

SHAPES OF MULTIQUADRATIC EXTENSIONS

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF THE  
UNIVERSITY OF HAWAI'I AT MĀNOA IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

AUGUST 2019

By

Jamal Hassan Haidar

Dissertation Committee:

Robert Harron, Chairperson

Michelle Manes

Pavel Guerzhoy

Piper H

Rosanna Alegado

Copyright 2019 by  
Jamal Hassan Haidar

## ACKNOWLEDGMENTS

I would like to thank my advisor, Robert Harron, for selecting an interesting problem for me to work on, as well as for all his patience and help along the way. I am grateful to the committee members, for taking the time to read my thesis and provide excellent feedback. I am especially thankful for Piper H for being my unofficial co-advisor and dissertation doula. Her dedication and willingness to help in all matters, mathematical and emotional, played a major role in my deliverance of a timely, healthy thesis.

I appreciate all the math conversations that took place in the graduate lounge. I want to thank Tom Craven, Rufus Willett, Clément Dell'Aiera, Asaf Hadari, Ruth Hass, and Elizabeth Gross for taking the time to answer many questions. I would also like to thank the secretaries, Sue and Alicia, for their continuous hard work to keep the math department, as well as all its constituents, in order. I want to thank Erik Holmes, as his curiosity and interest in my project led to some very useful realizations. I would like to give a very special thanks to Bella Tobin for being an indispensable colleague and friend and during our last year of grad school, helping me replace stress with laughter, meet deadlines, and have an enjoyable experience.

I am extremely grateful for my family, and all the sacrifices they made to ensure that I receive the best education they could provide. Lastly, I would like to thank Tom for his invaluable friendship and emotional support throughout my entire graduate experience. His wisdom spoke so deeply to me, without having to use any words.

# ABSTRACT

For a positive integer  $n$ , we compute the shape of a totally real multiquadratic extension of degree  $2^n$  in which the prime 2 does not ramify. From this calculation, we see that the shape of such a number field is parametrized by the generators of its  $2^n - 1$  quadratic subfields. Restricting to the case  $n = 3$ , we use this parametrization to count the number of triquadratic extensions of bounded discriminant and bounded shape parameters. We then show that, as the discriminant goes to infinity, these shapes become equidistributed in a regularized sense in the subset of the space of shapes of rank 7 lattices that contains them.

# TABLE OF CONTENTS

<b>Acknowledgments</b> . . . . .	<b>iii</b>
<b>Abstract</b> . . . . .	<b>iv</b>
<b>1 Introduction</b> . . . . .	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Statement of Main Results . . . . .	3
<b>2 Background Material</b> . . . . .	<b>4</b>
2.1 Lattices . . . . .	4
2.1.1 Basic Definitions . . . . .	4
2.1.2 The Shape of a Lattice . . . . .	7
2.1.3 Gram Matrices . . . . .	8
2.2 The Geometry of Numbers . . . . .	10
2.2.1 Number Fields . . . . .	10
2.2.2 Minkowski Space . . . . .	11
2.2.3 Orthogonal Projection . . . . .	12
2.2.4 The Shape of a Number Field . . . . .	13
2.3 A Special Family of Lattices . . . . .	14
2.3.1 The Matrix $A_n$ . . . . .	14
2.3.2 The Lattice $\mathcal{D}^*$ . . . . .	15
2.3.3 Primitive Orthorhombic Lattices . . . . .	16
2.4 The Space of Shapes . . . . .	20
2.4.1 Equidistribution . . . . .	21
<b>3 Multiquadratic Extensions and Their Shapes</b> . . . . .	<b>24</b>
3.1 Multiquadratic Extensions . . . . .	24

3.1.1	Basic Results . . . . .	24
3.1.2	The Case of Interest . . . . .	25
3.1.3	The Galois Group . . . . .	26
3.1.4	An Integral Basis for $K_n$ . . . . .	27
3.2	The Shape . . . . .	28
3.2.1	The Shape of $K_2$ . . . . .	29
3.2.2	A Geometric Point of View . . . . .	33
<b>4</b>	<b>Counting Number Fields . . . . .</b>	<b>35</b>
4.1	Counting Triquadratic Number Fields . . . . .	35
4.2	Parametrization . . . . .	36
4.2.1	Strongly Carefree Tuples . . . . .	36
4.2.2	Choosing Generators . . . . .	40
4.2.3	A Correspondence Between Fields and Points . . . . .	40
4.3	Volume . . . . .	44
4.4	Sieving . . . . .	49
4.4.1	Counting Strongly Carefree Tuples . . . . .	49
4.4.2	The $p$ -adic Density . . . . .	52
4.4.3	The Case $(D_1, \dots, D_7) \equiv (1, \dots, 1) \pmod{4}$ . . . . .	54
4.5	Equidistribution . . . . .	56
	<b>Bibliography . . . . .</b>	<b>58</b>

# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

The shape of a number field is an invariant that stems from the geometry of numbers. The study of shapes of number fields was first introduced in [Ter97], where the author shows that the shapes of (real or imaginary) cubic fields, when ordered by their absolute discriminants, become equidistributed in the space of shapes of rank-2 lattices. In [BH16], the authors show that, when ordered by their absolute discriminants,  $S_n$ -number fields of degree  $n = 3, 4$ , and  $5$  have shapes that become equidistributed in the space of shapes as the absolute discriminant tends to infinity. In particular, their calculations for  $n = 3$  simplify the methods used in [Ter97]. In [Har17] and [Har19], it is shown that the shape of complex cubic fields is a complete invariant of the field. The author also gives results regarding the equidistribution of these shapes. Furthermore, in [BS14] the authors show an equidistribution result for shapes of real cubics. More recently, in [HH19], the authors explore the equidistribution of shapes of Galois quartics.

The study of shapes of low-degree number fields is an area of active research. For example, in the case of quartic extensions, the shapes of these number fields are being studied according to their Galois closure. Little is known about the shapes of general number fields in higher dimensions. The computation of the shape relies on the ability to exhibit a nice integral basis for the corresponding ring of integers of the number field, which can be a difficult task. This thesis aims to tackle the computation of shapes of a specific family of number fields, called *multiquadratic extensions*, which are degree- $2^n$  analogues of quadratic extensions. Precisely, for a set  $\{D_{2^0}, \dots, D_{2^{n-1}}\}$  of  $n$  distinct, squarefree integers, a multiquadratic extension generated by these integers is defined as the number field

$$K_n := \mathbf{Q}(\sqrt{D_{2^0}}, \dots, \sqrt{D_{2^{n-1}}}).$$

These number fields have the advantage of being Galois over  $\mathbf{Q}$ . Additionally, the integral basis we use gives a representative of the shape that can be parametrized in a relatively simple way. This allows us to study the distribution of shapes of such extensions.

Chapter 2 will cover a general overview of the shape of a lattice. Here, we are taking full lattices in a finite-dimensional real inner product space  $V$ . Once this is achieved, we will define the space of shapes corresponding to full lattices in  $V$ , emphasizing the viewpoint of describing it as a space of matrices. We will also discuss a more geometric approach to the notion of shape in lower dimensions.

With the definition of shape of a lattice, we turn to number fields. As it turns out, the geometry of numbers enables us to embed a number field into its Minkowski space. Upon doing so, the image under this embedding of the ring of integers turns out to be a full lattice. This allows us to study the shapes of number fields.

With a specific family of number fields in mind, one is naturally led to the question of how the shapes of number fields in this collection are distributed. We will give a precise definition of equidistribution, which is dependent on the natural measure associated to the space of shapes.

In Chapter 3, we will define multiquadratic extensions in full generality. Then, we will see that these number fields are classified into three subfamilies, which will depend on congruence conditions modulo 4 on their set of generators. Corresponding to these subfamilies, we can then compute their integral bases, which is a crucial ingredient in the calculation of the shape.

This thesis covers one specific subfamily of multiquadratic extensions, namely, the case in which all the generators are congruent to 1 modulo 4. We also restrict our study to multiquadratic extensions that are *totally real*. As we will see, totally real multiquadratic fields are precisely those whose generating set consists of positive integers. These restrictions simplify arguments, but the essential ideas of the method should work in general.

Given these restrictions, we proceed to compute the shape. Furthermore, we explore the subset of the full space of shapes that our family corresponds to. In the computation of the shapes of these number fields, we will see that the entries of the representing matrices are in terms of the generators of the fields. By placing a bound on the discriminant of the number fields, we place a bound on these generators, which transform the problem into one of counting integers.

Chapter 4 will describe the methods we use for counting multiquadratic extensions. In this chapter, we further restrict our collection of number fields to the case when  $n = 3$ , studying the so called *triquadratic extensions*.

This chapter will be broken up into four major components. First, we *parametrize* our triquadratic extensions, turning the count of number fields into a count of integer points.

Next, by imposing a bound on the discriminant, our count becomes finite. Along with counting number fields with a prescribed shape, we see that these number fields, parametrized by integer points, occupy some bounded Euclidean region. The *principle of Lipschitz* allows us to approximate the number of points in this region with the region's volume.

Since not all of the points in this region correspond to a number field of interest, we refine the count with a *sieve* that discards these extra points.

Chapter 4 concludes with two important theorems. The first is a statement regarding the count of triquadratic extensions with the right congruence conditions modulo 4, with bounded discriminant and prescribed shape. Lastly, this theorem lends itself to the proof that the shapes of these fields are indeed equidistributed in the subset of the space of shapes in which they reside.

## 1.2 Statement of Main Results

The motivation behind this thesis is to prove that, as the discriminant tends to infinity, the shapes of totally real multiquadratic extensions  $K_n$  in which 2 does not ramify become equidistributed in the subset of the space of shapes that contains them.

We let  $\ell = 2^n - 1$ . With  $\mathcal{S}_\ell$  denoting the space of shapes of rank  $\ell$  lattices, we let  $\mathcal{S}_{K_n}$  denote the subset of  $\mathcal{S}_\ell$  containing the shapes of the multiquadratic extensions we study. We equip this space with a natural measure  $\mu$ . In Chapter 2, we will see that this subset can be parametrized by tuples  $(X_2, \dots, X_\ell)$  of real numbers that encode the shapes of multiquadratic extensions.

For fixed positive real numbers  $R_2, \dots, R_\ell$ , we look at the subset  $W(R_2, \dots, R_\ell) \subset \mathcal{S}_{K_n}$  which places bounds on each of the shape parameters. Specifically,

$$W(R_2, \dots, R_\ell) = \{\text{sh}(X_2, \dots, X_\ell) \in \mathcal{S}_{K_n} : X_2 < \dots < X_\ell \leq R_\ell, R_j < X_j \text{ for } 2 \leq j \leq \ell - 1\}.$$

We let  $\mathcal{M}_n^+(i)$  denote the collection of totally real multiquadratic extensions in which 2 does not ramify. Furthermore, for a fixed real number  $X$ , we let

$$\mathcal{N}_n(X, R_2, \dots, R_\ell) = \#\{K_n \in \mathcal{M}_n^+(i) : \Delta(K_n) < X, \text{sh}(K_n) \in W(R_2, \dots, R_\ell)\}$$

denote the number of extensions in  $\mathcal{M}_n^+(i)$ , whose discriminants are bounded by  $X$  and whose shapes lie in  $W(R_2, \dots, R_\ell)$ . The most general statement that we wish to prove is the following:

**Conjecture 1.1.** The shapes of the fields in  $\mathcal{M}_n^+(i)$  are equidistributed in  $\mathcal{S}_{K_n}$  with respect to  $\mu$  in a regularized sense. That is, there is a positive constant  $C_n > 0$  such that for every compact  $\mu$ -continuity set  $W$  of  $\mathcal{S}_{K_n}$ , we have

$$\lim_{X \rightarrow \infty} X^{-\frac{1}{2^n-1}} \#\{K_n \in \mathcal{M}_n^+(i) : \Delta(K_n) < X, \text{sh}(K_n) \in W\} = C_n \mu(W).$$

In this thesis, we restrict to  $n = 3$ . We prove the following two results.

**Theorem 1.2.** The number of triquadratic extensions  $K_3 \in \mathcal{M}_3^+(i)$  with discriminant bounded by  $X$  and shape in  $W(R_2, \dots, R_7)$  is given by

$$\mathcal{N}_3(X, R_2, \dots, R_7) = \frac{1}{2^{10}} \prod_{p>2} (p^{-8}(p-1)^7(p+7)) \frac{30X^{\frac{1}{4}}}{56} F(R_2, \dots, R_7) + o\left(X^{\frac{1}{4}}\right),$$

where  $F(R_2, \dots, R_7)$  is a polynomial function in the variables  $\log(R_j)$ ,  $2 \leq j \leq 7$ .

**Theorem 1.3.** Conjecture 1.1 holds for  $n = 3$ .

## CHAPTER 2

### BACKGROUND MATERIAL

The first two sections of this chapter cover the background material needed for defining the shape of a number field. Section 1 begins by defining the shape of an arbitrary full-rank lattice in an  $n$ -dimensional real inner product space  $V$ . By choosing a basis of  $V$ , we get a representative of the shape of a lattice  $\Lambda$  relative to this basis which is viewed as an element of  $\mathrm{GL}_n(\mathbf{R})$ . We will want the shape of a lattice to be invariant under rotations, reflections, and scaling by a non-zero constant, so we define an action on lattices by appropriate subgroups. Furthermore, we want to identify two representatives of the same shape if the change of basis matrix is an element of  $\mathrm{GL}_n(\mathbf{Z})$ . We can encode the information of  $\Lambda$  relative to any basis with a Gram matrix.

In Section 2, we will shift our attention to number fields. From the geometry of numbers, any number field  $K$  can be embedded into its Minkowski space, which is a real inner product space. The ring of integers  $\mathcal{O}_K$  of  $K$  turns out to be a full-rank lattice in this space. As such, we wish to study its shape.

If one considers a collection of number fields of degree  $n$  and bounded discriminant, a natural question to ask is how are the shapes of these number fields distributed as the bound on the discriminant tends to infinity. The lattices arising from the ring of integers cannot be random as the discriminant grows, since  $\mathcal{O}_K$  always contains 1, which is a short vector as the discriminant goes to infinity. We will tweak the definition of shape of number fields by taking the orthogonal projection onto the orthogonal complement of the image of 1. Given a number field of degree  $n$ , the orthogonal projection onto the orthogonal complement of the image of 1 is a rank- $(n - 1)$  lattice.

Sections 3 and 4 will provide the background for the study of shapes of number fields that we encounter in Chapter 3. Section 3 is aimed at defining a specific family of lattices and computing their shapes. This simple family of shapes arises from *primitive orthorhombic lattices*. It contains the shapes of the multiquadratic extensions we study.

Once these shapes are defined, our next goal is to study the subset of the space of shapes associated to them. In section 4, we discuss these subsets, as well as define a natural measure on them. Once we are equipped with a measure, we will make a precise statement regarding equidistribution of shapes of number fields.

## 2.1 Lattices

### 2.1.1 Basic Definitions

**Definition 2.1.** Let  $V$  be a real inner product space of dimension  $n$ . For a set of linearly independent vectors  $\mathcal{B} = \{v_1, \dots, v_m\}$ , we define a *lattice*  $\Lambda$  to be the discrete subgroup of  $V$  given by the  $\mathbf{Z}$ -span

of the basis  $\mathcal{B}$ :

$$\Lambda = \mathbf{Z}v_1 + \dots + \mathbf{Z}v_m.$$

**Definition 2.2.** The integer  $m$  in the above definition is called the *rank* of the lattice, denoted by  $\text{rk}(\Lambda)$ . We say that a lattice  $\Lambda$  in  $V$  is *full* (or *of full rank in  $V$* ) if

$$\text{rk}(\Lambda) = \dim(V) = n.$$

**Definition 2.3.** Let  $\Lambda \subseteq \mathbf{R}^n$  be a full lattice generated by  $\mathcal{B} = \{v_1, \dots, v_n\}$ . A *fundamental region*  $\mathcal{R}_{\mathcal{B}}$  of  $\Lambda$  is the parallelotope determined by  $\mathcal{B}$ , described by the set

$$\mathcal{R}_{\mathcal{B}} = \left\{ \sum_{j=1}^n a_j v_j : 0 \leq a_j < 1 \right\}.$$

We denote the matrix  $M_{\mathcal{B}}$  attached to the basis  $\mathcal{B}$  by

$$M_{\mathcal{B}} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Since we are starting with a set of linearly independent vectors  $\langle v_1, \dots, v_n \rangle$ , it follows that

$$M_{\mathcal{B}} \in \text{GL}_n(\mathbf{R}).$$

Note that the volume of the fundamental region  $\mathcal{R}_{\mathcal{B}}$ , called the *covolume* of  $\Lambda$ , is given by

$$\text{Vol}(\mathcal{R}_{\mathcal{B}}) = |\det(M_{\mathcal{B}})|.$$

We get a decomposition of  $\mathbf{R}^n$  via the translates of  $\mathcal{R}_{\mathcal{B}}$  by elements of  $\Lambda$ :

$$\mathbf{R}^n = \bigcup_{x \in \Lambda} (x + \mathcal{R}_{\mathcal{B}}).$$

**Proposition 2.4.** Suppose  $\mathcal{B} = \{v_1, \dots, v_n\}$  is a basis of  $V$  that generates the lattice  $\Lambda$ . Let  $\mathcal{B}' = \{w_1, \dots, w_n\}$  be any other basis of  $V$  that also generates  $\Lambda$ . Then the corresponding change of basis matrix  $P$  is an element of  $\text{GL}_n(\mathbf{Z})$ .

*Proof.* Suppose that  $\mathcal{B}$  and  $\mathcal{B}'$  both generate a lattice  $\Lambda$ . Then, the change-of-basis matrix  $P$  is defined so that

$$M_{\mathcal{B}'} = PM_{\mathcal{B}}.$$

It follows from the definition of a lattice that  $P$  and its inverse have integer entries. It follows that

$$1 = \det(I) = \det(P) \det(P^{-1}),$$

which implies that their determinants are either 1 or  $-1$ . Thus,  $P \in \text{GL}_n(\mathbf{Z})$ .  $\square$

Since our matrix  $M_{\mathcal{B}}$  has the basis vectors  $v_1, \dots, v_n$  as its rows, we get a corresponding left action of  $\text{GL}_n(\mathbf{Z})$  on  $\text{GL}_n(\mathbf{R})$ :

$$M_{\mathcal{B}'} = P \cdot M_{\mathcal{B}}.$$

This action provides us with a bijection between lattices in  $V$  and elements of  $\text{GL}_n(\mathbf{Z}) \backslash \text{GL}_n(\mathbf{R})$  that is independent of a choice of basis, as follows.

**Definition 2.5.** We will denote by  $\mathcal{L}_n$  the set of all lattices of rank- $n$  in  $V$ . That is,

$$\mathcal{L}_n := \{\Lambda \subseteq V : \text{there exists a basis } \mathcal{B} = \{v_1, \dots, v_n\} \text{ of } V \text{ such that } \Lambda = \mathbf{Z}v_1 + \dots + \mathbf{Z}v_n\}.$$

**Lemma 2.6.** There is a one-to-one correspondence between rank- $n$  lattices  $\Lambda$  of  $V$  and elements of  $\text{GL}_n(\mathbf{Z}) \backslash \text{GL}_n(\mathbf{R})$ , given by

$$\mathcal{L}_n \longleftrightarrow \text{GL}_n(\mathbf{Z}) \backslash \text{GL}_n(\mathbf{R})$$

$$\Lambda \mapsto \text{GL}_n(\mathbf{Z}) M_{\mathcal{B}},$$

where  $\mathcal{B}$  is any basis of  $V$  that generates  $\Lambda$ .

**Example 2.7.** Consider the lattice  $\Lambda = (2\mathbf{Z})^2$  in  $\mathbf{R}^2$ . Then  $\Lambda$  can be generated by the bases  $\mathcal{B}_1$  and  $\mathcal{B}_2$ , given by

$$\mathcal{B}_1 = \{(-1, 1), (1, 1)\} \text{ and } \mathcal{B}_2 = \{(1, 1), (1, -1)\}.$$

The corresponding matrices are given by

$$M_{\mathcal{B}_1} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_{\mathcal{B}_2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Write the change of basis matrix from  $\mathcal{B}_1$  to  $\mathcal{B}_2$  as

$$P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Solving the matrix equation  $M_{\mathcal{B}_2} = PM_{\mathcal{B}_1}$  yields

$$-a + b = 1, \quad a + b = 1, \quad -c + d = 1, \quad c + d = -1.$$

We get that  $a = 0, b = 1, c = -1, d = 0$ . Hence,

$$P = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}).$$

### 2.1.2 The Shape of a Lattice

Now that we have defined a rank- $n$  lattice in  $V$ , our goal is to define a notion of *shape* of a lattice. Intuitively, we would like this shape to be an intrinsically geometric feature, which is independent of scalings and rigid motions.

We want to identify lattices that can be obtained from one another by a series of scaling, rotations and reflections. We will begin by dealing with rotations and reflections. From the matrix point of view, this is achieved by a right action on  $\mathrm{GL}_n(\mathbf{R})$  by  $\mathrm{O}_n(\mathbf{R})$ , the group of *orthogonal* matrices:

$$\mathrm{O}_n(\mathbf{R}) := \{U \in \mathrm{GL}_n(\mathbf{R}) : UU^T = U^T U = I_n\}.$$

**Definition 2.8.** We say that  $(\Lambda, \mathcal{B})$  is *equivalent* to  $(\Lambda', \mathcal{B}')$  up to rotations and reflections if there is an element

$$U \in \mathrm{O}_n(\mathbf{R})$$

such that

$$M_{\mathcal{B}'} = M_{\mathcal{B}} U.$$

We have the following lemma:

**Lemma 2.9.** There is a one-to-one correspondence between pairs  $(\Lambda, \mathcal{B})$  up to rotations and reflections, and the coset space  $\mathrm{GL}_n(\mathbf{R})/\mathrm{O}_n(\mathbf{R})$ , via the mapping

$$\{(\Lambda, \mathcal{B}) \text{ up to rotations and reflections}\} \longleftrightarrow \mathrm{GL}_n(\mathbf{R})/\mathrm{O}_n(\mathbf{R}),$$

$$(\Lambda, \mathcal{B}) \mapsto M_{\mathcal{B}} \mathrm{O}_n(\mathbf{R}).$$

**Example 2.10.** Consider the matrix

$$M_{\mathcal{B}_1} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

as before. The orthogonal matrix  $U$ , given by

$$U = \begin{pmatrix} \cos(\pi/4) & -\sin(\pi/4) \\ \sin(\pi/4) & \cos(\pi/4) \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

is a rotation matrix. By multiplying  $M_{\mathcal{B}_1}$  on the right with  $U$ , we get

$$M_{\mathcal{B}_1} \cdot U = \begin{pmatrix} 0 & \sqrt{2} \\ \sqrt{2} & 0 \end{pmatrix}.$$

This reflects the fact that the lattice associated to  $\mathcal{B}_1$  is the lattice  $(\sqrt{2}\mathbf{Z})^2$  rotated by  $\pi/4$  radians.

The next notion to consider when defining the shape of a lattice is scaling. Two distinct lattices will have the same shape if one is obtained from the other by a scaling factor. To remedy this, we act on the right by  $\mathbf{R}^\times$  (we choose a right action here, but a left action is equivalent).

**Lemma 2.11.** There is a one-to-one correspondence between pairs  $(\Lambda, \mathcal{B})$  up to scaling, rotations, and reflections, and the quotient  $\mathrm{GL}_n(\mathbf{R})/\mathbf{R}^\times \mathrm{O}_n(\mathbf{R})$  via the mapping

$$(\Lambda, \mathcal{B}) \mapsto M_{\mathcal{B}}\mathbf{R}^\times \mathrm{O}_n(\mathbf{R})$$

**Example 2.12.** A scaling matrix in  $\mathbf{R}^2$  takes the form

$$\lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

where  $\lambda$  is any nonzero real number. We get

$$M_{\mathcal{B}_1}\lambda = \begin{pmatrix} -\lambda & \lambda \\ \lambda & \lambda \end{pmatrix}.$$

### 2.1.3 Gram Matrices

**Definition 2.13.** Let  $V$  be a real inner product space. For a set  $\{v_1, \dots, v_n\}$  of linearly independent vectors of  $V$ , we define the *Gram matrix* to be the  $n \times n$  matrix of inner products

$$G := [\langle v_i, v_j \rangle].$$

We now define the mapping

$$\mathrm{Gram} : \mathrm{GL}_n(\mathbf{R}) \rightarrow \mathcal{G} := \{G \in \mathrm{GL}_n(\mathbf{R}) : G \text{ is positive-definite and symmetric}\}$$

as follows:

$$M \mapsto M \cdot M^T.$$

If  $\mathcal{B}$  is a basis for  $V$ , let  $G_{\mathcal{B}} = \mathrm{Gram}(M_{\mathcal{B}})$ . Notice that if  $(\Lambda', \mathcal{B}')$  is a lattice in  $V$  obtained by a series of rotations and reflections on  $(\Lambda, \mathcal{B})$ , then

$$M_{\mathcal{B}'} = M_{\mathcal{B}} \cdot U,$$

for some  $U \in \mathrm{O}_n(\mathbf{R})$ . It follows that

$$\begin{aligned}
G_{\mathcal{B}'} &= M_{\mathcal{B}'} M_{\mathcal{B}'}^T \\
&= M_{\mathcal{B}} \cdot U \cdot (M_{\mathcal{B}} \cdot U)^T \\
&= M_{\mathcal{B}} \cdot U \cdot U^T \cdot M_{\mathcal{B}}^T \\
&= M_{\mathcal{B}} \cdot M_{\mathcal{B}}^T \\
&= G_{\mathcal{B}}.
\end{aligned}$$

In other words, Gram induces a bijection

$$\{(\Lambda, \mathcal{B}) \text{ up to rotations and reflections}\} \longleftrightarrow \mathcal{G}.$$

Furthermore, the action of  $\mathrm{GL}_n(\mathbf{Z})$  on  $\mathrm{GL}_n(\mathbf{R})$  via left multiplication induces an action of  $\mathrm{GL}_n(\mathbf{Z})$  on  $\mathcal{G}$  as follows: For  $\gamma \in \mathrm{GL}_n(\mathbf{Z})$ ,

$$M_{\mathcal{B}'} = \gamma M_{\mathcal{B}},$$

so

$$G_{\mathcal{B}'} = \gamma M_{\mathcal{B}} M_{\mathcal{B}}^T \gamma^T = \gamma G_{\mathcal{B}} \gamma^T.$$

We define

$$\gamma \cdot G := \gamma G \gamma^T.$$

This yields the following lemma:

**Lemma 2.14.** The map  $(\Lambda, \mathcal{B}) \mapsto G_{\mathcal{B}}$  is  $\mathrm{GL}_n(\mathbf{Z})$ -equivariant.

This gives a one-to-one correspondence between lattices in  $V$  up to rotations and reflections, and the orbit space  $\mathrm{GL}_n(\mathbf{Z}) \backslash \mathcal{G}$ , via the mapping

$$\mathrm{GL}_n(\mathbf{Z}) M_{\mathcal{B}} \mapsto \mathrm{GL}_n(\mathbf{Z}) G_{\mathcal{B}}.$$

Note that for  $\lambda \in \mathbf{R}^\times$ , we have

$$\lambda M_{\mathcal{B}} \mapsto \lambda M_{\mathcal{B}} (\lambda M_{\mathcal{B}})^T = \lambda^2 G_{\mathcal{B}}.$$

That is,  $\mathbf{R}^\times$  acts on  $\mathcal{G}$  as follows: For  $\lambda \in \mathbf{R}^\times$ , we have  $G \cdot \lambda = \lambda^2 G$ . This finally gives us the following bijection.

**Lemma 2.15.** There is a one-to-one correspondence between rank  $n$  lattices in  $V$  up to rotations, reflections, and scalings, and  $\mathrm{GL}_n(\mathbf{Z}) \backslash \mathcal{G} / \mathbf{R}^\times$ , given by

$$\mathrm{GL}_n(\mathbf{Z}) M_{\mathcal{B}} \mathbf{R}^\times \mathrm{O}_n(\mathbf{R}) \mapsto \mathrm{GL}_n(\mathbf{Z}) \cdot G_{\mathcal{B}} \cdot \mathbf{R}^\times.$$

**Example 2.16.** Given the matrix  $M_{\mathcal{B}_1}$ , we get the corresponding Gram matrix

$$G_{\mathcal{B}_1} = M_{\mathcal{B}_1} M_{\mathcal{B}_1}^T = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

The entries on the main diagonal indicate the squares of the norms of the vectors, whereas the other entries give information about the angle between these vectors. Here, the cosine of the angle between them is zero, so the basis is orthogonal. This lattice is square.

We are finally ready to define the shape of a lattice.

**Definition 2.17.** We define the *shape* of a lattice  $\Lambda$  in  $V$  to be its equivalence class under rotations, reflections, and scaling. As such, the shape of  $\Lambda$ , denoted  $\text{sh}(\Lambda)$ , can be viewed as an element of the double coset space

$$\text{GL}_n(\mathbf{Z}) \backslash \mathcal{G} / \mathbf{R}^\times.$$

## 2.2 The Geometry of Numbers

In this section, we associate a full lattice of rank  $n$  to a number field of degree  $n$  over  $\mathbf{Q}$ . This lattice is given as the image under the Minkowski embedding of the ring of integers  $\mathcal{O}_K$ , which is a free  $\mathbf{Z}$ -module of rank  $n$ . We then define the shape of a number field.

### 2.2.1 Number Fields

In this section, we introduce some notation and concepts concerning number fields. We refer the reader to [Neu99, Chapter I] for details.

**Definition 2.18.** By a *number field*, we mean a finite algebraic extension  $K$  of the field  $\mathbf{Q}$  of rational numbers. The *degree of  $K$  over  $\mathbf{Q}$* , denoted  $[K : \mathbf{Q}]$ , is the dimension of  $K$  as a  $\mathbf{Q}$ -vector space.

**Definition 2.19.** Let  $K$  be a number field of degree  $n$ . The *signature of  $K$* , denoted  $[r_1, r_2]$ , is an ordered pair of non-negative integers, where  $r_1$  denotes the number of real embeddings of  $K$ , and  $r_2$  denotes the number of conjugate pairs of complex embeddings of  $K$ . Note that

$$n = r_1 + 2r_2.$$

**Definition 2.20.** Let  $K$  be a number field of degree  $n$  over  $\mathbf{Q}$ , and denote the embeddings of  $K$  into  $\mathbf{C}$  by  $\sigma_1, \dots, \sigma_n$ . We define the *trace* map on  $K$  as follows: For an element  $x \in K$ ,

$$\text{tr}(x) := \sum_{i=1}^n \sigma_i(x).$$

**Definition 2.21.** Let  $K$  be a number field of degree  $n$ . An element  $\alpha \in K$  is called *integral* if  $\alpha$  satisfies some monic polynomial in  $\mathbf{Z}[x]$ . The *ring of integers of  $K$* , denoted by  $\mathcal{O}_K$ , is the integral closure of  $\mathbf{Z}$  inside of  $K$ . That is,

$$\mathcal{O}_K = \{\alpha \in K : f(\alpha) = 0 \text{ for some monic } f(x) \in \mathbf{Z}[x]\}.$$

A system of elements  $w_1, \dots, w_n$  of  $\mathcal{O}_K$  is called an *integral basis of  $K$*  if every element  $\alpha \in \mathcal{O}_K$  can be written uniquely as an integer linear combination of the  $w_i$ . That is, there is a unique choice of integers  $a_1, \dots, a_n \in \mathbf{Z}$  such that

$$\alpha = \sum_{i=1}^n a_i w_i.$$

In [Neu99, Proposition 2.10], it is shown that every number field  $K$  has an integral basis. The existence of an integral basis for  $\mathcal{O}_K$  implies that  $\mathcal{O}_K$  is a free  $\mathbf{Z}$ -module of rank  $n$ . An integral basis for  $\mathcal{O}_K$  is also a basis of  $K$  as a  $\mathbf{Q}$ -vector space.

**Definition 2.22.** Let  $K$  be a number field of degree  $n$ , and denote the embeddings of  $K$  into  $\mathbf{C}$  by  $\sigma_1, \dots, \sigma_n$ . Let  $\mathcal{O}_K$  denote its ring of integers, and let  $\{w_1, \dots, w_n\}$  denote an integral basis of  $\mathcal{O}_K$ . The *discriminant of  $K$* , denoted  $\Delta(K)$  is defined as

$$\Delta(K) = \det \begin{pmatrix} \sigma_1(w_1) & \sigma_1(w_2) & \dots & \sigma_1(w_n) \\ \sigma_2(w_1) & \sigma_2(w_2) & \dots & \sigma_2(w_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(w_1) & \sigma_n(w_2) & \dots & \sigma_n(w_n) \end{pmatrix}^2.$$

**Proposition 2.23.** [Neu99, p. 14-15] The discriminant of  $K$  is independent of choice of integral basis.

## 2.2.2 Minkowski Space

Throughout this subsection, let  $K$  be a number field of degree  $n$ , with complex embeddings  $\sigma_1, \dots, \sigma_n$ . Let  $\mathcal{O}_K$  denote the ring of integers of  $K$ , and let  $\mathcal{B} = \{w_1, \dots, w_n\}$  be an integral basis of  $\mathcal{O}_K$ .

**Definition 2.24.** Associated to  $K$  is the complex inner product space  $K_{\mathbf{C}} = \prod_{\sigma} \mathbf{C}$ . The *Minkowski embedding*  $j_{\mathbf{C}} : K \rightarrow K_{\mathbf{C}}$  is given by

$$j_{\mathbf{C}}(x) = x_{\sigma} := (\sigma_1(x), \dots, \sigma_n(x)).$$

We define the *Minkowski space of  $K$*  to be the real inner product space  $K_{\mathbf{R}}$  consisting of the  $\mathbf{R}$ -span of  $j_{\mathbf{C}}(K)$  with inner product the restriction of that on  $K_{\mathbf{C}}$ .

To define the shape of  $K$ , we embed the elements of the integral basis  $\mathcal{B}$  of  $\mathcal{O}_K$  into  $K_{\mathbf{R}}$  via the Minkowski map  $j_{\mathbf{C}}$ . The resulting set  $\{j_{\mathbf{C}}(w_1), \dots, j_{\mathbf{C}}(w_n)\}$  generates a full lattice  $L_K$  of  $K_{\mathbf{R}}$ . We might be tempted to define the shape of  $K$  as the shape of  $L_K$ . However, for our purposes, we make a modification to the lattice  $j_{\mathbf{C}}(\mathcal{O}_K)$  by considering a specific orthogonal projection.

**Proposition 2.25.** We have that the volume of the lattice  $L_K$  is given by

$$\text{Vol}(L_K) = \sqrt{|\Delta(K)|}.$$

### 2.2.3 Orthogonal Projection

For a Euclidean vector space  $V$ , and non-zero vectors  $\vec{v}, \vec{w}$  of  $V$ , we let  $W$  be the subspace of  $V$  spanned by  $\vec{w}$ . We define the vectors

$$\vec{v}_{\parallel} = \vec{v}_{\parallel}[W] := \frac{\vec{v} \cdot \vec{w}}{\vec{w} \cdot \vec{w}} \vec{w},$$

$$\vec{v}_{\perp} = \vec{v}_{\perp}[W] := \vec{v} - \vec{v}_{\parallel}[W] = \vec{v} - \frac{\vec{v} \cdot \vec{w}}{\vec{w} \cdot \vec{w}} \vec{w}.$$

Let  $V$  be an  $n$ -dimensional Euclidean vector space, let  $W$  be a 1-dimensional subspace of  $V$ , and let  $\vec{0} \neq \vec{w} \in W$ . The *projection of  $V$  orthogonal to  $W$*  is the subspace of  $V$  defined by

$$V_{\perp} := \{\vec{u}_{\perp}[W] : \vec{u} \in V\} = \{\vec{v} \in V : \vec{v} \cdot \vec{w} = 0\}.$$

For any subset  $S \subseteq V$ , we can define the projection of  $S$  orthogonal to  $W$  as  $S_{\perp}[W] = \{\vec{u}_{\perp}[W] : \vec{u} \in S\}$ . In particular, we can talk about the orthogonal projection of a lattice  $L$  orthogonal to  $W$ .

Thus,  $V_{\perp}$  is an  $(n - 1)$ -dimensional subspace of  $V$ . Note that for  $\vec{u}, \vec{v} \in V$ , we have

$$\vec{u}_{\perp}[W] \cdot \vec{v}_{\perp}[W] = \vec{u} \cdot \vec{v} - \frac{(\vec{u} \cdot \vec{w})(\vec{v} \cdot \vec{w})}{\vec{w} \cdot \vec{w}}.$$

Now we return to number fields. In this thesis, we want our integral basis of  $\mathcal{O}_K$  to contain 1, which is always possible to do. So without loss of generality, we assume that  $\{w_1, \dots, w_n\}$  is an integral basis of  $\mathcal{O}_K$ , with  $w_1 = 1$ .

**Definition 2.26.** We have that  $K_{\mathbf{R}}$  is an  $n$ -dimensional real inner product space spanned by the vectors  $j_{\mathbf{C}}(1), j_{\mathbf{C}}(w_2), \dots, j_{\mathbf{C}}(w_n)$ . We let  $W$  be the one-dimensional subspace of  $K_{\mathbf{R}}$  spanned by  $j_{\mathbf{C}}(1)$ , and we define  $j_{\mathbf{C}}(\mathcal{O}_K)^{\perp}$  to be the projection of  $j_{\mathbf{C}}(\mathcal{O}_K)$  orthogonal to  $W$ .

We have the following useful equation.

**Proposition 2.27.** For elements  $x, y \in K$ , we have

$$(j_{\mathbf{C}}(x))_{\perp} \cdot (j_{\mathbf{C}}(y))_{\perp} = \langle j_{\mathbf{C}}(x), j_{\mathbf{C}}(y) \rangle - \frac{\langle j_{\mathbf{C}}(x), j_{\mathbf{C}}(1) \rangle \langle j_{\mathbf{C}}(y), j_{\mathbf{C}}(1) \rangle}{\langle j_{\mathbf{C}}(1), j_{\mathbf{C}}(1) \rangle} = \langle j_{\mathbf{C}}(x), j_{\mathbf{C}}(y) \rangle - \frac{\operatorname{tr}(x) \operatorname{tr}(y)}{n}. \quad (2.1)$$

*Proof.* For  $x \in K$ , it follows that

$$\langle j_{\mathbf{C}}(x), j_{\mathbf{C}}(1) \rangle = \sum_{i=1}^n \sigma_i(x) = \operatorname{tr}(x).$$

Then, with  $\langle j_{\mathbf{C}}(1), j_{\mathbf{C}}(1) \rangle = n$ , the result follows.  $\square$

## 2.2.4 The Shape of a Number Field

Let  $K$  be a number field of degree  $n$ , with complex embeddings  $\sigma_1, \dots, \sigma_n$ . Let  $\mathcal{O}_K$  denote the ring of integers of  $K$ , and let  $\mathcal{B} = \{w_1, \dots, w_n\}$  be an integral basis of  $\mathcal{O}_K$ , where  $w_1 = 1$ .

**Definition 2.28.** The *shape* of  $K$ , denoted  $\operatorname{sh}(K)$ , is defined to be the shape of the rank  $(n-1)$  lattice  $j_{\mathbf{C}}(\mathcal{O}_K)^{\perp}$ .

We describe how to compute the shape of a number field  $K$  given the integral basis  $\mathcal{B}$  of  $\mathcal{O}_K$ . For the sake of this thesis, it suffices to restrict to number fields that are totally real (i.e. all embeddings of  $K$  are real).

Let  $K$  be a totally real number field of degree  $n$ , and let  $\mathcal{B} = \{1, w_2, \dots, w_n\}$  be an integral basis for  $\mathcal{O}_K$ . Define the matrix  $M_{\mathcal{B}} \in \operatorname{GL}_n(\mathbf{R})$  by

$$M_{\mathcal{B}} = \begin{pmatrix} j_{\mathbf{C}}(1) \\ j_{\mathbf{C}}(w_2) \\ \vdots \\ j_{\mathbf{C}}(w_n) \end{pmatrix}.$$

Note that if  $\alpha, \beta \in K$ , then

$$\begin{aligned} \langle j_{\mathbf{C}}(\alpha), j_{\mathbf{C}}(\beta) \rangle &= \langle (\sigma_1(\alpha), \dots, \sigma_n(\alpha)), (\sigma_1(\beta), \dots, \sigma_n(\beta)) \rangle \\ &= \sum_{i=1}^n \sigma_i(\alpha\beta) \\ &= \operatorname{tr}(\alpha\beta). \end{aligned}$$

From here, the Gram matrix relative to  $\mathcal{B}$  is given by

$$G_{\mathcal{B}} = M_{\mathcal{B}} M_{\mathcal{B}}^T = \begin{pmatrix} \text{tr}(1) & \text{tr}(w_2) & \dots & \text{tr}(w_n) \\ \text{tr}(w_2) & \langle j_{\mathbf{C}}(w_2), j_{\mathbf{C}}(w_2) \rangle & \dots & \langle j_{\mathbf{C}}(w_2), j_{\mathbf{C}}(w_n) \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \text{tr}(w_n) & \langle j_{\mathbf{C}}(w_n), j_{\mathbf{C}}(w_2) \rangle & \dots & \langle j_{\mathbf{C}}(w_n), j_{\mathbf{C}}(w_n) \rangle \end{pmatrix}.$$

Next we take the orthogonal projection. It follows from equation (1) that a basis  $\mathcal{B}^\perp$  for  $j_{\mathbf{C}}(\mathcal{O}_K)^\perp$  is given by

$$\mathcal{B}^\perp = \{w_2^\perp, \dots, w_n^\perp\},$$

where, for  $2 \leq i \leq n$ , we have

$$w_i^\perp = w_i - \frac{\text{tr}(w_i)}{n}.$$

Then

$$\text{sh}(K, \mathcal{B}) = \text{GL}_{n-1}(\mathbf{Z}) \cdot G_{\mathcal{B}^\perp} \mathbf{R}^\times.$$

## 2.3 A Special Family of Lattices

In this section, we will introduce a family of lattices that will appear when determining the shapes of the number fields that we will study in Chapter 3. As we will see, these lattices will give a geometric interpretation of the shapes that we encounter.

### 2.3.1 The Matrix $A_n$

We will now present a recursively defined sequence of matrices, denoted  $A_n$ , and use it in our subsequent construction. The matrix  $A_n$  will turn out to play a crucial role in Chapter 3, specifically, this matrix will contain information about the Galois embeddings of the number fields we study.

**Definition 2.29.** For  $n \geq 0$  we define the following  $2^n \times 2^n$  matrices:

$$A_0 = [1], \quad A_{n+1} = \begin{bmatrix} A_n & A_n \\ A_n & -A_n \end{bmatrix}.$$

**Illustration 1.** The first few matrices are given below:

When  $n = 1$ , we get

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

When  $n = 2$ , we get

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

When  $n = 3$ , we get

$$A_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

As we can see, these matrices are symmetric of size  $2^n$ .

### 2.3.2 The Lattice $\mathcal{D}^*$

With the matrix  $A_n$  defined, we will now construct a lattice in  $(2^n - 1)$ -dimensional space, denoted  $\mathcal{D}^*$ , and study its shape.

Let  $n$  be a positive integer, let  $m = 2^n$ , and let  $\ell = m - 1 = 2^n - 1$ . We begin with the standard primitive cubic lattice  $\mathbf{Z}^m$  contained in  $\mathbf{R}^m$ . A basis for this lattice is given by the standard basis

$$\mathcal{B} = \{e_0, \dots, e_\ell\}$$

of  $\mathbf{R}^m$ , where  $e_j$  consists of a 1 in the  $j^{\text{th}}$  component and zeros elsewhere. Then the matrix  $M_{\mathcal{B}}$  is just the identity matrix  $I_m$ . Next, we define the vectors  $w_0, \dots, w_\ell$  to be the row vectors of the matrix

$$(w_0, \dots, w_\ell) = \frac{A_n}{2^n} I_m.$$

We proceed to compute the Gram matrix of the lattice relative to the basis  $\{w_0, \dots, w_\ell\}$ . We first take the orthogonal projection onto the vector  $e_0$ .

The lattice we want to define will be the  $\ell$ -dimensional lattice whose basis vectors are the columns of the matrix

$$\frac{A_n}{2^n}$$

after deleting the first row and column. Since scaling doesn't affect the shape, we will scale this

matrix by a factor of  $2^n$ , and denote this matrix by  $A_n^*$ . We get that the Gram matrix relative to  $A_n^*$  is given by

$$G_{A_n^*} = [\langle w_i^\perp, w_j^\perp \rangle] = A_n^* I_\ell (A_n^*)^T.$$

Denote by  $\mathcal{D}^*$  the lattice spanned by rows of  $A_n^*$ . Its Gram matrix with respect to the rows of  $A_n^*$  is given explicitly as

$$G_{A_n^*} = \begin{pmatrix} \ell & -1 & -1 & \dots & -1 \\ -1 & \ell & -1 & \dots & -1 \\ -1 & -1 & \ell & \dots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \dots & \ell \end{pmatrix}.$$

**Remark 2.30.** This lattice is called the *dual of the root lattice  $A_\ell$* . We refer the reader to [CS93, Chapter 4, Section 6.6] for more details regarding this lattice.

### 2.3.3 Primitive Orthorhombic Lattices

In this section, we fix a positive integer  $n$ . We let  $\ell = 2^n - 1$ .

The above construction of  $\mathcal{D}^*$  started with the primitive cubic lattice  $\mathbf{Z}^m$ . Now, rather than beginning with the primitive cubic lattice, we begin with a primitive orthorhombic lattice, i.e. a lattice that has as its fundamental region a right rectangular polytope.

Suppose that  $\mathcal{B} = \{v_0, \dots, v_\ell\}$  is a basis for  $\mathbf{R}^{2^n}$  such that the vectors  $v_i$  are pairwise orthogonal, and such that

$$\sqrt{2^n} = |v_0| \leq \dots \leq |v_\ell|.$$

**Definition 2.31.** We call a lattice

$$\Lambda = \mathbf{Z}v_0 + \dots + \mathbf{Z}v_\ell$$

whose basis vectors are pairwise orthogonal an  *$m$ -dimensional primitive orthorhombic lattice*.

Now, we get that the Gram matrix  $G_{\mathcal{B}}$  is given by

$$G_{\mathcal{B}} = M_{\mathcal{B}} M_{\mathcal{B}}^T = \begin{pmatrix} |v_0|^2 & & & \\ & |v_1|^2 & & \\ & & \ddots & \\ & & & |v_\ell|^2 \end{pmatrix}.$$

Next, we define the vectors  $w_0, \dots, w_\ell$  via

$$\begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_\ell \end{pmatrix} = \frac{A_n}{2^n} \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_\ell \end{pmatrix}.$$

Next, we take the projection of the  $w_i$  orthogonal to  $v_0$ . This gives the basis  $\mathcal{B}^\perp = \{w_1^\perp, \dots, w_\ell^\perp\}$ : Denote the  $ij$ -entry of the matrix  $A_n$  by  $a_{ij}$ . Then, for  $1 \leq i \leq \ell$ ,

$$\begin{aligned} w_i^\perp &= w_i - \frac{\langle w_i, v_0 \rangle}{\langle v_0, v_0 \rangle} v_0 \\ &= w_i - \frac{1}{2^{2n}} \left\langle \sum_{j=0}^{\ell} a_{ij} v_j, v_0 \right\rangle v_0 \\ &= w_i - \frac{1}{2^{2n}} \sum_{j=0}^{\ell} a_{ij} \langle v_j, v_0 \rangle v_0 \\ &= w_i - \frac{\langle v_0, v_0 \rangle}{2^{2n}} v_0 \\ &= w_i - \frac{v_0}{2^n}. \end{aligned}$$

Furthermore, for  $1 \leq i, j \leq \ell$ , we have that

$$w_i^\perp \cdot w_j^\perp = w_i \cdot w_j - \frac{1}{2^n}.$$

We now compute  $w_i \cdot w_j$ .

$$\begin{aligned} w_i \cdot w_j &= \left( \sum_{k=0}^{\ell} \frac{a_{ik}}{2^n} v_k \right) \cdot \left( \sum_{k'=0}^{\ell} \frac{a_{jk'}}{2^n} v_{k'} \right) \\ &= \sum_{k=0}^{\ell} \frac{a_{ik} a_{jk}}{2^n 2^n} |v_k|^2 \\ &= \frac{|v_0|^2}{2^{2n}} + \sum_{k=1}^{\ell} \frac{a_{ik} a_{jk}}{2^n 2^n} |v_k|^2 \\ &= \frac{1}{2^n} + \sum_{k=1}^{\ell} \frac{a_{ik} a_{jk}}{2^n 2^n} |v_k|^2. \end{aligned}$$

Hence, we get that

$$w_i^\perp \cdot w_j^\perp = \sum_{k=1}^{\ell} \frac{a_{ik} a_{jk}}{2^n 2^n} |v_k|^2.$$

**Definition 2.32.** We define the matrices  $M_1, \dots, M_\ell$  as follows. Let the entries of  $A_n^*$  be given by  $a_{ij}$ , where  $1 \leq i, j \leq \ell$ . Then the matrix  $M_k$  is given by

$$M_k = [m_{ij}],$$

where, for  $1 \leq i, j \leq \ell$ , we have

$$m_{ij} = a_{ik}a_{jk}.$$

With the above definition, we get that

$$G_{\mathcal{B}}^\perp = \frac{1}{2^{2n}} \sum_{k=1}^{\ell} |v_k|^2 M_k.$$

**Remark 2.33.** Notice that by adding these matrices together, we get

$$\sum_{j=1}^{\ell} M_j = \begin{pmatrix} \ell & -1 & \dots & -1 \\ -1 & \ell & \dots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \dots & \ell \end{pmatrix}.$$

This matrix is the Gram matrix of the lattice  $\mathcal{D}^*$  we presented in the previous section.

We now proceed to define the shapes associated to primitive orthorhombic lattices.

**Definition 2.34.** Let  $\Gamma$  be the set defined by

$$\Gamma = \left\{ A_n^* \begin{pmatrix} 1 & & & \\ & X_2 & & \\ & & \ddots & \\ & & & X_\ell \end{pmatrix} (A_n^*)^T : 1 \leq X_2 \leq \dots \leq X_\ell \right\}.$$

Then there is a mapping  $\Gamma \rightarrow \mathcal{S}_\ell$  from  $\Gamma$  to the space of shapes of rank  $\ell$  lattices given by

$$G \mapsto \text{GL}_\ell(\mathbf{Z})G\mathbf{R}^\times \text{O}_\ell(\mathbf{R}).$$

**Lemma 2.35.** The above mapping is injective.

*Proof.* Let  $\Lambda_1$  be a rank  $\ell$  lattice with Gram matrix in  $\Gamma$ . Then  $\Lambda_1$  contains a sublattice  $\Lambda_1'$  whose corresponding Gram matrix is given by

$$2^n \begin{pmatrix} 1 & & & \\ & X_1 & & \\ & & \ddots & \\ & & & X_\ell \end{pmatrix}.$$

In particular,  $\Lambda'_1$  is a primitive orthorhombic lattice. If  $\Lambda_2$  is any other rank  $\ell$  lattice with Gram matrix in  $\Gamma$  such that

$$\text{sh}(\Lambda_1) = \text{sh}(\Lambda_2),$$

then the corresponding sublattices also have the same shape. That is,

$$\text{sh}(\Lambda'_1) = \text{sh}(\Lambda'_2).$$

Since both sublattices are primitive orthorhombic lattices, it follows that  $X_2, \dots, X_\ell$  match, proving that the mapping is injective.  $\square$

**Definition 2.36.** For  $1 \leq X_2 \leq \dots \leq X_\ell$ , we define

$$\text{sh}(X_2, \dots, X_\ell) := \text{GL}_\ell(\mathbf{Z})A_n^* \begin{pmatrix} 1 & & & \\ & X_2 & & \\ & & \ddots & \\ & & & X_\ell \end{pmatrix} (A_n^*)^T \mathbf{R}^\times.$$

More generally, if we have  $1 \leq X_j$ , where the  $X_j$ 's are not necessarily ordered, then we define

$$\text{sh}(X_2, \dots, X_\ell) := \text{sh}(X_{\sigma(2)}, \dots, X_{\sigma(\ell)}),$$

where  $\sigma$  is a permutation that gives

$$1 \leq X_{\sigma(2)} \leq \dots \leq X_{\sigma(\ell)}.$$

**Lemma 2.37.** Suppose the  $v_1, \dots, v_\ell$  are vectors such that  $|v_i|^2 \geq |v_1|^2$ , but not necessarily increasing in norm. Let  $\{w_0, \dots, w_\ell\}$  and  $\{w_1^\perp, \dots, w_\ell^\perp\}$  be given as above. Then the shape of the lattice

$$\mathbf{Z}w_1^\perp + \dots + \mathbf{Z}w_\ell^\perp,$$

is given by  $\text{sh}(X_2, \dots, X_\ell)$ , where

$$X_i = \frac{|v_i|^2}{|v_1|^2}.$$

**Definition 2.38.** Let  $\mathcal{S}_{K_n}$  be defined as the subspace of  $\mathcal{S}_\ell$  with a set of representatives given by

$$M_1 + \mathbf{R}_{>0}M_2 + \dots + \mathbf{R}_{>0}M_\ell.$$

Moreover, we have that

$$\dim(\mathcal{S}_{K_n}) = \ell - 1.$$

Thus, any representative in  $\mathcal{S}_{K_n}$  can be written in terms of an  $(\ell - 1)$ -tuple of real numbers

$$\text{sh}(X_2, \dots, X_\ell),$$

where this tuple represents the expression

$$M_1 + \sum_{j=2}^{\ell} X_j M_j.$$

## 2.4 The Space of Shapes

Let  $\ell > 1$  be an integer. We recall from Section 2.1 that the space of shapes of rank- $\ell$  lattices is given by

$$\mathcal{S}_\ell := \text{GL}_\ell(\mathbf{Z}) \backslash \mathcal{G} / \mathbf{R}^\times.$$

We are interested in a particular subset of  $\mathcal{S}_\ell$  that contains the shapes that we will study in Chapter 3. These are the shapes discussed in the previous section. We will now define an appropriate measure on this set which will allow us to talk about equidistribution.

**Definition 2.39.** Let  $\mathcal{D}_\ell \subset \text{GL}_\ell(\mathbf{R})$  denote the subgroup of diagonal matrices. Then elements of  $\mathcal{D}_\ell$  are in bijection with  $\ell$ -tuples  $(a_1, \dots, a_\ell)$  of non-zero real numbers. This gives an isomorphism of  $\mathcal{D}_\ell$  with  $(\mathbf{R}^\ell)^\times$ . In particular, the Haar measure  $\tilde{\mu}$  on  $\mathcal{D}_\ell$  is that defined on  $(\mathbf{R}^\times)^\ell$ , namely:

$$d\tilde{\mu} = d^\times a_1 \cdots d^\times a_\ell,$$

where for  $1 \leq j \leq n$ ,

$$d^\times a_j = \frac{da_j}{a_j},$$

and  $da_j$  denotes Lebesgue measure.

**Definition 2.40.** Let  $R_2, \dots, R_\ell$  be positive real numbers. We define a subset  $T_n(R_2, \dots, R_\ell)$  of  $\mathcal{D}_\ell$  as follows. Let  $D(1, a_2, \dots, a_\ell)$  denote the diagonal matrix

$$D(1, a_2, \dots, a_\ell) := \begin{pmatrix} 1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_\ell \end{pmatrix}.$$

Fix positive real numbers  $0 < R_2 \leq \dots \leq R_\ell$ . Define the set

$$T_n(R_2, \dots, R_\ell) := \left\{ D(1, a_2, \dots, a_\ell) : \sqrt{R_2} \leq a_2 \leq \dots \leq a_\ell \leq \sqrt{R_\ell}, \sqrt{R_i} \leq a_i \text{ for } 2 \leq i \leq \ell - 1 \right\}.$$

**Proposition 2.41.** The measure of  $T_\ell(R_2, \dots, R_\ell)$  is given by

$$\tilde{\mu}(T_\ell(R)) = \int_{\sqrt{R_{\ell-1}}}^{\sqrt{R_\ell}} \int_{\sqrt{R_{\ell-1}}}^{a_\ell} \int_{\sqrt{R_{\ell-2}}}^{a_{\ell-1}} \cdots \int_{\sqrt{R_2}}^{a_3} d^\times a_2 \cdots d^\times a_\ell. \quad (2.2)$$

When  $\ell = 7$ , we get

$$\tilde{\mu}(T_7(R_2, \dots, R_7)) = \frac{1}{2^6 6!} F(R_2, \dots, R_7),$$

where  $F(R_2, \dots, R_7)$  is a homogeneous polynomial function of degree 6 in the variables  $\log(R_2), \dots, \log(R_7)$ .

Next, we define a mapping from the set  $\mathcal{D}_\ell$  of diagonal matrices to the set  $\Gamma$  as follows:

Let  $D_X = D(1, X_2, \dots, X_\ell)$ . Then, for a diagonal matrix  $D_a = D(1, a_2, \dots, a_\ell) \in \mathcal{D}_\ell$ , we have that  $D_a$  acts on  $G = A_n^* D_X (A_n^*)^T$  by scalings:

$$D_a \cdot G = (A_n^* D_a) D_X (A_n^* D_a)^T.$$

**Definition 2.42.** We define  $W(R_2, \dots, R_\ell)$  to be the image of  $T_\ell(R_2, \dots, R_\ell)$  under the mapping

$$D_a \mapsto D_a \cdot G_{A_n^*} = A_n^* D(1, a_2^2, \dots, a_n^2) (A_n^*)^T.$$

Explicitly, we have

$$W(R_2, \dots, R_\ell) = \left\{ A_n^* D_X (A_n^*)^T : X_2 \leq \dots \leq X_\ell \leq R_\ell, R_i \leq X_i \text{ for } 2 \leq i \leq \ell - 1 \right\}.$$

The map above is a bijection  $\varphi : T_\ell(\infty) \rightarrow \Gamma$ . We then get a measure  $\mu$  on  $\mathcal{S}_{K_n}$ . Specifically, for  $W \subset \mathcal{S}_{K_n}$ , define

$$\mu(W) := 2^{n-1} \tilde{\mu}(\varphi^{-1}(W)).$$

**Corollary 2.43.** The measure of  $W(R_2, \dots, R_\ell)$  is given by

$$\mu(W(R_2, \dots, R_\ell)) = \int_{R_{n-1}}^{R_n} \int_{R_{n-1}}^{a_n} \int_{R_{n-2}}^{a_{n-1}} \cdots \int_{R_2}^{a_3} d^\times a_2 \cdots d^\times a_n.$$

In particular, when  $\ell = 7$  we have

$$\mu(W(R_2, \dots, R_7)) = \frac{1}{6!} F(R_2, \dots, R_7).$$

### 2.4.1 Equidistribution

With the measure  $\mu$  given above, we define what it means for a family of number fields to be equidistributed with respect to  $\mu$ .

Let  $S$  be a subset of the space of shapes of rank  $n - 1$  lattices and suppose  $\mu$  is a Radon measure on  $S$ . Let  $\mathcal{K}$  be a family of degree  $n$  number fields whose discriminants are unbounded and such that  $\text{sh}(K) \in S$  for all  $K \in \mathcal{K}$ .

**Definition 2.44.** If  $\mu(S) < \infty$ , we say that the shapes of the fields in  $\mathcal{K}$  are *equidistributed in  $S$*  (with respect to  $\mu$ ) if for every  $\mu$ -continuity set  $W \subseteq S$ <sup>1</sup>

$$\lim_{X \rightarrow \infty} \frac{\#\{K \in \mathcal{K} : |\Delta(K)| < X, \text{sh}(K) \in W\}}{\#\{K \in \mathcal{K} : |\Delta(K)| < X\}} = \frac{\mu(W)}{\mu(S)}.$$

When  $\mu(S)$  is not finite, as will be the case for multiquadratic fields, this definition needs to be modified.

**Definition 2.45.** We say that the shapes of fields in  $\mathcal{K}$  are *equidistributed in  $S$*  (with respect to  $\mu$ ) in a regularized sense for the gauge  $g(x)$  if there is a positive constant  $C > 0$  such that for every compact  $\mu$ -continuity set  $W \subseteq S$

$$\lim_{X \rightarrow \infty} \frac{\#\{K \in \mathcal{K} : |\Delta(K)| < X, \text{sh}(K) \in W\}}{g(x)} = C\mu(W). \quad (2.3)$$

**Proposition 2.46.** Let  $\mathcal{C}$  be the following hypercube in  $\mathbf{R}^{\ell-1}$ : Begin with the standard unit cube in  $\mathbf{R}^{\ell-1}$ , scale it by a factor of  $r$ , then translate the origin to the point  $(z_2, \dots, z_{\ell-1}, z_\ell - r)$ . Then  $\mathcal{C}$  can be written as a linear combination of sets of the form  $W(R_2, \dots, R_\ell)$ .

*Proof.* We employ the principle of inclusion-exclusion. First, we get that  $\mathcal{C}$  is contained in the set  $W(z_2, \dots, z_\ell)$ . Since the latter set is larger than  $\mathcal{C}$ , we subtract sets that run adjacent to  $\binom{\ell-1}{1}$  faces of  $\mathcal{C}$ . These are precisely sets of the form

$$W(z_2, \dots, z_{j-1}, z_j + r, z_{j+1}, \dots, z_{\ell-1}, z_\ell)$$

if  $2 \leq j \leq \ell - 1$ , or the set

$$W(z_2, \dots, z_{\ell-1}, z_\ell - r)$$

if  $j = \ell$ . Let  $W_{j_1}(z_2, \dots, z_\ell)$  denote the set that adds  $r$  to the  $j_1$ -coordinate, where  $2 \leq j_1 \leq \ell - 1$  (or subtracts  $r$  when  $j_1 = \ell$ ).

However, by subtracting these sets, we have removed certain parts of  $W(z_2, \dots, z_\ell)$  twice, namely those lying in the intersection of any two of the sets  $W_{j_1}(z_2, \dots, z_\ell)$ . We add these back in with sets of the form

$$W(\dots, w_i + r, \dots, w_j + r, \dots),$$

where we are adding  $r$  to exactly two coordinates (or subtracting  $r$  if the coordinate is  $z_\ell$ ). There

---

<sup>1</sup>A  $\mu$ -continuity set  $W \subseteq S$  is a measurable subset whose boundary has measure 0.

are  $\binom{\ell}{2}$  such sets, which we denote by  $W_{j_1, j_2}(z_2, \dots, z_\ell)$ , for  $1 \leq j_1 < j_2 \leq \ell$ .

Continuing in this manner, we obtain the following expression for  $\mathcal{C}$ :

$$\mathcal{C} = W(z_2, \dots, z_\ell) + \sum_{i=1}^{\ell-1} \left( \sum_{2 \leq j_1 < \dots < j_i \leq \ell} (-1)^i W_{j_1, \dots, j_i}(z_2, \dots, z_\ell) \right).$$

□

We are interested in the case where  $S = \mathcal{S}_{K_n}$ . By a standard measure theoretic argument, any function  $f \in C_c(S)$  can be approximated arbitrarily well by finite linear combinations of step functions of cubes  $\mathcal{C}$  with respect to the  $L^1$  norm. Then, by the above proposition, we have that functions in  $C_c(S)$  can be approximated by finite linear combinations of step functions of the sets  $W(R_2, \dots, R_\ell)$ . It therefore suffices to prove (2.3) for subsets  $W$  of the form  $W(R_2, \dots, R_\ell)$  in order to establish equidistribution, by a similar argument to [Har17, Theorem 3.1].

In the next chapter, we compute the shapes of totally real multiquadratic extensions that are unramified at 2. Finally, in Chapter 4, we develop the tools for counting such number fields restricted to  $n = 3$ . We then combine this information with the results on shapes to prove an analogous result to Equation (2.3).

# CHAPTER 3

## MULTIQUADRATIC EXTENSIONS AND THEIR SHAPES

In this chapter, we specialize the study of shapes of number fields to the main objects of interest: multiquadratic fields. A multiquadratic field is a field that is a compositum of quadratic subfields. As we will see, a multiquadratic extension is an abelian number field of degree  $2^n$ , and in some sense, its shape is determined by its  $2^n - 1$  quadratic subfields.

We will see that this family of number fields can always be broken up into three categories, according to specific congruence conditions modulo 4. In [Cha73], the author describes a specific subdivision of multiquadratic extensions according to congruence type, and proceeds to compute the discriminant of the field as well as an integral basis for its ring of integers.

We will choose one specific category of multiquadratic extensions as portrayed in [Cha73], and from there, be able to compute the shape.

### 3.1 Multiquadratic Extensions

#### 3.1.1 Basic Results

**Definition 3.1.** Let  $n \geq 1$  be an integer, and suppose that  $D_{2^0}, \dots, D_{2^{n-1}}$  are  $n$  distinct, squarefree integers not equal to 1, such that the squarefree part of  $D_{2^i} D_{2^j} \neq D_{2^k}$  whenever  $i, j, k$  are distinct. We define the *multiquadratic extension*  $K_n$  generated by  $D_{2^0}, \dots, D_{2^{n-1}}$  to be the number field

$$K_n := \mathbf{Q}(\sqrt{D_{2^0}}, \dots, \sqrt{D_{2^{n-1}}}).$$

We let

$$\mathcal{D} = \{D_{2^0}, \dots, D_{2^{n-1}}\},$$

and call it a *generating set* for  $K_n$ . The condition on the  $D$ s implies that  $[K_n : \mathbf{Q}] = 2^n$ . From now on, let  $\ell$  denote the quantity

$$\ell = 2^n - 1.$$

Note that the subscripts are written down as powers of 2. This notation provides a convenient way to keep track of the  $\ell$  quadratic subfields of  $K_n$ . We describe these quadratic subfields as follows:

**Lemma 3.2.** The quadratic subfields of  $K_n$  are given by  $\mathbf{Q}(\sqrt{D_j})$ , for  $1 \leq j \leq \ell$ , where

$$D_j = \frac{D_i D_{2^k}}{\gcd(D_i, D_{2^k})^2}, \quad (3.1)$$

where  $j = i + 2^k$  for  $1 \leq k \leq n - 1$  and  $0 \leq i \leq 2^k - 1$ .

By convention, we set  $D_0 = 1$ . As we will see, the generators  $\{\sqrt{D_1}, \dots, \sqrt{D_\ell}\}$  of the quadratic subfields of  $K_n$  show up when finding an integral basis of the ring of integers of  $K_n$ . Before we can compute an integral basis, we shall state some basic facts about multiquadratic extensions. The following results are summarized from [Cha73].

For an element  $D_i \in \mathcal{D}$ , it follows that  $D_i \equiv 1, 2, 3 \pmod{4}$  (Note that  $D_i \not\equiv 0 \pmod{4}$  since  $D_i$  is, by definition, a squarefree integer). In order to classify all possible multiquadratic extensions, [Cha73] shows how to make modifications to the generators in such a way that  $K_n$  has at most one generator  $D_i$  that is congruent to 2 and one congruent to 3 modulo 4.

**Lemma 3.3.** [Cha73, p. 10] Let  $K_n = \mathbf{Q}(\sqrt{D_{2^0}}, \dots, \sqrt{D_{2^{n-1}}})$ , and let  $\mathcal{D} = \{D_{2^0}, D_{2^1}, \dots, D_{2^{n-1}}\}$ . Then without loss of generality, we have at most one of the generators congruent to 2 and 3 modulo 4.

With the above lemma, we can now reduce the study of multiquadratic extensions into four categories, according to congruence conditions modulo 4. The generating set for  $K_n$  falls under exactly one of the following cases:

$$D = \{D_{2^0}, \dots, D_{2^{n-1}}\} \equiv \begin{cases} \underbrace{\{1, \dots, 1\}}_n \\ \underbrace{\{1, \dots, 1, 3\}}_{n-1} \\ \underbrace{\{1, \dots, 1, 2\}}_{n-1} \\ \underbrace{\{1, \dots, 1, 2, 3\}}_{n-2} \end{cases} \pmod{4}.$$

Within each case, we can compute an integral basis  $\mathcal{B}$  for the ring of integers  $\mathcal{O}_{K_n}$ . As is demonstrated in [Cha73], the second and third set of congruence conditions give rise to integral bases for  $\mathcal{O}_{K_n}$  of the same form in terms of the  $\sqrt{D_j}$ . Hence, there really are only three cases to consider when one wants to compute the shape of  $K_n$ .

### 3.1.2 The Case of Interest

The goal of this thesis will be to study multiquadratic extensions of  $\mathbf{Q}$  that are *totally real* and whose generating set fall under the case  $\{1, \dots, 1\}$ . Thus, from now on, we make the following assumption:

*Assumption:*  $K_n = \mathbf{Q}(\sqrt{D_{2^0}}, \dots, \sqrt{D_{2^{n-1}}})$ , where  $\mathcal{D} = \{D_{2^0}, \dots, D_{2^{n-1}}\}$  is a generating set and  $D_{2^k} \equiv 1 \pmod{4}$  and positive.

By Definition 2, it follows that  $D_j \equiv 1 \pmod{4}$  for  $1 \leq j \leq \ell$ . We also define the following notation:

Let  $n \geq 2$  be an integer. Let  $\mathcal{M}_n$  denote the set of all multiquadratic extensions of degree  $2^n$ , let  $\mathcal{M}_n^+$  denote those that are totally real, and finally, let  $\mathcal{M}_n^+(i)$  denote totally real multiquadratic extensions whose generators are congruent to 1 modulo 4.

### 3.1.3 The Galois Group

A convenient feature of multiquadratic extensions is that they are abelian. Furthermore, we have a way of encapsulating information about the Galois automorphisms into a matrix. This will play a key role in determining the shape of  $K_n$ .

We will begin by looking at the Galois group  $\text{Gal}(K_n/\mathbf{Q})$ .

**Lemma 3.4** ([Cha73, p. 4]).  $K_n$  is an abelian extension over  $\mathbf{Q}$  of degree  $2^n$ , with Galois group isomorphic to  $\underbrace{C_2 \times \dots \times C_2}_{n \text{ times}}$ , where  $C_2$  denotes the cyclic group of order 2.

We have a nice way to keep track of how the Galois automorphisms act on the generators of  $K_n$ . In particular,  $\text{Gal}(K_n/\mathbf{Q})$  is generated by elements  $\sigma$  such that  $\sigma$  acts on exactly one of the generators  $\sqrt{D_{2^k}}$  by sending it to its negative, while keeping the other generators fixed. This in turn causes sign changes for the  $\sqrt{D_j}$  that are defined using  $\sqrt{D_{2^k}}$ . Since there are  $2^n$  Galois automorphisms acting on the  $2^n$  elements  $1, \sqrt{D_1}, \dots, \sqrt{D_\ell}$ , we can denote these actions using a  $2^n \times 2^n$  matrix whose entries are either 1 or  $-1$ . These matrices are the matrices  $A_n$  given in Definition 2.29. The Galois embeddings of  $K_n$  can be read off the matrix  $A_n$  as follows.

**Proposition 3.5** ([Cha73, Corollaire 1]). Write

$$A_n = (a_{ij}),$$

with  $0 \leq i, j \leq \ell$ . We may order the embeddings

$$\sigma_i \in \text{Gal}(K_n/\mathbf{Q})$$

such that

$$a_{i,j} = \frac{\sigma_i(\sqrt{D_j})}{\sqrt{D_j}}.$$

**Proposition 3.6.** The matrix  $A_n$  is symmetric. Furthermore, we have that

$$A_n^2 = A_n A_n^T = 2^n I_{2^n},$$

where  $I_{2^n}$  denotes the  $2^n \times 2^n$  identity matrix.

*Proof.* It is easy to see from the recursive definition that  $A_n$  is a symmetric matrix. We will prove the second statement by induction on  $n$

If  $n = 0$ , then

$$A_0^2 = [1][1] = [1].$$

Suppose the statement is true for  $n$ . Then we have

$$A_{n+1}^2 = \begin{pmatrix} A_n & A_n \\ A_n & -A_n \end{pmatrix} \begin{pmatrix} A_n & A_n \\ A_n & -A_n \end{pmatrix} = \begin{pmatrix} 2A_n^2 & 0 \\ 0 & 2A_n^2 \end{pmatrix} = \begin{pmatrix} 2(2^n I_{2^n}) & 0 \\ 0 & 2(2^n I_{2^n}) \end{pmatrix} = 2^{n+1} I_{2^{n+1}},$$

which is what we needed to show.  $\square$

With these basic results about multiquadratic extensions, we are now ready to compute their shape. We proceed with the shape of  $K_n$  in general. We then present the calculation more explicitly for the case when  $n = 2$ .

### 3.1.4 An Integral Basis for $K_n$

In this section, we will describe an integral basis for  $\mathcal{O}_{K_n}$ .

**Theorem 3.7** ([Cha73, Théorème 1(b)]). Let  $v$  be the vector in  $(K_n)^{2^n}$  defined by

$$v = \frac{1}{2^n} \left( 1, \sqrt{D_1}, \dots, \sqrt{D_l} \right)^T.$$

Then, with the matrix  $A_n$  defined above, an integral basis for  $K_n$  is given by the components of the vector

$$A_n \cdot v.$$

That is, if  $\alpha_j := (A_n \cdot v)_j$  denotes the  $j^{\text{th}}$  component of  $A_n \cdot v$  (with  $0 \leq j \leq l$ ), then

$$\mathcal{B}^* = \{\alpha_0, \dots, \alpha_l\}$$

is a (normal) integral basis of  $K_n$ .

**Lemma 3.8** ([Cha73, Théorème 1 (b)]). The discriminant of  $K_n$  is given by

$$\Delta(K_n) = \prod_{j=1}^{\ell} D_j.$$

**Remark 3.9.** Because we focus on the case that each  $D_j$  is congruent to 1 modulo 4, the discriminant of  $K_n$  is not divisible by 2. It follows that 2 is unramified in these extensions. It is shown in [Cha73] that 2 does ramify if the generating set of  $K_n$  exhibits elements that are not congruent to 1 modulo 4. Therefore, the multiquadratic fields we are interested in are precisely those in which 2 is unramified.

Note: In the process of computing the shape of  $K_n$ , it will be desirable that our integral basis contains 1. As such, we make a modification to the basis given above. We just need to make sure that the basis element we replace can be written as a linear combination of the other basis elements in an invertible way. We can indeed do this, for any basis element, and in particular, we choose to replace  $\alpha_0$ , since

$$\alpha_0 = \frac{1 + \sqrt{D_1} + \dots + \sqrt{D_\ell}}{2^n} = 1 - \sum_{j=1}^{\ell} \alpha_j.$$

We define the integral basis that we will work with below:

**Definition 3.10.** We define  $\mathcal{B}$  to be the integral basis for  $\mathcal{O}_{K_n}$  given by

$$\mathcal{B} = \{1, \alpha_1, \dots, \alpha_\ell\},$$

where  $\alpha_j$  denotes the  $j^{\text{th}}$  component of the vector  $A_n \cdot v$ .

## 3.2 The Shape

With the integral basis for  $\mathcal{O}_{K_n}$  in hand, we are now ready to compute the shape of  $K_n$ .

We begin with the basis  $2^n v$  of  $R = \mathbf{Z}[\sqrt{D_1}, \dots, \sqrt{D_\ell}]$ , which we denote by  $\mathcal{F}$ :

$$\mathcal{F} := \{1, \sqrt{D_1}, \dots, \sqrt{D_\ell}\}.$$

Now, applying the Minkowski embedding to these elements, we define the following vectors: For  $0 \leq j \leq \ell$ ,

$$v_j := j_{\mathbf{C}}(\sqrt{D_j}).$$

(Recall that  $D_0$  is defined to be 1.)

**Lemma 3.11.** With the definitions above,

$$|v_j|^2 = \langle j_{\mathbf{C}}(D_j), j_{\mathbf{C}}(D_j) \rangle = 2^n D_j.$$

Furthermore, these vectors are mutually orthogonal.

*Proof.* We have

$$|v_j|^2 = \langle v_j, v_j \rangle = \sum_{k=0}^{\ell} D_j = 2^n D_j.$$

Now suppose  $i \neq j$ . We have

$$\begin{aligned}
\langle v_i, v_j \rangle &= \text{tr} \left( \sqrt{D_i} \sqrt{D_j} \right) \\
&= \text{tr} \left( \sqrt{D_k} \gcd(D_i, D_j) \right) \\
&= \sqrt{D_k} \gcd(D_i, D_j) \sum_{j=0}^{\ell} a_{ij} \\
&= 0.
\end{aligned}$$

□

In particular, the above lemma tells us that

$$|v_0| \leq |v_j|$$

for  $1 \leq j \leq \ell$ . Next, we define the vectors  $w_j$  as the images under the Minkowski embedding of the integral basis elements  $\alpha_j$ . In other words,

$$w_j := j_{\mathbf{C}}(\alpha_j),$$

for  $0 \leq j \leq \ell$ .

We then have

$$\begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_\ell \end{pmatrix} = \frac{A_n}{2^n} \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_\ell \end{pmatrix},$$

which agrees with the setup given in Section 2.3. Thus, from Lemma 2.37, we get the following result.

**Corollary 3.12.** Let  $K_n$  be a multiquadratic extension, and let  $(D_1, \dots, D_\ell)$  be the corresponding tuple of quadratic generators. If  $D_1 \leq D_j$  for  $2 \leq j \leq \ell$ , then the shape of  $K_n$  is given by

$$\text{sh}(K_n) = \text{sh} \left( \frac{D_2}{D_1}, \dots, \frac{D_\ell}{D_1} \right),$$

as in Definition 2.36.

### 3.2.1 The Shape of $K_2$

In this section, we illustrate the computation of the shape of  $K_2$  relative to our integral basis. This section is meant to provide the reader with a more explicit presentation of the shape.

Define the biquadratic extension

$$K_2 = \mathbf{Q}(\sqrt{D_1}, \sqrt{D_2}),$$

with  $D_1, D_2 \equiv 1 \pmod{4}$ , squarefree, distinct, and greater than 1. Associated to  $K_2$ , we have the triple  $(D_1, D_2, D_3)$ , where

$$D_3 = \frac{D_1 D_2}{\gcd(D_1, D_2)^2}.$$

Let  $v = \frac{1}{4}(1, \sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3})$ . We also have the matrix  $A_2$  given by

$$A_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

An integral basis for  $\mathcal{O}_{K_2}$  is given by  $\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\}$ , where

$$\alpha_i = (A_2 v)_i, i = 0, 1, 2, 3.$$

This yields

$$\alpha_0 = \frac{1}{4}(1 + \sqrt{D_1} + \sqrt{D_2} + \sqrt{D_3}),$$

$$\alpha_1 = \frac{1}{4}(1 - \sqrt{D_1} + \sqrt{D_2} - \sqrt{D_3}),$$

$$\alpha_2 = \frac{1}{4}(1 + \sqrt{D_1} - \sqrt{D_2} - \sqrt{D_3}),$$

$$\alpha_3 = \frac{1}{4}(1 - \sqrt{D_1} - \sqrt{D_2} + \sqrt{D_3}).$$

Since we prefer our integral basis to contain 1, we replace  $w_0$  with 1, giving the integral basis

$$\mathcal{B} = \{1, w_1, w_2, w_3\}.$$

To compute the Gram matrix associated to this integral basis, we first compute the Gram matrix of the field basis  $\mathcal{F} = \{1, \sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3}\}$ . Our first step is to embed the field basis elements into the Minkowski space of  $K_2$ . With  $j$  denoting this embedding, we have

$$\begin{aligned} j(1) &= (1, 1, 1, 1), \\ j(\sqrt{D_1}) &= (\sqrt{D_1}, -\sqrt{D_1}, \sqrt{D_1}, -\sqrt{D_1}), \\ j(\sqrt{D_2}) &= (\sqrt{D_2}, \sqrt{D_2}, -\sqrt{D_2}, -\sqrt{D_2}), \\ j(\sqrt{D_3}) &= (\sqrt{D_3}, -\sqrt{D_3}, -\sqrt{D_3}, \sqrt{D_3}). \end{aligned}$$

With these vectors in hand, we get the matrix  $M_{\mathcal{F}}$  whose rows are a basis for the lattice  $j(R)$ :

$$M_{\mathcal{F}} = \begin{pmatrix} j(1) \\ j(\sqrt{D_1}) \\ j(\sqrt{D_2}) \\ j(\sqrt{D_3}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \sqrt{D_1} & -\sqrt{D_1} & \sqrt{D_1} & -\sqrt{D_1} \\ \sqrt{D_2} & \sqrt{D_2} & -\sqrt{D_2} & -\sqrt{D_2} \\ \sqrt{D_3} & -\sqrt{D_3} & -\sqrt{D_3} & \sqrt{D_3} \end{pmatrix}.$$

**Proposition 3.13.** The Gram matrix of the inner product on the Minkowski space of  $K_2$  with respect to this basis is

$$G_{\mathcal{F}} = M_{\mathcal{F}}M_{\mathcal{F}}^T = 4 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & D_1 & 0 & 0 \\ 0 & 0 & D_2 & 0 \\ 0 & 0 & 0 & D_3 \end{pmatrix}.$$

*Proof.* Define the diagonal matrix  $P$  by

$$P = \begin{pmatrix} 1 & & & \\ & \sqrt{D_1} & & \\ & & \sqrt{D_2} & \\ & & & \sqrt{D_3} \end{pmatrix}.$$

Note that

$$PA_2 = \begin{pmatrix} 1 & & & \\ & \sqrt{D_1} & & \\ & & \sqrt{D_2} & \\ & & & \sqrt{D_3} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \sqrt{D_1} & -\sqrt{D_1} & \sqrt{D_1} & -\sqrt{D_1} \\ \sqrt{D_2} & \sqrt{D_2} & -\sqrt{D_2} & -\sqrt{D_2} \\ \sqrt{D_3} & -\sqrt{D_3} & -\sqrt{D_3} & \sqrt{D_3} \end{pmatrix} = M_{\mathcal{F}}.$$

Thus, we have that

$$\begin{aligned} G_{\mathcal{F}} &= M_{\mathcal{F}}M_{\mathcal{F}}^T \\ &= PA_2(PA_2)^T \\ &= PA_2A_2^T P \\ &= P(4I_4)P^T \\ &= 4P^2. \end{aligned}$$

We have

$$4P^2 = 4 \begin{pmatrix} 1 & & & \\ & D_1 & & \\ & & D_2 & \\ & & & D_3 \end{pmatrix},$$

as desired. □

Next, we compute the Gram matrix attached to  $\mathcal{B}$ . To compute this Gram matrix, we use the change of basis matrix  $\frac{1}{4}B_2$  given by

$$B_2 = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Note that  $B_2$  is obtained by modifying the first row of  $A_2$  in order to get 1 in the integral basis. We get that

$$\begin{aligned} G_{\mathcal{B}} &= \left(\frac{1}{4}\right)^2 B_2 G_{\mathcal{F}} B_2^T \\ &= \left(\frac{1}{4}\right)^2 B_2 (4P^2) B_2^T \\ &= \frac{1}{4} B_2 P^2 B_2^T \\ &= \frac{1}{4} \begin{pmatrix} 4 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & D_1 & & \\ & & D_2 & \\ & & & D_3 \end{pmatrix} \begin{pmatrix} 4 & 1 & 1 & 1 \\ 0 & -1 & 1 & -1 \\ 0 & 1 & -1 & -1 \\ 0 & -1 & -1 & 1 \end{pmatrix} \\ &= \frac{1}{4} \begin{pmatrix} 4 & 0 & 0 & 0 \\ 1 & -D_1 & D_2 & -D_3 \\ 1 & D_1 & -D_2 & -D_3 \\ 1 & -D_1 & -D_2 & D_3 \end{pmatrix} \begin{pmatrix} 4 & 1 & 1 & 1 \\ 0 & -1 & 1 & -1 \\ 0 & 1 & -1 & -1 \\ 0 & -1 & -1 & 1 \end{pmatrix} \\ &= \frac{1}{4} \begin{pmatrix} 16 & & & \\ 4 & 1 + D_1 + D_2 + D_3 & 1 - D_1 - D_2 + D_3 & 1 + D_1 - D_2 - D_3 \\ 4 & 1 - D_1 - D_2 + D_3 & 1 + D_1 + D_2 + D_3 & 1 - D_1 + D_2 - D_3 \\ 4 & 1 + D_1 - D_2 - D_3 & 1 - D_1 + D_2 - D_3 & 1 + D_1 + D_2 + D_3 \end{pmatrix}. \end{aligned}$$

Next, to get the shape of  $K_2$ , we take the orthogonal projection onto  $j_{\mathbf{C}}(1)$ . According to Equation 2.1 we presented in Chapter 2, we get that the shape of  $K_2$  relative to the integral basis  $\mathcal{B}$  is given by

$$\text{sh}(K_2, \mathcal{B}) := G_{\mathcal{B}}^{\perp} = \frac{1}{4} \begin{pmatrix} D_1 + D_2 + D_3 & -D_1 - D_2 + D_3 & D_1 - D_2 - D_3 \\ -D_1 - D_2 + D_3 & D_1 + D_2 + D_3 & -D_1 + D_2 - D_3 \\ D_1 - D_2 - D_3 & -D_1 + D_2 - D_3 & D_1 + D_2 + D_3 \end{pmatrix}.$$

### 3.2.2 A Geometric Point of View

For a geometric interpretation of the shape we obtained, note that the entries of the Gram matrix can be seen as inner products. In general, if  $\mathcal{C} = \{v_1, \dots, v_n\}$ , the Gram matrix relative to  $\mathcal{C}$  is given by

$$G_{\mathcal{C}} = M_{\mathcal{C}} M_{\mathcal{C}}^T = [\langle v_i, v_j \rangle], \quad \text{with } 1 \leq i, j \leq n.$$

In our present case, the shape of  $K_2$  relative to the matrix  $\mathcal{B}$  is given by

$$\frac{1}{4} \begin{pmatrix} D_1 + D_2 + D_3 & -D_1 - D_2 + D_3 & D_1 - D_2 - D_3 \\ -D_1 - D_2 + D_3 & D_1 + D_2 + D_3 & -D_1 + D_2 - D_3 \\ D_1 - D_2 - D_3 & -D_1 + D_2 - D_3 & D_1 + D_2 + D_3 \end{pmatrix}.$$

Suppose that the three vectors in  $\mathbf{R}^3$  that define the lattice  $j(\mathcal{O}_{K_2}^{\perp})$  are denoted  $v_1, v_2$ , and  $v_3$ . Notice that the main diagonal entries are equal, meaning that the fundamental region of our lattice in  $\mathbf{R}^3$  is composed of three vectors of equal length:

$$|v_1| = |v_2| = |v_3| = \sqrt{\frac{1}{4}(D_1 + D_2 + D_3)}.$$

Additionally, the angles between these vectors are all distinct. The shape in this case is a *body-centered orthorhombic* lattice in  $\mathbf{R}^3$ .

Notice that we may write this matrix as

$$\text{sh}(K_2, \mathcal{B}) = \frac{1}{4} (D_1 M_1 + D_2 M_2 + D_3 M_3),$$

where

$$M_1 = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & 1 \\ -1 & 1 & 1 \end{pmatrix}, M_3 = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}.$$

The matrices  $M_1, M_2, M_3$  give a way of parametrizing the shapes of biquadratic extensions. In fact, these are the very matrices given in Definition 2.32.

To summarize, the shape of  $K_n$  relative to the integral basis  $\mathcal{B}$  is related to the matrix  $\mathcal{D}^*$ . If we scale each side of the primitive hypercubic lattice by  $\sqrt{D_j}$ , then  $\text{sh}(K_n, \mathcal{B})$  ends up being a scaled version of  $\mathcal{D}^*$ .

Since the shape allows for scaling, we can in fact express the shape of  $K_n$  in terms of ratios of the  $D_j$ 's. We make the following definitions.

**Definition 3.14.** Given a multiquadratic extension  $K_n$ , and its associated  $\ell$ -tuple  $(D_1, \dots, D_\ell)$ , we obtain an  $(\ell - 1)$ -tuple

$$\left( \frac{D_2}{D_1}, \dots, \frac{D_\ell}{D_1} \right)$$

by dividing through each term by  $D_1$  and dropping the first term. This resulting point in  $\mathbf{Q}^{\ell-1}$  characterizes the shape of  $K_n$ . We can write

$$\text{sh}(K_n, \mathcal{B}) = \text{sh} \left( \frac{D_2}{D_1}, \dots, \frac{D_\ell}{D_1} \right) = M_1 + \sum_{j=2}^{\ell} \frac{D_j}{D_1} M_j.$$

In order to prove a statement regarding equidistribution of multiquadratic extensions, we will need to develop a way of counting these fields. However, their infinitude must be handled by placing a bound  $X$  on the discriminant. As we have shown, the discriminant of  $K_n$  is equal to the product of all the  $D_j$ 's. We will need to measure how many fields have shape in a box in  $\mathcal{S}_{K_n}$ . This amounts to placing a bound on the ratios  $\frac{D_j}{D_1}$ .

The next chapter is devoted to counting our number fields, which will in turn allow us to prove the main result of this thesis, namely, that the shapes of multiquadratic fields are indeed equidistributed.

# CHAPTER 4

## COUNTING NUMBER FIELDS

In the previous chapter, we calculated the shapes of certain totally real multiquadratic fields  $K_n$ . We then represented the shape of  $K_n$  as a square matrix of dimension  $\ell = 2^n - 1$ . The entries in this shape matrix are given in terms of the numbers  $D_j, 1 \leq j \leq \ell$ , where  $\mathbf{Q}(\sqrt{D_j})$  are the quadratic subfields of  $K_n$ . We would like to determine a method of counting how many of these number fields there are with discriminant bounded by some positive real number  $X$  and with shape in a given region.

In this chapter, we restrict to the case  $n = 3$ . The main number theoretic ideas already occur in this case and suggest what steps are needed to show that, for general  $n$ , the shapes of multiquadratic fields (allowing the cases of complex number fields, as well as ramification at 2) also admit a regularized equidistribution as the absolute discriminant tends to infinity.

This chapter will be broken up into four parts. A multiquadratic extension  $K_n$  and, more importantly, its shape, is characterized by the  $\ell$ -tuple  $(D_1, \dots, D_\ell)$ . Therefore, these number fields correspond to certain lattice points in  $\mathbf{Z}^\ell$ . Since the discriminant of  $K_n$  is given in terms of the  $D_j$ s, bounding the discriminant by some real number  $X$  restricts to a finite number of lattice points that lie in some region. The first goal of this chapter will be to give an adequate parametrization of multiquadratic extensions in terms of lattice points that will allow us to count them.

Once a parametrization has been given, we compute the volume of the region in which these lattice points lie. The *Principle of Lipschitz* then allows us to determine the number of lattice points relative to this volume (up to some error).

Since not every lattice point in a given region represents a multiquadratic extension, our next goal will be to introduce a counting (sieving) method for determining how many number fields actually occur in a given region.

The final part of this chapter will focus on proving that the shapes of triquadratic extensions are equidistributed in the subset of the space of shapes in which they live as the discriminant goes to infinity.

### 4.1 Counting Triquadratic Number Fields

In this chapter, we will prove counting results pertaining to  $n = 3$ , as well as establish the equidistribution of shapes of triquadratic extensions.

For the setup, we let  $K_3 = \mathbf{Q}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_4})$ , with  $D_1, D_2, D_4$  positive, distinct squarefree

integers that are greater than 1, congruent to 1 modulo 4, and such that the squarefree part of  $D_1 D_2 \neq D_4$ . Associated to this field is a 7-tuple of positive squarefree integers

$$(D_1, D_2, D_3, D_4, D_5, D_6, D_7),$$

where  $\mathbf{Q}(\sqrt{D_j})$ ,  $1 \leq j \leq 7$  are the 7 quadratic subfields of  $K_3$  given in Equation (3.1). As we showed in Chapter 3, the shape  $\text{sh}(K_3, \mathcal{B})$  of  $K_3$  relative to the integral basis  $\mathcal{B}$  of  $\mathcal{O}_K$  is

$$\text{sh}(K_3, \mathcal{B}) = \text{sh} \left( \frac{D_2}{D_1}, \dots, \frac{D_7}{D_1} \right).$$

Our goal in the next section is to parametrize the collection of totally real triquadratic extensions unramified at 2, with bounded discriminant and whose shape lies in  $W(R_2, \dots, R_7)$  in a way that allows us to count such fields.

## 4.2 Parametrization

**Definition 4.1.** Fix real numbers  $X$  and  $R_2, \dots, R_7$ . Let  $\mathcal{N}_3(X, R_2, \dots, R_7)$  denote the integer

$$\mathcal{N}_3(X, R_2, \dots, R_7) := \#\{K_3 \in \mathcal{M}_3^+(i) : \Delta(K_3) < X; \text{sh}(K_3) \in W(R_2, \dots, R_7)\},$$

where  $W(R_2, \dots, R_7)$  is given in Definition 2.42.

The strategy for computing this number is to find a parametrization of our triquadratic extensions. The parameters we choose must be compatible with our notion of discriminant and shape.

Naively, one might expect to parametrize our fields with  $D_1, \dots, D_7$ . However, the set

$$\left\{ (D_1, \dots, D_7) \in \mathbf{Z}_{\geq 1}^7 : D_1 \cdot \dots \cdot D_7 < X; \text{sh} \left( \frac{D_2}{D_1}, \dots, \frac{D_7}{D_1} \right) \in W(R_2, \dots, R_7) \right\}$$

carries several dependencies that are ignored when considering the set above. A way to circumvent these dependencies is to work with a *strongly carefree* tuple  $(g_1, \dots, g_7)$ , whose entries are squarefree and pairwise relatively prime integers. We construct this tuple below.

### 4.2.1 Strongly Carefree Tuples

**Definition 4.2.** We call an  $\ell$ -tuple  $(g_1, \dots, g_\ell)$  of integers *strongly carefree* if the  $g_i$  are squarefree and pairwise relatively prime.

The following gives a way of constructing a strongly carefree tuple  $(g_1, \dots, g_7)$  from  $(D_1, \dots, D_7)$ .

Given a 7-tuple  $(D_1, \dots, D_7)$  corresponding to a field  $K_3$ , we look at the relatively prime factors of the generators  $D_1, D_2$ , and  $D_4$ .

First, every generator may have a common factor, which we denote by  $g_1$ . In other words, we have

$$D_1 = g_1 \dots,$$

$$D_2 = g_1 \dots,$$

$$D_4 = g_1 \dots$$

Next, note that  $D_4$  may share a factor with  $D_2$  and another with  $D_1$ , call these  $g_2$  and  $g_3$ , respectively. So

$$D_1 = g_1 g_3 \dots,$$

$$D_2 = g_1 g_2 \dots,$$

$$D_4 = g_1 g_2 g_3 \dots$$

To finalize the description of  $D_4$ , we note that it may have a factor, say  $g_4$ , that is not shared with the other generators. Thus,

$$D_1 = g_1 g_3 \dots,$$

$$D_2 = g_1 g_2 \dots,$$

$$D_4 = g_1 g_2 g_3 g_4.$$

Next, we proceed with  $D_2$ . We already addressed the factor it shares with  $D_4$ , but it might have a factor it only shares with  $D_1$ , call it  $g_5$ :

$$D_1 = g_1 g_3 g_5 \dots,$$

$$D_2 = g_1 g_2 g_5 \dots,$$

$$D_4 = g_1 g_2 g_3 g_4.$$

Finally,  $D_2$  may have its own factor, which we call  $g_6$ . This also leaves  $D_1$  to have its own factor as well. Denote it by  $g_7$ . Thus, we have

$$D_1 = g_1 g_3 g_5 g_7,$$

$$D_2 = g_1 g_2 g_5 g_6,$$

$$D_4 = g_1 g_2 g_3 g_4.$$

From the generators, we obtain  $D_3, D_5, D_6$ , and  $D_7$  according to their definition, keeping track of clearing any square factor. We get:

**Definition 4.3.** The generators  $D_1, \dots, D_7$  of  $K_3$  are written in terms of strongly carefree integers

$g_1, \dots, g_7$  as follows:

$$D_1 = g_1 g_3 g_5 g_7,$$

$$D_2 = g_1 g_2 g_5 g_6,$$

$$D_3 = g_2 g_3 g_6 g_7,$$

$$D_4 = g_1 g_2 g_3 g_4,$$

$$D_5 = g_2 g_4 g_5 g_7,$$

$$D_6 = g_3 g_4 g_5 g_6,$$

$$D_7 = g_1 g_4 g_6 g_7.$$

By construction, the 7-tuple  $(g_1, \dots, g_7)$  is strongly carefree. A faster way to recover this tuple (that also generalizes nicely for every  $n$ ) is with the use of the matrix  $A_3$ :

$$A_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

If we delete the first row and column, we obtain the matrix  $A_3^*$  given by

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

If we let each row of this matrix represent  $D_1, \dots, D_7$  and each column (from right to left) represent  $g_1, \dots, g_7$  respectively, then  $D_i$  picks up a factor  $g_j$  if the  $i, (7-j)$ -entry of the matrix is equal to  $-1$ .

With a strongly carefree tuple in hand, we proceed to express the discriminant and shape of  $K_3$  in terms of the  $g$ 's. We do this for  $n$  in general.

**Proposition 4.4.** The discriminant of  $K_n$  is given by

$$\Delta(K_n) = D_1 \cdots D_\ell = (g_1 \cdots g_\ell)^{2^{n-1}}.$$

*Proof.* We already showed that

$$\Delta(K_n) = \prod_{1 \leq j \leq \ell} D_j.$$

To prove the equation involving  $g_j$ 's, it suffices to show that each  $g_j$  occurs exactly  $2^{n-1}$  times. From the algorithm we introduced, the occurrence of each  $g_j$  is equal to the number of entries that are  $-1$  on each column of the matrix  $A_n^*$ . We will show that each column has  $2^{n-1}$  entries that are  $-1$ .

We argue by induction on  $n$ . If  $n = 1$  then

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Then  $A_1^* = (-1)$ , so  $-1$  occurs once, and  $1 = 2^0$ .

Suppose the claim holds for  $1 \leq k \leq n$ . In particular, it also holds for the matrix  $-A_n$ .

Now,  $A_{n+1}$  is defined recursively as

$$A_{n+1} = \begin{pmatrix} A_n & A_n \\ A_n & -A_n \end{pmatrix}.$$

So by the inductive step, the number of entries of each column of  $A_{n+1}$  that are equal to  $-1$  is

$$2(2^{n-1}) = 2^n = 2^{(n+1)-1}.$$

□

**Corollary 4.5.** For  $n = 3$ , we have

$$\Delta(K_3) = (g_1 \cdots g_7)^4.$$

With the discriminant in terms of the  $g_j$ 's, we proceed with computing the shape of  $K_3$  in terms of the  $g$ 's. Since the shape is defined in terms of the ratios, we make the following definition.

**Definition 4.6.** Define the variables  $x_2, \dots, x_j$  by

$$x_j := \frac{D_j}{D_1}, \quad 2 \leq j \leq 7.$$

Then we express these new variables in terms of  $g_1, \dots, g_7$  as follows:

$$x_2 = \frac{g_2 g_6}{g_3 g_7}, x_3 = \frac{g_2 g_6}{g_1 g_5}, x_4 = \frac{g_2 g_4}{g_5 g_7}, x_5 = \frac{g_2 g_4}{g_1 g_3}, x_6 = \frac{g_4 g_6}{g_1 g_7}, x_7 = \frac{g_4 g_6}{g_3 g_5}.$$

### 4.2.2 Choosing Generators

We would like a way of parametrizing triquadratic extensions  $K_3$  in terms of 7-tuples  $(g_1, \dots, g_7)$  that are strongly carefree. However, any mapping of the form

$$K_3 \mapsto (g_1, \dots, g_7)$$

will be multi-valued, since there can be several permutations of  $(g_1, \dots, g_7)$  that define the same field.

We want a way of counting the number of permutations of a given 7-tuple that gives rise to the same field. This is equivalent to counting the number of ways of choosing a generating set.

**Definition 4.7.** Let  $K_3$  be a triquadratic field, and denote its associated 7-tuple by  $(D_1, \dots, D_7)$ . By a *generating set* for  $K_3$ , we mean an ordered triple  $(D_i, D_j, D_k)$  chosen from  $(D_1, \dots, D_7)$  such that

$$K_3 = \mathbf{Q}(\sqrt{D_i}, \sqrt{D_j}, \sqrt{D_k}).$$

Recall that once a generating set for  $K_3$  has been established, the rest of the  $D$ 's are defined by taking the squarefree part of the product of two generators.

**Proposition 4.8.** Let  $(D_1, \dots, D_7)$  be the 7-tuple corresponding to a triquadratic extension  $K_3$ . Then there are exactly 24 ways of choosing a generating set  $(D_i, D_j, D_k)$  for  $K_3$  from  $(D_1, \dots, D_7)$  such that  $D_i$  is the minimum of  $D_1, \dots, D_7$ .

*Proof.* We are free to choose any of the  $D$ 's as the first generator, so we pick  $D_i = \min\{D_1, \dots, D_7\}$ . After that, we can choose any of the 6 remaining numbers as a second generator, and call it  $D_j$ . Of the remaining  $D$ 's in the list, one will be equal to the squarefree part of  $D_i D_j$ . We avoid choosing this number, which leaves us with 4 choices for the final generator.

This gives  $(6)(4) = 24$  possible generating sets. □

**Remark 4.9.** Using binary notation to denote the numbers  $1, \dots, 7$  and placing these bits as columns (or rows) of a  $3 \times 3$  matrix, then we get a generating set exactly when the corresponding matrix is invertible. We get that  $\#\text{GL}_3(\mathbb{F}_2) = 168$  generators for  $K_3$ . This argument shows that, in general, the  $\ell$ -tuple for  $K_n$  contains  $\#\text{GL}_n(\mathbb{F}_2)$  generating sets (without any ordering).

With the number of generating sets accounted for, we can now give a well-defined mapping between triquadratic extensions and points in  $\mathbf{Z}^7$ .

### 4.2.3 A Correspondence Between Fields and Points

Using  $g_1, \dots, g_7$  as new parameters, we want to define a mapping between our number fields and a subset of 7-tuples  $(g_1, \dots, g_7)$  which satisfy certain properties.

Recall that  $\mathcal{M}_3^+$  denotes the collection of totally real triquadratic extensions (ignoring congruence conditions modulo 4).

The following lemma describes a partition of 7-tuples  $(g_1, \dots, g_7)$  into four types, according to the number of 1's that can occur. If more than four 1's occur, then one of the  $D_j$  will be equal to 1. We therefore get the following lemma:

**Lemma 4.10.** Let  $K_3 \in \mathcal{M}_3^+$ . For a strongly carefree tuple  $(g_1, \dots, g_7)$  corresponding to  $K_3$ , we have that  $(g_1, \dots, g_7)$  falls under one of the following types:

- (i) All 7 entries are distinct.
- (ii) Two entries equal 1, the other 5 entries are distinct and not equal to 1.
- (iii) Three entries equal 1, the other 4 entries are distinct and not equal to 1.
- (iv) Four entries equal 1, the other 3 entries are distinct and not equal to 1.

The results that follow will be dependent on which case we specify. However, we will show in [4.27](#) that only the tuples of type (i) will affect the counting of number fields. We express  $\mathcal{M}_3^+$  as the disjoint union

$$\mathcal{M}_3^+ = \mathcal{M}_{3,i}^+ \cup \mathcal{M}_{3,ii}^+ \cup \mathcal{M}_{3,iii}^+ \cup \mathcal{M}_{3,iv}^+,$$

where  $\mathcal{M}_{3,k}^+$  denotes the triquadratic extensions  $K_3$  whose corresponding tuple  $(g_1, \dots, g_7)$  is of type (k).

Our goal is to relate the number of triquadratic extensions to the number of strongly carefree 7-tuples.

**Lemma 4.11.** Let  $(g_1, \dots, g_7)$  denote a strongly carefree tuple of type (i) that corresponds to some triquadratic extension  $K_3 \in \mathcal{M}_{3,i}^+$ . Then any permutation of  $(g_1, \dots, g_7)$  gives rise to some triquadratic field.

*Proof.* Let  $(g_1, \dots, g_7)$  denote a strongly carefree tuple that corresponds to some triquadratic field  $K_3$ . We can recover this field as follows. Define the tuple  $(D_1, \dots, D_7)$  as in [Definition 4.3](#).

From here, we can pick any generating set of  $K_3$ . For instance, we have

$$K_3 = \mathbf{Q}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_4}).$$

Now let  $\sigma \in S_7$ . Denote the permuted tuple by

$$(g_{\sigma(1)}, \dots, g_{\sigma(7)}).$$

From here, we can define the tuple

$$(D_1^\sigma, \dots, D_7^\sigma)$$

by

$$D_1^\sigma = g_{\sigma(1)}g_{\sigma(3)}g_{\sigma(5)}g_{\sigma(7)},$$

$$D_2^\sigma = g_{\sigma(1)}g_{\sigma(2)}g_{\sigma(5)}g_{\sigma(6)},$$

$$D_3^\sigma = g_{\sigma(2)}g_{\sigma(3)}g_{\sigma(6)}g_{\sigma(7)},$$

$$D_4^\sigma = g_{\sigma(1)}g_{\sigma(2)}g_{\sigma(3)}g_{\sigma(4)},$$

$$D_5^\sigma = g_{\sigma(2)}g_{\sigma(4)}g_{\sigma(5)}g_{\sigma(7)},$$

$$D_6^\sigma = g_{\sigma(3)}g_{\sigma(4)}g_{\sigma(5)}g_{\sigma(6)},$$

$$D_7^\sigma = g_{\sigma(1)}g_{\sigma(4)}g_{\sigma(6)}g_{\sigma(7)},$$

Then, for instance,  $\{D_1^\sigma, D_2^\sigma, D_4^\sigma\}$  is a generating set for some triquadratic extension  $K_s^\sigma$ . That is,

$$K_3^\sigma := \mathbf{Q}(\sqrt{D_1^\sigma}, \sqrt{D_2^\sigma}, \sqrt{D_4^\sigma}) \in \mathcal{M}_3^+. \quad \square$$

Now, by placing a bound on the discriminant, we get finitely many number fields. We are now ready to parametrize triquadratic extensions. Since we want to count triquadratic extensions whose shapes lie in the set  $W(R_2, \dots, R_7)$ , the next definition allows us to count strongly carefree tuples  $(g_1, \dots, g_7)$  in such a way that the corresponding ratios  $x_2, \dots, x_7$  are in increasing order.

**Definition 4.12.** Fix a permutation  $\sigma \in S_6$ . Let  $(k)$  represent type (i),(ii), (iii), or (iv), as in Definition 4.10. Define  $\mathcal{G}_{k,\sigma}^+(X, R_2, \dots, R_7)$  to be the set

$$\left\{ (g_1, \dots, g_7) \text{ str. carefree of type } (k) \in \mathbf{Z}_{\geq 1}^7 : \prod_{j=1}^7 g_j^4 < X, x_{\sigma(2)} < \dots < x_{\sigma(7)} \leq R_7, R_j \leq x_{\sigma(j)} \right\}.$$

Define the set

$$\mathcal{G}_k^+(X, R_2, \dots, R_7) := \bigcup_{\sigma \in S_6} \mathcal{G}_{k,\sigma}^+(X, R_2, \dots, R_7).$$

**Theorem 4.13.** There is a surjective mapping

$$\mathcal{G}_i^+((X, R_2, \dots, R_7)) \xrightarrow{24-1} \mathcal{M}_{3,i}^+(X, W(R_2, \dots, R_7))$$

given by

$$(g_1, \dots, g_7) \mapsto \mathbf{Q}(\sqrt{g_1 g_3 g_5 g_7}, \sqrt{g_1 g_2 g_5 g_6}, \sqrt{g_1 g_2 g_3 g_4}) = K_3.$$

*Proof.* Given  $(g_1, \dots, g_7) \in \mathcal{G}_k^+(X, R_2, \dots, R_7)$ , we define

$$K_3 = \mathbf{Q}(\sqrt{g_1 g_3 g_5 g_7}, \sqrt{g_1 g_2 g_5 g_6}, \sqrt{g_1 g_2 g_3 g_4}),$$

whose quadratic subfields are generated by the square roots of  $D_1, \dots, D_7$ . Note that  $(D_1, D_2, D_4)$  is not uniquely determined by  $K_3$ .

The 7-tuples  $(D_1, \dots, D_7)$  are uniquely determined by the 7-tuples  $(g_1, \dots, g_7)$ . Thus, with  $D_1 < D_j$  for  $j \geq 2$ , we get a tuple  $(g_1, \dots, g_7)$  with  $1 < x_j$  for  $j \geq 2$ . For  $\text{sh}(K_3) \in W(R_2, \dots, R_7)$ , there is a unique permutation  $\tau \in S_6$  such that

$$\frac{D_{\tau(2)}}{D_1} \leq \dots \leq \frac{D_{\tau(7)}}{D_1} \leq R_7,$$

and

$$R_j \leq \frac{D_{\tau(j)}}{D_1} \text{ for } 2 \leq j \leq 6.$$

Furthermore, for  $(g_1, \dots, g_7) \in \mathcal{G}_i^+(X, R_2, \dots, R_7)$  we must have

$$x_{\tau(2)} \leq \dots \leq x_{\tau(7)} \leq R_7, \text{ and } R_j \leq x_{\tau(j)} \text{ for } 2 \leq j \leq 6,$$

for this  $\tau \in S_6$ .

Since the shape of  $K_3$  is given by

$$\text{sh}(K_3) = \text{sh}(x_2, \dots, x_7) = \text{sh}(x_{\tau(2)}, \dots, x_{\tau(7)}),$$

it follows that  $\text{sh}(K_3) \in W(R_2, \dots, R_7)$  if and only if the corresponding tuple

$$(g_1, \dots, g_7) \in \mathcal{G}_{k,\tau}^+(X, R_2, \dots, R_7).$$

From Proposition 4.8,  $K_3$  has 24 distinct generating sets  $(D_i, D_j, D_k)$  with  $D_i$  smallest. To each of these generating sets, we have permutations  $\tau_j (1 \leq j \leq 24) \in S_6$  for which the corresponding tuple  $(g_1, \dots, g_7)$  of  $K_3$  lies in the union

$$(g_1, \dots, g_7) \in \bigcup_{j=1}^{24} \mathcal{G}_{k,\tau_j}^+(X, R_2, \dots, R_7).$$

This implies that this map is 24-to-1. □

**Corollary 4.14.** We have

$$\frac{1}{24} \#\mathcal{G}_i^+(X, R_2, \dots, R_7) = \#\mathcal{M}_{3,i}^+(X, W(R_2, \dots, R_7)).$$

This theorem gives a relationship between triquadratic number fields and an explicit set of strongly carefree points in  $\mathbf{Z}^7$ . Since we want to count triquadratic extensions of bounded discriminant and prescribed shape, this restricts the number of integer points to a bounded region. The next section describes the region in which these points live, and provides an approximation to the number of such points given by the region's volume.

### 4.3 Volume

Since we are counting totally real triquadratic extensions with bounded discriminant, the corresponding strongly carefree tuples  $(g_1, \dots, g_7)$  live in a bounded Euclidean region. We will count all integer tuples in this region. By abusing notation, we will use  $g_1, \dots, g_7$  to denote real variables. For fixed real numbers  $X$  and  $R$ , and for  $\sigma \in S_6$ , we define the region  $\mathcal{R}_{3,\sigma}(X, R_2, \dots, R_7)$  to be

$$\left\{ (g_1, \dots, g_7) \in \mathbf{R}_{>0}^7 : \prod_{j=1}^7 g_j^4 < X; x_{\sigma(2)} < \dots < x_{\sigma(7)} \leq R_7, R_j < x_{\sigma(j)} \text{ for } 2 \leq j \leq 6 \right\}, \quad (4.1)$$

where  $x_2, \dots, x_7$  are defined as in Definition 4.6, and denote

$$\mathcal{R}_3(X, R_2, \dots, R_7) := \bigcup_{\sigma \in S_6} \mathcal{R}_{3,\sigma}(X, R_2, \dots, R_7).$$

We will proceed to compute the volume of  $\mathcal{R}_{3,\text{id}}(X, R_2, \dots, R_7)$  corresponding to the identity permutation, then show that each region  $\mathcal{R}_{3,\sigma}(X, R_2, \dots, R_7)$  has the same volume, which shows that the volume of the union of all the regions is

$$6! \text{Vol}(\mathcal{R}_{3,\text{id}}(X, R_2, \dots, R_7)).$$

We are interested in the number of  $\mathbf{Z}$  points that occur in this region. From the previous section, if these integer points are to represent our number fields of interest, then we need to restrict to counting points that are strongly carefree. Lastly, we would like to count only those integer points satisfying congruence conditions modulo 4 that allow for

$$(D_1, \dots, D_7) \equiv (1, \dots, 1) \pmod{4}.$$

The last condition, as well as the condition of being strongly carefree, both rely on congruence conditions, and will be dealt with separately.

In this section, we will compute the volume of  $\mathcal{R}_3(X, R_2, \dots, R_7)$ , and use the *Principle of Lipschitz*, which gives an approximation to the number of integer points the region contains.

**Theorem 4.15.** The volume of  $\mathcal{R}_{3,\text{id}}(X, R_2, \dots, R_7)$  is given by

$$\text{Vol}(\mathcal{R}_{3,\text{id}}(X, R)) = \frac{X^{\frac{1}{4}}}{56} F(R_2, \dots, R_7),$$

where  $F(R_2, \dots, R_7)$  is given in Equation 2.4.

*Proof.* We set up the multiple integral for the volume by defining a change of coordinates. Rather than integrating with respect to  $g_1, \dots, g_7$ , we will use the functions  $x_2, \dots, x_7$ . We define a new variable,

$$x_1 = g_1 g_3 g_5 g_7.$$

We have that the bounds of integration for  $x_2, \dots, x_7$  are from 1 to  $R$ . We need a bound on  $x_1$ . Recall that the discriminant of  $K_3$  is given by

$$\Delta(K_3) = (g_1 \cdots g_7)^4.$$

Also, we have that

$$x_2 x_3 x_4 x_5 x_6 x_7 = \frac{(g_2 g_4 g_6)^4}{x_1^3} = \frac{\Delta(K_3)}{x_1^7}.$$

If we are bounding the discriminant by  $X$ , it follows that

$$0 < x_1 \leq \left( \frac{X}{x_2 x_3 x_4 x_5 x_6 x_7} \right)^{\frac{1}{7}}.$$

The volume is then given by

$$\text{Vol}(\mathcal{R}_{3,\text{id}}(X, R_2, \dots, R_7)) = \int_{R_6}^{R_7} \cdots \int_{R_2}^{x_3} \int_0^{\left(\frac{X}{x_2 \cdots x_7}\right)^{\frac{1}{7}}} \left| J \left( \frac{\partial g_i}{\partial x_j} \right) \right| dx_1 \cdots dx_7.$$

We compute the Jacobian of this change of basis. Note that the variables  $x_1, \dots, x_7$  are defined as rational expressions of  $g_1, \dots, g_7$ . In particular, the first partial derivatives exist and do not vanish away from 0. The inverse function theorem implies that

$$J \left( \frac{\partial g_i}{\partial x_j} \right) = \left( J \left( \frac{\partial x_i}{\partial g_j} \right) \right)^{-1}.$$

We compute the inverse of the Jacobian and express its determinant in terms of the  $x_j$ s. We have

$$J\left(\frac{\partial x_i}{\partial g_j}\right) = \begin{pmatrix} g_3 g_5 g_7 & 0 & g_1 g_5 g_7 & 0 & g_1 g_3 g_7 & 0 & g_1 g_3 g_5 \\ 0 & \frac{g_6}{g_3 g_7} & -\frac{g_2 g_6}{g_3^2 g_7} & 0 & 0 & \frac{g_2}{g_3 g_7} & -\frac{g_2 g_6}{g_3 g_7^2} \\ -\frac{g_2 g_6}{g_1^2 g_5} & \frac{g_6}{g_1 g_5} & 0 & 0 & -\frac{g_2 g_6}{g_1 g_5^2} & \frac{g_2}{g_1 g_5} & 0 \\ 0 & \frac{g_4}{g_5 g_7} & 0 & \frac{g_2}{g_5 g_7} & -\frac{g_2 g_4}{g_5^2 g_7} & 0 & -\frac{g_2 g_4}{g_5 g_7^2} \\ -\frac{g_2 g_4}{g_1^2 g_3} & \frac{g_4}{g_1 g_3} & -\frac{g_2 g_4}{g_1 g_3^2} & \frac{g_2}{g_1 g_3} & 0 & 0 & 0 \\ -\frac{g_4 g_6}{g_1 g_7^2} & 0 & 0 & \frac{g_6}{g_1 g_7} & 0 & \frac{g_4}{g_1 g_7} & -\frac{g_4 g_6}{g_1 g_7^2} \\ 0 & 0 & -\frac{g_4 g_6}{g_3^2 g_5} & \frac{g_6}{g_3 g_5} & -\frac{g_4 g_6}{g_3 g_5^2} & \frac{g_4}{g_3 g_5} & 0 \end{pmatrix}.$$

Taking the inverse of the determinant of this matrix yields

$$\left|\left(\frac{\partial x_i}{\partial g_j}\right)\right|^{-1} = \frac{1}{32} \left(\frac{g_1 g_3 g_5 g_7}{g_2 g_4 g_6}\right)^3.$$

Now we must express this as a function of  $x_j$ s. Note that the numerator is just  $x_1^3$ . We obtain the denominator by looking at the discriminant:

$$(g_2 g_4 g_6)^4 = x_1^3 (x_2 \cdots x_7),$$

from which we get

$$(g_2 g_4 g_6)^3 = x_1^{\frac{9}{4}} \cdot (x_2 \cdots x_7)^{\frac{3}{4}}.$$

This gives

$$\left|J\left(\frac{\partial g_i}{\partial x_j}\right)\right|^{-1} = \frac{1}{32} x_1^{\frac{3}{4}} (x_2 \cdots x_7)^{-\frac{3}{4}}.$$

Thus, the volume is given by

$$\begin{aligned} \text{Vol}(\mathcal{R}_{3,\text{id}}(X, R_2, \dots, R_7)) &= \frac{1}{32} \int_{R_6}^{R_7} \cdots \int_{R_2}^{x_3} \int_0^{\left(\frac{x}{x_2 \cdots x_7}\right)^{\frac{1}{7}}} x_1^{\frac{3}{4}} (x_2 \cdots x_7)^{-\frac{3}{4}} dx_1 dx_2 \cdots dx_7 \\ &= \frac{1}{32} \cdot \frac{4}{7} X^{\frac{1}{4}} \int_{R_6}^{R_7} \cdots \int_{R_2}^{x_3} (x_2 \cdots x_7)^{-1} dx_2 \cdots dx_7 \\ &= \frac{X^{\frac{1}{4}}}{56} F(R_2, \dots, R_7), \end{aligned}$$

where the last equation follows from Equations (2.2) and (2.4).  $\square$

Now, to compute the volume of  $\mathcal{R}_{3,\sigma}(X, R_2, \dots, R_7)$ , where  $\sigma$  is any permutation in  $S_6$ , we set up the integral with the variables  $y_i = x_{\sigma(i)}$  for  $1 \leq i \leq 7$ . This yields

$$\begin{aligned}\text{Vol}(\mathcal{R}_{3,\sigma}(X, R_2, \dots, R_7)) &= \frac{1}{32} \int_{R_6}^{R_7} \cdots \int_{R_2}^{y_3} \int_0^{\left(\frac{X}{y_2 \cdots y_7}\right)^{\frac{1}{7}}} y_1^{\frac{3}{4}} (y_2 \cdots y_7)^{-\frac{3}{4}} dy_1 dy_2 \cdots dy_7 \\ &= \text{Vol}(\mathcal{R}_{3,\text{id}}(X, R_2, \dots, R_7)).\end{aligned}$$

Thus, we get that the volume of  $\mathcal{R}_3(X, R_2, \dots, R_7)$  is given by

$$\text{Vol}(\mathcal{R}_3(X, R_2, \dots, R_7)) = \frac{6! X^{\frac{1}{4}}}{56} F(R_2, \dots, R_7).$$

Now we want to count how many lattice points lie in the region  $\mathcal{R}_3(X, R_2, \dots, R_7)$ . We have the following theorem.

**Theorem 4.16.** Denote the set of integer tuples that occur in the region  $\mathcal{R}_3(X, R_2, \dots, R_7)$  by

$$\mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_7) := \mathbf{Z}^7 \cap \mathcal{R}_3(X, R_2, \dots, R_7).$$

Then

$$\#\mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_7) = \text{Vol}(\mathcal{R}_3(X, R_2, \dots, R_7)) + O\left(X^{\frac{3}{14}}\right).$$

*Proof.* In [Bha05, Lemma 9], it is shown that the error is given by

$$|\mathcal{R}_3(X, R_2, \dots, R_7) - \mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_7)| = O\left(\max_{0 \leq m \leq 6} (V_m)\right),$$

where  $V_m$  denotes the maximum volume of any of the projections of  $\mathcal{R}_3(X, R_2, \dots, R_7)$  onto the the  $m$  dimensional coordinate hyperplanes obtained by setting the remaining  $7 - m$  coordinates equal to zero.

Let  $N := X^{1/4}$ . We will show that, for  $0 \leq m \leq 6$ ,

$$V_m = O(N^{m/7}).$$

In order to prove the above equation, it suffices to show that for  $(g_1, \dots, g_7) \in \mathcal{R}_3(X, R_2, \dots, R_7)$ ,

$$g_j = O(N^{1/7}),$$

for  $1 \leq j \leq 7$ , since this set contains  $\mathcal{R}_3(X, R_2, \dots, R_7)$ . It then follows that

$$V_m = V_m(g_{i_1}, \dots, g_{i_m}) = O(N^{m/7}),$$

where  $i_1, \dots, i_m$  represents any  $m$  numbers from 1 to 7. We show the computation that  $g_2 = O(N^{1/7})$ : Consider the expression

$$(x_2 x_3 x_4 x_5)^{3/2} (x_6 x_7)^{-2} (g_1 g_2 g_3 g_4 g_5 g_6 g_7).$$

Writing the  $x_j$ s in terms of the  $g$ s as in Definition 4.6, we get

$$\left(\frac{g_2g_6}{g_3g_7}\right)^{3/2} \left(\frac{g_2g_6}{g_1g_5}\right)^{3/2} \left(\frac{g_2g_4}{g_5g_7}\right)^{3/2} \left(\frac{g_2g_4}{g_1g_3}\right)^{3/2} \left(\frac{g_1g_7}{g_4g_6}\right)^2 \left(\frac{g_3g_5}{g_4g_6}\right)^2 (g_1g_2g_3g_4g_5g_6g_7).$$

Simplifying this expression yields  $g_2^7$ . Recall from (4.1), we have that

$$g_1g_2g_3g_4g_5g_6g_7 \leq X^{1/4} = N,$$

and

$$x_2, \dots, x_7 \leq R_7.$$

From these inequalities, we get that

$$g_2^7 = (x_2x_3x_4x_5)^{3/2}(x_6x_7)^{-2}(g_1g_2g_3g_4g_5g_6g_7) \leq R_7^{(3/2) \cdot 4 - 2 - 2} N = R_7^2 N.$$

Solving for  $g_2$ , we get

$$g_2 \leq R_7^{2/7} N^{1/7},$$

which implies that  $g_2 = O(N^{1/7})$ . Similar expressions allow us to obtain  $g_j^7$ . Explicitly, for  $1 \leq j \leq 7$ , we get

$$g_j^7 = x_2^{c_2} x_3^{c_3} x_4^{c_4} x_5^{c_5} x_6^{c_6} x_7^{c_7} g_1g_2g_3g_4g_5g_6g_7,$$

where the powers  $c_2 \dots, c_7$  are summarized in the following table:

$j$	$c_2$	$c_3$	$c_4$	$c_5$	$c_6$	$c_7$
1	$\frac{3}{2}$	-2	$\frac{3}{2}$	-2	-2	$\frac{3}{2}$
2	$\frac{3}{2}$	$\frac{3}{2}$	$\frac{3}{2}$	$\frac{3}{2}$	-2	-2
3	-2	$\frac{3}{2}$	$\frac{3}{2}$	-2	$\frac{3}{2}$	-2
4	-2	-2	$\frac{3}{2}$	$\frac{3}{2}$	$\frac{3}{2}$	$\frac{3}{2}$
5	$\frac{3}{2}$	-2	-2	$\frac{3}{2}$	$\frac{3}{2}$	-2
6	$\frac{3}{2}$	$\frac{3}{2}$	-2	-2	$\frac{3}{2}$	$\frac{3}{2}$
7	-2	$\frac{3}{2}$	-2	$\frac{3}{2}$	-2	$\frac{3}{2}$

With these equations, note that the powers of  $R_7$  differ slightly; however, we get

$$g_j = O(N^{1/7}),$$

for  $1 \leq j \leq 7$ . It then follows that the error is given by

$$O\left(\max_{0 \leq m \leq 6} (V_m)\right) = \max_{0 \leq m \leq 6} (O(N^{m/7})) = O(N^{6/7}) = O(X^{3/14}). \quad \square$$

Combining the last two theorems, we get:

**Corollary 4.17.**

$$\#\mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_7) = \frac{6!X^{\frac{1}{4}}}{56}F(R_2, \dots, R_7) + O\left(X^{\frac{3}{14}}\right).$$

Now, we need to be able to count strongly carefree 7-tuples in  $\mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_7)$  with the right congruence conditions modulo 4 that will produce

$$D_1 \equiv \dots \equiv D_7 \equiv 1 \pmod{4}.$$

To account for strongly carefree tuples, we also impose congruence conditions for every prime number. Given a prime  $p$ , we want to assure that  $p^2$  does not divide any of the  $g_j$ s (since they need to be squarefree), and we need to make sure that no pair  $(g_i, g_j)$  is congruent to  $(0, 0)$  modulo  $p$  (since they need to be pairwise relatively prime). This is the topic of the next section.

## 4.4 Sieving

In this section, we will state and prove all results for general  $n$ . We then state the main result of this section when  $n = 3$  as a corollary.

Now that the volume has been computed and the number of  $\mathbf{Z}^\ell$  lattice points in  $\mathcal{R}_n$  has been calculated, this section aims to determine which of these points correspond to multiquadratic extensions. This is accomplished by incorporating a sieve to count only the lattice points of interest. The number  $\#\mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_7)$  does not take into account the various congruence conditions that we need to impose in order to count the number fields in question. Specifically, we will require the  $\ell$ -tuples  $(g_1, \dots, g_\ell)$  to have entries that are strongly carefree and satisfy certain congruence conditions which in turn yield that the  $D_j \equiv 1 \pmod{4}$  for  $1 \leq j \leq \ell$ . This is where the notion of sieving comes into play.

### 4.4.1 Counting Strongly Carefree Tuples

Let's first begin by tackling the issue of counting strongly carefree tuples. We would like to count how many of these occur in  $\mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_7)$ . However, this count depends on infinitely many congruence conditions, since we must consider conditions imposed by every prime number.

We begin by considering a finite amount of primes. The sieve will allow us to expand our results concerning finitely many congruence conditions to infinitely many of them.

One of the requirements of being strongly carefree is that the entries are squarefree, and this is a statement about divisibility by  $p^2$ , where  $p$  is a prime number. This motivates the following setup:

**Definition 4.18.** Fix a positive real number  $Y$ , and define the integer  $m = m(Y)$  by

$$m = \prod_{p < Y} p^2,$$

where the product runs over all primes less than  $Y$ .

**Definition 4.19.** Let  $m, n_1, \dots, n_k \in \mathbf{Z}$ . We say that the  $k$ -tuple  $(n_1, \dots, n_k) \in \mathbf{Z}^k$  is *strongly carefree with respect to  $m$*  if for every prime  $p$  dividing  $m$ ,  $p^2$  doesn't divide  $n_i$  for  $1 \leq i \leq k$ , and no pair  $(n_i, n_j)$  are both divisible by  $p$ .

We want to obtain a way of calculating the proportion of strongly carefree points that lie in  $\mathbf{Z}^\ell$ . Our setup begins by considering only those  $\ell$ -tuples that are strongly carefree with respect to the integer  $m$ .

**Definition 4.20.** Let  $\mathcal{L}(Y)$  denote the subset of  $\mathbf{Z}^\ell$  consisting of strongly carefree points with respect to  $m$ :

$$\mathcal{L}(Y) = \{(g_1, \dots, g_\ell) \in \mathbf{Z}^\ell : (g_1, \dots, g_\ell) \text{ strongly carefree w.r.t. } m\},$$

Furthermore, let  $\mathcal{C}_m$  denote the image  $(\text{mod } m)$  of the points in  $\mathcal{L}(Y)$ . That is,

$$\mathcal{C}_m = \{(g_1, \dots, g_\ell) \in (\mathbf{Z}/m\mathbf{Z})^\ell : (g_1^*, \dots, g_\ell^*) \in \mathcal{L}(Y)\},$$

where  $g_j^*$  denotes any lift of  $g_j$ .

Fix a prime  $p < Y$ . The elements in  $\mathcal{C}_m$  are those in  $(\mathbf{Z}/m\mathbf{Z})^\ell$  that avoid the following two scenarios:

- (i)  $g_i \equiv 0 \pmod{p^2}$  (not square-free),
- (ii)  $g_i \equiv g_j \pmod{p}$  if  $i \neq j$  (not pairwise relatively prime).

Let  $\mathcal{C}_p$  denote the image  $(\text{mod } p^2)$  of the the set of  $\ell$ -tuples in  $\mathbf{Z}^\ell$  with these conditions. Specifically,

$$\mathcal{C}_p := \{(g_1, \dots, g_\ell) \in (\mathbf{Z}/p^2\mathbf{Z})^\ell : g_i \neq 0 \forall i, \text{ if } i \neq j, \text{ then } (g_i, g_j) \neq (0, 0)\}.$$

**Theorem 4.21.** With  $\mathcal{C}_p$  defined above, we have

$$\#\mathcal{C}_p = p^{\ell-1}(p-1)^\ell(p+\ell).$$

*Proof.* Let's begin with the first condition. Counting how many of these there are is simply a matter of choosing  $\ell$ -tuples in  $(\mathbf{Z}/p^2\mathbf{Z})^\ell$  that don't contain any zero-entries. This total is

$$(p^2 - 1)^\ell.$$

Now, we may assume that  $g_i \not\equiv 0 \pmod{p^2}$  for  $1 \leq i \leq \ell$ . Now let's attack the second condition. First consider pairs  $(g_i, g_j)$  with  $i \neq j$ . There are  $\binom{\ell}{2}$  such pairs. For each coordinate, there are  $p$  values that are  $0 \pmod{p}$ . However, one of these values is also  $0 \pmod{p^2}$ , namely, 0. Since this is already accounted for from the previous argument, we actually have  $p-1$  values. Since there are two coordinates, we get  $(p-1)^2$  options. Considering these pairs  $(g_i, g_j)$  as a sub-tuple of  $(g_1, \dots, g_\ell)$ , we have  $p^2 - p$  non-zero values for each of the other  $\ell - 2$  coordinates (since we are avoiding all values that are  $0 \pmod{p}$ ). This gives a total of

$$\binom{\ell}{2} (p-1)^2 (p^2 - p)^{\ell-2}$$

tuples with exactly two values that are  $0 \pmod{p}$ . Similarly, we count tuples with exactly three values that are  $0 \pmod{p}$ . We get

$$\binom{\ell}{3} (p-1)^3 (p^2 - p)^{\ell-3}.$$

Continuing in this manner, and adding up all such tuples, we get

$$\begin{aligned} & \sum_{j=2}^{\ell} \binom{\ell}{j} (p-1)^j (p^2 - p)^{\ell-j} \\ &= \sum_{j=2}^{\ell} \binom{\ell}{j} p^{\ell-j} (p-1)^\ell. \end{aligned}$$

Hence, the total number of strongly carefree  $\ell$ -tuples is given by

$$\begin{aligned} \#\mathcal{C}_p &= (p^2 - 1)^\ell - \sum_{j=2}^{\ell} \binom{\ell}{j} p^{\ell-j} (p-1)^\ell \\ &= (p-1)^\ell \left[ (p+1)^\ell - \sum_{j=2}^{\ell} \binom{\ell}{j} p^{\ell-j} \right] \\ &= (p-1)^\ell \left[ (p+1)^\ell - \left( \sum_{j=0}^{\ell} \binom{\ell}{j} p^{\ell-j} - p^\ell - \ell p^{\ell-1} \right) \right] \\ &= (p-1)^\ell \left[ (p+1)^\ell - (p+1)^\ell + p^\ell + \ell p^{\ell-1} \right] \\ &= p^{\ell-1} (p-1)^\ell (p + \ell). \end{aligned}$$

□

#### 4.4.2 The $p$ -adic Density

Now that we have counted the size of each  $\mathcal{C}_p$ , the next definition gives a way of obtaining the proportion of strongly carefree points with respect to  $m$ . As we will see, this proportion will carry over when we need to consider all primes.

**Definition 4.22.** Let  $p$  be a prime less than or equal to  $m$ . Define the  $p$ -adic density of  $\mathcal{L}(Y)$  to be

$$\mu_p(\mathcal{L}(Y)) := \frac{\#\mathcal{C}_p}{p^{2\ell}}.$$

It follows from Theorem 4.21 that

$$\mu_p(\mathcal{L}(Y)) = p^{-(\ell+1)}(p-1)^\ell(p+\ell).$$

The next lemma gives a count of how many points in  $\mathcal{L}(Y)$  lie in the region  $\mathcal{R}_n$ .

**Lemma 4.23.** Let  $\mathcal{R}_n = \mathcal{R}_n(X, R_2, \dots, R_\ell)$  denote the region in  $\mathbf{R}^\ell$  defined analogously to (4.1). With  $\mathcal{R}_{\mathbf{Z}} = \mathcal{R}_{\mathbf{Z}}(X, R_2, \dots, R_\ell)$  denoting the collection of integer points in  $\mathcal{R}_n$  and  $\mathcal{L}(Y)$  defined above, let

$$\mathcal{R}_{\mathcal{L}(Y)} := \mathcal{R}_{\mathbf{Z}} \cap \mathcal{L}(Y).$$

Then,

$$\#\mathcal{R}_{\mathcal{L}(Y)} = \left( \prod_{p < Y} \left( p^{-(\ell+1)}(p-1)^\ell(p+\ell) \right) \right) \text{Vol}(\mathcal{R}_n) + O\left(N^{\frac{\ell-1}{\ell}}\right),$$

where  $N = X^{\frac{1}{2n-1}}$ .

*Proof.* We have

$$\begin{aligned} \#\mathcal{C}_m &= \prod_{p < Y} \#\mathcal{C}_p \\ &= \prod_{p < Y} \mu_p(\mathcal{L}(Y)) p^{2\ell} \\ &= m^\ell \prod_{p < Y} \mu_p(\mathcal{L}(Y)) \quad \left( \text{since } m = \prod_{p < Y} p^2 \right). \end{aligned}$$

Now, we may write  $\mathcal{L}(Y)$  as

$$\mathcal{L}(Y) = \bigcup_{x \in \mathcal{C}_m} (x + m\mathbf{Z}^\ell).$$

Note that for  $x \in \mathcal{C}_m$ ,

$$\begin{aligned}
\#\mathcal{R}_{x+m\mathbf{Z}^\ell} &= \#[(x + m\mathbf{Z}^\ell) \cap \mathcal{R}_n] \\
&= \frac{1}{m^\ell} \# \left[ \left( \frac{x}{m^\ell} + \mathbf{Z}^\ell \right) \cap \mathcal{R}_n \right] \\
&= \frac{1}{m^\ell} \#\mathcal{R}_{\mathbf{Z}}.
\end{aligned}$$

It then follows from Corollary 4.17 that

$$\#\mathcal{R}_{x+m\mathbf{Z}^\ell} = \frac{1}{m^\ell} \text{Vol}(\mathcal{R}_n) + O\left(N^{\frac{\ell-1}{\ell}}\right).$$

Hence,

$$\begin{aligned}
\#\mathcal{R}_{\mathcal{L}(Y)} &= \sum_{x \in \mathcal{C}_m} \left( \frac{1}{m^\ell} \text{Vol}(\mathcal{R}_n) + O\left(N^{\frac{\ell-1}{\ell}}\right) \right) \\
&= \frac{1}{m^\ell} \#\mathcal{C}_m \text{Vol}(\mathcal{R}_n) + O\left(N^{\frac{\ell-1}{\ell}}\right) \\
&= \mu_p(\mathcal{L}(Y)) \text{Vol}(\mathcal{R}_n) + O\left(N^{\frac{\ell-1}{\ell}}\right) \\
&= \prod_{p < Y} \left( p^{-(\ell+1)} (p-1)^\ell (p+\ell) \right) \text{Vol}(\mathcal{R}_n) + O\left(N^{\frac{\ell-1}{\ell}}\right). \quad \square
\end{aligned}$$

The final step in counting strongly carefree points is to extend the above lemma for all primes.

**Definition 4.24.** Let  $\mathcal{L}_\infty$  denote the collection of all strongly carefree points in  $\mathbf{Z}^\ell$ .

The main purpose of this section is to compute the integer  $\#\mathcal{R}_{\mathcal{L}_\infty}$ . This is achieved by using a sieve that allows for taking all prime numbers into consideration. Our methods follow as an immediate generalization of [Bha05, Section 3].

**Theorem 4.25.**

$$\#\mathcal{R}_{\mathcal{L}_\infty} = \prod_p \left( p^{-(\ell+1)} (p-1)^\ell (p+\ell) \right) \text{Vol}(\mathcal{R}_n) + o(N).$$

*Proof.*

$$\begin{aligned}
\limsup_{N \rightarrow \infty} \frac{\#\mathcal{R}_{\mathcal{L}_\infty}}{N} &\leq \lim_{Y \rightarrow \infty} \lim_{N \rightarrow \infty} \frac{\#\mathcal{R}_{\mathcal{L}(Y)}}{N} \\
&= \frac{\text{Vol}(\mathcal{R}_n)}{N} \left( \prod_{p < Y} \left( p^{-(\ell+1)} (p-1)^\ell (p+\ell) \right) \right).
\end{aligned}$$

On the other hand, let

$$\mathcal{W}_p := \{(g_1, \dots, g_\ell) \in \mathbf{Z}^\ell : (g_1, \dots, g_\ell) \pmod{p} \notin \mathcal{C}_p\}.$$

Then we have that

$$\mathcal{R}_{\mathcal{L}(Y)} \subseteq \mathcal{R}_{\mathcal{L}_\infty} \cup \bigcup_{p \geq Y} \mathcal{R}_{\mathcal{W}_p}.$$

Hence, we also get that

$$\liminf_{N \rightarrow \infty} \frac{\#\mathcal{R}_{\mathcal{L}_\infty}}{N} \geq \frac{\#\mathcal{R}_{\mathcal{L}(Y)}}{N} - \mathcal{O}\left(\frac{\sum_{p \geq Y} \#\mathcal{R}_{\mathcal{W}_p}}{N}\right).$$

Now, since

$$\mu_p(\mathcal{L}(Y)) = p^{-(\ell+1)}(p-1)^\ell(p+\ell) = 1 - \ell^2 p^{-2} + (1 + \ell p^{-1}) \sum_{j=2}^{\ell} \binom{\ell}{j} (-1)^j p^{-j} = 1 - \mathcal{O}(p^{-2}),$$

it follows that  $\#\mathcal{W}_p = \mathcal{O}(N/p^2)$ . Therefore,

$$\lim_{Y \rightarrow \infty} \mathcal{O}\left(\frac{\sum_{p \geq Y} \#\mathcal{R}_{\mathcal{W}_p}}{N}\right) = 0,$$

since

$$\sum_{p \geq Y} \frac{1}{p^2}$$

is the tail of a convergent series. Thus, taking the limit as  $Y \rightarrow \infty$  yields

$$\#\mathcal{R}_{\mathcal{L}_\infty} = \prod_p \left( p^{-(\ell+1)}(p-1)^\ell(p+\ell) \right) \text{Vol}(\mathcal{R}_n) + o(N),$$

as desired. □

**Corollary 4.26.** When  $n = 3$ , we have

$$\#\mathcal{R}_{\mathcal{L}_\infty} = \prod_p \left( p^{-8}(p-1)^7(p+7) \right) \frac{6! X^{\frac{1}{4}}}{56} F(R_2, \dots, R_7) + o\left(X^{\frac{1}{4}}\right).$$

#### 4.4.3 The Case $(D_1, \dots, D_7) \equiv (1, \dots, 1) \pmod{4}$

Let  $K_3 = \mathbf{Q}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_4})$  with corresponding 7-tuple  $(D_1, \dots, D_7)$ . We gave a parametrization of  $K_3$  in terms of its strongly carefree tuple  $(g_1, \dots, g_7)$ . This allows us to write each  $D_i$  in terms of the  $g_j$ 's as in Definition 4.6.

We are studying triquadratic extensions whose generators  $D_1, D_2$ , and  $D_4$  are congruent to 1 modulo 4. So we have that each  $g_j$  can be congruent to either 1 or 3 modulo 4.

If we study the 7-tuple  $(g_1, \dots, g_7) \pmod{4}$ , there are a total of  $4^7$  tuples to consider. However, the entries we are interested in cannot equal 0 or 2, leaving us with  $2^7 = 128$  possibilities.

After inspecting each of these possible choices, we get  $2^4 = 16$  distinct 7-tuples  $(g_1, \dots, g_7) \pmod{4}$  that yield  $(D_1, \dots, D_7) \equiv (1, \dots, 1) \pmod{4}$ , namely

$(g_1, g_2, g_3, g_4, g_5, g_6, g_7)$
(1, 1, 1, 1, 1, 1, 1)
(1, 3, 3, 1, 3, 1, 1)
(3, 3, 3, 3, 1, 1, 1)
(3, 1, 1, 3, 3, 1, 1)
(3, 1, 3, 1, 1, 3, 1)
(3, 3, 1, 1, 3, 3, 1)
(1, 3, 1, 3, 1, 3, 1)
(1, 1, 3, 3, 3, 3, 1)
(3, 3, 1, 1, 1, 1, 3)
(3, 1, 3, 1, 3, 1, 3)
(1, 1, 3, 3, 1, 1, 3)
(1, 3, 1, 3, 3, 1, 3)
(1, 3, 3, 1, 1, 3, 3)
(1, 1, 1, 1, 3, 3, 3)
(3, 1, 1, 3, 1, 3, 3)
(3, 3, 3, 3, 3, 3, 3)

Recall that  $\mathcal{C}_2$  consists of points that are strongly carefree with respect to 2, meaning that neither entry is zero modulo 4 and at most one entry is zero modulo 2. The above conditions thus imply that  $(g_1, \dots, g_7) \in \mathcal{L}_\infty$ , which allows us to replace  $\mu_2(\mathcal{L}_\infty)$  with the proportion of 7-tuples that give the correct congruence relations on  $(D_1, \dots, D_7) \pmod{4}$ . This will be

$$\frac{2^4}{4^7} = \frac{2^4}{2^{14}} = \frac{1}{2^{10}}.$$

With this proportion, we obtain our main counting result:

**Theorem 4.27.** The number of triquadratic extensions  $K_3 \in \mathcal{M}_3^+(i)$  with discriminant bounded by  $X$  and shape in  $W(R_2, \dots, R_7)$  is given by

$$\mathcal{N}_3(X, R_2, \dots, R_7) = \#\mathcal{R}_{\mathcal{L}_\infty} = \frac{1}{2^{10}} \prod_{p>2} (p^{-8}(p-1)^7(p+7)) \frac{30X^{\frac{1}{4}}}{56} F(R_2, \dots, R_7) + o\left(X^{\frac{1}{4}}\right).$$

*Proof.* It remains to be shown that the strongly carefree tuples occurring in the region  $\mathcal{R}_3(X, R_2, \dots, R_7)$  whose entries are not all distinct become negligible. Recall that

$$\mathcal{N}_3(X, R_2, \dots, R_7) := \#\{K_3 \in \mathcal{M}_3^+(i) : \Delta(K_3) < X; \text{sh}(K_3) \in W(R_2, \dots, R_7)\}.$$

We claim that

$$\mathcal{N}_3(X, R_2, \dots, R_7) = \#\{K_3 \in \mathcal{M}_{3,i}^+ : \Delta(K_3) < X; \text{sh}(K_3) \in W(R_2, \dots, R_7)\} + o(X^{\frac{1}{4}}),$$

where  $\mathcal{M}_{3,i}^+$  corresponds to number fields of type (i) as in Lemma 4.10.

If we look at strongly carefree tuples  $(g_1, \dots, g_7) \in \mathcal{R}_3(X, R_2, \dots, R_7)$  that are not of type (i) (i.e. between two and four entries are equal to 1), the corresponding subregion these points occupy is lower dimensional. As such, the volume of this subregion is zero. Furthermore, in the proof of Theorem 4.16, we show that any of the region's lower dimensional shadows has volume  $O(X^{\frac{3}{14}})$ , so the number of integer points of that type is  $0 + O(X^{\frac{3}{14}})$ . This proves the claim.

From Corollary 4.14, it follows that the number of triquadratic extensions  $K_3 \in \mathcal{M}_{3,i}^+(X, (i))$  occur with frequency  $\frac{1}{24}$  among the number of strongly carefree tuples of type (i), which yields the factor of  $\frac{6!}{24} = 30$ . □

## 4.5 Equidistribution

In this section, we prove Equation (2.3) for our family of number fields when restricting to sets of the form  $W(R_2, \dots, R_7)$ . As seen in Section 2.7, this is sufficient to show equidistribution. We now have all the tools required to show that the collection of shapes of totally real triquadratic extensions  $K_3 = \mathbf{Q}(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_4})$ , such that

$$D_1 \equiv D_2 \equiv D_4 \equiv 1 \pmod{4}$$

are equidistributed. We have the following main result:

**Theorem 4.28.** Let  $1 < R_2 < \dots < R_7$  be real numbers. Recall that

$$W(R_2, \dots, R_7) = \{\text{sh}(X_2, \dots, X_7) \in \mathcal{S}_{K_3} : X_2 \leq \dots \leq X_7 \leq R_7, R_j \leq X_j \text{ for } 2 \leq j \leq 7\}.$$

Furthermore, let

$$\mathcal{N}_3(X, R_2, \dots, R_7) = \#\{K_3 \in \mathcal{M}_3^+(i) : \Delta(K_3) < X; \text{sh}(K_3) \in W(R_2, \dots, R_7)\}$$

denote the number of totally real triquadratic extensions of discriminant bounded by  $X$ , with shape in  $W(R_2, \dots, R_7)$ , and in which 2 does not ramify. Then there exists a constant  $C > 0$  such that

$$\mathcal{N}_3(X, R_2, \dots, R_7) \rightarrow C \cdot \mu(W(R_2, \dots, R_7))X^{\frac{1}{4}} + o(X^{\frac{1}{4}})$$

as  $X \rightarrow \infty$ .

*Proof.* From Theorem 4.27, we have that

$$\mathcal{N}_3(X, R_2, \dots, R_7) = \frac{1}{2^{10}} \prod_{p>2} (p^{-8}(p-1)^7(p+7)) \frac{30X^{\frac{1}{4}}}{56} F(R_2, \dots, R_7) + o\left(X^{\frac{1}{4}}\right).$$

We may rewrite this as

$$\mathcal{N}_3(X, R_2, \dots, R_7) = C' F(R_2, \dots, R_7) X^{\frac{1}{4}} + o\left(X^{\frac{1}{4}}\right),$$

where

$$C' = \frac{1}{2^{10}} \prod_{p>2} (p^{-8}(p-1)^7(p+7)) \frac{30}{56}$$

is constant.

On the other hand, by Corollary 2.43, we proved that the measure of  $W(R_2, \dots, R_7)$  is given by

$$\mu(W(R_2, \dots, R_7)) = C'' F(R_2, \dots, R_7),$$

where

$$C'' = \frac{1}{6!}.$$

Thus, we get that

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{1}{X^{\frac{1}{4}}} \mathcal{N}_3(X, R_2, \dots, R_7) &= \lim_{X \rightarrow \infty} \frac{1}{X^{\frac{1}{4}}} \left[ C' F(R_2, \dots, R_7) X^{\frac{1}{4}} + o\left(X^{\frac{1}{4}}\right) \right] \\ &= C' F(R_2, \dots, R_7) \\ &= C \mu(W(R_2, \dots, R_7)), \end{aligned}$$

where

$$C = \frac{C'}{C''}.$$

□

This shows that the shapes of totally real triquadratic extensions (with proper congruence type) are equidistributed in a regularized sense in the subset of the space of shapes in which they live.

## BIBLIOGRAPHY

- [BH16] Manjul Bhargava and Piper Harron, *The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields*, Compos. Math. **152** (2016), no. 6, 1111–1120. MR 3518306
- [Bha05] Manjul Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063. MR 2183288
- [BS14] Manjul Bhargava and Ariel Shnidman, *On the number of cubic orders of bounded discriminant having automorphism group  $C_3$ , and related problems*, Algebra Number Theory **8** (2014), no. 1, 53–88. MR 3207579
- [Cha73] D. Chatelain, *Bases des entiers des corps composés par des extensions quadratiques de  $\mathbf{Q}$* , Ann. Sci. Univ. Besançon Math. (3) (1973), no. 6, 38. MR 0349625
- [CS93] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1993, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. MR 1194619
- [Har17] Robert Harron, *The shapes of pure cubic fields*, Proc. Amer. Math. Soc. **145** (2017), no. 2, 509–524. MR 3577857
- [Har19] Robert Harron, *Equidistribution of shapes of complex cubic fields of fixed quadratic resolvent*, 2019, preprint, available at <https://arxiv.org/abs/1907.07209>.
- [HH19] Piper H and Robert Harron, *The shapes of Galois quartic fields*, 2019, in preparation.
- [Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schapacher, With a foreword by G. Harder. MR 1697859
- [Ter97] David Charles Terr, *The distribution of shapes of cubic orders*, ProQuest LLC, Ann Arbor, MI, 1997, Thesis (Ph.D.)—University of California, Berkeley. MR 2697241