

**From the holdings of the Department of Special Collections , Princeton University Library,
Princeton, NJ**

These documents are either in the public domain, or can only be used for educational and research purposes (Fair use) as per U.S. Copyright law (text below). By accessing this file, all users agree that their use falls in the public domain or within fair use as defined by the copyright law. We do not charge any permission or usage fees for the publication of images of material in our collections, including those provided by Princeton University Library, via our website, catalog, or directly from staff. For more information regarding copyright, credit, and citation please review the information on the Copyright, Credit and Citation Guidelines page of our website.

<https://library.princeton.edu/special-collections/policies/copyright-credit-and-citation-guidelines>. If you have any questions, including how to order higher-quality images from the collection, contact Special Collections Public Services via our Ask Us! Form. <https://library.princeton.edu/special-collections/ask-us>

Doctoral Dissertations, 2011-2026

Mathematics

2023

Successive minima of orders in number fields

Vemulapalli, Sameera

Princeton, NJ : Princeton University

<http://arks.princeton.edu/ark:/88435/dsp01000003328>

U.S. Copyright law: The copyright law of the United States (Title 17, §108, United States Code) governs the making of photocopies or other reproductions of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be used for any purpose other than private study, scholarship, or research. If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of fair use that user may be liable for copyright infringement. This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve a violation of copyright law. <https://www.copyright.gov/title17/title17.pdf>

SUCCESSIVE MINIMA OF ORDERS IN NUMBER FIELDS

SAMEERA VEMULAPALLI

A DISSERTATION

PRESENTED TO THE FACULTY

OF PRINCETON UNIVERSITY

IN CANDIDACY FOR THE DEGREE

OF DOCTOR OF PHILOSOPHY

RECOMMENDED FOR ACCEPTANCE

BY THE DEPARTMENT OF

MATHEMATICS

ADVISER: MANJUL BHARGAVA

MAY 2023

© Copyright by Sameera Vemulapalli, 2023.

All Rights Reserved

Abstract

Orders in number fields provide interesting examples of lattices. We ask: what lattices arise from orders in number fields and how are they distributed? In the first chapter of this thesis, we prove that all nontrivial multiplicative constraints on successive minima of orders come from multiplication. Moreover, for infinitely many positive integers n (including all $n < 18$), we explicitly determine all multiplicative constraints on successive minima of orders in degree n number fields. We also prove analogous results for scrollar invariants of curves. Now suppose $3 \leq n \leq 5$ and let $G \subseteq S_n$. An order $\mathcal{O}$ of absolute discriminant Δ in a degree n number field has n successive minima $1 = \lambda_0 \leq \lambda_1 \leq \dots \leq \lambda_{n-1}$. In the next three chapters, we compute for many G the distribution of the points $(\log_{\Delta} \lambda_1, \dots, \log_{\Delta} \lambda_{n-1}) \in \mathbb{R}^{n-1}$ as $\mathcal{O}$ ranges across orders in degree n fields with Galois group G as $\Delta \rightarrow \infty$.

Acknowledgements

I would like to express my utmost gratitude to my advisor, Manjul Bhargava. I always have so much fun talking to you and I am always inspired by your clarity of thought, sense of mathematical aesthetics, empathy, and boundless energy. Thank you for your support and encouragement throughout the years.

I am also deeply indebted to Ravi Vakil; the last three chapters of this thesis would not have been written without your support. From you, I have learned to think more geometrically, and this has profoundly shaped my mathematical perspective. I am thankful for your generosity with your time and your support. This thesis also would not have been possible without Hendrik Lenstra, who posed the question that motivated this thesis. I visited Hendrik in Leiden twice during graduate school, and both visits had a profound effect on how I think about mathematics; I am extremely grateful to Hendrik for his generosity with his time and ideas during these visits and for being a wonderful host in Leiden. This thesis was, in many ways, shaped by his perspective.

It is very energizing to be immersed in a community of amazing mathematicians; in particular, I have benefited hugely from discussions with, but not limited to, Jordan Ellenberg, Dan Fess, Noah Kravitz, Seok Hyeong Lee, Robert Lemke Oliver, Peter Sarnak, Arul Shankar, Ari Shnidman, Jacob Tsimerman, Ila Varma, Akshay Venkatesh, Floris Vermeulen, Melanie Wood, and Gilles Zémor. I am particularly thankful to Alina Bucur, Jordan Ellenberg, Ila Varma, and David Zureick-Brown for organizing an amazing conference in Schloss-Elmau that inspired the last three chapters of this thesis. I have had a fantastic time collaborating with Avi Kulkarni, and I must thank him for teaching me so much algebraic geometry. I must also thank my wonderful undergraduate mentors Bernd Sturmfels, Sug Woo Shin, and David Zureick-Brown for introducing me to mathematics, and Bernd in particular for three wonderful and productive summers in MPI Leipzig during graduate school. I would also like to thank the faculty at Princeton, especially Peter Sarnak for useful discussions and for being a reader of this thesis, and my committee members Akshay Venkatesh and Christopher Skinner. I've been lucky to have a large and vibrant arithmetic statistics community at Princeton – thank you all for answering so many questions and for so many semesters of fun seminars. I must also thank Jill LeClair, without whom I certainly wouldn't have filled any forms on time!

I am so, so grateful to my friends; you have made my time in Princeton much brighter. I am particularly grateful to Allie Green, who has been an integral part of my time in Princeton. I must also thank the friends I have been lucky enough to climb with throughout the years; I will miss

climbing on diabase. Thank you to the many wonderful people in the math department, and my MaxOut friends who made the early pandemic bearable. I would like to give a special thank you to Manali Begur, Hana Hyder, Neelima Mandava, and Megan Yelsangikar, without whose endless support, love, and encouragement I could have never completed this thesis.

I feel exceptionally lucky to have such a large and warm extended family who has always supported me. I am especially grateful to the Kommanas, who made their home feel like my own while I was in Princeton. I also would like to thank Sreepathy Uncle for always showing enthusiastic interest in my work and for always having so much confidence in me; it is difficult to finish a Ph.D. without this kind of support, and I am very grateful to have it. I also want to thank the rest of my extended family, including but not at all limited to, the Allankis, Mandavas, the Patimallas, the Potluris, the Talasilas, the Sreepathys, the rest of the Vemulapallis, and the Yarlaggaddas.

I would like to thank Dan for being an incredible partner, and in particular, for editing this entire thesis. I am beyond lucky to have you. I must also thank my parents, my grandma, and brother. To my grandma: I am eternally inspired by your strong will, independent thought, and persistence. You have been one of the biggest influences in my life. To my parents and my brother: I am beyond grateful for your love and support. Thank you for encouraging me throughout my life to pursue my various interests and endeavors. None of this would be possible without you.

To my parents.

Contents

Abstract	iii
Acknowledgements	iv
1 Introduction	1
1.1 Bounds on Successive Minima of Orders in Number Fields and Scrollar Invariants of Curves	3
1.2 Counting cubic rings by successive minima	8
1.2.1 Results on binary n -ic forms	11
1.3 Counting quartic rings by successive minima	12
1.4 Counting quintic rings by successive minima	15
1.5 The relationship between scrollar invariants and successive minima	17
1.6 Setup	23
2 Bounds on Successive Minima of Orders in Number Fields and Scrollar Invariants of Curves	25
2.1 Successive minima spectra are finite unions of polytopes	25
2.2 Computing the successive minima spectrum for S_n	28
2.3 Bounds on scrollar invariants of curves	30
2.4 Some theorems with exact constants	32
2.5 Taking logarithms of successive minima is not lossy	34
2.6 The polytopes associated to a flag type T	36
2.7 The successive minima spectrum when n is a prime power, a product of two primes, or 12	40
2.8 The successive minima spectrum when n is not a prime power, a product of two primes, or 12	47

3	Counting cubic rings by successive minima	67
3.1	Statement of results	67
3.2	The parametrization of cubic rings	71
3.3	Reduction theory of cubic rings	72
3.4	Computing density functions of cubic rings	76
3.5	Reduction theory of binary n -ic forms	82
3.6	Special families of cubic rings	90
3.7	Sieving for maximal orders in S_3 -cubic fields	93
4	Counting quartic rings by successive minima	97
4.1	Statement of results	97
4.1.1	Computing $\text{Poly}_4(G)$	98
4.1.2	Density functions of quartic rings	98
4.1.3	Special families of quartic rings	100
4.2	The parametrization of quartic rings	104
4.3	Reduction theory of quartic rings	105
4.4	Computing $\text{Poly}_4(G)$	109
4.5	Computing density functions of quartic rings	114
4.6	The generic points of D_4 and S_4	118
4.7	Special families of quartic rings	124
4.7.1	Quartic rings with a basis of the form $1, x, y, xy$	124
4.7.2	Quartic rings with a basis of the form $1, x, y, x^2$	129
4.7.3	Binary quartic forms	134
4.7.4	Monic quartic forms	135
4.8	Pictures of Poly_4 , $\text{Poly}_4(S_4)$, and $\text{Poly}_4(D_4)$	136
5	Counting quintic rings by successive minima	144
5.1	Statement of results	144
5.1.1	Computing $\text{Poly}_5(G)$	144
5.1.2	Density functions of quintic rings	146
5.1.3	Special families of quintic rings	147
5.2	The parametrization of quintic rings	149
5.3	Reduction theory of quintic rings	150
5.4	Computing $\text{Poly}_5(G)$	156

5.5	Computing density functions of quintic rings	161
5.6	Special families of quintic rings	162
5.6.1	Binary quintic forms	162
5.6.2	Monic quintic forms	163
5.6.3	The generic point of S_5	164
6	Appendix	166

Chapter 1

Introduction

Orders in number fields of degree n provide interesting examples of lattices via their natural embeddings into $\mathbb{R}^n$ using their real and complex places. The shapes of these lattices are constrained, due to multiplication: the length of the product of two vectors is roughly bounded above by the product of the lengths. In this thesis, we ask which lattices arise from orders in number fields and how these lattices are distributed.

We study lattices via their successive minima; see Section 1.6 for a definition. Our first major result, which we prove in Chapter 2, shows that all nontrivial multiplicative constraints on successive minima of orders in number fields come from the multiplicative structure of the order. More precisely, let $G \subseteq S_n$ be a permutation group. Each order $\mathcal{O}$ in a degree n number field gives rise to a point

$$p_{\mathcal{O}} := (\log_{\Delta} \lambda_1, \dots, \log_{\Delta} \lambda_{n-1}) \in \mathbb{R}^{n-1},$$

where here Δ is the absolute discriminant of $\mathcal{O}$ and $1 = \lambda_0 \leq \lambda_1 \leq \dots \leq \lambda_{n-1}$ are the successive minima of $\mathcal{O}$. We prove that the set of limit points, in the Euclidean topology, of the multiset $\{p_{\mathcal{O}}\}$ as $\mathcal{O}$ ranges across orders in degree n number fields with Galois group G , is a finite union of polytopes. Moreover, we show that all nontrivial facets of these polytopes “come from” multiplication. Inspired by a conjecture of Lenstra, our second major result computes this finite union of polytopes for many G . We also prove analogous results for scrollar invariants of curves, which are the function field analogue of successive minima of orders.

In the case of successive minima, our results are inspired by and generalize work of Chiche-lapierre, who computed these polytopes for $n = 3, 4$ [14]; work of Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and Zhao, and independently Piker and Rosen, who proved that $\lambda_{n-1} \ll \lambda_i \lambda_j$

for all $i + j = n - 1$ [6, 29]; and unpublished work of Bhargava and Lenstra, who proved that $\lambda_{i+j} \ll \lambda_i \lambda_j$ for all $1 \leq i \leq j \leq i + j < n$ for orders in primitive number fields. In the case of scrollar invariants, our work generalizes classical bounds on the Maroni invariant of trigonal covers [25]; results of Ohbuchi bounding the sum of scrollar invariants [27]; and results of Deopurkar and Patel bounding the smallest scrollar invariant [19].

In the next three chapters we ask: how many orders are there of bounded discriminant, fixed Galois group, and almost prescribed successive minima? More precisely, fix a point $p \in \mathbb{R}^{n-1}$, fix a permutation group $G \subseteq S_n$, and let $\mathcal{O}$ denote an order in a degree n number field. What are the asymptotics of

$$\#\{\mathcal{O} \mid \Delta \leq X \text{ and } \text{Gal}(\mathcal{O} \otimes \mathbb{Q}) \simeq G \text{ and } p_{\mathcal{O}} \text{ is “close” to } p\} \quad (1.1)$$

as $X \rightarrow \infty$? We will later quantify what “close” means. In the number field setting, this question was first raised by Chiche-lapierre [14], who gave partial results when $n = 3, 4, 5$ and $G = S_n$; in the function field setting when $n = 3$ and $G = S_3$, this question was addressed by Zhao [34]; and in the geometric setting, this question has been addressed for $n = 3, 4, 5$ and $G = S_n$ by Patel [28], who computed the dimensions of Maroni loci in an appropriate Hurwitz space. Patel’s results, appropriately interpreted, are analogous to ours; see Section 1.5 for a treatment of the relationship between Maroni loci of Hurwitz spaces and successive minima of orders in number fields.

Related distributional questions have been also addressed by Terr [32], who proved the equidistribution of shapes of cubic fields; by Bhargava and H [5], who proved the equidistribution of shapes of S_n -fields for $n = 4, 5$; and by Holmes [24], who proved the equidistribution of shapes in pure prime degree number fields. Our approach differs from that of Terr, Bhargava, H, and Holmes in the following meaningful sense; for $n = 3, 4, 5$, when ordered by absolute discriminant, 100% of orders in S_n -fields lie “near” the point $\frac{1}{2(n-1)}(1, \dots, 1)$. Thus, equidistribution theorems only “see” that one point, but give very refined information at that point. Conversely, our work is focused on computing asymptotics of phenomena that occur with density 0.

In this thesis, we compute these asymptotics for various Galois groups G when $n = 3, 4, 5$ using Delone and Faddeev’s parametrization of cubic rings and Bhargava’s parametrization of quartic and quintic rings respectively. We show that in many cases, (1.1) is $\asymp X^{d(p)}$, where $d: \mathbb{R}^{n-1} \rightarrow \mathbb{R}_{\geq 0}$ is a piecewise linear function supported on a convex body. These convex bodies can be interpreted as a picture of the “cusp” of the corresponding prehomogeneous vector space¹.

¹This explicit, linear description of the “cusp” can be used to simplify the existing proofs that the number of isomorphism classes of orders of absolute discriminant $\leq X$ in S_n -fields is $\asymp X$ for $n = 3, 4, 5$. We also give a proof using the parametrization of quartic rings that the number of quartic orders in D_4 -fields of discriminant $\leq X$ is $\asymp X$; this is a very different method than that of the original proof of Cohen, Diaz y Diaz, and Olivier [16].

We compute these convex bodies and piecewise linear functions for $n = 3, 4, 5$ for many permutation groups G , including $G = S_n$. Remarkably, although these convex bodies are defined through Euclidean geometry, we prove that the vertices often “correspond” to various interesting *algebraic* families of orders. Some of these algebraic families have been studied extensively, such as the family of monogenic orders in degree n fields and the family of orders arising from binary n -ic forms. Others have received comparatively less attention, such as the family of quartic rings with a basis of the form $1, x, y, xy$; however, such families appear to have a particularly nice structure (in fact, we prove that this particular family even admits a parametrization by the orbits of a group acting on affine space!). The author hopes that the perspective explored in this thesis encourages further study of such families. Furthermore, for general degree n we prove that the space of shapes of rank n rings, appropriately interpreted, forms a polytope in $\mathbb{R}^{n-1}$; it would be interesting to ask whether the vertices “correspond” to reasonable families of rank n rings².

We use the geometry of numbers methods pioneered by Davenport, Heilbronn, and Bhargava; our main point of departure from these methods is in how we “average”. In particular, even deep in the cusp, our counting is no more complicated than counting the number of lattice points in a box. In the cubic case, we show that a nondegenerate cubic ring that is “close” to p , is equipped with a “short” basis, and has bounded discriminant gives rise to an integral point in a certain box in $\text{Sym}^3 \mathbb{R}^2$; conversely, we show that every integral point of the box corresponds to a nondegenerate cubic ring of bounded discriminant “close” to p equipped with a “short” basis. Using Davenport’s lemma, we can easily count the number of lattice points in the box. We complete the proof by estimating the number of “short” bases such a cubic ring has, i.e. how many times a ring appears in the box. The quartic and quintic cases are completely analogous.

1.1 Bounds on Successive Minima of Orders in Number Fields and Scrollar Invariants of Curves

Let $n \geq 2$ be any integer. An order $\mathcal{O}$ in a degree n number field has n successive minima $1 = \lambda_0(\mathcal{O}) \leq \lambda_1(\mathcal{O}) \leq \dots \leq \lambda_{n-1}(\mathcal{O})$; see Section 1.6 for a precise definition. When $\mathcal{O}$ is implicit, we simply write λ_i . In this paper, $\mathcal{S}$ will refer to an infinite set of isomorphism classes of orders in

²One such reasonable family would be the family of monogenic rank n rings, which the author guesses corresponds to the vertex $1/2 \binom{n}{2} (1, \dots, n-1)$.

degree n number fields. We wish to understand which inequalities

$$1 \ll_{\mathcal{S}} \lambda_1^{f_1} \dots \lambda_{n-1}^{f_{n-1}}$$

hold for $f_1, \dots, f_{n-1} \in \mathbb{R}$ and $\mathcal{O} \in \mathcal{S}$. When $\mathcal{S}$ is “nice”, we prove that the inequality above is equivalent to showing that the set of limit points, in the Euclidean topology, of the multiset

$$\{(\log_{\Delta} \lambda_1, \dots, \log_{\Delta} \lambda_{n-1})\}_{\mathcal{O} \in \mathcal{S}} \subseteq \mathbb{R}^{n-1}$$

is contained in the linear half space defined by $0 \leq f_1 x_1 + \dots + f_{n-1} x_{n-1}$ (here $x_1, \dots, x_{n-1}$ are the coordinates of $\mathbb{R}^{n-1}$ and Δ is the absolute discriminant of $\mathcal{O}$). See Theorem 2.5.1 for more details.

In this paper, we will work with the latter perspective.

We call the set of limit points of the multiset above the *successive minima spectrum of $\mathcal{S}$* and denote it by $\text{Spectrum}(\mathcal{S})$. For a permutation group $G \subseteq S_n$, let $\mathcal{S}(G)$ be the family of orders $\mathcal{O}$ in degree n number fields such that $\mathcal{O} \otimes \mathbb{Q}$ has Galois group isomorphic to G as a permutation group. Our first theorem states that $\text{Spectrum}(\mathcal{S}(G))$ is a finite union of polytopes of a very special form; we now define these polytopes.

Let L/K be a degree n field extension and let $[n]$ be the set $\{0, \dots, n-1\}$. A *flag of L/K* is a sequence $\mathcal{F} = (F_0, \dots, F_{n-1})$ of K -vector spaces such that $K = F_0 \subset F_1 \subset \dots \subset F_{n-1} = L$ and $\dim_K F_i = i+1$ for all i . Associate to $\mathcal{F}$ the function

$$\begin{aligned} T_{\mathcal{F}}: [n] \times [n] &\longrightarrow [n] \\ (i, j) &\longmapsto \min\{k \in [n] \mid F_i F_j \subseteq F_k\}. \end{aligned}$$

Definition 1.1.1. The polytope $P_{T_{\mathcal{F}}}$ of $T_{\mathcal{F}}$ is the set of $\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1}$ satisfying the following conditions:

1. $\sum_{i=1}^{n-1} x_i = 1/2$;
2. $0 \leq x_1 \leq \dots \leq x_{n-1}$;
3. and $x_{T(i,j)} \leq x_i + x_j$ for $1 \leq i, j < n$.

Theorem 1.1.2. *We have*

$$\text{Spectrum}(\mathcal{S}(G)) = \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}$$

where $\mathcal{F}$ ranges across all flags of degree n number fields with Galois group G .

Condition (1) in the definition of $P_{T_{\mathcal{F}}}$ comes from Minkowski's second theorem, which states that $\prod_{i=1}^{n-1} \lambda_i \asymp_n \Delta^{1/2}$ (see [31], Lecture 10, §6). Condition (2) derives from the fact that $1 \leq \lambda_1 \leq \dots \leq \lambda_{n-1}$. Condition (3) “comes from multiplication”, in the following way. Every order $\mathcal{O}$ contains a linearly independent set $1 = v_0, \dots, v_{n-1}$ such that $\lambda_i = |v_i|$; this set gives rise to a flag $\mathcal{F}$ of $\mathcal{O} \otimes \mathbb{Q}$ given by $F_i = \text{span}\{v_0, \dots, v_i\}$. Then, for every $1 \leq i, j \leq n-1$, we have that

$$F_i F_j \subseteq \text{span}\{v_0, \dots, v_{T_{\mathcal{F}}(i,j)}\}$$

and

$$F_i F_j \not\subseteq \text{span}\{v_0, \dots, v_{T_{\mathcal{F}}(i,j)-1}\}.$$

Thus,

$$\text{span}(\{v_0, \dots, v_{T_{\mathcal{F}}(i,j)-1}\} \cup \{v_{i'} v_{j'}\}_{0 \leq i' \leq i, 0 \leq j' \leq j}) = \text{span}\{v_0, \dots, v_{T_{\mathcal{F}}(i,j)}\}$$

So

$$\lambda_{T_{\mathcal{F}}(i,j)} = |v_{T_{\mathcal{F}}(i,j)}| \leq \max_{0 \leq i' \leq i, 0 \leq j' \leq j} |v_{i'} v_{j'}| \ll_n |v_i| |v_j| = \lambda_i \lambda_j.$$

So, Theorem 1.1.2 tells us that all nontrivial multiplicative constraints on successive minima come from multiplication. See Section 2.6 for more information on the structure of $P_{T_{\mathcal{F}}}$.

Our next few theorems explicitly describe these multiplicative constraints. Let $\mathcal{S}_n$ be the set of isomorphism classes of orders in degree n number fields. Our second theorem explicitly computes the successive minima spectrum of $\mathcal{S}_n$ for infinitely many n . This explicit description was conjectured by Hendrik Lenstra. To state our theorem, we will need the following definitions.

A *tower type* is a t -tuple of integers $(n_1, \dots, n_t) \in \mathbb{Z}_{>1}^t$ for some $t \geq 1$. We say $\prod_{i=1}^t n_i$ is the *degree* of the tower type and t is the *length* of the tower type. Throughout this article, the variable $\mathfrak{T}$ will refer to a tower type of length t and degree n .

Definition 1.1.3. Choose a tower type $\mathfrak{T} = (n_1, \dots, n_t)$ and $i \in [n]$. Writing i in *mixed radix notation with respect to $\mathfrak{T}$* means writing

$$i = i_1 + i_2 n_1 + i_3 (n_1 n_2) + \dots + i_t (n_1 \dots n_{t-1})$$

where i_s is an integer such that $0 \leq i_s < n_s$ for $1 \leq s \leq t$. Note that the integers i_s are uniquely determined.

Definition 1.1.4. Fix a tower type $\mathfrak{T} = (n_1, \dots, n_t)$ and integers $0 \leq i, j \leq i + j < n$. Write i , j , and $k = i + j$ in mixed radix notation with respect to $\mathfrak{T}$ as

$$i = i_1 + i_2 n_1 + i_3(n_1 n_2) + \dots + i_t(n_1 \dots n_{t-1})$$

$$j = j_1 + j_2 n_1 + j_3(n_1 n_2) + \dots + j_t(n_1 \dots n_{t-1})$$

$$k = k_1 + k_2 n_1 + k_3(n_1 n_2) + \dots + k_t(n_1 \dots n_{t-1}).$$

We say the addition $i + j$ *does not overflow modulo $\mathfrak{T}$* if $i_s + j_s = k_s$ for all $1 \leq s \leq t$. Otherwise, we say the addition $i + j$ *overflows modulo $\mathfrak{T}$* .

Definition 1.1.5. The *Lenstra polytope* $\text{Len}(\mathfrak{T})$ of a tower type $\mathfrak{T}$ is the set of $\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1}$ satisfying the following conditions:

1. $\sum_{i=1}^{n-1} x_i = 1/2$;
2. $0 \leq x_1 \leq x_2 \leq \dots \leq x_{n-1}$;
3. and $x_{i+j} \leq x_i + x_j$ for $i + j$ not overflowing modulo $\mathfrak{T}$.

Recall that $\mathcal{S}_n$ is the set of isomorphism classes of orders in degree n number fields.

Theorem 1.1.6. *We have*

$$\text{Spectrum}(\mathcal{S}_n) = \bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T})$$

where $\mathfrak{T}$ ranges across tower types of degree n if and only if n is a prime power, n is a product of 2 distinct primes, or $n = 12$.

Theorem 1.1.7. *If G is the symmetric group on n letters, then*

$$\text{Spectrum}(\mathcal{S}(G)) = \text{Len}(n).$$

The Lenstra polytopes are polytopes of the form $P_{T_{\mathcal{F}}}$ where $\mathcal{F}$ has a particularly nice structure. Fix a tower type $\mathfrak{T} = (n_1, \dots, n_t)$ and choose elements $\alpha_1, \dots, \alpha_t \in \overline{\mathbb{Q}}$ such that $[\mathbb{Q}(\alpha_1, \dots, \alpha_t) : \mathbb{Q}] = n$ and $\deg(\alpha_i) = n_i$ for all $1 \leq i \leq t$. Define a basis $\mathcal{B} = \{1 = v_0, \dots, v_{n-1}\}$ of $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$ as follows: for $0 \leq i < n$, write i in mixed radix notation with respect to $\mathfrak{T}$ as

$$i = i_1 + i_2(n_1) + i_3(n_1 n_2) + \dots + i_t(n_1 \dots n_{t-1}).$$

Set $v_i = \alpha_1^{i_1} \dots \alpha_t^{i_t}$. Then $P_{T_{\mathcal{F}}} = \text{Len}(\mathfrak{T})$.

In the case of general n and G , we give the following combinatorial criterion to determine whether the successive minima spectrum of $\mathcal{S}(G)$ lies in certain linear half spaces. For positive integers i, j , let $i \% j$ denote the remainder of dividing i by j .

Theorem 1.1.8. *Choose $1 \leq i \leq j \leq i + j < n$. The following are equivalent:*

1. *the region $\text{Spectrum}(\mathcal{S}(G))$ is contained in the linear half space defined by $x_{i+j} \leq x_i + x_j$;*
2. *for any integer m that occurs as the degree of a subfield of a degree n number field of Galois group G , we have $(i \% m) + (j \% m) = (i + j) \% m$.*

We now change our focus and discuss analogous theorems in the geometric setting. Scrollar invariants of covers of $\mathbb{P}^1$ are the geometric analogue of the logarithms of successive minima. Let C be a smooth projective geometrically irreducible curve of genus g over a field k equipped with a finite morphism $\pi: C \rightarrow \mathbb{P}^1$ of degree $n \geq 2$. Let $0 = a_0 \leq a_1 \leq a_2 \leq \dots \leq a_{n-1}$ be the unique integers such that

$$\pi_* \mathcal{O}_C \simeq \mathcal{O}_{\mathbb{P}^1}(-a_0) \oplus \mathcal{O}_{\mathbb{P}^1}(-a_1) \oplus \dots \oplus \mathcal{O}_{\mathbb{P}^1}(-a_{n-1}).$$

We say a_i is the i -th scollar invariant of π . Let g be the genus of C and let G be the Galois group of π . Let $K(C)$ be the function field of C and let $K(\mathbb{P}^1)$ be the function field of $\mathbb{P}^1$.

Theorem 1.1.9. *We have*

$$\left(\frac{a_1}{2(g+n-1)}, \dots, \frac{a_{n-1}}{2(g+n-1)} \right) \in \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}$$

where $\mathcal{F}$ ranges across all flags of $K(C)/K(\mathbb{P}^1)$.

Theorem 1.1.10. *Let $\mathcal{F}$ range across all flags of degree n extensions of $K(\mathbb{P}^1)$. We have*

$$\bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}} = \bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T})$$

if and only if n is a prime power, n is a product of 2 distinct primes, or $n = 12$.

Theorem 1.1.11. *Choose $1 \leq i \leq j \leq i + j < n$. If $a_{i+j} > a_i + a_j$ then there exists an integer m such that $\pi: C \rightarrow \mathbb{P}^1$ has a subcover of degree m and $(i \% m) + (j \% m) \neq (i + j) \% m$.*

We now briefly summarize our proofs. We first discuss the proof of Theorem 1.1.2; the multiplicative structure shows that

$$\text{Spectrum}(\mathcal{S}(G)) \subseteq \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}.$$

To show the converse, we show that every function $T_{\mathcal{F}}$ arising from a flag of a degree n number field with Galois group G arises from a “short” basis of an order. Given such an order $\mathcal{O}$, we provide an explicit construction to fill up the polytope $P_{T_{\mathcal{F}}}$ with suborders of $\mathcal{O}$. Note that these suborders are in general not maximal; for general degree n , it is an interesting open question to fill up $P_{T_{\mathcal{F}}}$ with maximal orders.

The proofs of the remaining theorems consist of explicitly computing the elements $T_{\mathcal{F}}$; the methods come from additive combinatorics. The main question we address is the following: given a multiplication table of a basis of a field extension, how many zeroes can there be, and in which positions?

1.2 Counting cubic rings by successive minima

Henceforth, let R be a nondegenerate rank n ring of absolute discriminant Δ ; such a ring naturally has the structure of a lattice, and therefore we may speak of the *successive minima*

$$\frac{1}{\sqrt{n}} \leq \lambda_0(R) \leq \cdots \leq \lambda_{n-1}(R)$$

of R . See Section 1.6 for more details. When R is implicit, we simply write λ_i . For a permutation group $G \subseteq S_n$, we say R is a *G-ring* if $\text{Gal}(R \otimes \mathbb{Q}) \cong G$ as permutation groups. We now summarize the results of Chapter 3; henceforth assume that R is a nondegenerate *cubic* ring.

We ask: for a point $p \in \mathbb{R}^2$ and a permutation group $G \subseteq S_3$, what are the asymptotics of

$$\#\{R \mid \Delta \leq X \text{ and } R \text{ is a } G\text{-ring and } (\log_{\Delta} \lambda_1, \log_{\Delta} \lambda_2) \text{ is “close” to } p\}$$

as $X \rightarrow \infty$?

To this end, we make the following definitions. For any point $p = (p_1, p_2) \in \mathbb{R}^2$, any permutation group $G \subseteq S_3$, any positive real number ϵ , and any $X \in \mathbb{R}_{>1}$, define $\mathcal{F}(p, \epsilon, G, X)$ to be the set of isomorphism classes of G -rings R with $\Delta \leq X$ and

$$\max_{i=1,2} \{|\log_{\Delta} \lambda_i(R) - p_i|\} \leq \frac{\epsilon}{\log X}.$$

The number $\#\mathcal{F}(p, \epsilon, G, X)$ captures the number of cubic rings of bounded discriminant and fixed Galois group that are “ (ϵ, X) -close” to p . One should think of ϵ as being a large, fixed positive real number³. One might hope that Malle’s conjecture generalizes and $\#\mathcal{F}(p, \epsilon, G, X) \asymp_{\epsilon, n} X^A (\log X)^{B-1}$ for some real numbers A, B ; in this paper, we are interested in the value A , which we extract using the following definitions⁴. We define the following *density function*, which takes a point as input p and outputs the value A .

Define the density function $d_{\epsilon, G}: \mathbb{R}^2 \rightarrow \mathbb{R} \cup \{*\}$ which assigns to $p \in \mathbb{R}^2$ the value

$$\lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, G, X) + 1)}{\log X}$$

if the limit exists and else assigns $*$. We add 1 to $\#\mathcal{F}(p, \epsilon, G, X)$ simply to avoid taking a logarithm of zero.

Some of our main theorems consist of computing such density functions; the first such result was obtained by Chiche-lapierre.

Theorem 1.2.1. (Chiche-lapierre [14], Theorem 3.1.1) *There exists a positive real number C such that for every $\epsilon > C$ and every $p = (p_1, p_2) \in \mathbb{R}^2$, we have:*

$$d_{\epsilon, S_3}(p) = \begin{cases} 1 - (p_2 - p_1) & \text{if } p \text{ is contained in the closed line segment from } (1/6, 1/3) \text{ to } (1/4, 1/4) \\ 0 & \text{else.} \end{cases}$$

For a function $f: \mathbb{R}^2 \rightarrow \mathbb{R} \cup \{*\}$, we say the *support* of f is the set of points in $\mathbb{R}^2$ where f is nonzero. Remarkably, the density function is *linear* on its support. We reprove Theorem 1.2.1 using simpler counting methods, which enable us to sieve for maximal S_3 -rings. To that end, let $\mathcal{F}^{\max}(p, \epsilon, G, X)$ be the subset of $\mathcal{F}(p, \epsilon, G, X)$ consisting of maximal rings and define the density function $d_{\epsilon, G}^{\max}: \mathbb{R}^2 \rightarrow \mathbb{R} \cup \{*\}$ which assigns to $p \in \mathbb{R}^2$ the value

$$\lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}^{\max}(p, \epsilon, G, X) + 1)}{\log X}$$

if the limit exists and else assigns $*$.

³We encourage the reader to think of ϵ as a fixed quantity that is large enough to make certain estimates work, where here “large enough” depends only on the degree n . For $3 \leq n \leq 5$, taking ϵ to be one billion is certainly large enough for all our theorem statements.

⁴Malle’s conjecture roughly says that the number of isomorphism classes of degree n number fields of fixed Galois group and absolute discriminant bounded by X is $\asymp_n X^A (\log X)^{B-1}$ for some explicit values of A and B .

Theorem 1.2.2. *There exists a positive real number C such that for every $\epsilon > C$, we have*

$$d_{\epsilon, S_3} = d_{\epsilon, S_3}^{\max}.$$

We also compute the density functions of $\mathbb{Z}/2\mathbb{Z}$ and the trivial group; they are presented in Chapter 3. We also obtain a *total density function*, i.e. a density function where we do not impose any Galois condition, as follows. Let $\mathcal{F}(p, \epsilon, X)$ be the set of isomorphism classes of nondegenerate cubic rings R with $\Delta \leq X$ and

$$\max_{i=1,2} \{ |\log_{\Delta} \lambda_i(R) - p_i| \} \leq \frac{\epsilon}{\log X}$$

and let $d_{\epsilon,3}$ denote the corresponding density function. Similarly, let $\mathcal{F}_3^{\max}(p, \epsilon, X)$ be the subset of $\mathcal{F}_3(p, \epsilon, X)$ consisting of *maximal* cubic rings and define the density function of maximal cubic rings $d_{\epsilon,3}^{\max}$ as above.

Theorem 1.2.3. *There exists a positive real number C such that for every $\epsilon > C$ and every $p = (p_1, p_2) \in \mathbb{R}^2$, we have:*

$$d_{\epsilon,3}(p) = \begin{cases} 1 - (p_2 - p_1) + \max\{0, 1/2 - 3p_1\} & \text{if } p \text{ is contained in the closed line segment from} \\ & (0, 1/2) \text{ to } (1/4, 1/4) \\ 0 & \text{else.} \end{cases}$$

$$d_{\epsilon,3}^{\max}(p) = \begin{cases} 1 - (p_2 - p_1) & \text{if } p \text{ is contained in the closed line segment from } (1/6, 1/3) \text{ to } (1/4, 1/4) \\ 1 & \text{if } p = (0, 1/2) \\ 0 & \text{else.} \end{cases}$$

Observe that the total density function $d_{\epsilon,3}$ has a very particular structure; from 1 we subtract piecewise differences of the coordinates (the term $p_2 - p_1$) and add in correction terms in the “cusp” (the term $\max\{0, 1/2 - 3p_1\}$). We observe this phenomenon in the quartic and quintic total density functions as well.

The definitions of density functions and successive minima comes purely from Euclidean geometry; however, we can show that the rings lying near the boundary of these line segments tend to have to various interesting *algebraic* properties. In particular:

1. the point $(1/6, 1/3)$ “corresponds” to monogenic cubic rings (see Corollary 3.1.4);

2. irreducible cubic rings “tend” to lie “near” to $(1/4, 1/4)$ (see Corollary 3.1.5);

3. and reducible cubic rings “tend” to lie “near” to $(0, 1/2)$ (see Corollary 3.1.5).

(2) is also implied by Bhargava and H’s work on the equidistribution of orders in S_3 -cubic fields [5], although we give an independent proof.

1.2.1 Results on binary n -ic forms

By work of Delone and Faddeev [18], cubic rings are parametrized by orbits of binary cubic forms. To prove our theorems on density functions of cubic rings, we prove lemmas on binary cubic forms, many of which generalize to the case of binary n -ic forms for $n \geq 3$. Work of Birch and Merriman [9] and work of Nakagawa [26] associates to a binary n -ic form $f \in \text{Sym}^n \mathbb{Z}^2$ a rank n ring R_f . We now give partial results on successive minima of rings arising from binary n -ic forms.

For an integer $n \geq 3$, a point $p = (p_1, \dots, p_{n-1}) \in \mathbb{R}^{n-1}$, any positive real number ϵ , and any $X \in \mathbb{R}_{>1}$, define $\mathcal{F}_n^{\text{bin}}(p, \epsilon, X)$ to be the set of $\text{GL}_2(\mathbb{Z})$ -orbits of $\text{Sym}^n \mathbb{Z}^2$ of absolute discriminant Δ such that $\Delta \leq X$ and

$$\max_{1 \leq i < n} |\log_{\Delta} \lambda_i(R_f) - p_i| \leq \frac{\epsilon}{\log X}.$$

Birch and Merriman [9] prove that there are finitely many $\text{GL}_2(\mathbb{Z})$ -equivalence classes of integral binary n -ic forms of fixed discriminant, which implies that the set $\mathcal{F}_n^{\text{bin}}(p, \epsilon, X)$ is finite. Let

$$k := \frac{1}{2(1 + \dots + (n-1))}$$

and define ℓ to be the closed line segment from $(0, k)$ to $(k/2, k/2)$. Let $L: \ell \rightarrow \mathbb{R}^{n-1}$ be the linear map sending the point $(0, k)$ to $(k, 2k, \dots, (n-1)k)$ and sending the point $(k/2, k/2)$ to $\frac{1}{2(n-1)}(1, \dots, 1)$.

Theorem 1.2.4. *For $r = (r_1, r_2) \in \ell$, we have*

$$\#\mathcal{F}_n^{\text{bin}}(L(r), \epsilon, X) \gg_r X^{(n+1)/(2n-2)-(r_2-r_1)}.$$

In particular, specializing to $r = (k/2, k/2)$ proves that there are $\gg X^{(n+1)/(2n-2)}$ $\text{GL}_2(\mathbb{Z})$ -orbits of integral binary n -ic forms with $\Delta \leq X$; this is precisely the content of Theorem 2 of [26]. For $n = 3, 4, 5$, Theorem 1.2.4 in combination with the proofs of Theorem 1.2.3, Theorem 1.3.1, and

Theorem 1.4.1 respectively implies that

$$\#\mathcal{F}_n^{\text{bin}}(L(r), \epsilon, X) \asymp_r \exp[X, \frac{n+1}{2n-2} - (r_2 - r_1)].$$

1.3 Counting quartic rings by successive minima

We now move on to quartic rings and summarize the results of Chapter 4. We will consider pairs (R, C) , where R denotes a nondegenerate quartic ring equipped with a cubic resolvent ring C ; see Section 4.2 for background. Let Δ be the absolute discriminant of R , which is also the absolute discriminant of C . We first define certain regions that will be the support of our density functions; these are the analogues of the line segments from the cubic case.

For a permutation group $G \subseteq S_4$, define $\text{Poly}_4(G)$ to be the limit points of the multiset

$$\{(\log_{\Delta} \lambda_1(R), \log_{\Delta} \lambda_2(R), \log_{\Delta} \lambda_3(R), \log_{\Delta} \lambda_1(C), \log_{\Delta} \lambda_2(C))\} \subseteq \mathbb{R}^5$$

in the Euclidean metric as we range over isomorphism classes of pairs (R, C) where R is a G -ring. Define Poly_4 to be $\cup_G \text{Poly}_4(G)$ as we range over all permutation groups $G \subseteq S_4$. We will prove that $\text{Poly}_4(G)$ is a finite union of polytopes (Theorem 4.1.1). We also give explicit linear inequalities defining $\text{Poly}_4(S_4)$, $\text{Poly}_4(D_4)$, and Poly_4 ; see Theorem 4.1.2, Theorem 4.1.3, and Theorem 4.1.4.

We now define our density functions. Let $p = (p_1, p_2, p_3, q_1, q_2) \in \mathbb{R}^5$ denote a point. For any positive real number ϵ , any $X \in \mathbb{R}_{>1}$, and any permutation group $G \subseteq S_4$, define $\mathcal{F}(p, \epsilon, G, X)$ to be the set of isomorphism classes of pairs (R, C) such that R is a G -ring, $\Delta \leq X$, and

$$\max_{i=1,2,3} \{|\log_{\Delta} \lambda_i(R) - p_i|\} \leq \frac{\epsilon}{\log X} \quad (1.2)$$

$$\max_{i=1,2} \{|\log_{\Delta} \lambda_i(C) - q_i|\} \leq \frac{\epsilon}{\log X}. \quad (1.3)$$

Define the density function $d_{\epsilon, G}: \mathbb{R}^5 \rightarrow \mathbb{R} \cup \{*\}$ which assigns to $p \in \mathbb{R}^5$ the value

$$\lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, G, X) + 1)}{\log X}$$

if it exists and else assigns $*$.

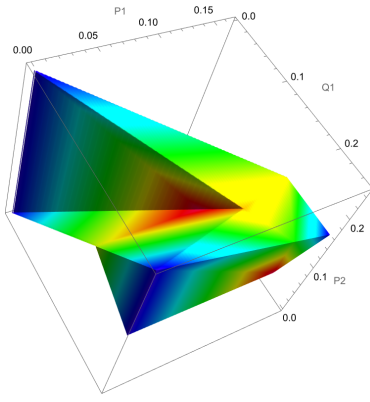


Figure 1.1: Poly_4 projected onto p_1 , p_2 , and q_1 . The color indicates the value of the density function $d_{\epsilon,4}$; blue is the highest value.

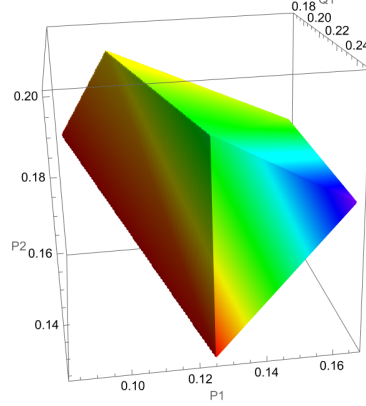


Figure 1.2: $\text{Poly}_4(S_4)$ projected onto p_1 , p_2 , and q_1 . The color indicates the values of the density function d_{ϵ,S_4} ; blue is the highest value.

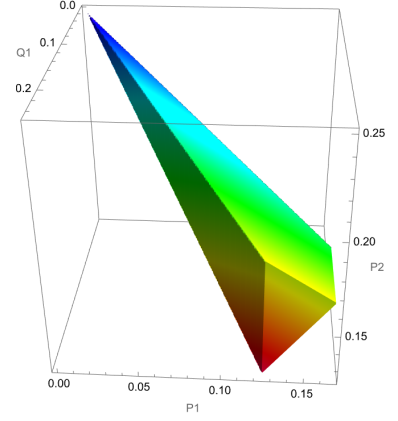


Figure 1.3: $\text{Poly}_4(D_4)$ projected onto p_1 , p_2 , and q_1 . The color indicates the value of the lower bound on the density function d_{ϵ,D_4} given in Theorem 1.3.3; blue is the highest value.

Theorem 1.3.1. *There exists a positive real number M such that for every $\epsilon > M$ and every $p \in \mathbb{R}^5$,*

$$d_{\epsilon,4}(p) = \begin{cases} 1 - (p_3 - p_2) - (p_3 - p_1) - (p_2 - p_1) - (q_2 - q_1) & \text{if } p \in \text{Poly}_4 \\ + \sum_{i \leq j, k} \max\{0, q_k - p_i - p_j\} & \\ 0 & \text{else.} \end{cases}$$

As in the cubic case and quintic case, $d_{\epsilon,4}$ has a very particular structure; from 1 we subtract piecewise differences of the coordinates (the terms $p_j - p_i$ and $q_j - q_i$) and add in correction terms (the terms $\max\{0, q_k - p_i - p_j\}$). The density function for S_4 is simply a restriction of the total density function.

Theorem 1.3.2. *There exists a positive real number M such that for every $\epsilon > M$ and every $p \in \mathbb{R}^5$ we have*

$$d_{\epsilon,S_4}(p) = \begin{cases} d_{\epsilon,4}(p) & \text{if } p \in \text{Poly}_4(S_4) \\ 0 & \text{else.} \end{cases}$$

Theorem 1.3.3. *There exists a positive real number M such that for every $\epsilon > M$ and every $p \in \mathbb{R}^5$, the following statements hold.*

1. If $p \in \text{Poly}_4(D_4) \setminus \text{Poly}_4(S_4)$, then

$$d_{\epsilon, D_4}(p) = d_{\epsilon, 4}(p) = 1 - (p_3 - p_2) - (p_3 - p_1) - (p_2 - p_1) - (q_2 - q_1) \\ + (q_2 - 2p_1) + (q_2 - p_1 - p_2) + (q_2 - p_1 - p_3).$$

2. If $p \notin \text{Poly}_4(D_4)$, then $d_{\epsilon, D_4}(p) = 0$.

3. If $p \in \text{Poly}_4(D_4)$, then

$$\liminf_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, D_4, X) + 1)}{\log X} \geq 1 - (p_3 - p_2) - (p_3 - p_1) - (p_2 - p_1) - (q_2 - q_1) \\ + (q_2 - 2p_1) + (q_2 - p_1 - p_2) + (q_2 - p_1 - p_3)$$

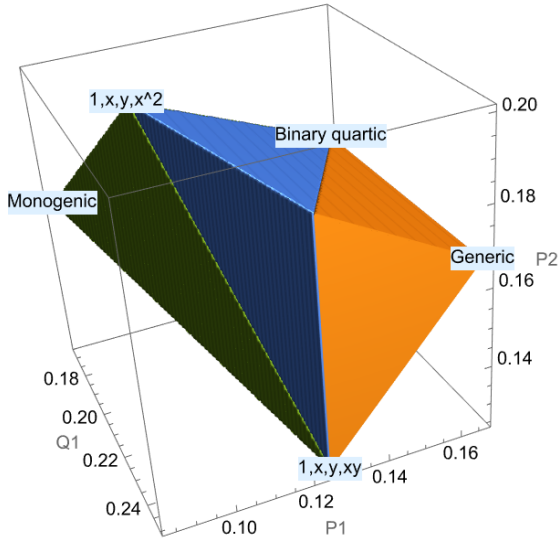


Figure 1.4: $\text{Poly}_4(S_4)$ projected onto p_1 , p_2 , and q_1 . The colored regions are the regions on which d_{ϵ, S_4} is linear. The vertices are labelled by the family of rings “corresponding” to them.

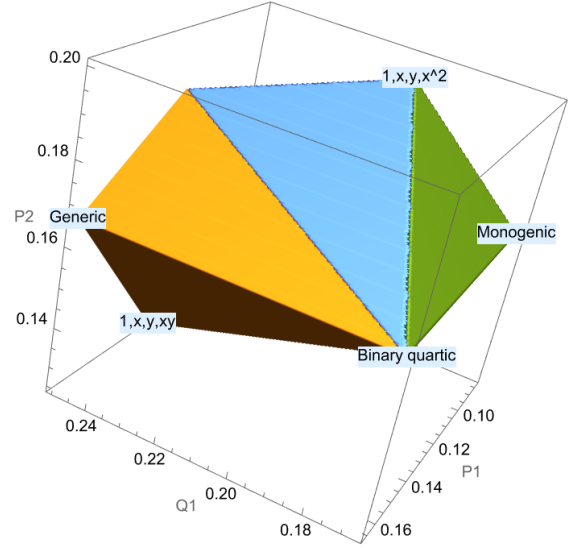


Figure 1.5: The other side of $\text{Poly}_4(S_4)$ projected onto p_1 , p_2 , and q_1 .

As in the cubic case, we observe *algebraic* phenomena at the vertices of these convex bodies. In particular, $\text{Poly}_4(S_4)$ is a polytope with 6 vertices. We give natural interpretations for 5 of these 6 vertices:

1. S_4 -rings “correspond” to $(1/6, 1/6, 1/6, 1/4, 1/4)$ by Theorem 4.1.5;
2. monogenic quartic rings “correspond” to $(1/12, 1/6, 1/4, 1/6, 1/3)$ by Theorem 4.1.6;

3. quartic rings arising from binary quartic forms “correspond” to $(1/6, 1/6, 1/6, 1/6, 1/3)$ by Theorem 4.1.7;
4. quartic rings with a basis of the form $1, x, y, xy$ with a pairing condition “correspond” to $(1/8, 1/8, 1/4, 1/4, 1/4)$ by Theorem 4.1.9;
5. and quartic rings with a basis of the form $1, x, y, x^2$ “correspond” to $(1/10, 1/5, 1/5, 1/5, 3/10)$ by Theorem 4.1.11.

The vertex missing from this list is $(1/8, 3/16, 3/16, 1/4, 1/4)$; it would be interesting to have a family of quartic rings naturally corresponding to this vertex! Moreover, one can show that D_4 -rings “correspond” to $(0, 1/4, 1/4, 0, 1/2)$ by Theorem 4.1.5, and this point is the unique vertex of $\text{Poly}_4(D_4)$ that is not a vertex of $\text{Poly}_4(S_4)$.

1.4 Counting quintic rings by successive minima

We now summarize the results of Chapter 5. We consider pairs (R, S) where R is a nondegenerate quintic ring equipped with a sextic resolvent ring S ; see Section 5.2 for background. Let Δ be the absolute discriminant of R . We proceed as in the quartic case; we first define certain regions that will be the support of our density functions, then compute our density functions, and then discuss special families of quintic rings.

For a permutation group $G \subseteq S_5$, define $\text{Poly}_5(G)$ to be the limit points of the multiset

$$\{(\log_{\Delta} \lambda_1(R), \dots, \log_{\Delta} \lambda_4(R), \log_{\Delta} \lambda_1(S), \dots, \log_{\Delta} \lambda_5(S))\} \subseteq \mathbb{R}^9$$

in the Euclidean metric as we range over all pairs (R, S) where R is a G -ring. We compute $\text{Poly}_5(S_5)$ and show that is a single polytope. For a positive number ϵ and a permutation group $G \subseteq S_5$, define the density functions $d_{\epsilon, G}$, and $d_{\epsilon, 5}$ analogously to the quartic case; in this case they are functions from $\mathbb{R}^9$ to $\mathbb{R} \cup \{*\}$; see Chapter 5 for more information. Let $p = (p_1, \dots, p_4, q_1, \dots, q_5) \in \mathbb{R}^9$ denote a point.

Theorem 1.4.1. *There exists a positive real number C such that for every $\epsilon > C$ and every $p \in \mathbb{R}^9$,*

$$d_{\epsilon, 5}(p) = \begin{cases} 1 - \sum_{1 \leq i < j \leq 4} (p_j - p_i) - \sum_{1 \leq i < j \leq 5} (q_j - q_i) & \text{if } p \in \text{Poly}_5 \\ + \sum_{i < j, k} \max\{0, -1/2 + q_i + q_j - p_k\} & \\ 0 & \text{else.} \end{cases}$$

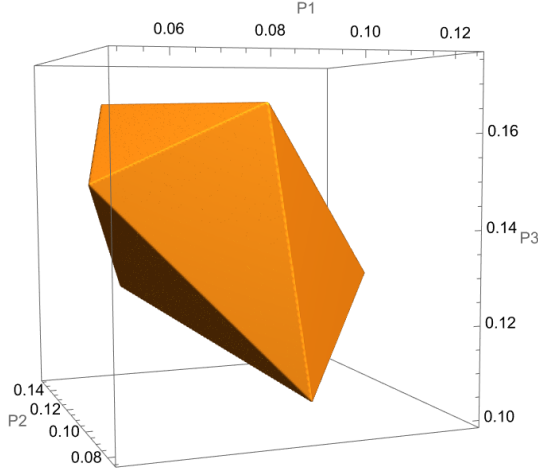


Figure 1.6: $\text{Poly}_5(S_5)$ projected onto p_1 , p_2 , and p_3 .

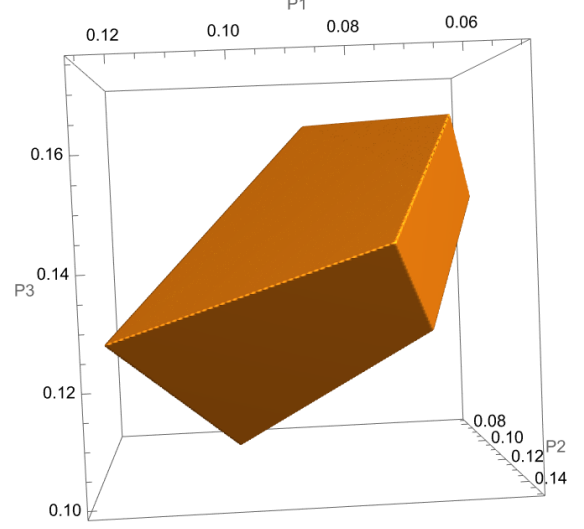


Figure 1.7: The other side of $\text{Poly}_5(S_5)$ projected onto p_1 , p_2 , and p_3 .

Again, observe that the structure of $d_{\epsilon,5}$ is similar to that of $d_{\epsilon,3}$ and $d_{\epsilon,4}$; from 1 we subtract piecewise differences ($\sum_{1 \leq i < j \leq 4} (p_j - p_i)$ and $\sum_{1 \leq i < j \leq 5} (q_j - q_i)$); and in the “cusp” we add in correction terms ($\sum_{i < j, k} \max\{0, -1/2 + q_i + q_j - p_k\}$).

Theorem 1.4.2. *There exists a positive real number C such that for every $\epsilon > C$ and every $p \in \mathbb{R}^9$,*

$$d_{\epsilon, S_5}(p) = \begin{cases} d_{\epsilon, 5}(p) & \text{if } p \in \text{Poly}_5(S_5) \\ 0 & \text{else.} \end{cases}$$

Again, the definitions of the density functions and $\text{Poly}_5(G)$ are purely Euclidean, but we observe *algebraic* phenomena along these convex bodies. In particular:

1. S_5 -rings “correspond” to the vertex

$$(1/8, 1/8, 1/8, 1/8, 3/10, 3/10, 3/10, 3/10, 3/10)$$

of $\text{Poly}_5(S_5)$ by Corollary 5.1.4;

2. monogenic quintic rings “correspond” to the vertex

$$(1/20, 2/20, 3/20, 4/20, 4/20, 5/20, 6/20, 7/20, 8/20)$$

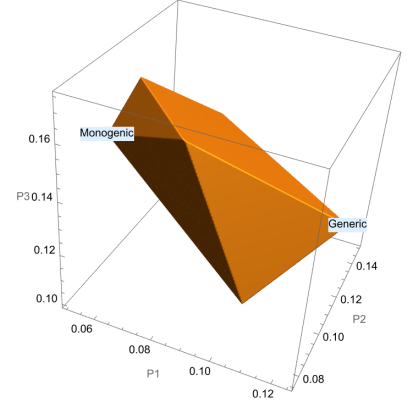


Figure 1.8: $\text{Poly}_5(S_5)$ projected to p_1 , p_2 , and p_3 . The image of the projection of the vertex corresponding to S_5 -rings is marked “generic”. The projection of the vertex corresponding to monogenic rings is marked “monogenic”.

of $\text{Poly}_5(S_5)$ by Theorem 5.1.7;

3. and quintic rings arising from binary quintic forms “correspond” to the vertex

$$(1/8, 1/8, 1/8, 1/8, 1/4, 1/4, 1/4, 3/8, 3/8)$$

of $\text{Poly}_5(S_5)$ by Theorem 5.1.5.

There are 18 vertices of $\text{Poly}_5(S_5)$; it would be interesting to give interpretations of the remaining 15 vertices!

1.5 The relationship between scrollar invariants and successive minima

For a permutation group $G \subseteq S_n$ and a point $p \in \mathbb{R}^{n-1}$, we expect the asymptotics of

$$\#\{\mathcal{O} \mid \Delta \leq X \text{ and } \text{Gal}(\mathcal{O} \otimes \mathbb{Q}) \simeq G \text{ and } p_{\mathcal{O}} \text{ is “close” to } p\} \quad (1.4)$$

as $X \rightarrow \infty$ to be closely related to the dimensions of loci in an appropriate Hurwitz space of covers of $\mathbb{P}^1$ with certain fixed invariants. In this section, we expound upon this relationship; in particular for $n = 3, 4, 5$, we explain how, appropriately interpreted, our density functions of orders in degree n number fields with Galois group S_n give the same quantities as results of Patel [28] on the dimensions of loci in appropriate Hurwitz spaces with certain fixed invariants.

For positive integers n and g , let $\mathcal{H}_{n,g}$ denote the Hurwitz space of simply branched genus g covers of $\mathbb{P}^1$; it is a Deligne-Mumford stack of dimension $2n + 2g - 5$. From a cover $[\pi: C \rightarrow \mathbb{P}^1] \in \mathcal{H}_{n,g}$, we obtain the sequence of sheaves:

$$0 \rightarrow \mathcal{O}_{\mathbb{P}^1} \rightarrow \pi_* \mathcal{O}_C \rightarrow \mathcal{E}^\vee \rightarrow 0$$

The sheaf $\mathcal{E}$ is called the *Tschirnhausen bundle* of π , and plays a crucial role in the study of covers of $\mathbb{P}^1$ and the geometry of the Hurwitz space of such covers. Casnati and Ekedahl [10, 11] canonically

defined a relative embedding:

$$\begin{array}{ccc} C & \xrightarrow{i} & \mathbb{P}\mathcal{E} \\ & \searrow \pi & \downarrow \alpha \\ & & \mathbb{P}^1 \end{array}$$

Casnati and Ekedahl also constructed a canonical resolution for the ideal sheaf I_C . If $n = 3$, the resolution has the form:

$$0 \rightarrow \alpha^* \det \mathcal{E}(-3) \rightarrow I_C \rightarrow 0. \quad (1.5)$$

If $n > 3$, the resolution has the form:

$$\begin{aligned} 0 \rightarrow \alpha^* \det \mathcal{E}(-n) \rightarrow \alpha^* \mathcal{N}_{n-3}(-n+2) \rightarrow \alpha^* \mathcal{N}_{n-4}(-n+3) \rightarrow \dots \\ \dots \rightarrow \alpha^* \mathcal{N}_3(-4) \rightarrow \alpha^* \mathcal{N}_2(-3) \rightarrow \alpha^* \mathcal{N}_1(-2) \rightarrow I_C \rightarrow 0 \end{aligned} \quad (1.6)$$

This resolution has a natural duality given by $\mathcal{N}_i \simeq \mathcal{N}_{n-2-i}^\vee \otimes \det \mathcal{E}$. Thus, to such a cover π we may canonically associate the sequence of locally free sheaves $\mathcal{E}, \mathcal{N}_1, \dots, \mathcal{N}_{n-3}$; it would be very interesting to know which sequences of locally free sheaves we obtain from simply branched covers of $\mathbb{P}^1$ of fixed degree and genus ⁵⁶!

In what follows, we will only be interested in $\mathcal{E}$ and $\mathcal{N}_1$; in fact, when $3 \leq n \leq 5$, the natural duality of the resolutions (1.5) and (1.6) imply that the sheaves $\mathcal{E}$ and $\mathcal{N}_1$ *determine* the sequence $\mathcal{E}, \mathcal{N}_1, \dots, \mathcal{N}_{n-3}$ of sheaves⁷. To that end, if $n > 3$ then let $\mathcal{F}$ refer to $\mathcal{N}_1$. A straightforward application of Riemann-Roch shows that $\mathcal{E}$ has degree $g + n - 1$ and rank $n - 1$, and $\mathcal{F}$ has degree $(n - 3)(g + n - 1)$ and rank $\frac{n(n-3)}{2}$.

Conversely, given a locally free sheaf $\mathcal{E}$ on $\mathbb{P}^1$ of degree $g + n - 1$ and rank $n - 1$, we define the *Maroni locus* of $\mathcal{E}$ to be

$$\mathcal{M}(\mathcal{E}) := \overline{\{[\pi: C \rightarrow \mathbb{P}^1] \in \mathcal{H}_{n,g} \mid \mathcal{E}_\pi \simeq \mathcal{E}\}}.$$

This locus was implicitly considered by Maroni [25] in the case $n = 3$. Similarly, given a locally free sheaf $\mathcal{F}$ on $\mathbb{P}^1$ of appropriate degree and rank, define the *Maroni-Casnati-Ekedahl locus* of $(\mathcal{E}, \mathcal{F})$ to be

$$\mathcal{M}(\mathcal{E}, \mathcal{F}) := \overline{\{[\pi: C \rightarrow \mathbb{P}^1] \in \mathcal{H}_{n,g} \mid \mathcal{E}_\pi \simeq \mathcal{E}, \mathcal{F}_\pi \simeq \mathcal{F}\}}.$$

⁵This is a natural generalization of the following classical question: which sheaves $\mathcal{E}$ arise as Tschirnhausen bundles of covers of $\mathbb{P}^1$? In Chapter 2, we prove strong constraints on such sheaves $\mathcal{E}$, generalizing former work of Ohbuchi and Patel [27, 28].

⁶In fact, Castryck, Vermeulen, and Zhao [13] show that each syzygy bundle corresponds to an irreducible representation of S_n . Moreover, for *every* irreducible representation λ of S_n , they naturally construct a locally free sheaf $\mathcal{N}_\lambda$ on $\mathbb{P}^1$. More generally, one could ask: which sequences of locally free sheaves $\{\mathcal{N}_\lambda\}$ do we get from simply branched covers π ?

⁷In fact, for $3 \leq n \leq 5$, in the simply branched case, results of Castryck, Vermeulen, and Zhao [13] imply that $\mathcal{E}$ and $\mathcal{N}_1$ determine *all* locally free sheaves $\mathcal{N}_\lambda$ as we range across irreducible representations λ of the symmetric group.

Given a cover $\pi \in \mathcal{H}_{n,g}$, the Tschirnhausen bundle $\mathcal{E}$ is a locally free rank $n - 1$ sheaf on $\mathbb{P}^1$ and thus decomposes as a sum of line bundles. We write:

$$\mathcal{E} \simeq \mathcal{O}_{\mathbb{P}^1}(a_1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(a_{n-1})$$

for integers $a_1 \leq a_2 \leq \cdots \leq a_{n-1}$. We say the integer a_i is the *i-th scollar invariant* of π (and we also say that $a_0 = 0$ is the 0-th scollar invariant of π). The scollar invariants of a cover are the natural geometric analogues of the logarithms of the successive minima of an order in a number field of degree n ; see [22] for more details. Let $\mathcal{O}$ denote an order in a degree n number field with absolute discriminant Δ . For simplicity, we restrict to the case of simply branched covers and orders with squarefree discriminant respectively, and summarize the relationship between these two objects in the following table.

Geometric object	Number field object
simply branched covers of $\mathbb{P}^1$	maximal orders $\mathcal{O}$ with squarefree discriminant
degree of the cover	degree of the number field $\mathcal{O} \otimes \mathbb{Q}$
$g + n - 1$	$\log \sqrt{\Delta}$
the <i>i</i> -th scollar invariant a_i	$\log \lambda_i(\mathcal{O})$
the point $\frac{1}{2(g+n-1)}(a_1, \dots, a_{n-1})$	the point $(\log_{\Delta} \lambda_1, \dots, \log_{\Delta} \lambda_{n-1})$

One should think of the Maroni locus $\mathcal{M}(\mathcal{E})$ as being analogous to the set of maximal orders $\mathcal{O}$ with squarefree discriminant such that $\log \Delta$ is “approximately” $2g$ and $\log \lambda_i(\mathcal{O})$ is “approximately” a_i . Under this analogy, one might compare:

1. the *dimension* of Maroni loci, appropriately normalized, as $g \rightarrow \infty$;
2. the *number* of orders $\mathcal{O}$, appropriately normalized, such that Δ is squarefree, $\Delta \leq X$, and $(\log_{\Delta} \lambda_1, \dots, \log_{\Delta} \lambda_{n-1})$ is “close” to $\frac{1}{2(g+n-1)}(a_1, \dots, a_{n-1})$, as $X \rightarrow \infty$.

We explicitly make this comparison below when $n = 3, 4, 5$. We show that, appropriately interpreted, both quantities are the same. Observe that if Δ is squarefree, then $\mathcal{O}$ is an order in a degree n S_n -number field. In our analysis below, we do not impose the condition that Δ is squarefree; instead we impose the weaker condition that $\mathcal{O}$ lies in an S_n -field. We expect the same results to hold if one were to restrict to orders with squarefree discriminant, but we do not prove this. We first analyze the case $n = 3$; the following proposition computes the dimension of the Maroni loci in this case.

Proposition 1.5.1 (Patel [28], Proposition 1.4). *Let $n = 3$ and suppose we have a locally free sheaf*

$$\mathcal{E} = \mathcal{O}(a_1) \oplus \mathcal{O}(a_2)$$

such that $a_1 \leq a_2$ and $\deg(\mathcal{E}) = g + n - 1$. Then if (a_1, a_2) lies in the cone over the closed line segment from $(1/6, 1/3)$ to $(1/4, 1/4)$, we have

$$\dim \mathcal{M}(\mathcal{E}) = \dim \mathcal{H}_{3,g} - h^1(\text{End}(\mathcal{E})).$$

Else, $\mathcal{M}(\mathcal{E}) = \emptyset$.

We'll now show how Proposition 1.5.1 above is analogous to the density function for S_3 -cubic rings, given in Theorem 1.2.1. To make this comparison, we will fix a point $p = (p_1, p_2) \in \mathbb{Q}^2$ with $p_1 + p_2 = 1/2$ and compare the dimensions of Maroni loci

$$\mathcal{M}(\mathcal{O}(2p_1(g+2)) \oplus \mathcal{O}(2p_2(g+2))) \subseteq \mathcal{H}_{3,g}$$

as $g \rightarrow \infty$ for values of g such that $2p_1(g+2), 2p_2(g+2) \in \mathbb{Z}$. To this end, we'll need the following notation. For any positive integer k a point $p = (p_1, \dots, p_k) \in \mathbb{R}^k$ and positive integers g and n , define the point

$$P_{g,n} := 2(g+n-1)(p_1, \dots, p_k) \in \mathbb{R}^k.$$

If $P_{g,n} \in \mathbb{Z}^k$, define the locally free sheaf

$$\mathcal{E}_{p,g,n} := \mathcal{O}(2(g+n-1)p_1) \oplus \dots \oplus \mathcal{O}(2(g+n-1)p_k).$$

For a point $p = (p_1, p_2) \in \mathbb{Q}^2$ with $p_1 + p_2 = 1/2$, combining Proposition 1.5.1 and Theorem 1.2.1 shows that for ϵ sufficiently large, we have:

$$\lim_{g \rightarrow \infty, P_{g,3} \in \mathbb{Z}^2} \frac{\dim \mathcal{M}(\mathcal{E}_{p,g,3})}{\dim \mathcal{H}_{3,g}} = d_{\epsilon, S_3}(p)$$

Therefore dimensions of Maroni loci of trigonal covers can be compared to asymptotics of orders in cubic S_3 -fields with almost prescribed successive minima. In other words, our density function d_{ϵ, S_3} is capturing dimensions of Maroni loci in the limit as $g \rightarrow \infty$.

We now analyze the case $n = 4$. In the number field case, we considered pairs (R, C) of quartic

rings equipped with a cubic resolvent ring. In the geometric case, for a cover $\pi \in \mathcal{H}_{4,g}$, we consider the Tschirnhausen bundle $\mathcal{E}$ along with the first syzygy bundle $\mathcal{F}$. From a tetragonal cover $\pi \in \mathcal{H}_{4,g}$, a classical construction of Recillas [30] obtains a *trigonal* cover of $\mathbb{P}^1$ of genus $g + 1$. We think of this trigonal cover as being analogous to the cubic resolvent ring C . Moreover, the Tschirnhausen bundle of the trigonal cover is precisely the first syzygy bundle $\mathcal{F}$, as observed by Casnati [12] and further discussed by Deopurkar and Patel [19]. Therefore, if we write

$$\mathcal{F} = \mathcal{O}(b_1) \oplus \mathcal{O}(b_2)$$

for integers $b_1 \leq b_2$, then $\log \lambda_i(C)$ is analogous to b_i for $i = 1, 2$. The following proposition computes the dimension of the Maroni-Casnati-Ekedahl loci in the quartic case. As given in [28], the proposition does not explicitly state when the Maroni-Casnati-Ekedahl locus is empty, so we have amended the statement below to account for this.

Theorem 1.5.2 (Patel [28], Proposition 1.5). *Let $n = 4$. Suppose we are given a locally free sheaf $\mathcal{E}$ on $\mathbb{P}^1$ of degree $g + n - 1$ and rank $n - 1$ and a locally free sheaf $\mathcal{F}$ on $\mathbb{P}^1$ of degree $(n - 3)(g + n - 1)$ and rank $\frac{n(n-3)}{2}$. Write*

$$\mathcal{E} = \mathcal{O}(a_1) \oplus \mathcal{O}(a_2) \oplus \mathcal{O}(a_3)$$

$$\mathcal{F} = \mathcal{O}(b_1) \oplus \mathcal{O}(b_2)$$

so $a_1 \leq a_2 \leq a_3$ and $b_1 \leq b_2$. Then if $(a_1, a_2, a_3, b_1, b_2)$ lies in the cone over $\text{Poly}_4(S_4)$, we have

$$\dim(\mathcal{M}(\mathcal{E}, \mathcal{F})) = \dim(\mathcal{H}_{4,g}) - h^1(\mathcal{E}nd(\mathcal{E})) - h^1(\mathcal{E}nd(\mathcal{F})) + h^1(\mathcal{F}^\vee \otimes \text{Sym}^2 \mathcal{E}).$$

Else, $\mathcal{M}(\mathcal{E}, \mathcal{F}) = \emptyset$.

For a point $p = (p_1, p_2, p_3) \in \mathbb{Q}^3$ and $q = (q_1, q_2) \in \mathbb{Q}^2$ with $p_1 + p_2 + p_3 = q_1 + q_2 = 1/2$, we have

$$\lim_{g \rightarrow \infty, (p_{g,4}, q_{g,4}) \in \mathbb{Z}^5} \frac{\dim \mathcal{M}(\mathcal{E}_{p,g,4}, \mathcal{E}_{q,g,4})}{\dim \mathcal{H}_{4,g}} = d_{\epsilon, S_4}(p, q),$$

for ϵ sufficiently large (here $q_{g,4}$ and $\mathcal{E}_{q,g,4}$ are defined identically to $p_{g,4}$ and $\mathcal{E}_{p,g,4}$). Again, we see that when $n = 4$, the dimensions of Maroni-Casnati-Ekedahl loci are captured, in the limit, by our density functions.

We now analyze the case $n = 5$. In the number field case, we considered pairs (R, S) of quintic

rings equipped with a sextic resolvent ring. Again, in the geometric case we consider the pair $(\mathcal{E}, \mathcal{F})$ attached to a cover $\pi \in \mathcal{H}_{5,g}$. There is a natural construction that attaches to the quintic cover π a sextic cover of $\mathbb{P}^1$ of genus $3g + 7$; see Corollary 37 of [13] for details. We think of sextic cover as being analogous to the sextic resolvent ring S . Moreover, [13] proves that the Tschirnhausen bundle of this sextic cover is precisely the second syzygy bundle $\mathcal{N}_2$! By the duality of the resolution (1.6), we have $\mathcal{N}_2 \simeq \mathcal{N}_1^\vee \otimes \det \mathcal{E} \simeq \mathcal{F}^\vee(g + n - 1)$. So, if we write

$$\mathcal{F} = \mathcal{O}(b_1) \oplus \cdots \oplus \mathcal{O}(b_5)$$

for integers $b_1 \leq \cdots \leq b_5$, then we should think of $\log \lambda_i(S)$ as being analogous to $-b_{6-i} + (g + n - 1)$ for $1 \leq i \leq 5$.

The following proposition computes the dimension of the Maroni-Casnati-Ekedahl loci in the quintic case; again, as given in [28], the proposition did not explicitly state when the Maroni-Casnati-Ekedahl locus was empty, so we have amended the statement to account for this.

Theorem 1.5.3 (Patel [28], Proposition 1.18). *Let $n = 5$. Suppose we are given a locally free sheaf $\mathcal{E}$ on $\mathbb{P}^1$ of degree $g + n - 1$ and rank $n - 1$ and a locally free sheaf $\mathcal{F}$ on $\mathbb{P}^1$ of degree $(n - 3)(g + n - 1)$ and rank $\frac{n(n-3)}{2}$. Write*

$$\mathcal{E} = \mathcal{O}(a_1) \oplus \cdots \oplus \mathcal{O}(a_4)$$

$$\mathcal{F} = \mathcal{O}(b_1) \oplus \cdots \oplus \mathcal{O}(b_5)$$

so that $a_1 \leq \cdots \leq a_4$ and $b_1 \leq \cdots \leq b_5$. If

$$(a_1, \dots, a_4, -b_5 + (g + n - 1), \dots, -b_1 + (g + n - 1))$$

lies in the cone over $\text{Poly}_5(S_5)$, we have

$$\dim(\mathcal{M}(\mathcal{E}, \mathcal{F})) = \dim(\mathcal{H}_{4,g}) - h^1(\text{End}(\mathcal{E})) - h^1(\text{End}(\mathcal{F})) + h^1(\wedge^2 \mathcal{F} \otimes \mathcal{E} \otimes \det \mathcal{E}^\vee).$$

Else, we have $\mathcal{M}(\mathcal{E}, \mathcal{F}) = \emptyset$.

Again, we see that for a point $p = (p_1, \dots, p_4) \in \mathbb{Q}^4$ and $q = (q_1, \dots, q_5) \in \mathbb{Q}^5$ with $p_1 + \cdots + p_4 =$

$1/2$ and $q_1 + \dots + q_5 = 3/2$, we have

$$\lim_{g \rightarrow \infty, (p_{g,5}, q_{g,5}) \in \mathbb{Z}^9} \frac{\dim \mathcal{M}(\mathcal{E}_{p,g,5}, \mathcal{E}_{q,g,5}^\vee \otimes \det \mathcal{E}_{p,g,5})}{\dim \mathcal{H}_{5,g}} = d_{\epsilon, S_5}(p, q)$$

for ϵ sufficiently large. Again, we see that when $n = 5$, the dimensions of Maroni-Casnati-Ekedahl loci are captured, in the limit, by our density functions.

1.6 Setup

We now introduce the precise setup and notation used throughout this paper. Let $n \geq 2$ be any integer. A *rank n ring* is a commutative unital ring that is isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$ -module. We attach to any such ring R the trace function $\text{Tr}: R \rightarrow \mathbb{Z}$ which assigns to any element $\alpha \in R$ the trace of the endomorphism $R \xrightarrow{\times \alpha} R$. The discriminant $\text{Disc}(R)$ of any such ring R is defined to be the determinant $\det(\text{Tr}(\alpha_i \alpha_j)) \in \mathbb{Z}$, where $\{\alpha_i\}_{i=1}^n$ is any $\mathbb{Z}$ -basis of R . We say a ring of rank n is *nondegenerate* if its discriminant is nonzero. For a nondegenerate rank n ring R , the $\mathbb{Q}$ -algebra $R \otimes \mathbb{Q}$ is étale of degree n .

We now define the successive minima of a nondegenerate rank n ring. For any étale algebra K of degree n over $\mathbb{Q}$, denote the homomorphisms of K into $\mathbb{C}$ by $\sigma_1, \dots, \sigma_n$, and define

$$|x| := \sqrt{\frac{1}{n} \sum_{i=1}^n |\sigma_i(x)|^2}$$

for $x \in K$. Observe that $|x|$ does not depend on the ambient étale algebra containing x . Let $\mathcal{L} \subset K$ be a subgroup that is isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$ -module. The norm above gives $\mathcal{L}$ the structure of a lattice. Let $[n]$ be the set $\{0, \dots, n-1\}$. For $i \in [n]$, the *i -th successive minimum* $\lambda_i(\mathcal{L})$ of $\mathcal{L}$ is defined to be the smallest positive real number r such that $\mathcal{L}$ contains at least $i+1$ linearly independent elements of length $\leq r$. When $\mathcal{L}$ is implicit, we will refer to the i -th successive minimum of $\mathcal{L}$ by λ_i .

What constraints exist on the successive minima of rank n rings? By definition, we have that $0 \leq \lambda_0 \leq \lambda_1 \leq \dots \leq \lambda_{n-1}$. There are two additional constraints that are not too difficult to show.

Lemma 1.6.1. *For any nondegenerate rank n ring R , we have $1/\sqrt{n} \leq \lambda_0 \leq 1$. If R is an order in a number field, then $\lambda_0 = 1$.*

Proof. Note that $|1| = 1$ so $\lambda_0 \leq 1$. Suppose first that R is an order in a number field. Let $\sigma_1, \dots, \sigma_{r_1}$ be the nonzero homomorphisms of R into the real numbers and let $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$

be the nonzero homomorphisms of R into the complex numbers whose image does not lie in the real numbers. Then for any nonzero $x \in R$:

$$\begin{aligned}
|x|^2 &= \frac{1}{n} \left(\sum_{i=1}^{r_1} \sigma_i(x)^2 + \sum_{i=r_1+1}^{r_1+r_2} 2|\sigma_i(x)|^2 \right) \\
&\geq \sqrt[n]{\prod_{i=1}^{r_1} \sigma_i(x)^2 \prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|^4} && \text{by the AM-GM inequality} \\
&= \sqrt[n]{\prod_{i=1}^{r_1} \sigma_i(x)^2 \prod_{i=r_1+1}^{r_1+r_2} \sigma_i(x)^2 \overline{\sigma_i(x)}^2} \\
&= |N_{R \otimes \mathbb{Q}/\mathbb{Q}}(x)|^{2/n} \\
&\geq 1,
\end{aligned}$$

Thus, $\lambda_0 \geq 1$.

Now suppose R is any nondegenerate rank n ring. Write $R \otimes \mathbb{Q}$ as $\prod_{i=1}^t K_i$ where K_i are all fields. For any $x \in R$, write $x = (x_i) \in \prod_i K_i$. If x is nonzero then:

$$n |x|^2 = \sum_{i=1}^t \deg(K_i) |x_i|^2 \geq \sum_{i=1}^t |x_i|^2 \geq 1.$$

□

There is an additional serious constraint on successive minima of lattices, coming from Minkowski's second theorem (see [31], Lecture 10, §6), which states that

$$\prod_{i=0}^{n-1} \lambda_i \asymp_n \text{Covol}(\mathcal{L}).$$

For a nondegenerate rank n ring R , we have $\text{Covol}(R) \asymp_n |\text{Disc}(R)|$.

Chapter 2

Bounds on Successive Minima of Orders in Number Fields and Scrollar Invariants of Curves

2.1 Successive minima spectra are finite unions of polytopes

Let $\mathcal{S}$ be an infinite set of isomorphism classes of orders in degree n number fields. In this section we provide a method to construct points in $\text{Spectrum}(\mathcal{S}_n)$; we then use this construction to prove Theorem 1.1.2.

Proposition 2.1.1. *The set $\text{Spectrum}(\mathcal{S})$ is closed.*

Proof. The set $\text{Spectrum}(\mathcal{S})$ is defined to be the set of limit points of a multiset; therefore it is closed. $\square$

Definition 2.1.2. Let $\mathcal{S}$ be an infinite set of isomorphism classes of orders in degree n number fields. If

$$\lim_{\mathcal{O} \in \mathcal{S}} \left(\log_{\Delta} \lambda_1, \dots, \log_{\Delta} \lambda_{n-1} \right)$$

exists in $\mathbb{R}^{n-1}$, call the limit the *Minkowski type* of $\mathcal{S}$ and denote it by $\mathbf{x}_{\mathcal{S}}$.

Given $\mathbf{x} \in \mathbb{R}^{n-1}$, when and how can we produce a set $\mathcal{S}$ such that $\mathbf{x}_{\mathcal{S}} = \mathbf{x}$? Proposition 2.1.3 provides an explicit construction of $\mathcal{S}$ when $\mathbf{x}$ satisfies certain constraints. Let $\mathcal{B} = \{1 = v_0, v_1, \dots, v_{n-1}\}$ be a basis of a degree n number field K . For $i \in [n]$ and $v \in K$, let $\pi_{i,\mathcal{B}}(v)$ be the coefficient of

v_i in the expansion of v with respect to the basis $\mathcal{B}$. Let $\mathcal{F} = \{F_i\}_{i \in [n]}$ be the flag given by $F_i = \text{span}\{v_0, \dots, v_i\}$.

Proposition 2.1.3. *Choose $\mathbf{x} = (x_1, \dots, x_{n-1})$ to be a rational point in the relative interior of $P_{T_{\mathcal{F}}}$.*

Define $\mathcal{M}$ to the set of $M \in \mathbb{Z}_{\geq 1}$ such that $M^{x_i+x_j-x_k} \pi_{k,\mathcal{B}}(v_i v_j) \in \mathbb{Z}$ for all $i, j, k \in [n]$. Then

$$\{\mathcal{O}_M = \mathbb{Z}\langle 1, M^{x_1}v_1, \dots, M^{x_{n-1}}v_{n-1} \rangle\}_{M \in \mathcal{M}}$$

is an infinite set of isomorphism classes of orders with Minkowski type $\mathbf{x}$.

If $\mathbb{Z}\langle 1 = v_0, v_1, \dots, v_{n-1} \rangle$ is an order, then it suffices to let $\mathbf{x} = (x_1, \dots, x_{n-1})$ be a rational point in $P_{T_{\mathcal{F}}}$.

Proof. Let $x_0 = 0$. For $M \in \mathcal{M}$,

$$(M^{x_i}v_i)(M^{x_j}v_j) = \sum_{k \in [n]} M^{x_i+x_j-x_k} \pi_{k,\mathcal{B}}(v_i v_j)(M^{x_k}v_k).$$

Suppose $\mathbf{x}$ is in the relative interior of $P_{T_{\mathcal{F}}}$. Then we have $0 < x_1 < \dots < x_{n-1}$ and $x_k < x_i + x_j$ for any $1 \leq i, j, k < n$ such that $k \leq T_{\mathcal{F}}(i, j)$. For any $i, j, k \in [n]$, if $\pi_{k,\mathcal{B}}(v_i v_j) \neq 0$, then $k \leq T_{\mathcal{F}}(i, j)$ so $x_i + x_j - x_k > 0$. Because $\mathbf{x}$ is rational, $x_i + x_j - x_k$ is a positive rational number. Therefore, $\mathcal{M}$ is an infinite set.

Now suppose instead that $\mathbb{Z}\langle 1 = v_0, v_1, \dots, v_{n-1} \rangle$ is an order and $\mathbf{x} \in P_{T_{\mathcal{F}}}$. Then $\pi_{k,\mathcal{B}}(v_i v_j) \in \mathbb{Z}$ and $\pi_{k,\mathcal{B}}(v_i v_j) \neq 0$ implies $x_i + x_j - x_k \geq 0$, so $\mathcal{M}$ is an infinite set.

Because $M^{x_i+x_j-x_k} \pi_{k,\mathcal{B}}(v_i v_j) \in \mathbb{Z}$ for all $i, j, k \in [n]$, the lattice $\mathcal{O}_M$ is an order for all $M \in \mathcal{M}$. For an order $\mathcal{O}_M$, we have $\Delta_{\mathcal{O}_M} \asymp_{\mathcal{B}} M^{2(x_1+\dots+x_{n-1})} = M$. Thus, we obtain:

$$\begin{aligned} M^{1/2} &\asymp_{\mathcal{B}} \Delta_{\mathcal{O}_M}^{1/2} \\ &\asymp \prod_{i=1}^{n-1} \lambda_i(\mathcal{O}_M) && \text{by Minkowski's second theorem} \\ &\ll_{\mathcal{B}} M^{x_1+\dots+x_{n-1}} && \text{because } \lambda_i(\mathcal{O}_M) \ll_{\mathcal{B}} M^{x_i} \\ &= M^{1/2} && \text{because } x_1 + \dots + x_{n-1} = 1/2 \end{aligned}$$

This implies that:

$$\lambda_i(\mathcal{O}_M) \asymp_{\mathcal{B}} M^{x_i}.$$

Therefore,

$$\lim_{M \in \mathcal{M}} \log_{\Delta_{\mathcal{O}_M}} \lambda_i(\mathcal{O}_M) = \lim_{M \in \mathcal{M}} \log_M M^{x_i} = x_i.$$

Thus, the infinite set of isomorphism classes of orders $\{\mathcal{O}_M\}_{M \in \mathcal{M}}$ has Minkowski type $\mathbf{x}$. $\square$

The infinite set of isomorphism classes of orders constructed in Proposition 2.1.3 will be essential in proving the theorems in this paper, so we give them a name.

Definition 2.1.4. Suppose $\mathcal{B} = \{1 = v_0, \dots, v_{n-1}\}$ is a basis of a degree n number field, $\mathcal{M} \subseteq \mathbb{Z}_{\geq 1}$ is an infinite subset, and $\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1}$ satisfies $x_1 \leq \dots \leq x_{n-1}$ and $\sum_i x_i = 1/2$. Moreover, suppose that for all $M \in \mathcal{M}$, the lattice $\mathcal{O}_M = \mathbb{Z}\langle 1, M^{x_1}v_1, \dots, M^{x_{n-1}}v_{n-1} \rangle$ is an order. Then, define $\mathcal{S}(\mathcal{B}, \mathcal{M}, \mathbf{x})$ to be $\{\mathcal{O}_M\}_{M \in \mathcal{M}}$.

The infinite set $\mathcal{S}(\mathcal{B}, \mathcal{M}, \mathbf{x})$ has Minkowski type $\mathbf{x}$, as $\Delta_{\mathcal{O}_M} \asymp_{\mathcal{S}(\mathcal{B}, \mathcal{M}, \mathbf{x})} M$ and $\lambda_i(\mathcal{O}_M) \asymp_{\mathcal{S}(\mathcal{B}, \mathcal{M}, \mathbf{x})} M^{x_i}$.

Given a basis $\mathcal{B}$ of a degree n number field, for which $\mathbf{x} \in \mathbb{R}^{n-1}$ does there exist a infinite set of the form $\mathcal{S}(\mathcal{B}, \mathcal{M}, \mathbf{x})$? Proposition 2.1.3 gives sufficient conditions on $\mathbf{x}$ for an infinite set of the form $\mathcal{S}(\mathcal{B}, \mathcal{M}, \delta)$ to exist; we will now prove necessary conditions on $\mathbf{x}$.

Proposition 2.1.5. Choose a set of the form $\mathcal{S}(\mathcal{B}, \mathcal{M}, \mathbf{x})$. Let $\mathcal{F}$ be the flag arising from $\mathcal{B}$. Then $\mathbf{x} \in P_{T_{\mathcal{F}}} \cap \mathbb{Q}^{n-1}$.

Proof. Again let $x_0 = 0$. By the definition of $\mathcal{S}(\mathcal{B}, \mathcal{M}, \mathbf{x})$, we have $0 \leq x_1 \leq \dots \leq x_{n-1}$ and $\sum_i x_i = 1/2$. Write $\mathcal{B} = \{1 = v_0, \dots, v_{n-1}\}$. As $\mathbb{Z}\langle 1, M^{x_1}v_1, \dots, M^{x_{n-1}}v_{n-1} \rangle$ is a ring for all $M \in \mathcal{M}$ and

$$(M^{x_i}v_i)(M^{x_j}v_j) = \sum_{k \in [n]} M^{x_i+x_j-x_k} \pi_{k,\mathcal{B}}(v_i v_j) (M^{x_k}v_k),$$

we must have that $M^{x_i+x_j-x_k} \pi_{k,\mathcal{B}}(v_i v_j) \in \mathbb{Z}$ for all $M \in \mathcal{M}$. Thus $\mathbf{x} \in \mathbb{Q}^{n-1}$ and $x_k \leq x_i + x_j$ if $\pi_{k,\mathcal{B}}(v_i v_j) \neq 0$. $\square$

Theorem 1.1.2. We have

$$\text{Spectrum}(\mathcal{S}(G)) = \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}$$

where $\mathcal{F}$ ranges across all flags of degree n number fields with Galois group G .

Proof. Choose $\mathcal{O} \in \mathcal{S}(G)$. Choose a set of linearly independent elements $1 = v_0, \dots, v_{n-1} \in \mathcal{O}$ such that $\lambda_i(\mathcal{O}) = |v_i|$ and let $\mathcal{F}$ be the flag given by the basis. For every $1 \leq i, j < n$, we have

$$\lambda_{T_{\mathcal{F}}(i,j)}(\mathcal{O}) = |v_{T_{\mathcal{F}}(i,j)}| \leq \sqrt{n} |v_i| |v_j| = \lambda_i(\mathcal{O}) \lambda_j(\mathcal{O}).$$

Therefore, $\text{Spectrum}(\mathcal{S}(G))$ is contained in the union of polytopes $P_{T_{\mathcal{F}}}$ for every flag $\mathcal{F}$ in a degree n number field with Galois group G .

On the other hand, pick a flag $\mathcal{F}$ of a degree n number field K with Galois group G . Then there exists a basis $\{1, v_0, \dots, v_{n-1}\}$ of K giving rise to $\mathcal{F}$. For any point $\mathbf{x}$ in the relative interior of the polytope $P_{T_{\mathcal{F}}}$, Proposition 2.1.3 shows that $\mathbf{x} \in \text{Spectrum}(\mathcal{S}(G))$. By Proposition 2.1.1, $P_T \subseteq \text{Spectrum}(\mathcal{S}(G))$. $\square$

2.2 Computing the successive minima spectrum for S_n

In this section we prove Theorem 1.1.7 and Theorem 1.1.8 using some theorems from additive combinatorics and the construction discussed in the previous section.

Lemma 2.2.1 (Bachoc, Serra, Zémor [1], Theorem 2). *Let L/K be a field extension of degree n . Choose integers $0 \leq i, j, i+j < n$. Let I, J be dimension $i+1$ (resp. $j+1$) K -vector subspaces of L and suppose $\dim_K IJ \leq i+j$. Set $m = \dim_K(\text{Stab}(IJ))$ and write i and j in mixed radix notation with respect to $(m, n/m)$ as*

$$i = i_1 + i_2 m$$

$$j = j_1 + j_2 m.$$

Then $m > 1$, the addition $i+j$ overflows modulo m , $\dim_{\mathbb{Q}} \text{Stab}(IJ)I = (i_2+1)m$, $\dim_K \text{Stab}(IJ)J = (j_2+1)m$, and $\dim_K IJ = (i_2 + j_2 + 1)m$.

Theorem 1.1.8. *Choose $1 \leq i \leq j \leq i+j < n$. The following are equivalent:*

1. *the region $\text{Spectrum}(\mathcal{S}(G))$ is contained in the linear half space defined by $x_{i+j} \leq x_i + x_j$;*
2. *for any integer m that occurs as the degree of a subfield of a degree n number field of Galois group G , we have $(i \% m) + (j \% m) = (i+j) \% m$.*

Proof. By Theorem 1.1.2,

$$\text{Spectrum}(\mathcal{S}(G)) = \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}.$$

We first prove (2) $\implies$ (1). Let $\mathcal{F}$ be a flag of a degree n number field K with Galois group G . If $\dim F_i F_j > i+j$ then $T_{\mathcal{F}}(i, j) \geq i+j$ so $P_{T_{\mathcal{F}}}$ lies in the linear halfspace $x_{i+j} \leq x_i + x_j$. If $\dim F_i F_j \leq i+j$ then by Lemma 2.2.1, $\text{Stab}(F_i F_j)$ is a nontrivial subfield of K of degree m . Thus,

we may write

$$i = i_1 + i_2 m$$

$$j = j_1 + j_2 m$$

and $i_1 + j_1 < m$. So,

$$\dim F_i F_j = (i_2 + j_2 + 1)m \geq i + j + 1,$$

which is a contradiction.

Conversely, suppose condition (2) does not hold. Then there exists a number field K with Galois group G and a nontrivial proper subfield L of degree m such that $(i \% m) + (j \% m) = (i + j \% m)$. Let α be a generator of the extension $L/\mathbb{Q}$ and let β be a generator of the extension K/L . For $\ell \in [n]$, write $\ell = \ell_1 + \ell_2 m$ in mixed radix notation with respect to $(m, n/m)$; then construct a basis $\{1 = v_0, \dots, v_{n-1}\}$ of K as follows. Set $v_i = \alpha^{i_1} \beta^{i_2}$. A computation shows that the polytope $T_{\mathcal{F}}$ is not contained in the linear half space given by $x_{i+j} \leq x_i + x_j$. $\square$

Theorem 1.1.7. *If G is the symmetric group on n letters, then*

$$\text{Spectrum}(\mathcal{S}(G)) = \text{Len}(n).$$

Proof. Theorem 1.1.2 shows that

$$\text{Spectrum}(\mathcal{S}_n) = \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}$$

where $\mathcal{F}$ ranges across flags in degree n extensions K with Galois group S_n . So, it suffices to show that

$$\bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}} = \text{Len}(n).$$

Theorem 1.1.8 shows that

$$\bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}} \subseteq \text{Len}(n)$$

because a degree n number field with Galois group S_n has no nontrivial proper subfields. On the other hand, pick a basis of the form $1, \alpha, \dots, \alpha^{n-1}$ of a degree n number field K with Galois group S_n and let $\mathcal{F}$ be the corresponding flag. Then a computation shows that $P_{T_{\mathcal{F}}} = \text{Len}(n)$, so

$$\text{Len}(n) \subseteq \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}.$$

□

2.3 Bounds on scrollar invariants of curves

Let C a smooth projective geometrically irreducible curve of genus g over a field k equipped with a finite morphism $\pi: C \rightarrow \mathbb{P}^1$ of degree $n \geq 2$. Let $0 = a_0 \leq a_1 \leq a_2 \leq \dots \leq a_{n-1}$ be the unique integers such that

$$\pi_* \mathcal{O}_C \simeq \mathcal{O}_{\mathbb{P}^1}(-a_0) \oplus \mathcal{O}_{\mathbb{P}^1}(-a_1) \oplus \dots \oplus \mathcal{O}_{\mathbb{P}^1}(-a_{n-1}).$$

We say a_i is the i -th *scrollar invariant* of π . Let g be the genus of C and let G be the Galois group of π . An application of Riemann–Roch shows that:

1. $a_0 + \dots + a_{n-1} = g + n - 1$;
2. and $a_0 = 0$ and $a_i > 0$ for any $1 \leq i < n$.

Let $K(C)$ be the function field of C and let $K(\mathbb{P}^1)$ be the function field of $\mathbb{P}^1$.

Theorem 1.1.9. *We have*

$$\left(\frac{a_1}{2(g+n-1)}, \dots, \frac{a_{n-1}}{2(g+n-1)} \right) \in \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}$$

where $\mathcal{F}$ ranges across all flags of $K(C)/K(\mathbb{P}^1)$.

Proof. The multiplication map $\psi: \mathcal{O}_C \otimes \mathcal{O}_C \rightarrow \mathcal{O}_C$ induces an action map

$$\widehat{\psi}: \pi_* \mathcal{O}_C \otimes \pi_* \mathcal{O}_C \rightarrow \pi_* \mathcal{O}_C$$

via the pushforward. Let η denotes the generic point of C , let L be the function field of C , let ν be the generic point of $\mathbb{P}^1$ and let K be the function field of $\mathbb{P}^1$. The map π induces an isomorphisms

$$\phi: (\mathcal{O}_C)_{|\eta} \simeq (\pi_* \mathcal{O}_C)_{|\nu}$$

making the following diagram commutes:

$$\begin{array}{ccc} (\mathcal{O}_C)_{|\eta} \otimes (\mathcal{O}_C)_{|\eta} & \xrightarrow{\psi_{|\eta}} & (\mathcal{O}_C)_{|\eta} \\ \phi \otimes \phi \downarrow & & \downarrow \phi \\ (\pi_*(\mathcal{O}_C))_{|\nu} \otimes (\pi_*(\mathcal{O}_C))_{|\nu} & \xrightarrow{\widehat{\psi}_{|\nu}} & (\pi_* \mathcal{O}_C)_{|\nu}. \end{array}$$

The top map $(\mathcal{O}_C)_{|\eta} \otimes (\mathcal{O}_C)_{|\eta} \rightarrow (\mathcal{O}_C)_{|\eta}$ is multiplication in the field L , represented as a K -vector space, because $(\mathcal{O}_C)_{|\eta} = L$. Define the flag over K given by $\mathcal{F} = \{F_i\}_{i \in [n]}$ given by

$$F_i = \phi_1^{-1} \left(\left(\mathcal{O}_{\mathbb{P}^1}(-a_0) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(-a_i) \right)_{|\nu} \right)$$

Choose $1 \leq i \leq j \leq i+j < n$. Recall that

$$T_{\mathcal{F}}(i, j) = \min\{k \in [n] \mid F_i F_j \subseteq F_k\}.$$

Thus, there is nonzero homomorphism

$$\mathcal{O}_{\mathbb{P}^1}(-a_i) \otimes \mathcal{O}_{\mathbb{P}^1}(-a_j) \rightarrow \mathcal{O}_{\mathbb{P}^1}(-a_{T_{\mathcal{F}}(i, j)})$$

which implies that $a_{T_{\mathcal{F}}(i, j)} \leq a_i + a_j$. Thus, the point lies in $P_{T_{\mathcal{F}}}$. $\square$

Theorem 1.1.10. *Let $\mathcal{F}$ range across all flags of degree n extensions of $K(\mathbb{P}^1)$. We have*

$$\bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}} = \bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T})$$

if and only if n is a prime power, n is a product of 2 distinct primes, or $n = 12$.

Proof. This is a direct corollary of Theorem 2.7.1. $\square$

Theorem 1.1.11. *Choose $1 \leq i \leq j \leq i+j < n$. If $a_{i+j} > a_i + a_j$ then there exists an integer m such that $\pi: C \rightarrow \mathbb{P}^1$ has a subcover of degree m and $(i \% m) + (j \% m) \neq (i+j) \% m$.*

Proof. We prove the contrapositive. Suppose for all integers m that occur as degrees of subcovers of π , we have $(i \% m) + (j \% m) = (i+j) \% m$. Let $\mathcal{F}$ be a flag of $K(C)$. If $\dim F_i F_j > i+j$ then $T_{\mathcal{F}}(i, j) \geq i+j$ so $a_{i+j} \leq a_i + a_j$. If $\dim F_i F_j \leq i+j$ then by Lemma 2.2.1, $\text{Stab}(F_i F_j)$ is a nontrivial subfield of $K(C)$ of degree m . Thus, we may write

$$i = i_1 + i_2 m$$

$$j = j_1 + j_2 m$$

and $i_1 + j_1 < m$. So,

$$\dim F_i F_j = (i_2 + j_2 + 1)m \geq i + j + 1$$

which is a contradiction. $\square$

Given a line bundle $\mathcal{L}$ on C , one could define the scrollar invariants of $\mathcal{L}$ to be the numbers, in increasing order, given by the vector bundle $\pi_*(\mathcal{L})^\vee$; denote these by $a_0(\mathcal{L}), \dots, a_{n-1}(\mathcal{L})$. The proof of Theorem 1.1.11 can be generalized to show that if $a_{i+j}(\mathcal{L}) > a_i(\mathcal{O}_C) + a_j(\mathcal{L})$, then there exists an integer m such that π has a subcover of degree m and $(i \% m) + (j \% m) = (i + j) \% m$; one simply replaces the multiplication map

$$\mathcal{O} \otimes \mathcal{O} \rightarrow \mathcal{O}$$

with the multiplication map

$$\mathcal{O} \otimes \mathcal{L} \rightarrow \mathcal{L}.$$

2.4 Some theorems with exact constants

In this section, we prove a few theorems on successive minima with exact constants.

Lemma 2.4.1. *Suppose we have $x, y \in K$ for some number field K of degree n . Then $|xy| \leq \sqrt{n} |x| |y|$.*

Proof. We have

$$\begin{aligned} |xy|^2 &= \frac{1}{n} \sum_{i=1}^n |\sigma_i(xy)|^2 \\ &= \frac{1}{n} \sum_{i=1}^n |\sigma_i(x)|^2 |\sigma_i(y)|^2 \\ &\leq \frac{1}{n} \left(\sum_{i=1}^n |\sigma_i(x)|^2 \right) \left(\sum_{i=1}^n |\sigma_i(y)|^2 \right) \\ &= n \left(\frac{1}{n} \sum_{i=1}^n |\sigma_i(x)|^2 \right) \left(\frac{1}{n} \sum_{i=1}^n |\sigma_i(y)|^2 \right) \\ &= n |x|^2 |y|^2. \end{aligned}$$

$\square$

Theorem 2.4.2. *Let $1 = k_1 < k_2 < \dots < k_\ell = n$ be positive integers such that $k_s \mid n$ for all $1 \leq s \leq \ell$. Choose any integers $0 \leq i, j \leq i + j < n$. The following statements are equivalent:*

1. *There exists a number field K of degree n whose subfields have precisely the degrees $k_1, \dots, k_\ell$*

and there exists a constant $c_K \in \mathbb{R}_{>0}$ depending only on K such that

$$\lambda_{i+j}(\mathcal{O}) \leq c_K \lambda_i(\mathcal{O}) \lambda_j(\mathcal{O})$$

for every order $\mathcal{O} \subseteq K$.

2. There exists a number field K of degree n whose subfields have precisely the degrees $k_1, \dots, k_\ell$ and there exists a constant $c_K \in \mathbb{R}_{>0}$ depending only on K such that

$$\lambda_{i+j}(I) \leq c_K \lambda_i(I) \lambda_j(\mathcal{O})$$

for every order $\mathcal{O} \subseteq K$ and every fractional ideal I of $\mathcal{O}$.

3. For every order $\mathcal{O}$ in a degree n number field such that $\mathcal{O} \otimes \mathbb{Q}$ has subfields of precisely the degrees $k_1, \dots, k_\ell$, we have

$$\lambda_{i+j}(\mathcal{O}) \leq \sqrt{n} \lambda_i(\mathcal{O}) \lambda_j(\mathcal{O}).$$

4. For every order $\mathcal{O}$ in a degree n number field such that $\mathcal{O} \otimes \mathbb{Q}$ has subfields of precisely the degrees $k_1, \dots, k_\ell$ and every fractional ideal I of $\mathcal{O}$, we have

$$\lambda_{i+j}(I) \leq \sqrt{n} \lambda_i(I) \lambda_j(\mathcal{O}).$$

5. We have

$$(i \% k_s) + (j \% k_s) = (i + j) \% k_s$$

for all $1 \leq s \leq \ell$.

Proof. Clearly, (4) $\implies$ (3) $\implies$ (1) and (4) $\implies$ (2) $\implies$ (1).

We will show that (5) $\implies$ (4) by Lemma 2.2.1. Suppose that $(i \% k_s) + (j \% k_s) = (i + j) \% k_s$ for all $1 \leq s \leq t$. Let $\mathcal{O}$ be an order in a degree n field with subfields of precisely the degrees $k_1, \dots, k_\ell$. Let I be a fractional ideal of $\mathcal{O}$. Choose linearly independent elements $1 = v_0, \dots, v_{n-1} \in \mathcal{O}$ such that $\lambda_i(\mathcal{O}) = |v_i|$ and choose linearly independent elements $w_0, \dots, v_{n-1} \in I$ such that $\lambda_i(I) = |w_i|$.

By Lemma 2.2.1, $\dim_{\mathbb{Q}} \mathbb{Q}\langle 1, w_1, \dots, w_i \rangle \dim_{\mathbb{Q}} \mathbb{Q}\langle 1, v_1, \dots, v_j \rangle \geq i + j + 1$ because $(i \% k_s) + (j \% k_s) = (i + j) \% k_s$ for all $1 \leq s \leq t$. Because I is an $\mathcal{O}$ -module,

$$\lambda_{i+j}(I) \leq |w_i v_j| \leq \sqrt{n} |w_i| |v_j| = \lambda_i(I) \lambda_j(\mathcal{O}),$$

where $|w_i v_j| \leq \sqrt{n} |w_i| |v_j|$ by Lemma 2.4.1.

Now it suffices to show that (1) $\implies$ (5); pick any number field K with a nontrivial proper subfield L of degree m such that $(i \% m) + (j \% m) = (i + j \% m)$. Let α be a generator of the extension $L/\mathbb{Q}$ and let β be a generator of the extension K/L . For $\ell \in [n]$, write $\ell = \ell_1 + \ell_2 m$ in mixed radix notation; then construct a basis $\{1 = v_0, \dots, v_{n-1}\}$ of K as follows. Set $v_i = \alpha^{i_1} \beta^{i_2}$. A computation shows that the polytope $T_{\mathcal{F}}$ is not contained in the linear half space given by $x_{i+j} \leq x_i + x_j$. Choose a rational point $\mathbf{x}$ in the relative interior of $T_{\mathcal{F}}$ such that $x_{i+j} > x_i + x_j$. Then Proposition 2.1.3 gives an infinite family $\mathcal{S}$ of orders in K such that

$$\lim_{\mathcal{O} \in \mathcal{S}} \frac{\lambda_i(\mathcal{O}) \lambda_j(\mathcal{O})}{\lambda_{i+j}(\mathcal{O})} = 0.$$

□

For a number field K , let $\mathcal{S}(K)$ be the family of orders in K .

2.5 Taking logarithms of successive minima is not lossy

Let $f, f_1, \dots, f_{n-1} \in \mathbb{R}$. In this section, we prove that for “nice” families $\mathcal{S}$, the inequality

$$\Delta^f \ll_{\mathcal{S}} \lambda_1^{f_1} \dots \lambda_{n-1}^{f_{n-1}}$$

for $\mathcal{O} \in \mathcal{S}$ is equivalent to $\text{Spectrum}(\mathcal{S})$ being contained in the linear half space defined by $0 \leq f_1 x_1 + \dots + f_{n-1} x_{n-1}$, where here $x_1, \dots, x_{n-1}$ are the coordinates of $\mathbb{R}^{n-1}$. In other words, we prove that taking logarithms of successive minima is not lossy.

Theorem 2.5.1. *Choose $f, f_1, \dots, f_{n-1} \in \mathbb{R}$. The following are equivalent:*

1. *and $\text{Spectrum}(\mathcal{S}(G))$ is contained in the linear half space defined by $f \leq f_1 x_1 + \dots + f_{n-1} x_{n-1}$;*
2. *and there exists a constant $c \in \mathbb{R}_{>0}$ such that $\Delta^f \leq c \lambda_1^{f_1} \dots \lambda_{n-1}^{f_{n-1}}$ for all $\mathcal{O} \in \mathcal{S}(G)$;*

Proof. Clearly, (2) $\implies$ (1). We now prove that (1) $\implies$ (2). For every order $\mathcal{O} \in \mathcal{S}(G)$, we pick a Minkowski basis $\{1 = v_0, \dots, v_{n-1}\}$ of $\mathcal{O}$. The Minkowski basis gives rise to flag giving rise to a function $T_{\mathcal{F}}$. As we range across all orders in $\mathcal{S}(G)$, we will obtain finitely many such functions; call them $T_1, \dots, T_k$. For $1 \leq \ell \leq k$, let $\mathcal{S}_{\ell}$ be the subset of $\mathcal{S}(G)$ such that our chosen Minkowski basis

gives rise to the function T_ℓ . Then for all $\mathcal{O} \in \mathcal{S}_\ell$ and all $1 \leq i, j < n$, we have

$$\lambda_{T_\ell(i,j)}(\mathcal{O}) \ll_n \lambda_i(\mathcal{O}) \lambda_j(\mathcal{O}) \quad (2.1)$$

so $\text{Spectrum}(\mathcal{S}_\ell) \subseteq P_{T_\ell}$. Applying the construction in Proposition 2.1.3 to the chosen Minkowski basis shows that the relative interior of P_{T_ℓ} is contained in $\text{Spectrum}(\mathcal{S}_\ell)$. Proposition 2.1.1 implies that $\text{Spectrum}(\mathcal{S}_\ell)$ is closed, which implies that $\text{Spectrum}(\mathcal{S}_\ell) = P_{T_\ell}$.

Fix ℓ . Assume $\text{Spectrum}(\mathcal{S}_\ell)$ is contained in the linear half space defined by $f \leq f_1 x_1 + \dots + f_{n-1} x_{n-1}$. It suffices to show that $c_\ell \in \mathbb{R}_{>0}$ such that $\Delta^f \leq c_\ell \lambda_1^{f_1} \dots \lambda_{n-1}^{f_{n-1}}$ for all $\mathcal{O} \in \mathcal{S}_\ell$. To this end, recall that the defining equations of T_ℓ are:

1. $x_1 + \dots + x_{n-1} = 1/2$;
2. $0 \leq x_1 \leq \dots \leq x_{n-1}$;
3. and $x_{T_\ell(i,j)} \leq x_i + x_j$ for all i, j .

Analogously, define the following affine linear functions on $\mathbb{R}^n$:

1. $p(\mathbf{x}) = x_1 + \dots + x_{n-1} - 1/2$;
2. $q_1(\mathbf{x}) = x_1$ and $q_i(x) = x_i - x_{i-1}$ for $1 < i < n$;
3. and $r_{i,j}(\mathbf{x}) = x_i + x_j - x_{T_\ell(i,j)}$ for all $1 \leq i, j < n$.

Let $s(\mathbf{x}) = f_1 x_1 + \dots + f_{n-1} x_{n-1} - f$. Then we because T_ℓ is in contained in the linear half space defined by $f \leq f_1 x_1 + \dots + f_{n-1} x_{n-1}$, we can write

$$s(\mathbf{x}) = c_p p(\mathbf{x}) + \sum_{1 \leq i < n} c_{q,i} q_i(\mathbf{x}) + \sum_{1 \leq i, j < n} c_{r,i,j} r_{i,j}(\mathbf{x})$$

where c_p is a real number and all the $c_{q,i}$ and $c_{r,i,j}$ are nonnegative real numbers. Then, for any $\mathcal{O} \in \mathcal{S}_i$, we may write

1. $\Delta^{1/2} \ll_{c_p} (\lambda_1 \dots \lambda_{n-1})^{c_p}$ due to Minkowski's second theorem;
2. $1 \leq \lambda_1^{c_{q,1}}$ and $1 \leq \lambda_i^{c_{q,i}} \lambda_{i-1}^{c_{q,i}}$ for $1 < i < n$;
3. and $1 \ll_{c_{r,i,j}} \lambda_i^{c_{r,i,j}} \lambda_j^{c_{r,i,j}} \lambda_{T_\ell(i,j)}^{c_{r,i,j}}$ for all $1 \leq i, j < n$ due to (2.1).

Multiplying these inequalities out gives

$$\Delta^f \ll \lambda_1^{f_1} \dots \lambda_{n-1}^{f_{n-1}}$$

as we range across $\mathcal{O} \in \mathcal{S}_\ell$. □

2.6 The polytopes associated to a flag type T

In this section we discuss the polytopes associated to a flag type and prove some crucial lemmas.

Let T be any flag type of degree n . In this section, we will prove Theorem 2.6.5.

Definition 2.6.1. A *flag type of degree n* is a function $T: [n] \times [n] \rightarrow [n]$ such that for any $i, j \in [n]$, we have:

1. $T(i, j) = T(j, i)$;
2. $T(i, 0) = i$;
3. and $T(i, j) \leq T(i + 1, j)$ if $i < n - 1$.

Definition 2.6.2. Let P_T be the set of $\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1}$ such that $x_1 + \dots + x_{n-1} = 1/2$ and $0 \leq x_1 \leq \dots \leq x_{n-1}$ and $x_{T(i,j)} \leq x_i + x_j$ for all $1 \leq i, j < n$.

Proposition 2.6.3. *The set P_T is a bounded polyhedron of dimension $n - 2$.*

Proof. We will show that P_T has dimension $n - 2$ by producing $n - 1$ linearly independent points in the cone over P_T . For $i \in [n - 1]$, define $\mathbf{x}^i = (x_1^i, \dots, x_{n-1}^i) \in \mathbb{R}^{n-1}$ by

$$\begin{aligned} x_1^i &= \dots = x_i^i = 1 \\ x_{i+1}^i &= \dots = x_{n-1}^i = 2 \end{aligned}$$

It is easy to verify that $\mathbf{x}^i$ is in the cone over P_T . The $(n - 1) \times (n - 1)$ matrix whose rows consist of the $(n - 1)$ -tuples $x^0, \dots, x^{n-2}$ has rank $(n - 1)$; this can be seen via elementary row and column operations. □

Definition 2.6.4. For $0 < i, j < n$, say (i, j) is a *corner* of T if $T(i - 1, j) < T(i, j)$ and $T(i, j - 1) < T(i, j)$.

Theorem 2.6.5. *For $i, j, k \in [n]$, the inequality $x_k \leq x_i + x_j$ defines a facet of P_T if and only if (i, j) is a corner and $T(i, j) = k$.*

Proof. Suppose (i, j) is not a corner of T . Then, there exists a corner (i', j') with $i' \leq i$, $j' \leq j$ and $T(i', j') = T(i, j)$. We will show that $x_{T(i,j)} \leq x_i + x_j$ does not define a facet of P_T by showing that

$P_T \cap \{\mathbf{x} \in \mathbb{R}^{n-1} \mid x_{T(i,j)} = x_{i'} + x_{j'}\}$ strictly contains $P_T \cap \{\mathbf{x} \in \mathbb{R}^{n-1} \mid x_{T(i,j)} = x_i + x_j\}$. In other words, we will produce $\mathbf{x}$ in the cone over P_T with $x_{T(i,j)} = x_{i'} + x_{j'} \neq x_i + x_j$.

If $i' \neq j'$, set $\mathbf{x} = (x_1, \dots, x_{n-1})$ where

$$\begin{aligned} x_1, \dots, x_{i'} &= 2 \\ x_{i'+1}, \dots, x_{j'} &= 3 \\ x_{j'+1}, \dots, x_{T(i,j)-1} &= 4 \\ x_{T(i,j)}, \dots, x_{n-1} &= 5. \end{aligned}$$

If $i' = j'$, set $\mathbf{x} = (x_1, \dots, x_{n-1})$ where

$$\begin{aligned} x_1, \dots, x_{i'} &= 2 \\ x_{i'+1}, \dots, x_{T(i,j)-1} &= 3 \\ x_{T(i,j)}, \dots, x_{n-1} &= 4. \end{aligned}$$

A computation verifies that $x_{T(i,j)} = x_{i'} + x_{j'} \neq x_i + x_j$, and $\mathbf{x}$ is in the cone over P_T . Therefore, P_T is the set of $\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1}$ such that $x_1 + \dots + x_{n-1}$, $0 \leq x_1 \leq \dots \leq x_{n-1}$, and $x_{T(i,j)} \leq x_i + x_j$ for all corners (i, j) of T . Now, suppose (i, j) is a corner of T . To show that $x_{T(i,j)} \leq x_i + x_j$ defines a facet of P_T , it suffices to produce a point $\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1}$ such that $0 \leq x_1 \leq \dots \leq x_{n-1}$, and $x_{T(i,j)} > x_i + x_j$ and $x_{T(i',j')} \leq x_{i'} + x_{j'}$ for any other corner (i', j') .

Set $\mathbf{x} = (x_1, \dots, x_{n-1})$ where If $i \neq j$, set $\mathbf{x} = (x_1, \dots, x_{n-1})$ where

$$\begin{aligned} x_1, \dots, x_i &= 2 \\ x_{i+1}, \dots, x_j &= 3 \\ x_{j+1}, \dots, x_{T(i,j)-1} &= 4 \\ x_{T(i,j)}, \dots, x_{n-1} &= 6. \end{aligned}$$

If $i = j$, set $\mathbf{x} = (x_1, \dots, x_{n-1})$ where

$$\begin{aligned} x_1, \dots, x_i &= 2 \\ x_{i+1}, \dots, x_{T(i,j)-1} &= 3 \\ x_{T(i,j)}, \dots, x_{n-1} &= 5. \end{aligned}$$

A computation verifies that $\mathbf{x}$ satisfies the necessary conditions. $\square$

We define a partial ordering $\leq$ on the set of flag types. For any two flag types T and T' , say $T \leq T'$ if $T(i, j) \leq T'(i, j)$ for all $i, j \in [n]$. We obtain the following lemma.

Lemma 2.6.6. *The map from flag types to polyhedra sending T to P_T is an injection.*

So, the poset of polyhedra P_T is canonically dual to the poset of flag types.

Proof. A flag type is determined by its corners, and a polyhedra is determined by its facets. Apply Theorem 2.6.5 to complete the proof. $\square$

Fix a tower type $\mathfrak{T} = (n_1, \dots, n_t)$. Let $\alpha_1, \dots, \alpha_{t-1}$ be a sequence of algebraic numbers such that $[\mathbb{Q}(\alpha_1, \dots, \alpha_\ell) : \mathbb{Q}(\alpha_1, \dots, \alpha_{\ell-1})] = n_\ell$ for $1 \leq \ell \leq t$. Write $i = i_1 + i_2(n_1) + i_3(n_1n_2) + \dots + i_t(n_1 \dots n_{t-1})$ in mixed radix notation with respect to $(n_1, \dots, n_t)$ and define a basis $1 = v_0, \dots, v_{n-1}$ of $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$ as follows; set $v_i = \alpha_1^{i_1} \dots \alpha_t^{i_t}$. Define the flag $\mathcal{F}(\mathfrak{T}) = \{F_i\}_{i \in [n]}$ by $F_i = \{v_0, \dots, v_i\}$.

Definition 2.6.7. Let $T(\mathfrak{T})$ be the flag type of $\mathcal{F}(\mathfrak{T})$.

Observe that $\text{Len}(\mathfrak{T}) = P_{T(\mathfrak{T})}$.

Corollary 2.6.8. *For any tower type $\mathfrak{T}$ and $0 \leq i, j, i + j < n$, the following are equivalent:*

1. $i + j$ does not overflow modulo $\mathfrak{T}$;
2. (i, j) is a corner of $\text{Len}(\mathfrak{T})$;
3. and $T(\mathfrak{T})(i, j) = i + j$.

Proof. This follows from the definition of $T(\mathfrak{T})$. $\square$

We may compare flag types using corners.

Lemma 2.6.9. *For any two flag types T and T' such that $T \not\preceq T'$, there exists a corner (i, j) of T' such that $T(i, j) < T'(i, j)$.*

Proof. Because $T \not\preceq T'$, we have $P_T \not\subseteq P_{T'}$. Thus, there exists integers $1 \leq i, j < n$ such that

$$P_{T'} \subset \{\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1} \mid x_{T'(i,j)} \leq x_i + x_j\},$$

$$P_{T'} \not\subset \{\mathbf{x} = (x_1, \dots, x_{n-1}) \in \mathbb{R}^{n-1} \mid x_{T'(i,j)} \leq x_i + x_j\},$$

and the linear inequality $x_{T'(i,j)} \leq x_i + x_j$ defines a facet of $P_{T'}$. Thus Theorem 2.6.5, there exists a corner (i, j) of T' such that $P_T \cap \{\mathbf{x} \in \mathbb{R}^{n-1} \mid x_{T'(i,j)} > x_i + x_j\} \neq \emptyset$. Because $P_T \subseteq \{\mathbf{x} \in \mathbb{R}^{n-1} \mid x_{T(i,j)} \leq x_i + x_j\}$, we have $T(i, j) < T'(i, j)$. $\square$

The following statement will be useful.

Theorem 2.6.10 (Bachoc, Serra, Zémor [1], Theorem 2). *For all field extensions L/K and nonempty K -subvector spaces $A, B \subseteq L$ of positive finite dimension, we have*

$$\dim_K AB \geq \dim_K A + \dim_K B - \dim_K \text{Stab}(AB).$$

Theorem 2.6.11. *For a flag $\mathcal{F}$ and every corner (i, j) of $T_{\mathcal{F}}$, we have $T_{\mathcal{F}}(i, j) \geq i + j$.*

Proof. Let (i, j) be a corner of T and suppose for the sake of contradiction that $T(i, j) < i + j$.

$$F_i F_{j-1} = F_i F_j$$

which would imply that (i, j) is not a corner.

To this end, set $M = \text{Stab}(F_i F_j)$ and $m = \dim \text{Stab}(M)$. Note that $m > 1$. Write i and j in mixed radix notation with respect to $(m, n/m)$ as $i = \alpha_1 + \alpha_2 m$ and $j = \beta_1 + \beta_2 m$ and note that $\alpha_1 + \beta_1 > m$ (because $k \neq i + j$). Thus, $\beta_1 \neq 1$.

Note that $m^{-1} \dim M F_{j-1} \geq \lceil j/m \rceil = \beta_2 + 1$ and $m^{-1} \dim M F_j = \beta_2 + 1$, so

$$M F_{j-1} = M F_j.$$

Note that $\text{Stab}(M F_i M F_{j-1}) = M$. Define

$$M' = \text{Stab}(F_i F_{j-1})$$

and set $m' = \dim M'$. Note that because

$$\text{Stab}(F_i F_{j-1}) \subseteq \text{Stab}(M F_i M F_{j-1}),$$

we have $M' \subseteq M$ and thus $m' \mid m$.

First suppose $\alpha_1 + \beta_1 - 1 - m < m'$. By Theorem 2.6.10, we have

$$\dim F_i F_{j-1} = (\alpha_1 + \beta_1 + 1)m$$

and thus

$$F_i F_{j-1} = F_i F_j.$$

Now suppose $\alpha_1 + \beta_1 - 1 - m \geq m'$. If $M' \neq M$, then

$$\dim F_i F_{j-1} > \dim F_i F_j,$$

which is a contradiction. Thus we must have $M' = M$ so by Theorem 2.6.10, we have

$$\dim F_i F_{j-1} = (\alpha_1 + \beta_1 + 1)m$$

and thus $F_i F_{j-1} = F_i F_j$. Thus, we have a contradiction so $k \geq i + j$. $\square$

We say a flag type is *realizable* if it arises from a flag of a field extension. We say it is *realizable over K* if it arises from a flag of a field extension of K . In contrast to Theorem 2.6.11, there exist realizable flag types T with a corner (i, j) such that $T(i + j) > i + j$.

Remark 2.6.12. For a tower type $\mathfrak{T} = (n_1, \dots, n_t)$, we denote the tower type $T(\mathfrak{T}) = T((n_1, \dots, n_t))$ by $T(n_1, \dots, n_t)$. When $t = 2$, we caution the reader to not confuse $T(n_1, n_2)$ with *evaluating* some flag type T at the numbers n_1 and n_2 .

2.7 The successive minima spectrum when n is a prime power, a product of two primes, or 12

Theorem 1.1.6. *We have*

$$\text{Spectrum}(\mathcal{S}_n) = \bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T})$$

where $\mathfrak{T}$ ranges across tower types of degree n if and only if n is a prime power, n is a product of 2 distinct primes, or $n = 12$.

Proof. Theorem 1.1.2 shows that

$$\text{Spectrum}(\mathcal{S}_n) = \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}.$$

So, it suffices to show that

$$\bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}} = \bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T}).$$

This is precisely the content of Theorem 2.7.1. □

In this following two sections, we prove the following theorem. Let K be a field with extensions of all finite degrees.

Theorem 2.7.1. *We have*

$$\bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T}) = \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}$$

as $\mathcal{F}$ ranges across flags over K if and only if n is a prime power, n is a product of 2 distinct primes, or $n = 12$.

Proof. Combine Lemma 2.7.2 and Theorem 2.8.1. □

The rest of this section is dedicated to proving Lemma 2.7.2. The next section will prove Theorem 2.8.1.

Lemma 2.7.2. *If n is a prime power, n is a product of 2 primes, or $n = 12$ then*

$$\bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T}) = \bigcup_{\mathcal{F}} P_{T_{\mathcal{F}}}$$

as $\mathcal{F}$ ranges across flags over K .

Proof. We separate into the following cases:

1. for $n = p^k$ for p prime and $k \geq 1$, apply Proposition 2.7.5;
2. for $n = 2p$ for p an odd prime, apply Proposition 2.7.3;
3. for $n = pq$ for p and q distinct odd primes, apply Proposition 2.7.4;
4. and for $n = 12$, apply Proposition 2.7.6.

□

The rest of this section is devoted to proving Proposition 2.7.3, Proposition 2.7.4, Proposition 2.7.5, and Proposition 2.7.6. We will first need the following definitions.

Proposition 2.7.3. *Suppose $n = 2p$ for p an odd prime. For every realizable flag type T , we have $T \geq T(2, p)$ or $T \geq T(p, 2)$.*

Proof. Assume for the sake of contradiction that there exists a flag $\mathcal{F}$ of K such that $T_{\mathcal{F}} \not\geq T(p, 2)$ and $T_{\mathcal{F}} \not\geq T(2, p)$. By Lemma 2.6.9, there exists integers $0 < i_2 \leq j_2 < i_2 + j_2 < 2p$ such that $i_2 + j_2$ does not overflow modulo $(p, 2)$ and $T_{\mathcal{F}}(i_2, j_2) < i_2 + j_2$. By Lemma 2.2.1 we must have that $F_{i_2} + F_{j_2}$ overflows modulo 2. Moreover,

$$\dim \text{Stab}(F_{i_2}F_{j_2})F_{i_2} = \dim F_{i_2}.$$

Hence F_{i_2} is a vector space over $\text{Stab}(F_{i_2}F_{j_2})$ and $\text{Stab}(F_{i_2}F_{j_2})$ is a quadratic field.

Similarly, because $T_{\mathcal{F}} \not\geq T(2, p)$, there must exist integers $0 < i_p \leq j_p < i_p + j_p < 2p$ such that $i_p + j_p$ does not overflow modulo $(2, p)$ and $T_{\mathcal{F}}(i_p, j_p) < i_p + j_p$. Again, by Lemma 2.2.1 we must have that $i_p + j_p$ overflows modulo p and $\text{Stab}(F_{i_p}F_{j_p})$ is a field of degree p ; therefore $F_{i_p}F_{j_p} \neq K$; therefore F_{j_p} is contained in the degree p field $\text{Stab}(F_{i_p}F_{j_p})$.

Because F_{i_2} is a vector space over a quadratic field, it cannot be contained in a degree p field. Therefore, we must have $F_{j_p} \subseteq F_{i_2}$ and hence

$$\begin{aligned} i_2 + 1 &= \dim F_{i_2} \\ &= \dim \text{Stab}(F_{i_2}F_{j_2})F_{i_2} \\ &\geq \dim \text{Stab}(F_{i_2}F_{j_2})F_{j_p} \\ &= 2\left(\frac{p+1}{2} + 1\right) = p + 3. \end{aligned}$$

The last step is because $j_p \geq \frac{p+1}{2}$ and F_{j_p} is contained in a degree p field. Thus $i_2 + j_2 \geq 2p$, which is a contradiction. $\square$

Proposition 2.7.4. *Suppose $n = pq$ for p and q distinct odd primes. Then for every realizable flag type T , we have $T \geq T(p, q)$ or $T \geq T(q, p)$.*

Proof. Assume for the sake of contradiction that there exists a flag $\mathcal{F}$ of K such that $T_{\mathcal{F}} \not\geq T(p, q)$ and $T_{\mathcal{F}} \not\geq T(q, p)$. By Lemma 2.6.9, there exists integers $0 < i_q \leq j_q < i_q + j_q < pq$ such that $i_q + j_q$ does not overflow modulo (p, q) , but $T_{\mathcal{F}}(i_q, j_q) > i_q + j_q$. By Lemma 2.2.1 we must have that $i_q + j_q$ overflows modulo q and $K_q = \text{Stab}(F_{i_q}F_{j_q})$ is a group of order q .

Similarly, because $T_{\mathcal{F}} \not\geq T(q, p)$, there must exist integers $0 < i_p \leq j_p < i_p + j_p < pq$ such that $i_p + j_p$ does not overflow modulo (q, p) , but $T(i_p, j_p) > i_p + j_p$. By Lemma 2.2.1 we must have that $i_p + j_p$ overflows modulo q and $K_p = \text{Stab}(F_{i_p} F_{j_p})$ is a field of degree p .

If $i_q \leq i_p$ and $j_q \leq j_p$ then

$$K_q \subseteq F_{i_q} F_{j_q} \subseteq F_{i_p} F_{j_p},$$

and because $F_{i_p} F_{j_p}$ is a K_p -vector space, we have

$$K = K_p K_q \subseteq F_{i_p} F_{j_p},$$

which is a contradiction. Similarly, it is not possible for $i_p \leq i_q$ and $j_p \leq j_q$. Hence without loss of generality we may suppose $i_p \leq i_q \leq j_q \leq j_p$. Write i_p and j_p in mixed radix notation with respect to (p, q) and write i_q and j_q in mixed radix notation with respect to (q, p) as

$$i_p = i_{1,p}p + i_{2,p}$$

$$j_p = j_{1,p}p + j_{2,p}$$

$$i_q = i_{1,q}q + i_{2,q}$$

$$j_q = j_{1,q}q + j_{2,q}.$$

By Lemma 2.2.1, we have that

$$\dim K_p F_{i_p} = (\dim K_p)(i_{1,p} + 1)$$

$$\dim K_p F_{j_p} = (\dim K_p)(j_{1,p} + 1)$$

$$\dim K_q F_{i_q} = (\dim K_q)(i_{1,q} + 1)$$

$$\dim K_q F_{j_q} = (\dim K_q)(j_{1,q} + 1).$$

Note that

$$i_q + 1 = \dim F_{i_q} \leq \frac{\dim K_q F_{i_q}}{\dim K_q} \frac{\dim K_p F_{i_q}}{\dim K_p} \leq (i_{1,q} + 1) \frac{\dim K_p F_{j_p}}{\dim K_p} = (i_{1,q} + 1)(j_{1,p} + 1)$$

$$j_q + 1 = \dim F_{j_q} \leq \frac{\dim K_q F_{j_q}}{\dim K_q} \frac{\dim K_p F_{j_q}}{\dim K_p} \leq (j_{1,q} + 1) \frac{\dim K_p F_{j_p}}{\dim K_p} = (j_{1,q} + 1)(j_{1,p} + 1).$$

Thus

$$\begin{aligned}
i_q + j_q &< (i_{1,q} + 1)(j_{1,p} + 1) + (j_{1,q} + 1)(j_{1,p} + 1) \\
&= (i_{1,q} + j_{1,q} + 2)(j_{1,p} + 1) \\
&\leq p(j_{1,p} + 1) \\
&\leq j_p.
\end{aligned}$$

Because $i_q + j_q \leq j_p$, we have $K_q \subseteq F_{i_q+j_q-1} \subseteq F_{j_p}$ and because $F_{i_p}F_{j_p}$ is a K_p -vector space, we have

$$K = K_q K_p \subseteq F_{i_p} F_{j_p},$$

which is a contradiction. $\square$

Proposition 2.7.5. *Suppose $n = p^k$ for p and odd prime and $k \geq 1$. Then for every realizable flag type T , we have $T \geq T(p, \dots, p)$.*

Proof. Suppose there exists a realizable flag type T such that $T_{\mathcal{F}} \not\geq T(p, \dots, p)$. By Lemma 2.6.9, there exists integers $0 < i \leq j < n$ such that $i + j$ does not overflow modulo $(p, \dots, p)$ and $T(i, j) < i + j$. By Lemma 2.2.1, $i + j$ must overflow over some positive integer m such that $m \mid p^k$, which is a contradiction. $\square$

Proposition 2.7.6. *Suppose $n = 12$. Then for every realizable flag type T , we have $T \geq T(3, 2, 2)$ or $T \geq T(2, 3, 2)$ or $T \geq T(2, 2, 3)$.*

Proof. Assume for the sake of contradiction that there exists a flag $\mathcal{F}$ over K such that $T_{\mathcal{F}} \not\geq T(3, 2, 2)$, $T_{\mathcal{F}} \not\geq T(2, 3, 2)$, and $T_{\mathcal{F}} \not\geq T(2, 2, 3)$. By Lemma 2.6.9, there exists $i_1, i_2, i_3, j_1, j_2, j_3$ such that

$$\begin{aligned}
0 &< i_1 \leq j_1 < i_1 + j_1 < 12 \\
0 &< i_2 \leq j_2 < i_2 + j_2 < 12 \\
0 &< i_3 \leq j_3 < i_3 + j_3 < 12,
\end{aligned}$$

and $i_1 + j_1$ (resp. $i_2 + j_2$, $i_3 + j_3$) does not overflow modulo $(3, 2, 2)$ (resp. $(2, 3, 2)$, $(2, 2, 3)$), and

$$T_{\mathcal{F}}(i_1 + j_1) > i_1 + j_1$$

$$T_{\mathcal{F}}(i_2 + j_2) > i_2 + j_2$$

$$T_{\mathcal{F}}(i_3 + j_3) > i_3 + j_3.$$

By Lemma 2.2.1 we have that

$$K_1 = \text{Stab}(F_{i_1}F_{j_1})$$

$$K_2 = \text{Stab}(F_{i_2}F_{j_2})$$

$$K_3 = \text{Stab}(F_{i_3}F_{j_3})$$

are a nontrivial proper subgroups; let $m_1 = \dim K_1$, let $m_2 = \dim K_2$, and let $m_3 = \dim K_3$.

The list of possible triples (i_1, j_1, m_1) for which $0 < i_1 \leq j_1 < i_1 + j_1 < 12$, the addition $i_1 + j_1$ overflows modulo m_1 , we have $1 < m_1 < 12$, we have $m_1 \mid 12$, and the addition $i_1 + j_1$ does not overflow modulo $(3, 2, 2)$ is

$$\{(1, 1, 2), (1, 3, 2), (1, 3, 4), (1, 7, 2), (1, 7, 4), (1, 9, 2), (2, 3, 4), (2, 6, 4), (3, 6, 4), (3, 7, 2), (3, 7, 4)\}.$$

The list of possible triples (i_2, j_2, m_2) for which $0 < i_2 \leq j_2 < i_2 + j_2 < 12$, the addition $i_2 + j_2$ overflows modulo m_2 , we have $1 < m_2 < 12$, we have $m_2 \mid 12$, and the addition $i_2 + j_2$ does not overflow modulo $(2, 3, 2)$ is

$$\{(1, 2, 3), (1, 8, 3), (2, 2, 3), (2, 2, 4), (2, 3, 4), (2, 6, 4), (2, 7, 3), (2, 7, 4), (2, 8, 3), (3, 6, 4)\}.$$

The list of possible triples (i_3, j_3, m_3) for which $0 < i_3 \leq j_3 < i_3 + j_3 < 12$, the addition $i_3 + j_3$ overflows modulo m_3 , we have $1 < m_3 < 12$, we have $m_3 \mid 12$, and the addition $i_3 + j_3$ does not overflow modulo $(2, 2, 3)$ is

$$\{(1, 2, 3), (1, 8, 3), (2, 4, 3), (2, 4, 6), (2, 5, 3), (2, 5, 6), (2, 8, 3), (3, 4, 6), (4, 4, 6), (4, 5, 3), (4, 5, 6)\}.$$

We will show that every combination of integers (i_1, j_1, m_1) , (i_2, j_2, m_2) , and (i_3, j_3, m_3) from the lists above give rise to a contradiction.

Then because $i_1 < m_1$, by Lemma 2.2.1, we have $K_1 F_{i_1} = K_1$ so $F_{i_1} \subseteq K_1$. Write $F_1 = \{1, v_1\}$.

Then $\deg(v_1) \mid m_1 \mid 4$.

If $\deg(v_1) = 4$ then as $\deg(v_1) \mid m_1 \mid 4$, we have that $m_1 = 4$. If $i_3 < m_3$ then $F_{i_3} \subseteq K_3$ and thus $\deg(v_1) \mid m_3 \mid 6$, which is a contradiction. Hence $i_3 > m_3$ so we must have $m_3 = 3$ and $i_3 = 4$ and $j_3 = 5$. Moreover, by Lemma 2.2.1, $\dim K_3 F_5 = 2 \dim K_3$. Because $m_1 = 4$ and $m_3 = 3$ are coprime, we have $F_{i_1} \subseteq K_1$ and

$$i_1 + 1 = \dim F_{i_1} = \frac{\dim K_3 F_{i_1}}{\dim K_3} \leq \frac{\dim K_3 F_5}{\dim K_3} = 2,$$

which is a contradiction.

Thus $\deg(v_1) = 2$, and therefore without loss of generality we may suppose $i_1 = j_1 = 1$ and $m_1 = 2$, as $\deg(v_1) = 2$ implies that

$$F_1 F_1 = F_1.$$

Notice that $i_2 < m_2$, so $F_{i_2} \subseteq K_2$ and thus $\deg(v_1) = 2 \mid \deg(K_2)$; hence $m_2 = 4$.

If $m_3 = 3$, then if $i_3 < m_3$ we have $F_{i_3} \subseteq K_3$ and thus $\deg(v_1) \mid K_3 \mid 3$, which is a contradiction.

Thus $i_3 > m_3$, so $i_3 = 4$ and $j_3 = 5$. By Lemma 2.2.1, $|K_3 F_5| = 2 |K_3|$; thus

$$F_5 = K_3 F_1$$

is a group of order 6. However,

$$\begin{aligned} K_3 F_1 &= \text{Stab}(F_5) \\ &\subseteq \text{Stab}(F_4 F_5) \\ &= K_3, \end{aligned}$$

which is a contradiction.

Hence, $m_3 = 6$. Because $i_2 < m_2$ and $i_3 < m_3$ and $2 \leq i_2, i_3$, we have $F_2 \subseteq K_2 \cap K_3$, which is a contradiction, because

$$|K_2 \cap K_3| \leq \gcd(m_2, m_3) = \gcd(4, 6) = 2.$$

□

2.8 The successive minima spectrum when n is not a prime power, a product of two primes, or 12

In this section, we prove Theorem 2.8.1.

Theorem 2.8.1. *Suppose n is not of the following form:*

1. $n = p^k$, with p prime and $k \geq 1$;
2. $n = pq$, with p and q distinct primes;
3. or $n = 12$.

Then there exists a flag type T , realizable over $\mathbb{Q}$, such that

$$P_T \not\subseteq \bigcup_{\mathfrak{T}} \text{Len}(\mathfrak{T}).$$

Proof. By Lemma 2.8.2, proving the statement of Theorem 2.8.1 for degree n implies the statement of Theorem 2.8.1 for degree nt for any positive integer t . Therefore, it suffices to prove the theorem when:

1. $n = p^2q$ for two distinct odd primes p and q with $p < q$, in which case Proposition 2.8.3 provides a proof;
2. $n = pqr$ for three primes p , q , and r with $p < q \leq r$, in which case Proposition 2.8.6 provides a proof;
3. $n = 4p$ for a prime $p \neq 2, 3$, in which case Proposition 2.8.7 provides a proof;
4. or $n = 24$, in which case Proposition 2.8.8 provides a proof.

□

The rest of this section is dedicated to proving Lemma 2.8.2, Proposition 2.8.3, Proposition 2.8.6, Proposition 2.8.7, and Proposition 2.8.8.

Lemma 2.8.2. *Let $n, m \in \mathbb{Z}_{>1}$ be such that $m \mid n$. If there exists a realizable flag type T of degree m such that*

$$P_T \not\subseteq \bigcup_{(p_1, \dots, p_t)} \text{Len}(p_1, \dots, p_t)$$

where $(p_1, \dots, p_t)$ range across all tuples with prime entries such that $p_1 \dots p_t = m$, then there exists a realizable flag type T' of degree n such that

$$P_{T'} \not\subseteq \bigcup_{(p'_1, \dots, p'_t)} \text{Len}(p'_1, \dots, p'_t)$$

where $(p'_1, \dots, p'_t)$ range across all tuples with prime entries such that $p'_1 \dots p'_t = n$.

Proof. The polyhedron P_T has dimension $m - 2$. Therefore, the set

$$S = \left(P_T \setminus \bigcup_{(p_1, \dots, p_t)} \text{Len}(p_1, \dots, p_t) \right) \cap \{ \mathbf{x} \in \mathbb{R}^{m-1} \mid x_k \neq x_i + x_j \ \forall \ 1 \leq i, j, k < m \}$$

is nonempty.

Let K be a field of degree m with a flag $\mathcal{F}$ realizing T . Let $\{v_0, \dots, v_{m-1}\}$ be a sequence of elements in K such that $F_i = \text{span}(v_0, \dots, v_i)$.

Let L be a degree p extension of K . Let α be a generator of L/K . Define the sequence $\{1 = v'_0, \dots, v'_{n-1}\}$ by $v'_i = v_{i_2} \alpha^{i_1}$ for $i = i_1 + i_2 p$ in mixed radix notation with respect to (p, m) . Define a flag $\mathcal{F}' = (F'_i)_{i \in [n]}$ of G' by $F'_i = \text{span}(v'_0, \dots, v'_i)$.

Choose $\mathbf{x} = (x_1, \dots, x_{m-1}) \in S$. Let

$$\epsilon = \min_{1 \leq i < m-1} \{x_{i+1} - x_i\}$$

and note that $\epsilon \neq 0$. Define the point $\mathbf{x}' = (x'_1, \dots, x'_{n-1}) \in \mathbb{R}^{n-1}$ by

$$x'_i = \epsilon \frac{i_1}{2p} + x_{i_2}.$$

We will show that $\mathbf{x}' \in P_{T'}$. We first show that $0 \leq x'_1 \leq \dots \leq x'_{mp-1}$. For $1 \leq i < n-1$, write $i = i_1 + i_2 p$ in mixed radix notation with respect to (p, m) . If $i_1 \neq p-1$, then

$$x'_{i+1} = \epsilon \frac{i_1 + 1}{2p} + x_{i_2} \geq \epsilon \frac{i_1}{2p} + x_{i_2} = x'_i.$$

If $i_1 = p-1$ then

$$x'_{i+1} = x_{i_2+1} \geq \epsilon + x_{i_2} \geq \epsilon \frac{i_1}{2p} + x_{i_2} = x'_i.$$

For any $1 \leq i, j, k < n$, we now show that $x'_{T_{\mathcal{F}'}(i,j)} \leq x'_i + x'_j$. Let $k = T_{\mathcal{F}'}(i, j)$. Write

$$\begin{aligned} i &= i_1 + i_2 p \\ j &= j_1 + j_2 p \\ k &= k_1 + k_2 p \end{aligned}$$

in mixed radix notation with respect to (p, m) . Then we have $k_1 \leq i_1 + j_1$ so $x_{k_2} \leq x_{i_2} + x_{j_2}$. Then

$$\begin{aligned} x'_k &= \epsilon \frac{k_1}{2p} + x_{k_2} \\ &\leq \epsilon \frac{k_1}{2p} + x_{k_2} \\ &\leq \epsilon \left(\frac{i_1}{2p} + \frac{j_1}{2p} \right) + x_{i_2} + x_{j_2} \\ &\leq \epsilon \frac{i_1}{2p} + x_{i_2} + \epsilon \frac{j_1}{2p} + x_{j_2} \\ &\leq x'_i + x'_j. \end{aligned}$$

We will now prove that $\mathbf{x}'$ is not contained in the cone over

$$\bigcup_{(p'_1, \dots, p'_t)} \text{Len}(p'_1, \dots, p'_t)$$

where $(p_1, \dots, p_t)$ ranges across all tuples with prime entiers such that $\prod_i p'_i = n$. Fix such a tuple $(p'_1, \dots, p'_t)$. If $p'_1 \neq p$ then

$$x'_1 + x'_{p-1} = \frac{\epsilon}{2} < x_1 = x'_p,$$

so $\mathbf{x}'$ is not in the cone over $\text{Len}(p_1, \dots, p_t)$ because $1 + (p-1)$ does not overflow modulo $(p_1, \dots, p_t)$ and $x'_p > x'_1 + x'_{p-1}$. If $p'_1 = p$ then $p'_2 \dots p'_t = m$. Because $\mathbf{x}$ is not in the cone over $\text{Len}(p'_2, \dots, p'_t)$, we can choose $1 \leq i \leq j < i+j < m$ such that $i+j$ does not overflow modulo $(p'_2, \dots, p'_t)$ and $x_{i+j} > x_i + x_j$. Note that $pi + pj$ does not overflow modulo $(p'_1, \dots, p'_t)$ and

$$x'_{pi+pj} = x_{i+j} > x_i + x_j = x'_{pi} + x'_{pj}.$$

Thus $\mathbf{x}'$ not in the cone over $\text{Len}(p'_1, \dots, p'_t)$. □

Proposition 2.8.3. *Let p and q be two distinct odd primes with $p < q$ and let $n = p^2 q$. Then there*

exists a realizable flag type T such that

$$P_T \not\subseteq \text{Len}(p, p, q) \cup \text{Len}(p, q, p) \cup \text{Len}(q, p, p).$$

Proof. Let $e_1, e_2, e_3 \in \overline{\mathbb{Q}}$ be such that e_1 and e_2 have degree p , the element e_3 has degree q , and $\deg(\mathbb{Q}(e_1, e_2, e_3)) = p^2q$.

Define a sequence $\{1 = v_0, \dots, v_{n-1}\}$ as follows. For $0 \leq i < q$, set $v_i = e_1^i$. For $q \leq i < n$ and $1 \leq i' < n$, write $i' = i'_1 + i'_2p + i'_3pq$ in mixed radix notation with respect to (p, q, p) . Inductively define v_i as follows. Choose i' minimal such that $e_2^{i'_1} e_1^{i'_2} e_3^{i'_3} \notin \{v_0, \dots, v_{i-1}\}$, and set $v_i = e_2^{i'_1} e_1^{i'_2} e_3^{i'_3}$. Observe that for $i \geq pq$, $e_2^{i'_1} e_1^{i'_2} e_3^{i'_3} = e_2^{i_1} e_1^{i_2} e_3^{i_3}$. Define a flag $\mathcal{F} = (F_i)_{i \in [n]}$ by $F_i = \text{span}(v_0, \dots, v_i)$.

Because

$$F_1 = \text{span}(1, e_1)$$

$$F_{q-1} = \mathbb{Q}(e_1)$$

$$F_{pq+1} = \mathbb{Q}(e_1, e_2) + \text{span}(e_3, e_2e_3)$$

$$F_{pq+p-1} = \mathbb{Q}(e_1, e_2) + \mathbb{Q}(e_2) \text{span}(e_3) = \mathbb{Q}(e_2)(\mathbb{Q}(e_1) + \text{span}(e_3))$$

$$F_{2pq+p-1} = \mathbb{Q}(e_1, e_2) \text{span}(1, e_3) + \mathbb{Q}(e_2) \text{span}(e_3^2),$$

we have

$$F_1 F_{q-1} = F_{q-1}$$

and

$$\begin{aligned} F_{pq+1} F_{pq+p-1} &= (\mathbb{Q}(e_1, e_2) + \text{span}(e_3, e_2e_3))(\mathbb{Q}(e_2)(\mathbb{Q}(e_1) + \text{span}(e_3))) \\ &= \mathbb{Q}(e_1, e_2) \text{span}(1, e_3) + \mathbb{Q}(e_2) \text{span}(e_3^2) \\ &= F_{2pq+p-1}. \end{aligned}$$

We claim there exists $\mathbf{x}$ in the cone over $P_{T_{\mathcal{F}}}$ such that $x_q > x_1 + x_{q-1}$ and $x_{2pq+p} > x_{pq+1} + x_{pq+p-1}$. In particular, for $1 \leq i < q$ set $x_i = \frac{i}{2q}$. For $q \leq i < pq$ set $x_i = 1$. For $pq \leq i < p^2q$ write $i = i_1 + i_2p + i_3pq$ in mixed radix notation with respect to (p, q, p) and set $x_i = i_1 \frac{1}{4pq} + i_2 \frac{1}{2q} + i_3$.

We first show that $0 \leq x_1 \leq \dots x_{n-1}$. If $1 \leq i < q - 1$, then

$$x_{i+1} = \frac{i+1}{2q} \geq \frac{i}{2q} = x_i.$$

Note also that

$$x_q = 1 > \frac{q-1}{2q} = x_{q-1}$$

If $q \leq i < pq - 1$,

$$x_{i+1} = 1 = x_i.$$

If $pq \leq i < n - 1$ then write $i + 1 = (i + 1)_1 + (i + 1)_2 p + (i + 1)_3 pq$ in mixed radix notation with respect to (p, q, p) as well. Then if $i_1 = p - 1$ and $i_2 = q - 1$ then $(i + 1)_1 = 0$ and $(i + 1)_2 = 0$ and $(i + 1)_3 = i_3 + 1$. Then

$$\begin{aligned} x_{i+1} &= (i + 1)_1 \frac{1}{4pq} + (i + 1)_2 \frac{1}{2q} + (i + 1)_3 \\ &= (i_3 + 1) \\ &> i_1 \frac{1}{4pq} + i_2 \frac{1}{2q} + i_3 \\ &= x_i. \end{aligned}$$

Instead if $i_1 = p - 1$ and $i_2 \neq q - 1$ then $(i + 1)_1 = 0$ and $(i + 1)_2 = i_2 + 1$ and $(i + 1)_3 = i_3$. Then

$$\begin{aligned} x_{i+1} &= (i + 1)_1 \frac{1}{4pq} + (i + 1)_2 \frac{1}{2q} + (i + 1)_3 \\ &= (i_2 + 1) \frac{1}{2q} + i_3 \\ &> i_1 \frac{1}{4pq} + i_2 \frac{1}{2q} + i_3 \\ &= x_i. \end{aligned}$$

Finally, if $i_1 \neq p - 1$ then $(i + 1)_1 = i_1 + 1$ and $(i + 1)_2 = i_2$ and $(i + 1)_3 = i_3$. Then

$$\begin{aligned} x_{i+1} &= (i + 1)_1 \frac{1}{4pq} + (i + 1)_2 \frac{1}{2q} + (i + 1)_3 \\ &= (i_1 + 1) \frac{1}{4pq} + i_2 \frac{1}{2q} + i_3 \\ &> i_1 \frac{1}{4pq} + i_2 \frac{1}{2q} + i_3 \\ &= x_i. \end{aligned}$$

Therefore, $0 \leq x_1 \leq \dots x_{n-1}$.

We now show that for all $1 \leq i, j < n$, we have $x_{T(i,j)} \leq x_i + x_j$. Let $k = T(i, j)$.

Case 1: $1 \leq i < q$ and $1 \leq j < q$. Then $k = \min(q-1, i+j)$. Thus

$$x_k = \frac{k}{2q} \leq \frac{i}{2q} + \frac{j}{2q} = x_i + x_j.$$

Case 2: $1 \leq i < q$ and $q \leq j < pq$. Then as $F_{pq-1} = \mathbb{Q}(e_1, e_2)$, we have $j < k < pq$. Thus

$$x_k = 1 \leq \frac{i}{2q} + 1 = x_i + x_j.$$

Case 3: $1 \leq i < q$ and $pq \leq j < n$. Write $j = j_1 + j_2p + j_3pq$ in mixed radix notation with respect to (p, q, p) . Then $j < k \leq j_1 + \min(q-1, i+j_2)p + j_3pq$. Then

$$\begin{aligned} x_k &\leq x_{j_1 + \min(q-1, i+j_2)p + j_3pq} \\ &= j_1 \frac{1}{4pq} + \min(q-1, i+j_2) \frac{1}{2q} + j_3 \\ &\leq \frac{i}{2q} + j_1 \frac{1}{4pq} + j_2 \frac{1}{2q} + j_3 \\ &= x_i + x_j. \end{aligned}$$

Case 4: $q \leq i < pq$ and $q \leq j < pq$. Then as $F_{pq-1} = \mathbb{Q}(e_1, e_2)$, we have $j < k < pq$. Thus

$$x_k = 1 \leq \frac{i}{2q} + 1 = x_i + x_j.$$

Case 5: $q \leq i < pq$ and $pq \leq j < n$. Write $j = j_1 + j_2p + j_3pq$ in mixed radix notation with respect to (p, q, p) . Because $F_{pq-1} = \mathbb{Q}(e_1, e_2)$, then $j < k \leq (p-1) + (q-1)p + j_3pq$. Then

$$\begin{aligned} x_k &\leq x_{(p-1) + (q-1)p + j_3pq} \\ &= (p-1) \frac{1}{4pq} + (q-1) \frac{1}{2q} + j_3 \\ &\leq 1 + j_3 \\ &= 1 + j_1 \frac{1}{4pq} + j_2 \frac{1}{2q} + j_3 \\ &= x_i + x_j. \end{aligned}$$

Case 6: $pq \leq i < n$. Write

$$i = i_1 + i_2p + i_3pq$$

$$j = j_1 + j_2p + j_3pq$$

in mixed radix notation with respect to (p, q, p) . Recall that for $i \geq pq$, we have $v_i = e_2^{i_1} e_1^{i_2} e_3^{i_3}$.

Thus, $j < k \leq \min(p-1, i_1 + j_1) + \min(q-1, i_2 + j_2)p + (i_3 + j_3)pq$. Then

$$\begin{aligned} x_k &\leq x_{\min(p-1, i_1 + j_1) + \min(q-1, i_2 + j_2)p + (i_3 + j_3)pq} \\ &= \min(p-1, i_1 + j_1) \frac{1}{4pq} + \min(q-1, i_2 + j_2) \frac{1}{2q} + (i_3 + j_3) \\ &\leq i_1 \frac{1}{4pq} + i_2 \frac{1}{2q} + i_3 + j_1 \frac{1}{4pq} + j_2 \frac{1}{2q} + j_3 \\ &= x_i + x_j. \end{aligned}$$

Thus, for all $1 \leq i, j < n$, we have if $x_{T(i,j)} \leq x_i + x_j$. Moreover, we have that

$$x_q = 1 > \frac{1}{2q} + \frac{q-1}{2q} = x_1 + x_{q-1}$$

and

$$x_{2pq+p} = \frac{1}{2q} + 2 > \left(\frac{1}{4pq} + 1 \right) + \left(\frac{p-1}{4pq} + 1 \right) = x_{pq+1} + x_{pq+p-1}.$$

Moreover

$$\text{Len}(p, p, q) \cup \text{Len}(p, q, p) \subseteq \{\mathbf{x} \in \mathbb{R}^{p^2q-1} \mid x_q \leq x_1 + x_{q-1}\}$$

and

$$\text{Len}(q, p, p) \subseteq \{\mathbf{x} \in \mathbb{R}^{p^2q-1} \mid x_{2pq+p} \leq x_{pq+1} + x_{pq+p-1}\}.$$

However, $\mathbf{x}$ is not in the cone over

$$\text{Len}(p, p, q) \cup \text{Len}(p, q, p) \cup \text{Len}(q, p, p),$$

which completes our proof. □

Lemma 2.8.4. *Let q be an odd prime. For $a \in \mathbb{Z}/q\mathbb{Z}$, we have*

$$a \left\{ \frac{q+1}{2}, \dots, q-1 \right\} = \left\{ \frac{q+1}{2}, \dots, q-1 \right\} \pmod{q}$$

if and only if $a \equiv 1 \pmod{q}$.

Proof. The statement

$$a \left\{ \frac{q+1}{2}, \dots, q-1 \right\} = \left\{ \frac{q+1}{2}, \dots, q-1 \right\} \pmod{q}$$

is equivalent to the statement

$$a \left\{ 1, \dots, \frac{q-1}{2} \right\} = \left\{ 1, \dots, \frac{q-1}{2} \right\} \pmod{q}.$$

If $q = 3$, it is clear that $a \equiv 1 \pmod{q}$; assume $q \neq 3$, and hence $q \geq 5$. Then as $a(q-1) \equiv -a \in \left\{ \frac{q+1}{2}, \dots, q-1 \right\} \pmod{q}$, we must have $a \in \left\{ 1, \dots, \frac{q-1}{2} \right\} \pmod{q}$. If $a \not\equiv 1 \pmod{q}$, then there exists $b \in \left\{ 1, \dots, \frac{q-1}{2} \right\} \pmod{q}$ such that $ab \in \left\{ \frac{q+1}{2}, \dots, q-1 \right\} \pmod{q}$, which is a contradiction. $\square$

Lemma 2.8.5. *Let p , q , and r be odd prime numbers such that $p < q \leq r$. There exists an integer m such that*

$$q \leq m \leq \lfloor qr/2 \rfloor,$$

the addition $pm + pm$ overflows modulo q , and the addition $m + m$ does not overflow modulo q or modulo r .

Proof. If $q = r$ then let

$$m = q + \left\lfloor \frac{q}{p} \right\rfloor.$$

Note that $m \% q = \lfloor q/p \rfloor$, as $0 \leq \lfloor q/p \rfloor < q$. As $0 \leq 2\lfloor \frac{q}{p} \rfloor < 2q/p \leq q$, we have $(2m) \% q = 2\lfloor q/p \rfloor$ and thus $m \% q + m \% q = (2m) \% q$, so $m + m$ does not overflow modulo q .

On the other hand, $pm = pq + p\lfloor q/p \rfloor$ and $0 \leq p\lfloor q/p \rfloor < q$, so $(pm) \% q = p\lfloor q/p \rfloor$. Because $p < q$, we have $q \% p \leq q/2$. Therefore,

$$\begin{aligned} (pm) \% q + (pm) \% q &= 2p \left\lfloor \frac{q}{p} \right\rfloor \\ &= 2p \left(\frac{q}{p} - \frac{q \% p}{p} \right) \\ &\geq 2p \left(\frac{q}{p} - \frac{q}{2p} \right) \\ &= q, \end{aligned}$$

so the addition $pm + pm$ overflows modulo q .

Because $p^{-1} \not\equiv 1 \pmod{q}$, by Lemma 2.8.4 the set

$$\left\{1, \dots, \frac{q-1}{2}\right\} \cap p^{-1} \left\{\frac{q+1}{2}, \dots, q-1\right\} \pmod{q}$$

is nonempty. Choose an element $\ell \in \mathbb{Z}/q\mathbb{Z}$ contained in the set above. Observe that

$$q(r-1)/2 + (q-1)/2 = \left\lfloor \frac{qr}{2} \right\rfloor.$$

and let

$$q \leq \ell_1, \dots, \ell_{\frac{r+1}{2}}$$

be the lifts of ℓ to $[q, \lfloor qr/2 \rfloor]$. Because $q \neq r$, the lifts $\ell_1, \dots, \ell_{\frac{r+1}{2}}$ all have distinct values modulo r by the Chinese remainder theorem. Thus, there exists ℓ_k such that $\ell_k \in \{0, \dots, \frac{r-1}{2}\} \pmod{r}$. Set $m = \ell_k$.

To see that the addition $pm + pm$ overflows modulo q , notice that $m \in p^{-1}\{\frac{q+1}{2}, \dots, q-1\} \pmod{q}$, so $(pm) \% q \geq \frac{q+1}{2}$, and hence

$$(pm) \% q + (pm) \% q \geq q + 1.$$

To see that the addition $m+m$ does not overflow modulo q or r , observe that $m \in \{1, \dots, \frac{q-1}{2}\} \pmod{q}$, hence

$$m \% q + m \% q < q.$$

Similarly, since $m \in \{1, \dots, \frac{r-1}{2}\} \pmod{r}$, we have

$$m \% r + m \% r < r.$$

□

Proposition 2.8.6. *Let $n = pqr$ for primes p, q , and r with $p < q \leq r$. Then there exists a realizable flag type T such that*

$$P_T \not\subseteq \text{Len}(p, q, r) \cup \text{Len}(p, r, q) \cup \text{Len}(q, p, r) \cup \text{Len}(q, r, p) \cup \text{Len}(r, p, q) \cup \text{Len}(r, q, p).$$

Proof. Let $e_1, e_2, e_3 \in \overline{\mathbb{Q}}$ be such that the element e_1 has degree p , the element e_2 has degree q , the element e_2 has degree r , and $\deg(\mathbb{Q}(e_1, e_2, e_3)) = p^2q$.

Define a sequence $1 = v_0, \dots, v_{n-1}$ as follows. For $0 \leq i < p$, set $v_i = e_1^i$. For $p \leq i < n$ and $1 \leq i' < n$, write $i' = i'_1 + i'_2 q + i'_3 p q$ in mixed radix notation with respect to (q, p, r) . Inductively define v_i as follows. Choose i' minimal such that $e_2^{i'_1} e_1^{i'_2} e_3^{i'_3} \notin \{v_0, \dots, v_{i-1}\}$. Set $v_i = e_2^{i'_1} e_1^{i'_2} e_3^{i'_3}$. Observe that for $i \geq p q$, we have $i = i'$. Define a flag $\mathcal{F} = (F_i)_{i \in [n]}$ by $F_i = \text{span}(v_0, \dots, v_i)$.

By Lemma 2.8.5, there existss an integer m such that

$$q \leq m \leq \lfloor q r / 2 \rfloor,$$

the addition $p m + p m$ overflows modulo q , and the addition $m + m$ does not overflow modulo q or modulo r . Moreover,

$$2 p m \leq 2 p \lfloor q r / 2 \rfloor < p q r.$$

Write $p m = (p m)_1 + (p m)_2 q + (p m)_3 p q$ in mixed radix notation with respect to (q, p, r) . Then we have

$$\begin{aligned} F_1 &= \text{span}(1, e_1) \\ F_{p-1} &= \mathbb{Q}(e_1) \\ F_{p m} &= \text{span}\{e_2^{i_1} e_1^{i_2} e_3^{i_3} \mid i_1 + i_2 q + i_3 p q \leq p m, 0 \leq i_1 < q, 0 \leq i_2 < p, 0 \leq i_3\} \\ F_{2 p m - 1} &= \text{span}\{e_2^{i_1} e_1^{i_2} e_3^{i_3} \mid i_1 + i_2 q + i_3 p q \leq 2 p m - 1, 0 \leq i_1 < q, 0 \leq i_2 < p, 0 \leq i_3\}. \end{aligned}$$

We have

$$F_1 F_{p-1} = F_{p-1}.$$

Moreover, because the addition $p m + p m$ overflows modulo q , we have $(p m)_1 + (p m)_1 \geq q$. We have that

$$\begin{aligned} F_{p m} F_{p m} &\subseteq \{e_2^{i_1} e_1^{i_2} e_3^{i_3} \mid i_1 + i_2 q + i_3 p q \leq (q - 1) + \min(p - 1, 2(p m)_2) q + 2(p m)_3 p q, \\ &\quad 0 \leq i_1 < q, 0 \leq i_2 < p, 0 \leq i_3\}. \end{aligned}$$

Because $i_1 + i_2 q + i_3 p q \leq (q - 1) + \min(p - 1, 2(p m)_2) q + 2(p m)_3 p q \leq 2 p m - 1$, we have

$$F_{p m} F_{p m} \subseteq F_{2 p m - 1}.$$

We claim there exists $\mathbf{x} \in P_{T_{\mathcal{F}}}$ such that $x_p > x_1 + x_{p-1}$ and $x_{2 p m} > 2 x_{p m}$. For $1 \leq i < p$ set

$x_i = \frac{i}{2p}$. For $p \leq i < pq$ set $x_i = 1$. For $pq \leq i < pqr$ write $i = i_1 + i_2q + i_3pq$ in mixed radix notation with respect to (q, p, r) and set $x_i = i_1 \frac{1}{4pq} + i_2 \frac{1}{2p} + i_3$.

We first show that $0 \leq x_1 \leq \dots \leq x_{n-1}$. If $1 \leq i < p-1$, then

$$x_{i+1} = \frac{i+1}{2p} \geq \frac{i}{2p} = x_i.$$

Note also that

$$x_p = 1 \geq \frac{p-1}{2p} = x_{p-1}.$$

If $p \leq i < pq-1$,

$$x_{i+1} = 1 = x_i.$$

If $pq \leq i < n-1$ then write $i+1 = (i+1)_1 + (i+1)_2q + (i+1)pq$ in mixed radix notation with respect to (q, p, r) . If $i_1 = q-1$ and $i_2 = p-1$ then $(i+1)_1 = (i+1)_2 = 0$ and $(i+1)_3 = i_3 + 1$.

Then

$$\begin{aligned} x_{i+1} &= (i+1)_1 \frac{1}{4pq} + (i+1)_2 \frac{1}{2p} + (i+1)_3 \\ &= i_3 + 1 \\ &> i_1 \frac{1}{4pq} + i_2 \frac{1}{2p} + i_3 \\ &= x_i. \end{aligned}$$

Instead if $i_1 = q-1$ and $i_2 \neq p-1$ then $(i+1)_1 = 0$ and $(i+1)_2 = i_2 + 1$ and $(i+1)_3 = i_3$.

Then

$$\begin{aligned} x_{i+1} &= (i+1)_1 \frac{1}{4pq} + (i+1)_2 \frac{1}{2p} + (i+1)_3 \\ &= (i_2 + 1) \frac{1}{2p} + i_3 \\ &> i_1 \frac{1}{4pq} + i_2 \frac{1}{2p} + i_3 \\ &= x_i. \end{aligned}$$

Finally, if $i \neq q - 1$ then $(i + 1)_1 = i_1 + 1$ and $(i + 1)_2 = i_2$ and $(i + 1)_3 = i_3$. Then

$$\begin{aligned}
x_{i+1} &= (i + 1)_1 \frac{1}{4pq} + (i + 1)_2 \frac{1}{2p} + (i + 1)_3 \\
&= (i_1 + 1) \frac{1}{4pq} + i_2 \frac{1}{2p} + i_3 \\
&> i_1 \frac{1}{4pq} + i_2 \frac{1}{2p} + i_3 \\
&= x_i.
\end{aligned}$$

Therefore, $0 \leq x_1 \leq \dots \leq x_{n-1}$.

We now show that for all $1 \leq i, j < n$, we have $x_{T_F(i,j)} \leq x_i + x_j$.

Case 1: $1 \leq i < p$ and $1 \leq j < p$. Then $k = \min(p - 1, i + j)$. Then

$$x_k = \frac{k}{2p} \leq \frac{i}{2p} + \frac{j}{2p} = x_i + x_j.$$

Case 2: $1 \leq i < p$ and $p \leq j < pq$. Then as $F_{pq-1} = \mathbb{Q}(e_1, e_2)$, we have $j < k < pq$. Thus

$$x_k = 1 \leq \frac{i}{2p} + 1 = x_i + x_j.$$

Case 3: $1 \leq i < p$ and $pq \leq j < n$. Write $j = j_1 + j_2q + j_3pq$ in mixed radix notation with respect to (q, p, r) . Then $j < k \leq j_1 + \min(p - 1, i + j_2)q + j_3pq$. Then

$$\begin{aligned}
x_k &\leq x_{j_1 + \min(p-1, i+j_2)q + j_3pq} \\
&= j_1 \frac{1}{4pq} + \min(p - 1, i + j_2) \frac{1}{2p} + j_3 \\
&\leq \frac{i}{2p} + j_1 \frac{1}{4pq} + j_2 \frac{1}{2p} + j_3 \\
&= x_i + x_j.
\end{aligned}$$

Case 4: $p \leq i < pq$ and $p \leq j < pq$. Then as $F_{pq-1} = \mathbb{Q}(e_1, e_2)$, we have $j < k < pq$. Thus

$$x_k = 1 \leq \frac{i}{2q} + 1 = x_i + x_j.$$

Case 5: $p \leq i < pq$ and $pq \leq j < n$. Write $j = j_1 + j_2q + j_3pq$ in mixed radix notation with respect

to (q, p, r) . Because $F_{pq-1} = \mathbb{Q}(e_1, e_2)$, we have $j < k \leq (q-1) + (p-1)q + j_3pq$. Then

$$\begin{aligned}
x_k &\leq x_{(q-1)+(p-1)q+j_3pq} \\
&= (q-1)\frac{1}{4pq} + (p-1)\frac{1}{2p} + j_3 \\
&\leq 1 + j_3 \\
&= 1 + j_1\frac{1}{4pq} + j_2\frac{1}{2p} + j_3 \\
&= x_i + x_j.
\end{aligned}$$

Case 6: $pq \leq i < n$. Write

$$\begin{aligned}
i &= i_1 + i_2q + i_3pq \\
j &= j_1 + j_2q + j_3pq
\end{aligned}$$

in mixed radix notation with respect to (q, p, r) . Recall that for $i \geq pq$, we have $v_i = e_2^{i_1} e_1^{i_2} e_3^{i_3}$. Thus, $j < k \leq \min(q-1, i_1 + j_1) + \min(p-1, i_2 + j_2)q + (i_3 + j_3)pq$. Then

$$\begin{aligned}
x_k &\leq x_{\min(q-1, i_1 + j_1) + \min(p-1, i_2 + j_2)q + (i_3 + j_3)pq} \\
&= \min(q-1, i_1 + j_1)\frac{1}{4pq} + \min(p-1, i_2 + j_2)\frac{1}{2p} + (i_3 + j_3) \\
&\leq (i_1\frac{1}{4pq} + i_2\frac{1}{2p} + i_3) + (j_1\frac{1}{4pq} + j_2\frac{1}{2p} + j_3) \\
&= x_i + x_j.
\end{aligned}$$

Thus, for any integers $1 \leq i, j < n$, we have $x_{T_{\mathcal{F}}(i,j)} \leq x_i + x_j$. Moreover, we have that

$$x_p = 1 > \frac{1}{2p} + \frac{p-1}{2p} = x_1 + x_{p-1}.$$

Write:

$$\begin{aligned}
pm &= (pm)_1 + (pm)_2q + (pm)_3pq \\
2pm &= (2pm)_1 + (2pm)_2q + (2pm)_3pq
\end{aligned}$$

in mixed radix notation with respect to (q, p, r) and recall that $pm + pm$ overflows modulo q . Therefore, either $(2pm)_3 = 2(pm)_3$ and $(2pm)_2 = 2(pm)_2 + 1$, or $(2pm)_3 = 2(pm)_3 + 1$. If $(2pm)_3 =$

$2(pm)_3$ and $(2pm)_2 > 2(pm)_2 + 1$ then

$$\begin{aligned}
x_{2pm} &= (2pm)_1 \frac{1}{4pq} + (2pm)_2 \frac{1}{2p} + (2pm)_3 \\
&\geq (2(pm)_2 + 1) \frac{1}{2p} + 2(pm)_3 \\
&> 2(pm)_1 \frac{1}{4pq} + 2(pm)_2 \frac{1}{2p} + 2(pm)_3 \\
&= 2x_{pm}.
\end{aligned}$$

Otherwise, if $(2pm)_3 = 2(pm)_3 + 1$, then

$$\begin{aligned}
x_{2pm} &= (2pm)_1 \frac{1}{4pq} + (2pm)_2 \frac{1}{2p} + (2pm)_3 \\
&\geq 2(pm)_3 + 1 \\
&> 2(pm)_1 \frac{1}{4pq} + 2(pm)_2 \frac{1}{2p} + 2(pm)_3 \\
&= 2x_{pm}.
\end{aligned}$$

Further note that

$$\text{Len}(q, p, r) \cup \text{Len}(q, r, p) \cup \text{Len}(r, q, p) \cup \text{Len}(r, p, q) \subseteq \{\mathbf{x} \in \mathbb{R}^{n-1} \mid x_p \leq x_1 + x_{p-1}\}$$

and

$$\text{Len}(p, q, r) \cup \text{Len}(p, r, q) \subseteq \{\mathbf{x} \in \mathbb{R}^{n-1} \mid x_{2pm} \leq 2x_{pm}\}.$$

We have $x_p > x_1 + x_{p-1}$ and $x_{2pm} > 2x_{pm}$, and thus our proof is complete. $\square$

Proposition 2.8.7. *Let $n = 4p$ for p a prime not equal to 2 or 3. Then there exists a realizable flag type T such that*

$$P_T \not\subseteq \text{Len}(2, 2, p) \cup \text{Len}(2, p, 2) \cup \text{Len}(p, 2, 2).$$

Proof. Let $e_1, e_2, e_3 \in \overline{\mathbb{Q}}$ be such that the element e_1 has degree p , the element e_2 has degree 2, the

element e_2 has degree 2, and $\deg(\mathbb{Q}(e_1, e_2, e_3)) = 4p$. Define the basis $\{v_0, \dots, v_{4p-1}\}$ as follows. Set

$$v_0 = 1$$

$$v_1 = e_1$$

$$v_2 = e_2$$

$$v_3 = e_2 e_1$$

$$v_4 = e_1^2$$

$$v_5 = e_2 e_1^2$$

$$v_6 = e_1^3$$

$$v_7 = e_2 e_1^3.$$

For $8 \leq i < n$ and $1 \leq i' < n$, write $i' = i'_1 + i'_2 p + i'_3 2p$ in mixed radix notation with respect to $(p, 2, 2)$. Inductively define v_i as follows. Choose i' minimal such that $e_1^{i'_1} e_2^{i'_2} e_3^{i'_3} \notin \{v_0, \dots, v_{i-1}\}$. Set $v_i = e_1^{i'_1} e_2^{i'_2} e_3^{i'_3}$. Observe that for $i \geq 2p$, we have $i = i'$. Let $\mathcal{F}$ be the corresponding flag.

Note that

$$F_1 = \text{span}(1, e_1)$$

$$F_3 = \mathbb{Q}(e_2) \text{span}(1, e_1)$$

$$F_5 = \mathbb{Q}(e_2) \text{span}(1, e_1, e_1^2)$$

$$F_7 = \mathbb{Q}(e_2) \text{span}(1, e_1, e_1^2, e_1^3)$$

$$F_{3p-1} = \mathbb{Q}(e_1) \text{span}(1, e_2, e_3).$$

Therefore

$$F_1 F_{3p-1} = F_{3p-1}$$

$$F_3 F_3 = F_5$$

$$F_3 F_5 = F_7.$$

Suppose $p = 5$. Then let $\mathbf{x} \in \mathbb{R}^{19}$ be as follows:

$$x_1 = 1$$

$$x_2, x_3 = 1.4$$

$$x_4, x_5 = 2$$

$$x_6, x_7 = 3$$

$$x_8, \dots, x_{14} = 4$$

$$x_{15}, \dots, x_{19} = 5.1.$$

We claim that $\mathbf{x} \in P_{T_{\mathcal{F}}}$ and $x_8 > x_5 + x_3$ and $x_{15} > x_1 + x_{14}$. It is clear that $0 \leq x_1 \leq \dots \leq x_{n-1}$.

We now show that for all $1 \leq i, j < n$, we have $x_{T_{\mathcal{F}}(i,j)} \leq x_i + x_j$. Let $k = T_{\mathcal{F}}(i, j)$.

Case 1: $i = 1$. If $j = 1$ then $k = 4$ and

$$x_4 = 2 \leq 2x_1.$$

Observe that if $j = 2, 3$ then $k = 4, 5$, and

$$x_k = 2 \leq 1.4 + 1 \leq x_1 + x_j.$$

If $j = 4, 5$, then $k = 6, 7$, and

$$x_k = 3 \leq 2 + 1 = x_1 + x_j.$$

If $j = 6, 7$, then $k \leq 10$, and

$$x_k \leq 4 \leq 3 + 1 = x_1 + x_j.$$

If $8 \leq j < 15$, then as $v_1 = e_1$ and $F_{14} = \langle e_1 \rangle \{1, e_2, e_3\}$, we have that $j < k < 14$. Thus

$$x_k \leq 4 \leq 4 + 1 = x_1 + x_j.$$

If $15 \leq j < n$ then

$$x_k \leq 5.1 \leq 5.1 + 1 \leq x_1 + x_j.$$

Case 2: $i = 2, 3$. If $j = 2, 3$, then $k = 4, 5$ so

$$x_k = 2 \leq 1.4 + 1.4 = x_i + x_j.$$

If $j = 4, 5$ then $k = 6, 7$ so

$$x_k = 3 \leq 2 + 1.4 = x_i + x_j.$$

If $j = 6, 7$ then $k < 15$ so

$$x_k \leq 4 \leq 3 + 1.4 \leq x_i + x_j.$$

If $8 \leq j < n$ then

$$x_k \leq 5.1 \leq 4 + 1.4 \leq x_i + x_j.$$

Case 3: $i = 4, 5$ If $j < 10$ then because $F_9 = \mathbb{Q}(e_1, e_2)$ we have $k < 10$. Thus

$$x_k \leq 4 \leq 2 + 2 \leq x_i + x_j.$$

If $10 \leq j < n$ then

$$x_k \leq 5.1 \leq 4 + 2 \leq x_i + x_j.$$

Case 4: $i \geq 6$. Then

$$x_k \leq 5.1 \leq 3 + 3 \leq x_i + x_j.$$

Thus $\mathbf{x}$ is in the cone over $P_{T_{\mathcal{F}}}$. One can see explicitly that $x_8 > x_5 + x_3$ and $x_{15} > x_1 + x_{14}$.

Because

$$\text{Len}(2, 2, 5) \cup \text{Len}(2, 5, 2) \subset \{\mathbf{x} \in \mathbb{R}^{19} \mid x_{15} \leq x_1 + x_{14}\}$$

and

$$\text{Len}(5, 2, 2) \subset \{\mathbf{x} \in \mathbb{R}^{19} \mid x_8 \leq x_5 + x_3\},$$

our proof is complete for $p = 5$.

If $p \neq 5$, let $\mathbf{x} \in \mathbb{R}^{4p-1}$ be as follows.

$$x_1 = 1$$

$$x_2, x_3 = 1.4$$

$$x_4, x_5 = 2$$

$$x_6, \dots, x_{3p-1} = 2.9$$

$$x_{3p}, \dots, x_{4p-1} = 4.$$

We claim that $\mathbf{x}$ is in the cone over $P_{T_{\mathcal{F}}}$ and $x_6 > x_3 + x_3$ and $x_{3p} > x_1 + x_{3p-1}$. It is clear that

$0 \leq x_1 \leq \dots \leq x_{n-1}$. We now show that for all integers $1 \leq i, j < n$, we have $x_{T(i,j)} \leq x_i + x_j$. Let $k = T(i, j)$.

Case 1: $i = 1$. If $j = 1$, then $k = 4$ and

$$x_4 = 2 \leq 2x_1.$$

Observe that if $j = 2, 3$, then $k = 4, 5$, and

$$x_k \leq x_5 = 2 \leq 1.4 + 1 \leq x_1 + x_j.$$

If $j = 4, 5$, then $k = 6, 7$, and

$$x_k \leq x_5 = 2.9 \leq 2 + 1 \leq x_1 + x_j.$$

If $6 \leq j < 3p$, then as $v_1 = e_1$ and $F_{3p-1} = \mathbb{Q}(e_1) \text{span}(1, e_2, e_3)$, we have $j < k < 3p$. Thus

$$x_k = 2.9 \leq 2.9 + 1 = x_j + x_1.$$

If $j \geq 3p$, then

$$x_k = 4 \leq 4 + 1 \leq x_1 + x_j.$$

Case 2: $i = 2, 3$. If $j = 2, 3$, then $k \leq 5$ and

$$x_k = 2 \leq 1.4 + 1.4 = x_i + x_j.$$

If $j = 4, 5$ then $k \leq 7$ and

$$x_k \leq 2.9 \leq 2 + 1.4 = x_i + x_j.$$

If $j \geq 6$, then

$$x_k \leq 4 \leq 2.9 + 1.4 = x_i + x_j.$$

Case 3: $i \geq 4$. Then we have

$$x_k \leq 4 \leq 2 + 2 \leq x_i + x_j.$$

Therefore, for any integers $1 < i, j < n$, we have $x_{T(i,j)} \leq x_i + x_j$, so x is in the cone over P_{T_F} . Moreover, it is clear that $x_6 > x_3 + x_3$ and $x_{3p} > x_1 + x_{3p-1}$.

Again, we have

$$\text{Len}(2, 2, p) \cup \text{Len}(2, p, 2) \subset \{\mathbf{x} \in \mathbb{R}^{4p-1} \mid x_{3p} \leq x_1 + x_{3p-1}\}$$

and because $p \geq 7$, we have

$$\text{Len}(p, 2, 2) \subset \{\mathbf{x} \in \mathbb{R}^{4p-1} \mid x_6 \leq x_3 + x_3\},$$

and thus our proof is complete. □

Proposition 2.8.8. *Let $n = 24$. Then there exists a realizable flag type T such that*

$$P_T \not\subseteq \text{Len}(2, 2, 2, 3) \cup \text{Len}(2, 2, 3, 2) \cup \text{Len}(2, 3, 2, 2) \cup \text{Len}(3, 2, 2, 2)$$

Proof. Let $e_1, e_2, e_3, e_4 \in \overline{\mathbb{Q}}$ be such that e_1, e_2, e_3 have degree 2, the element e_4 has degree 3, and

$$\deg(\mathbb{Q}(e_1, e_2, e_3, e_4)) = 24.$$

Define a flag $\mathcal{F}$ such that

$$F_1 = \text{span}(1, e_4)$$

$$F_2 = \mathbb{Q}(e_4)$$

$$F_7 = \mathbb{Q}(e_1) \text{span}(1, e_4, e_4^2, e_2)$$

$$F_{13} = \mathbb{Q}(e_1) \text{span}(1, e_4, e_4^2, e_2, e_4 e_2, e_4^2 e_2, e_3)$$

$$F_{19} = \mathbb{Q}(e_1) \text{span}(1, e_4, e_4^2, e_2, e_4 e_2, e_4^2 e_2, e_3, e_4 e_3, e_4^2 e_3, e_2 e_3)$$

Then, we have

$$F_1 F_2 = F_2$$

and

$$F_7 F_{13} = F_{19}.$$

A computation shows that there exists $\mathbf{x}$ in the cone over $P_{T_{\mathcal{F}}}$ such that $x_3 > x_2 + x_1$ and $x_{20} >$

$x_7 + x_{13}$. However, we have that

$$\text{Len}(2, 2, 2, 3) \cup \text{Len}(2, 2, 3, 2) \cup \text{Len}(2, 3, 2, 2) \subset \{\mathbf{x} \in \mathbb{R}^{23} \mid x_3 \leq x_2 + x_1\}$$

and

$$\text{Len}(3, 2, 2, 2) \subset \{\mathbf{x} \in \mathbb{R}^{23} \mid x_{20} \leq x_7 + x_{13}\}$$

so our proof is complete. □

Chapter 3

Counting cubic rings by successive minima

3.1 Statement of results

For the rest of this section, let R denote a nondegenerate cubic ring of absolute discriminant Δ ; such a ring naturally has the structure of a lattice (see Section 1.6), and therefore we may speak of the *successive minima*

$$\frac{1}{\sqrt{3}} \leq \lambda_0(R) \leq \lambda_1(R) \leq \lambda_2(R)$$

of R . For a permutation group $G \subseteq S_3$, we say R is a G -ring if $\text{Gal}(R \otimes \mathbb{Q}) \cong G$ as permutation groups. For any point $p = (p_1, p_2) \in \mathbb{R}^2$, any permutation group $G \subseteq S_3$, any positive real number ϵ , and any $X \in \mathbb{R}_{>1}$, define $\mathcal{F}(p, \epsilon, G, X)$ to be the set of isomorphism classes of G -rings R with $\Delta \leq X$ and

$$\max_{i=1,2} \{ |\log_{\Delta} \lambda_i(R) - p_i| \} \leq \frac{\epsilon}{\log X}. \quad (3.1)$$

Define the density function $d_{\epsilon, G}: \mathbb{R}^2 \rightarrow \mathbb{R} \cup \{*\}$ which assigns to $p \in \mathbb{R}^2$ the value

$$\lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, G, X) + 1)}{\log X}$$

if the limit exists and else assigns $*$. Our main theorems consist of computing such density functions; the first such result was obtained by Chiche-lapierre.

Theorem 1.2.1. (Chiche-lapierre [14], Theorem 3.1.1) *There exists a positive real number C such that for every $\epsilon > C$ and every $p = (p_1, p_2) \in \mathbb{R}^2$, we have:*

$$d_{\epsilon, S_3}(p) = \begin{cases} 1 - (p_2 - p_1) & \text{if } p \text{ is contained in the closed line segment from } (1/6, 1/3) \text{ to } (1/4, 1/4) \\ 0 & \text{else.} \end{cases}$$

We give a proof of Theorem 1.2.1 that is different than Chiche-lapierre's. Our counting methods are notably simpler, and allow us to sieve for maximal orders. Define $\mathcal{F}^{\max}(p, \epsilon, G, X)$ to be the subset of $\mathcal{F}(p, \epsilon, G, X)$ consisting of *maximal* G -rings and denote the corresponding density function $d_{\epsilon, G}^{\max}$.

Theorem 1.2.2. *There exists a positive real number C such that for every $\epsilon > C$, we have*

$$d_{\epsilon, S_3} = d_{\epsilon, S_3}^{\max}.$$

Define $\mathcal{F}(p, \epsilon, X)$ to be the set of isomorphism classes of nondegenerate cubic rings R such that $\Delta \leq X$ and (3.1) is satisfied, and denote the corresponding density function $d_{\epsilon, 3}$. Define $\mathcal{F}^{\max}(p, \epsilon, X)$ to be the subset of $\mathcal{F}(p, \epsilon, X)$ consisting of maximal rings, and denote the corresponding density function $d_{\epsilon, 3}^{\max}$.

Theorem 1.2.3. *There exists a positive real number C such that for every $\epsilon > C$ and every $p = (p_1, p_2) \in \mathbb{R}^2$, we have:*

$$d_{\epsilon, 3}(p) = \begin{cases} 1 - (p_2 - p_1) + \max\{0, 1/2 - 3p_1\} & \text{if } p \text{ is contained in the closed line segment from } (0, 1/2) \text{ to } (1/4, 1/4) \\ 0 & \text{else.} \end{cases}$$

$$d_{\epsilon, 3}^{\max}(p) = \begin{cases} 1 - (p_2 - p_1) & \text{if } p \text{ is contained in the closed line segment from } (1/6, 1/3) \text{ to } (1/4, 1/4) \\ 1 & \text{if } p = (0, 1/2) \\ 0 & \text{else.} \end{cases}$$

Theorem 3.1.1. *There exists a positive real number C such that for every $\epsilon > C$ and any $p =$*

$(p_1, p_2) \in \mathbb{R}^2$, we have:

$$d_{\epsilon, \mathbb{Z}/2\mathbb{Z}}(p) = \begin{cases} 1 - p_1 & \text{if } p \text{ is contained in the closed line segment from } (0, 1/2) \text{ to } (1/4, 1/4) \\ 0 & \text{else.} \end{cases}$$

$$d_{\epsilon, \mathbb{Z}/2\mathbb{Z}}^{\max}(p) = \begin{cases} 1 & \text{if } p = (0, 1/2) \\ 0 & \text{else.} \end{cases}$$

Let E denote the trivial group.

Theorem 3.1.2. *There exists a positive real number C such that for every $\epsilon > C$ and any $p = (p_1, p_2) \in \mathbb{R}^2$, we have:*

$$d_{\epsilon, E}(p) = \begin{cases} 1/2 & \text{if } p \text{ is contained in the closed line segment from } (0, 1/2) \text{ to } (1/4, 1/4) \\ 0 & \text{else.} \end{cases}$$

$$d_{\epsilon, E}^{\max} = 0$$

We do not compute the density function for $\mathbb{Z}/3\mathbb{Z}$ -rings but we can compute the following region.

Corollary 3.1.3. *The set of limit points of the multiset $(\log_{\Delta} \lambda_1, \log_{\Delta} \lambda_2)$ as R ranges across orders in cyclic cubic fields is the closed line segment from $(1/6, 1/3)$ to $(1/4, 1/4)$.*

Proof. This is a corollary of Corollary 3.4.1. □

Special families of cubic rings

Remarkably, there is a relationship between rings that have extremal successive minima and rings that are extremal in an *algebraic* sense, as we will see in the following theorems. Via this relationship, the endpoints of our line segments “correspond” to various interesting algebraic families of rings. The following results have appeared in various forms in the literature, but we state and reprove them here in the language of density functions.

We’ll now formalize what “correspond” means. Let $\mathcal{F}$ be an infinite set equipped with a map $H: \mathcal{F} \rightarrow \mathbb{R}_{>0}$ such that for all X , the set $\{f \in \mathcal{F} \mid H(f) \leq X\}$ is finite. We call H the *height function* of $\mathcal{F}$. Further suppose that $\mathcal{F}$ is also equipped with a map ψ from $\mathcal{F}$ to the set of isomorphism classes of nondegenerate cubic rings¹.

¹As a motivating example, consider the case when $\mathcal{F}$ is the set of integral binary cubic forms of nonzero discriminant and H is the naive height, i.e. the maximum of the absolute value of the coefficients.

For $\epsilon \in \mathbb{R}_{>0}$ and $X \in \mathbb{R}_{>1}$, we say a cubic ring R and a point $p \in \mathbb{R}^2$ are (ϵ, X) -close if

$$\max_{i=1,2} \{ |\log_{\Delta} \lambda_i - p_i| \} \leq \frac{\epsilon}{\log X}.$$

For a point p contained in the closed line segment from $(0, 1/2)$ to $(1/4, 1/4)$, we say the triple $(\mathcal{F}, H, \psi)$ corresponds to p if

$$\lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F} \mid H(f) \leq X \text{ and } \psi(f) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{f \in \mathcal{F} \mid H(f) \leq X\}} = 1 \quad (3.2)$$

and there exists a constant C such that for all $\epsilon > C$,

$$\liminf_{X \rightarrow \infty} \frac{\#\{R \in \mathcal{F}(p, \epsilon, X) \mid R \in \psi(\mathcal{F})\}}{\#\mathcal{F}(p, \epsilon, X)} > 0. \quad (3.3)$$

When H or ψ are implicit, we simply write that $\mathcal{F}$ corresponds to p . Heuristically, (3.2) says that “most” elements of $\mathcal{F}$, when ordered by height, are “near” p , and (3.3) says that when ordered by absolute discriminant, a positive proportion of rings “near” p come from $\mathcal{F}$.

We first study monogenic rings via monic polynomials with integral coefficients. Given a polynomial

$$f(x) = x^n + a_1 x^2 + \cdots + a_n \in \mathbb{Z}[x],$$

the *root height* of f is denoted $H_r(f)$ and is defined to be $\max_i \{|a_i|^{1/i}\}$. The polynomial $f(x)$ gives rise to the monogenic rank n ring $R_f := \mathbb{Z}[x]/(f(x))$. Our first results shows that when monic integral cubic polynomials are ordered by root height, the corresponding lattices tend to be skew; moreover skew rings tend to be monogenic.

Corollary 3.1.4. *Let $\mathcal{F}_3^{\text{mon}}$ be the set of monic cubic polynomials with integral coefficients and nonzero discriminant. Then $(\mathcal{F}_3^{\text{mon}}, H_r)$ corresponds to $(1/6, 1/3)$.*

In fact, our proof can be adapted to show that for any nonzero integer k , the set of polynomials $f(x) = kx^n + a_1 x^2 + \cdots + a_n \in \mathbb{Z}[x]$ of nonzero discriminant equipped with the root height corresponds to $(1/6, 1/3)$.

One might guess at the above result by guessing that for a monogenic cubic ring $\mathbb{Z}[\alpha]$ satisfying

$$|\alpha| = \min_{i \in \mathbb{Z}} \{ |\alpha + i| \},$$

a “short” basis of $\mathbb{Z}[\alpha]$ might look like $1, \alpha, \alpha^2$. Conversely, suppose R is a cubic ring “near”

$(1/6, 1/3)$, and suppose $\alpha \in R \setminus \mathbb{Z}$ is such that $|\alpha| = \lambda_1$. Then $\mathbb{Z}[\alpha]$ is a monogenic subring of R with small index, because

$$|\mathrm{Disc}(\mathbb{Z}[\alpha])|^{1/2} \ll |\alpha| |\alpha|^2 \asymp \lambda_1 \lambda_2 \asymp |\mathrm{Disc}(R)|^{1/2}.$$

One might further guess that the index of $\mathbb{Z}[\alpha]$ in R has a positive probability of being 1. Corollary 3.1.4 formalizes this heuristic reasoning.

Our next result shows that a general irreducible cubic ring is not very skew at all, and a general reducible ring is as skew as possible.

Corollary 3.1.5. *Let $\mathcal{F}^{\mathrm{irr}}$ be the set of isomorphism classes of nondegenerate irreducible cubic rings, and let H be the absolute discriminant. Then $(\mathcal{F}^{\mathrm{irr}}, H)$ corresponds to $(1/4, 1/4)$. Let $\mathcal{F}^{\mathrm{red}}$ be the set of isomorphism classes of nondegenerate reducible cubic rings, and again let H be the absolute discriminant. Then $(\mathcal{F}^{\mathrm{red}}, H)$ corresponds to $(0, 1/2)$.*

The statement above about $\mathcal{F}^{\mathrm{irr}}$ is in fact a corollary of Terr’s work [32] on the equidistribution of shapes of cubic orders, but we give an independent proof.

3.2 The parametrization of cubic rings

Our proofs utilize a theorem of Delone–Faddeev parametrizing isomorphism classes of cubic rings by $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of integral binary cubic forms. An element $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ acts on a binary cubic form $f(x, y)$ by

$$(\gamma f)(x, y) = \frac{1}{\det \gamma} f((x, y)\gamma).$$

A *based rank n ring* is a rank n ring R equipped with an ordered $\mathbb{Z}$ -basis of $R/\mathbb{Z}$. The group $\mathrm{GL}_2(\mathbb{Z})$ naturally acts on based cubic rings by change of basis.

Theorem 3.2.1 (Delone, Faddeev [18]). *There is a canonical discriminant-preserving bijection between the set of based cubic rings and integral binary cubic forms. Under the action of $\mathrm{GL}_2(\mathbb{Z})$, this bijection descends to a bijection between the set of isomorphism classes of cubic rings and the set of $\mathrm{GL}_2(\mathbb{Z})$ -orbits of integral binary cubic forms.*

We now describe a few important details of the Delone–Faddeev bijection. Given a cubic ring R with basis $\{1, \omega, \theta\}$ and an element $\alpha \in R$, let M_α be a 3×3 matrix such that

$$\begin{bmatrix} 1 & \alpha & \alpha^2 \end{bmatrix} = M_\alpha \begin{bmatrix} 1 & \omega & \theta \end{bmatrix}^t$$

One may define a map $\varphi: R \rightarrow \mathbb{Z}$ given by sending α to $\det M_\alpha$. This descends to a map $\varphi: R/\mathbb{Z} \rightarrow \mathbb{Z}$. The map φ is a cubic map and so the basis $\{\bar{\omega}, \bar{\theta}\}$ of $R/\mathbb{Z}$ expresses φ as an integral binary cubic form. In fact, the binary cubic form is determined by the basis $\{\bar{\omega}, \bar{\theta}\}$ of $R/\mathbb{Z}$.

Conversely, from an integral binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, we obtain a cubic ring R_f with basis $\{1, \omega, \theta\}$ defined by the following multiplication table:

$$\begin{aligned}\omega\theta &= -ad \\ \omega^2 &= -ac + b\omega - a\theta \\ \theta^2 &= -bd + d\omega - c\theta\end{aligned}\tag{3.4}$$

3.3 Reduction theory of cubic rings

In this section, we develop the relationship between “small” bases of cubic rings and integral binary cubic forms with “small” coefficients. Let $V_{\mathbb{R}}$ denote the set of real binary cubic forms and let $V_{\mathbb{Z}} \subseteq V_{\mathbb{R}}$ denote the lattice of integral binary cubic forms. For a point $p = (p_1, p_2) \in \mathbb{R}^2$ and a positive real number X , define the box $B(p, X)$ to be the set of real binary cubic forms $ax^3 + bx^2y + cxy^2 + dy^3$ such that:

$$\begin{aligned}|a| &\leq X^{3p_1-1/2} \\ |b| &\leq X^{2p_1+p_2-1/2} \\ |c| &\leq X^{p_1+2p_2-1/2} \\ |d| &\leq X^{3p_2-1/2}\end{aligned}$$

We now fix some notation that we use throughout this section. Let

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \text{Sym}^3 \mathbb{Z}^2$$

be a form of nonzero discriminant, let R_f denote the cubic ring associated to f under the Delone–Faddeev correspondence, let $\Delta = |\text{Disc}(f)| = |\text{Disc}(R_f)|$, let $p = (p_1, p_2)$ denote a point in $\mathbb{R}^2$, let ϵ denote a positive real number, let C, D denote real numbers ≥ 1 , and let $X \in \mathbb{R}_{>1}$. We say a pair (f, p) is (ϵ, X) -close if R_f and p are (ϵ, X) -close. We say f comes from a Minkowski basis if there exists a Minkowski basis of R_f giving rise to f under the Delone–Faddeev correspondence (see [31], Lecture 10, §6 for a definition of Minkowski basis). Our first result shows that Minkowski bases of cubic rings give rise to binary cubic forms with “small” coefficients.

Lemma 3.3.1. *There exists C such that for all ϵ , f , and p , if $\Delta > 1$ and (f, p) is (ϵ, Δ) -close and f comes from a Minkowski basis, then $f \in Ce^{3\epsilon}B(p, \Delta)$.*

Proof. Let (f, p) be an (ϵ, Δ) -close pair with $\Delta > 1$ coming from a Minkowski basis $\{1, \omega, \theta\}$ of R_f . Then:

$$|\omega| \asymp \lambda_1(R_f) \leq e^\epsilon \Delta^{p_1}$$

$$|\theta| \asymp \lambda_2(R_f) \leq e^\epsilon \Delta^{p_2}$$

Let $\sigma_1, \sigma_2, \sigma_3$ be the 3 homomorphisms of R_f into the complex numbers. For integers x and y , we have:

$$|\text{Disc}(\mathbb{Z}[x\omega + y\theta])|^{1/2} = \begin{vmatrix} 1 & \dots & 1 \\ x\sigma_1(\omega) + y\sigma_1(\theta) & \dots & x\sigma_3(\omega) + y\sigma_3(\theta) \\ (x\sigma_1(\omega) + y\sigma_1(\theta))^2 & \dots & (x\sigma_3(\omega) + y\sigma_3(\theta))^2 \end{vmatrix}$$

Expand out and collect monomials, now treating x and y as variables. Because $|\sigma_i(\omega)| \ll |\omega|$ and $|\sigma_i(\theta)| \ll |\theta|$, the absolute value of the coefficient of $x^i y^{3-i}$ in the expression above is $\ll |\omega|^i |\theta|^{3-i}$. Because $|f(x, y)|$ is the index of $\mathbb{Z}[x\omega + y\theta]$ in R_f , we have:

$$|a| \ll |\omega|^3 \Delta^{-1/2} \ll e^{3\epsilon} \Delta^{3p_1-1/2}$$

$$|b| \ll |\omega|^2 |\theta| \Delta^{-1/2} \ll e^{3\epsilon} \Delta^{2p_1+p_2-1/2}$$

$$|c| \ll |\omega| |\theta|^2 \Delta^{-1/2} \ll e^{3\epsilon} \Delta^{p_1+2p_2-1/2}$$

$$|d| \ll |\theta|^3 \Delta^{-1/2} \ll e^{3\epsilon} \Delta^{3p_2-1/2}$$

□

Our next result is a lower bound on the number of distinct binary cubic forms with “small” coefficients giving rise to isomorphic cubic rings. Let ℓ_1 be the closed line segment from $(0, 1/2)$ to $(1/4, 1/4)$.

Lemma 3.3.2. *There exists D such that for every $p \in \ell_1$, every f , and every C, X , if $f \in CB(p, X)$ then $\#\{f' \in DCB(p, X) \cap V_{\mathbb{Z}} \mid R_{f'} \simeq R_f\} \geq X^{p_2-p_1}$.*

Proof. Act on f by elements of $\text{GL}_2(\mathbb{Z})$ of the form

$$\begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$$

where $|u| \leq X^{p_2-p_1}$. □

For a form f , let $\{1, \omega, \theta\}$ denote the basis of R_f specified by the explicit multiplication table (3.4). The following lemma shows if f has “small” coefficients, then $\{1, \omega, \theta\}$ is a “small” basis.

Lemma 3.3.3. *For every $p \in \ell_1$, every C, X , and every f , if $f \in CB(p, X)$ then $|\omega| \ll_C X^{p_1}$ and $|\theta| \ll_C X^{p_2}$.*

Proof. The explicit multiplication coefficients imply that:

$$\begin{aligned} |\omega|^2 &\ll |\omega^2| \\ &\ll_C \max\{|ac|, |b||\omega|, |a||\theta|\} \\ &\ll_C \max\{X^{2p_1}, X^{p_1}|\omega|, X^{2p_1-p_2}|\theta|\} \end{aligned}$$

$$\begin{aligned} |\theta|^2 &\ll |\theta^2| \\ &\ll_C \max\{|bd|, |d||\omega|, |c||\theta|\} \\ &\ll_C \max\{X^{2p_2}, X^{2p_2-p_1}|\omega|, X^{p_2}|\theta|\} \end{aligned}$$

Applying Lemma 6.0.2 completes the proof. □

Our next lemma shows an upper bound on the number of distinct binary cubic forms with “small” coefficients giving rise to isomorphic cubic rings.

Lemma 3.3.4. *For every C, X , every f , and every $p \in \ell_1$, if $f \in CB(p, X)$ and $X/2 \leq \Delta \leq X$, there are $\ll_C X^{p_2-p_1}$ distinct binary cubic forms $f' \in CB(p, X)$ such that $R_{f'} \simeq R_f$.*

Proof. Let $\{1, \omega, \theta\}$ be the basis of R_f specified by (3.4). We have:

$$\begin{aligned} X^{1/2} &\asymp \Delta^{1/2} && \text{because } X/2 \leq \Delta \leq X \\ &\ll |\omega||\theta| \\ &\ll_C X^{p_1+p_2} && \text{by Lemma 3.3.3} \\ &= X^{1/2} \end{aligned}$$

Therefore, $|\omega||\theta| \asymp_C \Delta^{1/2}$.

Suppose $f' \in CB(p, X)$ is an integral binary cubic form such that $R_{f'} \simeq R_f$. Let $\{1, \omega', \theta'\}$ denote the basis corresponding to f' . Then Lemma 3.3.3 implies that $|\omega'| \ll_C X^{p_1}$ and $|\theta'| \ll_C X^{p_2}$.

Express ω' and θ' in terms of the basis $\{1, \omega, \theta\}$, i.e. write

$$\omega' = a + b\omega + c\theta$$

$$\theta' = d + e\omega + f\theta$$

where $a, b, c, d, e, f \in \mathbb{Z}$.

Because $|\omega| |\theta| \asymp_C \Delta^{1/2}$, we have:

$$|\omega'| \asymp_C \max\{|a|, |b| |\omega|, |c| |\theta|\}$$

$$|\theta'| \asymp_C \max\{|d|, |e| |\omega|, |f| |\theta|\}$$

The integral binary cubic form f' is determined by the choice of b, c, e , and f . The number of choices of b, c , and f is $\ll_C 1$. The number of choices of e is $\ll_C X^{p_2 - p_1}$. Therefore there are $\ll_C X^{p_2 - p_1}$ distinct integral binary cubic forms $f' \in CB(p, X)$ such that $R_{f'} \simeq R_f$. $\square$

The following lemma explicitly bounds the successive minima of R_f for f with “small” coefficients.

Lemma 3.3.5. *For every C, X , every $p \in \ell_1$, and every f , if $f \in CB(p, X)$ and $\frac{X}{2} \leq \Delta$ then*

$$\lambda_i(R_f) \asymp_C \Delta^{p_i}$$

for $i = 1, 2$.

Proof. We have:

$$\begin{aligned} \lambda_1(R)\lambda_2(R) &\ll |\omega| |\theta| && \text{by definition of successive minima} \\ &\ll_C X^{p_1} X^{p_2} && \text{by Lemma 3.3.3} \\ &\ll \Delta^{p_1} \Delta^{p_2} && \text{because } X/2 \leq \Delta \\ &\ll \Delta^{1/2} && \text{because } p_1 + p_2 = 1/2 \\ &\asymp \lambda_1(R)\lambda_2(R) && \text{by Minkowski's second theorem} \end{aligned}$$

Thus,

$$\lambda_i(R_f) \asymp_C \Delta^{p_i}$$

for $i = 1, 2$. $\square$

3.4 Computing density functions of cubic rings

Recall that ℓ_1 denotes the closed line segment from $(0, 1/2)$ to $(1/4, 1/4)$. We will also need the following two line segments. Let ℓ_2 denote the closed line segment from $(0, 1/2)$ to $(1/6, 1/3)$ and let ℓ_3 denote the closed line segment from $(1/6, 1/3)$ to $(1/4, 1/4)$.

Corollary 3.4.1. *For any permutation group $G \subseteq S_3$, the function $d_{\epsilon, G}$ has support contained in ℓ_1 . If G is transitive, then $d_{\epsilon, G}$ has support contained in ℓ_3 .*

Proof. This is a corollary of Theorem 1.1.2. □

For positive real numbers C and D , let $\exp[C, D]$ denote C^D .

Lemma 3.4.2 (Davenport's Lemma [17]). *Let B be a bounded, semi-algebraic set in $\mathbb{R}^n$ which is defined by at most k polynomial inequalities each having degree at most ℓ . Then the number of integer lattice points contained in the region B is*

$$\text{Vol}(B) + O(\max\{\text{Vol}(\overline{B}), 1\}),$$

where $\text{Vol}(\overline{B})$ denotes the greatest d -dimensional volume of any projection of B onto a coordinate subspace obtained by equating $n - d$ coordinates to zero, where d takes all values from 1 to $n - 1$. The implied constant in the second summand depends only on n , k , and ℓ .

Lemma 3.4.3. *For any C, X and $p \in \ell_1$, we have:*

$$\exp[X, 1 + \max\{0, 1/2 - 3p_1\}] \ll_p \#\{V_{\mathbb{Z}} \cap CB(p, X)\} \ll C^4 \exp[X, 1 + \max\{0, 1/2 - 3p_1\}].$$

In particular, the first implicit constant is independent of C and X , and the second implicit constant is independent of C , X , and p .

Proof. First suppose that $p \in \ell_3$ and $p \neq (1/6, 1/3)$. Then $\text{Vol}(CB(p, X)) = 2^4 C^4 X$. In this case, one sees that the projection of $CB(p, X)$ onto $a = 0$ has volume $2^3 C^3 \exp[X, 1 - (3p_1 - 1/2)]$, and the volume of any other coordinate projection is bounded above by this quantity. Lemma 3.4.2 now shows that there exists a constant $D \geq 1$, independent of C , X , and p , such that:

$$\begin{aligned} \#\{V_{\mathbb{Z}} \cap CB(p, X)\} &\leq 2^4 C^4 X + 2^3 C^3 D \exp[X, 1 - (3p_1 - 1/2)] \\ &\leq 2^5 D C^4 X \\ &\ll C^4 X \end{aligned}$$

We obtain the lower bound as follows:

$$\begin{aligned}
\#\{V_{\mathbb{Z}} \cap CB(p, X)\} &\geq \#\{V_{\mathbb{Z}} \cap B(p, X)\} \\
&\geq 2^4 X - D 2^3 \exp[X, 1 - (3p_1 - 1/2)] \\
&\gg_p X
\end{aligned}$$

Now suppose $p \in \ell_2$ and $p \neq (0, 1/2)$. Then every lattice point in $CB(p, X)$ satisfies $|a| \leq C$. For an integer $-C \leq i \leq C$, let $B_i \subseteq \mathbb{R}^3$ denote the subset of $CB(p, X)$ with $a = i$, projected onto $a = 0$. We will count the number of lattice points in each region B_i . An application of Lemma 3.4.2 shows that there exists a constant $D \geq 1$, independent of C , X and p , such that:

$$\begin{aligned}
\#\{V_{\mathbb{Z}} \cap CB(p, X)\} &= \sum_{i=-C}^C \#\{V_{\mathbb{Z}} \cap B_i(p, X)\} \\
&\leq (2C+1)(2^3 C^3 \exp[X, 1 + (1/2 - 3p_1)] + 2^2 C^2 D \exp[X, 1 + (1/2 - 3p_1) - p_1]) \\
&\ll C^4 \exp[X, 1 + (1/2 - 3p_1)]
\end{aligned}$$

Again, the lower bound follows from the fact that:

$$\begin{aligned}
\#\{V_{\mathbb{Z}} \cap CB(p, X)\} &\geq \#\{V_{\mathbb{Z}} \cap B(p, X)\} \\
&\geq 2^3 \exp[X, 1 + (1/2 - 3p_1)] - 2^2 D \exp[X, 1 + (1/2 - 3p_1) - p_1] \\
&\gg_p \exp[X, 1 + (1/2 - 3p_1)]
\end{aligned}$$

An analogous argument proves the lemma when $p = (0, 1/2)$. □

Proposition 3.4.4. *We have $\#\mathcal{F}_3(p, \epsilon, X) \ll e^{12\epsilon} \exp[X, 1 - (p_2 - p_1) + \max\{0, 1/2 - 3p_1\}]$ where the implicit constants are independent of ϵ , X , and p .*

Proof. Let S be the set of binary cubic forms arising from Minkowski bases of cubic rings in $\mathcal{F}_3(p, \epsilon, X)$. Lemma 3.3.1 implies that there exists a global constant C such that $f \in C e^{3\epsilon} B(p, X)$ for all $f \in S$. By Lemma 3.3.2, there exists a global constant D such that $\#\{f' \in D C e^{3\epsilon} B(p, X) \mid R_{f'} \simeq R_f\} \geq X^{p_2 - p_1}$ for all $f \in S$. Without loss of generality, we may suppose $D \geq 1$. Therefore, for all $f \in S$, we have $f \in D C e^{3\epsilon} B(p, X)$ and the ring R_f is obtained by at least $X^{p_2 - p_1}$ distinct

forms in $DCe^{3\epsilon}B(p, X)$. Therefore,

$$\begin{aligned}\#\mathcal{F}_3(p, \epsilon, X) &\leq \frac{\#\{DCe^{3\epsilon}B(p, X) \cap V_{\mathbb{Z}}\}}{\exp[X, p_2 - p_1]} \\ &\ll e^{12\epsilon} \exp[X, 1 + \max\{0, 1/2 - 3p_1\} - (p_2 - p_1)]. \quad \text{by Lemma 3.4.3}\end{aligned}$$

□

Recall that E is the trivial group.

Proposition 3.4.5. *There exists a constant C such that for all $\epsilon > C$, we have:*

1. *if $p \in \ell_1$, then $\#\mathcal{F}_3(p, \epsilon, X) \gg_p \exp[X, 1 + \max\{0, 1/2 - 3p_1\} - (p_2 - p_1)]$;*
2. *if $p \in \ell_3$, then $\#\mathcal{F}(p, \epsilon, S_3, X) \gg_p \exp[X, 1 - (p_2 - p_1)]$;*
3. *if $p \in \ell_1$, then $\#\mathcal{F}(p, \epsilon, \mathbb{Z}/2\mathbb{Z}, X) \gg_p \exp[X, 1 - p_1]$;*
4. *and if $p \in \ell_1$, then $\#\mathcal{F}(p, \epsilon, E, X) \gg_p \exp[X, 1/2]$.*

Proof. We first prove (1). Fix $p \in \ell_1$ and let f denote any integral binary cubic form. Lemma 3.3.5 shows that there exists a constant C such that for all $\epsilon > C$, if $f \in B(p, X)$ and $\frac{X}{2} \leq \Delta$, then f is (ϵ, X) -close to p . Let $S = \{f \in B(p, X) \cap V_{\mathbb{Z}} \mid \frac{X}{2} \leq \Delta \leq X\}$. Therefore for all $\epsilon > C$, we have

$$\begin{aligned}\#\mathcal{F}_3(p, \epsilon, X) &\geq \frac{\#S}{\max_{f \in S} \#\{f' \in B(p, X) \cap V_{\mathbb{Z}} \mid R_{f'} \simeq R_f\}} \\ &\asymp_p \frac{\#\{f \in B(p, X) \cap V_{\mathbb{Z}}\}}{\max_{f \in S} \#\{f' \in B(p, X) \cap V_{\mathbb{Z}} \mid R_{f'} \simeq R_f\}} \quad \text{by the definition of } B(p, X) \\ &\gg \frac{\#\{f \in B(p, X) \cap V_{\mathbb{Z}}\}}{\exp[X, p_2 - p_1]} \quad \text{by Lemma 3.3.4} \\ &\gg_p \frac{\exp[X, 1 + \max\{0, 1/2 - 3p_1\}]}{\exp[X, p_2 - p_1]} \quad \text{by Lemma 3.4.3} \\ &= \exp[X, 1 + \max\{0, 3p_1 - 1/2\} - (p_2 - p_1)].\end{aligned}$$

If an integral binary cubic form is irreducible and has a nonsquare discriminant, then it has Galois group S_3 . Therefore, to prove (2) it suffices to show that there exists a constant C such that the set

$$\{f \in CB(p, X) \cap V_{\mathbb{Z}} \mid \frac{X}{2} \leq \Delta \leq X, \Delta \equiv 5 \pmod{5}, f \text{ is irreducible modulo } 7\}$$

forms a positive proportion of S as $S \rightarrow \infty$. As these are congruence conditions, the statement

above follows from the fact that there exists C and f such that $\Delta \equiv 5 \pmod{5}$ and f is irreducible modulo 7, and for every $p \in \ell_3$, there exists a form $f \in \bigcup_X CB(p, X)$.

Similarly, if an integral binary cubic form has precisely one root with multiplicity 1, then it has Galois group $\mathbb{Z}/2\mathbb{Z}$. So, to prove (3) we simply replace S with

$$S \cap \{f \in B(p, X) \cap V_{\mathbb{Z}} \mid a = 0, \text{ Disc}(f) \not\equiv 0 \pmod{5} \text{ and } f \text{ has precisely 1 root modulo 5}\}.$$

Again, it is necessary (but easy) to check that for $p \in \ell_1$ and for X sufficiently large we have

$$S \cap \{f \in B(p, X) \cap V_{\mathbb{Z}} \mid a = 0, \text{ Disc}(f) \not\equiv 0 \pmod{5} \text{ and } f \text{ has precisely 1 root modulo 5}\} \neq \emptyset.$$

If an integral binary cubic form has 3 distinct roots, then its Galois group is trivial. So, to prove (4) it suffices to replace S with

$$S \cap \{f \in B(p, X) \cap V_{\mathbb{Z}} \mid \text{Disc}(f) \not\equiv 0 \pmod{5} \text{ and } a = d = 0\}.$$

Again, it is necessary (but easy) to check that for $p \in \ell_1$ and for X sufficiently large we have

$$S \cap \{f \in B(p, X) \cap V_{\mathbb{Z}} \mid \text{Disc}(f) \not\equiv 0 \pmod{5} \text{ and } a = d = 0\} \neq \emptyset.$$

□

We now easily compute the density function of S_3 -rings.

Proof of Theorem 1.2.1. Corollary 3.4.1 shows that the support of d_{ϵ, S_3} is contained in ℓ_3 . If $p \in \ell_3$, then combining Proposition 3.4.4 and Proposition 3.4.5 shows that there exists a constant C such that for all $\epsilon > C$, we have $\#\mathcal{F}(p, \epsilon, S_3, X) \asymp_{p, \epsilon} X^{1-(p_2-p_1)}$. Thus for all $p \in \ell_3$, we have

$$d_{\epsilon, S_3}(p) = \lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, S_3, X) + 1)}{\log X} = \lim_{X \rightarrow \infty} \frac{\log(X^{1-(p_2-p_1)})}{\log X} = 1 - (p_2 - p_1).$$

□

We now produce an upper bound for $\mathbb{Z}/2\mathbb{Z}$ -rings “near” p . The following proof is a slightly modified version of the argument given by Bhargava, Shankar, and Tsimerman in Lemma 21 of [7].

Lemma 3.4.6. *For all $p \in \ell_1$ and $\nu \in \mathbb{R}_{>0}$, the number of reducible integral binary cubic forms in $B(p, X)$ is $\ll_{\nu} X^{3/2-3p_1+\nu}$.*

Proof. By Davenport's lemma, the number of forms $f \in B(p, X)$ with $a = 0$ is $\ll X^{3/2-3p_1}$. Similarly, the number of forms $f \in B(p, X)$ with $d = 0$ is $\ll X^{3/2-3p_2} \leq X^{3/2-3p_1}$.

Let's now count the number of reducible integral binary cubic forms $f(x, y) \in B(p, X)$ with $ad \neq 0$. The total number of possibilities for the triple (a, b, d) is $O(X^{1-p_2})$. Suppose the values a, b, d are now fixed, and consider the possible number of values c such that the resulting form $f(x, y)$ is reducible. For $f(x, y)$ to be reducible, it must have some linear factor $rx + sy$ where $r, s \in \mathbb{Z}$ are relatively prime. Then r must be a factor of a , while s must be a factor of d ; thus they are both determined up to $O_\nu(X^\nu)$ possibilities. Once r and s are determined, computing $f(-s, r)$ and setting it equal to zero then uniquely determines c (if it is an integer at all) in terms of a, b, d, r, s . Thus the total number of reducible forms f with $ad \neq 0$ is $\ll_\nu X^{1-p_2+\nu} \ll_\nu X^{3/2-3p_1+\nu}$. $\square$

Lemma 3.4.7. *If $p \in \ell_1$, then $\#\mathcal{F}(p, \epsilon, \mathbb{Z}/2\mathbb{Z}, X) \ll_{\nu, \epsilon} X^{1-p_1+\nu}$.*

Proof. To obtain a proof of this lemma, take the proof of Proposition 3.4.4 and

1. replace $\mathcal{F}_3(p, \epsilon, X)$ with $\mathcal{F}(p, \epsilon, \mathbb{Z}/2\mathbb{Z}, X)$;
2. replace $\{DCe^{3\epsilon}B(p, X) \cap V_\mathbb{Z}\}$ with $\{f \in DCe^{3\epsilon}B(p, X) \cap V_\mathbb{Z} \mid f \text{ is reducible}\}$;
3. and replace the use of Lemma 3.4.3 with Lemma 3.4.6.

$\square$

We can now compute the density function of $\mathbb{Z}/2\mathbb{Z}$ -rings.

Proof of Theorem 3.1.1. Corollary 3.4.1 shows that the support of $d_{\epsilon, \mathbb{Z}/2\mathbb{Z}}$ is contained in ℓ_1 . If $p \in \ell_1$, then combining Lemma 3.4.7 and Proposition 3.4.5 shows that there exists a constant C such that for all $\epsilon > C$, we have

$$X^{1-p_1} \ll_p \#\mathcal{F}(p, \epsilon, \mathbb{Z}/2\mathbb{Z}, X) \ll_{\nu, \epsilon} X^{1-p_1+\nu}$$

Thus for all $p \in \ell_1$, we have

$$d_{\epsilon, \mathbb{Z}/2\mathbb{Z}}(p) = \lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, \mathbb{Z}/2\mathbb{Z}, X) + 1)}{\log X} = \lim_{X \rightarrow \infty} \frac{\log X^{1-p_1}}{\log X} = 1 - p_1.$$

We now compute $d_{\epsilon, \mathbb{Z}/2\mathbb{Z}}^{\max}$. Maximal $\mathbb{Z}/2\mathbb{Z}$ -rings are precisely rings that can be written as $\mathbb{Z} \oplus \mathcal{O}$ where $\mathcal{O}$ is a maximal order in a quadratic field; moreover, $\text{Disc}(\mathbb{Z} \oplus \mathcal{O}) = \text{Disc}(\mathcal{O})$. Hence, for

any maximal $\mathbb{Z}/2\mathbb{Z}$ -ring, we have $\lambda_1 = |(1, 0)| = 1/\sqrt{3}$. Moreover, the number of quadratic fields of absolute discriminant $\leq X$ is $\asymp X$. Hence, for ϵ sufficiently large, we have:

$$d_{\epsilon, \mathbb{Z}/2\mathbb{Z}}^{\max}(p) = \begin{cases} 1 & \text{if } p = (0, 1/2) \\ 0 & \text{else} \end{cases}$$

□

Lemma 3.4.8. *For any $p \in \ell_1$, the number of integral totally reducible binary cubic forms with nonzero discriminant in $B(p, X)$ is $\ll_{\nu} X^{1/2+(p_2-p_1)+\nu}$.*

Proof. The proof proceeds in cases.

1. The number of forms with $a = d = 0$ is $\ll X^{1/2}$.
2. Now suppose $a = 0$ and $d \neq 0$. Then the total number of possibilities for the pair (b, d) is $O(X^{p_1+3p_2-1/2})$. If $b = 0$ as well, then the discriminant of the form is 0. So, we may assume $b \neq 0$. Suppose the values of b and d are now fixed and consider the possible number of values c such that the resulting form $f(x, y)$ is totally reducible. For $f(x, y)$ to be totally reducible, it must have some linear factor $rx + sy$ where $r, s \in \mathbb{Z}$ are relatively prime and $rs \neq 0$. Then r must be a factor of b , while s must be a factor of d ; thus they are both determined up to $O_{\nu}(X^{\nu})$ possibilities. Once r and s are determined, computing $f(-s, r)$ and setting it equal to zero then uniquely determines c (if it is an integer at all) in terms of b, d, r, s . Thus the total number of such forms is $O_{\nu}(X^{p_1+3p_2-1/2+\nu})$.
3. Now suppose $a \neq 0$ and $d = 0$. An analogous argument to the previous case shows that the total number of such forms is $O_{\nu}(X^{p_2+3p_1-1/2+\nu})$.
4. If $ad \neq 0$, then the total number of possibilities for the tuple (a, d) is $O(X^{3p_1+3p_2-1})$. For $f(x, y)$ to be totally reducible, it must have two distinct linear factor $r_1x + s_1y$ and $r_2x + s_2y$ where $r_i, s_i \in \mathbb{Z}$ are relatively prime. As before, r_i must be a factor of a , while s_i must be a factor of d ; thus they are both determined up to $O_{\nu}(X^{\nu})$ possibilities. The two equations $f(-s_1, r_1) = 0$ and $f(-s_2, r_2) = 0$ determine b and c , unless

$$\det \begin{pmatrix} s_1^2 r_1 & -s_1 r_1^2 \\ s_2^2 r_2 & -s_2 r_2^2 \end{pmatrix} = 0.$$

Suppose the above determinant is zero. We expand out the determinant to see that

$$0 = \det \begin{pmatrix} s_1^2 r_1 & -s_1 r_1^2 \\ s_2^2 r_2 & -s_2 r_2^2 \end{pmatrix} = s_1 r_1^2 s_2^2 r_2 - s_1^2 r_1 s_2 r_2^2.$$

Because $ad \neq 0$, we have $s_1 r_1 s_2 r_2 \neq 0$, so $r_1 s_2 = s_1 r_2$. Because (r_i, s_i) are relatively prime, we have $r_1 = r_2$ and $s_1 = s_2$, which is a contradiction because we assumed the linear factors $r_1 x + s_1 y$ and $r_2 x + s_2 y$ are distinct. Thus the total number of such forms is $\ll_\nu (X^{3p_1+3p_2-1+\nu})$.

□

Let E denote the trivial group.

Lemma 3.4.9. *If $p \in \ell_1$, then $\#\mathcal{F}_3(p, \epsilon, E, X) \ll_{\nu, \epsilon} X^{1/2+\nu}$.*

Proof. To obtain a proof of this lemma, take the proof of Proposition 3.4.4 and

1. replace $\mathcal{F}_3(p, \epsilon, X)$ with $\mathcal{F}(p, \epsilon, E, X)$;
2. replace $\{DCe^{3\epsilon}B(p, X) \cap V_{\mathbb{Z}}\}$ with

$$\{f \in DCe^{3\epsilon}B(p, X) \cap V_{\mathbb{Z}} \mid f \text{ is totally reducible and nondegenerate}\};$$

3. and replace the use of Lemma 3.4.3 with Lemma 3.4.8.

□

Proof of Theorem 3.1.2. Corollary 3.4.1 shows that the support of $d_{\epsilon, E}$ is contained in ℓ_1 . If $p \in \ell_1$, then combining Lemma 3.4.9 and Proposition 3.4.5 shows that there exists a constant C such that for all $\epsilon > C$,

$$X^{1/2} \ll_p \#\mathcal{F}(p, \epsilon, E, X) \ll_{\nu, \epsilon} X^{1/2+\nu}$$

Thus for all $p \in \ell_1$, we have $d_{\epsilon, E}(p) = 1/2$. We now compute $d_{\epsilon, E}^{\max}$. There is a unique maximal E -ring (which is $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$) so $d_{\epsilon, E}^{\max} = 0$. □

3.5 Reduction theory of binary n -ic forms

We now generalize the reduction theory of binary cubic forms that we developed in Section 3.3 to general degree n . This will be useful to prove our later results on binary quartic and binary quintic

forms. In this section, we will discuss Birch, Merriman, and Nakagawa's [9, 26] construction of a rank n ring from an integral binary n -ic form. We develop the relationship between:

1. nondegenerate rank n rings R equipped with “small” bases arising from integral binary n -ic forms;
2. and integral binary n -ic forms with “small” coefficients.

For the rest of this section, let $f = f_0x^n + \cdots + f_ny^n \in \text{Sym}^n \mathbb{Z}^2$ denote a binary n -ic form. To a form f , Birch, Merriman, and Nakagawa [9, 26] associated a rank n ring R_f equipped with a basis $\{\zeta_0 = 1, \zeta_1, \dots, \zeta_{n-1}\}$. The multiplication table of the basis $\{\zeta_0 = 1, \zeta_1, \dots, \zeta_{n-1}\}$ is given by:

$$\zeta_i \zeta_j = \sum_{\max\{i+j-n, 1\} \leq k \leq i} f_{i+j-k} \zeta_k + \sum_{j < k \leq \min\{i+j, n\}} f_{i+j-k} \zeta_k$$

for $1 \leq i, j \leq n-1$ where $\zeta_n := -f_n$. An element $\gamma \in \text{GL}_2(\mathbb{Z})$ acts on f via

$$(\gamma f)(x, y) := f((x, y)\gamma);$$

this action of $\text{GL}_2(\mathbb{Z})$ on $\text{Sym}^n \mathbb{Z}^2$ induces an action of $\text{GL}_2(\mathbb{Z})$ on the basis $\{\zeta_1, \dots, \zeta_{n-1}\}$ of $R_f/\mathbb{Z}$. This action has an invariant called the *discriminant*, which is a homogeneous polynomial of degree $2n-2$ in the coefficients of f . Nakagawa's construction is *discriminant-preserving*: we have $\text{Disc}(R_f) = \text{Disc}(f)$. In this section, let $\Delta = |\text{Disc}(f)|$. We say a form f is *nondegenerate* if $\Delta \neq 0$. For the rest of this section, any f we consider will be nondegenerate.

Recall that in Section 3.3, for any point $p \in \mathbb{R}^2$ and any positive real number X , we defined a box $B(p, X) \subseteq \text{Sym}^3 \mathbb{R}^2$. We roughly showed that integral binary cubic forms lying in this box correspond to cubic rings of discriminant $\leq X$ equipped with a “short” basis that were “close” to p . We'll now generalize our definition of the box $B(p, X) \subseteq \text{Sym}^3 \mathbb{R}^2$ for general binary n -ic forms. Let

$$k := \frac{1}{2(1 + \cdots + (n-1))},$$

and define ℓ to be the closed line segment from $(0, k)$ to $(k/2, k/2)$.

Let $L: \ell \rightarrow \mathbb{R}^{n-1}$ be the linear map sending the point $(0, k)$ to $(k, 2k, \dots, (n-1)k)$ and sending the point $(k/2, k/2)$ to $\frac{1}{2(n-1)}(1, \dots, 1)$. For a point $r = (r_1, r_2) \in \ell$ and a positive real number X , define $B_n^{\text{bin}}(r, X)$ to be the subset of $\text{Sym}^n \mathbb{R}^2$ such that:

$$|f_i| \leq X^{(n-i)r_1 + ir_2}$$

for all $0 \leq i \leq n$. The boxes $B_n^{\text{bin}}(r, X) \subseteq \text{Sym}^n \mathbb{R}^2$ are the natural generalization of the box $B(p, X) \subseteq \text{Sym}^3 \mathbb{R}^2$ that we defined in Section 3.3. if $n = 3$, then a computation shows that

$$B_n^{\text{bin}}(r, X) = B(L(r), X).$$

In what follows, we will relate a form being in $B_n^{\text{bin}}(r, X)$ to the ring R_f being “close” to $L(r)$.

We’ll first show that if R_f is “close” to $L(r)$ and $\{1, \zeta_1, \dots, \zeta_{n-1}\}$ is “small”, then f is roughly contained in this box $B_n^{\text{bin}}(r, X)$. Our proof will require the following beautiful formula of Fess. Given a nondegenerate rank n ring R equipped with a basis $1, \zeta_1, \dots, \zeta_{n-1}$ and an element $\alpha \in R$, let M_α be an $n \times n$ matrix such that

$$\begin{bmatrix} 1 & \alpha & \dots & \alpha^2 \end{bmatrix} = M_\alpha \begin{bmatrix} 1 & \zeta_1 & \dots & \zeta_{n-1} \end{bmatrix}^t$$

A nondegenerate rank n ring R equipped with a basis $1, \zeta_1, \dots, \zeta_{n-1}$ naturally gives rise to an *index form*, defined by:

$$\begin{aligned} I: R/\mathbb{Z} &\longrightarrow \mathbb{Z} \\ \alpha &\longrightarrow \det(M_\alpha) \end{aligned}$$

The basis $\{\zeta_1, \dots, \zeta_{n-1}\}$ of $R/\mathbb{Z}$ presents the index form as a homogeneous polynomial with integer coefficients of degree $\binom{n}{2}$ in $n - 1$ variables. In this way, a nondegenerate integral binary n -ic form f naturally gives rise to a homogeneous polynomial I_f of degree $\binom{n}{2}$ in $n - 1$ variables.

Theorem 3.5.1 (Fess [21], Theorem 3.2.4). *For any $f \in \text{Sym}^n \mathbb{Z}^2$, we have:*

$$I_f(x^{n-2}, x^{n-3}y, \dots, y^{n-2}) = f(x, y)^{\binom{n-1}{2}}$$

Our proof strategy is as follows. Suppose R_f is “close” to $L(r)$ and $\{1, \zeta_1, \dots, \zeta_{n-1}\}$ is “small”. Then we use this information to bound the sizes of the coefficients of the index form I_f , and hence the sizes of the coefficients of the binary form $I_f(x^{n-2}, x^{n-3}y, \dots, y^{n-2})$. By Fess’ index formula, we have obtained a bound on the coefficients of $f(x, y)^{\binom{n-1}{2}}$; a classical theorem of Gelfand (Lemma 3.5.3) then gives a bound on the coefficients of $f(x, y)$.

Let θ denote a positive real number. We say f gives rise to a θ -reduced basis if every pair of elements of the basis $1, \zeta_1, \dots, \zeta_{n-1}$ of R_f have angle greater than θ in the Minkowski embedding of

R_f . For a positive real number ϵ , we say f is (ϵ, Δ) -close to a point $p \in \mathbb{R}^{n-1}$ if $\Delta > 1$ and R_f is (ϵ, Δ) -close to p . Let $r = (r_1, r_2) \in \ell_1$ denote a point.

Proposition 3.5.2. *For all $\theta, \epsilon \in \mathbb{R}_{>0}$ and all $n \in \mathbb{Z}_{>1}$, there exists $C_{n,\theta,\epsilon} \in \mathbb{R}_{>0}$ such that for all nondegenerate $f \in \text{Sym}^n \mathbb{Z}^2$ and all $r \in \ell$, if $\Delta > 0$ and f is (ϵ, Δ) -close to $L(r)$ and f gives rise to a θ -reduced basis, then $f \in C_{n,\theta,\epsilon} B_n^{\text{bin}}(r, \Delta)$.*

Proof. View I_f as a homogeneous polynomial of degree $\binom{n}{2}$ with integer coefficients in $n-1$ variables $x_1, \dots, x_{n-1}$. For any $\mathbf{k} = (k_1, \dots, k_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ such that $\sum_{\ell=1}^{n-1} k_\ell = \binom{n}{2}$, let $a_{\mathbf{k}}$ denote the coefficient of $\prod_{\ell=1}^{n-1} x_\ell^{k_\ell}$ in I_f . We now bound $a_{\mathbf{k}}$. Let $\sigma_1, \dots, \sigma_n$ be the n homomorphisms of R_f into the complex numbers. For an element $\alpha = \sum_{\ell=0}^{n-1} x_\ell \zeta_\ell$, we have:

$$|\text{Disc}(\mathbb{Z}[\alpha])|^{1/2} = \begin{vmatrix} 1 & \dots & 1 \\ \sum_{\ell=0}^{n-1} x_\ell \sigma_1(\zeta_\ell) & \dots & \sum_{\ell=0}^{n-1} x_\ell \sigma_1(\zeta_\ell) \\ \dots & \dots & \dots \\ (\sum_{\ell=0}^{n-1} x_\ell \sigma_1(\zeta_\ell))^{n-1} & \dots & (\sum_{\ell=0}^{n-1} x_\ell \sigma_n(\zeta_\ell))^{n-1} \end{vmatrix}$$

Expand the determinant above and collect monomials. Observe that because $|\sigma_i(\zeta_\ell)| \ll_n |\zeta_\ell|$, the coefficient of $\prod_{\ell=1}^{n-1} x_\ell^{k_\ell}$ in the determinant of the matrix above is $\ll_n \prod_{\ell=1}^{n-1} |\zeta_\ell|^{k_\ell}$. Because

$$|I_f(\alpha)| = |\text{Disc}(\mathbb{Z}[\alpha])|^{1/2} \Delta^{-1/2},$$

we have:

$$\begin{aligned} |a_{\mathbf{k}}| &\ll_n \Delta^{-1/2} \prod_{\ell=1}^{n-1} |\zeta_\ell|^{k_\ell} \\ &\ll_{\epsilon,\theta,n} \Delta^{-1/2} \prod_{\ell=1}^{n-1} \Delta^{k_\ell L(r)_\ell} \\ &\leq \exp[\Delta, -1/2 + \sum_{\ell=1}^{n-1} k_\ell L(r)_\ell] \\ &\leq \exp[\Delta, -1/2 + \sum_{\ell=1}^{n-1} \frac{k_\ell}{n-2} ((n-1-\ell)L(r)_1 + (\ell-1)L(r)_{n-1})] \\ &\leq \exp[\Delta, -1/2 + \frac{L(r)_1}{n-2} \sum_{\ell=1}^{n-1} k_\ell (n-1-\ell) + \frac{L(r)_{n-1}}{n-2} \sum_{\ell=1}^{n-1} k_\ell (\ell-1)] \end{aligned} \tag{3.5}$$

We now use (3.5) to bound the coefficients of $I_f(x^{n-2}, x^{n-3}y, \dots, y^{n-2})$. For any $0 \leq i \leq (n-2)\binom{n}{2}$, let b_i denote the coefficient of $x^{(n-2)\binom{n}{2}-i} y^i$ in $I_f(x^{n-2}, x^{n-3}y, \dots, y^{n-2})$. We can express b_i as a

linear polynomial in the variables $a_{\mathbf{k}}$. Suppose $a_{\mathbf{k}} = a_{(k_1, \dots, k_{n-1})}$ appears in the expansion of b_i . Then substituting in $x^{n-1-\ell}y^{\ell-1}$ for x_ℓ in $\prod_{\ell=1}^{n-1} x_\ell^{k_\ell}$ gives $x^{(n-2)\binom{n}{2}-i}y^i$, so:

$$\begin{aligned} (n-2)\binom{n}{2} - i &= \sum_{\ell=1}^{n-1} k_\ell(n-1-\ell) \\ i &= \sum_{\ell=1}^{n-1} k_\ell(\ell-1) \end{aligned} \tag{3.6}$$

Substituting (3.6) into (3.5), we obtain:

$$|a_{\mathbf{k}}| \ll_{n,\epsilon,\theta} \exp[\Delta, -1/2 + \frac{L(r)_1}{n-2}((n-2)\binom{n}{2} - i) + \frac{L(r)_{n-1}}{n-2}i]. \tag{3.7}$$

Note that (3.7) is *not* dependent on the choice of $a_{\mathbf{k}}$! Thus:

$$|b_i| \ll_{n,\epsilon,\theta} \exp[\Delta, -1/2 + \frac{L(r)_1}{n-2}((n-2)\binom{n}{2} - i) + \frac{L(r)_{n-1}}{n-2}i] \tag{3.8}$$

We can write out the linear map L explicitly and obtain:

$$\frac{n-1}{2}(L(r)_1 + L(r)_{n-1}) = 1/2 \tag{3.9}$$

$$L(r)_1 = \frac{1}{2\binom{n}{2}} + \frac{\frac{1}{2(n-1)} - \frac{1}{2\binom{n}{2}}}{\frac{1}{4\binom{n}{2}}} r_1 \tag{3.10}$$

$$L(r)_{n-1} = \frac{n-1}{2\binom{n}{2}} + \frac{\frac{1}{2(n-1)} - \frac{n-1}{2\binom{n}{2}}}{\frac{1}{4\binom{n}{2}} - \frac{1}{2\binom{n}{2}}} \left(r_2 - \frac{1}{2\binom{n}{2}} \right). \tag{3.11}$$

Substitute (3.9), (3.10), and (3.11) into (3.8) and simplify to obtain:

$$|b_i| \ll_{n,\epsilon,\theta} \exp[\Delta, ((n-2)\binom{n}{2} - i)r_1 + ir_2] \tag{3.12}$$

Recall that Theorem 3.5.1 says:

$$I_f(x^{n-2}, x^{n-3}y, \dots, y^{n-2}) = f(x, y)^{\binom{n-1}{2}}$$

Let $M = \lfloor \Delta^{r_2-r_1} \rfloor$ and let $g(x, y) := f(Mx, y)$. For any $0 \leq i \leq (n-2)\binom{n}{2}$, let c_i denote the

coefficient of $x^{(n-2)\binom{n}{2}-i}y^i$ in $g(x, y)^{\binom{n-1}{2}}$. By Theorem 3.5.1, we have

$$g(x, y)^{\binom{n-1}{2}} = I_f(M^{n-2}x^{n-2}, M^{n-3}x^{n-3}y, \dots, y^{n-2})$$

Note that $c_i = M^{(n-2)\binom{n}{2}-i}b_i$; substituting in (3.12) gives:

$$|c_i| \ll_{n, \epsilon, \theta} \exp[\Delta, (n-2)\binom{n}{2}r_2].$$

For $0 \leq i \leq n$ let g_i be the coefficient of $x^{n-i}y^i$ in $g(x, y)$. By Lemma 3.5.3, for all $0 \leq i \leq n$ we have

$$|g_i| \ll_{n, \epsilon, \theta} \Delta^{nr_2}.$$

Because $g_i = M^{n-i}f_i$, we have

$$|f_i| \ll_{n, \epsilon, \theta} \Delta^{(n-i)r_1+ir_2}$$

for $0 \leq i \leq n$, completing the proof of the proposition. $\square$

For a polynomial $f(x_1, \dots, x_m) \in \mathbb{Z}[x_1, \dots, x_m]$, let $H(f)$ be the maximum of the absolute value of the coefficients of f .

Lemma 3.5.3 (Gelfand's Inequality [23], Proposition B.7.3). *Let $d_1, \dots, d_m$ be integers, and let $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_m]$ be polynomials whose product satisfies $\deg_{x_i}(f_1 \dots f_r) = d_m$ for each $1 \leq i \leq r$. Then*

$$\prod_i H(f_i) \leq e^{d_1 + \dots + d_m} H(f_1 \dots f_r).$$

For the rest of this section, let C, D denote positive real numbers, let $X \in \mathbb{R}_{>1}$, let $n \in \mathbb{Z}_{>1}$, and let $r \in \ell$.

Lemma 3.5.4. *If $f \in CB_n^{\text{bin}}(r, X)$ then*

$$|\zeta_i| \ll_{C, n} X^{L(r)_i}$$

for all $1 \leq i < n$.

Proof. Let $L(r)_0 = 0$. The explicit multiplication coefficients imply that

$$|\zeta_i|^2 \ll_{C, n} \max_{0 \leq j < n} \{X^{2L(r)_i - L(r)_j} |\zeta_j|\}.$$

Applying Lemma 6.0.2 completes the proof. $\square$

Lemma 3.5.5. *If $f \in CB_n^{\text{bin}}(r, X)$ and $X/2 \leq \Delta$ then*

$$\lambda_i(R_f) \asymp_{C,n} X^{L(r)_i}$$

for $1 \leq i \leq n-1$.

Proof. Follows from Lemma 3.5.4, Minkowski's second theorem, and the fact that

$$\sum_{i=1}^{n-1} L(r)_i = 1/2.$$

$\square$

Lemma 3.5.6. *If $f \in CB_n^{\text{bin}}(r, X)$ and $\Delta \geq X/2$, we have*

$$\#\{f' \in CB_n^{\text{bin}}(r, X) \cap \text{Sym}^n \mathbb{Z}^2 \mid \exists \gamma \in \text{GL}_2(\mathbb{Z}) \text{ s.t. } f' = \gamma f\} \ll_{C,n} X^{r_2-r_1}$$

Proof. By Lemma 3.5.4, the form f gives rise to a basis $\{\zeta_1, \dots, \zeta_{n-1}\}$ of $R_f/\mathbb{Z}$ with the property that

$$|\zeta_i| \ll_{C,n} X^{L(r)_i} \asymp_{C,n} \lambda_i(R_f)$$

for $1 \leq i \leq n-1$. Let $\gamma \in \text{GL}_2(\mathbb{Z})$ be such that $f' = \gamma f$ and $f' \in B_n^{\text{bin}}(r, X)$. Let $\{\zeta'_1, \dots, \zeta'_{n-1}\}$ be the basis of $R_{f'}/\mathbb{Z}$ corresponding to f' . Then again by Lemma 3.5.4, we have

$$|\zeta'_i| \ll_{C,n} X^{L(r)_i} \asymp_{C,n} \lambda_i(R_{f'}).$$

Write

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

for an element $\gamma \in \text{GL}_2(\mathbb{Z})$. As given by Nakagawa [26], the action of γ on the bases is given by the following matrix equation:

$$\begin{bmatrix} a^{n-2} & a^{n-3}b & \dots & ab^{n-3} & b^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ c^{n-2} & c^{n-3}d & \dots & cd^{n-3} & d^{n-2} \end{bmatrix} \begin{bmatrix} \zeta_1 \\ \dots \\ \zeta_{n-1} \end{bmatrix} = \begin{bmatrix} \zeta'_1 \\ \dots \\ \zeta'_{n-1} \end{bmatrix}$$

For our purposes, it is not important what the ... entries are. Thus:

$$\begin{aligned} |\zeta_1| &\asymp_{C,n} |\zeta'_1| \asymp_{C,n} \max_{1 \leq i \leq n-1} \{ |a^{n-1-i} b^{i-1}| |\zeta_i| \} \\ |\zeta_{n-1}| &\asymp_{C,n} |\zeta'_{n-1}| \asymp_{C,n} \max_{1 \leq i \leq n-1} \{ |c^{n-1-i} d^{i-1}| |\zeta_i| \} \end{aligned}$$

Thus, the number of choices of a, b, d is $\ll_{C,n} 1$, and the number of choices of c is $\ll_{C,n} X^{r_2-r_1}$. $\square$

Lemma 3.5.7. *There exists D such that for all f, n, r , and X , if $f \in CB_n^{\text{bin}}(r, X)$ then*

$$\#\{f' \in DCB_n^{\text{bin}}(r, X) \cap \text{Sym}^n \mathbb{Z}^2 \mid \exists \gamma \in \text{GL}_2(\mathbb{Z}) \text{ s.t. } f' = \gamma f\} \geq X^{r_2-r_1}$$

Proof. Act on f by elements of $\text{GL}_2(\mathbb{Z})$ of the form

$$\gamma = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$$

where $|u| \leq X^{r_2-r_1}$. $\square$

The following theorem will be useful later.

Theorem 3.5.8 (Evertse, Györy [20]). *For any nondegenerate rank n ring R , there are at most 2^{5n^2} classes of integral binary n -ic forms f such that $R \simeq R_f$.*

Proof of Theorem 1.2.4. By Lemma 3.5.5, there exists a constant C such that for all $\epsilon > C$, if $f \in B_n^{\text{bin}}(r, X)$ and $X/2 \leq \Delta$ and $1 < \Delta$, then R_f is (ϵ, Δ) -close to $L(r)$. By Lemma 3.5.6, for a form $f \in B_n^{\text{bin}}(r, X)$ with $X/2 \leq \Delta$, there are $\ll_n X^{r_2-r_1}$ $\text{GL}_2(\mathbb{Z})$ conjugates of f contained in $B_n^{\text{bin}}(r, X)$. Thus,

$$\begin{aligned} \#\mathcal{F}_n^{\text{bin}}(L(r), \epsilon, X) &\gg_n \frac{\#\{B_n^{\text{bin}}(r, X) \cap \text{Sym}^n \mathbb{Z}^2 \mid X/2 \leq \Delta \leq X\}}{X^{r_2-r_1}} \\ &\gg_n \frac{\#\{B_n^{\text{bin}}(r, X) \cap \text{Sym}^n \mathbb{Z}^2\}}{X^{r_2-r_1}} \\ &\gg_{r,n} \frac{\exp[X, \sum_{i=0}^n (n-i)r_1 + ir_2]}{\exp[X, r_2 - r_1]} \end{aligned} \tag{3.13}$$

Now observe that:

$$\sum_{i=0}^n (n-i)r_1 + ir_2 = \binom{n+1}{2} (r_1 + r_2) = \frac{n+1}{2n-2}. \tag{3.14}$$

Substituting (3.14) into (3.13) proves the theorem. $\square$

3.6 Special families of cubic rings

In this section we will prove Corollary 3.1.5 and Corollary 3.1.4.

Proof of Corollary 3.1.5. Let $\mathcal{F}^{\text{irr}}$ be the set of isomorphism classes of irreducible nondegenerate cubic rings, let $H: \mathcal{F}^{\text{irr}} \rightarrow \mathbb{R}_{>0}$ be the absolute discriminant, and let $p = (1/4, 1/4)$. We will prove that $(\mathcal{F}^{\text{irr}}, H)$ corresponds to p .

We first prove (3.2) by demonstrating that:

$$\lim_{\epsilon \rightarrow \infty} \limsup_{X \rightarrow \infty} \frac{\#\{R \in \mathcal{F}^{\text{irr}} \mid \Delta \leq X \text{ and } R \text{ is not } (\epsilon, X)\text{-close to } p\}}{\#\{R \in \mathcal{F}^{\text{irr}} \mid \Delta \leq X\}} = 0. \quad (3.15)$$

We bound the denominator using Proposition 3.4.5 and obtain:

$$\#\{R \in \mathcal{F}^{\text{irr}} \mid \Delta \leq X\} \gg X. \quad (3.16)$$

We will now upper bound the numerator; our proof strategy is as follows. We fix a positive integer k and count the number of rings $R \in \mathcal{F}^{\text{irr}}$ of bounded discriminant that are $(\epsilon/k, X)$ -close to some *other* point p' on the line segment ℓ_1 with the property that that p' has distance at least $\epsilon/\log X$ from p . We conclude by summing up across an appropriate set of points p' .

Let $k = 6$ and let

$$p_{i,\epsilon} := \left(p_1 - \frac{\epsilon(ik^{-1} + 1)}{\log X}, p_2 + \frac{\epsilon(ik^{-1} + 1)}{\log X} \right) \in \mathbb{R}^2$$

Let $j_{X,\epsilon}$ be the smallest integer such that $p_1 - \frac{\epsilon(j_{X,\epsilon}k^{-1} + 1)}{\log X} \leq 1/6$. The set $\{p_{i,\epsilon}\}_{i=1}^{j_{X,\epsilon}}$ will be our appropriate set of points. By Minkowski's second theorem, there exists a global constant C such that for all $\epsilon > C$, every element of $R \in \mathcal{F}^{\text{irr}}$ is (ϵ, Δ) -close to some point on the closed line segment from $(1/6, 1/3)$ to $(1/4, 1/4)$. Thus, for any $\epsilon > C$, we have:

$$\#\{R \in \mathcal{F}^{\text{irr}} \mid \Delta \leq X \text{ and } R \text{ is not } (\epsilon, X)\text{-close to } (1/4, 1/4)\} \quad (3.17)$$

$$\leq \sum_{i=1}^{j_{X,\epsilon}} \#\{R \in \mathcal{F}^{\text{irr}} \mid \Delta \leq X \text{ and } R \text{ is } (\epsilon/k, X)\text{-close to } p_{i,\epsilon}\} \quad (3.18)$$

Proposition 3.4.4 proves that each of the terms in the sum in (3.18) is

$$\ll e^{-2\epsilon(ik^{-1} + 1)} e^{12\epsilon/k} X,$$

where the implied constant is independent of i and ϵ . Thus, we obtain that (3.18) is

$$\ll X e^{12\epsilon/k} \sum_{i=1}^{j_{X,\epsilon}} e^{-2\epsilon(ik^{-1}+1)} \quad (3.19)$$

$$\leq X e^{12\epsilon/k} \frac{e^{-2\epsilon(k^{-1}+1)}}{1 - e^{-2\epsilon k^{-1}}} \quad (3.20)$$

Plugging (3.20) into the numerator of (3.15), and plugging (3.16) into the denominator of (3.15), we obtain:

$$\limsup_{X \rightarrow \infty} \frac{\#\{R \in \mathcal{F}^{\text{irr}} \mid \Delta \leq X \text{ and } R \text{ is not } (\epsilon, X)\text{-close to } p\}}{\#\{R \in \mathcal{F}^{\text{irr}} \mid \Delta \leq X\}} \ll e^{12\epsilon/k} \frac{e^{-2\epsilon(k^{-1}+1)}}{1 - e^{-2\epsilon k^{-1}}} \quad (3.21)$$

where the implicit constant is independent of ϵ . Now observe that:

$$\lim_{\epsilon \rightarrow \infty} e^{12\epsilon/k} \frac{e^{-2\epsilon(k^{-1}+1)}}{1 - e^{-2\epsilon k^{-1}}} = \lim_{\epsilon \rightarrow \infty} \frac{e^{-2\epsilon k^{-1}}}{1 - e^{-2\epsilon k^{-1}}} = 0.$$

This proves (3.15), and (3.3) is a corollary of Proposition 3.4.4 and Proposition 3.4.5.

Now let $\mathcal{F}^{\text{red}}$ be the set of isomorphism classes of reducible nondegenerate cubic rings, let $H: \mathcal{F}^{\text{red}} \rightarrow \mathbb{R}_{>0}$ be the absolute discriminant, and let $p = (0, 1/2)$. We will now prove that $(\mathcal{F}^{\text{red}}, H)$ corresponds to p . The second condition is easy to see; observe that for any fixed ϵ and Δ large enough with respect to ϵ , Theorem 1.1.2 implies that any ring (ϵ, Δ) -close to p is reducible. Hence, (3.3) follows immediately from Proposition 3.4.4 and Proposition 3.4.5. We now prove that (3.2) holds by demonstrating:

$$\lim_{\epsilon \rightarrow \infty} \limsup_{X \rightarrow \infty} \frac{\#\{R \in \mathcal{F}^{\text{red}} \mid \Delta \leq X \text{ and } R \text{ is not } (\epsilon, X)\text{-close to } p\}}{\#\{R \in \mathcal{F}^{\text{red}} \mid \Delta \leq X\}} = 0 \quad (3.22)$$

By considering maximal reducible orders, we obtain: $\{R \in \mathcal{F}^{\text{red}} \mid \Delta \leq X\} \gg X$. Again let k be some integer, to fixed later, and let

$$p_{i,\epsilon} := \left(p_1 + \frac{\epsilon(ik^{-1}+1)}{\log X}, p_2 - \frac{\epsilon(ik^{-1}+1)}{\log X} \right) \in \mathbb{R}^2.$$

Let $j_{X,\epsilon}$ be the largest integer such that $p_1 + \epsilon(j_{X,\epsilon}k^{-1}+1) \log X < 1/6$ and let $k_{X,\epsilon}$ be the smallest integer such that $p_1 + \epsilon(j_{X,\epsilon}k^{-1}+1) \log X \geq 1/4$. There exists a constant C such that for all $\epsilon > C$,

we have:

$$\begin{aligned}
& \#\{R \in \mathcal{F}^{\text{red}} \mid \Delta \leq X \text{ and } R \text{ is not } (\epsilon, X)\text{-close to } p\} \\
& \leq \sum_{i=1}^{j_{X,\epsilon}} \#\{R \in \mathcal{F}^{\text{red}} \mid \Delta \leq X \text{ and } R \text{ is } (\epsilon/k, X)\text{-close to } p_{i,\epsilon}\} \\
& \quad + \sum_{i=j_{X,\epsilon}+1}^{k_{X,\epsilon}} \#\{R \in \mathcal{F}^{\text{red}} \mid \Delta \leq X \text{ and } R \text{ is } (\epsilon/k, X)\text{-close to } p_{i,\epsilon}\}
\end{aligned}$$

Using Lemma 3.4.6, we see the second term is

$$\ll_{\nu,\epsilon} \sum_{i=j_{X,\epsilon}+1}^{k_{X,\epsilon}} X^{5/6+\nu} \ll X^{5/6+\nu} \log X = o(X).$$

As before, for $1 \leq i \leq j_{X,\epsilon}$, Proposition 3.4.4 implies:

$$\#\{R \in \mathcal{F}^{\text{red}} \mid \Delta \leq X \text{ and } R \text{ is } (\epsilon/k, X)\text{-close to } p_{i,\epsilon}\} \ll e^{12\epsilon/k} X e^{-2\epsilon(ik^{-1}+1)}$$

Fixing k to be large enough and summing the first term proves (3.22).

□

In fact, in the proof of Corollary 3.1.5, we showed that the number of isomorphism classes of irreducible cubic rings of absolute discriminant $\leq X$ is $\asymp X$! We also showed that the number of isomorphism classes of reducible cubic rings of absolute discriminant $\leq X$ is $\asymp X$.

Proof of Corollary 3.1.4. Let $\mathcal{F}_3^{\text{mon}}$ be the set of monic cubic polynomials with integer coefficients and nonzero discriminant and let $p = (1/6, 1/3)$. If $f \in \mathcal{F}_3^{\text{mon}}$, then a computation shows that $H_r(f) \leq X^{1/6}$ if and only if $f \in B(p, X)$. Let C be any positive real number. By Lemma 3.3.5, if $\Delta \geq X^6/C$ and $H_r(f) \leq X^{1/6}$, then

$$\lambda_i(R_f) \asymp_C \Delta^{p_i}.$$

To prove (3.2), it suffices to show:

$$\lim_{C \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F}_3^{\text{mon}} \mid H_r(f) \leq X \text{ and } \Delta > X^6/C\}}{\#\{f \in \mathcal{F}_3^{\text{mon}} \mid H_r(f) \leq X\}} = 1.$$

Because the number of monic integral cubic forms with $H_r(f) \leq X$ and $\Delta = 0$ is $o(X^6)$, the denominator is equal to $X^6 + o(X^6)$. Let $\text{Disc} \in \mathbb{Z}[a, b, c, d]$ denote the discriminant polynomial for

binary cubic forms. By Davenport's lemma, we have

$$\begin{aligned}
& \#\{f \mid H_r(f) \leq X \text{ and } \Delta > X^6/C\} \\
&= \#\{(b, c, d) \in \mathbb{Z}^3 \mid \max\{|b|^6, |c|^3, |d|^2\} \leq X^6 \text{ and } |\text{Disc}(1, b, c, d)| > X^6/C\} \\
&= \text{Vol}\{(b, c, d) \in \mathbb{R}^3 \mid \max\{|b|^6, |c|^3, |d|^2\} \leq X^6 \text{ and } |\text{Disc}(1, b, c, d)| > X^6/C\} + O(X^5) \\
&= \text{Vol}\{(b, c, d) \in \mathbb{R}^3 \mid \max\{|b|^6, |c|^3, |d|^2\} \leq X^6 \text{ and} \\
&\quad |\text{Disc}(1, bX^{-1}, cX^{-2}, dX^{-3})| > 1/C\} + O(X^5) \\
&= X^6 \text{Vol}\{(b, c, d) \in \mathbb{R}^3 \mid \max\{|b|, |c|, |d|\} \leq 1 \text{ and } |\text{Disc}(1, b, c, d)| > 1/C\} + O(X^5).
\end{aligned}$$

Thus:

$$\begin{aligned}
& \lim_{C \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F}_3^{\text{mon}} \mid H_r(f) \leq X \text{ and } \Delta > X^6/C\}}{\#\{f \in \mathcal{F}_3^{\text{mon}} \mid H_r(f) \leq X\}} \\
&= \lim_{C \rightarrow \infty} \text{Vol}\{(b, c, d) \in \mathbb{R}^3 \mid \max\{|b|, |c|, |d|\} \leq 1 \text{ and } |\text{Disc}(1, b, c, d)| > 1/C\} \\
&= 1
\end{aligned}$$

We obtain (3.3) by observing that a positive proportion (depending on ϵ) of lattice points in $B(p, X)$ lie on the hyperplane $a = 1$, and then executing the proof of Proposition 3.4.4. $\square$

3.7 Sieving for maximal orders in S_3 -cubic fields

In this section, we will prove Theorem 1.2.2 by sieving for maximal orders in S_3 -cubic fields. Throughout this section, let $p = (p_1, p_2) \in \ell_3$ be a point and let ℓ denote a prime number. As before, let f denote an integral binary cubic form and let $X \in \mathbb{R}_{>1}$. We will need the following tail estimate for “small” primes. Let $\text{Disc} \in \mathbb{Z}[a, b, c, d]$ be the discriminant polynomial of binary cubic forms.

Lemma 3.7.1. *If $\ell \leq \sqrt{X^{3p_2-1/2}}$ then*

$$\#\{f \in B(p, X) \cap V_{\mathbb{Z}} \mid \text{Disc}(f) \equiv 0 \pmod{\ell^2}\} \ll X/\ell^2$$

where the implicit constant is independent of X , p , and ℓ .

Proof. Without loss of generality suppose $\ell \neq 2, 3$. Fix integer values of a , b , and c such that:

$$\begin{aligned} |a| &\leq X^{3p_1-1/2} \\ |b| &\leq X^{2p_1+p_2-1/2} \\ |c| &\leq X^{p_1+2p_2-1/2} \end{aligned}$$

We will count the number of integer values of d where $|d| \leq X^{3p_2-1/2}$ and $\ell^2 \mid \text{Disc}(a, b, c, d)$. We separate into the following 3 cases:

1. $\ell^2 \mid a$;
2. $\ell \mid a$ and $\ell^2 \nmid a$;
3. and $\ell \nmid a$.

We first analyze case (1). If $\ell \leq \sqrt{X^{3p_1-1/2}}$, Case (1) occurs with probability $1/\ell^2$. If $\ell > \sqrt{X^{3p_1-1/2}}$, then case (1) never occurs. Therefore we may bound the quadruples (a, b, c, d) with $\ell^2 \mid a$ by $O(X/\ell^2)$.

Similarly, if $\ell > X^{3p_1-1/2}$, then case (2) never occurs. If $\ell \leq X^{3p_1-1/2}$ case (2) occurs with probability $1/\ell$. Suppose we have a quadruple (a, b, c, d) such that $\ell \mid a$ and $\ell^2 \nmid a$ and write $a'\ell = a$. We have

$$\text{Disc} \equiv (18a'\ell bc - 4b^3)d + (b^2c^2 - 4a'\ell c^3) \pmod{\ell^2}$$

The above expression has more than 1 solution for d modulo ℓ^2 if and only if $\ell \mid b$ and $\ell \mid c$, which occurs with probability $1/\ell^2$; in this case, we have ℓ^2 solutions for d modulo ℓ^2 . Therefore we may bound the number of quadruples (a, b, c, d) with $\ell \mid a$ and $\ell^2 \nmid a$ and $\ell^2 \mid \text{Disc}(a, b, c, d)$ by $O(X/\ell^3)$.

Now suppose we have a quadruple (a, b, c, d) with $\ell \nmid a$: then either (i): Disc , when considered as a monic quadratic polynomial in d , has no double roots modulo ℓ ; or (ii): Disc , when considered as a monic quadratic polynomial in d has a double root modulo ℓ . We write the discriminant of a binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + d^3$ as

$$\text{Disc}(f) = (27a^2)d^2 + (18abc - 4b^3)d + (b^2c^2 - 4ac^3).$$

In subcase (i), Hensel's lemma shows that there are at most 2 solutions for d modulo ℓ^2 ; because $\ell \leq \sqrt{X^{3p_2-1/2}}$ and d is chosen in the range $[-X^{3p_2-1/2}, X^{3p_2-1/2}]$, the number of such quadruples is $O(X/\ell^2)$. In subcase (ii) there are at most ℓ solutions for d modulo ℓ^2 because $f \not\equiv 0 \pmod{\ell}$, so it suffices to show that the second subcase occurs with probability $1/\ell$. The second case only occurs

if the discriminant of $\text{Disc}(a, b, c, d)$, when $\text{Disc}(a, b, c, d)$ is considered as a quadratic polynomial in d , is divisible by ℓ . The discriminant of $\text{Disc}(a, b, c, d)$, when considered this way, is:

$$(18abc - 4b^3)^2 - 4(27a^2)(b^2c^2 - 4ac^3)$$

which we simplify to:

$$16b^6 - 144ab^4c + 216a^2b^2c^2 + 432a^3c^3.$$

Recall that we have assumed $\ell \nmid a$. Therefore, each choice of a and b gives at most 3 values for c modulo ℓ . Recall that c is chosen in the range $[-X^{p_1+2p_2-1/2}, -X^{p_1+2p_2-1/2}]$ and $X^{p_1+2p_2-1/2} \geq \ell$; so the probability that the discriminant of $\text{Disc}(a, b, c, d)$ is divisible by ℓ is $O(1/\ell)$. Therefore, the number of such quadruples is $O(X/\ell^2)$. $\square$

For “big” primes, we use the following tail estimate of Bhargava, Shankar, and Tsimerman.

Proposition 3.7.2 (Bhargava, Shankar, Tsimerman [7], Proposition 29). *The number of isomorphism classes of nondegenerate cubic rings such of absolute discriminant $\leq X$ that are not maximal at a prime ℓ is $O(X/\ell^2)$, where the explicit constant is independent of X and ℓ .*

We can now combine these two tail estimates and prove our theorem on the density function of maximal orders in S_3 -cubic fields.

Proof of Theorem 1.2.2. For any prime ℓ , let $\mathcal{U}_\ell$ denote the subset of $V_{\mathbb{Z}_\ell}$ corresponding to maximal cubic rings over $\mathbb{Z}_\ell$. Let μ_ℓ be the Haar measure on $V_{\mathbb{Z}_\ell}$, normalized such that $\mu_\ell(V_{\mathbb{Z}_\ell}) = 1$. Let $\mathcal{U} = \cap_\ell \mathcal{U}_\ell$. Then $\mathcal{U}$ is the set of $f \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings over $\mathbb{Z}$.

Let $p = (p_1, p_2) \in \ell_3$. By Proposition 3.4.4 and the fact that 100% of the integral forms in $B(p, X)$ are irreducible, it suffices to show that a positive proportion of forms in $B(p, X)$ have squarefree discriminant. For any positive integer Y , we have

$$\begin{aligned} & \liminf_{X \rightarrow \infty} \frac{\#\{\mathcal{U} \cap B(p, X) \cap V_{\mathbb{Z}}\}}{X} \\ & \geq \liminf_{X \rightarrow \infty} \frac{\#\{f \in \cap_{\ell \leq Y} \mathcal{U}_\ell \cap B(p, X) \cap V_{\mathbb{Z}} \mid \Delta \geq X/2\} - \sum_{\ell > Y} \#\{f \in \overline{\mathcal{U}}_\ell \cap B(p, X) \cap V_{\mathbb{Z}} \mid \Delta \geq X/2\}}{X} \end{aligned}$$

We lower bound the right hand side by:

$$\liminf_{X \rightarrow \infty} \frac{\#\{f \in \cap_{\ell \leq Y} \mathcal{U}_\ell \cap B(p, X) \cap V_{\mathbb{Z}} \mid \Delta \geq X/2\}}{X} \quad (3.23)$$

$$- \limsup_{X \rightarrow \infty} \frac{\sum_{\ell > Y} \#\{f \in \overline{\mathcal{U}}_\ell \cap B(p, X) \cap V_{\mathbb{Z}} \mid \Delta \geq X/2\}}{X} \quad (3.24)$$

We estimate the second term of (3.23). Using the tail estimates given in Lemma 3.7.1 and Proposition 3.7.2 and the bound in Lemma 3.3.4, we obtain:

$$\sum_{\ell > Y} \#\{f \in \overline{\mathcal{U}}_\ell \cap B(p, X) \cap V_{\mathbb{Z}} \mid \Delta \geq X/2\} \quad (3.25)$$

$$\ll \sum_{Y < \ell \leq \sqrt{X^{3p_2-1/2}}} O(X/\ell^2) + \sum_{Y, \sqrt{X^{3p_2-1/2}} < \ell} O(X^{1+p_2-p_1}/\ell^2) \quad (3.26)$$

The fact that $\sqrt{X^{3p_2-1/2}} < \ell$ in the second term of (3.25) implies that there exists a positive real number η such that the second term of (3.25) is bounded above by:

$$\sum_{Y, \sqrt{X^{3p_2-1/2}} < \ell} O(X^1/\ell^{1+\eta})$$

Therefore,

$$\lim_{Y \rightarrow \infty} \limsup_{X \rightarrow \infty} \frac{\sum_{\ell > Y} \#\{f \in \overline{\mathcal{U}}_\ell \cap B(p, X) \cap V_{\mathbb{Z}} \mid \Delta \geq X/2\}}{X} = 0.$$

We now estimate the first term of (3.23). First suppose $p \neq (1/6, 1/3)$. Then, because $B(p, X)$ is a box expanding in all coordinates with volume X , we have

$$\lim_{X \rightarrow \infty} \frac{\#\{f \in \cap_{\ell \leq Y} \mathcal{U}_\ell \cap B(p, X) \cap V_{\mathbb{Z}} \mid \Delta \geq X/2\}}{X} = \prod_{\ell \leq Y} \mu_\ell(\mathcal{U}_\ell).$$

Letting Y tend to infinity completes the proof, as a computation of the local densities, given in [7], shows the the product of the local densities is nonzero. An analogous proof proves the theorem for $p = (1/6, 1/3)$, given that one restricts $B(p, X)$ to the subset where $a = 1$. The same estimate of the first term of (3.23) applies, but but we obtain a different set of local densities. A computation shows that in this case, the product of relevant local densities is still nonzero, which completes the proof. $\square$

Chapter 4

Counting quartic rings by successive minima

In this chapter, we compute density functions of quartic rings. We will make use of the notion of *cubic resolvent rings* throughout; see Section 4.2 for background. In this chapter let R denote a quartic ring and let C denote a cubic resolvent ring of R . Let $\Delta = |\text{Disc}(R)| = |\text{Disc}(C)|$. We say a pair (R, C) is *nondegenerate* if $\Delta \neq 0$; in this chapter, all pairs (R, C) are assumed to be nondegenerate.

4.1 Statement of results

In the cubic case, the support of our density functions were contained in the line segments obtained by taking appropriate sets of limit points. We now adapt this notion to the quartic case. Let $G \subseteq S_4$ be a permutation group and define $\text{Poly}_4(G)$ to be the set of limit points of the multiset

$$\{(\log_{\Delta} \lambda_1(R), \log_{\Delta} \lambda_2(R), \log_{\Delta} \lambda_3(R), \log_{\Delta} \lambda_1(C), \log_{\Delta} \lambda_2(C))\} \subseteq \mathbb{R}^5$$

in the Euclidean metric as we range over isomorphism classes of pairs (R, C) where R is a G -ring. Define Poly_4 to be the union $\cup_G \text{Poly}_4(G)$ as we range over all permutation groups $G \subseteq S_4$. Our results are threefold: we explicitly compute $\text{Poly}_4(G)$ for various G , we compute various density functions, and then we discuss how various interesting families of quartic rings correspond to various vertices of $\text{Poly}_4(G)$.

4.1.1 Computing $\text{Poly}_4(G)$

Theorem 4.1.1. *For every permutation group $G \subseteq S_4$, the set $\text{Poly}_4(G)$ is a finite union of polytopes of dimension 3.*

Theorem 4.1.1 is a natural generalization of Theorem 1.1.2 when $n = 4$. See Theorem 4.4.2 for an even more explicit description of these polytopes. For many applications it is useful to provide explicit linear inequalities defining $\text{Poly}_4(G)$; in the following two theorems, we do this when $G = S_4$ or $G = D_4$. Let $p = (p_1, p_2, p_3, q_1, q_2)$ be the coordinates of $\mathbb{R}^5$. By the definition of successive minima and Minkowski's second theorem, the set $\text{Poly}_4(G)$ satisfies the following constraints:

$$0 \leq p_1 \leq p_2 \leq p_3; \quad 1/2 = p_1 + p_2 + p_3; \quad 0 \leq q_1 \leq q_2; \quad \text{and } 1/2 = q_1 + q_2. \quad (4.1)$$

Theorem 4.1.2. *The set $\text{Poly}_4(S_4)$ consists of the points $p \in \mathbb{R}^5$ satisfying (4.1) and*

$$q_2 \leq p_1 + p_3; \quad q_1 \leq 2p_1; \quad \text{and } q_2 \leq 2p_2.$$

Theorem 4.1.3. *The set $\text{Poly}_4(D_4)$ consists of the points $p \in \mathbb{R}^5$ satisfying (4.1) and*

$$q_1 \leq 2p_1 \quad \text{and } q_2 \leq 2p_2.$$

Theorem 4.1.4. *The set Poly_4 is the union of three polytopes. The first polytope consists of the points $p \in \mathbb{R}^5$ satisfying (4.1) and*

$$q_2 \leq p_2 + p_3 \quad \text{and } q_1 \leq 2p_1.$$

The second polytope consists of the points $p \in \mathbb{R}^5$ satisfying (4.1) and

$$q_2 \leq p_1 + p_3 \quad \text{and } q_1 \leq p_1 + p_2.$$

The third polytope consists of the points $p \in \mathbb{R}^5$ satisfying (4.1) and

$$q_2 \leq p_1 + p_3 \quad \text{and } q_2 \leq 2p_2.$$

It is interesting to note that $\text{Poly}_4(S_4)$ is the intersection of all three polytopes given in Theorem 4.1.4.

4.1.2 Density functions of quartic rings

We now define our density functions. Let $p = (p_1, p_2, p_3, q_1, q_2) \in \mathbb{R}^5$ denote a point. For every $\epsilon \in \mathbb{R}_{>0}$, $p \in \mathbb{R}^5$, $X \in \mathbb{R}_{>1}$, and permutation group $G \subseteq S_4$, define $\mathcal{F}(p, \epsilon, G, X)$ to be the set of

isomorphism classes of pairs (R, C) such that R is a G -ring, $\Delta \leq X$, and

$$\max_{i=1,2,3} \{ |\log_{\Delta} \lambda_i(R) - p_i| \} \leq \frac{\epsilon}{\log X} \quad (4.2)$$

$$\max_{i=1,2} \{ |\log_{\Delta} \lambda_i(C) - q_i| \} \leq \frac{\epsilon}{\log X}. \quad (4.3)$$

Define the density function $d_{\epsilon, G}: \mathbb{R}^5 \rightarrow \mathbb{R} \cup \{*\}$ which assigns to $p \in \mathbb{R}^5$ the value

$$\lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, G, X) + 1)}{\log X}$$

if it exists and else assigns $*$. Similarly, let $\mathcal{F}(p, \epsilon, X)$ be the set of isomorphism classes of pairs (R, C) such that $\Delta \leq X$, (4.2) holds, and (4.3) holds. Let $d_{\epsilon, 4}$ denote the corresponding density function. We now compute the total density function for quartic rings, the S_4 -density function, and prove partial results on the D_4 -density function.

Theorem 1.3.1. *There exists a positive real number M such that for every $\epsilon > M$ and every $p \in \mathbb{R}^5$,*

$$d_{\epsilon, 4}(p) = \begin{cases} 1 - (p_3 - p_2) - (p_3 - p_1) - (p_2 - p_1) - (q_2 - q_1) & \text{if } p \in \text{Poly}_4 \\ + \sum_{i \leq j, k} \max\{0, q_k - p_i - p_j\} & \\ 0 & \text{else.} \end{cases}$$

Theorem 1.3.2. *There exists a positive real number M such that for every $\epsilon > M$ and every $p \in \mathbb{R}^5$ we have*

$$d_{\epsilon, S_4}(p) = \begin{cases} d_{\epsilon, 4}(p) & \text{if } p \in \text{Poly}_4(S_4) \\ 0 & \text{else.} \end{cases}$$

We compute the density function for D_4 on the complement of $\text{Poly}_4(S_4)$; this is not an empty statement because $\text{Poly}_4(D_4)$ strictly contains $\text{Poly}_4(S_4)$.

Theorem 1.3.3. *There exists a positive real number M such that for every $\epsilon > M$ and every $p \in \mathbb{R}^5$, the following statements hold.*

1. *If $p \in \text{Poly}_4(D_4) \setminus \text{Poly}_4(S_4)$, then*

$$\begin{aligned} d_{\epsilon, D_4}(p) = d_{\epsilon, 4}(p) = & 1 - (p_3 - p_2) - (p_3 - p_1) - (p_2 - p_1) - (q_2 - q_1) \\ & + (q_2 - 2p_1) + (q_2 - p_1 - p_2) + (q_2 - p_1 - p_3). \end{aligned}$$

2. If $p \notin \text{Poly}_4(D_4)$, then $d_{\epsilon, D_4}(p) = 0$.

3. If $p \in \text{Poly}_4(D_4)$, then

$$\liminf_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, D_4, X) + 1)}{\log X} \geq 1 - (p_3 - p_2) - (p_3 - p_1) - (p_2 - p_1) - (q_2 - q_1) \\ + (q_2 - 2p_1) + (q_2 - p_1 - p_2) + (q_2 - p_1 - p_3)$$

4.1.3 Special families of quartic rings

Unsurprisingly, rings with extremal successive minima tend to also be extremal in an *algebraic* sense; in other words the vertices of our polytopes “correspond” to various interesting families of quartic rings. As in the cubic case, we first formalize what the word “correspond” means for families of quartic rings. We say a pair (R, C) is (ϵ, X) -close to p if:

$$\max_{1 \leq i \leq 3} \{|\log_{\Delta} \lambda_i(R) - p_i|\} \leq \frac{\epsilon}{\log X} \\ \max_{1 \leq i \leq 2} \{|\log_{\Delta} \lambda_i(C) - q_i|\} \leq \frac{\epsilon}{\log X}$$

Let $\mathcal{F}$ be an infinite set equipped with a map $H: \mathcal{F} \rightarrow \mathbb{R}_{>0}$ such that for all X , we have $\#\{f \in \mathcal{F} \mid H(f) \leq X\} < \infty$. We call H the *height function* of $\mathcal{F}$. Further suppose that $\mathcal{F}$ is equipped with a map ψ from $\mathcal{F}$ to isomorphism classes of nondegenerate pairs of quartic rings equipped with a cubic resolvent ring. For a point $p \in \text{Poly}_4$, we say the triple $(\mathcal{F}, H, \psi)$ *corresponds to p* if

$$\lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F} \mid H(f) \leq X \text{ and } \psi(f) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{f \mid H(f) \leq X\}} = 1 \quad (4.4)$$

and there exists a constant M such that for all $\epsilon > M$, we have

$$\liminf_{X \rightarrow \infty} \frac{\#\{(R, C) \in \mathcal{F}(p, \epsilon, X) \mid (R, C) \in \psi(\mathcal{F})\}}{\#\mathcal{F}(p, \epsilon, X)} > 0. \quad (4.5)$$

When H or ψ are implicit, we simply write that $\mathcal{F}$ corresponds to p .

Theorem 4.1.5. *The set of isomorphism classes of S_4 -rings (where H is the absolute discriminant) corresponds to*

$$(1/6, 1/6, 1/6, 1/4, 1/4).$$

The set of isomorphism classes of D_4 -rings (where H is the absolute discriminant) corresponds to

$$(0, 1/4, 1/4, 0, 1/2).$$

The points above are vertices of $\text{Poly}_4(S_4)$ and $\text{Poly}_4(D_4)$ respectively.

Vertices of $\text{Poly}_4(S_4)$

We now discuss various special families of quartic rings that correspond to the vertices of $\text{Poly}_4(S_4)$.

The vertices of $\text{Poly}_4(S_4)$ are:

1. $(1/6, 1/6, 1/6, 1/4, 1/4)$;
2. $(1/6, 1/6, 1/6, 1/6, 1/3)$;
3. $(1/8, 1/8, 1/4, 1/4, 1/4)$;
4. $(1/8, 3/16, 3/16, 1/4, 1/4)$;
5. $(1/10, 1/5, 1/5, 1/5, 3/10)$;
6. and $(1/12, 1/6, 1/4, 1/6, 1/3)$.

We will give families that correspond to each vertex except $(1/8, 3/16, 3/16, 1/4, 1/4)$. Recall that we define the root height H_r of a monic degree n polynomial $f(x) = x^n + a_1x^2 + \cdots + a_n \in \mathbb{Z}[x]$ by $H_r(f) = \max_i \{|a_i|^{1/i}\}$. Given a binary n -ic form $f(x, y) = a_0x^n + \cdots + a_ny^n$, define the *coefficient height of f* to be $H_c(f) = \max_i \{|a_i|\}$. Wood [33] constructed a map from integral binary quartic forms into pairs of integral ternary quadratic forms; thus from an integral binary quartic form, we canonically obtain a quartic ring and a cubic resolvent ring. This construction is compatible with that of Birch and Merriman [9], i.e. both constructions give isomorphic quartic rings.

Theorem 4.1.6. *Let $\mathcal{F}_4^{\text{mon}}$ be the set of integral monic quartic polynomials with nonzero discriminant. Then $(\mathcal{F}_4^{\text{mon}}, H_r)$ corresponds to $(1/12, 1/6, 1/4, 1/6, 1/3)$.*

As in the monogenic cubic case, one might guess at the above result by guessing that for a monogenic quartic ring $\mathbb{Z}[\alpha]$ satisfying

$$|\alpha| = \min_{i \in \mathbb{Z}} \{|\alpha + i|\},$$

a “short” basis of $\mathbb{Z}[\alpha]$ might “look like” $1, \alpha, \alpha^2, \alpha^3$. Moreover, the (unique) cubic resolvent ring of a monogenic quartic ring is monogenic as well.

Theorem 4.1.7. *Let $\mathcal{F}_4^{\text{bin}}$ be the set of integral binary quartic forms with nonzero discriminant. Then $(\mathcal{F}_4^{\text{bin}}, H_c)$ corresponds to $(1/6, 1/6, 1/6, 1/3)$.*

One might guess at the above result by recalling from work of Wood [33] that a pair (R, C) arises from a binary quartic form if and only if C is monogenic. We now discuss the other vertices of $\text{Poly}_4(S_4)$, first considering the vertex $(1/8, 1/8, 1/4, 1/4, 1/4)$. One might look at the coordinates of this vertex and immediately consider the family of nondegenerate quartic rings having a basis of the form $1, x, y, xy$; however this is not quite the right family to consider. This is because monogenic rings *also* have a basis of the form $1, x, y, xy$, and for ϵ sufficiently large,

$$d_{\epsilon,4}((1/8, 1/8, 1/4, 1/4, 1/4)) = d_{\epsilon,4}((1/12, 1/6, 1/4, 1/6, 1/3)) = 3/4.$$

In fact, these two vertices are adjacent in $\text{Poly}_4(S_4)$ and the entire edge between these two vertices evaluates to $3/4$ under the density function $d_{\epsilon,4}$. Thus, to restrict to the vertex $(1/8, 1/8, 1/4, 1/4, 1/4)$, we must impose one more condition. Consider triples (R, x, y) where R is a quartic ring and $x, y \in R$ have the property that $R = \mathbb{Z}\langle 1, x, y, xy \rangle$ and $\varphi(x + y) = \varphi(x) + \varphi(y)$ (here, φ denotes the cubic resolvent map). We say two such triples (R, x, y) and (R', x', y') are *isomorphic* if there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that $\alpha(x) = x'$ and $\alpha(y) = y'$. We say such a triple is *nondegenerate* if R is nondegenerate. Let $\mathcal{F}^{x,y,xy}$ be the set of isomorphism classes of nondegenerate such triples (R, x, y) .

We will embed $\mathcal{F}^{x,y,xy}$ in the space of pairs of integral ternary quadratic forms, and use this embedding to define a height function on $\mathcal{F}^{x,y,xy}$. In particular, consider the set of pairs of ternary quadratic forms of the form¹:

$$(A, B) = \begin{bmatrix} 1 & 0 & * \\ - & 0 & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & * \\ - & 1 & * \\ - & - & * \end{bmatrix}. \quad (4.6)$$

Similarly, now consider quadruples (R, x, y, ϵ) where $x, y \in R$, $\epsilon = \pm 1$, and $1, x, y, \epsilon xy$ is a basis of R . Again, we say such a quadruple is *nondegenerate* if R is nondegenerate. We say two such quadruples (R, x, y, ϵ) and (R', x', y', ϵ') are isomorphic if $\epsilon = \epsilon'$ and there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that $\alpha(x) = x'$ and $\alpha(y) = y'$.

¹The $*$ symbol means any real number is permitted to be in this entry, and $-$ means that this entry is determined by symmetry.

Theorem 4.1.8. *There is a canonical discriminant-preserving bijection between:*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{nondegenerate quadruples } (R, x, y, \varepsilon) \\ \text{where } x, y \in R \text{ are such that} \\ R = \mathbb{Z}\langle 1, x, y, xy \rangle \text{ and} \\ \varphi(x+y) = \varphi(x) + \varphi(y) \text{ and } \varepsilon = \pm 1 \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{nondegenerate pairs of} \\ \text{integral ternary quadratic forms} \\ \text{of the form (4.6)} \end{array} \right\}$$

For a triple $T \in \mathcal{F}^{x,y,xy}$, we attach a pair of nondegenerate ternary quadratic forms via the map above (setting $\varepsilon = 1$); define the *height* to be

$$H(T) := \max\{|a_{13}|^2, |a_{23}|^2, |b_{13}|^2, |b_{23}|^2, |a_{33}|, |b_{33}|\},$$

where here a_{ij}, b_{ij} are the entries of (A, B) ; see (4.8) for more details². Moreover, observe that the theorem above canonically attaches a cubic resolvent ring to a triple $(R, x, y) \in \mathcal{F}^{x,y,x^2}$ via Bhargava's parametrization of quartic rings. Refer to the forward direction of the map from Theorem 4.1.8 as ψ ; via Bhargava's parametrization of quartic rings [2], it can be interpreted as map from such triples to pairs of based quartic rings equipped with a based cubic resolvent ring.

Theorem 4.1.9. *The pair $(\mathcal{F}^{x,y,xy}, H, \psi)$ corresponds to $(1/8, 1/8, 1/4, 1/4, 1/4)$.*

We now discuss the vertex $(1/10, 1/5, 1/5, 1/5, 3/10)$ of $\text{Poly}_4(S_4)$. The coordinates of this vertex suggest considering the family of quartic rings having a basis of the form $1, x, y, x^2$. We consider a slight variant; consider triples (R, x, y) where R is a quartic ring, $x \in R$, $y \in R/\mathbb{Z}$, and x, y, x^2 forms a basis of $R/\mathbb{Z}$. We say two such triples (R, x, y) and (R', x', y') are *isomorphic* if there exists a ring isomorphism $\alpha: R \rightarrow R'$ with the property that $\alpha(x) = x'$ and $\alpha(y) \equiv \alpha(y') \pmod{\mathbb{Z}}$. We say such a triple is *nondegenerate* if R is nondegenerate. Let $\mathcal{F}^{x,y,x^2}$ be the set of isomorphism classes of nondegenerate such triples (R, x, y) . We employ the same strategy as previously.

Consider the set of pairs of ternary quadratic forms of the form:

$$(A, B) = \begin{bmatrix} 1 & 0 & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 1/2 & 0 \\ - & * & * \\ - & - & * \end{bmatrix}. \quad (4.7)$$

We consider quintuples $(R, x, y, \varepsilon, \nu)$ where $x \in R$, $y \in R/\mathbb{Z}$, $\varepsilon = \pm 1$, $\nu \in \{0, 1\}$, and x, y, x^2 is

²Another natural height function would be the $H((R, x, y)) := \max\{|x|, |y|\}$. The author expects that with respect to this height function, the family $\mathcal{F}^{x,y,xy}$ still corresponds to $(1/8, 1/8, 1/4, 1/4, 1/4)$.

a basis of $R/\mathbb{Z}$. We say such a quintuple is *nondegenerate* if R is nondegenerate. We say two such quintuples $(R, x, y, \varepsilon, \nu)$ and $(R', x', y', \varepsilon', \nu')$ are isomorphic if $\varepsilon = \varepsilon'$, $\nu = \nu'$, and there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that $\alpha(x) = x'$ and $\alpha(y) = y' \pmod{\mathbb{Z}}$.

Theorem 4.1.10. *There is a canonical discriminant-preserving bijection between:*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{nondegenerate quintuples } (R, x, y, \varepsilon, \nu) \\ \text{where } x \in R \text{ and } y \in R/\mathbb{Z} \text{ are such that} \\ x, y, x^2 \text{ is a basis of } R/\mathbb{Z} \text{ and } \varepsilon = \pm 1 \text{ and } \nu \in \{0, 1\} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{nondegenerate pairs of} \\ \text{integral ternary quadratic forms} \\ \text{of the form (4.7)} \end{array} \right\}$$

For a triple $T \in \mathcal{F}^{x, y, x^2}$ we attach a nondegenerate pair of integral ternary quadratic forms via the map above (setting $\varepsilon = 1$ and $\nu = 0$); define the *height* to be

$$H(T) := \max\{|a_{13}|^2, |a_{22}|, |a_{23}|, |a_{33}|, |b_{22}|^2, |b_{23}|^2, |b_2|^2\}.$$

As in the previous case, the theorem above canonically attaches a cubic resolvent ring to a triple (R, x, y) in $\mathcal{F}^{x, y, x^2}$; we will prove that this is the *unique* cubic resolvent ring of R . Refer to the forward direction of map from the theorem above as ψ .

Theorem 4.1.11. *The pair $(\mathcal{F}^{x, y, x^2}, H, \psi)$ corresponds to $(1/10, 1/5, 1/5, 1/5, 3/10)$.*

4.2 The parametrization of quartic rings

Our primary tool will be Bhargava's parametrization of quartic rings, which we now briefly summarize. Let $V_{\mathbb{R}} = \mathbb{R}^2 \otimes \text{Sym}^2 \mathbb{R}^3$. We write an element of $(A, B) \in V_{\mathbb{R}}$ as a pair of 3×3 real symmetric matrices as follows:

$$2(A, B) = \left(\begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}, \begin{bmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{bmatrix} \right). \quad (4.8)$$

An element (A, B) is said to be *integral* if $a_{ij}, b_{ij} \in \mathbb{Z}$, and the lattice of integral elements is denoted $V_{\mathbb{Z}}$. The group $G(\mathbb{R}) = \text{GL}_2(\mathbb{R}) \times \text{GL}_3(\mathbb{R})$ acts on $V_{\mathbb{R}}$ in the following way; an element

$(g_2, g_3) \in G(\mathbb{R})$ sends (A, B) to

$$(rg_3Ag_3^t + sg_3Bg_3^t, tg_3Ag_3^t + ug_3Bg_3^t)$$

where we write

$$g_2 = \begin{bmatrix} r & s \\ t & u \end{bmatrix}.$$

The subgroup $G(\mathbb{Z})$ acts on $V_{\mathbb{R}}$ and preserves the lattice $V_{\mathbb{Z}}$. The action of $G_{\mathbb{Z}}$ on $V_{\mathbb{R}}$ has a unique polynomial invariant given by the formula $\text{Disc}(4\text{Det}(Bx - Ay))$. This fundamental invariant is known as the *discriminant* and is denoted $\text{Disc}(A, B)$. The orbits of $G_{\mathbb{Z}}$ acting on $V_{\mathbb{Z}}$ parametrize quartic rings equipped with a cubic resolvent ring; see [2] for more details.

Theorem 4.2.1 (Bhargava, [2]). *There is a canonical, discriminant-preserving bijection between $V_{\mathbb{Z}}$ and isomorphism classes of pairs (R, C) where R is a based quartic ring and C is a based cubic resolvent ring of R . Under the action of $G_{\mathbb{Z}}$, this bijection descends to a bijection between the set of $G_{\mathbb{Z}}$ orbits of $V_{\mathbb{Z}}$ and the set of isomorphism classes of pairs (R, C) where R is a quartic ring and C is a cubic resolvent ring of R .*

We now describe a few important details of this bijection. A cubic resolvent ring C of a quartic ring R comes equipped with a quadratic map $\varphi: R/\mathbb{Z} \rightarrow C/\mathbb{Z}$ called a *cubic resolvent map*. Choosing bases for $R/\mathbb{Z}$ and $C/\mathbb{Z}$ gives rise to an element of $V_{\mathbb{Z}}$. Conversely, for an element $(A, B) \in V_{\mathbb{Z}}$, Bhargava constructed certain polynomials in the a_{ij}, b_{ij} that form the structure coefficients for a basis of R . Moreover, the binary cubic form $4\text{Det}(Bx - Ay)$ via (3.4) gives structure coefficients for a basis of C .

4.3 Reduction theory of quartic rings

We now fix some notation we use throughout this section. Unless otherwise specified, (A, B) will denote a nondegenerate element of $V_{\mathbb{Z}}$ and (R, C) will denote the corresponding quartic ring and cubic resolvent ring respectively. Let $\Delta = |\text{Disc}(A, B)|$. Analogously to the cubic case, in this section we develop the relationship between:

1. pairs (R, C) equipped with “small” bases;
2. and pairs (A, B) with “small” coefficients.

Our proofs are almost identical to those in the cubic case.

Lemma 4.3.1. *Let $\{1, v_1, v_2, v_3\}$ and $\{1, w_1, w_2\}$ be Minkowski bases of any nondegenerate quartic ring R and any cubic resolvent ring C of R . Let (A, B) be the corresponding matrices given by the cubic resolvent map. Then $|a_{ij}| \ll |v_i| |v_j| / |w_1|$ and $|b_{ij}| \ll |v_i| |v_j| / |w_2|$.*

Proof. Let $\sigma_1, \dots, \sigma_4$ be the 4 nonzero homomorphisms of R into the complex numbers. The cubic resolvent map $\varphi: R/\mathbb{Z} \otimes R/\mathbb{Z} \rightarrow \frac{1}{2}C/\frac{1}{2}\mathbb{Z}$ is given by

$$\varphi(x \otimes y) \rightarrow \frac{1}{2}(\sigma_1(x)\sigma_2(y) + \sigma_2(x)\sigma_1(y) + \sigma_3(x)\sigma_4(y) + \sigma_3(y)\sigma_4(x))$$

For an element $z \in C \otimes \mathbb{Q}$, let $\langle w_i \rangle z$ denote the coefficient of z with respect to the basis $\{1, w_1, w_2\}$. Because $\{1, v_1, v_2, v_3\}$ and $\{1, w_1, w_2\}$ are Minkowski bases,

$$\begin{aligned} |a_{ij}| &\asymp \langle w_1 \rangle (\varphi(v_i \otimes v_j)) \\ &\ll \frac{|\varphi(v_i \otimes v_j)|}{|w_1|} \\ &\ll \frac{|v_i| |v_j|}{|w_1|}. \end{aligned}$$

An analogous argument shows that $|b_{ij}| \ll |v_i| |v_j| / |w_2|$. □

For any $p = (p_1, p_2, p_3, q_1, q_2) \in \mathbb{R}^5$ and any positive real number X , define $B(p, X)$ to be the set of elements $(A, B) \in V_{\mathbb{R}}$ such that $a_{ij} \leq X^{p_i+p_j-q_1}$ and $b_{ij} \leq X^{p_i+p_j-q_2}$. Let $p = (p_1, p_2, p_3, q_1, q_2) \in \mathbb{R}^5$ denote a point. Moreover ϵ will denote a positive real number, M, D will denote real numbers ≥ 1 , and X will denote a real number > 1 . Recall that we say the pair (R, C) is (ϵ, X) -close to p if

$$\begin{aligned} \max_{i=1,2,3} \{|\log_{\Delta} \lambda_i(R) - p_i|\} &\leq \frac{\epsilon}{\log X} \\ \max_{i=1,2} \{|\log_{\Delta} \lambda_i(C) - q_i|\} &\leq \frac{\epsilon}{\log X}. \end{aligned}$$

We say $((A, B), p)$ are (ϵ, X) -close if the corresponding rings (R, C) and p are (ϵ, X) -close. We say (A, B) comes from Minkowski bases if there exist Minkowski bases of the corresponding rings (R, C) giving rise to (A, B) .

Lemma 4.3.2. *There exists M such that for every pair (A, B) , point p , and positive real number ϵ , the following statement holds: if $\Delta > 1$ and $((A, B), p)$ are (ϵ, Δ) -close and (A, B) comes from Minkowski bases, then $(A, B) \in Me^{3\epsilon}B(p, \Delta)$.*

Proof. Let $\{1, v_1, v_2, v_3\}$ and $\{1, w_1, w_2\}$ be the Minkowski bases of (R, C) giving rise to (A, B) . We

have

$$\begin{aligned}
|a_{i,j}| &\ll \frac{|v_i| |v_j|}{|w_1|} && \text{by Lemma 4.3.1} \\
&\asymp \frac{\lambda_i(R)\lambda_j(R)}{\lambda_1(C)} \\
&\leq e^{3\epsilon} \Delta^{p_i+p_j-q_1} && \text{because } ((A, B), p) \text{ is } (\epsilon, \Delta)\text{-close.}
\end{aligned}$$

An analogous argument shows that $|b_{i,j}| \ll e^{3\epsilon} \Delta^{p_i+p_j-q_2}$. $\square$

Lemma 4.3.3. *There exists D such that for all p satisfying (4.1), all (A, B) , and all M, X the following statement holds: if $(A, B) \in MB(p, X)$ then*

$$\#\{(A', B') \in DMB(p, X) \cap V_{\mathbb{Z}} \mid (R, C) \simeq (R', C')\} \geq \exp[X, (p_3-p_2)+(p_3-p_1)+(p_2-p_1)+(q_2-q_1)]\}$$

where here (R', C') is the quartic ring and cubic resolvent ring arising from the pair (A', B') .

Proof. Recall that $V_{\mathbb{Z}}$ admits an action of $G_{\mathbb{Z}} = \text{GL}_2(\mathbb{Z}) \times \text{GL}_3(\mathbb{Z})$. Act on (A, B) by elements of $G_{\mathbb{Z}}$ of the form

$$\left(\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ n_{12} & 1 & 0 \\ n_{13} & n_{23} & 1 \end{bmatrix} \right)$$

where $|n_{ij}| \leq \lceil X^{p_j-p_i} \rceil$ and $|m| \leq \lceil X^{q_2-q_1} \rceil$. $\square$

For a pair (A, B) , let $\{1, v_1, v_2, v_3\}$ and $\{1, w_1, w_2\}$ denote the explicit bases of R and C obtained from the structure coefficients.

Lemma 4.3.4. *For every p satisfying (4.1), every (A, B) , and every M, X the following statement holds: if $(A, B) \in MB(p, X)$, then $|v_i| \ll_M X^{p_i}$ for $i = 1, 2, 3$ and $|w_i| \ll_M X^{q_i}$ for $i = 1, 2$.*

Proof. The binary cubic form corresponding to the basis $\{1, w_1, w_2\}$ is given by $4\text{Det}(Bx - Ay)$. Lemma 3.3.3 implies that $|w_i| \ll_M X^{q_i}$ for $i = 1, 2$. The formulae in [2] of the explicit structure coefficients for the basis $\{1 = v_0, v_1, v_2, v_3\}$ imply that if $(A, B) \in MB(p, X)$ then the v_j -coefficient of v_i^2 is $\ll_M X^{2p_i-p_j}$. Let $p_0 = 0$. Thus,

$$|v_i|^2 \ll_M \max_{j=0,1,2,3} \{X^{2p_i-p_j} |v_j|\}. \quad (4.9)$$

Applying Lemma 6.0.2 completes the proof. $\square$

Lemma 4.3.5. *For every p satisfying (4.1) and every (A, B) , X , and M , the following statement holds: if*

$$(A, B) \in MB(p, X)$$

and $X/2 \leq \Delta \leq X$, then there are $\ll_M \exp[X, (p_3 - p_2) + (p_3 - p_1) + (p_2 - p_1) + (q_2 - q_1)]$ distinct elements $(A', B') \in MB(p, X) \cap V_{\mathbb{Z}}$ such that $(R', C') \simeq (R, C)$.

Proof. Let $\{v_0 = 1, v_1, v_2, v_3\}$ and $\{w_0 = 1, w_1, w_2\}$ be the explicit bases of R and C obtained from (A, B) . By Lemma 4.3.4, we have $|v_i| \ll_M X^{p_i}$ for $i = 1, 2, 3$ and $|w_i| \ll_M X^{q_i}$ for $i = 1, 2$. Because

$$X^{1/2} \asymp \Delta^{1/2} \ll |v_1| |v_2| |v_3| \ll_M X^{p_1+p_2+p_3} = X^{1/2}$$

and

$$X^{1/2} \asymp \Delta^{1/2} \ll |w_1| |w_2| \ll_M X^{q_1+q_2} = X^{1/2},$$

we have $|v_i| \asymp_M X^{p_i}$ for $i = 1, 2, 3$ and $|w_i| \asymp_M X^{q_i}$ for $i = 1, 2$.

Suppose $(A', B') \in MB(p, X) \cap V_{\mathbb{Z}}$ is such that $(R', C') \simeq (R, C)$. Let $\{1, v'_1, v'_2, v'_3\}$ and $\{1, w'_1, w'_2\}$ denote the bases of R' and C' given by (A', B') . By Lemma 4.3.4, we have $|v'_i| \ll_M X^{p_i}$ for $i = 1, 2, 3$ and $|w'_i| \ll_M X^{q_i}$ for $i = 1, 2$. Moreover, write

$$\begin{aligned} v'_i &= c_{i0} + \sum_{j=0}^3 c_{ij} v_j \\ w'_i &= d_{i0} + \sum_{j=0}^2 d_{ij} w_j. \end{aligned}$$

The pair (A', B') is determined by the choices of c_{ij} for $1 \leq i, j \leq 3$ and d_{ij} for $1 \leq i, j \leq 2$. We have:

$$\begin{aligned} X^{p_i} &\asymp_M |v'_i| \asymp_M \max_{0 \leq j < 4} \{|c_{ij}| |v_j|\} \asymp_M \max_{0 \leq j < n} \{|c_{ij}| X^{p_j}\} \\ X^{q_i} &\asymp_M |w'_i| \asymp_M \max_{0 \leq j < 3} \{|d_{ij}| |w_j|\} \asymp_M \max_{0 \leq j < n} \{|d_{ij}| X^{q_j}\} \end{aligned}$$

where $p_0 = q_0 = 0$. If $j \leq i$, the number of choices for c_{ij} and d_{ij} is $\ll_M 1$. If $j > i$, the number of choices for c_{ij} is $\ll_M X^{p_j - p_i}$ and the number of choices for d_{ij} is $\ll_M X^{q_j - q_i}$. Hence, there are $\ll_M \exp[X, (p_3 - p_2) + (p_3 - p_1) + (p_2 - p_1) + (q_2 - q_1)]$ distinct integral $(A', B') \in MB(p, X)$ such that $(R', C') \simeq (R, C)$. $\square$

Lemma 4.3.6. *For all p satisfying (4.1) and all (A, B) , M , and X the following statement holds:*

if $(A, B) \in MB(p, X)$ and $\frac{X}{2} \leq \Delta$ then

$$\lambda_i(R) \asymp_M \Delta^{p_i}.$$

for $i = 1, 2, 3$ and

$$\lambda_i(C) \asymp_M \Delta^{q_i}.$$

for $i = 1, 2$.

Proof. Lemma 3.3.5 immediately implies that $\lambda_i(C) \asymp_M \Delta^{q_i}$ for $i = 1, 2$. We have

$$\begin{aligned} \lambda_1(R)\lambda_2(R)\lambda_3(R) &\ll |v_1| |v_2| |v_3| && \text{by definition of successive minima} \\ &\ll_M X^{p_1} X^{p_2} X^{p_3} && \text{by Lemma 4.3.4} \\ &= X^{1/2} && \text{because } p_1 + p_2 + p_3 = 1/2 \\ &\asymp_M \Delta^{1/2} && \text{because } \Delta \geq X/2 \text{ and } (A, B) \in MB(p, X) \\ &\asymp \lambda_1(R)\lambda_2(R)\lambda_3(R). && \text{by Minkowski's second theorem} \end{aligned}$$

Thus $\lambda_i(R) \asymp_M \Delta^{p_i}$ for $i = 1, 2, 3$. □

4.4 Computing $\text{Poly}_4(G)$

In this section, we will compute $\text{Poly}_4(G)$ and Poly_4 . Let $p = (p_1, p_2, p_3, q_1, q_2) \in \mathbb{R}^5$ be any point in $\mathbb{R}^5$. Let K denote a quartic étale algebra over $\mathbb{Q}$ and L denote the cubic resolvent algebra of K . Let $\varphi: K/\mathbb{Q} \otimes K/\mathbb{Q} \rightarrow L/\mathbb{Q}$ denote the symmetric bilinear form given by the cubic resolvent map. A *flag* $(\mathcal{F}, \mathcal{G})$ of (K, L) is a pair of sequences $\mathcal{F} = (F_0, F_1, F_2, F_3)$ and $\mathcal{G} = (G_0, G_1, G_2)$ of $\mathbb{Q}$ -vector spaces such that

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset F_3 = K$$

$$\mathbb{Q} = G_0 \subset G_1 \subset G_2 = L$$

and $\dim_{\mathbb{Q}} F_i = i+1$ and $\dim_{\mathbb{Q}} G_i = i+1$. For a positive integer n , let $[n]$ refer to the set $\{0, \dots, n-1\}$.

Associate to a flag $(\mathcal{F}, \mathcal{G})$ the function

$$\begin{aligned} T_{\mathcal{F}, \mathcal{G}}: [4] \times [4] &\longrightarrow [3] \\ (i, j) &\longmapsto \min\{k \in [3] \mid \varphi\langle F_i \otimes F_j \rangle \subseteq G_k\}. \end{aligned}$$

Definition 4.4.1. Let $P_{\mathcal{F},\mathcal{G}}$ be the set of $p = (p_1, p_2, p_3, q_1, q_2) \in \mathbb{R}^5$ satisfying (4.1) and the following condition: for all $1 \leq i, j \leq 3$, if $T_{\mathcal{F},\mathcal{G}}(i, j) > 0$ then

$$q_{T_{\mathcal{F},\mathcal{G}}(i,j)} \leq p_i + p_j.$$

The proof of the following theorem is almost exactly analogous to that of Theorem 1.1.2; the reader is encouraged to refer to the proof of Theorem 1.1.2 for more details. We will need the following definition, which we recall from Chapter 2.

Theorem 4.4.2. *We have $\text{Poly}_4(G) = \bigcup_{(\mathcal{F},\mathcal{G})} P_{\mathcal{F},\mathcal{G}}$ where $(\mathcal{F},\mathcal{G})$ ranges across flags of pairs (K, L) with the property that $\text{Gal}(K) \simeq G$ as a permutation group.*

Proof. We will first show that $\text{Poly}_4(G)$ is contained in $\bigcup_{(\mathcal{F},\mathcal{G})} P_{\mathcal{F},\mathcal{G}}$. By Minkowski's second theorem and the definition of successive minima, $\text{Poly}_4(G)$ satisfies the linear inequalities given in (4.1). Let R be any nondegenerate quartic G -ring and let C be a cubic resolvent ring of R . Let $K = R \otimes \mathbb{Q}$ and let $L = C \otimes \mathbb{Q}$. Picking Minkowski bases $\{v_0 = 1, v_1, v_2, v_3\}$ and $\{w_0 = 1, w_1, w_2\}$ of R and C respectively gives rise to a flag $(\mathcal{F}, \mathcal{G})$ of (K, L) given by $F_i := \mathbb{Q}\langle v_0, \dots, v_i \rangle$ and $G_i := \mathbb{Q}\langle w_0, \dots, w_i \rangle$. For every $1 \leq i, j \leq 3$ such that $T_{\mathcal{F},\mathcal{G}}(i, j) > 0$, we have

$$\varphi\langle \mathbb{Z}\langle v_0, \dots, v_i \rangle \otimes \mathbb{Z}\langle v_0, \dots, v_j \rangle \rangle \subseteq \mathbb{Z}\langle w_0, \dots, w_{T_{\mathcal{F},\mathcal{G}}(i,j)} \rangle$$

and

$$\varphi\langle \mathbb{Z}\langle v_0, \dots, v_i \rangle \otimes \mathbb{Z}\langle v_0, \dots, v_j \rangle \rangle \not\subseteq \mathbb{Z}\langle w_0, \dots, w_{T_{\mathcal{F},\mathcal{G}}(i,j)-1} \rangle.$$

Therefore, there exists $0 \leq i' \leq i$ and $0 \leq j' \leq j$ such that $\langle w_{T_{\mathcal{F},\mathcal{G}}(i,j)} \rangle \varphi(v_{i'} \otimes v_{j'}) \neq 0$. So,

$$|w_{T_{\mathcal{F},\mathcal{G}}(i,j)}| \ll |\varphi(v_{i'} \otimes v_{j'})| \ll |v_{i'}| |v_{j'}| \ll |v_i| |v_j|.$$

This implies that $\text{Poly}_4(G)$ is contained in the set $\bigcup_{(\mathcal{F},\mathcal{G})} P_{\mathcal{F},\mathcal{G}}$ where $(\mathcal{F},\mathcal{G})$ ranges across flags of (K, L) with the property that $\text{Gal}(K) \simeq G$.

Now let $(\mathcal{F}, \mathcal{G})$ be a flag of a pair (K, L) with the property that $\text{Gal}(K) \simeq G$. Choose bases $\{v_0 = 1, v_1, v_2, v_3\}$ and $\{w_0 = 1, w_1, w_2\}$ of K and L giving rise to the flag $(\mathcal{F}, \mathcal{G})$. Writing the

symmetric bilinear map φ with respect to these bases gives a pair $(A, B) \in V_{\mathbb{R}}$, which we write as

$$2(A, B) = \left(\begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}, \begin{bmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{bmatrix} \right).$$

For a positive integer M , define the pair of matrices (A_M, B_M) to be

$$2A_M = \begin{bmatrix} 2a_{11}M^{p_1+p_1-q_1} & a_{12}M^{p_1+p_2-q_1} & a_{13}M^{p_1+p_3-q_1} \\ a_{12}M^{p_1+p_2-q_1} & 2a_{22}M^{p_2+p_2-q_1} & a_{23}M^{p_2+p_3-q_1} \\ a_{13}M^{p_1+p_3-q_1} & a_{23}M^{p_2+p_3-q_1} & 2a_{33}M^{p_3+p_3-q_1} \end{bmatrix}$$

$$2B_M = \begin{bmatrix} 2b_{11}M^{p_1+p_1-q_2} & b_{12}M^{p_1+p_2-q_2} & b_{13}M^{p_1+p_3-q_2} \\ b_{12}M^{p_1+p_2-q_2} & 2b_{22}M^{p_2+p_2-q_2} & b_{23}M^{p_2+p_3-q_2} \\ b_{13}M^{p_1+p_3-q_2} & b_{23}M^{p_2+p_3-q_2} & 2b_{33}M^{p_3+p_3-q_2} \end{bmatrix}.$$

For a rational point p in the relative interior of $P_{\mathcal{F}, \mathcal{G}}$, one may check that there exists an infinite set $\mathcal{M} \subseteq \mathbb{Z}_{>0}$ such that for all $M \in \mathcal{M}$, the pair (A_M, B_M) is contained in $V_{\mathbb{Z}}$; the proof is exactly identical to that of Proposition 2.1.3. Each $M \in \mathcal{M}$ gives rise to a distinct quartic ring and cubic resolvent ring (R_M, C_M) with absolute discriminant Δ_M ; for each $M \in \mathcal{M}$, write the bases of R_M and C_M obtained from (A_M, B_M) by $\{1, v_{1,M}, \dots, v_{3,M}\}$ and $\{1, w_{1,M}, w_{2,M}\}$ respectively. Then for $M, N \in \mathcal{M}$, we have:

$$N\Delta_M = M\Delta_N$$

$$N^{p_i}v_{i,M} = M^{p_i}v_{i,N}$$

$$N^{q_i}w_{i,M} = M^{q_i}w_{i,N}$$

Therefore,

$$\lim_{M \in \mathcal{M}} \left(\log_{\Delta_M} \lambda_1(R_M), \dots, \log_{\Delta_M} \lambda_3(R_M) \right) = (p_1, p_2, p_3)$$

$$\lim_{M \in \mathcal{M}} \left(\log_{\Delta_M} \lambda_1(C_M), \log_{\Delta_M} \lambda_2(C_M) \right) = (q_1, q_2)$$

Therefore, $p \in \text{Poly}_4(G)$. Because $\text{Poly}_4(G)$ is defined to be a set of limit points, it must be closed; therefore $P_{\mathcal{F}, \mathcal{G}}$ is contained in $\text{Poly}_4(G)$, which completes the proof of the theorem. $\square$

Proof of Theorem 4.1.1. Theorem 4.4.2 expresses $\text{Poly}_4(G)$ as a finite union of polytopes. A computation shows that these polytopes all have dimension 3. $\square$

Proof of Theorem 4.1.4. Let $p \in \text{Poly}_4$ be any point. Suppose that $q_2 > p_1 + p_3$. By Theorem 4.4.2, $\text{Poly}_4(G) = \bigcup_{(\mathcal{F}, \mathcal{G})} P_{\mathcal{F}, \mathcal{G}}$ where $(\mathcal{F}, \mathcal{G})$ ranges across flags of pairs (K, L) where K is a quartic étale algebra. Choose such a flag $(\mathcal{F}, \mathcal{G})$ such that $P_{\mathcal{F}, \mathcal{G}}$ contains p . Choose bases of K and L giving rise to that flag; in these bases, the cubic resolvent map is a pair $(A, B) \in V_{\mathbb{Q}}$ of the form

$$(A, B) = \left(\begin{bmatrix} * & * & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ - & * & * \\ - & - & * \end{bmatrix} \right).$$

If $q_2 > p_2 + p_3$ then $b_{22} = b_{33} = 0$. If $q_1 > 2p_1$ then $a_{11} = 0$. In what ensues, we will show that neither of these events occur.

Because $\text{Disc}(A, B) \neq 0$, the binary cubic form $\text{Det}(Bx + Ay)$ does not have a double root, and hence $\text{Rank}(B) > 1$. Therefore we cannot have both $b_{22} = 0$ and $b_{23} = 0$. Now let Q_A and Q_B be the conics in $\mathbb{P}^2$ given by A and B respectively. Because $\text{Disc}(A, B) \neq 0$, the intersection $Q_A \cap Q_B$ is 4 geometric points in $\mathbb{P}^2$ with the property that no 3 are collinear. If $a_{11} = 0$ then $[1 : 0 : 0] \in Q_A \cap Q_B$; however because $\text{Rank}(B) = 2$, the conic Q_B is a union of two lines intersecting at the point $[1 : 0 : 0]$, which forces three of the 4 points in $Q_A \cap Q_B$ to be collinear, contradiction. Hence, $a_{11} \neq 0$.

A computation shows that there exists $(A, B) \in V_{\mathbb{Q}}$ of the form

$$(A, B) = \left(\begin{bmatrix} * & * & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ - & 0 & * \\ - & - & * \end{bmatrix} \right)$$

generating a nondegenerate quartic ring. The pair (A, B) gives rise to a flag $(\mathcal{F}, \mathcal{G})$ via the explicit structure coefficients. It is easy to see that $P_{\mathcal{F}, \mathcal{G}}$ is precisely the first polytope in the theorem statement. Therefore, the first polytope specified in the theorem statement is contained in Poly_4 and the subset of Poly_4 with $q_2 > p_1 + p_3$ is contained in the first polytope specified in the theorem statement.

Now suppose that $p \in \text{Poly}_4(S_4)$ is any point with $q_2 \leq p_1 + p_3$ and $q_1 > 2p_1$. Let $(A, B) \in V_{\mathbb{Q}}$ be the set of matrices arising from an appropriate flag generating a nondegenerate quartic étale algebra; then $a_{11} = b_{11} = 0$. If $q_2 > 2p_2$ then further $b_{12} = b_{22} = 0$. So, the quadric Q_B contains the line $z = 0$, where x, y, z are the coordinates of $\mathbb{P}^2$; thus we may suppose two distinct points on

the line $z = 0$ are contained in the intersection $Q_A \cap Q_B$; hence $a_{12} \neq 0$ so $q_1 \leq p_1 + p_2$. Therefore if $q_2 \leq p_1 + p_3$ and $q_1 > 2p_1$ then $q_1 \leq p_1 + p_2$ or $q_2 \leq 2p_2$. This shows that the part of $\text{Poly}_4(S_4)$ not lying in the first polytope stated in the theorem statement is contained in the union of the second polytope and third polytope stated in the theorem statement. Similarly, a computation shows that there exists $(A, B) \in V_{\mathbb{Q}}$ of the form

$$(A, B) = \left(\begin{bmatrix} 0 & * & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & * \\ - & 0 & * \\ - & - & * \end{bmatrix} \right)$$

and

$$(A, B) = \left(\begin{bmatrix} 0 & 0 & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & * \\ - & * & * \\ - & - & * \end{bmatrix} \right)$$

generating a nondegenerate quartic ring, so Theorem 4.4.2 implies that the second and third polytopes in the theorem statement are contained in Poly_4 . $\square$

Proof of Theorem 4.1.3. As in the proof of Theorem 4.1.4, to show that $\text{Poly}_4(D_4)$ is contained in the given region, it suffices to show that for any element $(A, B) \in V_{\mathbb{Q}}$ giving rise to a quartic étale algebra K , we have:

1. if $a_{11} = b_{11} = 0$, then K is reducible;
2. if $b_{11} = b_{12} = b_{22} = 0$, then K is reducible.

Suppose K is a quartic étale algebra given by a pair $(A, B) \in V_{\mathbb{Q}}$, and let Q_A and Q_B be the quadratic forms in $\mathbb{P}_{\mathbb{Q}}^2$. Then

$$K \simeq \Gamma(V(Q_A, Q_B)).$$

If $a_{11} = b_{11} = 0$ then $[1: 0: 0]$ is a common intersection of the conics defined by A and B , which implies that K is reducible. Similarly, if $b_{11} = b_{12} = b_{22} = 0$ then the conic by B in $\mathbb{P}^2$ is of the form $axz + bxz + cz^2 = z(ax + by + cz)$, where here x, y, z are the coordinates of $\mathbb{P}^2$; this implies that K is reducible. Therefore, the set $\text{Poly}_4(D_4)$ is contained in the region specified in the theorem statement.

A computation shows that there exists $(A, B) \in V_{\mathbb{Q}}$ of the form

$$(A, B) = \left(\begin{bmatrix} * & * & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ - & * & * \\ - & - & * \end{bmatrix} \right)$$

generating a D_4 -quartic field, so Theorem 4.4.2 implies the region in the theorem statement is contained in $\text{Poly}_4(D_4)$. $\square$

Proof of Theorem 4.1.2. Let $p \in \text{Poly}_4(S_4)$ be any point. The proof of Theorem 4.1.3 shows that $q_1 \leq 2p_1$ and $q_2 \leq 2p_2$. As in the proof of Theorem 4.1.4, to show that $\text{Poly}_4(S_4)$ is contained in the given region, it suffices to show that for any element $(A, B) \in V_{\mathbb{Q}}$ giving rise to a quartic étale algebra K , we have that if $b_{11} = b_{12} = b_{13} = 0$ then $\text{Gal}(K) \not\cong S_4$. If $b_{11} = b_{12} = b_{13} = 0$ then $(1, 0)$ is a root of the cubic resolvent polynomial $\text{Det}(By - Ax)$, which implies that the cubic resolvent algebra of K is reducible, which implies that $\text{Gal}(K) \not\cong S_4$. Therefore, the set $\text{Poly}_4(S_4)$ is contained in the region specified in the theorem statement.

A computation shows that there exists $(A, B) \in V_{\mathbb{Q}}$ of the form

$$(A, B) = \left(\begin{bmatrix} * & * & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & * \\ - & * & * \\ - & - & * \end{bmatrix} \right)$$

generating a S_4 -quartic field, so Theorem 4.4.2 implies the region in the theorem statement is contained in $\text{Poly}_4(S_4)$. $\square$

4.5 Computing density functions of quartic rings

We now define some notation we use throughout this section to shorten our formulae. For a point $p \in \mathbb{R}^5$, let

$$f(p) := 1 + \sum_{1 \leq i \leq j \leq 3, 1 \leq k \leq 2} \max\{0, q_k - p_i - p_j\}$$

and

$$g(p) := (p_3 - p_2) + (p_3 - p_1) + (p_2 - p_1) + (q_2 - q_1).$$

As before, ϵ will denote a positive real number, M, D will denote real numbers ≥ 1 , X will denote a real number > 1 , and (A, B) will denote a nondegenerate pair in $V_{\mathbb{Z}}$. As usual, p will denote a point

in $\mathbb{R}^5$.

Lemma 4.5.1. *For any M , X , and p satisfying (4.1), we have*

$$\exp[X, f(p)] \ll_p \# \{V_{\mathbb{Z}} \cap MB(p, X)\} \ll M^{12} \exp[X, f(p)].$$

The first implicit constant is independent of X and M and the second implicit constant is independent of p , X , and M .

Proof. Let S_k denote the set of pairs (i, j) such that $q_k \geq p_i + p_j$ for $k = 1, 2$. Then for every $(i, j) \in S_1$ and every lattice point $(A, B) \in MB(p, X)$, we have $|a_{ij}| \leq M$. Similarly, for every $(i, j) \in S_2$ and every lattice point $(A, B) \in MB(p, X)$, we have $|b_{ij}| \leq M$. Let $\pi: V_{\mathbb{R}} \rightarrow \mathbb{R}^{12-\#S_1-\#S_2}$ denote the projection map away from a_{ij} for every pair $(i, j) \in S_1$ and b_{ij} for every pair $(i, j) \in S_2$. Then

$$\begin{aligned} \#\{\pi(B(p, X)) \cap \mathbb{Z}^{12-\#S_1-\#S_2}\} &\leq \#\{MB(p, X) \cap V_{\mathbb{Z}}\} \\ &\leq M^{\#S_1+\#S_2} \#\{\pi(MB(p, X)) \cap \mathbb{Z}^{12-\#S_1-\#S_2}\}. \end{aligned}$$

Davenport's lemma implies that

$$\#\{\pi(MB(p, X)) \cap \mathbb{Z}^{12-\#S_1-\#S_2}\} = \text{Vol}(\pi(MB(p, X))) + O\left(\frac{\text{Vol}(\pi(MB(p, X)))}{Y}\right)$$

where

$$Y = M \min_{(i,j,k)} \{\exp[X, p_i + p_j - q_k] \mid (i, j) \notin S_k\}$$

and the implicit constant is independent of p , M , and X . To finish, a computation shows that

$$\text{Vol}(\pi(MB(p, X))) = M^{12-\#S_1-\#S_2} \exp[X, f(p)].$$

□

Lemma 4.5.2. *We have*

$$\#\mathcal{F}_4(p, \epsilon, X) \ll e^{36\epsilon} \exp[X, f(p) - g(p)]$$

where the implicit constant does not depend on X , p , or ϵ .

Proof. Let S be the set of (A, B) arising from Minkowski bases of pairs $(R, C) \in \mathcal{F}_4(p, \epsilon, X)$. Lemma 4.3.2 implies that there exists a constant M such that $(A, B) \in Me^{3\epsilon}B(p, X)$ for all

$(A, B) \in S$. By Lemma 4.3.3, there exists $D \geq 1$, independent of X , p , M , and ϵ , such that

$$\#\{(A', B') \in DMe^{3\epsilon}B(p, X) \mid (R, C) \simeq (R', C')\} \geq \exp[X, g(p)]$$

for all elements of S . Therefore,

$$\#\mathcal{F}_4(p, \epsilon, X) \ll \frac{\#\{DMe^{3\epsilon}B(p, X) \cap V_{\mathbb{Z}}\}}{\exp[X, g(p)]}.$$

Applying Lemma 4.5.1 to estimate the numerator completes the proof. $\square$

Lemma 4.5.3. *There exists a constant M such that for all $\epsilon > M$, we have:*

1. *if $p \in \text{Poly}_4$, then*

$$\#\mathcal{F}_4(p, \epsilon, X) \gg_{p, \epsilon} \exp[X, f(p) - g(p)];$$

2. *if $p \in \text{Poly}_4(S_4)$, then*

$$\#\mathcal{F}(p, \epsilon, S_4, X) \gg_{p, \epsilon} \exp[X, f(p) - g(p)];$$

3. *if $p \in \text{Poly}_4(D_4)$, then*

$$\#\mathcal{F}(p, \epsilon, D_4, X) \gg_{p, \epsilon} \exp[X, 1 - g(p) + (q_2 - 2p_1) + (q_2 - p_1 - p_2) + (q_2 - p_1 - p_3)].$$

Proof. We first prove (1). Choose $p \in \text{Poly}_4$. Lemma 4.3.6 shows that there exists a constant M such that for all $\epsilon > M$, if $(A, B) \in B(p, X) \cap V_{\mathbb{Z}}$ and $X/2 \leq \Delta$, then (A, B) is (ϵ, X) -close to p . Let $S = \{(A, B) \in B(p, X) \cap V_{\mathbb{Z}} \mid X/2 \leq \Delta \leq X\}$. Therefore

$$\begin{aligned} \#\mathcal{F}_4(p, \epsilon, X) &\geq \frac{\#S}{\max_{(A, B) \in S} \#\{(A', B') \in B(p, X) \mid (R', C') \simeq (R, C)\}} \\ &\asymp \frac{\#\{(A, B) \in B(p, X) \cap V_{\mathbb{Z}}\}}{\max_{(A, B) \in S} \#\{(A', B') \in B(p, X) \mid (R', C') \simeq (R, C)\}} \quad \text{by the definition of } B(p, X). \end{aligned}$$

Applying Lemma 4.5.1 to estimate the numerator and applying Lemma 4.3.5 to upper bound the denominator completes the proof of (1).

The argument above also proves (2), with the additional input that there exists $D \in \mathbb{R}_{\geq 1}$ such that a positive proportion, as $X \rightarrow \infty$, of the lattice points in $DB(p, X) \cap V_{\mathbb{Z}}$ have Galois group S_4

and $\Delta \geq X/2$. In fact, we may replace the $\Delta \geq X/2$ condition with $\Delta \geq X/M$ for arbitrarily large M . Observe that

$$\lim_{M \rightarrow \infty} \lim_{X \rightarrow \infty} \frac{\#\{(A, B) \in DB(p, X) \cap V_{\mathbb{Z}} \mid \Delta > X/M\}}{\#(DB(p, X) \cap V_{\mathbb{Z}})} = 1.$$

Thus it suffices to prove that there exists $D \in \mathbb{R}_{\geq 1}$ such that a positive proportion of the lattice points in $DB(p, X) \cap V_{\mathbb{Z}}$ have Galois group S_4 as $X \rightarrow \infty$. Consider the subset of lattice points of $DB(p, X)$ such that $\Delta \equiv 5 \pmod{25}$, the ring R is irreducible modulo 7, and the ring C is irreducible modulo 11; every element of this subset has Galois group S_4 . If this set is nonempty for large enough X , then it forms a positive proportion of $DB(p, X)$. The nonemptiness follows from the fact that there exists a pair of integral ternary quadratic forms

$$(A, B) = \left(\begin{bmatrix} * & * & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & * \\ - & * & * \\ - & - & * \end{bmatrix} \right)$$

such that $\Delta \equiv 5 \pmod{25}$, the ring R is irreducible modulo 7, and the ring C is irreducible modulo 11. Choosing D to be large enough such that $(A, B) \in DB(p, X)$ completes the proof of this case.

Similarly, to prove (3) we will show that there exists $D \in \mathbb{R}_{\geq 1}$ such that a positive proportion, as $X \rightarrow \infty$, of the lattice points $(A, B) \in B(p, X) \cap V_{\mathbb{Z}}$ satisfying $b_{11} = b_{12} = b_{13} = 0$ have Galois group D_4 . First, it is easy to see that there exists a pair of integral ternary quadratic forms

$$(A, B) = \left(\begin{bmatrix} * & * & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ - & * & * \\ - & - & * \end{bmatrix} \right)$$

giving rise to a D_4 -ring. Choose D large enough so that $(A, B) \in DB(p, X)$. Let $S_k = \{(i, j) : q_k = p_i + p_j\}$ for $k = 1, 2$. Let

$$Z = \{(A', B') \in V_{\mathbb{Z}} \mid \forall (i, j) \in S_1, \ a'_{ij} = a_{ij} \text{ and } \forall (i, j) \in S_2, \ b'_{ij} = b_{ij} \text{ and } b_{11} = b_{12} = b_{13} = 0\}.$$

Observe that $Z \cap DB(p, X)$ contains a positive proportion of the lattice points in $DB(p, X)$. Further, observe that a general pair of integral ternary quadratic forms in Z gives rise to a D_4 -ring. Thus, by Hilbert's irreducibility theorem, the subset of Z with Galois group $\neq D_4$ is a thin set; an application of quantitative Hilbert irreducibility (specifically Theorem 2.1 of [15]) shows that the density, as

$X \rightarrow \infty$, of lattice points in Z with Galois group $\neq D_4$ is 0. $\square$

Proof of Theorem 1.3.1. Clearly, the support of $d_{\epsilon,4}$ is contained in Poly_4 . If $p \in \text{Poly}_4$, then combining Lemma 4.5.2 and Lemma 4.5.3 shows that there exists a constant M such that for all $\epsilon > M$, we have

$$\begin{aligned} \#\mathcal{F}_4(p, \epsilon, X) &\asymp_{\epsilon,p} \exp[X, 1 - (p_3 - p_2) - (p_3 - p_1) - (p_2 - p_1) - (q_2 - q_1) \\ &\quad + \sum_{i \leq j, k} \max\{0, q_k - p_i - p_j\}; \end{aligned}$$

$\square$

Proof of Theorem 1.3.2. The proof is analogous to that of Theorem 1.3.1. Combine Theorem 4.1.2, Lemma 4.5.2, and Lemma 4.5.3. $\square$

Proof of Theorem 1.3.3. Again, the proof is analogous to that of Theorem 1.3.1. Combine Theorem 4.1.3, Lemma 4.5.2, and Lemma 4.5.3. $\square$

4.6 The generic points of D_4 and S_4

In this section, we prove Theorem 4.1.5, first for D_4 and then for S_4 . To prove Theorem 4.1.5 for D_4 , we will need the following lemma³.

Lemma 4.6.1. *Choose $p \in \text{Poly}_4(S_4)$ such that $p_i + p_j - q_k > 0$ for all $1 \leq i, j \leq 3$ and $1 \leq k \leq 2$. Then*

$$\#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon, X)\text{-close to } p\} \ll_{\epsilon, \gamma} \exp[X, 1 - \delta_p + \gamma]$$

where $\delta_p = \frac{1}{2} \max_{1 \leq i, j \leq 3, 1 \leq k \leq 2} \{p_i + p_j - q_k\}$. Moreover, the implicit constant is independent of p .

Proof. By Lemma 4.3.2, it suffices to show that for any $M \geq 1$, we have

$$\{(A, B) \in MB(p, X) \mid R \text{ is a } D_4\text{-ring and } \Delta \leq X\} \ll_{M, \gamma} X^{1 - \delta_p + \gamma}.$$

Observe that if (A, B) gives rise to a D_4 -ring, then the binary cubic form $\text{Det}(Ax + By)$ is reducible. We now use a version of quantitative Hilbert irreducibility (specifically an easy generalization of Theorem 2.1 of [15]) and Lemma 4.5.1 to conclude. $\square$

³This lemma can be strengthened significantly, but for our application this statement suffices.

Proof of Theorem 4.1.5 for D_4 . Let $p(D_4) = (0, 1/4, 1/4, 0, 1/2)$. We prove (4.4) for D_4 by demonstrating the following equivalent statement:

$$\lim_{\epsilon \rightarrow \infty} \limsup_{X \rightarrow \infty} \frac{\#\{(R, C) \mid \Delta \leq X \text{ and } R \text{ is a } D_4\text{-ring that is not } (\epsilon, X)\text{-close to } p(D_4)\}}{\#\{(R, C) \mid \Delta \leq X \text{ and } R \text{ is a } D_4\text{-ring}\}} = 0. \quad (4.10)$$

It is easy to bound the denominator; when ordered by absolute discriminant, 100% of quadratic extensions of $\mathbb{Q}(i)$ are quartic D_4 -extensions, and there are $\asymp X$ quadratic extensions of $\mathbb{Q}(i)$ of absolute discriminant $\leq X$. Hence

$$\#\{(R, C) \mid \Delta \leq X \text{ and } R \text{ is a } D_4\text{-ring}\} \gg X. \quad (4.11)$$

We now focus our attention on bounding the numerator of (4.10). Let $\ell \leq k$ be positive integers whose values we fix their value later. Our proof strategy is very similar to that of Corollary 3.1.5; we count the number of D_4 -rings of absolute discriminant $\leq X$ that are $(\epsilon/\ell, X)$ -close to some *other* point p' on $\text{Poly}_4(D_4)$ with the property that p' has distance at least $\epsilon/\log X$ from p . We then sum over an appropriate set of points p' ; we evaluate this sum by splitting it into a *main term* and a *cusp*. We bound both the main term and the cusp to conclude.

To this end, there exists a constant M such that for all $\epsilon > M$, we have:

$$\begin{aligned} & \#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is not } (\epsilon, X)\text{-close to } p(D_4)\} \\ & \leq \text{Main} + \text{Cusp} \end{aligned}$$

where:

$$\text{Main} := \#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon/k, X)\text{-close to a point in}$$

$$\text{Poly}_4(D_4) \cap \{p \in \mathbb{R}^5 \mid \frac{\epsilon}{\log X} \leq p_1 \leq 1/100\}$$

$$\text{Cusp} := \#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon, X)\text{-close to a point in}$$

$$\text{Poly}_4(D_4) \cap \{p \in \mathbb{R}^5 \mid p_1 \geq 1/100\}$$

Therefore, to prove (4.10) it suffices to show that

$$\lim_{\epsilon \rightarrow \infty} \limsup_{X \rightarrow \infty} \frac{\text{Main}}{X} = \lim_{\epsilon \rightarrow \infty} \limsup_{X \rightarrow \infty} \frac{\text{Cusp}}{X} = 0. \quad (4.12)$$

We begin by evaluating Main. Choose values of ℓ and k such that:

1. $\ell > 36$;
2. and for any point $(p_1, p_2, p_3, q_1, q_2) \in \text{Poly}_4$ and any pair (R, C) , if

$$\begin{aligned} |\log_{\Delta} \lambda_1(R) - p_1| &\leq \frac{\epsilon}{k \log \Delta} \\ |\log_{\Delta} \lambda_2(R) - p_2| &\leq \frac{\epsilon}{k \log \Delta} \\ |\log_{\Delta} \lambda_1(C) - q_1| &\leq \frac{\epsilon}{k \log \Delta}, \end{aligned}$$

then (R, C) is $(\epsilon/\ell, \Delta)$ -close to $(p_1, p_2, p_3, q_1, q_2)$.

We now define our appropriate set of points; they will form a grid whose points are spaced $\frac{\epsilon}{k \log X}$ distance apart and lie in the subset of $\text{Poly}_4(D_4)$ where $p_1 \leq 1/100$. For any integers x, y , and z , define the point

$$p_{xyz} := (p_1(x), p_2(x, y), p_3(x, y), q_1(x, y, z), q_2(x, y, z))$$

via the following formulae:

$$\begin{aligned} p_1(x) &:= \frac{\epsilon}{\log X} + \frac{\epsilon x}{k \log X} \\ p_2(x, y) &:= \left(\frac{1}{4} - \frac{1}{2} p_1(x) \right) - \frac{\epsilon y}{k \log X} \\ p_3(x, y) &:= 1/2 - p_1(x) - p_2(x, y) \\ q_1(x, y, z) &:= 1/2 - 2p_2(x, y) + \frac{\epsilon z}{k \log X} \\ q_2(x, y, z) &:= 1/2 - q_1(x, y, z) \end{aligned}$$

Let M be the smallest positive integer such that

$$p_1(M) \geq 1/100.$$

For any nonnegative integer x , let N_x be the smallest positive integer such that

$$p_2(x, N_x) \leq \frac{1}{4} - p_1(x).$$

For any nonnegative integers x and y , let L_{xy} be the smallest positive integer such that

$$q_1(x, y, L_{xy}) \geq 2p_1(x).$$

The values M , N_x , and L_{xy} indicate where the grid meets the boundaries of $\text{Poly}_4(D_4)$; see Theorem 4.1.3 for an explicit description of the facets. Thus, we may write Main as the following triple sum⁴:

$$\text{Main} \leq \sum_{x=0}^M \sum_{y=0}^{N_x} \sum_{z=0}^{L_{xy}} \#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon/\ell, X)\text{-close to } p_{xyz}\} \quad (4.13)$$

Without loss of generality, fix ϵ to be large enough so that $d_{\epsilon/k, 4}$ does not depend on ϵ ; for conciseness, let $h = d_{\epsilon/k, 4}$. We now bound the inner sum of (4.13); choose positive integers x and y such that $0 \leq x \leq M$ and $0 \leq y \leq N_x$. Then:

$$\begin{aligned} & \sum_{z=0}^{L_{xy}} \#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon/\ell, X)\text{-close to } p_{xyz}\} \\ & \ll \sum_{z=0}^{L_{xy}} e^{36\epsilon/\ell} \exp[X, h(p_{xyz})] && \text{by Lemma 4.5.2} \\ & = \sum_{z=0}^{L_{xy}} e^{36\epsilon/\ell} \exp[X, h(p_{xy0})] X^{-\epsilon z/k \log X} && \text{by Theorem 1.3.1} \\ & = e^{36\epsilon/\ell} \exp[X, h(p_{xy0})] \sum_{z=0}^{L_{xy}} e^{-\epsilon z/k} \\ & \leq e^{36\epsilon/\ell} \exp[X, h(p_{xy0})] \frac{1}{1 - e^{-\epsilon/k}} \end{aligned}$$

Moreover, the implicit constants are independent of x , y , and ϵ . We now bound the second sum, also using Lemma 4.5.2 and Theorem 1.3.1. Fix a positive integer $0 \leq x \leq M$; there exists a positive real number s such that:

$$\begin{aligned} \sum_{y=0}^{N_x} \exp[X, h(p_{xy0})] &= \exp[X, h(p_{x00})] \sum_{y=0}^{N_x} X^{-\epsilon sy/k \log X} \\ &\leq \exp[X, h(p_{x00})] \frac{1}{1 - e^{-\epsilon s/k}}. \end{aligned}$$

We bound the outer sum in exactly the same way; again Lemma 4.5.2 implies that there exists a

⁴This is essentially Riemann integration on $\text{Poly}_4(D_4)$!

positive real number t such that:

$$\begin{aligned} \sum_{x=0}^M \exp[X, h(p_{x00})] &= \exp[X, h(p_{000})] \sum_{z=1}^M X^{-\epsilon t x/k \log X} \\ &\leq \exp[X, h(p_{000})] \frac{1}{1 - e^{-\epsilon t/k}}. \end{aligned}$$

Thus,

$$\begin{aligned} \frac{\text{Main}}{X} &\ll e^{36\epsilon/\ell} X^{-1} \exp[X, h(p_{000})] \frac{1}{1 - e^{-\epsilon t/k}} \frac{1}{1 - e^{-\epsilon s/k}} \frac{1}{1 - e^{\epsilon/k}} \\ &= e^{36\epsilon/\ell} X^{-\epsilon/\log X} \frac{1}{1 - e^{-\epsilon t/k}} \frac{1}{1 - e^{-\epsilon s/k}} \frac{1}{1 - e^{-\epsilon/k}} \\ &= e^{36\epsilon/\ell - \epsilon} \frac{1}{1 - e^{-\epsilon t/k}} \frac{1}{1 - e^{-\epsilon s/k}} \frac{1}{1 - e^{-\epsilon/k}} \end{aligned}$$

where the implicit constant is independent of ϵ . Because $\ell > 36$, we have

$$\lim_{\epsilon \rightarrow \infty} e^{36\epsilon/\ell - \epsilon} \frac{1}{1 - e^{-\epsilon t/k}} \frac{1}{1 - e^{-\epsilon s/k}} \frac{1}{1 - e^{\epsilon/k}} = 0.$$

So,

$$\lim_{\epsilon \rightarrow \infty} \limsup_{X \rightarrow \infty} \frac{\text{Main}}{X} = 0.$$

We now bound Cusp. For $p \in \text{Poly}_4$, Lemma 4.5.2 implies that:

$$\#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon, X)\text{-close to } p\} \ll e^{36\epsilon} \exp[X, h(p)] \quad (4.14)$$

where the implicit constant is independent of ϵ and p . Let B be an open ball of radius $1/100$ around $(1/6, 1/6, 1/6, 1/4, 1/4)$. For $p \in B \cap \text{Poly}_4(S_4)$, Lemma 4.6.1 shows that

$$\#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon, X)\text{-close to } p\} \ll_{\epsilon, \gamma} \exp[X, 1 - \delta_p + \gamma] \quad (4.15)$$

where $\delta_p = \frac{1}{2} \max_{1 \leq i, j \leq 3, 1 \leq k \leq 2} \{p_i + p_j - q_i\}$ and the implicit constant is independent of p . Combining (4.14) and (4.15), we conclude there exists a positive real number $\eta < 1$ such that for every $p \in \text{Poly}_4(D_4)$ with $p_1 \geq 1/100$, we have

$$\#\{(R, C) \mid \Delta \leq X, R \text{ is a } D_4\text{-ring, and } R \text{ is } (\epsilon, X)\text{-close to } p\} \ll_{\epsilon} \exp[X, \eta],$$

with an implicit constant independent of p . Summing over an appropriate grid in $\text{Poly}_4(D_4)$, we see

that:

$$\text{Cusp} \ll_{\epsilon} (\log X)^3 \exp[X, \eta].$$

Thus

$$\lim_{\epsilon \rightarrow \infty} \lim_{X \rightarrow \infty} \frac{\text{Cusp}}{X} = 0.$$

We now show (4.5), which translates to showing that

$$\liminf_{X \rightarrow \infty} \frac{\#\{(R, C) \mid \Delta \leq X \text{ and } (R, C) \text{ is a } D_4\text{-ring and is } (\epsilon, X)\text{-close to } p(D_4)\}}{\#\{(R, C) \mid \Delta \leq X \text{ and } (R, C) \text{ is } (\epsilon, X)\text{-close to } p(D_4)\}} > 0.$$

Combining Lemma 4.5.2 and Lemma 4.5.3 shows that the denominator is $\asymp_{\epsilon} X$.

We now show that the numerator is $\gg X$. When ordered by absolute discriminant, 100% of quadratic extensions of $\mathbb{Q}(i)$ are quartic D_4 -extensions. Let R be a maximal order in a quartic D_4 -extension containing $\mathbb{Q}(i)$. Then $i \in R$, so $\lambda_1(R) = 1$; moreover, let $v \in R \setminus \mathbb{Z}[i]$ be such that $|v| = \lambda_2(R)$; then $|iv| = |v|$, so $\lambda_3(R) = \lambda_2(R)$. Moreover, R has a unique cubic resolvent ring C ; let $\varphi: R/\mathbb{Z} \rightarrow C/\mathbb{Z}$ be the cubic resolvent map. Then because R is irreducible, $\varphi(i)$ must be a nonzero element of $C/\mathbb{Z}$; moreover, $\lambda_1(C) \leq |\varphi(i)| \ll 1$. Therefore there exists a positive real number M such that for all $\epsilon > M$, every such ring R is (ϵ, Δ) -close to $p(D_4)$. Observing that there are $\asymp X$ many quadratic extensions of $\mathbb{Q}(i)$ of absolute discriminant $\leq X$ concludes the proof. $\square$

To prove Theorem 4.1.5 when $G = S_4$, we appeal to upcoming work of H and Vincent. Given a nondegenerate rank n ring R , we consider the rank $(n-1)$ sublattice $\mathcal{L}_R := \{x \in \mathbb{Z} + nR \mid \text{Tr}(x) = 0\}$, up to isometry. It is naturally seen as an element of the double coset space

$$\mathcal{S}_{n-1} := \text{GL}_{n-1}(\mathbb{Z}) \backslash \text{GL}_{n-1}(\mathbb{R}) / \text{GO}_{n-1}(\mathbb{R}).$$

The space $\mathcal{S}_{n-1}$ has a natural measure μ_{n-1} , obtained from the Haar measure on $\text{GL}_{n-1}(\mathbb{R})$ and $\text{GO}_{n-1}(\mathbb{R})$. To a nondegenerate pair (R, C) we associate an element $(\mathcal{L}_R, \mathcal{L}_C) \in \mathcal{S}_3 \times \mathcal{S}_2$; we call this the *shape* of the pair (R, C) .

Theorem 4.6.2 (H, Vincent). *When ordered by absolute discriminant, the shapes of pairs (R, C) where R is an S_4 -ring are equidistributed with respect to $\mu_3 \times \mu_2$.*

Proof of Theorem 4.1.5 when $G = S_4$. Let $p(S_4) = (1/6, 1/6, 1/6, 1/4, 1/4)$. We will first prove (4.4). For an integer $n \geq 2$, an element $\mathcal{L} \in \mathcal{S}_n$, and an integer $0 \leq i < n$, define $\lambda_i(\mathcal{L})$ to be the i -th successive minimum of a lattice representing $\mathcal{L}$ with determinant 1. For a positive real

number ϵ and an integer $n \geq 2$, define

$$\mathcal{S}_{n,\epsilon} := \{\mathcal{L} \in \mathcal{S}_n \mid \max_{1 \leq i < n} \{\log \lambda_i(\mathcal{L})\} \leq \epsilon\}.$$

Then

$$\begin{aligned} & \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{(R, C) \mid \Delta \leq X \text{ and } R \text{ is a } S_4\text{-ring that is } (\epsilon, X)\text{-close to } p(S_4)\}}{\#\{(R, C) \mid \Delta \leq X \text{ and } R \text{ is a } S_4\text{-ring}\}} \\ & \geq \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{(R, C) \mid \Delta \leq X \text{ and } R \text{ is a } S_4\text{-ring and } (\mathcal{L}_R, \mathcal{L}_C) \in \mathcal{S}_{3,\epsilon} \times \mathcal{S}_{2,\epsilon}\}}{\#\{(R, C) \mid \Delta \leq X \text{ and } R \text{ is a } S_4\text{-ring}\}} \\ & = \lim_{\epsilon \rightarrow \infty} \frac{(\mu_3 \times \mu_2)(\mathcal{S}_{3,\epsilon} \times \mathcal{S}_{2,\epsilon})}{(\mu_3 \times \mu_2)(\mathcal{S}_3 \times \mathcal{S}_2)} \\ & = 1 \end{aligned}$$

We prove (4.5) with the following observation: Lemma 4.5.2 and Lemma 4.5.3 combine to prove that there exists a positive real number M such that for all $\epsilon > M$, a positive proportion of rings in $\mathcal{F}(p(S_4), \epsilon, X)$ as $X \rightarrow \infty$ are S_4 -rings. $\square$

4.7 Special families of quartic rings

4.7.1 Quartic rings with a basis of the form $1, x, y, xy$

The following index formula of Bhargava [2] is essential to our study of quartic rings equipped with a basis of the form $1, x, y, xy$. For a rank n ring R and n elements $v_1, \dots, v_n \in R$, define $\text{Ind}(v_1, \dots, v_n)$ to be the index of $\mathbb{Z}\langle v_1, \dots, v_n \rangle$ in R if $v_1, \dots, v_n$ are linearly independent, and 0 otherwise.

Proposition 4.7.1 (Bhargava [2], Lemma 9). *If R is a quartic ring and C is a cubic resolvent ring of R , then for any $x, y \in R$,*

$$\text{Ind}(1, x, y, xy) = \text{Ind}(1, \varphi(x), \varphi(y)).$$

The above proposition implies that any nondegenerate quartic ring with a basis $1, x, y, xy$ has a *unique* cubic resolvent ring, namely $\mathbb{Z}\langle 1, \varphi(x), \varphi(y) \rangle$. Suppose R is a nondegenerate quartic ring with a basis $1, x, y, xy$. Let C be the unique cubic resolvent ring of R and equip $C/\mathbb{Z}$ with the basis $\varphi(x), \varphi(y)$. Choose a basis x, y, z for $R/\mathbb{Z}$. Then, the cubic resolvent map $\varphi: R/\mathbb{Z} \rightarrow C/\mathbb{Z}$, expressed

in these bases, has the form:

$$(A, B) = \begin{bmatrix} 1 & * & * \\ - & 0 & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & * & * \\ - & 1 & * \\ - & - & * \end{bmatrix} \quad (4.16)$$

Conversely, a nondegenerate element of $V(\mathbb{Z})$ of the form (4.16) gives rise to the following data: a pair (R, C) , a basis x, y, z of $R/\mathbb{Z}$, and a basis $\varphi(x), \varphi(y)$ of $C/\mathbb{Z}$. Proposition 4.7.1 implies that

$$\text{Ind}(1, x, y, xy) = \text{Ind}(1, \varphi(x), \varphi(y)) = 1,$$

so x, y, xy is also a basis of $R/\mathbb{Z}$. There are unique lifts $X, Y \in R$ of $x, y \in R/\mathbb{Z}$ and a unique value $\varepsilon = \pm 1$ such that $z \equiv \varepsilon XY \pmod{\mathbb{Z}}$. This discussion will prove Theorem 4.7.2, which we state after making the following definitions.

Consider quadruples (R, x, y, z) where $x, y, z \in R/\mathbb{Z}$ is a basis of $R/\mathbb{Z}$ and $1, X, Y, XY$ is a basis of R for any lift $X, Y \in R$ of x, y . We say such a quadruple is *nondegenerate* if R is nondegenerate. Moreover, we say two such quadruples (R, x, y, z) and (R', x', y', z') are isomorphic if there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that:

$$\alpha(x) \equiv x' \pmod{\mathbb{Z}}$$

$$\alpha(y) \equiv y' \pmod{\mathbb{Z}}$$

$$\alpha(z) \equiv z' \pmod{\mathbb{Z}}$$

Similarly, now consider quadruples (R, X, Y, ε) where $X, Y \in R$, $\varepsilon = \pm 1$, and $1, X, Y, \varepsilon XY$ is a basis of R . Again, we say such a quadruple is *nondegenerate* if R is nondegenerate. We say two such quadruples (R, X, Y, ε) and $(R', X', Y', \varepsilon')$ are isomorphic if $\varepsilon = \varepsilon'$ and there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that:

$$\alpha(X) = X'$$

$$\alpha(Y) = Y'$$

Theorem 4.7.2. *There is a canonical discriminant-preserving bijection between the following three*

sets:

$$\left\{ \begin{array}{l} \text{isomorphism classes of nondegenerate quadruples } (R, x, y, z) \text{ such that} \\ x, y, z \in R/\mathbb{Z} \text{ and } x, y, z \text{ is a basis of } R/\mathbb{Z} \text{ and } 1, X, Y, XY \\ \text{is a basis of } R \text{ for any lifts } X, Y \in R \text{ of } x, y \in R/\mathbb{Z} \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{isomorphism classes of nondegenerate quadruples } (R, X, Y, \varepsilon) \\ \text{such that } X, Y \in R, \varepsilon = \pm 1, \text{ and } 1, X, Y, \varepsilon XY \text{ is a basis of } R \end{array} \right\}$$

$$\left\{ \begin{array}{l} \text{nondegenerate pairs of integral ternary} \\ \text{quadratic forms of the form (4.16)} \end{array} \right\}$$

Let H be the subgroup of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ acting on pairs of matrices of the form (4.16); H is generated by the following matrices:

$$\begin{aligned} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ * & * & \pm 1 \end{bmatrix} \\ & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{aligned} \tag{4.17}$$

Suppose R is a nondegenerate quartic ring. Consider pairs $(x, y) \in R$ such that $1, x, y, xy$ is a basis of R . Consider the equivalence relation on such pairs generated by $(x, y) \sim (y, x)$ and $(x, y) \sim (\pm x + a, y)$ for any $a \in \mathbb{Z}$. We define a *digenization* of R to be such an equivalence class (x, y) . A *digenized quartic ring* is defined to be a nondegenerate quartic ring equipped with a digenization⁵. We say two digenized quartic rings (R, x, y) and (R', x', y') are isomorphic if there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that $(\alpha(x), \alpha(y)) \sim (x', y')$. Then we obtain:

Theorem 4.7.3. *There is a canonical discriminant-preserving bijection between:*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{digenized quartic rings} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{nondegenerate orbit classes of} \\ \text{pairs of integral ternary quadratic forms} \\ \text{of the form (4.16)} \\ \text{under the action of } H \end{array} \right\}$$

A theorem of Bhargava [4] proves that a nondegenerate quartic ring has at most 2760 many

⁵The notion of digenized quartic rings is a natural variant of the concept of a *monogenized* quartic ring.

monogenizations; it is natural to ask if the number of digenizations of a quartic ring is uniformly bounded! However, it is clear that a monogenic quartic ring has infinitely digenizations. It is interesting to ask if there is a positive integer N such that for every nondegenerate quartic ring R :

1. if R has infinitely many digenizations, then it is monogenic;
2. else, R has at most N digenizations.

We now consider matrices of the form (4.6), which we repeat here:

$$(A, B) = \begin{bmatrix} 1 & 0 & * \\ - & 0 & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 0 & * \\ - & 1 & * \\ - & - & * \end{bmatrix}.$$

We obtain the following theorem as a corollary of Theorem 4.7.2.

Theorem 4.1.8. *There is a canonical discriminant-preserving bijection between:*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{nondegenerate quadruples } (R, x, y, \varepsilon) \\ \text{where } x, y \in R \text{ are such that} \\ R = \mathbb{Z}\langle 1, x, y, xy \rangle \text{ and} \\ \varphi(x + y) = \varphi(x) + \varphi(y) \text{ and } \varepsilon = \pm 1 \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{nondegenerate pairs of} \\ \text{integral ternary quadratic forms} \\ \text{of the form (4.6)} \end{array} \right\}$$

Recall that $\mathcal{F}^{x,y,xy}$ is defined to be the set of isomorphism classes of triples (R, x, y) where R is a nondegenerate quartic ring and $x, y \in R$ are such that $1, x, y, xy$ is a basis of R and $\varphi(x + y) = \varphi(x) + \varphi(y)$. Let $W(\mathbb{Z})$ denote the set of matrices of the form (4.6) and let ψ be the map from triples $(R, x, y) \in \mathcal{F}^{x,y,xy}$ to pairs of integral ternary quadratic forms referred to in Theorem 4.1.8 given by setting $\varepsilon = 1$. We now prove Theorem 4.1.9. Let $p = (1/8, 1/8, 1/4, 1/4, 1/4)$.

Proof of Theorem 4.1.9. Let $T = (R, x, y) \in \mathcal{F}^{x,y,xy}$ be any such triple of absolute discriminant Δ and let C be the unique cubic resolvent ring. A computation shows that $H(T) \leq X^{1/4}$ if and only if $\psi(T) \in B(p, X)$; thus for any real numbers $M \geq 1$ and $X > 1$, an easy generalization of Lemma 4.3.6 implies that if $\Delta \geq X/M$ and $H(T)^4 \leq X$, then

$$\lambda_i(R) \asymp_M \Delta^{p_i}$$

$$\lambda_i(C) \asymp_M \Delta^{q_i}.$$

So, for each $M \geq 1$, there exists a positive real number ϵ_M such that if $\Delta \geq X/M$ and $H(T)^4 \leq X$, we have that $\psi(T)$ is (ϵ_M, X) -close to p . Moreover, we may suppose $\lim_{M \rightarrow \infty} \epsilon_M = \infty$. We now prove (4.4). We have:

$$\begin{aligned}
& \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T) \leq X \text{ and } \psi(T) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T) \leq X\}} \\
&= \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T) \leq X^{1/4} \text{ and } \psi(T) \text{ is } (\epsilon, X^{1/4})\text{-close to } p\}}{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T) \leq X^{1/4}\}} \\
&= \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X \text{ and } \psi(T) \text{ is } (4\epsilon, X)\text{-close to } p\}}{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X\}} \\
&= \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X \text{ and } \psi(T) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X\}} \\
&\geq \lim_{M \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X \text{ and } \Delta \geq X/M\}}{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X\}}.
\end{aligned}$$

Davenport's lemma gives:

$$\begin{aligned}
\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X\} &= \frac{1}{2} \#\{(A, B) \in W(\mathbb{Z}) \cap B(p, X) \mid \text{Disc}(A, B) \neq 0\} \\
&= \frac{X}{2} \text{Vol}\{(A, B) \in W(\mathbb{R}) \cap B(p, 1)\} + O(X^{7/8}).
\end{aligned}$$

We now compute the numerator: Let

$$g_X = \left(\begin{bmatrix} X^{1/4} & 0 \\ 0 & X^{1/4} \end{bmatrix}, \begin{bmatrix} X^{-1/8} & 0 & 0 \\ 0 & X^{-1/8} & 0 \\ 0 & 0 & X^{-1/4} \end{bmatrix} \right).$$

The element g_X maps $B(p, X)$ to $B(p, 1)$. By Davenport's lemma, we have

$$\begin{aligned}
& \#\{T \in \mathcal{F}^{x,y,xy} \mid H(T)^4 \leq X \text{ and } \Delta \geq X/M\} \\
&= \frac{1}{2} \#\{(A, B) \in W(\mathbb{Z}) \cap B(p, X) \mid |\text{disc}(A, B)| \geq X/M\} \\
&= \frac{1}{2} \#\{(A, B) \in W(\mathbb{Z}) \cap B(p, X) \mid |\text{disc}(g(A, B))| \geq 1/M\} \\
&= \frac{1}{2} X \text{Vol}\{(A, B) \in W(\mathbb{R}) \cap B(p, 1) \mid |\text{disc}(A, B)| \geq 1/M\} + O(X^{7/8}).
\end{aligned}$$

Note that $W(\mathbb{R})$ lies on an affine linear subspace, so the “volume” above is taken relatively. Now observe that

$$\lim_{M \rightarrow \infty} \text{Vol}\{(A, B) \in W(\mathbb{R}) \cap B(p, 1) \mid |\text{disc}(A, B)| \geq 1/M\} = 1$$

so

$$\lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T) \leq X \text{ and } \psi(T) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{T \in \mathcal{F}^{x,y,xy} \mid H(T) \leq X\}} = 1.$$

We obtain Condition (3.3) via the proof of Lemma 4.5.2, using the additional observation that a positive proportion (depending on ϵ) of lattice points in $B(p, X)$ lie on the affine linear subspace defined by $a_{11} = b_{22} = 1$ and $a_{12} = b_{12} = a_{22} = b_{11} = 0$. $\square$

4.7.2 Quartic rings with a basis of the form $1, x, y, x^2$

As in the case of quartic rings with a basis of the form $1, x, y, xy$, our proofs crucially rely on an *index formula*.

Proposition 4.7.4. *If R is a quartic ring and C is a cubic resolvent ring of R , then for any $x, y \in R$,*

$$\text{Ind}(1, x, y, x^2) = \text{Ind}(1, \varphi(x), \varphi(x+y) - \varphi(x) - \varphi(y)).$$

Proof. The proof proceeds exactly as that of Proposition 4.7.1. Namely, the assertion of the lemma is equivalent to the following identity:

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ x & x' & x'' & x''' \\ y & y' & y'' & y''' \\ x^2 & (x')^2 & (x'')^2 & (x''')^2 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ xx' + x''x''' & xx'' + x'x''' & xx''' + x'y''' \\ f & g & h \end{vmatrix}$$

where

$$f = (x+y)(x'+y') + (x''+y'')(x''' + y''') - (xx' + x''x''') - (yy' + y''y''')$$

$$g = (x+y)(x''+y'') + (x'+y')(x''' + y''') - (xx'' + x'x''') - (yy'' + y'y''')$$

$$h = (x+y)(x''' + y''') + (x' + y')(x'' + y'') - (xx''' + x'x'') - (yy''' + y'y'').$$

The identity may be verified by direct calculation. $\square$

From the above proposition, we see that any nondegenerate quartic ring with a basis of the form $1, x, y, x^2$ has a *unique* cubic resolvent ring, namely the ring spanned by the vectors $1, \varphi(x), \varphi(x+y) - \varphi(x) - \varphi(y)$. Let R be a nondegenerate quartic ring equipped with the basis $1, x, y, x^2$ and let C be the unique cubic resolvent ring; equip $C/\mathbb{Z}$ with the basis $\varphi(x), \varphi(x+y) - \varphi(x) - \varphi(y)$. Choose a

basis x, y, z for $R/\mathbb{Z}$. Then, the cubic resolvent map $\varphi: R/\mathbb{Z} \rightarrow C/\mathbb{Z}$, expressed in these bases, has the form:

$$(A, B) = \begin{bmatrix} 1 & 0 & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 1/2 & * \\ - & * & * \\ - & - & * \end{bmatrix}. \quad (4.18)$$

Conversely, a nondegenerate element of $V(\mathbb{Z})$ of the form (4.18) gives rise to the following data: a pair (R, C) , a basis x, y, z of $R/\mathbb{Z}$, and a basis $\varphi(x), \varphi(x+y) - \varphi(x) - \varphi(y)$ of $C/\mathbb{Z}$. Proposition 4.7.4 implies that

$$\text{Ind}(1, x, y, x^2) = \text{Ind}(1, \varphi(x), \varphi(x+y) - \varphi(x) - \varphi(y)) = 1$$

so $1, X, Y, X^2$ is a basis of R for any lifts $X, Y \in R$ of $x, y \in R/\mathbb{Z}$. This discussion proves the following theorem.

Theorem 4.7.5. *There is a canonical discriminant-preserving bijection between:*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{nondegenerate quadruples } (R, x, y, z) \\ \text{where } x, y, z \in R/\mathbb{Z} \text{ are such that} \\ 1, X, Y, X^2 \text{ is a basis of } R \\ \text{for any lifts } X, Y \in R \text{ of } x, y \in R/\mathbb{Z} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{nondegenerate pairs of} \\ \text{integral ternary quadratic forms} \\ \text{of the form (4.18)} \end{array} \right\}$$

Let H be the largest subgroup of $\text{GL}_2(\mathbb{Z}) \times \text{GL}_3(\mathbb{Z})$ acting on matrices of the form (4.18); H is generated by elements of the form:

$$\begin{aligned} & \begin{bmatrix} 1 & -2u \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ u & 1 & 0 \\ * & * & 1 \end{bmatrix} \\ & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix} \\ & \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{aligned} \quad (4.19)$$

Suppose R is a nondegenerate quartic ring. Consider pairs $(x, y) \in R$ such that $1, x, y, x^2$ is a

basis of R . Consider the equivalence relation on all pairs generated by $(x, y) \sim (\pm x + a, b + cx + \pm y)$ for integers $a, b, c \in \mathbb{Z}$. Now consider triples (R, x, y) where $x \in R/\mathbb{Z}$, $y \in R/\mathbb{Z}\langle 1, x \rangle$ are such that $R = \mathbb{Z}\langle 1, x, y, x^2 \rangle$. We say the triple is *nondegenerate* if R is nondegenerate. We say two such triples (R, x, y) and (R', x', y') are isomorphic if there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that $\alpha(x) \equiv x' \pmod{\mathbb{Z}}$ and $\alpha(y) \equiv y' \pmod{\mathbb{Z}\langle 1, x \rangle}$. We obtain:

Theorem 4.7.6. *There is a canonical discriminant preserving bijection between:*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{nondegenerate triples } (R, x, y) \\ \text{where } x \in R/\mathbb{Z}, y \in R/\mathbb{Z}\langle 1, x \rangle \text{ are such that} \\ R = \mathbb{Z}\langle 1, X, Y, X^2 \rangle \text{ for any lifts} \\ X, Y \in R \text{ of } x, y \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{nondegenerate orbit classes of} \\ \text{pairs of integral ternary quadratic forms} \\ \text{of the form (4.18)} \\ \text{under the action of } H \end{array} \right\}$$

We now restrict our attention to matrices of the form (4.7), which we repeat here:

$$(A, B) = \begin{bmatrix} 1 & 0 & * \\ - & * & * \\ - & - & * \end{bmatrix}, \begin{bmatrix} 0 & 1/2 & 0 \\ - & * & * \\ - & - & * \end{bmatrix}.$$

We consider quintuples $(R, x, y, \varepsilon, \nu)$ where $x \in R$, $y \in R/\mathbb{Z}$, $\varepsilon = \pm 1$, $\nu \in \{0, 1\}$, and x, y, x^2 is a basis of $R/\mathbb{Z}$. We say such a quintuple is *nondegenerate* if R is nondegenerate. We say two such quintuples $(R, x, y, \varepsilon, \nu)$ and $(R', x', y', \varepsilon', \nu')$ are isomorphic if $\varepsilon = \varepsilon'$, $\nu = \nu'$, and there exists a ring isomorphism $\alpha: R \rightarrow R'$ such that $\alpha(x) = x'$ and $\alpha(y) = y' \pmod{\mathbb{Z}}$.

Theorem 4.1.10. *There is a canonical discriminant-preserving bijection between:*

$$\left\{ \begin{array}{l} \text{isomorphism classes of} \\ \text{nondegenerate quintuples } (R, x, y, \varepsilon, \nu) \\ \text{where } x \in R \text{ and } y \in R/\mathbb{Z} \text{ are such that} \\ x, y, x^2 \text{ is a basis of } R/\mathbb{Z} \text{ and } \varepsilon = \pm 1 \text{ and } \nu \in \{0, 1\} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{nondegenerate pairs of} \\ \text{integral ternary quadratic forms} \\ \text{of the form (4.7)} \end{array} \right\}$$

Proof. Given such a nondegenerate pair of integral ternary quadratic forms, Theorem 4.7.5 gives a nondegenerate quartic ring with a basis x, y, z of $R/\mathbb{Z}$ with the property that $1, X, Y, X^2$ is a basis of R for any lifts $X, Y \in R$ of $x, y \in R/\mathbb{Z}$. There is a unique lift $X \in R$ of x and a unique value $\varepsilon = \pm 1$ and $\nu \in \{0, 1\}$ such that $z \equiv \varepsilon X^2 + \nu X \pmod{\mathbb{Z}\langle 1, y \rangle}$. We take the quintuple $(R, X, y, \varepsilon, \nu)$.

Conversely, given such a quintuple (R, x, y, ϵ, ν) , there exists a unique integer a such that

$$\varphi(x + (\epsilon x^2 + \nu x + ay)) - \varphi(\epsilon x^2 + \nu x + ay) \equiv 0 \pmod{\mathbb{Z}\langle 1, \varphi(x) \rangle}.$$

Equip $R/\mathbb{Z}$ with the basis $x, y, \epsilon x^2 + \nu x + ay$. Let C be the unique cubic resolvent ring of R and equip $C/\mathbb{Z}$ with the basis $1, \varphi(x), \varphi(x+y) - \varphi(x) - \varphi(y)$; taking the cubic resolvent map with respect to these bases gives an element of (4.7). A computation shows that these two maps are inverse to each other. $\square$

Recall that $\mathcal{F}^{x,y,x^2}$ is defined to be the set of isomorphism classes of triples (R, x, y) where R is a nondegenerate quartic ring and $x \in R$ and $y \in R/\mathbb{Z}$ is such that x, y, x^2 forms a basis of $R/\mathbb{Z}$. Let $W(\mathbb{Z})$ denote the set of matrices of the form (4.7) and ψ be the map from triples $(R, x, y) \in \mathcal{F}^{x,y,x^2}$ to pairs of integral ternary quadratic forms referred to in Theorem 4.1.10 given by setting $\epsilon = 1$ and $\nu = 0$. We now prove Theorem 4.1.11. Let $p = (1/10, 1/5, 1/5, 1/5, 3/10)$.

Proof of Theorem 4.1.11. The proof is almost identical to that of Theorem 4.1.9. Let $T = (R, x, y) \in \mathcal{F}^{x,y,x^2}$ be any triple of absolute discriminant Δ and let C be the unique cubic resolvent ring. A computation shows that $H(T) \leq X^{1/5}$ if and only if $\psi(T) \in B(p, X)$; thus for any positive real numbers M and X , Lemma 4.3.6 implies that if $\Delta \geq X/M$, then

$$\lambda_i(R) \asymp_M \Delta^{p_i}$$

$$\lambda_i(C) \asymp_M \Delta^{q_i}.$$

So, for each M there exists a constant ϵ_M such that if $\Delta \geq X/M$ and $H(T)^5 \leq X$, we have that T is (ϵ_M, X) -close to p . Moreover, we may suppose $\lim_{M \rightarrow \infty} \epsilon_M = \infty$. We first prove (4.4).

$$\begin{aligned} & \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,x^2} \mid H(T) \leq X \text{ and } \psi(T) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{T \in \mathcal{F}^{x,y,x^2} \mid H(T) \leq X\}} \\ & \geq \lim_{M \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,x^2} \mid H(T)^5 \leq X \text{ and } \Delta \geq X/M\}}{\#\{T \in \mathcal{F}^{x,y,x^2} \mid H(T)^5 \leq X\}}. \end{aligned}$$

Davenport's lemma gives:

$$\begin{aligned} \#\{T \in \mathcal{F}^{x,y,s^2} \mid H(T)^5 \leq X\} & \asymp \frac{1}{4} \#\{(A, B) \in W(\mathbb{Z}) \cap B(p, X) \mid \text{Disc}(A, B) \neq 0\} \\ & = \frac{X}{4} \text{Vol}\{(A, B) \in W(\mathbb{R}) \cap B(p, 1)\} + O(X^{9/10}). \end{aligned}$$

We now compute the numerator. Let

$$g_X = \left(\begin{bmatrix} X^{1/5} & 0 \\ 0 & X^{3/10} \end{bmatrix}, \begin{bmatrix} X^{-1/10} & 0 & 0 \\ 0 & X^{-1/5} & 0 \\ 0 & 0 & X^{-1/5} \end{bmatrix} \right).$$

By Davenport's lemma, we have

$$\begin{aligned} & \#\{T \in \mathcal{F}^{x,y,x^2} \mid H(T)^5 \leq X \text{ and } \Delta \geq X/M\} \\ & \asymp \frac{1}{4} \#\{(A, B) \in W(\mathbb{Z}) \cap B(p, X) \mid |\text{disc}(A, B)| \geq X/M\} \\ & = \frac{1}{4} \#\{(A, B) \in W(\mathbb{Z}) \cap B(p, X) \mid |\text{disc}(g(A, B))| \geq 1/M\} \\ & = \frac{1}{4} X \text{Vol}\{(A, B) \in W(\mathbb{R}) \cap B(p, 1) \mid |\text{disc}(A, B)| \geq 1/M\} + O(X^{9/10}). \end{aligned}$$

Now observe that

$$\lim_{M \rightarrow \infty} \text{Vol}\{(A, B) \in W(\mathbb{R}) \cap B(p, 1) \mid |\text{disc}(A, B)| \geq 1/M\} = 1$$

so

$$\lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{T \in \mathcal{F}^{x,y,x^2} \mid H(T) \leq X \text{ and } \psi(f) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{T \in \mathcal{F}^{x,y,x^2} \mid H(T) \leq X\}} = 1$$

We now prove Condition (4.5). Observe that a positive proportion of lattice points in $B(p, X)$ satisfy the conditions $a_{11} = b_{12} = 1$ and $a_{12} = b_{11} = 0$. Moreover, there exists C such that for every lattice point in $B(p, X)$ with $a_{11} = b_{12} = 1$ and $a_{12} = b_{11} = 0$, there exists a $\text{GL}_2(\mathbb{Z})$ -translate with $a_{11} = b_{12} = 1$ and $a_{12} = b_{11} = b_{13} = 0$ in $CB(p, X)$. Thus, a positive proportion of lattice points in $CB(p, X)$ arise from elements of $\mathcal{F}^{1,x,y,x^2}$; combining this observation with the proof of Lemma 4.5.2 shows that for ϵ sufficiently large, we have:

$$\#(\mathcal{F}(p, \epsilon, X) \cap \psi(\mathcal{F}^{1,x,y,x^2})) \ll_{\epsilon} X^{4/5}$$

Conversely, Lemma 4.5.3 shows that

$$\#\mathcal{F}(p, \epsilon, X) \gg X^{4/5}.$$

□

4.7.3 Binary quartic forms

Let $f = f_0x^4 + f_1x^3y + f_2x^2y^2 + f_3xy^3 + f_4y^4 \in \text{Sym}^4 \mathbb{Z}^2$ be a binary quartic form. Wood defines a map $\text{Sym}^4 \mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$ which canonically attaches to a binary quartic form a based quartic ring equipped with a cubic resolvent ring ([33]). In this thesis we use a slight variant of Wood's map⁶. In particular, we send a form f to the following element of $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$:

$$\begin{bmatrix} f_0 & f_1/2 & 0 \\ - & f_2 & f_3/2 \\ - & - & f_4 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1/2 \\ - & 1 & 0 \\ - & - & 0 \end{bmatrix}.$$

Let $p = (1/6, 1/6, 1/6, 1/6, 1/3)$ and let ψ denote the map from $\text{Sym}^4 \mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$. Observe that for any form $f \in \text{Sym}^4 \mathbb{Z}^2$, we have $H_c(f) \leq X^{1/6}$ if and only if $\psi(f) \in B(p, X)$.

Proof of Theorem 4.1.7. Again, the proof is almost identical to that of Theorem 4.1.9. Let M be any constant. Let $f \in \mathcal{F}_4^{\text{bin}}$ and let (R, C) be the corresponding rings. By Lemma 4.3.6, if $\Delta \geq X/M$ and $\psi(f) \in B(p, X)$, then

$$\lambda_i(R) \asymp_M \Delta^{p_i}$$

$$\lambda_i(C) \asymp_M \Delta^{q_i}.$$

To prove (4.4), it suffices to show that

$$\lim_{M \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F}_4^{\text{bin}} \mid H_c(f) \leq X \text{ and } \Delta \geq X^6/M\}}{\#\{f \in \mathcal{F}_4^{\text{bin}} \mid H_c(f) \leq X\}} = 1.$$

The denominator is clearly $X^5 + o(X^5)$. By Davenport's lemma, we have:

$$\begin{aligned} & \#\{f \in \mathcal{F}_4^{\text{bin}} \mid H_c(f) \leq X \text{ and } \Delta > X^6/M\} \\ &= \#\{(f_0, \dots, f_4) \in \mathbb{Z}^5 \mid \max\{|f_i|\} \leq X \text{ and } |\text{disc}(f_0, \dots, f_4)| > X^6/M\} \\ &= \text{Vol}\{(f_0, \dots, f_4) \in \mathbb{R}^5 \mid \max\{|f_i|\} \leq X \text{ and } |\text{disc}(f_0, \dots, f_4)| > X^6/M\} + O(X^4) \\ &= X^5 \text{Vol}\{(f_0, \dots, f_5) \in \mathbb{R}^5 \mid \max\{|f_i|\} \leq 1 \text{ and } |\text{disc}(f_0, \dots, f_4)| > 1/M\} + O(X^4) \end{aligned}$$

We now prove (4.5). Observe that by Lemma 4.5.2, there exists a constant M such that for all $\epsilon > M$, there are $\ll_\epsilon X^{5/6}$ isomorphism classes of tuples (R, C) such that $\Delta \leq X$ and (R, C) is (ϵ, X) -

⁶Our map and the map of Wood send a form f to isomorphic quartic rings and cubic resolvent rings. The only difference is a choice of basis of the quartic ring and cubic resolvent ring.

close to p . Theorem 3.5.8 shows that there are at most 2^{80} $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of binary quartic forms giving rise to the same quartic ring. Therefore, it suffices to show that there are $\gg X^{5/6}$ $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of binary quartics such that $\Delta \leq X$ and the corresponding rings (R, C) are (ϵ, X) -close to p ; this is precisely the statement of Theorem 1.2.4 when $r = (1/24, 1/24)$. $\square$

4.7.4 Monic quartic forms

Let $p = (1/12, 1/6, 1/4, 1/6, 1/3)$. Observe that for any monic integral quartic form f , we have $H_r(f) \leq X^{1/12}$ if and only if $H_r(f) \in B(p, X)$. Let $\mathcal{F}_4^{\mathrm{mon}}$ denote the set of monic quartic forms with integral coefficients and nonzero discriminant.

Proof of Theorem 4.1.6. Again, the proof is almost identical to that of Theorem 4.1.9. Let M be any constant. For any $f \in \mathcal{F}_4^{\mathrm{mon}}$ let (R, C) be the corresponding rings. By Lemma 4.3.6, if $\Delta \geq X/M$ and $\psi(f) \in B(p, X)$, then

$$\begin{aligned}\lambda_i(R) &\asymp_M \Delta^{p_i} \\ \lambda_i(C) &\asymp_M \Delta^{q_i}.\end{aligned}$$

To prove (4.4), it suffices to show that

$$\lim_{M \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F}_4^{\mathrm{mon}} \mid H_r(f) \leq X \text{ and } \Delta \geq X^{12}/M\}}{\#\{f \in \mathcal{F}_4^{\mathrm{mon}} \mid H_r(f) \leq X\}} = 1.$$

The denominator is clearly $X^{10} + o(X^{10})$. By Davenport's lemma, we have:

$$\begin{aligned}&\#\{f \in \mathcal{F}_4^{\mathrm{mon}} \mid H_r(f) \leq X \text{ and } \Delta > X^{12}/M\} \\ &= \#\{(f_1, \dots, f_4) \in \mathbb{Z}^4 \mid \max\{|f_i|^{1/i}\} \leq X \text{ and } |\mathrm{disc}(1, f_1, \dots, f_4)| > X^{12}/M\} \\ &= \mathrm{Vol}\{(f_1, \dots, f_4) \in \mathbb{R}^4 \mid \max\{|f_i|^{1/i}\} \leq X \text{ and } |\mathrm{disc}(1, f_1, \dots, f_4)| > X^{12}/M\} + O(X^9) \\ &= X^{10} \mathrm{Vol}\{(f_1, \dots, f_4) \in \mathbb{R}^4 \mid \max\{|f_i|\} \leq 1 \text{ and } |\mathrm{disc}(1, f_1, \dots, f_4)| > 1/M\} + O(X^9)\end{aligned}$$

We now prove (4.5). Observe that by Lemma 4.5.2, there exists a constant M such that for all $\epsilon > M$, there are $\ll_\epsilon X^{3/4}$ isomorphism classes of tuples (R, C) such that $\Delta \leq X$ and (R, C) is (ϵ, X) -close to p . Theorem 3.5.8 shows that there are at most 2^{80} $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of binary quartic forms giving rise to the same quartic ring. Therefore, it suffices to show that there are $\gg X^{3/4}$ $\mathrm{GL}_2(\mathbb{Z})$ -equivalence classes of binary quartics such that $\Delta \leq X$, the binary

quartic represents 1, and the corresponding rings (R, C) are (ϵ, X) -close to p ; this follows from Theorem 1.2.4 when $r = (0, 1/12)$. $\square$

4.8 Pictures of Poly_4 , $\text{Poly}_4(S_4)$, and $\text{Poly}_4(D_4)$

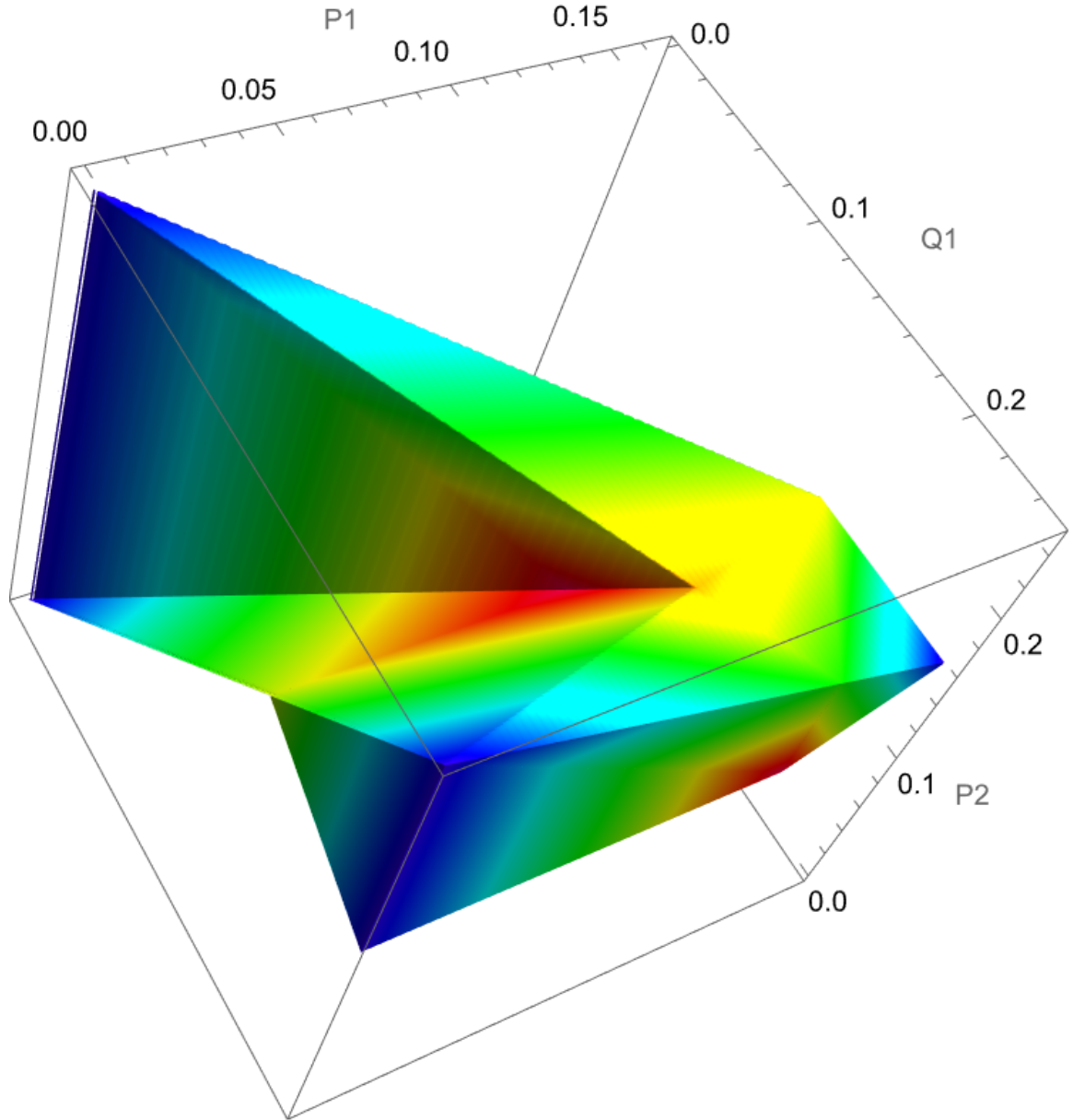


Figure 4.1: Poly_4 projected onto p_1 , p_2 , and q_1 . The color indicates the value of the density function $d_{\epsilon,4}$; blue is the highest value.

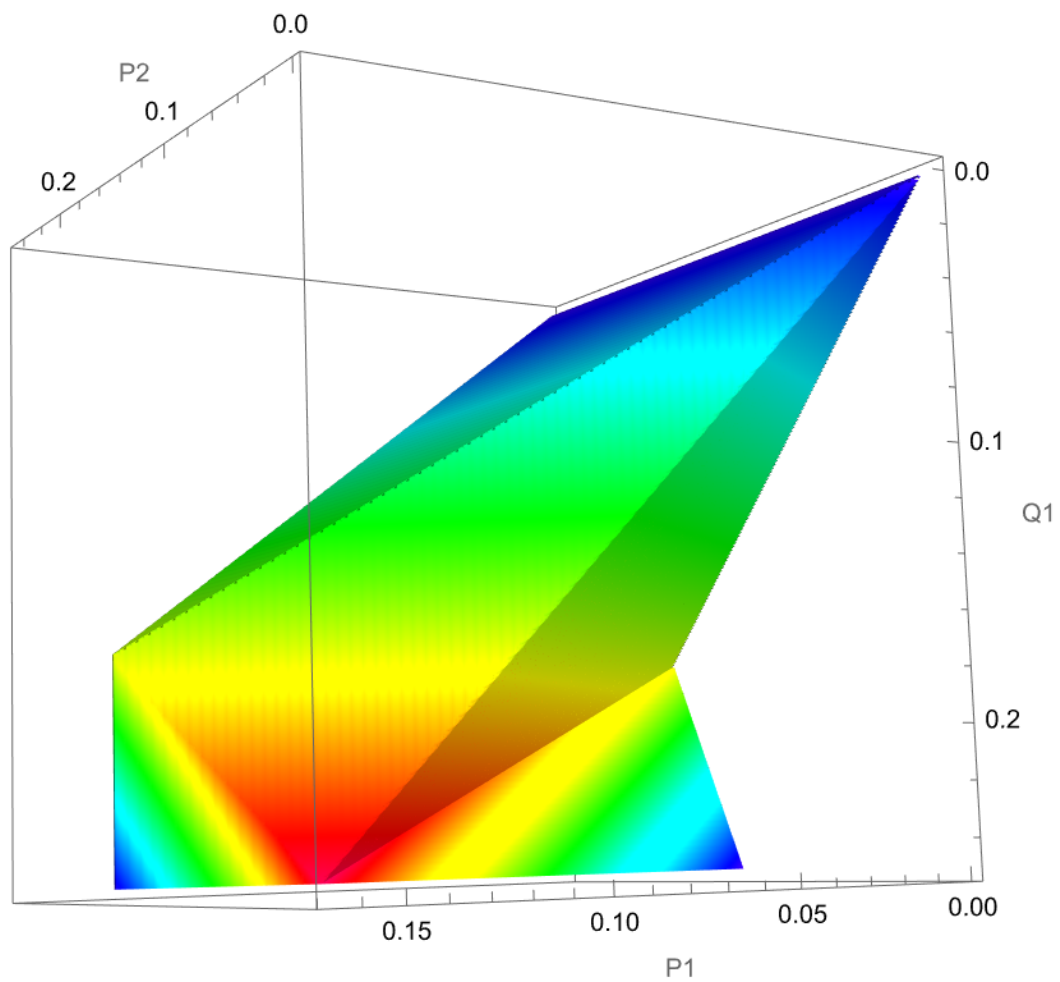


Figure 4.2: A rotated version of the previous image.

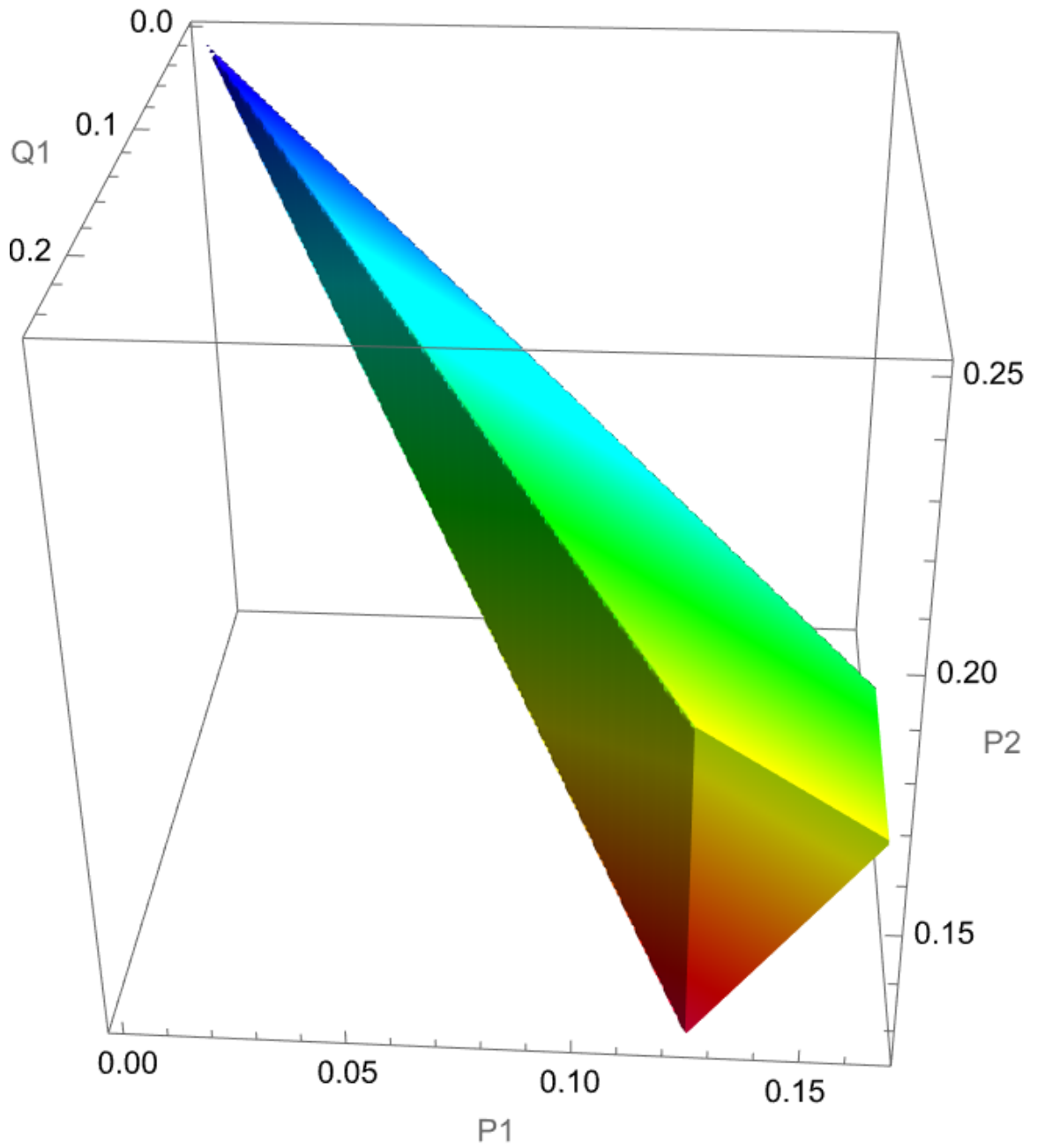


Figure 4.3: $\text{Poly}_4(D_4)$ projected onto p_1 , p_2 , and q_1 . The color indicates the value of the lower bound on the density function d_{ϵ, D_4} given in Theorem 1.3.3; blue is the highest value.

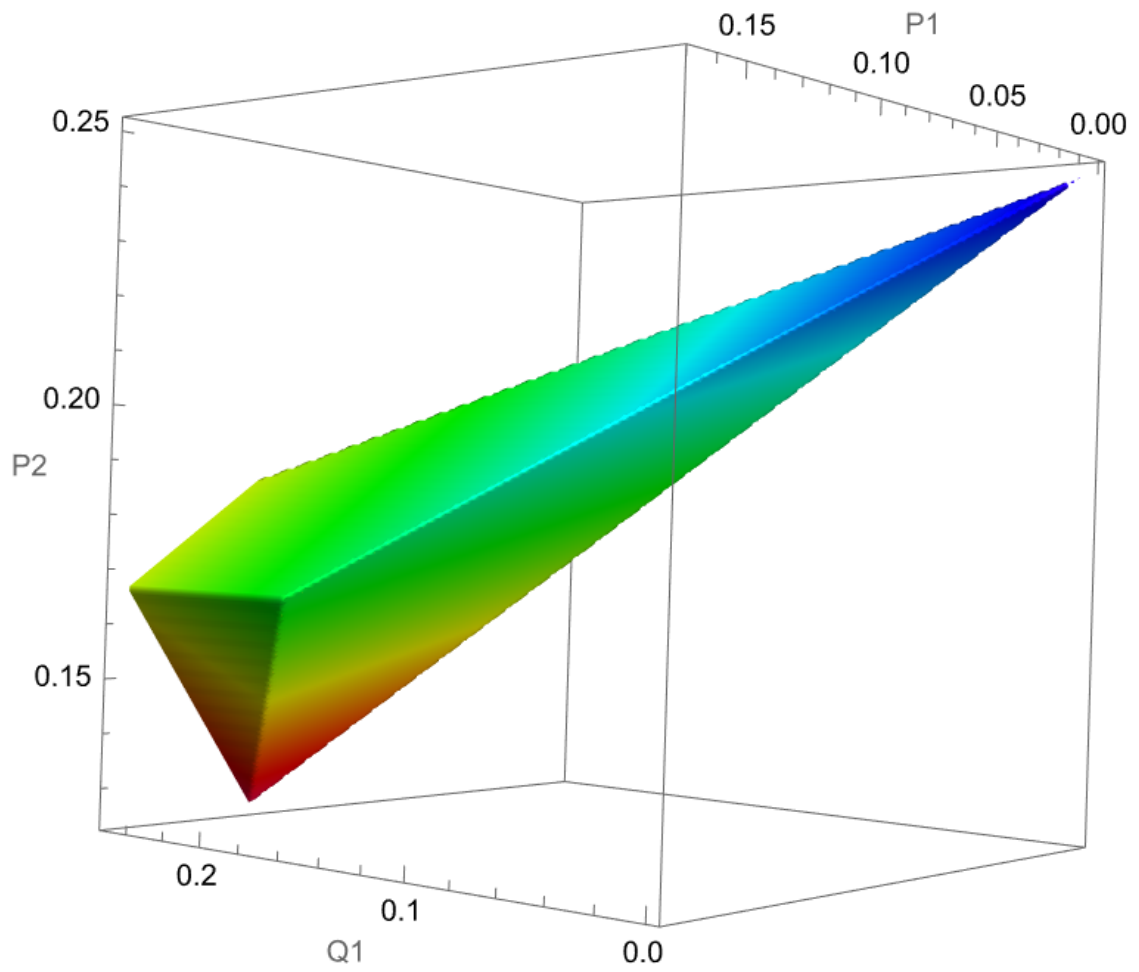


Figure 4.4: A rotated version of the previous image.

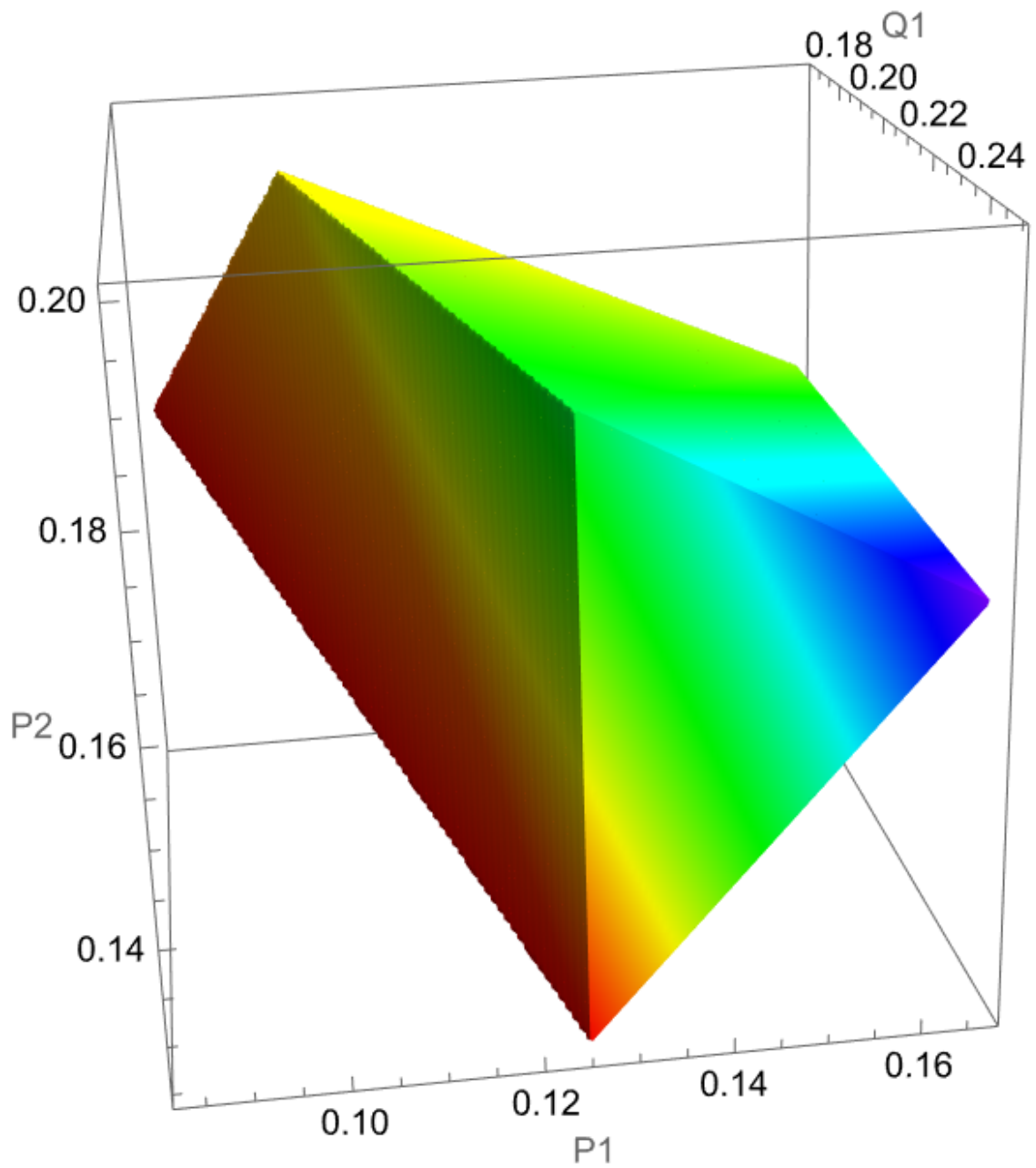


Figure 4.5: $\text{Poly}_4(S_4)$ projected onto p_1 , p_2 , and q_1 . The color indicates the value of the density function d_{ϵ, S_4} ; blue is the highest value.

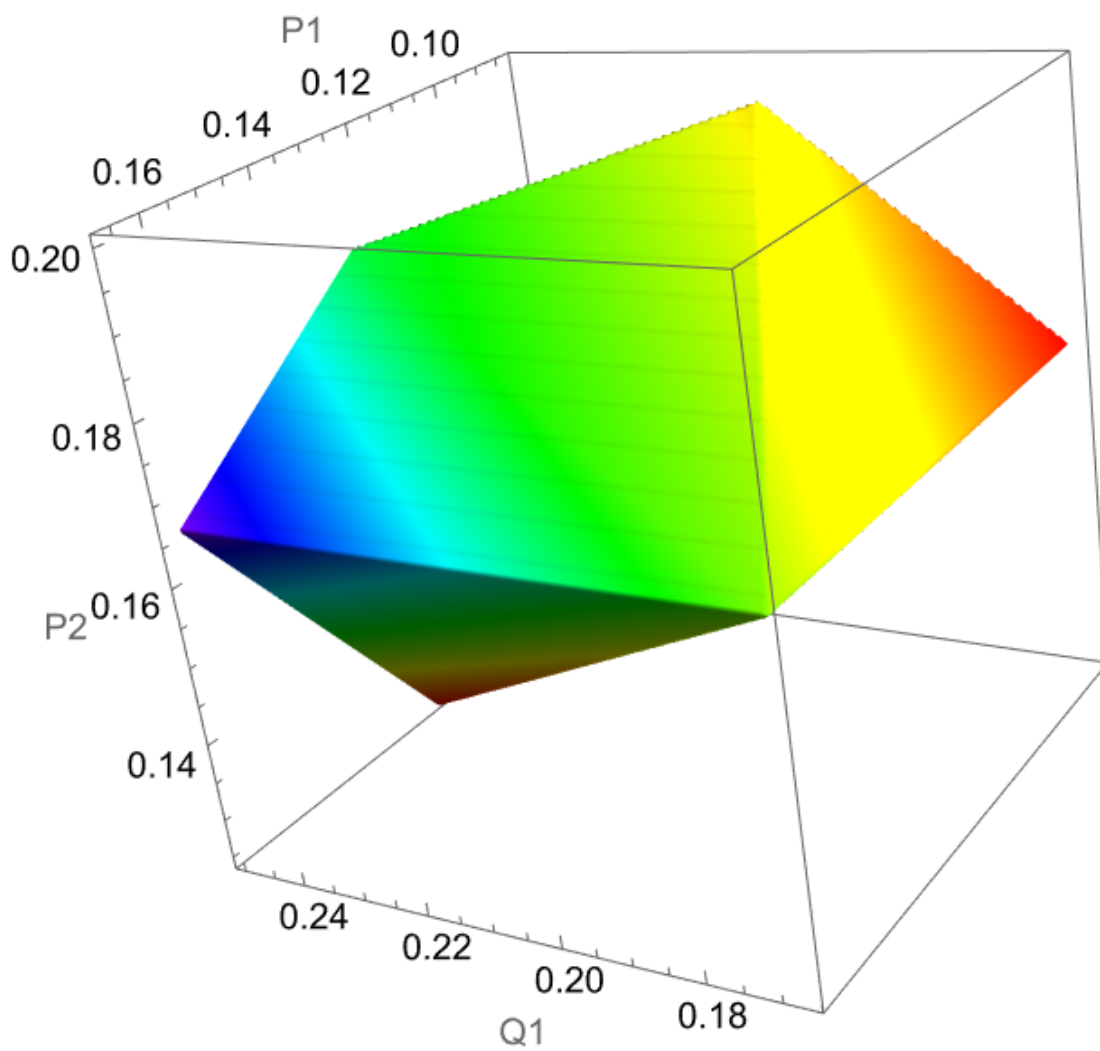


Figure 4.6: A rotated version of the previous image.

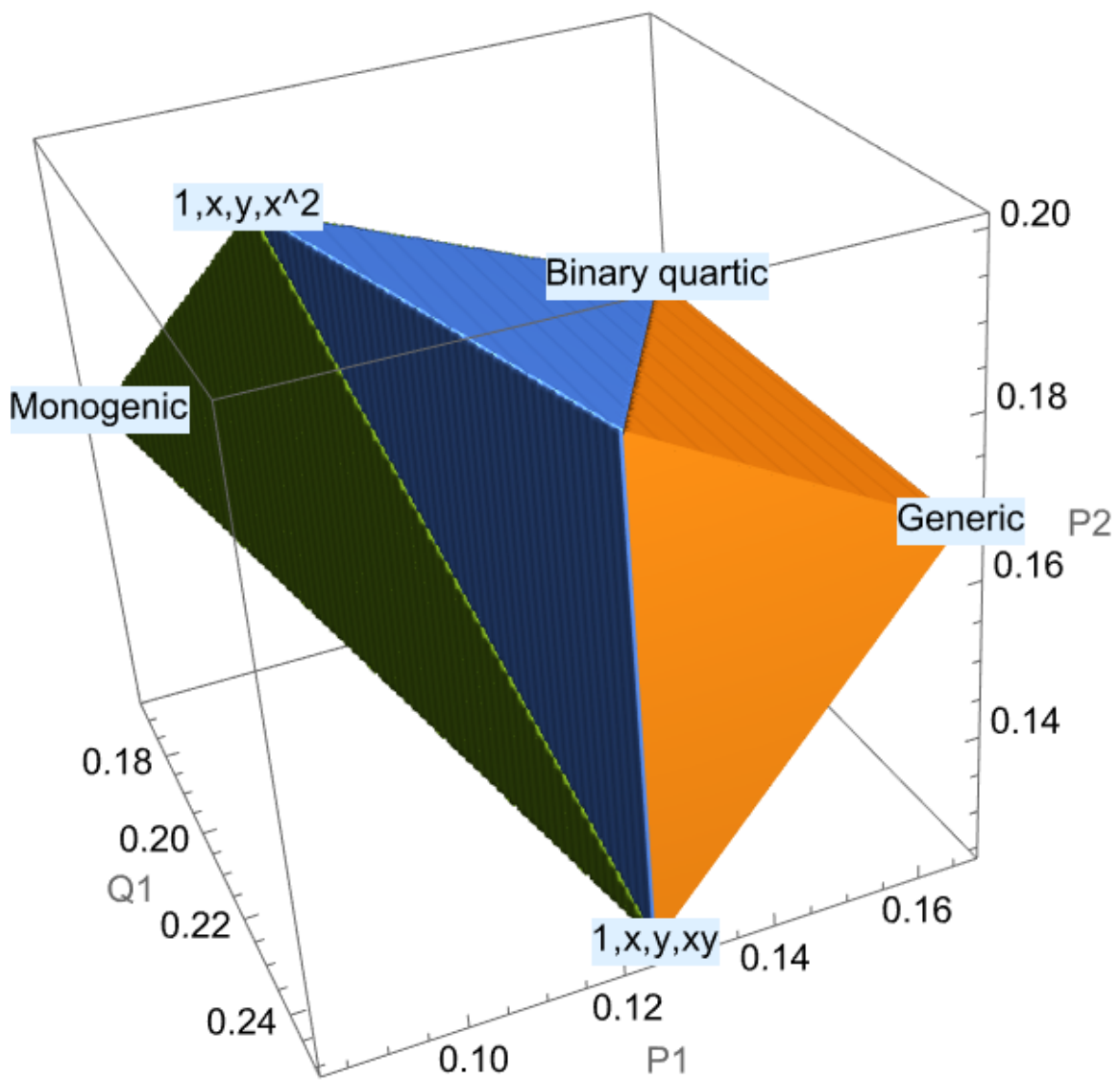


Figure 4.7: $\text{Poly}_4(S_4)$ projected onto p_1 , p_2 , and q_1 . The colored regions are the regions on which d_{ϵ, S_4} is linear. The vertices are labelled by the family of rings “corresponding” to them.

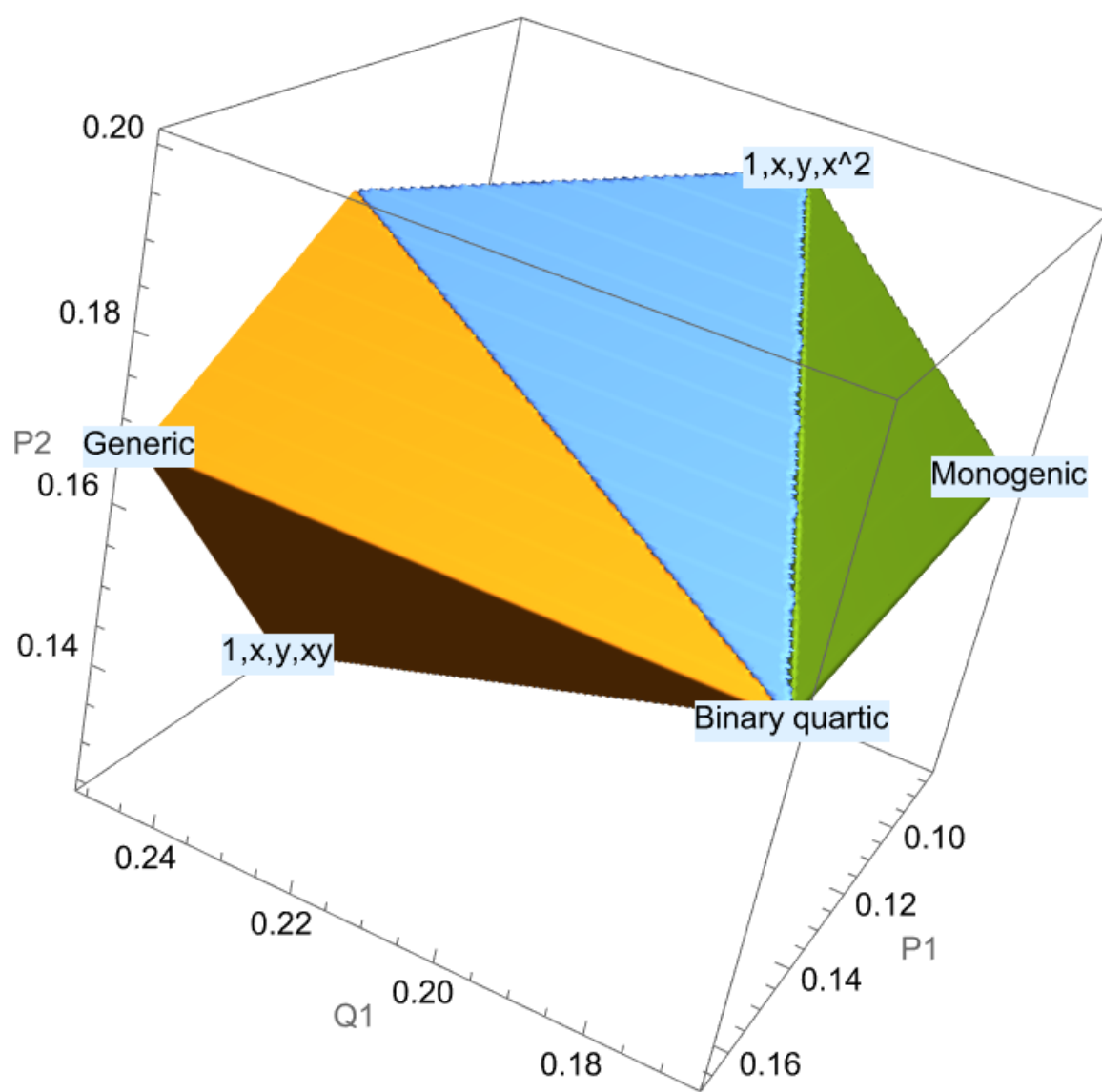


Figure 4.8: A rotated version of the previous image.

Chapter 5

Counting quintic rings by successive minima

We now investigate density functions of quintic rings. We will need to make use of the notion of a *sextic resolvent ring* of a quintic ring; see Section 5.2 for background. In this chapter, let R denote a quintic ring and let S denote a sextic resolvent ring of R . We say a pair (R, S) is *nondegenerate* if R is nondegenerate. Let $\Delta = |\text{Disc}(R)|$; by the definition of sextic resolvent rings, $\Delta^3 = |\text{Disc}(S)|$. Every pair (R, S) we reference in this chapter is assumed to be nondegenerate.

5.1 Statement of results

For a permutation group $G \subseteq S_5$, define $\text{Poly}_5(G)$ to be the set of limit points of the multiset

$$\{(\log_{\Delta} \lambda_1(R), \dots, \log_{\Delta} \lambda_4(R), \log_{\Delta} \lambda_1(S), \dots, \log_{\Delta} \lambda_5(S))\} \subseteq \mathbb{R}^9$$

in the Euclidean metric as we range over isomorphism classes of pairs (R, S) where R is a G -ring. Our results are threefold: we compute $\text{Poly}_5(S_5)$, we compute various density functions for quintic rings, and we discuss various interesting families of quintic rings.

5.1.1 Computing $\text{Poly}_5(G)$

Theorem 5.1.1. *For every permutation group $G \subseteq S_5$, the set $\text{Poly}_5(G)$ is a finite union of polytopes of dimension 7.*

In fact, the facets of these polytopes can be defined quite explicitly; see Theorem 5.4.2 for an explicit description of these polytopes. Theorem 5.1.1 is a natural generalization of Theorem 1.1.2 in the quintic case. We now explicitly describe this finite union of polytopes when $G = S_5$. Let

$$p = (p_1, \dots, p_4, q_1, \dots, q_5) \in \mathbb{R}^9$$

refer to a point of $\mathbb{R}^9$. By the definition of successive minima and Minkowski's theorem, the set $\text{Poly}_5(G)$ satisfies the linear inequalities

$$0 \leq p_1 \leq \dots \leq p_4, \quad 1/2 = \sum_i p_i, \quad 0 \leq q_1 \leq \dots \leq q_5, \quad \text{and } 3/2 = \sum_i q_i. \quad (5.1)$$

Theorem 5.1.2. *The set $\text{Poly}_5(S_5)$ is the set of points $p \in \mathbb{R}^9$ such that (5.1) and*

$$\begin{aligned} 1/2 + p_1 &\geq q_4 + q_1, & 1/2 + p_1 &\geq q_3 + q_2, & 1/2 + p_2 &\geq q_1 + q_5, & 1/2 + p_2 &\geq q_2 + q_4, \\ 1/2 + p_3 &\geq q_5 + q_2, & 1/2 + p_3 &\geq q_3 + q_4, & \text{and } 1/2 + p_4 &\geq q_5 + q_3. \end{aligned}$$

Moreover, $\text{Poly}_5(S_5) = \cup_G \text{Poly}_5(G)$ as G ranges across transitive subgroups of S_5 .

Thus, we see that $\text{Poly}_5(S_5)$ is in fact a single polytope! We now make a slight detour and discuss successive minima of resolvent rings. A sextic resolvent ring of a quintic S_5 -ring is a sextic $\psi(S_5)$ -ring, where ψ is a transitive embedding $\psi: S_5 \hookrightarrow S_6$; the embedding ψ is unique up to outer automorphism. It is a natural question to ask if the successive minima of sextic resolvent rings satisfy the same constraints as those of sextic $\psi(S_5)$ -rings. More precisely, is the set of limit points of the multiset

$$\{(\log_{|\text{Disc}(S)|} \lambda_1(S), \dots, \log_{|\text{Disc}(S)|} \lambda_5(S))\} \subseteq \mathbb{R}^5$$

as S ranges across sextic resolvent rings of quintic S_5 -rings equal to set of limit points of the multiset

$$\{(\log_{|\text{Disc}(S)|} \lambda_1(S), \dots, \log_{|\text{Disc}(S)|} \lambda_5(S))\} \subseteq \mathbb{R}^5$$

as S ranges across sextic $\psi(S_5)$ -rings? Let R_1 denote the first set of limit points and let R_2 denote the second.

Corollary 5.1.3. *R_1 is strictly contained in R_2 .*

Proof. The first region R_1 is $1/3$ times the projection of $\text{Poly}_5(S_5)$ onto the last 5 coordinates of $\mathbb{R}^9$. By Theorem 1.1.8, the second region R_2 is contained in of the set of points $q = (q_1, \dots, q_5) \in \mathbb{R}^5$ such that:

1. $1/2 = q_1 + \cdots + q_5$;
2. $0 \leq q_1 \leq \cdots \leq q_5$;
3. and $q_{i+j} \leq q_i + q_j$ for all $1 \leq i \leq j < i+j < 6$.

Notice that this region is precisely $\text{Len}(6)$; by Theorem 1.1.2, $\text{Len}(6)$ is contained in R_2 , as $\text{Len}(6)$ is the polytope of the flag generated by a monogenic basis of number field. In particular, the second region contains the point $\frac{1}{30}(1, 2, 3, 4, 5)$ but the first does not. $\square$

5.1.2 Density functions of quintic rings

Let $p = (p_1, \dots, p_4, q_1, \dots, q_5) \in \mathbb{R}^9$ denote a point. For any $\epsilon \in \mathbb{R}_{>0}$, $X \in \mathbb{R}_{>1}$, and permutation group $G \subseteq S_5$, define $\mathcal{F}(p, \epsilon, G, X)$ to be the set of isomorphism classes of pairs (R, S) such that R is a G -ring, $\Delta \leq X$, and

$$\max_{i=1,2,3,4} \{|\log_{\Delta} \lambda_i(R) - p_i|\} \leq \frac{\epsilon}{\log X} \quad (5.2)$$

$$\max_{i=1,2,3,4,5} \{|\log_{\Delta} \lambda_i(S) - q_i|\} \leq \frac{\epsilon}{\log X}. \quad (5.3)$$

Define the density function $d_{\epsilon, G}: \mathbb{R}^9 \rightarrow \mathbb{R} \cup \{*\}$ which assigns to $p \in \mathbb{R}^9$ the value

$$\lim_{X \rightarrow \infty} \frac{\log(\#\mathcal{F}(p, \epsilon, G, X) + 1)}{\log X}$$

if it exists and else assigns $*$. Similarly, let $\mathcal{F}(p, \epsilon, X)$ be the set of isomorphism classes of pairs (R, S) such that $\Delta \leq X$, (5.2), and (5.3). Let $d_{\epsilon, 5}$ denote the corresponding density function. We now compute the total density function for quintic rings and the S_5 -density function.

Theorem 1.4.1. *There exists a positive real number C such that for every $\epsilon > C$ and every $p \in \mathbb{R}^9$,*

$$d_{\epsilon, 5}(p) = \begin{cases} 1 - \sum_{1 \leq i < j \leq 4} (p_j - p_i) - \sum_{1 \leq i < j \leq 5} (q_j - q_i) & \text{if } p \in \text{Poly}_5 \\ + \sum_{i < j, k} \max\{0, -1/2 + q_i + q_j - p_k\} & \\ 0 & \text{else.} \end{cases}$$

Theorem 1.4.2. *There exists a positive real number C such that for every $\epsilon > C$ and every $p \in \mathbb{R}^9$,*

$$d_{\epsilon, S_5}(p) = \begin{cases} d_{\epsilon, 5}(p) & \text{if } p \in \text{Poly}_5(S_5) \\ 0 & \text{else.} \end{cases}$$

5.1.3 Special families of quintic rings

Again, we see that quintic rings with extremal successive minima tend to also be extremal in an *algebraic* sense. In the quartic case, we considered vertices of $\text{Poly}_4(S_4)$ and showed that many of these vertices corresponded to interesting families of quintic rings. The polytope $\text{Poly}_5(S_5)$ is significantly more complicated than $\text{Poly}_4(S_4)$; the polytope $\text{Poly}_5(S_5)$ has 18 vertices, and the author believes that many of them likely give rise to interesting and natural families of quartic rings. In this section, we discuss the following 3 of these vertices:

$$(1/8, 1/8, 1/8, 1/8, 3/10, 3/10, 3/10, 3/10, 3/10)$$

$$(1/8, 1/8, 1/8, 1/8, 1/4, 1/4, 1/4, 3/8, 3/8)$$

$$(1/20, 2/20, 3/20, 4/20, 4/20, 5/20, 6/20, 7/20, 8/20)$$

We'll show that the first “corresponds” to generic S_5 -rings, the second “corresponds” to binary quintic forms, and the third “corresponds” to monogenic quintic rings. We now formalize our definition of “correspond”.

We say a pair (R, S) is (ϵ, X) -close to p if

$$\max_{1 \leq i \leq 4} \{ |\log_{\Delta} \lambda_i(R) - p_i| \} \leq \frac{\epsilon}{\log X} \quad (5.4)$$

$$\max_{1 \leq i \leq 5} \{ |\log_{\Delta} \lambda_i(S) - q_i| \} \leq \frac{\epsilon}{\log X}. \quad (5.5)$$

Let $\mathcal{F}$ be an infinite set equipped with a map $H: \mathcal{F} \rightarrow \mathbb{R}_{>0}$ such that for all X , we have $\#\{f \in \mathcal{F} \mid H(f) \leq X\} < \infty$. We call H the *height function* of $\mathcal{F}$. Further suppose that ψ is a map from $\mathcal{F}$ to isomorphism classes of nondegenerate pairs of quintic rings equipped with a sextic resolvent. For a point $p \in \text{Poly}_5$, we say the triple $(\mathcal{F}, H, \psi)$ *corresponds to* p if

$$\lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F} \mid H(f) \leq X \text{ and } \psi(f) \text{ is } (\epsilon, X)\text{-close to } p\}}{\#\{f \mid H(f) \leq X\}} = 1 \quad (5.6)$$

and there exists a constant C such that for all $\epsilon > C$, we have

$$\liminf_{X \rightarrow \infty} \frac{\#\{(R, S) \in \mathcal{F}(p, \epsilon, X) \mid (R, S) \in \psi(\mathcal{F})\}}{\#\mathcal{F}(p, \epsilon, X)} > 0. \quad (5.7)$$

When H or ψ are implicit, we simply write that $\mathcal{F}$ corresponds to p . The following is a corollary of upcoming work of H.

Corollary 5.1.4. *The set of isomorphism classes of nondegenerate S_5 -rings, where H is the absolute discriminant, corresponds to*

$$(1/8, 1/8, 1/8, 1/8, 3/10, 3/10, 3/10, 3/10, 3/10).$$

The root height of a monic degree n polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ is defined to be $H_r(f) := \max_i \{|a_i|^{1/i}\}$. Given a binary n -ic form $f(x, y) = a_0x^n + \cdots + a_ny^n$, define the *coefficient height of f* to be $H_c(f) := \max_i \{|a_i|\}$. Fess [21] constructed a map from $\text{Sym}^5 \mathbb{Z}^2 \rightarrow \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$; via Bhargava's parametrization of quintic rings [3], this map canonically associates to an integral binary quintic form the data of a quintic ring and a sextic resolvent ring. Fess' construction is compatible with that of Birch and Merriman [9]; both constructions give isomorphic quintic rings from a binary quintic form. Let $\mathcal{F}_5^{\text{bin}}$ be the set of binary quintic forms with integral coefficients and nonzero discriminant.

Theorem 5.1.5. *Then $(\mathcal{F}_5^{\text{bin}}, H_c)$ corresponds to*

$$(1/8, 1/8, 1/8, 1/8, 1/4, 1/4, 1/4, 3/8, 3/8).$$

As in the case of monogenic cubics, monogenic quartics, and quartic rings coming from binary quartic forms (Corollary 3.1.4, Theorem 4.1.6, Theorem 4.1.7), there is a good reason to expect that $\mathcal{F}_5^{\text{bin}}$ (equipped with the coefficient height) corresponds to the point above; this reason comes from Fess' characterization of pairs (R, S) arising from binary quintic forms. For a rank n ring R , let $\tilde{R} := \text{Hom}(R/\mathbb{Z}, \mathbb{Z})$. Recall that a pair (R, S) comes equipped with a *sextic resolvent map* $\varphi: \tilde{S} \otimes \tilde{S} \rightarrow \tilde{R}$. For an basis $\{v_0 = 1, v_1, \dots, v_{n-1}\}$ of a nondegenerate rank n ring, let $\{v_0^*, v_1^*, \dots, v_{n-1}^*\}$ denote the dual basis with respect to the trace pairing.

Theorem 5.1.6 (Fess [21], Theorem 5.1.4). *Let (R, S) be a nondegenerate pair. There exists $f \in \text{Sym}^5 \mathbb{Z}^2$ giving rise to the pair (R, S) if and only if S has a basis $\{1, w_1, \dots, w_5\}$ such that*

$$(w_1, w_2, w_3) \equiv 8 \text{Disc}(R)((w_5^*)^2, 2w_4^*w_5^*, (w_4^*)^2) \pmod{\mathbb{Q}}$$

and $\varphi(w_4^*, w_5^*) = 0$.

From this classification, one might naively guess the following: if a pair (R, S) arises from a nondegenerate binary quintic form and $\{1, w_1, \dots, w_5\}$ is a Minkowski basis of S , then it is likely

that

$$\begin{aligned} |w_1| &\asymp \Delta |w_5|^{-2} \\ |w_2| &\asymp \Delta |w_4|^{-1} |w_5|^{-1} \\ |w_3| &\asymp \Delta |w_4|^{-2}. \end{aligned}$$

For lack of other information, one might also guess that $|w_4|$ is of similar size to $|w_5|$ and that the successive minima of the quintic ring R are roughly equal as well. Theorem 5.1.5 formalizes this heuristic. A similar heuristic informs the monogenic case. Let $\mathcal{F}_5^{\text{mon}}$ be the set of binary quintic forms with integral coefficients and nonzero discriminant.

Theorem 5.1.7. *Then $(\mathcal{F}_5^{\text{mon}}, H_r)$ corresponds to*

$$(1/20, 2/20, 3/20, 4/20, 4/20, 5/20, 6/20, 7/20, 8/20).$$

Observe that, as case of Theorem 5.1.5, the vertex

$$(1/20, 2/20, 3/20, 4/20, 4/20, 5/20, 6/20, 7/20, 8/20)$$

satisfies the conditions:

$$\begin{aligned} q_1 &= 1 - 2q_5 \\ q_2 &= 1 - q_4 - q_5 \\ q_3 &= 1 - 2q_4 \end{aligned}$$

5.2 The parametrization of quintic rings

Our primary tool will be Bhargava's parametrization of quintic rings; we now briefly summarize this parametrization. Let $V_{\mathbb{R}} = \mathbb{R}^4 \otimes \wedge^2 \mathbb{R}^5$. We write an element $\mathcal{A} = (A_1, A_2, A_3, A_4)$ as a quadruple of

5×5 real alternating matrices as follows:

$$A_k = \begin{bmatrix} 0 & a_{12}^k & a_{13}^k & a_{14}^k & a_{15}^k \\ -a_{12}^k & 0 & a_{23}^k & a_{24}^k & a_{25}^k \\ -a_{13}^k & - & 0 & a_{34}^k & a_{35}^k \\ -a_{14}^k & -a_{24}^k & -a_{34}^k & 0 & a_{45}^k \\ -a_{15}^k & -a_{25}^k & -a_{35}^k & -a_{45}^k & 0 \end{bmatrix}.$$

An element $\mathcal{A}$ is said to be *integral* if $a_{ij}^k \in \mathbb{Z}$, and the lattice of integral elements is denoted $V_{\mathbb{Z}}$.

The group $\mathrm{GL}_4(\mathbb{R}) \times \mathrm{GL}_5(\mathbb{R})$ acts on $V_{\mathbb{R}}$ in a natural way; an element (g_4, g_5) sends $\mathcal{A}$ to

$$g_4 \begin{bmatrix} g_5 A_1 g_5^t \\ g_5 A_2 g_5^t \\ g_5 A_3 g_5^t \\ g_5 A_4 g_5^t \end{bmatrix}.$$

The subgroup $G(\mathbb{Z}) = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$ acts on $V_{\mathbb{R}}$ and preserves the lattice $V_{\mathbb{Z}}$. The action of $G_{\mathbb{Z}}$ on $V_{\mathbb{Z}}$ has a unique polynomial invariant, denoted $\mathrm{Disc}(\mathcal{A})$. The orbits of $G_{\mathbb{Z}}$ acting on $V_{\mathbb{Z}}$ parametrize quintic rings equipped with a sextic resolvent ring; see [3] for more details.

Theorem 5.2.1 (Bhargava, [3]). *There is a canonical, discriminant-preserving bijection between $V_{\mathbb{Z}}$ and isomorphism classes of pairs (R, S) where R is a based quintic ring and S is a based sextic resolvent ring of R . Under the action of $G_{\mathbb{Z}}$, this bijection descends to a bijection between the set of $G_{\mathbb{Z}}$ orbits of $V_{\mathbb{Z}}$ and the set of isomorphism classes of pairs (R, S) where R is a quintic ring and S is a sextic resolvent ring of R .*

We now describe a few important details of this bijection. Let $\tilde{R}$ and $\tilde{S}$ denote $\mathrm{Hom}(R/\mathbb{Z}, \mathbb{Z})$ and $\mathrm{Hom}(S/\mathbb{Z}, \mathbb{Z})$ respectively. A sextic resolvent ring S of a quintic ring comes equipped with an alternating map $\tilde{S} \otimes \tilde{S} \rightarrow \tilde{R}$. Choosing bases for $R/\mathbb{Z}$ and $S/\mathbb{Z}$ gives rise to an element of $V_{\mathbb{Z}}$. Conversely, given an element $\mathcal{A} \in V_{\mathbb{Z}}$, we obtain bases for R and S via certain explicit polynomials in the a_{ij}^k that form the structure coefficients for these bases.

5.3 Reduction theory of quintic rings

We now fix some notation we use throughout this chapter. Unless otherwise specified, let $\mathcal{A} = (A_1, A_2, A_3, A_4)$ denote an element of $V_{\mathbb{Z}}$ and let (R, S) denote the corresponding quintic ring and

sextic resolvent ring. Let $\Delta = |\text{Disc}(\mathcal{A})| = |\text{Disc}(R)|$. For a basis $\{v_0 = 1, v_1, \dots, v_{n-1}\}$ of a nondegenerate rank n ring R , let $\{v_0^*, v_1^*, \dots, v_{n-1}^*\}$ denote the dual basis with respect to the trace pairing and let $R^* = \text{Hom}(R, \mathbb{Z})$. Unless otherwise specified, $\{1 = v_0, \dots, v_4\}$ and $\{1 = w_0, \dots, w_5\}$ will denote bases of the quintic ring R and the sextic resolvent ring S respectively. Given a pair (R, S) and bases $\{1 = v_0, \dots, v_4\}$ and $\{1 = w_0, \dots, w_5\}$ respectively, we obtain a tensor $\mathcal{A}$ by writing the resolvent $\varphi: \tilde{S} \otimes \tilde{S} \rightarrow \tilde{R}$ map in terms of the bases $\{v_4^*, \dots, v_1^*\}$ and $\{w_5^*, \dots, w_1^*\}$ of $\tilde{R}$ and $\tilde{S}$ respectively¹. In this section, we develop the relationship between:

1. pairs (R, S) equipped with “small” bases;
2. and tensors $\mathcal{A}$ with “small” coefficients.

We will need to relate the lengths of $\{v_1^*, \dots, v_4^*\}$ and $\{w_1^*, \dots, w_5^*\}$ to the lengths of $\{1, v_1, \dots, v_4\}$ and $\{1, w_1, \dots, w_5\}$, when the latter two bases are “short”; the content of the following lemma consists of the relationship between these two lengths.

Lemma 5.3.1. *Let R be any nondegenerate rank n ring and let $\{1 = v_0, \dots, v_{n-1}\}$ be a basis of R . Let θ be a positive real number such that the angle between any v_i and v_j in $\mathbb{R}^n$ is bounded below by θ in the Minkowski embedding of R . For all $0 \leq i \leq n-1$, we have*

$$|v_i| \asymp_{n,\theta} \lambda_i(R) \asymp_{n,\theta} \lambda_{n-1-i}(R^*)^{-1} \asymp_{n,\theta} |v_i^*|^{-1}.$$

Proof. Let r be the number of nonzero homomorphisms of R into $\mathbb{R}$ and let s be the number of complex conjugate pairs of nonzero homomorphisms of R into $\mathbb{C}$ whose image does not lie in $\mathbb{R}$. The Minkowski embedding of R into $\mathbb{R}^n$ is given via the composition of $R \rightarrow \mathbb{R}^r \oplus \mathbb{C}^s$ with the map

$$\begin{aligned} \mathbb{R}^r \oplus \mathbb{C}^s &\rightarrow \mathbb{R}^n \\ (y_1, \dots, y_r, z_1, \dots, z_s) &\rightarrow (y_1, \dots, y_r, \text{Re}(z_1), \text{Im}(z_1), \dots, \text{Re}(z_s), \text{Im}(z_s)). \end{aligned}$$

Because all norms on finite dimensional vector spaces are equivalent, it suffices to suppose that all lengths are taken with respect to the Euclidean norm on $\mathbb{R}^n$, i.e. let $|\cdot|$ denote the Euclidean norm. Note that $v_0, \dots, v_{n-1}$ form a set of linearly independent vectors in $\mathbb{R}^n$ via the Minkowski embedding; let $\{v_0^\vee, \dots, v_{n-1}^\vee\}$ denote the dual basis with respect to the standard Euclidean norm. We will show that the length of v_i^* is comparable to the length of $v_i^\vee$. Afterwards, we compute the lengths of $v_i^\vee$.

¹This ordering is very important! We encourage the reader to keep this ordering of the basis elements in mind throughout this chapter.

On $\mathbb{R}^n$, the trace form is given by the quadratic form

$$q(x_1, \dots, x_n) = \sum_{1 \leq i \leq r} x_i^2 + \sum_{1 \leq i \leq s} (2x_{r+2i-1}^2 - 2x_{r+2i}^2).$$

Let $\sigma: \mathbb{R}^n \rightarrow \mathbb{R}^n$ be the map sending

$$(y_1, \dots, y_r, z_1, \dots, z_s) \rightarrow (y_1, \dots, y_r, \frac{1}{2}\overline{z_1}, \dots, \frac{1}{2}\overline{z_s}).$$

For $0 \leq i \leq n-1$ write $v_i = (v_{1,i}, \dots, v_{n,i})$ and $v_i^\vee = (v_{1,i}^\vee, \dots, v_{n,i}^\vee)$.

$$\begin{aligned} q(\sigma(v_i^\vee), v_j) &= \sum_{1 \leq k \leq r} v_{k,i}^\vee v_{k,j} + \sum_{1 \leq k \leq s} (2\frac{1}{2}v_{r+2k-1,i}^\vee v_{r+2k-1,j} - 2\frac{-1}{2}v_{r+2k,i}^\vee v_{r+2k,j}) \\ &= \sum_{1 \leq k \leq r} v_{k,i}^\vee v_{k,j} + \sum_{1 \leq k \leq s} (v_{r+2k-1,i}^\vee v_{r+2k-1,j} + v_{r+2k,i}^\vee v_{r+2k,j}) \\ &= \delta_{ij} \end{aligned}$$

Thus, $\sigma(v_i^\vee) = v_i^*$ for all $0 \leq i \leq n-1$. Moreover, the angle between $v_i^\vee$ and v_i is $\leq c_\theta \pi/2$ where $0 \leq c_\theta < 1$ and c_θ is dependent only on θ . Hence

$$\begin{aligned} 1 &= v_i^\vee \cdot v_i && \text{because } v_i^\vee \cdot v_j = \delta_{ij} \\ &\asymp_\theta |v_i^\vee| |v_i| && \text{because of the angle bound } c_\theta \\ &= |\sigma^{-1}(v_i^*)| |v_i| && \text{because } \sigma(v_i^\vee) = v_i^* \\ &\asymp_n |v_i^*| |v_i|. \end{aligned}$$

Moreover,

$$\text{Covol}(R)^{-1} \asymp_{n,\theta} \prod_{i=0}^{n-1} |v_i|^{-1} \asymp_{n,\theta} \prod_{i=0}^{n-1} |v_i^*| \gg_n \prod_{i=0}^{n-1} \lambda_i(R^*) \asymp_n \text{Covol}(R^*) \asymp_n \text{Covol}(R)^{-1}.$$

Hence, $|v_i^*| \asymp_{n,\theta} \lambda_{n-1-i}(R^\vee)$, which completes the proof. $\square$

We now show that if the sextic resolvent map is expressed with respect to “short” bases of R and S , then the coefficients of the map are “small”. To do so, we will need the following explicit description of the sextic resolvent map. Let $\sigma_1, \dots, \sigma_6$ be the 6 nonzero homomorphisms of S into

the complex numbers. The sextic resolvent map $\varphi: \tilde{S} \otimes \tilde{S} \rightarrow \tilde{R}$ is given by the formula:

$$\varphi(u \otimes v) = \frac{\sqrt{\text{Disc}(S)}}{48 \text{Disc}(R)} \begin{vmatrix} 1 & 1 & 1 \\ \sigma_1(u) + \sigma_2(u) & \sigma_3(u) + \sigma_6(u) & \sigma_4(u) + \sigma_5(u) \\ \sigma_1(v) + \sigma_2(v) & \sigma_3(v) + \sigma_6(v) & \sigma_4(v) + \sigma_5(v) \end{vmatrix}$$

Lemma 5.3.2. *If $\{1, v_1, \dots, v_4\}$ and $\{1, w_1, \dots, w_5\}$ are Minkowski bases of R and S respectively, then for any $1 \leq i, j \leq 4$ and any $1 \leq k \leq 5$, we have:*

$$|a_{ij}^k| \ll \frac{\Delta^{1/2} |v_{5-k}|}{|w_{6-i}| |w_{6-j}|}$$

Proof. From the definition of the sextic resolvent map, we have that:

$$\begin{aligned} |a_{ij}^k| &\ll \frac{|\varphi(w_{6-i}^* \otimes w_{6-j}^*)|}{|v_{5-k}^*|} \\ &\ll \frac{\Delta^{1/2} |w_{6-i}^*| |w_{6-j}^*|}{|v_{5-k}^*|} && \text{by the explicit description of } \varphi \\ &\ll \frac{\Delta^{1/2} |v_{5-k}|}{|w_{6-i}| |w_{6-j}|} && \text{by Lemma 5.3.1} \end{aligned}$$

□

Let $p = (p_1, \dots, p_4, q_1, \dots, q_5) \in \mathbb{R}^9$ be any point. Let $B(p, X)$ denote the set of elements $\mathcal{A} \in V_{\mathbb{R}}$ such that

$$|a_{ij}^k| \leq \exp[X, 1/2 + p_{5-k} - q_{6-i} - q_{6-j}].$$

We now fix more notation we use throughout this chapter. Let ϵ denote a positive real number, let C, D denote real numbers ≥ 1 , and let X denote a real number > 1 . Recall that we say the pair (R, S) is (ϵ, X) -close to p if:

$$\begin{aligned} \max_{1 \leq i \leq 4} \{|\log_{\Delta} \lambda_i(R) - p_i|\} &\leq \frac{\epsilon}{\log X} \\ \max_{1 \leq i \leq 5} \{|\log_{\Delta} \lambda_i(S) - q_i|\} &\leq \frac{\epsilon}{\log X} \end{aligned}$$

For an integral element $\mathcal{A}$, we say $(\mathcal{A}, p)$ are (ϵ, X) -close if the corresponding pair (R, S) is (ϵ, X) -close to p . We say an integral element $\mathcal{A}$ comes from Minkowski bases if there exist Minkowski bases of the corresponding rings giving rise to $\mathcal{A}$.

Lemma 5.3.3. *There exists C such that for all ϵ , $\mathcal{A}$ and p the following statement holds: if $\Delta > 1$ and $(\mathcal{A}, p)$ are (ϵ, Δ) -close and $\mathcal{A}$ comes from Minkowski bases, then $\mathcal{A} \in Ce^{3\epsilon}B(p, \Delta)$.*

Proof. Let $\{1, v_1, \dots, v_4\}$ and $\{1, w_1, \dots, w_5\}$ be the Minkowski bases of (R, S) giving rise to $\mathcal{A}$. We have:

$$\begin{aligned}
|a_{ij}^k| &\ll \frac{\Delta^{1/2} |v_{5-k}|}{|w_{6-i}| |w_{6-j}|} && \text{by Lemma 5.3.2} \\
&\asymp \frac{\Delta^{1/2} \lambda_{5-k}(R)}{\lambda_{6-i}(S) \lambda_{6-j}(S)} && \text{by Lemma 5.3.1} \\
&\leq e^{3\epsilon} \exp[X, 1/2 + p_{5-k} - q_{6-i} - q_{6-j}] && \text{because } (\mathcal{A}, p) \text{ is } (\epsilon, \Delta)\text{-close}
\end{aligned}$$

□

Lemma 5.3.4. *There exists D such that for all p , X , C and $\mathcal{A}$, the following statement holds: if p satisfies (5.1) and $\mathcal{A} \in CB(p, X)$ then*

$$\#\{\mathcal{A}' \in DCB(p, X) \cap V_{\mathbb{Z}} \mid (R, S) \simeq (R', S')\} \geq \exp[X, \sum_{1 \leq i < j \leq 4} (p_j - p_i) + \sum_{1 \leq i < j \leq 5} (q_j - q_i)].$$

where here (R', S') denotes the quintic ring and sextic resolvent ring arising from tensor $\mathcal{A}'$.

Proof. Recall that $V_{\mathbb{Z}}$ admits an action of $G_{\mathbb{Z}} = \text{GL}_4(\mathbb{Z}) \times \text{GL}_5(\mathbb{Z})$. Act by elements of $G_{\mathbb{Z}}$ of the form

$$\left(\begin{bmatrix} 1 & n_{12} & n_{13} & n_{14} \\ 0 & 1 & n_{23} & n_{24} \\ 0 & 0 & 1 & n_{34} \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ m_{12} & 1 & 0 & 0 & 0 \\ m_{13} & m_{23} & 1 & 0 & 0 \\ m_{14} & m_{24} & m_{34} & 1 & 0 \\ m_{15} & m_{25} & m_{35} & m_{45} & 1 \end{bmatrix} \right)$$

where $|n_{ij}| \leq \lceil \exp[X, p_{5-i} - p_{5-j}] \rceil$ and $|m_{ij}| \leq \lceil \exp[X, q_{6-i} - q_{6-j}] \rceil$. □

Choose $\mathcal{A} \in V_{\mathbb{Z}}$ and let $\{v_0 = 1, v_1, \dots, v_4\}$ and $\{w_0 = 1, w_1, \dots, w_5\}$ be the explicit bases of R and S obtained from $\mathcal{A}$ via the explicit multiplication coefficients in [3].

Lemma 5.3.5. *For all $\mathcal{A}$, C , p , and X , the following statement holds: if p satisfies (5.1) and $\mathcal{A} \in CB(p, X)$, then $|v_i| \ll_C X^{p_i}$ for $i = 1, 2, 3, 4$ and $|w_i| \ll_C X^{q_i}$ for $i = 1, 2, 3, 4, 5$.*

Proof. Using the fact that $\mathcal{A} \in B(p, X)$, we may bound the size of the multiplication coefficients

given in [3]. We obtain:

$$|v_i|^2 \ll_C \max_{0 \leq j \leq 4} \{X^{2p_i - p_j} |v_j|\}$$

$$|w_i|^2 \ll_C \max_{0 \leq j \leq 5} \{X^{2q_i - q_j} |w_j|\}$$

Applying Lemma 6.0.2 completes the proof. $\square$

Lemma 5.3.6. *For all p satisfying (5.1), all X, C , and all $\mathcal{A}$, the following statement holds: if $\mathcal{A} \in V_{\mathbb{Z}} \cap CB(p, X)$ and $X/2 \leq \Delta \leq X$, then there are*

$$\#\{\mathcal{A}' \in CB(p, X) \cap V_{\mathbb{Z}} \mid (R, S) \simeq (R', S')\} \ll_C \exp[X, \sum_{1 \leq i < j \leq 4} (p_j - p_i) + \sum_{1 \leq i < j \leq 5} (q_j - q_i)].$$

Proof. Let $\{v_0 = 1, v_1, v_2, v_3, v_4\}$ and $\{w_0 = 1, w_1, \dots, w_5\}$ be the explicit bases of R and S obtained from $\mathcal{A}$. By Lemma 5.3.5, we have $|v_i| \ll_C X^{p_i}$ for $i = 1, 2, 3, 4$ and $|w_i| \ll_C X^{q_i}$ for $i = 1, 2, 3, 4, 5$.

Because

$$X^{1/2} \asymp \Delta^{1/2} \ll \prod_{i=1}^4 |v_i| \ll_C X^{\sum_{i=1}^4 p_i} = X^{1/2}$$

and

$$X^{3/2} \asymp \Delta^{3/2} \ll \prod_{i=1}^5 |w_i| \ll_C X^{\sum_{i=1}^5 q_i} = X^{3/2}$$

we have $|v_i| \asymp_C X^{p_i}$ for $i = 1, 2, 3, 4$ and $|w_i| \asymp_C X^{q_i}$ for $i = 1, 2, 3, 4, 5$.

Suppose $\mathcal{A}' \in CB(p, X) \cap V_{\mathbb{Z}}$ is such that $(R', S') \simeq (R, S)$. Let $\{1, v'_1, \dots, v'_4\}$ and $\{1, w'_1, \dots, w'_5\}$ denote the bases of R' and S' given by $\mathcal{A}'$. By Lemma 5.3.5, we have $|v'_i| \asymp_C X^{p_i}$ for $i = 1, 2, 3, 4$ and $|w'_i| \asymp_C X^{q_i}$ for $i = 1, 2, 3, 4, 5$. Moreover, write

$$\begin{aligned} v'_i &= c_{i0} + \sum_{j=1}^4 c_{ij} v_j \\ w'_i &= d_{i0} + \sum_{j=1}^5 d_{ij} w_j. \end{aligned}$$

The tensor $\mathcal{A}'$ is determined by the choices of c_{ij} and d_{ij} . Letting $p_0 = q_0 = 0$, we have:

$$X^{p_i} \asymp_C |v'_i| \asymp_C \max_{0 \leq j < 5} \{|c_{ij}| |v_j|\} \asymp_C \max\{0 \leq j < 5\} \{|c_{ij}| X^{p_j}\}$$

$$X^{q_i} \asymp_C |w'_i| \asymp_C \max_{0 \leq j < 6} \{|d_{ij}| |w_j|\} \asymp_C \max\{0 \leq j < 6\} \{|d_{ij}| X^{q_j}\}$$

Thus if $j \leq i$, the number of choices for c_{ij} and d_{ij} is $\ll_C 1$. If $j > i$, the number of choices for c_{ij} is $\ll_C X^{p_j - p_i}$ and the number of choices for d_{ij} is $\ll_C X^{q_j - q_i}$. Hence, there are $\ll_C$

$\exp[X, \sum_{1 \leq i < j \leq 4} (p_j - p_i) + \sum_{1 \leq i < j \leq 5} (q_j - q_i)]$ distinct integral $\mathcal{A}' \in CB(p, X)$ such that $(R', S') \simeq (R, S)$. $\square$

Lemma 5.3.7. *For all p satisfying (5.1), all X, C , and all $\mathcal{A}$, the following statement holds: if $\mathcal{A} \in V_{\mathbb{Z}} \cap CB(p, X)$ and $\frac{X}{2} \leq \Delta$ then*

$$\lambda_i(R) \asymp_C \Delta^{p_i}$$

for $i = 1, 2, 3, 4$ and

$$\lambda_i(C) \asymp_C \Delta^{q_i}$$

for $i = 1, 2, 3, 4, 5$.

Proof. We have

$$\begin{aligned} \prod_{i=1}^4 \lambda_i(R) &\ll \prod_{i=1}^4 |v_i| && \text{by definition of successive minima} \\ &\ll_C \prod_{i=1}^4 X^{p_i} && \text{by Lemma 5.3.5} \\ &= X^{1/2} && \text{because } p_1 + p_2 + p_3 + p_4 = 1/2 \\ &\asymp \Delta^{1/2} && \text{because } \Delta \geq X/2 \\ &\asymp \prod_{i=1}^4 \lambda_i(R). && \text{by Minkowski's second theorem} \end{aligned}$$

Thus $\lambda_i(R) \asymp_C \Delta^{p_i}$ for $i = 1, 2, 3, 4$. The same argument shows, for the sextic resolvent, that $\lambda_i(S) \asymp_C \Delta^{q_i}$ for $i = 1, 2, 3, 4, 5$. $\square$

5.4 Computing $\text{Poly}_5(G)$

Let K denote a quintic étale algebra over $\mathbb{Q}$ and L denote the sextic resolvent algebra of K . Let K_0 denote the subspace of K with trace 0, and let L_0 denote the subspace of L with trace 0. Let $\varphi: L_0 \otimes L_0 \rightarrow K_0$ denote the alternating bilinear form given by the sextic resolvent map. A *flag* $(\mathcal{F}, \mathcal{G})$ of (K, L) is a pair of sequences $\mathcal{F} = (F_0, \dots, F_5)$ and $\mathcal{G} = (G_0, \dots, G_4)$ of $\mathbb{Q}$ -vector spaces such that

$$\{0\} = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_5 = L_0$$

$$\{0\} = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_4 = K_0$$

and $\dim_{\mathbb{Q}} F_i = i$ and $\dim_{\mathbb{Q}} G_i = i$. Recall that for an integer $n > 1$, the set $[n] = \{0, \dots, n-1\}$. Associate to the flag $(\mathcal{F}, \mathcal{G})$ the function

$$T_{\mathcal{F}, \mathcal{G}}: [6] \times [6] \longrightarrow [5]$$

$$(i, j) \longmapsto \min\{k \in [5] \mid \varphi\langle F_i \otimes F_j \rangle \subseteq G_k\}.$$

Definition 5.4.1. The polytope $P_{\mathcal{F}, \mathcal{G}}$ is the set of $p = (p_1, \dots, p_4, q_1, \dots, q_5) \in \mathbb{R}^9$ satisfying (5.1) and the following condition: for all $1 \leq i \leq j \leq 5$, if $T_{\mathcal{F}, \mathcal{G}}(i, j) > 0$ then

$$p_{5-T_{\mathcal{F}, \mathcal{G}}(i, j)} + 1/2 \geq q_{6-i} + q_{6-j}.$$

The proof of the following theorem is almost exactly analogous to that of Theorem 4.4.2.

Theorem 5.4.2. *We have $\text{Poly}_5(G) = \bigcup_{(\mathcal{F}, \mathcal{G})} P_{\mathcal{F}, \mathcal{G}}$ where $(\mathcal{F}, \mathcal{G})$ ranges across flags of pairs (K, L) with the property that $\text{Gal}(K) \simeq G$ as a permutation group.*

Proof. We first show that $\text{Poly}_5(G)$ is contained in $\bigcup_{(\mathcal{F}, \mathcal{G})} P_{\mathcal{F}, \mathcal{G}}$. By Minkowski's second theorem and the definition of successive minima, $\text{Poly}_5(G)$ satisfies the linear inequalities given in (5.1). Let R be any nondegenerate quintic G -ring and let S be a sextic resolvent ring of G . Let $K = R \otimes \mathbb{Q}$ and let $L = S \otimes \mathbb{Q}$. Picking Minkowski bases $\{v_0 = 1, \dots, v_4\}$ and $\{w_0 = 1, \dots, w_5\}$ of R and S gives rise to dual bases $\{v_0^*, \dots, v_4^*\}$ and $\{w_0^*, \dots, w_5^*\}$ of R and S respectively. These give rise to a flag $(\mathcal{F}, \mathcal{G})$ of (K, L) given by $F_0 = G_0 := \{0\}$ and

$$F_i := \mathbb{Q}\langle w_5^*, \dots, w_{6-i}^* \rangle$$

$$G_i := \mathbb{Q}\langle v_4^*, \dots, v_{5-i}^* \rangle.$$

Choose $1 \leq i \leq j \leq 5$ and suppose $T_{\mathcal{F}, \mathcal{G}}(i, j) > 0$. Then if $T_{\mathcal{F}, \mathcal{G}}(i, j) = 1$ then

$$0 \neq \varphi\langle \mathbb{Z}\langle w_5^*, \dots, w_{6-i}^* \rangle \otimes \mathbb{Z}\langle w_5^*, \dots, w_{6-j}^* \rangle \rangle \subseteq \mathbb{Z}\langle v_4^*, \dots, v_{5-T_{\mathcal{F}, \mathcal{G}}(i, j)}^* \rangle.$$

If $T_{\mathcal{F}, \mathcal{G}}(i, j) > 1$ then

$$\varphi\langle \mathbb{Z}\langle w_5^*, \dots, w_{6-i}^* \rangle \otimes \mathbb{Z}\langle w_5^*, \dots, w_{6-j}^* \rangle \rangle \subseteq \mathbb{Z}\langle v_4^*, \dots, v_{5-T_{\mathcal{F}, \mathcal{G}}(i, j)}^* \rangle$$

and

$$\varphi\langle \mathbb{Z}\langle w_5^*, \dots, w_{6-i}^* \rangle \otimes \mathbb{Z}\langle w_5^*, \dots, w_{6-j}^* \rangle \rangle \not\subseteq \mathbb{Z}\langle v_4^*, \dots, v_{5-T_{\mathcal{F},\mathcal{G}}(i,j)+1}^* \rangle$$

In either case we obtain:

$$|v_{5-T_{\mathcal{F},\mathcal{G}}(i,j)}^*| \ll |w_{6-i}^*| |w_{6-j}^*| \Delta^{1/2}$$

which implies by Lemma 5.3.1 that

$$|v_{5-T_{\mathcal{F},\mathcal{G}}(i,j)}|^{-1} \ll |w_{6-i}|^{-1} |w_{6-j}|^{-1} \Delta^{1/2}.$$

Multiplying out the inverses, we obtain

$$|w_{6-i}| |w_{6-j}| \ll |v_{5-T_{\mathcal{F},\mathcal{G}}(i,j)}| \Delta^{1/2}.$$

So, $\text{Poly}_5(G)$ is contained in the set $\bigcup_{(\mathcal{F},\mathcal{G})} P_{\mathcal{F},\mathcal{G}}$ where $(\mathcal{F},\mathcal{G})$ ranges across flags of (K,L) with the property that $\text{Gal}(K) \simeq G$.

Now let $(\mathcal{F},\mathcal{G})$ be a flag of a pair (K,L) with the property that $\text{Gal}(K) \simeq G$. Choose bases $\{v_0 = 1, v_1, \dots, v_4\}$ and $\{w_0 = 1, w_1, \dots, w_5\}$ of K and L giving rise to bases $\{v_4^*, \dots, v_1^*\}$ and $\{w_5^*, \dots, w_1^*\}$ of K_0 and L_0 . These bases give rise to a flag $(\mathcal{F},\mathcal{G})$ of (K,L) . Moreover, the dual bases give rise to a tensor $\mathcal{A} \in V_{\mathbb{R}}$. For a positive integer M , define $g_M \in \text{GL}_4(\mathbb{R}) \times \text{GL}_5(\mathbb{R})$ to be

$$g_M = \left(\begin{bmatrix} M^{p_4} & 0 & 0 & 0 \\ 0 & M^{p_3} & 0 & 0 \\ 0 & 0 & M^{p_2} & 0 \\ 0 & 0 & 0 & M^{p_1} \end{bmatrix}, \begin{bmatrix} M^{-q_5} & 0 & 0 & 0 & 0 \\ 0 & M^{-q_4} & 0 & 0 & 0 \\ 0 & 0 & M^{-q_3} & 0 & 0 \\ 0 & 0 & 0 & M^{-q_2} & 0 \\ 0 & 0 & 0 & 0 & M^{-q_1} \end{bmatrix} \right)$$

Define $\mathcal{A}_M = \sqrt{M} g_M \mathcal{A}$. For a rational point p in the relative interior of $P_{\mathcal{F},\mathcal{G}}$, one may check that there exists an infinite set $\mathcal{M} \subseteq \mathbb{Z}_{>0}$ such that for all $M \in \mathcal{M}$ the tensor $\mathcal{A}_M \in V_{\mathbb{Z}}$. Each $M \in \mathcal{M}$ gives rise to a distinct quintic ring and sextic resolvent ring (R_M, S_M) with absolute discriminant Δ_M ; for each $M \in \mathcal{M}$, write the bases of R_M and S_M obtained from $\mathcal{A}_M$ by $\{1, v_{1,M}, \dots, v_{4,M}\}$

and $\{1, w_{1,M}, \dots, w_{5,M}\}$ respectively. Then for $M, N \in \mathcal{M}$, we have:

$$\begin{aligned} N\Delta_M &= M\Delta_N \\ N^{p_i}v_{i,M} &= M^{p_i}v_{i,N} \\ N^{q_i}w_{i,M} &= M^{q_i}w_{i,N} \end{aligned}$$

Therefore,

$$\begin{aligned} \lim_{M \in \mathcal{M}} \left(\log_{\Delta_M} \lambda_1(R_M), \dots, \log_{\Delta_M} \lambda_4(R_M) \right) &= (p_1, p_2, p_3, p_4) \\ \lim_{M \in \mathcal{M}} \left(\log_{\Delta_M} \lambda_1(S_M), \dots, \log_{\Delta_M} \lambda_5(S_M) \right) &= (q_1, q_2, q_3, q_4, q_5) \end{aligned}$$

Therefore, $p \in \text{Poly}_5(G)$. Because $\text{Poly}_5(G)$ is defined to be a set of limit points, it must be closed; therefore $P_{\mathcal{F}, \mathcal{G}}$ is contained in $\text{Poly}_5(G)$, which completes the proof of the theorem. $\square$

Proof of Theorem 5.1.1. Theorem 5.4.2 expresses $\text{Poly}_5(G)$ as a finite union of polytopes. A computation shows that these polytopes have dimension 7. $\square$

To compute $\text{Poly}_5(S_5)$, we will need the following lemma.

Lemma 5.4.3 (Bhargava [8], Lemma 10). *Let $\mathcal{A} \in V_{\mathbb{Q}}$ be an element such that all the variables in one of the following sets vanish:*

1. $\{a_{12}^4, a_{13}^4, a_{14}^4, a_{15}^4, a_{23}^4, a_{24}^4, a_{25}^4\}$
2. $\{a_{12}^4, a_{13}^4, a_{14}^4, a_{23}^4, a_{24}^4, a_{34}^4\}$
3. $\{a_{12}^4, a_{13}^4, a_{14}^4, a_{15}^4\} \cup \{a_{12}^3, a_{13}^3, a_{14}^3, a_{15}^3\}$
4. $\{a_{12}^4, a_{13}^4, a_{14}^4, a_{23}^4, a_{24}^4\} \cup \{a_{12}^3, a_{13}^3, a_{14}^3, a_{23}^3, a_{24}^3\}$
5. $\{a_{12}^4, a_{13}^4, a_{14}^4\} \cup \{a_{12}^3, a_{13}^3, a_{14}^3\} \cup \{a_{12}^2, a_{13}^2, a_{14}^2\}$
6. $\{a_{12}^4, a_{13}^4, a_{23}^4\} \cup \{a_{12}^3, a_{13}^3, a_{23}^3\} \cup \{a_{12}^2, a_{13}^2, a_{23}^2\}$
7. $\{a_{12}^4, a_{13}^4\} \cup \{a_{12}^3, a_{13}^3\} \cup \{a_{12}^2, a_{13}^2\} \cup \{a_{12}^1, a_{13}^1\}$

Then $\mathcal{A}$ is reducible.

Proof of Theorem 5.1.2. Let $(\mathcal{F}, \mathcal{G})$ be any flag of a pair (K, L) such that $\text{Gal}(K)$ is a transitive subgroup of S_5 . Then the seven statements of Lemma 5.4.3 imply that:

1. $T_{\mathcal{F},\mathcal{G}}(2,5) = 4$
2. $T_{\mathcal{F},\mathcal{G}}(3,4) = 4$
3. $T_{\mathcal{F},\mathcal{G}}(1,5) \geq 3$
4. $T_{\mathcal{F},\mathcal{G}}(2,4) \geq 3$
5. $T_{\mathcal{F},\mathcal{G}}(1,4) \geq 2$
6. $T_{\mathcal{F},\mathcal{G}}(2,3) \geq 2$
7. $T_{\mathcal{F},\mathcal{G}}(1,3) \geq 1$

The 7 statements above imply that $P_{\mathcal{F},\mathcal{G}}$ satisfies the linear inequalities:

1. $p_1 + 1/2 \geq q_4 + q_1$
2. $p_1 + 1/2 \geq q_3 + q_2$
3. $p_2 + 1/2 \geq q_5 + q_1$
4. $p_2 + 1/2 \geq q_4 + q_2$
5. $p_3 + 1/2 \geq q_5 + q_2$
6. $p_3 + 1/2 \geq q_4 + q_3$
7. $p_4 + 1/2 \geq q_5 + q_3$

In total, this proves that $\text{Poly}_5(\text{Gal}(K))$ is contained in the region stated in the theorem statement.

The converse is shown via computer calculation by producing an example of $\mathcal{A} = (A_1, A_2, A_3, A_4) \in V_{\mathbb{Q}}$ of the form

$$\left(\begin{bmatrix} - & 0 & * & * & * \\ - & - & * & * & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & * & * \\ - & - & * & * & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & 0 & * \\ - & - & 0 & * & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & 0 & 0 \\ - & - & 0 & 0 & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix} \right)$$

defining an S_5 -quintic field. □

5.5 Computing density functions of quintic rings

To make our formulas shorter, we use the following notation in this section. Define:

$$f(p) := 1 + \sum_{1 \leq i < j \leq 5, 1 \leq k \leq 4} \max\{0, -1/2 + q_i + q_j - p_k\}$$

$$g(p) := \sum_{1 \leq i < j \leq 4} (p_j - p_i) + \sum_{1 \leq i < j \leq 5} (q_j - q_i)$$

Lemma 5.5.1. *For any C, X and $p \in \mathbb{R}^5$ satisfying (5.1), we have*

$$\{V_{\mathbb{Z}} \cap CB(p, X)\} \asymp_C \exp[X, f(p)].$$

Proof. The argument is identical to that of Lemma 4.5.1. □

Lemma 5.5.2. *For any ϵ, X , and $p \in \text{Poly}_5$, we have*

$$\#\mathcal{F}_5(p, \epsilon, X) \ll_{\epsilon} \exp[X, f(p) - g(p)].$$

Proof. The proof is again completely identical to that of Lemma 4.5.2. □

Lemma 5.5.3. *There is a constant C such that for all $\epsilon > C$ we have:*

1. *if $p \in \text{Poly}_5$, then*

$$\#\mathcal{F}_4(p, \epsilon, X) \gg_{p, \epsilon} \exp[X, f(p) - g(p)];$$

2. *if $p \in \text{Poly}_5(S_5)$, then*

$$\#\mathcal{F}(p, \epsilon, S_5, X) \gg_{p, \epsilon} \exp[X, f(p) - g(p)];$$

Proof. The proof of (1) is completely analogous to that of (1) in Lemma 4.5.3. The argument in Lemma 4.5.3 also proves (2), with the additional input that there exists $D, M \in \mathbb{R}_{\geq 1}$ such that a positive proportion, as $X \rightarrow \infty$, of the lattice points in $DB(p, X) \cap V_{\mathbb{Z}}$ have Galois group S_5 and $\Delta \geq X/M$; it suffices to drop the latter condition and simply prove that there exists $D \in \mathbb{R}_{\geq 1}$ such that a positive proportion of the lattice points in $DB(p, X) \cap V_{\mathbb{Z}}$ have Galois group S_5 as $X \rightarrow \infty$. Consider the subset of lattice points of $DB(p, X)$ such that $\Delta \equiv 5 \pmod{25}$, the ring R is irreducible

modulo 7, and the ring S is irreducible modulo 11; every element of this subset has Galois group S_5 . If this set is nonempty for large enough X , then it forms a positive proportion of $DB(p, X)$. The nonemptiness follows from the fact that there exists $\mathcal{A}$ of the form

$$\left(\begin{bmatrix} - & 0 & * & * & * \\ - & - & * & * & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & * & * \\ - & - & * & * & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & 0 & * \\ - & - & 0 & * & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & 0 & 0 \\ - & - & 0 & 0 & * \\ - & - & - & * & * \\ - & - & - & - & * \\ - & - & - & - & - \end{bmatrix} \right)$$

such that $\Delta = 5 \pmod{25}$, the ring R is irreducible modulo 7, and the ring S is irreducible modulo 11. Choosing D to be large enough such that $\mathcal{A} \in DB(p, X)$ completes the proof of this case. $\square$

Proof of Theorem 1.4.1. This follows from Lemma 5.5.3 and Lemma 5.5.2. $\square$

Proof of Theorem 1.4.2. This follows from Lemma 5.5.3 and Lemma 5.5.2. $\square$

5.6 Special families of quintic rings

5.6.1 Binary quintic forms

Let $f(x, y) = f_0x^5 + f_1x^4y + f_2x^3y^2 + f_3x^2y^3 + f_4xy^4 + f_5y^5 \in \text{Sym}^5 \mathbb{Z}^2$ be a binary quintic form. In [21], Fess defines a map $\text{Sym}^5 \mathbb{Z}^2 \rightarrow \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$; we modify this map slightly and send a form f to the matrices²:

$$\begin{bmatrix} - & 0 & 0 & 0 & 0 \\ - & - & -1 & 0 & 0 \\ - & - & - & 0 & 0 \\ - & - & - & - & -f_5 \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 1 & 0 & 0 \\ - & - & 0 & 1 & 0 \\ - & - & - & 0 & -f_3 \\ - & - & - & - & -f_4 \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & -1 & 0 \\ - & - & 0 & 0 & -1 \\ - & - & - & -f_1 & -f_2 \\ - & - & - & - & 0 \\ - & - & - & - & - \end{bmatrix}, \begin{bmatrix} - & 0 & 0 & 0 & 1 \\ - & - & 0 & 0 & 0 \\ - & - & - & -f_0 & 0 \\ - & - & - & - & 0 \\ - & - & - & - & - \end{bmatrix}$$

Let $p = (1/8, 1/8, 1/8, 1/8, 1/4, 1/4, 1/4, 3/8, 3/8)$. Call the map above ψ . Observe that for any form $f \in \text{Sym}^5 \mathbb{Z}^2$, we have $H_c(f) \leq X^{1/8}$ if and only if $\psi(f) \in B(p, X)$.

Proof of Theorem 5.1.5. The proof is almost identical to that of Theorem 4.1.7. Let $C \in \mathbb{R}_{\geq 1}$.

Let $f \in \mathcal{F}_5^{\text{bin}}$ and let (R, S) be the corresponding rings. By Lemma 5.3.7, if $\Delta \geq X/C$ and

²Our map and the map of Fess send a form f to isomorphic quintic rings and sextic resolvent rings. The only difference is a choice of basis of the quintic ring and sextic resolvent ring.

$\psi(f) \in B(p, X)$, then

$$\lambda_i(R) \asymp_C \Delta^{p_i}$$

$$\lambda_i(S) \asymp_C \Delta^{q_i}.$$

To prove (5.6), it suffices to show that

$$\lim_{C \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F}_5^{\text{bin}} \mid H_c(f) \leq X \text{ and } \Delta \geq X^8/C\}}{\#\{f \in \mathcal{F}_5^{\text{bin}} \mid H_c(f) \leq X\}} = 1.$$

The denominator is clearly $X^6 + o(X^6)$. By Davenport's lemma, we have:

$$\begin{aligned} & \#\{f \in \mathcal{F}_5^{\text{bin}} \mid H_c(f) \leq X \text{ and } \Delta > X^8/C\} \\ &= \#\{(f_0, \dots, f_5) \in \mathbb{Z}^6 \mid \max\{|f_i|\} \leq X \text{ and } |\text{disc}(f_0, \dots, f_5)| > X^8/C\} \\ &= \text{Vol}\{(f_0, \dots, f_5) \in \mathbb{R}^6 \mid \max\{|f_i|\} \leq X \text{ and } |\text{disc}(f_0, \dots, f_5)| > X^8/C\} + O(X^5) \\ &= X^6 \text{Vol}\{(f_0, \dots, f_5) \in \mathbb{R}^5 \mid \max\{|f_i|\} \leq 1 \text{ and } |\text{disc}(f_0, \dots, f_5)| > 1/C\} + O(X^5) \end{aligned}$$

We now prove (5.7). Observe that by Lemma 5.5.2, there exists a constant C such that for all $\epsilon > C$, there are $\ll_\epsilon X^{3/4}$ isomorphism classes of tuples (R, S) such that $\Delta \leq X$ and (R, S) is (ϵ, X) -close to p . Theorem 3.5.8 shows that there are at most $O(1)$ $\text{GL}_2(\mathbb{Z})$ -equivalence classes of binary quintic forms giving rise to the same quintic ring. Therefore, it suffices to show that there are $\gg X^{3/4}$ $\text{GL}_2(\mathbb{Z})$ -equivalence classes of binary quintics such that $\Delta \leq X$ and the corresponding rings (R, S) are (ϵ, X) -close to p ; this follows from Theorem 1.2.4 when $r = (1/40, 1/40)$. $\square$

5.6.2 Monic quintic forms

Let $\mathcal{F}_5^{\text{mon}}$ denote the set of monic quintic forms with integral coefficients and nonzero discriminant. Let

$$p = (1/20, 2/20, 3/20, 4/20, 4/20, 5/20, 6/20, 7/20, 8/20).$$

Observe that for any monic integral quintic form f , we have $H_r(f) \leq X^{1/20}$ if and only if $\psi(f) \in B(p, X)$.

Proof of Theorem 5.1.7. Again, the proof is almost identical to that of Theorem 4.1.6. Let $C \in \mathbb{R}_{\geq 1}$. For any $f \in \mathcal{F}_5^{\text{mon}}$ let (R, S) be the corresponding rings. By Lemma 5.3.7, if $\Delta \geq X/C$ and

$\psi(f) \in B(p, X)$, then

$$\lambda_i(R) \asymp_C \Delta^{p_i}$$

$$\lambda_i(S) \asymp_C \Delta^{q_i}.$$

To prove (5.6), it suffices to show that

$$\lim_{C \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{f \in \mathcal{F}_5^{\text{mon}} \mid H_r(f) \leq X \text{ and } \Delta \geq X^{20}/C\}}{\#\{f \in \mathcal{F}_5^{\text{mon}} \mid H_r(f) \leq X\}} = 1.$$

The denominator is clearly $X^{15} + o(X^{15})$. By Davenport's lemma, we have:

$$\begin{aligned} & \#\{f \in \mathcal{F}_5^{\text{mon}} \mid H_r(f) \leq X \text{ and } \Delta > X^{20}/C\} \\ &= \#\{(f_1, \dots, f_5) \in \mathbb{Z}^5 \mid \max\{|f_i|^{1/i}\} \leq X \text{ and } |\text{disc}(1, f_1, \dots, f_5)| > X^{20}/C\} \\ &= \text{Vol}\{(f_1, \dots, f_5) \in \mathbb{R}^5 \mid \max\{|f_i|^{1/i}\} \leq X \text{ and } |\text{disc}(1, f_1, \dots, f_5)| > X^{20}/C\} + O(X^{14}) \\ &= X^{15} \text{Vol}\{(f_1, \dots, f_5) \in \mathbb{R}^5 \mid \max\{|f_i|\} \leq 1 \text{ and } |\text{disc}(1, f_1, \dots, f_5)| > 1/C\} + O(X^{14}) \end{aligned}$$

We now prove (5.7). Observe that by Lemma 5.5.2, there exists a constant M such that for all $\epsilon > M$, there are $\ll_\epsilon X^{7/10}$ isomorphism classes of tuples (R, S) such that $\Delta \leq X$ and (R, S) is (ϵ, X) -close to p . Theorem 3.5.8 shows that there are at most $O(1)$ $\text{GL}_2(\mathbb{Z})$ -equivalence classes of binary quintic forms giving rise to the same quintic ring. Therefore, it suffices to show that there are $\gg X^{7/10}$ $\text{GL}_2(\mathbb{Z})$ -equivalence classes of binary quintics such that $\Delta \leq X$, the binary quintic represents 1, and the corresponding rings (R, S) are (ϵ, X) -close to p ; this follows from Theorem 1.2.4 when we let $r = (0, 1/20)$. $\square$

5.6.3 The generic point of S_5

We now prove Corollary 5.1.4 by appealing to upcoming work of H. Given a nondegenerate rank n ring R , we consider the rank $(n-1)$ lattice $\{x \in \mathbb{Z} + nR \mid \text{Tr}(x) = 0\}$, up to isometry. It is naturally seen as an element of the double coset space

$$\mathcal{S}_{n-1} := \text{GL}_{n-1}(\mathbb{Z}) \backslash \text{GL}_{n-1}(\mathbb{R}) / \text{GO}_{n-1}(\mathbb{R}).$$

The space $\mathcal{S}_{n-1}$ has a natural measure μ_{n-1} , obtained from the Haar measure on $\text{GL}_{n-1}(\mathbb{R})$ and $\text{GO}_{n-1}(\mathbb{R})$. To a nondegenerate pair (R, S) , we can associate an element $(\mathcal{L}_R, \mathcal{L}_S) \in \mathcal{S}_4 \times \mathcal{S}_5$; we

call this the *shape* of the pair (R, S) .

Theorem 5.6.1 (H). *When ordered by discriminant, the shapes of pairs (R, S) , where R is an S_5 -ring, are equidistributed with respect to $\mu_4 \times \mu_5$.*

Proof of Corollary 5.1.4. Let $p(S_5) = (1/8, 1/8, 1/8, 1/8, 3/10, 3/10, 3/10, 3/10, 3/10)$. We will first prove (5.6). For an integer $n \geq 2$, an element $\mathcal{L} \in \mathcal{S}_n$, and an integer $0 \leq i < n$, define $\lambda_i(\mathcal{L})$ to be the i -th successive minimum of a lattice representing $\mathcal{L}$ with determinant 1. For a positive real number ϵ and an integer $n \geq 2$, define

$$\mathcal{S}_{n,\epsilon} := \{\mathcal{L} \in \mathcal{S}_n \mid \max_{1 \leq i \leq n} \{\log \lambda_i(\mathcal{L})\} \leq \epsilon\}.$$

Then:

$$\begin{aligned} & \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{(R, S) \mid \Delta \leq X \text{ and } R \text{ is a } S_5\text{-ring that is } (\epsilon, X)\text{-close to } p(S_5)\}}{\#\{(R, S) \mid \Delta \leq X \text{ and } R \text{ is a } S_5\text{-ring}\}} \\ & \geq \lim_{\epsilon \rightarrow \infty} \liminf_{X \rightarrow \infty} \frac{\#\{(R, S) \mid \Delta \leq X \text{ and } R \text{ is a } S_5\text{-ring and } (\mathcal{L}_R, \mathcal{L}_S) \in \mathcal{S}_{4,\epsilon} \times \mathcal{S}_{5,\epsilon}\}}{\#\{(R, S) \mid \Delta \leq X \text{ and } R \text{ is a } S_5\text{-ring}\}} \\ & = \lim_{\epsilon \rightarrow \infty} \frac{(\mu_4 \times \mu_5)(\mathcal{S}_{4,\epsilon} \times \mathcal{S}_{5,\epsilon})}{(\mu_4 \times \mu_5)(\mathcal{S}_4 \times \mathcal{S}_5)} \\ & = 1 \end{aligned}$$

We prove (5.6) with the following observation: Lemma 5.5.2 and Lemma 5.5.3 combine to prove that there exists a positive real number C such that for all $\epsilon > C$, a positive proportion of rings in $\mathcal{F}(p(S_5), \epsilon, X)$ as $X \rightarrow \infty$ are S_5 -rings. $\square$

Chapter 6

Appendix

We will need the following lemma on directed graphs.

Lemma 6.0.1. *Let G be any directed graph on ≥ 2 vertices. If every vertex of G has an outgoing edge, then G has a cycle.*

Proof. Start at a vertex and travel along an outgoing edge to another vertex. Continuing this way, because the graph has finitely many vertices, we will eventually return to a vertex that we have been at previously. Thus the graph contains a cycle. $\square$

Lemma 6.0.2. *Let $n \in \mathbb{Z}_{\geq 1}$, let $a_1, \dots, a_n, C$ be any positive real numbers, let $X \in \mathbb{R}_{\geq 1}$, and let $p = (p_1, \dots, p_n) \in \mathbb{R}^n$. If*

$$a_i^2 \leq C \max_{1 \leq j \leq n} \{X^{2p_i - p_j} a_j\} \quad (6.1)$$

for all $1 \leq i \leq n$, then $a_i \leq CX^{p_i}$ for all $1 \leq i \leq n$.

Proof. We proceed by induction on n . If $n = 1$ then $a_1^2 \leq CX^{p_1} a_1$ so $a_1 \leq CX^{p_1}$.

Now fix $n \geq 2$ and suppose the lemma is true for all $1 \leq m < n$. Let

$$S = \{1 \leq i \leq n \mid a_i \leq CX^{p_i}\}.$$

Assume for the sake of contradiction that $S = \emptyset$; equivalently, assume that

$$a_i > CX^{p_i} \quad (6.2)$$

for all $1 \leq i \leq n$. Define the directed graph G on the set of vertices $\{1, 2, \dots, n\}$ as follows: draw

an edge from i to j if

$$a_i^2 \leq CX^{2p_i - p_j} a_j. \quad (6.3)$$

(6.1) and (6.2) together imply that every vertex of G has an outgoing edge. Lemma 6.0.1 implies that G contains a cycle; choose any cycle of G and let T denote the set of vertices of that cycle. Multiplying (6.3) together for every edge in the cycle and dividing both sides by $\prod_{i \in T} a_i$, we obtain

$$\prod_{i \in T} a_i \leq C^{\#T} \prod_{i \in T} X^{p_i}.$$

However, (6.2) implies that

$$C^{\#T} \prod_{i \in T} X^{p_i} < \prod_{i \in T} a_i,$$

and hence we have arrived at a contradiction. Thus, $S \neq \emptyset$.

For all $i \notin S$ and for all $j \in S$, we have

$$\begin{aligned} a_i^2 &> C^2 X^{2p_i} && \text{because } i \notin S \\ &\geq CX^{2p_i - p_j} a_j. && \text{because } j \in S \end{aligned}$$

Therefore for all $i \notin S$, we may rewrite (6.1) as

$$a_i^2 \leq C \max_{k \notin S} \{X^{2p_i - p_k} a_k\}.$$

Because $S \neq \emptyset$ the induction assumption implies that $a_i \leq CX^{p_i}$ for all $i \notin S$.

□

Bibliography

- [1] C. Bachoc, O. Serra, and G. Zémor, *Revisiting Kneser’s theorem for field extensions*, *Combinatorica* **38** (2018), no. 4, 759–777.
- [2] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, *Annals of Mathematics* **159** (2004), 1329–1360.
- [3] ———, *Higher composition laws IV: The parametrization of quintic rings*, *Annals of Mathematics* **167** (2008), 53–94.
- [4] ———, *On the number of monogenizations of a quartic order* (2022). preprint, <https://arxiv.org/abs/2111.04215>.
- [5] M. Bhargava and P. H., *The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields*, *Compositio Mathematica* **152** (2016), 1111–1120.
- [6] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, *Journal of the American Mathematical Society* **33** (2020), 1087–1099.
- [7] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport–Heilbronn theorems and second order terms*, *Inventiones mathematicae* **193** (2013), 439–499.
- [8] M. Bhargava, *The Density of Discriminants of Quintic Rings and Fields*, *Annals of Mathematics* **172** (2010), no. 3, 1559–1591.
- [9] B.J. Birch and J.R. Merriman, *Finiteness theorems for binary forms with given discriminant*, *Proceedings of the London Mathematical Society* **24** (1971), 385–394.
- [10] G. Casnati and T. Ekedahl, *Covers of algebraic varieties I. A general structure theorem, covers of degree 3, 4 and Enriques’ surfaces*, *Journal of Algebraic Geometry* **5** (1996), no. 3, 439–460.
- [11] G. Casnati, *Covers of algebraic varieties II. Covers of degree 5 and constructions of surfaces*, *Journal of Algebraic Geometry* **5** (1996), 461–477.
- [12] ———, *Covers of algebraic varieties III. The discriminant of a cover of degree 4 and the trigonal construction*, *Transactions of the American Mathematical Society* **350** (1998), no. 4, 1359–1378.
- [13] W. Castryck, G. Vermeulen, and Y. Zhao, *Scrollar invariants, syzygies and representations of the symmetric group*, *Journal für die reine und angewandte Mathematik (Crelles Journal)* **796** (2023), 117–159.
- [14] V. Chiche-lapierre, *Length of elements in a Minkowski basis for an order in a number field*, University of Toronto, 2019. thesis, http://blog.math.toronto.edu/GraduateBlog/files/2019/06/val_chichelapierre_thesis.pdf.

- [15] S. D. Cohen, *The Distribution of Galois Groups and Hilbert's Irreducibility Theorem*, Proceedings of the London Mathematical Society **s3-43** (1981), no. 2, 227–250.
- [16] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Enumerating quartic dihedral extensions of $\mathbb{Q}$* , Compositio Mathematica **133** (2002), 65–93.
- [17] H. Davenport, *On a principle of Lipschitz*, Journal of the London Mathematical Society **26** (1951), 179–183.
- [18] B. N. Delone and D.K. Faddeev, *The theory of irrationalities of the third degree*, Vol. 10, Translations of Mathematical Monographs, 1964.
- [19] A. Deopurkar and A. Patel, *The Picard rank conjecture for the Hurwitz spaces of degree up to five*, Algebra & Number Theory **9** (2015), no. 2, 459 – 492.
- [20] J.H. Evertse and K. Györy, *Discriminant Equations in Diophantine Number Theory*, Cambridge University Press, 2016.
- [21] D. Fess, *Binary Forms, Quintic Rings and Sextic Resolvents*, Princeton University, 2022. thesis, <http://arks.princeton.edu/ark:/88435/dsp01xd07gw83d>.
- [22] F. Hess, *Computing Riemann–Roch Spaces in Algebraic Function Fields and Related Topics*, Journal of Symbolic Computation **33** (2002), 425–445.
- [23] M. Hindry and J. Silverman, *Diophantine Geometry*, Springer, 2000.
- [24] E. Holmes, *On the shapes of pure prime degree number fields* (2022). preprint, <https://arxiv.org/abs/2209.10638>.
- [25] A. Maroni, *Le serie lineari speciali sulle curve trigonali*, Annali di Matematica Pura ed Applicata **25** (1946), no. 1, 341–354.
- [26] J. Nakagawa, *Binary forms and orders of algebraic number fields*, Inventiones Math **2** (1989), 219–234.
- [27] A. Ohbuchi, *On some numerical relations of d -gonal linear systems*, Journal of Math, Tokushima University **31** (1997), 7–10.
- [28] A. Patel, *The geometry of the Hurwitz space*, Harvard University, 2013. preprint, https://dash.harvard.edu/bitstream/handle/1/11124835/Patel_gsas.harvard_0084L_10901.pdf.
- [29] C. Peikert and A. Rosen, *Lattices that Admit Logarithmic Worst-Case to Average-Case Connection Factors*, Proceedings of the thirty-ninth annual ACM symposium on theory of computing, 2007, pp. 478–487.
- [30] S. Recillas, *Jacobians of curves with a g_4^1 are Prym varieties of trigonal curves*, Boletín de la Sociedad Matemática Mexicana (1974), 9–13.
- [31] C. L. Siegel, *Lectures on the Geometry of Numbers*, Springer-Verlag, 1989.
- [32] D. Terr, *The distribution of shapes of cubic orders*, University of California, Berkeley, 1997. thesis, <https://www.proquest.com/docview/304343539>.
- [33] M. M. Wood, *Quartic Rings Associated to Binary Quartic Forms*, International Mathematics Research Notices **2012** (2011), no. 6, 1300–1320.
- [34] Y. Zhao, *On sieve methods for varieties over finite fields*, University of Wisconsin, Madison, 2013. thesis, <https://www.proquest.com/docview/1440406524>.