EPFL

Thèse n° 10 488

Mean value theorems for collections of lattices with a prescribed group of symmetries

Présentée le 12 janvier 2024

Faculté des sciences de base
Chaire d'Arithmétique
Programme doctoral en mathématiques

pour l'obtention du grade de Docteur ès Sciences

par

Nihar Prakash GARGAVA

Acceptée sur proposition du jury

Prof. F. Eisenbrand, président du jury
Prof. M. Viazovska, directrice de thèse
Prof. A. Gorodnik , rapporteur
Dr D. Radchenko, rapporteur
Prof. Ph. Michel, rapporteur

École
polytechnique
fédérale
de Lausanne

2024

Abstract

Euclidean lattices are mathematical objects of increasing interest in the fields of cryptography and error-correcting codes. This doctoral thesis is a study on high-dimensional lattices with the motivation to understand how efficient they are in terms of being able to pack spheres. We study this by establishing a formula for the average number of lattice points of random Euclidean lattices inside a measurable subset of a real vector space, given the constraint that all the lattices are invariant under a prescribed finite group of symmetries.

The thesis includes the discussion on what could be the appropriate probability space of random lattices with prescribed symmetries, when it is possible to derive an integration formula on these spaces and finally, and what the integration formula is given these conditions. The thesis then proceeds with an outline of recent applications of these integration formulas for the lattice packing problem. The techniques used involve number theory, representation theory, geometry and dynamics which the reader is introduced to in the text.

Resumé

Les réseaux euclidiens sont des objets mathématiques qui suscitent de plus en plus d'intérêt, notamment dans les domaines de la cryptographie et des codes correcteurs d'erreurs. Cette thèse de doctorat étudie les réseaux de grande dimension, avec la motivation de comprendre leur efficacité en terme d'empilement de sphères. Nous étudions cela en établissant une formule pour le nombre moyen de points de réseaux euclidiens aléatoires à l'intérieur d'un sous-ensemble mesurable d'un espace vectoriel réel, étant donnée la contrainte que tous les réseaux soient invariants par un groupe fini de symétries prescrites.

La thèse inclut une discussion sur quel espace de probabilité pourrait être l'espace approprié de réseaux aléatoires avec des symétries prescrites, sur quand il est possible de dériver une formule d'intégration sur ces espaces, et enfin sur quelle est la formule d'intégration compte tenu de ces conditions. L'article se poursuit par un aperçu des applications récentes de ces formules d'intégration aux empilements de sphères issus de réseaux. Les techniques utilisées font appel à la théorie des nombres, à la théorie des représentations, à la géométrie et à la dynamique, auxquelles le lecteur est initié à travers le texte.

Keywords

Sphere Packings · Random Lattices · Arithmetic Groups · Division Algebra · Homogeneous Spaces

Contents

Acknowledgements

This thesis is made possible due to the help of a lot of wonderful people. I would like to thank my advisor Prof. Maryna Viazovska for her guidance as my thesis advisor. It was a great honour to be supervised by her. Other than that, Dr. Vlad Serban has been an excellent collaborator in this research work.

Mathematically, I have interacted numerous people and some ideas emerging from such discussions could be found throughout the thesis. This includes a lot of people, partly because I had the fortune of meeting many mathematicians and partly because I talk a lot. I will try to mention as many as I can remember. Prof. Philippe Michel, Dr. Manuel Leuthi, Dr. Matthew deCourcy-Ireland, Gauthier Leterrier, Dr. Maxim Mornev, Dr. Riccardo Maffucci, Dr. Martin Stoller, Vignesh Nadarajan and Svenja Zur Verth are some number theorists that I have been in touch with during the doctorate while they were at EPFL. Some discussions with Dr. Danylo Radchenko and Prof. Alex Gorodnik have also been useful to clear out some loose ends in this research work. Prof. Ronnie Sebastian in Mumbai was also kind enough to let me discuss some things related to my thesis with him.

On the side of offering social support during my six years of mathematical education in Switzerland, I must thank the numerous people of the Indian community who I owe a great deal to in making my time memorable and for getting through the difficult times of the pandemic. Some of the people that I should definitely mention are Dr. Mukesh Thakur, Dr. Ankit Gupta, Harshvardhan, Dr. Bhushan Hegde, Dr. Shankha Nag, Dr. Rasool Ahmad, Moulik Choraria, Richa Agrawal, Aditi Mathur, Shreyas Joglekar and Santhanu Panikar. Aditi helped a lot in the proof reading process for this thesis as well. Some coworkers in the math department that I would destress myself by talking to are Dr. Gonzalo Ruiz, Dr. Ana Retegan, Bruno Correia, and Dr. Rahul Sharma. Prof. Gerard Duchamp in Paris has been a great supporter in my mathematical journey and I owe it to him to have introduced me with research level mathematics and European culture in general. Dr. Simon Burton has been a really nice mathematical companion while I was in Cambridge. I owe gratitude towards my family for their continued support for me despite me being too busy in my work sometimes.

Some words on the sponsors. The doctoral thesis was funded by the Swiss National Science Foundation (SNSF), Project funding (Div. I-III), "Optimal configurations in multidimensional spaces", 184927. Some part of the thesis work was also done during my stay in Cambridge, UK sponsored by Quantinuum. Other than that, the financial forces that helped me enter and survive in Switzerland as a masters student are the J N Tata Endowment scholarship and the Fondation Professeur Charles Rapin scholarship.

I also thank Monique Kiener who provides great secretarial support for our research group.

Chapter 1

Introduction

> The fundamental problem of communication is that of reproducing at one point, either exactly or approximately, a message selected at another point - Claude Shannon, 1944

The theory of error-correcting codes attempts to mitigate this fundamental problem. At its most basic level, a code is a discrete subset of a space that encodes information to be communicated on an error-prone channel. Codes are point distributions in vector spaces, graphs or manifolds, often with the desirable property that the points be optimally arranged so as to minimize the chance of an error-correcting algorithm to confuse two different points.

Sphere packings with high packing densities are sought after as error-correcting codes in the regime when codes are subsets of points in $\mathbb{R}^d$ and errors are random Gaussian vectors added randomly to the information. This is known as the Additive White Gaussian Noise (AWGN) model of error-propagation. Lattices are of high interest because of their simpler code descriptions and the ease of understanding [ELZ05].

Finding the densest sphere packing in $d = 3$ is at least a four centuries old problem going all the way back to Kepler and is very fundamental to understanding crystal structures of physical materials. This was solved by Hales using computer-assisted methods [Slo98].

Here is a quote from [CE03] about other dimensions:

> For $d \geq 4$, the problem remains unsolved. Upper and lower bounds on the density are known, but they differ by an exponential factor as $d \to \infty$. Each dimension seems to have its own peculiarities, and it does not seem likely that a single, simple construction will give the best packing in every dimension.

The problem for $d = 8, 24$ is now famously solved due to the work of Viazovska and others [Via17; CKMRV17]. Other dimensions remain out of reach and even the lower bounds and upper bounds differ exponentially as $d \to \infty$.

All the known asymptotic lower bounds on sphere packing densities are existence results of lattices. In fact, even more specifically, all such existence results are the application of some variation of the probabilistic method, where a random lattice among a large collection of lattices is shown to have the desirable property by the virtue of their statistical distribution.

There is computational evidence to believe that the best sphere packings are not lattice packings in high dimensions. Nonetheless, lattice packing arrangements with high packing densities connect with many areas in mathematics such as string theory, harmonic analysis, hyperbolic geometry, finite groups, error-correcting codes and some very beautiful areas of number theory like elliptic curves, modular forms, finite fields, etc [CS13].

In general, studying random lattices in high dimensions is also of interest from the point of view of cryptography, especially serving as the source of computational complexity in preventing post-quantum attacks against secret-sharing [MR09].

1.1 Lower bounds on lattice packing densities

Consider $\mathbb{R}^d$ with the standard inner product. A lattice $\Lambda \subseteq \mathbb{R}^d$ is a discrete subgroup such that the quotient space $\mathbb{R}^d/\Lambda$ has a finite induced volume which we henceforth will call the covolume of Λ.

Throughout this thesis, we only mean lattices to denote these Euclidean lattices[1].

A more simple but equivalent idea of a lattice is that it is a set

$$\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_d,$$

for some d vectors $v_1, v_2, \ldots, v_d \in \mathbb{R}^d$. If we were to write instead take $\Lambda' = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_d$ for some other basis of vectors $w_1, \ldots, w_d \in \mathbb{R}^d$, we must get the relation that $\Lambda' = \Lambda$ will be the same lattice if and only if

$$w_i = \sum_{j=1}^{d} a_{ij} v_j, \text{ for some } a_{ij} \in \mathbb{Z}$$

and the a_{ij} form a matrix whose inverse also has integer entries. Such a matrix $[a_{ij}]$ must have determinant ± 1. The covolume of the lattice Λ in this point of view is the volume of a d-dimensional parallelepiped that the vectors $v_1, \ldots, v_d$ span or in other words, the absolute value of a matrix whose columns are $v_1 \ldots v_d$.

Given a lattice Λ, choose $r = r_{\text{pack}}$ and consider the open balls $\{B_r(v)\}_{v\in\Lambda}$, which implies that for any $v_1, v_2 \in \Lambda$, $B_r(v_1) \cap B_r(v_2) \neq \emptyset \Rightarrow v_1 = v_2$. Here r_{pack} is the packing radius of the lattice, i.e., half of the length of the shortest non-zero vector.

This setup of spheres is called a lattice sphere packing, or simply lattice packing inside $(\mathbb{R}^d, \langle\ ,\ \rangle)$. Packing density of a lattice packing is

$$\Delta(\Lambda) = \lim_{R\to\infty} \frac{\mu\left(B_R(0) \cap \left(\bigsqcup_{v\in\Lambda} B_r(v)\right)\right)}{\mu\left(B_R(0)\right)} = \frac{\mu(B_{r_{\text{pack}}}(0))}{\mu(\mathbb{R}^d/\Lambda)}. \tag{1.1}$$

If we denote $\mathrm{SL}(V)$ to be the group of all unimodular linear transformations on V, we can now define

$$c_d = \sup\left\{\mu\left(gB_r(0)\right) \mid r > 0,\ g \in \mathrm{SL}(V) \text{ and } gB_r(0) \cap \Lambda_0 = \{0\}\right\}.$$

This quantity c_d is related to the definition in Equation (1.1) by

$$\tfrac{1}{2^d} c_d = \sup_{\substack{\Lambda\subseteq\mathbb{R}^d,\\ \Lambda \text{ a lattice}}} \Delta(\Lambda).$$

It then follows that for any lattice $\Lambda \subseteq \mathbb{R}^d$, $\Delta(\Lambda) \geq \frac{1}{2^d} c_d$. The exact value of c_d is known only for $d \in \{1, 2, 3, 4, 5, 6, 7, 8, 24\}$. Figure 1.1 is a visualization of the fact that $c_2 = \frac{2\pi}{\sqrt{3}}$.

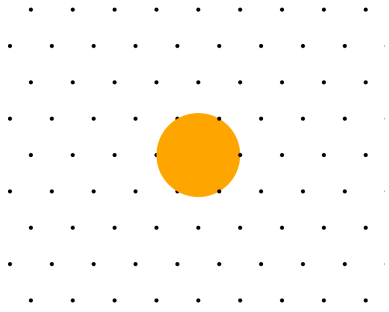
The goal of this thesis has been to improve and generalise the asymptotic lower bounds on the sphere packing problem. Table 1.1 displays some known lower bounds on the lattice packing problem. The list is non-exhaustive since some individual dimensions have explicit lattice constructions that work very nicely for packing. However, these are currently the best known lower bounds for very large dimensions d, let's say when $d > 400$. The common theme among all the results mentioned in Table 1.1 is the usage of probabilistic methods and Siegel transforms. That is, the proof techniques involve showing the existence of a well-rounded lattice by considering a large collection of random lattices.

Also, not all bounds mentioned in Table 1.1 are valid for all dimensions. To find which bound applies to given dimension could be computationally challenging as one would have to figure out the best way to express the dimension d as one of the parameters given in the table[2]. Nevertheless, one could still estimate what is the asymptotic al growth in each of those lower bounds with d.

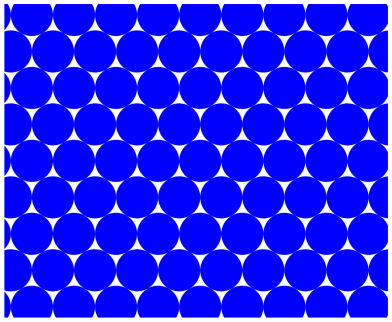
One additional remark about Table 1.1 is that these are lower bounds on the lattice packing problem and yet turn out to be the best lower bounds on the sphere packing problem. It is completely unclear why should asking for the densest arrangement of spheres in high dimensions lead to the lattice arrangements, nonetheless finding provably better non-lattice packings in high dimensions is currently an open problem.

[1] There is a more general notion of a lattice in an algebraic group as discussed in Section 2.1.3. We will never use the word lattice to discuss those for the sake of clarity.

[2] In the case of $d = 2\varphi(n)$, one is lead to the notorious inverse-phi problem.



(a) The largest ball that can avoid all non-zero points of some unit covolume lattice in two dimensions has volume equal to $\frac{2\pi}{\sqrt{3}}$. Any bigger disk around the origin will contain at least one non-zero point in any given unit covolume lattice.



(b) The honeycomb lattice or the hexagonal circle packing is the densest arrangement of equal balls in two dimensions. The packing density is $\frac{\pi}{\sqrt{12}}$.

Figure 1.1: The hexagonal circle packing.

Bound	Dimensions covered	Due to	Reference
$c_d \geq 2$	Any $d \geq 1$	Minkowski, Hlawka	[Hla43]
$c_d \geq \frac{2d}{e(1-e^{-d})}$	Any $d \geq 1$	Rogers	[Rog47]
$c_{4n} \geq \frac{24n}{e(1-e^{-n})}$	$d = 4n, n \geq 1$	Vance	[Van11]
$c_{2\varphi(n)} \geq n$	$d = 2\varphi(k)$ for some $k \in \mathbb{Z}_{\geq 1}$	Venkatesh	[Ven13]
$c_{2\dim D} \geq \#G_0$	$d = 2[D:\mathbb{Q}]$ for some $\mathbb{Q}$-division algebra, $G_0 \subseteq D^\times$ is any finite subgroup	G.	[Gar23]
$c_{n\dim D} \geq \frac{\#G_0 n}{e(1-e^{-n})}$	$d = n[D:\mathbb{Q}]$ for some $\mathbb{Q}$-division algebra, $G_0 \subseteq D^\times$ is any finite subgroup	G.,Serban	[GS22]

Table 1.1: Comparison of some lower bounds on c_d

1.2 Probability space of lattices and Siegel transforms

Let us introduce this proof technique to the reader by demonstrating the Minkowski-Hlawka lower bound from Table 1.1. Let $\mathrm{SL}_d(\mathbb{R})$ denote the group of unimodular square matrices of size d. Then the equivalence of the two definitions of lattices as given in the preceding section imply that the following is a surjective map onto unit covolume lattices in $\mathbb{R}^d$.

$$g \mapsto g\mathbb{Z}^d, \ g \in \mathrm{SL}_d(\mathbb{R}).$$

This informs us that the space of unit covolume lattices is in bijection with $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$. This has the structure of a smooth (d^2-1)-dimensional manifold. On this space, there is a very natural description of a measure due to the general theory of Haar measure on locally compact groups (see Section 2.1.1). What this means is that there is a natural way to compute volumes of reasonably defined subsets $A \subseteq \mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ and hence we can wonder if we can compute probabilities of some random events happening in the space of unit covolume lattices. Such a probabilistic modelling is however only meaningful when the total event space $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ has probability 1.

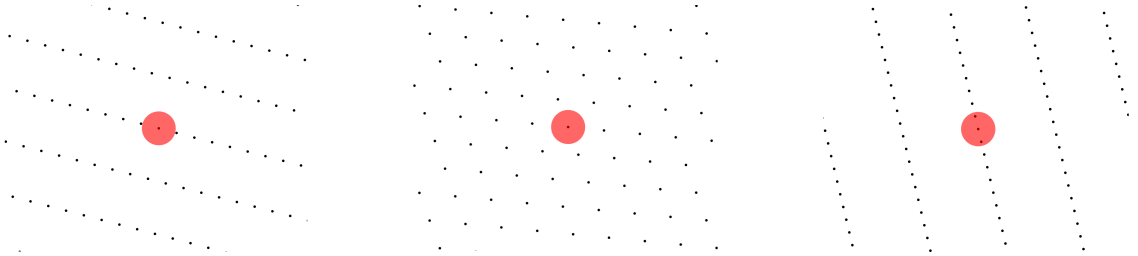
What is special in this situation is the following theorem that can perhaps be attributed to Siegel.

Theorem 1.1. *There exists a unique measure on* $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ *that is invariant under the left-*$\mathrm{SL}_d(\mathbb{R})$ *action on this space and furthermore, this measure yields a finite total volume.*

Hence, up to rescaling this natural choice of measure coming from Theorem 1.1, we can assume that the total volume of $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ is 1 and we can talk about random lattices.

Figure 1.2 is an attempt to show one such random event of interest. Figure 1.2a and Figure 1.2b are the cases when only the origin lies inside a ball, whereas Figure 1.2c shows the case when there are non-trivial points. We want to find the probability of how likely is that the ball has only the origin in

its intersection with the lattice. See also Figure 1.3 for a region in the upper half-plane corresponding to the lattices that we want to favour.



(a) (b) (c)

Figure 1.2: Some two dimensional lattices. We try to study how many points of a randomly chosen lattice are inside a ball centered at the origin.

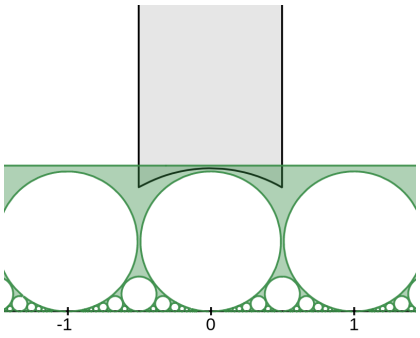


Figure 1.3: To each point (x_0, y_0) in the region $\{x + iy, y > 0\}$, it is standard to associate the lattice $\begin{bmatrix} \frac{1}{\sqrt{y_0}} & \frac{x_0}{\sqrt{y_0}} \\ 0 & \sqrt{y_0} \end{bmatrix} \mathbb{Z}^2$. In this picture, the green area depicts the region that corresponds to lattices that intersect with a ball of radius $R = 0.99$ with only the origin in the interior and the grey area denotes a fundamental region under $\mathrm{SL}_2(\mathbb{Z})$-action on the upper half plane. With $R = 1$, one gets the famous Ford circle arrangement.

Consider a function $f : \mathbb{R}^d \to \mathbb{R}$ that is the indicator function of a ball. That is

$$f(x) = \begin{cases} 1 & |x| < R \\ 0 & \text{otherwise} \end{cases},$$

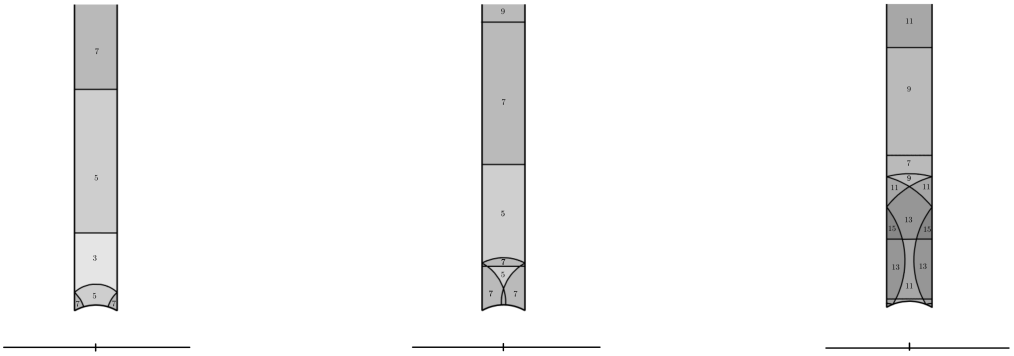
for some $R > 0$. Then, one can define a random variable valid on the probability space $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ given as follows

$$\begin{aligned} \mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z}) &\to \mathbb{R} \\ g &\mapsto \sum_{v \in \mathbb{Z}^d} f(gv). \end{aligned}$$

This construction, which we will call the Siegel transform[3], was considered by Siegel. It changes a function on the Euclidean space $\mathbb{R}^d$ to a function on the space of lattices $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$. Siegel transform has connections to some very interesting problems in number theory [BG19; ACM19]. See Figure 1.4 for a visualization in the case of $d = 2$.

Then, one can state the following theorem from [Sie45] which computes the expected value of the Siegel transform among random lattices.

[3] This definition might differ slightly from the ones in literature where sometimes the Siegel transform denotes the sum over only the primitive lattice points in $g\mathbb{Z}^d$ or sometimes only over non-zero points in the lattice.



(a) Radius $R = 1.22$. (b) Radius $R = 1.45$. (c) Radius $R = 1.99$.

Figure 1.4: When taking Siegel transforms of the indicator function of an origin centered ball of radius $R > 0$ in two dimensions, the Siegel transform can be seen as a function on the upper half-plane since in this case, the Siegel transform is invariant under rotating the lattice. One can then plot the Siegel transform in a fundamental domain with respect to $\mathrm{SL}_2(\mathbb{Z})$-action. Here, we plot the Siegel transforms for three different values of R. The odd numbers indicate the values taken by the Siegel transform, or equivalently the lattice point counts for each of the corresponding regions. For simplicity, not all the regions are marked.

Theorem 1.2. *Suppose $f : \mathbb{R}^d \to \mathbb{R}$ is a compactly supported bounded measurable function. Then, the following holds.*

$$\int_{\mathrm{SL}_d(\mathbb{R})/\,\mathrm{SL}_d(\mathbb{Z})} \left(\sum_{v \in g\mathbb{Z}^d} f(v) \right) dg = f(0) + \int_{\mathbb{R}^d} f(x)dx,$$

where the dx on the right hand side is the usual Lebesgue measure on $\mathbb{R}^d$ and dg is the unique $\mathrm{SL}_d(\mathbb{R})$-invariant probability measure on $\mathrm{SL}_d(\mathbb{R})/\,\mathrm{SL}_d(\mathbb{Z})$.

With this, one can show that $c_d \geq 2$ from Table 1.1 by the following simple arguments. Suppose that $c_d = 2 - \varepsilon$ for some $\varepsilon > 0$. This means that a ball of volume $2 - \varepsilon$ at the origin will have at least one non-zero point in a unit covolume lattice. Now, note that the number of lattice points for a random lattice $g\mathbb{Z}^d$ in a ball centered at the origin is always an odd number. Indeed, the non-zero points come in pairs due to ± 1 symmetries. Now, Theorem 1.2 tells us that the ball should have $3 - \varepsilon$ lattice points on average. Hence, at least one of those random lattices has a Siegel transform equal to 1. This contradicts that $c_d = 2 - \varepsilon$.

1.3 Lattices with additional symmetries

The preceding argument about ± 1 symmetries is what has been leveraged so far to create improvements given in Table 1.1.

In the table, the result due to Venkatesh [Ven13] is the best known lower bound asymptotically. From Mertens' theorem, we know that $\frac{n}{\varphi(n)}$ can be as big as $O(\log\log n) = O(\log\log d)$. This happens for the subsequence of dimensions $d = 2\varphi(k)$ where $k = p_1 p_2 \dots p_k$ where $\{p_1, p_2, \dots\}$ are prime numbers indexed increasingly. Hence, along a sequence of dimensions, the lower bound due to Venkatesh is better than any linear bound and has a growth of $O(d \log\log d)$.

Let us sketch how the result follows. Let $K = \mathbb{Q}(\mu_n)$ be a cyclotomic number field and let $\langle \mu_n \rangle$ be the finite group of torsional units in $\mathcal{O}_K^*$. Consider $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$. The moduli space of $\mathcal{O}_K$-lattices of a fixed (and finite) covolume in $K_{\mathbb{R}}^{\oplus t}$ is then denoted by $\mathrm{SL}_t(K_{\mathbb{R}})/\,\mathrm{SL}_t(\mathcal{O}_K)$ (although $t = 2$ works for obtaining the bound). It turns out that we can prove Siegel's mean value theorem, Theorem 1.2, for the number field K.

Theorem 1.3. *[Ven13]*

Let $d = 2\varphi(n)$ and $K = \mathbb{Q}(\mu_n)$. Suppose $f : K_{\mathbb{R}}^2 \to \mathbb{R}$ is a compactly supported bounded measurable function. Then the following holds.

$$\int_{\mathrm{SL}_2(K_{\mathbb{R}})/\mathrm{SL}_2(\mathcal{O}_K)} \left(\sum_{v \in g\mathcal{O}_K^{\oplus 2} \setminus \{0\}} f(v) \right) dg = \int_{\mathbb{R}^d} f(x)dx,$$

where the dx on the right hand side is that Lebesgue measure on $\mathbb{R}^d$ that makes $\mathcal{O}_K^{\oplus 2} \subseteq K_{\mathbb{R}}^2 \simeq \mathbb{R}^d$ of unit covolume and dg is the unique $\mathrm{SL}_2(K_{\mathbb{R}})$-invariant probability measure on $\mathrm{SL}_2(K_{\mathbb{R}})/\mathrm{SL}_2(\mathcal{O}_d)$.

Now if f is the indicator function of a ball whose volume is $n - \varepsilon$ and is invariant under these cyclic symmetries (such a ball exists due to "averaging"), there must exist one $g \in \mathrm{SL}_2(\mathcal{O}_K)$ such that $\sum_{v \in g\mathcal{O}_K^{\oplus 2} \setminus \{0\}} f(v) = 0$. This $g\mathcal{O}_K^{\oplus 2}$ is the lattice that we desire.

The main tool that seemed to help get the $O(n \log\log n)$ lower bound on c_n was the exploitation of a large group of symmetries acting on each lattice point in the lattices inside the homogeneous space $\mathrm{SL}_2(K_{\mathbb{R}})/\mathrm{SL}_2(\mathcal{O}_K)$. This leads to the natural question, can one increase the group of symmetries from a cyclic group to an arbitrary finite group and does it lead to any improvements on sphere packing densities?

This is the main research question motivating the thesis. Using tools from representation theory and number theory, it is possible to define spaces of lattices invariant under a finite group G and also describe analogues of Theorem 1.3 for such spaces of lattices. This is covered in Chapter 5.

In the paper [Gar23], I explored this scenario to get the following generalisation of [Ven13].

Theorem 1.4. *[Gar23]*
Let D be a finite-dimensional division algebra over $\mathbb{Q}$. Let $\mathcal{O} \subseteq D$ be an order and $G_0 \subseteq \mathcal{O}$ be a finite group embedded in the multiplicative group of D. Then with $d = 2\dim_{\mathbb{Q}} D$, we have

$$c_d \geq \#G_0.$$

Since a number field is also a division algebra over $\mathbb{Q}$, we recover the result of Venkatesh by setting $D = \mathbb{Q}(\mu_n)$, the nth cyclotomic field, $\mathcal{O}$ to be the ring of integers in $\mathbb{Q}(\mu_n)$ and the nth cyclotomic field and $G_0 = \langle \mu_n \rangle$. Hence, Venkatesh's construction can be recovered from this theorem.

However, because of the additional freedom that the division rings give us, we can adjust our parameters and go slightly beyond some of the lower bounds provided in [Ven13]. Additional points that this theorem can provide have resulted in improvements on the best packing densities in less than astronomical number of dimensions. For example, one of the sequences that can be produced using this theorem has the following comparison.

Theorem 1.5. *[Gar23]*
There exists a sequence of dimensions $\{d_i\}_{i=1}^{\infty}$ such that we have $c_{d_i} \geq 3d_i(\log\log d_i)^{\frac{7}{24}}$ and the lattices that achieve this bound in each dimension are symmetric under the linear action of a non-commutative finite group.

Figure 1.5 compares the novel sequence with the older sequence.

1.4 What about other groups of symmetries?

Since all the finite subgroups of division algebras over $\mathbb{Q}$ are completely classified [Ami55], it is possible to exhaust all options for this setup and it could be concluded that by just using these groups, it is impossible to go beyond an $O(n \log\log n)$ improvement on the lower bounds available on c_t. So, this is all that could be done with finite groups embedded in division algebras using these techniques.

To use groups other than finite subgroups of division algebras, one would need integration formulas similar to Theorem 1.3. This is a goal that has been achieved, as much as it seemed possible, in this doctoral thesis. The details are in Chapter 5, but the results are briefly written below.

Let G be a finite group with a $\mathbb{Q}$-representation $V = V_{\mathbb{Q}}$. Suppose V admits the following decomposition as $\mathbb{Q}[G]$-modules

$$V = V_1^{\oplus t_1} \oplus V_2^{\oplus t_2} \oplus \cdots \oplus V_k^{\oplus t_k}, \tag{1.2}$$

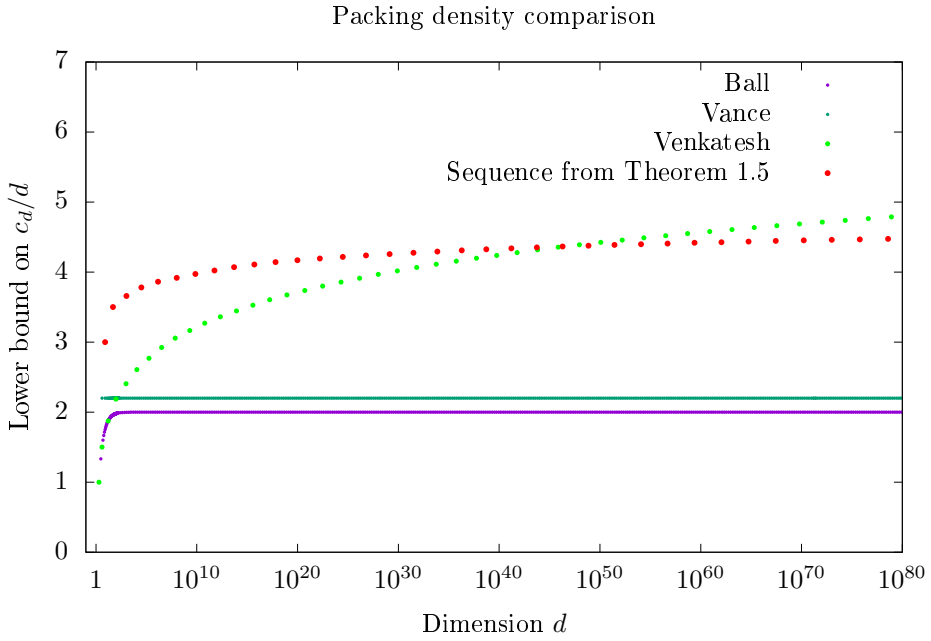


Figure 1.5: The sequence of Venkatesh is better after $d \sim 1.98 \times 10^{46}$ than the sequence obtained from Theorem 1.5 and outperforms any linear bound on c_d since it grows at $O(d(\log\log d)^{\frac{7}{24}})$.

where each V_i is an irreducible $\mathbb{Q}[G]$-representation. Then, for each V_i, there exists a division algebra $D_i = \mathrm{End}_{\mathbb{Q}[G]} V_i$, the ring of G-linear endomorphisms of V_i. This D_i acts on V_i to make $V_i \simeq D_i^{n_i}$ for some index n_i which we call the matrix index of V_i.

Then, starting with a G-invariant lattice $\Lambda \subseteq V \otimes \mathbb{R}$ (there must exist at least one), we can identify $\mathcal{G}(\mathbb{R})/\Gamma$ as a collection of G-invariant lattices where

$$\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_{t_1}(D_1) \oplus \cdots \oplus \mathrm{SL}_{t_k}(D_k),$$
$$\Gamma = \{g \in \mathcal{G}(\mathbb{Q}) \mid g\Lambda = \Lambda\}.$$

Then, due to a theorem of Borel and Harish-Chandra (or otherwise, using the reduction theory in Chapter 4), we find out that the space $\mathcal{G}(\mathbb{R})/\Gamma$ can be endowed a probability measure. And thus, we can state the following theorem.

Theorem 1.6. *Suppose $V_{\mathbb{Q}}$ be a $\mathbb{Q}[G]$-representation whose decomposition into irreducibles is given by Equation (1.2). Furthermore, suppose that for each V_i, the matrix index n_i and the number of copies t_i satisfies $n_i < t_i$.*

Then, we have that the expected value of the Siegel transform is finite on $\mathcal{G}(\mathbb{R})/\Gamma$ and equals

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v \in g\Lambda} f(v) \right) dg = \sum_{(W_1,\ldots,W_k) \in \mathcal{L}_1 \times \cdots \times \mathcal{L}_k} \frac{1}{H(W_1^{\perp}) \ldots H(W_k^{\perp})} \int_{(W_1^{\perp})_{\mathbb{R}} \times \cdots \times (W_k^{\perp})_{\mathbb{R}}} f(w) dw,$$

where

$$\mathcal{L}_i = \{W \subseteq D_i^{n_i} \mid W \text{ is a right } D\text{-module}\}$$

and for each $W_i \in \mathcal{L}_i$, $H(W_i^{\perp})$ is the height of $W_i^{\perp}$, a positive real number associated to W_i defined in Definition 5.11 and Theorem 5.12.

Here, the measure on $\mathcal{G}(\mathbb{R})/\Gamma$ is the unique left-$\mathcal{G}(\mathbb{R})$ invariant probability measure and on the right is the restriction, on the subspaces $(W_1^{\perp})_{\mathbb{R}} \times \cdots \times (W_k^{\perp})_{\mathbb{R}}$, of the Lebesgue measure on $V_{\mathbb{R}} = V \otimes \mathbb{R}$ scaled so that $\Lambda \subseteq V_{\mathbb{R}}$ is unit covolume.

Perhaps the easiest case that is not already a finite group inside a $\mathbb{Q}$-division ring is a finite group that has a matrix index $n = 2$, that is, it can be embedded into 2×2 matrices over a division ring. Such finite subgroups are also classified completely [Ban88].

One example of such a group is the dihedral group D_{2n}. An irreducible representation of this group over $\mathbb{Q}$ is the action on the cyclotomic field $\mathbb{Q}(\mu_n)$ with $\langle \mu_n \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ and Galois conjugation $\mu_n \mapsto \mu_n^{-1}$. The division algebra $D = \mathrm{End}_{\mathbb{Q}[D_{2n}]}\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_n + \mu_n^{-1})$ is the totally real subfield inside $\mathbb{Q}(\mu_n)$ and then we can think of the action as 2×2 matrices over D acting on $\mathbb{Q}(\mu_n) \simeq D^2$.

But already the integration formulas for such situations make lattice packing results difficult. For instance, if we consider G to be such a group that can be embedded in 2×2 matrices over a $\mathbb{Q}$-division algebra such that the G-action on $V_1 = D^2$ makes V_1 an irreducible $\mathbb{Q}[G]$-representation, then taking $t \geq 3$ copies of V_1 lets us use Theorem 1.6. We state the following corollary for $t = 3$ which potentially might help us in getting a lower bound on the $6 \dim_{\mathbb{Q}} D$-dimensional lattice packing problem.

Corollary 1.7. *Define $V_{\mathbb{Q}} = V_1^{\oplus 3}$ and G, D as in the preceding discussion. Then V admits a left action of $M_3(D_{\mathrm{op}})$ that commutes with the left action of G. Fix a G-invariant lattice $\Lambda \subseteq V$, let's say by taking points in $V \simeq D^{\oplus(2\times 3)}$ lying in an order $\mathcal{O} \subseteq D$. Define the groups*

$$\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_3(D_{\mathrm{op}}), \Gamma = \{g \in \mathcal{G}(\mathbb{Q}) \mid g\Lambda = \Lambda\}.$$

Then for a ball $B \subseteq V_{\mathbb{R}} = V \otimes \mathbb{R}$ of radius R defined with respect to a quadratic form that makes $\Lambda \subseteq V_{\mathbb{R}}$ unit covolume, we have

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} (\#\, B \cap \Lambda) dg = 1 + Z(3; \mathrm{LGr}(1,2,D)) \cdot V(3d) R^{2d} + V(6d) R^{6d},$$

where $d = \dim_{\mathbb{Q}} D$, $Z(3, \mathrm{LGr}(1,2,D)) \in \mathbb{R}_{>0}$ is a constant defined in Equation (5.6) and $V(n) = \frac{\pi^{\frac{n}{2}}}{(n/2)!}$ is the volume of a Euclidean unit ball in n dimensions.

One can see that as $d = \dim_{\mathbb{Q}} D$ increases, we have one additional term in this situation other than 1 and $V(6d)R^{6d} = \mathrm{vol}(B)$ which is exponentially bigger than $\mathrm{vol}(B)$. Hence, overall the mean value of the Siegel transform is much bigger than $1 + \mathrm{vol}(B)$ and this is a major limitation in this case. Also, in the situation of the $n = 1$ case, we had a very favourable property that the Siegel transform would take values in $\{1, \#\, G + 1, 2 \cdot \#\, G + 1, \dots\}$ which could be leveraged to make probabilistic arguments and this may not be the case in this more general situation as there might be some lattice points with small G-orbits. These considerations make the $n > 1$ case difficult to analyse.

Despite this, the integration formula of Theorem 1.6 is of independent interest. One such application has been the study of higher moments of the lattice point counts of $\mathcal{O}_K$-lattices. Consider $G = \frac{\mathbb{Z}}{n\mathbb{Z}}$, the cyclic group of order n. Then the nth cyclotomic number field $K = \mathbb{Q}(\mu_n)$ is an irreducible representation of G over $\mathbb{Q}$. One can then consider $V = K^t$ as a G-representation. A very obvious choice of G-invariant lattices is then the lattice $\Lambda = \mathcal{O}_K^t \subseteq K^t$. One can also endow on $V_{\mathbb{R}} = K \otimes \mathbb{R}^t$ the following positive definite real quadratic form on $K_{\mathbb{R}}$ taken t-fold times

$$\langle x, y \rangle = \Delta_K^{-\frac{2}{[K:\mathbb{Q}]}} \mathrm{tr}(x\overline{y}), \tag{1.3}$$

where Δ_K is the discriminant of K as a number field. This choice of the quadratic form makes $\Lambda \subseteq V_{\mathbb{R}}$ of unit covolume.

If we take a function $f : V_{\mathbb{R}} \to \mathbb{R}$ that is the indicator function of a ball with respect to the norm mentioned above, then we can use the theory developed in Chapter 5 to get the following theorem.

Theorem 1.8. *Let $n < t$ and let $g : K_{\mathbb{R}}^{t\times n} \to \mathbb{R}$ be a compactly supported Riemann-integrable function defined as*

$$g(x_1, \dots, x_n) = f(x_1) f(x_2) \dots f(x_n), x_1, x_2, \dots, x_n \in K_{\mathbb{R}}^t.$$

Equip $K_{\mathbb{R}}^t$ with the measure as discussed around Equation (1.3). Then, putting the Haar probability measure on $\mathrm{SL}_t(K_{\mathbb{R}})/\mathrm{SL}_t(\mathcal{O}_{\mathrm{K}})$, we have that

$$\int_{\mathrm{SL}_t(K_{\mathbb{R}})/\mathrm{SL}_t(\mathcal{O}_{\mathrm{K}})} \left(\sum_{v \in \gamma \mathcal{O}_K^{t\times n}} g(v) \right) d\gamma = g(0) + \sum_{m=1}^{n} \sum_{\substack{D \in M_{m\times n}(K) \\ \mathrm{rank}(D) = m \\ D \text{ is row reduced echelon}}} \mathfrak{D}(D)^{-t} \int_{x \in K_{\mathbb{R}}^{t\times m}} g(xD) dx, \tag{1.4}$$

where $\mathfrak{D}(D)$ is the index of the sublattice $\{C \in M_{1\times m}(\mathcal{O}_K) \mid C \cdot D \in M_{1\times n}(\mathcal{O}_K)\}$ in $M_{1\times m}(\mathcal{O}_K)$.

This formula has recently also been shown in this more specific case by somewhat different methods by [Kim19; Hug23]. In Section 6.3, we talk about how Theorem 1.8 can be leveraged to prove that behaviour of point counts for these random $\mathcal{O}_K$-lattices partially follows the Poisson distribution. Achieving this result involved dealing with tight upper bounds on the error terms on the right side of Equation (1.4), but under a somewhat relaxed condition of $t \geq \Omega(n^3 \log\log n)$. This generalised a result of Rogers [Rog56] for the case of the full space $\mathrm{SL}_t(\mathbb{R})/\mathrm{SL}_t(\mathbb{Z})$ in an orthogonal direction and required inventing some novel ideas in the geometry of numbers to deal with infinite order units in $\mathcal{O}_K^*$.

The research on the higher moments point counts for $\mathcal{O}_K$-lattice already captures the intricacies that would potentially arise in attempts to leverage Theorem 1.6 to work for general finite groups G.

1.4.1 André Weil's generalisation of Siegel mean value theorem

Lastly, before getting into the integration formulas, it must be noted that the Siegel mean value theorem was vastly generalised by André Weil in [Wei58], almost ten years after Rogers published the higher moment formulas [Rog56]. Weil's setup works for any semisimple algebraic group acting on an affine variety. From that point of view, Rogers' results are Weil's integration formulas for the case of the group SL_d acting on $\mathbb{A}^{d\times n}$. Our work can also be put into the framework of Weil in a similar way.

However, to come from Weil's setup to these specific cases would still require identification of orbits and would still require showing that the integral formula does not diverge to infinity, as done in Chapter 5. The only thing that Weil's theory could save us with is the reduction theory in Chapter 4, but since our G-invariant lattices naturally take us to division algebras and we need to integrate over Siegel domains, it is not without value to write out explicitly these Siegel domains for the reduction theory and the integration coordinates in this division algebra case.

Chapter 2

Preliminaries

In this section, we will discuss some material that will be used in the course of the thesis. The reader who is well-versed with these topics can freely move to the next chapter.

This expository material assumes the knowledge of basic group theoretical and topological notions.

2.1 Measure on quotient spaces of arithmetic groups

2.1.1 Haar measure

Some classical facts about the Haar measure are presented below without proofs. See [Nac76] for the details.

Every locally compact Hausdorff topological group $\mathcal{G}$ admits a measure dg which satisfies the following properties.

1. For any Borel set $A \subseteq \mathcal{G}$, $\int_A dg = \int_{hA} dg$ for any $h \in \mathcal{G}$.
2. For any compact set $K \subset \mathcal{G}$, $\int_K dg < \infty$.
3. For any Borel set $A \subseteq \mathcal{G}$,
$$\int_A dg = \inf_{\substack{U \supseteq A \\ U \text{ open}}} \int_U dg.$$
4. For any open set $A \subseteq \mathcal{G}$,
$$\int_A dg = \sup_{\substack{K \subseteq A \\ K \text{ compact}}} \int_K dg.$$

The last two properties define what is called a Borel measure on any topological space. Property 1 is called the left-invariance of the measure dg. An analogous property of right-invariance can be defined. A measure satisfying all of the above properties is called a (left-invariant) Haar measure on $\mathcal{G}$. Remarkably, a Haar measure is unique up to an action of a positive scalar. Hence, any two measures satisfying the above axioms will have to be proportional to each other.

The right multiplication of $h \in \mathcal{G}$ on $\mathcal{G}$ takes a Haar measure dg to another Haar measure $R_{h*}(dg) = \Delta_{\mathcal{G}}(h)dg$, where $\Delta_{\mathcal{G}}(h) \in \mathbb{R}_{>0}$. The assignment $h \mapsto \Delta_{\mathcal{G}}(h)$ is a continuous group homomorphism from $\mathcal{G}$ to $\mathbb{R}^*$. This function $\Delta_{\mathcal{G}}$ is called the modular function of the group $\mathcal{G}$. If $\mathcal{G}$ admits a Haar measure that is both left-invariant and right-invariant, then $\Delta_{\mathcal{G}}$ shall be identically 1 on $\mathcal{G}$. Such a group is called a unimodular group.

Also, remember that a discrete group is also locally compact and Hausdorff. It has a counting measure, which is a Haar measure that is both left and right invariant. Hence, the modular function on a discrete group is always trivial.

Here is an important theorem that will come to our aid multiple times.

Theorem 2.1. *Suppose $\mathcal{G}$ is a locally compact Hausdorff topological group and $\mathcal{H} \subset \mathcal{G}$ is a closed subgroup. Then $\mathcal{H}$ is also a locally compact Hausdorff topological group. With this, the following two conditions are equivalent.*

1. *The modular function on $\Delta_{\mathcal{G}} : \mathcal{G} \to \mathbb{R}$ when restricted to $\mathcal{H}$ is equal to the modular function $\Delta_{\mathcal{H}} \to \mathbb{R}$.*

2. *The topological space $\mathcal{G}/\mathcal{H}$ can be endowed with a unique (up to multiplication) Borel measure that is invariant under the left $\mathcal{G}$-action on $\mathcal{G}/\mathcal{H}$.*

Proof. See [Nac76]. □

2.1.2 Algebraic Groups

Let us present an overview of the topic of algebraic groups. Note that the definitions here are extremely stripped down versions that do not capture the intricacies of the general theory. For in-depth understanding, the reader may refer to [Bor19; Bor12].

Definition 2.2. *A linear algebraic group is a subgroup $\mathcal{G}$ of $\mathrm{SL}_n(\mathbb{C})$ for some $n \geq 1$ that is given as a zero set of some polynomials in the matrix entries $X_{ij} : \mathrm{SL}_n(\mathbb{C}) \to \mathbb{C}$.*

We say that $\mathcal{G}$ is an algebraic k-group for a subfield $k \subseteq \mathbb{C}$ if the ideal of the vanishing polynomials that define $\mathcal{G}$ has generators in the ring $k[X_{ij}]_{1\leq i,j\leq n}$.

For a subring $R \subseteq \mathbb{C}$, we denote $\mathcal{G}(R)$ to be the set of solutions of the polynomials in $\mathrm{SL}_n(R)$. We call $\mathcal{G}(R)$ to be the R-points of $\mathcal{G}$.

Remark 2.3. *The definitions of what really an algebraic group is are a bit outside the scope of our discussions. We work with very basic definitions to outline a general theory to get the overarching picture. Eventually our interests are going to be limited to very concrete algebraic groups.*

For an in-depth discussion on these subtleties, see [Mor15, §A1].

Example 2.4. *The group $\mathrm{GL}_n(\mathbb{C})$ can be embedded in $\mathrm{SL}_{n+1}(\mathbb{C})$ as per the following map:*

$$g \mapsto \begin{bmatrix} g & 0_{n\times 1} \\ 0_{1\times n} & \det(g)^{-1} \end{bmatrix}.$$

The image can easily be described as the zero set of some polynomials. Hence, it is an example of an algebraic group. In this sense, the group $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{Z})$ hold the obvious meanings as above.

So, in this framework, whenever we write $\mathrm{GL}_n(\mathbb{C})$ as an algebraic group, we secretly mean that it is embedded in $\mathrm{SL}_{n+1}(\mathbb{C})$. In more technical terms, this gives GL_n a structure of an affine algebraic variety and this is the algebraic structure that we care about on GL_n.

Example 2.5. *Every finite group G can be seen as an algebraic group.*

Since $\mathrm{SL}_n(\mathbb{C})$ and $\mathrm{SL}_n(\mathbb{R})$ are Lie groups, and closed subgroups of Lie groups are also Lie groups (according to the classically known closed subgroup theorem, see [Kna13]). In general, this is also true for $\mathcal{G}(\mathbb{R})$ and $\mathcal{G}(\mathbb{C})$ for an algebraic group $\mathcal{G}$.

We also have a notion of algebraic morphisms.

Definition 2.6. *For algebraic groups $\mathcal{G}$ and $\mathcal{H}$, a group homomorphism $f : \mathcal{G} \to \mathcal{H}$ is a morphism of algebraic groups if the individual matrix entries of $f(X) \in \mathcal{H}$ can be expressed as functions that are $\mathbb{C}$-polynomials in the entries $(X_{ij})_{1\leq i,j\leq r}$ of X. If those polynomials can actually be allowed to have coefficients in a subring $R \subseteq \mathbb{C}$, then the morphism f will be called an R-morphism.*

An R-morphism from $\mathcal{G} \to GL_d(\mathbb{C})$ is called a d-dimensional R-representation. 1-dimensional R-representations are called R-characters.

Let us present an interesting lemma that could aid the reader in putting these concepts together.

Lemma 2.7. *Suppose $\mathcal{G}$ is an algebraic group and let there be an arbitrary $\mathbb{Q}$-character $\chi : \mathcal{G} \to \mathrm{GL}_1(\mathbb{C})$. Then $\chi(\mathcal{G}(\mathbb{Z})) \subseteq \{-1, 1\}$. Furthermore, if $\mathcal{G}(\mathbb{R})$ is connected as a Lie group, then $\chi(\mathcal{G}(\mathbb{Z})) = \{1\}$.*

Proof. Clearly, image of $\mathcal{G}(\mathbb{Z})$ under χ will be a subgroup of $\mathrm{GL}_1(\mathbb{Q})$. Now, we identify $\mathrm{GL}_1(\mathbb{Q}) = \{\left[\begin{smallmatrix} t & 0 \\ 0 & 1/t \end{smallmatrix}\right], t \in \mathbb{Q}\}$. Observe that since χ is a $\mathbb{Q}$-morphism, $t(X)$ can be expressed as a $\mathbb{Q}$-polynomial in the entries of $X \in \mathcal{G}(\mathbb{Z})$ which are integers. The coefficients of these polynomials are rational and will

have a least common denominator N and therefore $t \in \frac{1}{N}\mathbb{Z} \subset \mathbb{Q}^*$. However, the only multiplicatively closed subgroups of $\frac{1}{N}\mathbb{Z}$ are $\{-1, 1\}$ and $\{1\}$.

For the latter statement, observe that $\mathbb{Q}$-morphisms are continuous functions and therefore, take connected sets to connected sets. Hence, $\chi(G_{\mathbb{R}})$ is a connected subset of $\mathrm{GL}_1(\mathbb{R})$ and must be entirely contained in the identity component of $\mathrm{GL}_1(\mathbb{R})$. This $\chi(g) \neq -1$ for any $g \in \mathcal{G}(\mathbb{Z})$. □

The group of all $\mathbb{Q}$-characters of an algebraic group $\mathcal{G}$ is denoted as $X(\mathcal{G})$.

2.1.3 Theorem of Borel and Harish-Chandra

Observe that both $\mathrm{SL}_d(\mathbb{Z})$ and $\mathrm{SL}_d(\mathbb{R})$ are unimodular groups. For $\mathrm{SL}_d(\mathbb{Z})$, this follows since it is discrete and for $\mathrm{SL}_d(\mathbb{R})$, this is a consequence of the fact that the modular function is a homomorphism $\mathrm{SL}_d(\mathbb{R}) \to \mathbb{R}^*$ which must be trivial since $\mathrm{SL}_d(\mathbb{R})$ can be generated by commutators in the group.

The following is a classical theorem, due to Siegel [Sie45].

Theorem 2.8. *With respect to any left $\mathrm{SL}_d(\mathbb{R})$-invariant Haar measure on $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ given by Theorem 2.1, the volume of $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ is finite.*

The fact that $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ has a finite volume makes it a probability space up to rescaling of the measure appropriately. In analogy with the finiteness of the Haar measure on $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$, the question we would like to ask is the following. As we will later see, answering this question will be important while addressing the existence of random lattices.

Question 2.9. *For a given $\mathbb{Q}$-algebraic group $\mathcal{G} \subseteq \mathrm{SL}_d(\mathbb{C})$, does the quotient space $\mathcal{G}(\mathbb{R})/\mathcal{G}(\mathbb{Z})$ admit a finite left $\mathcal{G}(\mathbb{R})$-invariant measure?*

Here is an obstruction that must be navigated while attempting this question.

Proposition 2.10. *Suppose $\chi : \mathcal{G} \to \mathrm{GL}_1(\mathbb{C})$ is a $\mathbb{Q}$-character such that $\chi|_{\mathcal{G}(\mathbb{R})} : \mathcal{G}(\mathbb{R}) \to \mathbb{R}^*$ takes non-trivial values in a neighbourhood of identity. Let $\mathcal{G}(\mathbb{R})^0 \subset \mathcal{G}(\mathbb{R})$ be the identity component of the Lie group $\mathcal{G}(\mathbb{R})$ and $\mathcal{G}(\mathbb{Z})^0 = \mathcal{G}(\mathbb{Z}) \cap \mathcal{G}(\mathbb{R})^0$. Then $\mathcal{G}(\mathbb{R})^0/\mathcal{G}(\mathbb{Z})^0$ cannot have a finite volume with respect to the Haar measure on $\mathcal{G}_0$.*

Proof. Suppose that there is a finite Haar measure μ on $\mathcal{G}(\mathbb{R})^0/\mathcal{G}(\mathbb{Z})^0$. By Lemma 2.7, we know that $\chi : \mathcal{G}(\mathbb{R})^0 \to \mathbb{R}^*$ descends to become a continuous surjective function $\chi : \mathcal{G}(\mathbb{R})^0/\mathcal{G}(\mathbb{Z})^0 \to \mathbb{R}^*$. This surjective function can be used to push a Borel measure on $\mathbb{R}^*$ by taking the measure of a Borel set $E \subset \mathbb{R}^*$ to be $\mu(\chi^{-1}(E))$. This gives us a finite measure on $\mathbb{R}^*$. However, by the left-invariance of μ, the measure induced must be left-invariant under multiplication in $\mathbb{R}^*$ (since χ is surjective). This means that the usual Haar measure on $\mathbb{R}^*$ equips it with the structure of a finite topological measure group, which is clearly false.[1] □

What Borel and Harish-Chandra proved in their 1962 work is that morally speaking, this is the only obstruction. The precise version of their statements is the following.

Theorem 2.12. *[BH62]*

Let $\mathcal{G}$ be an algebraic group defined over $\mathbb{Q}$. Then $\mathcal{G}(\mathbb{R})/\mathcal{G}(\mathbb{Z})$ has a finite invariant measure if and only if $X(\mathcal{G}^0) = \{1\}$, where $\mathcal{G}^0 \subseteq \mathcal{G}$ is the connected component of identity in the Zariski topology.

Remark 2.13. *As a subgroup of $\mathrm{SL}_{r+1}(\mathbb{C})$, the Zariski connected components and the usual connected components are the same for $\mathcal{G}$.*

[1] One can also prove the following lemma using the proof of Proposition 2.10.

Lemma 2.11. *If a connected Lie group G contains a discrete group Γ such that G/Γ has a finite Haar measure, then G must be unimodular.*

Proof. Since Γ is discrete, the modular function $\Delta_\Gamma : \Gamma \to \mathbb{R}^*$ is trivial. If Δ_G is non-trivial, it is surjective on $\mathbb{R}^*_{>0}$ and therefore $\Delta_G : G/\Gamma \to \mathbb{R}^*$ is a continuous surjective function that can be used to induce an absurd measure on $\mathbb{R}^*$. □

2.1.4 Arithmetic subgroups

Observe that Theorem 2.12 discusses the quotient space $\mathcal{G}(\mathbb{R})/\mathcal{G}(\mathbb{Z})$. The way we defined $\mathcal{G}(\mathbb{Z})$ in Definition 2.2, it depends critically on how $\mathcal{G} \subseteq \mathrm{SL}_n(\mathbb{C})$ embeds. This means that this is not an elegant formulation since we have to constantly keep track of the embedding while talking about $\mathcal{G}(\mathbb{Z})$. It is therefore more satisfying to replace $\mathcal{G}(\mathbb{Z})$ with a broader class of groups that we will call arithmetic subgroups. Here are some definitions to get us into this theory.

Definition 2.14. *For a field $k \subseteq \mathbb{C}$, we say that a $\mathbb{C}$-vector space V has a k-structure if there exists a vector space V_k over k such that $V = V_k \otimes_k \mathbb{C}$.*

The k-vector space V_k is said to be the k-structure of V.

In this thesis, we will always talk about vector spaces with an underlying $\mathbb{Q}$-structure.

Remark 2.15. *Let V be a finite-dimensional $\mathbb{C}$-vector space with a $\mathbb{Q}$-structure $V_\mathbb{Q}$. Let $v_1, \ldots, v_n$ be a $\mathbb{Q}$-basis of $V_\mathbb{Q}$. This gives us an identification*

$$\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbb{C}).$$

We can embed $\mathrm{GL}_n(\mathbb{C}) \subseteq \mathrm{SL}_{n+1}(\mathbb{C})$ like in Example 2.4. Then, the rational points $\mathrm{GL}_n(\mathbb{Q})$ naturally identify with the group

$$\mathrm{GL}(V_\mathbb{Q}) = \mathrm{GL}(V) \cap \mathrm{End}_\mathbb{Q} V_\mathbb{Q}.$$

Note that if we change the $\mathbb{Q}$-basis, the homomorphism $\mathrm{GL}(V) \to \mathrm{SL}_{n+1}(\mathbb{C})$ might change by a conjugation but as a $\mathbb{Q}$-algebraic group defined in $\mathrm{SL}_{n+1}(\mathbb{C})$, $\mathrm{GL}(V_\mathbb{Q})$ is still the same since the defining polynomials whose zero set is the $\mathbb{Q}$-group $\mathrm{GL}(V)$ are still the same. If the basis is a $\mathbb{C}$-basis of V but not a $\mathbb{Q}$-basis of $V_\mathbb{Q}$, the rational points $\mathrm{GL}(V_\mathbb{Q})$ will not be the set of points $\mathrm{GL}_n(\mathbb{Q})$.

Definition 2.16. *Let V be a finite dimensional vector space with a $\mathbb{Q}$-structure and let $\mathcal{G} \subseteq \mathrm{SL}_n(\mathbb{C})$ be an algebraic group for some $n \geq 1$.*

We say that $\mathcal{G}$ has a $\mathbb{Q}$-respresentation on V if there exists a $\mathbb{Q}$-homomorphism of algebraic groups $\pi : \mathcal{G} \to \mathrm{GL}(V)$.

We say that a $\mathbb{Q}$-representation π is faithful if it is an injective map such that $\pi(\mathcal{G})$ is itself a $\mathbb{Q}$-algebraic group and $\pi : \mathcal{G} \to \pi(\mathcal{G})$ is a $\mathbb{Q}$-isomorphism of $\mathbb{Q}$-algebraic groups.

Remark 2.17. *In the definition of what a faithful representation $\pi : \mathcal{G} \to \mathrm{GL}(V)$ is, it would have been enough to say that it is an injective $\mathbb{Q}$-morphism. It follows from [Bor12, §1.4] that $\pi(\mathcal{G})$, the image of a $\mathbb{Q}$-morphism of algebraic groups, is closed. Then, the injectivity implies that a reverse map exists, which one can show to be $\mathbb{Q}$-algebraic using that algebraic groups are smooth[2] [Bor12, §1.2]. We skip these details because it will be too far from the goals of this thesis.*

The following definition is from [Bor19, §7.11].

Definition 2.18. *A subgroup $\Gamma \subseteq \mathcal{G}(\mathbb{Q})$ is said to be an arithmetic subgroup if there exists a finite-dimensional vector space V with a $\mathbb{Q}$-structure $V_\mathbb{Q}$, a lattice $\Lambda \subseteq V_\mathbb{Q}$ of maximal $\mathbb{Z}$-rank and a faithful $\mathbb{Q}$-representation $\pi : \mathcal{G} \to \mathrm{GL}(V)$ such that Γ is commensurable with the group $\{g \in \mathcal{G}(\mathbb{Q}) \mid \pi(g)\Lambda = \Lambda\} \subseteq \mathcal{G}$.*

Remark 2.19. *The reader is advised to be a little prudent here about the lattice Λ. Although it is defined as a subset of $V_\mathbb{Q}$, what we really want is that it is a lattice in the sense that it is a discrete subgroup $\Lambda \subseteq V_\mathbb{R} = V_\mathbb{Q} \otimes_\mathbb{Q} \mathbb{R}$ with finite covolume.*

One can also clear this ambiguity by defining lattices as $\mathbb{Z}$-modules of maximal rank in a $\mathbb{Q}$-vector space.

Here, commensurable is in the sense of the following definition.

Definition 2.20. *For any group G, two subgroups $H_1, H_2 \subseteq G$ are said to be commensurable with each other if $[H_1 : H_1 \cap H_2] < \infty$ and $[H_2 : H_1 \cap H_2] < \infty$.*

[2] This is similar to how a smooth map admits a partial inverse locally around the identity, and then using the group structure it could be extended globally.

Remark 2.21. *Observe that $\mathcal{G}(\mathbb{Z})$ as defined in Definition 2.2 is naturally an arithmetic subgroup. Furthmore, $\mathrm{SL}_d(\mathbb{Z}) \subseteq \mathrm{SL}_d(\mathbb{C})$ is also an arithmetic group.*

The beauty of the above definition allows us to make elegant statements like the following proposition. Note that in the statement of the proposition, we do not make any mention of where $\mathcal{G}$ embeds into while it is defined.

Proposition 2.22. *Suppose $\mathcal{G}$ is a $\mathbb{Q}$-algebraic group. Then any two arithmetic groups Γ and Γ' are commensurable.*

Proof. Let $\mathcal{G} \subseteq \mathrm{SL}_n(\mathbb{C})$ be the embedding that defines $\mathcal{G}$ as an algebraic $\mathbb{Q}$-group. It is sufficient to show that $\mathcal{G}(\mathbb{Z})$ is commensurable with Γ since being commensurable is an equivalence relation.

Suppose that we have a faithful representation $\pi : \mathcal{G} \to GL(V)$ for a V being a vector space with a $\mathbb{Q}$-structure $V_{\mathbb{Q}}$. Let $\Lambda \subseteq V_{\mathbb{Q}}$ be a lattice of maximal $\mathbb{Z}$-rank and let Γ be commensurable with

$$\Gamma_0 = \{g \in \mathcal{G} \mid g\Lambda = \Lambda\}.$$

We will show that $\mathcal{G}(\mathbb{Z})$ is commensurable with Γ_0. Let $v_1, \ldots, v_m$ be a $\mathbb{Z}$-basis of Λ making the identification $V_{\mathbb{Q}} \simeq \mathbb{Q}^m$ and $\Lambda \simeq \mathbb{Z}^m$. Then, we can identify $\mathrm{GL}(V)$ as an algebraic subgroup of $\mathrm{SL}_{m+1}(\mathbb{C})$ as in Example 2.4 such that $\pi(g)$ acts on V by just using the top-left $m \times m$ matrix entries. The matrix entries of $\pi(g) \in \mathrm{SL}_{m+1}(\mathbb{C})$ are then some $\mathbb{Q}$-polynomials in the entries of g. Most importantly, in this identification $\pi(\Gamma_0) \subseteq \mathrm{SL}_{m+1}(\mathbb{Z})$.

Let $X_{i,j}$ be the matrix entries of $M_n(\mathbb{C})$. By doing some change of variables, we can find polynomials $Q_{p,q} \in \mathbb{Q}[X_{i,j}]_{1 \le i,j \le n}$ such that

$$Q_{p,q}(g - I_n) = (\pi(g) - I_{m+1})_{p,q}, \ \forall\ g \in \mathcal{G}$$

where $I_n \in M_n(\mathbb{C}), I_{m+1} \in M_{m+1}(\mathbb{C})$ are identity matrices and the right side above is the (p,q)th matrix coordinate of $\pi(g) - I_{m+1} \in M_{m+1}(\mathbb{C})$.

Observe that $Q_{p,q}$ have no constant terms because $\pi(I_n) = I_{m+1}$. Since all the coefficients of $Q_{p,q}$ are rational, there must exist some $N \in \mathbb{Z}_{\ge 1}$ independent of p, q such that $N \cdot Q_{p,q} \in \mathbb{Z}[X_{i,j}]_{1 \le i,j \le n}$. Because there is no constant term in $Q_{p,q}$, if $g \in \mathcal{G} \cap \mathrm{SL}_n(\mathbb{Z})$ is such that $g - I_n \equiv 0 \pmod N$, then $Q_{p,q}(g - I_n) \in \mathbb{Z}$ for all p, q which means that $\pi(g) \in \mathrm{SL}_{m+1}(\mathbb{Z})$.

In particular, this implies that the congruence subgroup $\{g \in \mathcal{G}(\mathbb{Z}) \mid g \equiv I_n \pmod N\}$ leaves the lattice Λ invariant and is therefore contained in $\mathcal{G}(\mathbb{Z}) \cap \Gamma_0$. Since the index of this congruence subgroup in $\mathcal{G}(\mathbb{Z})$ is at most $\#\,\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$, we get that it is finite index in $\mathcal{G}(\mathbb{Z})$. This implies that $\mathcal{G}(\mathbb{Z}) \cap \Gamma_0$ is finite index in $\mathcal{G}(\mathbb{Z})$.

Because $\pi^{-1} : \pi(\mathcal{G}) \to \mathrm{SL}_n(\mathbb{C})$ is also a $\mathbb{Q}$-morphism, we could interchange the roles of $\mathcal{G}(\mathbb{Z})$ and Γ_0 and conclude similarly that $\mathcal{G}(\mathbb{Z}) \cap \Gamma_0$ has finite index in Γ_0. □

With this, we can state the following version of Theorem 2.12.

Theorem 2.23. *[BH62]*

Let $\mathcal{G}$ be a $\mathbb{Q}$-algebraic group satisfying the conditions of Theorem 2.12. Then, for any arithmetic subgroup $\Gamma \subseteq \mathcal{G}(\mathbb{C})$, with respect to any left $\mathcal{G}(\mathbb{R})$-invariant Haar measure on $\mathcal{G}(\mathbb{R})/\Gamma$, the volume is finite.

Proof. (assuming Theorem 2.12) Suppose that $\mathcal{G}(\mathbb{R})/\Gamma$ has finite volume with respect to the measure mentioned in the statement. Then, for any other arithmetic group Γ', we observe that

$$[\Gamma : \Gamma \cap \Gamma']\,\mathrm{vol}\,(\mathcal{G}(\mathbb{R})/\Gamma) = [\Gamma' : \Gamma \cap \Gamma']\,\mathrm{vol}(\mathcal{G}(\mathbb{R})/\Gamma').$$

Hence, finiteness of volume with respect to all arithmetic groups follows once we have finiteness with respect to a single arithmetic group. □

2.1.5 Special linear groups

Observe firstly that Theorem 2.8 follows from Theorem 2.12. Indeed, SL_d has the structure of a $\mathbb{Q}$-algebraic group and the following claim shows that it admits no $\mathbb{Q}$-characters.

Proposition 2.24. $\mathrm{SL}_d(\mathbb{C})$ *is connected and* $X_{\mathbb{Q}}(\mathrm{SL}_d) = \{1\}$.

Proof. The part about connectedness is very well-known, so we skip it.

If $\chi : \mathrm{SL}_d \to \mathrm{GL}_1$ is a rational character, then it must be trivial on a commutator $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ for $g_1, g_2 \in \mathrm{SL}_d(\mathbb{C})$. Hence, if we show that $\mathrm{SL}_d(\mathbb{C})$ is generated by the commutators $[g_1, g_2]$, we show that there are no rational characters[3] on SL_d.

The upcoming proposition then settles the proof. □

Proposition 2.25. *For any field* k*, the group* $\mathrm{SL}_d(k)$ *can be generated by commutators within the group.*

Proof. It is sufficient to verify that the elementary matrices can be written as commutators. We leave this for the reader to verify. □

2.2 Semisimple algebra

In this section, we will talk about semisimple algebras. First let us begin with the definition of what an algebra is.

Definition 2.26. *Let* k *be a field. A* k*-algebra is a* k*-vector space such that it is also a ring. It is unital if there is unit* $1_A \in A$*. It is associative if associativity is satisfied. It is finite-dimensional if* $\dim_k A < \infty$.

Throughout this text, we will use the word k*-algebra when we actually mean a finite-dimensional associative unital* k*-algebra. Also, we always assume that* $A \neq \{0\}$.

Remark 2.27. *Whenever we have an algebra* A *over a field* k*,* $k \mapsto k \cdot 1_A$ *is an embedding of* k *into* A.

2.2.1 Division algebras

Here is a formal introduction to the main character of our story.

Definition 2.28. *A division algebra over* k *is a* k*-algebra* D *such that for every* $x \in D \setminus \{0\}$*, there is an* $x^{-1} \in D \setminus \{0\}$ *with*

$$x \cdot x^{-1} = x^{-1} \cdot x = 1_D.$$

Example 2.29. *Every field extension* K/k *is a* k*-division algebra.*

Example 2.30. *One very good example is* $\mathbb{H}$*, the ring of Hamiltonian quaternions. It is a division algebra over* $\mathbb{R}$ *(but not over* $\mathbb{C}$*). It is non-commutative.*

Over $\mathbb{R}$, the division algebras are not very interesting. Over $\mathbb{Q}$, however we have infinitely many division algebras even if we exclude all the number fields. This is the playground that interests us.

For now, we will talk about some properties of various algebras that are relevant to us. We will discuss about division algebras more specifically in the upcoming section.

2.2.2 Simple algebra

Definition 2.31. *For any ring* A *that may or may not be commutative, we denote* $M_{n_1 \times n_2}(A)$ *to be* $n_1 \times n_2$ *matrices with entries in* A*. We have the multiplication map*

$$\begin{aligned} M_{n_1 \times n_2}(A) \times M_{n_2 \times n_3}(A) &\to M_{n_1 \times n_3}(A) \\ (C, D) &\mapsto \left((i,j) \mapsto \sum_{r=1}^{n_2} C_{ir} D_{rj} \right). \end{aligned}$$

The algebra $M_n(A) = M_{n \times n}(A)$ *is called a matrix algebra over* A *and* n *will be called the matrix index of this matrix algebra.*

[3] In fact, this will show that there are no homomorphisms $\mathrm{SL}_d(\mathbb{C}) \to A$ for an abelian group A that are non-trivial.

Remark 2.32. *Given a k-algebra A, we will often abuse notations and write A^n when we actually mean $M_{n\times 1}(A)$ on which $M_n(A)$ can multiply on the left.*

We are going to be interested in matrix algebras over division rings in our work. There is a very "simple" property for such rings.

Definition 2.33. *A ring R is called simple if it has no two sided ideals other than 0 and R. That is, for any $x \in R \setminus \{0\}$, we get $RxR = R$.*

Let us write a very brief proof that indeed we have the property we defined above.

Lemma 2.34. *Suppose D is a k-division ring. Then $M_n(D)$ is a simple k-algebra.*

Proof. Let $x \in M_n(D) \setminus \{0\}$. Since division is allowed, we can multiply elementary matrices on the left and right of x to get a reduced form that has only $\{0, 1\}$ on the diagonal and zeroes elsewhere. By multiplying diagonal matrices with $\{0, 1\}$-entries, we can reach a diagonal matrix whose only non-zero entry is a 1 on the diagonal somewhere. Finally by using permutation matrices and taking linear combinations, we can reach the identity matrix. This completes the proof. □

The following is a well-known theorem which says that $M_n(D)$ is the only possible example of a simple k-algebra. One can find proofs and more information in [Ser77] and [Pie12].

Theorem 2.35. *(Artin-Wedderburn)*
Suppose A is a simple algebra over a field k. Then for some k-division algebras D and some $n \geq 1$,

$$A \simeq M_n(D).$$

2.2.3 Central simple algebra

Definition 2.36. *Let A be a k-algebra and by $\mathcal{Z}(A) \subseteq A$, we denote the centre of A which is defined to be the subring*

$$\mathcal{Z}(A) = \{x \in A \mid xy = yx,\ \forall y \in A\}.$$

Lemma 2.37. *The centre of a simple algebra is always a field.*

Proof. It is sufficient to see that the centre of $M_n(D)$, where D is a division algebra, is simply the set of scalar matrices with entries in $\mathcal{Z}(D)$. Since $\mathcal{Z}(D)$ is always a field, we are done. □

Definition 2.38. *We say that a k-algebra is central if $\mathcal{Z}(A) = k$.*

Example 2.39. *Examples of central simple k-algebras are $M_n(k)$. Any simple algebra A over a field k is central simple over the field $\mathcal{Z}(A)$.*

The following is a very important result in this theory.

Theorem 2.40. *(Skolem-Noether)*
Every k-automorphism of a central simple k-algebra is an inner automorphism.
That is, whenever A is a central simple k-algebra and whenever $\varphi : A \to A$ is a k-linear automorphism, then there exists some $a \in A^*$ such that

$$\varphi(x) = a^{-1}xa,\ \forall x \in A.$$

Proof. We refer the reader to [Pie12, §12.6]. □

2.2.4 Semisimple algebra

We are interested in a slightly broader class of algebras which are defined below.

Definition 2.41. *A k-algebra is semisimple if it is a direct sum of finitely many simple algebras. That is, as k-algebras*

$$A \simeq A_1 \oplus A_2 \oplus \cdots \oplus A_n,$$

for some $A_1, \ldots, A_n$ simple k-algebras. We can call each of these factors A_i the simple factors in A.

The following is a reformulation of Theorem 2.35.

Theorem 2.42. *(Artin-Wedderburn)*
Suppose A is a semisimple algebra over a field k. Then for some finite-dimensional k-division algebras $D_1, D_2, \ldots, D_k$ and natural numbers $n_1, \ldots, n_k$, we get the isomorphism

$$A \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k). \tag{2.1}$$

If A is simple, $k = 1$.

The right side of Equation (2.1) is always semisimple for any choice of finitely many finite-dimensional k-division algebras. Thus, any reader who is not familiar with these objects could take the definition of semisimple k-algebras as the object on the right side. Furthermore, all the semisimple algebras considered here will always be finite-dimensional, so we will not explicitly mention it every time in the context of semisimple algebras.

2.2.5 Real semisimple algebras

In Theorem 2.42, we can also exploit some additional structure given by the following theorem which tells us what the division algebras are.

Theorem 2.43. *(Frobenius)*
The only finite-dimensional $\mathbb{R}$-divison algebras (up to isomorphism) are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.

The three $\mathbb{R}$-division algebras all have a special "conjugation" involution that is compatible with the canonical inclusion $\mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}$. The map $\overline{(\ )} : \mathbb{H} \to \mathbb{H}$ given as $a+ib+jc+kd \mapsto a-ib-jc-kd$ ($a, b, c, d \in \mathbb{R}$ and i, j, k canonically span $\mathbb{H}$) satisfies that for any $x, y \in \mathbb{H}$ we have $\overline{x.y} = \overline{y}.\overline{x}$. When restricted to $\mathbb{C}$, this is the usual complex conjugation and when restricted to $\mathbb{R}$, this is the identity map. Another important property is that for any $a+ib+jc+kd = x \in \mathbb{H}$, $\overline{x}x = a^2+b^2+c^2+d^2 \in \mathbb{R}_{\geq 0}$.

The two theorems stated above give rise to the following corollary.

Corollary 2.44. *Any semisimple $\mathbb{R}$-algebra is isomorphic to the product of matrix algebras over $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.*

Matrix algebras over $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ are well understood. One important property is that the conjugation map defined above can be extended to a "conjugate transpose" involution on such matrices by simply defining the mapping $[x_{ij}]^* = [\overline{x_{ji}}]$. With this, we can also define a positive definite quadratic form on these matrix algebras by sending $a \mapsto \mathrm{tr}(a^*a)$.

On a given finite-dimensional algebra over $\mathbb{R}$, it is possible to define the trace map $\mathrm{tr}_A : A \to \mathbb{R}$ and the norm map $\mathrm{N}_A : A \to \mathbb{R}$ as the trace and the determinant of the matrix of the left-multiplication operation induced by any element (the functions tr_A and N_A do not depend of the choice of the basis used to construct these left-multiplication matrices). Similarly, it is also possible to generalise the above involution simply by taking direct sums of the respective involutions for matrix rings over $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$. We will omit the subscripts in tr_A and N_A when A is clear from the context.

Corollary 2.45. *Any semisimple $\mathbb{R}$-algebra A admits an involution $(\ )^* : A \to A$ such that the following conditions are satisfied.*

- *For any $a, b \in A$, we have $(ab)^* = b^*a^*$.*
- *The form $a \mapsto \mathrm{tr}(a^*a)$ is a positive definite quadratic form on A. That is, it is always non-negative and is zero only when $a = 0$.*

Proof. Simply take the direct sum of the "conjugate transpose" operation defined above on each matrix component of the semisimple algebra A. It is then to be seen that the trace function on A is a sum of traces on the right side of Equation (2.1), when they are realised as real matrix algebras. For instance, we must see $M_1(\mathbb{C})$ as a 2-dimensional matrix algebra under the mapping $a + ib \mapsto \left[\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right]$.

Let $a \in A \simeq \bigoplus_i M_{n_i}(D_i)$, where D_i are division $\mathbb{R}$-algebras. Let $L_a : A \to A$ be the left multiplication map of a for an algebra A. Then $L_a = \bigoplus_i L_{a_i}$ where $a_i \in M_{n_i}(D_i)$ and $\mathrm{tr}_A(a) = \sum_i \mathrm{tr}_{M_{n_i}(D_i)}(a_i)$. Hence, with the definition of $a \mapsto a^*$ as defined above, we get $\mathrm{tr}_A(a^*a) = \sum_i \mathrm{tr}_{M_{n_i}(D_i)}(a_i^* a_i) \geq 0$. □

Definition 2.46. *Any involution $A \to A$ satisfying the two properties of Corollary 2.45 is said to be a positive involution on A.*

Lemma 2.47. *Suppose $(\ )^* : A \to A$ is a positive involution. Then*

- $1_A^* = 1_A$.
- *If $u \in A$ is a zero non-divisor*[4]*, then $(u^*)^{-1} = (u^{-1})^*$.*
- *For $u \in A$, $\mathrm{tr}(u) = \mathrm{tr}(u^*)$.*
- *The inner product induced by the positive definite quadratic form $x \mapsto \mathrm{tr}(x^*x)$ is $\langle x, y\rangle = \mathrm{tr}(x^*y)$.*

Proof. The proofs are very enjoyable, so we leave all of them for the reader except for the third one, which is below.

For the third part, we must use the fact that in a semisimple $\mathbb{R}$-algebra, the trace induced by the left-multiplication map and the right-multiplication map are the same[5]. To see this, it is sufficient to verify this on the three types of simple components of the semisimple $\mathbb{R}$-algebra, because the trace map is just the sum of those individual trace maps as we saw in the Corollary 2.45. For such a simple $\mathbb{R}$-algebra, this fact is related to the observation that trace of a matrix is equal to trace of the transpose for a real matrix.

Now observe that right-multiplication by u^* is the same as left-multiplication by u preceded and succeeded by the anti-homomorphism $(\ )^*$. Hence, the right-multiplication by u^* is the left-multiplication by u operation up to conjugation by $(\ )^*$ operation. Since trace is invariant under conjugation by the linear map $(\ )^*$, the trace of the two maps are equal from the claim in the previous paragraph.

□

The notions of symmetric and positive definiteness can also be defined for $(A, (\ )^*)$.

Definition 2.48. *Given a finite-dimensional semisimple $\mathbb{R}$-algebra and an involution $(\ )^*$ as mentioned in Corollary 2.45, we shall call an element $a \in A$*

- *Symmetric, if $a^* = a$.*
- *Positive definite, if $x \mapsto \mathrm{tr}(x^*ax)$ is a positive definite quadratic form on A.*

Lemma 2.49. *The following holds.*

- *For any unit $a \in A$, a^*a is always symmetric and positive definite.*
- *If $a \in A$ is positive definite, then a is a zero non-divisor and $\mathrm{tr}(a) > 0$.*

Proof. The first is a trivial verification.

For the second, note that if a is a zero divisor then there exists some non-zero $x \in A$ such that $ax = 0 \Rightarrow \mathrm{tr}(x^*ax) = 0$ which contradicts the positive definiteness of a. Finally $\mathrm{tr}(a) = \mathrm{tr}(1_A^* a 1_A) > 0$. □

[4] In a finite-dimensional algebra over a field k, being a zero non-divisor is equivalent to being a unit and is also equivalent to the left/right multiplication map being full-rank.

[5] Caution: This is only valid for semisimple algebras. In general, it is not true that the left-trace and the right-trace agree.

Remark 2.50. *Another notion of positive definiteness and symmetry that comes to mind is the following. For any $a \in A$, you could call it positive definite if the left-multiplication matrix with respect to a basis of A is positive definite and symmetric if it is symmetric. This notion is actually compatible with the current notion, but is much less elegant.*

The above notions give us an opportunity to describe the following folklore lemma. It is often called the "norm-trace" inequality.

Lemma 2.51. *Consider a f.d. semisimple $\mathbb{R}$-algebra A with a positive involution $(\ )^*$. Let $a \in A$ be a symmetric positive definite element and let $d = \dim_{\mathbb{R}} A$. Then $\mathrm{N}(a) > 0$, $\mathrm{tr}(a) > 0$ and*

$$\frac{1}{d}\mathrm{tr}(a) \geq \mathrm{N}(a)^{\frac{1}{d}}.$$

Proof. This is just the arithmetic-geometric means inequality. Let us elaborate how.

We know that $x \mapsto \mathrm{tr}(x^*y)$ is an inner product on A. With respect to this, construct an orthonormal basis $e_1, e_2, \ldots, e_d$. Set $a_{ij} = \mathrm{tr}(e_i^* a e_j)$ which are the matrix entries of left-multiplication by a with respect to the basis $\{e_i\}_{i=1}^d$, i.e. for $\{r_i\}_{i=1}^d \subseteq \mathbb{R}^d$, $a(\sum_i r_i e_i) = \sum_i (\sum_j a_{ij} r_j) e_i$. Since a is symmetric, we get that $a_{ij} = a_{ji}$. Furthermore, by the positive definiteness of $x \mapsto \mathrm{tr}(x^*ax)$, the matrix a_{ij} can be seen to be positive definite as a real matrix by substituting $x = \sum_{i=1}^d x_i e_i$.

Hence, using the spectral theorem for real positive definite symmetric matrices, a_{ij} is diagonalisable matrix with respect to an orthonormal change of basis and has real and positive eigenvalues (i.e. the diagonal entries). Then trace is the sum of those eigenvalues and the norm is the product. The inequality is then exactly the arithmetic-geometric inequality on those eigenvalues. □

The following is a technical lemma that we will need eventually. The reader may skip this lemma and refer to it later when it is needed while proving Theorem 4.13.

Lemma 2.52. *For the setting of Lemma 2.51, let c be a positive constant and let K be the set of all symmetric positive definite $a \in A$ such that*

$$\mathrm{N}(a)^{\frac{1}{d}} \leq \frac{1}{d}\mathrm{tr}(a) \leq c\,\mathrm{N}(a)^{\frac{1}{d}}.$$

Then the following set is relatively compact in A (with respect to the Euclidean topology as an $\mathbb{R}$-vector space).

$$\left\{ \frac{a}{\mathrm{tr}(a)} \mid a \in K \right\}.$$

Proof. What we will show is that there exist constants $c_1', c_2' > 0$ depending only on c such that for any $x \in A$,

$$c_1' \leq \frac{\mathrm{tr}\left(x^*\left(\frac{a}{\mathrm{tr}(a)}\right)x\right)}{\mathrm{tr}(x^*x)} \leq c_2'.$$

This will imply our claim, since in general, the set of symmetric positive definite matrices $A \in M_d(\mathbb{R})$ that satisfy

$$c_1' \leq \frac{\mathrm{tr}(x^T A x)}{\mathrm{tr}(x^T x)} \leq c_2', \forall\ x \in \mathbb{R}^n \setminus \{0\}$$

is relatively compact in $M_d(\mathbb{R})$, where $d = \dim_{\mathbb{R}} A$. Indeed, this condition is just enforcing that all the eigenvalues of A must be in the compact set $[c_1', c_2']$.

The statement is really about eigenvalues, as we will see. Using the spectral theorem, we know that there exists a basis $\{e_i\}_{i=1}^d$ of A such that e_i are orthonormal with respect to $x \mapsto \mathrm{tr}(x^*x)$ and the matrix $\mathrm{tr}(e_i^* a e_j)$ is a diagonal matrix. Let $\{\lambda_i\}_{i=1}^d$ be those diagonal entries with the assumption that

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d.$$

Then, we have that if $x = \sum_{i=1}^{d} x_i e_i$, then $\operatorname{tr}(x^*x) = \sum_{i=1}^{d} x_i^2$ and $\operatorname{tr}(x^*ax) = \sum_{i=1} \lambda_i x_i^2$. On the other hand, $\mathrm{N}(a) = \prod_{i=1}^{d} \lambda_i$ and $\operatorname{tr}(a) = \sum_{i=1}^{d} \lambda_i$.

From the assumption, we already know that

$$\frac{1}{d}\sum_{i=1}^{d} \lambda_i \leq c\lambda_1^{\frac{1}{d}}\lambda_2^{\frac{1}{d}} \dots \lambda_d^{\frac{1}{d}} \leq c\lambda_1^{\frac{1}{d}}\lambda_d^{\frac{1}{d}}\lambda_d^{\frac{1}{d}} \dots \lambda_d^{\frac{1}{d}} = c\lambda_d \left(\frac{\lambda_1}{\lambda_d}\right)^{\frac{1}{d}}.$$

Division on both sides by $c\lambda_d$ tells us that

$$\frac{1}{cd} \leq \frac{1}{cd}\left(\sum_{i=1}^{d-1} \frac{\lambda_i}{\lambda_d} + 1\right) \leq \left(\frac{\lambda_1}{\lambda_d}\right)^{\frac{1}{d}},$$

and consequently that $\lambda_d \leq (cd)^d \lambda_1$. Let $c' = c^d d^{d+1}$, then

$$\lambda_1 \leq \operatorname{tr}(a) = \sum_{i=1}^{d} \lambda_i \leq d\lambda_d \leq c'\lambda_1.$$

This tells us that the trace is roughly proportional to the smallest eigenvalue. From this, we learn that

$$\operatorname{tr}(x^*x) = \sum_{i=1}^{d} x_i^2 = \frac{1}{\lambda_1}\sum_{i=1}^{d} \lambda_1 x_i^2 \leq \frac{1}{\lambda_1}\sum_{i=1}^{d} \lambda_i x_i^2 = \frac{1}{\lambda_1}\operatorname{tr}(x^*ax) \leq c'\frac{\operatorname{tr}(x^*ax)}{\operatorname{tr}(a)},$$

whereas

$$\operatorname{tr}(x^*x) \geq \frac{1}{\lambda_d}\sum_{i=1}^{d} \lambda_i x_i^2 = \frac{1}{\lambda_d}\operatorname{tr}(x^*ax) \geq \frac{d}{c'}\frac{1}{\lambda_1}\operatorname{tr}(x^*ax) \geq \left(\frac{d}{c'}\right)\frac{\operatorname{tr}(x^*ax)}{\operatorname{tr}(a)}.$$

This is what was needed. □

Remark 2.53. *Note that* $\{a/\operatorname{tr}(A) \mid a \in K\} \subseteq \{a \in A \mid \operatorname{tr}(a) = 1\}$.

The relatively compact set $\{a/\operatorname{tr}(a) \mid a \in K\}$ *can be made to lie in* A^**, the open set of invertible elements in* A*. In particular, this means that the norm of these elements is bounded away from* 0*, since* $A^* = \{a \in A \mid \mathrm{N}(a) \neq 0\}$.

Corollary 2.54. *For the setting of Lemma 2.51, let* c *be a positive constant and let* K *be the set of all symmetric positive definite* $a \in A$ *such that*

$$\mathrm{N}(a)^{\frac{1}{d}} \leq \frac{1}{d}\operatorname{tr}(a) \leq c\,\mathrm{N}(a)^{\frac{1}{d}}.$$

Then the following holds for some constants $C_1, C_2 > 0$.

$$C_1 \operatorname{tr}(x^*x)\operatorname{tr}(a) \leq \operatorname{tr}(x^*ax) \leq C_2 \operatorname{tr}(x^*x)\operatorname{tr}(a).$$

2.2.6 Orders in semisimple rings

Definition 2.55. *Let* $A_{\mathbb{Q}}$ *be a* $\mathbb{Q}$*-algebra. Then an additive subgroup* $\mathcal{O} \subseteq A_{\mathbb{Q}}$ *is called an order of* $A_{\mathbb{Q}}$ *if the following properties hold.*

- *It is a finitely generated abelian group.*
- *It is discretely embedded in* $A_{\mathbb{R}} = A \otimes_{\mathbb{Q}} \mathbb{R}$ *under the Euclidean topology.*
- *It is closed under multiplication, that is* $a, b \in \mathcal{O} \Rightarrow ab \in \mathcal{O}$.
- $1_A \in \mathcal{O}$.
- *The* $\mathbb{Q}$*-span of all the points in* $\mathcal{O}$ *is* A*. This is equivalent to saying that* $\mathcal{O}$ *is not contained in any proper vector subspace of* A*. In particular, we have* $\operatorname{rank}_{\mathbb{Z}} \mathcal{O} = \dim_{\mathbb{Q}} A$.

Remark 2.56. *The definition of what an order is varies through literature. Sometimes the condition $1_A \in \mathcal{O}$ is denoted in a more specific type of order called a unital order.*

Example 2.57. *$\mathbb{Z} \subset \mathbb{Q}$ is an order.*

Example 2.58. *If K is a number field, then $K \otimes_{\mathbb{Q}} \mathbb{R}$ is a semisimple algebra in which $\mathcal{O}_K$, the ring of integers in K is an order.*

When $\mathcal{O} \subseteq A$ is an order, $M_k(\mathcal{O})$ is an order within $M_k(A)$. We can refer to $\mathcal{O}$ as the "integral points of A" and elements of $M_k(\mathcal{O})$ as "integral matrices" in $M_k(A)$.

Remark 2.59. *This notion of "integral matrices" can be reconciled with common sense in the following way. Since $\mathcal{O}$ spans A, we can make a basis of A from elements of $\mathcal{O}$. Extending this basis to a basis of A^k, we can recognize the algebra $M_k(A)$ as an algebra of real matrices acting on A^k. Under this identification, the elements of $M_k(\mathcal{O})$ are exactly those elements of $M_k(A)$ whose entries as real matrices are integers.*

Making this more precise, denote $d = \dim_{\mathbb{Q}} A$. Then there exists a faithful $\mathbb{Q}$-algebra morphism $\pi : M_k(A) \to M_{kd}(\mathbb{Q})$ that maps $M_k(\mathcal{O})$ inside $M_{kd}(\mathbb{Z})$. In fact, we see that $M_k(\mathcal{O}) = \pi^{-1}(M_{kd}(\mathbb{Z}))$ because if $\pi(m) \in M_{kd}(\mathbb{Z})$, $me_i \in \mathcal{O}^k$ when $e_i = (0, \ldots, 0, 1_A, 0, \ldots, 0) \in \mathcal{O}^k$. We will exploit this representation π a few times throughout the text.

Lemma 2.60. *Let $\mathcal{O} \subseteq A$ be an order inside a semisimple algebra. Then $m \in M_k(\mathcal{O}) \Rightarrow \mathrm{N}(m), \mathrm{tr}(m) \in \mathbb{Z}$.*

Proof. Identify $\mathrm{End}_{\mathbb{R}}(M_k(A)) \simeq M_{[A:\mathbb{R}]k^2}(\mathbb{R})$ with respect to a basis $M_k(A)$ made by using a $\mathbb{Z}$-basis of $\mathcal{O} \subset A$ written k^2 times (once for each matrix element of $M_k(A)$).

With this, $M_k(\mathcal{O})$ is the $\mathbb{Z}$-span of this basis and hence integral matrices have integer entries under the left-multiplication map. Hence, norm and trace are integers. □

Corollary 2.61. *If $m \in M_k(A)$ and π is the representation from Remark 2.59, then $\mathrm{N}_{M_k(A)}(m) = [\det \pi(m)]^k$ and $\mathrm{tr}_{M_k(A)}(m) = k \,\mathrm{trace}(\pi(m))$.*

Proof. To get this, we must identify $M_k(A) \simeq (A^k)^{\oplus k}$ as a left $M_k(A)$-module and use the basis mentioned in Remark 2.59. □

2.3 More on division rings

2.3.1 Linear algebra with division rings

Proposition 2.62. *Finitely generated left division ring modules are vector spaces over the division ring.*

Proof. We skip this proof as it is boring. Basically, all linear algebra of vector spaces of fields generalises to division rings as long as we keep track of left multiplication and right multiplication. □

Here is a matrix decomposition lemma that will be useful for us.

Lemma 2.63. *For any $\omega \in M_{n_1 \times n_2}(D)$, we can uniquely write*

$$\omega = c \cdot f, \tag{2.2}$$

where $c \in M_{n_1 \times m}(D)$ and $f \in M_{m \times n_2}(D)$ such that

1. *m is the D-rank of right D-module in $M_{n_1 \times 1}(D)$ generated by the columns of ω.*
2. *f is in column reduced echelon form. This means that for each column in the matrix*
   (a) *the top-most entry is 1,*
   (b) *this top-most entry is in a row strictly below that of any row which contains the top-most entry of a column to the left of the column,*

(c) the row containing the top-most entry has zeroes at all the positions except where there is a 1.

Proof. This is exactly like the rank-factorization in standard linear algebra. Here are the details.

Let $\omega_1, \omega_2, \ldots, \omega_{n_2} \in M_{n_1 \times 1}(D)$ be the columns of the matrix ω. Suppose that

$$\begin{aligned} V_1 &= \omega_1 \cdot D, \\ V_2 &= \omega_1 \cdot D + \omega_2 \cdot D, \\ V_3 &= \omega_1 \cdot D + \omega_2 \cdot D + \omega_3 \cdot D, \\ &\vdots \end{aligned}$$

Then, we have that for each $i \in \{1, \ldots, n\}$, the difference of the right D-ranks of V_i and V_{i-1} is either 0 or 1. This depends exactly on whether or not ω_i can be written as a right-D linear combination of $\omega_1, \omega_2, \ldots, \omega_{i-1}$ or not.

Let I be the set of indices i such that ω_i cannot be written as a linear combination of the $\omega_1, \ldots, \omega_{i-1}$. Then, clearly $\#I = m$ and the right D-span of $\{\omega_i\}_{i \in I}$ is also the right D-span of $\{\omega_i\}_{i=1,\ldots,n}$. Then, $c \in M_{n_1 \times m}(D)$ is the matrix made from the columns $\{\omega_i\}_{i \in I}$ arranged left to right with increasing i and $f \in M_{m \times n_2}(D)$ is the matrix whose ith row contains appropriate coefficients to satisfy Equation (2.2).

The uniqueness follows from the column-reduced echelon form of f, which implies that the columns of c must be of the form outlined above. □

2.3.2 Division rings in finite group representations

Let G be a finite group as before and let $\mathbb{Q}[G]$ be the group ring of G. For the uninitiated, we define a group ring below.

Definition 2.64. *For a group G and a field k, the group ring $k[G]$ is the ring of functions*

$$k[G] = \{f : G \to k\},$$

under the convolution product defined as

$$f_1 \cdot f_2(g) = \sum_{g_1 g_2 = g} f_1(g_1) f_2(g_2), \quad \forall\ f_1, f_2 \in k[G].$$

Any n-dimensional G representation over $\mathbb{Q}$ could be seen as a group homomorphism $G \to \mathrm{GL}_n(\mathbb{Q})$ which extends to a linear map $\mathbb{Q}[G] \to M_n(\mathbb{Q})$. This makes the representation a module over $\mathbb{Q}[G]$. Therefore, in the literature, $\mathbb{Q}[G]$-modules or $\mathbb{Q}[G]$-representations actually mean just representations of G over $\mathbb{Q}$. The notation allows us to talk about $\mathbb{Q}$-vector spaces without identifying a basis. We will henceforth use this terminology for representations of G over $\mathbb{Q}$.

Definition 2.65. *For a $\mathbb{Q}[G]$-representation W, we denote $\mathrm{End}_{\mathbb{Q}[G]} W$ to be the endomorphisms of W that commute with the G-action on W.*

In general, for a left R-module V where R is a ring, we denote $\mathrm{End}_R V$ to be the ring of R-linear endomorphisms of V.

Definition 2.66. *A $\mathbb{Q}[G]$-module V is said to be irreducible if there are no $\mathbb{Q}[G]$-submodules $W \subseteq V$, $W \neq 0, V$.*

The following proposal clarifies why division algebras are such a central object of study in this research.

Proposition 2.67. *Let W be an irreducible $\mathbb{Q}[G]$-module. Then, the ring $\mathrm{End}_{\mathbb{Q}[G]} W$ is an associative division ring which is non-commutative in general.*

Proof. $\mathrm{End}_{\mathbb{Q}[G]} W$ is clearly associative. We need to show that every non-zero element has an inverse. Let $a \in \mathrm{End}_{\mathbb{Q}[G]} W$. Then $\ker a$ is a $\mathbb{Q}[G]$-submodule of W. By irreducibility, we must have that $\ker a$ is either W or 0. This happens exactly when a is zero or an invertible linear map. It then follows that the inverse must also lie in $\mathrm{End}_{\mathbb{Q}[G]} W$, since $a \,\mathrm{End}_{\mathbb{Q}[G]} W = \mathrm{End}_{\mathbb{Q}} W$. □

Theorem 2.68. *Any finite dimensional $\mathbb{Q}[G]$-module $V_\mathbb{Q}$ has a decomposition of the form*

$$V_\mathbb{Q} \simeq (V_1)_\mathbb{Q}^{\oplus r_1} \oplus \cdots \oplus (V_k)_\mathbb{Q}^{\oplus r_k}, \tag{2.3}$$

where $(V_i)_\mathbb{Q}$ are irreducible $\mathbb{Q}[G]$-modules and V_i is not isomorphic to V_j for $i \neq j$.

Proof. This classical theorem is due to Maschke. The idea is basically that in characteristic 0 (or more generally when $\#G$ is invertible in the base field), we are allowed to average over the group G. □

The decomposition of Equation (2.3) is not unique. However, decomposition into the bigger (albeit, not necessarily irreducible) blocks $(V_i)_\mathbb{Q}^{r_i}$ exists canonically [cf. Ser77]. In fact, the following proposition shows that a large class of automorphisms act on this decomposition.

Proposition 2.69. *The decomposition of $\mathrm{End}_{\mathbb{Q}[G]}(V)$ happens as the following.*

$$\mathrm{End}_{\mathbb{Q}[G]}(V) = M_{r_1}\left(\mathrm{End}_{\mathbb{Q}[G]} V_1\right) \oplus M_{r_2}\left(\mathrm{End}_{\mathbb{Q}[G]} V_2\right) \oplus \cdots \oplus M_{r_k}\left(\mathrm{End}_{\mathbb{Q}[G]} V_k\right).$$

Proof. Observe that any $\mathbb{Q}[G]$-linear map from V_i to V_j for $i \neq j$ must be trivial due to irreducibility. Indeed, the kernel of such a map cannot be trivial since it would imply that V_i and V_j are isomorphic and hence, the kernel must be all of V_i.

So, the only maps from V to V are those that map r_i copies of V_i to itself for each $i = 1 \ldots k$. This gives us the matrix algebras above. □

Corollary 2.70. *The ring $\mathrm{End}_{\mathbb{Q}[G]} V$ is semisimple.*

Each $\mathrm{End}_{\mathbb{Q}[G]} V_i = D_i$ is a division algebra because of Proposition 2.67. Then, we get that V_i is a finitely generated left D_i-module over $\mathbb{Q}$. This implies from Proposition 2.62 that $V_i \simeq D^{n_i}$.

Definition 2.71. *For an irreducible $\mathbb{Q}[G]$-representation $V_\mathbb{Q}$, we call the $\mathrm{End}_{\mathbb{Q}[G]}$-rank of $V_\mathbb{Q}$ the matrix index of $V_\mathbb{Q}$.*

We will now try to make sense of this matrix index by introducing the following concept.

Definition 2.72. *Let R be any ring. Then we denote R_{op} to be the division algebra with the same set of elements as R and the multiplication given by*

$$(r_1, r_2) \mapsto r_2 r_1, \forall\ r_1, r_2 \in R.$$

Remark 2.73. *It is clear that $M_n(D_{\mathrm{op}})$ acting on the left on D^n is tacitly just $M_n(D)$ acting on $D^{1\times n}$ on the right.*

With this, we can observe that the n_i appearing in $V \simeq D^{n_i}$ has another interpretation. The Artin-Wedderburn decomposition of $\mathbb{Q}[G]$ is

$$\mathbb{Q}[G] \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_k}(D_k),$$

for some k, where $D_1, D_2, \ldots$ are $\mathbb{Q}$-division algebras. Each of the matrix algebras over division rings above corresponds to an irreducible representation of G over $\mathbb{Q}$ on which $\mathbb{Q}[G]$ acts upon as a ring of matrices over a division ring. The corresponding n_i is then the matrix index of the irreducible representation associated to the ith factor.

To make things more precise, if $V_\mathbb{Q}$ is an irreducible $\mathbb{Q}[G]$-module, $D = \mathrm{End}_G V_\mathbb{Q}$ is a $\mathbb{Q}$-division algebra whereas the image of $\mathbb{Q}[G]$ in $\mathrm{End}\, V_\mathbb{Q}$ must lie in

$$\mathrm{End}_{\mathrm{End}_G V_\mathbb{Q}} V_\mathbb{Q} \simeq \mathrm{End}_D D^n \simeq M_n(D_{\mathrm{op}}).$$

Hence, if $V_\mathbb{Q}$ has a decomposition as in Equation (2.3), then $\mathbb{Q}[G]$ maps into the space

$$\bigoplus_i M_{n_i}((D_i)_{\mathrm{op}}),$$

where $D_i = \mathrm{End}_G V_i$ as usual.

2.3.3 Tensoring a division algebra with reals

We are interested in evaluating $D \otimes_{\mathbb{Q}} \mathbb{R}$. Let $F = \mathcal{Z}(D)$ be the centre of the division ring D. Then, $[D : F]$ is always a perfect square (see [Jac09]), which we denote to be n^2 in the discussion below.

For this, consider the following chain of isomorphisms.

$$\begin{aligned} D \otimes_{\mathbb{Q}} \mathbb{R} &\simeq (D \otimes_F F) \otimes_{\mathbb{Q}} \mathbb{R} \\ &\simeq D \otimes_F (F \otimes_{\mathbb{Q}} \mathbb{R}). \end{aligned}$$

Now, suppose F has r_F real embeddings $\{\sigma_1, \sigma_2, \ldots, \sigma_{r_F}\}$ and c_F pairs of complex embeddings $\{\{\tau_1, \overline{\tau}_1\}, \ldots, \{\tau_{c_F}, \overline{\tau}_{c_F}\}\}$, then it is well known that the following is an $\mathbb{R}$-algebra isomorphism.

$$\begin{aligned} F \otimes_{\mathbb{Q}} \mathbb{R} &\xrightarrow{\sim} \mathbb{R}^{\oplus r_F} \oplus \mathbb{C}^{\oplus c_F} \\ x \otimes 1 &\mapsto (\sigma_1(x), \ldots, \sigma_{r_F}(x), \tau_1(x), \ldots, \tau_{c_F}(x)) \,. \end{aligned}$$

Hence, we write that

$$D \otimes_{\mathbb{Q}} \mathbb{R} \simeq (\bigoplus_{i=1}^{r_F} D \otimes_{\sigma_i(F)} \mathbb{R}) \oplus (\bigoplus_{i=1}^{c_F} D \otimes_{\tau_i(F)} \mathbb{C}).$$

Now, for any τ_i, $D \otimes_{\tau_i(F)} \mathbb{C}$ is a simple $\mathbb{C}$-algebra[6] and is therefore isomorphic to $M_n(\mathbb{C})$. On the other hand, depending on F and σ_i, $D \otimes_{\sigma_i(F)} \mathbb{R}$ is either isomorphic to $M_n(\mathbb{R})$ or $M_{n/2}(\mathbb{H})$, that is, either $D \otimes_{\sigma_i(F)} \mathbb{R}$ splits or does not split respectively. This gives us the following few propositions.

Proposition 2.74. *When n is odd, we get the following isomorphism.*

$$D \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_n(\mathbb{R})^{\oplus r_F} \oplus M_n(\mathbb{C})^{\oplus c_F}.$$

Proof. Clearly, since n is odd $M_{n/2}(\mathbb{H})$ cannot exist! □

Proposition 2.75. *When $F/\mathbb{Q}$ is a Galois, then either all the embeddings are real or they are all complex. Hence, when F is Galois and at least one strictly complex $\mathbb{Q}$-embedding of F exists, then*

$$D \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_n(\mathbb{C})^{\oplus (\frac{[F:\mathbb{Q}]}{2})}.$$

We can also consider the case of $D \otimes_{\mathbb{Q}} \mathbb{C}$ in a very similar fashion.

Proposition 2.76.

$$D \otimes_{\mathbb{Q}} \mathbb{C} \simeq M_n(\mathbb{C})^{\oplus [F:\mathbb{Q}]}.$$

Proof. Observe that for a number field F, if $\{\sigma_1, \sigma_2, \ldots, \sigma_{[F;\mathbb{Q}]}\}$ are all the embeddings $F \hookrightarrow \mathbb{C}$ over $\mathbb{Q}$, then the following map is an isomorphism.

$$\begin{aligned} F \otimes_{\mathbb{Q}} \mathbb{C} &\xrightarrow{\sim} \mathbb{C}^{\oplus [F:\mathbb{Q}]} \\ x \otimes 1 &\mapsto \left(\sigma_1(x), \ldots, \sigma_{[F:\mathbb{Q}]}(x)\right) . \end{aligned}$$

Then, we get that

$$\begin{aligned} D \otimes_{\mathbb{Q}} \mathbb{C} &\simeq (D \otimes_F F) \otimes_{\mathbb{Q}} \mathbb{C} \\ &\simeq D \otimes_{\mathbb{Q}} (F \otimes_{\mathbb{Q}} \mathbb{R}) \\ &\simeq \bigoplus_{i=1}^{[K:\mathbb{Q}]} D \otimes_{\sigma_i(F)} \mathbb{C} \\ &\simeq \bigoplus_{i=1}^{[K:\mathbb{Q}]} M_n(\mathbb{C}). \end{aligned}$$

□

[6] Extending scalars preserves simplicity.

2.3.4 Cyclic division algebras

Theorem 2.43 allows only 3 finite dimensional $\mathbb{R}$-division algebras, namely $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$. The only non-trivial and non-commutative extension of $\mathbb{R}$ is $\mathbb{H}$. However, over $\mathbb{Q}$, the story is completely different. There are infinitely many finite dimensional $\mathbb{Q}$-division algebras apart from the finite field extensions of $\mathbb{Q}$. All of these division algebras have the form of a cyclic division algebra.

We now give the construction of cyclic division algebras below. For a thorough introduction, one can refer to [Jac09], for instance. For a gentler introduction, read [For73].

Definition 2.77. *We define a cyclic $\mathbb{Q}$-division algebra as the quadruplet $D = (E, F, \sigma, \gamma)$, where*

1. *F is a number field over $\mathbb{Q}$,*
2. *E/F is a cyclic extension of degree n, i.e. the field extension E/F is Galois and the Galois group is cyclic,*
3. *σ is a generator of the cyclic group $\mathrm{Gal}(E/F)$ and*
4. *$\gamma \in F^*$, with the property that the multiplicative order of γ in the group $F^*/N_F^E(E^*)$ is exactly n. That is, $\gamma^k \notin N_F^E(E^*)$ for any $k \in \{1, 2, \ldots, n-1\}$ and $\gamma^n = N_F^E(x)$ for some $x \in E^*$. When this happens, we say that $\gamma \in F^*$ is a non-norm element. Note that $\gamma^n = \mathrm{N}_F^E(\gamma)$.*

Consider a formal element b that does not commute with E and satisfies $b^n = \gamma$. As an E-module, D is defined as per the isomorphism

$$D \simeq E \oplus Eb \oplus Eb^2 \oplus \cdots \oplus Eb^{n-1}, \tag{2.4}$$

which can be given the structure of an F-algebra by implementing the rule

$$bl = \sigma(l)b \text{ for all } l \in E. \tag{2.5}$$

If we identify $D \simeq E^n$ according to the identification (2.4), then for $g = (g_0, g_1, \ldots, g_{n-1})$, we observe that for some $x_0 \in E$, we get the following from repeatedly using Equation (2.5).

$$\begin{aligned} gb =& (g_0 + g_1 b + g_2 b^2 + \cdots + g_{n-1} b^{n-1}) x_0 \\ =& \begin{bmatrix} x_0 & & & & & & & \\ & \sigma(x_0) & & & & & & \\ & & \sigma^2(x_0) & & & & & \\ & & & \sigma^3(x_0) & & & & \\ & & & & \sigma^4(x_0) & & & \\ & & & & & \ddots & & \\ & & & & & & \sigma^{n-1}(x_0) \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ \\ \\ g_{n-1} \end{bmatrix}, \end{aligned}$$

whereas multiplying by b on the right looks like

$$\begin{aligned} gb =& (g_0 + g_1 b + g_2 b^2 + \cdots + g_{n-1} b^{n-1}) b \\ =& \begin{bmatrix} & & & & & & \gamma \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ \\ \\ g_{n-1} \end{bmatrix}. \end{aligned}$$

Extending this to the right multiplication by some $y = y_0 + y_1 b + \cdots + y_{n-1}b^{n-1}$, we write that

$$\begin{aligned} gy =& g(y_0 + y_1 b + y_2 b^2 + \cdots + y_n b^{n-1}) \\ =& g(y_0 + b\sigma^{-1}(y_1) + b^2\sigma^{-2}(y_2) + b^3\sigma^{-3}(y_3) + \cdots + b^{n-1}\sigma^{-n+1}(y_{n-1})) \end{aligned}$$

$$= \begin{bmatrix} y_0 & \gamma\sigma(y_{n-1}) & \gamma\sigma^2(y_{n-2}) & \gamma\sigma^3(y_{n-3}) & & \gamma\sigma^{n-2}(y_2) & \gamma\sigma^{n-1}(y_1) \\ y_1 & \sigma(y_0) & \gamma\sigma^2(y_{n-1}) & \gamma\sigma^3(y_{n-2}) & & \gamma\sigma^{n-2}(y_3) & \gamma\sigma^{n-1}(y_2) \\ y_2 & \sigma(y_1) & \sigma^2(y_0) & \gamma\sigma^3(y_{n-1}) & \cdots & \gamma\sigma^{n-2}(y_4) & \gamma\sigma^{n-1}(y_3) \\ y_3 & \sigma(y_2) & \sigma^2(y_1) & \sigma^3(y_0) & & \gamma\sigma^{n-2}(y_5) & \gamma\sigma^{n-1}(y_4) \\ y_4 & \sigma(y_3) & \sigma^2(y_2) & \sigma^3(y_1) & & \gamma\sigma^{n-2}(y_6) & \gamma\sigma^{n-1}(y_5) \\ & \vdots & & & \ddots & & \\ y_{n-1} & \sigma(y_{n-2}) & \sigma^2(y_{n-3}) & \sigma^3(y_{n-4}) & & \sigma^{n-2}(y_1) & \sigma^{n-1}(y_0) \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ \\ \\ g_{n-1} \end{bmatrix}.$$

Since this is a matrix representation of the right multiplication, we get from the above matrix a map $D_{\text{op}} \to M_n(E)$.

Clearly, F lies in the centre $\mathcal{Z}(D)$. In fact, after some matrix computations, one can see that F is the centre.

Remark 2.78. *From the identification in Equation* (2.4)*, it is clear that* $\dim_F(D) = n^2$.

Remark 2.79. *If only the first three conditions are satisfied in the definition without condition 4, then we simply call D a cyclic $\mathbb{Q}$-algebra. A cyclic $\mathbb{Q}$-algebra is a division algebra if and only if condition 4 is satisfied. That is, (E, F, σ, γ) is a division algebra if and only if γ is a non-norm element.*

Let us consider some examples.

Example 2.80. *Consider $D = (\mathbb{Q}[i], \mathbb{Q}, \sigma, -1)$, where $\sigma : \mathbb{Q}[i] \to \mathbb{Q}[i]$ is the unique non-trivial Galois automorphism. Here $n = 2$ and since $N_{\mathbb{Q}}^{\mathbb{Q}[i]}(a + ib) = a^2 + b^2 \geq 0$ for any $a, b \in \mathbb{Q}$, -1 is not a norm of any element in $\mathbb{Q}[i]^*$.*

This division algebra fits inside the quaternion group $\{\pm 1, \pm i, \pm j, \pm ij\}$, where $j \neq i$ such that $j^2 = -1$.

Example 2.81. *This example is from [Lam01], but is also mentioned in [Ami55]. This is the smallest odd order non-commutative group that can fit inside a division algebra.*

Take $E = \mathbb{Q}[\zeta_{21}]$, the 21st cyclotomic field. We know that $[E : \mathbb{Q}] = 12$. Take $\sigma \in \text{Gal}(E/\mathbb{Q})$ defined by $\zeta_{21} \mapsto \zeta_{21}^{16}$. Then the order of σ in $\text{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/21\mathbb{Z})^*$ is 3. Take $F = E^{\langle\sigma\rangle}$, that is, the field of those elements of E that are fixed under σ. Clearly, $[E : F] = 3$ and $[F : \mathbb{Q}] = 4$. We declare ζ_{21}^7 to be the non-norm element γ . The fact that this works is explained in [For73].

This makes $D = (E, F, \sigma, \gamma)$ a 9-dimension division algebra over F and 36-dimensional division algebra over $\mathbb{Q}$. In [Lam01], we see that this division algebra fits a finite group G of 63 elements, which is generated by the non-commutative formal element b and ζ_{21}^3.

G is in fact full-span inside D. To see this, observe that $b^3 = \gamma = \zeta_{21}^7$ and $\zeta_{21}^7\zeta_{21}^3 = \zeta_{21}^{10}$ which is primitive and generates all the powers of ζ_{21}. The $\mathbb{Q}$-span of those powers is E and along with b, it generates D.

As we have mentioned, division algbras over $\mathbb{Q}$ are completely classified. Indeed, the following is the theorem which explains this.

Theorem 2.82. *(Albert, Brauer, Hasse, Noether)*
All division algebras over $\mathbb{Q}$ are cyclic division algebras.

The proof of Theorem 2.82 is well outside the scope of the thesis, but [Pie12] contains a detailed account.

Chapter 3

Random lattices with prescribed symmetries

Let G be a finite group acting on a finite dimensional real vector space $\mathbb{R}^d$. We want to consider all the full-span lattices $\Lambda \subseteq \mathbb{R}^d$ that are invariant under the action of G. Hence, we assume that there must exist at least one such lattice Λ. This restricts our G-action in the following way.

Let $v_1, v_2, \ldots, v_d \subset \Lambda$ be a basis of $\mathbb{R}^d$. It is then clear that G will take each vector v_i to a $\mathbb{Z}$-linear combination of the v_i. Hence, we conclude that using this basis, G can actually get a homomorphism $G \to \mathrm{GL}_d(\mathbb{Q})$. In other words, G can actually afford a d-dimensional $\mathbb{Q}$-representation $V_{\mathbb{Q}}$ such that $\mathbb{R}^d \simeq V_{\mathbb{Q}} \otimes \mathbb{R} = V_{\mathbb{R}}$.

Let us then try to construct the right candidate to study as our space of G-symmetric lattices in $V_{\mathbb{R}}$.

3.1 The most general space of lattices

Let us start, without loss of generality, with a finite group G that is a subgroup[1] of $\mathrm{SL}_d(\mathbb{Z})$. The most immediate candidate then to have a space of G-invariant lattices is the following.

$$C_1 = \{g\mathbb{Z}^d \mid g \in \mathrm{SL}_d(\mathbb{R}), g^{-1}hg \in \mathrm{SL}_d(\mathbb{Z}) \text{ for each } h \in G\}.$$

Indeed, any such lattice Λ in the set above will have the property that $h\Lambda = \Lambda$ for $h \in G$.

However, the condition given on g above does not define a subgroup of $\mathrm{SL}_d(\mathbb{R})$. That is, the following is not a group in general.

$$\mathbb{G}_1 = \{g \in \mathrm{SL}_d(\mathbb{R}) \mid g^{-1}hg \in \mathrm{SL}_d(\mathbb{Z}) \text{ for each } h \in G\} \subseteq \mathrm{SL}_d(\mathbb{R}). \tag{3.1}$$

It is not clear how to proceed studying this space of lattices. This construction could be considered in future works on this topic.

Here is an example of such a construction.

Example 3.1. *Let $I = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and consider the group $G = \langle I \rangle \subseteq \mathrm{SL}_2(\mathbb{R})$. As a group, G is simply a cyclic group of order 4.*

We know that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

and the condition for membership in the set $\mathbb{G}_1$ defined in Equation (3.1) is that

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$
$$\Leftrightarrow \begin{bmatrix} dc + ab & d^2 + b^2 \\ -a^2 - c^2 & -cd - ab \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

[1] It is known [Ser09, App. 3] that for a fixed d, there are finitely many choices of a group G.

It is clear that $\mathrm{SL}_2(\mathbb{Z}) \subseteq \mathbb{G}_1$. *Furthermore, observe that* $\mathbb{G}_1$ *must be closed under multiplication by rotation matrices on the left. That is*

$$\begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} \mathbb{G}_1 \subseteq \mathbb{G}_1.$$

So we know that

$$\mathrm{SO}(2)\,\mathrm{SL}_2(\mathbb{Z}) \subseteq \mathbb{G}_1.$$

In fact, with a bit of work we can show that the above is an equality. Observe that we know that if $g\mathbb{Z}^2$ *is invariant under* I *and if* $v \in g\mathbb{Z}^2$ *is the shortest vector, then the closure of the square spanned by* v *and* Iv *must not contain any lattice points in* $g\mathbb{Z}^2$ *(follows from a geometric argument left for the reader). Hence* $g\mathbb{Z}^2$ *contains* $\mathbb{Z}^2$ *up to a rotation and therefore it* $g\gamma \in \mathrm{SO}(2)$ *for some* $\gamma \in SL_2(\mathbb{Z})$.

3.2 Quotient spaces of $\mathbb{Q}$-algebraic groups

We can instead consider the set

$$C_{\mathrm{aut}} = \{g\mathbb{Z}^d \mid g \in \mathrm{SL}_d(\mathbb{R}), g^{-1}hg \in G \text{ for each } h \in G\}.$$

And this is now the image of a subgroup of $\mathrm{SL}_d(\mathbb{R})$ that is an algebraic $\mathbb{Q}$-group. Namely, the following is an algebraic group.

$$\mathcal{G}_{\mathrm{aut}}(\mathbb{R}) = \{g \in \mathrm{SL}_d(\mathbb{R}), g^{-1}hg \in G \text{ for each } h \in G\}. \tag{3.2}$$

With this definition, we have that

$$C_{\mathrm{aut}} \simeq \mathcal{G}_{\mathrm{aut}}(\mathbb{R})/\mathcal{G}_{\mathrm{aut}}(\mathbb{Z}).$$

Note that the following group is a subgroup with a finite index in $\mathcal{G}_{\mathrm{aut}}$.

$$\mathcal{G}_{\mathrm{com}}(\mathbb{R}) = \{g \in \mathrm{SL}_d(\mathbb{R}), g^{-1}hg = h \text{ for each } h \in G\}. \tag{3.3}$$

To see that $\mathcal{G}_{\mathrm{com}}$ is a finite index subgroup of $\mathcal{G}_{\mathrm{aut}}$, we observe that the quotient of the two subgroups of $\mathrm{SL}_d(\mathbb{R})$ will be some subgroup of automorphisms $\mathrm{Aut}\,G$ of G. In fact, we will shortly describe this subset a bit more.

With the choice of the algebraic group as $\mathcal{G}_{\mathrm{com}}$, we can again define the space of lattices to be

$$C_{\mathrm{com}} = \{g\mathbb{Z}^d \mid g \in SL_d(\mathbb{R}), g^{-1}hg = h \text{ for each } h \in G\} \simeq \mathcal{G}_{\mathrm{com}}(\mathbb{R})/\mathcal{G}_{\mathrm{com}}(\mathbb{Z}).$$

Both C_{aut} and C_{com} are interesting candidates to study as a space of G-symmetric lattices. They both have a nice structure of a quotient of some smooth group modulo a discrete subgroup. This opens us to the set of tools at our disposal from the preliminaries developed in Chapter 2.

Let us first see an example of the constructions C_{com} and C_{aut}.

Example 3.2. *Consider the same setup as Example 3.1. As before, we have*

$$I = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right],$$

and $G = \langle I \rangle$.

Note that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} I = I \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\Rightarrow\; c = -b, a = d.$$

What this implies is that the algebra

$$\{A \in M_2(\mathbb{R}) \mid AI = IA\} = \mathbb{R} + \mathbb{R}I \simeq \mathbb{C}.$$

Thus, the group $\mathcal{G}_{\mathrm{com}}(\mathbb{R})$ *defined in Equation* (3.3) *is then simply*

$$\mathcal{G}_{\mathrm{com}}(\mathbb{R}) \simeq \{z \in \mathbb{C} \mid \|z\| = 1\}.$$

Furthermore, $\mathcal{G}_{\mathrm{com}}(\mathbb{Z}) = \{\pm 1, \pm I\}$.

On the other hand, if we were to consider the group $\mathcal{G}_{\mathrm{aut}}$ *in Equation* (3.2)*, then things become slightly different. For any* $A \in \mathrm{SL}_2(\mathbb{R})$, $A^{-1}IA \in \langle I \rangle \Rightarrow A^{-1}IA = \pm I$. *Then, the following vector space*

$$\{A \in M_2(\mathbb{R}) \mid IA = -AI\} = \mathbb{R}J + \mathbb{R}K,$$

where

$$J = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \; K = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]. \tag{3.4}$$

With this setup, we get

$$\mathcal{G}_{\mathrm{aut}}(\mathbb{R}) = \mathcal{G}_{\mathrm{com}}(\mathbb{R}) \sqcup \mathcal{G}_{\mathrm{com}}(\mathbb{R}) \cdot J,$$

and

$$\mathcal{G}_{\mathrm{aut}}(\mathbb{Z}) = \{\pm 1, \pm I, \pm J, \pm K\}.$$

Coincidentally, in this case we have

$$C_1 = C_{\mathrm{com}} = C_{\mathrm{aut}},$$

even if $\mathbb{G}_1, \mathcal{G}_{\mathrm{com}}, \mathcal{G}_{\mathrm{aut}}$ *are all different.*

Example 3.3. *Let us show an example where* $C_1 \neq C_{\mathrm{com}}$. *Take the same group* $G = \langle I \rangle$ *as before and let us change the representation to be the following.*

Let $\pi : G \to \mathrm{GL}_3(\mathbb{R})$ *be given by*

$$\pi(I) = \left[\begin{smallmatrix} I & \\ & 1 \end{smallmatrix}\right] = \begin{bmatrix} & 1 & \\ -1 & & \\ & & 1 \end{bmatrix}.$$

In this case, we observe that

$$\mathcal{G}_{\mathrm{com}}(\mathbb{R}) = \left\{ \begin{bmatrix} a\cos\theta & a\sin\theta & \\ -a\sin\theta & a\cos\theta & \\ & & \frac{1}{a^2} \end{bmatrix} \mid \theta, a \in \mathbb{R}, a \neq 0 \right\}.$$

But observe that

$$B = \begin{bmatrix} 1 & & 1/2 \\ & 1 & 1/2 \\ & & 1 \end{bmatrix} \in \mathbb{G}_1$$

is not inside $\mathcal{G}_{\mathrm{com}}(\mathbb{R}) \cdot \mathrm{SL}_3(\mathbb{Z})$. *To see why, note that any* $A \in \mathcal{G}_{\mathrm{com}}(\mathbb{R})\,\mathrm{SL}_3(\mathbb{Z})$ *will correspond to a lattice* $A\mathbb{Z}^3$ *which will be a direct sum* $\Lambda_1 \oplus a\mathbb{Z} \subseteq \mathbb{R}^2 \oplus \mathbb{R}$ *of two lattices, one* 2*-dimensional and one* 1*-dimensional. However, the layers of the lattice generated by* B *in the* xy*-plane are alternating between two affine lattices.*

3.2.1 Representation theoretic viewpoint

Let $V_{\mathbb{Q}}$ be $\mathbb{Q}^d$ and let $\pi : \mathbb{Q}[G] \to \operatorname{End} V_{\mathbb{Q}}$ be a $\mathbb{Q}$-algebra homomorphism. This makes $V_{\mathbb{Q}}$ a $\mathbb{Q}[G]$-module and $V = V_{\mathbb{Q}} \otimes \mathbb{C}$. Note that we have the map $\det : \operatorname{End} V_{\mathbb{Q}} \to \mathbb{Q}$ and we have the canonical inclusion

$$\operatorname{End}_G V_{\mathbb{Q}} = \operatorname{End}_{\mathbb{Q}[G]} V_{\mathbb{Q}} \subseteq \operatorname{End} V_{\mathbb{Q}}.$$

With this, we can write that the group from Equation (3.3) is nothing but

$$\mathcal{G}_{\mathrm{com}}(\mathbb{Q}) = \{A \in \operatorname{End}_{\mathbb{Q}[G]} V \mid \det A = 1\},$$

and $\mathcal{G}_{\mathrm{com}}(\mathbb{R})$ is the corresponding set of real points.

We can simplify the definition of $\mathcal{G}_{\mathrm{aut}}$ of Equation (3.2) in a similar way. Let $\sigma \in \operatorname{Aut} G$ be an automorphism of the finite group G. We then define

$$\operatorname{End}_G^{\sigma} V_{\mathbb{Q}} = \{A \in \operatorname{End} V_{\mathbb{Q}} \mid \pi(g^{\sigma})A = A\pi(g) \text{ for each } g \in G\}. \tag{3.5}$$

It is clear that $\operatorname{End}_G^{\sigma} V_{\mathbb{Q}}$ is a vector space and also an $\operatorname{End}_G V_{\mathbb{Q}}$-module. It satisfies

$$\operatorname{End}_G^{\sigma} V_{\mathbb{Q}} \cdot \operatorname{End}_G^{\sigma'} V_{\mathbb{Q}} \subseteq \operatorname{End}_G^{\sigma\cdot\sigma'} V_{\mathbb{Q}}, \forall\, \sigma, \sigma' \in \operatorname{Aut} G.$$

Lemma 3.4.

$$\dim_{\mathbb{Q}} \operatorname{End}_G^\sigma V_{\mathbb{Q}} = \begin{cases} 0 & \operatorname{End}_G^\sigma V = \{0\} \\ \dim_{\mathbb{Q}} \operatorname{End}_G V_{\mathbb{Q}} & \textit{otherwise} \end{cases}.$$

Proof. Observe that being a $\mathbb{Q}$-vector space implies that $\operatorname{End}_G^\sigma V_{\mathbb{Q}} \cap \mathrm{GL}(V_{\mathbb{Q}})$ must be non-empty whenever $\operatorname{End}_G^\sigma V_{\mathbb{Q}} \neq \{0\}$. When this happens, for $A_\sigma \in \operatorname{End}_G^\sigma V_{\mathbb{Q}} \cap \mathrm{GL}(V_{\mathbb{Q}})$, the following is an isomorphism of $\mathbb{Q}$-vector spaces.

$$\begin{aligned} \operatorname{End}_G V_{\mathbb{Q}} &\to \operatorname{End}_G^\sigma V_{\mathbb{Q}} \\ x &\mapsto xA_\sigma. \end{aligned}$$

□

Lemma 3.4 inspires us to define the following finite group inside $\operatorname{Aut} G$.

$$\operatorname{Aut}_V G = \{\sigma \in \operatorname{Aut} G \mid \operatorname{End}_G^\sigma V_{\mathbb{Q}} \neq \{0\}\}.$$

With this notation, we can rewrite Equation (3.2) as

$$\mathcal{G}_{\mathrm{aut}}(\mathbb{Q}) = \bigcup_{\sigma \in \operatorname{Aut}_V G} \{A \in \operatorname{End}_G^\sigma V_{\mathbb{Q}} \mid \det A = 1\}.$$

We then have the identification

$$\operatorname{Aut}_V G \simeq \mathcal{G}_{\mathrm{aut}}/\mathcal{G}_{\mathrm{com}}.$$

Example 3.5. *Let us consider the same group $G = \langle I \rangle$ as Example 3.1, 3.2 but this time, let us change the representation to be 4-dimensional.*

Let $\pi : G \to \mathrm{GL}_4(\mathbb{R})$ be given by

$$\pi(I) = \begin{bmatrix} & I \\ I & \end{bmatrix} = \begin{bmatrix} & 1 & & \\ -1 & & & \\ & & & 1 \\ & & -1 & \end{bmatrix}.$$

Let $V_{\mathbb{Q}} = \mathbb{Q}^d$. Then, we have that

$$\operatorname{End}_G V_{\mathbb{Q}} = \left\{ \begin{bmatrix} E & F \\ G & H \end{bmatrix} \mid E, F, G, H \in \mathbb{Q} + \mathbb{Q}I \right\} \simeq M_2(\mathbb{C}).$$

So, after all, we get

$$\mathcal{G}_{\mathrm{com}}(\mathbb{R}) = \left\{ \begin{bmatrix} E & F \\ G & H \end{bmatrix} \mid E, F, G, H \in \mathbb{R} + \mathbb{R}I, \det(EH - FG) = 1 \right\}.$$

As a Lie group, this is almost like $\mathrm{SL}_2(\mathbb{C})$, except that it has a compact factor of S_1 as a unit circle. That is,

$$\mathcal{G}_{\mathrm{com}}(\mathbb{R}) \simeq \mathrm{SL}_2(\mathbb{C}) \times S_1.$$

There is exactly one automorphism of the group G which is $\sigma : I \mapsto -I$. We see that the following matrix A_σ is invertible and must satisfy $A\pi(I) = \pi(-I)A$

$$A_\sigma = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}.$$

Then, if we follow the proof of Lemma 3.4, we see that

$$\operatorname{End}_G^\sigma V_{\mathbb{Q}} = \operatorname{End}_G V_{\mathbb{Q}} \cdot A_\sigma,$$

and

$$\mathcal{G}_{\mathrm{aut}}(\mathbb{R}) = \mathcal{G}_{\mathrm{com}}(\mathbb{R}) \sqcup \mathcal{G}_{\mathrm{com}}(\mathbb{R}) A_\sigma.$$

Here is a third candidate, again using the automorphism group $\mathrm{Aut}_V\, G$. We can define

$$\widetilde{\mathrm{End}}_G V = \sum_{\sigma \in \mathrm{Aut}_V\, G} \mathrm{End}_G^{\sigma} V.$$

$\widetilde{\mathrm{End}}_G V$ is a $\mathbb{Q}$-subalgebra of $\mathrm{End}_{\mathbb{Q}}\, V$ embedded via π.

We can then conjure up a new $\mathbb{Q}$-algebraic group given as

$$\mathcal{G}_{\mathrm{twist}}(\mathbb{Q}) = \mathrm{SL}(V_{\mathbb{Q}}) \cap \widetilde{\mathrm{End}}_G V.$$

Observe that we still have the remarkable property that for every $A \in \mathcal{G}_{\mathrm{twist}}(\mathbb{R})$ and if $\Lambda \subseteq V_{\mathbb{Q}}$ is a lattice invariant under G-action, then

$$\pi(g)A \cdot \Lambda = A\Lambda,\ \forall\ g \in G.$$

Indeed, we can write $A = A_{\sigma_1} + A_{\sigma_2} + \dots$ where $A_{\sigma_i} \in \mathrm{End}_G^{\sigma_i} V$. Then for any $g \in G$, we have

$$\pi(g) \cdot A = A_{\sigma_1} \pi(g^{\sigma_1^{-1}}) + A_{\sigma_2} \pi(g^{\sigma_2^{-1}}) + \cdots .$$

And this implies that the lattice $A\Lambda \subseteq V_{\mathbb{R}}$ is preserved under the action of G. Thus, we get that the following is also homogeneous space of G-invariant lattices:

$$\mathcal{G}_{\mathrm{twist}}(\mathbb{R})/\Gamma,$$

where $\Gamma = \{A \in \mathcal{G}_{\mathrm{twist}}(\mathbb{Q}) \mid A\Lambda = \Lambda\}$.

Let us try to illustrate this with our running example.

Example 3.6. *Suppose $G \simeq \langle I \rangle$ is the group from Example 3.1, 3.2 acting on $\mathbb{R}^2$ as before. Then, observe that the ring*

$$\widetilde{\mathrm{End}}_G V = \mathrm{End}_G\, V \oplus \mathrm{End}_G\, V \cdot J \simeq \mathbb{Q}[I, J],$$

where J is defined in Equation (3.4). This tells us that the ring $\widetilde{\mathrm{End}}_G V_{\mathbb{Q}}$ is the ring of rational quaternions. The real points of this ring form the Hamiltonian quaternion ring $\mathbb{H}$. Hence, the group $\mathcal{G}_{\mathrm{twist}}(\mathbb{R})$ would be isomorphic to the three dimensional sphere as a Lie group.

If we were to instead consider the action of G given in Example 3.5, then we would get that

$$\mathcal{G}_{\mathrm{twist}}(\mathbb{R}) \simeq \mathrm{SL}_2(\mathbb{H}).$$

3.2.2 $\mathrm{Aut}_V\, G$ is not easy to understand

Observe the following.

Lemma 3.7. *Let $\mathrm{Aut}_V\, G$ be as defined in Equation (3.5). There is a homomorphism of groups given below.*

$$\mathrm{Aut}_V\, G \to \frac{\mathrm{Aut}\,(\mathrm{End}_G\, V_{\mathbb{Q}})}{\mathrm{Inn}\,(\mathrm{End}_G\, V_{\mathbb{Q}})} \simeq \mathrm{Out}(\mathrm{End}_G\, V_{\mathbb{Q}}).$$

Here, $\mathrm{Aut}(\mathrm{End}_G\, V_{\mathbb{Q}})$, $\mathrm{Out}(\mathrm{End}_G\, V_{\mathbb{Q}})$ and $\mathrm{Inn}(\mathrm{End}_G\, V_{\mathbb{Q}})$ are the groups of automorphisms, inner automorphisms and outer automorphisms of $\mathrm{End}_G\, V_{\mathbb{Q}}$ respectively.

Proof. Note that for any $\sigma \in \mathrm{Aut}_V\, G$, we have that any $A_\sigma, B_\sigma \in \mathrm{End}_G^{\sigma} V \cap \mathrm{GL}(V_{\mathbb{Q}})$ acts on $\mathrm{End}_G\, V_{\mathbb{Q}}$ by

$$x \mapsto A_\sigma^{-1} x A_\sigma.$$

Since $y = A_\sigma^{-1} B_\sigma \in \mathrm{End}_G\, V$, so in fact the automorphism defined above is well-defined upto an inner automorphism. □

We remind the reader that V has a decomposition of the form

$$V_{\mathbb{Q}} \simeq (V_1)_{\mathbb{Q}}^{\oplus r_1} \oplus \cdots \oplus (V_k)_{\mathbb{Q}}^{\oplus r_k},$$

as in Theorem 2.68. Then using Proposition 2.69

$$\operatorname{End}_G V \simeq M_{r_1}(D_1) \oplus M_{r_2}(D_2) \oplus \cdots \oplus M_{r_k}(D_k),$$

where $D_i = \operatorname{End}_G V_i$ is a division algebra by Proposition 2.67. Then, the group of automorphisms $\operatorname{Aut}(\operatorname{End}_G V)$ is therefore the group of automorphisms of these products of matrix algebras. Hence, the automorphism group itself can be written as a direct product of automorphism groups of each of the simple factors given above. Any automorphism of a $\mathbb{Q}$-algebra must automatically be $\mathbb{Q}$-linear and Theorem 2.40 tells us that the automorphisms that are linear over the centre are simply the inner automorphisms.

For simplicity, let's assume for now that $k = 1$ and $r_1 = 1$. Hence, we are in the case where $\operatorname{End}_G V_{\mathbb{Q}} = D$ is a division algebra over $\mathbb{Q}$. Observe that any automorphism that is $\mathbb{Q}$-linear must send $\mathcal{Z}(D)$ to itself and hence becomes a Galois automorphism of a number field. But in general, not every Galois automorphism of $\mathcal{Z}(D)$ can be extended to an automorphism of D even when we have the structure theorem Theorem 2.82 that classifies all $\mathbb{Q}$-division algebras [Han07].

On the other hand in the same setting when $k = 1$, $\operatorname{Aut}_G V$ could be as complicated as any finite group of $\mathbb{Q}$-division algebra automorphisms of D. Indeed, recall that towards the end of Section 2.3.2, we discussed that if V has a matrix index t then $\pi : G \to \operatorname{End}_{\mathbb{Q}} V_{\mathbb{Q}}$ maps into

$$\pi(\mathbb{Q}[G]) \subseteq \operatorname{End}_{\operatorname{End}_G V_{\mathbb{Q}}} V_{\mathbb{Q}} \simeq M_t(D^{\mathrm{op}}),$$

where D is the division algebra $\operatorname{End}_G V_{\mathbb{Q}}$. In fact, this inclusion is surjective since $M_t(D^{\mathrm{op}})$ is one of the simple components inside $\mathbb{Q}[G]$. Thus, we get that

$$\operatorname{Aut}_{\mathbb{Q}}\left(\pi(\mathbb{Q}[G])\right) \simeq \operatorname{Aut}_{\mathbb{Q}}\left(M_t(D^{\mathrm{op}})\right).$$

3.2.3 Finiteness of measure

Note that we want to create a probability space of lattices invariant under the action of G. From the discussion above, we are in the domain of having the real points of a $\mathbb{Q}$-algebraic group $\mathcal{G}(\mathbb{R})$ modulo an arithmetic subgroup. Hence, using Theorem 2.12, we must have only those groups for which $X_{\mathbb{Q}}(\mathcal{G}^0) = \{0\}$.

Since, we know that our subgroup satisfies

$$\mathcal{G}_{\mathrm{com}}(\mathbb{Q}) \subseteq \operatorname{End}_G V,$$

we can identify it as a $\mathbb{Q}$-subgroup of

$$\mathrm{GL}_{r_1}(D_1) \oplus \mathrm{GL}_{r_2}(D_2) \oplus \cdots \mathrm{GL}_{r_k}(D_k),$$

where $D_i = \operatorname{End}_{\mathbb{Q}[G]} V_i$ is the division ring coming from V_i.

In order to make sure that our measure space $\mathcal{G}(\mathbb{R})/\mathcal{G}(\mathbb{Z})$ is a probability space, we are forced to choose

$$\mathcal{G}^{(1)}(\mathbb{Q}) = \mathrm{SL}_{r_1}(D_1) \oplus \mathrm{SL}_{r_2}(D_2) \oplus \cdots \mathrm{SL}_{r_k}(D_k),$$

which we get when we make all the reduced norms in each simple factor equal to 1. And indeed, due to the discussion of Section 4.1, the homogeneous space of this group is of finite covolume.

In line with the constructions $\mathcal{G}_{\mathrm{twist}}$ and $\mathcal{G}_{\mathrm{aut}}$, it is possible to make analogous constructions $\mathcal{G}^{(1)}_{\mathrm{twist}}$ and $\mathcal{G}^{(1)}_{\mathrm{aut}}$. We will not pursue those ideas due to the previously mentioned reasons.

Chapter 4

Integrating on $\mathrm{SL}_t(D)$

Here, we describe the special linear group over division algebra that we settled on as our algebraic group candidate in Chapter 3. Recall what a reduced norm is from Remark 4.17.

Definition 4.1. *Let D be a $\mathbb{Q}$-division algebra and $t \geq 1$.*

We denote $\mathrm{SL}_t(D)$ to be the group of matrices $M_{t\times t}(D)$ with reduced norm equal to 1. This is the set of $\mathbb{Q}$-points algebraic group $\mathcal{G}$, whose real points $\mathcal{G}(\mathbb{R})$ are $\mathrm{SL}_t(D_{\mathbb{R}})$.

We state the following proposition about these groups that will be important in classifying rational orbits under the group action of $\mathrm{SL}_t(D)$.

Lemma 4.2. *Let $M_{t\times n}(D)$ be acted upon $\mathrm{SL}_t(D_{\mathbb{R}})$ from the left. Then this action is transitive on the set of full-rank matrices when $n < t$.*

Proof. What is being asked here is if the first n columns on the left are fixed to be a matrix in $M_{t\times n}(D)$, can it be completed to create a matrix in $\mathrm{SL}_t(D)$? The answer is yes, since we can line up some 1s on the diagonal except for the bottom right where we put a suitable rational number so that the reduced norm 1 condition holds. □

Remark 4.3. *Lemma 4.2 will not work for $n \geq t$. Indeed, for example when $n = t$, the $\mathrm{SL}_t(D)$ action will not be able to change the norm of a matrix in $M_{t\times t}(D)$.*

4.1 Reduction theory

4.1.1 Cholesky decomposition

Let A be a semisimple $\mathbb{R}$-algebra with a positive involution $(\ )^*$. The algebra $M_k(A)$ is also a semisimple $\mathbb{R}$-algebra and the involution $(\ )^*$ can be easily extended to $M_k(A)$ via the mapping $[a_{ij}] \mapsto [a^*_{ji}]$. We will denote this involution with same notation $(\ )^*$. With this, the meaning of positive definite and symmetric matrices in $M_k(A)$ is unambiguous. For clarity, we will distinguish between the norms and traces of A and $M_k(A)$ by using the notations $\mathrm{tr}_A, \mathrm{N}_A, \mathrm{tr}_{M_k(A)}, \mathrm{N}_{M_k(A)}$ whenever appropriate.

For any $a \in M_k(A)$, we can create a bilinear form $\beta_a : A^k \times A^k \to \mathbb{R}$ as

$$\beta_a(x, y) = \sum_{i,j=1}^{k} \mathrm{tr}_A(x_i^* a_{ij} y_j).$$

The following lemma then shows that the conventional intuition of positive definiteness is in accordance with Definition 2.48.

Lemma 4.4. *An element $a \in M_k(A)$ is positive definite if and only if β_a is a positive definite quadratic form on A^k as an $\mathbb{R}$-vector space.*

Proof. By checking with appropriate basis elements, we conclude that $\mathrm{tr}_{M_k(A)}(a) = k\,\mathrm{tr}_A\left(\sum_{i=1}^k a_{ii}\right)$ for any $a \in M_k(A)$. Now, if $\{x_{\bullet p}\}_{p=1}^k \subseteq A^k$ are the columns of the matrix $x \in M_k(A)$, we get that

$$\begin{aligned}\mathrm{tr}_{M_k(A)}(x^*ax) &= k\sum_{p,q,r=1}^k \mathrm{tr}_A(x_{pr}^* a_{pq} x_{qr}) \\ &= k\sum_{r=1}^k \beta_a(x_{\bullet p}, x_{\bullet p}).\end{aligned}$$

Hence, the above quadratic form is just $k\beta_a \oplus \cdots \oplus k\beta_a = k\beta_a^{\oplus k}$ on the space $M_k(A) \simeq (A^k)^{\oplus k}$. Therefore, β_a is positive definite if and only if the above quadratic form is, which is exactly the definition of a being positive definite as an element of A. □

This lemma leads to the following decomposition for quadratic forms β_a induced by symmetric positive definite matrices a. What the upcoming theorem is really going to tell us is that the quadratic form β_a can be "diagonalised" up to a "triangular" change of basis.

When $A = \mathbb{R}$, this is simply the Cholesky decomposition of real symmetric positive definite matrices. In [Wei58], the theorem below is referred to as the Babylonian reduction theorem, perhaps because it is spiritually similar to "completing the square" in a quadratic equation of one variable.

Theorem 4.5. *Let $a \in M_k(A)$ be a symmetric positive definite matrix. Then there is an upper triangular matrix $t \in M_k(A)$ with 1_A on the diagonal entries, and a diagonal matrix d with symmetric positive definite elements of A on the diagonal such that*

$$a = t^*dt.$$

Proof. Writing explicitly in terms of A-valued matrix entries, what we want is to find $d, t \in M_k(A)$ such that

$$\begin{aligned}\begin{bmatrix} a_{11} & a_{12} & & a_{1k} \\ a_{21} & a_{22} & & a_{2k} \\ & & \ddots & \\ a_{k1} & a_{k2} & & a_{kk} \end{bmatrix} &= \begin{bmatrix} 1_A & & & \\ t_{12}^* & 1_A & & \\ \vdots & & \ddots & \\ t_{1k}^* & t_{2k}^* & & 1_A \end{bmatrix} \begin{bmatrix} d_{11} & & & \\ & d_{22} & & \\ & & \ddots & \\ & & & d_{kk} \end{bmatrix} \begin{bmatrix} 1_A & t_{12} & \dots & t_{1k} \\ & 1_A & & t_{2k} \\ & & \ddots & \\ & & & 1_A \end{bmatrix} \\ &= \begin{bmatrix} d_{11} & d_{11}t_{12} & \dots & d_{11}t_{1k} \\ t_{12}^*d_{11} & t_{21}^*d_{11}t_{12} + d_{22} & & t_{12}^*d_{11}t_{1k} + d_{22}t_{2k} \\ \vdots & & \ddots & \\ t_{1k}^*d_{11} & & & \sum_{i=1}^k t_{ki}^* d_{ii} t_{ik} \end{bmatrix}. \end{aligned} \tag{4.1}$$

That is, in symbols

$$a_{ij} = \sum_{r=1}^{\min(i,j)} t_{ri}^* d_{rr} t_{rj}.$$

Here, the diagonal entries $t_{ii} = 1_A$.

This implies for $i \leq j$, we get

$$d_{ii} = a_{ii} - \sum_{j=1}^{i-1} t_{ji}^* d_{jj} t_{ij}. \tag{4.2}$$

$$t_{ij} = d_{ii}^{-1}\left(a_{ij} - \sum_{r=1}^{i-1} t_{ri}^* d_{rr} t_{rj}\right). \tag{4.3}$$

The two previous equations can be used to inductively generate the matrix elements d_{ii} and t_{ij} by calculating them row-wise from top to bottom. But how do we know that d_{ii}^{-1} will exist at every stage

of the induction? Let us show this by induction on i. For $i = 1$, it is clear that $a_{11} = d_{11}$ and a_{11} is positive definite since for $x \in A$, $\mathrm{tr}_A(x^* a_{11} x) = \beta_a(x, 0, 0, \ldots, 0)$ is non-negative and zero only when $x = 0$.

For the general case, let $1 \leq k' \leq k$ be an index and let us truncate Equation (4.1) at the top-left $k' \times k'$ entries. Note that any upper triangular matrix $t' \in M_{k'}(A)$ with units in the diagonal entries admits an inverse in $M_{k'}(A)$. The entries of t'^{-1} will be some non-commutative polynomials in the entries of t' which one can find inductively via "forward substitution".

With this, we can conclude that whenever we write $a' \in M_{k'}(A)$ that is symmetric and positive definite and wherever a diagonal matrix d' and a unit upper triangular matrix t' exist so that $a' = t'^* d' t'$, the diagonal entries of $d' = t'^{*^{-1}} a' t'^{-1}$ are automatically symmetric and positive definite. This follows from d' itself being symmetric and positive definite. The fact that d' is symmetric is easy to compute and to see positive definiteness, observe that for any $x, y \in M_{k'}(A)$, we get $\mathrm{tr}_{M_k(A)}(x^* d' y) = \mathrm{tr}_{M'_k(A)}((t'^{-1}x)^* a' (t'^{-1} y))$. Hence, in particular the diagonal entries of d' are invertible in A. Note that this claim is valid for all $k' \leq k$ and it will now aid us in induction.

Suppose that $\{d_{ii}\}_{i=1}^{k'}$ are positive definite. Then using Equation (4.2) and Equation (4.3), we can compute $d_{(k'+1)(k'+1)}$ and $\{t_{(k'+1)j}\}_{j \geq k'+1}$. Now note that this gives us a solution for 4.1 when k is replaced by $k' + 1$. Hence, each $\{d_{ii}\}_{i=1}^{k'+1}$ is symmetric and positive definite and in particular $d_{(k'+1)(k'+1)}$ is invertible. □

Remark 4.6. *The decomposition above is unique because the elements d_{ii} and t_{ij} are completely determined by Equation* (4.1)*.*

Remark 4.7. *It is possible to view A^k as a $(k \dim_{\mathbb{R}} A)$-dimensional vector space over $\mathbb{R}$ and all the matrices in $M_k(A)$ can be seen as block matrices with each entry a_{ij} being replaced by its left-multiplication matrix as an element of A. From this point of view, Theorem 4.5 is the same thing as the block matrix variant of the Cholesky decomposition.*

A further improvement is possible here using the proposition below.

Proposition 4.8. *Suppose that $a \in A$ is a positive definite symmetric element. Then, there exists another positive definite symmetric element $b \in A$ such that $b^2 = a$.*

Proof. Just like in the proof of Lemma 2.52, using the spectral theorem for positive definite matrices, we can construct a basis $\{e_1, e_2, \ldots, e_d\}$ of A, orthonormal with respect to $x \mapsto \mathrm{tr}(x^* x)$, such that the matrix $a_{ij} = \mathrm{tr}(e_i^* a e_j)$ is a diagonal matrix. Then the a_{ii} in the diagonal are the non-zero entries and are positive.

Note that the map $a \mapsto a_{ij}$ is a faithful representation, since the matrix a_{ij} is just the left-multiplication matrix with respect to the basis $\{e_i\}_{i=1}^d$. Moreover, in general $b \in A$ is positive definite if and only if the matrix $b_{ij} = \mathrm{tr}(e_i^* b e_j)$ is positive definite and is symmetric if and only if $b_{ij} = (b^*)_{ij} = b_{ji}^*$. In terms of this matrix representation, finding $b \in A$ such that $b^2 = a$ is the same as showing that the diagonal matrix with diagonal entries $\sqrt{a_{ii}}$ lies in the image of this representation.

To see this, note that there exists a polynomial $f(x) \in \mathbb{R}[X]$ such that $f(a_{ii}) = \sqrt{a_{ii}}$ for $i \in \{1, 2, \ldots, d\}$. Then put $b = f(a) \in A$ and this satisfies all the requirements. □

Corollary 4.9. *For every positive definite symmetric element $a \in A$, you can write it as $a = b^* b$ for some positive definite symmetric $b \in A$.*

Corollary 4.10. *Every element $a \in M_k(A)$ that is positive definite can be written in the form of*

$$a = t^* b^* b t = p^* p,$$

where $t \in M_k(A)$ is upper triangular with 1_A on the diagonal, $b \in M_k(A)$ is diagonal and $p \in M_k(A)$ is just upper triangular.

Proof. Use Theorem 4.5 and decompose a as $t^* d t$. Then each diagonal entry of d can be split as $d_{ii} = b_{ii}^* b_{ii}$ according to the previous corollary. □

4.1.2 Reduction theory of matrices over division algebras

For a positive definite symmetric quadratic form $q : \mathbb{R}^n \to \mathbb{R}$, what is the set $\{q(x)\}_{x\in\mathbb{Z}^n\setminus\{0\}}$? There is an enormous amount of literature and decades of mathematical research around this question. But one important step before proceeding anywhere is to realise when two quadratic forms for any $g \in \mathrm{GL}_n(\mathbb{Z})$, $\{q(x)\}_{x\in\mathbb{Z}^n\setminus\{0\}} = \{q(g(x))\}_{x\in\mathbb{Z}^n\setminus\{0\}}$. Hence q and $q\circ g$ are essentially the same quadratic forms as far as their values on integral points are concerned.

Reduction theory of quadratic forms generally refers to attempts at finding some suitable representative of a quadratic form modulo this equivalence. In this section, we will generalise the classical Minkowski-Siegel reduction theory of quadratic forms to the case of the types of quadratic forms we have talked about so far.

In our setting of division algebras, the integral points will be substituted by orders. We refer the reader to Section 2.2.6 for the relevant definitions and examples.

Let us state a very important lemma that we will be using shortly to prove Theorem 4.13. This is nothing but the classically known Minkowski lemma of lattice sphere packings. Eventually, we will use this to establish our reduction theory results.

Lemma 4.11. *Let V be a d-dimensional $\mathbb{R}$-vector space and let $\Lambda \subset V$ be a discrete subgroup of V that is not contained in any proper subspace of V. Choose a $\mathbb{Z}$-basis $\{v_i\}_{i=1}^d \subseteq \Lambda$ of Λ. Then there exists a constant $C > 0$ depending only on Λ and V such that for any positive definite symmetric quadratic form $q : V \to \mathbb{R}$*

$$\min_{v\in\Lambda\setminus\{0\}} q(v) \leq C\left(\det\left[q(v_i,v_j)\right]_{i,j=1,\ldots,d}\right)^{\frac{1}{d}}.$$

Proof. The constant C can be chosen as γ_d, where γ_d is the d-dimensional Hermite's constant. We sketch a quick proof that C exists.

Let us fix a positive definite quadratic form $q_0 : V \to \mathbb{R}$. Then for any $q : V \to \mathbb{R}$ in the statement, one can find an $A \in \mathrm{GL}(V)$ such that $q = q_0 \circ A$ and we check that

$$\left(\det\left[q(v_i,v_j)\right]_{i,j=1}^d\right) = \left(\det\left[q_0(v_i,v_j)\right]_{i,j=1}^d\right)(\det A)^2.$$

This means what we need to show is that there exists a constant $C' > 0$ such that

$$\min_{x\in\Lambda} q_0(Ax) \leq C'(\det A)^{2/d}.$$

If $B_r(0)$ is a ball of radius r around 0, let us define

$$B_{A,r} = A\left(B_{r(\det A)^{-1/d}}(0)\right),$$

which is the ball $B_r(0)$ after getting its radius scaled by $(\det A)^{-1/d}$ and getting transformed by the linear transformation A. Observe that $\mathrm{vol}(B_{A,r})$, which is the volume of $B_{A,r}$ measured in terms of the measure induced on V with respect to q_0, is independent of A and is equal to $\mathrm{vol}(B_r(0))$.

Then we claim that there is a choice of $r > 0$, such that for any $A \in \mathrm{GL}(V)$, $\mathrm{vol}(B_{A,r/2})$ is greater than $\mathrm{vol}(V/\Lambda)$, which is again measured in terms of q_0. Then the projection map $V \to V/\Lambda$ cannot map $B_{A,r/2}$ injectively into V/Λ and if x_1, x_2 get mapped to the same point modulo Λ, then $x_1 - x_2 \in \Lambda \cap B_{A,r} \setminus \{0\}$. Therefore, with this choice of r, we get that

$$\left(AB_{r(\det A)^{-1/d}}(0)\right) \cap \Lambda \supsetneq \{0\}, \text{ for any } A \in \mathrm{GL}(V).$$

This gives us that

$$\min_{x\in A^{-1}\Lambda} q_0(x) \leq r^2(\det A)^{-2/d}, \text{ for any } A \in \mathrm{GL}(V).$$

This last inequality is essentially what we want. □

Corollary 4.12. *Let A be a finite-dimensional real semisimple algebra and $d = \dim_{\mathbb{R}} A$. Then there exists a constant $C > 0$ depending only on $k, \mathcal{O}$ and A such that for all symmetric and positive definite $p \in M_k(A)$,*

$$\min_{v\in\mathcal{O}^k\setminus\{0\}} \beta_p(v) \leq C\,\mathrm{N}(p)^{\frac{1}{d}}.$$

Proof. To see the result, we will need to find a relation between $\mathrm{N}(p)$ and the determinant $q(v_i, v_j)$ that appears in Lemma 4.11. Choose $\{v_i\}_{i=1}^{dk}$ as needed in Lemma 4.11 as a basis of A^k residing within $\mathcal{O}^k$ (see Remark 2.59). We know that the inner product $\beta_1 : A^k \to \mathbb{R}$ induced by $1 = 1_{M_k(A)}$ is also symmetric and positive definite. Note that for any two vectors $x, y \in A^K$, $\beta_1(x, py) = \beta_p(x, y)$.

Now $\mathrm{N}(p)$ will be the determinant of the matrix $q \in M_{dk}(\mathbb{R})$ which is defined as $p(\sum_{i=1}^{dk} r_i v_i) = \sum_{i=1}^{dk}(\sum_{j=1}^{dk} q_{ij} r_j)v_i$ for all $\{r_i\}_{i=1}^{dk} \subseteq \mathbb{R}$. This implies that $\beta_p(v_i, v_j) = \sum_{r=1}^{dk} q_{rj}\beta_1(v_i, v_r)$ and consequently that

$$\det\left[\beta_p(v_i, v_j)\right] = \det\left[\beta_1(v_i, v_j)\right] \det\left[q_{ij}\right] = \det\left[\beta_1(v_i, v_j)\right] \mathrm{N}(p)^k$$

following Corollary 2.61. We then get that for some $C > 0$,

$$\min_{v \in \mathcal{O}^k \setminus \{0\}} \beta_p(v) \leq C \left(\det\left[\beta_1(v_i, v_j)\right] \mathrm{N}(p)^k\right)^{\frac{1}{dk}}.$$

Since $\det\left[\beta_1(v_i, v_j)\right]$ depends only on $k, \mathcal{O}$ and A, we are done. □

From now on, we will restrict our setting to the following. Instead of talking about a general semisimple $\mathbb{R}$-algebra, we will talk of when A is of the form[1] $D_{\mathbb{R}}$ for some $\mathbb{Q}$-division algebra D. We will now also fix an order $\mathcal{O} \subseteq D \subseteq D_{\mathbb{R}}$ and they will be the "integral points" of $D_{\mathbb{R}}$.

The following theorem is now to be stated. It is a generalisation of the classical Minkowski-Siegel reduction theorem as mentioned in [Wei58].

Theorem 4.13. *Then, there exist constants $C_1, C_2, C_3 > 0$ and a relatively compact set $\omega_0 \subseteq D_{\mathbb{R}}$ depending only on $\mathcal{O}, D_{\mathbb{R}}$ and k such that whenever there exists a positive definite symmetric element $a \in M_k(D_{\mathbb{R}})$, there exists an $m \in M_k(\mathcal{O})$ such that the following conditions are met.*

1. $|\mathrm{N}(m)| < C_3$.
2. *The Cholesky decomposition of $m^* a m = t^* d t$ satisfies*
   (a) $\frac{d_{ij}}{\mathrm{tr}(d_{ij})}$ *lies in* ω_0.
   (b) $\mathrm{tr}(d_{ii}) \leq C_1 \mathrm{tr}(d_{(i+1)(i+1)})$.
   (c) $\mathrm{tr}(t_{ij}^* t_{ij}) \leq C_2$.

Proof. The proof will be in several steps. First we will announce our candidate for m and then show that it has the properties stated above.

Candidate for m:

The construction of m is given as follows. Let $\beta_a : D_{\mathbb{R}}^k \to \mathbb{R}$ be the quadratic form associated to a. We will choose the columns of m as elements of the lattice $\mathcal{O}^k \subset D_{\mathbb{R}}^k$ in the following inductive manner. Choose $v_1 \in \mathcal{O}^k \setminus \{0\}$ such that

$$\beta_a(v_1) = \min_{v \in \mathcal{O}^k \setminus \{0\}} \beta_a(v).$$

Inductively, let $V_i = \{v_1 a_1 + v_2 a_2 + \cdots + v_i a_i \mid a_1, \ldots, a_i \in D\}$. This is a $\mathbb{Q}$-vector space for each i lying in D^k, since $\mathcal{O} \subseteq D$. Now choose v_{i+1} so that

$$\beta_a(v_{i+1}) = \min_{v \in \mathcal{O}^k \setminus V_i} \beta_a(v).$$

But why does such a v_{i+1} always exist? To see that $\mathcal{O}_K \setminus V_i$ is non-empty, it is sufficient to observe that $\dim_{\mathbb{Q}} V_i = [D : \mathbb{Q}]i$. This is because $\{v_1, \ldots, v_i\}$ are "linearly independent" over D. That is

$$v_1 a_1 + v_2 a_2 + \cdots + v_i a_i = 0 \Rightarrow a_1, a_2, \ldots, a_i = 0, \forall a_1, \ldots, a_i \in D.$$

Indeed, if the equation holds and if we take the largest index $i' \in \{1, \ldots, i\}$ such that $a_{i'} \neq 0$, then multiplying[2] $a_{i'}^{-1}$ on the right and slightly rearranging tells us that $v_{i'} \in V_{i'-1}$ (take $V_0 = \{0\}$). Hence, $\dim_{\mathbb{Q}} V_{i+1} = \dim_{\mathbb{Q}} V_i + [D : \mathbb{Q}]$ always.

[1] Why is $D_{\mathbb{R}}$ semisimple? The trace form $(a, b) \mapsto \mathrm{tr}(ab)$ is clearly non-degenerate on D. It is classically known that the trace form on a finite-dimensional k-algebra is non-degenerate if and only if it is absolutely semisimple, i.e. $A \otimes_k L$ is semisimple for any field extension L of k.

[2] This is why we can only do this theorem for division algebras.

Hence, the construction of v_i and therefore of m is well-defined. Let us now prove the claimed properties.

Proof of Condition 1:
For dimensional reasons, m will admit an inverse in $M_k(D_{\mathbb{R}})$ (but not necessarily in $M_k(\mathcal{O})$). Also, by definition of v_i, we have that

$$0 < \beta_a(v_1) \leq \beta_a(v_2) \leq \beta_a(v_3) \leq \cdots \leq \beta_a(v_k).$$

Let $m^*am = t^*dt$ be the Cholesky decomposition of $m^*am \in M_k(D_{\mathbb{R}})$ as guaranteed by Theorem 4.5. Construct an auxilary linear map $p \in M_k(D_{\mathbb{R}})$ defined by

$$m^*pm = t^* \begin{bmatrix} \frac{1}{\beta_a(v_1)} d_{11} & & & \\ & \frac{1}{\beta_a(v_2)} d_{22} & & \\ & & \ddots & \\ & & & \frac{1}{\beta_a(v_k)} d_{kk} \end{bmatrix} t. \tag{4.4}$$

Then for any $x \in \mathcal{O}^k \setminus \{0\}$, we claim that $\beta_p(x) \geq 1$. Let d' be the "diagonal" matrix between t^* and t in Equation (4.4). Indeed, suppose $x \in V_i \cap \mathcal{O}^k$ and suppose that i is the largest such index in $\{1, 2, \ldots, k\}$. Then

$$\beta_p(x) = \beta_{m^*pm}(m^{-1}x) = \beta_{t^*d't}(m^{-1}x) = \beta_{d'}(tm^{-1}x).$$

If $e_i \in D_{\mathbb{R}}^k$ is the column vector with 1_D on the ith "coordinate" and 0 elsewhere, we know that $me_i = v_i$ by design. By assumption, $x \in V_i$ and hence, for some $\{a_j\}_{j=1}^i$,

$$\begin{aligned} m^{-1}x = m^{-1}\left(\sum_{j=1}^{i} v_j a_j\right) = e_1a_1 + e_2a_2 + \cdots + e_ia_i, \\ \Rightarrow tm^{-1}x = \sum_{s=1}^{i} e_s \left(a_s + \sum_{j=s+1}^{i} t_{sj}a_j\right). \end{aligned}$$

The last expression tells us that $tm^{-1}x$ as a column vector in $D_{\mathbb{R}}^k$ is supported in the top i entries with a non-zero ith entry. Hence, it is clear that for such a vector $tm^{-1}x$, we have

$$\beta_{d'}(tm^{-1}x) \geq \frac{1}{\beta_a(v_i)}\beta_d(tm^{-1}x) = \frac{1}{\beta_a(v_i)}\beta_a(x),$$

and since $\beta_a(x) \geq \beta_a(v_i)$ for $x \in \mathcal{O}^k \cap V_i$ by definition, we get our claim that $\beta_p(x) \geq 1$.

Using the Minkowski lemma in the form of Corollary 4.12 and that $\mathrm{N}(t) = 1$ since it is the determinant of an upper triangular matrix, we get that for some constant C depending only on $k, D_{\mathbb{R}}$ and $\mathcal{O}$,

$$1 \leq C\,\mathrm{N}(p) = C\,\mathrm{N}(m)^{-2}\prod_{i=1}^{k}\frac{\mathrm{N}_{D_{\mathbb{R}}}(d_{ii})}{\beta_a(v_i)^d},$$

which shows that

$$\mathrm{N}(m)^2 \leq C\prod_{i=1}^{k}\frac{\mathrm{N}_{D_{\mathbb{R}}}(d_{ii})}{\beta_a(v_i)^d}, \tag{4.5}$$

where $d = \dim_{\mathbb{R}} D_{\mathbb{R}}$. We can now show that each of the factors of the right side are bounded. To see this, observe

$$\begin{aligned} \beta_a(v_i) = \beta_a(me_i) = \beta_{m^*am}(e_i) \\ = \beta_{t^*dt}(e_i) = \mathrm{tr}_{D_{\mathbb{R}}}(d_{ii}) + \sum_{j=1}^{i-1}\mathrm{tr}_{D_{\mathbb{R}}}(t_{ji}^* d_{jj} t_{ji}) \geq \mathrm{tr}_{D_{\mathbb{R}}}(d_{ii}). \end{aligned} \tag{4.6}$$

From the norm-trace inequality of Lemma 2.51, it follows that $\frac{1}{d}\beta_a(v_i) \geq \mathrm{N}(d_{ii})^{\frac{1}{d}}$, where $d = \dim_{\mathbb{R}} D_{\mathbb{R}}$. This implies that for another constant C' depending only on $k, D_{\mathbb{R}}$ and $\mathcal{O}$, we can have that $\beta_a(v_i)^d \geq C'\,\mathrm{N}(d_{ii})$.

This tells us that overall the norm $\mathrm{N}(m)$ must be bounded. Hence, we get the first property of m that we claimed.

Proof of Condition 2a:
For the next statement, notice that the left side of inequality in (4.5) is a positive integer and is therefore ≥ 1 (the norm is non-zero since m is invertible). Since we saw that each factor $\frac{\mathrm{N}_{D_{\mathbb{R}}}(d_{ii})}{\beta_a(v_i)^d} = \mathrm{N}\left(\frac{d_{ii}}{\beta_a(v_i)}\right)$ is bounded above by $\frac{1}{C'}$ and since their product is bounded below by $\frac{1}{C}$ according to (4.5), we get that

$$\frac{1}{C} \leq \prod_{j=1}^{k} \mathrm{N}\left(\frac{d_{jj}}{\beta_a(v_{jj})}\right) \leq \mathrm{N}\left(\frac{d_{ii}}{\beta_a(v_i)}\right) \frac{1}{(C')^{k-1}},$$

and so $\mathrm{N}\left(\frac{d_{ii}}{\beta_a(v_i)}\right) \geq C''$ for some constant $C'' > 0$.

Hence, we can conclude the following by using Equation (4.6).

$$\frac{1}{C''d^d}\,\mathrm{N}(d_{ii}) \geq \left(\frac{\beta_a(v_i)}{d}\right)^d \geq \left(\frac{\mathrm{tr}(d_{ii})}{d}\right)^d \geq \mathrm{N}(d_{ii}).$$

This makes d_{ii} satisfy the conditions of Lemma 2.52 and therefore we get the required conclusion about the d_{ii}.

Proof of Condition 2b:
In particular, the last inequality implies from Corollary 2.54 that for some constant $C''' > 0$,

$$C'''\,\mathrm{tr}(d_{ii}) \geq \beta_a(v_i) \geq \mathrm{tr}(d_{ii}). \tag{4.7}$$

Finally, since $\beta_a(v_{ii}) \leq \beta_a(v_{i+1,i+1})$, with this we get that

$$\mathrm{tr}(d_{ii}) \leq \beta_a(v_i) \leq \beta_a(v_{i+1,i+1}) \leq C'''\,\mathrm{tr}(d_{i+1,i+1}).$$

which is what we want.

Proof of Condition 2c:
Now let us obtain the condition on the t_{ij}, for $i < j$, we choose some $u'_1, u'_2, u'_3, \ldots, u'_i \in \mathcal{O}$, to be adjusted later, and set the vector u as defined by

$$u = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ \vdots \\ u_k \end{bmatrix} = \begin{bmatrix} 1_D & t_{12} & t_{13} & t_{14} & & t_{1k} \\ & 1_D & t_{23} & t_{24} & \cdots & t_{2k} \\ & & 1_D & t_{34} & & t_{3k} \\ & & & 1_D & & \\ & & & & \ddots & \end{bmatrix} \begin{bmatrix} u'_1 \\ u'_2 \\ u'_3 \\ \vdots \\ u'_i \\ 0 \\ \vdots \\ 0 \\ 1_D \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{4.8}$$

Here, the 1_D on the "column vector" on the right is on the jth position from the top. With this

now, observe that by the definition of v_j, we have that

$$\begin{aligned}\beta_a(v_j) \leq & \beta_a(v_j + v_1u'_1 + v_2u'_2 + \cdots + v_iu'_i)\\ = & \beta_a(me_j + me_1u'_1 + me_2u'_2 + \cdots + me_iu'_i)\\ = & \beta_{m^*am}(e_j + e_1u'_1 + e_2u'_2 + \cdots + e_iu'_i)\\ = & \beta_{t^*dt}(e_j + e_1u'_1 + e_2u'_2 + \cdots + e_iu'_i)\\ = & \beta_d(te_j + te_1u'_1 + te_2u'_2 + \cdots + te_iu'_i)\\ = & \beta_d(u)\\ = & \sum_{r=1}^{k} \operatorname{tr}(u_r^* d_{rr} u_r).\end{aligned}$$

Using Equation (4.6), we get that

$$\operatorname{tr}(d_{jj}) + \sum_{r=1}^{j-1} \operatorname{tr}(t_{rj}^* d_{rr} t_{rj}) \leq \sum_{r=1}^{k} \operatorname{tr}(u_r^* d_{rr} u_r).$$

From Equation (4.8), we get that the value of $u_r = t_{rj}$ for $i < r \leq j$ and thus, we can cancel those terms and get the following.

$$\sum_{r=1}^{i} \operatorname{tr}(t_{rj}^* d_{rr} t_{rj}) \leq \sum_{r=1}^{i} \operatorname{tr}(u_r^* d_{rr} u_r).$$

All of the terms on the left are positive. This implies that

$$\operatorname{tr}(t_{ij}^* d_{ii} t_{ij}) \leq \sum_{r=1}^{i} \operatorname{tr}(u_r^* d_{rr} u_r).$$

Now because Lemma 2.52 was true for each d_{ii}, and in particular, Corollary 2.54 is also true, we get that for some constant $C'_0 > 0$,

$$\operatorname{tr}(t_{ij}^* t_{ij}) \operatorname{tr}(d_{ii}) \leq C'_0 \sum_{r=1}^{i} \operatorname{tr}(u_r^* u_r) \operatorname{tr}(d_{rr}).$$

Combining this with the knowledge of Equation (4.7), we see that there is another constant $C''_0 > 0$ such that

$$\begin{aligned}\operatorname{tr}(t_{ij}^* t_{ij}) \beta_a(v_i) \leq C''_0 \sum_{r=1}^{i} \operatorname{tr}(u_r^* u_r) \beta_a(v_r) \leq \beta_a(v_i) \left(C''_0 \sum_{r=1}^{i} \operatorname{tr}(u_r^* u_r) \right)\\ \Rightarrow \operatorname{tr}(t_{ij}^* t_{ij}) \leq C''_0 \sum_{r=1}^{i} \operatorname{tr}(u_r^* u_r).\end{aligned}$$

This finally implies that $\operatorname{tr}(t_{ij}^* t_{ij})$ is bounded by a value only depending on the u_r. This in turn, depends only the choice of u'_r. But we can adjust the u'_r inductively to make the RHS bounded for whatever the t_{ij} are. Simply observe that

$$\begin{aligned}u_1 &= u'_1 + t_{12}u'_2 + t_{13}u'_3 + \cdots + t_{1i}u'_i, + t_{1j},\\ u_2 &= u'_2 + t_{23}u'_3 + \cdots + t_{2i}u'_i, + t_{2j},\\ &\vdots\\ u_i &= u_{i'} + t_{ij}.\end{aligned}$$

For $\mathcal{O} \subseteq D_{\mathbb{R}}$, there is a global constant $K > 0$ (i.e. the covering radius of $\mathcal{O} \subseteq D_{\mathbb{R}}$) such that for any $x \in D_{\mathbb{R}}$, there exists a $d \in \mathcal{O}$ such that $\operatorname{tr}((x+d)^*(x+d)) < K^2$. Using this principle, since the leftmost term for each u_r in the sum above is $u'_r \in \mathcal{O}$, we can inductively choose each u'_r starting from $r = i$ to $r = 1$ so that $\operatorname{tr}(u_r^* u_r) \leq K^2$ for each r. This way, we see that $\operatorname{tr}(t_{ij}^* t_{ij})$ is absolutely bounded. □

Remark 4.14. *The set ω_0 can be assumed to be inside $\{d \in D_{\mathbb{R}} \mid \mathrm{tr}(d) = 1\}$. This is because $\mathrm{tr}(d_{ii}/\mathrm{tr}(d_{ii})) = 1$. Furthermore, ω_0 can be chosen to be relatively compact inside $D_{\mathbb{R}}^*$, the invertible elements of $D_{\mathbb{R}}$. In particular, this means that $\{N_{D_{\mathbb{R}}}(x)\}_{x\in\omega_0}$ is bounded away from 0.*

See Remark 2.53.

We can reformulate the above using the definition of a Siegel domain.

Definition 4.15. *Given a relatively compact set $\omega_0 \subseteq D_{\mathbb{R}}$ and two constants $C_1, C_2 > 0$, then we define a Siegel domain*

$$\begin{aligned}\mathfrak{S} = \mathfrak{S}_{\omega_0,C_1,C_2} =\{&a \in M_k(D_{\mathbb{R}}) \mid a \text{ is symmetric positive definite}\\ &\text{whose Cholesky decomposition } a = t^*dt \text{ satisfies}\\ &\text{conditions (a), (b) and (c) of Theorem 4.13}\}.\end{aligned} \tag{4.9}$$

In this context, what Theorem 4.13 tells us is that there exists a Siegel domain $\mathfrak{S}$ such that, for any positive definite symmetric $a \in M_k(D_{\mathbb{R}})$ an integral matrix m of bounded norm can make $m^*am \in \mathfrak{S}$.

However, we can do a small correction to replace m with $m'b$, where m' is such that $\mathrm{N}(m') = 1$ and b is among finitely many candidates in $M_k(\mathcal{O})$. This will soon be useful while dealing with groups in the upcoming parts.

Lemma 4.16. *Given a constant $C > 1$, we can find finitely many elements $b_1, b_2, b_3, \ldots, b_m \in M_k(D)$ such that any $b \in M_k(\mathcal{O})$ with $1 \le |\mathrm{N}(b)| \le C$ can be written as $b = b'b_i$ for some i, with $\mathrm{N}(b') = 1$.*

Proof. First, we will do this under the assumption that $D = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$. What we will really prove, is that the set

$$M_t = \{a \in M_k(\mathbb{Z}) \mid \det(a) = t\} \subseteq \mathrm{GL}_k(\mathbb{Q})$$

for some fixed $t \in \mathbb{Z}$ is contained in finitely many $\mathrm{GL}_k(\mathbb{Z})$-orbits of the left-action of it on $\mathrm{GL}_k(\mathbb{Q})$. Indeed, this is sufficient because if $\bigcup_{i=1}^{m_t} \mathrm{GL}_k(\mathbb{Z})b_i^t \supseteq M_t$, then $\bigcup_{t=1}^{C}\{\pm b_i^t\}_{i=1}^{m_t}$ can be the set of representatives we need (noting here that elements of $\mathrm{GL}_k(\mathbb{Z})$ have determinant ± 1).

Then we recall that there exists a Smith decomposition over $\mathbb{Z}$, so that any $b \in M_t$ can be written as $b = xdy$ for $x, d, y \in M_k(\mathbb{Z})$ with $\det(x) = \det(y) = 1$ and d a diagonal matrix with $\det(d) = \prod_{i=1}^{k} d_{ii} = t$. Consider the projection map $\pi_t : M_k(\mathbb{Z}) \to M_k(\mathbb{Z}/t\mathbb{Z})$ and choose representatives $c_1, c_2, \ldots, c_{m_t} \in \mathrm{GL}_k(\mathbb{Z})$ such that $\{\pi_t(c_i)\}_{i=1}^{m_t} = \mathrm{GL}_k(\mathbb{Z}/t\mathbb{Z})$. Then clearly, for the y in the decomposition $b = xdy$, $\pi_t(y)$ is also invertible, and therefore $y = y'c_i$ for some $i \in \{1, \ldots, m_t\}$ with $\pi_t(y') = 1_{\mathrm{GL}_k(\mathbb{Z}/t\mathbb{Z})}$. Then finally $b = xdy = xdy'c_i = (xdy'd^{-1})dc_i$. Now we claim that $dy'd^{-1} \in \mathrm{GL}_k(\mathbb{Z})$. Indeed, $(dy'd^{-1})_{ij} = y'_{ij}d_{ii}/d_{jj}$, and for $i \neq j$, y'_{ij} is a multiple of t but d_{jj} divides t (since $\prod_{i=1}^{k} d_{ii} = t$). Hence, setting $b_i = dc_i$ settles our claim for the case of $D = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$.

For the general setting, recall the faithful morphism $\pi : M_k(\mathcal{O}) \to M_{kd}(\mathbb{Z})$, where $d = [D_{\mathbb{R}} : \mathbb{Q}]$, as mentioned in Remark 2.59. Observe that $\pi^{-1}(\mathrm{GL}_{kd}(\mathbb{Q})) = \mathrm{GL}_k(D)$ and $\pi^{-1}(\mathrm{GL}_{kd}(\mathbb{Z})) = \mathrm{GL}_k(\mathcal{O})$. We must keep in mind that an alternative description of $\mathrm{GL}_k(\mathcal{O})$ is the set of units in $M_k(\mathcal{O})$. Then the following diagram commutes. The vertical maps are inclusions.

$$\begin{array}{ccc} \mathrm{GL}_k(D) & \xrightarrow{\pi} & \mathrm{GL}_{kd}(\mathbb{Q}) \\ \uparrow & & \uparrow \\ \mathrm{GL}_k(\mathcal{O}) & \xrightarrow{\pi} & \mathrm{GL}_{kd}(\mathbb{Z}) \end{array}$$

Now note that for any $b \in M_k(D) = \pi^{-1}(M_{kd}(\mathbb{Z}))$, we have that $\mathrm{N}(b) = \det(\pi(b))^k$ from Corollary 2.61. Hence, the condition $1 \le |\mathrm{N}(b)| \le C$ translates to the requirement that $1 \le |\det(\pi(b))| \le C^k$. Therefore, it is clear that the set $\{\pi(b)\}_{1\le \mathrm{N}(b)\le C} \subset \mathrm{GL}_{kd}(\mathbb{Q})$ is contained in finitely many cosets of $\mathrm{GL}_{kd}(\mathbb{Z})$. Hence, we can find finitely many $b_1, \ldots, b_n \in \mathrm{GL}_k(D)$ such that $\{\pi(b)\}_{1\le \mathrm{N}(b)\le C} \subseteq \bigcup_{i=1}^{n} \mathrm{GL}_{kd}(\mathbb{Z})\pi(b_i)$. But note that $\pi^{-1}(\mathrm{GL}_{kd}(\mathbb{Z})\pi(b_i)) = \mathrm{GL}_k(\mathcal{O})b_i$, because if $\pi(bb_i^{-1}) \in \mathrm{GL}_{kd}(\mathbb{Z})$, then $bb_i^{-1} \in \mathrm{GL}_k(\mathcal{O})$. Hence, we get that

$$\{b \in M_k(\mathcal{O}) \mid 1 \le |\mathrm{N}(b)| \le C\} \subseteq \bigcup_{i=1}^{n} \mathrm{GL}_k(\mathcal{O})b_i$$

and therefore, $\{\pm b_i\}_{i=1}^{n}$ is the set that we need. □

Remark 4.17. *The function* $\det \circ \pi : M_k(D_{\mathbb{R}}) \to \mathbb{R}$ *seen above is often also called the reduced norm. The usual norm* N *is just the* k*th power of the reduced norm.*

Remark 4.18. *Unlike Theorem 4.13, there is nothing special about being in a division algebra in Lemma 4.16. This particular lemma can be suitably generalised by substituting* $D_{\mathbb{R}}$ *with a semisimple* $\mathbb{R}$*-algebra* A*.*

4.2 Integration coordinates

Recall that we want to consider the quotient space $\mathcal{G}(\mathbb{R})/\Gamma$ where

$$\begin{aligned}\mathcal{G}(\mathbb{R}) &= \{a \in M_t(D_{\mathbb{R}}) \mid \mathrm{N}(a) = 1\},\\ \Gamma &= \{a \in M_t(\mathcal{O}) \mid \mathrm{N}(a) = 1\}.\end{aligned}$$

We want to describe an integration on $\mathcal{G}(\mathbb{R})$ that is equal to integrating with respect to the Haar measure up to scaling. For that, we will use an analogue of the Iwasawa decomposition for $\mathrm{SL}_t(D_{\mathbb{R}})$. Optically, it might look very similar to the Iwasawa decomposition seen for $\mathrm{SL}_t(\mathbb{R})$ but see Remark 4.22 for a clear difference where the analogy fails.

Let us first define the following notations.

Definition 4.19. *We define the following.*

$$\begin{aligned}K &= \{\kappa \in \mathcal{G}(\mathbb{R}) \mid \kappa^*\kappa = 1_{M_k(A)}, \mathrm{N}(\kappa) = 1\},\\ A_0 &= \{a \in \mathcal{G}(\mathbb{R}) \mid a \textit{ is diagonal}, a_{ii} \textit{ invertible}, \mathrm{N}(a_{ii}) > 0\},\\ N &= \{n \in \mathcal{G}(\mathbb{R}) \mid n \textit{ is upper triangular with } 1_A \textit{ on the diagonal entries}\}.\end{aligned}$$

Topologically, $\mathcal{G}(\mathbb{R})$ is a Lie group and the groups K, A_0, N are also Lie group topologies as closed subgroups of $\mathcal{G}(\mathbb{R})$. Note that $A_0 \subseteq \mathcal{G}(\mathbb{R})$, so $a \in A_0 \Rightarrow \mathrm{N}(a) = 1$.

Proposition 4.20. *The following map is a surjective open map. As a smooth map, it is a submersion.*

$$\begin{aligned}K \times A_0 \times N &\to \mathcal{G}(\mathbb{R})\\ (\kappa, a, n) &\mapsto \kappa a n.\end{aligned}$$

Proof. First, let us see that this multiplication map is surjective.

For any $g \in \mathcal{G}(\mathbb{R})$, we know that $g^*g \in M_t(D_{\mathbb{R}})$ is a positive definite symmetric matrix. Consequently, by Theorem 4.5 and Corollary 4.10, we have a decomposition $g^*g = n^*a^*an = (an)^*an$, for $n \in N$ and a being some diagonal matrix. Clearly $N(a) = \pm 1$ for this to hold, but since a can be assumed to be positive definite in Corollary 4.10, we can ensure that $N(a_{ii}) > 0$ and so, $a \in A_0$. Now $g(an)^{-1} = (g^*)^{-1}(an)^*$ which means that $g(an)^{-1}$ is preserved under the "conjugate inverse" automorphism, so it lies in K. So, $g = \kappa an$ for some $\kappa \in K$.

Using the following transportation scheme, we can see that the given map has a constant rank. The following commutative diagram demonstrates that the rank at (κ, a, n) is the same as the rank at $(1, 1, 1)$, wherein the vertical arrows are the derivatives of the respective indicated maps and are therefore isomorphisms of tangent spaces.

$$\begin{array}{ccc}
\big(\kappa\kappa', a'a, (a^{-1}n'a)n\big) & T_{(\kappa,a,n)}(K \times A_0 \times N) \longrightarrow T_{\kappa an}\mathcal{G}(\mathbb{R}) & \kappa g a n \\
\uparrow & \uparrow \qquad\qquad \uparrow & \uparrow \\
(\kappa', a', n') & T_{(1,1,1)}(K \times A_0 \times N) \longrightarrow T_1\mathcal{G}(\mathbb{R}) & g
\end{array}$$

To learn what the rank on $(1, 1, 1)$ is, we note that on the level of Lie algebras the lower horizontal map in the diagram, up to appropriate identifications, is just the addition map. More precisely, we can make the identification of $T_{(1,1,1)}(K \times A_0 \times N) \simeq T_1K \times T_1A_0 \times T_1N$ and identifying $T_1\mathcal{G}(\mathbb{R}), T_1K, T_1A_0$ and T_1N as subspaces of $T_1 \mathrm{GL}_t(D_{\mathbb{R}}) \simeq M_t(D_{\mathbb{R}})$ as follows.

$$\begin{aligned} T_1\mathcal{G}(\mathbb{R}) &= \{g \in M_t(D_{\mathbb{R}}) \mid \mathrm{tr}(g) = 0\}, \\ T_1K &= \{\kappa \in M_t(D_{\mathbb{R}}) \mid \kappa^* + \kappa = 0\}, \\ T_1A_0 &= \{a \in M_t(D_{\mathbb{R}}) \mid a \text{ is diagonal}, \mathrm{tr}(a) = 0\}, \\ T_1N &= \{n \in M_t(D_{\mathbb{R}}) \mid n \text{ is strictly upper triangular }\}. \end{aligned}$$

Since every traceless matrix in $M_t(D_{\mathbb{R}})$ can be written as the sum of matrices in the three subspaces above, the bottom map is surjective and hence overall, the given map is a submersion using the global rank theorem of differential geometry as follows.

To see that it is an open map, it is sufficient to show that the image $U_1U_2U_3 \subseteq G$ of a basic open set of the product topology $U_1 \times U_2 \times U_3 \subseteq K \times A_0 \times N$ is open[3]. For this goal, it is sufficient to show this when $U_1 \times U_2 \times U_2$ is a sufficiently small neighbourhood of the identity $(1,1,1) \in K \times A_0 \times N$ as we can transport such a neighbourhood and a get a neighbourhood $(\kappa, a, n) \in K \times A_0 \times N$ of the form $\kappa U_1 \times U_2 a \times (a^{-1}U_3 a)n$, whose image must be $\kappa U_1U_2U_3an \subseteq \mathrm{GL}_t(A)$. For this, it is also sufficient to show that the given multiplication map restricted to $U_1 \times U_2 \times U_3$ is an open map for sufficiently small U_1, U_2, U_3.

We can use the constant rank theorem of differential geometry now. Let $F : K \times A_0 \times N \to \mathcal{G}(\mathbb{R})$ be the given multiplication map. If U_1, U_2, U_3 are sufficiently small, then there exists an open neighbourhood $U_1' \times U_2' \times U_3' \subseteq T_1K \times T_1A_0 \times T_1N$ of $(0,0,0)$ with homeomorphisms $u_i : U_i \to U_i'$ for $i \in \{1,2,3\}$ and an open neighbourhood $V \subseteq \mathcal{G}(\mathbb{R})$ containing identity along with a homeomorphism $v : V \to V' \subseteq T_1\mathcal{G}(\mathbb{R})$, V' containing 0, such that the map $F|_{U_1 \times U_2 \times U_3} = v^{-1} \circ dF_{(e,e,e)} \circ u$, where the map $u = u_1 \times u_2 \times u_3 : U_1 \times U_2 \times U_3 \to U_1' \times U_2' \times U_3'$. But $dF_{(1,1,1)}$ is an open map, because it is a surjective linear map and hence, we are done. □

Corollary 4.21. *Let $B = A_0N = NA_0 \subset \mathcal{G}(\mathbb{R})$ be the closed subgroup of upper-triangular matrices. Then the following is also an open surjective map.*

$$\begin{aligned} K \times B &\to \mathcal{G}(\mathbb{R}) \\ (\kappa, b) &\mapsto \kappa b. \end{aligned}$$

Proof. Surjectivity is clear from Proposition 4.20 if we write $b = an$ for some $n \in N$ and $a \in A_0$. To show that the map is open, the proof is very similar to Proposition 4.20 and we leave this to the reader for verification. □

Remark 4.22. *The map in Proposition 4.20 is generally not injective. Indeed, if $\kappa' \in K \cap A_0$, then $(\kappa\kappa'^{-1}, \kappa' a, n)$ and (κ, a, n) are mapped to the same element $\kappa an \in \mathcal{G}(\mathbb{R})$.*

This is the only obstruction to injectivity. That's to say that, two elements of $K \times A_0 \times N$ have the same image if and only if they are in the above situation.

Note that in the usual Iwasawa decomposition for $\mathrm{SL}_t(\mathbb{R})$, the map is indeed injective since $K \cap A_0 = \{1_{\mathrm{SL}_k(\mathbb{R})}\}$.

We will now use the following proposition to settle some more technicalities about our decomposition above.

Proposition 4.23. *1. $K \subset \mathcal{G}(\mathbb{R})$ is a compact group.*

2. $K \cap B = K \cap A_0$, which is also a compact subgroup of $\mathcal{G}(\mathbb{R})$.

Proof. 1. K is at most an index-2 subgroup of $\{a \in M_t(D_{\mathbb{R}}), a^*a = 1_{M_k(\mathbb{R})}\}$. The compactness of this group follows from the following more general claim.

Let A be a semisimple algebra with a positive involution *, then the group $\{a \in A \mid a^*a = 1_A\}$ must be a compact group in the induced topology from A. Indeed, it is a closed group that lives inside the compact ball $\{a \in A \mid \mathrm{tr}_A(a^*a) \leq [A : \mathbb{R}]\}$.

[3] for any continuous map of topological spaces $f : X \to Y$, $f(\bigcup_{i \in I} U_i) = \bigcup_{i \in I} f(U_i)$.

2. We see that if $\kappa \in K \cap A_0 N$ then $\kappa = an$ has to be an upper triangular matrix such that $\kappa^*\kappa = 1_{\mathcal{G}(\mathbb{R})}$. As a matrix, what this means is that

$$\begin{bmatrix} 1_{D_\mathbb{R}} & & & \\ & 1_{D_\mathbb{R}} & & \\ & & \ddots & \\ & & & 1_{D_\mathbb{R}} \end{bmatrix} = \begin{bmatrix} \kappa_{11}^* & & & \\ \kappa_{12}^* & \kappa_{22}^* & & \\ & \vdots & \ddots & \\ \kappa_{1t}^* & \kappa_{2t}^* & & \kappa_{tt}^* \end{bmatrix} \begin{bmatrix} \kappa_{11} & \kappa_{12} & \dots & \kappa_{1t} \\ & \kappa_{22} & & \kappa_{2t} \\ & & \ddots & \\ & & & \kappa_{tt} \end{bmatrix}$$
$$= \begin{bmatrix} \kappa_{11}^*\kappa_{11} & \kappa_{11}\kappa_{12} & \dots & \kappa_{11}\kappa_{1t} \\ \kappa_{12}^*\kappa_{11} & \kappa_{12}^*\kappa_{12} + \kappa_{22}^*\kappa_{22} & & \kappa_{12}^*\kappa_{1t} + \kappa_{22}\kappa_{2t} \\ \vdots & & \ddots & \\ \kappa_{1t}^*\kappa_{11} & & & \sum_{i=1}^t \kappa_{ti}^*\kappa_{it} \end{bmatrix}.$$

We will show that $\kappa_{ij} = 0$ for $i < j$. When $i = 1$, we see that $\kappa_{11}^*\kappa_{11} = 1_A$, so κ_{11} is invertible and therefore, from the first row above, we see that $\kappa_{11}\kappa_{1j} = 0 \Rightarrow \kappa_{1j} = 0$ for $j > 1$. This makes the entire first row of κ, except κ_{11} to be 0. This reduces the case to a $(t-1) \times (t-1)$ upper triangular matrix satisfying the same matrix equality as above. Hence, we can show the rest of the entries 0 by induction.

Now $K \cap A_0 \simeq \{a \in D_\mathbb{R} \mid a^*a = 1_{D_\mathbb{R}}\}^{\oplus k}$ as a topological group. From the discussion of the previous part, it is compact.

□

One last piece of the puzzle describes something special about Haar measure on $\mathcal{G}$.

Proposition 4.24. *The group $\mathcal{G}(\mathbb{R})$ is unimodular. That is, a left-invariant Haar measure is also right-invariant.*

Proof. First, observe that the group $\mathrm{GL}_t(D_\mathbb{R})$ is unimodular.

$\mathrm{GL}_t(D_\mathbb{R})$ is an open subset of $M_t(D_\mathbb{R})$. This is because for any $u \in \mathrm{GL}_t(D_\mathbb{R})$ and $u' \in M_t(D_\mathbb{R})$, $u + \nu u' = u(1 + \nu u^{-1}u')$ is invertible if $\nu \in \mathbb{R}$ satisfies $|\nu|^2 \operatorname{tr}((u^{-1}u')^*(u^{-1}u')) < 1$. Hence, any Lebesgue measure da of $M_t(D_\mathbb{R})$ can be restricted to get a measure da on $\mathrm{GL}_t(D_\mathbb{R})$. Now set $dg = |\operatorname{N}(a)|^{-1} da$. This measure is in fact both left and right invariant. Indeed, this is because the determinant of the left-multiplication of $a \in M_t(D_\mathbb{R})$ is the same as that of the right-multiplication, both being equal to $|\operatorname{N}(a)|$.

Now on $\mathcal{G}(\mathbb{R}) = \mathrm{SL}_t(D_\mathbb{R})$, we can induce a Haar measure as follows. For any open set $U \subseteq G$, consider the set $(0,1]U = \bigcup_{t \in (0,1]} tU \subseteq \mathrm{GL}_t(D_\mathbb{R})$ and define $\mu_G(U) = \int_{(0,1]U} dg$. This defines a Haar measure on G that is both left-invariant and right-invariant. □

We are now ready to describe a coordinate system to integrate some scaling of the Haar measure on $\mathcal{G}(\mathbb{R})$. Here is a definition to set us up for the discourse.

Definition 4.25. *For any topological space X, we will denote the vector space of compactly supported continuous $\mathbb{R}$-functions on X as $\mathcal{C}_c(X)$.*

Proposition 4.26. *Let $d\kappa, da, dn$ be Haar measures on K, A_0, N respectively. Then the following is a Haar measure on $\mathcal{G}(\mathbb{R})$.*

$$\mathcal{C}_c(\mathcal{G}(\mathbb{R})) \to \mathbb{R}$$
$$f \mapsto \int_N \int_{A_0} \int_K f(\kappa a n) \left(\prod_{i<j} \frac{|\operatorname{N}(a_{ii})|}{|\operatorname{N}(a_{jj})|} \right) d\kappa da dn.$$

Proof. We use the following classically known lemma. See [Kna13] for a proof.

Lemma 4.27. *Let G' be a Lie group. Let S, T be closed subgroups such that $S \cap T$ is compact and the multiplication $S \times T \to G'$ is an open map whose image is surjective (except possibly a measure*

0 subset of G'). Let Δ_T and $\Delta_{G'}$ denote the modular functions of T and G'. Then the following is a Haar measure on G'.

$$\begin{aligned} \mathcal{C}_c(G') &\to \mathbb{R} \\ f &\mapsto \int_{S\times T} f(st)\frac{\Delta_T(t)}{\Delta_{G'}(t)}dsdt. \end{aligned}$$

We will use this lemma twice. First with $(G', S, T) = (\mathcal{G}(\mathbb{R}), K, B)$, which fits due to Corollary 4.21 and Proposition 4.23, and then $(G', S, T) = (B, A_0, N)$ which fits because $A_0 \cap N = \{1_{\mathcal{G}(\mathbb{R})}\}$ and $(a, n) \mapsto an$ is an open map. Then, we get that the following is a Haar integral for $f \in \mathcal{C}_c(\mathcal{G}(\mathbb{R}))$.

$$\begin{aligned} \int_{K\times B} f(\kappa b)\frac{\Delta_B(b)}{\Delta_{\mathcal{G}(\mathbb{R})}(b)}d\kappa db &= \int_B \left(\int_K f(\kappa b)\frac{\Delta_B(b)}{\Delta_{\mathcal{G}(\mathbb{R})}(b)}d\kappa\right) db \\ &= \int_N \int_{A_0} \left(\int_K f(\kappa an)\frac{\Delta_B(an)}{\Delta_{\mathcal{G}(\mathbb{R})}(an)}d\kappa\right)\frac{\Delta_N(n)}{\Delta_B(n)}dadn \\ &= \int_N \int_{A_0}\int_K f(\kappa an)\Delta_B(a)d\kappa dadn. \end{aligned}$$

Here, for the last equality we have used that $\mathcal{G}(\mathbb{R})$ and N are unimodular, that is $\Delta_{\mathcal{G}(\mathbb{R})}, \Delta_N$ are trivial. $\mathcal{G}(\mathbb{R})$ is unimodular by Proposition 4.24 and N is unimodular because it is nilpotent[4]. Finally, we use the following identity that is classically known and also given in [Kna13].

$$\Delta_B(a) = |\det \mathrm{Ad}_B(b)|,$$

where $\mathrm{Ad}_B : B \to \mathrm{GL}(T_1B)$ is the adjoint representation of B. Identify

$$T_1B = \{m \in M_t(D_\mathbb{R}) \mid \mathrm{tr}(m) = 0, m \text{ is upper triangular}\}.$$

Then, clearly $(ama^{-1})_{ij} = a_{ii}n_{ij}a_{jj}^{-1}$. Since determinant of right multiplication and left multiplication on $D_\mathbb{R}$ is the same, we get

$$\Delta_B(a) = \prod_{i<j}\left|\frac{N(a_{ii})}{N(a_{jj})}\right|.$$

□

Let $D_\mathbb{R}^{(1)}$ denote the kernel of $\mathrm{N} : D_\mathbb{R}^* \to \mathbb{R}^*$. In other words, $D_\mathbb{R}^{(1)}$ is the set of unit norm elements of $D_\mathbb{R}$.

Definition 4.28. *The group A_0 as defined in Definition 4.19 can be further decomposed as $A_0 = A^{(1)}A^\mathbb{R}$ where*

$$\begin{aligned} A^{(1)} &= \{a \in \mathcal{G}(\mathbb{R}) \mid i \neq j \Rightarrow a_{ij} = 0, \mathrm{N}(a_{ii}) = 1\}, \\ A^\mathbb{R} &= \{a' \in \mathcal{G}(\mathbb{R}) \mid i \neq j \Rightarrow a'_{ij} = 0, a'_{ii} \in \mathbb{R}_{>0} \subseteq D_\mathbb{R}\}. \end{aligned}$$

Note that $A^\mathbb{R} \cap A^{(1)} = \{1_D\}$. This decomposition is simply a consequence of writing

$$a_{ii} = N(a_i)^{1/d}\left(a_{ii}N(a_{ii})^{-1/d}\right),$$

where $d = [D_\mathbb{R} : \mathbb{R}]$ so that $a_{ii}N(a_{ii})^{-1/d}$ is of norm one.

Remark 4.29. *The group $A^\mathbb{R}$ is the identity component of a maximal $\mathbb{Q}$-torus of G. This agrees with Chapter 18.5 of [Mor15], where the $\mathbb{Q}$-rank of $\mathrm{SL}_t(D)$ is mentioned as $(t-1)$, which is exactly the rank of this torus.*

[4] Alternatively, one can check this through the identity $\Delta_N(n) = |\det \mathrm{Ad}(n)|$.

Corollary 4.30. *Let $d\kappa$, da', da, dn be Haar measures on $K, A^{\mathbb{R}}, A^{(1)}, N$ respectively. Then, the following is a Haar measure on $\mathcal{G}(\mathbb{R})$.*

$$\begin{aligned}&\mathcal{C}_c(\mathcal{G}(\mathbb{R})) \to \mathbb{R}\\ &f \mapsto \int_N \int_{A^{(1)}} \int_{A^{\mathbb{R}}} \int_K f(\kappa a' a n) \left(\prod_{i<j} \frac{a'_{ii}}{a'_{jj}}\right)^d d\kappa da' da dn.\end{aligned}$$

Remark 4.31. *It should be possible to generalise this treatment of Haar measure to the setting of a general semisimple algebra A instead of $D_{\mathbb{R}}$ by meaningfully defining groups like $\mathrm{GL}_t(A)$, $\mathrm{SL}_t(A)$ and so on.*

4.3 Integration on $\mathcal{G}(\mathbb{R})/\Gamma$

Observe that $\mathcal{O}^k \subseteq D_{\mathbb{R}}^k$ is a lattice that remains invariant under the action of elements of the group $\Gamma \subseteq G$. Hence, we can make the following identification of topological measure spaces.

$$\mathcal{G}(\mathbb{R})/\Gamma \simeq \{g\mathcal{O}^k \mid g \in G\}.$$

We will shortly show that this measure space has a finite measure by performing an explicit computation in terms of the integration coordinates defined above.

Recall that in Section 4.1, we defined a Siegel domain in Definition 4.15. We will now make a more useful version of a Siegel domain $\mathfrak{S}^* \subset \mathcal{G}(\mathbb{R})$, one that we can fit inside $\mathcal{G}(\mathbb{R})$ and such that $\mathfrak{S}^*\Gamma = \mathcal{G}(\mathbb{R})$. This $\mathfrak{S}^*$ shall be a Siegel domain of matrices, whereas the previous definition $\mathfrak{S}$ was a Siegel domain of quadratic forms.

Definition 4.32. *Let $\omega_1 \subseteq D_{\mathbb{R}}^{(1)}$ be a relatively compact set and let $c_1, c_2 > 0$. Also, let $b_1, b_2, \ldots, b_m$ be some elements of $\mathrm{GL}_t(D)$. Recall the definition of K, A_0, N and $A^{(1)}, A^{\mathbb{R}}$ as defined in Definition 4.19 and Definition 4.28.*

$$\begin{aligned}
\underline{A}^{\mathbb{R}} &= \{a \in \mathrm{GL}_t(D_{\mathbb{R}}) \mid a'_{ij} = 0 \text{ for } i \neq j, a'_{ij} \in \mathbb{R}_{>0} \subset D_{\mathbb{R}}\},\\
A^{(1)}_{\omega_1} &= \{a \in A^{(1)} \mid a_{ii} \in \omega_1\},\\
A^{\mathbb{R}}_{c_1} &= \{a' \in A^{\mathbb{R}} \mid a'_{ii} \in \mathbb{R}^{>0} \subseteq D_{\mathbb{R}}, a'_{ii} \leq c_1 a'_{i+1,i+1}\},\\
\underline{A}^{\mathbb{R}}_{c_1} &= \{a' \in \underline{A}^{\mathbb{R}} \mid a'_{ii} \in \mathbb{R}_{>0} \subset D_{\mathbb{R}}, a'_{ii} \leq c_1 a'_{i+1,i+1}\},\\
N_{c_2} &= \{n \in G \mid n \text{ is upper triangular with } 1_D \text{ on diagonals }, \mathrm{tr}(n^*_{ij} n_{ij}) < c_2\},\\
\mathfrak{S}^1 &= \mathfrak{S}^1_{\omega_1,c_1,c_2} = K A^{(1)}_{\omega_1} \underline{A}^{\mathbb{R}}_{c_1} N_{c_2},\\
\mathfrak{S}^* &= \mathfrak{S}^*_{\omega_1,c_1,c_2} = \left(\bigcup_{i=1}^m \mathfrak{S}^1 b_i^{-1}\right) \cap \mathcal{G}(\mathbb{R}) = \bigcup_{i=1}^m \mathrm{N}(b_i)^{\frac{1}{dt}} (K A^{(1)}_{\omega_1} A^{\mathbb{R}}_{c_1} N_{c_2}) b_i^{-1}.
\end{aligned}$$

Here, $d = [D : \mathbb{Q}]$.

We can now relate this to the previously discussed generalisation of Minkowski-Siegel, i.e. Theorem 4.13.

Lemma 4.33. *For some choice of ω_1, c_1, c_2 in the definition above and for some choice of $b_1, b_2, \ldots, b_m \in \mathrm{GL}_k(D)$, the set $\mathfrak{S}^* \subseteq \mathcal{G}(\mathbb{R})$ from Definition 4.32 satisfies $\mathfrak{S}^*\Gamma = \mathcal{G}(\mathbb{R})$. In other words, $\mathfrak{S}^* \subseteq \mathcal{G}(\mathbb{R})$ surjects via the map $\mathcal{G}(\mathbb{R}) \to \mathcal{G}(\mathbb{R})/\Gamma$.*

Proof. What we want to really show is that for some choice of $\mathfrak{S}^*$, for every $g \in \mathcal{G}(\mathbb{R})$, there will exist some $b \in \Gamma$ such that $gb \in \mathfrak{S}^*$.

Let $\mathfrak{S} = \mathfrak{S}_{\omega_0,C_1,C_2} \subset M_t(D_{\mathbb{R}})$ be the set defined in Equation (4.9), where ω_0, C_1, C_2 are chosen such that they satisfy conditions of Theorem 4.13 for the given choice of $D_{\mathbb{R}}, \mathcal{O}$ and t. Consider the map $F : g \mapsto g^* g$. We claim that there is a choice of ω_1, c_1, c_2 such that

$$\mathfrak{S}_{\omega_0,C_1,C_2} \subseteq F(K A^{(1)}_{\omega_1} \underline{A}^{\mathbb{R}}_{c_1} N_{c_2}).$$

Let $C', C > 0$ be such that $C' \geq \mathrm{N}(h) \geq C$ for all $h \in \omega_0$ (See Remark 4.14). Set

$$\omega_1 = \{a \in D_{\mathbb{R}}^{(1)} \mid \tfrac{a^*a}{\mathrm{tr}(a^*a)} \in \omega_0\}.$$

This is a compact set because $a \in \omega_1$ implies that

$$\mathrm{N}\left(\frac{a^*a}{\mathrm{tr}(a^*a)}\right) = \frac{1}{\mathrm{tr}(a^*a)^d} \in \mathrm{N}(\omega_0) \Rightarrow (C')^{\frac{1}{d}} \leq \mathrm{tr}(a^*a) \leq C^{\frac{1}{d}}.$$

Now set $c_1 = \sqrt{C_1(C'/C)^{\frac{1}{d}}}$ and $c_2 = C_2$. Let $t^*dt \in \mathfrak{S}_{\omega_0,C_1,C_2}$ where t^*dt is the Cholesky decomposition, then $t \in N_{c_2}$. Write $d = a'a$ uniquely for $a' \in \underline{A}^{\mathbb{R}}$ and $a \in A^{(1)}$. Then

$$\begin{aligned}
&\frac{d_{ii}}{\mathrm{tr}(d_{ii})} = \frac{(a_{ii}^*a_{ii})(a'_{ii})^2}{\mathrm{tr}(a_{ii}^*a_{ii})(a'_{ii})^2} = \frac{a_{ii}^*a_{ii}}{\mathrm{tr}(a_{ii}^*a_{ii})} \in \omega_0 \Rightarrow a_{ii} \in \omega_1,\\
&\frac{\mathrm{tr}(d_{ii})}{\mathrm{tr}(d_{i+1,i+1})} = \frac{\mathrm{tr}(a_{ii}^*a_{ii})(a'_{ii})^2}{\mathrm{tr}((a_{i+1,i+1})^*a_{i+1,i+1})(a'_{i+1,i+1})^2} \leq \frac{C^{\frac{1}{d}}}{(C')^{\frac{1}{d}}}c_1^2 = C_1,\\
&\mathrm{tr}(t_{ij}^*t_{ij}) \leq c_2 = C_2.
\end{aligned}$$

Hence, $t^*dt = F(\kappa aa't)$ for any $\kappa \in K$ and the above choice of $a \in A_{\omega_1}^{(1)}, a' \in \underline{A}_{c_1}^{\mathbb{R}}$ and this settles the claim.

Now for any $g \in \mathcal{G}(\mathbb{R})$, we know from Theorem 4.13 that for some $b \in M_k(\mathcal{O})$, we have $b^*g^*gb \in \mathfrak{S} \Rightarrow b^*g^*gb \in KA_{\omega_1}^{(1)}\underline{A}_{c_1}^{\mathbb{R}}N_{c_2} \Rightarrow gb \in K(KA_{\omega_1}^{(1)}\underline{A}_{c_1}^{\mathbb{R}}N_{c_2}) = KA_{\omega_1}^{(1)}\underline{A}_{c_1}^{\mathbb{R}}N_{c_2}$. From Lemma 4.16, we know that we can find finitely many $b_1, b_2, \ldots, b_m \in M_k(D)$ such that $b = b'b_i$ for some $b' \in \Gamma$ and for some $1 \leq i \leq m$. This implies that $gb' \in \bigcup_{i=1}^m (KA_{\omega_1}^{(1)}\underline{A}_{c_1}^{\mathbb{R}}N_{c_2})b_i^{-1}$.

Observe that $\mathrm{N}(gb') = 1$, whereas for

$$(\kappa aa'n)b_i^{-1} \in (KA_{\omega_1}^{(1)}\underline{A}_{c_1}^{\mathbb{R}}N_{c_2})b_i^{-1}$$

we have

$$\mathrm{N}(\kappa aa'nb_i^{-1}) = \mathrm{N}(a')/\mathrm{N}(b_i).$$

So $\mathrm{N}(b_i) > 0$ and

$$(\kappa aa'n)b_i^{-1} \in (KA_{\omega_1}^{(1)}\underline{A}_{c_1}^{\mathbb{R}}N_{c_2})b_i^{-1} \cap G = \mathrm{N}(b_i)^{\frac{1}{dk}}(KA_{\omega_1}^{(1)}A_{c_1}^{\mathbb{R}}N_{c_2})b_i^{-1}.$$

□

Remark 4.34. *Note that $\{b_i\}_{i=1}^n$ lie in $\mathrm{GL}_k(D)$. This means that for some $N \in \mathbb{N}$, $Nb_i \in M_k(\mathcal{O})$. We will use this in the proof of our integration formula in Chapter 5.*

Now we are in a position to consider $\mathcal{G}(\mathbb{R})/\Gamma$ as a probability space.

Proposition 4.35. *The space $\mathcal{G}(\mathbb{R})/\Gamma$ carries a unique probability measure that is left-invariant over the action of $\mathcal{G}(\mathbb{R})$.*

Proof. The Haar measure of $\mathcal{G}(\mathbb{R})$ restricts to left-invariant measure on $\mathcal{G}(\mathbb{R})/\Gamma$ since Γ is discrete inside $\mathcal{G}(\mathbb{R})$. Since $\mathfrak{S}^* \subseteq \mathcal{G}(\mathbb{R})$ surjects onto $\mathcal{G}(\mathbb{R})/\Gamma$, it is sufficient to show that $\mathfrak{S}^*$ has a finite measure in $\mathcal{G}(\mathbb{R})$.

The set $\mathfrak{S}^*$ is just a union of finitely many translates of $\mathfrak{S}^1$. So let us show that $\mathfrak{S}^1 \subseteq \mathcal{G}(\mathbb{R})$ has finite measure. This is to show that the following integral is convergent.

$$\int_{N_{c_2}} \int_{A_{\omega_1}^{(1)}} \int_{A_{c_1}^{\mathbb{R}}} \int_K \left(\prod_{i<j} \frac{a'_{ii}}{a'_{jj}}\right)^d d\kappa da' da dn.$$

We can separate the variables in the above integral. Observe that all the integrals other than the one over $A^{\mathbb{R}}_{c_1}$ is over a compact set and so must be finite. It simply remains to be shown that the following integral is finite.

$$\int_{A^{\mathbb{R}}_{c_1}} \left(\prod_{i<j} \frac{a'_{ii}}{a'_{jj}} \right)^d da'.$$

The group $A^{\mathbb{R}}$ is topologically isomorphic to $(\mathbb{R}_{>0})^{t-1}$, but let us make this identification in the following slightly convoluted manner to make the integral easier for us.

$$\begin{aligned} A^{\mathbb{R}} &\to (\mathbb{R}_{>0})^{t-1} \\ a' &\to \frac{a'_{ii}}{a'_{(i+1)(i+1)}}. \end{aligned}$$

The above is an isomorphism of locally compact topological groups and therefore, the Haar measure da' can be replaced by a Haar measure of $(\mathbb{R}_{>0})^{t-1}$. Write $y_i = a'_{ii}/a'_{(i+1)(i+1)}$ and now all that remains is to see that the following is a finite integral which is true whenever $d \geq 1$.

$$\int_0^{c_1} \int_0^{c_1} \cdots \int_0^{c_1} \left(\prod_{i<j} y_i^d y_{i+1}^d \cdots y_{j-1}^d \right) \frac{dy_1}{y_1} \frac{dy_2}{y_2} \cdots \frac{dy_{t-1}}{y_{t-1}}.$$

□

Chapter 5

Integration formula for G-symmetric lattices

We remind the reader that the idea is to consider random lattices that come with a prescribed group of symmetries given by G.

We remind the reader of the setting we are working with. We work with a finite group G acting on $V_{\mathbb{Q}}$ satisfying the decomposition given by Equation (2.3). In light of the discussions in Chapter 3, we decided to focus on the space of lattices to be the quotient space of an arithmetic subgroup inside the following algebraic group.

$$\mathcal{G}(\mathbb{Q}) = \prod_{i=1..k} \mathrm{SL}_{t_i}(D_i), \text{ where } D_i = \mathrm{End}_{\mathbb{Q}[G]}(V_i)_{\mathbb{Q}}.$$

More specifically, we work with the representation of $\mathcal{G}(\mathbb{Q})$ with respect to the left action on the vector space

$$V_{\mathbb{Q}} = \bigoplus_{i=1}^{k} D_i^{\oplus(t_i \times n_i)},$$

where n_i is the matrix index of V_i as discussed in Section 2.3.2. Then, for a base lattice $\Lambda \subseteq V_{\mathbb{Q}}$, we define

$$\Gamma = \{g \in \mathcal{G}(\mathbb{Q}) \mid g\Lambda = \Lambda\},$$

and $\mathcal{G}(\mathbb{R})/\Gamma$ models a space of G-invariant lattices in $V_{\mathbb{R}}$ where G acts on $V_{\mathbb{Q}}$ and has a finite $\mathcal{G}(\mathbb{R})$-invariant measure. Without loss of generality, we assume from now onwards that it has a probability measure after scaling this finite measure appropriately.

5.1 Siegel transforms

Suppose $\mathcal{C}_c(V_{\mathbb{R}})$ is the space of compactly supported measurable functions on $V_{\mathbb{R}}$. For any $f \in \mathcal{C}_c(V_{\mathbb{R}})$ and for any lattice $\Lambda \subseteq V_{\mathbb{R}}$, we define

$$\Phi_f(\Lambda) = \sum_{v \in \Lambda} f(v).$$

Φ_f is a function defined on a space of lattices, such as $\mathcal{G}(\mathbb{R})/\Gamma$ or $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$. This function, or some variants of this function, is known as the Siegel transform of f.

In general, $\Phi_f(\Lambda)$ as a function of Λ is not bounded. The lattice Λ could have arbitrarily short vectors, which means more and more lattice points might lie in support of f making $\sum_{v \in \Lambda} f(v)$ arbitrarily large. However, one can still hope that the following integral is bounded.

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \Phi_f(g\Lambda) dg, \text{ where } \Lambda \subseteq V_{\mathbb{Q}} \text{ is a fixed lattice.}$$

According to the following lemma, knowing the above integral basically amounts being able to integrate $f \in \mathcal{C}_c(V_{\mathbb{R}})$ on the orbits of $\mathcal{G}$.

Lemma 5.1. *Suppose $\mathcal{G}$ is a unimodular $\mathbb{Q}$-group with a $\mathbb{Q}$-representation $\mathcal{G} \to \mathrm{SL}(V_{\mathbb{Q}})$. $\Lambda \subseteq V_{\mathbb{Q}}$ be a lattice and let $\Gamma \subseteq \{g \in G(\mathbb{Q}) \mid g\Lambda = \Lambda\}$ be an arithmetic subgroup. Furthermore, suppose we have that for any $\omega \in V_{\mathbb{Q}}$, the stabilizer subgroup $\mathcal{G}_\omega \subseteq \mathcal{G}$ is unimodular.*

Then for any $f \in \mathcal{C}_c(V_{\mathbb{R}})$, assuming that Φ_f is absolutely integrable on the space $\mathcal{G}(\mathbb{R})/\Gamma$, we have

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \Phi_f(g\Lambda)dg = \sum_{\Gamma\omega\in\Gamma\backslash\Lambda} \mathrm{vol}\left(\mathcal{G}_\omega(\mathbb{R})/\Gamma_\omega\right) \int_{\mathcal{G}(\mathbb{R})/\mathcal{G}_\omega(\mathbb{R})} f(g\omega)dg. \tag{5.1}$$

Here Γ_ω is the stabilizer group of ω in Γ.

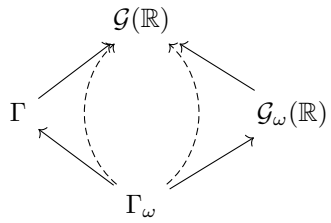
Proof. We want to decompose Λ into

$$\Lambda = \bigsqcup_{\Gamma\omega\in\Gamma\backslash\Lambda} \{\gamma\omega \mid \gamma \in \Gamma\}.$$

So, we write that

$$\begin{aligned}\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v\in\Lambda} f(gv)\right) dg &= \int_{\mathcal{G}(\mathbb{R})/\Gamma} \sum_{\Gamma\omega\in\Gamma\backslash\Lambda} \sum_{\gamma\in\Gamma/\Gamma_\omega} f(g\gamma w)dg \\ &= \sum_{\Gamma\omega\in\Gamma\backslash\Lambda} \left(\int_{\mathcal{G}(\mathbb{R})/\Gamma} \sum_{\gamma\in\Gamma/\Gamma_\omega} f(g\gamma w)\right) dg.\end{aligned}$$

We then observe that the following inclusion of groups holds.



Notice that in the last expression, the integration is happening over $\mathcal{G}(\mathbb{R})/\Gamma_\omega$ broken into two integrations along the left dashed path in the diagram. We want to instead break it down into the path on the right.

Since we have assumed that $\mathcal{G}_\omega$ is a unimodular algebraic group, we get that the homogeneous space $\mathcal{G}_\omega(\mathbb{R})/\Gamma_\omega$ has a well-defined Haar measure on which we can unfold our integral as the following.

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v\in\Lambda} f(gv)\right) dg = \sum_{\Gamma\omega\in\Gamma\backslash\Lambda} \int_{\gamma_1\in\mathcal{G}(\mathbb{R})/\mathcal{G}_\omega(\mathbb{R})} \left(\int_{\gamma_2\in\mathcal{G}_\omega(\mathbb{R})/\Gamma_\omega} f(\gamma_1\gamma_2\omega)d\gamma_2\right) d\gamma_1.$$

Now we know that $\gamma_2\omega = \omega$. This gives us the expression that we need. □

Remark 5.2. *Weil considers the above integral, albeit in an adelic setting [Wei65]. There, the hypothesis that $\mathcal{G}_\omega$ needs to be unimodular is dropped and is deduced by some more sophisticated machinery. We do not need this in our methods.*

Remark 5.3. *Observe that for any $v \in V_{\mathbb{Q}}$, we have that for some $N \in \mathbb{Z}_{\geq 1}$, $Nv \in \Lambda$. Since scaling commutes with action of $\mathcal{G}$, it is clear that the sum over the groups $\mathcal{G}_\omega$ appearing above contains all the stabilizers of rational points $v \in V_{\mathbb{Q}}$.*

Remark 5.4. *Note that if for two different orbits $\omega_1, \omega_2 \in \Gamma \setminus \Lambda$, we have $\mathcal{G}(\mathbb{R})\omega_1 = \mathcal{G}(\mathbb{R})\omega_2$, then it is clear that*

$$\int_{\mathcal{G}(\mathbb{R})/\mathcal{G}_{\omega_1}(\mathbb{R})} f(g\omega_1)d\omega_1 = \int_{\mathcal{G}(\mathbb{R})/\mathcal{G}_{\omega_2}(\mathbb{R})} f(g\omega_2)d\omega_1,$$

which can be shown by doing a change of coordinates. Then we can rewrite Equation (5.1) *as*

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma}\left(\sum_{v\in g\Lambda} f(v)\right)dg = \sum_{\mathcal{G}(\mathbb{R})v\in\{\mathcal{G}(\mathbb{R})\omega\}_{\omega\in\Lambda}} c_v \int_{\mathcal{G}(\mathbb{R})v} f(x)dx,$$

for some constants c_v that are formed from collecting together some terms.

Although the lemma is for a general algebraic group, for the case $\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_t(D)$, we must justify that we can use Lemma 5.1. We will offer the justification later with Lemma 5.8.

5.1.1 Choice of base lattice: finiteness concerns

What should be the choice of our base lattice Λ? We are especially interested in the cases where this integral is finite. For this end, we state the following lemma.

Lemma 5.5. *Suppose $\mathcal{G}$ is a semisimple $\mathbb{Q}$-group with a $\mathbb{Q}$-representation on $V_\mathbb{Q}$. Let $\Lambda_1 \subseteq V_\mathbb{Q}$ and $\Lambda_2 \subseteq V_\mathbb{Q}$ be two lattices and*

$$\Gamma_i = \{g \in \mathcal{G}(\mathbb{Q}) \mid g\Lambda_i = \Lambda_i\} \text{ for } i = 1, 2.$$

Then suppose for all compactly supported functions f, we have

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma_1} \Phi_f(g\Lambda_1)dg < \infty, \forall\ f \in \mathcal{C}_c(V_\mathbb{R})_{\geq 0}.$$

Then we must also have

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma_2} \Phi_f(g\Lambda_2)dg < \infty, \forall\ f \in \mathcal{C}_c(V_\mathbb{R})_{\geq 0},$$

Proof. Observe that for some $N \in \mathbb{Z}_{\geq 1}$, we have that $N\Lambda_2 \subseteq \Lambda_1$. This implies that for any $g \in \mathcal{G}(\mathbb{R})$,

$$\sum_{v\in\Lambda_2} f(gv) \leq \sum_{v\in\Lambda_1} f(\tfrac{1}{N}gv).$$

Also, we know that $\Gamma_1 \cap \Gamma_2$ is finite index in both Γ_1 and Γ_2 from Proposition 2.22. So, we get that

$$\begin{aligned}\int_{\mathcal{G}(\mathbb{R})/\Gamma_2}\left(\sum_{v\in\Lambda_2} f(gv)\right)dg &= \tfrac{1}{[\Gamma_2:\Gamma_1\cap\Gamma_2]}\int_{\mathcal{G}(\mathbb{R})/\Gamma_1\cap\Gamma_2}\left(\sum_{v\in\Lambda_2} f(gv)\right)dg \\ &\leq \tfrac{1}{[\Gamma_2:\Gamma_1\cap\Gamma_2]}\int_{\mathcal{G}(\mathbb{R})/\Gamma_1\cap\Gamma_2}\left(\sum_{v\in\Lambda_1} f(\tfrac{1}{N}gv)\right)dg \\ &= \tfrac{[\Gamma_1:\Gamma_1\cap\Gamma_2]}{[\Gamma_2:\Gamma_1\cap\Gamma_2]}\int_{\mathcal{G}(\mathbb{R})/\Gamma_1}\left(\sum_{v\in\Lambda_1} f(\tfrac{1}{N}gv)\right)dg.\end{aligned}$$

By hypothesis, this last expression is $< \infty$. □

So, this implies that as long as we want to have finite integrals, the choice of the base lattice Λ_1 does not matter.

Later we will go on to describe what exactly does changing the base lattice do for integration formula on the G-symmetric space of lattices.

5.2 Integration formula

5.2.1 Single irreducible representation

For "simplicity", let us assume that the $\mathbb{Q}[G]$-representation $V_\mathbb{Q}$ has t powers of the same irreducible representation $W_\mathbb{Q}$. Hence, as a $\mathbb{Q}[G]$-representation, we assume that

$$V_\mathbb{Q} \simeq W_\mathbb{Q}^{\oplus t}.$$

Hence, we let $D = \mathrm{End}_{\mathbb{Q}[G]} W$ be the corresponding $\mathbb{Q}$-division algebra and consider the action of $\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_t(D)$ on $W^{\oplus t}$. We can assume that $W \simeq D^n$ for some n. In effect, we get

$$V_{\mathbb{Q}} \simeq W^{\oplus t} \simeq D^{t\times n}.$$

Hence, we can identify $D^{t\times n} = M_{t\times n}(D)$, that is $t\times n$ matrices over the division ring D. The action of $\mathrm{SL}_t(D)$ on this is exactly the same as left-multiplication of a matrix in $M_{t\times t}(D)$ with $M_{t\times n}(D)$.

Following the discussion in Section 5.1.1, we are free to choose a base lattice as per our convenience. While applying the results, we often take lattices coming from some orders in the division ring, but the mean value theorems that we will see are more general!

5.2.2 The case of $t = 1$

When $t = 1$, we may not have a very nice formula like the one that will soon appear.

Here is an example to demonstrate the intricacies involved in this.

Example 5.6. *Consider the action of the quaternion group*

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

We look at the representation of the group via left multiplication on the 4-dimensional space of rational Hamiltonian quaternions

$$H_{\mathbb{Q}} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Q}\ \}.$$

Then $H_{\mathbb{R}} = \mathbb{H}$ are the usual Hamiltonian quaternions. We look at the Q_8-invariant lattice $H_{\mathbb{Z}}$ which is the set of quaternions with integer coefficients. Then the group $\mathrm{SL}_1(\mathbb{H})$ is the group of unit quaternions acting on the right via Hamiltonian quaternion multiplication (which is the same thing as $\mathrm{SL}_1(\mathbb{H}_{\mathrm{op}})$ on the left but for simplicity, let us have the right action instead).

The space of Q_8 invariant lattices that we are interested in is

$$\{H_{\mathbb{Z}} \cdot g \mid g \in \mathrm{SL}_1(\mathbb{H})\}.$$

Then it is clear that for any $\alpha \in H_{\mathbb{Z}}$, $g\,\mathrm{SL}_1(\mathbb{H})$ is given by a three-sphere

$$\{a + bi + cj + dk \mid a^2 + b^2 + c^2 + d^2 = \|g\|\}.$$

Therefore, this implies that the right hand side of the Siegel-Weil formula in Lemma 5.1 will reduce to a sum over integrals on spheres of radius $\{\sqrt{n}\}_{n\in\mathbb{Z}_{\geq 0}}$.

In general, it is known that for any order $\mathcal{O} \subseteq D$, the homogeneous space $\mathrm{SL}_1(D_{\mathbb{R}})/\mathcal{O}^*$ is compact (cf. [Mor15]). This means that when $t = 1$, the space $\mathcal{G}(\mathbb{R})/\Gamma$ is compact and therefore, surely the integral

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v\in\Lambda} f(gv) \right) dg < \infty.$$

However, what is happening here is that the group $\mathcal{G}(\mathbb{R}) = \mathrm{SL}_1(D_{\mathbb{R}})$ is acting on $D_{\mathbb{R}}^{1\times n}$ for some $n \geq 1$ and if $\dim_{\mathbb{Q}} D = d$, then $\mathrm{SL}_1(D_{\mathbb{R}})$ is a $(d-1)$-dimensional Lie group acting on a space of dn real dimensions. Hence, the right side of Equation (5.1) will be a sum over integrals of some varieties of $\leq d-1$ real dimensions in the nd-dimensional Euclidean space $V_{\mathbb{R}}$.

It is not clear if we can say something more than this.

5.2.3 The case of $t > 1$

We will have to subdivide it into further cases.

5.2.3.i When $t > n$

For this case, we can comfortably state a version of our Siegel mean value theorem for G-invariant lattices for a single irreducible representation when the number of copies is at least 2 and also strictly greater than the matrix index of the representation.

We find from Lemma 5.1 that if the left hand side exists, it must be given by Equation (5.1). So, the question to ask is, what are the orbits $\mathcal{G}(\mathbb{R})\omega$ for $\omega \in \Lambda$? To answer this question, let us first separate out the trivial orbit $\{0\} = \{\mathcal{G}(\mathbb{R}) \cdot 0\}$. Then the rest can be answered through the upcoming setup.

Let $\omega \in \Lambda \subseteq V_{\mathbb{Q}} \simeq M_{t\times n}(D)$ be a matrix whose columns are $\omega_1, \omega_2, \ldots, \omega_n$. Since $n < t$, we must have that for some $a_1, a_2, \ldots, a_n \in D_{\mathbb{R}}$, we get

$$\begin{aligned} \omega_1 a_1 + \omega_2 a_2 + \cdots + \omega_n a_n = 0 \in D^t \qquad (5.2)\\ \Rightarrow g \cdot \omega_1 a_1 + g \cdot \omega_2 a_2 + \cdots + g \cdot \omega_n a_n = 0 \in D^t, \quad \forall\ g \in \mathcal{G}(\mathbb{R}) \end{aligned}$$

For a given $\omega_1, \ldots, \omega_n \in D^t$, we collect all the coefficients $(a_1, \ldots, a_n) \in D^n$ satisfying the relation in Equation (5.2). Note that these relations form a right-D submodule in D^n which we call $\mathrm{Ann}(\omega)$. We see that the if $\omega' \in \mathcal{G}(\mathbb{R})\omega \cap \Lambda$, we must have $\mathrm{Ann}(\omega) = \mathrm{Ann}(\omega')$.

Lemma 5.7. *The map $\omega \mapsto \mathrm{Ann}(\omega)$ creates a bijection between orbits $\{\mathcal{G}(\mathbb{R})\omega\}_{\omega\in\Lambda}$ and right D-submodules of D^n.*

Proof. It is clear that $\omega = 0 \Leftrightarrow \mathrm{Ann}(\omega) = D^n$.

Assume that $\omega \neq 0$. Invoke the rank factorization mentioned in Lemma 2.63 and write $\omega = c \cdot f$. We recall to the reader that this factorization is unique for a given $\omega \in M_{t\times n}(\mathcal{O})$.

Here $f \in M_{m\times n}(D)$. We claim that the reduced matrix f completely determines the right D-module $\mathrm{Ann}(\omega)$. Indeed, if $a \in M_{n\times 1}(D)$ satisfies

$$c \cdot f \cdot a = 0.$$

Then for any other ω' which has the rank factorization $\omega' = c' \cdot f$, according to Lemma 4.2, we can find some $g \in \mathcal{G}(\mathbb{R})$ such that $gc = c_1 \Rightarrow g\omega = \omega_1$. Hence, we must find that

$$c_1 \cdot f \cdot a = 0.$$

This implies that $a \in \mathrm{Ann}(\omega) \Rightarrow a \in \mathrm{Ann}(\omega_1)$. □

The above proof also gives us an opportunity to show the following lemma.

Lemma 5.8. *The group $\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_t(D)$ satisfies the conditions of Lemma 5.1.*

Proof. We want to show that for any $\omega \in M_{t\times n}(D)$, $\mathcal{G}_\omega(\mathbb{R})$ is unimodular. Due to Proposition 4.24, we know that $\mathrm{SL}_t(D)$ is unimodular. Also, due to Lemma 4.2, we know that $\mathrm{SL}_t(D)$ acts transitively on right D-submodules of a fixed rank $m < t$ insider D^t.

It is clear that the orbit $\mathcal{G}(\mathbb{R})\omega$ is in bijection with $\mathcal{G}(\mathbb{R})/\mathcal{G}_\omega(\mathbb{R})$. Let $W = \mathrm{Ann}(\omega) \subseteq D^n$ be the right D-module associated to this orbit. Then, what Lemma 4.2 actually tells us is that $\mathcal{G}(\mathbb{R})\omega$ is bijectively mapped to a dense open set within the vector space

$$\{[\omega_1, \ldots, \omega_n] \in M_{t\times n}(D_{\mathbb{R}}) \mid \omega_1 a_1 + \cdots + \omega_n a_n = 0,\ \forall (a_1, \ldots, a_n) \in W \subseteq D^n\}.$$

Furthermore, this bijection is a homeomorphism since the orbit $\mathcal{G}(\mathbb{R})\omega$ is locally compact and any vector space is also locally compact. Therefore, we know that the Lebesgue measure on this vector space induces a bi-invariant Haar measure on $\mathcal{G}(\mathbb{R})/\mathcal{G}_\omega(\mathbb{R})$ and hence, $\mathcal{G}_\omega(\mathbb{R})$ must be unimodular.

□

Here is a definition to get us started before the upcoming proposition.

Definition 5.9. *Let X be any set and $\varepsilon > 0$. For a function $f : X \to \mathbb{R}$, we define the ε-dilate of*

$$\begin{aligned} f_\varepsilon : X &\to \mathbb{R} \\ x &\mapsto f(\varepsilon x). \end{aligned}$$

Proposition 5.10. *Let $V_{\mathbb{Q}} = D^{t\times n}$ and let $\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_n(D)$ be acting on left. Let $\Lambda = \mathcal{O}^{t\times n} \subseteq V_{\mathbb{Q}}$ be a lattice where $\mathcal{O} \subseteq D$ is an order inside our division ring. We thus have that $\Gamma = \mathrm{SL}_t(\mathcal{O})$ is a discrete subgroup in $\mathcal{G}(\mathbb{R})$ that preserves the lattice Λ.*

Suppose that $f : V_{\mathbb{R}} \to \mathbb{R}$ is a bounded and compactly supported function. Then, for any $0 < \varepsilon \leq 1$, we have that

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\varepsilon^d \sum_{v\in g\Lambda} |f(\varepsilon v)| \right) dg$$

is uniformly bounded (independent of ε) from above by a function on $\mathcal{G}(\mathbb{R})/\Gamma$ whose integral is finite.

Proof. Let $0 < \varepsilon \leq 1$ be a real number. As mentioned, we denote f_ε to the function $x \mapsto f(\varepsilon x)$, and let $d = \dim_{\mathbb{Q}} V$.

Recall $K, A^{\mathbb{R}}, A^{(1)}, N$ as discussed in Proposition 4.35. Let $R > 0$ be such that f is supported inside $B_R(0) \subset V_{\mathbb{R}}$ where $B_{\mathbb{R}}(0)$ is a ball invariant under the action of a compact group K. We can create such a ball by averaging any quadratic form over K.

With this, we get that

$$\begin{aligned}
\int_{\mathcal{G}(\mathbb{R})/\Gamma} \varepsilon^d \Phi_{f_\varepsilon}(g\Lambda)dg = \ & \varepsilon^d \int_{\mathfrak{S}^*} \left(\sum_{v\in\Lambda} f_\varepsilon(gv) \right) dg \\
\ll & \varepsilon^d \int_{\mathfrak{S}^*} \left((g\Lambda) \cap B_{R/\varepsilon}(0) \right) dg \\
\leq & \varepsilon^d \sum_{i=1}^{n} \int_{\mathfrak{S}^1} \# \left((gb_i^{-1}\Lambda) \cap B_{R/\varepsilon}(0) \right) dg \\
= & \sum_{i=1}^{m} \varepsilon^d \int_{N_{c_2}} \int_{A^{(1)}_{\omega_1}} \int_{A^{\mathbb{R}}_{c_1}} \int_K \# \left(\mathrm{N}(b_i)^{\frac{n}{d}} (\kappa a' a\eta) b_i^{-1}\Lambda \cap B_{R/\varepsilon}(0) \right) \prod_{i<j} \left(\frac{a'_{ii}}{a'_{jj}} \right)^{[D:\mathbb{Q}]} d\kappa da' da d\eta.
\end{aligned}$$

We remind the reader that the relation $d = nt[D : \mathbb{Q}]$. Since $B_{R/\varepsilon}(0)$ is chosen to be invariant under K, we know that for any $\kappa \in K$,

$$\# \left(\mathrm{N}(b_i)^{\frac{n}{d}} (\kappa a' a\eta) b_i^{-1}\Lambda \cap B_{R/\varepsilon}(0) \right) = \# \left(\mathrm{N}(b_i)^{\frac{n}{d}} (a' a\eta) b_i^{-1}\Lambda \cap B_{R/\varepsilon}(0) \right).$$

Because of Remark 4.34, we know that there exists some $N \in \mathbb{N}$ such that $b_i^{-1}\Lambda \subseteq \frac{1}{N}\Lambda$ for every $1 \leq i \leq n$. Hence, this tells us that

$$\# \left(\mathrm{N}(b_i)^{\frac{n}{d}} (a' a\eta) b_i^{-1}\Lambda \cap B_{R/\varepsilon}(0) \right) \ll \# \left((a' a\eta)\Lambda \cap B_{R/\varepsilon}(0) \right).$$

Note that in this last step, we might have to move to a slightly bigger radius R. But this does not affect anything.

Now consider the set

$$Y = \{ a'an(a')^{-1} \mid a' \in A^{\mathbb{R}}_{c_1}, a \in A^{(1)}_{\omega_1}, n \in N_{c_2} \} \subseteq \mathcal{G}(\mathbb{R}).$$

For $y \in Y$, note that $y_{ij} = a'_{ii} a_{ii} n_{ij} (a'_{jj})^{-1}$. Hence, $\mathrm{tr}(y_{ij}^* y_{ij}) = \left(\frac{a'_{ii}}{a'_{jj}} \right)^2 \mathrm{tr}\left((a_{ii}n_{ij})^* (a_{ii}n_{ij}) \right)$. Here, $\left(\frac{a'_{ii}}{a'_{jj}} \right)$ is a positive number bounded by c_1^{j-i} because of the construction of $A^{\mathbb{R}}_{c_1}$, and the other term is bounded because it continuously depends on $a_{ii}n_{ij}$ which lie in a compact set. Hence, overall the set Y must lie inside a relatively compact set of $\mathcal{G}(\mathbb{R})$. Furthermore, the set Y is only dependent on c_1, c_2 and ω_1.

Now what do we want to do with this set $Y \subseteq \mathcal{G}(\mathbb{R})$? Let $R' > 0$ be a radius such that $Y^{-1}B_R(0) \subseteq B_{R'}(0) \Rightarrow Y^{-1}B_{R/\varepsilon}(0) \subseteq B_{R'/\varepsilon}(0)$. Then we write that

$$\begin{aligned}
\# \left((a'an)\Lambda \cap B_{R/\varepsilon}(0) \right) = & \# \left((a'an(a')^{-1})a'\Lambda \cap B_{R/\varepsilon}(0) \right) \\
\leq & \# \left(a'\Lambda \cap Y^{-1}B_{R/\varepsilon}(0) \right) \\
\leq & \# \left(a'\Lambda \cap B_{R'/\varepsilon}(0) \right).
\end{aligned}$$

At this point, we invoke the identification $\Lambda = M_{t\times n}(\mathcal{O}) \subseteq M_{t\times n}(D) = V_{\mathbb{Q}}$. With having to possibly replace R' with a bigger radius, we assume that the norm on $V_{\mathbb{R}} \simeq {D_{\mathbb{R}}}^{t\times n}$ is the one given by

$$(x_1, \ldots, x_{tn}) \mapsto \sum_{i,j} \mathrm{tr}(x_{ij}^* x_{ij}).$$

Then the value of the last expression is equal to the number of integer solutions $(x_1, \ldots, x_{tn}) \in M_{t\times n}(\mathcal{O})$ such that

$$\sum_{i=1}^{t}\sum_{j=1}^{n} {a'_{ii}}^2 \,\mathrm{tr}_{D_{\mathbb{R}}}(x_{ij}^* x_{ij}) \leq \frac{R'^2}{\varepsilon^2}.$$

This is the number of points in a lattice intersecting with some ellipsoid. By considering a suitable "axis-parallel cuboid" that contains this ellipsoid, an upper bound for the number of these lattice points in the ellipsoid is the following quantity.

$$\prod_{i=1}^{t} \#\left\{ x \in \mathcal{O}^n \mid \sum_{i=1}^{n} \mathrm{tr}_{D_{\mathbb{R}}}(x_i^* x_i) \leq \frac{R'^2}{{a'_{ii}}^2 \varepsilon^2} \right\}.$$

Each term in the product is the number of points in a ball of radius $R'/a'_{ii}\varepsilon$ in a $\frac{d}{t}$-dimensional $\mathbb{R}$-vector space. Hence, there exist constants $B_1, B_2 > 0$ depending only on $\mathcal{O}, D$ such that

$$\#\left\{ x \in \mathcal{O}^n \mid \sum_{i=1}^{n} \mathrm{tr}_{D_{\mathbb{R}}}(x_i^* x_i) \leq \frac{R'^2}{{a'_{ii}}^2 \varepsilon^2} \right\} \leq B_1 + B_2 \left(\frac{R'}{a'_{ii}\varepsilon} \right)^{\frac{d}{t}},$$

and therefore,

$$\begin{aligned}
&\int_{\mathcal{G}(\mathbb{R})/\Gamma} \varepsilon^d \Phi_{f_\varepsilon}(g\Lambda) dg \\
&\ll \sum_{i=1}^{m} \varepsilon^d \int_{N_{c_2}} \int_{A^{(1)}_{\omega_1}} \int_{A^{\mathbb{R}}_{c_1}} \int_K \left(\prod_{i=1}^{t} \left(B_1 + B_2 \left(\frac{R'}{a'_{ii}\varepsilon} \right)^{\frac{d}{t}} \right) \right) \prod_{i<j} \left(\frac{a'_{ii}}{a'_{jj}} \right)^{\frac{d}{nt}} d\kappa da' da d\eta \\
&\ll \int_{N_{c_2}} \int_{A^{(1)}_{\omega_1}} \int_{A^{\mathbb{R}}_{c_1}} \int_K \left(\prod_{i=1}^{t} \left(B_1 \varepsilon^{\frac{d}{t}} + B_2 \left(\frac{R'}{a'_{ii}} \right)^{\frac{d}{t}} \right) \right) \prod_{i<j} \left(\frac{a'_{ii}}{a'_{jj}} \right)^{\frac{d}{nt}} d\kappa da' da d\eta.
\end{aligned}$$

Now $\varepsilon \leq 1 \Rightarrow B_1 \varepsilon^d \leq B_1$. Therefore, we can bound the integral above by

$$\int_{N_{c_2}} \int_{A^{(1)}_{\omega_1}} \int_{A^{\mathbb{R}}_{c_1}} \int_K \left(\prod_{i=1}^{t} \left(B_1 + B_2 \left(\frac{R'}{a'_{ii}} \right)^{\frac{d}{t}} \right) \right) \prod_{i<j} \left(\frac{a'_{ii}}{a'_{jj}} \right)^{\frac{d}{nt}} d\kappa da' da d\eta.$$

This last integral does not contain any appearance of ε. Note that for a decomposition of $g = \kappa a' a \eta$, the matrix a' is unique. Therefore, some appropriate scaling of the function $g \mapsto \prod_{i=1}^{t} \left(B_1 + B_2 (R' {a'_{ii}}^{-1})^{\frac{d}{t}} \right)$ on a fundamental domain of $\mathcal{G}(\mathbb{R})/\Gamma$ is a dominating function of $\varepsilon^{dk}\Phi_{f_\varepsilon}$ if we prove that the integral above is convergent.

The sets $K, A^{(1)}_{\omega_1}$ and N_{c_2} are compact and thus, $\int_K dk \int_{N_{c_2}} dn$ and $\int_{A^{(1)}_{\omega_1}} da$ are finite. Hence, we just need to show the finiteness of

$$\int_{A^{\mathbb{R}}_{c_1}} \left(\prod_{i=1}^{t} \left(B_1 + B_2 \left(\frac{R'}{a'_{ii}} \right)^{\frac{d}{t}} \right) \right) \prod_{i<j} \left(\frac{a'_{ii}}{a'_{jj}} \right)^{\frac{d}{nt}} da'. \tag{5.3}$$

Let us first do this for the case $t = 2$, that is, when $G = \mathrm{SL}_2(D_{\mathbb{R}})$ and $\Gamma = \mathrm{SL}_2(\mathcal{O})$. In that case, $A^{\mathbb{R}} \simeq \mathbb{R}^{>0}$, and we can parametrize it as $a'_{11} = {a'_{22}}^{-1} = s \in \mathbb{R}$. Since $n < t$, the only possible value is

when $n = 1$. The condition $a'_{11} \leq c_1 a'_{22}$ is just saying that $s^2 \leq c_1$. The measure da' is $\frac{1}{s}ds$. So, the integral becomes

$$\int_0^{\sqrt{c_1}} \left(B_1 + B_2 \left(\frac{R'}{s} \right)^{\frac{d}{2}} \right) \left(B_1 + B_2 (R's)^{\frac{d}{2}} \right) \frac{s^{\frac{d}{2}}}{(s^{-1})^{\frac{d}{2}}} \frac{ds}{s}$$

which is clearly finite.

For the general n, t, here it goes. We will use the coordinates of integration from Proposition 4.35. Define $y_i = a'_{ii}/a'_{i+1,i+1}$ for $i \in \{1, \ldots, t-1\}$. Then we have

$$\begin{bmatrix} 1 & -1 & & & & \\ & 1 & -1 & & & \\ & & 1 & -1 & & \\ & & & \ddots & & \\ & & & & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} \log a'_{11} \\ \log a'_{22} \\ \log a'_{33} \\ \vdots \\ \\ \log a'_{t-1,t-1} \end{bmatrix} = \begin{bmatrix} \log y_1 \\ \log y_2 \\ \log y_3 \\ \vdots \\ \\ \log y_{t-1} \end{bmatrix}.$$

The last row is so because $\sum_{i=1}^{t-1} \log a'_{ii} = 0$. The inverse of the square matrix above is

$$\frac{1}{t} \begin{bmatrix} t-1 & t-2 & t-3 & t-4 & & 1 \\ -1 & t-2 & t-3 & t-4 & \ldots & 1 \\ -1 & -2 & t-3 & t-4 & & 1 \\ -1 & -2 & -3 & t-4 & & \\ & \vdots & & & & \vdots \\ -1 & -2 & -3 & -4 & \ldots & 1 \end{bmatrix} = \left[\mathbb{I}_{i \leq j} - \frac{j}{t} \right]_{i,j=1}^{t-1},$$

and the determinant is t.

Then we get from the above calculations that

$$\frac{a'_{ii}}{a'_{jj}} = \prod_{r=i}^{j-1} y_r$$
$$\Rightarrow \prod_{i<j} \frac{a'_{ii}}{a'_{jj}} = \prod_{j=1}^{t-1} y_j^{j(t-j)}.$$

From the matrix inverse, we get that for $i \in \{1, 2, \ldots, t-1\}$,

$$a'_{ii} = e^{\log a'_{ii}} = e^{\sum_{j=i}^{t-1} \log y_j - \sum_{j=1}^{t-1} \frac{j}{t} \log y_j} = \prod_{j=i}^{t-1} y_j \prod_{j=1}^{t-1} y_j^{-\frac{j}{t}}$$

and

$$a'_{tt} = e^{-\sum_{j=1}^{t-1} \frac{j}{t} \log y_j} = \prod_{j=i}^{t-1} y_j^{-\frac{j}{t}}.$$

Finally, we replace the Haar measure $da' = \prod_{i=1}^{t-1} \frac{da'_{ii}}{a'_{ii}}$ with $\prod_{i=1}^{t-1} \frac{dy_i}{y_i}$. Indeed, such a change of measure will only change our integration by a constant and we can do this without loss of generality.

Putting this all together, the integral (5.3) becomes

$$\int_{0<y_i \leq c_1} \left[\prod_{i=1}^{t-1} \left(B_1 + B_2 R'^{\frac{d}{t}} \prod_{j=1}^{t-1} y_j^{\frac{jd}{t^2}} \prod_{j=i}^{t-1} y_j^{-\frac{d}{t}} \right) \right] \left(B_1 + B_2 R'^{\frac{d}{t}} \prod_{j=i}^{t-1} y_j^{\frac{jd}{t^2}} \right) \left(\prod_{j=1}^{t-1} y_j^{\frac{jd(t-j)}{nt}} \right) \prod_{i=1}^{t-1} \frac{dy_i}{y_i}.$$

Then the finiteness of the integral can be shown by simply chasing the powers of each y_i and showing that it is greater than -1. Indeed, any integral $\int_0^c y^s dy$ is finite if and only if $s > -1$.

Distributing the first product over subsets $I \subseteq \{1, 2, \ldots, t-1\}$ gives us

$$= \sum_{I \subseteq \{1,2,\ldots,t-1\}} \int_{0<y_i \leq c_1} B_1^{t-1} \left(\prod_{i \in I} \frac{B_2 R'^{\frac{d}{t}} \prod_{j=1}^{t-1} y_j^{\frac{jd}{t^2}}}{B_1 \prod_{j=i}^{t-1} y_j^{\frac{d}{t}}} \right) \left(B_2 R'^{\frac{d}{t}} \prod_{j=1}^{t-1} y_j^{\frac{jd}{t^2}} + B_1 \right) \left(\prod_{j=1}^{t-1} y_j^{\frac{jd(t-j)}{nt}} \right) \prod_{i=1}^{t-1} \frac{dy_i}{y_i}$$

$$= \sum_{I \subseteq \{1,2,\ldots,k-1\}} \int_{0<y_i \leq c_1} B_1^{t-1} \frac{\left(B_2 R'^{\frac{d}{t}} \prod_{j=1}^{t-1} y_j^{\frac{jd}{t^2}} \right)^{\#I}}{B_1^{\#I} \prod_{j=1}^{t-1} y_j^{\frac{d}{t}(\#I_{\leq j})}} \left(B_2 R'^{\frac{d}{t}} \prod_{j=1}^{t-1} y_j^{\frac{jd}{t^2}} + B_1 \right) \left(\prod_{j=1}^{t-1} y_j^{\frac{jd(t-j)}{nt}} \right) \prod_{i=1}^{t-1} \frac{dy_i}{y_i}.$$

where we have $I_{\leq j} = \{i \in I \mid i \leq j\}$. Now in the above expression, for each $I \subset \{1, 2, \ldots, t-1\}$, we have an integration of a sum of two products of some powers of y_j and some constant. As mentioned, if we prove that the power of y_j in each of those terms is > -1, then we are done. Note that the power of a y_j for $j \in \{1, 2, \ldots, t-1\}$ in the two summands would be

$$\frac{jd}{t^2}(\#I) - \frac{d}{t}(\#I_{\leq j}) + \frac{jd}{t^2} + \frac{jd(t-j)}{nt} - 1,$$

and

$$\frac{jd}{t^2}(\#I) - \frac{d}{t}(\#I_{\leq j}) + \frac{jd(t-j)}{nt} - 1.$$

Hence, it is sufficient to show that the latter is > -1 for each $I \subseteq \{1, 2, \ldots, t-1\}$ and for each j. So, we want that

$$\frac{dj}{t} \left(\left(\frac{\#I}{t} - \frac{\#I_{\leq j}}{j} \right) + \frac{(t-j)}{n} \right) > 0.$$

Let us prove this last inequality. Let $\#I_{>j} = \#I - \#I_{\leq j}$. Then what we want is equivalent to

$$\frac{\#I_{>j}}{t} > (t-j) \left(\frac{\#I_{\leq j}}{jt} - \frac{1}{n} \right)$$

$$\Leftrightarrow \quad \#I_{>j} > (t-j) \left(\frac{\#I_{\leq j}}{j} - \frac{t}{n} \right).$$

Here is why this inequality is true. The left hand side is ≥ 0 clearly. On the other hand, $\frac{\#I_{\leq j}}{j} \leq 1$ clearly whereas $\frac{t}{n} > 1$ by assumption. So, the right side is always < 0.

□

We are now ready to state the integration formula below. But before that, we must define the following term which appears in the integration formula.

Definition 5.11. *Let $W_{\mathbb{Q}}$ be a vector subspace inside the $\mathbb{Q}$-space $V_{\mathbb{Q}}$. Then given an inner product $\langle\ ,\ \rangle$ on $V_{\mathbb{R}}$ and a maximal rank $\mathbb{Z}$-lattice $\Lambda \subseteq V_{\mathbb{Q}}$, we denote the height of W to be*

$$H(W) = H(W; \Lambda, \langle\ ,\ \rangle) = \mathrm{vol}\left(\frac{W_{\mathbb{R}}}{W_{\mathbb{Q}} \cap \Lambda} \right).$$

Here, the volume is taken with respect to $\langle\ ,\ \rangle$ restricted to $W_{\mathbb{R}}$.

Theorem 5.12. *Let G be a finite group. Let W be an irreducible representation of G over $\mathbb{Q}$ and $D = \mathrm{End}_{\mathbb{Q}[G]} W$ and n be such that $W \simeq D^n$. Let $t > n$. Denote $V = V_{\mathbb{Q}} = W^{\oplus t}$, $\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_t(D)$, $\Lambda \subseteq V_{\mathbb{Q}}$ a lattice and*

$$\Gamma = \{g \in \mathcal{G}(\mathbb{Q}) \mid g\Lambda = \Lambda\}.$$

Let $V_{\mathbb{R}}$ be endowed with an inner product $\langle\ ,\ \rangle$ that gives Λ unit covolume in $V_{\mathbb{R}}$. Let $f \in \mathcal{C}_c(V_{\mathbb{R}})$. Then we have that

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v \in \Lambda} f(gv) \right) dg = f(0) + \sum_{m=1}^{n} \sum_{\substack{W \subseteq D^n \\ W \text{ is a rank } m \text{ right } D\text{-module}}} \frac{1}{H(W_{\mathbb{Q}}^{\perp})} \int_{W_{\mathbb{R}}^{\perp}} f(w) dw,$$

where on $W_{\mathbb{R}}^{\perp}$ is defined as

$$\{[\omega_1, \ldots, \omega_n] \in M_{t\times n}(D_{\mathbb{R}}) \mid \omega_1 a_1 + \cdots + \omega_n a_n = 0,\ \forall (a_1, \ldots, a_n) \in W \subseteq D^n\},$$

and the measure on any subspace of $D_{\mathbb{R}}^{n\times t}$ is simply the restriction of $\langle\ ,\ \rangle$ on that subspace.

Proof. First of all, by substituting $\varepsilon = 1$ in Proposition 5.10, we know that the left hand side is an absolutely convergent integral. Then using Lemma 5.1 (which we can use because of Lemma 5.8) in the form given in Remark 5.4, and incorporating the classification of orbits from Lemma 5.7, we can write that for some constants c_W,

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v\in\Lambda\setminus\{0\}} f(gv) \right) dg = f(0) + \sum_{m=1}^{n} \sum_{\substack{W\subseteq D^n \\ W \text{ is a rank } m \text{ right } D\text{-module}}} c_W \int_{W_{\mathbb{R}}^{\perp}} f(w)dw.$$

Now suppose that we replace the function f by the ε-dilate f_ε as defined in Definition 5.9. Then we get that

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v\in\Lambda\setminus\{0\}} f(\varepsilon gv) \right) dg = f(0) + \sum_{m=1}^{n} \varepsilon^{-mt[D:\mathbb{Q}]} \sum_{\substack{W\subseteq D^n \\ W \text{ is a rank } m \text{ right } D\text{-module}}} c_W \int_{W_{\mathbb{R}}^{\perp}} f(w)dw.$$

Multiplying by ε^d, we get

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\varepsilon^d \sum_{v\in\Lambda\setminus\{0\}} f(\varepsilon gv) \right) dg = f(0) + \sum_{m=1}^{n} \varepsilon^{(n-m)t[D:\mathbb{Q}]} \sum_{\substack{W\subseteq D^n \\ W \text{ is a rank } m \text{ right } D\text{-module}}} c_W \int_{W_{\mathbb{R}}^{\perp}} f(w)dw.$$

We will now show that the constants c_W are $H(W_{\mathbb{R}}^{\perp})^{-1}$. Consider a right D-module $W \subseteq D^n$ and look at the function

$$f_W = f \cdot \mathbf{1}_{W_{\mathbb{R}}^{\perp}},$$

that is, we restrict f to $W_{\mathbb{R}}^{\perp}$ and replace its value with 0 everywhere outside of $W_{\mathbb{R}}^{\perp}$.

Now note that for a fixed $g \in \mathcal{G}(\mathbb{R})$, if we let $\varepsilon \to 0$, then we know that for any lattice $\Lambda \subseteq V_{\mathbb{Q}}$, the limit

$$\varepsilon^{mt[D:\mathbb{Q}]} \sum_{v\in g\Lambda} f_W(\varepsilon v) \to \frac{1}{\mathrm{vol}(\frac{W_{\mathbb{R}}^{\perp}}{\Lambda\cap W_{\mathbb{Q}}^{\perp}})} \int_{W_{\mathbb{R}}^{\perp}} f(x)dx.$$

The right hand side is a constant that does not depend on Λ. So, this implies that as a function of $g \in \mathcal{G}(\mathbb{R})$, the pointwise limit of the function

$$\Lambda \mapsto \varepsilon^{mt[K:\mathbb{Q}]} \sum_{v\in g\Lambda} f_W(\varepsilon v) \tag{5.4}$$

is a constant function. Since $W_{\mathbb{Q}}^{\perp}$ is invariant under $\mathcal{G}(\mathbb{Q})$, we can use Proposition 5.10 with $W_{\mathbb{Q}}$ as the representation $V_{\mathbb{Q}}$ mentioned therein. This tells us that for any $\varepsilon \in (0, 1]$, the function in Equation (5.4) is dominated by an integrable function on $W_{\mathbb{R}}^{\perp}$, we should be able to exchange the limits in the integral. Hence, we get

$$\lim_{\varepsilon\to 0} \int_{g\in\mathcal{G}(\mathbb{R})/\Gamma} \left(\varepsilon^{mt[D:\mathbb{Q}]} \sum_{v\in g\Lambda} f_W(\varepsilon v) \right) dg = \frac{1}{H(W_{\mathbb{Q}}^{\perp})} \int_{W_{\mathbb{R}}^{\perp}} f(x)dx.$$

This tells us that the coefficient c_W is as claimed since for any other right D-submodule $W_1 \neq W$ inside D^n

$$\int_{(W_1^{\perp})_{\mathbb{R}}} f_W(x)dx = 0,$$

since $(W_1^{\perp})_{\mathbb{R}} \cap W_{\mathbb{R}}^{\perp}$ is a zero measure set in $(W_1^{\perp})_{\mathbb{R}}$. □

Remark 5.13. *Recall the definition of an order from Section 2.2.6. Let $\mathcal{O} \subseteq D_{\mathbb{Q}}$ be an order inside the division ring D. Equip $D_{\mathbb{R}}$ with a Euclidean norm $\langle\ ,\ \rangle$ and for any $k \geq 1$, we assume that $D_{\mathbb{R}}^k$ has the Euclidean norm $\langle\ ,\ \rangle^{\oplus k}$.*

If $W \subseteq D^n$ is a right D-module of rank m, we observe that $W^\perp \subseteq D^{t\times m}$

$$H(W^\perp; \mathcal{O}^{\oplus(t\times n)}; \langle\ ,\ \rangle^{\oplus(t\times n)}) = H(V_W; \mathcal{O}^{\oplus n}; \langle\ ,\ \rangle^{\oplus n})^t$$

where V_W is the simpler version of $W^\perp$ given by

$$\{(b_1, \ldots, b_n) \in D^n \mid b_1a_1 + \cdots + b_na_n = 0,\ \forall (a_1, \ldots, a_n) \in W \subseteq D^n\}. \tag{5.5}$$

Remark 5.14. *By Proposition 5.10, we find out that for any $m \in \{1, \ldots, n\}$, the sum*

$$\sum_{W \text{ is a rank } m \text{ right } D\text{-module}} \frac{1}{H(W_{\mathbb{Q}}^\perp)} < \infty.$$

This tells us that

$$\#\{W \mid W \subseteq D^n \text{ is a right } D\text{-module}, H(W_{\mathbb{Q}}^\perp) \leq T\} \ll T.$$

Remark 5.15. *Recall $V_W \subseteq D^n$ from Equation (5.5) defined for a right D-module $W \subseteq D^n$. It creates a bijection between the right D-modules of rank m and left D-modules in D^n of rank $n-m$. More precisely, it creates a bijection between the following two $\mathbb{Q}$-varieties.*

$$\mathrm{RGr}(m, n, D) \simeq \mathrm{LGr}(n-m, n, D),$$

where on the left we have the right-Grassmannian of rank-m right D-submodules in D^n and on the right we have the left-Grassmannian of rank-$(n-m)$ left D-submodules of D^n.

Suppose that $f = \mathbf{1}_B$ is the indicator function of a ball of radius R. Then the formula in Theorem 5.12 is saying

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v\in\Lambda} f(gv)\right) dg = V(d)R^d + \sum_{m=1}^{n} V(d\tfrac{m}{n})R^{\frac{m}{n}d} Z(t; \mathrm{LGr}(n-m, n, D)),$$

where

$$Z(t; \mathrm{LGr}(m, n, D)) = \sum_{W\in\mathrm{LGr}(m,n,D)} \frac{1}{H(W)^t}. \tag{5.6}$$

This last quantity is the height zeta function of $\mathrm{LGr}(m, n, D)$. So, from Theorem 5.12, we can actually conclude that this height zeta function in Equation (5.6) actually converges absolutely for $t \in \{1, \ldots, n-1\}$. More particularly, it tells us that

$$\#\{V \in \mathrm{LGr}(m, n, D), H(V) \leq T\} \ll T^t. \tag{5.7}$$

If one fixes m and n before instead, t can be set as $n+1$ and we can obtain a result that somewhat comes close to the true result of counting rational points of bounded height on Grassmannians where the estimate on the point counts in Equation (5.7) is actually $\simeq T^n$ as $T \to \infty$. See [RZ13] where they obtain these point counts by geometric elements generalised by the work of Schmidt [Sch67] (which works when D is a number field) and also compare their results to Franke, Manin, Tschinkel [FMT89].

5.2.3.ii When $1 < t \leq n$

If the condition $t > n$ or $t = 1$ is not satisfied, the integral formula diverges for functions whose support contains an open set.

For example, in the simplest case when $D = \mathbb{Q}$, one can see Schmidt [Sch58].

5.2.4 Multiple irreducible representations

Let $V_{\mathbb{R}} = V_{\mathbb{Q}} \otimes \mathbb{R}$ and analogously define $(V_i)_{\mathbb{R}} = (V_i)_{\mathbb{Q}} \otimes \mathbb{R}$. Recall that $V_{\mathbb{Q}}$ has the decomposition of Equation (2.3).

$$V_{\mathbb{Q}} \simeq (V_1)_{\mathbb{Q}}^{\oplus t_1} \oplus \cdots \oplus (V_k)_{\mathbb{Q}}^{\oplus t_k}. \tag{5.8}$$

Suppose $f_i : (V_i)_{\mathbb{R}}^{\oplus t_i} \to \mathbb{R}$ is a compactly supported continuous function and let $f : V_{\mathbb{R}} \to \mathbb{R}$ be defined as

$$f(v_1, v_2, \dots v_k) = f_1(v_1) f(v_2) \dots f(v_k) \text{ where } v_i \in (V_i)_{\mathbb{R}}^{\oplus t_i}. \tag{5.9}$$

In light of the discussion of Section 5.1.1, we are allowed to choose a base lattice that provides a convenient integration formula. We select a suitable lattice $\Lambda_i \subseteq (V_i)_{\mathbb{Q}}^{\oplus t_i}$ and define

$$\Lambda = \Lambda_1 \oplus \Lambda_2 \oplus \cdots \oplus \Lambda_k,$$

which embeds into $V_{\mathbb{Q}}$ using the decomposition above. We recall that we get the decomposition

$$\mathcal{G}(\mathbb{Q}) = \mathrm{SL}_{t_1}(D_1) \oplus \cdots \oplus \mathrm{SL}_{t_k}(D_k),$$

where $D_i = \mathrm{End}_G V_i$ is a division algebra.

Hence, we have the equality

$$\sum_{v \in \Lambda} f(gv) = \prod_{i=1\dots k} \left(\sum_{v_i \in \Lambda_i} f_i(g_i v_i) \right) \tag{5.10}$$

for each $(g_1, \dots, g_k) = g \in \mathcal{G}(\mathbb{R})$ such that $g_i \in \mathrm{SL}_{t_i}(D_i)$.

If we define

$$\Gamma_i = \{g \in \mathcal{G}_i(\mathbb{Q}) \mid g\Lambda_i = \Lambda_i\},$$

we get that the group

$$\Gamma = \Gamma_1 \oplus \cdots \oplus \Gamma_k$$

is our arithmetic subgroup defined as

$$\Gamma = \{g \in \mathcal{G}(\mathbb{Q}) \mid g\Lambda = \Lambda\}.$$

Let $n_i = \frac{\dim_{\mathbb{Q}} V_i}{\dim_{\mathbb{Q}} D_i}$ be the matrix index of the representation V_i. Then due to the preceding discussion in Section 5.2.1, we are only able to evaluate the integral if for each i, either $t_i > n_i$ or $t_i = 1$.

Observe that the left hand side of Equation (5.10) is linear in f. Hence, if f is not necessarily of the form given in Equation (5.9), but instead is a $\mathbb{R}$-linear combination of such functions, we can still have a result of this form. Approximating a function as a linear combination of variable separable functions, we can generalise Theorem 5.12 as follows.

Theorem 5.16. *Suppose $V_{\mathbb{Q}}$ be a $\mathbb{Q}[G]$-representation whose decomposition into irreducibles is given by Equation (5.8). Furthermore, suppose that for each V_i, the matrix index n_i and the number of copies t_i satisfy $n_i < t_i$.*

Then for any $f \in \mathcal{C}_c(V_{\mathbb{R}})$, one has

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v \in g\Lambda} f(v) \right) dg = \sum_{(W_1,\dots,W_k) \in \mathcal{L}_1 \times \cdots \times \mathcal{L}_k} \frac{1}{H(W_1^{\perp}) \dots H(W_k^{\perp})} \int_{(W_1^{\perp})_{\mathbb{R}} \times \cdots \times (W_k^{\perp})_{\mathbb{R}}} f(w) dw,$$

where

$$\mathcal{L}_i = \{W \subseteq D_i^{n_i} \mid W \text{ is a right } D\text{-module}\}.$$

Chapter 6

Applications to the lattice packing problem

In this chapter, we will talk about results and applications of the general theory considered before.

6.1 Lattice sphere packings through division algebra

Consider Theorem 5.12 for the case $n = 1$. In this case, we get the following.

Theorem 6.1. *[Gar23]*
Let D be a $\mathbb{Q}$-division algebra containing an order $\mathcal{O} \subseteq D$. Let $\mathcal{G}(\mathbb{R}) = \mathrm{SL}_t(D_{\mathbb{R}})$ and $\Gamma = \mathrm{SL}_t(\mathcal{O})$ for some $t \geq 2$. Let dg be the probability measure on $\mathcal{G}(\mathbb{R})/\Gamma$ that is left-invariant under $\mathcal{G}(\mathbb{R})$ action. Then for any $f \in \mathcal{C}_c(D_{\mathbb{R}}^t)$, we get

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v \in g\mathcal{O}^t \setminus \{0\}} f(v) \right) dg = \int_{D_{\mathbb{R}}^t} f(x)dx,$$

where dx is a Lebesgue measure on $D_{\mathbb{R}}^t$ with respect to which $\mathcal{O}^t$ has a covolume of 1.

Remark 6.2. *By an easy application of the dominated convergence theorem, one can take f to be any Riemann integrable compactly supported function.*

This can be used to prove the following lower bound on the sphere packing problem for certain dimensions.

Proposition 6.3. *Let $\mathcal{O} \subseteq D$ be an order in a division algebra and let $G \subseteq D$ be a finite multiplicative subgroup of $\mathcal{O}$. Then for any $\varepsilon > 0$, there exists a lattice packing in dimensions $d = 2\dim_{\mathbb{Q}} D$ whose packing efficiency is at least $\frac{1}{2^d}(\#G) - \varepsilon$.*

Proof. What we will show is that there exists a positive definite quadratic form on $D_{\mathbb{R}}^2$ and a covolume one lattice Λ_0 (with respect to this quadratic form), such that the ball $B_R(0)$ in this quadratic form with a volume $\#G - \varepsilon$, the lattice and the ball intersect only at $\{0\}$. If we prove this, then we get that the balls $B_{R/2}(v_1), B_{R/2}(v_2)$ are disjoint for any distinct $v_1, v_2 \in \Lambda_0$ and hence, $\bigsqcup_{v \in \Lambda_0} B_{R/2}(v)$ forms a lattice packing whose packing efficiency will be

$$\frac{\mathrm{vol}\, B_{R/2}(0)}{\mathrm{vol}(D_{\mathbb{R}}^2/\Lambda_0)} = 2^{-d}(\#G - \varepsilon).$$

Consider the left-action of G on $D_{\mathbb{R}}^2$ via $g.(v_1, v_2) = (v_1 g^{-1}, v_2 g^{-1})$. This action is $\mathbb{R}$-linear and therefore, it is possible to start with any positive definite quadratic form on $D_{\mathbb{R}}^2$ and average over G and make it G-invariant. After appropriate scaling, the lattice $\mathcal{O}^2$ will have covolume one with respect to the measure induced by this form. We fix this as the form on $D_{\mathbb{R}}^2$ as mentioned above.

Now let $B_R(0)$ be the ball of volume $\#G - \varepsilon$ and let f be the indicator function of $B_R(0)$. Then, we get from Theorem 6.1 and Remark 6.2

$$\int_{\mathcal{G}(\mathbb{R})/\Gamma} \left(\sum_{v \in g\mathcal{O}^2 \setminus \{0\}} f(v) \right) dg = \int_{D_{\mathbb{R}}^2} f(x)dx = \#G - \varepsilon.$$

However, note that for any $g \in \mathcal{G}(\mathbb{R})$, the lattice $g\mathcal{O}^2$ is G-invariant under the left-action defined above. Furthermore, the G-orbit of any non-zero element of $\mathcal{O}^2$ is of size $\#G$ because $\mathcal{O}^2$ and G are made of elements of the division algebra D. Therefore, $\sum_{v \in g\mathcal{O}^2 \setminus \{0\}} f(v)$ lies in $\{0, \#G, 2(\#G), 3(\#G), \dots\}$. Since the average is strictly less than $\#G$, we get that for some $g_0 \in \mathcal{G}(\mathbb{R})$, $\Lambda_0 = g_0\mathcal{O}^2 \cap B_R(0) = \{0\}$ and this is the required lattice. □

A slight improvement in the above theorem can be made by Mahler's compactness theorem.

Theorem 6.4. *Let $(G, \mathcal{O}, D)$ be as in Proposition 6.3. Then there exists a lattice packing in dimensions $d = 2\dim_{\mathbb{Q}} D$ whose packing efficiency is at least $\frac{1}{2^d}(\#G)$.*

Proof. Let $\Lambda_n = g_n\mathcal{O}^2$ be a unit covolume lattice in $D_{\mathbb{R}}^2$ whose packing efficiency is better than $\frac{1}{2^d}(\#G) - \frac{1}{n}$. Since all Λ_n are unit covolume and whose packing efficiency is bounded below, we get from Mahler's compactness that up to replacing g_n with $g_n\gamma_n$ for some $\gamma_n \in \Gamma$, we can force $\{g_n\}_{n \geq 1}$ to be a relatively compact set in $\mathcal{G}(\mathbb{R})$ and therefore, it contains a convergent subsequence converging to some point $g \in \mathcal{G}(\mathbb{R})$. Since packing efficiency is a continuous function on $\mathcal{G}(\mathbb{R})/\Gamma$, we get that $g\mathcal{O}^2$ is the required lattice. □

Hence, this gives us a methodology of producing lower bounds for lattice packings. Any tuple $(G, \mathcal{O}, D)$ gives us a packing from Proposition 6.3 which gives us a valid lower bound for the sphere packing problem in dimension $d = 2\dim_{\mathbb{Q}} D$.

Example 6.5. *For $n \geq 3$, put $D = \mathbb{Q}(\mu_n)$, and $\mathcal{O} \subset D$ as its ring of integers, and $G = \langle \mu_n \rangle \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$. Hence, for dimension $d = 2\varphi(n)$, there is a lattice packing of packing efficiency at least $\#G = n$. This gives us the lower bound in [Ven13].*

Note that the following "tightening" can be done once we have a tuple $(G, \mathcal{O}, D)$. When D is a $\mathbb{Q}$-division algebra, the $\mathbb{Q}$-span of G in D is also a division algebra. Indeed, denote $\mathbb{Q}\langle G \rangle \subseteq D$ as the span[1] of G, then any $\gamma \in \mathbb{Q}\langle G \rangle$ is an invertible $\mathbb{Q}$-map. Therefore it will map $\mathbb{Q}\langle G \rangle$ to itself under left-multiplication and therefore must map something to 1_D. Let $\mathbb{Z}\langle G \rangle \subseteq \mathcal{O}$ be the $\mathbb{Z}$-span of G, then we get that $(G, \mathbb{Z}\langle G \rangle, \mathbb{Q}\langle G \rangle)$ is another tuple that fits in Proposition 6.3.

Clearly, $\dim_{\mathbb{Q}} \mathbb{Q}\langle G \rangle \leq \dim_{\mathbb{Q}} D$. Therefore, we can get a packing in smaller dimension without losing the packing efficiency. Hence, to get tighter packings it is sufficient to consider the case where the $\mathbb{Q}$-span of G is precisely D. $\mathcal{O}$ can then be taken to be the $\mathbb{Z}$-span of G.

6.1.1 Improved bounds

A detailed analysis of the improvements obtained are already available in [Gar23] and we will simply restate the main ideas.

There exists a specific class of division algebras for which we can modestly improve on the bounds obtained in [Ven13]. This works in the following way.

Proposition 6.6. *Assume m is a positive integer such that 2 has odd order modulo m. Then the algebra $\mathbb{Q}(\zeta_m) \otimes_{\mathbb{Q}} \left(\frac{-1,-1}{\mathbb{Q}} \right)$ is a division algebra with center $\mathbb{Q}(\zeta_m)$ and has a maximal $\mathbb{Z}[\zeta_m]$-order $\mathcal{O}_K$ with subgroup $\mathfrak{T}^* \times \frac{\mathbb{Z}}{m\mathbb{Z}} \subset \mathcal{O}^\times$.*

Proof. See [Ami55, Theorems 6a, 7]. □

[1] Caution: This is not the group algebra of G. The group algebra of G over $\mathbb{Q}$ will almost never be a division algebra. More precisely, this is the image of the group algebra under $\mathbb{Q}[G] \to D$ induced from the inclusion $G \hookrightarrow D$.

For this particular set of division algebras, there is a slight improvement on the lattice packings in [Ven13]. The division algebra in Proposition 6.6 is of $\mathbb{Q}$-dimension $4 \cdot \varphi(m)$ whereas the group $\mathfrak{T}^* \times \frac{\mathbb{Z}}{m\mathbb{Z}} \subset \mathcal{O}^\times$. is of size $24 \cdot m$. Hence, using Theorem 6.4, we arrive at a packing density of $\frac{1}{2^{8\cdot\varphi}} 24 \cdot m$ is a space of $\mathbb{R}$-dimension $8 \cdot \varphi(m)$ whenever m is a number such that the multiplicative order of 2 modulo m is odd. Of course, this constrains our choice of m quite heavily.

To maximise the ration $m/\varphi(m)$, we must make m highly composite but we can only choose among the following set of primes whose density is known due to a theorem of Hasse [Has66].

Theorem 6.7. *Hasse, '66*
Define $\pi_2(x)$ as

$$\begin{aligned}\pi_2(x) &= \#\{p \mid 2 < p \leq x \text{ is prime and } p|(2^m+1) \text{ for some } m \in \mathbb{Z}_{\geq 0}\} \\ &= \#\{p \mid 2 < p \leq x \text{ is prime and } \operatorname{ord}_p 2 \text{ is even}\}.\end{aligned}$$

Then we have that

$$\pi_2(x) = \frac{17}{24}\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Corollary 6.8. *Using the prime number theorem, we get that if $\pi(x)$ is the prime-counting function, then the primes for which $\operatorname{ord}_p 2$ is odd follow the following growth.*

$$\pi(x) - \pi_2(x) = \frac{7}{24}\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Theorem 6.9. *There exists a sequence of dimensions $\{d_i\}_{i=1}^{\infty}$ such that for some $C > 0$, we have a lattice with packing density $\geq \frac{1}{2^{d_i}} \cdot 3d_i(\log\log d_i)^{\frac{7}{24}}$.*

Proof. We pick

$$m = \prod_{\substack{p \text{ is prime} \\ p \leq x \\ 2 \nmid \operatorname{ord}_p 2}} p.$$

Then observe that with this, we get that m is odd and $\operatorname{ord}_m 2$ is also odd. Using Proposition 6.6 and Theorem 6.4, we can obtain the statement by using Abel's summation formula which we skip describing. □

Attempting to plot this sequence gives the comparision obtained in Figure 1.5.

One important concluding remark here is that since all division algebras are classified as cyclic division algebras (see Section 2.3.4) and all finite subgroups of cyclic division algebras are classified by [Ami55], one can check through all possible improvements that can be done on [Ven13] by employing division algebras. This analysis leads to the conclusion that no asymptotic improvements beyond $O(n \log\log n)$ seem possible in packing density.

6.2 Effective packings through division algebra

The packing result described in Section 6.1 shows that there exist lattices using division rings that achieve sphere packings with good packing density. However, in coding theory, it is more useful to have something beyond the existence of a lattice packing. One must find a way to generate a lattice basis algorithmically or must have some explicit description of the lattices.

The lattices obtained in [Gar23] are non-constructive in the sense that the proof simply shows that a certain point exists on the manifold $\mathcal{G}(\mathbb{R})/\Gamma$ which has the claimed packing density. In the paper [GS22], we try to address this aspect of random lattice packings for coding theory applications.

Recall that we can assume that our division algebra is a cyclic division algebra, hence $\mathcal{Z}(D) = K$ is a number field over $\mathbb{Q}$.

Definition 6.10. *An $\mathcal{O}_K$-order in D is a subring $\mathcal{O}$ of D having the same identity element and such that $\mathcal{O}$ is a* full *$\mathcal{O}_K$-lattice in K, i.e., $\mathcal{O}$ is a finitely generated $\mathcal{O}_K$-submodule of D such that $K \cdot \mathcal{O} = A$.*

A prime ideal of $\mathcal{O}$ is a proper two-sided ideal $\mathfrak{P}$ in $\mathcal{O}$ such that $K \cdot \mathfrak{P} = D$ and such that for every pair of two sided ideals S, T in Λ, $S \cdot T \subset \mathfrak{P}$ implies $S \subset \mathfrak{P}$ or $T \subset \mathfrak{P}$.

We now summarise some important facts about prime ideals in $\mathcal{O}$.

Theorem 6.11. *1. For a $\mathbb{Q}$-division algebra D with centre K, there is a bijection $\mathfrak{P} \leftrightarrow \mathcal{P}$ between the set of primes of an $\mathcal{O}_K$-order $\mathcal{O} \subseteq D$ and of $\mathcal{O}_K$, given by*

$$\mathcal{P} = \mathcal{O}_K \cap \mathfrak{P}\,.$$

That is, the prime ideals of an $\mathcal{O}_K$-order $\mathcal{O}$ coincide with the maximal two-sided ideals of $\mathcal{O}$.

2. If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}$, then $\mathcal{P} = \mathfrak{P} \cap \mathcal{O}_K$ is a non-zero prime of $\mathcal{O}_K$, and $\mathcal{O}/\mathfrak{P}$ is a finite dimensional simple algebra over the residue field $\mathcal{O}_K/\mathcal{P}$.

3. For all but finitely many primes $\mathcal{P}$ of $\mathcal{O}_K$, the quotient $\mathcal{O}/\mathfrak{P}$ is isomorphic to $M_n(\mathbb{F}_q)$, where $\mathcal{O}_K/\mathcal{P} \simeq \mathbb{F}_q$. Here, n is the order of the division algebra, that is $n^2 = [D : \mathcal{Z}(D)]$.

4. Let $K = \mathcal{Z}(D)$. Then, for all but finitely many primes $\mathcal{P} \subseteq \mathcal{O}_K$, the division algebra D is split at $\mathcal{P}$. That is, if $K_{\mathcal{P}}$ is the $\mathcal{P}$-adic completion of K, then

$$D \otimes_K K_{\mathcal{P}} \simeq M_n(K_{\mathcal{P}}),$$

where $n^2 = [D : K]$. When this happens, the corresponding prime $\mathfrak{P} \subseteq \mathcal{O}$ is also sometimes called a splitting prime.

Proof. These are well-known results, see e.g. [Rei03, Theorems 17.3, 32.1]. □

Remark 6.12. *The primes $\mathfrak{P} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathfrak{P} \simeq M_n(\mathcal{O}_K/\mathcal{P})$ are called unramified primes. The theorem above says that except for some finitely many primes $\mathfrak{P}$, we have both unramified and splitting behaviour.*

Using these results, we can define following set of lattices. Let $\mathfrak{P} \subseteq \mathcal{O}$ be a prime such that $\mathcal{O}/\mathfrak{P}$ is isomoprhic to $M_n(\mathbb{F}_q)$ and $\pi_{\mathfrak{P}} : \mathcal{O} \to M_n(\mathbb{F}_q)$ be the projection modulo $\mathfrak{P}$ map which we extend to a map $\pi_{\mathfrak{P}} : \mathcal{O}^t \to M_n(\mathbb{F}_q)^t$. Define for any $1 \leq k \leq nt$

$$\begin{aligned} \mathcal{C}_{\mathfrak{P}} &= \{C \subseteq M_n(\mathbb{F}_q)^t \mid C \text{ is a } M_n(\mathbb{F}_q)\text{-submodule } \simeq (\mathbb{F}_q^n)^{\oplus k}\}, \\ \mathcal{L}_{\mathfrak{P}} &= \{\beta_{\mathfrak{P}} \pi_{\mathfrak{P}}^{-1}(C) \mid C \in \mathcal{C}_{\mathfrak{P}}\}, \quad \text{where } \beta_{\mathfrak{P}} = q^{-\frac{1}{m}\cdot\left(1-\frac{k}{nt}\right)}. \end{aligned} \tag{6.1}$$

The point of having the factor $\beta_{\mathfrak{P}}$ is that for any unramified prime $\mathfrak{P}$, $\mathcal{L}_{\mathfrak{P}}$ is a collection of lattices having unit covolume.

6.2.1 A lower bound on some lifts

Before coming to the main result in this section, let us set up few lemmas. The following two lemmas provide a lower bound on an undesirable set of lifts modulo $\mathfrak{P}$.

The following definition and ensuing lemma can also be found in [Rei03, §9.13-14].

Definition 6.13. *Suppose A is a central simple L-algebra and $K \subseteq L$ is a subfield such that $[L : K] < \infty$. Then for each $a \in A$, we define the "relative reduced trace" $\mathrm{tr}_{A/K} : A \to K$ and "relative reduced norm" $\mathrm{nr}_{A/K} : A \to K$ as*

$$\mathrm{tr}_{A/K} = \mathrm{T}_{L/K} \circ \mathrm{tr}_{A/L}, \ \mathrm{nr}_{A/K} = \mathrm{N}_{L/K} \circ \mathrm{nr}_{A/L}\,.$$

Lemma 6.14. *When $[L : K] < \infty$ for any $a \in A$:*

$$\mathrm{T}_{A/K}(a) = \sqrt{[A : L]}\,\mathrm{tr}_{A/K}, \ \mathrm{N}_{A/K}(a) = \mathrm{nr}_{A/K}(a)^{\sqrt{[A:L]}}.$$

Then, we can make the following commutative square.

Lemma 6.15. *Let A be a division algebra over $\mathbb{Q}$ whose centre is K and $[A:K] = n^2$. Let $\mathcal{O} \subseteq A$ be a maximal order in the division algebra. Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$ for which A splits and let $\mathbb{F}_q = \mathcal{O}_K/\mathcal{P}$ denote the residue field. Let $\mathfrak{P} \subseteq \mathcal{O}$ be the corresponding prime in $\mathcal{O}$ by the correspondence in Theorem 6.11.*

Then the following diagram commutes.

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\mathrm{nr}_{A/K}} & \mathcal{O}_K \\ \downarrow{\scriptstyle \pi_{\mathfrak{P}}} & & \downarrow{\scriptstyle \pi_{\mathcal{P}}} \\ \mathcal{O}/\mathfrak{P}\mathcal{O} \cong M_n(\mathbb{F}_q) & \xrightarrow{\det} & \mathbb{F}_q, \end{array}$$

Here, the vertical maps designate reduction modulo $\mathcal{P}$.

Proof. First note that $\mathrm{nr}_{A/K}(a) \in \mathcal{O}_K$ for each $a \in \mathcal{O}$ since $\mathrm{nr}_{A/K}(a) \in K$ and $\mathcal{O}_K$ is integrally closed (see also [Rei03, §10.1]). The reduced norm $\mathrm{nr}_{A/K}(a)$ may be computed as the determinant of the corresponding matrix in $M_n(E)$, where E is a splitting field for A (and is easily seen to be independent of that choice). We may, in particular, choose E to be the $\mathfrak{P}$-adic completion $\hat{K}_{\mathfrak{P}}$ since by our assumption, we have $A \otimes_K \hat{K}_{\mathfrak{P}} \cong M_n(\hat{K}_{\mathfrak{P}})$.

□

Lemma 6.16. *With the same setting, let $(\ )^* : A_{\mathbb{R}} \to A_{\mathbb{R}}$ be a positive involution. If $x \in \mathcal{O} \setminus \{0\}$ (which we may identify with its image in $A_{\mathbb{R}}$) is such that $\pi_{\mathfrak{P}}(x)$ is a non-invertible matrix, then*

$$\|x\| \geq \left(\sqrt{[A:\mathbb{Q}]}\,\mathrm{N}(a)^{\frac{1}{2[A:\mathbb{Q}]}}\right) q^{\frac{1}{\sqrt{[A:K]}[K:\mathbb{Q}]}}$$

where $a \in A_{\mathbb{R}}$ is symmetric positive definite and $\|x\|^2 := \mathrm{T}(x^*ax)$ on $A_{\mathbb{R}}$.

Proof. We get by Lemma 6.15 that $\mathfrak{P} \mid \mathrm{nr}_{A/K}(x)$ and hence

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}) \mid \mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{nr}_{A/K}(x) \quad \Rightarrow \quad N_{K/\mathbb{Q}}(\mathfrak{P}) \mid \mathrm{nr}_{A/\mathbb{Q}}(x) \quad \Rightarrow \quad N_{K/\mathbb{Q}}(\mathfrak{P})^{\sqrt{[A:K]}} \mid \mathrm{N}_{A/\mathbb{Q}}(x).$$

The claim then follows from the norm-trace inequality (see Lemma 2.51). □

Remark 6.17. *By taking $a = \sum_{g \in G} g^*g$ for a finite group $G \subseteq A^*$, we obtain that the quadratic form $\|x\|^2 := \mathrm{T}(x^*ax)$ on $A_{\mathbb{R}}$ is G-invariant.*

6.2.2 Balanced codes

The following condition tells us that our codes described in Equation (6.1) have roughly equal incidence among all vectors in the finite vector space. This sort of condition is often called a "balanced" condition in coding theory literature [Cam18].

Lemma 6.18. *Let k be a finite field. Let R be a f.d. semisimple k-algebra and V be a simple (left) R-module of finite dimension over k. Fix integers $n_1 \leq n_2 \leq n_3$. Consider $V^{\oplus n_3}$ as an R-module and consider the sets*

$$U = \{v \in V^{\oplus n_3} \mid Rv \simeq V^{\oplus n_1}\}, \quad \mathcal{C}_{n_2,n_3} = \{C \subseteq V^{\oplus n_3} \mid C \text{ is an } R\text{-submodule}, C \simeq V^{\oplus n_2}\}.$$

Assuming that U is non-empty, then the number $\#\{C \in \mathcal{C}_{n_2,n_3} \mid u \in C\}$ is independent of u.

Proof. For each $u \in U$, $C \mapsto C/Ru$ is a bijection from $\{C \in \mathcal{C}_{n_2,n_3} \mid u \in C\}$ to $\mathcal{C}_{n_2-n_1,n_3-n_1}$. □

6.2.3 Averaging over lifts of codes

The following is a result that was shown in [GS22].

Theorem 6.19. *Let D be a $\mathbb{Q}$-division algebra and $D_{\mathbb{R}} = D \otimes_{\mathbb{Q}} \mathbb{R}$. Fix an order $\mathcal{O} \subseteq D$ and let $\mathfrak{P} \subseteq \mathcal{O}$ be varying across unramified split prime ideals in $\mathcal{O}$.*

Let $f : (D \otimes \mathbb{R})^t \to \mathbb{R}$ be a compactly supported Riemann integrable function and $t \geq 2$. Then the set of lattices $\mathcal{L}_{\mathfrak{P}}$ defined in Equation (6.1) satisfy

$$\frac{1}{\#\mathcal{L}_{\mathfrak{P}}} \sum_{\Lambda \in \mathcal{L}_{\mathfrak{P}}} \left(\sum_{v \in \Lambda \setminus \{0\}} f(v) \right) \xrightarrow{\#(\mathcal{O}/\mathfrak{P}) \to \infty} \int_{D_{\mathbb{R}}^t} f(x)dx,$$

given that the parameter k defined in Equation (6.1) lies in $\{nt-t+1, \ldots, nt-1\}$. Here, the integral on the right is with respect to a Lebesgue measure that makes $\mathcal{O}^t \subseteq D_{\mathbb{R}}^t$ unit covolume.

Proof. Let $\mathbb{F}_q \simeq \mathcal{O}_K/\mathcal{P}$. Let us define $U_{\mathcal{P}} = \{v \in M_n(\mathbb{F}_q)^{\oplus t} \mid \dim_{\mathbb{F}_q}(M_n(\mathbb{F}_q)v) = n^2\}$.

Now, let us show that the expected value of the following, taken as $C \in \mathcal{L}_{\mathfrak{P}}$, equals zero when $\mathrm{N}(\mathcal{P})$ is large enough.

$$\sum_{\substack{x \in \beta_{\mathfrak{P}} \pi_{\mathfrak{P}}^{-1}(C) \setminus \{0\} \\ \pi_{\mathfrak{P}}(x\beta_{\mathfrak{P}}^{-1}) \notin U_{\mathcal{P}}}} f(x) = \sum_{\substack{x \in \pi_{\mathfrak{P}}^{-1}(C) \setminus \{0\} \\ \pi_{\mathfrak{P}}(x) \notin U_{\mathcal{P}}}} f(\beta_{\mathfrak{P}} x). \tag{6.2}$$

If $x \in \mathcal{O}^{\oplus t}$ is such that $\pi_{\mathfrak{P}}(x) \notin U_{\mathcal{P}}$, then at least one of the $\mathcal{O}$-coordinates will guarantee the following lower bound from Lemma 6.16,

$$\|\beta_{\mathfrak{P}} x\| \gg \beta_{\mathfrak{P}} \cdot q^{\frac{1}{nm}} = q^{\frac{nk-n^2t}{n^2mt}} \cdot q^{\frac{1}{nm}} = q^{\frac{1}{nmt}(k-(nt-t))},$$

which gets arbitrarily large as $q \to \infty$. Indeed, our assumption on k implies that the exponent of q is positive.

Since f is assumed to be compactly supported, we get for each individual lattice in $\mathcal{L}_{\mathfrak{P}}$ that this sum converges to 0 as $\mathrm{N}(\mathcal{P}) \to \infty$.

Now we discuss the terms that remain. Recall $\mathcal{C}_{\mathfrak{P}}$ defined in Equation (6.1). Observe that Lemma 6.18 forces that if $\pi_{\mathfrak{P}}(x) \in U_{\mathcal{P}}$, then

$$\#U_{\mathcal{P}} \cdot \#\{C \in \mathcal{C}_{\mathfrak{P}} \mid \pi_{\mathfrak{P}}(x) \in C\} \simeq \#\mathcal{C}_{\mathfrak{P}} \cdot q^{nt}.$$

Here $\simeq$ means that the ratio of both the quantities tends to 1 as $q \to \infty$. Note that $\#C_{\mathfrak{P}} = \#\mathcal{L}_{\mathfrak{P}}$. Now let $g : M_n(\mathbb{F}_q)^{\oplus t} \to \mathbb{R}^+$ denote the function $g(c) = \sum_{x \in \pi_{\mathfrak{P}}^{-1}(c) \setminus \{0\}} f(\beta_{\mathfrak{P}} x)$. We have that

$$\begin{aligned} \mathbb{E}_{C \in \mathcal{C}_{\mathfrak{P}}} \left(\sum_{c \in \mathcal{C} \cap U_p} g(c) \right) &= \sum_{x \in U_{\mathcal{P}}} \mathbb{E}\left(g(x)\mathbf{1}_C(x)\right) \\ &= \sum_{x \in U_{\mathcal{P}}} g(x) \frac{\#\{C \in \mathcal{C}_{\mathfrak{P}} \mid \pi_{\mathfrak{P}}(x) \in C\}}{\#\mathcal{C}_{\mathfrak{P}}} \simeq \sum_{x \in U_{\mathcal{P}}} g(x) \frac{q^{nk}}{\#U_{\mathcal{P}}}. \end{aligned} \tag{6.3}$$

Note that we have an approximation of the Riemann integral of f as

$$\lim_{q \to \infty} \sum_{x \in \mathcal{O}^{\oplus t} \setminus \{0\}} \beta_{\mathfrak{P}}^{n^2mt} f(\beta_{\mathfrak{P}} x) = \int_{\mathbb{R}^{n^2mt}} f(x)dx \tag{6.4}$$

since $\beta_{\mathfrak{P}} \to 0^+$ as $\mathrm{N}(\mathcal{P}) = q$ becomes large. The ratio $\frac{\#U_{\mathcal{P}}}{\#M_n(\mathbb{F}_q)^t} \to 1$, as $q \to \infty$ so we can replace $q^{nt}/\#U_{\mathcal{P}}$ with $q^{n(k-nt)}$ which is exactly

$$\beta_{\mathfrak{P}}^{n^2mt} = q^{-\frac{1}{m} \cdot \left(1 - \frac{k}{nt}\right) \cdot (n^2mt)}.$$

This completes the proof, because the contribution of the terms that are present in Equation (6.4) but not in Equation (6.3) is a multiple of Equation (6.2), which is zero for q large enough.

□

Hence, this tells us that the continuous average of Theorem 6.1 can be replaced by a discrete average over a sufficiently large number up to some arbitrarily small error. The paper [GS22] then contains a complete analysis of how large $\mathfrak{P}$ could be taken for this to work. This lets us compute the computational complexity of how long such a lattice generating algorithm will have to run for to create these lattices from division rings. This has exponential running time so a lot more work needs to be done in this direction.

Furthermore, the work in [GS22] also unifies the lower bounds due to Rogers [Rog47], Vance [Van11], Venkatesh [Ven13] and myself [Gar23] to create a general machinery to get lower bounds on sphere packings in an arbitrary dimension. This therefore leads to a large class of lower bounds that might be useful for improvements in individual dimensions.

6.2.4 Some words about Hecke points

The set of lattices in coding theory used to show these effective existence results are often the Hecke points for the corresponding homogeneous space.

Let us briefly discuss what Hecke points are using the following definition from [COU01]. Let $\mathcal{G}$ be a connected almost simple simply-connected linear algebraic group defined over $\mathbb{Q}$ such that $\mathcal{G}(\mathbb{R})$ is non-compact. Let $\Gamma \subseteq \mathcal{G}(\mathbb{Q})$ be a congruence subgroup. Then Theorem 2.12 implies that $\Gamma\backslash\mathcal{G}(\mathbb{R})$ has finite volume.

Definition 6.20. *With the above setup, for $a \in \mathcal{G}(\mathbb{Q})$, let $T_a x = \{[x\Gamma a\Gamma] \in \mathcal{G}(\mathbb{R})/\Gamma\}$.*

The Hecke operator on $L^2(\mathcal{G}(\mathbb{R})/\Gamma)$ is then defined to be the following.

$$\begin{aligned} T_a : L^2(\mathcal{G}(\mathbb{R})/\Gamma) &\to L^2(\mathcal{G}(\mathbb{R})/\Gamma) \\ f &\mapsto T_a(f) \\ T_a(f)(x) &= \frac{1}{|T_a x|} \sum_{y \in T_a x} f(y). \end{aligned}$$

The points $T_a x$ are called Hecke points.

Let us give an example of the setup with Hecke points. Consider the map $\pi_p : \mathbb{Z}^n \to \mathbb{F}_p^n$ and then consider the set

$$\mathcal{L}_p^k = \{\beta_p \pi_p^{-1}(C) \mid C \subseteq \mathbb{F}_p^n, \dim_{\mathbb{F}_p} C = k\},$$

where $\beta_p = p^{-\left(1-\frac{k}{n}\right)}$ is a constant chosen so that each lattice in $\mathcal{L}_p^k$ has covolume 1 in $\mathbb{R}^n$.

We can now consider this set a subset of

$$\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z}) = \{g\mathbb{Z}^n \mid g \in SL_n(\mathbb{R})\}.$$

Then, this set turns out to be the same as $T_a x$ for

$$x = I_n \text{ and } a = \begin{bmatrix} p^{\frac{k-n}{n}} I_k & 0 \\ 0 & p^{\frac{k}{n}} I_{n-k} \end{bmatrix}.$$

Rogers' original work [Rog47] can be thought of saying that these Hecke points equidistribute with respect to Siegel transforms. But what is also true, because of the strong results about equidistribution, is the fact that they equidistribute with respect to all test functions $\mathcal{C}_c(\mathrm{SL}_t(\mathbb{R})/\mathrm{SL}_t(\mathbb{Z}))$. Note that a Siegel transform is not a compactly supported function and therefore, equidistribution with respect to test functions is not sufficient to say that the average of Siegel transforms over the Hecke points converge to what the Siegel mean value theorem should give. If however one is able to use the bounded convergence theorem and show that the averages over Hecke points do not explode, this opens up another way to prove these theorems in the coding theory literature. Alternatively, this also allows using these coding theory results to prove mean value theorems in the continuous setting.

Using the general methods of [COU01], it should follow that the set of lattices $\mathcal{L}_{\mathfrak{P}}$ defined in Equation (6.1) equidistribute as $\#\mathcal{O}/\mathfrak{P} \to \infty$. This would involve using some S-arithmetic analogues of our algebraic group $\mathcal{G}$. Using that $\mathcal{L}_{\mathfrak{P}}$ equidistribute in the space of G-symmetric lattices that we consider, one can arrive at another proof of Theorem 1.6, if one establishes that the averages over Hecke points do not diverge to infinity by doing an analysis similar to [GSV23; GS22] for our division algebra groups.

6.3 Higher moments with $\mathcal{O}_K$-lattices

This is ongoing work [GSV23], and we will skip mentioning the proofs of the results in this section.

Siegel's mean value theorem [Sie45] answers the question of evaluating the average

$$\int_{\mathrm{SL}_t(\mathbb{R})/\,\mathrm{SL}_t(\mathbb{Z})} \left(\sum_{v \in g\mathbb{Z}^t} f(v) \right) dg.$$

Analytic formulas for higher moments were found by Rogers [Rog55]. This gives an analytic expression for the quantity

$$\int_{\mathrm{SL}_t(\mathbb{R})/\,\mathrm{SL}_t(\mathbb{Z})} \left(\sum_{v \in g\mathbb{Z}^t} f(v) \right)^n dg,$$

when $n < t$. Then in a subsequent paper, Rogers [Rog56] used these higher moments to show that random lattices in $\mathrm{SL}_t(\mathbb{R})/\,\mathrm{SL}_t(\mathbb{Z})$ behave somewhat like a Poisson point process. Here is the exact statement of this result.

Theorem 6.21. (Rogers, 1956) *Let $\Lambda \subseteq \mathbb{R}^t$ be a random unit covolume lattice in $\mathrm{SL}_t(\mathbb{R})/\,\mathrm{SL}_t(\mathbb{Z})dg$ and let S be a centrally symmetric Borel set of volume V. Consider the random variable*

$$\rho(\Lambda) := \#\left(S \cap (\Lambda \setminus \{0\})\right).$$

Then, provided the $\mathbb{Z}$-rank t of the lattices satisfies $t \geq \lceil \frac{1}{4}n^2 + 3 \rceil$, it follows that the n-th moment of the number of non-zero lattice points in S satisfies

$$2^n \cdot m_n(\tfrac{V}{2}) \leq \mathbb{E}[\rho(\Lambda)^n] \leq 2^n \cdot m_n(\tfrac{V}{2}) + E_{n,t} \cdot (V+1)^{n-1},$$

where

$$m_n(\lambda) = e^{-\lambda} \sum_{r=0}^{\infty} \frac{\lambda^r}{r!} r^n = \mathbb{E}_{X \sim \mathcal{P}(\lambda)}(X^n) \tag{6.5}$$

is the nth moment of a Poisson distribution with parameter λ and where $E_{n,t}$ is an error term decaying exponentially as t increases:

$$E_{n,t} \leq 2 \cdot 3^{\lceil \frac{n^2}{4} \rceil} \cdot (\tfrac{\sqrt{3}}{2})^t + 21 \cdot 5^{\lceil \frac{n^2}{4} \rceil} \cdot (\tfrac{1}{2})^t.$$

Given a number field K, the statement of Theorem 5.12 can be used to create an analytic formula for the expression

$$\int_{\mathrm{SL}_t(K_{\mathbb{R}})/\,\mathrm{SL}_t(\mathcal{O}_K)} \left(\sum_{v \in g\mathcal{O}_K^t} f(v) \right)^n dg,$$

for the case when $n < t$. This is Theorem 1.8 as given in the introduction.

As we mentioned before, such a result is also available in the context of $\mathcal{O}_\mathrm{K}$-lattices and implicit in the literature. For instance, S. Kim [Kim19] establishes an integral formula in the adelic language and deduces convergence of the second moment. See also, e.g., [Wei65] and [Hug23, Theorem 1]. However, what is new in our work is that the upper bounds on the higher moments are tight enough estimates with which we could imply a Poisson-like behaviour.

On $K_\mathbb{R}$, we define the following positive-definite real quadratic form on $K_\mathbb{R}$.

$$\langle x, y \rangle = \Delta_K^{-\frac{2}{[K:\mathbb{Q}]}} \operatorname{tr}(x\overline{y}). \tag{6.6}$$

Here Δ_K is the absolute value of the discriminant of the number field K. Note that the quadratic form makes $\mathcal{O}_K$ into a lattice in $K_\mathbb{R}$ and the normalisation in Equation (6.6) ensures it has unit covolume. When multiple copies $K_\mathbb{R}$ are considered, we will assume that the quadratic form is the sum of the quadratic forms from Equation (6.6) on each copy. This quadratic form therefore defines a Lebesgue measure on any number of copies of $K_\mathbb{R}$.

The theorem obtained in [GSV23] claims the following.

Theorem 6.22. (In preparation)
Let K be any number field and let n be fixed. Let ω_K be the root number of K, that is the number of roots of unity present in K. Then there is an explicit constant $t_0(K,n) = O_K(n^3 \log\log n)$ such that the n-th moment $\mathbb{E}[\rho(\Lambda)^n]$ of the number of nonzero lattice points lying in an origin-centered ball of volume V and a random unit covolume $\mathcal{O}_K$-lattice of rank t satisfies

$$\omega_K^n \cdot m_n(\tfrac{V}{\omega_K}) \leq \mathbb{E}[\rho(\Lambda)^n] \leq \omega_K^n \cdot m_n(\tfrac{V}{\omega_K}) + E_{n,t,K} \cdot (V+1)^{n-1}$$

with the error term

$$E_{n,t,K} \leq C_K \cdot t^{(n-2)/2} \cdot e^{-\varepsilon_K \cdot (t-t_0)}$$

provided that $t > t_0(K,n)$. Here, m_n is as defined in Equation (6.5) and the ball of volume V is with respect to the Euclidean norm given in Equation (6.6). The constants $C_K, \varepsilon_K > 0$ are uniform in the rank t of the $\mathcal{O}_K$-lattices and can also be explicitly described.

In fact, height considerations allow us to prove stronger asymptotic results by increasing not just the $\mathcal{O}_K$-rank of the lattices, but also the degree of the number field. More precisely, we show the following theorem.

Theorem 6.23. (In preparation)
Let $\mathcal{S}$ denote any set of number fields K such that the absolute Weil height of elements in $K^\times \setminus \mu_K$ has a strictly positive uniform lower bound on $\mathcal{S}$. There are then for a given n explicit constants $t_0(n,\mathcal{S}) = O_{\mathcal{S}}(n^3 \log\log n)$ as well as explicit constants $C, \varepsilon > 0$, all uniform in $\mathcal{S}$, such that for any $t > t_0$ and for any $K \in \mathcal{S}$ of degree d the n-th moment $\mathbb{E}[\rho(\Lambda)^n]$ of the number of nonzero $\mathcal{O}_K$-lattice points in an origin-centered ball of volume V and Λ in the space of unit covolume $\mathcal{O}_K$-lattices of rank t satisfies

$$\omega_K^n \cdot m_n(\tfrac{V}{\omega_K}) \leq \mathbb{E}[\rho(\Lambda)^n] \leq \omega_K^n \cdot m_n(\tfrac{V}{\omega_K}) + E_{n,t,K} \cdot (V+1)^{n-1}.$$

where the error term satisfies

$$E_{n,t,K} \leq C \cdot (td)^{(n-2)/2} \cdot \omega_K^{n^2/4} \cdot Z(K,t,n) \cdot e^{-\varepsilon \cdot d(t-t_0)}.$$

Here, ω_K are the number of roots of unity in K, $Z(K,t,n)$ denotes a finite product of Dedekind zeta values ζ_K at certain real values > 1 and m_n is as in Equation (6.5).

Remark 6.24. *Note that the terms $(td)^{(n-2)/2} \cdot \omega_K^{n^2/4}$ grow polynomially in t, d since $\omega_K = O(d \log\log d)$ and the error term indeed decays exponentially in the dimension of the lattices.*

The height bound assumption on $\bigcup_{K \in \mathcal{S}} K$ in Theorem 6.23 is in the literature referred to as the Bogomolov property. A prototypical example of an infinite tower satisfying the Bogomolov property are the cyclotomic numbers $\mathbb{Q}^{cyc} = \bigcup_{i \geq 2} \mathbb{Q}(\zeta_i)$, where ζ_i is the ith root of unity. Hence, the limiting results of Theorem 6.23 in particular apply to lattices over cyclotomic integers of increasing degree for fixed large enough rank.

We also partially prove in this result the necessity of the height bound assumption in Theorem 6.23, showing that for any fixed rank t, there exist number fields K_i of arbitrarily large degree with moments strictly larger than Poisson of mean V/ω_{K_i}.

We refer the reader unfamiliar with heights and the Bogomolov property to the following section for details and some examples of infinite extensions with this property.

6.3.1 Mahler measures and the Bogomolov property

For an algebraic number $\alpha \in K^\times$, recall that the Mahler measure (or non-normalised exponential Weil height) is given by the product over the set of places M_K of K:

$$H_W(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}$$

which will be more directly relevant for estimates in the Euclidean space associated to K. The two coincide for algebraic integers and in general differ by a denominator. We also recall that the absolute Mahler measure (or exponential Weil height) of an algebraic number α is given by $H_W(\alpha)^{\frac{1}{\deg(\alpha)}}$ and we shall denote by

$$h(\alpha) = \tfrac{1}{\deg(\alpha)} \log(H_W(\alpha)),$$

the Weil height of an algebraic number.

Remark 6.25. *Note that the absolute Mahler measure and Weil heights are independent of the subfield over which one is considering an algebraic integer. That is, if $\beta \in K$ we have $\deg \beta = \#\{\sigma : \mathbb{Q}(\beta) \to \mathbb{C}\}$ and*

$$\frac{\log\left(\prod_{\sigma:K\to\mathbb{C}} \max\{1, |\sigma(\beta)|\}\right)}{[K:\mathbb{Q}]} = \frac{\log\left(\prod_{\sigma:\mathbb{Q}(\beta)\to\mathbb{C}} \max\{1, |\sigma(\beta)|\}\right)}{[\mathbb{Q}(\beta):\mathbb{Q}]}.$$

Lehmer's famous problem asks for a uniform lower bound for $h(\alpha)\deg(\alpha)$. We shall consider algebraic numbers related to the stronger property:

Definition 6.26. *A subset $S \subset \overline{\mathbb{Q}}$ is said to satisfy the Bogomolov property if there exists a constant $C > 0$ such that*

$$h(\alpha) \geq C$$

provided $\alpha \in S$ has infinite multiplicative order.

We now recall some important examples from the literature when the Bogomolov property is satisfied. The first result is a bound due to Schinzel [Sch73].

Theorem 6.27. *Assume that an algebraic number α of infinite multiplicative order is contained in a totally real field. Then, denoting by $\varphi = \frac{1+\sqrt{5}}{2}$ the golden ratio, we have*

$$h(\alpha) \geq \frac{1}{2}\log\varphi \approx 0.2406\ldots.$$

Moreover, the same is true for α in a CM[2] field provided one (and equivalently, all) of its Archimedean embeddings satisfy $|\alpha| \neq 1$.

We therefore get that Theorem 6.27 also applies to algebraic integers in CM fields, however there exist algebraic numbers which are not roots of unity but all of whose conjugates lie on the unit circle-in fact the bound is violated for such numbers. We do, however, have for abelian extensions the bound due to Amoroso–Dvornicich [AD00].

Theorem 6.28. *Assume that an algebraic number α of infinite multiplicative order is contained in an abelian extension of $\mathbb{Q}$. Then we have*

$$h(\alpha) \geq \frac{\log 5}{12} \approx 0.1341\ldots.$$

Beyond these results, the Bogomolov property is well-studied and there are a number of subsets of $\overline{\mathbb{Q}}$ satisfying it leading to more towers of number fields with the Bogomolov property. We refer the reader to [MS21, Chapter 11] and [ADZ14] for more details.

We end our discussion with some height bounds that work for every number field, in particular, we state E. Dobrowolski's asymptotic result [Dob79, Theorem 1].

Theorem 6.29. *Let α be an algebraic integer of degree d, not zero or a root of unity, and let $\varepsilon > 0$. Then for $d \geq d(\varepsilon)$, we have that*

$$h(\alpha) \geq \frac{1-\varepsilon}{d} \cdot \left(\frac{\log\log d}{\log d}\right)^3.$$

Moreover, P.Voutier [Vou96] showed that for any $d \geq 2$, we may take

$$h(\alpha) \geq \frac{1}{4d} \cdot \left(\frac{\log\log d}{\log d}\right)^3.$$

[2] CM stands for complex multiplication. Cyclotomic fields are CM and so are quadratic extensions of $\mathbb{Q}$.

Chapter 7

Conclusion

Let us give some ideas about future works.

One obvious project for the future is to attempt to demystify some of the other candidates of lattices in Chapter 3. There may be some new types of homogeneous spaces of lattices there to explore for lattice packings. Another place to look further may be the $t = 1$ case of Section 5.2.2. Here, the Euclidean lattices are points on a compact manifold and the smaller value of t is useful to have a smaller dimension of the space, however the integration formulas are complicated.

A very important problem is the project of derandomizing lattice packings. That is, instead of giving a list of random lattices such that one of the lattices satisfies the Minkowski-Hlawka lower bound, one would like to give an explicit lattice in polynomial time in terms of the dimension d that has good packing density. One approach to do this derandomization is to pick pseudorandomly a lattice among the collections of lattices given in Section 6.2.

Other than this, the appearance of the height zeta functions provides us with analytic formulae involving these complicated objects. Height zeta functions are interesting because they are connected with counting rational points of bounded height [FMT89] and are related to Eisenstein series of certain algebraic groups. By playing around with the algebraic groups $\mathcal{G}$ and the representations V on which the group acts, one might see height zeta functions of other varieties and exploring these analytic formulae might be a useful in trying to prove their analytic continuity.

Additionally, the higher moment results for $\mathcal{O}_K$-lattices might lead to improvements in the lattice covering problem. Recent progress in [ORW22], other than relying on the bounds in Kakeya-type problems, also relies on Rogers' estimates on the probability of a random lattice being able to cover all space, let's say with balls of a fixed radius R [Rog58]. It is worth exploring if an improvement on this new result could be made by just restricting to $\mathcal{O}_K$-lattices and leveraging the extra symmetries.

So to conclude, the quest to improve lower bounds on lattice packings will continue beyond this work and I hope that humanity concurs lattices sooner than later. Although Prof. Henry Cohn says that the lack of clarity about high dimensional sphere packings is an embarrassment to humanity, it could also be sometimes consoling to know that lattice packings will continue to intrigue mankind for plenty of years to come and not just to pack spheres.

Bibliography

[Ami55] Shimshon Amitsur. "Finite Subgroups of Division Rings". In: *Transactions of the American Mathematical Society* 80.2 (1955), pp. 361–386.

[ADZ14] Francesco Amoroso, Sinnou David, and Umberto Zannier. "On Fields with Property (B)". In: *Proceedings of the American Mathematical Society* 142.6 (2014), pp. 1893–1910.

[AD00] Francesco Amoroso and Roberto Dvornicich. "A Lower Bound for the Height in Abelian Extensions". In: *Journal of Number Theory* 80.2 (2000), pp. 260–272.

[ACM19] Jayadev S. Athreya, Yitwah Cheung, and Howard Masur. "Siegel-Veech Transforms are in L2." In: *Journal of Modern Dynamics* 14 (2019).

[Ban88] Behnam Banieqbal. "Classification of Finite Subgroups of $2\times$ 2 Matrices over a Division Algebra of Characteristic Zero". In: *Journal of Algebra* 119.2 (1988), pp. 449–512.

[BG19] Michael Björklund and Alexander Gorodnik. "Central Limit Theorems for Diophantine Approximants". In: *Mathematische Annalen* 374.3-4 (2019), pp. 1371–1437.

[Bor12] Armand Borel. *Linear Algebraic Groups*. Vol. 126. Springer Science & Business Media, 2012.

[Bor19] Armand Borel. *Introduction to Arithmetic Groups*. Vol. 73. American Mathematical Soc., 2019.

[BH62] Armand Borel and Harish-Chandra. In: *Annals of Mathematics* 75.3 (1962), pp. 485–535.

[Cam18] Antonio Campello. "Random Ensembles of Lattices From Generalized Reductions". In: *IEEE Transactions on Information Theory* 64.7 (2018), pp. 5231–5239.

[COU01] Laurent Clozel, Hee Oh, and Emmanuel Ullmo. "Hecke Operators and Equidistribution of Hecke Points". In: *Inventiones mathematicae* 144.2 (2001), pp. 327–351.

[CE03] Henry Cohn and Noam Elkies. "New Upper Bounds on Sphere Packings I". In: *Annals of Mathematics* 157.2 (2003), pp. 689–714.

[CKMRV17] Henry Cohn, Abhinav Kumar, Stephen Miller, Danylo Radchenko, and Maryna Viazovska. "The Sphere Packing Problem in Dimension 24". In: *Annals of Mathematics* 185.3 (2017), pp. 1017–1033.

[CS13] J. Conway and Neil J. Sloane. *Sphere Packings, Lattices and Groups*. Grundlehren der mathematischen Wissenschaften. Springer New York, 2013.

[Dob79] Edward Dobrowolski. "On a Question of Lehmer and the Number of Irreducible Factors of a Polynomial". In: *Acta Arithmetica* 34.4 (1979), pp. 391–401.

[ELZ05] Uri Erez, Simon Litsyn, and Ram Zamir. "Lattices which are Good for (Almost) Everything". In: *IEEE Transactions on Information Theory* 51.10 (2005), pp. 3401–3416.

[For73] Charles Ford. "Finite Groups and Division Algebras". In: *L'Enseignement Mathématique* 19 (1973), pp. 313–327.

[FMT89] Jens Franke, Yuri I. Manin, and Yuri Tschinkel. "Rational Points of Bounded Height on Fano Varieties". In: *Inventiones Mathematicae* 95.2 (1989), pp. 421–435.

[Gar23] Nihar P. Gargava. "Lattice Packings Through Division Algebras". In: *Mathematische Zeitschrift* 303.1 (2023), pp. 1–32.

[GS22] Nihar P. Gargava and Vlad Serban. "Dense Packings via Lifts of Codes to Division Rings". In: *IEEE Transactions on Information Theory* (2022).

[GSV23] Nihar P. Gargava, Vlad Serban, and Maryna Viazovska. "Moments of the Number of Points in a Bounded Set for Number Field Lattices". In: *arXiv:2308.15275* (2023).

[Han07] Timo Hanke. "The Isomorphism Problem for Cyclic Algebras and an Application". In: *Proceedings of the 2007 international symposium on symbolic and algebraic computation*. 2007, pp. 181–186.

[Has66] Helmut Hasse. "Über die Dichte der Primzahlen p, für die eine Vorgegebene Ganzrationale Zahl a≠ 0 von Gerader Bzw. Ungerader Ordnung Mod. p ist". In: *Mathematische Annalen* 166.1 (1966), pp. 19–23.

[Hla43] Edmund Hlawka. "Zur Geometrie der Zahlen". In: *Mathematische Zeitschrift* 49.1 (1943), pp. 285–312.

[Hug23] Nathan Hughes. "Mean Values over Lattices in Number Fields and Effective Diophantine Approximation". In: *arXiv:2306.02499* (2023).

[Jac09] Nathan Jacobson. *Finite-dimensional Division Algebras over Fields*. Springer Science & Business Media, 2009.

[Kim19] Seungki Kim. "Counting Rational Points on a Grassmannian". In: *arXiv:1908.01245* (2019).

[Kna13] Anthony W. Knapp. *Lie Groups Beyond an Introduction*. Vol. 140. Springer Science & Business Media, 2013.

[Lam01] T Lam. "Finite Groups Embeddable in Division Rings". In: *Proceedings of the American Mathematical Society* 129.11 (2001), pp. 3161–3166.

[MS21] James McKee and Chris Smyth. *Around the Unit Circle: Mahler Measure, Integer Matrices and Roots of Unity*. Universitext. Springer International Publishing, 2021.

[MR09] Daniele Micciancio and Oded Regev. *Lattice-based Cryptography*. Springer, 2009, pp. 147–191.

[Mor15] Dave W. Morris. *Introduction to Arithmetic Groups*. Vol. 2. Deductive Press Lieu de publication inconnu, 2015.

[Nac76] Leopoldo Nachbin. *The Haar Integral*. RE Krieger Pub. Co., 1976.

[ORW22] Or Ordentlich, Oded Regev, and Barak Weiss. "New Bounds on the Density of Lattice Coverings". In: *Journal of the American Mathematical Society* 35.1 (2022), pp. 295–308.

[Pie12] Richard S. Pierce. *Associative Algebras*. Vol. 88. Springer Science & Business Media, 2012.

[Rei03] Irwing Reiner. *Maximal Orders*. London Mathematical Society monographs series: London Mathematical Society. Clarendon Press, 2003.

[RZ13] Gaël Rémond and Christine Zehrt-Liebendörfer. "Le Théorème de Schanuel pour un Corps Non-commutatif". In: *Rendiconti del Seminario Matematico della Università di Padova* 130 (2013), pp. 221–282.

[Rog47] Claude A. Rogers. "Existence Theorems in the Geometry of Numbers". In: *Annals of Mathematics* (1947), pp. 994–1002.

[Rog55] Claude A. Rogers. "Mean Values over the Space of Lattices". In: *Acta mathematica* 94 (1955), pp. 249–287.

[Rog56] Claude A. Rogers. "The Number of Lattice Points in a Set". In: *Proceedings of the London Mathematical Society* 3.2 (1956), pp. 305–320.

[Rog58] Claude A. Rogers. "Lattice Coverings of Space: the Minkowski-Hlawka Theorem". In: *Proceedings of the London Mathematical Society* 8.3 (1958), pp. 447–465.

[Sch73] Andrzej Schinzel. "On the Product of the Conjugates outside the Unit Circle of an Algebraic Number". In: *Acta Arithmetica* 24.4 (1973), pp. 385–399.

[Sch58] Wolfgang Schmidt. "On the Convergence of Mean Values over Lattices". In: *Canadian Journal of Mathematics* 10 (1958), pp. 103–110.

[Sch67] Wolfgang M. Schmidt. "On Heights of Algebraic Subspaces and Diophantine Approximations". In: *Annals of Mathematics* (1967), pp. 430–472.

[Ser77] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Vol. 42. Springer, 1977.

[Ser09] Jean-Pierre Serre. *Lie Algebras and Lie Groups: 1964 Lectures given at Harvard University*. Springer, 2009.

[Sie45] Carl L. Siegel. "A Mean Value Theorem in Geometry of Numbers". In: *Annals of Mathematics* (1945), pp. 340–347.

[Slo98] Neil J. Sloane. "Kepler's Conjecture Confirmed". In: *Nature* 395.6701 (1998), pp. 435–436.

[Van11] Stephanie Vance. "Improved Sphere Packing Lower Bounds from Hurwitz Lattices". In: *Advances in Mathematics* 227.5 (2011), pp. 2144–2156.

[Ven13] Akshay Venkatesh. "A Note on Sphere Packings in High Dimension". In: *International Mathematics Research Notices* 2013.7 (2013), pp. 1628–1642.

[Via17] Maryna Viazovska. "The Sphere Packing Problem in Dimension 8". In: *Annals of Mathematics* 185.3 (2017), pp. 991–1015.

[Vou96] Paul Voutier. "An Effective Lower Bound for the Height of Algebraic Numbers". In: *Acta Arithmetica* 74.1 (1996), pp. 81–95.

[Wei58] André Weil. *Discontinuous Subgroups of Classical Groups: Lectures*. University of Chicago, 1958.

[Wei65] André Weil. "Sur la Formule de Siegel dans la Théorie des Groupes Classiques". In: *Acta mathematica* 113.1-87 (1965), p. 2.

Curriculum Vitae

Email: nihar.gargava@epfl.ch, nihargargava@gmail.com
Website: nihargargava.com
Date of Birth: 06 August 1995
Nationality: India

1 Education

Doctor of Philosophy, Mathematics
Thesis: Mean value theorems for collections of lattices with a prescribed group of symmetries
Doctoral advisor: Prof. Maryna Viazovska
École Polytechnique Fédérale de Lausanne, Switzerland Sep 2019 - Sept 2023

Master of Science, Mathematics
Thesis: Asymptotic Bounds on Error-correcting Codes
École Polytechnique Fédérale de Lausanne, Switzerland Sep 2017 - Feb 2019

Bachelor of Science (Hons.), Mathematics and Scientific Computing
Indian Institute of Technology Kanpur, India Jul 2013 - May 2017

2 List of publications

- Moments of the number of $\mathcal{O}_K$-lattice points in a bounded set 2023
  with V. Serban and M. Viazovska.
  arXiv: 2308.15275
- Dense packings via lifts of codes to division rings 2022
  with V. Serban. *IEEE Trans. Inf. Theory*
  arXiv:2111.03684
- Lattice packings through division algebras 2022
  Math. Z.
  arXiv:2107.04844

3 List of talks

- Quantum Gate Synthesis and Ramanujan May 2023
  Quantum Science Days 2023, Online
- Random Arithmetic Lattices as Sphere Packings May 2023
  Arithmetic Statistics in Automorphic Forms and Analytic Number Theory, Lausanne
- Réseaux arithmétiques aléatoires en tant qu'empilage de sphères Mar 2023
  École de Printemps en Géométrie et Dynamique, Lille
- Random Lattices as Sphere Packings Nov 2022
  Combinatorics and Arithmetic for Physics: Special Days, Institut des Hautes Études Scientifiques, Paris

- Lattice Packings through Division Algebras May 2022
  Doctoral Day of the Swiss Math Society, Fribourg
- Dense Packings via Lifts of Codes to Division Rings Mar 2022
  Workshop on Coding and Cryptography 2022, University of Rostock, Online
- Lattice Packings through Division Algebras Jan 2022
  Optimal Point Configurations on Manifolds, Erwin Schrödinger International Institute, Vienna
- Lattice Packings through Division Algebras Oct 2021
  Maine-Quebec Number Theory Conference, Online
- Lattice Packings through Division Algebras Sep 2021
  Point Distributions Webinar, Online
- Lattice Packings through Division Algebras Aug 2021
  Young Researchers in Algebraic Number Theory III, Heilbronn Institute, Online
- Asymptotic Lower Bounds on Sphere Packing Efficiency of Lattices Nov 2020
  Algebraic geometry seminar, IIT Bombay, Online

4 Academic activities

4.1 Doctoral coursework at EPFL

- *Logic synthesis in quantum computing* Spring 2022
- *Modular forms and applications* Spring 2022
- *Monstrous moonshine* Fall 2021
- *Semidefinite optimization and applications to geometric and combinatorial Problems* Fall 2019
- *Topics in arithmetic number theory* Fall 2019

4.2 Training activities

- *Workshop: Renormalization and Visualization for packing, billiard and surfaces, Centre International de Rencontres Mathématiques, Marseille* Jul 2023
- *Workshop: Optimal Point Configurations on Manifolds, Erwin Schrödinger International Institute, Vienna* Jan 2022
- *Zoom Workshop on Sphere Packing and the Conformal Bootstrap, Simons Center for Geometry and Physics, Online* Dec 2020
- *Online Summer School on Optimization, Interpolation and Modular Forms, EPFL, Online* Aug 2020

4.3 Teaching experience

4.3.i Doctoral student

- Teaching assistant for *Discrete Mathematics* Spring 2023
- Head teaching assistant for *Discrete Mathematics* Spring 2022
- Teaching assistant for *Metric Spaces and Topology* Fall 2021
- Head teaching assistant for *Discrete Mathematics* Spring 2021
- Teaching assistant for *Metric Spaces and Topology* Fall 2020
- Teaching assistant for *Lie Groups* Spring 2020
- Teaching assistant for *Metric Spaces and Topology* Fall 2019

4.3.ii Master student

- Teaching assistant for *Advanced Linear Algebra for Physics - II* Spring 2018
- Teaching assistant for *Advanced Linear Algebra for Physics - I* Fall 2018

4.3.iii Bachelor student

- Interest group leader: Combinatorics, Number Theory, Representation, Algebra 2016-2017
- Academic Mentor for Mathematics, Counseling Service 2014-2015

5 Other professional experience

- Research intern, *Quantinuum, Cambridge (UK)* Sep 2022 - Jan 2023
- Research student, *Chair of Number theory, EPFL* Feb 2019 - Aug 2019
- Research intern, *Laboratoire d'Informatique de Paris-Nord, Université Paris-Nord* May 2016 - Jul 2016

6 Awards and achievements

- Outstanding performance award, École Doctorale de Mathématique, EPFL Fall 2021
- Charles Rapin grant for master studies, EPFL 2018
- J. N. Tata scholarship for higher education, India 2017
- Academic excellence award, IIT Kanpur, 2017
- Charpak research internship program, Embassy of France in India 2016
- INSPIRE Scholarship, Department of Science and Technology, Government of India 2013-17
- Cleared the Joint Entrance Exam, a two-phase engineering entrance test in India 2013

7 Languages

- English (professional, fluent)
- French (intermediate)
- Hindi (native)
- Gujarati (intermediate)