned} ||\varphi_v^\pi(g_j^{-1} \cdot g_i)||_{2+\varepsilon}^{2+\varepsilon} &= ||\varphi_v^\pi(\cdot g_i)||_{2+\varepsilon}^{2+\varepsilon} \\ &= \int_G |\varphi_v^\pi(g g_i)|^{2+\varepsilon} \, dm_G(g) \\ &= \triangle_G(g_i)^{-1} \int_G |\varphi_v^\pi(g)|^{2+\varepsilon} \, dm_G(g) \\ &= \triangle_G(g_i)^{-1} ||\varphi_v^\pi||_{2+\varepsilon} < \infty, \end{aligned}$$

by assumption. □

It is natural to ask whether the converse of Theorem 2.11 holds. We first provide a simple counterexample. If G is abelian yet non-compact, then G is ameanable and so the trivial representation 1_G is tempered. However the trivial representation is almost square integrable if and only if G is compact. Thus the converse to the above theorem does not hold for non-compact abelian groups. On the other hand, it is clear that the statement holds for compact groups as then all the unitary representations are almost square integrable and tempered. In chapter 2.4, we will show that, roughly speaking, if a group has an Iwasawa decomposition, then the converse to Theorem 2.11 holds.

The final aim of this subchpater is to discuss a suitable topology on the space of unitary representations of G, to which we already alluded to in the beginning of this subchapter. As usual, denote by $\widehat{G}$ the unitary dual, which is defined as the set of all irreducible unitary representations up to isomorphism. More generally we consider the set $\mathscr{U}(G)$ of all equivalence classes of unitary representations and denote by $\mathscr{U}_0(G)$ the subset of the latter set consisting of all unitary representations without invariant vectors. Furthermore we define for a unitary representation $(\pi, \mathscr{H})$ the set

$$\mathcal{P}^1_\pi = \{\phi^\pi = \sum_{j=1}^n \varphi^\pi_{v_j} \,:\, n \in \mathbb{N} \text{ and } v_1, \ldots, v_n \in \mathscr{H}_\pi \text{ so that } \sum_{j=1}^n ||v_j||^2 = 1\}$$

and call its elements the positive-definite functions associated to π.

Definition 2.13. The **Fell topology** on $\mathscr{U}(G)$ is the topology generated by any of the two subbases:

1. For $f \in L^1(G)$ and $\varepsilon \in \mathbb{R}$,
$$\mathscr{F}\mathscr{O}(f, \varepsilon) = \{\pi \in \mathscr{U}(G) \,:\, ||\pi(f)||_{\mathrm{op}} > \varepsilon\}.$$
2. For ϕ is some continuous positive definite function on G, $K \subset G$ a compact subset and $\varepsilon > 0$,
$$\mathscr{F}\mathscr{O}(\phi, K, \varepsilon) = \{\pi \,:\, ||\varphi^\pi - \phi||_{K,\infty} < \varepsilon \text{ for some } \varphi^\pi \in \mathcal{P}^1_\pi\}.$$

A proof that these two subbases generate the same topology is given in chapter 4.4 of [EW]. Using that G is σ-compact and hence $L^1(G)$ is a separable Banach space, it easily follows that the Fell topology is second countable.

Lemma 2.14. *Let $(\pi, \mathscr{H}_1)$ and $(\rho, \mathscr{H}_2)$ be unitary representations of G. Then π is weakly contained in ρ precisely if π is in the closure of $\{\rho\}$ with respect to the Fell topology.*

Proof. Assume $\pi \prec \rho$. Let $f \in L^1(G)$ and $\varepsilon > 0$ be so that $\rho \in \mathscr{F}\mathscr{O}(f, \varepsilon)^c$. Then

$$||\pi(f)|| \leq ||\rho(f)|| \leq \varepsilon$$

and so $\pi \in \mathscr{F}\mathscr{O}(f, \varepsilon)^c$, implying that $\pi \in \overline{\{\rho\}}$.

Conversely for $\pi \in \overline{\{\rho\}}$ assume for a contradiction $\pi \not\prec \rho$. Then there is a function $f \in L^1(G)$ and ε so that

$$||\pi(f)||_{\mathrm{op}} > \varepsilon > ||\rho(f)||_{\mathrm{op}}.$$

Thus $\rho \in \mathscr{F}\mathscr{O}(f, \varepsilon)^c$, yet $\pi \in \mathscr{F}\mathscr{O}(f, \varepsilon)$, contradicting $\pi \in \overline{\{\rho\}}$. $\square$

Proposition 2.15. *Let $(\pi_n, \mathscr{H}_n)_{n\in\mathbb{N}}$ and $(\rho, \mathscr{H})$ be unitary representations of G. The following properties are equivalent.*

(i) In the Fell topology, $\pi_n \to \rho$ as $n \to \infty$.

(ii) For any $f \in L^1(G)$,
$$\liminf_{n\to\infty} ||\pi_n(f)||_{\mathrm{op}} \geq ||\rho(f)||_{\mathrm{op}}.$$

(iii) For any increasing sequence n_k,
$$\rho \prec \bigoplus_{k\in\mathbb{N}} \pi_{n_k}$$

Proof. Assume (i). For any $f \in L^1(G)$ and $\varepsilon > 0$, $\mathscr{F}\mathscr{O}(f, ||\rho(f)||_{\mathrm{op}} - \varepsilon)$ is a neighborhood of ρ and hence for large enough n, $\pi_n \in \mathscr{F}\mathscr{O}(f, ||\rho(f)||_{\mathrm{op}} - \varepsilon)$ which implies (ii).

To see (ii) implies (iii) just use for $f \in L^1(G)$,

$$\left|\left| \left(\bigoplus_{k\in\mathbb{N}} \pi_{n_k} \right) (f) \right|\right|_{\mathrm{op}} = \sup_{k\in\mathbb{N}} ||\pi_{n_k}(f)||.$$

Finally assume (iii). Assume for a contradiction that π_n does not converge to ρ. Then there is some neighborhood U of ρ so that for an increasing sequence n_k, the unitary representations π_{n_k} are outside of U. Upon using a subsequence of n_k we can assume without loss generality that $U = \mathscr{F}\mathscr{O}(f, \varepsilon)$ for $f \in L^1(G)$ and $\varepsilon \in \mathbb{R}$. Thus

$$||\pi_{n_k}(f)||_{\mathrm{op}} \leq \varepsilon < ||\rho(f)||_{\mathrm{op}},$$

which contradicts (iii). □

2.2 Continuous Decomposition of Unitary Representations

We first discuss the direct integral of Hilbert spaces – a generalization of the direct sum – and then apply the developed material to deduce a general continuous decomposition of unitary representations. A reference for some parts of this chapter is [Kir76], yet we strive upon giving a more detailed treatment.

Let (X, μ) be a measure space and for each $x \in X$ denote by $\mathscr{H}_x$ a separable Hilbert space. We aim at defining a Hilbert space

$$\int_X^{\oplus} \mathscr{H}_x \, d\mu(x).$$

which should consist of functions

$$f : X \to \bigcup_{x\in X} \mathscr{H}_x$$

with the property that for each $x \in X$, $f(x) \in \mathscr{H}_x$. Such functions are called **sections**. The inner product should be

$$\langle f_1, f_2 \rangle = \int \langle f_1(x), f_2(x) \rangle_{\mathscr{H}_x} \, d\mu(x). \tag{2.1}$$

However, a priori the function $x \mapsto \langle f_1(x), f_2(x) \rangle_{\mathscr{H}_x}$ does not have to be measurable.

In order to circumvent this issue, consider the collection of Hilbert spaces $(\mathscr{H}_x)_{x\in X}$ together with a choice of measurable sections $\mathscr{M}$. More precisely, we require that $\mathscr{M}$ is a set of sections that satisfies the following properties:

1. For all $f_1, f_2 \in \mathscr{M}$, the function $x \mapsto \langle f_1(x), f_2(x) \rangle_{\mathscr{H}_x}$ is measurable.
2. If f is a section so that $x \mapsto \langle f(x), g(x) \rangle_{\mathscr{H}_x}$ is measurable for all $g \in \mathscr{M}$, then $f \in \mathscr{M}$.
3. There is a countable collection $f_1, f_2, \ldots$ in $\mathscr{M}$ so that for all $x \in X$, the span of the collection $\{f_n(x) : n \geq 1\}$ is dense in $\mathscr{H}_x$.

From now on we always view a collection $(\mathscr{H}_x)_{x\in X}$ as equipped with a choice of measurable sections. In dependence on $\mathscr{M}$, we define the **direct integral**

$$\mathscr{H}_{(X,\mu)} = \int_X^{\oplus} \mathscr{H}_x \, d\mu(x)$$

as the vector space of measurable sections $f \in \mathscr{M}$ that satisfy

$$\int ||f(x)||^2_{\mathscr{H}_x} \, d\mu(x) < \infty.$$

The vector space $\mathscr{H}_{(X,\mu)}$ is equipped with the inner product (2.1).

Proposition 2.16. *The direct integral $\mathscr{H}_{(X,\mu)}$ is a Hilbert space.*

Proof. It is clear that (2.1) defines an inner product. It remains to check completeness. The following proof is inspired by the proof of the Fischer-Riesz theorem, showing that any L^p-space is complete.

Consider a sequence $f_n \in \mathscr{H}_{(X,\mu)}$ so that

$$M = \sum_{n=1}^{\infty} ||f_n||_{\mathscr{H}_{(X,\mu)}} < \infty.$$

We aim to show that $\sum_{n=1}^{\infty} f_n$ converges in $\mathscr{H}_{(X,\mu)}$.

For each n define

$$h_n(x) = \sum_{k=1}^{n} ||f_k(x)||_{\mathscr{H}_x}.$$

Then h_n is clearly a measurable function on X as it is a finite sum of measurable functions. By the triangle inequality,

$$\int_X |h_n(x)|^2 \, d\mu(x) = ||h_n||_2^2 \le \left(\sum_{k=1}^{n} ||f_k||_{\mathscr{H}_{(X,\mu)}} \right)^2 \le M^2.$$

Moreover $h_n \uparrow h$ for $h : X \to [0, \infty]$ a measurable function satisfying by monotone convergence

$$||h||_2^2 = \lim_{n\to\infty} ||h_n||_2^2 \le M^2.$$

Thus for almost all $x \in X$, the sum $\sum_{n=1}^{\infty} f(x)$ is a well defined element of $\mathscr{H}_x$ and hence we set $f(x) = \sum_{n=1}^{\infty} f(x)$ defined for almost all $x \in X$.

We claim that f is a measurable section. In order to prove this we use the second property in the definition of measurable sections. So let $g \in \mathscr{M}$. Then for almost all $x \in X$,

$$\langle f(x), g(x) \rangle_{\mathscr{H}_x} = \lim_{n\to\infty} \sum_{k=1}^{n} \langle f_k(x), g(x) \rangle_{\mathscr{H}_x}.$$

The finite sums on the right hand side are clearly measurable as each $f_k \in \mathscr{M}$. Thus the function on the left hand side is the pointwise limit of measurable functions and hence by itself measurable. Thus we conclude $f \in \mathscr{M}$. Moreover, as by the triangle inequality we have pointwise $||f(x)||_{\mathscr{H}_x} \le h(x)$, it follows

$$||f||^2_{\mathscr{H}_{(X,\mu)}} = \int ||f(x)||^2_{\mathscr{H}_x} \, d\mu(x) \le \int |h(x)|^2 \, d\mu(x) \le M^2.$$

Hence $f \in \mathscr{H}_{(X,\mu)}$.

It remains to check that $\sum_{k=1}^n f_k \to f$ in $\mathscr{H}_{(X,\mu)}$, i.e.

$$\left|\left|\sum_{k=1}^n f_k - f\right|\right|_{\mathscr{H}_{(X,\mu)}} \to 0.$$

We note that pointwise

$$\left|\left|\sum_{k=1}^n f_k(x) - f(x)\right|\right|^2_{\mathscr{H}_x} \le (2h(x))^2$$

and we clearly have pointwise convergence. So we just use dominated convergence for

$$\left|\left|\sum_{k=1}^n f_k - f\right|\right|_{\mathscr{H}_{(X,\mu)}} = \int_X \left|\left|\sum_{k=1}^n f_k - f\right|\right|^2_{\mathscr{H}_x} d\mu(x),$$

which concludes the proof. □

We next discuss a few examples. We first observe that the direct integral is indeed a generalization of the direct sum. More precisely, let $(\mathscr{H}_n)_{n\in\mathbb{N}}$ be a countable collection of Hilbert spaces. We view $\mathbb{N}$ as a discrete topological space and hence clearly every section is measurable. Moreover we denote by μ the counting measure on $\mathbb{N}$. Then the map

$$\bigoplus_{n\in\mathbb{N}} \mathscr{H}_n \longrightarrow \int_{\mathbb{N}}^{\oplus} \mathscr{H}_n \, d\mu(n), \qquad (v_n)_{n\in\mathbb{N}} \longmapsto (n \in \mathbb{N} \mapsto v_n)$$

is an isometric isomorphism of Hilbert spaces.

On the other hand, one can also view the direct integral as a generalization of $L^2_\mu(X)$. More precisely, set $\mathscr{H}_x = \mathbb{C}$ for all $x \in X$ and choose $\mathscr{M}$ to be the smallest set of measurable sections that contains all sections corresponding to measurable functions. Then clearly $\mathscr{M}$ corresponds precisely to the set of measurable functions and the map

$$L^2_\mu(X) \longrightarrow \int_X^{\oplus} \mathbb{C}\, d\mu(x), \qquad f \longmapsto (x \in X \mapsto f(x))$$

is again an isometric isomorphism.

If for each $x \in X$, we have a bounded operator $T_x \in \mathscr{B}(\mathscr{H}_x, \mathscr{H}_x)$, we want to define a bounded operator

$$T = \int_X^{\oplus} T_x \, d\mu(x).$$

In order to arrive at a well defined operator, we need to assume for all $f_1, f_2 \in \mathscr{H}_{(X,\mu)}$ that the map

$$x \in X \longmapsto \langle T_x f_1(x), f_2(x)\rangle_{\mathscr{H}_x}$$

is measurable. Moreover, we assume that the function $x \mapsto ||T_x||_{\text{op}}$ is in $L^\infty_\mu(X)$. We denote by $||T||_\infty$ the latter $L^\infty_\mu(X)$ norm. Then we define T by

$$(Tf)(x) = T_x f(x)$$

for $f \in \mathscr{H}_{((X,\mu))}$, yielding a well defined operator T with operator norm $||T||_\infty$.

In particular if for each $x \in X$, the Hilbert space $\mathscr{H}_x$ carries a unitary representation π_x of the group G, then if we assume that for every fixed $g \in G$, the collection $\pi_{x,g} = (\pi_x)_g$ is a measurable collection of operators, then we can define the unitary representation

$$\pi = \pi_{(X,\mu)} = \int_X^\oplus \pi_x \, d\mu(x)$$

by

$$\pi_g = \int_X^\oplus \pi_{x,g} \, d\mu(x).$$

Given a unitary representation of a group G, we want to discuss how to decompose any representation as a direct integral of irreducible representations. In the case of abelian groups such a decomposition is straightforward consequence of Bochner's theorem and some ideas related in the proof can be generalized.

More precisely let $(\pi, \mathscr{H})$ be a cyclic representation of an abelian group G with cyclic vector v. By Bochner's theorem, there is a unique measure μ_v on $\widehat{G}$ so that

$$\varphi_v^\pi(g) = \int_{\widehat{G}} \chi(g) \, d\mu_v(\chi)$$

for all $g \in G$. Then the equivariant map

$$(\mathscr{H}, \pi) \longrightarrow \left(\mathscr{H}_{(X,\mu_v)} = \int_{\widehat{G}}^\oplus \mathbb{C} \, d\mu_v(\chi), \pi_{(X,\mu_v)} = \int_{\widehat{G}} \chi \, d\mu_v(\chi) \right),$$

which is characterized by the property that $\pi_g v$ is mapped to the section $(\chi \mapsto \chi(g))$, is an isomorphism of representations. To see the last claim, we note that the only problem is to show that the map is surjective or equivalently that $(\pi_{(X,\mu_v)}, \mathscr{H}_{(X,\mu_v)})$ is a cyclic representation. To prove this, denote by $1_{\widehat{G}}$ the constant section. Then notice that for $f \in L^1(G)$,

$$\begin{aligned}(\pi_{(X,\mu_v)}(f)1_{\widehat{G}})(\chi) &= \int_G f(g)((\pi_{(X,\mu_v)})_g 1_G)(\chi) \, dm_G(g) \\ &= \int_{\widehat{G}} f(g)\chi(g) \, dm_G(g) = \check{f}(\chi).\end{aligned}$$

As the functions $\{\check{f} : f \in L^1(G)\}$ are dense in $C_0(\widehat{G})$, the claim follows.

Towards more general groups, we briefly review a proof of Bochner's theorem. Denote by $\mathscr{P}^1(G)$ the set of continuous positive definite functions ϕ on G with $\phi(e) = 1$. We assume without loss of generality that the cyclic vector v as in the above example has unit norm so that $\varphi_v^\pi \in \mathscr{P}^1(G)$. Since G is abelian, each irreducible representation of G is one-dimensional and hence corresponds to a unique element of $\mathscr{P}^1(G)$.

As the matrix coefficients of irreducible representations correspond precisely to extremal elements of $\mathscr{P}^1(G)$, by applying Choquet's theorem we arrive at a probability measure μ_v on the extremal elements of $\mathscr{P}^1(G)$ which represents φ_v^π. By the argument in the last paragraph, we can view μ as a measure on $\widehat{G}$. In particular for each $\ell \in (L^\infty(G))^*$,

$$\ell(\varphi_v^\pi) = \int_{\widehat{G}} \ell(\chi) \, d\mu_v(\chi).$$

By choosing ℓ to be the evaluation map at $g \in G$, Bochner's theorem follows.

Proposition 2.17. *Let $(\pi, \mathscr{H})$ be a cyclic representation of G. Then there exists a compact metric space X with a probability measure μ on X and irreducible representations $(\pi_x, \mathscr{H}_x)$ for $x \in X$ so that $(\pi, \mathscr{H})$ is unitarily isomorphic to the representation*

$$\mathscr{H}_{(X,\mu)} = \int_X^{\oplus} \mathscr{H}_x \, d\mu(x), \qquad \pi_{(X,\mu)} = \int_X^{\oplus} \pi_x \, d\mu(x).$$

Proof. The strategy of the proof is analogous to the above outline of Bochner's theorem, yet we won't carry out the details. In contrast to the abelian case, the irreducible representations do not have to be one dimensional and there might be multiple extremal elements of $\mathscr{P}^1(G)$ corresponding to the same irreducible unitary representation.

Assume without loss of generality that $(\pi, \mathscr{H})$ is cyclic with cyclic vector of unit norm $v \in \mathscr{H}$. Denote by X the space of extremal elements of $\mathscr{P}^1(G)$. Again by Choquet's theorem, there is a Borel measure μ on X so that for all $\ell \in (L^\infty(G))^*$ (with respect to the weak* topology) we have

$$\ell(\varphi_v^\pi) = \int_X \ell(\phi_x) \, d\mu(x).$$

For the remainder of the proof we refer to [Kir76]. □

Lemma 2.18. *Let $(\pi, \mathscr{H})$ be a unitary representation of G and*

$$\pi = \int_X^{\oplus} \pi_x \, d\mu(x)$$

be an integral decomposition. Then for almost all $x \in X$, π_x is weakly contained in π.

Proof. Note that for all $f \in L^1(G)$, $||\pi(f)||$ is the essential supremum of $x \mapsto ||\pi_x(f)||$. Thus for fixed f, $||\pi_x(f)|| \leq ||\pi(f)||$ for almost all x. The claim follows as $L^1(G)$ is separable. □

2.3 Induced Representations and the Harish-Chandra Spherical Function

We consider unimodular groups G with an Iwasawa decomposition. More precisely we assume that we can write $G = KB$ for $K, B \subset G$ closed subgroups, where K is assumed to be compact. For example, if F is a local field of characteristic zero then the group of F-points of a semisimple algebraic group over F has an Iwasawa decomposition.

Denote by m_K the Haar probability measure on K, by m_B a left Haar measure on B and by $m_B^{(r)}$ the associated right Haar measure so that

$$\int_B f(b) \, dm_B^{(r)}(b) = \int_B f(b^{-1}) \, dm_B(b) = \int_B \triangle_B(b^{-1}) f(b) \, dm_B(b)$$

for all $f \in L^1(B)$. Further, recall that the modular character $\triangle_B$ satisfies for all $f \in L^1(B)$ and $h \in B$,

$$\int_B f(hb)\, dm_B^{(r)}(b) = \triangle_B(h) \int_B f(b)\, dm_B^{(r)}(b).$$

Lemma 2.19. *Let G be unimodular with an Iwasawa decomposition $G = KB$. Let m_G be a Haar measure on G. Then there is a suitable normalization of $dm_B^{(r)}$ so that for all $f \in L^1(G)$,*

$$\begin{aligned} \int_G f(g)\, dm_G(g) &= \int_B \int_K f(kb)\, dm_K(k) dm_B^{(r)}(b) \\ &= \int_B \int_K f(kb) \triangle_B(b^{-1})\, dm_K(k) dm_B(b). \end{aligned} \tag{2.2}$$

Proof. The presented proof can be found in chapter 8.3 of [Kna02]. Write $P = K \cap B$ and note that P is a compact subgroup of G. The map $(k, b) \mapsto kb^{-1}$ descends to a homeomorphism

$$(K \times B)/\operatorname{diag} P \to G$$

as multiplication $K \times B \to G$ is an open map. By a slight abuse of notation, we again denote by m_G the pull back of the Haar measure on G onto $(K \times B)/\operatorname{diag} P$.

Consider on $K \times B$ the measure m defined as

$$\int_{K \times B} g(k, b)\, dm(g) = \int_{(K \times B)/\operatorname{diag} P} \int_P g(kp, bp)\, dm_P(p) dm_G(k, b), \tag{2.3}$$

where $dm_P(p)$ is the Haar probability measure on P and $g \in L^1(K \times B)$. It is clear that m is a Haar measure on $K \times B$.

Finally, for a function $f \in L^1(G)$ we consider the function $(k, b) \mapsto f(kb^{-1})$ so that the inner integral over P in (2.3) is constant. Thus

$$\int f(g)\, dm_G(g) = \int_{K \times B} f(kb^{-1})\, dm_K(k) dm_B(b),$$

which implies the claim. $\square$

In the following, we discuss how to lift a representation on B onto the whole group G. For simplicity we only consider unitary characters χ on B, i.e. continuous group homomorphisms $\chi : B \to \mathbb{S}^1$. We aim to define the **induced representation** $(\pi_\chi, \mathscr{H}_\chi)$ which also will be denoted as

$$\operatorname{Ind}_B^G(\chi).$$

Towards defining the Hilbert space $\mathscr{H}_\chi$, we first consider

$$\mathscr{V}_\chi = \{f : G \to \mathbb{C} \text{ measurable} : ||f|_K||_{L^2(K)} < \infty \text{ and (2.4) holds}\},$$

where we define (2.4) to be the property that for all $g \in G$ and $b \in B$, it holds that

$$f(gb) = \chi(b) \triangle_B(b)^{\frac{1}{2}} f(g). \tag{2.4}$$

We equip $\mathscr{V}_\chi$ with the inner product

$$\langle f_1, f_2 \rangle_{\mathscr{V}_\chi} = \int_K f_1(k)\overline{f_2(k)}\, dm_K.$$

Then we define $\mathscr{H}_\chi$ as the completion of $\mathscr{V}_\chi$ and for each $g \in G$ we aim to define $(\pi_\chi)_g = \pi_{\chi,g}$ as the extension of the regular representation on $\mathscr{V}_\chi$, i.e. the representation

$$(\pi_{\chi,g} f)(x) = f(g^{-1}x)$$

for $f \in \mathscr{V}_\chi$ and $x \in G$. However, in this generality, it is not clear whether $\pi_{\chi,g}$ is well defined on $\mathscr{V}_\chi$. If we require the additional property that the Iwasawa decomposition of each element $g \in G$ is unique, then we show in the next proposition that $(\pi_{\chi,g})$ is indeed a unitary operator.

Proposition 2.20. *Assume $G = KB$ has an Iwasawa decomposition and additionally assume that*

$$K \times B \longrightarrow G, \qquad (k, b) \mapsto kb$$

is a homeomorphism. Then the map

$$\mathscr{V}_\chi \longrightarrow L^2(K), \qquad f \longmapsto f|_K$$

is an isomorphism of inner product spaces and so in particular, $\mathscr{V}_\chi$ is complete and $\mathscr{V}_\chi = \mathscr{H}_\chi$.

Moreover, for any unitary character χ on B, $(\pi_\chi, \mathscr{H}_\chi)$ is a unitary representation.

Proof. It is clear that restriction to K is an isometry of Hilbert spaces and hence it remains to show that the above map is surjective. So let $f_K \in L^2(K)$ and define for $k \in K$ and $b \in B$ the function f on G by

$$f(kb) = \chi(b)\triangle_B(b)^{\frac{1}{2}} f_K(k).$$

The function f is well defined on G as each element has a unique Iwasawa decomposition. In order to check (2.4) let $g = k'b' \in G$ for $k' \in K$ and $b' \in B$ and let $b \in B$ be another element. Then using that χ and $\triangle_B$ are group homomorphisms,

$$\begin{aligned} f(gb) = f(k'b'b) &= \chi(b'b)\triangle_B(b'b)^{\frac{1}{2}} f_K(k') \\ &= \chi(b)\triangle_B(b)^{\frac{1}{2}} \left(\chi(b')\triangle_B(b')^{\frac{1}{2}} f_K(k')\right) \\ &= \chi(b)\triangle_B(b)^{\frac{1}{2}} f(g). \end{aligned}$$

Fix $g \in G$ and write for $k \in K$, $g^{-1}k = c_k b_k$ for $c_k \in K$ and $b_k \in B$. Then for $f \in \mathscr{H}_\chi$,

$$f(g^{-1}k) = f(c_k b_k) = \chi(b_k)\triangle_B(b_k)^{\frac{1}{2}} f(c_k)$$

and

$$\begin{aligned} ||\pi_{\chi,g} f||^2_{\mathscr{H}_\chi} &= \int_K |f(g^{-1}k)|^2\, dk \\ &= \int_K \triangle_B(b_k)|\chi(b_k) f(c_k)|^2\, dk \\ &= \int_K \triangle_B(b_k)|f(c_k)|^2\, dk, \end{aligned}$$

where we used in the last line that χ is a unitary character. Thus to prove that $\pi_{\chi,g}$ is a unitary operator, it remains to check

$$||f||^2_{\mathscr{H}_\chi} = \int_K |f(k)|^2 \, dk = \int_K \triangle_B(b_k)|f(c_k)|^2 \, dk.$$

To see this consider more generally a function $\varphi \in L^1(G)$. As G is unimodular,

$$\begin{aligned}\int_B \int_K \varphi(kb) \, dm_K(k) dm_B^{(r)}(b) &= \int \varphi(h) \, dm_G(h) = \int \varphi(g^{-1}h) \, dm_G(h) \\ &= \int_B \int_K \varphi(g^{-1}kb) \, dm_K(k) dm_B^{(r)}(b) \\ &= \int_B \int_K \varphi(c_k b_k b) \, dm_K(k) dm_B^{(r)}(b) \\ &= \int_B \int_K \varphi(c_k b) \triangle_B(b_k) \, dm_K(k) dm_B^{(r)}(b).\end{aligned}$$

The prove from the last equality the above claim, we again evoke the uniqueness of the Iwasawa decomposition. Set $\varphi(kb) = |f(k)|^2\psi(b)$ for $\psi \in L^1(B)$ with $\int \psi \, dm_B^{(r)} = 1$. Then φ is a well defined function on G by uniqueness of the Iwasawa decomposition and the claim follows by Fubini's Theorem.

Finally the continuity condition for unitary representations follows by using that $C_c(K) \subset L^2(G)$ is dense. □

The last proposition is useful for semisimple Lie groups, as the Iwasawa decomposition of each element is unique. However, algebraic groups over local fields $\neq \mathbb{R}$ usually fail to have this property. In order to also treat the latter case, we require in the remainder the **additional assumption** that

$$\triangle_B|_{K\cap B} \equiv 1. \tag{2.5}$$

If the Iwasawa decomposition is unique, then $K \cap B = \{e\}$ and hence (2.5) is satisfied. To give an example where the Iwasawa decomposition is not unique yet (2.5) is still satisfied, consider $G = \mathrm{SL}_2(\mathbb{Q}_p) = K_p B_p$ for K_p and B_p as defined in chapter 1.1. Then recall for $a, b \in \mathbb{Q}_p$ with $a \neq 0$,

$$\triangle_{B_p}\left(\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix}\right) = |a|_p^{-2}.$$

Thus as

$$K_p \cap B_p = \left\{\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix} : a, b \in \mathbb{Q}_p \text{ with } |a|_p = 1 \text{ and } |b|_p \leq 1\right\},$$

it follows that indeed $\triangle_{B_p}|_{K_p \cap B_p} \equiv 1$.

We next aim to generalize Proposition 2.20 for groups that satisfy (2.5). In order to do so, we need to restrict to unitary characters $\chi : B \to \mathbb{S}^1$ that satisfy the analogous assumption

$$\chi|_{K\cap B} \equiv 1. \tag{2.6}$$

Then one defines $(\pi_\chi, \mathscr{H}_\chi)$ analogously to before.

Proposition 2.21. *Let $G = KB$ be a group with an Iwasawa decomposition so that* (2.5) *holds and consider a unitary character $\chi : B \to \mathbb{S}^1$ that satisfies* (2.6)*. Then $(\pi_\chi, \mathscr{H}_\chi)$ is a unitary representation.*

Proof. Denote by $L^2(K, B)$ the subspace of $L^2(K)$ consisting of functions that are right-invariant under $K \cap B$. Then we claim that

$$\mathscr{V}_\chi \longrightarrow L^2(K, B), \qquad f \mapsto f|_K$$

is an isometry of inner product spaces, which again implies $V_\chi = \mathscr{H}_\chi$. To see that the map is well defined, we observe for $f \in \mathscr{V}_\chi$ and for $k_1, k_2 \in K \cap B$ that

$$f(kk_1) = \chi(k_1)\triangle_B(k_1)^{\frac{1}{2}} f(k) = \chi(k_2)\triangle_B(k_2)^{\frac{1}{2}} f(k) = f(kk_2).$$

Thus indeed $f|_K$ is right-invariant under $K \cap B$.

It remains to check that the map is surjective. So consider $f_K \in L^2(K, B)$ and define

$$f(kb) = \chi(b)\triangle_B(b)^{\frac{1}{2}} f_K(k).$$

The function f is indeed well-defined on G as if for $g \in G$ we can write $g = k_1 b_1 = k_2 b_2$ with $k_1, k_2 \in K$ and $b_1, b_2 \in B$, then $k_2^{-1} k_1 = b_2 b_1^{-1} \in K \cap B$. By (2.5) and (2.6) it follows that $\chi(b_1)\triangle_B(b_1)^{\frac{1}{2}} = \chi(b_2)\triangle_B(b_2)^{\frac{1}{2}}$ and this implies as f_K is right invariant under $K \cap B$ and by (2.5),

$$f(k_1 b_1) = \chi(b_1)\triangle_B(b_1)^{\frac{1}{2}} f_K(k_1) = \chi(b_2)\triangle_B(b_2)^{\frac{1}{2}} f_K(k_2) = f(k_2 b_2),$$

showing that f is indeed well defined. The same calculation as in the proof of Proposition 2.20 shows that f is indeed an element of $\mathscr{V}_\chi$.

To show that $(\pi_\chi, \mathscr{H}_\chi)$ is indeed a unitary representation we again apply the same proof as in Proposition 2.20. The only difference is that in the last part, we choose $\psi \in L^1(B)$ to be a $K \cap B$-invariant function with $\int \psi \, dm_B^{(r)} = 1$ so that φ is again well-defined on G. Note that such a function ψ can be constructed by averaging over $K \cap B$. □

If χ is the tivial character, then we write $(\pi_0, \mathscr{H}_0) = (\pi_\chi, \mathscr{H}_\chi)$. We denote by f_0 the element of $\mathscr{H}_0$, whose restriction to K is $\equiv 1$. By the proof of Lemma 2.21, f_0 is indeed a well defined element of $\mathscr{H}_0$ and of the form

$$f_0(kb) = \triangle_B(b)^{\frac{1}{2}}$$

for $b \in B$ and $k \in K$.

Definition 2.22. The **Harish-Chandra spherical function** is defined as

$$\Xi(g) = \langle \pi_{0,g} f_0, f_0 \rangle_{\mathscr{H}_0} = \int_K f_0(g^{-1}k)\overline{f_0(k)} \, dm_K(k).$$

As f_0 is left-K-invariant, it follows that the Harish-Chandra spherical function is bi-K-invariant. Moreover, it was proved by Harish-Chandra ([HC58], [HC73]) that if G are the F-points of a a semisimple algebraic group over F, where F is a local field, then the additional assumption (2.5) holds and $\Xi \in L^{2+\varepsilon}(G)$ for all $\varepsilon > 0$, i.e. Ξ is almost-square integrable. Inspired by this property, we give the following definition.

Definition 2.23. Let G be a unimodular group that can be written as $G = KB$ for $K, B \subset G$ closed subgroups, where K is assumed to be compact. We call $G = KB$ a **Harish-Chandra group** if the following two properties are satisfied:

(i) $\triangle_B|_{K \cap B} \equiv 1$.

(ii) Ξ is almost square integrable.

Lemma 2.24. *A finite product of Harish-Chandra groups is again a Harish-Chandra group.*

Proof. Let $G_1, \ldots, G_n$ be Harish-Chandra groups with decompositions $G_i = K_i B_i$. Set $G = G_1 \times \ldots \times G_n$, $K = K_1 \times \ldots \times K_n$ and $B = B_1 \times \ldots \times B_n$. Then $K \subset G$ is compact and $G = KB$. Denote by Ξ_G and Ξ_{G_i} the Harish-Chandra function of G and G_i, then for $g = (g_1, \ldots, g_n)$,

$$\Xi_G(g) = \prod_{i=1}^{n} \Xi_{G_i}(g_i),$$

which implies the claim. $\square$

Corollary 2.25. *Let* $\mathrm{G} \subset \mathrm{GL}_n$ *be a semisimple algebraic group over* $\mathbb{Q}$ *and* S *a finite set of places. Then* $G_S = \prod_{p \in S} G(\mathbb{Q}_p)$ *is a Harish-Chandra group.*

Proof. This follows immediately from the last lemma and the discussion from before. $\square$

We next prove a calculative lemma of later use. Let $G = KB$ be a Harish-Chandra group. For $f \in L^2(G)$ we define the function $\widetilde{f}$ as

$$\widetilde{f}(g) = \left(\int_B |f(gb)|^2 \, dm_B^{(r)}(b) \right)^{\frac{1}{2}}$$

for all $g \in G$.

Lemma 2.26. *Let* $G = KB$ *be a Harish-Chandra group. If* $f \in L^2(G)$*, then* $\widetilde{f} \in \mathscr{H}_0$ *and* $||\widetilde{f}||_{\mathscr{H}_0} = ||f||_2$*. Moreover for all* $f_1, f_2 \in L^2(G)$ *and* $g \in G$,

$$|\langle \lambda_g f_1, f_2 \rangle_2| \leq \langle \pi_{0,g} \widetilde{f}_1, \widetilde{f}_2 \rangle_{\mathscr{H}_0}.$$

Proof. We check that $\widetilde{f} \in \mathscr{H}_0$. It is clear that f is measurable. If $g \in G, b_0 \in B$,

$$\begin{aligned}
\widetilde{f}(gb_0) &= \left(\int_B |f(gb_0 b)|^2 \, dm_B^{(r)}(b) \right)^{\frac{1}{2}} \\
&= \left(\triangle_B(b_0) \int_B |f(gb)|^2 \, dm_B^{(r)}(b) \right)^{\frac{1}{2}} \\
&= \triangle_B(b_0)^{\frac{1}{2}} \widetilde{f}(g).
\end{aligned}$$

Moreover

$$
\begin{aligned}
||\widetilde{f}||^2_{\mathscr{H}_0} &= \int_K |\widetilde{f}(k)|^2 \, dm_K(k) \\
&= \int_K \int_B |f(kb)|^2 \, dm_B^{(r)}(b) dm_K(k) \\
&= \int_G |f(g)|^2 \, dm_G(g) = ||f||_2^2 < \infty.
\end{aligned}
$$

Thus $\widetilde{f} \in \mathscr{H}_0$ and $||\widetilde{f}||_{\mathscr{H}_0} = ||f||_2$. If $f_1, f_2 \in L^2(G)$ and $g \in G$,

$$
\begin{aligned}
|\langle \lambda_g f_1, f_2 \rangle_2| &= \left| \int_G f_1(g^{-1}h) \overline{f_2(h)} \, dm_G(h) \right| \\
&= \left| \int_K \int_B f_1(g^{-1}kb) \overline{f_2(kb)} \, dm_B^{(r)}(b) dm_K(k) \right| \\
&\leq \int_K \int_B |f_1(g^{-1}kb)| \, |f_2(kb)| \, dm_B^{(r)}(b) dm_K(k) \\
&\leq \int_K \left(\int_B |f_1(g^{-1}kb)|^2 \, dm_B^{(r)}(b) \right)^{\frac{1}{2}} \\
&\qquad \left(\int_B |f_2(kb)|^2 \, dm_B^{(r)}(b) \right)^{\frac{1}{2}} dm_K(k) \\
&\leq \int_K \widetilde{f}_1(g^{-1}k) \widetilde{f}_2(k) \, dm_K(k) = \langle \pi_{0,g} \widetilde{f}_1, \widetilde{f}_2 \rangle_{\mathscr{H}_0},
\end{aligned}
$$

where we used the Cauchy-Schwarz inequality in the fourth line. □

We prove another lemma, which will turn out to be useful.

Lemma 2.27. *Let $G = KB$ be a Harish-Chandra group. If $f \in L^2(G)$ is left K-invariant, then*

$$\widetilde{f} = ||\widetilde{f}||_{\mathscr{H}_0} f_0.$$

Moreover, if $f_1, f_2 \in L^2(G)$ are left K-invariant, then

$$|\langle \lambda_g f_1, f_2 \rangle_2| \leq \Xi(g) ||f_1||_2 ||f_2||_2.$$

Proof. Let $f \in L^2(G)$ be left K-invariant. Then $\widetilde{f} \in \mathscr{H}_0$. Moreover, as $\mathscr{H}_0$ can be viewed as a subspace of $L^2(K)$ and as the constant functions are up to scaling the only left K-invariant functions in $L^2(K)$, the first equality follows since $||f_0||_{\mathscr{H}_0} = 1$.

By Proposition 2.26 and the first equality,

$$|\langle \lambda_g f_1, f_2 \rangle_2| \leq \langle \pi_g \widetilde{f}_1, \widetilde{f}_2 \rangle_{\mathscr{H}_0} \leq ||\widetilde{f}_1||_{\mathscr{H}_0} ||\widetilde{f}_2||_{\mathscr{H}_0} \langle \pi_g f_0, f_0 \rangle_{\mathscr{H}_0} = \Xi(g) ||f_1||_2 ||f_2||_2.$$

□

2.4 Tempered Representations of Harish-Chandra Groups

The aim of this subchapter is to prove the following theorem, which is the announced converse to Theorem 2.11.

Theorem 2.28. *([CHH88] Theorem 2) Let $G = KB$ be a Harish-Chandra group and let $(\pi, \mathscr{H})$ be a unitary representation of G. The following properties are equivalent.*

(a) π is almost square integrable.

(b) π is tempered.

(c) For all K-finite vectors $v, w \in \mathscr{H}$ with $d_v = \dim(\langle \pi(K)v \rangle)$ and $d_w = \dim(\langle \pi(K)w \rangle)$, it holds that

$$|\langle \pi_g v, w \rangle| \leq \sqrt{d_v d_w}\, ||v||\, ||w||\, \Xi(g).$$

Before proceeding with the proof, we recall that the convolution of two functions $f_1, f_2 \in L^1(G)$ is defined as

$$\begin{aligned}(f_1 * f_2)(x) &= \int f_1(g) f_2(g^{-1}x)\, dm_G(g) \\ &= \int f_1(xg^{-1}) f_2(g)\, dm_G(g).\end{aligned}$$

Thus in particular for $f_1, f_2 \in L^2(G)$ and $h \in G$,

$$(\lambda_G(f_1)f_2)(h) = \int f_1(g) f_2(g^{-1}h)\, dm_G(g) = (f_1 * f_2)(h).$$

Moreover if $f \in L^1(G)$, we set

$$f^\vee(x) = f(x^{-1}), \qquad \text{and} \qquad f^* = \overline{f^\vee}.$$

Let $(\pi, \mathscr{H})$ be a unitary representation and for $v, w \in \mathscr{H}$ write $\phi = \varphi^\pi_{v,w}$. Then for $f_1, f_2 \in L^1(G)$ and $h \in G$,

$$\begin{aligned}(\overline{f_2} * \phi * f_1^\vee)(h) &= \int_G (\overline{f_2} * \phi)(hg^{-1}) f_1^\vee(g)\, dm_G(g) \\ &= \int_G (\overline{f_2} * \phi)(hg) f_1(g)\, dm_G(g) \\ &= \int_G \int_G \overline{f_2}(h) \phi(s^{-1}hg) f_1(g)\, dm_G(g) dm_G(s) \\ &= \int_G \int_G \langle \pi_h f_1(g) \pi_g v, f_2(s) \pi_s w \rangle\, dm_G(g) dm_G(s) \\ &= \langle \pi_h \pi(f_1) v, \pi(f_2) w \rangle. \end{aligned} \tag{2.7}$$

Lemma 2.29. *Let $(\pi, \mathscr{H})$ be a unitary representation of a compact group K and let v be a K-finite vector in $\mathscr{H}$. Then there exists a function $f_v \in C(K)$ so that*

$$f_v = f_v * f_v = f_v^*, \qquad \pi(\overline{f_v})v = v$$

and

$$||f_v||_2^2 \leq d_v = \dim(\langle \pi(K)v \rangle).$$

Proof. We only consider the cyclic subrepresentation $\mathscr{V} = \langle \pi(K)v \rangle$. Since K is compact and $\mathscr{V}$ is cyclic, it follows that $\mathscr{V} < \lambda_K$ and hence we can view v as an element of $L^2(G)$. Thus the condition $\pi(\overline{f_v})v = v$ reads as $\overline{f_v} * v = v$.

We briefly recall the basic representation theory of compact Lie groups. For each irreducible (and hence finite dimensional) representation σ of K, denote by $(e_i^\sigma)_{i\in I_\sigma}$ an orthonormal basis, where I_σ is an index set of cardinality n_σ and by $\sigma_{ij}(g) = \sqrt{n_\sigma}\varphi^\sigma_{e_i^\sigma, e_j^\sigma} \in L^2(G)$ the normalized matrix coefficient for $i, j \in I_\sigma$. Then for irreducible representations σ and ρ,

$$\begin{aligned}
\langle \sigma_{ij}, \rho_{k\ell} \rangle &= \int \sigma_{ij}(g)\overline{\rho_{k\ell}(g)}\, dm_K(g) \\
&= \int \sigma_{ij}(g)\rho_{\ell k}(g^{-1})\, dm_K(g) \\
&= \begin{cases} 0 & \text{if } \sigma \ncong \rho, \\ \delta_{i,k}\delta_{j,\ell} & \text{if } \sigma = \rho. \end{cases}
\end{aligned}$$

We next perform two calculations. First, note

$$\sigma^*_{ij}(g) = \overline{\sigma_{ij}(g^{-1})} = \sigma_{ji}(g).$$

Second,

$$\begin{aligned}
(\sigma_{ij} * \sigma_{k\ell})(x) &= \int \sigma_{ij}(g)\sigma_{k\ell}(g^{-1}x)\, dm_K(g) \\
&= \int \sigma_{ij}(g)\sqrt{n_\sigma}\langle \pi_{g^{-1}x}e_k, e_\ell\rangle\, dm_K(g) \\
&= \int \sigma_{ij}(g)\sqrt{n_\sigma}\sum_{n=1}^{n_\sigma}\langle \pi_x e_k, e_n\rangle\langle e_n, \pi_g e_\ell\rangle\, dm_K(g) \\
&= \sum_{n=1}^{n_\sigma}\langle \pi_x e_k, e_n\rangle \int \sigma_{ij}(g)\overline{\sigma_{\ell n}(g)}\, dm_K(g) \\
&= \sum_{n=1}^{n_\sigma}\langle \pi_x e_k, e_n\rangle \delta_{i,\ell}\delta_{j,n} = \sigma_{kj}(x)\delta_{i,\ell},
\end{aligned}$$

where we expressed $\pi_x e_k = \sum_{n=1}^{n_\sigma}\langle \pi_x e_k, e_n\rangle e_n$. Finally, write $M_\sigma = \langle \sigma_{ij} : i, j \in I_\sigma\rangle$ and recall that the Peter-Weyl theorem states $L^2(K) = \bigoplus_{\sigma\in\widehat{K}} M_\sigma$.

Returning to the vector $v \in L^2(G)$, by the above we can write it as $v = \sum_{\sigma\in\widehat{K}} v_\sigma$ with $v_\sigma \in M_\sigma$ and denote by $J_v = \{\sigma \in \widehat{K} : v_\sigma \neq 0\}$. Then J_v is a finite collection of representations as v is K-finite. Now we are ready to construct the function f_v. Namely set

$$f_v = \sum_{\sigma\in J_v}\sum_{j=1}^{n_\sigma}\overline{\sigma_{jj}}.$$

Then by the above calculations,

$$f_v^* = \sum_{\sigma\in J_v}\sum_{j=1}^{n_\sigma}\overline{\sigma^*_{jj}} = \sum_{\sigma\in J_v}\sum_{j=1}^{n_\sigma}\overline{\sigma_{jj}} = f_v,$$

and

$$\begin{aligned} f_v * f_v &= \sum_{\sigma\in J_v}\sum_{j=1}^{n_\sigma}\sum_{k=1}^{n_\sigma}\overline{\sigma_{jj}} * \overline{\sigma_{kk}} \\ &= \sum_{\sigma\in J_v}\sum_{j=1}^{n_\sigma}\overline{\sigma_{jj}} = f_v. \end{aligned}$$

Furthermore, if we write $v = \sum_{\sigma\in J_v}\sum_{k,\ell=1}^{n_\sigma} a^\sigma_{k\ell}\sigma_{k\ell}$,

$$\begin{aligned} \overline{f_v} * v &= \sum_{\sigma\in J_v}\sum_{j=1}^{n_\sigma}\sum_{k,\ell=1}^{n_\sigma} a^\sigma_{k\ell}\,(\sigma_{jj} * \sigma_{k\ell}) \\ &= \sum_{\sigma\in J_v}\sum_{\ell,k=1}^{n_\sigma} a^\sigma_{k\ell}\,(\sigma_{\ell\ell} * \sigma_{k\ell}) \\ &= \sum_{\sigma\in J_v}\sum_{\ell,k=1}^{n_\sigma} a^\sigma_{k\ell}\sigma_{k\ell} = v. \end{aligned}$$

Finally to check the last property,

$$||f_v||_2^2 = \sum_{\sigma\in J_v} n_\sigma \le d_v = \dim(\langle\lambda_K(K)v\rangle),$$

where we used that $\langle\lambda_K(K)v\rangle$ contains at least one copy of σ as $v_\sigma \neq 0$ for $\sigma\in J_v$. $\square$

In the remainder, we fix for each K-finite $v\in\mathscr{H}$, a function f_v with the properties of Lemma 2.29.

Lemma 2.30. *Let $G = KB$ be a Harish-Chandra group and let $(\pi,\mathscr{H})$ be a unitary representation of G. For $v, w\in\mathscr{H}$ K-finite vectors denote by f_v and f_w functions as in Lemma 2.29. Let $g, h\in L^2(G)$ with the property that*

$$g = \overline{f_v} * g = \lambda_K(\overline{f_v})g, \qquad \text{and} \qquad h = \overline{f_w} * h = \lambda_K(\overline{f_w})g,$$

where the convolution is over K. Then for any $x\in G$,

$$|\langle\lambda_G(x)g, h\rangle_2| \le \sqrt{d_v d_w}||g||_2\,||f||_2\,\Xi(x).$$

Proof. We consider the left-K-invariant functions $\widetilde{g}$ and $\widetilde{h}$ on G defined for $x\in G$ by

$$\widetilde{g}(x) = \sup_{k\in K}|g(kx)| \qquad \text{and} \qquad \widetilde{h}(x) = \sup_{k\in K}|h(kx)|.$$

Then $\lambda_G(k)\widetilde{g} = \widetilde{g}$ and $\lambda_G(k)\widetilde{h} = \widetilde{h}$ for $k\in K$ and for $x\in G$,

$$\begin{aligned} |\langle\lambda_G(x)g, h\rangle_2| &= \left|\int_G g(x^{-1}y)\overline{h(y)}\,dm_G(y)\right| \\ &\le \int_G \widetilde{g}(x^{-1}y)\widetilde{h}(y)\,dm_G(y) = \langle\lambda_G(x)\widetilde{g}, \widetilde{h}\rangle_2. \end{aligned}$$

Using $g = \overline{f_v} * g$, it follows by Cauchy-Schwarz for $k' \in K$,

$$
\begin{aligned}
|g(k'x)| = |(\overline{f_v} * g)(k'x)| &= \left| \int_K \overline{f_v}(k) g(k^{-1}k'x)\, dm_K(k) \right| \\
&\le ||f_v||_{L^2(K)} \left(\int_K |g(k^{-1}k'x)|^2\, dm_K(k) \right)^{\frac{1}{2}} \\
&\le \sqrt{d_v} \left(\int_K |g(kx)|^2\, dm_K(k) \right)^{\frac{1}{2}}.
\end{aligned}
$$

Hence in particular

$$
\widetilde{g}(x) \le \sqrt{d_v} \left(\int_K |g(kx)|^2\, dm_K(k) \right)^{\frac{1}{2}}.
$$

Finally, it follows that

$$
\begin{aligned}
||\widetilde{g}||_{L^2(G)} &= \left(\int_G |\widetilde{g}(x)|^2\, dm_G(x) \right)^{\frac{1}{2}} \\
&\le \sqrt{d_v} \left(\int_G \int_K |g(kx)|^2\, dm_K(k) dm_G(g) \right)^{\frac{1}{2}} \\
&= \sqrt{d_v} \left(\int_K \left(\int_G |g(kx)|^2\, dm_G(x) \right) dm_K(k) \right)^{\frac{1}{2}} \\
&= \sqrt{d_v} \left(\int_K \left(\int_G |g(x)|^2\, dm_G(x) \right) dm_K(k) \right)^{\frac{1}{2}} = \sqrt{d_v} ||g||_2.
\end{aligned}
$$

Combining all this with Lemma 2.27, the claim follows:

$$
\begin{aligned}
|\langle \lambda_G(x) g, h \rangle_2| &\le |\langle \lambda_G(x) \widetilde{g}, \widetilde{h} \rangle_2| \\
&\le \Xi(x) ||\widetilde{g}||_2 \, ||\widetilde{h}||_2 \le \sqrt{d_v d_w} ||g||_2 \, ||h||_2 \, \Xi(x).
\end{aligned}
$$

□

Proof. (of Theorem 2.28) (a) implies (b) holds for general groups G by Theorem 2.11 ([CHH88] Theorem 1). To see (c) implies (a) we note that if we restrict π to K, we can decompose $\mathscr{H}$ as a Hilbert space direct sum of a countable number of irreducible representations of K. As each of those is finite-dimensional, it follows that the set of K-finite vectors is dense in $\mathscr{H}$. Since by assumption the Harish-Chandra spherical function is almost square integrable, it follows that a dense set of vectors has almost square integrable matrix coefficients and hence π is almost square integrable.

So it remains to prove (b) implies (c). Throughout this proof, convolution $f_1 * f_2$ is conducted over K. Let $v, w \in \mathscr{H}$ be K-finite vectors and set $\phi = \varphi^{\pi}_{v,w}$. Then by properties of f_v and f_w and by equation (2.7),

$$
\phi(x) = \langle \pi_x \pi(\overline{f_v}) v, \pi(\overline{f_w}) w \rangle = (f_v * \phi * \overline{f_w^{\vee}})(x) = (f_v * \phi * f_w)(x). \tag{2.8}
$$

As $\pi \prec \lambda_G$, the matrix coefficient ϕ can be approximated uniformly on compact sets by sums $\sum_{i=1}^n \psi_i$ of matrix coefficients $\psi_i = \varphi^{\lambda_G}_{g_i,h_i}$ for $g_i, h_i \in L^2(G)$ with the additional condition

$$\sum_{i=1}^{n} ||g_i||_2 \, ||h_i||_2 \leq ||v|| \, ||w||.$$

More precisely, assume that such an approximation holds for a bi-K-invariant set $Q \subset G$ and $\varepsilon > 0$. As f_v and f_w are continuous functions on the compact group K and $\lambda_K(\overline{f_v})$ and $\lambda_K(\overline{f_w})$ are projections, it follows that we can approximate ϕ by the sums of matrix coefficients $\sum_{i=1}^{n} f_v * \psi_i * f_w$ where again by using equation (2.7),

$$(f_v * \psi_i * f_w)(x) = \langle \lambda_G(x)\lambda_K(\overline{f_v})g_i, \lambda_K(\overline{f_w})h_i \rangle$$

and

$$\sum_{i=1}^{n} ||\lambda_K(\overline{f}_v)g_i|| \, ||\lambda_K(\overline{f}_w)h_i|| \leq ||v|| \, ||w||. \tag{2.9}$$

This follows as for instance using (2.8) and bi-K-invariance of Q,

$$\begin{aligned} |(\phi - f_v * \psi)(g)| &= |(f_v * \phi - f_v * \psi)(g)| \\ &= \left| \int f_v(k)(\phi - \psi)(k^{-1}g) \, dm_K(k) \right| \\ &\leq \int |f_v(k)| \, |(\phi - \psi)(k^{-1}g)| \, dm_K(k) \ll_v \varepsilon, \end{aligned}$$

for $g \in Q$.

Finally, using the properties of f_v, notice that $\overline{f_v} * \lambda_K(\overline{f_v})g_i = \lambda_K(\overline{f_v} * \overline{f_v})g_i = \lambda_K(\overline{f}_v)g_i$. Thus we have proved that we can approximate ϕ arbitrarily close at every point by sums of functions satisfying the assumption of Lemma 2.30 and which also satisfy (2.9). Thus we conclude using Lemma 2.30 that ϕ can be approximated at every point arbitrarily close by functions $\leq \sqrt{d_v d_w} \, ||v|| \, ||w|| \, \Xi$, which implies the claim. □

Definition 2.31. A representation $(\pi, \mathscr{H})$ of G is called m-tempered for $m \in \mathbb{N}$ if $(\pi^{\otimes m}, \mathscr{H}^{\otimes m})$ is tempered.

Definition 2.32. A representation $(\pi, \mathscr{H})$ of G is called m-almost square integrable for $m \in \mathbb{N}$ if for a dense set of vectors $v \in V$ we have that the diagonal matrix coefficient φ_v^π is contained in $L^{2m+\varepsilon}$ for all $\varepsilon > 0$.

We also define integrability exponents, which will we use later.

Definition 2.33. Let $(\pi, \mathscr{H})$ be a unitary representation of G. For $q \in [2, \infty]$, we say that $(\pi, \mathscr{H})$ is q-integrable if there exists a dense set of vectors $V \subset \mathscr{H}_G^\perp$ such for all $v, w \in V$ the matrix coefficients $\varphi_{v,w}^\pi$ satisfy $\varphi_{v,w}^\pi \in L^q(G)$. We define the **almost integrability exponent** $q(\pi) \in [2, \infty]$ as

$$q(\pi) = \inf\{q \in [2, \infty] \, : \, \pi \text{ is } q\text{-integrable}\}.$$

In analogy to Theorem 2.11 and Theorem 2.28, the following corollaries hold.

Corollary 2.34. *A unitary representation with m-almost square integrable matrix coefficients is m-tempered.*

Proof. As the generating set of the free tensors $v_1 \otimes \ldots \otimes v_m$ in $\mathscr{H}^{\otimes m}$ for $v_1, \ldots, v_m \in \mathscr{H}$ is equal to $\mathscr{H}^{\otimes m}$, it suffices by the same argument as in the proof of Corollary 2.12 to show that the matrix coefficients

$$\varphi^{\pi^{\otimes m}}_{v_1 \otimes \ldots \otimes v_m} = \prod_{i=1}^{m} \varphi^{\pi}_{v_i}$$

are in $L^{2+\varepsilon}(G)$ for all $\varepsilon > 0$. This follows by applying the Hölder inequality m-times. Namely we apply the Hölder inequality first with $(m, \frac{m}{m-1})$ so that

$$\begin{aligned}
||\varphi^{\pi^{\otimes m}}_{v_1 \otimes \ldots \otimes v_m}||^{2+\varepsilon}_{2+\varepsilon} &= \int_G \prod_{i=1}^{m} |\varphi^{\pi}_{v_i}|^{2+\varepsilon} \, dm_G \\
&= \int_G |\varphi^{\pi}_{v_1}|^{2+\varepsilon} \prod_{i=2}^{m} |\varphi^{\pi}_{v_i}|^{2+\varepsilon} \, dm_G \\
&\leq || \, |\varphi^{\pi}_{v_1}|^{2+\varepsilon} \, ||_m \cdot \left|\left| \prod_{i=2}^{m} |\varphi^{\pi}_{v_i}|^{2+\varepsilon} \right|\right|_{\frac{m}{m-1}} .
\end{aligned}$$

By assumption $|| \, |\varphi^{\pi}_{v_1}|^{2+\varepsilon} \, ||_m < \infty$ as

$$|| \, |\varphi^{\pi}_{v_1}|^{2+\varepsilon} \, ||_m^m = \int |\varphi^{\pi}_{v_1}|^{2m+\varepsilon m} \, dm_G(g) < \infty.$$

It remains to show that

$$\left|\left| \prod_{i=2}^{m} |\varphi^{\pi}_{v_i}|^{2+\varepsilon} \right|\right|^{\frac{m}{m-1}}_{\frac{m}{m-1}} = \int \prod_{i=2}^{m} |\varphi^{\pi}_{v_i}|^{2\frac{m}{m-1}+\varepsilon'} \, dm_G < \infty$$

for $\varepsilon' = \varepsilon \frac{m}{m-1}$. We next apply the Hölder inequality to $(m-1, \frac{m-1}{m-2})$ to conclude

$$\int \prod_{i=2}^{m} |\varphi^{\pi}_{v_i}|^{2\frac{m}{m-1}+\varepsilon'} \, dm_G \leq || \, |\varphi^{\pi}_{v_1}|^{2\frac{m}{m-1}+\varepsilon'} \, ||_{m-1} \cdot \left|\left| \prod_{i=3}^{m} |\varphi^{\pi}_{v_i}|^{2\frac{m}{m-1}+\varepsilon'} \right|\right|_{\frac{m-1}{m-2}} .$$

As before $|| \, |\varphi^{\pi}_{v_1}|^{2\frac{m}{m-1}+\varepsilon'} \, ||_{m-1} < \infty$. We continue this process by applying the Hölder inequality with $(m-2, \frac{m-2}{m-3}), (m-3, \frac{m-3}{m-4}), \ldots, (3, \frac{3}{2}), (2, 2)$. After having applied the Hölder inequality in total m times, the claim follows. We conclude that $\varphi^{\pi^{\otimes m}}_{v_1 \otimes \ldots \otimes v_n}$ is indeed almost square integrable. In particular $(\pi^{\otimes m}, \mathscr{H}^{\otimes m})$ is almost square integrable and hence tempered by Theorem 2.11. $\square$

Corollary 2.35. *Let $G = KB$ be a Harish-Chandra group and $(\pi, \mathscr{H})$ a unitary representation of G. The following properties are equivalent.*

(a) π is m-almost square integrable.

(b) π is m-tempered.

(c) For all K-finite vectors $v, w \in \mathscr{H}$ with $d_v = \dim(\langle \pi(K)v \rangle)$ and $d_w = \dim(\langle \pi(K)w \rangle)$ we have that

$$|\langle \pi_g v, w \rangle| \leq \sqrt{d_v d_w} \, ||v|| \, ||w|| \, \Xi(g)^{\frac{1}{m}} .$$

Proof. (a) implies (b) was just shown for any group in Corollary 2.34. (c) implies (a) since the set of K-finite vectors is dense in $\mathscr{H}$ as was shown in the proof of Theorem 2.28. It remains to check (b) implies (c). So let $v, w \in \mathscr{H}$ be K-finite vectors. Then $v^{\otimes m} := v \otimes \ldots \otimes v$ and $w^{\otimes m} := w \otimes \ldots \otimes w$ are also K-finite so that $d_{v^{\otimes m}} = d_v^m$ and $d_{w^{\otimes m}} = d_w^m$. Thus it follows by Theorem 2.28 that

$$\begin{aligned}|\langle \pi_g v, w\rangle|^m &= |\langle \pi_g^{\otimes m} v^{\otimes m}, w^{\otimes m}\rangle| \\ &\leq \sqrt{d_v^m d_w^m}\, ||v||^m\, ||w||^m\, \Xi(g).\end{aligned}$$

By taking the m-th square root, (c) is implied. □

2.5 Gelfand Pairs and Spherical Representations

Let G be a topological group and $K \subset G$ be a compact subgroup. Then the **Hecke algebra** $\mathcal{H}(G,K)$ is defined as the set of bi-K-invariant functions of compact support. We consider the L^1-norm on $\mathcal{H}(G,K)$. The Hecke algebra forms a Banach algebra, when equipped with convolution. In this subchapter, we expose content from chapter 4 of [Lan75].

Definition 2.36. Let G be a locally compact metric group and $K \subset G$ be a compact subgroup. The tuple (G,K) is called a Gelfand pair if the Hecke algebra $\mathcal{H}(G,K)$ is commutative.

We first discuss some examples of Gelfand pairs.

Lemma 2.37. *Let G be a unimodular group and $K \subset G$ a compact subgroup. Assume that for every $g \in G$ there exists $k_1, k_2 \in K$ so that*

$$g^{-1} = k_1 g k_2.$$

Then (G,K) is Gelfand pair.

Proof. Let $f_1, f_2 \in \mathcal{H}(G,K)$. Then clearly $f_i(g^{-1}) = f_i(g)$ for all $g \in G$ and $i = 1, 2$ and as $f_1 * f_2 \in \mathcal{H}(G,K)$ the same holds for $f_1 * f_2$. We calculate for $h \in G$,

$$\begin{aligned}(f_1 * f_2)(h) &= \int_G f_1(hg^{-1}) f_2(g)\, dm_G(g) \\ &= \int_G f_1(gh^{-1}) f_2(g^{-1})\, dm_G(g) \\ &= \int_G f_1(g) f_2((gh)^{-1})\, dm_G(g) \\ &= \int_G f_1(g) f_2(h^{-1}g^{-1})\, dm_G(g) \\ &= (f_2 * f_1)(h^{-1}) = (f_2 * f_1)(h),\end{aligned}$$

where we substituted g by gh in the third line. □

If G are the F-points of a linear algebraic group over the local field F and K is a maximal compact subgroup of G, then the assumption of Lemma 2.37 is satisfied. Thus (G,K) is a Gelfand pair. More generally, consider G a linear algebraic group over $\mathbb{Q}$ and S a finite set of places of $\mathbb{Q}$. For almost all primes

p, the subgroup $K_p = \mathrm{G}(\mathbb{Z}_p)$ is a maximal compact subgroup of $\mathrm{G}(\mathbb{Q}_p)$, yet we can always find a maximal compact subgroup that contains $\mathrm{G}(\mathbb{Z}_p)$. Thus again, by using the Cartan decomposition it follows that (G_S, K_S) is a Gelfand pair, where $G_S = \prod_{p\in S} G(\mathbb{Q}_p)$ and $K_S = \prod_{p\in S} K_p$.

The representation theory of Gelfand pairs will later turn out to be useful. The next result will be of particular importance.

Theorem 2.38. *Let (G, K) be a Gelfand pair and let $(\pi, \mathscr{H})$ be an irreducible unitary representation of G. Then the subspace of K-invariant vectors $\mathscr{H}_K$ satisfies*

$$\dim \mathscr{H}^K \leq 1.$$

The main idea of the proof of Theorem 2.38 is to associate to $(\pi, \mathscr{H})$ an irreducible algebra representation of the Hecke algebra. We review the notion of an algebra representation on a Hilbert space. If $\mathscr{A}$ is a Banach algebra and $\mathscr{H}$ is a Hilbert space, then a ring homomorphism

$$\pi : \mathscr{A} \longrightarrow B(\mathscr{H})$$

is called a representation of $\mathscr{A}$ if for all $v \in \mathscr{H}$ the map

$$\mathscr{A} \longrightarrow \mathscr{H}, \qquad a \longmapsto \pi_a v$$

is continuous. In this setting, Schur's Lemma holds.

Proposition 2.39. *(Schur's Lemma) Let $(\pi, \mathscr{H})$ be an irreducible representation of $\mathscr{A}$. Let $B \in B(\mathscr{H})$ be a bounded π-equivariant operator, i.e.*

$$B \circ \pi_a = \pi_a \circ B$$

for all $a \in \mathscr{A}$. Then $B = \lambda \cdot \mathrm{Id}_{\mathscr{H}}$ for some $\lambda \in \mathbb{C}$.

Proof. The proof is analogous to Schur's Lemma for representations of topological groups on Hilbert spaces, for which we refer to [EW] Theorem 1.25. □

In general, if $(\pi, \mathscr{H})$ is a unitary representation of G, then the map

$$\pi : L^1(G) \to B(\mathscr{H}), \qquad f \longmapsto \pi(f)$$

defines an algebra representation of $L^1(G)$. If $f \in L^1(G)$ is bi-K-invariant and $v \in \mathscr{H}_K$ then $\pi(f)v \in \mathscr{H}_K$ as for $k \in K$,

$$\pi_k \pi(f) v = \int f(g)\, \pi_{kg} v\, m_G(g) = \int f(k^{-1}g)\, \pi_g v\, m_G(g) = \pi(f)v.$$

Thus we get a well-defined representation of the Hecke algebra

$$\pi_K : \mathcal{H}(G, K) \longrightarrow B(\mathscr{H}_K), \qquad f \longmapsto \pi(f).$$

Proposition 2.40. *In the above setting, assume that $\mathscr{H}_K$ is non-zero and that*

$$\mathscr{H} = \overline{\langle \pi(G)\mathscr{H}_K \rangle}.$$

Then $\mathscr{H}_K$ is irreducible as an algebra representation of $\mathcal{H}(G, K)$ if and only if $\mathscr{H}$ is irreducible.

Proof. This can be found in chapter 4.2. of [Lan75]. □

We now are in a suitable position to prove Theorem 2.38.

Proof. (of Theorem 2.38) By Proposition 2.40, as $(\pi, \mathscr{H})$ is an irreducible unitary representation of G, the algebra representation $(\pi_K, \mathscr{H}_K)$ of the Hecke algebra $\mathcal{H}(G, K)$ is also irreducible. Using Schur's Lemma, as $\mathcal{H}(G, K)$ is a commutative algebra, every irreducible representation of $\mathcal{H}(G, K)$ is at most one dimensional and hence $\mathscr{H}_K$ is at most one dimensional. □

We next discuss spherical functions and spherical representations.

Proposition 2.41. *Let (G, K) be a Gelfand pair. For $\eta \in \mathcal{H}(G, K)$ the following properties are equivalent:*

1. *The map*
$$\chi_\eta : \mathcal{H}(G, K) \longrightarrow \mathbb{C}, \qquad f \mapsto \int_G f(g)\eta(g^{-1})\, dm_G(g)$$
is an algebra homomorphism.
2. *For all $g_1, g_2 \in G$ we have that*
$$\eta(g_1)\eta(g_2) = \int_K \eta(g_1 k g_2)\, dm_K(k).$$
3. *For all $f \in \mathcal{H}(G, K)$ the following property holds:*
$$f * \eta = \chi_\eta(f)\psi = (\chi * \eta)(e)\psi.$$

Proof. The proof is straightforward and can be found in chapter 4.3 of [Lan75]. □

Definition 2.42. Let (G, K) be a Gelfand pair. A function $\eta \in \mathcal{H}(G, K)$ with $\eta(e) = 1$ and for which any of the equivalent properties of Proposition 2.41 holds is called **spherical**.

Proposition 2.43. *Let (G, K) be a Gelfand pair and $(\pi, \mathscr{H})$ be a unitary representation of G. Assume that there exists a unit vector $v \in \mathscr{H}_K$ that generates $(\pi, \mathscr{H})$. Then $\dim \mathscr{H}_K = 1$ if and only if the diagonal matrix coefficient φ_v^π is a spherical function.*

Proof. See [Lan75] chapter 4.4. □

Proposition 2.43 motivates the final definition in this chapter.

Definition 2.44. Let (G, K) be a Gelfand pair. An irreducible unitary representation $(\tau, \mathscr{H})$ of G is called **spherical** if there exists a non-zero K-invariant vector.

Corollary 2.45. *Let (G, K) be a Gelfand pair. For each positive definite spherical function $\eta \in \mathcal{H}(G, K)$, there exists a uniquely characterized spherical representation $(\tau_\eta, \mathscr{H}_\eta)$ and a K-invariant generating vector $v_\eta \in \mathscr{H}_\psi$ so that $\psi = \varphi_{v_\eta}^{\pi_\eta}$.*

3 Spectral Gap and Tempered Representations

In the last chapter, we observed that the effective vanishing of matrix coefficients is related to temperdness. In this chapter, we define spectral gap of a unitary representation and discuss the equivalence of spectral gap and the effective vanishing of matrix coefficients.

To introduce some further important terms, which will be defined and discussed in this chapter in greater detail, a group G has property (T) if all of its unitary representations have a uniform spectral gap. In similar vein, an algebraic group G over $\mathbb{Q}$ is said to have property (τ) if for a fixed prime p the representations $\pi_{p,\ell}$ of the groups $\mathrm{G}(\mathbb{Q}_p)$ have a spectral gap that is uniform among ℓ and all possible $\mathbb{Q}_p$-structures of G.

3.1 Spectral Gap, Property (T) and Property (τ)

In this subchapter we review some notions and results contained in [EW], [BdlHV08] or [LZ]. We start with some definitions.

Definition 3.1. A unitary representation $(\pi, \mathscr{H})$ is said to have a **spectral gap** if the subrepresentation $(\pi|_{(\mathscr{H}_G)^\perp}, (\mathscr{H}_G)^\perp)$ does not have almost invariant unit vectors, i.e. there is some compact subset $K \subset G$ and $\varepsilon > 0$ so that for all unit vectors $v \in (\mathscr{H}_G)^\perp$ there is some $g \in K$ so that

$$||\pi_g v - v|| \geq \varepsilon.$$

Definition 3.2. Let $(\pi_i, \mathscr{H}_i)_{i\in I}$ be a collection of unitary representations of G, $K \subset G$ compact and $\varepsilon > 0$. We say that the collection $(\pi_i, \mathscr{H}_i)_{i\in I}$ has (K, ε) as a **uniform spectral gap** if for all $i \in I$ and all unit vectors $v \in (\mathscr{H}_{i,G})^\perp$ there is $g \in K$ so that

$$||(\pi_i)_g v - v|| \geq \varepsilon.$$

In the following we give some equivalent characterizations.

Proposition 3.3. *Let $(\pi, \mathscr{H})$ be a unitary representation of G. The following properties are equivalent:*

(i) $(\pi, \mathscr{H})$ has a spectral gap.

(ii) There exists a non-negative function $f \in L^1(G)$ with $\int f \, dm_G = 1$ so that

$$||\pi(f)|_{\mathscr{H}_G^\perp}||_{\mathrm{op}} < 1.$$

In fact, if $(\pi, \mathscr{H})$ has (K, ε) as a spectral gap, then for all compact $B \subset G$ with $K \subset B^\circ \subset B$ there is a $\delta = \delta(K, \varepsilon, B) > 0$ depending on (K, ε, B) so that the function $f_B = \frac{\chi_B}{m_G(B)}$ satisfies

$$||\pi(f_B)|_{\mathscr{H}_G^\perp}|| \leq 1 - \delta(K, \varepsilon, B) < 1.$$

Proof. This is Proposition 4.23 of [EW]. The direction (i) implies (ii) is left to the reference. We prove (ii) implies (i). In order to simplify our notation, assume without loss of generality that $(\pi, \mathscr{H})$ has no non-zero invariant vectors. So let $\varepsilon > 0$ so that

$$||\pi(f)||_{\text{op}} \leq 1 - 4\varepsilon < 1.$$

Choose K compact so that

$$\int_{G \setminus K} f(g)\, dm(g) \leq \varepsilon.$$

Then we have for all unit vectors $v \in \mathscr{H}$,

$$\begin{aligned} ||\pi(f|_K)v|| &= \left|\left| \int_K f(g)\pi_g v\, dm_G(g) \right|\right| \\ &= \left|\left| \int_G f(g)\pi_g v\, dm_G(g) - \int_{G\setminus K} f(g)\pi_g v\, dm_G(g) \right|\right| \\ &\leq ||\pi(f)v|| + \varepsilon \leq 1 - 3\varepsilon. \end{aligned}$$

Hence in particular

$$||\pi(f|_K)||_{\text{op}} \leq 1 - 3\varepsilon.$$

We claim that π has (K, ε) as a spectral gap, i.e. that for all unit vectors $v \in \mathscr{H}$ there is $g \in K$ so that $||\pi_g v - v|| \geq \varepsilon$. Assume that this is not the case for the unit vector $v \in \mathscr{H}$. Then for all $g \in K$ we have $||\pi_g v - v|| < \varepsilon$. Thus

$$\begin{aligned} ||\pi(f|_K)v - v|| &= \left|\left| \int_K f(g)\pi_g v\, dm_G(g) - v \right|\right| \\ &= \left|\left| \int_K f(g)(\pi_g v - v)\, dm_G(g) - \int_{G\setminus K} f(g) v\, dm_G(g) \right|\right| \\ &\leq \sup_{g \in K} ||\pi_g v - v|| + \varepsilon \leq 2\varepsilon \end{aligned}$$

Moreover we note that for the unit vector v,

$$1 - 2\varepsilon \leq ||v|| - ||\pi(f|_K)v - v|| \leq ||\pi(f|_K)v|| \leq ||\pi(f|_K)||_{\text{op}} \leq 1 - 3\varepsilon,$$

a contradiction. □

Proposition 3.4. *Let $(\pi_i, \mathscr{H}_i)_{i \in I}$ be a collection of unitary representations of G and let $K \subset G$ be a compact subset and $\varepsilon > 0$. The following properties are equivalent.*

(i) The collection $(\pi_i, \mathscr{H}_i)_{i \in I}$ has (K, ε) as a uniform spectral gap.

(ii) The collection $(\pi_i|_{(\mathscr{H}_{i,G})^\perp}, (\mathscr{H}_{i,G})^\perp)_{i \in I}$ is isolated from the trivial representation 1_G in the Fell topology.

(iii) There is some non-negative function $f \in L^1(G)$ with $\int f\, dm_G = 1$ and $\varepsilon > 0$ so that for all $i \in I$,

$$||\pi_i(f)|_{\mathscr{H}_G^\perp}||_{\text{op}} \leq 1 - \varepsilon.$$

(iv) If a unitary representation $(\pi_i, \mathscr{H}_i)$ with $i \in I$ has (K, ε)-almost invariant vectors, then it has non-zero invariant unit vectors.

Proof. For the equivalence of (i) and (iii) we again refer to Proposition 4.23 of [EW]. The argument given in the proof of Lemma 3.3 also suffices to show (iii) implies (i).

Assume (i). Let $(\pi, \mathscr{H}) = (\pi_i, \mathscr{H}_i)$ for $i \in I$ be a unitary representation with (K, ε)-invariant unit vectors. So there is a unit vector $v \in \mathscr{H}$ so that $||\pi_g v - v|| \leq \varepsilon$ for all $g \in K$. We decompose $v = v_G + v'_G$ for $v_G \in \mathscr{H}_G$ and $v'_G \in (\mathscr{H}_G)^\perp$. Assume for a contradiction that v_G is zero. Then $v \in (\mathscr{H}_G)^\perp$ contradicts the definition of uniform spectral gap so it follows that v_G is a non-zero element of $\mathscr{H}_G$. Thus $(\pi, \mathscr{H})$ has invariant vectors. So we have proved (iv).

Conversely assume (iv). We denote by $(\pi, \mathscr{H})$ any unitary representation from the collection $(\pi_i, \mathscr{H}_i)$ for $i \in I$. We want to show that for all unit vectors $v \in (\mathscr{H}_G)^\perp$ there is some $g \in K$ so that $||\pi_g v - v|| \geq \varepsilon$. So assume for a contradiction that there is a unit vector $v \in (\mathscr{H}_G)^\perp$ so that $||\pi_g v - v|| < \varepsilon$ for all $g \in K$. Then the unitary representation $(\pi|_{(\mathscr{H}_G)^\perp}, (\mathscr{H}_G)^\perp)$ has a (K, ε)-invariant unit vector and so by assumption it has a non-zero invariant unit vector. However, this contradicts the definition of $\mathscr{H}_G$. This proves (i).

The first subbasis in Definition 2.13 clearly shows that (ii) and (iii) are equivalent. We moreover give an additional argument that (iii) implies (i). Without loss of generality, we consider the case where the representations $(\pi, \mathscr{H}_i)$ do not have invariant vectors. Assume for a contradiction that the collection does not have a uniform spectral gap. Write $G = \bigcup_{n \geq 1} K_n$ for $K_n \subset G$ compact subsets. Then for each tuple $(K_n, \frac{1}{n})$ there is a unitary representation $(\pi_n, \mathscr{H}_n)$ so that π_n has $(K_n, \frac{1}{n})$-almost invariant unit vectors. Consider the representation

$$\bigoplus_{n \geq 1} \mathscr{H}_n.$$

Then clearly for any strictly increasing sequence (n_k) in $\mathbb{N}$ we have that $\bigoplus_{k=1}^\infty \mathscr{H}_{n_k}$ has almost invariant unit vectors or equivalently $1_G \prec \bigoplus_{k=1}^\infty \mathscr{H}_{n_k}$. So it follows by Proposition 2.15 that $\pi_n \to 1_G$ in the Fell topology. But then 1_G is contained in the closure of $(\pi_i, \mathscr{H}_i)_{i \in I}$, contradicting the assumption. $\square$

For semisimple algebraic groups one can moreover give the following characterization of spectral gap in terms of effective vanishing of matrix coefficients.

Theorem 3.5. *Let G be the F-points of an almost simple algebraic group over a local field F and $G = KB$ an Iwasawa decomposition. Assume that G is non-compact and let $(\pi_i, \mathscr{H}_i)_{i \in I}$ be a collection of unitary representations of G. The following properties are equivalent.*

(i) The collection $(\pi_i, \mathscr{H}_i)_{i \in I}$ has a uniform spectral gap.

(ii) There exists a sufficiently large integer m so that π_i is m-tempered for all $i \in I$.

(iii) There exists a sufficiently large integer m so that for all $(\pi, \mathscr{H}) = (\pi_i, \mathscr{H}_i)$ with $i \in I$ the following holds: For all K-finite vectors $v, w \in \mathscr{H}$ with

$d_v = \dim(\langle \pi(K)v \rangle)$ and $d_w = \dim(\langle \pi(K)w \rangle)$ we have that

$$|\langle \pi_g v, w \rangle| \ll \sqrt{d_v d_w}\, ||v||\, ||w||\, \Xi(g)^{\frac{1}{m}},$$

where the constant is absolute and in particular does not depend on v, w and $i \in I$.

(iv) There exists a sufficiently large integer m so that for all $(\pi, \mathscr{H}) = (\pi_i, \mathscr{H}_i)$ with $i \in I$ the following holds: For all K-invariant vectors $v, w \in \mathscr{H}$,

$$|\langle \pi_g v, w \rangle| \ll ||v||\, ||w||\, \Xi(g)^{\frac{1}{m}},$$

where the constant is absolute and in particular does not depend on v, w and $i \in I$.

Proof. For (i) implies (ii) we refer to [Nev98] if G has property (T). In the case $G = \mathrm{SL}_2(\mathbb{Q}_p)$ we give a proof in chapter 3.2. For the general case we refer to [Moo87]. (ii) implies (iii) is Corollary 2.35. As (iii) implies (iv) is clear, it remains to show (iv) implies (i). Assume without loss of generality that G is non-compact and let C_I be the explicit constant from the assumption (iv), i.e. so that

$$|\langle \pi_g v, w \rangle| \le C_I\, ||v||\, ||w||\, \Xi(g)^{\frac{1}{m}}$$

for all $i \in I$ and K-invariant $v, w \in \mathscr{H}$. As G is non-compact and as $\Xi \in L^{2+\varepsilon}(G)$ for $\varepsilon > 0$, there is for some $0 < \delta < 1$ a compact bi-K-invariant subset $C \subset G$ with $m_G(C) = 1$ so that

$$\int_C |\Xi(g)|^{\frac{1}{m}}\, dm_G(g) < \frac{\delta}{C_I}.$$

Set $f = \chi_C$, then $f \ge 0$, $\int_G f dm_G = 1$ and f is bi-K-invariant, i.e. $f(kgk') = f(g)$ for all $g \in G$ and $k, k' \in K$. If $v \in \mathscr{H}$, then we denote by

$$v_K = \int_{k \in K} \pi_k v\, dm_K(k)$$

and note that $||v_K|| \le \int_{k \in K} ||\pi_k v||\, dm_K(k) = ||v||$ as π is unitary.

So we have for $v, w \in \mathscr{H}$,

$$\begin{aligned}
\langle \pi(f)v, w \rangle &= \int_G f(g) \langle \pi_g v, w \rangle\, dm_G(g) \\
&= \int_G f(k_1 g k_2^{-1}) \langle \pi_g v, w \rangle\, dm_G(g) \\
&= \int_G \int_K \int_K f(k_1 g k_2^{-1}) \langle \pi_g v, w \rangle\, dm_G(g) dm_K(k_1) dm_K(k_2) \\
&= \int_G \int_K \int_K f(g) \langle \pi_{k_1^{-1} g k_2} v, w \rangle\, dm_G(g) dm_K(k_1) dm_K(k_2) \\
&= \int_G f(g)\, \langle \pi_g v_K, w_K \rangle\, dm_G(g).
\end{aligned}$$

Using the assumption of (iv) and the properties of f we conclude

$$\begin{aligned}|\langle \pi(f)v, w\rangle| &= \left| \int_G f(g) \langle \pi_g v_K, w_K\rangle \, dm_G(g) \right| \\ &\leq \int_G |f(g)| \, |\langle \pi_g v_K, w_K\rangle| \, dm_G(g) \\ &\leq C_I \left(\int_C |\Xi|^{\frac{1}{m}} \, dm_G \right) ||v_K|| \, ||w_K|| \\ &\leq \delta \, ||v|| \, ||w||.\end{aligned}$$

In particular

$$||\pi(f)||_{\mathrm{op}} \leq \delta < 1$$

Thus by Lemma 3.4 it follows that the collection $(\pi_i, \mathscr{H}_i)$ has a uniform spectral gap. □

On the other hand, for real Lie groups we get the following additional equivalent property.

Corollary 3.6. *Let G be a semisimple non-compact Lie group and $(\pi_i, \mathscr{H}_i)_{i \in I}$ a collection of unitary representation of G. The following properties are equivalent.*

(i) The collection $(\pi_i, \mathscr{H}_i)_{i \in I}$ has a uniform spectral gap.

(ii) There exists a sufficiently large integer m so that π_i is m-tempered for all $i \in I$.

(iii) There exists a sufficiently large integer m so that for all $(\pi, \mathscr{H}) = (\pi_i, \mathscr{H}_i)$ with $i \in I$ the following holds: For all K-finite vectors $v, w \in \mathscr{H}$ with $d_v = \dim(\langle \pi(K)v\rangle)$ and $d_w = \dim(\langle \pi(K)w\rangle)$ we have that

$$|\langle \pi_g v, w\rangle| \ll \sqrt{d_v d_w} \, ||v|| \, ||w|| \, \Xi(g)^{\frac{1}{m}}.$$

(v) There exists a sufficiently large integer m so that for all $(\pi, \mathscr{H}) = (\pi_i, \mathscr{H}_i)$ with $i \in I$ the following holds: For $d > \frac{\dim(K)}{2}$ and all smooth vectors $v, w \in \mathscr{H}$ we have

$$|\langle \pi_g v, w\rangle| \ll \mathcal{S}_d(v)\mathcal{S}_d(w)\Xi(g)^{\frac{1}{m}}.$$

Proof. We already know that (i), (ii) and (iii) are equivalent. (iii) implies (iv) is proven in [EMV09] in chapter 6.3.2. (iv) implies (ii) as the set of smooth vectors is dense. □

Definition 3.7. A locally compact Hausdorff group G has **property (T)** if every unitary representation with almost invariant unit vectors has non-zero invariant vectors.

Example 3.8. Every compact group has property (T). Moreover, let $\mathrm{G} \subset \mathrm{GL}_n$ be a linear algebraic group over a local field F that is connected, almost simple over F and has F-rank ≥ 2. Then $G = \mathrm{G}(F)$ has property (T). For a proof of these examples see [BdlHV08].

We next discuss some equivalent characterizations of property (T).

Theorem 3.9. *The following properties are equivalent.*

(i) G has property (T).

(ii) If a unitary representation $(\pi, \mathscr{H})$ satisfies $1_G \prec \pi$, then $1_G < \pi$.

(iii) The collection of all unitary representations of G has a uniform spectral gap.

Assume that G has property (T) with uniform spectral gap (K, ε) for $K \subset G$ compact and $\varepsilon > 0$. Then we furthermore have the following equivalent properties.

(iv) If a unitary representation has (K, ε)-almost invariant unit vectors, then it has non-zero invariant vectors, for some $K \subset G$ compact and $\varepsilon > 0$.

(v) The trivial representation of G is isolated from $\mathscr{U}_0(G)$ in the Fell topology on $\mathscr{U}(G)$, i.e. 1_G is not contained in the closure of $\mathscr{U}_0(G)$ with respect to the Fell topology.

Proof. (i) and (ii) are equivalent by the last chapter. Moreover, (iii), (iv) and (v) are equivalent by Proposition 3.4. We note that (iv) clearly implies (i). We show that (i) implies (iii). Assume for a contradiction that the collection of all unitary representations does not have a uniform spectral gap. As G is σ-compact, it follows that we can write $G = \bigcup_{n=1}^{\infty} K_n$ for $K_n \subset G$ compact subsets. Since we do not have a uniform spectral gap, for each n there is a unitary representation $(\pi_n, \mathscr{H}_n)$ without invariant vectors but with $(K_n, \frac{1}{n})$-invariant vectors. Then consider the representation

$$\bigoplus_{n \geq 1} \mathscr{H}_n,$$

which has almost invariant vectors but no invariant vectors. This contradicts the assumption that G has property (T). This implies the theorem

We moreover give the following argument for (v) implies (i). So assume that (v) is satisfied and for a contradiction that G does not have property (T). Then there is a unitary representation π of G so that $1_G \prec \pi$ but $1_G \not< \pi$. So $\pi \in \mathscr{U}_0(G)$. By Lemma 2.14, it follows that $1_G \in \overline{\{\pi\}}$, which is contained in the closure of $\mathscr{U}_0(G)$. But this contradicts the assumption that 1_G is isolated from the closure of $\mathscr{U}_0(G)$. So G satisfies property (T). □

Corollary 3.10. *Let G be the F-points of an almost simple algebraic group over a local field F. Then the following properties are equivalent:*

(i) The group G has property (T).

(ii) There exists a sufficiently large integer m so that all unitary representations without invariant vectors are m-tempered.

(iii) There exists a sufficiently large integer m so that for all unitary representations $(\pi, \mathscr{H})$ without invariant vectors of G we have the following property: For all K-finite vectors $v, w \in \mathscr{H}$ with $d_v = \dim(\langle \pi(K)v \rangle)$ and $d_w = \dim(\langle \pi(K)w \rangle)$ we have that

$$|\langle \pi_g v, w \rangle| \leq \sqrt{d_v d_w}\, ||v||\, ||w||\, \Xi(g)^{\frac{1}{m}}.$$

Proof. This is a combination of Theorem 3.9 and Theorem 3.5. □

We return to considering $\mathrm{G} \subset \mathrm{GL}_n$, a simply connected almost simple algebraic group over $\mathbb{Q}$.

Definition 3.11. The algebraic group G is said to have **property** (τ) if for each place p for which G is isotropic over $\mathbb{Q}_p$, there exists a constant $\tau_{\mathrm{G},p}$ so that the following holds: For all algebraic groups G' that are isomorphic to G over $\mathbb{Q}_p$ the representations $\pi_{p,\ell}$ for $\ell \geq 0$ of $\mathrm{G}'(\mathbb{Q}_p)$ satisfy

$$q(\pi_{p,\ell}) \leq \tau_{\mathrm{G},p}.$$

Combining work of of Selberg [Sel65], Kazhdan [Kaz67], Burger-Sarnak [BS91] and Clozel [Clo03], it follows that every such algebraic group over $\mathbb{Q}$ has property (τ). The proof of the latter result is beyond the scope of this thesis, however we aim to explore techniques developed by [GGN] to give a new proof of property (τ) for $\mathbb{Q}$-forms of SL_2. In fact, we will prove the next theorem.

Theorem 3.12. *Let* $\mathrm{G} = \mathrm{B}^1$ *be the unit norm elements of a quaternion algebra* B *over* $\mathbb{Q}$*. Then*

$$q(\pi_{p,\ell}) \leq 24.$$

Moreover, if B is a division algebra, then

$$q(\pi_{p,\ell}) \leq 4.$$

Proof. See chapter 5.5. □

As a final remark, we state the well-known and still open Ramanujan-Petersson conjecture for $\mathbb{Q}$-forms of SL_2.

Conjecture 3.13. *(Ramanujan-Petersson conjecture for* $\mathbb{Q}$*-forms of* SL_2*) Let* G *be a* $\mathbb{Q}$*-form of* SL_2*. Then for all* p *and* ℓ *the representations* $\pi_{p,\ell}$ *are tempered.*

3.2 Complementary Series Representation of $\mathrm{SL}_2(\mathbb{Q}_p)$

Let p be any place $\mathbb{Q}$ and write $G = \mathrm{SL}_2(\mathbb{Q}_p)$. The classification of irreducible unitary representations of $\mathrm{SL}_2(\mathbb{Q}_p)$, as conducted for instance in [GGPS], yields that the non-tempered and non-trivial irreducible unitary representations can be parametrized by $s \in (0,1)$. More precisely for each $s \in (0,1)$ we denote by $(\gamma_s, \mathscr{H}_s)$ the **complementary series** representation with parameter s. Then,

$$\widehat{\mathrm{SL}_2(\mathbb{Q}_p)} = \{1_G\} \cup \{\text{tempered } \sigma \in \widehat{\mathrm{SL}_2(\mathbb{Q}_p)}\} \cup \{\gamma^s \,:\, s \in (0,1)\}. \tag{3.1}$$

Before giving a precise definition of the complementary series representation, we discuss some central properties and state the main results of this chapter. For any unitary representation $(\pi, \mathscr{H})$ of $\mathrm{SL}_2(\mathbb{Q}_p)$, we define the **complementary series exponent** as

$$c(\pi) = \sup\left\{\{0\} \cup \{s \in (0,1) \,:\, \gamma^s \prec \pi\}\right\}.$$

Theorem 3.14. *For a unitary representation $(\pi, \mathscr{H})$ of $\mathrm{SL}_2(\mathbb{Q}_p)$ without almost invariant vectors,*

$$q(\pi) = \frac{2}{1 - c(\pi)}.$$

Moreover, $(\pi, \mathscr{H})$ has a spectral gap if and only if $q(\pi) < \infty$ or equivalently $c(\pi) < 1$.

Write $K = \mathrm{SO}_2(\mathbb{R})$ if $p = \infty$ and $K = \mathrm{SL}_2(\mathbb{Z}_p)$ for a prime p. Moreover we denote by

$$A_\infty = \left\{ a_t = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} : t \in \mathbb{R} \right\} \quad \text{and} \quad A_p = \left\{ a_n = \begin{pmatrix} p^n & 0 \\ 0 & p^{-n} \end{pmatrix} : n \in \mathbb{Z} \right\}$$

for p a prime number. Let $h \geq 0$. If $p = \infty$, then we set $A_h = \{a_t : 1 \leq e^t \leq h\}$ and if p is a prime $A_h = \{a_n : 1 \leq p^n \leq h\}$. For any place,

$$B_h = K A_h K.$$

We will prove that $m_G(B_h) \asymp_p h^2$.

Returning to the complementary series, we will show that for any $s \in (0, 1)$ the complementary series $(\gamma_s, \mathscr{H}_s)$ is a (non-unitarily) induced representation and hence spherical. Denote by F_s the element of $\mathscr{H}_s$ which arises as the extension of the function $\equiv 1$ on K and write by ϕ_s the matrix coefficient $\varphi_{F_s}^{\gamma_s}$.

Proposition 3.15. *Let p be a place of $\mathbb{Q}$ and $s \in (0, 1)$. Then the following properties hold:*

(i) The function ϕ_s is bi-K-invariant, satisfies for $g \in G$

$$\phi_s(g) \asymp_{p,s} ||g||^{s-1}$$

and is in $L^q(G)$ if and only if $q > \frac{2}{1-s}$. More precisely, there exists a continuous monotonously decreasing function $c_p(s)$ on $(0, 1]$ with $c_p(s) \to \infty$ as $s \to 0$ so that

$$c_p(s) ||g||^{s-1} \ll_p \phi_s(g) \ll_p c_p(s)^2 ||g||^{s-1}. \tag{3.2}$$

In fact,

$$c_p(s) = \begin{cases} s^{-1} & \textit{if } p = \infty, \\ (1 - p^{-s})^{-1} & \textit{if } p \textit{ is prime.} \end{cases}$$

(ii) For $s \in (0, 1)$,

$$||F_s||_{\mathscr{H}_s}^2 \asymp_p c_p(s),$$

for $c_p(s)$ the function from (i).

(iii) For $h > 0$ denote by $f_{B_h} = \frac{\chi_{B_h}}{m_{G_p}(B_h)}$. Then

$$||\gamma^s(f_{B_h})||_{\mathrm{op}} \asymp_{p,s} h^{s-1}.$$

The principal aim of this chapter is to establish Theorem 3.14 and Proposition 3.15. Assuming these two results, we discuss an application for later use.

Theorem 3.16. *Let $(\pi, \mathscr{H})$ be a unitary representation of $G_p = \mathrm{SL}_2(\mathbb{Q}_p)$ without almost invariant vectors. Assume there is $\rho > 0$ so that for any bi-K_p-invariant set $B \subset \mathrm{SL}_2(\mathbb{Q}_p)$,*

$$||\pi(f_B)||_{\mathrm{op}} \ll_\delta m_p(B)^{-\rho+\delta},$$

where $f_B = \frac{\chi_B}{m_p(B)}$ and $\delta > 0$. Then $q(\pi) \leq \max\{\frac{1}{\rho}, 2\}$.

Proof. Let $\gamma^s \prec \pi$ for some $s \in (0,1)$. Then the assumption of the theorem implies for $\delta > 0$,

$$||\gamma^s(f_B)||_{\mathrm{op}} \leq ||\pi(f_B)||_{\mathrm{op}} \ll_\delta m_p(B)^{-\rho+\delta}.$$

Using $B = B_h$ for $h > 0$ and $m_{G_p}(B_h) \asymp h^2$ we conclude by using Proposition 3.15 (iii),

$$h^{s-1} \ll_{\delta,s} h^{-2\rho+2\delta}$$

for all $h > 0$ and hence in particular $1 - s - 2\rho + 2\delta \geq 0$ or equivalently $s \leq 1 - 2\rho + 2\delta$ for all $\delta > 0$. Thus it follows $c(\pi) \leq \max\{1 - 2\rho, 0\}$ and by using Theorem 3.14,

$$q(\pi) = \frac{2}{1 - c(\pi)} \leq \max\left\{\frac{1}{\rho}, 2\right\}.$$

□

From the dynamical viewpoint, if $(\pi, \mathscr{H})$ is a Koopman representation (see the first paragraphs of chapter 4 for a discussion of Koopman representations), the assumption of Theorem 3.16 can be viewed as an effective mean ergodic theorem. Therefore, Theorem 3.16 says that an effective mean ergodic theorem implies a spectral gap. In our proof of property (τ) for $\mathbb{Q}$-forms of SL_2 we will use the following subtly more general version of Theorem 3.16. In fact, we will prove in chapter 5.5 the assumption of Theorem 3.17 with $\rho = \frac{1}{24}$ (and $\rho = \frac{1}{4}$ in the case of division algebras) uniformly for all the dynamical systems in question.

Theorem 3.17. *Let $(\pi, \mathscr{H})$ be a unitary representation of $G_p = \mathrm{SL}_2(\mathbb{Q}_p)$ without almost invariant vectors. Assume there is $\rho > 0$ so that for any $\gamma^s \prec \pi$ and $h > 0$,*

$$||\gamma^s(f_{B_h})||_{\mathrm{op}} \ll_{\delta,s} m_p(B_h)^{-\rho+\delta}.$$

Then $q(\pi) \leq \max\{\frac{1}{\rho}, 2\}$.

Proof. The proof is identical to the one of Theorem 3.16. □

For the proof of Theorem 3.14 and Proposition 3.15 we proceed as follows. First we deduce Theorem 3.14 by assuming Proposition 3.15. Then we give a construction of the complementary series and prove Proposition 3.15 first in the case $\mathrm{SL}_2(\mathbb{R})$ and then in the case $\mathrm{SL}_2(\mathbb{Q}_p)$ for p a prime. Thus in the following we assume Proposition 3.15 and the properties of the Harish-Chandra spherical function, which will be proved later on in this chapter.

Lemma 3.18. *Let $(\pi, \mathscr{H})$ be unitary representation of $G = \mathrm{SL}_2(\mathbb{Q}_p)$ with $q(\pi) < \infty$. Then $\pi \otimes \gamma^s$ is tempered for $s \in (0, \frac{2}{q(\pi)}) \cap (0,1)$. Moreover, for all K-finite vectors $v, w \in \mathscr{H}$,*

$$|\langle \pi_g v, w\rangle| \ll_p \sqrt{d_v d_w}\, ||v||\, ||w||\, \frac{\Xi(g)}{||g||^{s-1}},$$

where the constant does not depend on s. Hence in particular for $\varepsilon > 0$,

$$|\langle \pi_g v, w\rangle| \ll_{p,\varepsilon} \sqrt{d_v d_w}\, ||v||\, ||w||\, ||g||^{-\frac{2}{q(\pi)}+\varepsilon}.$$

Proof. Choose $q > 2$ so that $q(\pi) < q \leq \frac{2}{s}$. Then there is a dense set of vectors $W \subset \mathscr{H}$ with the property that all matrix coefficients of elements in W are in $L^q(G)$. Moreover, the subspace $W_s = \langle \gamma_g^s F_s \,:\, g \in G\rangle \subset \mathscr{H}_s$ is dense by irreducibility of γ^s and as G is unimodular, all the matrix coefficients of elements in W_s are in $L^{\frac{2}{1-\frac{2}{q}}}(G)$ as $\frac{2}{1-s} < \frac{2}{1-\frac{2}{q}}$. Moreover the subspace $W \otimes W_s$ is dense in $\mathscr{H} \times \mathscr{H}_s$.

Let ϕ be the matrix coefficient of $v \otimes F_s$ and $w \otimes F_s$ for $v, w \in W$. By Theorem 2.11, it suffices to show that ϕ is almost square integrable for all such vectors. Note $\phi(g) = \varphi^{\pi}_{v,w}(g)\phi_s(g)$. Thus by using $L^{p_1}(G) \cdot L^{p_2}(G) \subset L^{\frac{p_1 p_2}{p_1+p_2}}(G)$ for $p_1, p_2 > 0$, it follows that $\phi \in L^{\rho}(G)$ for

$$\rho = \frac{q\frac{2}{1-\frac{2}{q}}}{q + \frac{2}{1-\frac{2}{q}}} = \frac{2q}{q(1-\frac{2}{q})+2} = 2,$$

which implies the claim.

With the notation as above, it follows by Theorem 2.28 for K-finite vectors $v, w \in \mathscr{H}$ that

$$\phi(g) \leq \sqrt{d_v d_w}\, ||v||\, ||w||\, ||F_s||^2_{\mathscr{H}_s}\, \Xi(g).$$

Then using Proposition 3.15 (i) and (ii),

$$\begin{aligned} |\langle \pi_g v, w\rangle| &\ll_p \sqrt{d_v d_w}\, ||v||\, ||w||\, ||F_s||^2_{\mathscr{H}_s} \frac{\Xi(g)}{\phi_s(g)} \\ &\ll_p \sqrt{d_v d_w}\, ||v||\, ||w||\, \frac{\Xi(g)}{||g||^{s-1}}. \end{aligned}$$

for all such s, which also implies the last claim since $\Xi(g) \ll_\varepsilon ||g||^{-1+\varepsilon}$. □

Lemma 3.19. *For $s \in (0,1)$,*

$$q(\gamma^s) = \frac{2}{1-s}.$$

In particular, $(\gamma^s, \mathscr{H}_s)$ is non-tempered for any $s \in (0,1)$.

Proof. This follows quickly from Proposition 3.15 and Lemma 3.18. As γ^s is irreducible, the subspace $W_s = \langle \gamma_g^s F_s \,:\, g \in G\rangle$ is dense and by Proposition 3.15, matrix coefficients of all the vectors in W_s are in $L^{\frac{2}{1-s}+\varepsilon}(G)$ for all $\varepsilon > 0$ yet not in $L^{\frac{2}{1-s}}$. This shows $q(\gamma^s) \leq \frac{2}{1-s}$.

Towards the other inequality, we first show that $q(\gamma^s) > 2$, which also implies that γ^s is non-tempered. For a contradiction assume that $q(\gamma^s) = 2$. Then by Lemma 3.18 for all $t \in (0,1)$, the unitary representation $\gamma^s \otimes \gamma^t$ is tempered. This leads to a contradiction by choosing $t \in (1-s, 1)$ so that $s + t > 1$. Namely with such a choice of t it follows by considering the matrix ϕ coefficient of $F_s \otimes F_t$,

$$||g||^{s+t-2} \ll_{p,s,t} \varphi_{s,0}(g)\varphi_{t,0}(g) = \phi(g) \ll_{p,s,t} \Xi(g),$$

where we also used Theorem 2.28 and Lemma 3.27. As $s+t-2>-1$, this contradicts $\Xi(g) \ll_\varepsilon ||g||^{-1+\varepsilon}$. Thus $q(\gamma^s)>2$.

The same argument also shows that $q(\gamma^s) \geq \frac{2}{1-s}$. In fact, assume for a contradiction that $q(\gamma^s) < \frac{2}{1-s}$, in particular there is $q>2$ so that $q(\gamma^s) < q < \frac{2}{1-s}$ or equivalently $0<(1-s)<\frac{2}{q}<\frac{2}{q(\gamma^s)}<1$, where we used as already established above $2<q(\gamma^s)<\infty$. Using Lemma 3.18, we conclude that $\gamma^{\frac{2}{q}} \otimes \gamma^s$ is tempered which is again a contradiction by considering the matrix coefficient ϕ of $F_s \otimes F_{\frac{2}{q}}$ and noting

$$||g||^{\frac{2}{q}+s-2} \ll_{p,s,q} \phi(g) \ll_{p,s,q} \Xi(g).$$

$\square$

We turn to Theorem 3.14. Towards the proof, we define decay exponents of a unitary representations $(\pi, \mathscr{H})$. We say that $(\pi,\mathscr{H})$ has κ-decay for $\kappa>0$ if for all K-finite vectors $v \in \mathscr{H}_G^\perp$, it holds that

$$|\varphi_v^\pi(g)| = |\langle \pi_g v, v\rangle| \ll d_v\, ||v||^2\, ||g||^{-\kappa}$$

for all $g \in G$, where the constant is allowed to depend on π and κ. Then we define the **decay exponent of** $(\pi,\mathscr{H})$ as

$$\kappa(\pi) = \sup\{\kappa \in [0,1] \,:\, (\pi,\mathscr{H}) \text{ has } \kappa\text{-decay}\}.$$

Theorem 3.20. *For any unitary representation $(\pi,\mathscr{H})$ of $\mathrm{SL}_2(\mathbb{Q}_p)$ without almost invariant vectors,*

$$q(\pi) = \frac{2}{\kappa(\pi)} = \frac{2}{1-c(\pi)}.$$

The proof of the theorem splits into three part. First we show $q(\pi)=\frac{2}{\kappa(\pi)}$, then $q(\pi)=\frac{2}{\kappa(\pi)} \geq \frac{2}{1-c(\pi)}$ and finally $q(\pi)=\frac{2}{\kappa(\pi)} \leq \frac{2}{1-c(\pi)}$.

Proof. (of $q(\pi)=\frac{2}{\kappa(\pi)}$) Assume initially $q(\pi)=\infty$. The condition $\kappa(\pi)>0$ clearly implies $q(\pi)<\infty$ – a contradiction. On the other hand, if $\kappa(\pi)=0$ and $q(\pi)<\infty$, then since $(\pi,\mathscr{H})$ does not have almost invariant vectors, $(\pi,\mathscr{H})$ is m-almost square integrable for large enough m and hence Corollary 2.35 implies $\kappa(\pi)>0$.

In the remainder of the proof we assume $q(\pi)<\infty$. Then Lemma 3.18 shows that $\kappa(\pi) \geq \frac{2}{q(\pi)}$. For the other inequality assume for a contradiction that $\frac{2}{\kappa(\pi)} < q(\pi)$. Then choose $\kappa>0$ so that $\frac{2}{q(\pi)}<\kappa<\kappa(\pi)$. Then the matrix coefficients of all the K-finite vectors are $\frac{2}{\kappa}+\varepsilon$ integrable for all $\varepsilon>0$ as in the case $G=\mathrm{SL}_2(\mathbb{R})$,

$$\int (||g||^{-\kappa})^{\frac{2}{\kappa}+\varepsilon}\, m_G(g) \ll \int_0^\infty e^{(-2-\varepsilon\kappa)t} e^{2t}\, dt \ll \infty.$$

A similar calculation holds in the case $G=\mathrm{SL}_2(\mathbb{Q}_p)$ for p a prime number. Thus it follows that $q(\pi) \leq \frac{2}{\kappa}$, which contradicts our assumption on κ. $\square$

Before embarking upon the proof of $q(\pi) = \frac{2}{\kappa(\pi)} \geq \frac{2}{1-c(\pi)}$, we start with a preliminary observation concerning the definition of weak containment. Consider two unitary representation $(\pi, \mathscr{H}_1)$ and $(\rho, \mathscr{H}_2)$ of a Harish-Chandra group $G = KB$, where we assume that $(\pi, \mathscr{H}_1)$ is irreducible. Recall that by Proposition 2.2, as $(\pi, \mathscr{H}_1)$ is irreducible, π is weakly contained in ρ if and only if for any vector $v \in \mathscr{H}_1$, compact set $Q \subset K$ and $\varepsilon > 0$, there exists a vector $w \in \mathscr{H}_2$ with $||w|| = ||v||$ so that

$$||\varphi_v^\pi - \varphi_w^\rho||_{Q,\infty} < \varepsilon.$$

We strengthen this condition under the assumption that v is K-invariant and Q is a compact bi-K-invariant subset of G. In this case, set $w_K = \int_K \pi_k w \, dm_K(k)$ so that for all $g \in Q$,

$$\begin{aligned}
|\varphi_v^\pi(g) - \varphi_{w_K}^\rho(g)| &= \left| \int \int \varphi_v^\pi(k_1 g k_2) - \varphi_w^\rho(k_1 g k_2) \, m_K(k_1) m_K(k_2) \right| \\
&\leq \int \int \left| \varphi_v^\pi(k_1 g k_2) - \varphi_w^\rho(k_1 g k_2) \right| m_K(k_1) m_K(k_2) \\
&< \varepsilon.
\end{aligned}$$

Thus we conclude that under the above assumptions on π, v and Q, that the matrix coefficient φ_v^π can be approximated arbitrarily close on Q by K-invariant elements of $w \in \mathscr{H}_2$ with $||w|| \leq ||v||$. The same condition also holds if we drop the assumption of irreducibility. Namely, in this case, it holds for K-invariant $v \in \mathscr{H}$, bi-K-invariant $Q \subset G$ and $\varepsilon > 0$, that there exist K-invariant vectors $w_1, \ldots, w_n$ with $\sum_{i=1}^n ||w_i||^2 \leq ||v||^2$ so that

$$\left|\left| \varphi_v^\pi - \sum_{i=1}^n \varphi_{w_i}^\rho \right|\right|_{Q,\infty} < \varepsilon.$$

This observation, together with the classification of irreducible representations (3.1), yields the following consequence of general interest.

Proposition 3.21. *Any unitary representation $(\pi, \mathscr{H})$ of $\mathrm{SL}_2(\mathbb{Q}_p)$ without non-zero K-invariant vectors is tempered.*

Proof. The above discussion shows that γ^s is not weakly contained in π. More precisely, this follows as the matrix coefficient ϕ_s cannot be approximated by K-invariant vectors of $\mathrm{SL}_2(\mathbb{Q}_p)$, as there do not exist any non-trivial ones. The same argument also shows $1_G \not\prec \pi$. Hence by (3.1) all the irreducible unitary representations weakly contained in π are tempered. As π can be approximated in the compact-open topology by irreducible unitary representations weakly contained in π and since all the latter irreducible representations satisfy $\prec \lambda$, it clearly follows that $\pi \prec \lambda$. $\square$

Proof. (of $q(\pi) = \frac{2}{\kappa(\pi)} \geq \frac{2}{1-c(\pi)}$) We prove $\kappa(\pi) \leq 1 - c(\pi)$. If $\kappa(\pi) = 1$, then it follows that π is tempered and hence $c(\pi) = 0$. On the other hand if $c(\pi) = 0$, then as $1_G \not\prec \pi$, it follows that all the irreducible representations weakly contained in π are tempered. Thus π is tempered, which implies $q(\pi) = 2$ and $\kappa(\pi) = 1$. Thus we assume in the remainder of the proof that $c(\pi) > 0$ and $\kappa(\pi) < 1$.

For a contradiction, suppose $\kappa(\pi) > 1 - c(\pi)$. Then choose $s \in (0,1)$ with $\gamma^s \prec \pi$ and $c(\pi) > s > 1 - \kappa > 1 - \kappa(\pi)$ for $\kappa < \kappa(\pi) \leq 1$ so that π has κ-decay, where we use that $c(\pi) > 0$. By irreducibility of γ^s and the discussion before the proof, there exists for each bi-K-invariant $Q \subset G$ and $\varepsilon > 0$ a K-invariant vector $w \in \mathscr{H}$ with $||w|| \leq ||F_s||_{\mathscr{H}_s}$ so that

$$||\phi_s - \varphi^\pi_w||_{Q,\infty} < \varepsilon. \tag{3.3}$$

As $-\kappa < (s-1)$, the decay of ϕ_s is slower that the one of φ^π_w. We show how this decay discrepancy leads to a contradiction of (3.3) implying that $\kappa(\pi) \leq 1 - c(\pi)$. To see this, recall that by the definition of κ-decay and as w is K-invariant with $||w|| \leq ||F_s||$, it follows $|\varphi^\pi_w| \ll_{\pi,\kappa} ||w||^2\, ||g||^{-\kappa} \ll_{\pi,\kappa,s} ||g||^{-\kappa}$. Denote by $c_1 = c_1(\pi,\kappa,s)$ the constant so that $|\varphi^\pi_w| \leq c_1||g||^{-\kappa}$. Moreover, we write $c_2 = c_2(p,s)$ for a constant so that $c_2||g||^{s-1} \leq \phi_s(g)$. Next choose a large enough compact and bi-K-invariant set Q with the property

$$\frac{||g||^{-\kappa}}{||g||^{s-1}} \leq \frac{c_2}{2c_1} \tag{3.4}$$

for some $g \in Q$, which is possible as $-\kappa - (s-1) < 0$. For an element $g \in Q$ which satisfies (3.4),

$$|\varphi^\pi_w| \leq c_1||g||^{-\kappa} \leq \frac{c_2||g||^{s-1}}{2} \leq \frac{\phi_s(g)}{2}.$$

Thus it follows for a compact set $Q \subset G$ chosen as above and all K-invariant $w \in \mathscr{H}$ with $||w|| \leq ||F_s||$ that $||\phi_s - \varphi^\pi_w||_{Q,\infty} \geq \inf_{g\in Q} \frac{\phi_s(g)}{2} > 0$, contradicting $\gamma^s \prec \pi$. □

For the final part of the proof, we evoke integral decompositions.

Proposition 3.22. *Let $(\pi,\mathscr{H})$ be a unitary representation of a group G and*

$$\pi = \int_X^\oplus \pi_x\, d\mu(x)$$

be an integral decomposition. Denote by $q_{(X,\mu)}$ the function $x \mapsto q(\pi_x)$. Then

$$q(\pi) = ||q_{(X,\mu)}||_\infty.$$

Proof. We first prove $q(\pi) \leq ||q_{(X,\mu)}||_\infty$. Write for simplicity $q = ||q_{(X,\mu)}||_\infty$ and let $\varepsilon > 0$. Then there exists for almost all $x \in X$ a dense set of vectors v_x so that $\varphi^{\pi_x}_{v_x} \in L^{q+\varepsilon}$. The collection of vectors

$$v = \int_X v_x\, d\mu(x)$$

where for almost all $x \in X$ the vector v_x is from the above dense subset is again dense in $\mathscr{H}$. Then for each such v,

$$(\varphi^\pi_v)^{q+\varepsilon} = \int_X (\varphi^{\pi_x}_{v_x})^{q+\varepsilon}\, d\mu(x) < \infty$$

and hence $q(\pi) \leq q + \varepsilon$ for all $\varepsilon > 0$.

For the other inequality, assume for a contradiction that $||q_{(X,\mu)}||_\infty > q(\pi) + \varepsilon > q(\pi)$ for $\varepsilon > 0$. Then there is a set of positive measure of representations π_x with $q(\pi_x) > q(\pi) + \varepsilon$. This leads to a contradiction. $\square$

Proof. (of $q(\pi) = \frac{2}{\kappa(\pi)} \leq \frac{2}{1-c(\pi)}$) Let $\pi = \int_X^{\oplus} \pi_x \, \mu(x)$ be an integral decomposition into irreducible representations. By Proposition 2.18 almost all π_x are weakly contained in π. Thus by Proposition 3.22 and Lemma 3.19,

$$q(\pi) = ||q_{(X,\mu)}||_\infty \leq \max\left\{2, \sup_{\gamma^s \prec \pi} q(\gamma^s)\right\} = \frac{2}{1-c(\pi)}.$$

Note that we can only conclude $\leq$ since it does not have to be the case that if $\gamma^s \prec \pi$, that then γ^s appears in the above integral decomposition. $\square$

Theorem 3.23. *A unitary representation $(\pi, \mathscr{H})$ of $\mathrm{SL}_2(\mathbb{Q}_p)$ without almost invariant vectors has spectral gap if and only if $q(\pi) < \infty$.*

The main observation for the proof of Theorem 3.23 is the next proposition, which also shows that $\mathrm{SL}_2(\mathbb{Q}_p)$ does not have property (T).

Proposition 3.24. *Let $c \in (0, 1]$. Then the collection of unitary representations*

$$\mathscr{U}_c = \{\gamma^s \,:\, s \leq c\}$$

has a uniform spectral gap if and only if $c < 1$.

Proof. First assume $c < 1$. Then using Theorem 3.20 and Lemma 3.18 the collection of unitary representations $\mathscr{U}_c$ has a uniform effective decay of matrix coefficients. Thus using precisely the same proof as in the direction (iv) implies (i) of Theorem 3.5, it follows that $\mathscr{U}_c$ has a uniform spectral gap.

It remains to show that the collection $\mathscr{U}_1$ does not have a uniform spectral gap. Assume for a contradiction that it has (Q, ε) as a uniform spectral gap. Then choose $m \geq 1$ large enough so that $Q \subset B_m^\circ \subset B_m$, where B_m is the ball around $e \in G$ of elements of norm $\leq m$, for a bi-K-invariant matrix norm of G. By Proposition 3.3 there is $\delta = \delta(Q, \varepsilon, m)$ with

$$||\gamma^s(f_{B_m})||_{\mathrm{op}} \leq 1 - \delta < 1$$

for all $s \in (0, 1)$. In particular for a natural numbers n,

$$||\gamma^s(f_{B_m}^{*n})||_{\mathrm{op}} \leq ||\gamma^s(f_{B_m})||^n \leq (1-\delta)^n.$$

Observe that $f_{B_m}^{*n}$ has mass 1. Using that $f_{B_m}^{*n}$ is bi-K-invariant, one concludes

$$\begin{aligned} ||\gamma^s(f_{B_m}^{*n})||_{\mathrm{op}} &\asymp_{p,s} \langle \gamma^s(f_{B_m}^{*})F_s, F_s\rangle \\ &= \int f_{B_m}^{*n}(g)\phi_s(g)\, dm_G(g) \\ &\gg_{p,s} m^{n(s-1)}. \end{aligned}$$

Thus there is a constant $c = c(p, s) > 0$ only depending on p and s so that

$$m^{n(s-1)} \leq c(1-\delta)^n$$

for all $n \geq 1$. Hence taking the logarithm as $n \to \infty$, it follows that

$$(s-1) \leq \frac{\log(1-\delta)}{\log(m)} < 0.$$

In particular it follows that $1 \leq 1 + \frac{\log(1-\delta)}{\log(m)} < 1$, which is a contradiction. □

Proof. (of Theorem 3.23) The proof follows from Theorem 3.20 and Proposition 3.24.

First assume that $q(\pi) < \infty$. Then by Lemma 3.18 the matrix coefficients of π vanish effectively, which implies a spectral gap again by the proof of the direction (iv) implies (i) of Theorem 3.5.

On the other hand if $(\pi, \mathscr{H})$ has a spectral gap, then the collection of all irreducible representations weakly contained in π has a uniform spectral gap. Thus by Proposition 3.24 (or more precisely its proof), it follows that $c(\pi) < 1$ and hence by Theorem 3.20 $q(\pi) < \infty$. □

Combining the last two theorems yields Theorem 3.14. We now turn to proving Proposition 3.15, first in the case $G = \mathrm{SL}_2(\mathbb{R})$. On $\mathrm{SL}_2(\mathbb{R})$ we consider a bi-K-invariant matrix norm, which for example is constructed by averaging the sub-multiplicative matrix norm

$$||\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)|| = 2\max(|a|, |b|, |c|, |d|)$$

for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$.

In the following paragraphs denote

$$K = \mathrm{SO}_2(\mathbb{R}) = \left\{ k_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \,:\, \theta \in [0, 2\pi) \right\},$$

$$A = \left\{ a_t \text{ for } t \in \mathbb{R} \text{ and } a_t = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \right\}$$

and

$$N = U = \left\{ u_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \,:\, x \in \mathbb{R} \right\}.$$

By the Cartan decomposition, we have $G = KAK$. More precisely, every $g \in G$ can be written as $g = k_\theta a_t k_\psi$ for $\theta, \psi \in [0, 2\pi)$ and for $t \geq 0$. With this assumption the element a_t is uniquely determined by g.

We discuss the Harish-Chandra spherical function on $\mathrm{SL}_2(\mathbb{R})$. Before doing so, we prove a calculative lemma.

Lemma 3.25. *Let $t \in \mathbb{R}$ and $\theta \in [0, 2\pi)$. Write*

$$a_t^{-1} k_\theta = k_\psi a_{t_0} u_x$$

for $t_0, x \in \mathbb{R}$ and $\psi \in [0, 2\pi)$. Then

$$t_0 = \ln\left(\sqrt{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}\right), \tag{3.5}$$

$$x = \frac{\sin(2\theta)\sinh(2t)}{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}, \tag{3.6}$$

$$\psi = \arccos\left(\sqrt{\frac{e^{-2t}\cos^2\theta}{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}}\right). \tag{3.7}$$

Proof. The Iwasawa decomposition reflects the Gram-Schmidt algorithm. More precisely, if $g = (v_1, v_2) \in \mathrm{SL}_2(\mathbb{R})$ for $v_1, v_2 \in \mathbb{R}^2$, then by using Gram-Schmidt we arrive at

$$v_1' = \frac{1}{||v||_1} v_1 \qquad \text{and} \qquad v_2' = ||v||_1 v_2 - \frac{\langle v_1, v_2 \rangle}{||v_1||} v_1,$$

where the vectors v_1' and v_2' are orthogonal. As

$$(v_1', v_2') = g \begin{pmatrix} \frac{1}{||v_1||} & -\frac{\langle v_1, v_2 \rangle}{||v_1||}\rangle \\ 0 & ||v_1|| \end{pmatrix}$$

still has determinant 1 and v_1' has norm 1, it follows that v_2' also has norm 1 and hence $(v_1', v_2') = k_\psi \in K$. Moreover, setting $t_0 = \ln(||v_1||)$ and $x = \frac{\langle v_1, v_2 \rangle}{||v_1||^2}$ we can write

$$g u_{-x} a_{-t_0} = k_\psi$$

or equivalently

$$g = k_\psi a_{t_0} u_x.$$

In the concrete case, where

$$g = a_t^{-1} k_\theta = \begin{pmatrix} e^{-t} \cos\theta & -e^{-t} \sin\theta \\ e^t \sin\theta & e^t \cos\theta \end{pmatrix}$$

one calculates

$$t_0 = \ln(||v_1||) = \ln\left(\sqrt{e^{-2t} \cos^2\theta + e^{2t} \sin^2\theta}\right)$$

and

$$\begin{aligned} x = \frac{\langle v_1, v_2 \rangle}{||v_1||^2} &= \frac{-e^{-2t} \sin\theta\cos\theta + e^{2t} \sin\theta\cos\theta}{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta} \\ &= \frac{\sin(2\theta)\sinh(2t)}{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}. \end{aligned}$$

Finally, it follows that

$$\begin{pmatrix} \cos\psi \\ \sin\psi \end{pmatrix} = k_\psi e_1 = \frac{1}{||v_1||} v_1 = \frac{1}{\sqrt{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}} \begin{pmatrix} e^{-t}\cos\theta \\ e^t \sin\theta \end{pmatrix}.$$

Thus,

$$\cos^2\theta = \frac{e^{-2t}\cos^2\theta}{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}$$

which concludes the proof. □

Proposition 3.26. *For $G = \mathrm{SL}_2(\mathbb{R})$, the Harish-Chandra spherical function Ξ satisfies for all $\varepsilon > 0$,*

$$\Xi(g) \asymp ||g||^{-1}(1 + \log(||g||)) \ll_\varepsilon ||g||^{-1+\varepsilon}.$$

Moreover, $\Xi \in L^{2+\varepsilon}(G)$ for all $\varepsilon > 0$.

Proof. Recall that

$$\triangle_B\left(\begin{pmatrix} a & x \\ 0 & a^{-1}\end{pmatrix}\right) = |a|^{-2}$$

for all $a \in \mathbb{R}_{\neq 0}$ and $b \in \mathbb{R}$ and so in particular, using the notation from chapter 2.3, $f_0(ka_tu_x) = \triangle_B(a_t)^{\frac{1}{2}} = e^{-t}$. Recall that Ξ is bi-K-invariant.

By the Cartan decomposition, it suffices to prove the claimed estimate only for elements $g = a_t$ for $t \in \mathbb{R}_{\geq 0}$. We calculate using Lemma 3.25,

$$\begin{aligned}
\Xi(a_t) &= \langle \pi_{a_t} f_0, f_0\rangle_{\mathscr{H}_0} \\
&= \int_K f_0(a_t^{-1}k) f_0(k)\, dm_K(k) \\
&= \frac{1}{2\pi}\int_0^{2\pi} f_0(a_t^{-1}k_\theta)\, d\theta \\
&= \frac{1}{2\pi}\int_0^{2\pi} \triangle_B(a_{t_0})^{\frac{1}{2}}\, d\theta \\
&= \frac{1}{2\pi}\int_0^{2\pi} \triangle_B(a_{t_0})^{\frac{1}{2}}\, d\theta \\
&= \frac{1}{2\pi}\int_0^{2\pi} \left(\sqrt{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}\right)^{-1}\, d\theta \\
&= \frac{4}{2\pi}\int_0^{\frac{\pi}{2}} \left(e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta\right)^{-\frac{1}{2}}\, d\theta.
\end{aligned}$$

Observe

$$e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta \asymp \max\{e^{-2t}\cos^2\theta, e^{2t}\sin^2\theta\}$$

and the latter maximum is $e^{2t}\sin^2\theta$ unless $\tan^2\theta < e^{-4t}$ or equivalently $\tan\theta < e^{-2t}$. Thus

$$\Xi(a_t) \asymp \int_0^{\arctan e^{-2t}} (e^{-2t}\cos^2\theta)^{-\frac{1}{2}}\, d\theta + \int_{\arctan e^{-2t}}^{\frac{\pi}{2}} (e^{2t}\sin^2\theta)^{-\frac{1}{2}}\, d\theta.$$

As $t \geq 0$, $\arctan e^{-2t} < 1$. Hence on the interval $[0, \arctan e^{-2t}]$ it holds that $\frac{1}{2} \leq \cos\theta \leq 1$. Moreover on $[0, \frac{\pi}{2}]$, $\frac{\theta}{2} \leq \sin\theta \leq \theta$, which allows us to deduce the estimate

$$\begin{aligned}
\Xi(a_t) &\asymp e^t \arctan e^{-2t} + e^{-t}\int_{\arctan e^{-2t}}^{\frac{\pi}{2}} \frac{1}{|\theta|}\, d\theta \\
&\asymp e^t \arctan e^{-2t} + e^{-t}\left(\ln\left(\tfrac{\pi}{2}\right) - \ln\left(\arctan e^{-2t}\right)\right).
\end{aligned}$$

Recall that on $[0,1]$, $\frac{x}{2} \leq \arctan x \leq x$. Thus it follows

$$\Xi(a_t) \asymp e^{-t} + e^{-t}t = e^{-t}(1+t).$$

As $||a_t|| \asymp e^t$, the first claim follows.

For the second claim, we again use the Cartan decomposition and coordinates given by $g = k_\theta a_t k_\psi$ for $\theta \in [0, 2\pi)$, $t \in [0,\infty)$ and $\psi \in [0,\pi)$. Then

$$dm_G = c_{m_G}\left(\frac{e^{2t} - e^{-2t}}{2}\right) d\theta\, dt\, d\psi = c_{m_G} \sinh 2t\, d\theta\, dt\, d\psi.$$

Thus we conclude for $\varepsilon > 0$,

$$\begin{aligned}\int_G (\Xi(g))^{2+\varepsilon}\, dm_G(g) &\ll \int_0^\infty (\Xi(a_t))^{2+\varepsilon} \sinh 2t\, dt \\ &\ll_\delta \left(e^{-t(1-\delta)}\right)^{2+\varepsilon} e^{2t}\, dt \\ &= \int_0^\infty e^{t(-(2+\varepsilon)(1-\delta)+2)}\, dt < \infty\end{aligned}$$

for δ sufficiently small so that $-(2+\varepsilon)(1-\delta)+2 < 0$. □

We next define the complementary series representation for $\mathrm{SL}_2(\mathbb{R})$. For $s \in (0,1)$ the non-unitary character $\chi_{(s)}$ on $B = \{a_t u_x \ t, x \in \mathbb{R}\}$ is defined as

$$\chi_{(s)}(a_t u_x) = e^{st}$$

for $a_t u_x \in B$.

Consider the space $\mathscr{V}_s$ consisting of all functions $f : G \to \mathbb{C}$ with the properties:

(i) f is smooth.

(ii) f is even, i.e. $f(-g) = f(g)$ for all $g \in G$.

(iii) For $g \in G$ and $b \in B$,

$$f(gb) = \chi_{(s)}(b)^{-1} \triangle_B(b)^{\frac{1}{2}} f(g).$$

Then we define the operator γ_g^s for $g \in G$ as the regular representation so that for all $f \in \mathscr{V}_s$

$$(\gamma_g^s f)(h) = f(g^{-1}h)$$

for $h \in G$.

As the character is non-unitary, the standard inner product on $L^2(K)$ does not yield a unitary representation. Thus we need to define an alternative scalar product on $\mathscr{V}_s$. The scalar product we define is

$$\begin{aligned}\langle f_1, f_2\rangle_{\mathscr{V}_s} &= \frac{1}{\pi^2}\int_0^\pi \int_0^\pi \frac{f_1(k_{\theta_1})\overline{f_2(k_{\theta_2})}}{|\sin(\theta_1-\theta_2)|^{1-s}}\, d\theta_1 d\theta_2 \qquad (3.8)\\ &= \frac{1}{4\pi^2}\int_0^{2\pi} \int_0^{2\pi} \frac{f_1(k_{\theta_1})\overline{f_2(k_{\theta_2})}}{|\sin(\theta_1-\theta_2)|^{1-s}}\, d\theta_1 d\theta_2\end{aligned}$$

In [EW] chapter 9.5, it is shown that $\langle\cdot,\cdot\rangle_{\mathscr{V}_s}$ is a scalar product on $\mathscr{V}_s$. The **complementary series** is then defined as the completion $\mathscr{H}_s$ of $\mathscr{V}_s$, and we again denote by γ^s the extension of γ^s defined on $\mathscr{V}_s$ to $\mathscr{H}_s$. Also in chapter 9.5 of [EW] it is shown that $(\mathscr{H}_s, \gamma^s)$ is an irreducible unitary representation.

For $n \in 2\mathbb{Z}$, the function $F_{s,n}$ is defined to be the element of $\mathscr{V}_s$ given by

$$F_{s,n}(k_\theta a_t u_x) = e^{-in\theta} e^{-(s+1)t}$$

for θ, t, x as usual. Furthermore, denote the diagonal matrix coefficient of $F_{s,n}$ as

$$\phi_{s,n} = \varphi_{F_{s,n}}^{\gamma^s}.$$

Then clearly $|\phi_{s,n}| \leq |\phi_{s,0}|$. In particular, using the notation from the beginning of this subchapter, $F_s = F_{s,0}$ and $\phi_s = \phi_{s,0}$.

Lemma 3.27. *For $s \in (0,1)$ the matrix coefficients ϕ_s is bi-K-invariant, satisfies*

$$\phi_s(g) \asymp_s ||g||^{s-1}$$

for $g \in \mathrm{SL}_2(\mathbb{R})$ and belongs to $L^q(G)$ if and only if $q > \frac{2}{1-s}$. Moreover, the following explicit estimate holds:

$$\frac{||g||^{s-1}}{s} \ll \phi_s(g) \ll \frac{||g||^{s-1}}{s^2}.$$

In particular, $\phi_s(g) > 0$ for all $g \in G$.

Proof. We use a similar calculation to the one of Proposition 3.26. As F_s has K-weight zero, it is clear that ϕ_s is bi-K-invariant. Thus it suffices to consider $g = a_t$ for $t \geq 0$. Note that

$$\begin{aligned} F_s(a_t^{-1}k_\theta) &= F_s(k_\psi a_{t_0} u_x) = e^{-(s+1)t_0} \\ &= \left(\sqrt{e^{-2t}\cos^2\theta + e^{2t}\sin^2\theta}\right)^{-(s+1)} \\ &\asymp \max\left(e^{-t}|\cos\theta|, e^t|\sin\theta|\right)^{-(s+1)}. \end{aligned}$$

Thus analogous to the proof of Proposition 3.26,

$$\begin{aligned} \phi_s(a_t) &= \langle \gamma^s_{a_t} F_s, F_s\rangle_{\mathcal{V}_s} \\ &= \frac{1}{\pi^2}\int_0^\pi\int_0^\pi \frac{F_s(a_t^{-1}k_{\theta_1})\overline{F_s(k_{\theta_2})}}{|\sin(\theta_1-\theta_2)|^{1-s}}\, d\theta_1 d\theta_2 \\ &\asymp \int_0^\pi\int_0^\pi \frac{\max\left(e^{-t}|\cos\theta_1|, e^t|\sin\theta_1|\right)^{s-1}}{|\sin(\theta_1-\theta_2)|^{1-s}}\, d\theta_1 d\theta_2 \\ &\asymp \int_0^\pi \max\left(e^{-t}|\cos\theta_1|, e^t|\sin\theta_1|\right)^{-(s+1)} \int_0^\pi \frac{1}{|\sin(\theta_1-\theta_2)|^{1-s}}\, d\theta_2 d\theta_1 \\ &\asymp_s \int_0^{\frac{\pi}{2}} \max\left(e^{-t}\cos\theta_1, e^t\sin\theta_1\right)^{-(s+1)}\, d\theta_1 \\ &\asymp_s \int_0^{\arctan e^{-2t}} (e^{-t}\cos\theta_1)^{-(s+1)}\, d\theta_1 + \int_{\arctan e^{-2t}}^{\frac{\pi}{2}} (e^t\sin\theta_1)^{-(s+1)}\, d\theta_1 \\ &\asymp_s e^{t(s+1)}\arctan e^{-2t} + e^{-t(s+1)}\int_{\arctan e^{-2t}}^{\frac{\pi}{2}} \frac{1}{\theta^{s+1}}\, d\theta \\ &\asymp_s e^{t(s-1)} + e^{-t(s+1)}\frac{1}{s}\left((\arctan e^{-2t})^{-s} - (\tfrac{\pi}{2})^{-s}\right) \\ &\asymp_s e^{t(s-1)} + \frac{1}{s}e^{t(s-1)} \asymp_s e^{(s-1)t}, \end{aligned}$$

which implies the claim. Now we conclude for some $q > \frac{2}{1-s}$,

$$\int_G \phi_{(s)}(g)^q\, dm_G(g) \asymp \int_0^\infty \phi_{(s)}(a_t)^q \sinh 2t\, dt \asymp \int_0^\infty e^{t((s-1)q+2)}\, dt < \infty.$$

The latter integral is finite if and only if $(s-1)q+2 < 0$ or equivalently $q > \frac{2}{1-s}$. The explicit estimates for ϕ_s follow by using the next lemma. □

Lemma 3.28. *For $s \in (0,1)$,*

$$||F_s||^2_{\mathscr{H}_s} \asymp \frac{1}{s}.$$

Proof. Observe

$$||F_s||^2_{\mathscr{H}_s} = \langle F_s, F_s \rangle_{\mathscr{H}_s} = \frac{2}{\pi} \int_0^{\frac{\pi}{2}} \frac{1}{|\sin\theta|^{1-s}} \, d\theta.$$

To bound the latter integral, notice $\frac{\theta}{2} \le \sin\theta \le \theta$ on $[0, \frac{\pi}{2}]$, yielding

$$||F_s||^2_{\mathscr{H}_s} \asymp \int_0^{\frac{\pi}{2}} \frac{2^{s-1}}{\theta^{1-s}} \, d\theta \asymp \frac{1}{s}.$$

□

Towards the next lemma, we recall that for $h > 0$ we defined

$$A_h = \{a_t \,:\, 0 \le t \le \log(h)\} \qquad \text{and} \qquad B_h = K A_h K.$$

Then

$$\begin{aligned}
m_G(B_h) &= c_{m_G} \int_0^{\log h} \sinh(2t) \, dt \\
&= \frac{c_{m_G}}{2} \int_0^{\log h} e^{2t} - e^{-2t} \, dt \\
&= \frac{c_{m_G}}{2} \left(\left[\frac{1}{2} e^{2t} \right]_0^{\log h} - \left[-\frac{1}{2} e^{-2t} \right]_0^{\log h} \right) \\
&= \frac{c_{m_G}}{2} \left(\frac{1}{2} (h^2 - 1 + h^{-2} - 1) \right) \\
&= \frac{c_{m_G}}{4} (h^2 + h^{-2} - 2) \\
&\asymp h^2.
\end{aligned}$$

Moreover write $f_{B_h} = \frac{\chi_{B_h}}{m(B_h)}$.

Lemma 3.29. *For all $s \in (0,1)$,*

$$||\gamma^s(f_{B_h})||_{\text{op}} \asymp_s h^{s-1}.$$

Proof. As $f^*_{B_h} = f_{B_h}$, the operator $\gamma^s(f_{B_h})$ is self-adjoint. Thus

$$||\gamma^s(f_{B_h})||_{\text{op}} = \sup_{\substack{f \in \mathscr{H}_s \\ ||f||_{\mathscr{H}_s} \le 1}} |\langle \gamma^s(f_{B_h}) f, f \rangle|.$$

Moreover, since B_h is bi-K-invariant,

$$||\gamma^s(f_{B_h})||_{\text{op}} \asymp |\langle \gamma^s(f_{B_h}) F_s, F_s \rangle|.$$

The estimate of the lemma thus follows as

$$\begin{aligned}
|\langle\gamma^s(f_{B_h})F_s, F_s\rangle| &= \left|\frac{1}{m_G(B_h)}\int_{B_h}\langle\gamma^s_g F_s, F_s\rangle\, dm_G(g)\right| \\
&\asymp_s \frac{1}{h^2}\int_{B_h}||g||^{s-1}\, m_G(g) \\
&\asymp_s \frac{1}{h^2}\int_0^{\log h}||a_t||^{s-1}\sinh(2t)\, dt \\
&\asymp_s \frac{1}{h^2}\int_0^{\log h} e^{t(s+1)}\, dt \\
&\asymp_s h^{s-1}.
\end{aligned}$$

□

Combining the last three lemmas, we have proved Proposition 3.15 for $\mathrm{SL}_2(\mathbb{R})$. We next discuss the case $G = G_p = \mathrm{SL}_2(\mathbb{Q}_p)$ for a fixed prime number p. Denote by $||\cdot||$ the bi-K-invariant matrix norm from chapter 1.1. As in the real case, we first discuss the Harish-Chandra spherical function. Recall the notation for $n \in \mathbb{Z}$,

$$a_n = \begin{pmatrix} p^n & 0 \\ 0 & p^{-n}\end{pmatrix}.$$

Moreover we write $K = K_p = \mathrm{SL}_2(\mathbb{Z}_p)$, $A^+ = A^+_p = \{a_n : n \in \mathbb{Z}_{\geq 0}\}$ and

$$U = N = \left\{u_x = \begin{pmatrix} 1 & x \\ 0 & 1\end{pmatrix} : x \in \mathbb{Q}_p\right\}.$$

Finally denote by $B = B_p$ the upper triangular matrices. Then the modular character on B is given by

$$\triangle_B\left(\begin{pmatrix} a & x \\ 0 & a^{-1}\end{pmatrix}\right) = |a|_p^{-2}$$

for $a \in \mathbb{Q}_p^\times$ and $x \in \mathbb{Q}_p$.

Proposition 3.30. *For $G = \mathrm{SL}_2(\mathbb{Q}_p)$ the Harish-Chandra spherical function Ξ satisfies for $n \in \mathbb{Z}_{\geq 0}$ and $k_1, k_2 \in K$,*

$$\Xi(k_1 a_n k_2) = \Xi(a_n) \asymp_p p^{-n}.$$

Moreover, $\Xi \in L^{2+\varepsilon}(G)$ for all $\varepsilon > 0$.

Proof. Recall that f_0 is the element of $\mathscr{H}_0$ that satisfies $f_0 \equiv 1$ on K. Then $f_0(kb) = \triangle_B(b)^{\frac{1}{2}}$ for all $k \in K$ and $b \in B$ and

$$\Xi(a_n) = \int_K f_0(a_{-n}k)\, dm_K(k).$$

Denote by $k = \left(\begin{smallmatrix} x & y \\ z & w\end{smallmatrix}\right) \in K$ an arbitrary element of K. We want to calculate $f_0(a_{-n}k)$. In order to do so we need to know the Iwasawa decomposition of the matrix

$$a_{-n}k = \begin{pmatrix} p^{-n}x & p^{-n}y \\ p^n z & p^n w\end{pmatrix}.$$

If $|p^{-n}x|_p \geq |p^n z|_p$, then the Iwasawa decomposition is given as

$$\begin{pmatrix} p^{-n}x & p^{-n}y \\ p^n z & p^n w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^{2n}\frac{z}{x} & 1 \end{pmatrix} \begin{pmatrix} p^{-n}x & p^{-n}y \\ 0 & p^n x^{-1} \end{pmatrix}$$

and

$$f_0(a_{-n}k) = |p^{-n}x|_p^{-1} = p^{-n}|x|_p^{-1}.$$

On the other hand if $|p^{-n}x|_p \leq |p^n z|_p$ then the Iwasawa decomposition is given as

$$\begin{pmatrix} p^{-n}x & p^{-n}y \\ p^n z & p^n w \end{pmatrix} = \begin{pmatrix} p^{-2n}\frac{x}{z} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p^n z & p^n w \\ 0 & p^{-n}z^{-1} \end{pmatrix}$$

and

$$f_0(a_{-n}k) = |p^n z|_p^{-1} = p^n |z|_p^{-1}.$$

To summarize,

$$f_0(a_{-n}k) = \max(|p^{-n}x|_p, |p^n z|_p)^{-1} = p^{-n}\max(|x|_p, p^{-2n}|z|_p)^{-1}$$

and

$$\Xi(a_{-n}) = p^{-n}\int_K \max(|x|_p, p^{-2n}|z|_p)^{-1}\, dm_K(k).$$

As

$$|x|_p \leq \max(|x|_p, p^{-2n}|z|_p) \leq \max(|x|_p, |z|_p)$$

it follows that

$$|x|_p^{-1} \geq \max(|x|_p, p^{-2n}|z|_p)^{-1} \geq \max(|x|_p, |z|_p)^{-1}$$

and hence indeed

$$\int_K \max(|x|_p, p^{-2n}|z|_p)^{-1}\, dm_K(k) \asymp_p 1,$$

which implies the first claim.

For the second claim we evoke the integration formula from Proposition 1.7. Thus for $\varepsilon > 0$,

$$\int_G (\Xi(g))^{2+\varepsilon}\, dm_G \asymp_p \sum_{n\geq 0} p^{2n}\Xi(a_n)^{2+\varepsilon} \asymp_p \sum_{n\geq 0} p^{-n\varepsilon} < \infty.$$

$\square$

We now turn to the complementary series of $\mathrm{SL}_2(\mathbb{Q}_p)$. Choose again $s \in (0,1)$ and consider the character on B defined as

$$\chi_{(s)}\left(\begin{pmatrix} t & x \\ 0 & t^{-1} \end{pmatrix}\right) = |t|_p^s$$

for $t \in \mathbb{Q}_p^\times$ and $x \in \mathbb{Q}_p$. Denote by $\mathscr{V}_s$ the space consisting of functions $f : G \to \mathbb{C}$ with the properties:

(i) f is locally constant.

(ii) f is even, i.e. $f(-g) = f(g)$ for all $g \in G$.

(iii) For all $g \in G$ and $b \in B$,

$$f(gb) = \chi_{(s)}(b)^{-1} \triangle_B(b)^{\frac{1}{2}} f(g).$$

In order to equip $\mathscr{V}_s$ with an inner product, we denote for two vectors $v_1, v_2 \in \mathbb{Q}_p^2$ by

$$\mathcal{D}(v_1, v_2) = \det(v_1, v_2).$$

Then for $f_1, f_2 \in \mathscr{V}_s$ we define the inner product as

$$\langle f_1, f_2 \rangle_{\mathscr{V}_s} = \int_K \int_K \frac{f_1(k_1)\overline{f_2(k_2)}}{|\mathcal{D}(k_1 e_1, k_2 e_1)|_p^{1-s}} \, dm_K(k_1) dm_K(k_2),$$

where we denote by e_1 the vector $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. As before, for $g \in \mathrm{SL}_2(\mathbb{Q}_p)$, write γ_g^s for the representation on $\mathscr{V}_s$ given as

$$(\gamma_g^s f)(h) = f(g^{-1}h),$$

where $f \in \mathscr{V}_s$ and $h \in G$.

The completion $(\mathscr{H}_s, \gamma^s)$ of $(\mathscr{V}_s, \gamma^s)$ is called the **complementary series representation** of $\mathrm{SL}_2(\mathbb{Q}_p)$ with parameter $s \in (0,1)$. We refer to [GGPS] for a proof that $(\mathscr{H}_s, \gamma^s)$ is indeed an irreducible unitary representation. Moreover, it is clearly spherical and we denote by F_s the extension of the $\equiv 1$ function on K, which is a spherical vector, and by ϕ_s the diagonal matrix coefficient associated to F_s.

Lemma 3.31. *For $s \in (0,1)$ the matrix coefficient ϕ_s is bi-K-invariant, satisfies*

$$\phi_s(g) \asymp_{p,s} ||g||^{s-1}$$

for $g \in \mathrm{SL}_2(\mathbb{Q}_p)$ and belongs to $L^q(G)$ if and only if $q > \frac{2}{1-s}$. More precisely,

$$\phi_s(g) \asymp_p \frac{||g||^{s-1}}{1 - p^{-s}}.$$

Proof. Let $k_1 = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Q}_p)$. Then in the proof of Proposition 3.30 we showed that

$$a_{-n} k_1 = k \begin{pmatrix} a & * \\ 0 & a^{-1} \end{pmatrix}.$$

for some $k \in K$ and $a \in \mathbb{Q}_p^\times$ satisfying

$$|a|_p = \max(|p^{-n}x|_p, |p^n z|_p).$$

Hence

$$F_s(a_{-n}k_1) = \max(|p^{-n}x|_p, |p^n z|_p)^{-(s+1)} = p^{-n(s+1)} \max(|x|_p, p^{-2n}|z|_p)^{-(s+1)}.$$

Observe moreover that if k_1 is fixed, then

$$\begin{aligned} \int_K \frac{1}{|\mathcal{D}(k_1 e_1, k_2 e_1)|_p^{1-s}} \, dm_K(k_2) &= \int_K \frac{1}{|\mathcal{D}(e_1, k_1^{-1} k_2 e_1)|p^{1-s}} \, dm_K(k_2) \\ &= \int_K \frac{1}{|\mathcal{D}(e_1, k_2 e_1)|_p^{1-s}} \, dm_K(k_2) \end{aligned}$$

does not depend on k_1 and is a fixed positive number, which we estimate explicitly next.

In order to do so consider the primitive vectors of $\mathbb{Z}_p^2$ defined as

$$(\mathbb{Z}_p^2)_{\mathrm{prim}} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}_p^2 \,:\, |a|_p = 1 \text{ or } |b|_p = 1 \right\}.$$

Then $\mathrm{SL}_2(\mathbb{Z}_p)$ acts transitively on $(\mathbb{Z}_p^2)_{\mathrm{prim}}$ preserving the restricted volume probability of $\mathbb{Z}_p^2$. The stabilizer at the vector $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ is $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) < \mathrm{SL}_2(\mathbb{Z}_p)$. Thus writing again as $k_2 = \left(\begin{smallmatrix} x_2 & y_2 \\ z_2 & w_2 \end{smallmatrix}\right)$, we conclude,

$$\begin{aligned}
\int_K \frac{1}{|\mathcal{D}(e_1, k_2 e_1)|_p^{1-s}}\, dm_K(k_2) &= \int_K |z_2|_p^{s-1}\, dm_K(k_2) \\
&\asymp_p \int_{(\mathbb{Z}_p^2)_{\mathrm{prim}}} |z_2|_p^{s-1}\, dm_{(\mathbb{Z}_p^2)_{\mathrm{prim}}}(x_2, z_2) \\
&\asymp_p \sum_{n=0}^{\infty} \int_{z_2 \in p^n \mathbb{Z}_p^\times} |z_2|_p^{s-1}\, dm_{(\mathbb{Z}_p^2)_{\mathrm{prim}}}(x_2, z_2) \\
&\asymp_p (1-p^{-1}) + (1-p^{-1}) \sum_{n=1}^{\infty} p^{-n(s-1)} p^{-n} (1-p^{-1}) \\
&\asymp_p (1-p^{-1}) + (1-p^{-1})^2 \left(\frac{1}{1-p^{-s}} - 1 \right),
\end{aligned}$$

where we used that $m_{\mathbb{Z}_p}(p^n \mathbb{Z}_p^\times) = p^{-n}(1-p^{-1})$. Thus we conclude

$$\int_K \frac{1}{|\mathcal{D}(e_1, k_2 e_1)|_p^{1-s}}\, dm_K(k_2) \asymp_p \frac{1}{1-p^{-s}}.$$

We next calculate

$$\begin{aligned}
\phi_s(a_n) &= \langle \gamma_{a_n}^s F_s, F_s \rangle \\
&= \int_K \int_K \frac{F_s(a_{-n} k_1) \overline{F_s(k_2)}}{|\mathcal{D}(k_1 e_1, k_2 e_1)|_p^{1-s}}\, dm_K(k_1) dm_K(k_2) \\
&\asymp_{p,s} \int_K F_0(a_{-n} k_1)\, dm_K(k_1) \\
&\asymp_{p,s} p^{-n(s+1)} \int_{|x|_p > p^{-2n} |z|_p} |x|_p^{-(s+1)}\, dm_K(k_1) \\
&+ p^{n(s+1)} \int_{|x|_p \le p^{-2n} |z|_p} |z|_p^{-(s+1)}\, dm_K(k_1).
\end{aligned}$$

The same method as before is used to calculate the latter two integrals. As at least one of x and z is an element of $\mathbb{Z}_p^\times$, it follows that in the second integral,

$|z|_p = 1$ and hence the integrand is the constant function. Thus

$$\begin{aligned}\int_{|x|_p \le p^{-2n}|z|_p} |z|_p \, dm_K(k_1) &= \int_{|x|_p \le p^{-2n}} 1 \, dm_K(k_1) \\ &\asymp_p \int_{|x|_p \le p^{-2n}} 1 \, dm_{(\mathbb{Z}_p^2)_{\text{prim}}}(x,z) \\ &\asymp_p m_{\mathbb{Z}_p}(\mathbb{Z}_p^\times) m_{\mathbb{Z}_p}(p^{2n}\mathbb{Z}_p) \\ &\asymp_p (1-p^{-1})p^{-2n} \\ &\asymp_p p^{-2n}.\end{aligned}$$

The first integral is calculated by integrating over the $|x|_p = 1$ part and the $|x|_p \neq 1$ part:

$$\begin{aligned}\int_{|x|_p > p^{-2n}|z|_p} |x|_p^{-(s+1)} \, dm_K(k_1) &= \int_{|x|_p = 1 \text{ and } |x|_p > p^{-2n}|z|_p} |x|_p^{-(s+1)} \, dm_K(k_1) \\ &\quad + \int_{|x|_p \neq 1 \text{ and } |x|_p > p^{-2n}|z|_p} |x|_p^{-(s+1)} \, dm_K(k_1) \\ &\asymp_p (1-p^{-1}) + \int_{p^{-2n} < |x|_p < 1} |x|_p^{-(s+1)} \, dm_K(k_1) \\ &\asymp_p (1-p^{-1}) + \left(1 + \sum_{\ell=1}^{2n-1} (1-p^{-1}) p^{\ell s}\right) \\ &\asymp_p p^{2ns}.\end{aligned}$$

To summarize, we conclude the rough bound

$$\phi_s(a_n) \asymp_{p,s} p^{n(s-1)}$$

and the more precise bound

$$\phi_s(a_n) \asymp_p \frac{p^{n(s-1)}}{(1-p^{-s})}.$$

The final claim follows as for $q > 0$,

$$\int |\phi_s(g)|^q \, dm_G(g) \asymp_{p,s} \sum_{n \ge 0} p^{2n} p^{qn(s-1)}.$$

Thus $\phi \in L^q(G)$ if and only if $q(s-1) + 2 < 0$ or equivalently $q > \frac{2}{1-s}$. □

Corollary 3.32. *For $s \in (0,1)$,*

$$||F_s||^2_{\mathscr{H}_s} \asymp_p \frac{1}{1-p^{-s}}.$$

Proof. This was proved in Lemma 3.31. □

Next fix $h = p^m$ for some $m \in \mathbb{N}$ and recall

$$A_h = \{a_n \,:\, 0 \le n \le m\} \qquad \text{and} \qquad B_h = K A_h K.$$

so that

$$m_G(B_h) \asymp \sum_{n=0}^{m} p^{2n} \asymp_p h^2.$$

Lemma 3.33. *For all $s \in (0,1)$ and $h = p^m$ for $m \in \mathbb{N}$,*

$$||\gamma(f_{B_h})||_{\mathrm{op}} \asymp_{p,s} h^{s-1}.$$

Proof. As in the proof of Lemma 3.29, we just calculate

$$\begin{aligned} |\langle \gamma^s(f_{B_h})F_s, F_s\rangle| &= \left| \frac{1}{m_G(B_h)} \int_{B_h} \langle \gamma^s_g F_s, F_s\rangle \, dm_G(g) \right| \\ &\asymp_{p,s} \frac{1}{h^2} \sum_{n=0}^{m} p^{2n} p^{n(s-1)} \\ &\asymp_{p,s} \frac{1}{h^2} p^{m(s+1)} = h^{s-1}. \end{aligned}$$

□

This concludes the proof of Proposition 3.15 for $\mathrm{SL}_2(\mathbb{Q}_p)$ and hence the proof of Theorem 3.14. In fact, we have improved Proposition 3.15 (i) to the statement

$$\phi_s(g) \asymp_p c_p(s)||g||^{s-1}.$$

4 Effective Ergodic Theory and Spectral Gap

In ergodic theory one studies the action of a group G on a space X preserving a probability measure μ. A central aim is to understand the Birkhoff averages

$$\frac{1}{m_G(B)} \int_B f(g^{-1}.x)\, dm_G(g)$$

for a set of positive measure $B \subset G$ and for $f \in L^1_\mu(X)$. If the system is ergodic, one wishes to show convergence of the latter expression, either pointwise or in L^p, to the mean $\mu(f) = \int f\, d\mu$ as $B \uparrow G$. Results on the convergence properties of the Birkhoff averages are referred to as ergodic theorems.

In the above setting, one is lead to consider the **Koopman representation**, which establishes a link between ergodic theory and the theory of unitary representations. The Koopman representation is given on the Hilbert space $L^2_\mu(X)$ by

$$(\pi_g f)(x) = f(g^{-1}.x)$$

for $f \in L^2_\mu(X)$, $g \in G$ and $x \in X$. Dynamical properties of the measure preserving system (G, X, μ) can be translated to properties of the unitary representation $(\pi, L^2_\mu(X))$.

For example, if one considers the subspace $L^2_0(X) = \{f \in L^2_\mu(X) : \mu(f) = 0\}$, then the measure preserving system (G, X, μ) is ergodic if and only if $(\pi, L^2_0(X))$ has no non-zero invariant vectors. Moreover, the matrix coefficients of $(\pi, L^2_0(X))$ vanish as $g \to \infty$ if and only if (G, X, μ) is mixing.

From this viewpoint, the results from the last chapter establish the remarkable statement that if $G = \mathrm{SL}_n(\mathbb{Q}_p)$ for $n \geq 3$ (or more generally the F-points of a higher rank almost simple algebraic group over a local field F), then every ergodic G-systems is automatically effectively mixing.

The aim of this chapter is assume effective mixing of a G-system in order to establish effective ergodic theorems. In chapter 4.1 we prove a general L^2-ergodic theorem for Harish-Chandra groups. Then, in chapter 4.2, we apply the theory of spherical functions to establish a more effective L^2-ergodic theorem for the representations $\pi_{p,\ell}$. Finally in chapter 4.3 we discuss an effective pointwise ergodic theorem, following [EMV09].

4.1 The Kunze-Stein Phenomenon for Harish-Chandra Groups

Let $G = KB$ be a Harish-Chandra group. In this chapter, we will derive a general mean ergodic theorem for a large class of probability measure preserving systems equipped with a G action. The main engine is the Kunze-Stein inequality, which is discussed next. We note that a function $\psi \in L^1(G)$ is called bi-K-invariant if $\psi(kgk') = \psi(g)$ for $g \in G$ and $k, k' \in K$.

Theorem 4.1. *(Spherical Kunze-Stein inequality) Let $G = KB$ be a Harish-Chandra group and $(\pi, \mathscr{H})$ be a tempered unitary representation of G without invariant vectors. Then for all $p \in [1, 2)$ and all bi-K-invariant $\psi \in L^1(G) \cap L^p(G)$,*

$$||\pi(\psi)||_{\mathrm{op}} \ll_p ||\psi||_p.$$

In fact,

$$||\pi(\psi)||_{\mathrm{op}} \leq ||\Xi||_q ||\psi||_p$$

for q the Hölder conjugate of p.

Proof. We follow [EW] chapter 8.8. As π is tempered, $||\pi(\psi)||_{\mathrm{op}} \leq ||\lambda(\psi)||_{\mathrm{op}}$ and thus it suffices to show that

$$||\lambda(\psi)||_{\mathrm{op}} \leq ||\Xi||_q ||\psi||_p.$$

The latter term is finite as $q = \frac{p-1}{p} > 2$ and hence $||\Xi||_q < \infty$.

Let $f_1, f_2 \in L^2(G)$. Denote by f_i^K the K-invariant function

$$f_i^K = \int_K \lambda_k f_i \, m_K(k).$$

By the Cauchy-Schwarz inequality,

$$\begin{aligned} ||f_i^K||_2^2 &\leq \int |\langle \lambda_{k_1} f_i, \lambda_{k_2} f_i \rangle| \, dm_K(k_1) dm_K(k_2) \\ &\leq \int ||\lambda_{k_1} f_i|| \, ||\lambda_{k_2} f_i|| \, dm_K(k_1) dm_K(k_2) = ||f_i||_2^2. \end{aligned}$$

As ψ is bi-K-invariant and G is unimodular,

$$\begin{aligned} \langle \lambda(\psi) f_1, f_2 \rangle &= \int_G \psi(g) \langle \lambda_g f_1, f_2 \rangle \, dm_G(g) \\ &= \int_G \psi(k_1 g k_2^{-1}) \langle \lambda_g f_1, f_2 \rangle \, dm_G(g) \\ &= \int_G \int_K \int_K \psi(k_1 g k_2^{-1}) \langle \lambda_g f_1, f_2 \rangle \, dm_G(g) dm_K(k_1) dm_K(k_2) \\ &= \int_G \int_K \int_K \psi(g) \langle \lambda_{k_1^{-1} g k_2} f_1, f_2 \rangle \, dm_G(g) dm_K(k_1) dm_K(k_2) \\ &= \int_G \int_K \int_K \psi(g) \langle \lambda_{g k_2} f_1, \lambda_{k_1} f_2 \rangle \, dm_G(g) dm_K(k_1) dm_K(k_2) \\ &= \int_G \psi(g) \langle \lambda_g f_1^K, f_2^K \rangle \, dm_G(g). \end{aligned}$$

Now using Lemma 2.27 and the Hölder inequality,

$$\begin{aligned} |\langle \lambda(\psi) f_1, f_2 \rangle| &\leq \int_G |\psi(g)| \, |\langle \lambda_g f_1^K, f_2^K \rangle| \, dm_G(g) \\ &\leq \left(\int_G |\psi(g)| \, |\Xi(g)| \, dm_G(g) \right) ||f_1^K||_2 ||f_2^K||_2 \\ &\leq ||\Xi||_q ||\psi||_p ||f_1||_2 ||f_2||_2. \end{aligned}$$

The last inequality implies $||\lambda(\psi)||_{\mathrm{op}} \leq ||\Xi||_q ||\psi||_p$. □

Before proceeding with the next corollary, we prove the following lemma of immediate use.

Lemma 4.2. *Let $G = KB$ be a Harish-Chandra group and $(\pi, \mathscr{H})$ be a unitary representation of G and $m \in \mathbb{N}$. Then for any bi-K-invariant $\psi \in L^1(G)$ with $\psi \geq 0$, $\psi^* = \psi$ and $\int_G \psi \, dm_G = 1$,*

$$||\pi(\psi)||_{\mathrm{op}}^{2m} \leq ||\pi^{\otimes 2m}(\psi)||_{\mathrm{op}}.$$

Proof. As $\psi^* = \psi$, the associated operator is symmetric and hence

$$||\pi(\psi)||_{\mathrm{op}} = \sup_{\substack{v\in\mathscr{H}\\ ||v||\leq 1}} |\langle \pi(\psi)v, v\rangle|.$$

The lemma essentially follows by Jensen's inequality. More precisely as $t \mapsto t^{2m}$ is convex and by integrating over the probability measure $\psi(g)dm_G(g)$, it follows for $f_1, f_2 \in \mathscr{H}$,

$$\begin{aligned}
|\langle \pi_*(\psi)f_1, f_2\rangle|^{2m} &= \left|\int_G \langle \pi_g f_1, f_2\rangle \psi(g)\, dm_G(g)\right|^{2m} \\
&\leq \left|\int_G \langle \pi_g f_1, f_2\rangle^{2m} \psi(g)\, dm_G(g)\right| \\
&= \left|\int_G \langle \pi_g^{\otimes 2m} f_1^{\otimes 2m}, f_2^{\otimes 2m}\rangle \psi(g)\, dm_G(g)\right| \\
&= |\langle \pi^{\otimes 2m}(\psi) f_1^{\otimes 2m}, f_2^{\otimes 2m}\rangle|.
\end{aligned}$$

In particular,

$$\begin{aligned}
||\pi(\psi)||_{\mathrm{op}}^{2m} &= \sup_{\substack{v\in\mathscr{H}\\ ||v||\leq 1}} |\langle \pi(\psi)v, v\rangle|^{2m} \\
&\leq \sup_{\substack{v\in\mathscr{H}\\ ||v||\leq 1}} |\langle \pi^{\otimes 2m}(\psi) v^{\otimes 2m}, v^{\otimes 2m}\rangle| \leq ||\pi^{\otimes 2m}(\psi)||_{\mathrm{op}}.
\end{aligned}$$

□

Corollary 4.3. *Let $G = KP$ be a non-compact Harish-Chandra group and $(\pi, \mathscr{H})$ be a unitary representation of G without invariant vectors and almost integrability exponent $q(\pi)$. Let $m \in \mathbb{N}$ be an integer so that $q(\pi) < 4m$. Then for $p \in [1, 2)$ and a bi-K-invariant function $\psi \in L^1(G) \cap L^p(G)$ with $\psi \geq 0$, $\psi^* = \psi$ and $\int \psi\, m_G(g) = 1$,*

$$||\pi(\psi)||_{\mathrm{op}} \ll_p ||\psi||_p^{\frac{1}{2m}}.$$

Proof. By assumption, for a dense set of vectors $V \subset \mathscr{H}$ the matrix coefficients $\varphi^{\pi}_{v,w}$ for all $v, w \in V$ satisfy $\varphi^{\pi}_{v,w} \in L^{4m}(G) \subset L^{4m+\varepsilon}(G)$ for all $\varepsilon > 0$. Thus by Corollary 2.34, it follows that π is $2m$-tempered, i.e. that $\pi^{\otimes 2m}$ is tempered. Using Theorem 4.1 and Lemma 4.2, it follows that

$$||\pi(\psi)||_{\mathrm{op}}^{2m} \leq ||\pi^{\otimes 2m}(\psi)||_{\mathrm{op}} \ll_p ||\psi||_p$$

and so in particular $||\pi(\psi)||_{\mathrm{op}} \ll_p ||\psi||_p^{\frac{1}{2m}}$. □

Finally, we use the latter corollary to establish a mean ergodic theorem. Let (G, X, μ) be a measure preserving system. If $B \subset G$ is a set of non-zero finite measure, then we denote by

$$f_B = \frac{1}{m_G(B)} \chi_B$$

so that for $\phi \in L^2(X)$,

$$(\pi(f_B)\phi)(x) = \frac{1}{m_G(B)} \int_B \phi(g^{-1}.x)\, dm_p(g).$$

Theorem 4.4. *(Mean Ergodic Theorem for Harish-Chandra Groups) Let (G, X, μ) be an ergodic probability preserving system, where G is a non-compact Harish-Chandra group. Assume further that the Koopman representation $(\pi, L^2_\mu(X))$ satisfies $q(\pi) < 4m < \infty$ for $m \in \mathbb{N}$. Then for $\delta > 0$, bi-K-invariant, symmetric sets $B \subset G$ with and all $\phi \in L^2_\mu(X)$,*

$$||\pi(f_B)\phi - \mu(\phi) \cdot 1_X||_{L^2_\mu(X)} \ll_\delta m_G(B)^{-\frac{1}{4m}+\delta} ||\phi||_{L^2_\mu(X)}.$$

Proof. As $(\pi, L^2_0(X))$ has no non-zero invariant vectors, by Corollary 4.3 it follows for $p \in [1, 2)$ that

$$||\pi(f_B)|_{L^2_0(X)}||_{\mathrm{op}} \ll_p ||f_B||_p^{\frac{1}{2m}}.$$

We calculate

$$\begin{aligned} ||f_B||_p^{\frac{1}{2m}} &= \left(\int_G \left(\frac{\chi_B}{m_G(B)} \right)^p dm_G \right)^{\frac{1}{2mp}} \\ &= (m_G(B)^{1-p})^{\frac{1}{2mp}} \\ &= m_G(B)^{-\frac{1}{2m}+\frac{1}{2mp}}. \end{aligned}$$

As $p \in [1, 2)$, we can choose $\delta > 0$ so that $-\frac{1}{4m} + \delta = -\frac{1}{2m} + \frac{1}{2mp}$. Then

$$||\pi(f_B)|_{L^2_0(X)}||_{\mathrm{op}} \ll_\delta m_G(B)^{-\frac{1}{4m}+\delta}.$$

Applying this inequality to the vector $\phi - \mu(\phi) \cdot 1_X$ implies the claim. □

4.2 Spherical Functions and the Mean Ergodic Theorem

We return to considering a simply connected, almost simple algebraic group $\mathrm{G} \subset \mathrm{GL}_n$ over $\mathbb{Q}$. For a prime p, write as usual $G_p = \mathrm{G}(\mathbb{Q}_p)$ and denote for $\ell \geq 0$ coprime to p by $\pi_{p,\ell}$ the unitary representation of G_p on $L^2(X_{p,\ell})$.

The aim of this chapter is to exploit the theory of spherical functions to improve the bound of Theorem 4.4 for the representation $\pi_{p,\ell}$. In order to do so we introduce the **spherical integrability exponent**,

$$q_{p,\ell}(\mathrm{G}) = \inf\{q \geq 2 \,:\, \forall K_p\text{-invariant } v, w \in L^2_0(X_{p,\ell}) \text{ it holds } \varphi^{\pi_{p,\ell}}_{v,w} \in L^q(G_p)\}.$$

We note that it is possible that $q_{p,\ell}(\mathrm{G}) \geq q(\pi_{p,\ell})$. The main aim of this chapter is to prove the following theorem. To simplify the notation we shall make no difference between the operator $\pi_{p,\ell}(f)$ and $\pi_{p,\ell}(f)|_{L^2_0(X_{p,\ell})}$.

Theorem 4.5. *In the above setting, let $B \subset G_p$ be bi-K_p-invariant and of finite non-zero volume and denote by $f_B = \frac{1}{m_p(B)}\chi_B$. Choose $\delta > 0$. Then*

$$\left|\left|\pi_{p,\ell}(f_B)\right|\right|_{\mathrm{op}} \ll_\delta m_p(B)^{-\frac{1}{q_{p,\ell}(\mathrm{G})}+\delta}.$$

In view of Theorem 3.16, this is the optimal rate for the mean ergodic theorem provided that $q_{p,\ell}(\mathrm{G}) = q(\pi_{p,\ell})$. The main reference for this subchapter are chapters 3 and 4 of [GGN13]. We denote in the following by $\widehat{G_p}$ the unitary dual of G_p, i.e. all the unitary irreducible representations of G_p. Moreover, we denote by $\widehat{G_p^1}$ the subspace of spherical irreducible representations.

For the spherical function η_τ associated to the spherical representation $(\tau, \mathscr{H})$ of G_p, we denote for $f \in L^1(G_p)$ by

$$f(\eta_\tau) = \int f(g)\eta_\tau(g)\, dm_p(g).$$

Proposition 4.6. *Consider a unitary representation $(\pi, \mathscr{H})$ of G_p and $f \in L^1(G_p)$ a bi-K_p-invariant function. Then*

$$||\pi(f)|| \leq \sup\{\sqrt{|f^*(\eta_\tau)f(\eta_\tau)|} \,:\, \tau \in \widehat{G_S^1} \text{ and } \tau \prec \pi\}.$$

Proof. The main claim of this proposition is that if f is symmetric, i.e if $f^* = f$ so that $\pi(f)$ is a symmetric operator, then we have that

$$||\pi(f)|| \leq \{|f(\eta_\tau)| \,:\, \tau \in \widehat{G_p^1} \text{ and } \tau \prec \pi\}.$$

Assuming this claim for a moment, we note that for a general bi-K_p-invariant f, the C^*-property of the algebra of bounded operators on a Hilbert space yields

$$||\pi(f)||^2 = ||\pi(f)^*\pi(f)|| = ||\pi(f^* * f)||.$$

As $f^* * f$ is symmetric, it follows if we assume the claim that

$$||\pi(f)|| = \sqrt{||\pi(f^* * f)||} \leq \sup\{\sqrt{|(f^* * f)(\eta_\tau)|} \,:\, \tau \in \widehat{G_p^1} \text{ and } \tau \prec \pi\}.$$

Hence the statement of the proposition follows as

$$\begin{aligned}
(f^* * f)(\eta_\tau) &= \int_{G_p} (f^* * f)(h)\eta_\tau(h)\, dm_p(h) \\
&= \int_{G_p}\int_{G_p} f^*(g)f(g^{-1}h)\eta_\tau(h)\, dm_p(h)dm_p(g) \\
&= \int_{G_p}\int_{G_p} f^*(g)f(h)\eta_\tau(gh)\, dm_p(h)dm_p(g) \\
&= \int_{G_p}\int_{G_p}\int_{K_p} f^*(gk)f(h)\eta_\tau(gkh)\, dm_p(h)dm_p(g)dm_{K_p}(k) \\
&= \int_{G_p}\int_{G_p} f^*(g)f(h)\int_{K_p} \eta_\tau(gkh)dm_{K_p}(k)\; dm_p(h)dm_p(g) \\
&= \int_{G_p}\int_{G_p} f^*(g)f(h)\eta_\tau(g)\eta_\tau(h)\, dm_p(h)dm_p(g) \\
&= f^*(\eta_\tau)f(\eta_\tau),
\end{aligned}$$

where we used bi-K_p-invariance of f and the equivalent characterization of spherical functions of Proposition 2.41.

In order to prove the claim, let f be bi-K_p-invariant and symmetric. Recall that by Lemma 2.10,

$$||\pi(f)|| \leq \sup\{||\tau(f)|| \,:\, \tau \in \widehat{G_p} \text{ and } \tau \prec \pi\}.$$

We show that if the irreducible unitary representation $\tau \prec \pi$ is not spherical, then $||\tau(f)|| = 0$ and if it is, then $||\tau(f)|| \leq |f(\eta_\tau)|$. This then implies the claim.

So consider $(\tau, \mathscr{H}_\tau)$ an irreducible unitary representation of G_p. Then we observe

$$\tau(f)\mathscr{H}_\tau \subset \mathscr{H}_\tau^{K_p},$$

as by bi-K_p-invariance we have for $v \in \mathscr{H}_\tau$ and $k_p \in K_p$ that

$$\tau_{k_p}\tau(f)v = \int_{G_p} f(g)\tau_{k_p g} v \, dm_p(g) = \int_{G_p} f(k_p^{-1}g)\tau_g v \, dm_p(g) = \tau(f)v.$$

Moreover, as $\tau(f)$ is symmetric it follows that $\tau(f)(\mathscr{H}_\tau^{K_p})^\perp \subset (\mathscr{H}_\tau^{K_p})^\perp$ and hence $\tau(f)(\mathscr{H}_\tau^{K_p})^\perp = \{0\}$. If there are no K_p-invariant elements, this show then that $\tau(f) = 0$. Thus we can assume that $(\tau, \mathscr{H}_\tau)$ is spherical. In this case we can decompose $w \in \mathscr{H}_\tau$ as $w = w_p + w_p^\perp$ for $w_p \in \mathscr{H}_\tau^{K_p}$ and $w_p^\perp \in (\mathscr{H}_\tau^{K_p})^\perp$. Then as $\tau(f)$ is self-adjoint,

$$\begin{aligned}
||\tau(f)|| &= \sup_{||w||=1} |\langle \tau(f)w, w\rangle| \\
&= \sup_{||w||=1} |\langle \tau(f)w_p + \tau(f)w_p^\perp, w_p + w_p^\perp\rangle| \\
&= \sup_{w \in \mathscr{H}_\tau^{K_p}, ||w||=1} |\langle \tau(f)w, w\rangle| \\
&= \sup_{w \in \mathscr{H}_\tau^{K_p}, ||w||=1} \left| \int_{G_p} f(g)\langle \tau(g)w, w\rangle \, dm_p(g) \right| \\
&= |f(\eta_\tau)|,
\end{aligned}$$

where we used in the third line that $\tau(f)(\mathscr{H}_\tau^{K_p})^\perp = \{0\}$. Moreover in the last line, we used that $\dim \mathscr{H}_\tau^{K_p} = 1$ and hence for any $w \in \mathscr{H}_\tau^{K_p}$ with $||w|| = 1$ it holds that

$$\eta_\tau(g) = \langle \tau(g)w, w\rangle.$$

□

Proposition 4.7. *For all $q > q_{p,\ell}(\mathrm{G})$,*

$$\sup\{||\eta_\tau||_q \,:\, \tau \in \widehat{G_p^1} \textit{ and } \tau \prec \pi_{p,\ell}\} < \infty.$$

Proof. We refer to chapter 3.3 of [GGN13]. The proof requires the classification of spherical functions. □

We are now in a suitable position to prove Theorem 4.5.

Proof. (of Theorem 4.5) We aim to show

$$||\pi_{p,\ell}(f_B)|| \ll_\delta m_p(B)^{-\frac{1}{q_{p,\ell}(\mathrm{G})}+\delta}.$$

Let τ be a spherical representation weakly contained in $\pi_{p,\ell}$. By applying the Hölder inequality for $q > q_{p,\ell}(\mathrm{G})$ for the tuple $(q, \frac{q-1}{q})$ we conclude

$$\begin{aligned}|f_B(\eta_\tau)| = ||f_B\eta_\tau||_1 &= \left|\frac{1}{m_p(B)}\int_{G_p}\chi_B\eta_\tau\, dm_p\right|\\ &\le \frac{1}{m_p(B)}m_p(B)^{\frac{q-1}{q}}||\eta_\tau||_q\\ &\le m_p(B)^{-\frac{1}{q}}||\eta_\tau||_q.\end{aligned}$$

Note that the same estimate holds for $f_B^*(\eta_\tau)$. Thus the claim follows by Proposition 4.6 and Proposition 4.7. □

4.3 The Effective Birkhoff Ergodic Theorem for Semisimple Lie Groups

In this subchapter we apply the results obtained in the last chapter to a concrete setting in order to obtain effective results on Birkhoff's ergodic theorem – following chapter 9 of [EMV09]. We will use Sobolev norms and Sobolev spaces as discussed in appendix A. Consider a semisimple Lie group G arising from an algebraic group over $\mathbb{Q}$ and an arithmetic lattice $\Gamma < G$ so that we have a probability measure μ on G/Γ. We assume that the left regular representation π of G on $L^2_0(G/\Gamma)$ is $(m-1)$-tempered so that there is some d_0 so for all $f, g \in L^2_0(G/\Gamma)$ we have

$$|\langle \pi_g f, g\rangle| \ll \mathcal{S}_{d_0}(f)\mathcal{S}_{d_0}(g)\Xi(g)^{\frac{1}{m-1}}, \tag{4.1}$$

where the constant only depends on d_0. For simplicity we sometimes write $(\pi_g f)(x) = gf(x) = f(g^{-1}x)$.

We choose a unipotent one-parameter subgroup $u : \mathbb{R} \to G$ so that

$$\Xi(u(t)) \ll_\varepsilon (1+|t|)^{-1+\varepsilon}.$$

So in particular we have

$$|\langle \pi_{u(t)} f, g\rangle| \ll (1+|t|)^{-\frac{1}{m}}\mathcal{S}_{d_0}(f)\mathcal{S}_{d_0}(g). \tag{4.2}$$

Next choose $M = 20m$. Any $M = cm$ for large enough c will also be sufficient for our purposes. We first want to estimate the following quantity:

$$D_T(f)(x) = \frac{1}{(T+1)^M - T^M}\int_{T^M}^{T^{M+1}} f(u(-t)x)\, dt - \int_X f\, d\mu.$$

Lemma 4.8. *For any $s > 0$, $T > 0$ and $f \in \mathcal{H}^d_0(X)$ we have that*

$$\mu\left(\{x \in X \,:\, |D_T(f)(x)| \ge s\}\right) \ll s^{-2}T^{-4}\mathcal{S}_{d_0}(f)^2.$$

Proof. We assume without loss of generality that f is real valued. Throughout this proof write $\leftrightarrow$ for the interval $[T^M, (T+1)^M]$ and denote

$$|\leftrightarrow| = \operatorname{length}(\leftrightarrow) = (T+1)^M - T^M,$$

$\square$ for the cube $[T^M, (T+1)^M]^2$ and finally by

$$|\square| = \operatorname{vol}(\square) = ((T+1)^M - T^M)^2.$$

The binomial expansion of $(T+1)^M$ shows that

$$T^{M-1} \ll |\leftrightarrow| \ll T^{M-1} \qquad \text{and} \qquad T^{2M-2} \ll |\square| \ll T^{2M-2}.$$

The lemma follows by a series of elegant calculations. First we note

$$\begin{aligned}\left| \langle u(t)f, f\rangle - \left(\int_X f\,d\mu\right)^2 \right| &= \left\langle u(t)\left(f - \int f\,d\mu\right), f - \int f\,d\mu \right\rangle \\ &\ll (1+|t|)^{-\frac{1}{m}} \mathcal{S}_{d_0}(f)^2.\end{aligned}$$

Second, using Fubini we conclude,

$$\begin{aligned}\int_X |D_T(f)(x)|^2\,d\mu &= \int_X \frac{1}{|\square|}\left(\int_{\leftrightarrow} f(u(-t)x)\,dt\right)^2 \\ &\quad - \frac{2}{|\leftrightarrow|}\int_X f\,d\mu \int_{\leftrightarrow} f(u(-t)x)\,dt + \left(\int_X f\,d\mu\right)^2\,d\mu \\ &= \frac{1}{|\square|}\int_{\square} \langle u(t)f, u(s)f\rangle\,dsdt - \left(\int_X f\,d\mu\right)^2 \\ &= \frac{1}{|\square|}\int_{\square} \langle u(t)f, u(s)f\rangle - \left(\int_X f\,d\mu\right)^2\,dsdt \\ &= \frac{1}{|\square|}\int_{\square} \langle u(t-s)f, f\rangle - \left(\int_X f\,d\mu\right)^2\,dsdt \\ &\ll \frac{1}{|\square|}\int_{\square} (1+|t-s|)^{-\frac{1}{m}} \mathcal{S}_{d_0}(f)^2\,dsdt\end{aligned}$$

Finally we split $\square$ into $|t-s| \le T^{\frac{M}{2}}$ and $|t-s| > T^{\frac{M}{2}}$. By observing that $\operatorname{vol}(\square \cap \{|t-s| \le T^{\frac{M}{2}}\}) \ll T^{M-1+\frac{M}{2}}$ and on $|t-s| > T^{\frac{M}{2}}$ we have $(1+|t-s|)^{-\frac{1}{m}} \ll T^{-\frac{M}{2m}}$, it follows

$$\begin{aligned}\int_X |D_T(f)(x)|^2\,d\mu &\ll \frac{1}{|\square|}\int_{\square} (1+|t-s|)^{-\frac{1}{m}} \mathcal{S}_{d_0}(f)^2\,dsdt \\ &\ll \frac{1}{|\square|}\int_{|t-s| \le T^{\frac{M}{2}}} (1+|t-s|)^{-\frac{1}{m}} \mathcal{S}_{d_0}(f)^2\,dsdt \\ &\quad + \frac{1}{|\square|}\int_{|t-s| > T^{\frac{M}{2}}} (1+|t-s|)^{-\frac{1}{m}} \mathcal{S}_{d_0}(f)^2\,dsdt \\ &\ll \frac{\mathcal{S}_{d_0}(f)^2}{T^{2M-2}}\left(T^{M-1+\frac{M}{2}} + T^{2M-2-\frac{M}{2m}}\right) \\ &\ll T^{-4} S_{d_0}(f)^2.\end{aligned}$$

This allows us to conclude

$$\begin{aligned}\mu\left(\{x \in X \,:\, |D_T(f)(x)| \geq s\}\right) &= \frac{1}{s^2}\int_{\{x\,:\,|D_T(f)(x)|\geq s\}} s^2\, d\mu \\ &\leq \frac{1}{s^2}\int_X |D_T(f)(x)|^2\, d\mu \\ &\ll s^{-2}T^{-4}\mathcal{S}_{d_0}(f)^2.\end{aligned}$$

□

To formulate the next theorem, which is the main theorem of this subchapter, we use the following definition.

Definition 4.9. A point $x \in X$ is called T_0**-generic** with respect to the Sobolev norm $\mathcal{S}_d$ if for all $n \geq T_0$ and $f \in \mathcal{H}_0^d(X)$ we have that

$$|D_n(f)(x)| \leq n^{-1}\mathcal{S}_d(f)).$$

Theorem 4.10. *(Effective Birkhoff Ergodic Theorem) Let d be a sufficiently large integer. Then the set of points that are not T_0-generic with respect to the Sobolev norm $\mathcal{S}_d$ is $\ll T_0^{-1}$.*

Proof. We choose $d > d' > d_0$ sufficiently large so that

$$\mathrm{tr}(\mathcal{S}_{d'}, \mathcal{S}_d) \quad \text{and} \quad \mathrm{tr}(\mathcal{S}_{d_0}, \mathcal{S}_{d'})$$

are finite. Recall that by Proposition A.19 there exists a trace class and hence compact operator $\mathrm{Op}_{\mathcal{S}_{d'},\mathcal{S}_d}$ so that

$$\langle f, g\rangle_{\mathcal{S}_{d'}} = \langle \mathrm{Op}_{\mathcal{S}_{d'},\mathcal{S}_{d_0}} f, g\rangle_{\mathcal{S}_d}$$

for all functions $f, g \in \mathcal{H}_0^d(X) \subset \mathcal{H}_0^{d'}(X)$. We note that $\mathrm{Op}_{\mathcal{S}_{d'},\mathcal{S}_d}$ is self-adjoint as it is positive definite and hence by the spectral theorem we can choose an orthonormal basis $f_1, f_2, \ldots$ of $\mathcal{H}_0^d(X)$ consisting of eigenvectors of $\mathrm{Op}_{\mathcal{S}_{d'},\mathcal{S}_d}$. Thus $f_1, f_2, \ldots$ is an orthonormal basis for $\mathcal{S}_d$ and orthogonal for $\mathcal{S}_{d'}$, so that

$$\mathrm{tr}(\mathcal{S}_{d'}, \mathcal{S}_d) = \sum_{n\geq 1} \mathcal{S}_{d'}(f_n)^2 < \infty \quad \text{and} \quad \mathrm{tr}(\mathcal{S}_{d_0}, \mathcal{S}_{d'}) = \sum_{n\geq 1} \frac{\mathcal{S}_{d_0}(f_n)^2}{\mathcal{S}_{d'}(f_n)^2} < \infty.$$

We apply Lemma 4.8 to conclude that the set

$$E = \bigcup_{n\geq T_0, k\geq 1} \{x \in X \,:\, n|D_n(f_k)(x)| \geq c\mathcal{S}_{d'}(f_k)\}$$

for some $c > 0$ to be chosen later satisfies

$$\mu\left(E\right) \ll \sum_{n\geq T_0, k\geq 1} \frac{n^2}{c^2 n^4} \frac{\mathcal{S}_{d_0}(f_k)^2}{\mathcal{S}_{d'}(f_k)^2} \ll c^{-2}T_0^{-1} \ll T_0^{-1}.$$

We now want to show that if $x \in X$ is not T_0-generic then $x \in E$, which then implies the statement of the theorem. To see this assume $x \notin E$ and let

$f = \sum_{k \geq 1} a_k f_k$. Then we have by using the Cauchy-Schwarz inequality for $n \geq T_0$,

$$\begin{aligned} n|D_n(f)(x)| \leq c\mathcal{S}_{d'}(f) &= c\sum_{k\geq 1} |a_k|\mathcal{S}_{d'}(f_k) \\ &\leq c\left(\sum_{k\geq 1} \mathcal{S}_{d'}(f_k)^2\right)^{\frac{1}{2}} \left(\sum_{k\geq 1} |a_k|^2\right)^{\frac{1}{2}} \leq \mathcal{S}_d(f), \end{aligned}$$

using the constant c so that $c\left(\sum_{k\geq 1} \mathcal{S}_{d'}(f_k)^2\right)^{\frac{1}{2}} \leq 1$. So x is T_0-generic and hence the claim follows. $\square$

5 Diophantine Approximation

This chapter is the main part of this thesis. We first prove results on Diophantine approximation by applying an effective mean ergodic theorem (Theorem 4.5). Then we discuss discrepancy bounds for Diophantine approximation. Finally we explain how results established by the circle method imply certain discrepancy bounds and then deduce property (τ) for $\mathbb{Q}$-forms of SL_2. The main references for this subchapter are [GGN13] and [GGN].

5.1 Notation and Lower Bound

Throughout this subchapter we consider $\mathrm{G} \subset \mathrm{GL}_n$ a simply connected, almost simple algebraic group over $\mathbb{Q}$ and the homogeneous space

$$X_{p,\ell} = (\mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p))/\Gamma_{p,\ell}.$$

Write as usual $G_\infty = \mathrm{G}(\mathbb{R})$ and $G_p = \mathrm{G}(\mathbb{Q}_p)$. Furthermore, denote by $m_{X_{p,\ell}}$ the Haar probability measure on X_p. We consider on G_∞ the norm

$$||x||_\infty = \max_{1\leq i,j\leq n} |x_{ij}|$$

and on G_p the norm

$$||x||_p = \max_{1\leq i,j\leq n} |x_{ij}|_p.$$

The first aim of this chapter is to prove the following theorem.

Theorem 5.1. *Let $\mathrm{G} \subset \mathrm{GL}_n$ be a simply connected almost simple algebraic group over $\mathbb{Q}$ and assume that G is isotropic over $\mathbb{Q}_p$. For almost all $x \in \mathrm{G}(\mathbb{R})$ the following property holds: For all $\delta > 0$ there exists $\varepsilon_0(x, \delta)$ so that for all $0 < \varepsilon < \varepsilon_0(x, \delta)$ there exists some $z \in \Gamma_{p,\ell}$ so that*

$$||x - z||_\infty \leq \varepsilon \qquad \text{and} \qquad ||z||_p \leq \varepsilon^{-(\theta_{G,p,\ell}+\delta)},$$

where $\theta_{p,\ell,G}$ is a positive constant only depending on p, ℓ and G.

The proof of Theorem 5.1 is deferred to the next subchapter. In this subchapter we are concerned with discussing a lower bound for Diophantine approximation.

Let $Y \subset G_\infty$ be a bounded subset. For $\varepsilon > 0$, we denote by $D(Y, \varepsilon)$ the smallest number of ε-balls with respect to $||\cdot||_\infty$ needed to cover Y, which is a finite number as Y is bounded. We then define the **Minkowski dimension** of Y as

$$d_{\mathrm{M}}(Y) = \liminf_{\varepsilon\to 0^+} \frac{\log(D(Y,\varepsilon))}{\log(\varepsilon^{-1})}.$$

Lemma 5.2. *For any bounded measurable subset $Y \subset G_\infty$ of positive measure,*

$$d_{\mathrm{M}}(Y) = \dim_{\mathbb{R}}(G_\infty) = \dim_{\mathbb{Q}}(\mathrm{G}).$$

Proof. It suffices to consider bounded measurable subsets $Y \subset \mathbb{R}^d$ of positive measure and the Lebesgue measure. We note that $d_{\mathrm{M}}(Y)$ is well defined as Y is bounded and hence $D(Y, \varepsilon)$ is finite for any $\varepsilon > 0$. Observe that

$$\frac{\mathrm{vol}(Y)}{\mathrm{vol}(B_\varepsilon(0))} - 1 \leq D(Y, \varepsilon).$$

As

$$\frac{\mathrm{vol}(Y)}{\mathrm{vol}(B_\varepsilon(0))} = c_{d,Y}\varepsilon^{-d}$$

for some constant $c_{d,Y}$ depending only on Y and d, it follows that $d \leq d_{\mathrm{M}}(Y)$. To show $\leq$, we note that as Y is bounded there is some $Y \subset B_c(0)$ for some $c > 0$. Observe $d_{\mathrm{M}}(B_c(0)) \leq d$ as $B_c(0)$ can be covered by $(\frac{2c}{\varepsilon})^d$-many ε-balls, which implies the claim as $d_{\mathrm{M}}(Y) \leq d_{\mathrm{M}}(B_c(0))$. $\square$

In the following we again consider a bounded subset $U \subset G_\infty$. We define

$$a_{p,\ell}(U) = \sup_{Y \subset U} \limsup_{h \to \infty} \frac{\log(A_{p,\ell}(Y,h))}{\log(h)},$$

where the supremum is taken over all open subsets $Y \subset U$ and where we set

$$A_{p,\ell}(Y,h) := \Big| \{z \in \Gamma_{p,\ell} \cap Y \,:\, ||z||_p \leq h\} \Big|.$$

We furthermore define

$$a_{p,\ell}(\mathrm{G}) = \sup_{U \subset G_\infty} a_{p,\ell}(U),$$

where the supremum is taken over all bounded sets of G_∞. Finally we denote for $x \in G_\infty$ and $\varepsilon > 0$,

$$\omega_p(x,\varepsilon) = \min\{||z||_p \,:\, z \in \Gamma_{p,\ell} \text{ and } ||x - z||_\infty < \varepsilon\}$$

and set for a subset $Y \subset G_\infty$,

$$\omega_{p,\ell}(Y,\varepsilon) = \sup_{y \in Y} \omega_p(y,\varepsilon).$$

Lemma 5.3. *Let $Y \subset G_\infty$ be a bounded subset and $Y \subsetneq U$ be open so that $B_{\varepsilon_0}(Y) \subset U$. Then for all $0 < \varepsilon < \varepsilon_0$,*

$$D(Y,\varepsilon) \leq A_{p,\ell}(U, \omega_{p,\ell}(Y,\varepsilon)).$$

Proof. Fix $0 < \varepsilon < \varepsilon_0$. If $A_{p,\ell}(U, \omega_{p,\ell}(Y,\varepsilon))$ is infinite, there is nothing to show. So assume that $A_{p,\ell}(U, \omega_{p,\ell}(Y,\varepsilon))$ is finite and that

$$\{z \in \Gamma_{p,\ell} \cap U \,:\, ||z||_p \leq \omega_{p,\ell}(Y,\varepsilon)\} = \{z_1, \ldots, z_n\}.$$

We claim that $Y \subset \bigcup_{i=1}^n B_\varepsilon(z_i)$, which implies the claim. Assume for a contradiction that this is not the case. Then there is some $y \in Y$ so that $y \notin \bigcup_{i=1}^n B_\varepsilon(z_i)$. By definition of $\omega_p(y,\varepsilon)$, there is some $z^* \in \Gamma_{p,\ell}$ so that $||y - z^*||_\infty \leq \varepsilon$ and $||z^*||_p = \omega_{p,\ell}(x,\varepsilon) \leq \omega_{p,\ell}(Y,\varepsilon)$. We note that $z^* \notin U$ as otherwise, since $z \in \Gamma_{p,\ell}$ it follows that $z^* = z_i$ for some i. But then $y \in B_\varepsilon(z_i)$, contradicting the assumption on y. So we conclude that $z^* \notin U \supset B_\varepsilon(Y)$, contradicting that $||y - z||_\infty < \varepsilon$. $\square$

Putting all this together we derive a lower bound for Diophantine approximation.

Proposition 5.4. *Let $Y \subset G_\infty$ be a subset of positive measure so that $Y \not\subset \Gamma_{p,\ell}$. For every $\delta > 0$, there is some $\varepsilon_0(\delta)$ so that for all $0 < \varepsilon < \varepsilon_0(\delta)$,*

$$\varepsilon^{-\frac{\dim_{\mathbb{Q}}(\mathrm{G})}{a_{p,\ell}(\mathrm{G})}+\delta} \leq \omega_{p,\ell}(Y, \varepsilon).$$

Proof. As $Y \not\subset \Gamma_{p,\ell}$, it follows that $\omega_{p,\ell}(Y, \varepsilon) \to \infty$ as $\varepsilon \to 0^+$. Thus we can choose for each $\delta_1, \delta_2 > 0$ some close enough open subset $U \supset Y$ so that for all $0 < \varepsilon < \varepsilon_0(U, \delta_1, \delta_2)$, using the last two lemmas, we have that

$$\varepsilon^{-\dim(G)+\delta_1} \leq D(Y, \varepsilon) \leq A_{p,\ell}(U, \omega_{p,\ell}(Y, \varepsilon)) \leq \omega_{p,\ell}(Y, \varepsilon)^{a_{p,\ell}(\mathrm{G})+\delta_2},$$

which implies the claim. □

5.2 Diophantine Approximation for Groups at almost every point

In this subchapter we use exactly the same notation as in the last subchapter. We set

$$\theta_{G,p,\ell} := \frac{\dim_{\mathbb{Q}}(\mathrm{G}) q_{p,\ell}(\mathrm{G})}{2a_{p,\ell}(\mathrm{G})}.$$

The main aim of this subchapter is to prove Theorem 5.1, which we restate here for convenience by using the notation introduced last subchapter.

Theorem 5.5. *Let $\mathrm{G} \subset \mathrm{GL}_n$ be a simply connected, $\mathbb{Q}_p$-isotropic almost simple algebraic group over $\mathbb{Q}$. For almost all $x \in \mathrm{G}(\mathbb{R})$ the following property holds: For all $\delta > 0$ there exists $\varepsilon_0(x, \delta)$ so that for all $0 < \varepsilon < \varepsilon_0(x, \delta)$,*

$$\omega_{p,\ell}(x, \varepsilon) \leq \varepsilon^{-(\theta_{G,p,\ell}+\delta)}.$$

The main ingredients for the proof Theorem 5.5 are the mean ergodic theorem for the p-adic extension (Theorem 4.5) and the so called duality principle, which we discuss next. To simplify the notation we write for the remainder of this subchapter $X = X_{p,\ell}$ and $\Gamma = \Gamma_{p,\ell}$.

Fix a bounded subset $\Omega \subset G_\infty$. We denote by $c_\Omega \geq 1$ a constant so that

$$||x \cdot g||_\infty \leq c_\Omega \cdot ||g||_\infty \qquad \text{and} \qquad ||x^{-1} \cdot g||_\infty \leq c_\Omega \cdot ||g||_\infty$$

for all $g \in G_\infty$ and $x \in \Omega$. In fact we can take $c_\Omega = n \cdot \sup_{x\in\Omega} |x_{ij}|$. For $\delta > 0$ we denote by $B_\delta(e) = \{g \in G_\infty : ||g - e||_\infty \leq \delta\}$. Further, for $\varepsilon > 0$ we set

$$\Phi_\varepsilon = B_{\frac{\varepsilon}{c_\Omega}}(e) \times \mathrm{G}(\mathbb{Z}_p) \subset G_\infty \times G_p$$

and $\Phi_{\varepsilon,\Gamma} = \Phi_\varepsilon \Gamma \subset X$. Finally for $h > 0$ we denote $B_h = \mathrm{G}(\mathbb{Z}_p)\{g \in G_p : ||g - e||_p = ||g||_p \leq h\}\mathrm{G}(\mathbb{Z}_p)$. Now we are ready to state and prove the duality principle.

Proposition 5.6. *If $x \in \Omega$ satisfies $B_h^{-1}x^{-1} \cap \Phi_{\varepsilon,\Gamma} \neq \emptyset$, for $\varepsilon > 0$, where we view $B_h^{-1}x^{-1}$ as projected onto X, then there is $z \in \Gamma$ so that*

$$||x - z||_\infty \leq \varepsilon \qquad \textit{and} \qquad ||z||_p \leq h.$$

Moreover, if $0 < \varepsilon < 1$ then

$$m_X(\Phi_{\varepsilon,\Gamma}) \asymp_\Omega \varepsilon^{\dim_{\mathbb{Q}}(\mathrm{G})}.$$

Proof. Assume that $x \in \Omega$ satisfies the above property. Then there is $z \in \Gamma$ and $b \in B_h$ so that

$$(x^{-1}z, b^{-1}z) \in \Phi_\varepsilon = B_{\frac{\varepsilon}{c_\Omega}}(e) \times \mathrm{G}(\mathbb{Z}_p).$$

So we have that $z \in b\mathrm{G}(\mathbb{Z}_p)$ and hence $||z||_p \leq ||b||_p \leq h$. Furthermore we have that $||x^{-1}z - e||_\infty \leq \frac{\varepsilon}{c_\Omega}$ and hence

$$||x - z||_\infty = ||x(e - x^{-1}z)||_\infty \leq c_\Omega ||e - zx^{-1}||_\infty \leq \varepsilon.$$

To prove the second claim, we note that if we have some $\gamma \in \Gamma$ with

$$\Phi_\varepsilon \gamma \cap \Phi_\varepsilon = \emptyset$$

then there is $g_1, g_2 \in \mathrm{G}(\mathbb{Z}_p)$ so that $g_1\gamma = g_2$ and so $\gamma = g_1^{-1}g_2 \in \mathrm{G}(\mathbb{Z}_p)$. Using $\gamma \in \Gamma$, it follows that $\gamma \in \mathrm{G}(\mathbb{Z})$. As $\mathrm{G}(\mathbb{Z}) < \mathrm{G}(\mathbb{R})$ is discrete, there is some $\varepsilon_0 > 0$ so that $\gamma \notin B_{\varepsilon_0}(e)$ for all $\gamma \in \mathrm{G}(\mathbb{Z})\backslash\{e\}$. Thus we conclude that if $\frac{\varepsilon}{c_\Omega} \leq \varepsilon_0$ then $\Phi_\varepsilon\gamma \cap \Phi_\varepsilon = \emptyset$ for all $\gamma \in \Gamma\backslash\{e\}$ and hence we have that

$$m_X(\Phi_{\varepsilon,\Gamma}) \asymp m_{G_\infty \times G_p}(\Phi_\varepsilon) \asymp \left(\frac{\varepsilon}{c_\Omega}\right)^{\dim_{\mathbb{Q}}(\mathrm{G})} \asymp_\Omega \varepsilon^{\dim_{\mathbb{Q}}(\mathrm{G})}.$$

If on the other hand $\varepsilon_0 < \frac{\varepsilon}{c_\Omega} < 1$ then we set $\varepsilon' = \varepsilon\varepsilon_0 < \varepsilon_0$ and hence

$$m_X(\Phi_{\varepsilon,\Gamma}) \asymp m_X(\Phi^\Omega_{\varepsilon'}) \asymp (\varepsilon\varepsilon_0)^{\dim_{\mathbb{Q}}(\mathrm{G})} \asymp \varepsilon^{\dim_{\mathbb{Q}}(\mathrm{G})}.$$

□

We observe that we can also prove a converse to the above proposition. For this denote for $\varepsilon > 0$ the set

$$\Psi_\varepsilon = B_{c_\omega \varepsilon}(e) \times \mathrm{G}(\mathbb{Z}_p) \subset G_\infty \times G_p$$

and

$$\Psi_{\varepsilon,\Gamma} = \Psi_\varepsilon \Gamma \subset X.$$

Proposition 5.7. *If $0 < \varepsilon < 1$ then*

$$m_X(\Psi^\Omega_\varepsilon) \asymp_\Omega \varepsilon^{\dim_{\mathbb{Q}}(\mathrm{G})}.$$

Moreover, if for $x \in \Omega$ there is some $z \in \Gamma$ so that

$$||z||_p \leq h \qquad \textit{and} \qquad ||x - z||_p \leq \varepsilon,$$

then $B_h^{-1}x^{-1} \cap \Psi^\Omega_\varepsilon \neq \emptyset$.

Proof. The first statement is proved completely analogously to Proposition 5.6. For the second statement, we first claim that

$$(zx^{-1}, e) \in B_{c_\Omega \varepsilon}(e) \times \mathrm{G}(\mathbb{Z}_p).$$

This follows as clearly $e \in \mathrm{G}(\mathbb{Z}_p)$ and as

$$||e - x^{-1}z||_\infty = ||x^{-1}(x-e)||_\infty \leq c_\Omega ||e-z||_\infty \leq c_\Omega \cdot \varepsilon.$$

So it follows as $(x^{-1}z, e) = (x^{-1}, z^{-1})z$ that $(x^{-1}, z^{-1})\Gamma \in \Psi_\varepsilon$ and also clearly as $||z||_p \leq h$ that $(x^{-1}, z^{-1}) \in B_h^{-1}x^{-1}$. □

We next investigate the volume growth of B_h.

Lemma 5.8. *Let $\Omega \subset G_\infty$ be bounded. Then there exist constants $c > 0$ and $h_0 > 0$ so that for every $h \geq h_0$*

$$A_{p,\ell}(\Omega, h) \ll_\Omega m_p(B_{ch}).$$

In particular, for every $\delta > 0$ and $h \geq h_0(p, \delta)$

$$m_p(B_{ch}) \gg_\delta h^{a_{p,\ell}(\mathrm{G})-\delta}.$$

Proof. We consider the set

$$\mathcal{A}_{p,\ell}(\Omega, h) = \{\gamma \in \Gamma \cap (\Omega \times G_p) \,:\, ||\gamma||_p \leq h\}.$$

As Γ is a discrete subgroup of $G_{\infty,p}$ it follows that there is some open bounded neighborhood $\mathcal{O}$ of the identity so that $\mathcal{O}\gamma \cap \mathcal{O} = \emptyset$ for all $\gamma \in \Gamma$. Thus we have that

$$A_{p,\ell}(\Omega, h) = |\mathcal{A}_{p,\ell}(\Omega, h)| \leq \frac{m_{G_{\infty,p}}(\mathcal{O}\mathcal{A}_{p,\ell}(\Omega, h))}{m_{G_{p,\infty}}(\mathcal{O})}.$$

Furthermore we note that there is $c > 0$ and bounded $\Omega' \supset \Omega$ so that

$$\mathcal{O}\mathcal{A}_{p,\ell}(\Omega, h) \subset \mathcal{O}(\Omega \times B_h) \subset \Omega' \times B_{ch}$$

and hence the claim follows as $\mathcal{O}$ and Ω' are bounded. □

Finally, the proof of Theorem 5.5 uses the Borel-Cantelli lemma, which we recall for completeness.

Lemma 5.9. *(Borel-Cantelli) Let $(X, \mathcal{B}_X, \mu)$ be a probability space and let $A_n \in \mathcal{B}_X$ be a sequence of measurable subsets so that*

$$\sum_{n \geq 1} \mu(A_n) < \infty.$$

Then the measurable set

$$\limsup A_n = \bigcap_{n\geq 1} \bigcup_{m \geq n} A_n = \{\omega \in X \,:\, \omega \textit{ is contained in infinitely many } A_n\}$$

has zero measure.

Proof. We use dominated convergence to see that

$$\int \sum_{n\geq 1} \chi_{A_n}\, d\mu = \sum_{n\geq 1} \mu(A_n) < \infty.$$

Thus it follows that

$$\sum_{n\geq 1} \chi_{A_n} < \infty$$

almost everywhere, which implies the claim. □

Proof. (of Theorem 5.5) We fix throughout this proof some bounded $\Omega \subset G_\infty$. As $G_\infty \subset \mathrm{GL}_n(\mathbb{R})$ is σ-compact, it suffices to prove the statement for almost all points of Ω. Furthermore, the statement is easily implied if we have proved the statement for a sequence of $\varepsilon_n \to 0$. Thus we set $\varepsilon_n = 2^{-n}$. To further simplify the notation, we write throughout this proof

$$\pi = \pi_{p,\ell}, \qquad q = q_{p,\ell}(\mathrm{G}) \qquad a = a_{p,\ell}(\mathrm{G}).$$

We denote by $f_{B_h} = \frac{\chi_{B_h}}{m_p(B_h)}$. By Theorem 4.5, as B_h is bi-$\mathrm{G}(\mathbb{Z}_p)$-invariant,[2] we have for every $\delta' > 0$

$$||\pi(f_{B_h})||_{\mathrm{op}} \ll_{\delta'} m_p(B_h)^{-\frac{1}{q}+\delta'}.$$

Thus using Lemma 5.8 it follows that there is $h_0(p,\delta')$ so that for all $h \geq h_0(p,\delta')$,

$$||\pi(f_{B_h})||_{\mathrm{op}} \ll_{\delta'} h^{-\frac{a}{q}+\delta'}. \tag{5.1}$$

We set $h_{\varepsilon_n} = \varepsilon_n^{-(\theta_{\mathrm{G},p,\ell}+\delta)}$ and

$$X_n = \{x \in X \,:\, B_{h_{\varepsilon_n}}^{-1} x \cap \Phi_{\varepsilon_n} = \emptyset\}.$$

We aim at showing that $\limsup X_n$ has measure zero. By the Borel-Cantelli lemma, it suffices to show that

$$\sum_{n\geq 1} m_X(X_n) < \infty.$$

So we need to estimate the measure of the sets X_n. By (5.1), we have that for $h_{\varepsilon_n} \geq h_0(p,\delta')$,

$$\begin{aligned}
&\int_X \left|\pi(f_{B^{-1}_{h_{\varepsilon_n}}})\chi_{\Phi_{\varepsilon_n}} - m_X(\Phi_{\varepsilon_n})\cdot 1_X\right|^2 dm_X \\
&= \left|\left|\pi(f_{B^{-1}_{h_{\varepsilon_n}}})\chi_{\Phi_{\varepsilon_n}} - m_X(\Phi_{\varepsilon_n})\cdot 1_X\right|\right|_2^2 \\
&\leq \left|\left|\pi(f_{B^{-1}_{h_{\varepsilon_n}}})\right|\right|_{\mathrm{op}}^2 \cdot ||\chi_{\Phi_{\varepsilon_n}}||_2^2 \\
&\ll_{\delta'} h_{\varepsilon_n}^{-\frac{2a}{q_{p,\ell}(\mathrm{G})}+\delta'} m_X(\Phi_{\varepsilon_n}).
\end{aligned}$$

[2]We assume here that $K_p = \mathrm{G}(\mathbb{Z}_p)$. It is straightforward to circumvent this issue if we only have $K_p \supset \mathrm{G}(\mathbb{Z}_p)$ by simply considering a bi-K_p-invariant norm.

If $x \in X_n$, then we have that

$$\pi(f_{B_{h_{\varepsilon_n}}^{-1}})\chi_{\Phi_{\varepsilon_n}}(x) = 0$$

and hence it follows that

$$\begin{aligned} m_X(X_n) m_X(\Phi_{\varepsilon_n})^2 &\ll \int_X \left| \pi(f_{B_{h_{\varepsilon_n}}^{-1}})\chi_{\Phi_{\varepsilon_n}} - m_X(\Phi_{\varepsilon_n}) \cdot 1_X \right|^2 dm_X \\ &\ll_{\delta'} h_{\varepsilon_n}^{-\frac{2a}{q}+\delta'} m_X(\Phi_{\varepsilon_n}). \end{aligned}$$

Thus it follows that

$$m_X(X_n) \ll_{\delta'} h_{\varepsilon_n}^{-\frac{2a}{q}+\delta'} m_X(\Phi_{\varepsilon_n})^{-1}.$$

Using Proposition 5.6 and the definition of h_{ε_n} we have that

$$h_{\varepsilon_n}^{-\frac{2a}{q}+\delta'} m_X(\Phi_{\varepsilon_n})^{-1} \ll \varepsilon_n^{\theta_{\delta,\delta'}}$$

for

$$\begin{aligned} \theta_{\delta,\delta'} &= -(\theta_{G,p,\ell} + \delta)(-\tfrac{2a}{q} + \delta') - \dim_{\mathbb{Q}}(\mathrm{G}) \\ &= (\tfrac{\dim_{\mathbb{Q}}(\mathrm{G})q}{2a} + \delta)(\tfrac{2a}{q} - \delta') - \dim_{\mathbb{Q}}(\mathrm{G}) \\ &= \delta \tfrac{2a}{q} - \delta'(\tfrac{\dim_{\mathbb{Q}}(\mathrm{G})q}{2a} + \delta). \end{aligned}$$

So we choose δ' small enough so that $\theta_{\delta,\delta'} > 0$. Then it follows that

$$\begin{aligned} \sum_{n \geq 1} m_X(X_n) &= \sum_{h_{\varepsilon_n} < h_0(p,\delta')} m_X(X_n) + \sum_{h_{\varepsilon_n} \geq h_0(p,\delta')} m_X(X_n) \\ &\ll_{\delta'} \sum_{h_{\varepsilon_n} < h_0(p,\delta')} m_X(X_n) + \sum_{h_{\varepsilon_n} \geq h_0(p,\delta')} \varepsilon_n^{\theta_{\delta,\delta'}} \\ &\ll_{\delta'} \sum_{h_{\varepsilon_n} < h_0(p,\delta')} m_X(X_n) + \sum_{h_{\varepsilon_n} \geq h_0(p,\delta')} 2^{-n\theta_{\delta,\delta'}} \\ &< \infty, \end{aligned}$$

as $\theta_{\delta,\delta'}$ is positive and as $h_{\varepsilon_n} \to \infty$ so that for only finitely many n we have that $h_{\varepsilon_n} < h_0(p, \delta')$. Thus we conclude that the set

$$X_0 = \limsup X_n$$

has zero measure. We now show that this easily implies the claim of the theorem. Denote by $\widetilde{X_0}$ the lift of X_0 onto $G_\infty \times G_p$. Then again $\widetilde{X_0}$ has zero measure as Γ is countable.

We consider the subset

$$\Omega' = \{x \in \Omega \,:\, \exists y \in \mathrm{G}(\mathbb{Z}_p) \text{ such that } (x^{-1}, y) \notin \widetilde{X_0}\}.$$

Note that as

$$(\Omega \backslash \Omega') \times \mathrm{G}(\mathbb{Z}_p) \subset \widetilde{X_0}$$

and as $\mathrm{G}(\mathbb{Z}_p)$ has positive measure in G_p, it follows that $\Omega\backslash\Omega'$ has measure zero. Thus it suffices to show that every $x \in \Omega'$ satisfies the claim of the theorem.

Assume that $x \in \Omega'$. Then there is $y \in \mathrm{G}(\mathbb{Z}_p)$ so that $(x^{-1}, y) \notin \widetilde{X_0}$. So there is some $n_0(x,\delta)$ so that for all $n \geq n_0(x,\delta)$ it holds that $B^{-1}_{h_{\varepsilon_n}}(x^{-1}, y) \cap \Phi_{\varepsilon_n} \neq \emptyset$. As $y \in \mathrm{G}(\mathbb{Z}_p)$, note $B^{-1}_{h_{\varepsilon_n}} y \subset B^{-1}_{h_{\varepsilon_n}}$ and hence it follows that $x^{-1}B^{-1}_{h_{\varepsilon_n}} \cap \Phi_{\varepsilon_n} \neq \emptyset$. Hence by Proposition 5.6, there is $z \in \Gamma$ so that

$$||x - z||_\infty \leq h_{\varepsilon_n} = \varepsilon_n^{-(\theta_{G,p}+\delta)} \qquad \text{and} \qquad ||z||_p \leq \varepsilon_n.$$

This shows the theorem. □

5.3 Diophantine Approximation for Groups at every point

We alter the result of last subchapter to approximate all points in $\mathrm{G}(\mathbb{R})$, however with a weaker exponent. Namely, we need to multiply the exponent from before by 2, so that we set

$$\theta_{G,p,\ell} := \frac{\dim_{\mathbb{Q}}(\mathrm{G}) q_{p,\ell}(\mathrm{G})}{a_{p,\ell}(\mathrm{G})}.$$

We then have in similar vein to the last theorem the following result.

Theorem 5.10. *Let $\mathrm{G} \subset \mathrm{GL}_n$ be a simply connected, $\mathbb{Q}_p$-isotropic almost simple algebraic group over $\mathbb{Q}$. Fix a bounded subset $\Omega \subset \mathrm{G}_\infty$. Then we have for all $\delta > 0$ some $\varepsilon_0(\Omega,\delta)$ so that for all $0 < \varepsilon < \varepsilon_0(\Omega,\delta)$ and all $x \in \Omega$ there is some $z \in \Gamma$ so that*

$$||x - z||_\infty \leq \varepsilon \qquad \textit{and} \qquad ||z||_p \leq \varepsilon^{-(\theta_{G,p,\ell}+\delta)}.$$

The proof is similar to the one of Theorem 5.5. The main difference is that we need an altered version of the duality principle. In this subchapter we consider the constant $c_\Omega \geq 1$ characterized by

$$||x \cdot g||_\infty \leq c_\Omega ||g||_\infty \qquad \text{and} \qquad ||g \cdot x||_\infty \leq c_\Omega ||g||_\infty$$

for all $x \in \Omega$ and $g \in \mathrm{G}_\infty$. We then set for $\varepsilon > 0$

$$\Phi_\varepsilon = B_{\frac{\varepsilon}{(n+1)c_\Omega}}(e) \times \mathrm{G}(\mathbb{Z}_p) \subset G_\infty \times G_p$$

and $\Phi_{\varepsilon,\Gamma} = \Phi_\varepsilon \Gamma \subset X$.

Proposition 5.11. *Fix $0 < \varepsilon < 1$. Let $B \subset G_p$ be a bounded measurable subset. If $x \in \Omega$ satisfies*

$$B^{-1}(\Phi_\varepsilon)^{-1}x^{-1} \cap \Phi_{\varepsilon,\Gamma} \neq \emptyset,$$

then there exists $z \in \Gamma$ so that

$$||x - z||_\infty \leq \varepsilon \qquad \textit{and} \qquad ||z||_p \leq \max_{b\in B} ||b||_p.$$

Moreover, as $0 < \varepsilon < 1$, we have that $m_{G_\infty \times G_p}(\Phi_\varepsilon) \asymp_\Omega \varepsilon^{\dim_{\mathbb{Q}}(\mathrm{G})}$ and for all $x \in \Omega$, $m_{G_\infty \times G_p}(x^{-1}\Phi_\varepsilon) \gg_\Omega \varepsilon^{\dim_{\mathbb{Q}}(\mathrm{G})}$.

Proof. The estimates on the volume follow similarly to Proposition 5.6. To prove the first claim, if $x \in \Omega$ satisfies the property, then there is $z \in \Gamma$, $(\phi, \phi') \in \Phi_\varepsilon = B_{\frac{\varepsilon}{(n+1)c_\Omega}}(e) \times \mathrm{G}(\mathbb{Z}_p)$ and $b \in B$ so that

$$(\phi^{-1}x^{-1}z, b^{-1}(\phi')^{-1}z) \in \Phi_\varepsilon = B_{\frac{\varepsilon}{(n+1)c_\Omega}}(e) \times \mathrm{G}(\mathbb{Z}_p) \subset G_\infty \times G_p.$$

Then we have that $z \in \phi' b\mathrm{G}(\mathbb{Z}_p)$ and so $||z||_p \leq ||b||_p \leq \max_{b\in B} ||b||_p$. Observe that $\phi \in B_{\frac{\varepsilon}{(n+1)c_\Omega}}(e) \subset \mathcal{O}_\infty(1)$. Thus we have that

$$||g \cdot \phi||_\infty \leq n \cdot ||g||_\infty \cdot ||\phi||_\infty \leq n \cdot ||g||_\infty,$$

for all $g \in \mathrm{GL}_n(\mathbb{R})$. We conclude,

$$\begin{aligned}
||x - z||_\infty &\leq ||x - x\phi||_\infty + ||x\phi - z||_\infty \\
&= ||x(e-\phi)||_\infty + ||x\phi(e - \phi^{-1}x^{-1}z)||_\infty \\
&\leq c_\Omega \left(||e-\phi||_\infty + ||\phi(e-\phi^{-1}x^{-1}z)||_\infty\right) \\
&\leq c_\Omega \left(||e-\phi||_\infty + n||e-\phi^{-1}x^{-1}z||_\infty\right) \\
&\leq c_\Omega \left(\frac{\varepsilon}{(n+1)c_\Omega} + n\frac{\varepsilon}{(n+1)c_\Omega}\right) \\
&\leq (n+1)c_\Omega \frac{\varepsilon}{(n+1)c_\Omega} \\
&\leq \varepsilon.
\end{aligned}$$

□

Proof. (of Theorem 5.10). The proof is similar to the one of Theorem 5.5. We again write

$$\pi = \pi, \qquad q = q_{p,\ell}(\mathrm{G}) \qquad a = a_{p,\ell}(\mathrm{G}).$$

Fix $\Omega \subset G_\infty$ bounded. Let $\delta > 0$ and $\varepsilon > 0$ and set

$$h_\varepsilon = \varepsilon^{-(\theta_{G,p,\ell}+\delta)} = \varepsilon^{-(\frac{\dim_\mathbb{Q}(\mathrm{G})q}{a}+\delta)}$$

We denote for $0 < \varepsilon < 1$,

$$X_\varepsilon = \{x \in X \,:\, B_{h_\varepsilon}^{-1}x \cap \Phi_{\varepsilon,\Gamma} = \emptyset\}.$$

Similar to the proof of Theorem 5.5 it follows for $h_\varepsilon \geq h_0(p, \delta')$,

$$m_X(X_\varepsilon) \ll_{\Omega,\delta'} \varepsilon^{\theta_{\delta,\delta'}}$$

for

$$\begin{aligned}
\theta_{\delta,\delta'} &= -\left(\frac{\dim_\mathbb{Q}(\mathrm{G})q}{a} + \delta\right)\left(-\frac{2a}{q} + \delta'\right) - \dim_\mathbb{Q}(\mathrm{G}) \\
&= \dim_\mathbb{Q}(\mathrm{G}) + \delta\frac{2a}{q} - \delta'\left(\frac{\dim_\mathbb{Q}(\mathrm{G})q}{a} + \delta\right).
\end{aligned}$$

Now choose δ' small enough so that $\theta_{\delta,\delta'} > \dim_\mathbb{Q}(\mathrm{G})$. By Proposition 5.11, we have for all $x \in \Omega$ that

$$\varepsilon^{\dim_\mathbb{Q}(\mathrm{G})} \ll_\Omega m_X((\Phi_\varepsilon)^{-1}x^{-1}).$$

Thus there is $\varepsilon_0(\Omega, \delta)$ small enough so that for all $0 < \varepsilon < \varepsilon_0(\Omega, \delta)$ we have that $h_\varepsilon \geq h_0(p, \delta')$ and $m_X(X_\varepsilon) \leq m_X((\Phi_\varepsilon)^{-1}x^{-1})$. This implies that $(\Phi_\varepsilon)^{-1}x^{-1} \not\subset X_\varepsilon$ and $x^{-1}(\Phi_\varepsilon)^{-1}B_{h_\varepsilon}^{-1} \cap \Phi_{\varepsilon,\Gamma} \neq \emptyset$ and hence the claim is implied by the last proposition. □

5.4 Discrepancy Bound for Diophantine Approximation

We proceed with the same setting as in the last subchapter, however change the metrics on G_∞ and G_p. On G_∞ we consider a left-invariant metric d_∞ induced by a left-invariant Riemannian metric, whereas on G_p we turn the matrix norm from before into a bi-K_p-invariant one by averaging, where K_p is a maximal compact subgroup containing $\mathrm{G}(\mathbb{Z}_p)$. Moreover, we fix a Haar measure m_p on G_p that assigns unit volume to the set K_p. Then we choose a normalization of Haar measure m_∞ on G_∞ with the property that the Haar measure $m_{G_\infty \times G_p} = m_\infty \times m_p$ descends to the probability measure $m_{X_{p,\ell}}$, i.e. so that for all $f \in L^1(G_\infty \times G_p)$,

$$\int_X \sum_{\gamma\in\Gamma} f(x\gamma)\, dm_{X_{p,\ell}} = \int f(g)\, dm_{G_\infty\times G_p}(g).$$

We again write throughout this subchapter $X = X_{p,\ell}$ and $\Gamma = \Gamma_{p,\ell}$. We further write Γ_ℓ for the ℓ-congruence subgroup of $\mathrm{G}(\mathbb{Z})$ and denote by

$$\Gamma(h) = \{\gamma \in \Gamma \,:\, ||\gamma||_p \le h\} \quad \text{and} \quad B_h = \{g \in G_p \,:\, ||g||_p \le h\}.$$

For $x \in G_\infty$, denote

$$B_\varepsilon(x) := \{y \in G_\infty \,:\, d_\infty(x,y) < \varepsilon\}.$$

We note that for all $x \in G_\infty$ and $\varepsilon > 0$,

$$m_\infty(B_\varepsilon(x)) = m_\infty(xB_\varepsilon(e)) = m_\infty(B_\varepsilon(e)).$$

Theorem 5.12. *There is $\varepsilon_0 > 0$ so that for all $0 < \varepsilon < \varepsilon_0$ and $\Omega \subset G_\infty$ bounded,*

$$\left|\left| \frac{|\Gamma(h)\cap B_\varepsilon(\cdot)|}{m_p(B_h)} - m_\infty(B_\varepsilon(e)) \right|\right|_{L^2(\Omega)} \ll_{\Omega,\delta} (m_\infty(B_\varepsilon(e)))^{\frac{1}{2}} m_p(B_h)^{-\frac{1}{q_{p,\ell}(\mathrm{G})}+\delta}.$$

Moreover, if Ω is Γ_ℓ-injective, then the bound does not depend on Ω.

Proof. The result follows by expressing the quantity

$$\frac{|\Gamma(h)\cap B_\varepsilon(\cdot)|}{m_p(B_h)}$$

in terms of the operator $\pi_{p,\ell}(f_{B_h})$ and then applying Theorem 4.5. Choose ε_0 small enough so that in G_∞ we have $B_{\varepsilon_0}(\gamma)\cap \mathrm{G}(\mathbb{Z}) = \{\gamma\}$ for all $\gamma \in \mathrm{G}(\mathbb{Z})$. The set

$$\Phi_\varepsilon = B_\varepsilon(e) \times K_p \subset G_\infty \times G_p$$

is left-Γ-injective and denote by χ_ε the characteristic function of Φ_ε. Write

$$\phi_\varepsilon(g) = \sum_{\gamma\in\Gamma} \chi_\varepsilon(g\gamma)$$

for $g \in G_\infty \times G_p$. The function ϕ_ε is well defined on X. By our normalization of the Haar measure on G_p,

$$\begin{aligned}\int_X \phi_\varepsilon \, dm_X &= \int_{(G_\infty \times G_p)/\Gamma} \sum_{\gamma \in \Gamma} \chi_\varepsilon(g\gamma) \, dm_X(g) \\ &= \int_{G_\infty \times G_p} \chi_\varepsilon \, dm_{G_\infty \times G_p} = m_\infty(B_\varepsilon(e)).\end{aligned}$$

Moreover, if $x \in G_\infty$ and $z \in K_p$ then

$$\begin{aligned}\int_{B_h} \phi_\varepsilon(x^{-1}, g^{-1}z) \, dm_p(g) &= \sum_{\gamma \in \Gamma} \int_{B_h} \chi_\varepsilon(x^{-1}\gamma, g^{-1}z\gamma) \, dm_p(g) \\ &= \sum_{\gamma \in B_\varepsilon(x)} m_p(z\gamma K_p \cap B_h) \\ &= |\Gamma(h) \cap B_\varepsilon(x)|,\end{aligned}$$

where the second line follows as $(x^{-1}\gamma, g^{-1}z\gamma) \in B_\varepsilon(e) \times K_p$ implies that $\gamma \in B_\varepsilon(x)$ and $g \in z\gamma K_p$ and the last line follows by K_p-invariance of the norm $||\cdot||_p$. Set $f_{B_h} = \frac{\chi_{B_h}}{m_p(B_h)}$. These two equations combined yield

$$\frac{|\Gamma(h) \cap B_\varepsilon(x)|}{m_p(B_h)} - m_\infty(B_\varepsilon(e)) = \pi_{p,\ell}(f_{B_h})\phi_\varepsilon(x^{-1}, z) - \int_X \phi_\varepsilon \, dm_X. \tag{5.2}$$

Furthermore,

$$\begin{aligned}||\phi_\varepsilon||_2^2 &= \int_X \sum_{\gamma_1, \gamma_2 \in \Gamma} \chi_\varepsilon(g\gamma_1)\chi_\varepsilon(g\gamma_2) \, dm_X(g) \\ &= \int_X \sum_{\gamma, \delta \in \Gamma} \chi_\varepsilon(g\gamma)\chi_\varepsilon(g\gamma\delta) \, dm_X(g) \\ &= \sum_{\delta \in \Gamma} \int_X \sum_{\gamma \in \Gamma} \chi_\varepsilon(g\gamma)\chi_\varepsilon(g\gamma\delta) \, dm_X(g) \\ &= \int_X \sum_{\gamma \in \Gamma} \chi_\varepsilon(g\gamma) \, dm_X(g) \\ &= m_\infty(B_\varepsilon(e)).\end{aligned}$$

The mean ergodic theorem (Theorem 4.5) gives

$$||\pi_{p,\ell}(f_{B_h})||_{\mathrm{op}} \ll_\delta m_p(B_h)^{-\frac{1}{q_{p,\ell}(\mathrm{G})}+\delta}.$$

Thus we have for fixed $z \in K_p$ that

$$\begin{aligned}
&\left|\left|\frac{|\Gamma(h) \cap B_\varepsilon(\cdot)|}{m_p(B_h)} - m_\infty(B_\varepsilon(e))\right|\right|_{L^2(\Omega)} \\
&= \left|\left|\frac{1}{m_p(B_h)} \int_{B_h} \phi_\varepsilon(\cdot^{-1}, g^{-1}z)\, dm_p(g) - \int_X \phi_\varepsilon \, dm_X\right|\right|_{L^2(\Omega)} \\
&= \left|\left|\frac{1}{m_p(B_h)} \int_{B_h} \phi_\varepsilon(\cdot^{-1}, g^{-1}\cdot)\, dm_p(g) - \int_X \phi_\varepsilon \, dm_X\right|\right|_{L^2(\Omega \times K_p)} \\
&= \left|\left|\pi(f_{B_h})\phi_\varepsilon(\cdot, \cdot) - \int_X \phi_\varepsilon(g)\, dm_X(g)\right|\right|_{L^2(\Omega^{-1} \times K_p)} \\
&\ll_\Omega \left|\left|\pi(f_{B_h})\phi_\varepsilon - \int_X \phi_\varepsilon \, dm_X\right|\right|_{L^2(X)} \\
&\ll_{\Omega,\delta} ||\phi_\varepsilon||_2 m_p(B_h)^{-\frac{1}{q_{p,\ell}(\mathrm{G})}+\delta} = (m_\infty(B_\varepsilon(e)))^{\frac{1}{2}} m_p(B_h)^{-\frac{1}{q_{p,\ell}(\mathrm{G})}+\delta},
\end{aligned}$$

where the bound does not depend on Ω if the set is Γ_ℓ-injective. □

The next result assumes the consequence of Theorem 5.12 and has as implication almost a mean ergodic theorem. In view of Theorem 3.17, if $G_p = \mathrm{SL}_2(\mathbb{Q}_p)$ the next result almost implies a spectral gap. Before proceeding, we review a general fact from measure theory.

Lemma 5.13. *Let G be a locally compact metric group with Haar measure m_G. Let $f \in L^1(G)$. Then for almost all $x \in G$,*

$$\lim_{\varepsilon \to 0} \frac{\int_{B_\varepsilon(x)} f \, dm_G}{m_G(B_\varepsilon(x))} = f(x).$$

Proof. We briefly review the proof given in Corollary 2.14 of [Mat95]. Consider the measure μ defined for Borel sets A as

$$\mu(A) = \int_A f \, dm_G.$$

Since $\mu \ll m_G$, there is a Radon-Nikodym derivative $F(m_G, \mu)$ so that

$$\int_A F(m_G, \mu)\, dm_G = \mu(A) = \int_A f \, dm_G.$$

Hence $f = F(m_G, \mu)$ almost everywhere. The claim follows as the Radon-Nikodym derivative $F(m_G, \mu)$ satisfies at almost all points $x \in G$,

$$F(m_G, \mu)(x) = \lim_{\varepsilon \to 0} \frac{\mu(B_\varepsilon(x))}{m_G(B_\varepsilon(x))} = \lim_{\varepsilon \to 0} \frac{\int_{B_\varepsilon(x)} f \, dm_G}{m_G(B_\varepsilon(x))}.$$

□

Theorem 5.14. *Assume there is some $\rho > 0$ so that for all Γ_ℓ-injective $\Omega \subset G_\infty$,*

$$\left|\left|\frac{|\Gamma(h) \cap B_\varepsilon(\cdot)|}{m_p(B_h)} - m_\infty(B_\varepsilon(e))\right|\right|_{L^2(\Omega)} \ll_\varepsilon m_p(B_h)^{-\rho}.$$

Let τ be an irreducible representation of G_p contained in $L^2_0(X)$. Then

$$||\tau(f_{B_h})||_{\mathrm{op}} \ll_\tau m_p(B_h)^{-\rho}.$$

Proof. By equation (5.2), the assumption is equivalent to the condition that for $z \in K_p$ fixed

$$\left|\left|\pi_{p,\ell}(f_{B_h})\phi_\varepsilon(\cdot^{-1}, z) - \int_X \phi_\varepsilon \, dm_X\right|\right|_{L^2(\Omega)} \ll_\varepsilon m_p(B_h)^{-\rho}.$$

Thus, using similar arguments to the proof of Theorem 5.12,

$$\left|\left|\pi_{p,\ell}(f_{B_h})\phi_\varepsilon(\cdot, \cdot) - \int_X \phi_\varepsilon \, dm_X\right|\right|_{L^2(F^{-1} \times K_p)} \ll_\varepsilon m_p(B_h)^{-\rho},$$

by choosing a fundamental domain F^{-1} for $\Gamma_\ell < \mathrm{G}(\mathbb{R})$. As the class number of G is finite,

$$\left|\left|\pi_{p,\ell}(f_{B_h})\phi_\varepsilon - \int_X \phi_\varepsilon \, dm_X\right|\right|_{L^2(X)} \ll_\varepsilon m_p(B_h)^{-\rho}.$$

We furthermore denote by $\phi_{x,\varepsilon}$ the function on X defined as

$$\phi_{x,\varepsilon}(g) = \sum_{\gamma \in \Gamma} \chi_{x,\varepsilon}(g\gamma),$$

where $\chi_{x,\varepsilon}$ is the characteristic function of $B_\varepsilon(x) \times K_p$. Then by left-invariance of d_∞, it follows that

$$\left|\left|\pi_{p,\ell}(f_{B_h})\phi_{x,\varepsilon} - \int_X \phi_\varepsilon \, dm_X\right|\right|_{L^2(X)} \ll_\varepsilon m_p(B_h)^{-\rho}. \tag{5.3}$$

Consider an irreducible unitary representation τ contained in $L^2_0(X)$. If τ is not spherical, as B_h is bi-K_p-invariant, $\tau(f_{B_h}) = 0$. So we assume without loss of generality that τ is spherical and that $v_\tau \in L^2_0(X)$ is an associated unit K_p-invariant vector, which is unique up to a multiple of $\mathbb{S}^1$, and $\eta_\tau(g) = \langle \tau_g v_\tau, v_\tau \rangle$ be the associated spherical function. Recall that

$$||\tau(f_{B_h})|| = |\langle \tau(f_{B_h})v_\tau, v_\tau \rangle| = |\eta_\tau(f_{B_h})| = \left|\frac{1}{m_p(B_h)} \int_{B_h} \eta_\tau(g) \, dm_p(g)\right|.$$

Then as $\tau(f_{B_h})v_\tau$ is K_p-invariant it follows by one dimensionality of K_p-invariant vectors that

$$\tau(f_{B_h})v_\tau = \eta_\tau(f_{B_h})v_\tau.$$

Set $f(g) = v_\tau((g,e)\Gamma)$ for $g \in G_\infty$. As v_τ is K_p-invariant, it follows that f is a well defined measurable function $f \in L^2(G_\infty)$ and $f \neq 0$. Further, again as f is K_p-invariant and as $\chi_{x,\varepsilon}$ is the characteristic function of $B_\varepsilon(x) \times K_p$,

$$\begin{aligned}\langle \phi_{x,\varepsilon}, v_\tau \rangle &= \int_X \left(\sum_{\gamma\in\Gamma} \chi_{x,\varepsilon}(g\gamma) \right) \overline{v_\tau(g)}\, dm_X(g) \\ &= \int_{G_\infty \times G_p} \chi_{x,\varepsilon}(g) \overline{v_\tau(g)}\, dm_{G_\infty\times G_p}(g) \\ &= \int_{B_\varepsilon(x)} \overline{f(g)}\, dm_\infty(g).\end{aligned}$$

Thus it follows by Lemma 5.13, that for almost all $x \in G_\infty$,

$$\frac{\langle v_\tau, \phi_{x,\varepsilon}\rangle}{m_\infty(B_\varepsilon(x))} \longrightarrow \overline{f(x)}$$

as $\varepsilon \to 0$. So we fix some x_0, depending on τ, so that $f(x_0) \neq 0$ and choose some ε_0 so that

$$\frac{\langle \phi_{x_0,\varepsilon_0}, v_\tau\rangle}{m_\infty(B_{\varepsilon_0}(x_0))}$$

is close to $f(x_0)$ and in particular non-zero.

Using that v_τ is orthogonal to the constant functions,

$$\begin{aligned}|\langle \pi_{p,\ell}(f_{B_h})\phi_{x_0,\varepsilon_0}, v_\tau\rangle| &= \left| \left\langle \pi_{p,\ell}(f_{B_h})\phi_{x_0,\varepsilon_0} - \int_X \phi_{\varepsilon_0}\, dm_X, v_\tau \right\rangle \right| \\ &\ll_\tau \left\| \pi_{p,\ell}(f_{B_h})\phi_{x_0,\varepsilon_0} - \int_X \phi_{\varepsilon_0}\, dm_X \right\|_{L^2(X)} \\ &\ll_{\tau,\varepsilon_0} m_p(B_h)^{-\rho}.\end{aligned}$$

Moreover,

$$|\langle \pi_{p,\ell}(f_{B_h})\phi_{x_0,\varepsilon_0}, v_\tau\rangle| = |\langle \phi_{x_0,\varepsilon_0}, \pi_{p,\ell}(f_{B_h}^*)v_\tau\rangle| = \eta_\tau(f_{B_h}^*) \cdot |\langle \phi_{x_0,\varepsilon_0}, v_\tau\rangle|.$$

As η_τ is symmetric, $\eta_\tau(f_{B_h}^*) = \eta_\tau(f_{B_h})$ and so we obtain the following:

$$||\tau(f_{B_h})|| = |\eta_\tau(f_{B_h})| \ll_{\tau,\varepsilon_0} \frac{1}{|\langle \phi_{x_0,\varepsilon_0}, v_\tau\rangle|} m_p(B_h)^{-\rho} \ll_{\tau,\varepsilon_0} m_p(B_h)^{-\rho}.$$

□

The next corollary combines Theorem 5.14 with Theorem 3.17 using the additional assumption $\mathrm{G} = \mathrm{B}^1$ for B as usual a quaternion algebra over $\mathbb{Q}$. Towards our proof of property (τ) for $\mathbb{Q}$-forms of SL_2, we replace the condition of Theorem 5.14 with (5.4).

Theorem 5.15. *In the above setting, assume that* $\mathrm{G} = \mathrm{B}^1$ *and let* p *be an isotropic place of* G. *Assume that there is some* $\rho > 0$ *so that for all* $x \in G_\infty$ *and* $\varepsilon > 0$,

$$\left\| \pi_{p,\ell}(f_{B_h})\phi_{x,\varepsilon} - \int_X \phi_\varepsilon\, dm_X \right\|_{L^2(X)} \ll_{\varepsilon,\delta} m_p(B_h)^{-\rho+\delta} \tag{5.4}$$

for all $\delta > 0$. *Then* $q(\pi_{p,\ell}) \leq \max\{\frac{1}{\rho}, 2\}$.

Proof. We recall that by [Bor97], we have a decomposition

$$L_0^2(X_{p,\ell}) = L^2_{\mathrm{tem}}(X_{p,\ell}) \oplus \bigoplus_{\substack{\sigma\in\widehat{G_p},\, \sigma\prec\pi_{p,\ell} \\ \sigma \text{ not tempered}}} \sigma,$$

for $L^2_{\mathrm{tem}}(X_{p,\ell})$ a tempered subrepresentation. Thus the conclusion of Theorem 5.14 implies the assumption of Theorem 3.17 and hence by Theorem 3.17 we conclude $q(\pi_{p,\ell}) \leq \max\{\frac{1}{\rho}, 2\}$. □

5.5 Property (τ) for $\mathbb{Q}$-forms of SL_2

In this subchapter we consider a quaternion algebra $\mathrm{B}_{a,b}$ over $\mathbb{Q}$ for $a, b \in \mathbb{Q}^\times$. Without loss of generality, we assume that $a, b \in \mathbb{Z}$. We moreover drop the a, b in the notation and just write $\mathrm{B} = \mathrm{B}_{a,b}$. As usual denote by $\mathrm{G} = \mathrm{B}^1$ the algebraic subgroup consisting of elements of unit norm and for simplicity we denote $\mathbb{Z}^4 = \mathrm{B}(\mathbb{Z})$. As we assume $a, b \in \mathbb{Z}$, the algebraic group G can be viewed as an affine $\mathbb{Z}$-scheme. Throughout this subchapter, we fix a prime p with the property that G is isotropic over $\mathbb{Q}_p$ so that in particular $G_p = \mathrm{SL}_2(\mathbb{Q}_p)$. The central aim is to show that $q(\pi_{p,\ell}) \leq \frac{1}{\rho}$ for all p and ℓ, where

$$\rho = \begin{cases} \frac{1}{24} & \text{if } \mathrm{G} \cong \mathrm{SL}_2, \\ \frac{1}{4} & \text{if B is a division algebra.} \end{cases}$$

This proves Theorem 3.12 and in particular implies property (τ) for $\mathbb{Q}$-forms of SL_2.

The strategy is to prove the bound (5.4) for the above choice of ρ by using results established by Heath-Brown's [HB96] approach to the circle method. This implies $q(\pi_{p,\ell}) \leq \frac{1}{\rho}$ by Theorem 5.15. The main observation is that the norm Nr on $\mathrm{B}(\mathbb{R})$ is an integer quadratic form in four variables. To link bounds as in (5.4) to counting the number of integral solutions of quadratic forms in four variables, consider a positive smooth compactly supported function $w : \mathrm{B}(\mathbb{R}) \to \mathbb{R}$ and the function ϕ_w on $X_{p,\ell}$ defined by

$$\phi_w(g_\infty, g_p) := \sum_{\gamma\in\Gamma_{p,\ell}} w(g_\infty\gamma)\chi_{\mathrm{G}(\mathbb{Z}_p)}(g_p\gamma),$$

for $(g_\infty, g_p) \in \mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p)$. Then we observe as in the proof of Theorem 5.12 for fixed $g \in \mathrm{G}(\mathbb{R})$, $u \in \mathrm{G}(\mathbb{Z}_p)$ and h,

$$\begin{aligned} \int_{B_h} \phi_w(g^{-1}, h^{-1}u)\, dm_p(h) &= \sum_{\gamma\in\Gamma_{p,\ell}} \int_{B_h} w(g^{-1}\gamma)\chi_{\mathrm{G}(\mathbb{Z}_p)}(h^{-1}u\gamma)\, dm_p(h) \\ &= \sum_{\gamma\in\Gamma_{p,\ell}} w(g^{-1}\gamma) m_p(B_h \cap u\gamma\mathrm{G}(\mathbb{Z}_p)) \\ &= \sum_{\gamma\in\Gamma_{p,\ell}\cap B_h} w(g^{-1}\gamma) = \sum_{\gamma\in\Gamma_{p,\ell}\cap B_h} w_g(\gamma), \end{aligned}$$

where for simplicity we write $w_g(\cdot) = w(g^{-1}\cdot)$. The relation between the latter sum and the number of solutions of the norm-form is given by the following bijection:

$$\Gamma_{p,\ell} \cap B_h \longrightarrow \{x \in I + (\ell\mathbb{Z})^4 \,:\, \mathrm{Nr}(x) = h^2\}, \qquad \gamma \longmapsto h\gamma.$$

Thus it follows,

$$\int_{B_h} \phi_w(g^{-1}, h^{-1}u)\, dm_p(h) = \sum_{\gamma \in \Gamma_{p,\ell} \cap B_h} w_g(\gamma) = \sum_{\substack{x \in I + (\ell\mathbb{Z})^4 \\ \mathrm{Nr}(x) = h^2}} w_g(h^{-1}x). \tag{5.5}$$

In order to deduce (5.4), it suffices to understand the latter term as compactly supported functions are dense in $L^2(\mathbb{R}^4)$. To introduce further notation, write

$$N_h(w_g) = \sum_{\substack{x \in I + (\ell\mathbb{Z})^4 \\ \mathrm{Nr}(x) = h^2}} w_g(h^{-1}\gamma).$$

The latter sum can be estimated by the methods developed by [HB96]. In chapter 7, we will expose [HB96] and prove in chapter 7.8 the necessary results on the sum $N_h(w_g)$. In the remainder of this chapter, we state the latter results and deduce from them (5.4) for ρ.

Write

$$\sigma_\infty(\mathrm{Nr}, w) := \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|\mathrm{Nr}(x) - 1| \le \varepsilon} w(x)\, dx, \tag{5.6}$$

where we refer to chapter 7 for a discussion around such integrals. Moreover, write $\ell = \prod_{p \text{ prime}} p^{\nu_p}$. Then we denote by $M_h(p^k)$ the number of solutions of the equation

$$\mathrm{Nr}(x) = h^2 \mod p^k$$

for $x \in \{1, \dots, p^{k+\nu_p}\}^4$ under the additional assumption $x = I \mod p^{\nu_p}$. Finally write

$$\sigma_p = \lim_{k \to \infty} \frac{M_h(p^k)}{p^{3k}}$$

and

$$\sigma(\mathrm{Nr}, h^2, I) = \prod_{p \text{ prime}} \sigma_p,$$

where we again refer to chapter 7 for convergence issues.

Corollary 5.16. *For every ℓ, there exists a measurable subset $Q \subset \mathrm{G}(\mathbb{R})$ that surjects onto $\mathrm{G}(\mathbb{R})/\Gamma_\ell$ so that for all $\varepsilon > 0$ and all suitable compactly supported functions $w : \mathrm{B}(\mathbb{R}) \to \mathbb{R}$ (see the discussion in chapter 7),*

$$\left\| N_h(w_g) - \frac{1}{\ell^4} \sigma_\infty(\mathrm{Nr}, w) \sigma(\mathrm{Nr}, h^2, I) h^2 \right\|_{L^2(Q)} \ll_{w,\ell,Q,\varepsilon} h^{\frac{23}{12}+\varepsilon}.$$

If moreover B *is a division algebra,*

$$\left\| N_h(w_g) - \frac{1}{\ell^4} \sigma_\infty(\mathrm{Nr}, w) \sigma(\mathrm{Nr}, h^2, I) h^2 \right\|_{L^2(Q)} \ll_{w,\ell,Q,\varepsilon} h^{\frac{3}{2}+\varepsilon}.$$

Before proceeding, we recall that we denote by m_∞^{Tam} and m_p^{Tam} the Tamagawa measure on $\mathrm{G}(\mathbb{R})$ and $\mathrm{G}(\mathbb{Q}_p)$, which is induced by a fixed gauge form on G. Moreover, we recall that as G is simply connected,

$$m_\infty^{\mathrm{Tam}}(\mathrm{G}(\mathbb{R})/\mathrm{G}(\mathbb{Z})) \prod_{p \text{ prime}} m_p^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)) = 1.$$

In the following, we use a more explicit choice of the compactly supported function w. In fact, we fix some compactly supported function on $\mathrm{G}(\mathbb{R})$, which we denote by w_{G}. Then we choose a compactly supported function $w : B(\mathbb{R}^4) \to \mathbb{R}$ with the property

$$\sigma_\infty(\mathrm{Nr}, w) = \int_{\mathrm{G}(\mathbb{R})} w_{\mathrm{G}} \, dm_\infty^{\mathrm{Tam}}.$$

Lemma 5.17. *In the above setting for $h = p^n$,*

$$\frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr}, w)\sigma(\mathrm{Nr}, h^2, I)h^2 = m_p(B_h) \int_{X_{p,\ell}} \phi_w \, dm_{X_{p,\ell}}.$$

Assuming the lemma for the moment, together with Corollary 5.16 it follows by dividing by $m_p(B_h)$ together with equation (5.5) that

$$\left\| \pi_{p,\ell}(f_{B_h})\phi_w - \int_{X_{p,\ell}} \phi_w \, m_{X_{p,\ell}} \right\|_{L^2(X_{p,\ell})} \ll_{w,\ell,\varepsilon} m_p(B_h)^{-\rho+\varepsilon},$$

which then implies

$$\left\| \pi_{p,\ell}(f_{B_h})\phi_{x,\varepsilon} - \int_{X_{p,\ell}} \phi_\varepsilon \, dm_{X_{p,\ell}} \right\|_{L^2(X_{p,\ell})} \ll_{w,\ell,\varepsilon} m_p(B_h)^{-\rho+\varepsilon}.$$

Thus by Theorem 5.15 it follows that $q(\pi_{p,\ell}) \leq \frac{1}{\rho}$.

Proof. (of Lemma 5.17) Throughout this proof we introduce the more precise notation $M_h(q^k, q^{\nu_p})$ for the same quantity as $M_h(q^k)$.

Let q be a prime number. We aim to calculate σ_q, which will be done by a case distinction. First assume that q is coprime to ℓ and h. Then

$$\begin{aligned} |\mathrm{G}(\mathbb{Z}/q^k\mathbb{Z})| &= |\{x \mod q^k \,:\, \mathrm{Nr}(x) \equiv 1 \mod q^k\}| \\ &= |\{x \mod q^k \,:\, \mathrm{Nr}(x) \equiv h^2 \mod q^k\}|. \end{aligned}$$

Thus it follows by Lemma 1.23,

$$\begin{aligned} \sigma_q &= \lim_{k\to\infty} \frac{M_h(q^k, q^{\nu_q})}{q^{3k}} \\ &= \lim_{k\to\infty} \frac{M_h(q^k, 1)}{q^{3k}} \\ &= \frac{|\mathrm{G}(\mathbb{Z}/q^k\mathbb{Z})|}{q^{3k}} = m_q^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)). \end{aligned}$$

If q divides ℓ, then as ℓ is coprime to h for $k \geq \nu_q$,

$$\begin{aligned} M_h(q^k, q^{\nu_q}) &= q^{4\nu_q}|\{x \mod q^k \,:\, x = I \mod q^{\nu_p} \text{ and } \mathrm{Nr}(x) = h^2 \mod q^k\}| \\ &= q^{4\nu_q}|\{x \mod q^k \,:\, x = h'^2 \mod q^{\nu_p} \text{ and } \mathrm{Nr}(x) = 1 \mod q^k\}| \\ &= q^{4\nu_q}\frac{|\mathrm{G}(\mathbb{Z}/q^k\mathbb{Z})|}{|\mathrm{G}(\mathbb{Z}/q^{\nu_q}\mathbb{Z})|}, \end{aligned}$$

where h' is an inverse of h modulo q^k. Then again by Lemma 1.23,

$$\begin{aligned}\sigma_q &= \lim_{k\to\infty} \frac{M_h(q^k, q^{\nu_q})}{q^{3k}} \\ &= \lim_{k\to\infty} \frac{M_h(q^k, 1)}{q^{3k}} \\ &= q^{4\nu_q} \frac{|\mathrm{G}(\mathbb{Z}/q^k\mathbb{Z})|}{p^{3k}|\mathrm{G}(\mathbb{Z}/q^{\nu_q}\mathbb{Z})|} \\ &= \frac{q^{4\nu_q}}{|\mathrm{G}(\mathbb{Z}/q^{\nu_q}\mathbb{Z})|} m_q^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)).\end{aligned}$$

Moreover if q divides h (i.e. $q = p$), then $\nu_q = 0$ as h and ℓ are coprime. Thus by Lemma 1.24,

$$\sigma_q = h^{-2} m_q^{\mathrm{Tam}}(B_h).$$

Putting all this together and by using the Tamagawa volume formula, it follows as $h = p^n$,

$$\begin{aligned}\sigma(\mathrm{Nr}, h^2, I) &= \prod_{q \text{ prime}} \sigma_q \\ &= \prod_{\substack{q \text{ prime} \\ (q,\ell)=1, (q,h)=1}} m_q^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)) \prod_{\substack{q \text{ prime} \\ q|\ell}} \frac{q^{4\nu_q}}{|\mathrm{G}(\mathbb{Z}/q^{\nu_q}\mathbb{Z})|} m_q^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)) \prod_{\substack{q \text{ prime} \\ q|h}} h^{-2} m_q^{\mathrm{Tam}}(B_h) \\ &= \frac{h^{-2}\ell^4}{|\mathrm{G}(\mathbb{Z}/\ell\mathbb{Z})|} m_p(B_h) m_p^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)) \prod_{\substack{q \text{ prime} \\ q\neq p}} m_q^{\mathrm{Tam}}(\mathrm{G}(\mathbb{Z}_p)). \\ &= \frac{h^{-2}\ell^4}{|\mathrm{G}(\mathbb{Z}/\ell\mathbb{Z})|} m_p(B_h) m_\infty^{\mathrm{Tam}}(\mathrm{G}(\mathbb{R})/\mathrm{G}(\mathbb{Z}))^{-1}.\end{aligned}$$

As the probability measure on $\mathrm{G}(\mathbb{R})/\Gamma_\ell$ is induced by $\frac{m_\infty^{\mathrm{Tam}}(\mathrm{G}(\mathbb{R})/\mathrm{G}(\mathbb{Z}))^{-1}}{|\mathrm{G}(\mathbb{Z}/\ell\mathbb{Z})|} dm_\infty^{\mathrm{Tam}}$, the claim follows. More precisely,

$$\begin{aligned}\frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr}, w)\sigma(\mathrm{Nr}, h^2, I)h^2 &= m_p(B_h) \frac{m_\infty^{\mathrm{Tam}}(\mathrm{G}(\mathbb{R})/\mathrm{G}(\mathbb{Z}))^{-1}}{|\mathrm{G}(\mathbb{Z}/\ell\mathbb{Z})|} \sigma_\infty(\mathrm{Nr}, w) \\ &= m_p(B_h) \frac{m_\infty^{\mathrm{Tam}}(\mathrm{G}(\mathbb{R})/\mathrm{G}(\mathbb{Z}))^{-1}}{|\mathrm{G}(\mathbb{Z}/\ell\mathbb{Z})|} \int_{\mathrm{G}(\mathbb{R})} w_{\mathrm{G}}\, dm_\infty^{\mathrm{Tam}} \\ &= m_p(B_h) \int_{\mathrm{G}(\mathbb{R})/\Gamma_\ell} \sum_{\gamma\in\Gamma_\ell} w_{\mathrm{G}}(g\gamma)\, dm_{\mathrm{G}(\mathbb{R})/\Gamma_\ell}(g) \\ &= m_p(B_h) \int_{X_{p,\ell}} \phi_w\, dm_{X_{p,\ell}}.\end{aligned}$$

□

As a final remark, we observe that if B is a division algebra over $\mathbb{Q}$, then an improvement of Corollary 5.16 implies Conjecture 3.13. This observation is formulated in the next theorem.

Theorem 5.18. *Let* B *be a division algebra over* $\mathbb{Q}$. *Assume that for every* ℓ, *there exists a compact subset* $Q \subset \mathrm{G}(\mathbb{R})$ *that surjects onto* $\mathrm{G}(\mathbb{R})/\Gamma_\ell$ *so that for all* $\varepsilon > 0$ *and all suitable compactly supported functions* $w : \mathrm{B}(\mathbb{R}) \to \mathbb{R}$,

$$\left\| N_h(w_g) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr}, w)\sigma(\mathrm{Nr}, h^2, I)h^2 \right\|_{L^2(Q)} \ll_{w,\ell,Q,\varepsilon} h^{1+\varepsilon}.$$

Then Conjecture 3.13 holds for $\mathrm{G} = \mathrm{B}^1$.

Proof. This follows from the above. $\square$

6 The Hardy-Littlewood Circle Method

In this chapter we give an expository account of the circle method. Good references for the circle method are [Dav05], [Vau97] and [Nat96], which contain the entire content of this chapter. In the next chapter we will discuss Heath-Brown's [HB96] version of the circle method.

The circle method, as exposed in this chapter, is concerned with understanding the number of solutions to integer-valued equations. One of the motivating questions is Waring's problem, which we introduce in the following paragraphs.

Denote by $g(k)$ the smallest number n so that **every** positive integer can be written as a sum of n terms consisting of k-th powers of positive integers. By considering numbers mod 8 it follows that integers of the form $8n+7$ cannot be written as a sum of three squares. Thus $g(2) > 3$. By Lagrange's four squares theorem it hence follows that $g(2) = 4$.

More generally we claim that

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

To prove the claim observe that

$$2^k \left[\left(\frac{3}{2}\right)^k\right] - 1 = \left(\left[\left(\frac{3}{2}\right)^k\right] - 1\right) \cdot 2^k + (2^k - 1) \cdot 1^k,$$

where the left hand side of the latter equation is clearly the representation using the least number of k-th powers as it maximizes the number of times the term 2^k is used. This shows the claim.

In fact, one conjectures that for all k the above inequality is an equality so that

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

However, this is only proved for almost all values of k (see the references in [Vau97]), yet in the other cases a small alteration of the above formula for $g(k)$ is known to hold.

To summarize, the number $g(k)$ is rather well understood. Instead of $g(k)$, it is more interesting to study the number $G(k)$, which is defined to be the smallest number n so that every **large enough** positive integer can be written as a sum of n terms consisting of k-th powers of positive integers. By the above argument it again follows that $G(2) = 4$. In contrast to $g(3)$, the precise value of $G(3)$ is only known to be ≥ 4 and ≤ 7. A well-known result by Davenport [Dav39] states that $G(4) = 16$.

The central aim of this chapter is to show $G(k) \leq 2^k + 1$. This is by far not the optimal result, yet the proof provides a good introduction to the circle method. Better results are for example due to Vinogradov [Vin47], who showed for $k > 2$ that $G(k) \leq 3k \log k + 11k$. Even more refined estimates are known today. The reason we focus on the proof that $G(k) \leq 2^k + 1$ is that the explored methods have structural similarity to the techniques developed by Heath-Brown, which are discussed next chapter.

For fixed positive integers k and n denote by $r_{k,n}(m)$ for $m \geq 1$ the number of positive integer tuples $x_1, \ldots, x_n > 0$ so that

$$m = x_1^k + x_2^k + \ldots + x_n^k.$$

In order to show that $G(k) \leq n$ it suffices to show for large enough m that $r_{k,n}(m) > 0$. The main result of this chapter is an asymptotic formula for $r_{k,n}(m)$ under the condition that $n \geq 2^k + 1$. Namely, we will show the **Hardy-Littlewood asymptotic formula**: There exists $\delta = \delta(k,s) > 0$ so that

$$r_{k,n}(m) = C_{k,n}\sigma_{k,n}(m)m^{\frac{n}{k}-1} + O_{k,n}(m^{\frac{n}{k}-1-\delta}),$$

where $\sigma_{k,n}(m)$ is the **singular series**, a function depending only on k and n which satisfies $0 \ll_{k,n} \sigma_{k,n}(m) \ll_{k,n} 1$. The constant $C_{k,n}$ has the explicit value

$$C_{k,n} = \frac{\Gamma(1+\frac{1}{k})^n}{\Gamma(\frac{n}{k})},$$

where as usual for $t > 0$,

$$\Gamma(t) = \int_0^\infty x^{t-1}e^{-x}\,dx.$$

The above asymptotic formula clearly shows for m large that $r_{k,n}(m) > 0$ provided that $n \geq 2^k + 1$.

Before starting to develop the theory, we briefly comment on the strategy to establish the asymptotic formula. Denote by $A \subset \mathbb{N}$ a set of positive integers and consider for $z \in \mathbb{C}$ with $|z| < 1$ the following converging sum

$$F(z) = \sum_{a \in A} z^a.$$

For a positive integer n one observes

$$F(z)^n = \sum_{a_1,\ldots,a_n \in A} z^{a_1+\ldots+a_n} = \sum_{\ell=1}^{\infty} r_{A,n}(m)z^\ell$$

for $r_{A,n}(m)$ the number of representations of m as a sum of n-elements of A. Recall from complex analysis that

$$r_{A,n}(m) = \frac{1}{2\pi i}\int_{|z|=\rho} \frac{F(z)^n}{z^{m+1}}\,dz$$

for $\rho \in (0,1)$. In the original approach by Hardy and Littlewood [HL], this expression of $r_{A,n}(m)$ was analyzed by analytic methods.

Vinogradov observed the following simplification. Namely, in order to study $r_{A,n}(m)$, instead of the above power series $F(z)$, it suffices to consider the polynomial

$$T(\alpha) = \sum_{\substack{a \in A \\ a \leq N}} e(a\alpha)$$

so that

$$T(\alpha)^n = \sum_{\substack{a_1,\ldots,a_n\in A\\ a_i\le N}} e((a_1+\ldots+a_n)\alpha) = \sum_{m=1}^{\infty} r_{A,n}^{(N)}(m)e(m\alpha),$$

where $r_{A,n}^{(N)}(m)$ is the corresponding number to $r_{A,n}(m)$ where one only considers elements of A that are $\le N$. As the elements of A are positive, it holds that $r_{A,n}^{(N)}(m) = r_{A,n}(m)$ for $m \le N$ and $r_{A,n}^{(N)}(m) = 0$ for $m > nN$. Thus it follows that

$$T(\alpha)^n = \sum_{m=1}^{nN} r_{A,n}^{(N)}(m)e(m\alpha).$$

By the basic orthogonality relations

$$\int_0^1 e(k\alpha)e(-\ell\alpha)\,d\alpha = \begin{cases} 1 & \text{if } k=\ell, \\ 0 & \text{if } n\neq \ell \end{cases}$$

one concludes for $m \le N$

$$r_{A,n}(m) = \int_0^1 T(\alpha)^n e(-m\alpha)\,d\alpha.$$

Returning to Waring's problem, we consider the set $A_k = \{n^k : n \in \mathbb{N}\}$ so that $r_{k,n}(m) = r_{A_k,n}(m)$. In order to calculate $r_{k,n}(m)$ it thus suffices to consider the sum

$$T(\alpha) = \sum_{n=1}^{P} e(\alpha n^k)$$

for $P = [m^{\frac{1}{k}}]$. By the above

$$r_{k,n}(m) = \int_0^1 T(\alpha)^n e(-\alpha m)\,d\alpha.$$

So we have reduced the calculation of $r_{k,n}(m)$ to evaluating the above integral on the circle. In this chapter we develop methods in order to prove the Hardy-Littlewood asymptotic formula by analyzing the latter integral.

In this exposition we mostly follow [Dav05], yet also consult [Nat96].

6.1 Weyl's Lemma and Hua's Inequality

Throughout this subchapter we consider a polynomial

$$f(x) = \alpha x^k + \alpha_1 x^{k-1} + \ldots + \alpha_k.$$

The first aim of this subchapter is to estimate the sum

$$\left|\sum_{x=1}^{P} e(f(x))\right|$$

for P some large integer and with the additional assumption that α has a suitable rational approximation.

Let $P \geq 0$ and let $P_1, P_2 \in \mathbb{Z}$ so that $0 \leq P_2 - P_1 \leq P$. Then we set

$$S_k(f) = \sum_{x=P_1+1}^{P_2} e(f(x)),$$

where we suppress in our notation the dependence on P, P_1 and P_2 for convenience. Observe that trivially $|S_k(f)| \leq P$, yet we aim to improve the latter bound. For $x, y \in \mathbb{Z}$ we write

$$\triangle_y f(x) = f(x+y) - f(x)$$

and for $y_1, \dots, y_n \in \mathbb{Z}$ we inductively define

$$\triangle_{y_1,\dots,y_n} f(x) = \triangle_{y_n}(\triangle_{y_1,\dots,y_{n-1}} f(x)).$$

Notice that by the binomial expansion formula, $\triangle_{y_1,\dots,y_n} f$ is of the degree $k-n$.

Proposition 6.1. *For $\nu \geq 0$,*

$$|S_k(f)|^{2^\nu} \ll_\nu P^{2^\nu - 1} + P^{2^\nu - \nu - 1} \cdot \sum_{y_1,\dots,y_\nu=1}^{P} |S_{k-\nu}(\triangle_{y_1,\dots,y_\nu} f)|.$$

Proof. We calculate,

$$\begin{aligned}
|S_k(f)|^2 = S_k(f)\overline{S_k(f)} &= \sum_{x_2} e(f(x_2)) \cdot \sum_{x_1} e(-f(x_1)) \\
&= \sum_{x_1,x_2} e(f(x_2) - f(x_1)) \\
&= P_2 - P_1 + 2\mathrm{Re}\left(\sum_{\substack{x_1,x_2 \\ x_2 > x_1}} e(f(x_2) - f(x_1)) \right) \\
&= P_2 - P_1 + 2\mathrm{Re}\left(\sum_{y=1}^{P} \sum_{x} e(\triangle_y f(x)) \right),
\end{aligned}$$

where in the last line we relabeled the variables as $x = x_1$ and $y = x_2 - x_1$ so that x varies over the interval $[P_1 + 1 - y, P_2 - y] \cap [P_1 + 1, P_2]$. The only observation of importance is that x varies over a possibly empty interval depending on y, whose length is bounded by P. In particular,

$$|S_k(f)|^2 \leq P + 2\sum_{y=1}^{P} |S_{k-1}(\triangle_y f)|.$$

By the same argument, we prove

$$|S_{k-1}(\triangle_y f)|^2 \leq P + 2\sum_{z=1}^{P} |S_{k-2}(\triangle_{y,z} f)|$$

and hence

$$\begin{aligned}
|S_k(f)|^4 = (|S_k(f)|^2)^2 &\leq \left(P + 2\sum_{y=1}^{P} |S_{k-1}(\triangle_y f)|\right)^2 \\
&= P^2 + 4P\sum_{y=1}^{P} |S_{k-1}(\triangle_y f)| + 4\left(\sum_{y=1}^{P} |S_{k-1}(\triangle_y f)|\right)^2 \\
&\leq 5P^3 + 8P\sum_{y=1}^{P} |S_{k-1}(\triangle_y f)|^2 \\
&\leq 45P^3 + 32P\sum_{y,z=1}^{P} |S_{k-2}(\triangle_{y,z} f)| \\
&\ll P^3 + P\sum_{y,z=1}^{P} |S_{k-2}(\triangle_{y,z} f)|,
\end{aligned}$$

where we used in the third line the inequality $(\sum_{i=1}^{n} |x_i|)^2 \leq 2n\sum_{i=1}^{n} |x_i|^2$. By the same proof, the claim follows inductively. □

Before stating and proving the first major result, we discuss a couple of lemmas.

Lemma 6.2. *It holds that*

$$\triangle_{y_1,\ldots,y_{k-1}} f(x) = k!\alpha y_1 \cdot \ldots \cdot y_{k-1} x + \beta,$$

for β a collection of terms independent of x.

Proof. It suffices to consider the case $f(x) = \alpha x^k$, as the lower order terms either vanish or contribute to β. Moreover, we also assume without loss of generality $\alpha = 1$. Then by the binomial expansion formula,

$$\triangle_{y_1} f(x) = (x + y_1)^k - x^k = k y_1 x^{k-1} + \beta_{k-2}$$

for β_{k-2} terms of degree $\leq k-2$. Proceeding,

$$\triangle_{y_1,y_2} f(x) = k(k-1) y_1 y_2 x^{k-2} + \beta_{k-3}$$

and by continuing this process the claim follows. □

Lemma 6.3. *For $\alpha \in \mathbb{R}$ and $N_1 < N_2$,*

$$\left|\sum_{n=N_1+1}^{N_2} e(\alpha n)\right| \leq \frac{1}{2||\alpha||},$$

where $||\alpha||$ denotes the distance of α to the nearest integer.

Proof. We calculate by using the formula for geometric progressions,

$$\begin{aligned}\left|\sum_{x=x_1+1}^{x_2} e(\alpha x)\right| &= \left|e(\alpha(x_1+1))\sum_{n=0}^{x_2-x_1-1} e(\alpha)^n\right| \\ &= \left|\frac{e((x_2-x_1)\alpha)-1}{e(\alpha)-1}\right| \leq \frac{2}{|e(\alpha)-1|} \\ &= \frac{2}{|e(\frac{\alpha}{2})-e(-\frac{\alpha}{2})|} = \frac{2}{|2i\sin\pi\alpha|} \\ &= \frac{1}{|\sin\pi\alpha|} = \frac{1}{\sin\pi||\alpha||} \leq \frac{1}{2||\alpha||}.\end{aligned}$$

In the last line it was used that $2x \leq \sin\pi x$ for $0 \leq x \leq \frac{1}{2}$. □

As usual, we denote by $d(m) = \sum_{d|m} 1$ the number of divisors of m.

Lemma 6.4. *For any* $\varepsilon > 0$,

$$d(m) \ll_\varepsilon m^\varepsilon.$$

Proof. Write $m = p_1^{\lambda_1} p_2^{\lambda_2} \cdot \ldots$ and observe

$$\frac{d(m)}{m^\varepsilon} = \prod_i \frac{\lambda_i+1}{p^{\varepsilon\lambda_i}} \leq \prod_{p_i \leq 2^{\frac{1}{\varepsilon}}} \frac{\lambda_i+1}{2^{\varepsilon\lambda_i}} \ll_\varepsilon 1,$$

where the first inequality follows as if $p_i^\varepsilon > 2$, then $p_i^{-\varepsilon} < \frac{1}{2}$ and hence omitting the term for that i just makes the total product larger. The last inequality follows as for each $\varepsilon > 0$ the product is finite and also $2^{-\varepsilon\lambda}(\lambda+1)$ is a bounded function. □

Lemma 6.5. *Assume that α is a real number that has a rational approximation $\frac{a}{q}$ for coprime $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ that satisfies*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

Then

$$\sum_{1 \leq r \leq \frac{q}{2}} \frac{1}{||\alpha r||} \leq 3q\log q.$$

Proof. The lemma clearly holds for $q = 1$. So we assume $q \geq 2$. For each integer r, there exists $s(r) \in [0, \frac{q}{2}]$ and an integer $m(r)$ so that

$$\frac{s(r)}{q} = \left|\left|\frac{ar}{q}\right|\right| = \pm\left(\frac{ar}{q} - m(r)\right).$$

As $(a,q) = 1$, it follows that $s(r) = 0$ if and only if $r \equiv 0 \mod q$ and hence $s(r) \in [1, \frac{q}{2}]$ if $r \in [1, \frac{q}{2}]$. We only consider $r \in [1, \frac{q}{2}]$ for the remainder of the proof.

Choose $-1 \leq \theta \leq 1$ so that $\alpha - \frac{a}{q} = \frac{\theta}{q^2}$ and similarly choose $\theta' = \frac{2\theta r}{q}$ with $|\theta'| \leq 1$ so that

$$\alpha r = \frac{ar}{q} + \frac{\theta r}{q^2} = \frac{ar}{q} + \frac{\theta'}{2q}.$$

Thus using that $||\alpha + \beta|| \leq ||\alpha|| + ||\beta||$ for all real numbers α and β,

$$\begin{aligned} ||\alpha r|| &= \left|\left|\frac{ar}{q} + \frac{\theta'}{2q}\right|\right| = \left|\left|m(r) \pm \frac{s(r)}{q} + \frac{\theta'}{2q}\right|\right| \\ &= \left|\left|\frac{s(r)}{q} \pm \frac{\theta'}{2q}\right|\right| \geq \left|\left|\frac{s(r)}{q}\right|\right| - \left|\left|\frac{\theta'}{2q}\right|\right| \\ &\geq \frac{s(r)}{q} - \frac{1}{2q}. \end{aligned}$$

Let $1 \leq r_1 \leq r_2 \leq \frac{q}{2}$. We note that $s(r_1) = s(r_2)$ only if $r_1 \equiv r_2 \mod q$ and hence $s(r_1) = s(r_2)$ only if $r_1 = r_2$. Therefore it follows that

$$\left\{ \left|\left|\frac{ar}{q}\right|\right| : 1 \leq r \leq \frac{q}{2} \right\} = \left\{ \frac{s(r)}{q} : 1 \leq r \leq \frac{q}{2} \right\} = \left\{ \frac{s}{q} : 1 \leq s \leq \frac{q}{2} \right\}.$$

Hence the claim of the lemma follows as,

$$\begin{aligned} \sum_{1 \leq r \leq \frac{q}{2}} \frac{1}{||\alpha r||} &\leq \sum_{1 \leq r \leq \frac{q}{2}} \frac{1}{\frac{s(r)}{q} - \frac{1}{2q}} = \sum_{1 \leq s \leq \frac{q}{2}} \frac{1}{\frac{s}{q} - \frac{1}{2q}} \\ &= 2q \sum_{1 \leq s \leq \frac{q}{2}} \frac{1}{2s - 1} \leq 2q \sum_{1 \leq s \leq \frac{q}{2}} \frac{1}{s} \\ &\leq 2q \left(1 + \int_1^{\frac{q}{2}} \frac{1}{x}\, dx \right) = 2q(1 + \log q) \\ &\leq 3q \log q. \end{aligned}$$

□

Lemma 6.6. *Assume that α is a real number that has a rational approximation $\frac{a}{q}$ for coprime $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ that satisfies*

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q^2}.$$

Then for any non-negative real number $P \geq q$ and non-negative integer h, we have

$$\sum_{r=1}^{q} \min\left(P, \frac{1}{||\alpha(hq + r)||} \right) \leq 9(P + q \log q).$$

Proof. Write again $\alpha = \frac{a}{q} + \frac{\theta}{q^2}$ for $|\theta| \leq 1$. Then

$$\begin{aligned} \alpha(hq + r) &= ah + \frac{ar}{q} + \frac{\theta h}{q} + \frac{\theta r}{q^2} \\ &= ah + \frac{ar}{q} + \frac{[\theta h] + \{\theta h\}}{q} + \frac{\theta r}{q^2} = ah + \frac{ar + [\theta h] + \delta(r)}{q} \end{aligned}$$

for $-1 \leq \delta(r) = \{\theta h\} + \frac{\theta r}{q} < 2$.

For each $r = 1, \ldots, q$ there is a unique integer r' so that

$$\{\alpha(hq + r)\} = \frac{ar + [\theta h] + \delta(r)}{q} - r'.$$

Let $0 \leq t \leq 1 - \frac{1}{q}$. If $t \leq \{\alpha(hq+r)\} \leq t + \frac{1}{q}$, then $qt \leq ar - qr' + [\theta h] + \delta(r) \leq qt + 1$. This shows that

$$ar - qr' \leq qt - [\theta h] + 1 - \delta(r) \leq qt - [\theta h] + 2$$

and

$$ar - qr' \geq qt - [\theta h] - \delta(r) > qt - [\theta h] - 2.$$

It follows that $ar - qr'$ lies in the half-open interval J of length 4, where

$$J = (qt - [\theta h] - 2, qt - [\theta h] + 2].$$

If $1 \leq r_1 \leq r_2 \leq q$ and $ar_1 - qr_1' = ar_2 - qr_2'$ then $ar_1 = ar_2 \mod q$ and so $r_1 = r_2$. Thus it follows that for any $t \in [0, \frac{q-1}{q}]$, there are at most four integers $r \in [1, q]$ so that $\{\alpha(hq + r)\} \in [t, t + \frac{1}{q}]$.

Next we note that $||\alpha(hq + r)|| \in [t, t + \frac{1}{q}]$ if and only if either $\{\alpha(hq + r)\} \in [t, t + \frac{1}{q}]$ or $1 - \{\alpha(hq + r)\} \in [t, t + \frac{1}{q}]$. The second inclusion is equivalent to $\{\alpha(hq + r)\} \in [t', t' + \frac{1}{q}]$ for $0 \leq t' = 1 - \frac{1}{q} - t \leq \frac{1}{q}$. To summarize, it follows that for every $t \in [1, \frac{q-1}{q}]$, there are at most eight integers $r \in [1, q]$ for which $||\{\alpha(hq+r)\}|| \in [t, t + \frac{1}{q}]$. In conclusion, if we set $J(s) = [\frac{s}{q}, \frac{s+1}{q}]$ for $s = 0, 1, \ldots$, then $||\alpha(hq + r)|| \in J(s)$ for at most eight $r \in [1, q]$.

This observation implies the estimate. More precisely, if $||\alpha(hq + r)|| \in J(0)$, then we use the inequality

$$\min\left(P, \frac{1}{||\alpha(hq + r)||}\right) \leq P.$$

If $||\alpha(hq + r)|| \in J(s)$ for $s \geq 1$, then

$$\min\left(P, \frac{1}{||\alpha(hq + r)||}\right) \leq \frac{q}{s}.$$

As $||\alpha(hq + r)|| \in J(s)$ for some $s \leq \frac{q}{2}$, it follows that

$$\sum_{1 \leq r \leq q} \min\left(P, \frac{1}{||\alpha(hq + r)||}\right) \leq 8P + 8 \sum_{1 \leq s < \frac{q}{2}} \frac{q}{s} \leq 9(P + q \log q).$$

$\square$

The first major result of this subchapter is Weyl's Inequality.

Theorem 6.7. *(Weyl's Inequality) Assume that α is a real number that has a rational approximation $\frac{a}{q}$ for coprime $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ that satisfies*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

Then for any $\varepsilon > 0$ *and* $K = 2^{k-1}$*,*

$$\left|\sum_{x=1}^{P} e(f(x))\right| \ll_{k,\varepsilon} P^{1+\varepsilon}(P^{-1} + q^{-1} + P^{-k}q)^{\frac{1}{K}}.$$

Proof. We assume $q \leq P^k$ as otherwise the result follows from the trivial bound. Applying Proposition 6.1 and Lemma 6.2, yields

$$\begin{aligned}\left|\sum_{x=1}^{P} e(f(x))\right|^K &\ll_k P^{K-1} + P^{K-k} \sum_{y_1,\dots y_{k-1}=1}^{P} |S_1(\triangle_{y_1,\dots,y_{k-1}} f(x))| \\ &\ll_k P^{K-1} + P^{K-k} \sum_{y_1,\dots y_{k-1}=1}^{P} |S_1(k!\alpha y_1 \dots y_{k-1} x)| \\ &\ll_k P^{K-1} + P^{K-k} \sum_{m=1}^{k!P^{k-1}} \min(P, ||\alpha m||^{-1}),\end{aligned}$$

where we used in the last line Lemma 6.3 together with the trivial estimate $\leq P$. The task at hand is now to estimate the last term by using the Diophantine condition on α.

The sum over m is divided into blocks of q consecutive terms so that the number of such blocks is $\ll_k \frac{P^{k-1}}{q} + 1$. We only consider the sum over any such block, which will be of the form

$$\sum_{r=0}^{p} \min\left(P, \frac{1}{||\alpha(hq+r)||}\right)$$

for h some non-negative integer. Using Lemma 6.6 the claim of the theorem follows:

$$\begin{aligned}\left|\sum_{x=1}^{P} e(f(x))\right|^K &\ll_k P^{K-1} + P^{K-k} \sum_{m=1}^{k!P^{k-1}} \min(P, ||\alpha m||^{-1}), \\ &\ll_k P^{K-1} + P^{K-k}\left(\frac{P^{k-1}}{q} + 1\right)(P + q\log q) \\ &\ll_{k,\varepsilon} P^{K-1} + P^{K-k+\varepsilon}\left(\frac{P^{k-1}}{q} + 1\right)(P + q) \\ &\ll_{k,\varepsilon} P^{K-1} + P^{K-k+\varepsilon}\left(\frac{P^{k}}{q} + P^{k-1} + P + q\right) \\ &\ll_{k,\varepsilon} P^{K-1} + P^{K-k+\varepsilon}\left(\frac{P^{k}}{q} + P^{k-1} + q\right) \\ &\ll_{k,\varepsilon} P^{K+\varepsilon}(P^{-1} + q^{-1} + P^{-k}q),\end{aligned}$$

where we used that as $q \leq P^k$, we have $\log q \ll_\varepsilon P^\varepsilon$. □

Theorem 6.8. *(Hua's Inequality) For* $k \geq 1$ *and* $\alpha \in \mathbb{R}$*, consider*

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k).$$

Then

$$\int_0^1 |T(\alpha)|^{2^k}\, d\alpha \ll_{k,\varepsilon} P^{2^k-k+\varepsilon}.$$

Proof. Denote for $\nu = 1, \ldots, k$ by

$$I_\nu = \int_0^1 |T(\alpha)|^{2^\nu}\, d\alpha.$$

We show by induction the claim

$$I_\nu \ll_{k,\nu,\varepsilon} P^{2^\nu-\nu+\varepsilon}$$

for all $\nu = 1, \ldots, k$.

The case $\nu = 1$ is straightforward, as

$$I_1 = \int |T(\alpha)|^2\, d\alpha = \sum_{x_1,x_2=1}^{P} \int_0^1 e(\alpha(x_1^k - x_2^k))\, d\alpha = P.$$

Next assume that the claim holds for $1 \le \nu \le k-1$ and we want to prove the claim for $\nu+1$. As in the proof of Lemma 6.2, it follows

$$|T(\alpha)|^{2^\nu} \ll_\nu P^{2^\nu-1} + P^{2^\nu-\nu-1}\mathrm{Re}\left(\sum_{y_1,\ldots,y_\nu=1}^{P} S_{k-\nu}\right)$$

for

$$S_{k-\nu} = \sum_x e(\alpha\triangle_{y_1,\ldots,y_\nu}(x^k))$$

where x ranges in an interval depending on $y_1, \ldots, y_\nu$ yet contained in $[1, P]$.

Multiplying both sides of the inequality by $|T(\alpha)|^{2^\nu}$ and integrating, it follows

$$I_{\nu+1} \ll_\nu P^{2^\nu-1} I_\nu + P^{2^\nu-\nu-1} \sum_{y_1,\ldots,y_\nu} \mathrm{Re}\left(\int_0^1 S_{k-\nu}|T(\alpha)|^{2^\nu}\, d(\alpha)\right).$$

Notice that the last integral is of the form

$$\begin{aligned}
&\int_0^1 \sum_x e(\alpha\triangle_{y_1,\ldots,y_\nu}(x^k))T(\alpha)^{2^{\nu-1}}\overline{T(\alpha)}^{2^{\nu-1}}\, d\alpha \\
&= \int_0^1 \sum_x e(\alpha\triangle_{y_1,\ldots,y_\nu}(x^k)) \sum_{\substack{u_1,\ldots,u_{2^{\nu-1}}\\ v_1,\ldots,v_{2^{\nu-1}}}} e(\alpha u_1^k + \ldots + \alpha u_{2^{\nu-1}}^k)e(-\alpha v_1^k - \ldots - \alpha v_{2^{\nu-1}}^k)\, d(\alpha),
\end{aligned}$$

where the u_i and v_i go from 1 to P. The latter integral is equal to the number of solutions of

$$\triangle_{y_1,\ldots,y_\nu}(x^k) + u_1^k + \ldots + u_{2^{\nu-1}}^k - v_1^k - \ldots - v_{2^{\nu-1}}^k = 0.$$

Denote by N the number of solutions for all possible values of $y_1, \ldots, y_\nu$. Then

$$I_{\nu+1} \ll_\nu P^{2^\nu-1} I_\nu + P^{2^\nu-\nu-1} N.$$

We next estimate N. As the $y_1, \ldots, y_\nu$ range over $[1, P]$ they are positive and as x is also positive, it follows that $\triangle_{y_1,\ldots,y_\nu}(x^k) > 0$. Also, the latter number is divisible by $y_1, \ldots, y_v$. Fix for the moment $u_1, \ldots, u_{2^{\nu-1}}$ and $v_1, \ldots, v_{2^{\nu-1}}$. Then the corresponding sum $u_1^k + \ldots - v_1^k - \ldots$ is contained in $[-2^\nu P^k, 2^\nu P^k]$. Since each y_i divides the latter sum, we can only choose y_i in the set of divisors of the latter sum which satisfies by Lemma 6.4 $\ll_{k,\varepsilon} P^\varepsilon$. So there are only $\ll_{k,\nu,\varepsilon} P^\varepsilon$ many possibilities for $y_1, \ldots, y_\nu$. Furthermore, since $\triangle_{y_1,\ldots,y_\nu}(x^k)$ is strictly increasing in x as $\nu \leq k-1$ there is at most one possibility for x. As the number of possibilities for u_i and v_i is $\ll P^{2^\nu}$ it follows that

$$N \ll_{k,\nu,\varepsilon} P^{2^\nu + \nu\varepsilon}.$$

Combining all this, it follows that

$$I_{\nu+1} \ll_{k,\nu,\varepsilon} P^{2^\nu - 1} P^{2^\nu - \nu + \varepsilon} + P^{2^\nu - \nu - 1} P^{2^\nu - \nu\varepsilon} \ll_{k,\nu,\varepsilon} P^{2^{\nu+1} - (\nu+1) + \nu\varepsilon}.$$

□

6.2 The Singular Series

For $a, q \in \mathbb{N}$ with $(a, q) = 1$ and $m \geq 1$ we define

$$S_{a,q} = \sum_{z=1}^{q} e\left(\frac{az^k}{q}\right), \qquad A_m(q) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{S_{a,q}}{q}\right)^n e\left(-\frac{am}{q}\right).$$

Using this notation, we define the **singular series** for $m \geq 1$ as

$$\sigma_{k,n}(m) = \sum_{q=1}^{\infty} A_m(q) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{S_{a,q}}{q}\right)^n e\left(-\frac{am}{q}\right).$$

We also introduce the notation for $Q \geq 1$,

$$\sigma_{k,n}(Q, m) = \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{S_{a,q}}{q}\right)^n e\left(-\frac{am}{q}\right).$$

As a consequence of Weyl's inequality (Theorem 6.7) we prove the first lemma.

Lemma 6.9. *For $k \geq 2$ and $a, q \in \mathbb{N}$ with $(a, q) = 1$,*

$$S_{a,q} \ll_{k,\varepsilon} q^{1 - \frac{1}{K} + \varepsilon}$$

for $K = 2^{k-1}$. Moreover, for $n \geq 2^k + 1$ the singular series converges absolutely.

Proof. To bound $S_{a,q}$ we notice that the assumptions for Weyl's inequality are clearly satisfied. Thus

$$\begin{aligned} S_{a,q} &\ll_{k,\varepsilon} q^{1+\varepsilon}(q^{-1} + q^{-1} + q^{-k} q)^{\frac{1}{K}} \\ &\ll_{k,\varepsilon} q^{1+\varepsilon}(q^{-1})^{\frac{1}{K}} = q^{1 - \frac{1}{K} + \varepsilon}. \end{aligned}$$

Using this estimate, we bound the singular series:

$$|\sigma_{k,n}(m)| \ll_{k,\varepsilon} \sum_{q=1}^{\infty} \sum_{\substack{a=1\\(a,q)=1}}^{q} |q^{-1}S_{a,q}|^n$$
$$\ll_{k,\varepsilon} \sum_{q=1}^{\infty} \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-\frac{n}{K}+\varepsilon} \ll_{k,\varepsilon} \sum_{q=1}^{\infty} q^{1-\frac{n}{K}+\varepsilon} < \infty,$$

for suitable ε where we used the assumption that $1 - \frac{n}{K} < -1$ as $n > 2^k$. $\square$

We next investigate multiplicative properties of the expressions $S_{a,q}$ and $A_m(q)$.

Lemma 6.10. *Let $b, r \in \mathbb{N}$ so that $(q, r) = 1$. Then*

$$S_{qr,ar+bq} = S_{q,a}S_{r,b}.$$

Proof. By the Chinese remainder theorem, since $(q, r) = 1$, every congruence class of qr can be written uniquely in the form $xr + yq$ for $1 \le x \le q$ and $1 \le y \le r$. Thus it follows that

$$\begin{aligned}
S_{qr,ar+br} &= \sum_{z=1}^{qr} e\left(\frac{(ar+bq)z^k}{qr}\right) = \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{(ar+bq)(xr+yq)^k}{qr}\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{(ar+bq)}{qr}\sum_{\ell=0}^{k}\binom{k}{\ell}(xr)^{\ell}(yq)^{k-\ell}\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{(ar+bq)}{qr}((xr)^k + (yq)^k)\right) \\
&= \sum_{x=1}^{q}\sum_{y=1}^{r} e\left(\frac{a(xr)^k}{q}\right) e\left(\frac{b(yq)^k}{r}\right) \\
&= \sum_{x=1}^{q} e\left(\frac{ax^k}{q}\right)\sum_{y=1}^{r} e\left(\frac{by^k}{q}\right) = S_{q,a}S_{r,b}.
\end{aligned}$$

$\square$

Lemma 6.11. *If $(q, r) = 1$, then*

$$A_m(qr) = A_m(q)A_m(r).$$

Proof. If $(c, qr) = 1$, then c is congruent modulo qr to a number of the form

$ar + bq$ where $(a,q) = (b,r) = 1$. Thus by the last lemma it follows that

$$\begin{aligned} A_m(qr) &= \sum_{\substack{c=1 \\ (c,qr)=1}}^{qr} \left(\frac{S_{qr,c}}{qr}\right)^n e\left(-\frac{cm}{qr}\right) \\ &= \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ (b,r)=1}}^{r} \left(\frac{S_{qr,ar+bq}}{qr}\right)^n e\left(-\frac{(ar+bq)m}{qr}\right) \\ &= \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ (b,r)=1}}^{r} \left(\frac{S_{q,a}}{q}\right)^n \left(\frac{S_{r,b}}{r}\right)^n e\left(-\frac{am}{q}\right) e\left(-\frac{bm}{r}\right) \\ &= A_m(q)A_m(r). \end{aligned}$$

□

For fixed m and for a prime number p we denote by $M_m(q)$ the number of solutions to the congruence

$$x_1^k + \ldots + x_n^k \equiv m \mod q$$

for integers $1 \le x_i \le q$. For a prime p, we set

$$\sigma_p = \lim_{\ell \to \infty} \frac{M_m(p^\ell)}{p^{\ell(n-1)}}.$$

Lemma 6.12. *Let $n \ge 2^k + 1$. For every prime p, it holds*

$$\sigma_p = 1 + \sum_{\ell=1}^{\infty} A_m(p^\ell).$$

Proof. We first check that the right hand side converges. To see this we use again $S_{a,q} \ll_{k,\varepsilon} q^{1-\frac{1}{K}+\varepsilon}$ and hence

$$A_m(q) \ll_{k,\varepsilon} \frac{q}{q^{\frac{n}{K}-n\varepsilon}} \le \frac{1}{q^{1+\delta(k)}}$$

for ε small enough. This clearly shows that the right hand side converges.
Next notice that if $(a,q) = d$, then

$$\begin{aligned} S_{a,q} &= \sum_{x=1}^{q} e\left(\frac{ax^k}{q}\right) = \sum_{x=1}^{q} e\left(\frac{(a/d)x^k}{q/d}\right) \\ &= d\sum_{x=1}^{q/d} e\left(\frac{(a/d)x^k}{q/d}\right) = dS_{q/d,a/d}. \end{aligned}$$

Recall that the geometric series implies

$$\frac{1}{q}\sum_{a=1}^{q} e\left(\frac{am}{q}\right) = \begin{cases} 1 & \text{if } m \equiv 0 \mod q, \\ 0 & \text{if } m \not\equiv 0 \mod q. \end{cases}$$

Thus for any integers $x_1, \ldots, x_n$ it follows

$$\frac{1}{q}\sum_{a=1}^{q} e\left(\frac{a(x_1^k+\ldots+x_n^k-m)}{q}\right) = \begin{cases} 1 & \text{if } x_1^k+\ldots+x_n^k \equiv m \mod q, \\ 0 & \text{if } x_1^k+\ldots+x_n^k \not\equiv m \mod q. \end{cases}.$$

With this observation, we can write

$$\begin{aligned} M_m(q) &= \sum_{x_1=1}^{q} \cdots \sum_{x_n=1}^{q} \frac{1}{q}\sum_{a=1}^{q} e\left(\frac{a(x_1^k+\ldots+x_n^k-m)}{q}\right) \\ &= \frac{1}{q}\sum_{a=1}^{q}\sum_{x_1=1}^{q} \cdots \sum_{x_n=1}^{q} e\left(\frac{ax_1^k}{q}\right)\cdot \ldots \cdot e\left(\frac{ax_n^k}{q}\right) e\left(\frac{-am}{q}\right) \\ &= \frac{1}{q}\sum_{a=1}^{q} S_{q,a}^n e\left(\frac{-am}{q}\right) \\ &= \frac{1}{q}\sum_{d\mid q}\sum_{\substack{a=1 \\ (a,q)=d}}^{q} d^n S_{q/d,a/d}^n e\left(\frac{-(a/d)m}{(q/d)}\right) \\ &= \frac{1}{q}\sum_{d\mid q}\sum_{\substack{a=1 \\ (a,q)=d}}^{q} q^n \left(\frac{S_{q/d,a/d}}{q/d}\right)^n e\left(\frac{-(a/d)m}{(q/d)}\right) \\ &= q^{n-1}\sum_{d\mid q} A_m(q/d). \end{aligned}$$

In particular,

$$\sum_{d\mid q} A_m(q/d) = q^{1-n} M_m(q)$$

for all $q \geq 1$ and so for $q = p^\ell$,

$$1 + \sum_{j=1}^{\ell} A_m(p^j) = \sum_{d\mid p^\ell} A_m(p^\ell/d) = p^{\ell(1-n)} M_m(p^\ell),$$

which implies the claim as $k \to \infty$. □

Corollary 6.13. *For $n \geq 2^k+1$, it holds that*

$$\sigma_{k,n}(m) = \prod_{p \text{ prime}} \sigma_p.$$

Proof. This follows immediately by the last lemma and since $A_m(q)$ is multiplicative for coprime numbers. Hence

$$\sigma_{k,n}(m) = \sum_{q=1}^{\infty} A_m(q) = \prod_{p \text{ prime}} \left(1 + \sum_{\ell=1}^{\infty} A_m(p^\ell)\right) = \prod_{p \text{ prime}} \sigma_p.$$

□

Corollary 6.14. *If $n \geq 2^k + 1$, there exists a prime $p_0 = p_0(k)$ so that*

$$\frac{1}{2} \leq \prod_{p > p_0} \sigma_p \leq \frac{3}{2}.$$

Proof. We already know

$$|A_m(q)| \ll_k q^{-1-\delta(k)}$$

for $\delta = \delta(k)$. This implies

$$|\sigma_p - 1| \ll_k \sum_{\ell=1}^{\infty} p^{-\ell(1+\delta)} \ll_k p^{-(1+\delta)}.$$

In particular, there is a constant $c = c(k, s)$ so that

$$1 - \frac{c}{p^{1+\delta}} \leq \sigma_p \leq 1 + \frac{c}{p^{1+\delta}}$$

for all p. Thus the claim of the lemma follows if we establish that the product

$$\prod_{p > p_0} \left(1 \pm \frac{c}{p^{1+\delta}}\right)$$

converges. To see this just apply the logarithm and recall that $\ln(1 + x) \leq x$ so that

$$\ln\left(\prod_p 1 + \frac{c}{p^{1+\delta}}\right) = \sum_p \ln\left(1 + \frac{c}{p^{1+\delta}}\right) \leq \sum_p \frac{c}{p^{1+\delta}} < \infty.$$

□

The last corollary implies that $\sigma_{k,n}(m)$ is bounded from above independently of m. Towards proving that the singular series is bounded from below, we discuss some congruence lemmas. For the moment fix a prime p and write

$$k = p^{\tau} k_0$$

with $(k_0, p) = 1$. Then define

$$\gamma = \begin{cases} \tau + 1 & \text{if } p > 2, \\ \tau + 2 & \text{if } p = 2. \end{cases}$$

Lemma 6.15. *Let m be an integer not divisible by p. If the congruence*

$$x^k \equiv m \mod p^{\gamma}$$

is solvable, then the congruence

$$y^k \equiv m \mod p^h$$

is solvable for every $h \geq \gamma$.

Before proving the lemma, we prove the claim that if $a, b, c \in \mathbb{Z}$ are non-zero integers and $a \equiv 0 \bmod (b, c)$ then there is an integers ℓ so that $b\ell \equiv a \bmod c$. To see this denote by d the integer with the property $a = d(b, c)$. As $\frac{b}{(b,c)}$ is coprime to c, on concludes,

$$a \equiv d(b,c)\frac{b}{(b,c)}\left(\frac{b}{(b,c)}\right)^{-1} \equiv bd\left(\frac{b}{(b,c)}\right)^{-1} \mod c,$$

which proves the claim.

Proof. Denote by $\varphi(n)$ the Euler function so that $\varphi(p^h) = (p-1)p^{h-1}$. Assume first that p is an odd prime. Then for $h \geq \gamma = \tau + 1$, it holds

$$(k, \varphi(p^h)) = (k, (p-1)p^{h-1}) = (k, (p-1)p^{\tau}) = (k, \varphi(p^{\gamma})).$$

Recall that as p is odd, the group $(\mathbb{Z}/p^h\mathbb{Z})^{\times}$ is cyclic and it consists precisely of all congruence classes that are relatively prime to p and hence has order $\varphi(p^h) = (p-1)p^{h-1}$. Let g be a generator of this cyclic group, then g is a primitive root modulo p^h and hence also a primitive root modulo p^{γ}. If $x^k \equiv m \mod p^{\gamma}$ then $(x, p) = 1$ and hence we can choose integers r and u so that

$$x \equiv g^u \mod p^h \quad \text{and} \quad m = g^r \mod p^h.$$

Then

$$ku \equiv r \mod \varphi(p^{\gamma})$$

and

$$r \equiv 0 \mod (k, \varphi(p^{\gamma})) \quad \text{and} \quad r \equiv 0 \mod (k, \varphi(p^h)).$$

Hence, by the argument before the proof, there exists an integer v so that

$$kv \equiv r \bmod \varphi(p^h).$$

Then setting $y = g^v$ proves the claim.

Now assume $p = 2$ so that m and x are odd. If $\tau = 0$, then k is odd. As y runs through the odd congruence classes of 2^h then so does y^k as otherwise one derives a solution to the equation $y^k \equiv 0 \mod 2^h$ which cannot exist. Hence the congruence $y^k \equiv m \mod 2^h$ is solvable for all $h \geq 1$ and any odd m without any hypothesis. If $\tau \geq 1$, then k is even and $m \equiv x^k \equiv 1 \mod 4$. Also $x^k = (-x^k)$ and hence we can assume without loss of generality that $x \equiv 1 \mod 4$. The congruence classes modulo 2^h that are congruent to 1 modulo 4 form a cyclic subgroup of order 2^{h-2} and 5 is a generator of this subgroup. Then choose integers r and u so that

$$m \equiv 5^r \mod 2^h \quad \text{and} \quad x \equiv 5^u \mod 2^h.$$

Then $x^k \equiv m \mod 2^{\gamma}$ implies

$$ku \equiv r \mod 2^{\gamma-2}.$$

So r is divisible by $(k, 2^{\tau}) = 2^{\tau} = (k, 2^{h-2})$. It follows analogously to before that there exists an integer v so that

$$kv \equiv r \mod 2^{h-2}$$

which again implies the claim by setting $y = 5^v$. □

Lemma 6.16. *Let p be a prime number. If there exist integers $a_1, \ldots, a_n$ not all divisible by p so that*

$$a_1^k + \ldots + a_n^k \equiv m \mod p^\gamma$$

then

$$\sigma_p \geq p^{\gamma(1-n)} > 0.$$

Proof. Suppose that $a_1 \not\equiv 0 \mod p$. Let $h > \gamma$. For each $i = 2, \ldots, n$ there exist $p^{h-\gamma}$ pairwise incongruent integers x_i so that

$$x_i \equiv a_i \mod p^h.$$

As the congruence

$$x_1^k \equiv m - x_2^k - \ldots - x_n^k \mod p^\gamma$$

is solvable with $x_1 = a_1 \not\equiv 0$, it follows by Lemma 6.15 that the congruence

$$x_1^k \equiv m - x_2^k - \ldots - x_n^k \mod p^h$$

is solvable. In particular this implies that

$$M_m(p^h) \geq p^{(h-\gamma)(n-1)}$$

and so

$$\sigma_p = \lim_{\ell \to \infty} \frac{M_m(p^\ell)}{p^{\ell(n-1)}} \geq \frac{1}{p^{\gamma(n-1)}} > 0.$$

□

Lemma 6.17. *Assume $n \geq 2k$ for k odd or $n \geq 4k$ for k even, then*

$$\sigma_p \geq p^{\gamma(1-n)} > 0$$

Proof. By the last lemma, it suffices to show that the congruence

$$a_1^k + \ldots + a_n^k \equiv m \mod p^\gamma$$

has a solution in integers a_i not all divisible by p. The proof has similarity to previous arguments and is omitted here. See chapter 5.7 of [Nat96]. □

Combining all this, the following result is readily implied.

Theorem 6.18. *Let $n \geq 2^k + 1$. There exist positive constants $C_1 = C_1(k, s)$ and $C_2 = C_2(k, s)$ only depending on k and s so that*

$$C_1 < \sigma_{k,n}(m) < C_2$$

for all m. Moreover, there is some $\delta > 0$ so that for sufficiently large m,

$$\sigma_{k,n}(P^\nu, m) = \sigma_{k,n}(m) + O_{k,n}(P^{-\nu\delta})$$

for $\nu > 0$.

Proof. In the proof of Lemma 6.9 it was shown that $\sigma_{k,n}(m) \ll_{k,n} 1$. To prove the a lower bound on the singular series we combine Lemma 6.14 and Lemma 6.17 to deduce

$$\sigma_{k,n}(m) = \prod_p \sigma_p > \frac{1}{2} \prod_{p \le p_0} \sigma_p \ge \frac{1}{2} \prod_{p \le p_0} p^{\gamma(1-n)} > 0.$$

To prove the last claim, just choose $\delta > 0$ so that $A_m(q) \ll_{k,n} \frac{1}{q^{1+\delta}}$. Then

$$\sigma_{k,n}(m) - \sigma_{k,n}(P^\nu, m) = \sum_{q > P^\nu} A_m(q) \ll_{k,n} \sum_{q > P^\nu} \frac{1}{q^{1+\delta}} \ll_{k,n} P^{-\nu\delta}.$$

□

6.3 Major and Minor Arcs

Throughout this chapter fix some δ small, $P \ge 2$ and $k \ge 2$. Around every rational number $\frac{a}{q}$ in its lowest terms, we consider

$$\mathfrak{M}_{a,q} = \left\{ \alpha \in [0,1] \,:\, \left| \alpha - \frac{a}{q} \right| < P^{-k+\delta} \right\}.$$

Moreover we set

$$\mathfrak{M} = \bigcup_{1 \le q \le P^\delta} \bigcup_{\substack{1 \le a \le q \\ (a,q)=1}} \mathfrak{M}_{a,q}$$

and call the latter set the **major arc**. The intervals are contained in $[0,1]$, yet we think of the point 1 as the same point as 0.

We claim that the intervals $\mathfrak{M}_{a,q}$ in the definition of $\mathfrak{M}$ are disjoint. To see this assume for a contradiction that $\alpha \in \mathfrak{M}_{a,q} \cap \mathfrak{M}_{a',q'}$ for a, q and a', q' as in the definition of $\mathfrak{M}$ and with the assumption that $\frac{a}{q} \ne \frac{a'}{q'}$. Then $|aq' - a'q| \ge 1$ and

$$\frac{1}{P^{2\delta}} \le \frac{1}{qq'} \le \left| \frac{a}{q} - \frac{a'}{q'} \right| \le \left| \alpha - \frac{a}{q} \right| + \left| \alpha - \frac{a'}{q'} \right| \le \frac{2}{P^{k-\delta}},$$

which is a contradiction for $P \ge 2$ and $k \ge 2$.

The **minor arc** $\mathfrak{m}$ is defined as the complement of $\mathfrak{M}$ in $[0,1]$. As before we consider

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k).$$

The inequalities of Weyl and Hua readily imply the next claim.

Proposition 6.19. *If* $n \ge 2^k + 1$,

$$\int_{\mathfrak{m}} |T(\alpha)|^n \ll_{k,\delta} P^{n-k-\delta'},$$

for $\delta' > 0$ *only depending on* δ.

Before proving this proposition, we recall Dirichlet's classical result on Diophantine approximation.

Lemma 6.20. *(Dirichlet) Let α and Q be real numbers, $Q \geq 1$. Then there exist coprime integers a, q so that*

$$1 \leq q \leq Q$$

and

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

Proof. Let $N = [Q]$ and suppose that $\{q\alpha\} \in [0, \frac{1}{N+1})$ for some positive integer $q \leq N \leq Q$. If $a = [q\alpha]$ then $0 \leq \{q\alpha\} \leq q\alpha - [q\alpha] = q\alpha - a < \frac{1}{N+1}$ and so

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q(N+1)} \leq \frac{1}{qQ}.$$

A similar argument also works if $\{q\alpha\} \in [\frac{N}{N+1}, 1)$ for $q \leq N \leq Q$. Namely, if so, then set $a = [q\alpha] + 1$ so that

$$\frac{N}{N+1} < \{q\alpha\} = q\alpha - a + 1 < 1.$$

This implies that

$$|q\alpha - a| \leq \frac{1}{N+1}$$

and hence the claim.

Finally if $\{q\alpha\} \in [\frac{1}{N+1}, \frac{N}{N+1})$ for all $q = 1, \ldots N$, then each of the N numbers $\{q\alpha\}$ lie in one of the $N-1$ intervals $[\frac{i}{N+1}, \frac{i+1}{N+1})$ for $i = 1, \ldots, N-1$. Thus there exists $1 \leq i \leq N-1$ and $1 \leq q_1 \leq q_2 \leq N$ so that

$$\{q_1\alpha\}, \{q_2\alpha\} \in \left[\frac{i}{N+1}, \frac{i+1}{N+1}\right).$$

Then choose

$$q = q_2 - q_1 \in [1, N-1], \qquad \text{and} \qquad a = [q_2\alpha] - [q_1\alpha]$$

and observe finally,

$$|q\alpha - a| = |(q_2\alpha - [q_2\alpha]) - (q_1\alpha - [q_1\alpha])| = |\{q_2\alpha\} - \{q_1\alpha\}| < \frac{1}{N+1} < \frac{1}{Q}.$$

□

Proof. (of Proposition 6.19) By Lemma 6.20, every α has a rational approximation $\frac{a}{q}$ with $(a, q) = 1$ and

$$1 \leq q \leq P^{k-\delta} \qquad \text{and} \qquad \left|\alpha - \frac{a}{q}\right| < q^{-1}P^{-k+\delta}.$$

Moreover we can choose $1 \leq a \leq q$ whenever $0 < \alpha < 1$.

As the last inequality is stronger than the one in the definition of $\mathfrak{M}_{a,q}$, it follows that $\alpha \in \mathfrak{M}_{a,q}$ if $q \leq P^\delta$. Hence if $\alpha \in \mathfrak{m}$, it follows $q > P^\delta$. As in that case $|\alpha - \frac{a}{q}| < q^{-2}$ we can apply Weyl's inequality (Theorem 6.7) to $T(\alpha)$ and as $\frac{P^k}{q} \geq P^\delta$, it follows

$$|T(\alpha)| \ll_{k,\varepsilon} P^{1+\varepsilon-\frac{\delta}{K}}$$

for $K = 2^{k-1}$. Then using Hua's inequality (Theorem 6.8), it follows as $n \geq 2^k - 1$

$$\begin{aligned}\int_{\mathfrak{m}} |T(\alpha)|^n \, d\alpha &= \int_{\mathfrak{m}} |T(\alpha)|^{n-2^k} |T(\alpha)|^{2^k} \\ &\ll_{k,\varepsilon} P^{(n-2^k)(1+\varepsilon+\frac{\delta}{K})} \int_0^1 |T(\alpha)|^{2^k} \, d\alpha \\ &\ll_{k,\varepsilon,\varepsilon'} P^{(n-2^k)(1+\varepsilon+\frac{\delta}{K})} P^{2^k-k+\varepsilon'} \\ &\ll_{k,\varepsilon,\varepsilon'} P^{n-k+n(\varepsilon+\frac{\delta}{K})-2^k(\varepsilon+\frac{\delta}{K})+\varepsilon'} \ll_{k,\varepsilon} P^{n-k-\delta'}\end{aligned}$$

for a suitably chosen δ'. □

We next study the major arc. In order to do so we recall the notation

$$S_{a,q} = \sum_{z=1}^{q} e\left(\frac{az^k}{q}\right)$$

and introduce for $c \in \mathbb{R}$,

$$I(c) = \int_0^P e(cx^k)\, dx.$$

Lemma 6.21. *For $\alpha \in \mathfrak{M}_{a,q}$ setting $\alpha = c + \frac{a}{q}$, it holds*

$$T(\alpha) = q^{-1} S_{a,q} I(c) + O(P^{2\delta}).$$

Proof. We collect the values of x in the sum defining $T(\alpha)$ that are in the same residue class mod q. So set $x = qy + z$ for $1 \leq z \leq q$ and y runs through an interval depending on z which corresponds to $0 < x \leq P$. Thus

$$\begin{aligned}T(\alpha) &= \sum_{x=1}^{P} e(\alpha x^k) = \sum_{z=1}^{q} \sum_{y} e\left(\left(\frac{a}{q} + c\right)(qy+z)^k\right) \\ &= \sum_{z=1}^{q} e\left(\frac{az^k}{q}\right) \sum_{y} e(c(qy+z)^k).\end{aligned}$$

We next want to replace y by a continuous parameter. In order to so recall that for any differentiable function f on the interval $[A, B]$, it holds by using the mean value theorem for intervals of length 1,

$$\left| \int_A^B f(\eta)\, d\eta - \sum_{\substack{y \in \mathbb{Z} \\ A<y<B}} f(y) \right| \ll (B-A) \max_{x \in [A,B]} |f'(x)| + \max_{x \in [A,B]} |f(x)|.$$

Using this for the function $f(\eta) = e(c(q\eta + z)^k)$ on the interval $\eta \in [0, \frac{P}{q}]$ with the property

$$\max_{x\in[0,\frac{P}{q}]} |f'(x)| \ll q|c|P^{k-1} \quad \text{and} \quad \max_{x\in[0,\frac{P}{q}]} |f(x)| = 1$$

it follows that

$$\begin{aligned}|q^{-1}S_{a,q}I(c) - T(\alpha)| &= \left|\sum_{z=1}^{q} e\left(\frac{az^k}{q}\right) \cdot \left(q^{-1}\int_0^P e(cx^k)\,dx - \sum_y e(\beta)\right)\right| \\ &= \left|\sum_{z=1}^{q} e\left(\frac{az^k}{q}\right) \cdot \left(\int_0^{\frac{P}{q}} e(c(q\eta+z)^k)\,dx - \sum_y e(\beta)\right)\right| \\ &\ll q\left(\frac{P}{q}q|c|P^{k-1} + 1\right) \ll qP^\delta \ll P^{2\delta},\end{aligned}$$

where we used a substitution $x = q\eta + z$ in the second line and in the last line we used $|c| < P^{-k+\delta}$ and $q \ll P^\delta$. □

Recall the notation

$$\sigma_{k,n}(P^\delta, m) = \sum_{q\le P^\delta} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left(\frac{S_{a,q}}{q}\right)^n e\left(-\frac{am}{q}\right).$$

Moreover set

$$J(P^\delta) = \int_{|\gamma|<P^\delta} \left(\int_0^1 e(\gamma x^k)\,dx\right)^n e(-\gamma)\,d\gamma.$$

Proposition 6.22. *It holds,*

$$\int_{\mathfrak{M}} T(\alpha)^n e(-m\alpha)\,d\alpha = P^{n-k}\sigma_{k,n}(P^\delta, m)J(P^\delta) + O_{k,n}(P^{n-k-\delta'})$$

for some δ'.

Proof. Fix for the moment $a \le P^\delta$, q coprime to a and $\alpha = c + \frac{a}{q} \in \mathfrak{M}_{a,q}$ with $|c| < P^{-k+\delta}$. Then using $|q^{-1}S_{a,q}I(c)| \le P$, it follows by Lemma 6.21

$$T(\alpha)^n = (q^{-1}S_{a,q})^n I(c)^n + O_{k,n}(P^{n-1+2\delta}). \tag{6.1}$$

Multiplying by $e(-m\alpha)$ and integrating over $\mathfrak{M}_{a,q}$, i.e. over $|c| < P^{-k+\delta}$, the main term in the last expression gives

$$(q^{-1}S_{a,q})^n e\left(-\frac{am}{b}\right)\int_{|c|<P^{-k+\delta}} (I(c))^n e(-mc)\,dc.$$

Thus summing over all a and q in the definition of $\mathfrak{M}$ gives that the main term is

$$\sigma_{k,n}(P^\delta, m)\int_{|c|<P^{-k+\delta}} (I(c))^n e(-mc)\,dc.$$

We can replace in the integrand m by P^k only with a small error. Indeed, as $m - P^k \ll P^{k-1}$ it follows that

$$|e(-cm) - e(-cP^k)| \ll |c|P^{k-1} \ll P^{-1+\delta}$$

as $|c| < P^{-k+\delta}$. Thus the error in the integral is $\ll P^{-k+\delta}P^n P^{1-\delta}$. Using that trivially $\sigma_{k,n}(P^\delta, m) \leq P^{2\delta}$, this leads to the final error $P^{n-k-1+4\delta}$ and so is negligible. Thus the integral of the main term is up to a negligible error

$$\int_{|c|<P^{-k+\delta}} \left(\int_0^P e(cx^k)\, dx \right)^n e(-P^k c)\, dc = P^{n-k} J(P^\delta),$$

where we used the substitutions $x = Px'$ and $c = P^{-k}\gamma$. Thus the main term is of the form we desired.

It remains to deal with the error term of (6.1). Integrating over $|c| < P^{-k+\delta}$ it becomes $\ll P^{n-k-1+3\delta}$ and finally as summing over all a and q are $\ll P^{2\delta}$ summands, the error term is $\ll P^{n-k-1+5\delta}$, which implies the claim. □

6.4 The Asymptotic Formula for Waring's Problem

We proof the main theorem of this chapter. Recall

$$C_{k,n} = \frac{\Gamma(1 + \frac{1}{k})^n}{\Gamma(\frac{n}{k})}.$$

Theorem 6.23. *If $n \geq 2^k + 1$, the number $r_{k,n}(m)$ of representations of m as a sum of n positive integral k-th powers satisfies*

$$r_{k,n}(m) = C_{k,n}\sigma_{k,n}(m)m^{\frac{n}{k}-1} + O_{k,n}(m^{\frac{n}{k}-1-\delta'})$$

for some fixed $\delta' = \delta'(k,n) > 0$.

Proof. Recall that we fixed $P = [m^{\frac{1}{k}}]$ and

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k).$$

As discussed in the introduction to this chapter

$$r_{k,n}(m) = \int_0^1 T(\alpha)^n e(-\alpha m)\, d\alpha = \int_{\mathfrak{M}} T(\alpha)^n e(-\alpha m)\, d\alpha + \int_{\mathfrak{m}} T(\alpha)^n e(-\alpha m)\, d\alpha.$$

Using Proposition 6.19 and Proposition 6.22, it follows

$$r_{k,n}(m) = P^{n-k}\sigma_{k,n}(P^\delta, m)J(P^\delta) + O_{k,n}(P^{n-k-\delta'}). \tag{6.2}$$

As $P = [m^{\frac{1}{k}}]$, the error term is negligible and hence we can focus on the main term.

To analyze $J(P^\delta)$, we calculate by first performing the substitution $\xi = x^k$ and then replacing ξ by $\gamma\xi$,

$$\int_0^1 e(\gamma x^k)\, dx = k^{-1} \int_0^1 \xi^{-1+\frac{1}{k}} e(\gamma\xi)\, d\xi = k^{-1}\gamma^{-\frac{1}{k}} \int_0^\gamma \xi^{-1+\frac{1}{k}} e(\xi)\, d\xi.$$

We claim that the integral in the last expression $\int_0^\gamma \xi^{-1+\frac{1}{k}} e(\xi)\, d\xi$ is a bounded function in γ. To see this write $e(\xi) = e^{2\pi i \xi} = \cos(2\pi\xi) + i\sin(2\pi\xi)$ and note that $|\int_0^\gamma \cos(2\pi\xi)\, d\xi| \leq 10$ for all γ. As $\xi{-1} + \frac{1}{k}$ is a monotonically deceasing function, Dirichlet's criterion for the convergence of an integral applies. Thus it follows that

$$\left| \int_0^1 e(\gamma x^k)\, dx \right| \ll_k |\gamma|^{-\frac{1}{k}}.$$

Set

$$J_{k,n} = \int_{-\infty}^{\infty} \left(k^{-1} \int_0^1 \xi^{-1+\frac{1}{k}} e(\gamma\xi)\, d\xi \right)^n e(-\gamma)\, d\gamma.$$

Then using the last estimate it follows that

$$|J_{k,n} - J(P^\delta)| \ll_k \int_{|\gamma|>P^\delta} |\gamma|^{-\frac{n}{k}}\, d\gamma \ll_k P^{-\delta(\frac{n}{k}-1)}.$$

In the next lemma we will prove $J_{k,n} = C_{k,n}$. Also using Theorem 6.18, we conclude from (6.2) that

$$r_{k,n}(m) = C_{k,n} P^{n-k} \sigma_{k,n}(m) + O_{k,n}(P^{n-k-\delta'}).$$

Finally replacing P by $m^{\frac{1}{k}}$ has also negligible error and so the theorem follows. $\square$

Lemma 6.24. *In the notation of the proof of Theorem 6.23, $J_{k,n} = C_{k,n}$.*

Proof. Since we only care for the fact that $J_{k,n} > 0$, we only give a sketch of the proof. For more details, see [Dav05] and [Nat96]. Observe

$$\int_{-\lambda}^{\lambda} e(\mu\gamma)\, d\gamma = \frac{\sin 2\pi\lambda\mu}{\pi\mu}.$$

Using Fubini,

$$\begin{aligned}
k^n J_{k,n} &= \lim_{\lambda\to\infty} \int_{-\lambda}^{\lambda} \left(\int_0^1 \xi^{-1+\frac{1}{k}} e(\gamma\xi)\, d\xi \right)^n e(-\gamma)\, d\gamma \\
&= \lim_{\lambda\to\infty} \int_0^1 \dots \int_0^1 (\xi_1 \dots \xi_n)^{-1+\frac{1}{k}} \int_{-\lambda}^{\lambda} e(\gamma(\xi_1 + \dots + \xi_n - 1))\, d\gamma d\xi_1 \dots d\xi_n \\
&= \lim_{\lambda\to\infty} \int_0^1 \dots \int_0^1 (\xi_1 \dots \xi_n)^{-1+\frac{1}{k}} \frac{\sin 2\pi\lambda(\xi_1 + \dots + \xi_n - 1)}{\pi(\xi_1 + \dots + \xi_n - 1)} d\xi_1 \dots d\xi_n \\
&= \lim_{\lambda\to\infty} \int_0^n \dots \int_0^1 (\xi_1 \dots \xi_{n-1}(u - \xi_1 - \dots - \xi_{n-1}))^{-1+\frac{1}{k}} \frac{\sin 2\pi\lambda(u-1)}{\pi(u-1)} d\xi_1 \dots d\xi_{n-1} du \\
&= \lim_{\lambda\to\infty} \int_0^1 \phi(u) \frac{\sin 2\pi\lambda(u-1)}{\pi(u-1)}\, du,
\end{aligned}$$

where we used the substitution $u = \xi_1 + \dots + \xi_n$ and denote by ϕ the function

$$\phi(u) = \int_0^1 \dots \int_0^1 (\xi_1 \dots \xi_{n-1}(u - \xi_1 - \dots - \xi_{n-1}))^{-1+\frac{1}{k}}\, d\xi_1 \dots d\xi_{n-1},$$

where the integral is taken aver all values of $\xi_1, \ldots, \xi_{n-1}$ so that $\xi_n = u - \xi_1 - \ldots - \xi_{n-1} \in [0,1]$. We note that ϕ is of bounded variation. This follows if one sets $\xi_j = ut_j$, then

$$\phi(u) = u^{\frac{n}{k}-1} \int_0^{\frac{1}{u}} \cdots \int_0^{\frac{1}{u}} (t_1 \ldots t_{n-1}(1 - t_1 - \ldots - t_{n-1}))^{-1+\frac{1}{k}} \, dt_1 \ldots dt_{n-1},$$

where the integral is taken over $t_1, \ldots, t_{n-1}$ with $1 - \frac{1}{u} \leq t_1 + \ldots + t_{n-1} \leq 1$. Thus $\phi(u)$ is the product of $u^{\frac{n}{k}-1}$ and a positive monotonic decreasing function and hence has bounded variation.

Recall Fourier's integral theorem for finite intervals, which states that if ϕ has bounded variation then

$$\lim_{\lambda \to \infty} \int_A^B \phi(u) \frac{\sin 2\pi\lambda(u - C)}{\pi(u - C)} \, du = \phi(C).$$

Thus it follows $k^n J_{k,n} = \phi(1) > 1$ and moreover,

$$\begin{aligned} \phi(1) &= \int_0^1 \cdots \int_0^1 (\xi_1 \ldots \xi_{n-1}(1 - \xi_1 - \ldots - \xi_{n-1}))^{-1+\frac{1}{k}} \, d\xi_1 \ldots d\xi_{n-1} \\ &= \frac{\Gamma(\frac{1}{k})^n}{\Gamma(\frac{n}{k})}, \end{aligned}$$

where the integral is over the domain $0 < \xi_1 + \ldots + \xi_{n-1} < 1$. The last line is proven analogously to identities of the from

$$\int_0^1 x^{p-1}(1 - x)^{q-1} \, dx = \frac{\Gamma(p)\Gamma(q)}{\Gamma(p + q)},$$

which we leave to discussion in the reference [Dav05] (page 22). $\square$

7 The Heath-Brown Circle Method

The aim of this chapter is to expose the central results of the paper [HB96] by Heath-Brown and to apply the developed methods to deduce the necessary bounds (Corollary 5.16) for our proof of property (τ).

The circle method, as exposed in chapter 6, deals with counting the number of solutions of equations of the form

$$x_1^k + \ldots + x_n^k = m$$

for $n \geq 2^k + 1$. It is not too difficult (see [Dav05] chapter 7) to use the same methods in order to deduce an analogous asymptotic expression for solutions of

$$c_1 x_1^k + \ldots + c_n x_n^k = m,$$

where we still assume $n \geq 2^k + 1$ and fix some positive non-zero integers $c_1, \ldots, c_n$. The main statement of this chapter is an analogous result for non-singular quadratic forms in $n \geq 4$ variables. In fact, we will prove an asymptotic formula for the number of solutions of such a quadratic form with an effective error rate. This is an improvement to the results accessible by the techniques of last chapter, as the latter theorems only apply to positive-definite quadratic forms in ≥ 5 variables and the error rate in the asymptotic formula is non-effective.

In order to further elaborate on the main results of this chapter, denote by F a positive-definite quadratic form in four variables. Then we will show as $m \to \infty$,

$$|\{x \in \mathbb{Z}^4 \,:\, F(x) = m\}| = C_F \sigma(F, m) m + O_{F,\varepsilon}(m^{\frac{3}{4}+\varepsilon}), \tag{7.1}$$

where C_F is a positive constant only depending on F and $\sigma(F, m)$ is the singular series. Moreover, the results of this chapter also provide a counting statement for a general non-singular quadratic form in $n \geq 4$ variables for the quantity

$$\sum_{\substack{x \in \mathbb{Z}^4 \\ F(x)=m}} w\left(\frac{x}{\sqrt{m}}\right), \tag{7.2}$$

where $w : \mathbb{R}^n \to \mathbb{R}$ is a suitable smooth compactly supported function. The structure of the proof of these theorems will reflect the theory developed in chapter 6.

The effectiveness of the error term of (7.1) is a crucial part in our proof of property (τ) for $\mathbb{Q}$-forms of SL_2. In rough terms, the coefficient $\frac{3}{4}$ in the error term of (7.1) (and of the asymptotic formula of (7.2)) leads to Theorem 3.12. Connecting to the discussion at the end of chapter 5.5, an improvement of the error term to $O_{F,\varepsilon}(m^{\frac{1}{2}+\varepsilon})$ is likely to imply the Ramanujan-Petersson conjecture for division algebras over $\mathbb{Q}$ (Conjecture 3.13).

Finally, we remark that the methods exposed will also be sufficient to treat quadratic forms in three variables with moderate additional effort. We refer for these results to the original paper [HB96] as for our application the case of four variables is sufficient.

7.1 Counting the Number of Solutions of Quadratic Forms in Bounded Domains

Let F be a polynomial with integer coefficients in n variables. The first aim of this subchapter is to derive an analytic expression for

$$\sum_{\substack{x\in\mathbb{Z}^n \\ F(x)=0}} w(x),$$

where $w : \mathbb{R}^n \to \mathbb{R}$ is a compactly supported smooth function.

Write

$$\delta_n = \begin{cases} 1 & n = 0, \\ 0 & n \neq 0, \end{cases}$$

and observe

$$\sum_{\substack{x\in\mathbb{Z}^n \\ F(x)=0}} w(x) = \sum_{x\in\mathbb{Z}^n} w(x)\delta_{F(x)}.$$

Thus, in order to derive an analytic expression of the latter sum, we first deal with δ_n on $\mathbb{R}$. The following result is due to [DFI93] and is also discussed in the paper [HB96], whose proof we roughly follow. As usual, we write for any integers n and q, where q is non-zero,

$$e_q(n) = e(n/q) = e^{\frac{2\pi i n}{q}}.$$

Theorem 7.1. *There exists a function $h \in C^\infty((0,\infty)\times\mathbb{R})$ with the property that for all $Q > 1$ there is a positive constant c_Q with*

$$\delta_n = c_Q Q^{-2} \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e_q(an) h(Q^{-1}q, Q^{-2}n).$$

The constant c_Q satisfies

$$c_Q = 1 + O_N(Q^{-N})$$

for $N > 0$ and the function h has the property that

$$h(x,y) \leq 32x^{-1}$$

for all y. Moreover, $h(x,y)$ is non-zero only if $x \leq \max(1, 2|y|)$.

Before proceeding with the proof of Theorem 7.1, we discuss some calculative lemmas.

Lemma 7.2. *Let n be an integer. Then for all positive integers $q > 0$,*

$$\frac{1}{q}\sum_{a=1}^{q} e_q(an) = \begin{cases} 1 & \text{if } q \text{ divides } n, \\ 0 & \text{if } q \text{ does not divide } n. \end{cases}$$

Proof. If $q|n$, then $e_q(an) = 1$ and the claim follows. If q does not divide n, then $q^{-1}n$ is not an integer and hence

$$\begin{aligned}\frac{1}{q}\sum_{a=1}^{q} e_q(an) &= \frac{1}{q}\sum_{a=1}^{q} e_q(n)^a \\ &= \frac{e_q(n)}{q}\sum_{a=0}^{q-1} e_q(n)^a \\ &= \frac{e_q(n)}{q}\frac{1-e_q(n)^q}{1-e_q(n)} = 0.\end{aligned}$$

□

Lemma 7.3. *Let $f, g : \mathbb{R} \to \mathbb{C}$. Then*

$$\sum_{q=1}^{\infty}\sum_{a=1}^{q} f(q^{-1}a)g(q) = \sum_{j=1}^{\infty}\sum_{\substack{i=1\\(i,j)=1}}^{j}\sum_{k=1}^{\infty} f(j^{-1}i)g(kj)$$

Proof. The idea is to reduce $q^{-1}a$ to lowest terms by writing $k = (a, q)$, $q = kj$ and $a = ki$ so that $(i, j) = 1$. Then

$$\begin{aligned}\sum_{q=1}^{\infty}\sum_{a=1}^{q} f\left(\frac{a}{q}\right) g(q) &= \sum_{q=1}^{\infty}\sum_{a=1}^{q} f\left(\frac{(a,q)^{-1}a}{(a,q)^{-1}q}\right) g\left((q,a)\frac{q}{(a,q)}\right) \\ &= \sum_{k=1}^{\infty}\sum_{\substack{q=1\\k|q}}^{\infty}\sum_{\substack{a=1\\k|a\\(a,q)=k}}^{q} f\left(\frac{k^{-1}a}{k^{-1}q}\right) g\left(k\frac{q}{k}\right) \\ &= \sum_{k=1}^{\infty}\sum_{j=1}^{\infty}\sum_{\substack{i=1\\(i,j)=1}}^{q} f\left(\frac{i}{j}\right) g(kj),\end{aligned}$$

where the second line follows by setting $k = (a, q)$ and reordering the sums accordingly and the third line follows by setting $j = \frac{q}{k}$ and $i = \frac{a}{k}$. □

Lemma 7.4. *For all $x \in (0, \infty)$ and $y \in \mathbb{R}$,*

$$\sum_{\substack{k=1\\\frac{1}{2x}<k<\frac{1}{x}}}^{\infty} \frac{1}{k} \leq 1 \qquad \textit{and} \qquad \sum_{\substack{k=1\\\frac{|y|}{x}<k<\frac{2|y|}{x}}}^{\infty} \frac{1}{k} \leq 1.$$

Proof. The first inequality follows from the second by setting $y = \frac{1}{2}$. The main observation is that there are at most $\left(\frac{2|y|}{x} - \frac{|y|}{x}\right)$ many integers $\frac{|y|}{x} < k < \frac{2|y|}{x}$. Thus

$$\sum_{\frac{|y|}{x}<k\leq\frac{2|y|}{x}}^{\infty} \frac{1}{k} \leq \left(\frac{2|y|}{x} - \frac{|y|}{x}\right)\frac{x}{|y|} = 1.$$

□

Proof. (of Theorem 7.1) We denote by w_0 the smooth function defined for $x \in \mathbb{R}$ as

$$w_0(x) = \begin{cases} e^{-(1-x^2)^{-1}} & |x| < 1, \\ 0 & |x| \geq 1. \end{cases}$$

Notice, $0 \leq w_0 \leq 1$. Set $c_0 = \int_{-\infty}^{\infty} w_0(x)\, dx$ and observe $\frac{1}{4} \leq c_0 \leq 1$. Finally set

$$w(x) = \frac{4w_0(4x-3)}{c_0}.$$

Then $w \in C^{\infty}(\mathbb{R})$ is supported in $[\frac{1}{2}, 1]$, $0 \leq w \leq 16$ and $\int_{-\infty}^{\infty} w(x)\, dx = 1$. If $Q > 0$, by the Poisson summation formula,

$$\sum_{q=1}^{\infty} w(Q^{-1}q) = \sum_{q\in\mathbb{Z}} w(Q^{-1}q) = \sum_{n\in\mathbb{Z}} \int_{-\infty}^{\infty} w(Q^{-1}x)e(-nx)\, dx.$$

We analyze the sum over n. If $n = 0$, then $\int_{-\infty}^{\infty} w(Q^{-1}x)e(-nx)\, dx \ll Q$. For non-zero n, integration by parts yields

$$\int_{-\infty}^{\infty} w(Q^{-1}x)e(-nx)\, dx = \frac{1}{2\pi iQn} \int_{-\infty}^{\infty} w'(Q^{-1}x)e(-nx)\, dx \ll Q(Q|n|)^{-1}$$

Performing integration by parts N-times,

$$\int_{-\infty}^{\infty} w(Q^{-1}x)e(-nx)\, dx \ll_N Q(Q|n|)^{-N}.$$

Setting $c_Q = \frac{Q}{\sum_{q=1}^{\infty} w(Q^{-1}q)}$, we conclude by the above discussion

$$c_Q = \frac{Q}{Q + O_N(Q^{-(N-1)})} = 1 + O_N(Q^{-N}).$$

If n is a positive integer, then as q runs over the divisors of n, so does $q^{-1}n$. Thus

$$\sum_{\substack{q=1 \\ q|n}}^{\infty} \left(w(Q^{-1}q) - w(Q^{-1}q^{-1}n) \right) = 0.$$

Similarly if $n < 0$,

$$\sum_{\substack{q=1 \\ q|n}}^{\infty} \left(w(Q^{-1}q) - w(Q^{-1}q^{-1}|n|) \right) = 0.$$

In the case $n = 0$, $w(Q^{-1}q^{-1}n) = 0$ as $w(0) = 0$ and

$$\sum_{\substack{q=1 \\ q|0}}^{\infty} \left(w(Q^{-1}q) - w(Q^{-1}q^{-1} \cdot 0) \right) = \sum_{q=1}^{\infty} w(Q^{-1}q) = c_Q^{-1}Q.$$

Thus it follows,

$$\delta_n = c_Q Q^{-1} \sum_{\substack{q=1 \\ q|n}}^{\infty} \left(w(Q^{-1}q) - w(Q^{-1}q^{-1}|n|) \right).$$

By Lemma 7.2,

$$\sum_{\substack{q=1\\q|n}}^{\infty}\left(w(Q^{-1}q)-w(Q^{-1}q^{-1}|n|)\right)=\sum_{q=1}^{\infty}\frac{1}{q}\sum_{a=1}^{q}e_q(an)\left(w(Q^{-1}q)-w(Q^{-1}q^{-1}|n|)\right).$$

We define

$$h(x,y)=\sum_{k=1}^{\infty}\frac{1}{kx}\left(w(kx)-w((kx)^{-1}|y|)\right). \tag{7.3}$$

By using Lemma 7.3, again denoting $(a,q)=k$, $a=ki$ and $q=kj$, it follows

$$\begin{aligned}
&\sum_{q=1}^{\infty}\frac{1}{q}\sum_{a=1}^{q}e_q(an)\left(w(Q^{-1}q)-w(Q^{-1}q^{-1}|n|)\right)\\
&=\sum_{j=1}^{\infty}\sum_{\substack{i=1\\(i,j)=1}}^{j}\sum_{k=1}^{\infty}e_j(in)\frac{1}{kj}\left(w(Q^{-1}kj)-w(Q^{-1}(kj)^{-1}|n|)\right)\\
&=Q^{-1}\sum_{j=1}^{\infty}\sum_{\substack{i=1\\(i,j)=1}}^{j}\sum_{k=1}^{\infty}e_j(in)\frac{1}{kQ^{-1}j}\left(w(kQ^{-1}j)-w((kQ^{-1}j)^{-1}|Q^{-2}n|)\right)\\
&=Q^{-1}\sum_{j=1}^{\infty}\sum_{\substack{i=1\\(i,j)=1}}^{j}e_j(in)h(Q^{-1}j,Q^{-2}n).
\end{aligned}$$

By relabeling the variables,

$$\delta_n=c_QQ^{-2}\sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}e_q(an)h(Q^{-1}q,Q^{-2}n).$$

It remains to check the properties of $h(x,y)$. To see that h is infinitely differentiable, we use that ω is supported in $(\frac{1}{2},1)$, which implies

$$\begin{aligned}
h(x,y)&=\sum_{k=1}^{\infty}\frac{w(kx)}{kx}-\sum_{k=1}^{\infty}\frac{w((kx)^{-1}|y|)}{kx}\\
&=\sum_{\frac{1}{2}<kx<1}\frac{w(kx)}{kx}-\sum_{\frac{1}{2}<(kx)^{-1}|y|<1}^{\infty}\frac{w((kx)^{-1}|y|)}{kx}\\
&\sum_{\frac{1}{2x}<k<\frac{1}{x}}\frac{w(kx)}{kx}-\sum_{\frac{|y|}{x}<k<\frac{2|y|}{x}}^{\infty}\frac{w((kx)^{-1}|y|)}{kx}.
\end{aligned}$$

If we fix (x,y), the latter sums are in fact finite around a small neighborhood of (x,y). Thus $h(x,y)$ is locally the sum of a finite number of smooth functions, showing that $h\in C^{\infty}((0,\infty)\times\mathbb{R})$. Moreover, if $x>\max(1,2|y|)$, then clearly the above sums are empty. Finally using that $0\le\omega\le 16$ we derive an explicit bound for $h(x,y)$ in terms of x^{-1}. In fact,

$$\begin{aligned}
h(x,y) &\leq \sum_{\frac{1}{2}<kx<1} \frac{w(kx)}{kx} + \sum_{\frac{1}{2}<(kx)^{-1}|y|<1}^{\infty} \frac{w((kx)^{-1}|y|)}{kx} \\
&\leq 16 \left(\sum_{\frac{1}{2x}<k<\frac{1}{x}} \frac{1}{kx} + \sum_{\frac{|y|}{x}<k<\frac{2|y|}{x}}^{\infty} \frac{1}{kx} \right) \\
&\leq 16x^{-1} \left(\sum_{\frac{1}{2x}<k<\frac{1}{x}} \frac{1}{k} + \sum_{\frac{|y|}{x}<k<\frac{2|y|}{x}}^{\infty} \frac{1}{k} \right) \leq 32x^{-1},
\end{aligned}$$

where we used Lemma 7.4 in the last line. □

We introduce the notation

$$N^{(0)}(F,w) = \sum_{\substack{x\in\mathbb{Z}^n \\ F(x)=0}} w(x).$$

In dependence of F, we set for $c \in \mathbb{Z}^n$,

$$S_q(c) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ b\in\mathbb{Z}^n}}^{q} e_q(aF(b) + \langle b,c\rangle), \tag{7.4}$$

where we denote by the inner sum all the integers $b \in \mathbb{Z}^n$ so that all components are between 1 and q, and

$$I_q^{(0)}(c) = \int_{\mathbb{R}^n} w(x)h(Q^{-1}q, Q^{-2}F(x))e_q(-\langle c,x\rangle)\, dx, \tag{7.5}$$

where dx is the Lebesgue measure on $\mathbb{R}^n$.

Theorem 7.5. *(Theorem 2 of [HB96]) Let $F \in \mathbb{Z}[X_1,\ldots,X_n]$ and $\omega \in C_c^\infty(\mathbb{R}^n)$. Then*

$$\begin{aligned}
N^{(0)}(F,w) &= c_Q Q^{-2} \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{x\in\mathbb{Z}^n} w(x)e_q(aF(x))h(Q^{-1}q, Q^{-2}F(x)) \\
&= c_Q Q^{-2} \sum_{c\in\mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q^{(0)}(c).
\end{aligned}$$

Proof. The first equality just follows by writing

$$N^{(0)}(F,w) = \sum_{\substack{x\in\mathbb{Z}^n \\ F(x)=0}} w(x) = \sum_{x\in\mathbb{Z}^n} w(x)\delta_{F(x)}$$

and using Theorem 7.1. Writing $x = b + q\cdot y$, we express

$$\sum_{x\in\mathbb{Z}^n} w(x)e_q(aF(x))h(Q^{-1}q, Q^{-2}F(x)) = \sum_{\substack{b=1 \\ b\in\mathbb{Z}^n}}^{q} e_q(aF(b)) \sum_{y\in\mathbb{Z}^n} f_b(y),$$

where we used that F has integral coefficients and denote

$$f_b(y) = w(b + q \cdot y)h(Q^{-1}q, Q^{-2}F(b + q \cdot y)).$$

By the Poisson summation formula,

$$\sum_{y \in \mathbb{Z}^n} f_b(y) = \sum_{c \in \mathbb{Z}^n} \hat{f}_b(c) = \sum_{c \in \mathbb{Z}^n} \int_{\mathbb{R}^n} f_b(y) e(-\langle c, y \rangle)\, dy.$$

Substituting $x = b + q \cdot y$ and $dx = q^n dy$,

$$\begin{aligned}
\hat{f}_b(c) &= \int_{\mathbb{R}^n} w(b + q \cdot y)h(Q^{-1}q, Q^{-2}F(b + q \cdot y))e(-\langle c, y \rangle)\, dy \\
&= q^{-n} \int_{\mathbb{R}^n} w(x)h(Q^{-1}q, Q^{-2}F(x))e\left(-\left\langle c, \frac{x-b}{q} \right\rangle\right) dx \\
&= q^{-n} e_q(\langle b, c \rangle) \int_{\mathbb{R}^n} w(x)h(Q^{-1}q, Q^{-2}F(x))e_q\left(-\langle c, x \rangle\right)\, dx \\
&= q^{-n} e_q(\langle b, c \rangle) I_q^{(0)}(c).
\end{aligned}$$

To summarize,

$$\begin{aligned}
&\sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{x \in \mathbb{Z}^n} w(x)e_q(aF(x))h(Q^{-1}q, Q^{-2}F(x)) \\
&= \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ b \in \mathbb{Z}^n}}^{q} e_q(aF(b)) \sum_{y \in \mathbb{Z}^n} f_b(y) \\
&= \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ b \in \mathbb{Z}^n}}^{q} e_q(aF(b)) \sum_{c \in \mathbb{Z}^n} q^{-n} e_q(\langle b, c \rangle) I_q^{(0)}(c) \\
&= \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} \left(\sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ b \in \mathbb{Z}^n}}^{q} e_q(aF(b) + \langle b, c \rangle) \right) I_q^{(0)}(c) \\
&= \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q^{(0)}(c).
\end{aligned}$$

□

We next introduce an additional parameter $P > 0$. Instead of investigating $N^{(0)}(F, w)$, we consider

$$N(F, w, P) = \sum_{\substack{x \in \mathbb{Z}^n \\ F(x)=0}} w(P^{-1}x),$$

where we understand P as tending to infinity. In dependence of P we set for $c \in \mathbb{Z}^n$,

$$I_q(c) = \int_{\mathbb{R}^n} w(P^{-1}x)h(Q^{-1}q, Q^{-2}F(x))e_q(-\langle c, x \rangle)\, dx. \tag{7.6}$$

In analogy to Theorem 7.5, we have the following corollary.

Corollary 7.6. *Let* $F \in \mathbb{Z}[X_1, \dots, X_n]$ *and* $\omega \in C_c^\infty(\mathbb{R}^n)$*. Then*

$$\begin{aligned} N(F, w, P) &= c_Q Q^{-2} \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{x \in \mathbb{Z}^n} w(P^{-1}x) e_q(aF(x)) h(Q^{-1}q, Q^{-2}F(x)) \\ &= c_Q Q^{-2} \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c). \end{aligned}$$

Proof. The same proof as the one of Theorem 7.5 applies. □

Assume that F is a polynomial of degree k in n variables. Throughout the rest of this chapter we will assume that F is of the form $F = F^{(0)} - m$, where $F^{(0)}$ is a fixed form and m tends to infinity. Fix throughout this chapter $P = m^{\frac{1}{k}}$. Moreover, we set $G = F^{(0)} - 1$ so that $G(x) = P^{-k} F(Px)$.

Lemma 7.7. *In the above setting, assume that* $\nabla G \neq 0$ *on* $\operatorname{supp}(w)$*. Then the limit*

$$\sigma_\infty(G, w) = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} w(x)\, dx$$

exists. Moreover, if $w \geq 0$ *and takes a strictly positive value for some* $x \in \mathbb{R}^n$ *with* $G(x) = 0$*, then* $\sigma_\infty(G, w) > 0$*.*

Proof. See Lemma 7.19 and Corollary 7.20. □

Throughout the remainder of this chapter, we only consider compactly supported functions $w : \mathbb{R}^n \to \mathbb{R}$, that satisfy the non-singularity condition of the above lemma. Denote by $M_m(p^k)$ the number of solutions to the equation

$$F^0(x) \equiv m \mod p^k$$

in $[1, p^k]^n$. Then we write

$$\sigma_p = \lim_{k \to \infty} \frac{M_m(p^k)}{p^{k(n-1)}}$$

and define the **singular series** in this setting as

$$\sigma(F^{(0)}, m) = \prod_{p \text{ prime}} \sigma_p.$$

For further discussion on the singular series see chapter 7.5. We next state the central result of this chapter ,which is Theorem 4 of [HB96], and defer its proof to chapter 7.6.

Theorem 7.8. *Let* $n \geq 4$ *and* $F^{(0)}$ *be a non-singular quadratic form in* n *variables,* m *be a positive integer and* $w : \mathbb{R}^n \to \mathbb{R}$ *be a compactly supported function that satisfies the condition of Lemma 7.7. Set* $F = F^{(0)} - m$*. Then as* $m \to \infty$*,*

$$\begin{aligned} N(F, w, m^{\frac{1}{2}}) &= \sum_{\substack{x \in \mathbb{Z}^n \\ F^{(0)}(x) = m}} w\left(\frac{x}{\sqrt{m}}\right) \\ &= \sigma_\infty(G, w) \sigma(F^{(0)}, m) m^{\frac{n}{2} - 1} + O_{F^{(0)}, w, \varepsilon}(m^{\frac{n-1}{4} + \varepsilon}). \end{aligned}$$

7.2 Properties of the Function h

We recall the definition of the function $h(x, y)$ as defined in (7.3). Set $w(x) = \frac{4w_0(4x-3)}{c_0}$. Then $h(x, y)$ is defined for $x \in (0, \infty)$ and $y \in \mathbb{R}$ as

$$h(x,y) = \sum_{k=1}^{\infty} \frac{1}{kx} \left(w(kx) - w((kx)^{-1}|y|) \right).$$

We aim at proving the following result, showing that $h(x, y)$ behaves like a δ function for small x.

Proposition 7.9. *Let f be a smooth function on $\mathbb{R}$. If $x \ll 1$, then for any $M > 0$,*

$$\int_{-\infty}^{\infty} f(y)h(x,y)\,dy = f(0) + O_{f,M}(x^M).$$

Towards proving Proposition 7.9, we estimate the derivatives of the function h. The main tool we use is the Euler-Maclaurin summation formula which for $a, b \in \mathbb{R}$ and $f \in C^\infty([a, b])$ takes the form

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)\,dt + (\{a\} - \tfrac{1}{2})f(a) - (\{b\} - \tfrac{1}{2})f(b)$$
$$+ \sum_{\ell=2}^{N} \frac{(-1)^\ell}{\ell!} \left[P_\ell f^{\ell-1}\right]_a^b - \frac{(-1)^N}{N!} \int_a^b P_N f^{(N)}(t)\,dt, \tag{7.7}$$

where $\{a\}$ and $\{b\}$ are the integer parts of a and b and $P_\ell(t)$ is the ℓ-th periodic Bernoulli polynomial so that $P_N \ll_N 1$.

Recall that we have shown in Theorem 7.1 that the function $h(x, y)$ vanishes if $x \geq 1$ and $|y| \leq x/2$.

Lemma 7.10. *If $|y| \leq x/2$, then the function $h(x, y)$ does not depend on y and*

$$h(x,y) = h(x,y) = \sum_{k=1}^{\infty} \frac{w(kx)}{kx} \leq 16x^{-1}.$$

Moreover, for $|y| \leq \frac{x}{2}$,

$$\frac{\partial^m h(x,y)}{\partial x^m} \ll_m x^{-m-1}.$$

Finally, when $|y| > x/2$,

$$\frac{\partial^{m+n}}{\partial x^m \partial y^n} h(x,y) \ll_{m,n} x^{-m-1}|y|^{-n}.$$

Proof. As in the proof of Theorem 7.1, if $|y| \leq x/2$, then

$$h(x,y) = \sum_{k=1}^{\infty} \frac{w(kx)}{kx} = \sum_{\frac{1}{2}<kx<1} \frac{w(kx)}{kx} \leq 16x^{-1}.$$

Since $\frac{1}{2} \leq kx \leq 1$ it follows $k \leq \frac{1}{x}$ and hence for $\ell \geq 1$,

$$\frac{\partial^\ell w(kx)}{\partial x^\ell} = k^\ell w^{(\ell)}(kx) \ll_\ell x^{-\ell}$$

and together with the Leibniz formula

$$\begin{aligned}
\frac{\partial^m}{\partial x^m} \frac{w(kx)}{x} &= \sum_{\ell=0}^{m} \binom{m}{\ell} \frac{\partial^\ell w(kx)}{\partial x^\ell} \frac{\partial^{m-\ell}}{\partial x^{m-\ell}} \frac{1}{x} \\
&= \sum_{\ell=0}^{m} \binom{m}{\ell} (-1)^{m-\ell} (m-\ell)! x^{-(m-\ell+1)} \frac{\partial^\ell w(kx)}{\partial x^\ell} \\
&\leq \sum_{\ell=0}^{m} \binom{m}{\ell} (-1)^{m-\ell} c_\ell x^{-(m-\ell+1)} x^{-\ell} \\
&\ll_m x^{-m-1},
\end{aligned}$$

where c_ℓ is a constant depending only on ℓ. As by Lemma 7.4,

$$\sum_{\frac{1}{2} < kx < 1} \frac{1}{k} \ll 1$$

it follows that

$$\frac{\partial^m h(x,y)}{\partial x^m} \ll_m \sum_{\frac{1}{2} < kx < 1} \frac{x^{-m-1}}{k} \ll_m x^{-m-1}.$$

To prove the final claim, assume $|y| > x/2$. Then

$$h(x,y) = \sum_{\frac{1}{2} < kx < 1} \frac{w(kx)}{kx} - \sum_{\frac{1}{2} < (kx)^{-1}|y| < 1} \frac{w(((kx)^{-1}|y|)}{kx}.$$

The sum $\sum_{\frac{1}{2} < kx < 1} \frac{w(kx)}{kx}$ only contributes for $x \leq 1$. By the first part,

$$\sum_{\frac{1}{2} < kx < 1} \frac{w(kx)}{kx} \ll_m x^{-m-1} \ll_{m,n} x^{m-1}|y|^{-n},$$

using $|y| \leq \frac{x}{2} \ll 1$ so that $|y|^{-n} \gg 1$. It remains to deal with

$$\sum_{\frac{1}{2} < (kx)^{-1}|y| < 1} \frac{w(((kx)^{-1}|y|)}{kx}.$$

One shows by induction over m that

$$\frac{\partial^{m+n}}{\partial x^m \partial y^n} \frac{w((xk)^{-1}y)}{x} = y^{-n} x^{-m-1} \sum_{\ell=0}^{m} c_{m,n,\ell} \left(\frac{y}{xk}\right)^{n+\ell} w^{(n+\ell)} \left(\frac{y}{xk}\right),$$

for certain constants $c_{m,n,\ell}$. In particular, as ω is a Schwartz function,

$$\left(\frac{y}{xk}\right)^{n+\ell} w^{(n+\ell)} \left(\frac{y}{xk}\right) \ll_{n,\ell} 1,$$

it follows
$$\frac{\partial^{m+n}}{\partial x^m \partial y^n} \frac{w((xk)^{-1}|y|)}{x} \ll_{m,n} x^{-m-1}|y|^{-n}.$$
Thus we conclude using Lemma 7.4,
$$\begin{aligned}\frac{\partial^{m+n}}{\partial x^m \partial y^n} \sum_{\frac{1}{2}<(kx)^{-1}|y|<1} \frac{w(((kx)^{-1}|y|)}{kx} &\ll_{m,n} x^{-m-1}|y|^{-n} \sum_{\frac{1}{2}<(kx)^{-1}|y|<1} \frac{1}{k} \\ &\ll_{m,n} x^{-m-1}|y|^{-n}.\end{aligned}$$
□

Proposition 7.11. *Let N, m, n be non-negative integers. Then for all $(x, y) \in (0, \infty) \times \mathbb{R}$,*
$$\frac{\partial^{m+n}}{\partial x^m \partial y^n} h(x, y) \ll_{N,m,n} x^{-m-n-1} \left(x^N + \min\left\{1, \left(\frac{x}{|y|}\right)^N\right\}\right),$$
The term x^N on the right may be omitted for $n \neq 0$.

Proof. Assuming $|y| \leq \frac{x}{2}$, the function does not depend on y and the result follows from Lemma 7.10. If $\frac{x}{2} \leq |y| \leq x$, then also by Lemma 7.10,
$$\frac{\partial^{m+n}}{\partial x^m \partial y^n} h(x, y) \ll_{m,n} x^{-m-1}|y|^{-n} \ll_{m,n} x^{-m-n-1}.$$
Hence we only need to treat the case $|y| > x > 0$ or equivalently $\frac{1}{x} < \frac{1}{|y|}$. Moreover, if $n = 0$, then also by Lemma 7.10 the result holds if $x \geq 1$. So we assume $x \leq 1$ if $n = 0$. In particular, in the case $n = 0$ and $x \leq 1$, it suffices to show the statement for N large enough.

As w is supported in $(\frac{1}{2}, 1)$ by using the Euler-Maclaurin summation formula (7.7),
$$\begin{aligned}\sum_{k=1}^{\infty} \frac{w(kx)}{kx} &= \sum_{\substack{k=1 \\ \frac{1}{2x}<k<\frac{1}{x}}}^{\infty} \frac{w(kx)}{kx} \\ &= \int_{\frac{1}{2x}}^{\frac{1}{x}} \frac{w(tx)}{tx}\,dt - \frac{(-1)^N}{N!} \int_{\frac{1}{2x}}^{\frac{1}{x}} P_N(t) \frac{\partial^N}{\partial t^N} \frac{w(xt)}{xt}\,dt \\ &= \int_{\frac{1}{2x}}^{\frac{1}{x}} \frac{w(tx)}{tx}\,dt - x^{N-1} \frac{(-1)^N}{N!} \int_{\frac{1}{2}}^{1} P_N\left(\frac{u}{x}\right) \omega^{(N)}(u)\,du, \qquad (7.8)\end{aligned}$$

where we substituted $u = xt$ defined $\omega(u) := \frac{w(u)}{u}$ and used the Leibniz formula,

$$\begin{aligned}\frac{\partial^N}{\partial t^N}\frac{w(xt)}{xt} &= \sum_{\ell=0}^{N}\binom{N}{\ell}\frac{\partial^\ell}{\partial t^\ell}w(xt)\frac{\partial^{N-\ell}}{\partial t^{N-\ell}}\frac{1}{xt}\\ &= \sum_{\ell=0}^{N}\binom{N}{\ell}w^{(\ell)}(xt)x^\ell(-1)^{N-\ell}x^{N-\ell}(N-\ell)!(xt)^{-(N-\ell)-1}\\ &= x^N\sum_{\ell=0}^{N}\binom{N}{\ell}w^{(\ell)}(xt)(-1)^{N-\ell}(N-\ell)!(xt)^{-(N-\ell)-1}\\ &= x^N\frac{\partial^N}{\partial u^N}\frac{w(u)}{u}\\ &= x^N\omega^{(N)}(u)\end{aligned}$$

yielding

$$\begin{aligned}\int_{\frac{1}{2x}}^{\frac{1}{x}} P_N(t)\frac{\partial^N}{\partial t^N}\frac{w(xt)}{xt}\,dt &= \int_{\frac{1}{2x}}^{\frac{1}{x}} P_N(t)x^N\frac{\partial^N}{\partial u^N}\omega(u)\,dt\\ &= x^{N-1}\int_{\frac{1}{2}}^{1} P_N\left(\frac{u}{x}\right)\omega^{(N)}(u)\,du.\end{aligned}$$

We analogously have

$$\begin{aligned}&\sum_{k=1}^{\infty}\frac{w((kx)^{-1}|y|)}{kx}\\ &= \sum_{\substack{k=1\\ \frac{1}{2x}<k<\frac{1}{x}}}^{\infty}\frac{w((kx)^{-1}|y|)}{kx}\\ &= \int_{\frac{|y|}{x}}^{\frac{2|y|}{x}}\frac{w((kx)^{-1}|y|)}{tx}\,dt - \frac{(-1)^N}{N!}\int_{\frac{1}{2x}}^{\frac{1}{x}} P_N(t)\frac{\partial^N}{\partial t^N}\frac{w((kx)^{-1}|y|)}{xt}\,dt\\ &= \int_{\frac{1}{2x}}^{\frac{1}{x}}\frac{w(tx)}{tx}\,dt - \frac{1}{x}\left(\frac{x}{|y|}\right)^N\frac{(-1)^N}{N!}\int_1^2 P_N\left(\frac{u|y|}{x}\right)\frac{\partial^N}{\partial u^N}u^{-2}\omega(u^{-1})\,du, \quad (7.9)\end{aligned}$$

where we substituted in the first integral $u = (x^2t)^{-1}|y|$ and in the second integral $u = \frac{x}{|y|}u$.

Combining (7.8) and (7.9),

$$\begin{aligned}h(x,y) = &-x^{N-1}\frac{(-1)^N}{N!}\int_{\frac{1}{2}}^{1} P_N\left(\frac{u}{x}\right)\omega^{(N)}(u)\,du\\ &- \frac{1}{x}\left(\frac{x}{|y|}\right)^N\frac{(-1)^N}{N!}\int_1^2 P_N\left(\frac{u|y|}{x}\right)\frac{\partial^N}{\partial u^N}u^{-2}\omega(u^{-1})\,du.\end{aligned}$$

Denote by $F_1(x)$ the first part and by $F_2(x,y)$ the second part of the latter equation. The term $F_1(x)$ only vanishes if $n = 0$, and then we can assume $x \leq 1$

and so $\frac{1}{x} \geq 1$. Write $F_1(x) = x^{N-1} I_1(x)$, then

$$\frac{\partial^m F_1(x)}{\partial x^m} = \sum_{\ell=0}^{m} c_{\ell,N} x^{N-\ell-1} x^{N-(m-\ell)-1} \ll_{N,m} x^{N-m-2}$$

Thus replacing N by $n+1$, we are done. The second term $F_2(x, y)$ is treated analogously (for more detail see [HB96] Lemma 5). $\square$

Lemma 7.12. *If $x \ll \min(1, X)$, then*

$$\int_{-X}^{X} h(x, y)\, dy = 1 + O_N(X x^{N-1}) + O_N\left(\left(\frac{X}{x}\right)^{-N}\right).$$

Before treating Lemma 7.12, we prove the following lemma.

Lemma 7.13. *Let $w : \mathbb{R} \to \mathbb{R}$ be a smooth function supported in $(\frac{1}{2}, 1)$. Then for any $N > 0$ and $Y > 0$,*

$$Y \int_0^\infty \frac{w(u)}{u}\, du - \sum_{j=1}^{\infty} \int_0^{\frac{Y}{j}} w(u)\, du = \frac{1}{2} \int_0^\infty w(u)\, du + O_N(Y^{-N}).$$

Proof. Throughout this proof fix $Y > 0$. Set for $t \in \mathbb{R}_{>0}$,

$$\phi(t) = \int_0^{\frac{Y}{t}} w(u)\, du,$$

so that

$$\phi(t) = \begin{cases} 0 & \text{if } 2Y \leq t, \\ \int_0^\infty w(u)\, du & \text{if } Y \geq t. \end{cases}$$

Moreover

$$\phi'(t) = -\frac{Y}{t^2} w\left(\frac{Y}{t}\right)$$

which is supported in $\frac{1}{2} \leq \frac{Y}{t} \leq 1$ or equivalently $Y \leq t \leq 2Y$. In particular

$$\phi'(t) \ll -\frac{Y}{t^{-2}}$$

and hence we conclude as the function is supported on $Y \leq t \leq 2Y$,

$$\phi^{(k)}(t) \ll_k -\frac{Y}{t^{(k+1)}} \ll_k Y^{-k}. \tag{7.10}$$

Finally, we apply the Euler-Maclaurin summation formula (7.7) for $a \to 0$ and $b > 2N$,

$$\sum_{j=1}^{\infty} \phi(j) = \int_0^\infty \phi(x)\, dx - \frac{1}{2} \int_0^\infty w(u)\, du - \frac{(-1)^N}{N!} \int_Y^{2Y} P_N(t) \phi^{(N)}(t)\, dt.$$

Finally, as

$$\begin{aligned}\int_0^\infty \phi(x)\,dx &= \int_0^{2Y}\int_{\frac{1}{2}}^{\frac{Y}{t}} w(u)\,du\\ &= \int_{\frac{1}{2}}^{1} w(u)\int_0^{\frac{Y}{u}} dtdu\\ &= Y\int_{\frac{1}{2}}^{1}\frac{w(u)}{u}\,du\\ &= Y\int_0^\infty \frac{w(u)}{u}\,du.\end{aligned}$$

the claim follows by (7.10). □

Proof. (of Lemma 7.12) By (7.8),

$$\begin{aligned}\sum_{k=1}^{\infty}\frac{w(kx)}{kx} &= \int_{\frac{1}{2x}}^{\frac{1}{x}}\frac{w(tx)}{tx}\,dt - x^{N-1}\frac{(-1)^N}{N!}\int_{\frac{1}{2}}^{1} P_N\left(\frac{u}{x}\right)\omega^{(N)}(u)\,du,\\ &= \frac{1}{x}\int_0^\infty \frac{w(u)}{u}\,du + O_N(x^{N-1}).\end{aligned}$$

where we substituted $u = tx$ in the first integral and used that $P_N \ll_N 1$. By integrating over $-X \leq y \leq X$, the error term is satisfactory. To prove the lemma,

$$\begin{aligned}\int_{-X}^{X} h(x,y)\,dy &= \int_{-X}^{X}\sum_{k=1}^{\infty}\frac{w(kx)}{kx}\,dy - \int_{-X}^{X}\sum_{k=1}^{\infty}\frac{w((kx)^{-1}|y|)}{kx}\,dy\\ &= \frac{2X}{x}\int_0^\infty \frac{w(u)}{u}\,du - \sum_{k=1}^{\infty}\int_{-X}^{X}\frac{w((kx)^{-1}|y|)}{kx}\,dy + O_N(Xx^{N-1})\\ &= 2\left(\frac{X}{x}\int_0^\infty\frac{w(u)}{u}\,du - \sum_{k=1}^{\infty}\frac{1}{kx}\int_0^X w\left(\frac{y}{kx}\right)\,dy\right) + O_N(Xx^{N-1})\\ &= 2\left(\frac{X}{x}\int_0^\infty\frac{w(u)}{u}\,du - \sum_{k=1}^{\infty}\int_0^{X/kx} w\left(u\right)\,du\right) + O_N(Xx^{N-1})\\ &= 2\left(\frac{1}{2}\int_{-\infty}^{\infty} w(u)\,du + O_N\left(\left(\frac{X}{x}\right)^{-N}\right)\right) + O_N(Xx^{N-1})\\ &= 1 + O_N(Xx^{N-1}) + O_N\left(\left(\frac{X}{x}\right)^{-N}\right),\end{aligned}$$

where we used Lemma 7.13 for $Y = \frac{X}{x}$ in the penultimate line and $\int_{-\infty}^{\infty} w(u)\,du = 1$ in the last line. □

Lemma 7.14. *Let $X \geq 1$. Let n be a positive integer and suppose that $x \ll \min(1, X)$. Then for any $N > 0$,*

$$\int_{-X}^{X} y^n h(x,y)\,dy \ll_{N,n} X^n\left(Xx^{N-1} + \left(\frac{X}{x}\right)^{-N}\right).$$

Proof. As $h(x,\cdot)$ is an even function the integral vanishes for odd n. The case $n=0$ was treated in Lemma 7.12 so assume $n\geq 2$ to be even. It suffices to consider the integral

$$\int_0^X y^n h(x,y)\,dy.$$

As in the proof of Lemma 7.12,

$$\int_0^X y^n \sum_{k=1}^{\infty} \frac{w(kx)}{kx}\,dy = \int_0^X \frac{y^n}{x}\int_0^{\infty}\frac{w(u)}{u}\,dudy + O_N(X^{n+1}x^{N-1}).$$

We can ignore the first term of the latter equation, as by (7.9) it cancels with the integral of the first part of the second term of $h(x,y)$. So it remains to deal with the integral over $[0,X]$ of

$$\frac{x^{n-1}}{y^n}\frac{(-1)^n}{n!}\int_1^2 P_n\left(\frac{u|y|}{x}\right)\frac{\partial^n}{\partial u^n}u^{-2}\omega(u^{-1})\,du.$$

We want to show for any in $(1,2)$ supported function ψ, that

$$\int_0^X x^{n-1}\int_1^2 P_n\left(\frac{uy}{x}\right)\psi(u)\,dudy \ll_{N,n} X^{n-N}x^N,$$

which clearly implies the claim. Equivalently we show

$$\int_0^X \int_1^2 P_n\left(\frac{uy}{x}\right)\psi(u)\,dudy \ll_{N,n,\psi} X^{n-N}x^{N-n+1}.$$

To establish the latter claim, recall that for $Z>0$,

$$\int_0^Z P_n(z)\,dz = \frac{P_{n+1}(Z)}{n+1} - \frac{P_{n+1}(0)}{n+1} = \frac{P_{n+1}(Z)}{n+1}.$$

Thus by a substitution of $y=\frac{zx}{u}$,

$$\begin{aligned}\int_0^X \int_1^2 P_n\left(\frac{uy}{x}\right)\psi(u)\,dudy &= \int_1^2\int_0^X P_n\left(\frac{uy}{x}\right)\,dy\,\psi(u)\,dz\\ &= x\int_1^2\int_0^{\frac{Xu}{x}} P_n(z)\,dz\frac{\psi(u)}{u}\,du\\ &= \frac{x}{n+1}\int_1^2 P_{n+1}\left(\frac{Xu}{x}\right)\frac{\psi(u)}{u}\,du.\end{aligned}$$

Finally integration by parts yields as $\frac{d}{dx}P_k(x) = kP_{k-1}(x)$,

$$\begin{aligned}&\frac{x}{n+1}\int_1^2 P_{n+1}\left(\frac{Xu}{x}\right)\frac{\psi(u)}{u}\,du\\ &= \frac{x}{n+1}(-1)^{N-n}\frac{(n+1)!}{(N+1)!}\left(\frac{x}{X}\right)^{N-n}\int_1^2 P_{N+1}\left(\frac{Xu}{x}\right)\frac{d^{N-n}}{d^{N-n}}\frac{\psi(u)}{u}\,du\\ &\ll_{N,n,\psi} X^{n-N}x^{N-n+1}.\end{aligned}$$

□

Finally, we prove Proposition 7.9. We restate it for convenience.

Proposition 7.15. *Let f be a smooth, compactly supported function on $\mathbb{R}$. If $x \ll 1$, then for any $M > 0$,*

$$\int_{-\infty}^{\infty} f(y)h(x,y)\,dy = f(0) + O_{f,M}(x^M).$$

Proof. Write $X = \min\{1, x^{\frac{1}{2}}\}$. If $|y| \geq X \geq 1$, then by Lemma 7.11,

$$h(x,y) \ll_N x^{N-1} + \frac{x^{N-1}}{|y|^N} \ll_N x^{\frac{N}{2}-1},$$

using $|y| \geq x^{\frac{1}{2}}$ and $x \ll 1$. As $f \ll_f 1$, the range $|y| \geq X$ makes a satisfactory contribution. For $|y| \leq X$, we use a Taylor series

$$f(y) = f(0) + yf^{'}(0) + \ldots + \frac{y^{2M}}{(2M)!}f^{(2M)}(0) + \frac{y^{2M+1}}{(2M+1)!}f^{(2M+1)}(\xi_{f,M,x})$$

for $\xi_{f,M,x} \in [0, X]$. We bound the error term

$$\frac{y^{2M+1}}{(2M+1)!}f^{(2M+1)}(\xi_{f,M,x}) \ll_{f,M} X^{2M+1}.$$

As $h(x,y) \ll x^{-1}$, the latter error contributes $\ll_{f,M} x^{-1}X^{2M+2} \ll_{f,M} x^M$. Finally, we conclude by using Lemma 7.12 and Lemma 7.14. □

7.3 General Analytic Statements

In this subchapter we collect some lemmas concerning general analytic statements of later use. We first start with two lemmas involving functions of compact support.

Lemma 7.16. *Let $B \subset \mathbb{R}^n$ be a bounded Jordan measurable subset. Then for any $\varepsilon > 0$ there are smooth compactly supported functions $w_\pm(x)$ on $\mathbb{R}^n$ so that*

$$w_- \leq \chi_B \leq w_+$$

and

$$\mathrm{vol}(B) - \varepsilon \leq \int_{\mathbb{R}^n} w_-\,dx \leq \mathrm{vol}(B) \leq \int w_+\,dx \leq \mathrm{vol}(B) + \varepsilon.$$

Proof. By definition, χ_B is Riemann integrable, hence there is a finite set of disjoint n-dimensional cuboids $C_1, \ldots, C_N \subset B$ whose edges are parallel to the coordinate axes with total volume at least $\mathrm{vol}(B) - \frac{\varepsilon}{2}$. Hence, it suffices to find non-negative compactly supported functions w_i so that $w_i \leq \chi_{C_i}$ for which

$$\mathrm{vol}(C_i) - \frac{\varepsilon}{2N} \leq \int w_i\,dx$$

as setting $w_- = \sum_{i=1}^N w_i$ then has the property

$$\mathrm{vol}(B) - \varepsilon \leq \sum_{i=1}^N \Big(\mathrm{vol}(C_i) - \frac{\varepsilon}{2N}\Big) \leq \int_{\mathbb{R}^n} w_-\,dx.$$

In order to construct such functions w_i, we use the function w_0 given by

$$w_0(x) = \begin{cases} e^{-(1-x^2)^{-1}} & |x| < 1, \\ 0 & |x| \geq 1. \end{cases}$$

and set

$$c_0 = \int_{-\infty}^{\infty} w_0 \, dx.$$

Write for suitable $A \leq B$ and $\eta > 0$,

$$w_{A,B,\eta}(x) = \eta^{-1} c_0^{-1} \int_{A+\eta}^{B-\eta} w_0 \left(\frac{x-y}{\eta} \right) dy.$$

As

$$\int_{A+\eta}^{B-\eta} w_0 \left(\frac{x-y}{\eta} \right) dy \leq \int_{\infty}^{\infty} w_0 \left(\frac{x-y}{\eta} \right) dy = \eta c_0,$$

it follows that $0 \leq w_{A,B,\eta} \leq 1$ and as w_0 is supported in $[-1,1]$, one concludes that $w_{A,B,\eta}$ is supported in $[A,B]$. Finally, observe that

$$\begin{aligned} \int_{-\infty}^{\infty} w_{A,B,\eta}(x) &= \eta^{-1} c_0^{-1} \int_{A+\eta}^{B-\eta} w_0 \left(\frac{x-y}{\eta} \right) dxdy \\ &= \eta^{-1} c_0^{-1} \int_{A+\eta}^{B-\eta} \eta c_0 \, dy = B - A - 2\eta. \end{aligned}$$

This if $C_i = \prod_{j=1}^n [A_j, B_j]$ the one takes

$$w_i(x) = \prod_{j=1}^{n} w(x_j, A_j, B_j, \eta)$$

for a small enough η so that w_- satisfies the properties we want. □

Lemma 7.17. *Let $w : \mathbb{R}^n \to \mathbb{R}$ be a smooth function of compact support. Then for any $\delta \in (0,1]$ there is a compactly supported smooth function $w_\delta \in \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ so that*

$$w(x) = \delta^{-n} \int w_\delta \left(\frac{x-y}{\delta}, y \right) dy.$$

Moreover $\mathrm{supp}(w_\delta(*, y)) \subset [-1,1]^n$ *for all $y \in \mathbb{R}^n$ and the function*

$$F(x) = w_\delta(\delta^{-1}(x-y), y)$$

has $\mathrm{supp}(F) \subset \mathrm{supp}(w)$ *for all fixed $y \in \mathbb{R}^n$.*

Proof. We choose the function

$$w_\delta(x,y) = c_0^{-n} w_0^{(n)}(x) w(\delta x + y).$$

Clearly this function is compactly supported. Moreover,

$$\int w_\delta \left(\frac{x-y}{\delta}, y \right) = w(x) c_0^{-n} \int w_0^{(n)} \left(\frac{x-y}{\delta} \right) dy = \delta^n w(x).$$

The claim on the support of $\mathrm{supp}(w_\delta(*, y))$ follows as w_0 is supported in $[-1,1]$. □

Let $w \in C_c^\infty(\mathbb{R}^n)$ and $f \in C_c^\infty(\mathrm{supp}(w))$. Suppose there is a positive real number λ and a set $A = \{A_2, A_3, \ldots\}$ of positive real numbers such that for all $x \in \mathrm{supp}(w)$ we have

$$|\nabla f(x)| \geq \lambda$$

and

$$|\partial_j f(x)| \leq A_{||j||_1}\lambda,$$

where $j = (j_1, \ldots, j_n) \in \mathbb{N}_0^n$ and $||j||_1 = j_1 + \ldots + j_n \geq 2$.

Lemma 7.18. *In the above setting, for any positive integer $N > 0$,*

$$\int w(x)e(f(x))\,dx \ll_{A,w,N} \lambda^{-N}.$$

Proof. We proceed by induction on N. If $N = 0$, then

$$\Big|\int w(x)e(f(x))\,dx\Big| \ll_w 1.$$

Assume that the statement is proved for N. Choose $\delta = (1 + 2nA_2)^{-1}$. By construction of the function w_δ,

$$\int w(x)e(f(x))\,dx = \delta^{-n} \int\int w_\delta\left(\frac{x-y}{\delta}, y\right) e(f(x))\,dxdy.$$

As w_δ is a function of compact support, which only depends on w and δ, it follows

$$\int w(x)e(f(x))\,dx \ll_{A,w} \int w_\delta\left(\frac{x-y}{\delta}, y\right) e(f(x))\,dx$$

for some fixed $y = (y_1, \ldots, y_n) \in \mathrm{supp}(w)$. Write for convenience $w_1(x) = w_\delta(\delta^{-1}(x-y), y)$. As $|\nabla f(y)| \geq \lambda$, it follows that without loss of generality,

$$\left|\frac{\partial f(y)}{\partial y_1}\right| \geq \frac{\lambda}{n}.$$

By the assumption of the lemma, it follows that

$$\left|\frac{\partial^2 f(x)}{\partial x_1^2}\right| \leq A_2\lambda.$$

Whenever $x = (x_1, y_2, \ldots, y_n)$ with $|x_1 - y_1| \leq \delta$, then by the mean value theorem,

$$\frac{\partial f(x)}{\partial x_1} = \frac{\partial f(y)}{\partial y_1} + (x_1 - y_1)\frac{\partial^2 f(\xi_x)}{\partial x_1^2}$$

for $\xi_x = (\xi_x^1, y_2, \ldots, y_n)$ with $\xi_x \in [y_1, x_1]$. Hence, by our choice of δ,

$$\left|\frac{\partial f(x)}{\partial x_1}\right| \geq \frac{\lambda}{n} - \delta \cdot A_2 \cdot \lambda > \frac{\lambda}{2n}, \tag{7.11}$$

whenever $|x_1 - y_1| < \delta$ and in particular if

$$w_1(x) = w_\delta\left(\frac{x-y}{\delta}, y\right) \neq 0.$$

We now prove under the assumption (7.11) on $\mathrm{supp}(w_1)$ the bound

$$\int w_1(x) e(f(x))\, dx \ll_{A,w,N} \lambda^{-(N+1)},$$

which clearly implies the statement of the lemma.

In order to prove this claim, we write the integrand as

$$\frac{w_1(x)}{2\pi i f_1(x)} \frac{\partial}{\partial x_1} e(f(x))$$

where $f_1 = \frac{\partial f}{\partial x_1}$. So we can integrate by parts with respect to x_1, to achieve

$$\int w_1(x) e(f(x))\, dx = -\left(\frac{2n}{\lambda}\right) \int w_2(x) e(f(x))\, dx$$

for

$$w_2(x) = \frac{\partial}{\partial x_1} \frac{w_1(x)}{2\pi i (\lambda/2n)^{-1} f_1(x)}.$$

The claim now follows by the induction hypothesis. □

Recall that $G = F^{(0)} - 1$. Define $\mathscr{C}(G)$ to be the class of compactly supported functions w so that there exists a real number $R \ll_{G,w} 1$ with the property that whenever $(x_0, y) \in \mathrm{supp}(w)$ where y is fixed, the function $G(x, y)$ has exactly one zero for $x \in \mathbb{R}$ and on $|x_0 - x| \leq R$,

$$\frac{\partial G(x,y)}{\partial x} \gg_{G,w} 1.$$

Lemma 7.19. *Let $w \in \mathscr{C}(G)$. Then*

$$\sigma_\infty(G, w) = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|G(v)| \leq \varepsilon} w(v)\, dv$$

exists and can be computed as

$$\sigma_\infty(G, w) = \int_{\mathbb{R}^{n-1}} \frac{w(x_1, y)}{(\partial_{x_1} G)(x_1, y)}\, dy,$$

where y runs over all vectors of $\mathbb{R}^{n-1}$ for which there is at least one $x \in \mathbb{R}$ with $(x, y) \in \mathrm{supp}(w)$ and $x_1 \in \mathbb{R}$ is the unique element so that $(x_1, y) \in \mathrm{supp}(w)$ and $G(x_1, y) = 0$.

If furthermore $w \in \mathscr{C}(G)$ is real-valued and non-negative everywhere and takes a strictly positive value for some real solution x of $G(x) = 0$, then $\sigma_\infty(G, w) > 0$.

Proof. Write $v \in \mathrm{supp}(w)$ as $v = (x, y)$ for $x \in \mathbb{R}$ and $y \in \mathbb{R}^{n-1}$. Let x_1 be the unique solution of $G(x_1, y) = 0$ given by the definition of $\mathscr{C}(G)$. Then if $|G(v)| \le \varepsilon$ we will have $|G(x, y) - G(x_1, y)| \le \varepsilon$. By Taylor's theorem

$$G(x, y) - G(x_1, y) = (x - x_1)(\partial_x G)(x_\xi, y)$$

for $x_\xi \in [x, x_1]$. As $(\partial_x G)(x, y) \gg_{G,w} 1$ on $|x - x_1| \le R$, it follows that

$$|x - x_1| = \frac{|G(x, y) - G(x_1, y)|}{|(\partial_x G)(x_\xi, y)|} \ll_{G,w} \varepsilon.$$

Thus, again by Taylor's theorem, $w(v) = w(x_1, y) + O_{G,w}(\varepsilon)$ and in particular,

$$\frac{1}{2\varepsilon} \int_{|G(v)| \le \varepsilon} w(v)\, dv = \frac{1}{2\varepsilon} \int_{|G(v)| \le \varepsilon} w(x_1, y)\, dv + O_{G,w}\left(\int_{|G(v)| \le \varepsilon} 1\, dv \right)$$

All of these integrals are over $\mathrm{supp}(w)$ and as each possible x belongs to an interval of length $\ll_{G,w} \varepsilon$ and as w is compactly supported, it follows that the error term is $O_{G,w}(\varepsilon)$. It remains to deal with

$$\frac{1}{2\varepsilon} \int_{|G(v)| \le \varepsilon} w(x_1, y)\, dv.$$

Again by Taylor's theorem

$$G(x, y) = (x - x_1)(\partial_{x_1} G)(x_1, y) + O_{G,w}(\varepsilon^2),$$

as the second partial derivative is $O_{G,w}(1)$ in the relevant region. In particular, the condition $|G(x, y)| \le \varepsilon$ defines an interval I_y of possible values for x of length

$$\frac{2\varepsilon}{(\partial_{x_1} G)(x_1, y)} + O_{G,w}(\varepsilon^2).$$

Thus if y is fixed and $v = (x, y) \in \mathrm{supp}(w)$ for all $x \in I_y$, then

$$\begin{aligned} \frac{1}{2\varepsilon} \int_{|G(v)| \le \varepsilon} w(x_1, y)\, dx &= \frac{w(x_1, y)}{2\varepsilon} \cdot \left(\frac{2\varepsilon}{(\partial_{x_1} G)(x_1, y)} + O_{G,w}(\varepsilon^2) \right) \\ &= \frac{w(x_1, y)}{(\partial_{x_1} G)(x_1, y)} + O_{G,w}(\varepsilon), \end{aligned}$$

where the integral is over those x for which $(x, y) \in \mathrm{supp}(w)$.

On the other hand if $(x_0, y) \notin \mathrm{supp}(w)$ for some $x_0 \in I_y$, then $w(x_0, y) = 0$ and as $|x_1 - x_0| \ll_{G,w} \varepsilon$ it follows that $w(x_1, y) \ll_{G,w} \varepsilon$. Thus

$$\frac{1}{2\varepsilon} \int_{|G(x)| \le \varepsilon} w(x_1, y)\, dx \ll_{G,w} |\{x \in \mathbb{R} : |G(x, y)| \le \varepsilon\}| \ll_{G,w} \varepsilon$$

and

$$\frac{w(x_1, y)}{(\partial_{x_1} G)(x_1, y)} \ll_{G,w} \varepsilon$$

so that we still have

$$\frac{1}{2\varepsilon} \int_{|G(v)| \le \varepsilon} w(x_1, y)\, dx = \frac{w(x_1, y)}{(\partial_{x_1} G)(x_1, y)} + O_{G,w}(\varepsilon).$$

To summarize we have proved that

$$\frac{1}{2\varepsilon}\int_{|G(v)|\leq\varepsilon} w(v)\,dv = \frac{1}{2\varepsilon}\int_{|G(v)|\leq\varepsilon} \frac{w(x_1,y)}{(\partial_{x_1}G)(x_1,y)}\,dy + O_{G,w}(\varepsilon),$$

which implies the main claim.

The positivity property is immediate. □

Corollary 7.20. *In the above setting, assume that* $\nabla G \neq 0$ *on* $\operatorname{supp}(w)$*. Then the limit*

$$\sigma_\infty(G,w) = \lim_{\varepsilon\to 0}\frac{1}{2\varepsilon}\int_{|G(x)|\leq\varepsilon} w(x)\,dx$$

exists.

Proof. This follows by just applying the last lemma locally. □

7.4 Estimating $I_q(c)$

Recall that the function $I_q(c)$, depending on w, P, Q and $c \in \mathbb{Z}^n$, was defined in (7.6) as

$$\begin{aligned} I_q(c) &= \int_{\mathbb{R}^n} w(P^{-1}x)h(Q^{-1}q, Q^{-2}F(x))e_q(-\langle c,x\rangle)\,dx. \\ &= P^n\int_{\mathbb{R}^n} w(x)h(Q^{-1}q, Q^{-2}P^kG(x))e_q(-\langle c,Px\rangle)\,dx, \end{aligned}$$

where we substituted x by Px. By this formula, it is suitable to fix from now on $Q = P^{k/2}$. The aim of this subchapter is to give useful estimates of $I_q(c)$.

Lemma 7.21. *In the above setting, for* $q \gg_{G,w} Q$*,* $I_q(c) = 0$*.*

Proof. In Theorem 7.1 we have seen that $h(x,y)$ is zero unless $x \leq \max(1, 2|y|)$. Thus if

$$Q^{-1}q > 2\sup_{x\in\operatorname{supp}(w)} 2|G(x)|,$$

then $w(x)h(Q^{-1}q, G(x)) = 0$ for all $x \in \mathbb{R}^n$. □

We introduce some more notation. For $v \in \mathbb{R}^n$ and $r \in \mathbb{R}$, set

$$I_r^*(v) = \int_{\mathbb{R}^n} w(x)h(r, G(x))e_r(-\langle v,x\rangle)\,dx.$$

Thus

$$I_q(c) = P^nI_r^*(v)$$

for $r = Q^{-1}q$ and $v = Q^{-1}Pc$.

Lemma 7.22. *Let* $w \in \mathscr{C}(G)$*. Then for* $r \ll 1$ *and* $N > 0$*,*

$$I_r^*(0) = \sigma_\infty(G,w) + O_{G,w,N}(r^N).$$

In particular for $q \ll Q$*,*

$$I_q(0) = P^n(\sigma_\infty(G,w) + O_{G,w,N}((Q^{-1}q)^N).$$

Proof. As $w \in \mathscr{C}(G)$,

$$\partial_{x_1} G \gg_{G,w} 1$$

on supp(w). Thus we can substitute $y = G(x)$ for x_1 in the integral

$$I_r^*(0) = \int_{\mathbb{R}^n} w(x)h(r, G(x))\, dx = \int_{\mathbb{R}} I(y)h(r, y)\, dy,$$

where

$$I(y) = \int_{\mathbb{R}^{n-1}} \frac{w(x_1, z)}{(\partial_{x_1} G)(x_1, z)} dz$$

and for fixed y and z we choose x_1 to be the unique solution of $G(x_1, z) = y$. As I has compact support, it follows from Proposition 7.9,

$$\int I(y)h(r, y)\, dy = I(0) + O_{G,w,N}(r^N) = \sigma_\infty(G, w) + O_{G,w,N}(r^N).$$

□

In the remainder of this subchapter, we aim at giving upper bounds for $I_r^*(v)$ or $I_q(c)$. In order to discern the required properties of the function w, we define the vector space $\mathscr{F}$ consisting of smooth functions $f : (0, \infty) \times \mathbb{R} \to \mathbb{R}$ with the property that for any positive integer N there are positive real numbers $K_{0,N}, K_{1,N}, \ldots$ so that

$$|f(r, x)| \leq K_{0,N} \left(r^N + \min\left\{ 1, \left(\frac{r}{|x|}\right)^N \right\} \right)$$

and for $\ell \geq 1$,

$$\left| \frac{\partial^\ell f(r, x)}{\partial x^\ell} \right| \leq K_{\ell,N} \cdot r^{-\ell} \cdot \min\left\{ 1, \left(\frac{r}{|x|}\right)^N \right\}.$$

In order to bound $I_r^*(v)$, we introduce in the dependence on the function $f \in \mathscr{F}$ and $\omega \in \mathscr{C}(G)$,

$$I(u) = I(r, u) = \int_{\mathbb{R}^n} \omega(x) f(r, G(x)) e(-\langle u, x\rangle)\, dx,$$

for $r > 0$ and $u \in \mathbb{R}^n$.

Lemma 7.23. *Let $r \ll 1$. Then*

$$|I_r^*(v)| \ll r^{-1} |I(r^{-1}v)|$$

for appropriate functions $f \in \mathscr{F}$ and $\omega \in \mathscr{C}(G)$. Moreover, if $v = 0$,

$$|\partial_r I_r^*(v)| \ll r^{-2} |I(r^{-1}v)|,$$

for appropriate functions $f \in \mathscr{F}$ and $\omega \in \mathscr{C}(G)$.

Proof. For $k = 0, 1$ write

$$f^k(r,x) = r^{k+1}\frac{\partial^k h(r,x)}{\partial r^k}.$$

Then by Lemma 7.11, $f^0, f^1 \in \mathscr{F}$ and so

$$|I_r^*(v)| \leq \frac{1}{r}\left|\int_{\mathbb{R}^n} w(x) f^k(r, G(x)) e(-\langle r^{-1}v, x\rangle)\, dx\right| = r^{-1}|I(r^{-1}v)|.$$

We begin to discuss $\partial_r I_r^*(v)$. Notice

$$\begin{aligned}
\partial_r I_r^*(v) &= \int_{\mathbb{R}^n} w(x)\partial_r\big(\, h(r,G)e_r(-\langle v,x\rangle)\,\big)\, dx \\
&= \int_{\mathbb{R}^n} w(x)(\partial_r h)(r,G)e_r(-\langle v,x\rangle)\, dx \\
&+ \int_{\mathbb{R}^n} w(x)h(r,G)e_r(-\langle v,x\rangle)\left(-\frac{2\pi i\langle v,x\rangle}{r}\right)\, dx
\end{aligned}$$

By a slight abuse of notation, we drop the r in the expression $f(r,x)$ for convenience. Set for $k = 0, 1$,

$$I^{(k)}(u) = \int_{\mathbb{R}^n} w(x) f^k(G(x)) e(-\langle u,x\rangle)(-2\pi i\langle u,x\rangle)^k\, dx$$

so that for either $k = 0$ or 1,

$$\frac{\partial I_r^*(v)}{\partial r} \ll r^{-2}|I^{(k)}(r^{-1}v)|,$$

depending on which of the two terms is larger. Setting either $k = 0$ or $v = 0$, the claim follows. $\square$

Lemma 7.24. *For $r \ll 1$ and any vector $u \in \mathbb{R}^n$,*

$$|I(r,u)| \ll_{G,\omega} r.$$

Proof. We calculate using the definition of $f \in \mathscr{F}$,

$$\begin{aligned}
|I(r,u)| &\leq \int_{\mathbb{R}^n} |\omega(x)||f(r,G(x))|\, dx \\
&\ll_\omega \int_{\mathrm{supp}(\omega)} |f(r,G(x))|\, dx \\
&\ll_\omega \int_{\mathrm{supp}(\omega)} \left(r + \min\left\{1, \left(\frac{r}{|G(x)|}\right)\right\}\right)\, dx.
\end{aligned}$$

As $\partial_{x_1} G \gg_{G,\omega} 1$, it follows that the set S where $|G(x)| \leq r$ is of measure $O_{G,\omega}(r)$ and so the claim follows as on the set S, by definition $\frac{r}{|G(x)|} \geq 1$, showing,

$$\begin{aligned}
&\ll_w \int_{\mathrm{supp}(\omega)} \left(r + \min\left\{1, \left(\frac{r}{|G(x)|}\right)\right\}\right)\, dx \\
&\ll_w \int_{\mathrm{supp}(\omega)} r\, dx + \int_S 1\, dx \\
&\ll_{G,w} r + |S| \ll_{G,w} r.
\end{aligned}$$

$\square$

As a consequence of the previous lemmas, we deduce the next claim.

Lemma 7.25. *For $j = 0, 1$ and $q \ll Q$,*

$$|\partial_q^j I_q(0)| \ll_{G,w} P^n q^{-j},$$

were we assume $1 \ll Q^{-1}q$ in the case $j = 1$.

Proof. For $j = 0$ this is Lemma 7.22. For $j = 1$, recall $I_q(0) = P^n I^*_{Q^{-1}q}(0)$ and so by Lemma 7.23,

$$\begin{aligned}|\partial_q I_q(0)| &= P^n |\partial_q I^*_{Q^{-1}q}(0)| \\ &\ll P^n (Q^{-1}q)^{-2} |I(0)| Q^{-1} \\ &\ll_{G,w} P^n Q q^{-2} \ll_{G,w} P^n q^{-1},\end{aligned}$$

where we used $1 \ll Q^{-1}q$ so that in particular $Qq \ll 1$. □

Lemma 7.26. *There exist weights $w_1, w_2 \in \mathscr{C}(G)$ with $\operatorname{supp}(w_2) \subset \operatorname{supp}(\omega)$ so that if p is the Fourier transform of $w_1(x)f(x)$ then*

$$I(r,u) = \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w_2(x) e(tG(x) - \langle u, x\rangle)\, dxdt$$

and

$$p(t) \ll_{G,f,N} r(r|t|)^{-N}$$

for any $N \geq 0$.

Proof. Choose $1 \ll_{G,f} K \ll_{G,f} 1$ so that $|G(x)| \leq K$ on $\operatorname{supp}(\omega)$. Write $w_1(t) = w_0((2K)^{-1}t)$ and as $w_1(G(x)) \gg 1$ on $\operatorname{supp}(\omega)$, we set

$$w_2(x) = \frac{\omega(x)}{w_1(G(x))}.$$

Thus

$$I(r,u) = \int_{\mathbb{R}^n} w_2(x) w_1(G(x)) f(G(x)) e(-\langle u, x\rangle)\, dx.$$

Using the Fourier transform, we write

$$w_1(G(x)) f(G(x)) = \int_{-\infty}^{\infty} p(t) e(tG(x))\, dt$$

with

$$p(t) = \int_{-\infty}^{\infty} w_1(v) f(v) e(-tv)\, dv$$

so that

$$I(r,u) = \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w_2(x) e(tG(x) - \langle u, x\rangle)\, dxdt.$$

Finally, to prove the bound on $p(t)$, as $f \in \mathscr{F}$ and the support of w_1 depends only on G and f,

$$\frac{d^N}{dv^N} w_1(v) f(v) \ll_{N,G,f} r^{-N} \min\left\{1, \left(\frac{r}{|v|}\right)^2\right\}.$$

Thus by partial integration,

$$\begin{aligned}
|p(t)| &\le \frac{1}{|t|^N} \int_{-\infty}^{\infty} \left| \frac{d^N}{dv^N} w_1(v) f(v) \right| dv \\
&\ll_{N,G,f} \frac{1}{|t|^N} \int_{|v|\le r} r^{-N}\, dv + \frac{1}{|t|^N} \int_{|v|>r} \frac{r^{-N+2}}{|v|^2}\, dv \\
&\ll_{N,G,f} \frac{r^{-N+1}}{|t|^N}.
\end{aligned}$$

□

Lemma 7.27. *For any $N \ge 0$ and $r \ll 1$,*

$$I(r,u) \ll_{G,w,N} r^{-N} |u|^{-N}.$$

Proof. We use Lemma 7.26 to write

$$I(r,u) = \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w_2(x) e(tG(x) - \langle u, x \rangle)\, dx dt.$$

For $|u| \gg_{G,w} |t|$, by Lemma 7.18 for $M > 0$,

$$\int_{\mathbb{R}^n} w_2(x) e(tG(x) - \langle u, x\rangle)\, dx \ll_{G,w} |u|^{-M}.$$

If $|u| \ll_{G,w} |t|$, then we use the trivial estimate $\ll_{G,w} 1$. Using $r \ll 1$,

$$\begin{aligned}
|I(r,u)| &\le \left| \int_{|u| \ll_{G,w} |t|} p(t) \int_{\mathbb{R}^n} (w_3(x) e(tG(x) - \langle u, x\rangle)\, dx dt \right| \\
&\quad + \left| \int_{|u| \gg_{G,w} |t|} p(t) \int_{\mathbb{R}^n} (w_3(x) e(tG(x) - \langle u, x\rangle)\, dx dt \right| \\
&\ll_{G,w,M} \int_{|u| \ll_{G,w} |t|} |p(t)|\, dt + \int_{|u| \gg_{N,G,w} |t|} |p(t)| |u|^{-M} dt \\
&\ll_{G,w,M} \int_{|u| \ll_{G,w} |t|} r^{1-M} |t|^{-M}\, dt + \int_{|u| \gg_{N,G,w} |t|} r |t|^{-M} dt \\
&\ll_{G,w,M} r^{1-M} |u|^{1-M} + r \int_{|u| \gg_{N,G,w} |t|} |t|^{-M} dt \\
&\ll_{G,w,M} r^{1-M} |u|^{1-M} + r|u|^{1-M} \ll_{M,G,w} r^{1-M} |u|^{1-M},
\end{aligned}$$

were we used in the third line the bound from Lemma 7.26 in the case $N = M$ for the first integral and in the case $N = 0$ in the second integral. In the last line we used $r \ll 1$, in which implies the claim by setting $N = M - 1$. □

Lemma 7.28. *When $k = 2$ and $c \neq 0$,*

$$|I_q(c)| \ll_{G,w,N} P^{n+1} q^{-1} |c|^{-N}.$$

Proof. As $k = 2$, $P = Q$ and by Lemmas 7.23 and 7.27,

$$\begin{aligned} |I_q(c)| &= P^n |I^*_{Q^{-1}q}(Q^{-1}Pc)| \\ &= P^n |I^*_{Q^{-1}q}(c)| \\ &\ll P^n Q q^{-1} |I(Q^{-1}q, Qq^{-1}c)| \\ &\ll_{G,w,N} P^n Q q^{-1} |c|^{-N} \\ &\ll_{G,w,N} P^{n+1} q^{-1} |c|^{-N}. \end{aligned}$$

□

We next want to give improved estimates of $I(r, u)$. Let $R \geq 1$ and $u \in \mathbb{R}^n$ be fixed for the moment. For an appropriate value of t in the range

$$|u| \ll_{G,w} |t| \ll_{G,w} |u|$$

we set

$$\mathcal{S} = \{x \in \operatorname{supp}(\omega) \, : \, |t\nabla G(x) - u| \ll_{G,w} R|u|^{\frac{1}{2}}\}.$$

Lemma 7.29. *Let $R \gg_G 1$. If $u \in \mathbb{R}^n$ with $|u| \geq R^3$, then*

$$|I(r, u)| \ll_{G,w,N} R^{-N} + r \cdot |u| \cdot \operatorname{vol}(\mathcal{S}).$$

Proof. If $r|u| \geq R$, then $r^{-N}|u|^{-N} \leq R^{-N}$ and so the claim follows from Lemma 7.27. Thus in the following we assume $r|u| \leq R$.

We use the functions w_δ from Lemma 7.17 for w_2 as in Lemma 7.26 and some $\delta = |u|^{-\frac{1}{2}}$, whose choice will be explained later. Then

$$\begin{aligned} I(r, u) &= \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w_2(x) e(tG(x) - \langle u, x\rangle) \, dxdt \\ &= \delta^{-n} \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} \int_{\mathbb{R}^n} w_\delta \left(\frac{x-y}{\delta}, y \right) e(tG(x) - \langle u, x\rangle) \, dxdydt \\ &= \int_{\mathbb{R}^n} \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w_\delta\,(z, y)\, e(tG(x) - \langle u, x\rangle) \, dzdtdy, \end{aligned}$$

where we substituted $x = y + \delta z$ in the last line. In particular,

$$|I(r, u)| \leq \int_{\mathbb{R}^n} \int_{-\infty}^{\infty} |p(t)| \left| \int_{\mathbb{R}^n} w_\delta\,(z, y)\, e(tG(x) - \langle u, x\rangle) \, dz \right| dtdy.$$

The variable y runs over a range $\ll_w 1$. We analyze the inner most integral further, for which we fix for the moment the values y and t. For convenience write

$$f(z) = tG(y + \delta z) + \langle u, y + \delta z\rangle.$$

Notice that

$$|\nabla f(0)| = \delta |t\nabla G(y) - u| = |u|^{-\frac{1}{2}} |t\nabla G(y) - u|.$$

Moreover, the partial derivatives of order $k \geq 2$ are $O_{G,k}(|t|\delta^k)$. So we choose $R \gg_G 1$ yielding δ is small enough so that for all $z \in \operatorname{supp}(w_\delta(*, y))$,

$$|\nabla f(z)| = |\nabla f(0)| + O_G(|t|\delta^2) \gg_G |\nabla f(0)|.$$

We want to apply Lemma 7.18. In order to do this we distinguish two cases. First assume that the point (y, t) is *good*, i.e.

$$|\nabla f(0)| = |u|^{-\frac{1}{2}} |t\nabla G(y) - u| \geq R \max\{\tfrac{t}{|u|}, 1\}.$$

Then $|\nabla f(z)| \gg R$ and so in by Lemma 7.18,

$$\int_{\mathbb{R}^n} w_\delta(x, y) e(tG(x) - \langle u, x\rangle)\, dz \ll_{G,N} R^{-N}.$$

On the other hand, if (y, t) is *bad*, i.e.

$$|t\nabla G(y) - u| \leq R|u|^{\frac{1}{2}} \max\{\tfrac{|t|}{|u|}, 1\}$$

Notice that any relevant y is within δ of some point of $\operatorname{supp}(w)$. As $\delta = |u|^{-\frac{1}{2}} \leq R^{-\frac{3}{2}}$ it follows for $R \gg_G 1$, that $|\nabla G(y)| \gg 1$. As $|u| \ll_G |t| \ll_G |u|$, we have

$$|t\nabla G(y) - u| \ll_G R|u|^{\frac{1}{2}}$$

for all bad (y, t). Together with the estimate on the good (y, t),

$$|I(r, u)| \ll_{G,w,N} R^{-N} + \int_y \int_{-\infty}^{\infty} |p(t)| \int_z |w_\delta(z, y)|\, dzdtdy$$

where (y, t) runs over the *bad* values and $y \ll_{G,w} 1$. Finally we substitute $x = y + \delta z$ for y and observe that

$$t\nabla G(y) - t\nabla G(y) \ll_{G,w} |t|\delta \ll_{G,w} |u|^{\frac{1}{2}} \ll_{G,w} R|u|^{\frac{1}{2}}.$$

So if y satisfies $|t\nabla G(y) - u| \ll_G R|u|^{\frac{1}{2}}$ then so does x with a different constant. Moreover, $w_\delta(z) \neq 0$ implies that $x \in \operatorname{supp}(w)$ and $z \ll_{G,w} 1$. Finally, by Lemma 7.26, $|p(t)| \ll_{G,w} r$. Thus the claim follows. □

We denote the Hessian of $G(x)$ by $H(x)$ so that

$$H_{ij}(x) = \frac{\partial^2}{\partial x_i \partial x_j} G(x).$$

Lemma 7.30. *If* $|\det H(x)| \gg_{G,w} 1$ *for all* $x \in \operatorname{supp}(\omega)$, *then*

$$\operatorname{vol}(\mathcal{S}) \ll_{G,w} |u|^{-\frac{n}{2}} R^n.$$

Proof. As $|u| \ll_{G,w} |t| \ll_{G,w} |u|$ the condition in the definition of $\mathcal{S}$, translates to $|\nabla G(x) - u| \ll_{G,w} R|u|^{-\frac{1}{2}}$. As each of the entries of H satisfies $\ll_{G,w} 1$, the Hessian condition implies that none of the columns of $H(x)$ has too small entries which implies the claim. □

Combining the last two lemmas, we arrive at the following statement.

Corollary 7.31. *Suppose that $n \geq 3$ and that the condition on the Hessian of Lemma 7.30 holds. Then for any $\varepsilon \in (0, \frac{1}{2})$ we have*

$$|I(r,u)| \ll_{G,w,\varepsilon} (r^{-1}|u|)^{\varepsilon} r|u|^{1-\frac{n}{2}}.$$

Hence

$$I_q(c) \ll_{G,w,\varepsilon} P^n \left(\frac{PQ|c|}{q^2}\right)^{\varepsilon} \left(\frac{P|c|}{q}\right)^{1-\frac{n}{2}}.$$

Proof. To deduce the second claim from the first, recall for $r = Q^{-1}q$ and $v = Q^{-1}Pc$, with Lemma 7.23,

$$|I_q(c)| = P^n|I_r^*(v)| \ll P^n|I(r, r^{-1}v)| \ll P^n P^n \left(\frac{PQ|c|}{q^2}\right)^{\varepsilon} \left(\frac{P|c|}{q}\right)^{1-\frac{n}{2}},$$

assuming the first claim. So it remains to show the first claim.

If $|u| \ll_{G,w} r^{-\frac{2\varepsilon}{n}}$ then

$$|u|^{\frac{n}{2}-1-\varepsilon} \ll |u|^{-\frac{n}{2}} \ll_{G,w} r^{-\varepsilon}$$

as since $n \geq 3$,

$$0 < \frac{n}{2} - 1 - \varepsilon < \frac{n}{2}.$$

Thus

$$r \ll (r^{-1}|u|)^{\varepsilon} r|u|^{1-\frac{n}{2}}$$

and so the estimate follows from Lemma 7.24.

If $u \gg r^{\frac{2\varepsilon}{n}}$, we set $R = C_{G,w}(r^{-1}|u|)^{\frac{\varepsilon}{3n}}$ for $C_{G,w}$ a suitably large constant. The condition $|u| \geq R^3$ is equivalent to $|u| \gg_{G,w} r^{-\frac{\varepsilon}{n-\varepsilon}}$ which is satisfactory as

$$\frac{2\varepsilon}{n} \geq \frac{\varepsilon}{n-\varepsilon}.$$

Thus Lemma 7.30 yields

$$|I(r,u)| \ll_{G,w,N} R^{-N} + r|u|^{1-\frac{n}{2}} R^n.$$

We clearly have $R^n \ll_{G,w} (r^{-1}|u|)^{\varepsilon}$ by our choice of R and $R^{-N} \ll_{G,w} (r^{-1}|u|)r|u|^{1-\frac{n}{2}}$ provided that

$$\frac{\varepsilon}{3n} N \geq \max\left\{\frac{n}{2} - 1 - \varepsilon, 1 - \varepsilon\right\},$$

which we are allowed to assume. □

7.5 Estimating $S_q(c)$

Throughout this entire subchapter we assume that $k = 2$, i.e. that $F^{(0)}$ is a quadratic form. Recall that $F = F^{(0)} - m$ for some integer m. We write $F^{(0)}(x) = x^T M x$ for $M \in \mathrm{M}_{n,n}(\mathbb{Z})$ a symmetric matrix.

By (7.4), $S_q(c)$ is defined in dependence of F, $q \geq 1$ and $c \in \mathbb{Z}^n$ as

$$S_q(c) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ b \in \mathbb{Z}^n}}^{q} e_q(aF(b) + \langle b, c \rangle).$$

Lemma 7.32. *Let q_1 and q_2 be coprime positive integers and denote by q_1' and q_2' any integers so that $q_1q_1' \equiv 1 \mod q_2$ and $q_2q_2' \equiv 1 \mod q_1$. Then*

$$S_{q_1q_2}(c) = S_{q_1}(q_2'c)S_{q_2}(q_1'c).$$

Proof. By definition,

$$S_{q_1q_2}(c) = \sum_{\substack{a=1\\(a,q_1q_2)=1}}^{q_1q_2} \sum_{\substack{b=1\\b\in\mathbb{Z}^n}}^{q_1q_2} e_{q_1q_2}(aF(b) + \langle b, c\rangle).$$

The idea of the proof is to write $a = q_1a_2 + q_2a_1$ for a_1 varying from 1 to q_1 with $(a_1, q_1) = 1$ and a_2 varying from 1 to q_2 for $(a_2, q_2) = 1$ and $b = q_1q_1'b_2 + q_2q_2'b_1$ for b_1 and b_2 varying analogously. In the calculation below we also use that

$$\begin{aligned} q_1a_2F(b_2) + q_2a_1F(b_1) &\equiv (q_1a_2 + q_2a_1)\left(F(q_2q_2'b_1) + F(q_1q_1'b_2)\right) \mod q_1q_2 \\ &\equiv (q_1a_2 + q_2a_1)F(q_2q_2'b_1 + q_1q_1'b_2) \mod q_1q_2, \end{aligned}$$

which quickly follows by our definition of F and as $q_2q_2' \equiv 1 \mod q_1$ and $q_1q_1' \equiv 1 \mod q_2$.

Thus

$$\begin{aligned} S_{q_1}(q_2'c)S_{q_2}(q_1'c) &= \left(\sum_{\substack{a_1=1\\(a_1,q_1)=1}}^{q_1} \sum_{\substack{b_1=1\\b_1\in\mathbb{Z}^n}}^{q_1} e_{q_1}(a_1F(b_1) + \langle b_1, q_2'c\rangle)\right)\cdot \\ &\cdot\left(\sum_{\substack{a_2=1\\(a_2,q_2)=1}}^{q_2} \sum_{\substack{b_2=1\\b_2\in\mathbb{Z}^n}}^{q_2} e_{q_2}(a_2F(b_2) + \langle b_2, q_1'c\rangle)\right) \\ &= \sum_{a_1,b_1,a_2,b_2} e^{2\pi i\left(\frac{a_1F(b_1)+\langle b_1,q_2'c\rangle}{q_1} + \frac{a_2F(b_2)+\langle b_2,q_1'c\rangle}{q_2}\right)} \\ &= \sum_{a_1,b_1,a_2,b_2} e^{2\pi i\left(\frac{q_1a_2F(b_2)+q_2a_1F(b_1)+\langle q_2q_2'b_1+q_1q_1'b_2,c\rangle}{q_1q_2}\right)} \\ &= \sum_{a_1,b_1,a_2,b_2} e^{2\pi i\left(\frac{(q_1a_2+q_2a_1)F(q_2q_2'b_1+q_1q_1'b_2)+\langle q_2q_2'b_1+q_1q_1'b_2,c\rangle}{q_1q_2}\right)} \\ &= \sum_{\substack{a=1\\(a,q_1q_2)=1}}^{q_1q_2} \sum_{\substack{b=1\\b\in\mathbb{Z}^n}}^{q_1q_2} e_{q_1q_2}(aF(b) + \langle b, c\rangle) = S_{q_1q_2}(c). \end{aligned}$$

□

Lemma 7.33. *Let p be a prime number. Let $t \geq 2$ and $s = [\frac{t}{2}]$. Then for $c \in \mathbb{Z}^n$,*

$$S_{p^t}(c) = p^{s(n+1)} \sum_{\substack{d=1\\(d,p^{t-s})=1}}^{p^{t-s}} \sum_{\substack{x=1,x\in\mathbb{Z}^n\\p^s|F(x)\\p^s|d\nabla F(x)+c}}^{p^{t-s}} e_{p^t}(dF(x) + \langle x, c\rangle).$$

Proof. In the definition for $S_{p^t}(c)$, we substitute for $a = d + p^{t-s}f$. Thus

$$\begin{aligned}
S_{p^t}(c) &= \sum_{\substack{a=1\\(a,p^t)=1}}^{p^t} \sum_{\substack{b=1\\b\in\mathbb{Z}^n}}^{p^{t-s}} e_{p^t}(aF(b) + \langle b,c\rangle)\\
&= \sum_{\substack{d=1\\(d,p^{t-s})=1}}^{p^{t-s}} \sum_{f=1}^{p^s} \sum_{\substack{b=1\\b\in\mathbb{Z}^n}}^{p^t} e_{p^t}(dF(b) + \langle b,c\rangle) e_{p^s}(fF(b))\\
&= p^s \sum_{\substack{d=1\\(d,p^{t-s})=1}}^{p^{t-s}} \sum_{\substack{b=1\\b\in\mathbb{Z}^n\\p^s|F(b)}}^{p^t} e_{p^t}(dF(b) + \langle b,c\rangle),
\end{aligned}$$

where we used Lemma 7.2 in the last line.

In the last equation we want to replace $b = x + p^{t-s}y$, for $x \in \mathbb{Z}^n$ varying from 1 to p^{t-s} and $y \in \mathbb{Z}^n$ varying from 1 to p^s. In order to proceed with this calculation further, we claim that

$$d \cdot F(x + p^{t-s}y) = d \cdot F(x) + p^{t-s} \cdot d \cdot \langle y, \nabla F(x)\rangle \mod p^t.$$

To see this, we recall that $F(x) = F^{(0)}(x) - m = x^T Mx - m$ for M a symmetric matrix and m an integer which might be zero. As $(d, p^{t-s}) = 1$, we can drop the d in the above formula. Then using $\nabla F(x) = 2Mx$ in the third line,

$$\begin{aligned}
F(x + p^{t-s}y) &= (x + p^{t-s}y)^T M(x + p^{t-s}y) - m\\
&= x^T Mx - m + p^{t-s}(y^T Mx + x^T My) + p^{2t-s} y^T My\\
&= F(x) + p^{t-s}\langle y, \nabla F(x)\rangle + p^{2(t-s)} y^T My.
\end{aligned}$$

As $2(t - s) \geq t$, it follows that mod p^t the last term vanishes and the above claim follows. Thus as $p^s | p^{t-s}$ by our choice of s,

$$\begin{aligned}
S_{p^t}(c) &= p^s \sum_{\substack{d=1\\(d,p^{t-s})=1}}^{p^{t-s}} \sum_{\substack{b=1\\b\in\mathbb{Z}^n\\p^s|F(b)}}^{p^t} e_{p^t}(dF(b) + \langle b,c\rangle)\\
&= p^s \sum_{\substack{d=1\\(d,p^{t-s})=1}}^{p^{t-s}} \sum_{\substack{x=1\\x\in\mathbb{Z}^n\\p^s|F(x)}}^{p^{t-s}} \sum_{\substack{y=1\\y\in\mathbb{Z}^n}}^{p^s} e_{p^t}(dF(x + p^{t-s}y) + \langle x + p^{t-s}y, c\rangle)\\
&= p^s \sum_{\substack{d=1\\(d,p^{t-s})=1}}^{p^{t-s}} \sum_{\substack{x=1\\x\in\mathbb{Z}^n\\p^s|F(x)}}^{p^{t-s}} \sum_{\substack{y=1\\y\in\mathbb{Z}^n}}^{p^s} e_{p^t}(dF(x) + \langle x,c\rangle) e_{p^s}(d \cdot \langle y, \nabla F(x)\rangle + \langle y,c\rangle).
\end{aligned}$$

As

$$\sum_{\substack{y=1\\ y\in\mathbb{Z}^n}}^{p^s} e_{p^s}(d\cdot\langle y,\nabla F(x)+\langle y,c\rangle) = \prod_{i=1}^{n}\sum_{y_i=1}^{p^s} e_{p^s}(y_i(d\tfrac{\partial F(x)}{\partial x_i}+c_i))$$

$$= \begin{cases} p^{sn} & \text{if } p^s|d\nabla F(x)+c,\\ 0 & \text{else,}\end{cases}$$

The claim follows:

$$S_{p^t}(c) = p^s \sum_{\substack{d=1\\ (d,p^{t-s})=1}}^{p^{t-s}} \sum_{\substack{x=1,x\in\mathbb{R}^n\\ p^s|F(x)\\ p^s|d\nabla F(x)+c}}^{p^{t-s}} e_{p^t}(dF(x)+\langle x,c\rangle)e_{p^s}(d\cdot\langle y,\nabla F(x)+\langle y,c\rangle).$$

□

We set throughout the remainder of this subchapter $\triangle = 2|\det(M)|$. Before proceeding with the next statement, we discuss a general lemma on homogeneous polynomials.

Lemma 7.34. *Let $F^{(0)}:\mathbb{R}^n\to\mathbb{R}$ be a homogeneous polynomial function of degree k. Then for all $x\in\mathbb{R}^n$,*

$$\langle x,\nabla F^{(0)}(x)\rangle = k\cdot F^{(0)}(x).$$

Moreover, if $k=2$ and $F^(0))(x) = x^TMx$ for $M\in \mathrm{M}_{n,n}(\mathbb{R})$ a symmetric matrix, then

$$\nabla F^{(0)}(x) = 2Mx.$$

Proof. Let $\alpha\in\mathbb{R}$. Then as $F^{(0)}$ is homogeneous, $F^{(0)}(\alpha x) = \alpha^k F^{(0)}(x)$ for $x\in\mathbb{R}^n$. Differentiating the latter equation with respect to α, yields

$$\sum_{i=1}^{n}\frac{\partial F^{(0)}}{\partial x_i}(\alpha x)x_i = k\alpha^{k-1}F^{(0)}(x).$$

By setting $\alpha=1$ the first claim follows.

For the second claim denote by $(D_xF^{(0)})(v)$ the directional derivative of $F^{(0)}$ at the point $x\in\mathbb{R}^n$ in the direction of $v\in T_x\mathbb{R}^n\cong\mathbb{R}^n$. The second statement of the lemma is implied by the calculation

$$\begin{aligned}(D_xF^{(0)})(v) &= \lim_{t\to 0}\frac{F^{(0)}(x+tv)-F^{(0)}(x)}{t}\\ &= \lim_{t\to 0}\frac{(x+tv)^TM(x+tv)-x^TMx}{t}\\ &= \lim_{t\to 0}\frac{t(v^TMx+x^TMv)+t^2v^TMx}{t}\\ &= v^TMx+x^TMv\\ &= v^TMx+v^TMx = \langle v,2Mx\rangle.\end{aligned}$$

□

Lemma 7.35. *For any $q \geq 1$ and $c \in \mathbb{Z}^n$,*

$$S_q(c) \ll_\triangle q^{1+\frac{n}{2}}.$$

Proof. We calculate for $\varphi(q) = |\{a : a \in \{1, \dots q\} \text{ and } (a,q) = 1\}|$,

$$\begin{aligned}
|S_q(c)|^2 &= \left| \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1 \\ b \in \mathbb{Z}^n}}^{q} e_q(aF(b) + \langle b, c \rangle) \right|^2 \\
&\leq \varphi(q) \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{\substack{b=1 \\ b \in \mathbb{Z}^n}}^{q} e_q(aF(b) + \langle b, c \rangle) \right|^2 \\
&= \varphi(q) \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{u,v=1 \\ u,v \in \mathbb{Z}^n}}^{q} e_q(a(F(u) - F(v)) + \langle u - v, c \rangle)
\end{aligned}$$

Then substitute $u = v + w$, where $w \in \mathbb{Z}^n$ varies from 1 to q. We claim that

$$a(F(u) - F(v)) + \langle u - v, c \rangle = aF^{(0)}(w) + \langle w, c \rangle + a \langle v, \nabla F(w) \rangle \mod q.$$

As $u - v = w$, $(a, q) = 1$ and by Lemma 7.34 $\nabla F(w) = 2Mw$, this follows as

$$\begin{aligned}
F(u) - F(v) = F(v + w) - F(v) &= F^{(0)}(v + w) - F^{(0)}(v) \\
&= (v + w)^T M (v + w) - v^T M v \\
&= v^T M w + w^T M v + w^T M w \\
&= w^T M w + 2v^T M w = F^{(0)}(w) + \langle v, \nabla F(w) \rangle.
\end{aligned}$$

Thus using $\varphi(q) \leq q$

$$\begin{aligned}
|S_q(c)|^2 &\leq q \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{v,w=1 \\ u,w \in \mathbb{Z}^n}}^{q} |e_q(aF^{(0)}(w) + \langle w, c \rangle) e_q(a \langle v, \nabla F(w) \rangle)| \\
&= q^{n+1} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{w=1 \\ w \in \mathbb{Z}^n \\ q | \nabla F(w)}}^{q} |e_q(aF^{(0)}(w) + \langle w, c \rangle)| \\
&\ll_\triangle q^{n+1} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} 1 \ll_\triangle q^{2+n}
\end{aligned}$$

where we used in the last line the trivial bound on e_q and that the number of solutions $q | \nabla F(w)$ is of order $O_\triangle(1)$. The claim now follows by simply taking the square root. $\square$

Using Lemma 7.35,

$$\sum_{1 \leq q \leq X} |S_q(c)| \ll_\triangle \ll_\triangle q^{1+\frac{n}{2}} \ll_\triangle X \cdot X^{1+\frac{n}{2}} \ll_\triangle X^{\frac{4+n}{2}}.$$

We denote for $x \in \mathbb{Z}^n$ by $M^{-1}(x)$ the quadratic form whose matrix is M^{-1}. If p does not divide $\triangle$, we can think of M^{-1} as defined modulo p. Before proceeding with the next lemma we recall some results on sums over finite fields. We denote the Kloosterman sum for a, b, m natural numbers,

$$K(a, b; p) = \sum_{x=1}^{p-1} e_p(ax + bx'),$$

where x' is the inverse mod p of x. A well known (c.f. chapter 11 of [IK04]) bound for the Kloosterman sum is

$$|K(a, b; p)| \leq 2p^{\frac{1}{2}}(a, b, p)^{\frac{1}{2}}. \tag{7.12}$$

The Salié sum is defined as

$$T(a, b; p) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e_p(ax + bx'),$$

where $\left(\frac{x}{p}\right)$ is the Legendre symbol given by

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if there exists } 1 \leq y \leq p \text{ such that } y^2 = x \mod p, \\ -1 & \text{if there does not exists } 1 \leq y \leq p \text{ such that } y^2 = x \mod p. \end{cases}$$

For the Salie sum we have the stronger bound

$$|T(a, b; p)| \leq 2p^{\frac{1}{2}}. \tag{7.13}$$

Finally we discuss quadratic Gauss sums (see chapter 3.5 of [IK04]). Assume that p is an odd prime and let c be an integer coprime to p. Then

$$\sum_{x=1}^{p} e_p(cx^2) = \left(\frac{c}{p}\right) \tau_p,$$

where

$$\tau_p = \sum_{x=1}^{p} e_p(x^2) = i^{\frac{(p-1)^2}{4}} \sqrt{p}.$$

Lemma 7.36. *Let p be a prime number not dividing $\triangle$. Then*

$$S_p(c) \ll_\triangle p^{\frac{n+1}{2}},$$

except when n is even and p divides both m and $M^{-1}(c)$. More precisely, when n is even,

$$S_p(c) = \begin{cases} -\left(\frac{(-1)^{\frac{n}{2}} \det(M)}{p}\right) p^{\frac{n}{2}} & \textit{if } p \textit{ divides exactly one of } m, M^{-1}(c), \\ (p-1)\left(\frac{(-1)^{\frac{n}{2}} \det(M)}{p}\right) p^{\frac{n}{2}} & \textit{if } p \textit{ divides both of } m, M^{-1}(c). \end{cases}$$

If n is odd,

$$S_p(c) = \begin{cases} \left(\frac{(-1)^{\frac{n-1}{2}} \det(M) m}{p}\right) p^{\frac{n+1}{2}} & \textit{if } p \textit{ divides } M^{-1}(c), \\ \left(\frac{(-1)^{\frac{n-1}{2}} \det(M) M^{-1}(c)}{p}\right) p^{\frac{n+1}{2}} & \textit{if } p \textit{ divides } m. \end{cases}$$

Proof. As $p \not| \triangle$, it follows that p is odd. Moreover, viewing the quadratic form over $F^{(0)}$ over $\mathbb{Z}/p\mathbb{Z}$, we can diagonalize it to arrive at

$$R^T MR = \mathrm{diag}(\beta_1, \ldots, \beta_n)$$

for $\beta_1, \ldots, \beta_n \in \mathbb{Z}/p\mathbb{Z}$ all non-zero and $R \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Substitute $b = Rx$ and $R^T c = d$,

$$\begin{aligned}
S_p(c) &= \sum_{a=1}^{p-1} \sum_{\substack{b=1 \\ b\in\mathbb{Z}^n}}^{p} e_p(aF(b) + \langle b, c\rangle) \\
&= \sum_{a=1}^{p-1} \sum_{\substack{b=1 \\ b\in\mathbb{Z}^n}}^{p} e_p(a(b^T Mb - m) + \langle b, c\rangle) \\
&= \sum_{a=1}^{p-1} \sum_{\substack{x=1 \\ x\in\mathbb{Z}^n}}^{p} e_p(a(\beta_1 x_1^2 + \ldots + \beta_n x_n^2 - m) + x_1 d_1 + \ldots + x_n d_n) \\
&= \sum_{a=1}^{m} e_p(-am) \prod_{i=1}^{n} \sum_{x=1}^{p} e_p(a\beta_i x^2 + xd_i).
\end{aligned}$$

Then as p is odd, using the above formulas for quadratic Gauss sums,

$$\begin{aligned}
\sum_{x=1}^{p} e_p(a\beta_i x^2 + xd_i) &= \sum_{x=1}^{p} e_p(a\beta_i(x + d_i(2a\beta_i)')^2 - d_i^2(4a\beta_i)') \\
&= \left(\frac{a\beta_i}{p}\right) e_p(-d_i^2(4a\beta_i)')\tau_p.
\end{aligned}$$

It hence follows that

$$S_p(c) = \tau_p^n \left(\frac{\det(M)}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n e_p\left(-am - \sum_{i=1}^{n} d_i^2(4a\beta_i)'\right).$$

However

$$\sum_{i=1}^{n} \beta_i^{-1} d_i^2 = d^T \mathrm{diag}(\beta_1, \ldots, \beta_n)^{-1} d = c^T R(R^T MR)^{-1} R^T c = c^T M^{-1} c$$

implying

$$S_p(c) = \tau_p^n \left(\frac{\det(M)}{p}\right) S(-m, -4' M^{-1}(c); p),$$

where S is the Kloosterman sum for n even and the Salié sum for odd n. Using (7.12) in the even case when p does not divide m and $M^{-1}(c)$ and (7.13) in the odd case, we conclude implies $S_p(c) \ll_\triangle p^{\frac{n+1}{2}}$ as stated in the lemma.

For the more precise values of $S_p(c)$, when n is even, note that $S = -1$ if p divides exactly one of a and b and $K_p = p - 1$ if p divides both a and b. Analogous formulas conclude the odd case. □

Before proceeding with the next lemma, we recall that a natural number n is called square-full if whenever a prime p divides n, then so does p^2.

Lemma 7.37. *For any $X \geq 1$,*

$$\sum_{\substack{1 \leq q \leq X \\ q \text{ is square-full}}} \frac{1}{\sqrt{q}} \ll_\varepsilon X^\varepsilon.$$

Moreover, the sum

$$\sum_{q \text{ square-full}} \frac{1}{q}$$

converges.

Proof. We first claim that the number of square-full numbers $\leq V$ is $\ll V^{\frac{1}{2}}$. To see this we observe that each square-full number can be written as $n^2 m^3$ for $m, n \in \mathbb{N}$. Moreover, we can assume m to be square-free, yielding a unique such decomposition. Thus the number of square-full numbers $\leq V$ is equal to

$$\sum_{\substack{m=1 \\ m \text{ square-free}}}^{\infty} \left[\left(\frac{V}{m^3} \right)^{\frac{1}{2}} \right] \leq V^{\frac{1}{2}} \sum_{m=1}^{\infty} \frac{1}{m^{\frac{3}{2}}} \ll V^{\frac{1}{2}}.$$

Assuming this, we notice that for any n and $\varepsilon > 0$,

$$\sum_{\substack{X^{n\varepsilon} \leq q \leq X^{(n+1)\varepsilon} \\ q \text{ is square full}}} \frac{1}{\sqrt{q}} \ll X^{\frac{(n+1)\varepsilon}{2}} X^{-\frac{n\varepsilon}{2}} \ll X^{\frac{\varepsilon}{2}}.$$

Thus for $\varepsilon > 0$ we choose $n(\varepsilon)$ to be the smallest number so that $1 \leq n(\varepsilon)\varepsilon$, then

$$\begin{aligned} \sum_{\substack{1 \leq q \leq X \\ q \text{ is square full}}} \frac{1}{\sqrt{q}} &\leq \sum_{\substack{1 \leq q \leq X^{n(\varepsilon)\varepsilon} \\ q \text{ is square full}}} \frac{1}{\sqrt{q}} \\ &\leq \sum_{1 \leq q \leq X^\varepsilon} \frac{1}{\sqrt{q}} + \sum_{X^\varepsilon \leq q \leq X^{2\varepsilon}} \frac{1}{\sqrt{q}} + \ldots + \sum_{X^{(n(\varepsilon)-1)\varepsilon} \leq q \leq X^{n(\varepsilon)\varepsilon}} \frac{1}{\sqrt{q}} \\ &\ll n(\varepsilon) X^{\frac{\varepsilon}{2}} \ll_\varepsilon X^{\frac{\varepsilon}{2}}, \end{aligned}$$

implying the first statement.

For the second statement, note that clearly

$$\sum_{q \text{ square-full}} \frac{1}{q} = \prod_p \left(1 + \frac{1}{p^2} + \frac{1}{p^3} + \ldots \right) = \prod_p \left(1 + \frac{1}{p(p-1)} \right).$$

The latter product converges as

$$\begin{aligned} \ln \left(\prod_p \left(1 + \frac{1}{p(p-1)} \right) \right) &\leq \sum_p \ln \left(1 + \frac{1}{p(p-1)} \right) \\ &\leq \sum_p \frac{1}{p(p-1)} \leq \sum_{n \in \mathbb{N}} \frac{1}{n^2} \ll 1. \end{aligned}$$

□

Lemma 7.38. *Let $|c| \leq P$. Then for any $\varepsilon > 0$ we have*

$$\sum_{1 \leq q \leq X} |S_q(c)| \ll_{M,\varepsilon} X^{\frac{3+n}{2}+\varepsilon} P^{\varepsilon},$$

except when n is even and $m = M^{-1}(c) = 0$, in which case

$$\sum_{1 \leq q \leq X} |S_q(c)| \ll_{\triangle} X^{\frac{4+n}{2}}.$$

Proof. We write $q = q_1 q_2$, where q_1 is square-free and q_2 is a square-full with $(q_1, q_2) = 1$. Then by Lemma 7.32 and 7.35,

$$|S_{q_1 q_2}(c)| = |S_{q_1}(q_2' c)| \cdot |S_{q_2}(q_1' c)| \ll_{\triangle} q_2^{1+\frac{n}{2}} |S_{q_1}(q_2' c)|.$$

As q_1 is square-free, it has a prime factorization $q_1 = p_1 \ldots p_k$ for distinct primes p_i. Thus by using Lemma 7.32 once more,

$$|S_{q_1}(q_2' c)| = |S_{p_1}(c_1)| \cdots |S_{p_k}(c_k)|$$

for some numbers $c_1, \ldots, c_k$. If p_i does divide $\triangle$, then the trivial bound satisfies $|S_{p_i}(c_i)| \leq p^{n+1} \ll_{\triangle} 1$.

Thus assume that p does not divide $\triangle$. First assume that n is odd. Then by Lemma 7.36,

$$|S_{p_i}(c_i)| \ll_{\triangle} p^{\frac{n+1}{2}}.$$

It remains to consider even n. If p_i does not divide both of m and $M^{-1}(c)$, then again by Lemma 7.36,

$$|S_{p_i}(c_i)| \ll_{\triangle} p^{\frac{n+1}{2}}.$$

If on the other hand p divides m and $M^{-1}(c)$, then $(p, m, M^{-1}(c)) = p$ and thus by Lemma 7.35,

$$|S_{p_i}(c_i)| \ll_{\triangle} p^{\frac{n+2}{2}} \ll_{\triangle} p_i^{\frac{n+1}{2}} (p_i, m, M^{-1}(c))^{\frac{1}{2}}.$$

The latter bound holds in any case, which allows us to conclude

$$|S_{q_1}(q_2' c)| \ll_{\triangle} q_1^{\frac{n+1}{2}} (q_1, m, M^{-1}(c))^{\frac{1}{2}},$$

where the final factor can be omitted if n is odd.

If $k \neq 0$, it holds

$$\sum_{u \leq U} (u, k) \leq \sum_{d|k} d \sum_{u \leq U, d|u} 1 \leq \sum_{d|k} d \frac{U}{d} = U d(k).$$

Moreover, as $|c| \leq P$, it follows that $M^{-1}(c)$ is $O_M(P^2)$ and hence in particular $d(M^{-1}(c)) \ll_{M,\varepsilon} P^{\varepsilon}$. Assume in the following calculation that it does not hold that n is even and $m = M^{-1}(c) = 0$. Then,

$$\begin{aligned}
\sum_{1\le q\le X} |S_q(c)| &\le \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} \sum_{\substack{1\le q_1\le \frac{X}{q_2}\\ q_1 \text{ square-free}}} |S_{q_1}(q_2'c)|\cdot|S_{q_2}(q_1'c)| \\
&\ll_\triangle \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} \sum_{\substack{1\le q_1\le \frac{X}{q_2}\\ q_1 \text{ square-free}}} q_2^{1+\frac{n}{2}} q_1^{\frac{n+1}{2}} (q_1, m, M^{-1}(c)) \\
&\ll_\triangle X^{\frac{n+1}{2}} \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} q_2^{\frac{1}{2}} \sum_{\substack{1\le q_1\le \frac{X}{q_2}\\ q_1 \text{ square-free}}} (q_1, m, M^{-1}(c)) \\
&\ll_\triangle X^{\frac{n+1}{2}} \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} q_2^{\frac{1}{2}} \sum_{\substack{1\le q_1\le \frac{X}{q_2}\\ q_1 \text{ square-free}}} (q_1, M^{-1}(c)) \\
&\ll_\triangle X^{\frac{n+1}{2}} \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} q_2^{\frac{1}{2}} \frac{X}{q_2} d(M^{-1}(c)) \\
&\ll_{M,\varepsilon} X^{\frac{n+3}{2}+\varepsilon} P^\varepsilon \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} q_2^{-\frac{1}{2}} \\
&\ll_\triangle X^{\frac{n+1}{2}+\varepsilon} P^\varepsilon,
\end{aligned}$$

where we used Lemma 7.37 in the last line. This implies the claim.

Finally, in the case where n is even and $m = M^{-1}(c) = 0$, we just use the weaker estimate $|S_{p_i}(c_i)| \ll_\triangle p^{\frac{n+2}{2}}$ to conclude

$$\begin{aligned}
\sum_{1\le q\le X} |S_q(c)| &\le \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} \sum_{\substack{1\le q_1\le \frac{X}{q_2}\\ q_1 \text{ square-free}}} |S_{q_1}(q_2'c)|\cdot|S_{q_2}(q_1'c)| \\
&\ll_\triangle X^{\frac{n+2}{2}} \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} 1 \sum_{\substack{1\le q_1\le \frac{X}{q_2}\\ q_1 \text{ square-free}}} 1 \\
&\ll_\triangle X^{\frac{n+2}{2}} \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} \frac{X}{q_2} \\
&\ll_\triangle X^{\frac{n+4}{2}} \sum_{\substack{1\le q_2\le X\\ q_2 \text{ square-full}}} \frac{1}{q_2} \ll_\triangle X^{\frac{n+4}{2}},
\end{aligned}$$

where we used in the last line that the sum of reciprocals of square-full numbers converges as was shown in Lemma 7.37. □

Recall that we defined $M_m(q)$ as the number of solutions to the equation

$$F^0(x) \equiv m \mod q$$

in $[1,q]^n$. Moreover for a prime number p,

$$\sigma_p = \lim_{k\to\infty} \frac{M_m(p^k)}{p^{k(n-1)}}$$

and the **singular series** is defined as

$$\sigma(F^{(0)}, m) = \prod_{p \text{ prime}} \sigma_p.$$

Analogously to Lemma 6.12, the next result holds.

Lemma 7.39. *For $n \geq 3$ and any prime number p the limit σ_p exists and can be computed as,*

$$\sigma_p = \sum_{t=0}^{\infty} p^{-nt} S_{p^t}(0).$$

Proof. We use precisely the same calculative methods as in Lemma 6.12. In particular, recall that the geometric series implies

$$\frac{1}{q}\sum_{a=1}^{q} e\left(\frac{aF(b)}{q}\right) = \begin{cases} 1 & \text{if } F^{(0)} \equiv m \mod q, \\ 0 & \text{if } F^{(0)} \not\equiv m \mod q. \end{cases}$$

Thus it follows

$$\begin{aligned} M_m(q) &= \sum_{\substack{b=1 \\ b\in\mathbb{Z}^n}}^{q} \frac{1}{q}\sum_{a=1}^{q} e_q(aF(b)) \\ &= \sum_{\substack{b=1 \\ b\in\mathbb{Z}^n}}^{q} \frac{1}{q}\sum_{d|q} \sum_{\substack{a=1 \\ (a,q)=d}}^{q} e_{\frac{q}{d}}(\tfrac{a}{d}F(b)) \\ &= \frac{1}{q}\sum_{d|q} d^n \sum_{\substack{a=1 \\ (a,\frac{q}{d})=1}}^{\frac{q}{d}} \sum_{\substack{b=1 \\ b\in\mathbb{Z}^n}}^{\frac{q}{d}} e_{\frac{q}{d}}(aF(b)) \\ &= \frac{1}{q}\sum_{d|q} d^n S_{\frac{q}{d}}(0) \\ &= q^{n-1}\sum_{d|q}\left(\frac{q}{d}\right)^{-n} S_{\frac{q}{d}}(0). \end{aligned}$$

In particular if $q = p^k$, then

$$\frac{M_m(p^k)}{p^{k(n-1)}} = \sum_{d|p^k}\left(\frac{q}{d}\right)^{-n} S_{\frac{q}{d}}(0) = \sum_{t=0}^{k} p^{-nt} S_{p^t}(0).$$

By using the bound from Lemma 7.35, it follows that the sum on the right hand side of the latter equation converges for $n \geq 3$ as $k \to \infty$ since

$$\sum_{t=0}^{k} p^{-nk} S_{p^k}(0) \ll \sum_{t=0}^{k} p^{-nt} p^{t(1+\frac{n}{2})} = \sum_{t=0}^{k} p^{t(1-\frac{n}{2})} \ll 1$$

for $n \geq 3$. This implies all the claims. $\square$

Lemma 7.40. *For $n \geq 4$ and $m \neq 0$ the sum*

$$\sum_{q=1}^{\infty} q^{-n} S_q(0)$$

converges.

Proof. We calculate as in Lemma 7.38,

$$\begin{aligned}
\sum_{1 \leq q \leq X} q^{-n} |S_q(0)| &\leq \sum_{\substack{1 \leq q_2 \leq X \\ q_2 \text{ square-full}}} \sum_{\substack{1 \leq q_1 \leq \frac{X}{q_2} \\ q_1 \text{ square-free}}} (q_1 q_2)^{-n} |S_{q_1}(0)| \cdot |S_{q_2}(0)| \\
&\ll_{\triangle} \sum_{\substack{1 \leq q_2 \leq X \\ q_2 \text{ square-full}}} \sum_{\substack{1 \leq q_1 \leq \frac{X}{q_2} \\ q_1 \text{ square-free}}} q_2^{1-\frac{n}{2}} q_1^{\frac{1-n}{2}} (q_1, m)^{\frac{1}{2}} \\
&\ll_{\triangle, m} \sum_{\substack{1 \leq q_2 \leq X \\ q_2 \text{ square-full}}} q_2^{1-\frac{n}{2}} \sum_{\substack{1 \leq q_1 \leq \frac{X}{q_2} \\ q_1 \text{ square-free}}} q_1^{\frac{1-n}{2}} \\
&< \infty,
\end{aligned}$$

independent of X where we used that $(q_1, m) \leq m$ and both of the sums

$$\sum_{\substack{q_2=1 \\ q_2 \text{ square-full}}}^{\infty} q_2^{1-\frac{n}{2}} \leq \sum_{\substack{q_2=1 \\ q_2 \text{ square-full}}}^{\infty} q_2^{-1}$$

and

$$\sum_{\substack{q_1=1 \\ q_1 \text{ square-free}}}^{\infty} q_1^{\frac{1-n}{2}} < \infty$$

converge. □

Thus, the last two lemmas show for $n \geq 4$ and $m \neq 0$,

$$\sigma(F^{(0)}, m) = \prod_{p \text{ prime}} \sigma_p = \sum_{q=1}^{\infty} q^{-n} S_q(0).$$

Lemma 7.41. *For $n \geq 4$ and $m \neq 0$, it holds*

$$\sum_{q \leq X} q^{-n} S_q(0) = \prod_{p} \sigma_p + O_{M,\varepsilon}(X^{\frac{3-n}{2}+\varepsilon} P^{\varepsilon}).$$

Proof. In order to prove the claim, we show

$$\sum_{q \geq X} q^{-n} S_q(0) \ll_{M,\varepsilon} X^{\frac{3-n}{2}+\varepsilon} P^{\varepsilon}.$$

Denote throughout this proof $L_X = \sum_{1\leq \ell \leq X} S_\ell(0)$. Then

$$\begin{aligned}\sum_{q\geq X} q^{-n} S_q(0) &= \sum_{q\geq X} q^{-n}(L_q - L_{q-1}) \\ &= X^{-n}L_{X-1} + \sum_{q\geq X}\left(\frac{1}{q^n} - \frac{1}{(q+1)^n}\right) L_q \\ &\ll_{M,\varepsilon} X^{\frac{3-n}{2}P^\varepsilon + \varepsilon} + \sum_{q\geq X} \frac{q^{n-1}}{q^{2n}} L_q, \\ &\ll_{M,\varepsilon} X^{\frac{3-n}{2}+\varepsilon} P^\varepsilon + P^\varepsilon \sum_{q\geq X} q^{\frac{1-n}{2}+\varepsilon}, \\ &\ll_{M,\varepsilon} X^{\frac{3-n}{2}+\varepsilon} P^\varepsilon\end{aligned}$$

where we used Lemma 7.38. □

7.6 Proof of the Main Theorem

We combine the previous subchapters to prove the main theorem (Theorem 7.8), which we restate for convenience.

Theorem 7.42. *Let $n \geq 4$ and $F^{(0)}$ be a non-singular quadratic form in n variables, m be a positive integer and $w : \mathbb{R}^n \to \mathbb{R}$ be a compactly supported function that satisfies the condition of Lemma 7.7. Set $F = F^{(0)} - m$. Then as $m \to \infty$,*

$$N(F, w, m^{\frac{1}{2}}) = \sigma_\infty(G, w)\sigma(F^{(0)}, m)m^{\frac{n}{2}-1} + O_{F^{(0)},w,\varepsilon}(m^{\frac{n-1}{4}+\varepsilon}).$$

The main statement is the next proposition. As before, we set $P = Q$.

Proposition 7.43. *For $n \geq 4$, $m \neq 0$ and any P,*

$$\sum_{c\in\mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) = P^n \sigma_\infty(G, w) \prod_p \sigma_p + O_{G,w,\varepsilon}(P^{\frac{n+3}{2}+\varepsilon})$$

as $P \to \infty$.

Proof. Fix $\varepsilon > 0$. For convenience, we use the convention that we will be concerned with changes of ε by multiples of itself. We first consider the case $|c| > P^\varepsilon$. Recall that $I_q(c) = 0$ for $q \gg_w P$. Thus by Lemma 7.28 and Lemma 7.35, for N large enough in dependence of ε,

$$\begin{aligned}\sum_{|c|>P^\varepsilon} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) &\ll_{G,w,\varepsilon} \sum_{|c|>P^\varepsilon} \sum_{q\ll P} q^{-n} q^{1+\frac{n}{2}} q^{-1} P^{n+1} |c|^{-N(\varepsilon)} \\ &\ll_{G,w,\varepsilon} P^{n+1} \sum_{|c|>P^\varepsilon} \sum_{q\ll P} q^{-\frac{n}{2}} |c|^{-N(\varepsilon)} \\ &\ll_{G,w,\varepsilon} 1.\end{aligned}$$

In the remainder of the proof assume $|c| \ll P^{\varepsilon}$ and we further distinguish the case $c \neq 0$ and $c = 0$. If $c \neq 0$, then by Lemma 7.31, as $P = Q$,

$$I_q(c) \ll_{G,w,\varepsilon} P^n P^{1-\frac{n}{2}} q^{\frac{n}{2}-1} P^{\varepsilon} \ll_{G,w,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} q^{\frac{n}{2}-1}.$$

Thus using Lemma 7.38, for any R,

$$\begin{aligned}
\sum_{R<q\leq 2R} q^{-n} S_q(c) I_q(c) &\ll_{G,w,\varepsilon} \sum_{R<q\leq 2R} q^{-n} S_q(c) P^{\frac{n}{2}+1+\varepsilon} q^{\frac{n}{2}-1} \\
&\ll_{G,w,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} \sum_{R<q\leq 2R} q^{-\frac{n}{2}-1} S_q(c) \\
&\ll_{G,w,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} R^{-\frac{n}{2}-1} \sum_{R<q\leq 2R} S_q(c) \\
&\ll_{G,w,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} R^{-\frac{n}{2}-1} R^{\frac{3+n}{2}+\varepsilon} \\
&\ll_{G,w,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} R^{\frac{1}{2}+\varepsilon},
\end{aligned}$$

replacing ε by a multiple of itself. Thus, still in the case $c \neq 0$,

$$\begin{aligned}
\sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) &\leq \sum_{R=1}^{\ll P} \sum_{R\leq q\leq 2R} q^{-n} S_q(c) I_q(c) \\
&\ll_{G,w,\varepsilon} \sum_{R=1}^{\ll P} P^{\frac{n}{2}+1+\varepsilon} R^{\frac{1}{2}+\varepsilon} \\
&\ll_{G,w,\varepsilon} P^{\frac{n+3}{2}+\varepsilon},
\end{aligned}$$

where we used in the last line

$$\sum_{R=1}^{\ll P} R^{\frac{1}{2}+\varepsilon} = \sum_{P^{1-\varepsilon}\ll R\ll P} R^{\frac{1}{2}+\varepsilon} + \sum_{P^{1-2\varepsilon}\ll R\ll P^{1-\varepsilon}} R^{\frac{1}{2}+\varepsilon} + \ldots + \sum_{R\ll P^{\varepsilon}} R^{\frac{1}{2}+\varepsilon} \ll_{\varepsilon} P^{\frac{1}{2}+\varepsilon}.$$

As we only consider c in the range $c \ll P^{\varepsilon}$, it follows

$$\sum_{c\neq 0} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_{G,w,\varepsilon} P^{\frac{n+3}{2}+\varepsilon}.$$

It remains to treat the case $c = 0$. Using Lemma 7.25 and Lemma 7.38 for $q > QP^{-\varepsilon} = P^{1-\varepsilon}$,

$$\begin{aligned}
\sum_{R<q\leq 2R} q^{-n} S_q(0) I_q(0) &\ll_{G,w,\varepsilon} P^n R^{-n} \sum_{R<q\leq 2R} S_q(0) \\
&\ll_{G,w,\varepsilon} P^n R^{-n} R^{\frac{3+n}{2}+\varepsilon} P^{\varepsilon} \\
&\ll_{G,w,\varepsilon} P^{n+\varepsilon} R^{\frac{3-n}{2}+\varepsilon}.
\end{aligned}$$

Hence

$$\sum_{P^{1-\varepsilon}<q\ll P} q^{-n} S_q(0) I_q(0) \ll_{G,w,\varepsilon} P^{\frac{3+n}{2}+\varepsilon}.$$

For $q \le P^{1-\varepsilon}$ we use Lemma 7.22 and Lemma 7.41,

$$\sum_{q\le P^{1-\varepsilon}} q^{-n}S_q(0)I_q(0) = P^n\sigma_\infty(G,w)\sum_{q\le P^{1-\varepsilon}} q^{-n}S_q(0) + O_{G,w,\varepsilon}(1)$$
$$= P^n\sigma_\infty(G,w)\prod_p \sigma_p + O_{G,w,\varepsilon}(P^{\frac{3-n}{2}+\varepsilon}).$$

□

Proof. (of Theorem 7.42) We use the choice $P = Q = m^{\frac{1}{2}}$. By Corollary 7.6,

$$N(F,w,m^{\frac{1}{2}}) = c_m m^{-1}\sum_{c\in\mathbb{Z}^n}\sum_{q=1}^{\infty} q^{-n}S_q(c)I_q(c),$$

where

$$c_m = 1 + O_N(m^{-N}).$$

By Proposition 7.43,

$$N(F,w,m^{\frac{1}{2}}) = \left(m^{-1} + O_N(m^{-N})\right)\left(m^{\frac{n}{2}}\sigma_\infty(G,w)\sigma(F^{(0)},m) + O_{F^{(0)},w,\varepsilon}(m^{\frac{n+3}{4}+\varepsilon})\right)$$
$$= \sigma_\infty(G,w)\sigma(F^{(0)},m)m^{\frac{n}{2}-1} + O_{F^{(0)},w,\varepsilon}(m^{\frac{n-1}{4}+\varepsilon}).$$

□

Corollary 7.44. *Let $n \ge 4$ and $F^{(0)}$ be a positive-definite quadratic form in n variables. Then as $m \to \infty$,*

$$|\{x\in\mathbb{Z}^n : F^{(0)}(x) = m\}| = C_{F^{(0)}}\sigma(F^{(0)},m)m^{\frac{n}{2}-1}O_{F^{(0)},\varepsilon}(m^{\frac{n-1}{4}+\varepsilon}),$$

where $C_{F^{(0)}}$ is a constant > 0 only depending on $F^{(0)}$.

Proof. Choose

$$w(x) = ew_0(2G(x)).$$

The function $w(x)$ has the value $w(x) = 1$ if and only if $G(x) = F^{(0)}(x) - 1 = 0$. Further note that if $x \in \mathbb{Z}^n$ satisfies $F^{(0)}(x) = m$, then $F^{(0)}(\frac{x}{\sqrt{m}}) = 1$. Thus

$$N(F^{(0)},w,m^{\frac{1}{2}}) = \sum_{\substack{x\in\mathbb{Z}^n\\ F^{(0)}(x)=m}} w\left(\frac{x}{\sqrt{m}}\right)$$
$$= \sum_{\substack{x\in\mathbb{Z}^n\\ F^{(0)}(x)=m}} 1 = |\{x\in\mathbb{Z}^n : F^{(0)}(x) = m\}|.$$

Note that since $F^{(0)}$ is positive definite, it follows that w is compactly supported. It remains to check the regularity condition of Lemma 7.7. Note that $|G| \le \frac{1}{2}$ on $\mathrm{supp}(w)$. Assume for a contradiction that $\nabla G(x) = 0$ for $x \in \mathrm{supp}(w)$. Then using Lemma 7.34,

$$0 = \langle x, \nabla F^{(0)}(x)\rangle = 2F^{(0)}(x) = 2(G(x)+1),$$

a contradiction. Thus setting $C_{F^{(0)}} = \sigma_\infty(G,w)$ implies the claim by using Theorem 7.42. □

7.7 Counting the Number of Solutions in Fixed Congruence Classes

As in the previous chapter, we consider a quadratic form $F^{(0)}$ in n variables and set $F = F^{(0)} - m$ for some m. Fix a positive integer ℓ. We aim at counting solutions of the form $\xi + \ell\mathbb{Z}^n$. More precisely, choose some element $\xi \in (\mathbb{Z}/\ell\mathbb{Z})^n$ and set

$$N(w, F, \xi) = N(w, F, P, \xi) = \sum_{\substack{x \in \xi + \ell\mathbb{Z}^n \\ F(x)=0}} w(P^{-1}x),$$

where again $w : \mathbb{R}^n \to \mathbb{R}$ is a compactly supported function that satisfies the regularity condition of Lemma 7.7. As before, we always consider the case $P = m^{\frac{1}{2}}$. The principal aim of this subchapter is to prove an analogue of Theorem 7.8.

Write $\ell = \prod_p p^{s_p}$. Denote by $M_m(p^k)$ the number of solutions of the equation

$$F(x) = F^{(0)}(x) - m \equiv 0 \mod p^k$$

for $x \in [1, p^{k+s_p}]^n$ with the additional condition $x \equiv \xi \mod p^{s_p}$. Then we define as usual

$$\sigma_p = \lim_{k\to\infty} \frac{M_m(p^k)}{p^{(n-1)k}}$$

and

$$\sigma(F^{(0)}, m, \xi) = \prod_p \sigma_p.$$

Theorem 7.45. *In the above setting,*

$$N(w, F, m^{\frac{1}{2}}, \xi) = \frac{1}{\ell^n}\sigma_\infty(G, w)\sigma(F^{(0)}, m, \xi)m^{\frac{n}{2}-1} + O_{F^{(0)},w,\ell,\varepsilon}(m^{\frac{n-1}{4}+\varepsilon}).$$

We apply the same ideas as in the proof of Theorem 7.8. We first establish an analogous result to Theorem 7.5. Therefore we introduce the notation for $c \in \mathbb{Z}^n$,

$$S_{q,\ell}(c, \xi) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1, b\in\mathbb{Z}^n \\ b\equiv\xi \mod \ell}}^{q\ell} e_{q\ell}(a\ell F(b) + \langle b, c\rangle).$$

Moreover, we define

$$\begin{aligned} I_{q,\ell}(c) &= \int_{\mathbb{R}^n} w(P^{-1}x)h(P^{-1}q, P^{-2}F(x))e_{q\ell}(-\langle c, x\rangle)\, dx \\ &= P^n \int_{\mathbb{R}^n} w(x)h(P^{-1}q, F(x))e_{q\ell}(-\langle Pc, x\rangle)\, dx. \end{aligned}$$

Lemma 7.46. *For any $m \geq 1$,*

$$N(w, F, P, \xi) = c_P P^{-2} \sum_{c\in\mathbb{Z}^n} \sum_{q=1}^{\infty} (q\ell)^{-n} S_{q,\ell}(c, \xi) I_{q,\ell}(c).$$

Proof. The proof is parallel to Theorem 7.5. We write with the help of Theorem 7.1,

$$\begin{aligned} N(w,F,P,\xi) &= \sum_{x\in\xi+\ell\mathbb{Z}^n} w(x)\delta_{F(x)} \\ &= c_P P^{-2}\sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{x\in\xi+\ell\mathbb{Z}^n} w(x)e_q(aF(x))h(P^{-1}q,P^{-2}F(x)). \end{aligned}$$

Setting first $x=\xi+\ell(b+qy)$ and then $z=\xi+\ell b$, where we sum over the suitable collection of numbers, we derive

$$\begin{aligned} &\sum_{x\in\xi+\ell\mathbb{Z}^n} w(x)e_q(aF(x))h(P^{-1}q,P^{-2}F(x)) \\ &= \sum_{\substack{b=1\\b\in\mathbb{Z}^n}}^{q}\sum_{y\in\mathbb{Z}^n} w(\xi+\ell(b+qy))e_q(aF(\xi+\ell(b+qy)))h(P^{-1}q,P^{-2}F(\xi+\ell(b+qy))) \\ &= \sum_{\substack{b=1\\b\in\mathbb{Z}^n}}^{q}\sum_{y\in\mathbb{Z}^n}\sum_{\substack{z=1,z\in\mathbb{Z}^n\\z\equiv\xi \mod \ell\\z=b \mod q}}^{q\ell} w(z+\ell qy)e_q(aF(z+\ell qy))h(P^{-1}q,P^{-2}F(z+\ell qy)) \\ &= \sum_{\substack{b=1\\b\in\mathbb{Z}^n}}^{q}\sum_{\substack{z=1,z\in\mathbb{Z}^n\\z\equiv\xi \mod \ell\\z=b \mod q}}^{q\ell} e_q(aF(z))\sum_{y\in\mathbb{Z}^n} f_z(y) \\ &= \sum_{\substack{b=1,b\in\mathbb{Z}^n\\b\equiv\xi \mod \ell}}^{q\ell} e_q(aF(b))\sum_{y\in\mathbb{Z}^n} f_z(y) \\ &= \sum_{\substack{b=1,b\in\mathbb{Z}^n\\b\equiv\xi \mod \ell}}^{q\ell} e_{q\ell}(a\ell F(b))\sum_{y\in\mathbb{Z}^n} f_z(y) \end{aligned}$$

for

$$f_z(y)=w(P^{-1}(z+\ell qy))h(P^{-1}q,P^{-2}F(z+\ell qy)).$$

Then by the Poisson summation formula,

$$\sum_{y\in\mathbb{Z}^n} f_z(y)=\sum_{c\in\mathbb{Z}^n}\widehat{f}_z(c)=\sum_{c\in\mathbb{Z}^n}\int_{\mathbb{R}^n} f_z(y)e(-\langle c,y\rangle)\,dy.$$

Substituting $x=z+\ell qy$ and

$$\begin{aligned} \widehat{f}_z(c) &= \int_{\mathbb{R}^n} w(P^{-1}(z+\ell qy))h(P^{-1}q,P^{-2}F(z+\ell qy))e(-\langle c,y\rangle)\,dy \\ &= (q\ell)^{-n}\int_{\mathbb{R}^n} w(P^{-1}x)h(P^{-1}q,P^{-2}F(x))e\left(-\left\langle c,\frac{x-z}{q\ell}\right\rangle\right)dx \\ &= (q\ell)^{-n}e_{q\ell}(\langle c,z\rangle)\int_{\mathbb{R}^n} w(P^{-1}x)h(P^{-1}q,P^{-2}F(x))e_{q\ell}(-\langle c,x\rangle)\,dx \\ &= (q\ell)^{-n}e_{q\ell}(\langle c,z\rangle)I_{q,\ell}(c). \end{aligned}$$

In conclusion,

$$\begin{aligned}
N(w,F,P,\xi) &= c_P P^{-2} \sum_{q=1}^{\infty} \sum_{\substack{q=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1, b\in\mathbb{Z}^n \\ b\equiv\xi \mod \ell}}^{q\ell} e_{q\ell}(a\ell F(b)) \sum_{y\in\mathbb{Z}^n} f_z(y) \\
&= c_P P^{-2} \sum_{q=1}^{\infty} \sum_{\substack{q=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1, b\in\mathbb{Z}^n \\ b\equiv\xi \mod \ell}}^{q\ell} e_{q\ell}(a\ell F(b)) \sum_{c\in\mathbb{Z}^n} (q\ell)^{-n} e_{q\ell}(\langle c,z\rangle) I_{q,\ell}(c). \\
&= c_P P^{-2} \sum_{c\in\mathbb{Z}^n} \sum_{q=1}^{\infty} \sum_{\substack{q=1 \\ (a,q)=1}}^{q} \sum_{\substack{b=1, b\in\mathbb{Z}^n \\ b\equiv\xi \mod \ell}}^{q\ell} (q\ell)^{-n} e_{q\ell}(a\ell F(b) + \langle c,z\rangle) I_{q,\ell}(c). \\
&= c_P P^{-2} \sum_{c\in\mathbb{Z}^n} \sum_{q=1}^{\infty} (q\ell)^{-n} S_{q,\ell}(c,\xi) I_{q,\ell}(c).
\end{aligned}$$

□

We next discuss properties and estimates for $I_{q,\ell}(c)$ and $S_{q,\ell}(c,\xi)$, which are analogous to the results in chapters 7.4 and 7.5. As the proofs follow along the lines of the corresponding results in chapters 7.4 and 7.5, we omit them here.

Lemma 7.47. *The following properties hold for $I_{q,\ell}(c)$.*

(i) For $q \gg_w P$,

$$I_{q,\ell}(c) = 0.$$

(ii) For $c \neq 0$ and $N > 0$,

$$I_{q,\ell}(c) \ll_{w,N} P^{n+1}(q\ell)^{-1}|c|^{-N}.$$

(iii) For $c \neq 0$,

$$I_{q,\ell}(c) \ll_{w,\varepsilon} P^{1+\frac{n}{2}+2\varepsilon}|c|^{1-\frac{n}{2}+\varepsilon}(q\ell)^{\frac{n}{2}-1+2\varepsilon}.$$

(iv) For $q \ll P$,

$$I_{q,\ell}(0) = P^n(\sigma_\infty(G,w) + O_{G,w,N}((P^{-1}q)^N)).$$

Lemma 7.48. *Let $q = q_1q_2$ and $\ell = \ell_1\ell_2$ so that $(q_1\ell_1, q_2\ell_2) = 1$. Choose $q_1', q_2', \ell_1', \ell_2'$ so that*

$$\begin{aligned}
q_1q_1' &\equiv 1 \mod q_2\ell_2, \\
q_2q_2' &\equiv 1 \mod q_1\ell_1, \\
\ell_1\ell_1' &\equiv 1 \mod q_2\ell_2, \\
\ell_2\ell_2' &\equiv 1 \mod q_1\ell_1.
\end{aligned}$$

Then for $\xi \in (\mathbb{Z}/\ell\mathbb{Z})^n$,

$$S_{q,\ell}(c,\xi) = S_{q_1,\ell_1}(q_2'\ell_2'c,\xi)S_{q_2,\ell_2}(q_1'\ell_1'c,\xi).$$

Lemma 7.49. *We have the following properties for $n \geq 4$ and $m \neq 0$.*

(i) $S_{q,\ell}(x,\xi) \ll_{\triangle,\ell} q^{1+\frac{n}{2}}$.

(ii) For $|c| \leq P$ *and* $\varepsilon > 0$,

$$\sum_{q \leq X} |S_{q,\ell}(c,\xi)| \ll_{M,\varepsilon} X^{\frac{3+n}{2}+\varepsilon} P^{\varepsilon}.$$

Proposition 7.50. *For $n \geq 4$ and $m \neq 0$ and any P,*

$$\sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} (q\ell)^{-n} S_{q,\ell}(c,\xi) I_{q,\ell}(c) = \left(\frac{P}{\ell}\right)^n \sigma_\infty(G,w) \prod_p \sigma_p + O_{G,w,\ell,\varepsilon}(P^{\frac{n+3}{2}+\varepsilon})$$

as $P \to \infty$.

Proof. The proof is similar to the one of Proposition 7.43. As before, we first consider the case $|c| > P^{\varepsilon}$. Recall that $I_{q,\ell}(c) = 0$ for $q \gg_w P$. Thus by Lemma 7.47 (ii) and Lemma 7.49 (i), for N large enough in dependence of ε,

$$\begin{aligned}
\sum_{|c|>P^\varepsilon} \sum_{q=1}^{\infty} (q\ell)^{-n} S_{q,\ell}(c) I_{q,\ell}(c) &\ll_{G,w,\varepsilon} \sum_{|c|>P^\varepsilon} \sum_{q \ll P} (q\ell)^{-n} q^{1+\frac{n}{2}} (q\ell)^{-1} P^{n+1} |c|^{-N(\varepsilon)} \\
&\ll_{G,w,\ell,\varepsilon} P^{n+1} \sum_{|c|>P^\varepsilon} \sum_{q \ll P} q^{-\frac{n}{2}} |c|^{-N(\varepsilon)} \\
&\ll_{G,w,\ell,\varepsilon} 1.
\end{aligned}$$

In the remainder of the proof we restrict to the case $c \ll P^{\varepsilon}$. We further distinguish the case $c \neq 0$ and $c = 0$. If $c \neq 0$, then by Lemma 7.47 (iii),

$$I_{q,\ell}(c) \ll_{G,w,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} q^{\frac{n}{2}-1}.$$

Thus using Lemma 7.49 (ii), for any R,

$$\begin{aligned}
\sum_{R<q\leq 2R} (q\ell)^{-n} S_{q,\ell}(c) I_{q,\ell}(c) &\ll_{G,w,\ell,\varepsilon} \sum_{R<q\leq 2R} q^{-n} S_q(c) P^{\frac{n}{2}+1+\varepsilon} q^{\frac{n}{2}-1} \\
&\ll_{G,w,\ell,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} \sum_{R<q\leq 2R} q^{-\frac{n}{2}-1} S_{q,\ell}(c) \\
&\ll_{G,w,\ell,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} R^{-\frac{n}{2}-1} \sum_{R<q\leq 2R} S_{q,\ell}(c) \\
&\ll_{G,w,\ell,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} R^{-\frac{n}{2}-1} R^{\frac{3+n}{2}+\varepsilon} \\
&\ll_{G,w,\ell,\varepsilon} P^{\frac{n}{2}+1+\varepsilon} R^{\frac{1}{2}+\varepsilon}.
\end{aligned}$$

Thus, still in the case $c \neq 0$,

$$\begin{aligned}
\sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) &\leq \sum_{R=1}^{\ll P} \sum_{R \leq q \leq 2R} q^{-n} S_q(c) I_q(c) \\
&\ll_{G,w,\ell,\varepsilon} \sum_{R=1}^{\ll P} P^{\frac{n}{2}+1+\varepsilon} R^{\frac{1}{2}+\varepsilon} \\
&\ll_{G,w,\ell,\varepsilon} P^{\frac{n+3}{2}+\varepsilon}.
\end{aligned}$$

As we only consider c in the range $c \ll P^{\varepsilon}$,

$$\sum_{c\neq 0}\sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_{G,w,\ell,\varepsilon} P^{\frac{n+3}{2}+\varepsilon}.$$

It remains to treat the case $c = 0$. Using Lemma 7.47 (iv) and Lemma 7.49 (ii) for $q > P^{1-\varepsilon}$,

$$\begin{aligned}\sum_{R<q\leq 2R} (q\ell)^{-n} S_{q,\ell}(0) I_{q,\ell}(0) &\ll_{G,w,\ell,\varepsilon} P^n R^{-n} \sum_{R<q\leq 2R} S_{q,\ell}(0)\\ &\ll_{G,w,\ell,\varepsilon} P^n R^{-n} R^{\frac{3+n}{2}+\varepsilon} P^{\varepsilon}\\ &\ll_{G,w,\ell,\varepsilon} P^{n+\varepsilon} R^{\frac{3-n}{2}+\varepsilon}.\end{aligned}$$

Hence

$$\sum_{P^{1-\varepsilon}<q\ll P} (q\ell)^{-n} S_{q,\ell}(0) I_{q,\ell}(0) \ll_{G,w,\ell,\varepsilon} P^{\frac{3+n}{2}+\varepsilon}.$$

For $q \leq P^{1-\varepsilon}$ we use again Lemma 7.47 (iv) and the analogue of Lemma 7.41,

$$\begin{aligned}\sum_{q\leq P^{1-\varepsilon}} (q\ell)^{-n} S_q(0) I_q(0) &= \left(\frac{P}{\ell}\right)^n \sigma_\infty(G,w) \sum_{q\leq P^{1-\varepsilon}} q^{-n} S_{q,\ell}(0) + O_{G,w,\ell,\varepsilon}(1)\\ &= \left(\frac{P}{\ell}\right)^n \sigma_\infty(G,w) \prod_p \sigma_p + O_{G,w,\ell,\varepsilon}(P^{\frac{3-n}{2}+\varepsilon}).\end{aligned}$$

□

Proof. (of Theorem 7.45) By Lemma 7.46,

$$N(F,w,m^{\frac{1}{2}},\xi) = c_m m^{-1} \sum_{c\in\mathbb{Z}^n}\sum_{q=1}^{\infty} (q\ell)^{-n} S_{q,\ell}(c) I_{q,\ell}(c),$$

where

$$c_m = 1 + O_N(m^{-N}).$$

Thus together with Proposition 7.50,

$$\begin{aligned}N(F,w,m^{\frac{1}{2}}) &= \left(m^{-1} + O_N(m^{-N})\right)\left(\ell^{-n} m^{\frac{n}{2}} \sigma_\infty(G,w)\sigma(F^{(0)},m,\xi) + O_{F^{(0)},w,\ell,\varepsilon}(m^{\frac{n+3}{4}+\varepsilon})\right)\\ &= \frac{1}{\ell^4}\sigma_\infty(G,w)\sigma(F^{(0)},m,\xi) m^{\frac{n}{2}-1} + O_{F^{(0)},w,\ell,\varepsilon}(m^{\frac{n-1}{4}+\varepsilon}).\end{aligned}$$

□

Finally, we can again deduce the following corollary.

Corollary 7.51. *Let $n \geq 4$ and $F^{(0)}$ a positive-definite quadratic form in n variables. Then as $m \to \infty$,*

$$|\{x \in \xi + (\ell\mathbb{Z})^n \,:\, F^{(0)}(x) = m\}| = \frac{C_{F^{(0)}}}{\ell^n}\sigma(F^{(0)},m,\xi) m^{\frac{n}{2}-1} O_{F^{(0)},\ell,\varepsilon}(m^{\frac{n-1}{4}+\varepsilon}),$$

where $C_{F^{(0)}}$ is a constant > 0 only depending on $F^{(0)}$.

Proof. The proof is verbatim the one of Corollary 7.44 □

7.8 Application to Quaternion Algebras

In this subchapter, we apply the results from previous subchapter to a quaternion algebra $\mathrm{B} = \mathrm{B}_{a,b}$ over $\mathbb{Q}$ so that $a, b \in \mathbb{Q}^\times$. We assume without loss of generality that $a, b \in \mathbb{Z}\backslash\{0\}$ so that $\mathrm{B}_{a,b}$ has a $\mathbb{Z}$-structure. Denote as usual by $\mathrm{G} = \mathrm{B}^1$ the elements of unit norm, by Γ_ℓ the ℓ-congruence subgroup of $\mathrm{G}(\mathbb{Z})$ and by $\Gamma_{p,\ell}$ the corresponding lattice in $\mathrm{G}(\mathbb{R}) \times \mathrm{G}(\mathbb{Q}_p)$.

To link this setting to the one of the last subchapter, we observe that B can be viewed as $\mathbb{A}^4$ and the norm Nr defines a quadratic form in four variables over $\mathbb{Z}$. Moreover, to simplify the notation, we simply denote by $\mathbb{Z}^4$ the $\mathbb{Z}$ points of B. For h a positive integer, write $F(x) = \mathrm{Nr}(x) - h^2$ for $x \in \mathrm{B}(\mathbb{R}) \cong \mathbb{R}^4$. Then for a compactly supported function $w : \mathrm{B}(\mathbb{R}) \to \mathbb{R}$ and $\xi \in (\mathbb{Z}/\ell\mathbb{Z})^4$ write

$$N_h(w, \xi) = N(w, F, h, \xi) = \sum_{\substack{x \in \xi + \ell\mathbb{Z}^4 \\ F(x)=0}} w(h^{-1}x).$$

With this notation, Theorem 7.45 reads as

$$N_h(w, \xi) = \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr}, w)\sigma(\mathrm{Nr}, h^2, \xi)h^2 + O_{\mathrm{Nr},w,\ell,\varepsilon}(h^{\frac{3}{2}+\varepsilon}). \tag{7.14}$$

In this concrete setting, we first want to derive a uniform version of (7.14) as we shift w by some element $g \in \mathrm{G}(\mathbb{R})$ and then apply this result to prove Corollary 5.16. For $g \in \mathrm{G}(\mathbb{R})$, set

$$w_g(x) = w(g^{-1}x)$$

for $x \in \mathrm{B}(\mathbb{R})$.

In the following we view $\mathrm{G}(\mathbb{R})$ as a subgroup of $\mathrm{O}_{Q_{a,b}}(\mathbb{R})$, which is possible by the proof of Proposition 1.18. We moreover denote by $||\cdot||$ a norm on $\mathrm{G}(\mathbb{R})$ which is given as $||g|| = \max(||g||_{\mathrm{Mat}}, ||g^{-1}||_{\mathrm{Mat}})$ for $||\cdot||_{\mathrm{Mat}}$ a fixed sub-multiplicative matrix norm.

Theorem 7.52. *Let $w : \mathrm{B}(\mathbb{R}) \to \mathbb{R}$ be a positive smooth compactly supported function satisfying the regularity condition of Lemma 7.7, ℓ a positive integer, $\xi \in \Lambda/\ell\Lambda$ and $g \in \mathrm{G}(\mathbb{R})$. Then for every $\delta > 0$ and $N > 4$,*

$$\begin{aligned} N_h(w_g, \xi) = &\frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr}, w)\sigma(\mathrm{Nr}, h^2, \xi)h^2 \\ &+ O_{w,\ell,N,\varepsilon}(||g||^N h^{3-(N-4)\delta} + ||g||h^{\frac{3}{2}+4\delta+\varepsilon}). \end{aligned}$$

Proof. In order to avoid a notational conflict, we denote in this proof by H the function h from previous chapters. For the proof we introduce the notation, where we write as before $P = h$,

$$\begin{aligned} I_{g,q,\ell}(c) &= \int_{\mathbb{R}^4} w(g^{-1}P^{-1}x)H(P^{-1}q, P^{-2}F(x))e_{q\ell}(-\langle c, x\rangle)\, dx \\ &= h^4 \int_{\mathbb{R}^4} w(g^{-1}x)H(h^{-1}q, F(x))e_{q\ell}(-\langle hc, x\rangle)\, dx. \end{aligned}$$

By the proof of Proposition 1.18, we can view $\mathrm{G}(\mathbb{R})$ as a subgroup of $\mathrm{O}_{Q_{a,b}}(\mathbb{R})$ and hence each element of $\mathrm{G}(\mathbb{R})$ is considered to be a matrix of determinant ± 1. Thus, also using that $\mathrm{G}(\mathbb{R})$ preserves $F(x)$, it follows

$$I_{g,q,\ell}(c) = h^4 \int_{\mathbb{R}^4} w(x) H(h^{-1}q, F(x)) e_{q\ell}(-\langle hc, gx\rangle)\, dx = I_{q,\ell}(g^T c).$$

In particular, by Lemma 7.46,

$$N_h(w_g, \xi) = c_h h^{-2} \sum_{c\in\mathbb{Z}^4} \sum_{q=1}^{\infty} (q\ell)^{-4} S_{q,\ell}(c,\xi) I_{q,\ell}(g^T c).$$

The remainder of the proof is analogous to the proofs of Theorem 7.8 and of Theorem 7.45.

Fix $\delta > 0$. First we consider terms with $|c| > h^\delta$. Then by Lemma 7.47 (ii) for $N > 4$,

$$\sum_{\substack{c\in\mathbb{Z}^4\\ |c|>h^\delta}} \sum_{q=1}^{\infty} (q\ell)^{-4} S_{q,\ell}(c,\xi) I_{q,\ell}(g^T c) \ll_{w,\ell,N} h^5 \left(\sum_{|c|>|h|^\delta} |g^T c|^{-N} \right) \sum_{q=1}^{\infty} q^{-5} S_{q,\ell}(c,\xi).$$

By Lemma 7.49 the second sum is finite. The first sum is estimated as

$$\sum_{|c|>h^\delta} |g^T c|^{-N} \ll ||g||^N \sum_{|c|>h^\delta} |c|^{-N} \ll ||g||^N h^{-(N-4)\delta}, \tag{7.15}$$

where we used that $|c| = |g^{-1}gc| \ll ||g^{-1}||\, |gc|$ and hence in particular by our choice of norm, $||g||^{-1}\, |c| \le |gc|$. Thus

$$\sum_{\substack{c\in\mathbb{Z}^4\\ |c|>h^\delta}} \sum_{q=1}^{\infty} (q\ell)^{-4} S_{q,\ell}(c,\xi) I_{q,\ell}(g^T c) \ll_{w,\ell,N} ||g||^N h^{5-(N-4)\delta}.$$

Next we analyze $0 < |c| \le h^\delta$. Then by Lemma 7.47 (i) and (iii),

$$\begin{aligned} &\sum_{0<|c|\le h^\delta} \sum_{q=1}^{\infty} (q\ell)^{-4} S_{q,\ell}(c,\xi) I_{q,\ell}(g^T c) \\ &\ll_{w,\ell,\varepsilon} h^{3+\varepsilon} \left(\sum_{0<|c|<h^\delta} |g^T c|^{-1+\varepsilon} \left(\sum_{q=1}^{\ll h} q^{-3} S_{q,\ell}(c,\xi) \right) \right). \end{aligned}$$

Using Lemma 7.49 (ii) as in the proof of Proposition 7.43,

$$\sum_{q=1}^{\ll h} q^{-3} S_{q,\ell}(c,\xi) \ll_{\mathrm{Nr},\ell,\varepsilon} h^{\frac{1}{2}+\varepsilon}.$$

Moreover

$$\sum_{0<|c|\le h^\delta} |g^T c|^{-1+\varepsilon} \ll ||g|| \cdot |\{c\in\mathbb{Z}^4 \,:\, |c| \le h^\delta\}| \ll ||g|| h^{4\delta}.$$

In summary,

$$\sum_{0<|c|\le h^\delta}\sum_{q=1}^{\infty}(q\ell)^{-4}S_{q,\ell}(c,\xi)I_{q,\ell}(g^Tc) \ll_{w,\ell,\varepsilon} ||g||h^{\frac{7}{2}+4\delta+\varepsilon}.$$

Combining all this, we conclude

$$\begin{aligned}N_h(w_g,\xi) &= c_h h^{-2}\ell^{-4}\sum_{q=1}^{\infty} q^{-4}S_{q,\ell}(0,\xi)I_{q,\ell}(0)\\ &\quad + O_{w,\ell,N,\varepsilon}(||g||^N h^{3-(N-4)\delta} + ||g||h^{\frac{3}{2}+4\delta+\varepsilon}),\end{aligned}$$

which implies the claim as in the proof of Theorem 7.45. $\square$

Corollary 7.53. *For every ℓ, there exists a measurable subset $Q \subset \mathrm{G}(\mathbb{R})$ with finite measure that surjects onto $\mathrm{G}(\mathbb{R})/\Gamma_\ell$ so that for all $\varepsilon > 0$,*

$$\left|\left|N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2\right|\right|_{L^2(Q)} \ll_{w,\ell,Q,\varepsilon} h^{\frac{23}{12}+\varepsilon}.$$

If moreover G is anisotropic over $\mathbb{Q}$, or equivalently B is a division algebra over $\mathbb{Q}$, then

$$\left|\left|N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2\right|\right|_{L^2(Q)} \ll_{w,\ell,Q,\varepsilon} h^{\frac{3}{2}+\varepsilon}.$$

Proof. If B is a division algebra, then Γ_ℓ is cocompact (cf. [Ber16] chapter 2) and hence there is a compact fundamental domain Q for $\mathrm{G}(\mathbb{R})/\Gamma_\ell$. Thus it follows directly by Theorem 7.52, by choosing a large N,

$$\left|\left|N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2\right|\right|_{L^2(Q)} \ll_{w,\ell,Q,\varepsilon} h^{\frac{3}{2}+\varepsilon}.$$

If G is isotropic over $\mathbb{Q}$, then as a consequence of Corollary 1.17 it follows that $\mathrm{G} = \mathrm{SL}_2$. We use the standard notation for $\mathrm{SL}_2(\mathbb{R})$. Recall that a surjective set Q of finite measure can be chosen to be of the form $Q = Q_0 \cup Q_1 \cup \ldots \cup Q_s$ where Q_0 is compact and

$$Q_i = \{ka_t u g_i \,:\, k \in K, t \ge 0 \text{ and } u \in U_0\},$$

where U_0 is a compact subset of the unipotent group U and g_i is some fixed element. Thus it suffices to prove the estimate for $Q = Q_i$ for $1 \le i \le s$.

Set

$$Q_{<R} = \{ka_t u g_i \,:\, k \in K, 0 \le t < \ln(R) \text{ and } u \in U_0\}$$

and

$$Q_{\ge R} = \{ka_t u g_i \,:\, k \in K, t \ge \ln(R) \text{ and } u \in U_0\}.$$

Note that $m_G(Q_{\ge R}) \ll R^{-2}$ and for $g \in Q_{<R}$,

$$N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2 = O_{w,\ell,N,\varepsilon}(R^N h^{3-(N-4)\delta} + Rh^{\frac{3}{2}+4\delta+\varepsilon}).$$

Thus it follows for any N large enough,

$$
\begin{aligned}
&\left\|N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2\right\|_{L^2(Q)} \\
&\le \left(\int_{Q_{\le R}} \left|N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2\right|^2 dm_G(g)\right)^{\frac{1}{2}} \\
&+ \left(\int_{Q_{\ge R}} \left|N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2\right|^2 dm_G(g)\right)^{\frac{1}{2}} \\
&\le m_G(Q_{\le R})^{\frac{1}{2}} O_{w,\ell,N,\varepsilon}(R^N h^{3-(N-4)\delta} + Rh^{\frac{3}{2}+4\delta+\varepsilon}) + m(Q_{\ge R})^{\frac{1}{2}} O_{w,\ell,\varepsilon}(h^{2+\varepsilon}) \\
&\ll_{w,\ell,Q,N,\delta,\varepsilon} R^N h^{3-(N-4)\delta} + Rh^{\frac{3}{2}+4\delta+\varepsilon} + R^{-1}h^{2+\varepsilon}.
\end{aligned}
$$

We next choose R so that the last two terms are essentially equal, namely $R = h^{\frac{1}{4}-2\delta}$. Then

$$
\left\|N_h(w_g,\xi) - \frac{1}{\ell^4}\sigma_\infty(\mathrm{Nr},w)\sigma(\mathrm{Nr},h^2,\xi)h^2\right\|_{L^2(Q)} \ll_{w,\ell,Q,N,\delta,\varepsilon} h^{\sigma+\varepsilon}
$$

for

$$
\sigma = \max\left\{\frac{N}{4} + 3 - (3N-4)\delta, \frac{7}{4} + 2\delta\right\}.
$$

To optimize the error term, we choose

$$
\delta = \frac{N+50}{12N}.
$$

Then as $N \to \infty$, $\sigma \to \frac{23}{12}$. $\square$

A Sobolev Norms on Homogeneous Spaces

A.1 Sobolev Spaces on Lie Groups

We first review some general notions on Lie groups with a generalization of these notions for homogeneous spaces in mind. Let G be a (real) Lie group of dimension n with Lie algebra $\mathfrak{g}$ and unit element e. We fix a Haar measure on G and denote by $L^2(G)$ the space of square-integrable functions.

Definition A.1. Let $f : G \to \mathbb{R}$ be a function and $X \in \mathfrak{g}$. If

$$(D_X f)(g) := \frac{d}{dt}\bigg|_{t=0} f(\exp(-tX)g)$$

exists for all g, then f is called **differentiable** in the direction of X and $D_X f$ is called the **derivative** of f in the direction of X. The function f is called **smooth** if for all $X_1, \ldots, X_n \in \mathfrak{g}$ the derivative

$$D_{X_1,\ldots,X_n} f := D_{X_1} D_{X_2} \ldots D_{X_n} f$$

exists and is continuous. We denote by $C^\infty(G)$ the space of smooth functions on G and by $C_c^\infty(G)$ the space of smooth compactly supported functions.

We next discuss Sobolev spaces on Lie groups. Let $k \in \mathbb{N}$ and fix a basis $X_1, \ldots, X_n$ of $\mathfrak{g}$. For $\alpha \in \mathbb{N}_0^n$ we write $||\alpha||_1 = |\alpha_1| + \ldots + |\alpha_n|$ and for a function $f : G \to \mathbb{R}$ we denote

$$D_\alpha f := D_{X_{\alpha_1}} \ldots D_{X_{\alpha_n}} f.$$

Definition A.2. For any $f \in C_c^\infty(G)$ we define the **Sobolev norm** as

$$\mathcal{S}_d(f) = ||f||_{\mathcal{H}^d(G)} = \sqrt{\sum_{||\alpha||_1 \le d} ||D_\alpha f||^2_{L^2(G)}}.$$

The **Sobolev space** $\mathcal{H}^d(G)$ is the completion of

$$\{f \in C^\infty(G) \, : \, \mathcal{S}_d(f) \text{ exists and is finite}\}$$

with respect to the norm $|| \circ ||_{\mathcal{H}^d(G)}$ viewed as a subspace of $L^2(G)$.[3] Finally, we define the space $\mathcal{H}_0^d(G)$ as the completion of

$$\{f \in C_c^\infty(G) \, : \, \mathcal{S}_d(f) \text{ exists and is finite}\}$$

with respect to the norm $|| \circ ||_{\mathcal{H}^d(G)}$ viewed as a subspace of $L^2(G)$.

Lemma A.3. *The Sobolev spaces $\mathcal{H}^d(G)$ and $\mathcal{H}_0^d(G)$ do not depend on the choice of basis $X_1, \ldots, X_n$ of $\mathfrak{g}$.*

Proof. We refer to chapter 7.1 of [EW]. □

Lemma A.4. *For any $d \in \mathbb{N}$, the Sobolev spaces $\mathcal{H}^d(G)$ and $\mathcal{H}_0^d(G)$ are Hilbert spaces.*

[3]See the proof of Lemma A.4 for a proof why $\mathcal{H}^d(G)$ can be viewed as a subspace of $L^2(G)$.

Proof. We only show that $\mathcal{H}^d(G)$ is a Hilbert space as the other case is analogous. The inner product on $\mathcal{H}^d(G)$ is given for $f, g \in \mathcal{H}^d(G)$ by

$$\langle f, g\rangle_{\mathcal{H}^d(G)} = \sum_{||\alpha||_1 \leq d} \langle D_\alpha f, D_\alpha g\rangle.$$

It remains to show that the induced norm is complete, which will follow from an alternate description of Sobolev spaces. Namely, consider the embedding

$$\iota : C^\infty(G) \longrightarrow \bigoplus_{||\alpha||_1 \leq d} L^2(G), \qquad f \longmapsto (D_\alpha f)_\alpha$$

and denote by W the closure of $\iota(C^\infty(G))$. As W is a closed subspace of a Hilbert space, it is itself a Hilbert space. Since each element of W is determined by the first coordinate, the map

$$\mathcal{H}^d(G) \longrightarrow W, \qquad f \mapsto (f_\alpha)_\alpha$$

is an isometric isomorphism. This shows that $\mathcal{H}^d(G)$ is a Hilbert space. □

We want to prove an analogue of the Sobolev embedding theorem for Lie groups, as a consequence of the Sobolev embedding theorem for open subset. We first recall the latter theorem.

Theorem A.5. *Let $U \subset \mathbb{R}^n$ be an open subset and choose $d > \frac{n}{2}$. Then any $f \in H^d(U)$ has a continuous representative. Moreover, any $f \in C_c^\infty(U)$ satisfies*

$$||f||_\infty \ll \mathcal{S}_d(f).$$

Proof. See [EW17] Theorem 5.34 on Page 150. □

Corollary A.6. *Let $d > \frac{\dim(G)}{2}$. Then any $f \in \mathcal{H}^d(G)$ has a continuous representative. Moreover, if $f \in C_c^\infty(G)$, then*

$$||f||_\infty \ll \mathcal{S}_d(f).$$

Proof. Let $U \subset \mathfrak{g}$ be a neighborhood of $\{0\}$ on which the exponential map is a diffeomorphism. As continuity is a local property, it suffices to assume that $f \in \mathcal{H}^k(G)$ is supported in $\exp(U)$. Pulling the function back onto U, we apply the Sobolov embedding theorem for open subsets of $\mathbb{R}^d$ to conclude the statement. The second claim follows by the same argument. □

More generally, one can define analogously for every unitary representation $(\pi, \mathscr{H})$ of a Lie group G a Sobolev norm and a Sobolev space. More precisely, for a vector $v \in \mathscr{H}$ and $X \in \mathfrak{g}$ one defines

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

and says that v is differentiable in the direction of X if $D_X v$ is a well-defined element of $\mathscr{H}$. Then one defines as before smooth vectors, Sobolev norms and Sobolev spaces. However, in this general setting, there is no analogue for a Sobolev embedding theorem.

A.2 Sobolev Spaces on Arithmetic Homogeneous Spaces

In this chapter we consider the special case of homogeneous spaces on which we discuss Sobolev norms and Sobolev spaces. As outlined in the last chapter, for a general unitary representation, there is no hope to prove an analogue of a Sobolev embedding theorem. Yet this is possible for suitable homogeneous spaces, with an slightly altered definition of a Sobolev norm. In this subchapter we discuss content from chapter 5 of [EMV09].

Throughout this chapter let G be a linear algebraic group defined over $\mathbb{Q}$. For simplicity we assume that $\mathrm{G} \subset \mathrm{GL}_n$ and denote by $G = \mathrm{G}(\mathbb{R})$ its real points with Lie algebra $\mathfrak{g}$. Write

$$\mathfrak{g}_{\mathbb{Q}} = \mathfrak{g} \cap \mathfrak{gl}_n(\mathbb{Q}).$$

As G is defined over $\mathbb{Q}$ we have that $\mathfrak{g}$ is spanned by elements of $\mathfrak{g}_{\mathbb{Q}}$.

Before treating arithmetic subgroups and arithmetic homogeneous spaces, we discuss matrix norms on G and inner products on $\mathfrak{g}$. On G we consider the matrix norm

$$||g|| = \max_{1 \le i,j \le n} \{|g_{ij}|, |(g^{-1})_{ij}|\}.$$

For $g, h \in G$ we have the properties

$$||g|| = ||g^{-1}||, \qquad ||gh|| \ll ||g|| \cdot ||h||, \tag{A.1}$$

where the constant only depends on G or more precisely on n.

On $\mathfrak{g}$ we fix some positive-definite inner product $\langle \cdot, \cdot \rangle$ which gives rise to some Euclidean norm $|| \cdot ||_{\mathfrak{g}}$ on $\mathfrak{g}$. We note that for $g \in G$,

$$||g||^2 \ll ||\mathrm{Ad}(g)||_{\mathrm{op}} = \sup_{||v||_{\mathfrak{g}} \le 1} ||gvg^{-1}||_{\mathfrak{g}} \ll ||g||^2. \tag{A.2}$$

Denote by $R_g : G \to G$ right multiplication by g. We can use the inner product on $\mathfrak{g}$ to define a Riemannian metric on G. Namely, we set for $u, v \in \mathfrak{g} = T_e G$

$$\langle D_e R_g u, D_e R_g v \rangle_g = \langle u, v \rangle.$$

By the chain rule, it follows for $g, h \in G$ and $u, v \in T_g G$ that

$$\langle D_g R_h u, D_g R_h v \rangle_{gh} = \langle u, v \rangle_g,$$

so that the Riemannian metric on G is right-invariant. The length of a smooth curve $\gamma : [0, 1] \to G$ is given as

$$L(\gamma) = \int_0^1 ||\dot{\gamma}(t)||_{\gamma(t)} \, dt = \int_0^1 \sqrt{\langle \dot{\gamma}(t), \dot{\gamma}(t) \rangle_{\gamma(t)}} \, dt.$$

The induced metric on G is

$$d_G(h_1, h_2) = \inf_{\gamma} L(\gamma),$$

for $h_1, h_2 \in G$, where the infimum is taken over all smooth curves connecting h_1 and h_2. For a smooth curve $\gamma : [0, 1] \to G$ and some $g \in G$, we have as a consequence of (A.2),

$$L(g\gamma g^{-1}) \ll ||g||^2 L(\gamma)$$

and so we have that

$$d_G(gh_1, gh_2) = d_G(gh_1g^{-1}, gh_2g^{-1}) \ll ||g||^2 d_G(h_1, h_2).$$

For a discrete subgroup $\Gamma < G$, we define a metric on the homogeneous space G/Γ for points $x = \Gamma g_x, y = \Gamma g_y \in G/\Gamma$ as

$$d_{G/\Gamma}(x, y) = \inf_{\gamma_1,\gamma_2\in\Gamma} d_G(g_x\gamma_1, g_y\gamma_2).$$

Then it follows by left-invariance and from the above that

$$\begin{aligned} d_{G/\Gamma}(hx, hy) &= \inf_{\gamma_1,\gamma_2\in\Gamma} d_G(hg_x\gamma_1, hg_y\gamma_2) \\ &= \inf_{\gamma_1,\gamma_2\in\Gamma} d_G(hg_x\gamma_1h^{-1}, hg_y\gamma_2h^{-1}) \\ &\ll \inf_{\gamma_1,\gamma_2\in\Gamma} ||h||^2 d_G(g_x\gamma_1, g_y\gamma_2) \\ &\ll ||h||^2 d_{G/\Gamma}(x, y). \end{aligned}$$

We are now ready to discuss arithmetic lattices and arithmetic homogeneous spaces.

Definition A.7. Let $\mathrm{G} \subset \mathrm{GL}_n$ be an algebraic group defined over $\mathbb{Q}$ and denote by G the real points of G. A subgroup $\Gamma < G$ is called **arithmetic** if it is commensurable to $\mathrm{G}(\mathbb{Z})$, i.e. if $\Gamma \cap \mathrm{G}(\mathbb{Z})$ has finite index in both Γ and $\mathrm{G}(\mathbb{Z})$. If $\Gamma \subset G$ is an arithmetic lattice we call G/Γ an **arithmetic homogeneous space**.

We next discuss some examples.

Example A.8. Consider the diagonal subgroup $\mathrm{G} \subset \mathrm{GL}_n$ so that $\mathrm{G}(\mathbb{R}) = \mathbb{R}^n$. Then the arithmetic subgroups $\Gamma \subset \mathbb{R}^n$ are precisely the lattices spanned by rational vectors.

Example A.9. We now consider $\mathrm{G} = \mathrm{SL}_2$. Then

$$\Gamma = \left\{ \begin{pmatrix} \sqrt{2}a & b \\ c & \frac{\sqrt{2}}{2}d \end{pmatrix} \,:\, a, b, c, d \in \mathbb{Z} \text{ so that } ad - bd = 1 \right\}$$

is a non-arithmetic subgroup of $\mathrm{G}(\mathbb{R})$.

Lemma A.10. *Let* $\mathrm{G} \subset \mathrm{GL}_n$ *be a linear algebraic group over* $\mathbb{Q}$ *and* $\Gamma < \mathrm{G}(\mathbb{Q})$ *be an arithmetic lattice. Then there is a* $\mathrm{Ad}(\Gamma)$*-invariant lattice* $\mathfrak{g}_{\mathbb{Z}} \subset \mathfrak{g}$ *that is contained in* $\mathfrak{g}_{\mathbb{Q}}$.

Proof. Choose a rational basis $e_1, \ldots, e_n$ of $\mathfrak{g}_{\mathbb{Q}}$ and set $L = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$ so that

$$\mathrm{G}(\mathbb{Z}) = \{\gamma \in \mathrm{G}(\mathbb{Q}) \,:\, \mathrm{Ad}(\gamma)(L) = L\}.$$

As $[\Gamma : \Gamma\cap\mathrm{G}(\mathbb{Z})]$ has finite index, it follows that the collection of lattices $\mathrm{Ad}(\gamma)(L)$ for $\gamma \in \Gamma$ is finite. So let $\mathfrak{g}_{\mathbb{Z}}$ be the $\mathbb{Z}$-span of

$$\bigcup_{\gamma\in\Gamma} \mathrm{Ad}(\gamma)(L),$$

which defines a lattice in $\mathfrak{g}_{\mathbb{Q}}$ which satisfies all our properties. $\square$

Throughout the rest of this chapter we fix an arithmetic lattice $\Gamma < G$ and $X = G/\Gamma$. Moreover, we fix a $\mathfrak{g}_{\mathbb{Z}} \subset \mathfrak{g}$ with the above properties.

Definition A.11. Let $x \in X$. Then we define the **height** of x as

$$\mathrm{ht}(x) = \sup\left\{\left|\left|\mathrm{Ad}(g^{-1})v\right|\right|^{-1} \,:\, \Gamma g = x \text{ and } v \in \mathfrak{g}_{\mathbb{Z}}\backslash\{0\}\right\}$$

By (A.2), it follows that

$$\mathrm{ht}(gx) \ll ||g||^2 \mathrm{ht}(x). \tag{A.3}$$

We will now use the height to define a Sobolev norm on G/Γ. As preliminary remark, note a function $f : G/\Gamma \to \mathbb{R}$ is called **smooth** if the lift $\tilde{f} : G \to \mathbb{R}$ is smooth. From this viewpoint, we can define the derivative of f analogously to before and so will use the same notation as in Definition A.1.

Definition A.12. For any $f \in C^\infty(X)$ we define the **arithmetic Sobolev norm** as

$$\mathcal{S}_d(f) = ||f||_{\mathcal{H}^d(X)} = \sqrt{\sum_{||\alpha||_1 \le d} ||(1+\mathrm{ht})^d D_\alpha f||^2_{L^2(X)}}.$$

Moreover, we define the **arithmetic Sobolev space** as the closure of

$$\{f \in C^\infty(X) \,:\, \mathcal{S}_d(f) \text{ exists and is finite}\}$$

with respect to the norm $||\circ||_{\mathcal{H}^d(X)}$ inside $L^2(X)$. Finally, $\mathcal{H}^d_0(X)$ is the closure of

$$\{f \in C_c^\infty(X) \,:\, \mathcal{S}_d(f) \text{ exists and is finite}\}$$

with respect to the norm $||\circ||_{\mathcal{H}^d(X)}$ inside $L^2(X)$.

In analogy to Lemma A.4, it follows that $\mathcal{H}^d(X)$ and $\mathcal{H}^d_0(X)$ are Hilbert spaces. We next investigate some properties of Sobolev norms.

Proposition A.13. *(Sobolev embedding theorem) Let $k > \dim(G)$. Then any $f \in \mathcal{H}^k(X)$ has a continuous representative. Moreover, if $f \in C_c^\infty(X)$, then*

$$||f||_\infty \ll \mathcal{S}_k(f).$$

Proof. For a proof we refer to chapter 6 of [EMV09]. □

Denote by $\lambda : G \to U(L^2(X))$ the left regular representation, so that $(\lambda(g)f)(x) = f(g^{-1}x)$ for $f \in L^2(X)$ with $g \in G$ and $x \in X$.

Proposition A.14. *Let $k > \dim(G)$. The following properties hold.*

(a) Then for all $f \in C_c^\infty(X)$ and $||\alpha||_1 \le d$ we have

$$||(1+\mathrm{ht})^d D_\alpha f||_\infty \ll \mathcal{S}_{d+k}(f).$$

(b) For all $f \in \mathcal{H}^d(X)$ and $g \in G$

$$\mathcal{S}_d(\lambda(g)f) \ll ||g||^{4d} \mathcal{S}_d(f).$$

(c) *For all $f, g \in \mathcal{H}_0^d(X)$ and $k > \frac{\dim(G)}{2}$ we have*

$$\mathcal{S}_d(f \cdot g) \ll_d \mathcal{S}_{d+k}(f)\mathcal{S}_{d+k}(g).$$

(d) *For all $f \in \mathcal{H}^d(X)$ and $g \in G$ small enough we have*

$$||f - \lambda(g)f||_\infty \ll d(e, g)\mathcal{S}_{k+1}(f).$$

Proof. We show (a) by using the last proposition:

$$||(1 + \mathrm{ht})^d D_\alpha f||_\infty \ll \mathcal{S}_k((1 + \mathrm{ht})^d D_\alpha f) \ll \mathcal{S}_{d+k}(f).$$

Clearly, (a) implies (c). To prove (b) just use (A.3). Finally, to prove (d) recall that by equation (6.25) of [EW], we have for $v \in \mathfrak{g}$ and all $x \in X$

$$f(\exp(-tv)x) - f(x) = \int_0^t (D_v f)(\exp(-sv)x)\, ds$$

So by choosing a unit vector v so that $\exp(-tv) = g$ for $t = d(e, g)$ we conclude

$$\begin{aligned} ||f - \lambda(g)f||_\infty &\leq \sup_{x \in X} \int_0^t \left|(D_v f)(\exp(-sv)x)\right| ds \\ &\leq d(e, g)||D_v f||_\infty \ll d(e, g)\mathcal{S}_{k+1}(f). \end{aligned}$$

□

A.3 The Relative Trace of Sobolev Norms

In this subchapter we discuss the notion of a relative trace and apply it to the Sobolev norm defined in the last subchapter. Content from Appendix A of [BR02] and chapter 5 of [EMV09] is summarized.

We start with an interlude on the trace of two Hermitian inner products. First consider a finite dimensional complex vector space V and denote by V^+ the Hermitian dual consisting of anti-linear maps $f : V \to \mathbb{C}$. Let $\langle \cdot, \cdot \rangle_A$ and $\langle \cdot, \cdot \rangle_B$ be two non-negative Hermitian inner products on V. By a slight abuse of notation we simply denote by A the inner product $\langle \cdot, \cdot \rangle_A$ and we use the same convention for B.

We denote by A_+ the map

$$A_+ : V \longrightarrow V^+, \qquad v \longmapsto \langle v, \cdot \rangle_A,$$

where B_+ is analogously defined. If A is positive definite, then A_+ is an isomorphism of finite dimensional vector spaces.

Definition A.15. Let V be a complex finite dimensional vector space and assume that $\langle \cdot, \cdot \rangle_A$ and $\langle \cdot, \cdot \rangle_B$ are two non-negative Hermitian inner products. Assume moreover that B is positive-definite. Then we define the **relative trace** of A and B as

$$\mathrm{tr}(A, B) = \mathrm{tr}(B_+^{-1} A_+).$$

Lemma A.16. *In the above setting, let $e_1, \ldots, e_n$ be an orthogonal basis of V with respect to $\langle \cdot, \cdot \rangle_B$. Then we have that*

$$\operatorname{tr}(A, B) = \sum_{i=1}^{n} \frac{\langle e_i, e_i \rangle_A}{\langle e_i, e_i \rangle_B}.$$

Proof. For each $i \in \{1, \ldots, n\}$ there are some $\lambda_{i1}, \ldots, \lambda_{in}$ so that

$$B_+^{-1} A_+(e_i) = \sum_{j=1}^{n} \lambda_{ij} e_j.$$

We then have that $\operatorname{tr}(A, B) = \sum_{i=1}^{n} \lambda_{ii}$. Moreover, it follows that $A_+(e_i) = \sum_{j=1}^{n} \lambda_{ij} B_+(e_j)$ or equivalently

$$\langle e_i, v \rangle_A = \sum_{j=1}^{n} \lambda_{ij} \langle e_j, v \rangle_B$$

for all $v \in V$. Plugging in $v = e_i$ we conclude that $\lambda_{ii} = \frac{\langle e_i, e_i \rangle_A}{\langle e_i, e_i \rangle_B}$ and so the claim follows. $\square$

The above treatment of the relative norm in the finite dimensional case allows a generalization to the infinite dimensional case.

Definition A.17. Let V be a complex topological vector space and let $\langle \cdot, \cdot \rangle_A$ and $\langle \cdot, \cdot \rangle_B$ be two non-negative Hermitian inner products so that $\langle \cdot, \cdot \rangle_B$ is positive definite. The **relative trace** of A and B is defined as

$$\operatorname{tr}(A, B) = \sup_{W \subset V} \operatorname{tr}(A_W, B_W),$$

where the supremum is taken over all finite dimensional subspaces $W \subset V$ and A_W respectively B_W denotes the restriction of A respectively B onto W.

Proposition A.18. *In the above setting assume that V is separable and consider $W_1 \subset W_2 \subset \ldots \subset V$ an increasing sequence of subspaces so that V is equal to the closure of $\bigcup_{i=1}^{\infty} W_i$. Then,*

$$\operatorname{tr}(A, B) = \lim_{n \to \infty} \operatorname{tr}(A_{W_n}, B_{W_n}).$$

In particular, if $(e_i)_{i \in \mathbb{N}}$ is an orthogonal basis of V with respect to B, then

$$\operatorname{tr}(A, B) = \sum_{i=1}^{\infty} \frac{\langle e_i, e_i \rangle_A}{\langle e_i, e_i \rangle_B}.$$

Proof. The second equality is clearly implied by the first one. To show the first equality, note that $\geq$ is obvious. To see $\leq$ we distinguish the cases where $\operatorname{tr}(A, B)$ is finite or infinite. Assume for now that $\operatorname{tr}(A, B)$ is finite. Let $\varepsilon > 0$ and choose $V' \subset V$ finite dimensional so that

$$\operatorname{tr}(A, B) - \varepsilon \leq \operatorname{tr}(A_{V'}, B_{V'}) \leq \operatorname{tr}(A, B).$$

Write $V' = \langle v_1, \ldots, v_n \rangle$ for an orthonormal basis $v_1, \ldots, v_n$ with respect to B. As by assumption a Hermitian inner product is continuous and $\bigcup_{k=1}^{\infty} W_k$ is dense in V, we can choose for each v_i some $w_i \in \bigcup_{k=1}^{\infty} W_k$ so that for all i, j we have

$$|\langle v_i, v_j \rangle_A - \langle w_i, w_j \rangle_A| \leq \frac{\varepsilon}{n}$$

and

$$|\langle v_i, v_j \rangle_B - \langle w_i, w_j \rangle_B| = |\delta_{ij} - \langle w_i, w_j \rangle_B| \leq \varepsilon.$$

Set $W = \langle w_1, \ldots, w_n \rangle$. Upon using the Gram-Schmidt algorithm on $w_1, \ldots, w_n$ for the inner product $\langle \cdot, \cdot \rangle_B$, we can assume without loss of generality that $w_1, \ldots, w_n$ are a B-orthonormal basis of W and satisfy the above inequalities. This follows as by assumption $\langle w_i, w_j \rangle_B$ is for $i \neq j$ close to 0 and $\langle w_i, w_i \rangle_B$ is close to 1 and hence the Gram-Schmidt algorithm does not change the vectors w_i by much. Thus it follows for $W = \langle w_1, \ldots, w_n \rangle$ that

$$|\mathrm{tr}(A_{V'}, B_{V'}) - \mathrm{tr}(A_W, A_W)| \leq \sum_{i=1}^{n} |\langle v_i, v_i \rangle_A - \langle w_i, w_i \rangle_A| \leq \varepsilon.$$

Hence it follows that

$$\mathrm{tr}(A, B) - 2\varepsilon \leq \mathrm{tr}(A_W, B_W) \leq \mathrm{tr}(A, B).$$

Now choose some large enough W_i so that $W \subset W_i$. Then $\mathrm{tr}(A_W, A_W) \leq \mathrm{tr}(A_{W_i}, A_{W_i})$, showing that

$$\mathrm{tr}(A, B) - 2\varepsilon \leq \mathrm{tr}(A_{W_i}, B_{W_i}) \leq \mathrm{tr}(A, B).$$

This implies the claim under the assumption that $\mathrm{tr}(A, B)$ is finite. If $\mathrm{tr}(A, B)$ is infinite, the same argument applies to a finite dimensional subset $V' \subset V$ so that $n \leq \mathrm{tr}(A_{V'}, B_{V'})$. $\square$

Proposition A.19. *In the setting of the last proposition, assume that* $||v||_A \leq c||v||_B$ *for a constant* $c > 0$. *Then there exists an operator* $\mathrm{Op}_{A,B} : V \to V$ *uniquely characterized by*

$$\langle v, w \rangle_A = \langle \mathrm{Op}_{A,B} v, w \rangle_B$$

for all $v, w \in V$. *Moreover, the* $\mathrm{tr}(A, B)$ *is finite if and only if* $\mathrm{Op}_{A,B}$ *is of trace class and if so then*

$$\mathrm{tr}(A, B) = \mathrm{tr}(\mathrm{Op}_{A,B}).$$

Proof. Fix some $v \in V$ and consider the map $w \mapsto \langle v, w \rangle_A$. By Cauchy-Schwarz

$$||\langle v, w \rangle_A|| \leq ||v||_A ||w||_A \leq c^2 ||v||_B ||w||_B$$

and so by Frechet- Riesz, for each $v \in V$ there is some $v' \in V$ so that

$$\langle v, w \rangle_A = \langle v', w \rangle_B.$$

Set $\mathrm{Op}_{A,B}v = v'$ and this hence defined a bounded operator $V \to V$. To prove the second claim recall that

$$\mathrm{tr}(\mathrm{Op}_{A,B}) = \sup_{(v_n),(w_n)} \sum_{i=1}^{N} |\langle \mathrm{Op}_{A,B} v_i, w_i \rangle_B|,$$

where the supremum is taken over all B-orthonormal lists (v_n) and (w_n). So we conclude by Cauchy-Schwarz

$$\begin{aligned}
\mathrm{tr}(\mathrm{Op}_{A,B}) &= \sup_{(v_n),(w_n)} \sum_{i=1}^{N} |\langle \mathrm{Op}_{A,B} v_i, w_i \rangle_B| \\
&= \sup_{(v_n),(w_n)} \sum_{i=1}^{N} |\langle v_i, w_i \rangle_A| \\
&= \sup_{(v_n)} \sum_{i \geq 1} \langle v_i, v_i \rangle_A \\
&= \mathrm{tr}(A, B),
\end{aligned}$$

which implies the claim. □

We return to the setting of the last subchapter. As before, consider a linear algebraic group $\mathrm{G} \subset \mathrm{GL}_n$ over $\mathbb{Q}$ with real points $G = \mathrm{G}(\mathbb{R})$ and a arithmetic lattice $\Gamma < \mathrm{G}(\mathbb{Q})$, so that G/Γ is an arithmetic homogeneous space. We use $\mathcal{S}_d^2$ as a shorthand for the inner product defined for $f, g \in \mathcal{H}^d(X)$ as

$$\langle f, g \rangle = \sum_{||\alpha||_1 \leq d} \langle (1+\mathrm{ht})^d D_\alpha f, (1+\mathrm{ht})^d D_\alpha g \rangle_{L^2(X)}.$$

Let $k > \dim(G)$. By the Sobolev embedding theorem and by Proposition A.14 we have for all $f \in \mathcal{H}_0^{d+k}(X)$ and $||\alpha||_1 \leq d$ that

$$||(1+\mathrm{ht})^d D_\alpha f||_\infty \ll \mathcal{S}_{d+k}(f). \tag{A.4}$$

We will use (A.4) to deduce that the relative trace of two Sobolev inner products $\mathcal{S}_d^2$ and $\mathcal{S}_{d'}^2$ and is finite provided that d and d' are far enough away.

Proposition A.20. *Let $d > d' > 0$ be integers so that*

$$d - d' > \dim(G).$$

Then the relative trace $\mathrm{tr}(\mathcal{S}_{d'}, \mathcal{S}_d)$ on the Hilbert space $\mathcal{H}_0^d(X)$ is finite.

Proof. We consider for a fixed $x \in X$ and $\alpha \in \mathbb{N}_0^d$ with $||\alpha||_1 \leq d'$ the map

$$L_x : \mathcal{H}_0^d(X) \to \mathbb{C}, \qquad f \mapsto (1+\mathrm{ht}(x))^d (D_\alpha f)(x),$$

where we note that this map is well defined by the Sobolev embedding theorem. We note that L_x is not the zero map as $\mathcal{H}_0^d(X)$ contains $C_c(X)$ thus we observe that $\ker(L_x)$ is a closed proper subspace of $\mathcal{H}_0^d(X)$. Choosing some vector $g \in \ker(L_x)^\perp$ with $L_x(g) = 1$ we conclude that we have an orthogonal direct sum

$$\mathcal{H}_0^d(X) = \ker(L_x) \oplus \mathbb{C}g,$$

where each function $f \in \mathcal{H}_0^d(X)$ has the decomposition

$$f = f - L_x(f)g + L_x(f)g.$$

Finally we chose an orthonormal basis $f_1, f_2, \ldots$ of $\ker(L_x)$ with respect to $\mathcal{S}_d^2$ so that $g, f_1, f_2, \ldots$ is an orthogonal basis of $\mathcal{H}_0^d(X)$. Using that $L_x(f_n) = |L_x(f_n)|^2 = 0$ for all $n \geq 1$, we conclude

$$\begin{aligned}\operatorname{tr}(|L_x|^2, \mathcal{S}_d^2) &= \frac{\langle g, g\rangle_{L_x}}{\langle g, g\rangle_{\mathcal{H}_0^d(X)}} + \sum_{n\geq 1} \frac{\langle f_n, f_n\rangle_{L_x}}{\langle f_n, f_n\rangle_{\mathcal{H}_0^d(X)}} \\ &= \frac{\langle g, g\rangle_{L_x}}{\langle g, g\rangle_{\mathcal{H}_0^d(X)}} \\ &= \frac{|(1+\operatorname{ht}(x))^d (D_\alpha g)(x)|^2}{\mathcal{S}_d^2} \ll 1,\end{aligned}$$

where in the last inequality we used (A.4). Integrating now over x, using that X is a probability space, and summing over all $||\alpha||_1 \leq d'$ we conclude that the relative trace $\operatorname{tr}(\mathcal{S}_{d'}, \mathcal{S}_d)$ on the Hilbert space $\mathcal{H}_0^d(X)$ is finite. □

References

[Bay] Nadir Bayo. Classification of quaternion algebras over the field of rational numbers. Bachelor Thesis, Available at `https://people.math.ethz.ch/~pink/Theses/2017-Bachelor-Nadir-Bayo.pdf`.

[BdlHV08] Bachir Bekka, Pierre de la Harpe, and Alain Valette. *Kazhdan's property (T)*, volume 11 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2008.

[Ber16] Nicolas Bergeron. *The spectrum of hyperbolic surfaces*. Universitext. Springer, Cham; EDP Sciences, Les Ulis, 2016. Appendix C by Valentin Blomer and Farrell Brumley, Translated from the 2011 French original by Brumley [2857626].

[Bor97] Armand Borel. *Automorphic forms on* $\mathrm{SL}_2(\mathbf{R})$, volume 130 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1997.

[BR95] Mikhail Borovoi and Zeév Rudnick. Hardy-Littlewood varieties and semisimple groups. *Invent. Math.*, 119(1):37–66, 1995.

[BR02] Joseph Bernstein and Andre Reznikov. Sobolev norms of automorphic functionals. *Int. Math. Res. Not.*, (40):2155–2174, 2002.

[BS91] M. Burger and P. Sarnak. Ramanujan duals. II. *Invent. Math.*, 106(1):1–11, 1991.

[BT72] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. *Inst. Hautes Études Sci. Publ. Math.*, (41):5–251, 1972.

[CHH88] M. Cowling, U. Haagerup, and R. Howe. Almost L^2 matrix coefficients. *J. Reine Angew. Math.*, 387:97–110, 1988.

[Clo03] Laurent Clozel. Démonstration de la conjecture τ. *Invent. Math.*, 151(2):297–328, 2003.

[Dav39] H. Davenport. On Waring's problem for fourth powers. *Ann. of Math. (2)*, 40:731–747, 1939.

[Dav05] H. Davenport. *Analytic methods for Diophantine equations and Diophantine inequalities*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 2005.

[DFI93] W. Duke, J. Friedlander, and H. Iwaniec. Bounds for automorphic L-functions. *Invent. Math.*, 112(1):1–8, 1993.

[EKL06] Manfred Einsiedler, Anatole Katok, and Elon Lindenstrauss. Invariant measures and the set of exceptions to Littlewood's conjecture. *Ann. of Math. (2)*, 164(2):513–560, 2006.

[ELMV09] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Distribution of periodic torus orbits on homogeneous spaces. *Duke Math. J.*, 148(1):119–174, 2009.

[ELMV11] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Distribution of periodic torus orbits and Duke's theorem for cubic fields. *Ann. of Math. (2)*, 173(2):815–885, 2011.

[ELMV12] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. The distribution of closed geodesics on the modular surface, and Duke's theorem. *Enseign. Math. (2)*, 58(3-4):249–313, 2012.

[EMMV19] Manfred Einsiedler, Grigory Margulis, Amir Mohammadi, and Akshay Venkatesh. Effective equidistribution and property (τ). *J. Amer. Math. Soc.*, 2019.

[EMV09] Manfred Einsiedler, Grigory Margulis, and Akshay Venkatesh. Effective equidistribution for closed orbits of semisimple groups on homogeneous spaces. *Invent. Math.*, 177(1):137–212, 2009.

[EW] Manfred Einsiedler and Thomas Ward. *Unitary Representations and Unitary Duals*. In preparation, Available at `https://tbward0.wixsite.com/books/unitary`.

[EW17] Manfred Einsiedler and Thomas Ward. *Functional analysis, spectral theory, and applications*, volume 276 of *Graduate Texts in Mathematics*. Springer, Cham, 2017.

[GGN] Anish Ghosh, Alexander Gorodnik, and Amos Nevo. Discrepancy of distribution of rational points on algebraic groups. In preparation.

[GGN13] Anish Ghosh, Alexander Gorodnik, and Amos Nevo. Diophantine approximation and automorphic spectrum. *Int. Math. Res. Not. IMRN*, (21):5002–5058, 2013.

[GGPS] I. M. Gelfand, M. I. Graev, and I. I. Pyatetskii-Shapiro. *Generalized functions. Vol. 6*. Representation theory and automorphic functions, Translated from the 1966 Russian original by K. A. Hirsch.

[HB96] D. R. Heath-Brown. A new form of the circle method, and its application to quadratic forms. *J. Reine Angew. Math.*, 481:149–206, 1996.

[HC58] Harish-Chandra. Spherical functions on a semisimple Lie group. I. *Amer. J. Math.*, 80:241–310, 1958.

[HC73] Harish-Chandra. Harmonic analysis on reductive p-adic groups. In *Harmonic analysis on homogeneous spaces (Proc. Sympos. Pure Math., Vol. XXVI, Williams Coll., Williamstown, Mass., 1972)*, pages 167–192, 1973.

[HL] Gordfrey Harold Hardy and John Edensor Littlewood. A new solution of waring's problem. *Quart. J. Math.*, 48:272–293. See also Hardy's collected papers, Volume 1, Clarendon Press, Oxford, 1966, pp. 382-403.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Jer] Charlotte Jergitsch. Der satz von hasse-minkowski. Bachelor Thesis, Available at `https://people.math.ethz.ch/~pink/Theses/2017-Bachelor-Charlotte-Jergitsch.pdf`.

[Kaz67] D. Kazhdan. On the connection of the dual space of a group with the structure of its closed subgroups. *Funkcional. Anal. i Prilozen.*, 1:71–74, 1967.

[Kir76] A. A. Kirillov. *Elements of the theory of representations*. Springer-Verlag, Berlin-New York, 1976. Translated from the Russian by Edwin Hewitt, Grundlehren der Mathematischen Wissenschaften, Band 220.

[Kna02] Anthony W. Knapp. *Lie groups beyond an introduction*, volume 140 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, second edition, 2002.

[Kot88] Robert E. Kottwitz. Tamagawa numbers. *Ann. of Math. (2)*, 127(3):629–646, 1988.

[Lan75] Serge Lang. $\mathrm{SL}_2(\mathbf{R})$. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1975.

[LZ] Alexander Lubotzky and Andrzej Zuk. *On property tau*. In preparation, Available at `http://www.ma.huji.ac.il/~alexlub/BOOKS/On%20property/On%20property.pdf`.

[Mar] Grigory Margulis. Oppenheim conjecture. 5:272–327.

[Mat95] Pertti Mattila. *Geometry of sets and measures in Euclidean spaces*, volume 44 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995. Fractals and rectifiability.

[Moo87] Calvin C. Moore. Exponential decay of correlation coefficients for geodesic flows. In *Group representations, ergodic theory, operator algebras, and mathematical physics (Berkeley, Calif., 1984)*, volume 6 of *Math. Sci. Res. Inst. Publ.*, pages 163–181. Springer, New York, 1987.

[Nat96] Melvyn B. Nathanson. *Additive number theory*, volume 164 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. The classical bases.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[Nev98] Amos Nevo. Spectral transfer and pointwise ergodic theorems for semi-simple Kazhdan groups. *Math. Res. Lett.*, 5(3):305–325, 1998.

[PR94] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1994.

[Sel65] Atle Selberg. On the estimation of Fourier coefficients of modular forms. In *Proc. Sympos. Pure Math., Vol. VIII*, pages 1–15. Amer. Math. Soc., Providence, R.I., 1965.

[Spr98] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, second edition, 1998.

[Vau97] R. C. Vaughan. *The Hardy-Littlewood method*, volume 125 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, second edition, 1997.

[Vin47] I. M. Vinogradov. The method of trigonometrical sums in the theory of numbers. *Trav. Inst. Math. Stekloff*, 23:109, 1947.

[VW02] R. C. Vaughan and T. D. Wooley. Waring's problem: a survey. In *Number theory for the millennium, III (Urbana, IL, 2000)*, pages 301–340. A K Peters, Natick, MA, 2002.

[Wei82] André Weil. *Adeles and algebraic groups*, volume 23 of *Progress in Mathematics*. Birkhäuser, Boston, Mass., 1982. With appendices by M. Demazure and Takashi Ono.