

**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

2013

Three perspectives on n points in P^{n-2}

Wilson, Kevin Hayes

Princeton, NJ : Princeton University

<http://arks.princeton.edu/ark:/88435/dsp018k71nh131>

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>

THREE PERSPECTIVES ON n POINTS IN $\mathbb{P}^{n-2}$

KEVIN H. WILSON

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

JANUARY 2013

© Copyright by Kevin H. Wilson, 2012.

All Rights Reserved

Abstract

This thesis is divided into three parts, each focused on extending the work of Bhargava's Higher Composition Laws [9, 10, 11, 14] and his asymptotics of the density of discriminants [12, 15].

The first part is focused on the geometry of numbers methods of [12, 15]. In this part, we prove asymptotics for the class number times the regulator of cubic fields and orders, and for the square of the same for quadratic fields and orders. This requires extending Bhargava's methods to prehomogeneous vector spaces with a positive-dimensional generic isotropy group.

The second part focuses on more traditional analytic methods. In it, we demonstrate that the values $L(1, k)$ for k an S_3 -cubic or S_4 -quartic number field behave like random Euler products, extending work of Barban and Elliott from the quadratic case. More generally, we show that the same holds if k is replaced by an order in such a field. Conditional on the Strong Artin Conjecture for Galois representations $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_{n-1}(\mathbb{C})$ with image S_n and what we call the Strong Malle Conjecture for S_n number fields, we prove that $L(1, k)$ behaves like a random Euler product for k an S_n number field for any $n \geq 2$.

In the final part, we turn to putting Bhargava's Higher Composition Laws in a more commutative algebraic context. In particular, taking inspiration from a letter of Deligne to Bhargava and Wood's thesis, we produce a canonical associative, commutative, differential graded algebra structures on the minimal free resolutions of n general points in $\mathbb{P}_{\mathbb{Q}}^{n-2}$. We believe our method is novel, relying on the representation theory of the symmetric group. In our penultimate chapter, we show that this method extends to produce canonical multiplicative structures on other free resolutions associated to the representation theory of the symmetric group. Of particular interest is that all of the resolutions we produce are pure and do not appear to arise from the so-called tensor complexes of Berkesch, Erman, Kummini, and Sam.

Finally, in the last chapter, we briefly discuss the representation theoretic import of the sextic resolvent of a quintic field. At this time, we have not been able to use this to extend Bhargava's parameterization of quintic rings to arbitrary base schemes in the spirit of Deligne and Wood, but we believe that this chapter forms an important start in that direction.

Acknowledgements

I would like to take this opportunity to thank everyone I have had the opportunity to converse with over the course of my graduate studies. In particular, I would like to thank my adviser, M. Bhargava, whose work provided the vast majority of the inspiration for this thesis. Top of the list of others to thank is A. Shankar with whom I spent innumerable hours daydreaming of math and other things, and R. Peckner who spent far too many hours listening to me wax poetic about commutative algebra.

I must thank among faculty members D. Eisenbud, N. Elkies, N. Katz, J. Kollàr, P. Sarnak, T. Taniguchi, and F. Thorne for some particularly useful conversations. Among graduate students, S.A. Altug, O. Biesel, Y. Cooper, D. Erman, W. Ho, B. Hough, K.J. Hughes, S. Ruth, G. Saccà, V.V. Shende, J. Tsimerman, I. Varma, and M.M. Wood played particularly important roles in my graduate school career.

And, of course, I cannot forget my loving family and friends, who provided me with support, encouragement, and decorating advice along the way.

Contents

Abstract	iii
Acknowledgements	v
1 Introduction	1
1.1 Introduction	1
1.2 Notation	2
1.2.1 (Graded) Rings	2
1.2.2 The Vocabulary of Commutative Algebra	3
1.3 Free Resolutions and Extra Structure	5
1.3.1 Projective Resolutions	9
1.3.2 Why Projective Resolutions: Derived Functors	10
1.3.3 Minimal Free Resolutions	10
1.3.4 A Brief Interlude: The Koszul Complex	12
1.3.5 The Finiteness of Minimal Free Resolutions	12
1.3.6 Injective Modules and Resolutions and the Gorenstein Condition . . .	13
1.3.7 Differential Graded Algebras	15
1.4 The Inspiring Geometry: Varieties of (Almost) Minimal Degree	16
1.4.1 Minimal Degree	17
1.4.2 Almost Minimal Degree	19
1.5 Siegel's Theorem	21

1.6	Some Future Work	23
I	Geometry of Numbers	24
2	Asymptotics of the Class Number Times the Regulator of Cubic Fields and Orders	25
2.1	Introduction	25
2.2	Ideal Classes in Nonmaximal Orders	30
2.2.1	An overview of commutative monoids	30
2.2.2	Invertible Ideals	31
2.2.3	Noninvertible ideals	33
2.2.4	Weak Inverses and Regulators	35
2.3	Some Facts about Regulators	36
2.3.1	Dedekind zeta functions and Artin L functions	37
2.3.2	The Strong Artin Conjecture	38
2.3.3	Zeta functions of nonmaximal orders	39
2.4	The density of discriminants	41
2.5	Binary cubic forms and cubic rings	45
2.5.1	The Delone-Fadeev Correspondence	46
2.5.2	The Davenport-Heilbronn Correspondence	48
2.6	The Hilbert-Burch Theorem and Ideals in Cubic Rings	48
2.6.1	Bhargava's Boxes	49
2.6.2	Over Arbitrary PIDs	52
2.6.3	Stabilizers and Weights	53
2.7	Local Densities for Invertible and Proper Ideals	54
2.7.1	A Mass Formula	55
2.7.2	Maximal Rings	56

2.7.3	Invertible Ideals	57
2.7.4	Proper Ideals	58
2.8	A Geometry of Numbers Argument	61
2.8.1	Reduction Theory	61
2.8.2	An Averaging Argument	62
2.8.3	A Lemma from the Geometry of Numbers	66
2.8.4	A More General Regulator	66
2.8.5	The main term	67
2.8.6	Congruence Conditions	68
2.8.7	Controlling the Error: Proofs of Lemmas 82 and 83	69
2.9	A Sieve and the Proof of Theorem 40	74
2.9.1	The imprimitive and improper cases	77
2.9.2	Invertible ideals in nonmaximal rings	79
2.A	Appendix: Comment on Conjecture 65	84
3	Asymptotics of the Square of the Class Number Times the Regulator of Quadratic Fields and Orders	88
3.1	Introduction	88
3.2	Points in Products of Projective Spaces	90
3.3	Gauss–Bhargava Composition	92
3.4	Some remarks on invertibility	95
3.5	Local Densities for Maximal Rings and Invertible Ideals	96
3.5.1	A Mass Formula	97
3.5.2	Maximal Rings	98
3.5.3	Invertible Ideals	99
3.6	A Geometry of Numbers Argument	100
3.6.1	Reduction Theory	101

3.6.2	An Averaging Argument	102
3.6.3	A Lemma from the Geometry of Numbers	103
3.6.4	A More General Regulator	104
3.6.5	The main term	105
3.6.6	Congruence Conditions	106
3.6.7	Controlling the Error: Proofs of Lemmas 113 and 114	107
3.7	A Sieve and the Proof of the Main Theorem	108
3.7.1	The error from nonmaximal orders	109
3.7.2	Proof of the Main Theorem	109

II Analytic Number Theory 111

4	$L(1, k)$ Behaves Like a Random Euler Product 112
4.1	Introduction 112
4.2	A false—but instructive—proof 116
4.2.1	From Special Values to Class Number and Regulator 116
4.2.2	The False Proof 117
4.2.3	The Constants 119
4.2.4	Invertible Ideals 121
4.2.5	Higher Moments 122
4.2.6	Double Checking 125
4.3	An Actual Proof 125
4.3.1	The main term 128
4.3.2	The Error Term 130
4.3.3	Invertible Ideals and Congruence Conditions 135
4.3.4	Stepping Back 137
4.4	From moments to a distribution 137

4.5	Future Work	138
III	Commutative Algebra and the Symmetric Group	140
5	Multiplicative Structures on the Free Resoulution of n Points in $\mathbb{P}^{n-2}$	141
5.1	Introduction	141
5.2	An S_n -equivariant resolution of X	146
5.3	An ACDGA structure for the Resolution of X	165
5.4	A Remark on Canonicity and Smaller Fields	173
5.5	A Remark on Integrality	176
6	Free Resolutions and Multiplicative Structures Thereon Attached to Two-Rowed Specht Ideals	180
6.1	Introduction	180
6.2	Notation	185
6.2.1	The Representation Theory of the Symmetric Group	185
6.2.2	Some Commutative Algebra	188
6.3	Two-rowed Specht Ideals are Cohen-Macaulay	190
6.4	Purity of the resolution	192
6.4.1	Some Combinatorics	193
6.4.2	Some Equivariant Maps: The $(c - 1)$ Strand	196
6.4.3	Some More Equivariant Maps: The c Strand	199
6.5	A Multiplicative Structure	200
6.6	Conclusions and Future Work	203
7	Sextic Resolvents of Quintic Fields and the Representation Theory of S_5	205
7.1	Introduction	205
7.2	The Representation Theory of S_5 and S_6	207

7.2.1	The Transitive S_5 in S_6	207
7.2.2	Some Special Representations of S_5 and S_6	208
7.2.3	The Representation-Theoretic Sextic Resolvent of a Quintic Ring . .	211
7.2.4	Galois Invariance	213
7.3	A Specific Case	214

Chapter 1

Introduction

1.1 Introduction

In this chapter, we explore several of the motivations for this thesis, each of which was inspired by a generalization of Bhargava's Higher Composition Laws [9, 10, 11, 14, 8]. There are three basic angles from which we attack the inspiration: commutative algebra and low codimension algebraic geometry, representation theory, and analytic number theory.

In the first several sections, we review much of the theory of commutative algebra (and a dash of category theory) which is probably unfamiliar to readers of this thesis who are traditional number theorists. In the process we introduce free resolutions (Section 1.3) and varieties of (almost) minimal degree (Section 1.4). These are our inspirations for Chapters 5, 6, and 7.

We briefly discuss the seminal work of Siegel [101] on the average product of the class number and regulator of quadratic fields. This will be our inspiration for Chapters 2, 3, and 4, which, like Siegel, gives an analytic and a geometry of numbers-based proof of the average product of the class number and regulator of *cubic* rings. Moreover, the analytic result extends immediately to quartic rings, and the method of proof immediately implies the result for S_d rings for *all* d given the Strong Artin Conjecture and a strong version of

the Number of Number Fields Conjecture (see Section 2.3 in Chapter 2).

1.2 Notation

In this section we briefly collect some notation which appears throughout this thesis for the convenience of the reader.

1.2.1 (Graded) Rings

Unless otherwise specified, all rings are associative, commutative, unital, and noetherian. A ring R is said to be graded if

- there is a ring R_0 such that R is an R_0 algebra,
- there are R_0 modules R_n ($n \in \mathbb{Z}$) such that $R \cong \bigoplus R_n$ as R_0 modules,
- for all $i, j \in \mathbb{Z}$ and all $r \in R_i$ and $s \in R_j$ we have $rs \in R_{i+j}$.

The canonical example of such modules are when we take R_0 to be a ring and V to be a free R_0 module of finite rank r . Then $R[x_1, \dots, x_r] = \text{Sym}^\bullet V$ is a graded R module with the usual multiplication structure of polynomials. Unless otherwise specified, by graded ring we will mean *nonnegatively graded*, i.e., $R_n = 0$ for all $n < 0$. In this case, the submodule $\mathfrak{m} = R_+ = \sum_{n \geq 1} R_n$ of *positively graded elements*, also called the *irrelevant ideal*, is actually a graded R module.

Then we say that an R module M is *graded* provided that there are R_0 modules M_n ($n \in \mathbb{Z}$) such that $M \cong \bigoplus M_n$ and for all $i, j \in \mathbb{Z}$ and all $r \in R_i$ and $m \in M_j$ we have $rm \in M_{i+j}$. If M is a graded R module, we define the *twisted module* $M(j)$ to be the module such that $M(j)_n = M_{j+n}$ with the obvious R structure. Direct sums of the twists $R(j)$ of R are the *free R modules*.

We say that an R module M is finitely generated if there is a finite collection $a_1, \dots, a_N$ and a surjection $\bigoplus R(a_i) \rightarrow M$. Unless otherwise specified, we assume that a graded module is finitely-generated. In particular, since we are assuming $R_n = 0$ for $n < 0$, this implies that $M_m = 0$ for $m \ll 0$.

An important note is that $M \otimes R(j)$ is canonically isomorphic to $M(j)$.

1.2.2 The Vocabulary of Commutative Algebra

Perhaps the best reference for this section for the unfamiliar is D. Eisenbud's "Jog Through Commutative Algebra" in the appendix of [46]. Here we present no proofs, only definitions for the convenience of the reader.

Throughout, let the triple $(R, \mathfrak{m}, k)$ be one of the following:

- R is a local ring with maximal ideal $\mathfrak{m}$ and residue field k , or
- $R = k[x_1, \dots, x_r]$ and $\mathfrak{m} = (x_1, \dots, x_r)$ is the irrelevant ideal, and k is a field, which we regard as the R module $R/\mathfrak{m}$.

In the latter case, an R module will always be graded.

We say that the dimension $\dim R$ of the ring R is the maximal length of any strictly increasing sequence of prime ideals $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \dots \subseteq \mathfrak{p}_n$. If M is an R module, let $\text{Ann } M = \{r \in R : rm = 0\}$ be the *annihilator of M* . This is obviously an ideal. Then define $\dim M = \dim R/\text{Ann}(M)$. Since R is noetherian and M is finitely generated, this is always finite.

We say that a nonzero $r \in R$ is a *nonzerodivisor* for M whenever for every nonzero $m \in M$ we have $rm \neq 0$. A *regular sequence* for M is a sequence $r_1, \dots, r_s \in \mathfrak{m}$ such that r_i ($1 \leq i \leq s$) is a nonzerodivisor for $M/(r_1, \dots, r_{i-1})M$. The *depth of M* $\text{depth } M$ is the maximal length of any regular sequence for M . By Krull's Hauptidealsatz and induction, this is bounded by the dimension of M .

Definition 1. A module M over R is *Cohen-Macaulay* whenever $\dim M = \text{depth } M$. We say a variety $X \subseteq \mathbb{P}^n$ is *Cohen-Macaulay* whenever all of its local rings are Cohen-Macaulay, and we say it is *arithmetically Cohen-Macaulay* whenever the ring R/I_X is Cohen-Macaulay, where $R = k[x_0, \dots, x_n]$ is the homogeneous coordinate ring of $\mathbb{P}^n$ and I_X is the ideal cutting out X .

Remark 2. Note that from the bound $\text{depth } R \leq \dim R$, any zero-dimensional ring is necessarily Cohen-Macaulay. In particular, any scheme of points in $\mathbb{P}^n$ is Cohen-Macaulay, though it may not be *arithmetically* Cohen-Macaulay.

Remark 3. This is perhaps not the standard definition of “arithmetically Cohen-Macaulay” but it will be the one that we use. To see why there are other possible choices, note that if X is not projectively normal, then there is a difference between the ring R/I_X and the ring $\bigoplus_{i \geq 0} H^0(X, \mathcal{O}_X(i))$. As such, perhaps a more common definition involves the local cohomology of X . An explication of this theory may be found in the opening sections of [5].

Cohen-Macaulay modules and rings, i.e., rings which are Cohen-Macaulay as modules over themselves, are a fundamental construction of commutative algebra and of algebraic geometry. Moreover, like noetherian rings, they are not at all uncommon. Simple examples include the polynomial ring $k[x_0, \dots, x_n]$ and the homogeneous coordinate rings of complete intersections in projective space.

We will also make extensive use of one other much more complicated notion of commutative algebra, that of a *Gorenstein module*. There are many possible definitions (and we will see several in the next section), but there is a simple, intuitive one. Let $\mathcal{C}$ be an abelian category (whose definition we recall in the next section for the unfamiliar). Then a *dualizing functor* on $\mathcal{C}$ is an endofunctor $D : \mathcal{C} \rightarrow \mathcal{C}$ such that $D \circ D$ is the identity functor. It is not a hard exercise to show that such a functor is *exact*.

For example, if $\mathcal{C}$ is the category of finite dimensional vector spaces over a field k , then the functor $\text{Hom}(-, k)$ is a dualizing functor. This is actually an instance of a more general

notion. Specifically, it turns out [45, Proposition 21.2] that the category of finitely generated modules over a ring $(R, \mathfrak{m}, k)$ *always* admits a dualizing functor which is *representable* in the sense that there is a module ω_R such that the functor $\text{Hom}(-, \omega_R)$ is a dualizing functor. By Yoneda's Lemma the module ω_R is unique up to unique isomorphism, and as such is called the *canonical module* of R .

Definition 4. A Cohen-Macaulay ring $(R, \mathfrak{m}, k)$ is *Gorenstein* provided that (some twist of) R is ω_R .

1.3 Free Resolutions and Extra Structure

We begin with a concept which shows up throughout our work but which may be unfamiliar to number theorists: the *minimal free resolution*. We provide the necessary theory for an arbitrary abelian category $\mathcal{C}$. For an introduction to abelian categories, see [83], but we recall their definition here. A category $\mathcal{C}$ is called *abelian* provided that

- $\mathcal{C}$ has a zero object, i.e., an object 0 such that for every object M in $\mathcal{C}$ there is a unique map $0 \rightarrow M$ and a unique map $M \rightarrow 0$;
- Binary products and binary coproducts exist; and
- Every monomorphism is the kernel of some map and every epimorphism is the cokernel of some map.

In much of this thesis, we will be working with a polynomial ring $R = k[x_0, \dots, x_n]$ where k is either a field or a PID and our abelian category will be the category of finitely-generated (graded) modules over R .

Another important example for us will be the category of G -modules over $R = k[x_0, \dots, x_n]$. Here we regard $R = \text{Sym}^\bullet V$ where V is a free k module of rank $(n + 1)$. Then $\text{GL}(V)$ acts in the natural way on V . For us $G \subseteq \text{GL}(V)$ will be a finite subgroup.

Then a (graded) G module will be a finitely generated module M over R on which G acts such that for all $g \in G$, $r, s \in R$, and $m, n \in M$ we have $g(rm + sn) = g(r)g(m) + g(s)g(n)$. We recall

Proposition 5. *The category of G modules is an abelian category.*

Proof. Each construction in the category of G modules follows the construction in the category of R modules. Then each property may be checked using the fact that the functor from the category of G modules to the category of R modules is faithful. $\square$

Let us now recall a bit more of the language of category theory. A functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is *covariant* if it takes maps $A \rightarrow B$ to maps $F(A) \rightarrow F(B)$. It is *contravariant* if it takes maps $A \rightarrow B$ to maps $F(B) \rightarrow F(A)$. A covariant functor between abelian categories is *left (resp. right) exact* if for every exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow C \quad \text{resp.} \quad A \rightarrow B \rightarrow C \rightarrow 0$$

of objects in $\mathcal{C}$ the sequences

$$0 \rightarrow F(A) \rightarrow F(B) \rightarrow F(C) \quad \text{resp.} \quad F(A) \rightarrow F(B) \rightarrow F(C) \rightarrow 0$$

are exact. A contravariant functor F is *left (resp. right) exact* if for every exact sequence

$$A \rightarrow B \rightarrow C \rightarrow 0 \quad \text{resp.} \quad 0 \rightarrow A \rightarrow B \rightarrow C$$

of objects in $\mathcal{C}$ the sequences

$$0 \rightarrow F(C) \rightarrow F(B) \rightarrow F(A) \quad \text{resp.} \quad F(C) \rightarrow F(B) \rightarrow F(A) \rightarrow 0$$

are exact. A functor F is *exact* if it is both left and right exact.

For example, if M is a graded module over R , then the functor $-\otimes_R M$ is *right exact* but not necessarily *left exact*. However, if M is free, then the tensor functor is exact. In particular, if

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

is exact, then for any $a \in \mathbb{Z}$ the sequence

$$0 \rightarrow M_1(a) \rightarrow M_2(a) \rightarrow M_3(a) \rightarrow 0$$

is exact.

Another basic example is the functor $\text{Hom}(P, -)$, which is always left exact. Then we have the following definition.

Definition 6. An object P in $\mathcal{C}$ is called *projective* when the functor $\text{Hom}(P, -)$ is exact.

In the category of finitely-generated R modules, the most obvious projective objects are the *free* objects. Indeed, it is not hard to see that in any abelian category, the functors $\text{Hom}(\bigoplus A_i, -)$ and $\bigoplus \text{Hom}(A_i, -)$ are equivalent. As such, to check right exactness, we need only check right exactness of $\text{Hom}(R(a), -)$. In fact, this often characterizes projective modules.

Theorem 7. *If k is a PID and $R = k[x_1, \dots, x_r]$, then any projective module in the category of finitely generated R -modules is free.*

Remark 8. The proof of this theorem when k is a field is essentially an application of Nakayama's Lemma. When k is an arbitrary PID, then the theorem is a bit harder. In fact, the theorem remains true as stated if one removes the "finitely generated" requirement, which is an extremely difficult theorem to prove essentially because one does not even have a local version of Nakayama's Lemma. This variant is known as the *Quillen–Suslin theorem*.

An abelian category is said to have *enough projectives* if for every object A in $\mathcal{C}$ there is a projective object P in $\mathcal{C}$ and a surjection $P \rightarrow A$. Theorem 7 obviously implies that the category of finitely generated R modules has enough projectives.

In the category of G -modules, it turns out that something similar is true. In particular, suppose that W is a free module of finite rank over k and let G act on W . Then the R module $W \otimes R(j)$ has a canonical structure of G module (finitely generated since W has finite rank). We call these the *free G modules*.

If k has characteristic 0 or the characteristic of k is coprime to the order of G , then in fact every representation is *completely reducible*, i.e., every (finite-dimensional) representation of G can be written (essentially uniquely) as a direct sum of irreducible representations. In particular, every inclusion and every surjection *splits*. That is to say,

- if we have an injection $i : A \rightarrow B$, then there is a map $j : B \rightarrow A$ such that $j \circ i$ is the identity map, or
- if we have a surjection $p : B \rightarrow C$, then there is a map $q : C \rightarrow B$ such that $p \circ q$ is the identity map.

Using this, we see that every free G module over R is actually projective. For any map $W \otimes R(j) \rightarrow M$ is determined by the image of $W \otimes R_0$. As such, if $\psi : W \otimes R(j) \rightarrow N$ is a map and $\pi : M \rightarrow N$ is a surjection, then looking at the image $\psi(W) \subseteq N_{-j}$, we see that $\pi^{-1}\psi(W) \subseteq M_{-j}$ surjects onto $\psi(W)$ and so we get a splitting map $\psi(W) \rightarrow \pi^{-1}\psi(W)$. This gives our map. So we arrive at:

Proposition 9. *Suppose that k is a field of characteristic 0 or prime to the order of G . Then the category of G modules has enough projectives.*

1.3.1 Projective Resolutions

Our most important application of projective objects will be the construction of projective resolutions. Note that from Theorem 7 and Proposition 9 we know that the category of finitely generated R modules and G modules both have enough projectives. Now consider the following definition.

Definition 10. If A is an object in an abelian category $\mathcal{C}$, then a *projective resolution* of A is a sequence of maps

$$P_\bullet : \cdots \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow A$$

such that $P_0 \rightarrow A$ is an epimorphism and $P_i \rightarrow P_{i-1}$ ($i > 0$) has image the kernel of the map $P_{i-1} \rightarrow P_{i-2}$ (where $P_{-1} = A$).

Note that if a category has enough projectives, then every object necessarily has a projective resolution. However, there is no need for it to be unique or otherwise canonical, but there is the following important “comparison theorem”.

Theorem 11. Suppose $\mathcal{C}$ is abelian and $P_\bullet \rightarrow M$ and $Q_\bullet \rightarrow M$ are two projective resolutions of an object $M \in \mathcal{C}$. Then there is a map $P_\bullet \rightarrow Q_\bullet$ making the below diagram commute:

$$\begin{array}{ccccccc} \cdots & \rightarrow & P_2 & \rightarrow & P_1 & \rightarrow & P_0 \rightarrow M \\ & & \downarrow & & \downarrow & & \downarrow id \\ \cdots & \rightarrow & Q_2 & \rightarrow & Q_1 & \rightarrow & Q_0 \rightarrow M. \end{array} \tag{1.1}$$

Proof. The map $Q_0 \rightarrow M$ is surjective, so there is a map $P_0 \rightarrow Q_0$ factoring the map $P_0 \rightarrow M$. The image of the map $Q_1 \rightarrow Q_0$ is the kernel K_0 of the map $Q_0 \rightarrow M$. Moreover, we see that the composite of the map $P_1 \rightarrow P_0 \rightarrow Q_0$ has image inside K_0 by the commutativity of the diagram. Hence, since $Q_1 \rightarrow K_0$ is epic, there is a factor map $P_1 \rightarrow Q_1$ of the map $P_1 \rightarrow K_0$.

This process repeated *ad infinitum* yields the desired map of complexes. □

Remark 12. This proposition will be extremely important to us when constructing multiplicative structures on free resolutions over fields. However, when we try to descend to $\mathbb{Z}$, we will need a stronger result, which will require much more *ad hoc* tools.

1.3.2 Why Projective Resolutions: Derived Functors

Suppose that $F : \mathcal{C} \rightarrow \mathcal{D}$ is a covariant right exact functor of abelian categories. Then applying F to a projective resolution $P_\bullet$ of an object M in $\mathcal{C}$, we obtain a *complex* of objects in $\mathcal{D}$. That is, the composition of any two maps $F(P_i) \rightarrow F(P_{i-1}) \rightarrow F(P_{i-2})$ is 0. We define the *derived functor* DF^i of F to be the homology at the map $F(P_{i+1}) \rightarrow F(P_i) \rightarrow F(P_{i-1})$, i.e., the kernel of the second map modulo the image of the first. In the case $i = 0$, we by convention take $P_{-1} = 0$ and so $DF^0(M) = F(M)$.

Of course, none of this is *a priori* well-defined, but one checks that two projective resolutions yield the same derived functors, i.e., the derived functors are well-defined.

For us, the most important derived functor will be $\text{Tor}_i(-, M)$, which is the derived functor of the functor $- \otimes M$ where M is a finitely generated R module. It is a simple application of spectral sequences [110, Chapter 5] to show that Tor is “commutative” in the sense that $\text{Tor}_i(A, B)$ is isomorphic to $\text{Tor}_i(B, A)$. As such, we may compute $\text{Tor}_i(A, B)$ either from a projective resolution of A or a projective resolution of B . This will be extremely important for us later.

1.3.3 Minimal Free Resolutions

For certain rings, free resolutions admit a nice structure theory. Suppose $R = k[x_0, \dots, x_n]$ is a polynomial ring over a field k . Let $\mathfrak{m} = (x_0, \dots, x_n)$ be the irrelevant ideal. We say a free resolution $P_\bullet \rightarrow M$ is *minimal* provided that the image of $F_i \rightarrow F_{i-1}$ is contained in $\mathfrak{m}F_{i-1}$. We have the following well-known theorem. (See, e.g., [46, Chapter 1].)

Theorem 13. *Any two minimal free resolutions of a finitely generated R module are isomorphic. That is, if $P_\bullet$ and $Q_\bullet$ are two minimal free resolutions of the same R module, then there exist isomorphisms $P_i \rightarrow Q_i$ such that the diagram (1.1) commutes.*

Remark 14. Actually, to prove this theorem one requires that the minimal free resolution be finite, but this will follow from our discussion of the Koszul complex.

Example 15. The homogeneous coordinate ring of a hypersurface of degree d in $\mathbb{P}_k^n$ is $R/(f)$ where $f \in R_d$ is some degree d homogeneous polynomial. Then the minimal free resolution of $R/(f)$ is given by

$$0 \rightarrow R(-d) \rightarrow R$$

where $R(-d) \rightarrow R$ is the multiplication by f map.

Example 16. A codimension 2 subvariety $X \subseteq \mathbb{P}_k^n$ is said to be a *complete intersection* provided that its saturated ideal is generated by 2 homogeneous elements $f, g \in R$ of positive degree. It is easy to see that the following complex is exact and minimal and in fact resolves the R module $R/(f, g)$:

$$0 \rightarrow R(-\deg(f) - \deg(g)) \xrightarrow{\begin{bmatrix} g \\ -f \end{bmatrix}} \begin{matrix} R(-\deg(f)) \\ \oplus \\ R(-\deg(g)) \end{matrix} \xrightarrow{\begin{bmatrix} f & g \end{bmatrix}} R.$$

This is called the *Koszul complex* of f and g .

Theorem 13 allows us to make the following definition unambiguously.

Definition 17. Suppose that $P_\bullet$ is the minimal free resolution of a finitely generated R module M . Suppose that

$$P_i = \bigoplus_j R(-j)^{\beta_{ij}}.$$

Then the nonnegative integers β_{ij} (almost all 0) are called the *Betti numbers* of M .

1.3.4 A Brief Interlude: The Koszul Complex

In this section, we construct the so-called “mother of all free resolutions”, the *Koszul complex*. Suppose that $(R, \mathfrak{m}, k)$ is as in Section 1.2.2 and let $r_1, \dots, r_s \in \mathfrak{m}$ (homogeneous of the same degree d in the graded case¹). Then we consider the free module $F = R^s$ with basis $e_1, \dots, e_s$. Then the $e_{i_1} \wedge \dots \wedge e_{i_j}$ with $i_1 < \dots < i_j$ are a basis of $\wedge^j R^s$. Now we get maps $\wedge^j F \rightarrow \wedge^{j-1} F$ when $j > 0$ given by

$$e_{i_1} \wedge \dots \wedge e_{i_j} \mapsto \sum_{\ell} (-1)^\ell r_{i_\ell} e_{i_1} \wedge \dots \wedge \hat{e}_{i_\ell} \wedge \dots \wedge e_{i_j}.$$

That this is a complex is rather easy to see. But it has the following absolutely critical property.

Theorem 18. *The Koszul complex is exact if and only if $r_1, \dots, r_s$ is a regular sequence in which case it is the minimal free resolution of the cyclic R module $R/(r_1, \dots, r_s)$.*

1.3.5 The Finiteness of Minimal Free Resolutions

Now we are in a position to show that minimal free resolutions must exist and be finite. First note from the definitions that $\dim_k \operatorname{Tor}_i(M, k)_j = \beta_{ij}$ for any finitely generated module M . But Tor may be computed from a projective resolution of either M or k . If $(R, \mathfrak{m}, k)$ is *regular*, i.e. $\mathfrak{m}$ is generated by a regular sequence, then from Theorem 18, the minimal free resolution of k is given by the Koszul complex. In particular, it is finite! Hence, $\operatorname{Tor}_i(M, k) = 0$ for $i \gg 0$. Moreover, for fixed i , since everything in sight is finitely generated, we have that $\operatorname{Tor}_i(M, k)_j = 0$ for $|j| \gg 0$. That is, the minimal free resolution of any finitely generated module over a regular ring $(R, \mathfrak{m}, k)$ is finite and hence unique. From this discussion and Theorem 13, we may make the following definition.

Definition 19. The length of a minimal free resolution of M is called its *projective dimension*

¹This is not necessary, but it makes notation easier and we will not need the more general case.

and is denoted by $\text{pd } M$.

Now that we have this in hand, we may state the following theorem.

Theorem 20 (Auslander-Buchsbaum Formula). *If M is a module over R , then $\text{pd } M = \text{depth } R - \text{depth } M$. When M and R are Cohen-Macaulay, this says that the length of the minimal free resolution of M is precisely its codimension.*

1.3.6 Injective Modules and Resolutions and the Gorenstein Condition

In this section, we briefly discuss the dual notion to *projective* modules, viz. *injective* modules, and the role they play in the Gorenstein condition. To begin, we note that just as $\text{Hom}(P, -)$ is covariant and left-exact, $\text{Hom}(-, I)$ is *contravariant* and left-exact when I is an object in an abelian category. That is, given a map $\varphi : A \rightarrow B$ and a map $f : B \rightarrow I$, there is a natural map $f \circ \varphi : A \xrightarrow{\varphi} B \xrightarrow{f} I$. Moreover, if $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is exact, then so is $0 \rightarrow \text{Hom}(C, I) \rightarrow \text{Hom}(B, I) \rightarrow \text{Hom}(A, I)$. For instance, the injectivity of the left-hand map is simply the assertion that there is a left-inverse to the map $\text{Hom}(C, I) \rightarrow \text{Hom}(B, I)$, which follows from the surjectivity of the map $B \rightarrow C$. With some diagram chasing, this may be proved for general abelian categories, but is easily seen for modules over a ring.

Just as an object P is called *projective* whenever $\text{Hom}(P, -)$ is *exact*, we say that an object I is *injective* whenever $\text{Hom}(-, I)$ is exact. Injective objects in general tend to be *much* more difficult to comprehend than projective objects. For instance, it is not even true that free objects need be injective. Indeed, it is not hard to check that if $(R, \mathfrak{m}, k)$ is a ring, then the free object $\bigoplus R(a_i)$ is injective if and only if $R(a_i)$ is injective for all i . But twisting is an exact operation, so this is simply the assertion that R is injective.

Again as with projectives, we say that an abelian category $\mathcal{C}$ has *enough injectives* provided that for every object M of $\mathcal{C}$ there is an injective object I in $\mathcal{C}$ and an injection

$M \rightarrow I$. Just as the condition of having enough projectives allowed us to build projective resolutions, this condition allows us to build *injective resolutions*.

Proposition 21. *The category of finitely generated R modules has enough injectives.*

However, injective resolutions need not be finite! In fact, this is sufficiently rare that we make the following definition.

Definition 22. A module over R is called *Gorenstein* if it has a finite injective resolution.

As this will be a rather difficult condition to verify in any particular case, we recall the following beautiful equivalent definition of Gorenstein due to R. Stanley.

Theorem 23 ([104]). *A cyclic Cohen-Macaulay module $M = R/I$ is Gorenstein if and only if the coefficients of the numerator of the Hilbert polynomial are palindromic.*

This theorem may be rephrased in a much more convenient pictorial way. First, we note that from the definition of *minimal*, we know that if $\beta_{ij} = 0$ then $\beta_{i+1,j+1} = 0$. As such, it makes sense to write $b_{ij} = \beta_{i,i+j}$ and then the nonzero Betti numbers will show up in the table

$$\begin{array}{ccccccccc}
 \beta_{00} & \beta_{11} & \beta_{22} & \cdots & b_{00} & b_{10} & b_{20} & \cdots \\
 \beta_{01} & \beta_{12} & \beta_{23} & \cdots & b_{10} & b_{11} & b_{12} & \cdots \\
 \beta_{02} & \beta_{13} & \beta_{24} & \cdots & b_{20} & b_{21} & b_{22} & \cdots \\
 \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots
 \end{array} = \tag{1.2}$$

Moreover, if $d = \text{pd}(M)$ and J is maximal among all j such that $b_{dj} \neq 0$ then $b_{ij} = 0$ for all i and all $j > J$. That is, (1.2) has $d + 1$ columns and $J + 1$ rows. We call the diagram (1.2) the *Betti table* of M . We say that a Betti table is *symmetric* if $b_{ij} = b_{d-i,J-j}$ for all i, j . In other words, the diagram (1.2) is symmetric about its antidiagonal. It is a lovely exercise to deduce the following from Stanley's Theorem 23.

Corollary 24. *A cyclic Cohen-Macaulay R module is Gorenstein if and only if its Betti table is symmetric.*

Example 25. For instance, Examples 15 and 16 will be Gorenstein. More generally, Theorem 18 shows that the homogeneous coordinate ring of a complete intersection in projective space is Gorenstein.

1.3.7 Differential Graded Algebras

Suppose then that $F_\bullet$ is a complex over R with $F_0 = R$. Then we can regard (abusing notation) $F_\bullet = \bigoplus F_i$ as a graded R module. Suppose in addition to this module structure $F_\bullet$ has the structure of an R algebra (which we do not require to be commutative or associative), such that the *Leibniz rule* is satisfied:

$$f_i \in F_i \text{ and } f_j \in F_j \text{ implies } d(f_i f_j) = f_i d(f_j) + (-1)^i d(f_i) f_j,$$

then we say that $F_\bullet$ is a *differential graded algebra* (DGA).

Remark 26. In the above, we have labeled the maps $d_i : F_i \rightarrow F_{i-1}$. It is traditional to drop the subscripts on the d maps when it is clear from context which d map is meant.

Now $F_\bullet$ may be associative using the normal definition. However, it is traditional to say that $F_\bullet$ is commutative if it is *graded commutative*, i.e., $f_i f_j = (-1)^{i+j} f_j f_i$ for $f_i \in F_i$ and $f_j \in F_j$. We will often call associative, commutative, differential graded algebras ACDGAs (dropping the A or the C will have the obvious meaning).

Example 27. The resolution

$$R(-d) \rightarrow R$$

of a hypersurface of degree d has an associative, commutative, differential graded algebra structure. Here $F_0 = A$ and $F_1 = R(-d)$. The map $R(-d) \otimes R(-d) \rightarrow 0$ is the only one. The map $R \otimes R \rightarrow R$ is the canonical one. And the map $R \otimes R(-d) \rightarrow R(-d)$ is also the canonical one.

Example 28. The Koszul complex also has an ACDGA structure. For we note that for any R module M the exterior algebra $\wedge^\bullet M$ has a canonical algebra structure. It is not hard to see that it is compatible with the complex maps defined in Section 1.3.4.

1.4 The Inspiring Geometry: Varieties of (Almost) Minimal Degree

Suppose that $X \subseteq \mathbb{P}^n$ is a subvariety over a field k . Then one of the most important invariants of X is its *degree*, and perhaps one of the most important facts about the degree is the following elementary bound.

Theorem 29. *If $X \subseteq \mathbb{P}^n$ is connected in codimension one and nondegenerate, then $\deg(X) \geq \text{codim}(X) + 1$.*

The vocabulary here deserves a bit of an explanation. *Nondegenerate* means that X does not live in any hyperplane. As for connected in codimension d , we have the following Proposition–Definition.

Proposition-Definition 30 ([65, Proposition 1.1]). *A noetherian topological space X is connected in codimension d if it satisfies either of the following equivalent conditions:*

- *If $Y \subseteq X$ is a subvariety of codimension at least $d + 1$, then $X - Y$ is connected, or*
- *If X' and X'' are irreducible components of X , then there is a sequence of irreducible components $X' = X_1, \dots, X_r = X''$ such that $X_i \cap X_{i+1}$ has codimension at most d for all $1 \leq i < r$.*

In particular, irreducible varieties are connected in all codimensions and every variety of dimension d is connected in all codimensions $\geq d$. In particular, dimension 0 schemes are always connected in codimension 1. This will be important for us later on.

1.4.1 Minimal Degree

Suppose for now that $X \subseteq \mathbb{P}^n$ is a nondegenerate, irreducible variety. We say that X is a *variety of minimal degree* whenever the bound of Theorem 29 is actually an equality, i.e., whenever $\deg(X) = \operatorname{codim}(X) + 1$. It turns out that there are very few such varieties.

Theorem 31 ([46, Theorem A2.64]). *If $X \subseteq \mathbb{P}^n$ is an irreducible variety of minimal degree then it is one of the following:*

- *a quadric hypersurface,*
- *a cone over the Veronese embedding of $\mathbb{P}^2$ into $\mathbb{P}^5$, or*
- *a rational normal scroll.*

The first two of these should be familiar. As for the latter, there are many equivalent definitions [47], but the most intuitive is as follows. Let $H_1, \dots, H_r \subseteq \mathbb{P}^n$ be linear subspaces which span $\mathbb{P}^n$ but which do not intersect pairwise. Let $\lambda_i : \mathbb{P}^1 \hookrightarrow H_i$ be a parameterized rational normal curve. Then the *rational normal scroll* associated with this data is the closure of the union of the $(r - 1)$ -planes P_t spanned by $\{\lambda_1(t), \dots, \lambda_r(t)\}$.

Remark 32. When $r = 1$, rational normal scrolls are just rational normal curves.

Varieties of minimal degree are important to us because the 0 dimensional case corresponds to ideals in rank $n + 1$ rings. To see why, consider a rank $n + 1$ ring R over $\mathbb{Z}$. Then a line bundle I on $\operatorname{Spec}(R)$ is the same thing as an ideal, and an equivalence class of line bundles is the same as an element of the class group $\operatorname{Pic}(R) = \operatorname{Pic}(\operatorname{Spec} R)$. But since $\mathbb{Z}$ is a PID, this is free of rank n as a $\mathbb{Z}$ module, and so we get an embedding $\operatorname{Spec} R \rightarrow \mathbb{P}(I) = \mathbb{P}_{\mathbb{Z}}^n$.

Indeed, the case of “quadric hypersurfaces” in $\mathbb{P}_{\mathbb{Z}}^1$ is Gauss’s parameterization of ideal classes in quadratic rings by binary quadratic forms. And the case of rational normal cubic curves yields Bhargava’s parameterization [10] (see also Chapter 2) of ideal classes in cubic

rings. So we might expect to find generalized parameterizations of ideals in rank n rings beyond the work of Bhargava in the parameterizations of varieties of minimal degree.

So what parameterizes varieties of minimal degree? Well, beyond the quadrics and cones (which are obvious) we are left with the scrolls. Now every scroll over a field has equations determined as follows. Let for $1 \leq i \leq r$, let $1 \geq a_i$ and let $\sum(a_i + 1) = n + 1$ and number the coordinates $\mathbf{x}$ of $\mathbb{P}^n$ as $x_{i,j}$ with $1 \leq i \leq r$ and $0 \leq j \leq a_i$. Then form the matrices

$$A_i = \begin{pmatrix} x_{i,0} & x_{i,1} & \cdots & x_{i,a_i-1} \\ x_{i,1} & x_{i,2} & \cdots & x_{i,a_i} \end{pmatrix}$$

and finally the block matrix

$$A = \begin{pmatrix} A_1 & A_2 & \cdots & A_r \end{pmatrix}.$$

Then up to PGL_{n+1} equivalence, all rational normal scrolls are given by the 2×2 minors of A . Note that if $r = 1$, then these are the traditional equations of a rational normal curve.

So one might hope that, similar to Gauss's and Bhargava's parameterizations, the integral orbits of $2 \times n$ matrices of linear forms on $\mathbb{P}^{n-1}$ might yield a parameterization of rank n rings. However, this is not the case. In fact, they only parameterize rank n rings which may be embedded into $\mathbb{P}^1$ as subschemes. While this is certainly true of nondegenerate rings over a characteristic 0 field where every such extension is separable, it is no longer true over an arbitrary base (nor even $\mathbb{Z}$). See the detailed study in M. Wood's thesis [112] for more information.

We are thus left with the question: What further conditions are necessary to parameterize ideal classes by the integral points on some variety? Our answer begins by first examining another case.

1.4.2 Almost Minimal Degree

Our real inspiration is the “next case” of Theorem 29. Specifically, instead of considering varieties X of degree $\text{codim}(X) + 1$, we consider varieties of degree $\text{codim}(X) + 2$. These are the so-called *varieties of almost minimal degree*. Like varieties of minimal degree, there is a classification theorem of such varieties. To make it easy to state, we only concern ourselves with the *nonsingular* case.

Theorem 33 ([53]). *Suppose that $X \subseteq \mathbb{P}^n$ is an irreducible, nonsingular variety of almost minimal degree. Then X is either*

- *a genus one curve embedded by a degree $\deg(X)$ line bundle,*
- *a del Pezzo surface,*
- *a cubic hypersurface,*
- *a complete intersection of two quadrics,*
- *a linear section of $\text{Gr}(2, 5) \subseteq \mathbb{P}^9$ the Grassmannian of 2-planes in 5-space,*
- *$\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ in its Segre embedding in $\mathbb{P}^7$,*
- *$\mathbb{P}^2 \times \mathbb{P}^2$ in its Segre embedding in $\mathbb{P}^8$,*
- *the blow up of $\mathbb{P}^3$ at a point, or*
- *the 2-uple embedding $\mathbb{P}^3 \hookrightarrow \mathbb{P}^9$.*

We once again see several of Bhargava’s family of parameterizations popping up. For instance, “cubic hypersurfaces” in $\mathbb{P}^1$ are binary cubic forms, i.e., the Delone-Fadeev parameterization of cubic rings [42]. Complete intersections of pairs of quadrics are given by the $\text{GL}_2(k) \times \text{GL}_3(k)$ orbits on $k^2 \otimes \text{Sym}^2 k^3$, which should remind us of the Wright-Yukie-Bhargava [116, 11] parameterization of quartic algebras and rings. Similarly, linear

sections of the Grassmannian of 2-planes in 5-space are cut out by the Pfaffians of a 5×5 skew-symmetric matrix of linear forms on $\mathbb{P}^n$ with $n \leq 9$. In the case $n = 4$, we have once again found Bhargava's parameterization of quintic rings [14].

Indeed, one may interpret Bhargava's parameterizations of rank n rings as taking hyperplane sections of an appropriate variety of almost minimal degree and keeping very careful track of what problems that causes over bases which are not fields. And one may further interpret much of the work of Bhargava-Ho as taking hyperplane sections of an appropriate variety of almost minimal degree as well. So if we were to find any immediate extensions of Bhargava's theory, we should look to this list.

However, as with varieties of minimal degree, the more general varieties of almost minimal degree do not lend themselves so well to the parameterization of rings. Notably, $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2 \times \mathbb{P}^2$ both have degree 6, but if a nondegenerate degree 6 ring could be embedded in a hyperplane section of $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ (resp. $\mathbb{P}^2 \times \mathbb{P}^2$), then via the projection maps it could be embedded in $\mathbb{P}^1 \times \mathbb{P}^1$ (resp. $\mathbb{P}^2$). This is again always possible over characteristic 0 fields. For if B is a PID and R is a ring of rank n over B , then R embeds into $\mathbb{A}_B^1$ if and only if $R \cong B[x]/(f)$ for some *monic* $f \in B[x]$ of degree n . From the primitive element theorem, this is always true for nondegenerate extensions of characteristic 0 fields. For instance, the ring $\mathbb{Z} + \mathbb{Z}[x]/(x^3 - 2)$ cannot be generated by a single element.

So we are again left wondering what we can do from here. But there is hope. An idea of Deligne [41] taken to its extreme conclusions by Wood in her thesis [114, 113] begins by exploring the *minimal free resolution* of n points in $\mathbb{P}^{n-2}$ (for her $n = 3, 4$). In each case, the minimal free resolution is the Koszul complex and so has a canonical multiplicative structure, as explicated in the previous section.

But Buchsbaum and Eisenbud [25] gave a canonical multiplicative structure on the minimal free resolution of 5 points in $\mathbb{P}^3$, and so one wonders what the impediment to a similar parameterization to [114, 113] is. The answer is a lack of satisfying definition of

“sextic resolvent”. We summarize the representation theory of the situation in Chapter 7, though there is a problem at 2 which makes it difficult to descend our results to the integers and more general bases. (We believe that this is essentially the same problem which causes a power of 2 to arise in the formula for the discriminant of the sextic resolvent of a rank n quintic ring over $\mathbb{Z}$ in [14].) We hope to rectify this in future work.

Moreover, we see that multiplicative structures on minimal free resolutions allow one to get a handle on parameterizations of rings. So we set out to put a multiplicative structure on the minimal free resolution of n points in $\mathbb{P}^{n-2}$. This is Chapter 5.

It turns out that these resolutions and multiplicative structures are just a part of a larger story. Boij-Söderberg Theory [22, 49, 48] has led to a renewed interest in the construction of pure resolutions, i.e., those in which each column of the Betti table (1.2) contains only one nonzero integer. To contribute to this theory, we give a new family of free resolutions with a multiplicative structure associated to what we call *two-rowed Specht ideals* (see Chapter 6).

1.5 Siegel’s Theorem

Finally, we recall the work of Siegel [101] in which he gave two proofs of the asymptotic average size of the product of the class number and regulator of quadratic fields and rings. In particular, he showed

Theorem 34. *We have*

$$\sum_{\substack{\mathcal{O} \text{ quadratic} \\ 0 < \text{Disc}(\mathcal{O}) < X}} h(\mathcal{O}) \text{Reg}(\mathcal{O}) \sim \frac{\pi^2}{36\zeta(3)} \cdot X^{3/2}, \text{ and}$$

$$\sum_{\substack{\mathcal{O} \text{ quadratic} \\ 0 < -\text{Disc}(\mathcal{O}) < X}} h(\mathcal{O}) \text{Reg}(\mathcal{O}) \sim \frac{\pi}{36\zeta(3)} \cdot X^{3/2}.$$

These sums are both over orders in quadratic fields ordered by their discriminant. The first

concerns real quadratic fields and the second covers imaginary quadratic fields, where, it should be noted, $\text{Reg}(\mathcal{O}) = 1$.

His first proof of this fact used a lovely argument via the geometry of numbers. Specifically, he used the correspondence due to Gauss between (equivalence classes of) binary quadratic forms and elements of the class groups of the associated quadratic field to relate these sums to counting points in a subspace of $\mathbb{R}^2$. He was aided by reduction theory which gave him a tractable correspondence between binary quadratic forms whose coefficients satisfied certain easily written inequalities and equivalence classes of forms.

This proof technique underlies Davenport and Heilbronn's work [40] counting the number of cubic fields up to a given discriminant. It is also the technique which Bhargava and his coauthors exploit to spectacular effect to count the number of quartic and quintic number fields up to a given discriminant ([12], [15]), to compute the average size of the 2-, 3-, 4-, and 5-Selmer groups of elliptic curves ordered by height ([17], [18], and forthcoming works), and to prove many other beautiful results. Our contribution to this growing literature will be to extend Siegel's techniques (with Bhargava's improvements and some of our own) to compute the average size of the product of the class group of cubic fields and certain subsets of the orders therein.

Siegel's second proof uses Dirichlet's Class Number Formula to relate the sums in Theorem 34 to the average size of $L(1, \chi)$ where χ ranges over quadratic characters of bounded conductor. As with many such arguments, the proof comes down to switching the order of summation from first summing the Dirichlet series then summing over the characters to the reverse to the reverse. Such a feat becomes relatively simple under the Generalized Riemann Hypothesis for quadratic characters, but requires more delicate arguments in its absence.

We extend Siegel's techniques, combining them with a technique of W. Luo [89], to compute the average size of the product of the class number and regulator of cubic and quartic fields as well as the same for certain subsets of orders contained therein. To avoid

relying on the Riemann Hypothesis, we must instead rely on the Strong Artin Conjecture for L -functions attached to cubic and quartic number fields as well as knowledge of the total number of number fields up to a given discriminant. These two results are known by results of Langlands and Tunnell (and using the fact that every subgroup of S_4 is solvable) and the work of Bhargava, respectively. Assuming these two results, we conjecture a similar result for number fields of every degree.

1.6 Some Future Work

In our exploration of varieties of almost minimal degree, Delone-Faddeev's parameterization of cubic rings² [42] and Bhargava's parameterizations of quartic [11] and quintic [14] rings are rather apparent. As such, we can ask the question about higher dimensional versions of these parameterizations.

The case of curves was explored by Ho in her thesis [67] and led to her beautiful joint work with Bhargava on describing the integral orbits of coregular vector spaces [16]. In future work, we will generalize these one step further to the case of del Pezzo surfaces. We have omitted discussion of these topics here since they are not immediately relevant, but the reader should keep these examples in mind as further examples of this circle of ideas.

²It has been pointed out by F. Lemmermeyer that F. Levi actually gave this correspondence [88] before Delone and Faddeev had written their book. Indeed, Delone and Faddeev even credit Levi for the result in their preface, but not in the main body of the text. Unfortunately, the name Delone-Faddeev correspondence has become standard, and so we will use it throughout this work.

Part I

Geometry of Numbers

Chapter 2

Asymptotics of the Class Number Times the Regulator of Cubic Fields and Orders

2.1 Introduction

Many mathematicians have given results on the product of class numbers and regulators of number fields of a fixed degree. The two most famous results are those of Brauer-Siegel addressing worst-case bounds on the product and Gauss-Mertens-Siegel addressing the average for quadratic fields. To state their theorems, if k is a number field, let $[k : \mathbb{Q}]$ be the degree of k over $\mathbb{Q}$ and $\Delta(k) = |\text{Disc}(k)|$ be the absolute value of its discriminant. Further, let $h(k)$ be the class number of k and $\text{Reg}(k)$ its regulator. Then we have the following.

Theorem 35 (Brauer-Siegel [24]). *Let $k_1, k_2, \dots$, be a sequence of number fields with $[k_i : \mathbb{Q}] = o(\log \Delta(k_i))$ as $i \rightarrow \infty$. Then*

$$\frac{\log h(k_i) \text{Reg}(k_i)}{\log \sqrt{\Delta(k_i)}} \rightarrow 1$$

as $i \rightarrow \infty$.

In particular, Landau showed that $h(k) \operatorname{Reg}(k) = O_{[k:\mathbb{Q}], \varepsilon}(\operatorname{Disc}(K)^{1/2+\varepsilon})$. Several refinements have been made to this result, for instance [100, 87]. It is conjectured that the number of number fields of a fixed degree d with absolute discriminant at most X is on the order of X (and is proved in the cases $2 \leq d \leq 5$ [40, 12, 15]). This immediately gives a conjectural average case bound of $O(X^{3/2+\varepsilon})$ for the sum of $h(k) \operatorname{Reg}(k)$ where k runs over fields of a fixed degree and discriminant up to X . In the case $d = 2$, we can actually compute exact asymptotics.

Theorem 36 (Gauss-Mertens-Siegel [91, 101]). *We have*

$$\begin{aligned} \sum_{\substack{\mathcal{O} \text{ quadratic} \\ 0 < \operatorname{Disc}(\mathcal{O}) < X}} h(\mathcal{O}) \operatorname{Reg}(\mathcal{O}) &\sim \frac{\pi^2}{36\zeta(3)} \cdot X^{3/2}, \text{ and} \\ \sum_{\substack{\mathcal{O} \text{ quadratic} \\ 0 < -\operatorname{Disc}(\mathcal{O}) < X}} h(\mathcal{O}) \operatorname{Reg}(\mathcal{O}) &\sim \frac{\pi}{36\zeta(3)} \cdot X^{3/2}. \end{aligned}$$

These sums are both over orders in quadratic fields ordered by their discriminant. The first concerns real quadratic fields and the second covers imaginary quadratic fields, where, it should be noted, $\operatorname{Reg}(\mathcal{O}) = 1$.

Using a detailed study of the Fourier expansion of Eisenstein series of $\frac{1}{2}$ -integral weight, Goldfeld and Hoffstein were able to restrict the sums in Theorem 36 to *maximal* orders.

Theorem 37 ([58]).

$$\begin{aligned} \sum_{\substack{k \text{ quadratic} \\ 0 < \operatorname{Disc}(k) < X}} h(k) \operatorname{Reg}(k) &\sim \frac{\zeta(2)}{3\pi} \prod_p (1 - p^{-2} - p^{-3} + p^{-4}) \cdot X^{3/2}, \text{ and} \\ \sum_{\substack{k \text{ quadratic} \\ 0 < -\operatorname{Disc}(k) < X}} h(k) \operatorname{Reg}(k) &\sim \frac{\zeta(2)}{6} \prod_p (1 - p^{-2} - p^{-3} + p^{-4}) \cdot X^{3/2}, \end{aligned}$$

where both sums are over quadratic field extensions of $\mathbb{Q}$.

The purpose of this chapter and Chapter 4 is to give the analogues of Theorem 36 and Theorem 37 for cubic and quartic orders and fields as well as conjectures when $G = S_d$. In the course of this chapter, we shall prove the following generalizations. First, let us consider the cubic case $d = 3$.

Theorem 38. *Let $\mathcal{M}_3^{(i)}(X)$ be the set of degree 3 field extensions of $\mathbb{Q}$ having $3 - 2i$ real embeddings with absolute discriminant at most X . Further let $\mathcal{F}_3^{(i)}(X)$ be the set of all orders $\mathcal{O} \subseteq k$ where $k \in \mathcal{M}_3^{(i)}(X)$. Then*

$$\begin{aligned} \sum_{k \in \mathcal{M}_3^{(0)}(X)} h(k) \operatorname{Reg}(k) &\sim \frac{1}{72} \cdot \prod_p \left(\frac{p^7 + p^6 + 2p^5 - 2p^3 - 2p^2 + 1}{p^7 + p^6 - p^4 - p^3} \right) \cdot X^{3/2} \\ \sum_{\mathcal{O} \in \mathcal{F}_3^{(0)}(X)} h(\mathcal{O}) \operatorname{Reg}(\mathcal{O}) &\sim \frac{1}{72} \cdot \prod_p \left(\frac{p^4 + p^3 + 3p^2 + 3p + 2}{p^4 + p^3 - p - 1} \right) \cdot X^{3/2} \end{aligned}$$

when k is a totally real field or $\mathcal{O}$ is an order therein, and

$$\begin{aligned} \sum_{k \in \mathcal{M}_3^{(1)}(X)} h(k) \operatorname{Reg}(k) &\sim \frac{1}{12\pi} \cdot \prod_p \left(\frac{p^7 + p^6 + 2p^5 - 2p^3 - 2p^2 + 1}{p^7 + p^6 - p^4 - p^3} \right) \cdot X^{3/2} \\ \sum_{\mathcal{O} \in \mathcal{F}_3^{(1)}(X)} h(\mathcal{O}) \operatorname{Reg}(\mathcal{O}) &\sim \frac{1}{12\pi} \cdot \prod_p \left(\frac{p^4 + p^3 + 3p^2 + 3p + 2}{p^4 + p^3 - p - 1} \right) \cdot X^{3/2} \end{aligned}$$

when k has one complex place.

Remark 39. The collection of all cubic field extensions of $\mathbb{Q}$ is not actually a set. By “the set of degree 3 field extensions of $\mathbb{Q}$ ” we mean “the set of isomorphism classes of degree 3 field extensions of $\mathbb{Q}$ ”. However, we find this phrasing to be a bit bulky, and throughout this thesis, when we say “degree n field” or “degree n ring”, we really mean “isomorphism class of degree n fields” and similarly for degree n rings.

We can also prove a result in the case $d = 4$, however, the techniques we apply in

this chapter cannot be extended at this time. So the proof of the following theorem will be delayed until Chapter 4.

Theorem 40. *Let $\mathcal{M}_4^{(i)}(X)$ be the set of degree 4 field extensions of $\mathbb{Q}$ having $4 - 2i$ real embeddings with discriminant at most X . Then*

$$\begin{aligned} & \sum_{k \in \mathcal{M}_4^{(0)}(X)} h(k) \operatorname{Reg}(k) \\ & \sim \frac{1}{576} \cdot \prod_p \left(\frac{p^{12} + p^{11} + 3p^{10} + 3p^9 - 4p^7 - 5p^6 - 3p^5 + p^4 + 3p^3 + 2p^2 - 1}{p^{12} + p^{11} - p^9 - 2p^8 - p^7 + p^5 + p^4} \right) \cdot X^{3/2} \end{aligned}$$

$$\begin{aligned} & \sum_{k \in \mathcal{M}_4^{(1)}(X)} h(k) \operatorname{Reg}(k) \\ & \sim \frac{1}{48\pi} \cdot \prod_p \left(\frac{p^{12} + p^{11} + 3p^{10} + 3p^9 - 4p^7 - 5p^6 - 3p^5 + p^4 + 3p^3 + 2p^2 - 1}{p^{12} + p^{11} - p^9 - 2p^8 - p^7 + p^5 + p^4} \right) \cdot X^{3/2} \end{aligned}$$

$$\begin{aligned} & \sum_{k \in \mathcal{M}_4^{(2)}(X)} h(k) \operatorname{Reg}(k) \\ & \sim \frac{1}{48\pi^2} \cdot \prod_p \left(\frac{p^{12} + p^{11} + 3p^{10} + 3p^9 - 4p^7 - 5p^6 - 3p^5 + p^4 + 3p^3 + 2p^2 - 1}{p^{12} + p^{11} - p^9 - 2p^8 - p^7 + p^5 + p^4} \right) \cdot X^{3/2} \end{aligned}$$

In [101], Siegel actually gives two proofs of Theorem 36. In one, he uses the geometry of numbers and the correspondence between ideal classes in quadratic rings and equivalence classes of binary quadratic forms. This technique will be the focus of this chapter and the next. In Chapter 4 we will focus on his other method of proof, which involves averaging the

values of $L(1, \mathcal{O})$ where $L(s, \mathcal{O})$ is a certain L -function attached to the order $\mathcal{O}$.

In our geometry of numbers proof, we will employ a space studied by Bhargava in [10]. This “higher composition law” gives an explicit parameterization of ideal classes in *cubic* rings in terms of orbits of $\mathrm{GL}_2 \mathbb{Z} \times \mathrm{SL}_3 \mathbb{Z} \times \mathrm{SL}_3 \mathbb{Z}$ on $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$. This parameterization is reviewed in Sections 2.5 and 2.6, and our proof is given in Section 2.8 with some necessary computations performed in Section 2.7.

Throughout the course of this proof, we are actually able to recover another theorem. Specifically, recall that a fractional ideal I of an order $\mathcal{O}$ is *proper* whenever $(I : I) = \{x \in \mathcal{O} \otimes \mathbb{Q} : xI \subseteq I\} = \mathcal{O}$. Of course, being an ideal of $\mathcal{O}$ is equivalent to the assertion that $\mathcal{O} \subseteq (I : I)$, but if $\mathcal{O}' \subseteq \mathcal{O}$ is a suborder, then any ideal of $\mathcal{O}$ is also an (improper!) ideal of $\mathcal{O}'$.

Theorem 41. *For an order $\mathcal{O}$ in a number field, let $\bar{h}(\mathcal{O})$ be the total number of proper ideal classes of $\mathcal{O}$. Then*

$$\begin{aligned} \sum_{\mathcal{O} \in \mathcal{F}_3^{(0)}(X)} \bar{h}(\mathcal{O}) \mathrm{Reg}(\mathcal{O}) &\sim \frac{1}{72} \cdot \prod_p \frac{p^6 + p^5 + 3p^4 + 3p^3 + p + 1}{p^2(p^2 - 1)(p^2 + p + 1)} \cdot X^{3/2}, \text{ and} \\ \sum_{\mathcal{O} \in \mathcal{F}_3^{(1)}(X)} \bar{h}(\mathcal{O}) \mathrm{Reg}(\mathcal{O}) &\sim \frac{1}{12\pi} \cdot \prod_p \frac{p^6 + p^5 + 3p^4 + 3p^3 + p + 1}{p^2(p^2 - 1)(p^2 + p + 1)} \cdot X^{3/2}. \end{aligned}$$

We will return to the second method of proof, which actually allows us to prove facts about the *distribution* of $L(1, k)$ for k an S_n number field, in the next part of this thesis.

We would also like to note that there are two other known spaces on which we can apply similar geometry of numbers techniques. One is the space of binary quadratic forms which Siegel exploited in [101]. The other is the space of so-called $2 \times 2 \times 2$ boxes which Bhargava produced in [9]. While these results are subsumed by Theorem 120 of Chapter 4, the method of proof is sufficiently interesting that we have devoted Chapter 3 to its explication. Chapter 3 also contains an explanation of why it will be difficult (though, as

[20] indicates, certainly not impossible) to find more prehomogeneous vector spaces to which these techniques may be directly applied.

Authorship Disclaimer

This chapter, in particular, is joint work with my adviser and appears here to give future readers an overall picture of techniques available to the study of rank n rings.

2.2 Ideal Classes in Nonmaximal Orders

Traditionally, algebraic number theory texts only cover ideal classes in *maximal* orders of number fields. There it is proven that there are a finite number of ideal classes, that every ideal is invertible, and that every ideal has a unique factorization into powers of prime ideals. If instead one examines the *nonmaximal* orders of a number field, only the first of these assertions remains true.

In this section, we describe briefly the theory of ideals in nonmaximal orders, insofar as we will need for this thesis. In particular, we will show that the number of ideal classes in any order is finite, as well as give a characterization of invertible ideals. We will also discuss the notion of a *proper ideal* and the notion of a *weak inverse*.

In preparing this section, we relied heavily on [36, Section 7] and [93, Section I.12]. In particular, any omitted proof may be found in [93]. However, not all of the material appearing here may be found in [93].

2.2.1 An overview of commutative monoids

In what follows, we will be dealing with a commutative monoid M . This is a set along with a binary operation $M \times M \rightarrow M$ which is commutative, associative, and for which there

exists a unit $e \in M$ with $em = me = m$ for all $m \in M$. Note that what separates a monoid from a group is the lack of inverse elements.

Example 42. The natural numbers $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}$ form a monoid under addition. The positive integers $\mathbb{Z}_{>0} = \{1, 2, \dots\}$ form a commutative monoid under multiplication. Our most important example will be the monoid of (fractional) ideals $\mathcal{J}(\mathcal{O})$ under multiplication in an order $\mathcal{O}$ of a number field k .

The category of commutative monoids is *not* abelian. In particular, quotients by submonoids do not necessarily exist! However, if $G \subseteq M$ is a *subgroup*, then there is a well-defined categorical quotient M/G . For being in the same G -coset is an *equivalence relation*. Reflexivity follows from the fact that $e \in G$. Transitivity follows for if $m, n, p \in M$ and $g, h \in G$ such that $m = ng$ and $n = ph$ then $m = pgh$. But *symmetry* is where the group aspect comes in: if $m = ng$ then $n = mg^{-1}$. This equivalence relation allows us to construct the set M/G and after that, the proof of the existence of quotients follows as usual.

Example 43. Consider $\mathcal{J}(\mathcal{O})$ as in the previous example. Let $\mathcal{P}(\mathcal{O})$ be the submonoid of *principal* ideals. But a principal ideal is obviously invertible, so it makes sense to define the *ideal class monoid* $\mathcal{I}(\mathcal{O}) = \mathcal{J}(\mathcal{O})/\mathcal{P}(\mathcal{O})$. The rest of this section will be devoted to the study of this object.

2.2.2 Invertible Ideals

For any (fractional) ideals I, J of $\mathcal{O}$, let $(I : J) = \{x \in k : xJ \subseteq I\}$. If $\mathcal{O} = \mathcal{O}_k$ is maximal, then $I^{-1} = (\mathcal{O}_k : I)$. Indeed, we define an ideal I to be *invertible* whenever there exists an ideal J such that $IJ = \mathcal{O}$. Then it is easy to show that $J = (\mathcal{O} : I)$. The following is well-known and is part of a much more general phenomenon (see, e.g., [66, Exc. II.5.1]). Recall that for any property P of an $\mathcal{O}$ module, $\mathcal{O}$ is *locally* P if $\mathcal{O}_{\mathfrak{q}}$ is for every prime $\mathfrak{q}$ of $\mathcal{O}$.

Lemma 44. *For a fractional ideal I of $\mathcal{O}$, the following are equivalent:*

- I is invertible,
- I is locally free,
- I is locally principal,
- I is a projective $\mathcal{O}$ module.

This lemma allows one to prove many pleasant properties of the subgroup $\mathcal{J}'(\mathcal{O}) \subseteq \mathcal{J}(\mathcal{O})$ of invertible ideals. For instance, for any two invertible I and J we have that the norm $\mathfrak{N}(IJ) = \mathfrak{N}(I)\mathfrak{N}(J)$. This is *not* true¹ of more general ideals! Moreover, it allows us to prove the following proposition, which gives a hint of the idèles.

Proposition 45. *There is a norm preserving isomorphism $\mathcal{J}'(\mathcal{O}) \rightarrow \bigoplus_{\mathfrak{q}} \mathcal{P}(\mathcal{O}_{\mathfrak{q}})$ where $\mathcal{P}(\mathcal{O}_{\mathfrak{q}})$ is the set of principal ideals in $\mathcal{O}_{\mathfrak{q}}$, the completion of $\mathcal{O}$ at a prime $\mathfrak{q}$.*

Let $\text{Pic}(\mathcal{O}) = \mathcal{J}'(\mathcal{O})/\mathcal{P}(\mathcal{O})$ be the *ideal class group* of $\mathcal{O}$. Moreover, we define the (absolute) conductor $\mathfrak{f}$ of $\mathcal{O}$ in $\mathcal{O}_k$ to be the largest integral ideal of $\mathcal{O}_k$ which is also contained in $\mathcal{O}$.

Proposition 46. *Every ideal which is coprime to the conductor $\mathfrak{f}$ of $\mathcal{O}$ in $\mathcal{O}_k$ is invertible. Moreover, every ideal class in $\text{Pic}(\mathcal{O})$ has a representative coprime to $\mathfrak{f}$, and indeed, coprime to $\mathfrak{N}(\mathfrak{f})$.*

We may combine this proposition and a few other nontrivial results to prove the following theorem.

Theorem 47. *For any order $\mathcal{O}$ in a number field, $\text{Pic}(\mathcal{O})$ is finite.*

Proof. From Proposition 46 we know that $\text{Pic}(\mathcal{O}) \subseteq \text{Pic}(\mathcal{O}[1/\mathfrak{N}(\mathfrak{f})])$, the ring in which we invert all primes p which divide $\mathfrak{N}(\mathfrak{f})$. But $\mathcal{O}[1/\mathfrak{N}(\mathfrak{f})] = \mathcal{O}_k[1/\mathfrak{N}(\mathfrak{f})]$ as they are equal everywhere locally. So this group, in turn, is a subgroup of $\text{Pic}(\mathcal{O}_k)$, where $\mathcal{O}_k$ is the maximal

¹Consider the primes above 2 in $\mathbb{Z}[\sqrt{-3}]$.

order of $k = \mathcal{O} \otimes \mathbb{Q}$. This is just the class group of the number field k , which is well-known to be finite. $\square$

2.2.3 Noninvertible ideals

While this covers the class *group* of an order in a number field, we will be interested in the larger ideal class *monoid*. Let us start with a lemma showing that this problem is tractable.

Lemma 48. $\mathcal{I}(\mathcal{O})$ is finite.

Proof. Since $\text{Pic}(\mathcal{O})$ is finite, it suffices to show that $\mathcal{I}(\mathcal{O})/\text{Pic}(\mathcal{O})$ is finite. Let $I \subseteq \mathcal{O}$ be an integral representative of a fractional ideal class in $\mathcal{I}(\mathcal{O})$. Then $I\mathcal{O}_k$ is invertible in $\mathcal{O}_k$. Let $\bar{J} \subseteq \mathcal{O}_k$ be an ideal which is coprime to the conductor $\mathfrak{f}$ of $\mathcal{O} \subseteq \mathcal{O}_k$ and such that $I\bar{J} = a\mathcal{O}_k$ is principal. Then let $J = \mathcal{O} \cap \bar{J}$. Since J is coprime to the conductor, we know that J is invertible in $\mathcal{O}$ (Proposition 46). Moreover, we know that $J\mathcal{O}_k = \bar{J}$ since they are equal everywhere locally. As such, since we are proving $\mathcal{I}(\mathcal{O})/\text{Pic}(\mathcal{O})$ is finite, we may replace I by IJ .

Then $I\mathcal{O}_k = a\mathcal{O}_k$ is principal. Let $M = (1/a)I$ so that

$$\mathcal{O}_k \supseteq M \supseteq M\mathfrak{f} = M(\mathcal{O}_k\mathfrak{f}) = \mathfrak{f}$$

where $\mathfrak{f} = (\mathcal{O} : \mathcal{O}_k)$ is the *conductor of $\mathcal{O}$ in $\mathcal{O}_k$* . So we have shown that I has a representative between $\mathcal{O}_k$ and $\mathfrak{f}$. Since $\mathcal{O}_k/\mathfrak{f}$ is finite, we have completed the proof. $\square$

Now we would like to introduce a different adjective to describe ideals of $\mathcal{O}$. In general since I is an ideal, we know that $(I : I) = \{x \in k : xI \subseteq I\}$ is a ring containing $\mathcal{O}$. However, $(I : I)$ might be strictly larger than $\mathcal{O}$. We say that an ideal is *proper* whenever $(I : I) = \mathcal{O}$. This condition is obviously invariant under the action of principal $\mathcal{O}$ ideals. For example, the conductor $\mathfrak{f}$ of $\mathcal{O}$ in $\mathcal{O}_k$ is by definition proper if and only if $\mathcal{O} = \mathcal{O}_k$. All other ideals are called *improper*.

Lemma 49. *Invertible ideals are proper.*

Proof. From Proposition 46, we may choose an integral representative of I which is coprime to the absolute conductor of $\mathcal{O} \subseteq \mathcal{O}_k$ and as such has norm coprime to the *index* of $\mathcal{O}$ in $\mathcal{O}_k$. However, since I is an integral ideal of $\mathcal{O}$ it is certainly an integral ideal of $(I : I)$. Now we may define $\mathfrak{f}$ to be the *relative* conductor of $\mathcal{O}$ in $(I : I)$, i.e., the largest integral $(I : I)$ ideal which is contained in $\mathcal{O}$. This is nonzero and has norm which is *not* coprime to the index. On the other hand, $I \subseteq \mathfrak{f}$. Hence the norm of I is *not* coprime to the index of $\mathcal{O}$ in $\mathcal{O}_k$ unless $\mathcal{O} = (I : I)$. $\square$

Recall that to any rank n ring R over a PID B we may define the *dual module* of an R -module M to be $\text{Hom}(M, B)$. We say that the ring R is *Gorenstein* when $R^\vee$ is a projective R -module, or what is the same, when R is an injective R -module. Since everything in sight is Noetherian, this is actually a local condition.

Example 50. Maximal rings are Gorenstein since every fractional ideal is projective. Moreover, if $\mathcal{O}$ is *imprimitive*, i.e., $\mathcal{O} = \mathbb{Z} + n\mathcal{O}'$ for some $n > 1$ and some other ring $\mathcal{O}'$, and the rank d of $\mathcal{O}'$ is at least 3, then $\mathcal{O}$ is *not* Gorenstein. For then

$$\mathcal{O} \otimes \mathbb{F}_p = \mathbb{F}_p[x_1, \dots, x_{d-1}] / (x_1, \dots, x_{d-1})^2$$

for any $p \mid n$, and this ring is easily seen to be non-Gorenstein. In fact, a cubic ring is Gorenstein if and only if it is primitive [56, Theorem 5.12].

On the other hand, every monogenic order in a number field is Gorenstein (for a map $\mathbb{Z}[x] \rightarrow \mathbb{Z}$ is determined by the images of $1, x$, and x^2 , and so $\text{Hom}(\mathbb{Z}[x], \mathbb{Z})$ is generated by the map which sends 1 to 1 and x and x^2 to 0), hence every nondegenerate quadratic ring is Gorenstein.

Lemma 51. *An order $\mathcal{O}$ in a number field is Gorenstein if and only if every proper ideal is invertible.*

Proof. It follows from [56, Lemma 5.4] that every proper ideal in a Gorenstein order is invertible. For the other direction, note that $\text{Hom}(\mathcal{O}, \mathbb{Z})$ is always proper. For if $x/p \in (\mathcal{O}^\vee : \mathcal{O}^\vee)$ with $1, x, x_2, \dots, x_{d-1}$ a basis of $\mathcal{O}$, then for *every* $\varphi \in \text{Hom}(\mathcal{O}, \mathbb{Z})$ and $y \in \mathcal{O}$ we must have that $\varphi(xy) \in p\mathbb{Z}$. But in particular, if φ is the map which sends x to 1 and x_i and 1 to 0, then $\varphi(x \cdot 1) = 1$. As such, since we are assuming that every proper ideal is invertible, $\text{Hom}(\mathcal{O}, \mathbb{Z})$ is invertible and hence projective. $\square$

2.2.4 Weak Inverses and Regulators

Even if an ideal is noninvertible, then it can almost admit an inverse. In particular, we say that an ideal I' is a *weak inverse* of an ideal I of an order $\mathcal{O}$ whenever $II' \subseteq \mathcal{O}$ and $\mathfrak{N}(I)\mathfrak{N}(I') = 1$. Of course, if I is invertible, then these two conditions together imply that $I' = I^{-1}$. On the other hand, if I is not invertible, then an ideal can have many weak inverses, as we will see in Corollary 75.

Now for any order $\mathcal{O}$ in a number field, we may define the regulator $\text{Reg}(\mathcal{O})$ as follows. Let $\sigma = (r_1, r_2)$ be the *signature* of k , i.e., r_1 (resp. r_2) is the number of copies of $\mathbb{R}$ (resp. $\mathbb{C}$) in $k \otimes_{\mathbb{Q}} \mathbb{R}$. Let $r = \#\sigma = r_1 + r_2$. If $\mathcal{O}$ were maximal, then Dirichlet's Unit Theorem would immediately imply that $\mathcal{O}^\times \cong \mu(\mathcal{O}^\times) \times \mathbb{Z}^{r-1}$ where $\mu(\mathcal{O}^\times)$ are the roots of unity in $\mathcal{O}$. For nonmaximal orders, let $\mathcal{O}_k$ be the maximal order containing $\mathcal{O}$. Then by Theorem I.12.9 of [93] we know that $\mathcal{O}_k^\times / \mathcal{O}^\times$ injects into $(\mathcal{O}_k/\mathfrak{f})^\times / (\mathcal{O}/\mathfrak{f})^\times$, which is finite since $\mathcal{O}_k/\mathfrak{f}$ is. Hence, $\mathcal{O}^\times$ has finite index in $\mathcal{O}_k^\times$ and so $\mathcal{O}^\times \cong \mu(\mathcal{O}^\times) \times \mathbb{Z}^{r-1}$ as well. From here, we define the regulator as usual: For each of the r (conjugate sets of) maps $\sigma_i : k \hookrightarrow \mathbb{C}$ for $x \in k$ let

$$\|x\|_i = \begin{cases} |\sigma_i(x)| & \sigma_i \text{ is real} \\ 2|\sigma_i(x)| & \sigma_i \text{ is complex} \end{cases}$$

Then we define the *regulator* $\text{Reg}(\mathcal{O})$ of $\mathcal{O}$ to be the absolute value of the determinant of

any of the $(r-1) \times (r-1)$ minors of the matrix

$$\begin{pmatrix} \log \|\varepsilon_1\|_1 & \log \|\varepsilon_2\|_1 & \cdots & \log \|\varepsilon_{r-1}\|_1 \\ \log \|\varepsilon_1\|_2 & \log \|\varepsilon_2\|_2 & \cdots & \log \|\varepsilon_{r-1}\|_2 \\ \vdots & \vdots & \ddots & \vdots \\ \log \|\varepsilon_1\|_r & \log \|\varepsilon_2\|_r & \cdots & \log \|\varepsilon_{r-1}\|_r \end{pmatrix}.$$

To a pair (I, I') where I' is a weak inverse of I , we associate the ring $\rho = \rho(I, I') = (I : I) \cap (I' : I')$. Since $\rho(I, I^{-1}) = \mathcal{O}$ for all invertible ideals I , we see that $\text{Reg}(I) = \text{Reg}(\rho(I, I^{-1}))$ is well-defined for invertible ideals. More generally, if I is a proper ideal of $\mathcal{O}$, then $(I : I) = \mathcal{O}$. Since any weak inverse I' of I is an ideal of $\mathcal{O}$, we then have that $\rho(I, I') = \mathcal{O}$. In particular, $\text{Reg}(I) = \text{Reg}(\rho(I, I'))$ is well-defined for any *proper* ideal and is equal to $\text{Reg}(\mathcal{O})$, assuming that a weak-inverse exists (which is guaranteed by Cor 75).

Remark 52. If $\mathcal{O}$ is an order in a quadratic number field or a primitive order in a cubic number field, then Lemma 51 and Example 50 imply that $\bar{h}(\mathcal{O}) = h(\mathcal{O})$ where $\bar{h}(\mathcal{O})$ is the total number of proper ideal classes of $\mathcal{O}$. As such, we immediately have from the Siegel bound that $\bar{h}(\mathcal{O}) \text{Reg}(\mathcal{O}) = O(\Delta(\mathcal{O})^{1/2+\varepsilon})$.

2.3 Some Facts about Regulators

In this section, we recall some basic facts about $h(\mathcal{O}) \text{Reg}(\mathcal{O})$, relating it to certain ζ functions and Artin L -functions. Most of this material is standard, and a more thorough reference may be found in [93, Chapter 7]. As for the analytic theory of zeta functions of nonmaximal orders, our proofs were motivated by Cohn's [35, Chapter 13] overview of the quadratic case, which we later found had been developed further by Bushnell and Reiner under the heading *Solomon's Conjecture for noncommutative orders*. See [27, 28] for the relevant original sources, and [29] for an overview Bushnell and Reiner prepared for a conference at

Oberwolfach.

2.3.1 Dedekind zeta functions and Artin L functions

Suppose k is a number field with ring of integers $\mathcal{O}_k$. Then we may define the *Dedekind zeta function*

$$\zeta_k(s) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_k} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}} = \sum_{\mathfrak{a} \subseteq \mathcal{O}_k} \mathfrak{N}(\mathfrak{a})^{-s} \quad (2.1)$$

where $\mathfrak{N}$ is the norm map from ideals of $\mathcal{O}_k$ to positive integers, the product is taken over all prime ideals of $\mathcal{O}_k$ and the sum is taken over all (integral) ideals of $\mathcal{O}_k$. The following well-known theorem summarizes the basic properties of ζ_k .

Theorem 53. *The sum and product in (2.1) converge for the real part of $s > 1$. Moreover, $\zeta_k(s)$ may be meromorphically continued to the entire complex plane with a unique simple pole at $s = 1$. The residue at that pole is precisely*

$$\text{Res}_{s=1} \zeta_k(s) = \frac{\pi^\sigma h(k) \text{Reg}(k)}{w_k \sqrt{\Delta(k)}} \quad (2.2)$$

where

- σ is the signature of k ,
- $\pi^\sigma = 2^{r_1} (2\pi)^{r_2}$ where r_1 is the number of real places of k and r_2 are the number of (conjugate pairs of) complex places of k ,
- w_k is the number of roots of unity contained in the ring of integers $\mathcal{O}_k$, and
- $\Delta(k) = |\text{Disc}(k)|$ is the norm of the discriminant of k .

It turns out that the representation theory of finite groups allows us to factor the Dedekind zeta function into a product of Artin L -functions attached to Galois representations. Recall that if $k/\mathbb{Q}$ is a field extension with Galois closure K and $G = \text{Gal}(K/\mathbb{Q})$ and

$H = \text{Gal}(K/k) \leq G$, then

$$\zeta_k(s) = \prod_{\rho} L(\rho, s)^{\dim W^H}$$

where (ρ, W) runs over the irreducible representations of G and W^H is the subspace of invariant vectors, and $L(\rho, s)$ is the Artin L -function attached to (ρ, W) . Notably, the Riemann zeta function $\zeta(s) = L(\mathbb{1}, s)$ divides $\zeta_k(s)$. Write $L(k, s) = \zeta_k(s)/\zeta(s)$. Since $\text{Res}_{s=1} \zeta(s) = 1$, Theorem 53 may be rewritten to say $L(k, 1)$ is *equal to* the right hand side of (2.2).

In particular, if k is a degree d number field with Galois group S_d , then $L(k, s) = L(\rho, s)$ where ρ is the standard representation of S_d in $\text{GL}_{d-1}(\mathbb{C})$. For any prime $p \in \mathbb{Z}$, let $\tau(p) = (f_1^{e_1} f_2^{e_2} \cdots)$ be the splitting type of p in $\mathcal{O}_k$. That is, $p\mathcal{O}_k = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots$ where $\mathfrak{p}_i$ are primes and $\mathcal{O}_k/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}$. From this information, one may compute the local L -factors $L_p(k, s) = L_p(\rho, s)$ for $\Re(s) > 1$.

Writing $L(k, s) = \sum_{n=1}^{\infty} a_n(k) n^{-s}$, we see from the definition that the a_n are multiplicative functions, i.e., $a_m a_n = a_{mn}$ for m and n coprime. For k a degree d field, we have that $a_{p^e} = O(\log(p^e))$ and since the number of divisors of n is $\ll n^\varepsilon$ we have that $a_n = O(n^\varepsilon)$. This may be seen directly for the quadratic and cubic cases by examining Tables 4.1 and 4.2.

2.3.2 The Strong Artin Conjecture

Artin conjectured that $L(\rho, s)$ admits an analytic continuation to the whole complex plane whenever $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}(W)$ does not contain a trivial representation (and a meromorphic continuation when it does). The method by which this has always been proved is to show that $L(\rho, s)$ is *modular*, that is, that there exists an automorphic representation $\pi(\rho)$ such that $L(\rho, s) = L(\pi(\rho), s)$ (up to appropriate normalizations of the Fourier coefficients). This is called the *Strong Artin Conjecture*. As discussed in the introduction, it is known when the image of ρ is solvable and a few other sporadic cases.

An important consequence of this conjecture is that the Dirichlet series $\sum a_n(k)n^{-s}$ converges a little to the left of the line $\Re(s) = 1$. In fact, when k is a cubic field, then using the functional equation of $L(\rho, s)$ and a method of Landau and Walfisz [82, 109, 32] one sees that the tail sum

$$\sum_{n \geq X} a_n(k) = O(\Delta(k)^{1/2+\varepsilon} X^{-2/3}) \quad (2.3)$$

with the implied constant being independent² of k and depending only on ε . Then by partial summation, one can show that $\sum a_n(k)n^{-s}$ converges when $\Re(s) > 1/3$. For higher degree automorphic representations, one must use the detailed study of this argument in [33].

Our most important application of the Strong Artin Conjecture will be to prove certain zero density results in the spirit of Barban [4]. We shall return to this in Section 4.3.

2.3.3 Zeta functions of nonmaximal orders

As is obvious from the definition, the zeta function of a number field k is really an *integral* construction, i.e., it is attached to the ring of integers $\mathcal{O}_k$ of k . As such, we might try to define a zeta function of *nonmaximal* orders in number fields. A naïve definition might be to define $\zeta_{\mathcal{O}}(s) = \sum_{\mathfrak{a}} \mathfrak{N}(\mathfrak{a})^{-s}$ where the sum is over all integral ideals of $\mathcal{O}$. But it is rather difficult to get a handle on $\mathcal{I}(\mathcal{O})$, the full ideal class monoid of $\mathcal{O}$.

Instead, we are led to study

$$\zeta_{\mathcal{O}}(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O} \\ \mathfrak{a} \text{ invertible}}} \frac{1}{\mathfrak{N}(\mathfrak{a})^{-s}}. \quad (2.4)$$

As we will see, this may be divided into an Euler product which differs from ζ_k at a finite number of places. Examining the Euler factors, the meromorphicity in the following proposition is nearly immediate. As for the residue, the same proof used to demonstrate

²None of Landau, Walfisz, and Chandrasekharan–Narasimhan explicitly address how (2.3) depends on k , instead only giving a right hand side that looks like $O_k(X^{-2/3})$ as $n \rightarrow \infty$. In tracing through their proofs and keeping track of the k -dependence yields the displayed expression above.

Theorem 53 yields the following analogue.

Proposition 54. *The sum (2.4) converges for the real part of $s > 1$. Moreover, $\zeta_{\mathcal{O}}(s)$ may be meromorphically continued to the whole complex plane. Then $\zeta_{\mathcal{O}}$ has a single pole, a simple pole located at $s = 1$ with residue*

$$\frac{\pi^{\sigma} h(\mathcal{O}) \operatorname{Reg}(\mathcal{O})}{w_{\mathcal{O}} \sqrt{\Delta(\mathcal{O})}}$$

Now we would like to build an Euler product for $\zeta_{\mathcal{O}}$. As we saw in Section 2.2, invertible ideals are determined by their localizations at all primes, which in each case is principal. Moreover, since each $\mathcal{O}_q = \mathcal{O} \otimes \mathbb{Z}_q$ is an order in an étale algebra over $\mathbb{Q}_q$, we know that the localization at each prime ideal $\mathfrak{q}|q$ of $\mathcal{O}_q$ must be an order in a separable *field extension* of $\mathbb{Q}_q$. In particular, the q th factor of $\zeta_{\mathcal{O}}$ can be written as a product of $\mathfrak{q}|q$ as

$$\prod_{\mathfrak{q}|q} \sum_{(a) \subseteq \mathcal{O}_{\mathfrak{q}}} \mathfrak{N}(a)^{-s} \quad (2.5)$$

where the sum is over all principal ideals of $\mathcal{O}_{\mathfrak{q}}$, the completion of the localization of $\mathcal{O}$ at the prime $\mathfrak{q}$. So our task is reduced to the following lemma. To state it, let $\mu_{\mathcal{O}_q}$ be an additive Haar probability measure on $\mathcal{O}_q$. Note that $\mu_{\mathcal{O}_q}(\mathcal{O}_q^{\times})$ depends only on the structure of $\mathcal{O}/(q)$. In particular, if we write $\mathcal{O}/(q) = F_1 \times F_2 \times \cdots$ as a product of connected Artinian algebras over $\mathbb{F}_q$, and we let F_i^0 be the fields which are F_i modulo their nilpotents, then

$$\mu_{\mathcal{O}_q}(\mathcal{O}_q^{\times}) = \prod \frac{\#(F_i^0)^{\times}}{\#F_i^0}. \quad (2.6)$$

In analogy of the global regulator, we define $\operatorname{Reg}_q(\mathcal{O})$ to be equal to (2.6).

Lemma 55. *The value (2.5) when $s = 1$ is equal to $\mu_{\mathcal{O}_q}(\mathcal{O}_q^{\times})^{-1}$.*

Proof. In the definition of (2.5) we have already broken up the local factor into a product depending only on a given prime ideal $\mathfrak{q}$. Moreover, as noted in the previous paragraph, the

total $\mu_{\mathcal{O}_q}(\mathcal{O}_q^\times)$ depends only on $\mathcal{O}_q/(q)$ which in turn may be written as $\prod_{q|q} \mathcal{O}_q/(q)$ by the Chinese Remainder Theorem. So to prove the lemma it suffices to prove the claim for each prime q .

Defining $\mathfrak{N}(0)^{-1} = 0$, we may rewrite the sum in (2.5) as

$$\sum_{a \in \mathcal{O}_q / \mathcal{O}_q^\times} \mathfrak{N}(a)^{-s}$$

where a runs over a set of representatives of the cosets of the action of $\mathcal{O}_q^\times$ on $\mathcal{O}_q$. But then we may average over $\mathcal{O}_q^\times$ and switch the order of summation and integration to arrive (when $s = 1$) at

$$\mu_{\mathcal{O}_q}(\mathcal{O}_q^\times) \sum_{a \in \mathcal{O}_q / \mathcal{O}_q^\times} \mathfrak{N}(a)^{-1} = \int_{x \in \mathcal{O}_q^\times} \sum_{a \in \mathcal{O}_q / \mathcal{O}_q^\times} \mathfrak{N}(ax)^{-1} d\mu_{\mathcal{O}_q}(x) = \int_{a \in \mathcal{O}_q} d\mu_{\mathcal{O}_q}(a) = 1.$$

Hence the claim. □

Remark 56. As mentioned in the introduction to this section, there was much interest in this subject 30 years ago, led especially by Bushnell and Reiner under the heading of *Solomon's Conjecture*. The above proof, for instance, is rather close to a specific case of Section 2 of [27] and this whole subsection may be viewed as a special case of [28].

2.4 The density of discriminants

In this section, we recall what is known about counts of number fields by discriminant.

We begin with a folk conjecture we call the Number of Number Fields Conjecture (or NNF for short). The exact form we state is due to Malle [90]. It concerns asymptotics of counts of number fields. To state it, we need some notation. Recall that if a group G acts

on a set Ω , then the *index* $\text{ind}(g)$ of $g \in G$ is

$$\text{ind}(g) = \#\Omega - \#(\Omega/(g))$$

where $(g) \subseteq G$ is the cyclic subgroup generated by g and $\Omega/(g)$ is the set of orbits of this subgroup. Note that $\text{ind}(g) = \text{ind}(g')$ if g is conjugate to g' , so we say that $\text{ind}(C)$ of a conjugacy class $C \subseteq G$ is the index of any of its elements. Now suppose that $\Omega = \{1, \dots, d\}$ so that $G \subseteq S_d$. Then $\text{ind}(G) = \text{ind}(G \subseteq S_d)$ is the minimum index of all of its nontrivial conjugacy classes. Let $a(G) = \text{ind}(G)^{-1}$.

Example 57. Note that $a(G) = 1$ if and only if G contains a transposition. In particular, $a(S_d) = 1$ and $a(D_4) = 1$. On the other hand, if $G = C_d$ is cyclic, then $a(C_d) = 1/(d-1)$.

Recall that if G is a finite group, then its character table is a square matrix whose rows are indexed by the irreducible representations of G and whose columns are indexed by the conjugacy classes of G . Moreover, it is a beautiful exercise to prove that for any number field k , the absolute Galois group $G_k = \text{Gal}(\bar{\mathbb{Q}}/k)$ permutes the columns of the character table, and hence permutes the conjugacy classes. This action preserves the index of the conjugacy class, and so it makes sense to define the set of orbits $\{C \subseteq G \text{ conjugacy classes} : \text{ind}(C) = \text{ind}(G)\}/G_k$. Then $b(k, G)$ is the cardinality of this set.

Example 58. For instance, when p is a prime, $G = C_p \subseteq S_p$ is a cyclic subgroup, and $k = \mathbb{Q}$, then $b(\mathbb{Q}, C_p) = 1$. However, $b(\mathbb{Q}(\zeta_p), C_p) = p-1$ where ζ_p is a nontrivial p th root of unity.

Conjecture 59 (Number of Number Fields Conjecture (NNF)). *Let $\mathcal{M}_X = \mathcal{M}(X; d, G, \sigma)$ consisting of all number fields k over a base number field K with degree $d > 0$, Galois group G , and signature σ . Then there exists $c = c(K, d, G, \sigma)$ such that*

$$\sum_{k \in \mathcal{M}_X} 1 \sim c X^{a(G)} \log^{b(K, G)-1} X.$$

Note that Malle does not predict the constant c . Rather, this is the topic of Ellenberg and Venkatesh's work [51], which was inspired by Bhargava's [13], which in turn only covers S_d extensions. However, the general heuristic of Ellenberg and Venkatesh is rather complicated, and so we restrict our attention to Bhargava's much simpler heuristic for S_d extensions. Informally, this states that the expected weighted number of degree d extensions of $\mathbb{Q}$ of discriminant D is equal to product of the total weighted number of discriminant-compatible extensions of degree d of $\mathbb{Q}_p$ where p ranges over all finite and infinite places.

Here a *degree d extension of $\mathbb{Q}_p$* is simply an étale algebra of degree d over $\mathbb{Q}_p$. A degree d extension L of $\mathbb{Q}_p$ is *discriminant-compatible* with D if $v_p(D) = v_p(\text{Disc}_p(L))$ for all finite primes. If $p = \infty$, then the condition is that the sign of the discriminants match. By *weighted* we mean that we count each extension with weight $(\# \text{Aut}_{\mathbb{Q}_p}(L))^{-1}$, and similarly for global extensions. So for instance, cyclic cubic fields over $\mathbb{Q}$ are counted with weight $1/3$ whereas non-Galois cubic fields are counted with weight 1 . Similarly, $\mathbb{R}^3/\mathbb{R}$ is counted with weight $1/6$ whereas $(\mathbb{R} \oplus \mathbb{C})/\mathbb{R}$ is counted with weight $1/2$.

In fact, Bhargava's heuristics say more. First, they actually are heuristics about degree d *rings* and they say that we should be able to make certain local specifications in the following sense. We say that a local condition Σ_p at a prime p of $\mathbb{Q}$ is a collection of rank d rings over $\mathbb{Z}_p$. We denote by $\Sigma = \{\Sigma_p\}$ a collection of local conditions, one for every (archimedean and non-archimedean) prime of $\mathbb{Q}$. Let $\mathcal{F}_\Sigma(X)$ denote the collection of all orders in degree d fields $k/\mathbb{Q}$ with Galois group S_d such that $\mathcal{O} \in \mathcal{F}_\Sigma(X)$ if and only if $\mathcal{O} \otimes \mathbb{Z}_p \in \Sigma_p$ for all p . We make the following slight modification of the definition of $\#\mathcal{F}_\Sigma(X)$:

Definition 60. Let $\mathcal{F}_\Sigma(X)$ be as above. Then

$$\#\mathcal{F}_\Sigma(X) = \sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} \frac{1}{\# \text{Aut}(\mathcal{O})}$$

Remark 61. In the case that Σ represents the collection of local specifications that $\mathcal{O}$ is *maximal* at every p , then we are counting each field with weight 1 *except* when $d = 2$ as quadratic fields are all Galois.

Conjecture 62 (Bhargava’s Heuristic for S_d [13]). *If Σ is a “good” collection of local specifications, then $\#\mathcal{F}_\Sigma(X) \sim c(\Sigma)X$, where*

$$c(\Sigma) = \left(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{\#\text{Aut}_{\mathbb{R}}(R)} \right) \prod_{p \text{ finite}} \frac{p-1}{p} \sum_{R \in \Sigma_p} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\#\text{Aut}(R/\mathbb{Z}_p)}$$

where $\text{Disc}_p(R)$ is the discriminant of R over $\mathbb{Z}_p$ as a power of p .

Remark 63. Some examples of conjectured “good” collections are the collection of all maximal algebras, the collection of all algebras with squarefree discriminant, and collections which differ from these at a finite number of places. The first of these collections is good for $d = 2, 3, 4, 5$ by [101, 58], [19], [11], [14], respectively. The squarefree case is known for $d = 2, 3$ by the same references.

Remark 64. For Galois groups which are not S_d , the naïve heuristic is that we should only allow those rings in the local specifications whose Galois groups are “compatible” with the global Galois group we are seeking. However, this is not quite right: there are correction factors due to the roots of unity in the base field as well as the Schur multiplier of the group. For more information, see [51] or [57] which relates the heuristics to statistics of random symplectic matrices.

For our purposes, we will need a bit more. In particular, we will require some knowledge of the error term in Conjecture 62. In particular, we will need a uniform power saving error term. Let Σ_p^{triv} (resp. Σ_p^{max}) be the collection of all (resp. maximal) degree d algebras over $\mathbb{Z}_p$ compatible with G . We say that a collection Σ is *almost trivial* (resp. *almost maximal*) whenever Σ differs from Σ^{triv} (resp. Σ^{max}) in at most finitely many primes. Let $\mathfrak{N}(\Sigma)$ be the product of those exceptional primes.

Conjecture 65 (NNF with a Power Saving for S_d). *Let Σ be an almost trivial (resp. almost maximal) collection of local specifications. Then exist $\gamma, \delta > 0$ uniform in Σ such that*

$$\#\mathcal{F}_\Sigma(X) = c(\Sigma)X + O\left(\mathfrak{N}(\Sigma)^\gamma X^{1-\delta}\right)$$

where the implied constant does not depend on Σ .

Theorem 66 ([6]). *NNF with a power saving error bound for S_d is known when $d = 2, 3, 4$.*

Remark 67. When $d > 7$, there is some doubt that Conjecture 65 for almost trivial local specifications. See the appendix to this chapter.

Remark 68. There is a related conjecture that can be made for other Galois groups, namely there should exist some function $f(X) = f(X; G, \Sigma) \sim c(G; \Sigma) \log^{b(k, G)-1} X$ such that if $\mathcal{F}_X(G; \Sigma)$ are those orders in fields with Galois group G and almost trivial or maximal local specifications Σ , then

$$\mathcal{F}_X(G; \Sigma) = Xf(X) + O\left(\mathfrak{N}(\Sigma)^\gamma X^{a(G)-\delta}\right)$$

where γ and δ are some positive numbers. This brings up the important point that what will be necessary for our computations is only the final error term, not any of the secondary main terms.

2.5 Binary cubic forms and cubic rings

We begin with our geometry of numbers method. In this section we briefly recall the relationship between cubic rings and binary cubic forms $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. We omit most proofs as they are beautifully presented in Sections 2 and 3 of [19].

2.5.1 The Delone-Fadeev Correspondence

For us, a *cubic ring* is a (commutative, associative, unital) $\mathbb{Z}$ -algebra which is free of rank 3 as a $\mathbb{Z}$ -module. In this section, we recall the correspondence of Delone-Fadeev³ [88, 42] (refined by Gan-Gross-Savin [55] and Wood [114]) between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral binary cubic forms, where $\mathbb{Z}$ is a PID. Let V be a rank 2 free $\mathbb{Z}$ -module and consider the representation $(\wedge^2 V)^\vee \otimes \mathrm{Sym}^3 V$. That is, if $f(x, y)$ is a binary cubic form, then the action of $\gamma \in \mathrm{GL}_2(\mathbb{Z}) = \mathrm{GL}(V)$ is given by

$$(\gamma \cdot f)(x, y) = \frac{1}{\det \gamma} f((x, y) \cdot \gamma). \quad (2.7)$$

If $f(x, y) = x^3 + bx^2y + cxy^2 + dy^3$, then we can form a cubic ring $R(f) = \mathbb{Z}[x]/(f(x, 1))$. For any $\mathrm{GL}_2(\mathbb{Z})$ transformation taking f to another monic form f' , we immediately see that $R(f) = R(f')$.

In fact, since $\mathbb{Z}$ is a PID, we may always assume that a cubic ring has a basis $(1, \omega, \theta)$. In fact, we may assume that $1, \omega, \theta$ are such that

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m + b\omega - a\theta \\ \theta^2 &= \ell + d\omega - c\theta \end{aligned} \quad (2.8)$$

for some $a, b, c, d, \ell, m, n \in \mathbb{Z}$. To such a cubic ring we associate the form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. Conversely, the associativity relations $(\omega\theta)\theta = \omega(\theta^2)$ and $(\omega^2)\theta = (\omega\theta)\theta$

³It has been pointed out by F. Lemmermeyer that F. Levi actually gave this correspondence [88] before Delone and Faddeev had written their book. Indeed, Delone and Faddeev even credit Levi for the result in their preface, but not in the main body of the text. Unfortunately, the name Delone-Faddeev correspondence has become standard, and so we will use it throughout this work.

show that

$$\begin{aligned} n &= -ad \\ m &= -ac \\ \ell &= -bd \end{aligned} \tag{2.9}$$

So to any binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ we associate the cubic ring $R(f)$ with basis $(1, \omega, \theta)$ and multiplication table determined by (2.8) and (2.9).

One checks that (2.8) and (2.9) actually define a commutative, associative, unital $\mathbb{Z}$ algebra of rank 3, and that the $\mathrm{GL}_2(\mathbb{Z})$ action on binary cubic forms (2.7) and the obvious action on $R(f)/\mathbb{Z} \cong \mathbb{Z}\omega \oplus \mathbb{Z}\theta$ are compatible. This proves the following theorem.

Theorem 69 (Delone-Fadeev Correspondence). *There is a natural bijection between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral binary cubic forms and isomorphism classes of cubic rings.*

Before moving on, we collect a few facts about this correspondence. First, there is a unique invariant of the action (2.7), namely the *discriminant*

$$\mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Moreover, to any cubic ring R there is a notion of discriminant $\mathrm{Disc}(R)$ familiar from elementary algebraic number theory. It turns out that $\mathrm{Disc}(R) = \mathrm{Disc}(R(f))$. Two other properties of f and $R(f)$ also correspond. First, $R(f)$ is an integral domain precisely when f is irreducible over $\mathrm{Frac}(\mathbb{Z})$. Second, $\mathrm{Aut}(R(f))$ is precisely the stabilizer of f in $\mathrm{GL}_2(\mathbb{Z})$.

Remark 70. In fact, the only property we have used in explicating the Delone–Fadeev Correspondence is the fact that $\mathbb{Z}$ is a PID. Indeed, one may replace every mention of $\mathbb{Z}$ in this section with any PID B .

2.5.2 The Davenport-Heilbronn Correspondence

We say a cubic ring is *maximal* when it is not contained in any other cubic ring. For instance, maximal cubic rings over $\mathbb{Z}$ which are also integral domains are the rings of integers of their fields of fractions. For this reason, it will be useful to know when $R(f)$ is maximal given only the binary cubic form f .

If R is a cubic ring over $\mathbb{Z}$, then it turns out that R is maximal if and only if $R_p = R \otimes \mathbb{Z}_p$ is maximal for every p . We have the following lemma.

Lemma 71 ([19, Lemma 13], [39]). *Suppose R is not maximal at p . Then there is $\mathbb{Z}$ basis $(1, \omega, \theta)$ such that either*

(i) $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot \theta \subseteq R \otimes \mathbb{Q}$ is a ring, or

(ii) $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot (\theta/p) \subseteq R \otimes \mathbb{Q}$ is a ring.

On the forms side, this says that $R(f)$ is nonmaximal at p if either f is a multiple of p or there is some $\mathrm{GL}_2(\mathbb{Z})$ transformation of f such that $p \mid b$ and $p^2 \mid a$.

2.6 The Hilbert-Burch Theorem and Ideals in Cubic Rings

One early lesson in algebraic geometry is that if a line bundle $\mathcal{L}$ of a scheme X is generated by global sections, then we get a map $X \rightarrow \mathbb{P}H^0(X, \mathcal{L})^\vee$. If B is a PID and R is a torsion free B algebra of rank r , then line bundles on $\mathrm{Spec} R$ correspond to ideal classes, which in turn are free of rank r over B . Thus, they yield an embedding $\mathrm{Spec} R \rightarrow \mathbb{P}_B^{r-1}$. Moreover, an embedding $\mathrm{Spec} R \rightarrow \mathbb{P}_B^{r-1}$ yields an ideal class. This is a canonical one-to-one correspondence.

In the case $r = 3$, we are dealing with cubic rings over a PID and $\mathrm{Spec} R$ is a codimension 2 subscheme of $\mathbb{P}_B^2$. If $B = k$ is a field and R is étale, then $\mathrm{Spec} R \subseteq \mathbb{P}_k^2$

consists of a dimension 0 scheme of degree 3, i.e., is geometrically a set of 3 points. But a quick application of the Auslander-Buchsbaum formula [46, Theorem A2.15] and the Hilbert-Burch theorem [46, Theorem 3.2] implies that *any* set of points in $\mathbb{P}^2$ is cut out by the $t \times t$ minors of a $(t + 1) \times t$ matrix of homogeneous forms for some t . From the Hilbert function, one may then compute that a general set of 3 points in $\mathbb{P}_k^2$, i.e. 3 points which span all of $\mathbb{P}_k^2$, is cut out by the 2×2 minors of a 2×3 matrix of linear forms on $\mathbb{P}_k^2$. In fact, from the uniqueness of minimal free resolutions, one quickly finds that to every embedding $\text{Spec } R \hookrightarrow \mathbb{P}_k^2$, there is a *unique* $\text{GL}_2 k \times \text{GL}_3 k \times \text{GL}_3 k$ orbit of 2×3 matrices of linear forms on $\mathbb{P}_k^2$ which corresponds to that embedding.

In fact, the Hilbert-Burch theorem can be pushed much farther, as explicated by Wood in her thesis [112]. We will use Bhargava's version of this theorem [10, Theorem 2] which inspired Wood. Stating this theorem and understanding its nuances occupies the rest of this section.

2.6.1 Bhargava's Boxes

Let $V_{\mathbb{R}} = \mathbb{R}^2 \otimes \mathbb{R}^3 \otimes \mathbb{R}^3$ and let $G_{\mathbb{R}} = \text{GL}_2 \mathbb{R} \times \text{SL}_3 \mathbb{R} \times \text{SL}_3 \mathbb{R}$ act on $V_{\mathbb{R}}$ with its natural action. We call elements $v \in V_{\mathbb{R}}$ $2 \times 3 \times 3$ boxes, or *boxes* for short. Moreover, we will often view $v \in V_{\mathbb{R}}$ as a pair of 3×3 matrices $v = (A, B)$, with the first $\text{SL}_3 \mathbb{R}$ acting on the left and the second $\text{SL}_3 \mathbb{R}$ acting on the right.

We may define $V_{\mathbb{Z}} \subseteq V_{\mathbb{R}}$ to be the lattice of integer points and $G_{\mathbb{Z}} \subseteq G_{\mathbb{R}}$ to be the subgroup $\text{GL}_2 \mathbb{Z} \times \text{SL}_3 \mathbb{Z} \times \text{SL}_3 \mathbb{Z}$. Then obviously $G_{\mathbb{Z}}$ preserves $V_{\mathbb{Z}}$. Moreover, the action of $G_{\mathbb{Z}}$ on $V_{\mathbb{R}}$ (or $V_{\mathbb{Z}}$) has a unique polynomial invariant, namely the degree 12 polynomial in 18 variables

$$\text{Disc}(A, B) = \text{Disc}(\det(Ax - By))$$

where the discriminant on the right is the discriminant of the binary cubic form $f(x, y) = \det(Ax - By)$. We will sometimes write this form as simply $f = \det(v)$.

An element $v \in V_{\mathbb{R}}$ is *degenerate* whenever $\text{Disc}(v) = 0$ and nondegenerate otherwise. It turns out that $V_{\mathbb{R}}$ has two nondegenerate orbits under the action of $G_{\mathbb{R}}$, which we call $V^{\pm}$ where V^+ (resp. V^-) is the orbit containing elements of positive (resp. negative) discriminant.

Now f is a binary cubic form, and we have just seen that to any binary cubic form we may associate a cubic ring $R(f)$. It turns out that an element $v = (A, B) \in V_{\mathbb{Z}}$ gives us a little extra data. The following is [10, Theorem 2].

Theorem 72. *There is a canonical bijection between the nondegenerate $G_{\mathbb{Z}}$ orbits on $V_{\mathbb{Z}}$ and the set of isomorphism classes of pairs $(R, (I, I'))$ where R is a cubic ring and I is a fractional ideal of R and I' is a weak inverse. Under this bijection, the discriminant of the box is equal to the discriminant of the cubic ring.*

Remark 73. In fact, the proof of Theorem 72 goes via a *rigidified* version of the theorem. That is, to a pair $v = (A, B) \in V_{\mathbb{Z}}$ Bhargava shows the existence of a canonical basis $(1, \omega, \theta)$ of $R(v)$ (as in Theorem 69) and a basis $\alpha_1, \alpha_2, \alpha_3$ of I and $\beta_1, \beta_2, \beta_3$ of I' in which the explicit action of R on I and I' can be computed. This may be found in equation (11) of [10]. As it will be important for us in the proof of Lemma 81, we list the action here for the convenience of the reader. In what follows, if M is a square matrix, we let M_i denote its i th column and $|M|$ denote its determinant. If M, M', M'' are 3×3 matrices, then $M_i M'_j M''_k$ will be the 3×3 matrix with columns M_i, M'_j, M''_k .

$$\begin{aligned}
-\omega \cdot \alpha_1 &= |B_1 A_2 A_3| \cdot \alpha_1 + |A_1 B_1 A_3| \cdot \alpha_2 + |A_1 A_2 B_1| \cdot \alpha_3 \\
-\omega \cdot \alpha_2 &= |B_2 A_2 A_3| \cdot \alpha_1 + |A_1 B_2 A_3| \cdot \alpha_2 + |A_1 A_2 B_2| \cdot \alpha_3 \\
-\omega \cdot \alpha_3 &= |B_3 A_2 A_3| \cdot \alpha_1 + |A_1 B_3 A_3| \cdot \alpha_2 + |A_1 A_2 B_3| \cdot \alpha_3 \\
-\theta \cdot \alpha_1 &= |A_1 B_2 B_3| \cdot \alpha_1 + |B_1 A_1 B_3| \cdot \alpha_2 + |B_1 B_2 A_1| \cdot \alpha_3 \\
-\theta \cdot \alpha_2 &= |A_2 B_2 B_3| \cdot \alpha_1 + |B_1 A_2 B_3| \cdot \alpha_2 + |B_1 B_2 A_2| \cdot \alpha_3 \\
-\theta \cdot \alpha_3 &= |A_3 B_2 B_3| \cdot \alpha_1 + |B_1 A_3 B_3| \cdot \alpha_2 + |B_1 B_2 A_3| \cdot \alpha_3
\end{aligned} \tag{2.10}$$

The module structure for I' is identical if we replace α with β and let M_i mean the i th row instead of column.

An interesting corollary of this theorem is the following, which one might think could be proven “by hand”, but such a proof has eluded us. To state it, let $d(n)$ be the total number of divisors of n .

Corollary 74. *Let R be an order in a number field and let I be any ideal class. Let n be the maximum integer such that $R \subseteq \mathbb{Z} + n(I : I)$. Then the total number of weak inverses of I is $\sum_{a|n} ad(a)$, the total number of index n sublattices of $\mathbb{Z}^3$.*

Proof. After choosing a normalized basis $(1, \omega, \theta)$ of R and a basis $(\alpha_1, \alpha_2, \alpha_3)$ of I , let λ_{ij}^1 be the coefficient of α_j in $-\omega\alpha_i$ as in (2.10) and λ_{ij}^2 be the coefficient of α_j in $-\theta\alpha_i$. These are necessarily integers, not all 0. Note that by definition n is the gcd of all the λ_{ij}^k .

We now show that there exists a unique $\mathrm{SL}_3 \mathbb{C}$ (row action) on $V_{\mathbb{C}}$ with the stated invariants. Without loss of generality, we may assume that $B_1 A_2 A_3$ is the identity matrix. Now $a_{21}, a_{31}, b_{12}, b_{13}$ are determined by $\lambda_{12}^1, \lambda_{13}^1, \lambda_{21}^1, \lambda_{31}^1$. Similarly, $b_{22}, b_{23}, b_{32}, b_{33}$ are determined by the λ_{ij}^2 with $i, j \geq 2$.

Last, we must determine what a_{11} is. But if λ_{12}^1 or λ_{13}^1 is nonzero, then a_{21} or a_{31} is nonzero and so by acting with $\mathrm{SL}_3 \mathbb{C}$ (row action), we may force $a_{11} = 0$. If however $\lambda_{12}^1 = \lambda_{13}^1 = 0$, then $a_{11} \neq 0$ or else θ would act on α_1 trivially, which cannot happen since we are assuming that R and I originally appeared as an order in a number field and one of its ideals. Similarly, this implies that at least one of the λ_{1j}^2 must be nonzero, and this will determine a_{11} .

In turn, if instead of using $\mathbb{C}$ we had used $\mathbb{Z}$, then we could have put the first matrix in *Smith normal form* and a similar analysis would give us some *rational* (A, B) in the $\mathrm{SL}_3 \mathbb{C}$ orbit. But then the theory of elementary divisors would allow us to find an integral representative.

Next suppose that $n = 1$, so that the gcd of the $\lambda_{ij}^k = 1$. Then let $X_{\mathbb{Z}}$ be the span

of (A, B) over $\mathbb{Z}$ and let $X_{\mathbb{C}}$ be the same over $\mathbb{C}$. Since the gcd of the $\lambda_{ij}^k(A, B)$ is 1, we know that $X_{\mathbb{Z}}$ is a maximal integral sublattice. Then $W_{\mathbb{C}} = \{(A', B') : \{A', B'\} \text{ spans } W_{\mathbb{C}}\}$ is the $G_{\mathbb{C}}$ orbit of (A, B) in $V_{\mathbb{C}}$, and since $X_{\mathbb{Z}}$ is maximal, we see that the sub- $G_{\mathbb{Z}}$ orbits are precisely the sets of $\mathbb{Z}$ -bases of sublattices of $X_{\mathbb{Z}}$. If (A', B') is a representative basis of such a lattice, then the gcd of the $\lambda_{ij}^k(A', B')$ is the index of the lattice.

So now if we start with λ_{jk}^i with $n \neq 1$, then we may divide each of these by n and follow the recipe of the previous paragraph to arrive at the corollary. $\square$

The corollary has an obvious corollary, for which we again have no simple proof.

Corollary 75. *Every ideal has a weak inverse and every proper ideal has a unique weak inverse.*

2.6.2 Over Arbitrary PIDs

More generally, suppose that B is any PID and let G'_B be the group

$$G'_B = (\mathrm{GL}_2 B \times \mathrm{GL}_3 B \times \mathrm{GL}_3 B) / \{(rsI_2, r^{-1}I_3, s^{-1}I_3) : r, s \in B^\times\}.$$

Then we have the following.

Theorem 76. *There is a canonical bijection between the nondegenerate G'_B orbits on V_B and the set of isomorphism classes of pairs $(R, (I, I'))$ where R is a nondegenerate cubic ring over B and I is a fractional ideal of R and I' is a weak inverse. Under this bijection, the discriminant of the box is equal to the discriminant of the cubic ring.*

The proof of this theorem is the same as the proof of Theorem 72 and may be deduced⁴ directly from Wood's main theorem in [112]. Notice that $G_B \cong G'_B$ whenever $B^\times / (B^\times)^3$ is trivial. In particular, $G_{\mathbb{Z}} \cong G'_{\mathbb{Z}}$.

⁴Wood only considers the action of $\mathrm{SL}_3 \times \mathrm{SL}_3$ in that paper, but it is not hard to extend her results to this case.

In both cases, a corollary of the proof of the theorem is the following.

Corollary 77 ([10, Corollary 3]). *The stabilizer in G'_B of a nondegenerate element $v \in V_B$ is isomorphic to a semidirect product*

$$\mathrm{Aut}_B(R(v)) \ltimes [((I : I) \cap (I' : I')) / B^\times]$$

In particular, if I is proper, then $(I : I) \cap (I' : I') = R$ and so this is simply $\mathrm{Aut}(R) \ltimes [R^\times / B^\times]$.

2.6.3 Stabilizers and Weights

Recall that we defined $\rho(I, I') = (I : I) \cap (I' : I')$. Moreover, the appearance of $\rho^\times / B^\times$ in Corollary 77 should remind us of the regulator of a pair of ideals that we defined in Section 2.2. This is not a coincidence. To begin, note the following Proposition.

Proposition 78. *The group $G_{\mathbb{R}}$ acts transitively on $V^\pm$ and the isotropy groups for $v \in V^\pm$ are*

- $S_3 \ltimes [\mathrm{GL}_1(\mathbb{R}) \times \mathrm{GL}_1(\mathbb{R})]$ for $v \in V^+$; and
- $S_2 \ltimes \mathbb{C}^\times$ for $v \in V^-$.

Proof. This follows from Corollary 77 and the fact that any $v \in V^+$ corresponds to the triple $(\mathbb{R}^3, (\mathbb{R}^3, \mathbb{R}^3))$ and the generic $v \in V^-$ corresponds to $(\mathbb{R} \oplus \mathbb{C}, (\mathbb{R} \oplus \mathbb{C}, \mathbb{R} \oplus \mathbb{C}))$. $\square$

Now $\mathrm{GL}_1(\mathbb{R}) \times \mathrm{GL}_1(\mathbb{R})$ has many automorphisms, and so we choose now a particular realization. Suppose that $B = \mathbb{Z}$ and that $\rho = \rho(I, I')$. In the totally real case, we know that $\rho^\times$ is isomorphic to the roots of unity of ρ times a rank two free abelian group. Let $\varepsilon_1, \varepsilon_2$ be fundamental units, i.e., they span this free abelian group. Then under the Galois embedding, we may $\rho^\times \rightarrow (\rho \otimes \mathbb{R})^\times / \mathbb{R}^\times$. Further, if we take logs, then we see that the image of $\rho^\times$ under

the composition spans the two-dimensional space which is the log of $(\rho \otimes \mathbb{R})^\times / \mathbb{R}^\times$. This in turn fixes an isomorphism of $(\rho \otimes \mathbb{R})^\times / \mathbb{R}^\times$ with $\mathrm{GL}_1(\mathbb{R}) \times \mathrm{GL}_1(\mathbb{R})$.

Under this isomorphism, by choosing $d^\times t_1 d^\times t_2$ as the Haar measure on $\mathrm{GL}_1(\mathbb{R}) \times \mathrm{GL}_1(\mathbb{R})$, we find that the integral over a fundamental region for the action of the image of $\rho^\times$ is precisely the regulator of ρ .

Similarly, in the non-totally real case, we may choose an isomorphism of $(\rho \otimes \mathbb{R})^\times / \mathbb{R}^\times$ with $\mathbb{C}^\times$ by first choosing one of the complex embeddings of $\rho \otimes \mathbb{Q} \hookrightarrow \mathbb{C}$. Now $\mathbb{C}^\times \cong \mathbb{R}_{>0} \times \mathrm{SO}_2$ and so by taking the Haar measure on $\mathbb{C}^\times$ to be $d^\times t dk$ with $\int_{\mathrm{SO}_2} dk = 2\pi$, we find that the integral over a fundamental domain for the action of $\rho^\times$ on $\mathbb{C}^\times$ is exactly $\mathrm{Reg}(\rho)$.

Combining the past three paragraphs, we arrive at the following proposition.

Proposition 79. *Suppose that $v \in V_{\mathbb{Z}}$. Then for a fundamental domain $\mathcal{F}_v$ of $G_{v,\mathbb{Z}}$ acting on $G_{v,\mathbb{R}}$ we have*

$$\int_{\mathcal{F}_v} \mu(g_v) = \frac{\# \mathrm{Aut}_{\mathbb{R}}(R(v_{\mathbb{R}}))}{\# \mathrm{Aut}_{\mathbb{Z}}(R(v))} \mathrm{Reg}(\rho).$$

Proof. The rational factor comes from the finite groups on the left hand side of the semidirect product in the previous proposition. The origin of the regulator was described in the last three paragraphs. □

2.7 Local Densities for Invertible and Proper Ideals

As we have noted, whether a ring is maximal or not and whether an ideal is invertible or proper or not are all *local* conditions. So we would like to say that the total proportion of pairs $(R, (I, I'))$ satisfying these conditions is just given by a product of local densities. We will in fact prove this later, but for now, we compute these local densities.

2.7.1 A Mass Formula

For any free module W of finite rank over $\mathbb{Z}_p$, let μ_W be the additive Haar probability measure. Then for any subset $S \subseteq V_{\mathbb{Z}_p}$ defined by finitely many congruence conditions, let $\mu_{V_{\mathbb{Z}_p}}(S)$ be the p -adic density of S in $V_{\mathbb{Z}_p}$. To a cubic ring R over $\mathbb{Z}_p$, let $\text{Disc}_p(R)$ be the power of p appearing in the discriminant of R and let the *local regulator*, $\text{Reg}_p(R)$ be defined by $\text{Reg}_p(R) = \mu_R(R^\times) / \mu_{\mathbb{Z}_p}(\mathbb{Z}_p^\times)$, which is as in Section 2.3. Using these definitions, we can compute the p -adic density of those pairs $(R, (I, I'))$ when I is invertible.

Proposition 80. *Let R be a nondegenerate cubic ring over $\mathbb{Z}_p$ and let I be an invertible ideal of R . Then the p -adic density of all elements in $V_{\mathbb{Z}_p}$ corresponding to the pair $(R, (I, I^{-1}))$ in Theorem 76 is*

$$\frac{\#G'_{\mathbb{F}_p}}{p^{20}} \cdot \frac{1}{\# \text{Aut}(R)} \cdot \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\text{Reg}_p(R)}. \quad (2.11)$$

Proof. Since I is invertible, we saw in Section 2.2 that I must be principal (remember we are working over $\mathbb{Z}_p$). Hence, $(R, (I, I')) \cong (R, (R, R))$, so we need only handle this case. But there are only a finite number of cubic rings over $\mathbb{Z}_p$ with any fixed nonzero discriminant, so the cubic ring R is determined from its ring structure modulo p^n for some $n \gg 0$. That is, $R/p^n R$ determines R . On the other hand, the correspondence of Theorem 76 is compatible with reduction by p^n since all the structure coefficients are determined by polynomials in the entries of $v \in V_{\mathbb{Z}_p}$. As such, if two $v, v' \in V_{\mathbb{Z}_p}$ lie in the same $G'_{\mathbb{Z}_p}$ orbit, then they lie in the same $G'_{\mathbb{Z}/p^n\mathbb{Z}}$ orbit and vice-versa.

From the orbit-stabilizer theorem, we know that the total number of elements in the orbit is $\#G'_{\mathbb{Z}/p^n\mathbb{Z}} / \#G'_{v, \mathbb{Z}/p^n\mathbb{Z}}$, so it suffices to determine the order of the stabilizer. However, Corollary 77 reduced modulo p^n yields that

$$\begin{aligned} \#G'_{v, \mathbb{Z}/p^n\mathbb{Z}} &= \# \text{Aut}(R/p^n R) \cdot \#(R/p^n R)^\times / \#(\mathbb{Z}_p/p^n \mathbb{Z}_p)^\times \\ &= (\# \text{Aut}(R) \text{Disc}_p(R)) \cdot (p^{2n} \text{Reg}_p(R)) \end{aligned}$$

As such, the p -adic density of the inverse image in $V_{\mathbb{Z}_p}$ corresponding to the set of all $v \in V_{\mathbb{Z}/p^n\mathbb{Z}}$ corresponding to $(R/p^n R, (R/p^n R, R/p^n R))$ is

$$\frac{1}{p^{18n}} \cdot \frac{\#G'_{\mathbb{Z}/p^n\mathbb{Z}}}{p^{2n} \cdot \# \text{Aut}(R) \cdot \text{Disc}_p(R) \cdot \text{Reg}_p(R)} = \frac{p^{20(n-1)} \cdot \#G'(\mathbb{F}_p)}{p^{20n} \cdot \# \text{Aut}(R) \cdot \text{Disc}_p(R) \cdot \text{Reg}_p(R)}.$$

□

In what follows, let $\text{MAX}_p \subseteq V_{\mathbb{Z}_p}$ (resp. INV_p , resp. PROP_p) denote the set of elements corresponding to cubic rings which are maximal at p (resp. such that the ideal I is invertible, resp. proper, at p). Note that $\text{MAX}_p \subseteq \text{INV}_p \subseteq \text{PROP}_p$. In the next several sections, we compute the densities of these sets.

2.7.2 Maximal Rings

To begin, note that $\text{Reg}_p(R)$ is determined simply by R/pR . In particular, an element of R is a unit if and only if it is a unit in R/pR . As such,

$$\text{Reg}_p(R) = \frac{\#(R/pR)^\times}{\#(R/pR)} \cdot \frac{p}{p-1} = \frac{\#(R/pR)^\times}{p^2(p-1)}.$$

Now there are five possible reductions of a cubic ring R over $\mathbb{Z}_p$ modulo p corresponding to the five possible splitting types of a prime in $\mathbb{Z}$. We denote these splitting types $(f_1^{e_1} f_2^{e_2} \dots)$ where $R/pR \cong \bigoplus \mathbb{F}_{p^{f_i}}[x]/(x^{e_i})$. As is traditional, we drop the superscripts when they are 1. As such, the five possible splitting types are (111) , (12) , (3) , $(1^2 1)$, and (1^3) . We will typically denote the splitting type of an object by τ , for instance $\tau(\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p) = (111)$.

Then

$$\sum^{\max} \frac{1}{\# \text{Aut}(R)} \cdot \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\text{Reg}_p(R)} = \sum_{\tau} \frac{1}{\text{Reg}_p(\tau)} \sum_{\tau(R/pR)=\tau}^{\max} \frac{1}{\# \text{Aut}(R)} \cdot \frac{1}{\text{Disc}_p(R)}. \quad (2.12)$$

Where $\sum^{\max}$ means the sum restricted to *maximal* cubic rings. These inner sums were

computed in [13] and again appear in the table at the end of this article.

Finally, we note that

$$\#G'_{\mathbb{F}_p} = (p^2 - 1)(p^2 - p)(p^3 - 1)^2(p^3 - p)^2(p^3 - p^2)^2/(p - 1)^2 = p^7(p - 1)(p^2 - 1)^3(p^3 - 1)^2.$$

Combining all this information, we arrive at

$$\begin{aligned} \mu_{V_{\mathbb{Z}_p}}(\text{MAX}_p) &= \frac{p^7(p - 1)(p^2 - 1)^3(p^3 - 1)^2}{p^{20}} \\ &\quad \times \left[\frac{1}{6} \cdot \frac{p^2}{(p - 1)^2} + \frac{1}{2} \cdot \frac{p^2}{p^2 - 1} + \frac{1}{3} \cdot \frac{p^2}{p^2 + p + 1} + \frac{1}{p} \cdot \frac{p}{(p - 1)} + \frac{1}{p^2} \cdot 1 \right] \\ &= \frac{(p^2 - 1)^2(p^3 - 1)(p^8 + p^6 - 2p^5 - 2p^4 + 2p^2 + p - 1)}{p^{15}}. \end{aligned}$$

2.7.3 Invertible Ideals

When we instead count *invertible* ideals, we do not restrict ourselves to maximal cubic rings. In particular, there is now a *sixth* splitting type, which we call (0) and which corresponds to the ring with discriminant 0, viz. $\mathbb{F}_p[x, y]/(x^2, xy, y^2)$. The regulator for this ring is quickly seen to be 1.

Now to find the total mass, we need only modify (2.12) to run over *all* cubic rings, and not just maximal ones. Then in [13], the inner sums were computed to be $\# \text{Aut}(R/pR)$. Combining all of this data we get

$$\begin{aligned}
& \mu_{V_{\mathbb{Z}_p}}(\text{INV}_p) \\
&= \frac{p^7(p-1)(p^2-1)^3(p^3-1)^2}{p^{20}} \times \\
& \quad \times \left[\frac{1}{6} \cdot \frac{p^2}{(p-1)^2} + \frac{1}{2} \cdot \frac{p^2}{p^2-1} + \frac{1}{3} \cdot \frac{p^2}{p^2+p+1} + \frac{1}{p-1} \cdot \frac{p}{(p-1)} + \right. \\
& \quad \left. \frac{1}{p(p-1)} \cdot 1 + \frac{1}{(p^2-1)(p^2-p)} \cdot 1 \right] \\
&= \frac{(p^2-1)^2(p^3-1)(p^5+2p^3-p-2)}{p^{12}}.
\end{aligned}$$

2.7.4 Proper Ideals

Unfortunately, Proposition 80 no longer is useful for computing the density of proper ideals. Note that if $(I : I) \neq R$, then there is some prime number p and some element $r \in R$ such that $r/p \in (I : I)$. When this occurs is the topic of the following lemma.

Lemma 81. *Let $v = (A, B) \in V_{\mathbb{Z}}$ be nondegenerate and let $(R, (I, I'))$ be the pair corresponding to v in Theorem 72. Let $(1, \omega, \theta)$ denote the associated $\mathbb{Z}$ -basis of R as in Theorem 69. If $(\omega + c)/p \in (I : I)$ (where $c \in \mathbb{Z}$) then exactly one of the following holds:*

- (i) *A and B are linearly dependent over $\mathbb{F}_p$ but at least one has rank 3 over $\mathbb{F}_p$,*
- (ii) *A has rank 1 but the 3×6 matrix $(A B)$ has rank 3 over $\mathbb{F}_p$, or*
- (iii) *$(A B)$ has rank at most 2 over $\mathbb{F}_p$.*

Proof. First note that the three possibilities listed are mutually exclusive, so we have shown that if one must happen then *exactly* one must happen. Moreover, note that the condition in the theorem is that ω acts by a *scalar* mod p . We check that this occurs in each of the three cases and in no other case.

As noted in Remark 73, the proof of Theorem 72 actually gives the *explicit* action of R on I and I' , which is recounted there. In particular, $\omega/p \in (I : I)$ if and only if all of the determinants in the action of $-\omega \cdot \alpha_i$ are divisible by p .

The statement that $(A \ B)$ has rank at most 2 is precisely the statement that *all* 3×3 submatrices of $(A \ B)$ have vanishing determinant, so certainly (iii) implies that $\omega/p \in (I : I)$. So now we have to consider the case when $(A \ B)$ has rank 3.

Suppose first that A has rank 0 mod p , i.e., $A = 0 \pmod{p}$. Then B necessarily has rank 3 and so (i) holds. Also, all the determinants in (2.10) are obviously 0 mod p in this case.

If A has rank 1, then since every determinant in the multiplication table (2.10) defining the action of ω has at least two columns from A , they are all 0. Hence, (ii) also implies that $\omega/p \in (I : I)$.

Next consider the case where the rank of A is 2. Then at most one pair of columns of A , say A_i, A_j , span the same one-dimensional space over $\mathbb{F}_p$. Then, letting the third column be A_k , we see that A_i, A_k and A_j, A_k span the *same* two-dimensional space. Since $(A \ B)$ has rank 3, we know that B must have some column, say B_ℓ , *not* in the span of the columns of A . In particular, at least two of the determinants in the definition of $-\omega \cdot \alpha_\ell$ must be nonzero. In particular, ω cannot act by a scalar mod p .

Finally, we consider the case when A has rank 3. Then in order for ω to act as a scalar mod p , we need all the off-diagonal terms in (2.10) to be 0. This immediately implies that B_1 is in the span of A_1, A_2 and A_1, A_3 , and so is necessarily in the span of A_1 . Similarly for B_2 and B_3 . That is, each column of B is a multiple of the corresponding column of A , say $B_i = b_i A_i$.

Then the corresponding diagonal entries of (2.10) are $b_i \det(A)$. In order for ω to act as a scalar, we must have all the b_i being equal. That is, B is a (possibly 0) scalar multiple of A , and we are in the case of (i). □

So to determine $\mu(\text{PROP}_p)$ it suffices to determine the total number of $v \in V_{\mathbb{F}_p}$ which do not take on the forms (i), (ii), or (iii) in the lemma *after* a $\text{GL}_2(\mathbb{F}_p)$ transformation. This corresponds to taking the $r \in R$ such that $r/p \in (I : I)$ in the discussion above to the $\omega \in R$ in the statement of the lemma.

For form (i), note that one of A and B is nonzero and the other is a constant (possibly 0) multiple of the nonzero matrix. As such, form (i) is true of any (A, B) in the same $G_{\mathbb{F}_p}$ orbit. So we need only count pairs of matrices satisfying (i). Now there are $(p^3 - 1)(p^3 - p)(p^3 - p^2)/(p - 1)$ rank 3 matrices over $\mathbb{F}_p$ up to scalars. Then of the p^2 possible choices of pairs of matrices on this line, only one (the pair of 0 matrices) is forbidden. As such, we multiply the total number of lines by $(p^2 - 1)$ to obtain

$$p^3(p^2 - 1)^2(p^3 - 1). \quad (2.13)$$

For form (ii), note that since (AB) has full rank that the rank of B is at least 2 and the span of the columns of B along with any nontrivial column of A span all of $\mathbb{F}_p^3$. As such, the $\mathbb{F}_p$ span of A and B contains precisely one line of rank 1 matrices, namely the one spanned by A . The number of choices for this rank 1 matrix up to scaling is $(p^3 - 1)^2/(p - 1)^2$. Then the total number for choices for B up to scaling and modulo adding some multiple of A is $p^2(p^3 - 1)(p^3 - p)/(p - 1)$. So in total, the number of pairs (A, B) having form (ii) after some $\text{GL}_2(\mathbb{F}_p)$ transformation is

$$(p^2 + p + 1)^2 \cdot p^3(p^3 - 1)(p + 1) \cdot \# \text{GL}_2(\mathbb{F}_p) = p^4(p^2 - 1)^2(p^2 + p + 1)^2(p^3 - 1). \quad (2.14)$$

Finally, we come to form (iii). But under any $\text{GL}_2(\mathbb{F}_p)$ transformation, (AB) will still have rank at most 2. So the total number of 3×6 matrices with rank at most 2 is

$$p^{18} - (p^6 - 1)(p^6 - p)(p^6 - p^2). \quad (2.15)$$

Subtracting (2.13), (2.14) and (2.15) from $p^{18} = \#V_{\mathbb{F}_p}$ we arrive at

$$\mu(\text{PROP}_p) = \frac{(p^2 - 1)^2(p^3 - 1)(p^7 + 2p^5 - 2p^2 - 1)}{p^{14}}.$$

2.8 A Geometry of Numbers Argument

Let $V = V_{\mathbb{R}}$ be the vector space of boxes over $\mathbb{R}$. Then the action of $G(\mathbb{R})$ has two nondegenerate orbits, viz. V^+ consisting of elements with positive discriminant, and V^- consisting of elements with negative discriminant. Let $V_{\text{irr}}^{\pm} \subseteq V_{\mathbb{Z}}$ be the subset of all integral boxes (A, B) such that $\det(Ax - By)$ is an irreducible cubic polynomial over $\mathbb{Q}$, i.e., such that (A, B) corresponds to an order in a number field. In this section, we will get a handle on the total

$$N(V^{\pm}; X) = \sum \text{Reg}(v)$$

where the sum is over $G_{\mathbb{Z}}$ orbits represented by v in $V_{\mathbb{Z}}$ lying in $V_{\text{irr}}^{\pm}$ and having absolute discriminant at most X . That is, we are summing the regulator of ideal classes of orders in cubic fields.

2.8.1 Reduction Theory

Recall that $G = \text{GL}_2 \times \text{SL}_3 \times \text{SL}_3$. We may express elements of $G(\mathbb{R})$ via the Iwasawa decomposition $NAK\Lambda$ where N consists of triples of upper triangular matrices, A consists of triples of diagonal matrices of determinant one, $K = \text{O}_2 \times \text{SO}_3 \times \text{SO}_3$ is the maximal compact, and Λ consists of positive scalar matrices in $\text{GL}_2(\mathbb{R})$. Let $\mathcal{F}$ be a fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$. Then according to Minkowski's theory of such

fundamental domains, we may take $\mathcal{F} = \{nak\lambda : n \in N'(a), a \in A', K \in K, \lambda \in \Lambda\}$ where

$$N'(a) = \left[\begin{pmatrix} 1 & & \\ n_1 & 1 & \end{pmatrix}, \begin{pmatrix} 1 & & \\ n_2 & 1 & \\ n_3 & n_4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ n_5 & 1 & \\ n_6 & n_7 & 1 \end{pmatrix} \right]$$

$$A' = \left[\begin{pmatrix} s_1^{-1} & & \\ & s_1 & \end{pmatrix}, \begin{pmatrix} s_2^{-2} s_3^{-1} & & \\ & s_2 s_3^{-1} & \\ & & s_2 s_3^2 \end{pmatrix}, \begin{pmatrix} s_4^{-2} s_5^{-1} & & \\ & s_4 s_5^{-1} & \\ & & s_4 s_5^2 \end{pmatrix} \right],$$

where $s_1 \geq \sqrt[4]{3}/\sqrt{2}$, and $s_i \geq \sqrt[6]{3}/\sqrt[3]{2}$ for $i > 1$, and $n_j \in \tau_j(a)$ where each $\tau_j(a)$ is a measurable subset of $\mathbb{R}$ bounded independent of a for each $a \in A'$. The exact values $\tau_j(a)$ will not matter for us, only that they are bounded.

In these coordinates, the Haar measure on G may be taken to be

$$dg = s_1^{-2} s_2^{-6} s_3^{-6} s_4^{-6} s_5^{-6} d^\times s \, dn \, dk \, d^\times \lambda$$

where

- $dn = \prod dn_i$ is the usual additive Haar measure,
- $d^\times s = \prod d^\times s_i = \prod s_i^{-1} ds_i$ is the usual multiplicative Haar measure,
- $d^\times \lambda$ is also the usual multiplicative Haar measure, and
- dk is the Haar probability measure on K .

2.8.2 An Averaging Argument

Let $B = B(C) = \{v \in V_{\mathbb{R}} : \|v\| \leq C\}$ where $\|v\|$ denotes the usual Euclidean norm. For what we do now, $C = 100$ will suffice. Moreover, the main features of B that we will use is

that it is bounded, has positive volume in V , and that it is K invariant. Then as v ranges over $B \cap V^\pm$ we know that

$$\sum_{\substack{f \in \mathcal{F}v \cap V_{\text{irr}}^\pm \\ |\text{Disc}(f)| < X}} \text{Reg}(v)$$

is *constant* and is equal to $N(V^\pm; X)$. Then

$$N(V^\pm; X) = \frac{\int_{v \in B \cap V_{\text{irr}}^\pm} \sum_{\substack{f \in \mathcal{F}v \cap V^\pm \\ |\text{Disc}(f)| < X}} \text{Reg}(f) |\text{Disc}(v)|^{-3/2} dv}{\int_{v \in B \cap V^\pm} |\text{Disc}(v)|^{-3/2} dv}. \quad (2.16)$$

Note that we choose the measure $|\text{Disc}(v)|^{-3/2} dv$ precisely because it is a G -invariant measure on V .

More generally, for any $G_\mathbb{Z}$ invariant subset $S \subseteq V_\mathbb{Z}^\pm$ let $N(S, X)$ be defined the same way as $N(V^\pm, X)$. That is, if

$$M_\pm(C) = \int_{v \in B \cap S} |\text{Disc}(v)|^{-3/2} dv,$$

then define

$$N(S; X) = \frac{1}{M_\pm(C)} \int_{v \in B \cap S} \sum_{\substack{f \in \mathcal{F}v \cap S_{\text{irr}} \\ |\text{Disc}(f)| < X}} \text{Reg}(f) |\text{Disc}(v)|^{-3/2} dv. \quad (2.17)$$

Similarly, define $N^*(S, X)$ to be the same sum but *not* restricted to irreducible orbits.

Now recall that if G is a locally compact topological group and $H \subseteq G$ is some closed subgroup, then a function on G/H is just a function on G which is constant on the cosets of H . In particular, if $f \in C_c(G)$ is a function on G with compact support, then there is a map $\varphi : C_c(G) \rightarrow C_c(G/H)$ given by

$$\varphi(f)(gH) = \int_H f(gh) dh$$

where dh is a fixed Haar measure⁵ on H . In fact, this map is surjective. Moreover, if we fix a Haar measure dg on G , then there is a *unique*⁶ measure $d(gH)$ on G/H such that

$$\int_G f(g)dg = \int_{G/H} \varphi(f)(gH)d(gH)$$

for every $f \in C_c(G)$. Up to scaling, this is the unique G invariant measure on G/H .

As we saw in Section 2.6, the regulator $\text{Reg}(f)$ of a point $f = gv \in \mathcal{F}v \cap V^\pm$ is equal to

$$\text{Reg}(f) = \frac{\# \text{Aut}(R_{\mathbb{Z}}(f))}{\# \text{Aut}(R_{\mathbb{R}}(f_{\mathbb{R}}))} \int_{G_{f,\mathbb{R}}/G_{f,\mathbb{Z}}} dg_f = \frac{\# \text{Aut}(R_{\mathbb{Z}}(f))}{\# \text{Aut}(R_{\mathbb{R}}(f_{\mathbb{R}}))} \int_{h \in G_{f,\mathbb{R}}(v)} 1_{\mathcal{F}}(gh)dh$$

We would then like to make the following manipulations, exploiting the fact that $|\text{Disc}(v)|^{-3/2}dv$ is $G(\mathbb{R})$ invariant:

$$N(S; X) = \frac{1}{M_{\pm}(C)} \int_{v \in B \cap S} \sum_{\substack{f \in \mathcal{F}v \cap V^\pm \\ |\text{Disc}(f)| < X}} \text{Reg}(f) |\text{Disc}(v)|^{-3/2} dv \quad (2.18)$$

$$= \frac{1}{M_{\pm}(C)} \int_{v \in B \cap V^\pm} \sum_{\substack{f \in \mathcal{F}v \cap V^\pm \\ \pm \text{Disc}(f) < X}} \frac{\# \text{Aut}(R(f))}{\# \text{Aut}(R(f_{\mathbb{R}}))} \int_{h \in G_{f,\mathbb{R}}} 1_{\mathcal{F}}(gh) dh |\text{Disc}(v)|^{-3/2} dv \quad (2.19)$$

$$= \frac{c_{\pm}}{M_{\pm}(C)} \int_{g \in \mathcal{F}} \# \{f \in V^\pm \cap Bg : |\text{Disc}(f)| < X\} dg \quad (2.20)$$

where $c_{\pm}$ is the Jacobian of the change of variables times $\frac{1}{\# \text{Aut}(f_{\mathbb{R}})}$ which is constant for all $f \in \mathcal{F}v \cap V^\pm$. Moreover, here $\#$ means the total number weighted by $\# \text{Aut}(\mathbb{R}(v))$. (Of course, orders in cyclic cubic fields are known to be extremely rare and orders in S_3 fields have no automorphisms, so we will henceforth ignore this weighting factor.)

However, we note that $1_{\mathcal{F}}$ certainly does not have compact support, so this is not a

⁵Of course, G and H need not be unimodular. In such a case, we take ‘‘Haar measure’’ to mean ‘‘left Haar measure’’, though the statements work perfectly well if we instead use right Haar measures.

⁶Here uniqueness occurs because we already chose dg and dh . Another way to phrase this is that the triple of measures $(dg, dh, d(gH))$ are unique up to scaling by triples $(\lambda, \eta, \lambda\eta^{-1})$.

a priori true. In order to make this change of coordinates, we will instead only sum over those f with $a_{11} \neq 0$ and $|\text{Disc}(f)| < X$. We will see below that this will bound the values of a_{ij} and b_{ij} since they must be integers. Hence we may replace $1_{\mathcal{F}}$ with a function with compact support. But by doing so, we might be throwing out too many points and thus affecting the main term of our count. To avoid this, we note the following lemma, whose proof is delayed for now.

Lemma 82. *Let $V(a_{11} = 0) \subseteq V^{\pm}$ be the set of all $f \in V^{\pm}$ which are irreducible and such that $a_{11} = 0$. Then $N(V(a_{11} = 0); X) = O(X^{17/12})$.*

Performing the sum inside the integral (2.20) is rather difficult to handle due to the restriction to *irreducible* boxes. The following lemma allows us to lift that restriction. Again, we avoid the proof for now.

Lemma 83. *The contribution to the sum $N^*(V^{\pm}; X)$ coming from reducible boxes with $a_{11} \neq 0$ is $o(X^{3/2})$.*

Remark 84. We expect that the actual bound in this lemma may be pushed to $O(X^{17/12+\varepsilon})$. However, our current method of proof only will give $o(X^{3/2})$ with no explicit power saving.

Before moving on, we would like to rewrite (2.20) in a convenient form. Specifically, write $B(n, s, \lambda, X) = n(u)a(s)\lambda B \cap \{v \in V^{\pm} : |\text{Disc}(v)| < X\}$. Then since B is K -invariant, we may write

$$\begin{aligned} N(S; X) &= \frac{c_{\pm}}{M_{\pm}(C)} \int_{g \in N'(a)A'\Lambda} \#\{x \in S_{\text{irr}} \cap B(u, s, \lambda, X)\} s_1^{-2} s_2^{-6} s_3^{-6} s_4^{-6} s_5^{-6} d^{\times} s \, dn \, d^{\times} \lambda + o(X^{3/2}). \end{aligned} \tag{2.21}$$

Also, $N^*(S; X)$ is the same, but with the subscript *irr* removed, and since Lemma 83 is no longer necessary, with $o(X^{3/2})$ replace by $O(X^{17/12})$.

2.8.3 A Lemma from the Geometry of Numbers

In later sections, we will need to estimate the number of lattice points in $B(u, s, \lambda, X)$, which we will do using the following elementary proposition due to Davenport [38].

Proposition 85. *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ which is defined by finite number of polynomial inequalities⁷. Let $\mathcal{R}'$ be the image of $\mathcal{R}$ under any (upper or lower) triangular unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points contained in the region $\mathcal{R}'$ is*

$$\text{vol}(\mathcal{R}) + O(\max\{\text{vol}(\bar{\mathcal{R}}), 1\})$$

where $\text{vol}(\bar{\mathcal{R}})$ is the greatest d -dimensional volume ($1 \leq d \leq n - 1$) of any projection of $\mathcal{R}$ onto a coordinate subspace, i.e., by setting $n - d$ coordinates to 0. The implied constant depends only on n , the total number of defining polynomials, and their maximum degree.

Although Davenport states the above lemma only for compact semi-algebraic sets $\mathcal{R} \subseteq \mathbb{R}^n$, his proof adapts essentially without change to the above proposition.

2.8.4 A More General Regulator

Let $\mathcal{R}_X(v) = \mathcal{F}v$ for any $v \in B$. Then we may define the *regulator* of a point $gv \in \mathcal{R}_X(v)$ to be

$$\text{Reg}(f) = \int_{h \in G_{f, \mathbb{R}}} 1_{\mathcal{F}}(gh) dh.$$

Then, considering $\mathcal{R}_X(v)$ as a weighted set, we may define its volume to be

$$\text{Vol}(\mathcal{R}_X(v)) = \int_{f \in \mathcal{R}_X(v)} \text{Reg}(f) df.$$

⁷For any property (P) of a set, we extend its meaning to multisets by saying a multiset $\mathcal{R}$ has property (P) if and only if $\mathcal{R}_k$ has property (P) for all k . Here $\mathcal{R}_k$ is the set of all $x \in \mathcal{R}$ with weight k .

Note that this volume is constant for any $v \in B$ by the invariance of the Haar measures.

2.8.5 The main term

Combining Proposition 85 with (2.21), we see that it suffices to compute the Euclidean volume of $B(u, s, \lambda, X)$ for every u, s, λ, X and then to show that none of its projections are too terribly large.

For the first task, we note simply that

$$c_{\pm} \int_{g \in \mathcal{F}} B(u, s, \lambda, X) dg = \int_{v \in B \cap V^{\pm}} \text{Vol}(\mathcal{R}_X(v)) |\text{Disc}(v)|^{-3/2} dv.$$

(Recall from (2.20) that $c_{\pm}$ is the Jacobian of the change of variables.) Since $\text{Vol}(\mathcal{R}_X(v))$ is constant, this yields a total of $M_{\pm}(C) \cdot \text{Vol}(\mathcal{R}_X(v))$.

As for the second task, we note that the region $B(u, s, \lambda, X)$ contains an integer point with $|a_{11}| \geq 1$ only if we have

$$C \cdot \frac{\lambda}{s_0 s_1^2 s_2 s_3^2 s_4} \geq 1.$$

One easily checks that the projection to the coordinate plane $a_{11} = 0$ has maximal volume among all possible projections (as we will see in a more formal context in the proof of Lemma 82 a little later), and that this volume is $\ll \lambda^{18} s_0 s_1^2 s_2 s_3^2 s_4 / \lambda$. Hence the error coming from Proposition 85 is at most a constant times

$$\int_{\lambda \gg 0}^{X^{1/12}} \int_{s_i \gg 0}^{\infty} \int_{N'(a(s))} \lambda^{17} s_0 s_1^2 s_2 s_3^2 s_4 s_0^{-2} s_1^{-6} s_2^{-6} s_3^{-6} s_4^{-6} du d^{\times} s d^{\times} \lambda \ll X^{17/12}.$$

Finally, we note that [84, Proposition 20] tells us that

$$\int_{G_{\mathbb{Z}} \backslash G_{\mathbb{R}}^1} dg = \zeta(2)^2 \zeta(3)^2$$

where $G_{\mathbb{R}}^1 = \text{SL}_2 \mathbb{R} \times \text{SL}_3 \mathbb{R} \times \text{SL}_3 \mathbb{R} \subseteq G_{\mathbb{R}}$ and dg is taken to be the measure $dn d\bar{n} d^{\times} a d^{\times} \lambda$

arising from the $NA\bar{N}A$ decomposition of $G_{\mathbb{R}}$. Using the change of variables formula, our computation of the automorphism group, and [105], we compute that for $v \in V_{\mathbb{R}}^{\pm}$ that

$$\text{Vol}(\mathcal{R}_X(v)) = \frac{6}{n_{\pm}} \int_0^{X^{1/12}} t^{18} d^{\times}t \int_{G_{\mathbb{Z}} \backslash G_{\mathbb{R}}^1} dg = \frac{\zeta(2)^3 \zeta(3)^2}{3n_{\pm}} X^{3/2}.$$

Here $n_{\pm}$ is given by

$$n_{\pm} = \int_{g \in G_{v, \mathbb{R}} \cap G_{\mathbb{R}}^1} dh$$

which we can easily compute is

$$n_{+} = 24$$

$$n_{-} = 4\pi$$

2.8.6 Congruence Conditions

We can also prove a version of Theorem 40 for a set in $V^{\pm}$ defined by any finite number of congruence conditions. Specifically,

Theorem 86. *Suppose that $S \subseteq V_{\mathbb{Z}}^{\pm}$ is defined by finitely many congruence conditions. Then we have*

$$\lim_{X \rightarrow \infty} \frac{N(S \cap V^{\pm}; X)}{X} = \frac{\zeta(2)^2 \zeta(3)^2}{3n_{\pm}} \prod_p \mu_p(S),$$

where $\mu_p(S)$ denotes the p -adic density of S in $V_{\mathbb{Z}}$ and $n_{+} = 24$ and $n_{-} = 4\pi$.

Proof. Suppose that S is defined by congruence conditions modulo m . Then S can be viewed as the union of (say) k translates $L_1, \dots, L_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each such lattice L_j we may compute $N(L_j; X)$ using Proposition 85 but where each d -dimensional volume is scaled by a factor of $1/m^d$ since our new lattice has been scaled by a factor of m . As such,

$$N(L_j; X) = m^{-18} \text{vol}(\mathcal{R}_X(v)) + O(m^{-17} X^{17/12})$$

with $v \in V^\pm$ and the implied constant *independent* of m provided that $m \ll X^{1/12}$. Summing over j and noting that $km^{-18} = \prod_p \mu_p(S)$ we obtain the theorem. $\square$

2.8.7 Controlling the Error: Proofs of Lemmas 82 and 83

Now we have the tools to prove Lemmas 82 and 83. Let us start with the former. The proof amounts to slicing the set $V(a_{11} = 0)$ into several smaller subsets and then using Proposition 85 in order to deduce an upper bound on their total number. The following lemma lets us do the slicing.

Lemma 87. *Let $(A, B) \in V_{\mathbb{Z}}$ be a box. Then if any of the following sets of coordinates vanish, then the box is not irreducible.*

$$(i) \{a_{11}, a_{12}, a_{13}\},$$

$$(ii) \{a_{11}, a_{21}, a_{31}\},$$

$$(iii) \{a_{11}, a_{12}, a_{21}, a_{22}\},$$

$$(iv) \{a_{11}, a_{12}, b_{11}, b_{12}\}, \text{ or}$$

$$(v) \{a_{11}, a_{21}, b_{11}, b_{21}\}.$$

Proof. In the first three cases, $\det(A) = 0$, and so $\det(v)$ is a multiple of x and obviously *not* irreducible. In case (iv), either a_{13} or b_{13} is zero, or can be made zero through a rational linear combination of A and B . Hence, one of A and B will have determinant zero and $\det(v)$ will once again be reducible. Similarly for case (v). $\square$

Proof of Lemma 82. Following the method developed in [14], we divide the set of all $(A, B) \in V_{\mathbb{Z}}$ into a number of cases depending on which initial coordinates are zero and which are nonzero. These cases are described in the second column of Table 1. The vanishing conditions in the various subcases of Case $n + 1$ have been obtained by setting equal to 0—one at a

time—each variable that was assumed to be nonzero in Case n . If such a resulting subcase satisfies the reducibility conditions of Lemma 87, it is not listed. In this way, it becomes clear that any absolutely irreducible element in $V_{\mathbb{Z}}$ must satisfy precisely one of the conditions enumerated in the second column of Table 1. In particular, there is no Case 5, because assuming any nonzero variables in Case 4 to be zero immediately results in reducibility by Lemma 87.

Let T denote the set of all eighteen variables a_{ij}, b_{ij} . For a subcase $\mathcal{C}$ of Table 2.1, we use $T_0 = T_0(\mathcal{C})$ to denote the set of variables in T assumed to be 0 in Subcase $\mathcal{C}$, and T_1 to denote the set of variables in T assumed to be nonzero.

Each variable $t \in T$ has a *weight*, defined as follows. The action of $a(s) \cdot \lambda$ on $(A, B) \in V$ causes each variable t to multiply by a certain weight which we denote by $w(t)$. These weights $w(t)$ are evidently rational functions in $\lambda, s_0, s_1, s_2, s_3, s_4$.

Let $V(\mathcal{C})$ denote the set of $(A, B) \in V_{\mathbb{R}}$ such that (A, B) satisfies the vanishing and nonvanishing conditions of Subcase $\mathcal{C}$. For example, in Subcase 2a we have $T_0(2a) = \{a_{11}, b_{11}\}$ and $T_1(2a) = \{a_{12}, a_{21}\}$; thus $V(2a)$ denotes the set of all $(A, B) \in V_{\mathbb{Z}}$ such that $a_{11} = b_{11} = 0$ but $a_{12}, a_{21} \neq 0$.

For each subcase $\mathcal{C}$ of Case n ($n > 0$), we wish to show that $N(V(\mathcal{C}); X)$, as defined by (2.17), is $O(X^{17/12})$. The equality (2.21) implies that

$$N^*(V(\mathcal{C}); X) \ll \int_{\lambda=c'}^{X^{1/12}} \int_{s_0, s_2, \dots, s_4=c}^{\infty} \sigma(V(\mathcal{C})) s_0^{-2} s_1^{-6} s_2^{-6} s_3^{-6} s_4^{-6} d^\times r d^\times s d^\times t d^\times \lambda, \quad (2.22)$$

where $\sigma(V(\mathcal{C}))$ denotes the number of integer points in the region $B(u, s, \lambda, X)$ that also satisfy the conditions

$$t = 0 \text{ for } t \in T_0 \text{ and } |t| \geq 1 \text{ for } t \in T_1. \quad (2.23)$$

Now for an element $(A, B) \in B(u, s, \lambda, X)$, we evidently have

$$|t| \leq Cw(t) \quad (2.24)$$

and therefore the number of integer points in $B(u, s, \lambda, X)$ satisfying (2.23) will be nonzero only if we have

$$Cw(t) \geq 1 \quad (2.25)$$

for all weights $w(t)$ such that $t \in T_1$. Now the sets T_1 in each subcase of Table 2.1 have been chosen to be precisely the set of variables having the minimal weights $w(t)$ among the variables $t \in T \setminus T_0$ (by “minimal weight” in $T \setminus T_0$, we mean there is no other variable $t \in T \setminus T_0$ with weight having smaller exponents for all parameters $\lambda, s_0, \dots, s_4$). Thus if the condition (2.25) holds for all weights $w(t)$ corresponding to $t \in T_1$, then—by the very choice of T_1 —we will also have $Cw(t) \gg 1$ for all weights $w(t)$ such that $t \in T \setminus T_0$.

Therefore, if the region $\mathcal{B} = \{(A, B) \in B(u, s, \lambda, X) : t = 0 \ \forall t \in T_0; \ |t| \geq 1 \ \forall t \in T_1\}$ contains an integer point, then (2.25) and Lemma 85 together imply that the number of integer points in $\mathcal{B}$ is $O(\text{Vol}(\mathcal{B}))$, since the volumes of all the projections of $u^{-1}\mathcal{B}$ will in that case also be $O(\text{Vol}(\mathcal{B}))$. Now clearly

$$\text{Vol}(\mathcal{B}) = O\left(C^{18-|T_0|} \prod_{t \in T \setminus T_0} w(t)\right),$$

so we obtain

$$N(V(\mathcal{C}); X) \ll \int_{\lambda=c'}^{X^{1/12}} \int_{s_1, s_2, \dots, s_7=c}^{\infty} \prod_{t \in T \setminus T_0} w(t) s_0^{-2} s_1^{-6} s_2^{-6} s_3^{-6} s_4^{-6} d^\times s d^\times \lambda \quad (2.26)$$

where the variables of integration are restricted by the conditions (2.25) for $t \in T_1$.

The integral (2.26) can be carried out in a straightforward manner for each of the eight subcases $\mathcal{C}$ occurring in Table 2.1. For example, consider Case 3a. The integral (2.26)

Case	The set $S \subset V_{\mathbb{Z}}$ defined by	$N(S; X) \ll$
0.	$a_{11} \neq 0$	$X^{18/12}$
1.	$a_{11} = 0$; $a_{12}, a_{21}, b_{11} \neq 0$	$X^{17/12}$
2a.	$a_{11}, b_{11} = 0$; $a_{12}, a_{21} \neq 0$	$X^{16/12}$
2b.	$a_{11}, a_{12} = 0$; $a_{13}, a_{21}, b_{11} \neq 0$	$X^{16/12} \log X$
2c.	$a_{11}, a_{21} = 0$; $a_{31}, a_{12}, b_{11} \neq 0$	$X^{16/12} \log X$
3a.	$a_{11}, a_{12}, a_{21} = 0$; $a_{13}, a_{31}, a_{22}, b_{11} \neq 0$	$X^{16/12}$
3b.	$a_{11}, a_{12}, b_{11} = 0$; $a_{21}, b_{12} \neq 0$	$X^{15/12} \log X$
3c.	$a_{11}, a_{21}, b_{11} = 0$; $a_{12}, b_{21} \neq 0$	$X^{15/12} \log X$
4.	$a_{11}, a_{12}, a_{21}, b_{11} = 0$; $a_{22}, b_{12}, b_{21} \neq 0$	$X^{14/12} \log X$

Table 2.1: Cases 1–4 occurring in the proof of Lemma 82.

then becomes

$$N(V(3a); X) \ll \int_{\lambda=c'}^{X^{1/12}} \int_{s_1, s_2, \dots, s_7=c}^{\infty} \prod_{t \in T \setminus T_0} (\lambda^{15} s_0^3 s_1^3 s_2^3 s_3^3 s_4^3) s_0^{-2} s_1^{-6} s_2^{-6} s_3^{-6} s_4^{-6} d^{\times} s d^{\times} \lambda, \quad (2.27)$$

where the variables of integration are restricted to the region

$$\frac{C s_3 s_4^2}{s_0 s_1^2 s_2} \geq 1, \quad \frac{C s_1 s_2^2}{s_0 s_3^2 s_4} \geq 1, \quad \frac{C s_1 s_3}{s_0 s_2 s_4} \geq 1, \quad \frac{C s_0}{s_1^2 s_2 s_3^2 s_4} \geq 1. \quad (2.28)$$

Choosing first to integrate over s_0 , and then over the other variables (which is then trivial), yields $O(X^{16/12})$, as given in the third column of Table 2.1.

The identical arguments may also be applied to the remaining subcases in Table 2.1, yielding the estimates listed in the third column of Table 2.1. This completes the proof. $\square$

Finally, Lemma 83 was a lemma about how many reducible boxes we were counting

when we use $N^*(S; X)$ instead of $N(S; X)$. In particular, we are in the case when $a_{11} \neq 0$.

Proof of Lemma 83. Recall we wish to show that the total contribution to $N^*(V; X)$ by reducible forms with $a_{11} \neq 0$ is $o(X^{3/2})$. To see this, consider the collection $(\mathcal{Z})_p \subseteq V_{\mathbb{Z}_p}$ consisting of the complement of those forms with splitting type (3). Then Proposition 80 and Figure 4.2 in Chapter 4 imply that the p -adic density of $(\mathcal{Z})_p$ is

$$\begin{aligned} 1 - \frac{1}{3} \cdot \frac{p^7(p-1)(p^2-1)^3(p^3-1)^2}{p^{20}} \cdot \frac{p^2}{p^2+p+1} &= 1 - \frac{1}{3} \cdot \frac{(p-1)^2(p^2-1)^3(p^3-1)}{p^{11}} \\ &= \frac{2}{3} + \frac{2p^{10} + 2p^9 - 5p^8 - 2p^7 + 4p^6 + 4p^5 - 2p^4 - 5p^3 + 2p^2 + 2p - 1}{p^{11}} \end{aligned}$$

and so in particular

$$\prod_p \mu_p((\mathcal{Z})_p) = 0 \quad (2.29)$$

Next we note that in the previous proof we saw that $N^*(V_{\mathbb{Z}}; X) = O(X^{3/2})$ and the proof of Theorem 86 shows that for any $Y > 0$

$$\lim_{X \rightarrow \infty} \frac{N^*(V^{\pm} \cap_{p < Y} (\mathcal{Z})_p; X)}{X^{3/2}} = O\left(\prod_{p < Y} \mu_p((\mathcal{Z})_p)\right)$$

where the constant is independent of Y . Letting Y run to infinity, we can immediately compute the lim sup to be

$$\limsup_{X \rightarrow \infty} \frac{N^*(V^{\pm} \cap (\mathcal{Z}); X)}{X^{3/2}} = 0.$$

In particular, $N^*((\mathcal{Z}); X) = o(X^{3/2})$.

□

2.9 A Sieve and the Proof of Theorem 40

So far we have shown how to compute the sum $N(S; X)$ for S defined by a *finite* number of congruence conditions. Of most interest to us are those congruence conditions which define the maximality of an order at a given prime, for if S corresponds to *maximal* cubic orders, then $N(S; X)$ is precisely the sum of the class number times the regulator of the associated cubic field. However, this S is defined by an *infinite* number of congruence conditions, we must use a sieve.

We let $\text{MAX} = \cap_p \text{MAX}_p$ be the set of all $f \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings $R(f)$. From Section 2.7, p -adic density of MAX_p is $\mu(\text{MAX}_p) = (p^2 - 1)^2(p^3 - 1)(p^8 + p^6 - 2p^5 - 2p^4 + 2p^2 + p - 1)/p^{15}$. From Theorem 86, we then know that

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{N(V^{\pm} \cap_{p < Y} \text{MAX}_p; X)}{X^{3/2}} \\ = \frac{\zeta(2)^3 \zeta(3)^2}{3n_{\pm}} \prod_{p < Y} \frac{(p^2 - 1)^2(p^3 - 1)(p^8 + p^6 - 2p^5 - 2p^4 + 2p^2 + p - 1)}{p^{15}} \end{aligned}$$

Now $\text{MAX} \subseteq \cap_{p < Y} \text{MAX}_p$, so $N(\text{MAX} \cap V^{\pm}; X) \leq N(V^{\pm} \cap_{p < Y} \text{MAX}_p; X)$. Thus, for all Y we have

$$\begin{aligned} \limsup_{X \rightarrow \infty} \frac{N(V^{\pm} \cap \text{MAX}; X)}{X^{3/2}} \\ \leq \frac{\zeta(2)^3 \zeta(3)^2}{3n_{\pm}} \prod_{p < Y} \frac{(p^2 - 1)^2(p^3 - 1)(p^8 + p^6 - 2p^5 - 2p^4 + 2p^2 + p - 1)}{p^{15}}. \end{aligned}$$

Since each factor in the product is less than 1, the right hand side is decreasing as $Y \rightarrow \infty$,

so we have that

$$\begin{aligned} \limsup_{X \rightarrow \infty} \frac{N(V^\pm \cap \text{MAX}; X)}{X^{3/2}} \\ \leq \frac{\zeta(2)^3 \zeta(3)^2}{3n_\pm} \prod_p \frac{(p^2 - 1)^2 (p^3 - 1) (p^8 + p^6 - 2p^5 - 2p^4 + 2p^2 + p - 1)}{p^{15}}. \end{aligned}$$

Now we would like to handle the $\liminf$. To do so, let $\mathcal{Z}_p$ be the sublattice of $V_\mathbb{Z}$ corresponding to triples $(\mathcal{O}, (I, I'))$ such that $\mathcal{O}$ is nonmaximal at p and one of the following is true:

- $\mathcal{O}$ is imprimitive at p ,
- $\mathcal{O}$ is primitive at p and I is globally invertible, or
- $\mathcal{O}$ is primitive and I is not proper at p .

We call these situations $\mathcal{Z}_p^{(1)}$, $\mathcal{Z}_p^{(2)}$, and $\mathcal{Z}_p^{(3)}$, respectively. Write $\mathcal{Z}_p = \mathcal{Z}_p^{(1)} \cup \mathcal{Z}_p^{(2)} \cup \mathcal{Z}_p^{(3)}$.

Lemma 88. *For any Y , we have that*

$$\text{MAX} = \left[\bigcap_{p < Y} \text{MAX}_p \right] - \left[\bigcup_{p \geq Y} \mathcal{Z}_p \right].$$

Proof. Certainly $\text{MAX} \subseteq \bigcap_{p < Y} \text{MAX}_p$ and by definition $\text{MAX} \cap \mathcal{Z}_p = \emptyset$.

In the other direction, we note that we are assuming first that $\mathcal{O}$ is maximal at all primes less than Y , so if $\mathcal{O}$ is nonmaximal then it must be nonmaximal at some prime $p \geq Y$. At this prime, it can either be imprimitive ($\mathcal{Z}_p^{(1)}$) or primitive. So suppose that $\mathcal{O}$ is globally primitive. Then since $\mathcal{O}$ is cubic it is Gorenstein [56, Theorem 5.12], and hence I being globally invertible is equivalent to being globally proper. So the lemma is proved. $\square$

As such,

$$N(V^\pm \cap \text{MAX}; X) = N(V^\pm \bigcap \bigcap_{p < Y} \text{MAX}_p; X) - N\left(\bigcup_{p \geq Y} V^\pm \cap \mathcal{Z}_p; X\right) \quad (2.30)$$

$$\geq N(V^\pm \bigcap \bigcap_{p < Y} \text{MAX}_p; X) - \sum_{p \geq Y} N(V^\pm \cap \mathcal{Z}_p; X). \quad (2.31)$$

So for *every* Y , we have that

$$\liminf_{X \rightarrow \infty} \frac{N(V^\pm \cap \text{MAX}; X)}{X^{3/2}} \geq \liminf_{X \rightarrow \infty} \frac{N(V^\pm \bigcap \bigcap_{p < Y} \text{MAX}_p; X)}{X^{3/2}} - \limsup_{X \rightarrow \infty} \sum_{p \geq Y} \frac{N(V^\pm \cap \mathcal{Z}_p; X)}{X^{3/2}}.$$

Now we know from Theorem 86 that the $\liminf$ on the right hand side is equal to

$$\begin{aligned} \liminf_{X \rightarrow \infty} \frac{N(V^\pm \bigcap \bigcap_{p < Y} \text{MAX}_p; X)}{X^{3/2}} &= \frac{\zeta(2)^3 \zeta(3)^2}{3n_\pm} \prod_{p < Y} \frac{(p^2 - 1)^2 (p^3 - 1)(p^8 + p^6 - 2p^5 - 2p^4 + 2p^2 + p - 1)}{p^{15}}. \end{aligned}$$

So we are left to deal with the $\limsup$ on the right hand side. But by Fatou's Lemma, we know that

$$\limsup_{X \rightarrow \infty} \sum_{p \geq Y} \frac{N(V^\pm \cap \mathcal{Z}_p; X)}{X^{3/2}} \leq \sum_{p \geq Y} \limsup_{X \rightarrow \infty} \frac{N(V^\pm \cap \mathcal{Z}_p; X)}{X^{3/2}}.$$

So we are left with determining the $\limsup$ s in the various addends. The main result is the following lemma.

Lemma 89. *We have that*

$$\limsup_{X \rightarrow \infty} \frac{N(V^\pm \cap \mathcal{Z}_p; X)}{X^{3/2}} \ll \frac{1}{p^2}.$$

We prove this lemma in the following sections by showing that each $N(\mathcal{Z}_p^{(i)}; X) \ll X/p^2$.

This lemma then implies that

$$\sum_{p \geq Y} \limsup_{X \rightarrow \infty} \frac{N(V^\pm \cap \mathcal{Z}_p; X)}{X^{3/2}} \ll \frac{1}{Y},$$

and so sending $Y \rightarrow \infty$ yields that the $\liminf$ is bounded below by the same quantity as the $\limsup$, and hence we have proved the main theorem.

Remark 90. Here we would like to thank A. Shankar for pointing out that our first version of the proof of Lemma 89 was incorrect. That proof was in the style of Bhargava's uniformity estimates in [12, 15], which is sufficient for $\mathcal{Z}_p^{(1)}$ and $\mathcal{Z}_p^{(3)}$. However, we eventually saw that $\mathcal{Z}_p^{(2)}$ is much more problematic than first believed. We discuss in Section 2.9.2 why this method of proof fails for $\mathcal{Z}_p^{(2)}$ and provide an alternate proof based on average case methods.

2.9.1 The imprimitive and improper cases

Lemma 91. *We have that*

$$\limsup_{X \rightarrow \infty} \frac{N(\mathcal{Z}_p^{(1)}; X)}{X^{3/2}} \ll \frac{1}{p^{4-\varepsilon}}.$$

Proof. If $(A, B) \in V_{\mathbb{Z}}$ corresponds to $(\mathcal{O}, (I, I'))$ and $\mathcal{O}$ is imprimitive at p , then we know that $f(x, y) = \det(Ax - By) \equiv 0 \pmod{p}$. The coefficients of f over $\mathbb{Z}$ are algebraically independent and cut out a subvariety of $V_{\mathbb{Z}}$ of codimension 4. As such, we know that $\mathcal{Z}_p^{(1)}$ is a subset of $V_{\mathbb{Z}}$ cut out by congruence conditions of codimension 4. So Theorem 86 and the Weil conjectures imply that

$$\limsup_{X \rightarrow \infty} \frac{N(\mathcal{Z}_p^{(1)}; X)}{X^{3/2}} \ll \frac{1}{p^{4-\varepsilon}}$$

with the implied constant *independent* of p . □

Next consider the case of $\mathcal{Z}_p^{(3)}$. (We will handle $\mathcal{Z}_p^{(2)}$ in the next section.)

Lemma 92. *When $\mathcal{O}$ is primitive at p and I is improper at p , there is some $\mathcal{O}'$ such that $\mathcal{O} \subseteq \mathcal{O}' \subseteq (I : I)$ such that I is an ideal of $\mathcal{O}'$ and $[\mathcal{O}' : \mathcal{O}] = p$.*

Proof. Note that we are under the jurisdiction of Lemma 81. In case (iii) it is easy to see that $\det(Ax - By) \equiv 0 \pmod{p}$ so $\mathcal{O}$ is imprimitive at p , and hence we are in case (i) or case (ii).

Suppose that we are in case (i). Then we may assume that either $A \equiv 0 \pmod{p}$ or $A = cB \pmod{p}$ for some $c \in \mathbb{F}_p^\times$ with $\det(B) \not\equiv 0 \pmod{p}$. In the first case, it is obvious that $-\omega$ acts by 0 on both I and I' from (2.10). On other hand, the determinant of the matrix which is the same as B but with a single row or column exchanged with the same row or column of A , then the linearity of the determinant implies that $-\omega$ acts by $-c \det(B)$ on both I and I' .

Now suppose we are in case (ii). Since A has rank 1, so does its transpose, and so $-\omega$ acts by 0 on both I and I' according to (2.10). So we have shown that both I and I' are $\mathcal{O}'$ ideals. Moreover, $II' \subseteq \mathcal{O} \subseteq \mathcal{O}'$ and the *product* of the norms of I and I' remain the same. As such, I' is *still* a weak inverse of I . $\square$

Note that $\rho(I, I')$ depends *only* on the pair (I, I') , and hence regulator *also* only depends on the pair (I, I') . Similarly, since we are considering the case when $\mathcal{O}$ is nondegenerate, we know that the equivalence of (I, I') and (J, J') only depends on elements of $\mathcal{O} \otimes \mathbb{Q}$. So the sum of the regulators of (I, I') over ideal classes of $\mathcal{O}$ is bounded above by the sum of the regulators of (I, I') over ideal classes of $\mathcal{O}'$ times the total number of subrings of $\mathcal{O}'$ of index p .

To arrive at this latter bound, we break the remainder of $\mathcal{Z}_p^{(3)}$ into two further subsets based upon $\mathcal{O}'$ in the previous lemma. Let $\mathcal{Z}_p^{(3\text{prim})}$ consist of those triples for which $\mathcal{O}'$ is primitive, and $\mathcal{Z}_p^{(3\text{imp})}$ consist of those triples for which $\mathcal{O}'$ is imprimitive.

Lemma 93. *We have that*

$$\limsup_{X \rightarrow \infty} \frac{N\left(\mathcal{Z}_p^{(3\text{prim})}; X\right)}{X^{3/2}} \ll \frac{1}{p^3}.$$

Proof. If $\mathcal{O}'$ is primitive, then we know from [19, Lemma 30] that there are at most 3 subrings of $\mathcal{O}'$ of index p . Moreover, $\Delta(\mathcal{O}') = \Delta(\mathcal{O})/p^2$. Combining these facts, we find that

$$\frac{N\left(\mathcal{Z}_p^{(3\text{prim})}; X\right)}{X^{3/2}} \ll \frac{N\left(V; \frac{X}{p^2}\right)}{X^{3/2}} \ll \frac{1}{p^3}.$$

□

Lemma 94. *We have that*

$$\limsup_{X \rightarrow \infty} \frac{N\left(\mathcal{Z}_p^{(3\text{imp})}; X\right)}{X^{3/2}} \ll \frac{1}{p^{5-\varepsilon}}.$$

Proof. If $\mathcal{O}'$ is imprimitive, then we no longer have the bound of [19, Lemma 30], but we do have that there are $O(p^2)$ sublattices of $\mathcal{O}'$ of index p . As such, we may compute (using Lemma 91)

$$\limsup_{X \rightarrow \infty} \frac{N\left(\mathcal{Z}_p^{(3\text{imp})}; X\right)}{X^{3/2}} \ll \limsup_{X \rightarrow \infty} \frac{p^2 N\left(\mathcal{Z}_p^{(1)}; \frac{X}{p^2}\right)}{X^{3/2}} \ll \frac{1}{p^{5-\varepsilon}}.$$

□

2.9.2 Invertible ideals in nonmaximal rings

We now address the set $\mathcal{Z}_p^{(2)}$ which consists of triples $(\mathcal{O}, (I, I'))$ with $\mathcal{O}$ nonmaximal and primitive but I globally invertible. We first explain why the style of proof where we use worst case bounds on the addends of the sum $N(\mathcal{Z}_p^{(2)}; X)$ presents major difficulties. Then we prove our bound by turning to *average* case methods.

Why worst case bounds fail

The total number of triples in $\mathcal{Z}_p^{(2)}$ is bounded above by the product of

- the total number of cubic rings which are nonmaximal at p , i.e., how many $\mathcal{O}$ are there, and
- the maximum size of the class number times the regulator of a primitive cubic ring with discriminant at most X .

We now give a heuristic that such bounds will *not* yield any uniformity of the form $N(\mathcal{Z}_p^{(2)}; X)/X^{3/2} \ll 1/p^{1+\delta}$ for any $\delta > 0$.

To the first bullet point, we recall Proposition 29 of [19], which states that the total number of cubic rings with discriminant at most X which are nonmaximal at p is $O(X/p^2)$. As to the second bullet point, we have a theorem of Sands, which is as follows.

Theorem 95 ([96]). *Suppose that $\mathcal{O}$ is an order in a number field of degree n . Then*

$$h(\mathcal{O}) \operatorname{Reg}(\mathcal{O}) \ll_n \Delta(\mathcal{O})^{1/2} (\log \Delta(\mathcal{O}))^{n-1} (\log \log \Delta(\mathcal{O}))^{n/2}.$$

As such, we see⁸ from (the proof of) Theorem 86

$$\frac{N(\mathcal{Z}_p^{(2)}; X)}{X^{3/2}} \ll \frac{1}{X^{3/2}} \cdot \frac{X}{p^2} \cdot X^{1/2} (\log X)^2 (\log \log X)^{1/2} + pX^{-1/12}.$$

So in order that $N(\mathcal{Z}_p^{(2)}; X) \ll O(X/p^{1+\delta})$ for some δ , we will need $p \gg \log^{3/2+\delta'} X$ where $\delta' > \delta/2$. So we will need to send Y and X to ∞ simultaneously with Y growing like $\log^{3/2+\delta'} X$.

⁸ The uniformity claimed here is not exactly proven in Theorem 86. In particular, the constant there depends on m being fixed! In order to get a uniform bound in p and X , one must convert the argument to using a homogeneously expanding region, as, for example is done in [12].

However, Theorem 86 is also how we were able to write

$$N(V^\pm \bigcap \cap_{p < Y} \text{MAX}_p; X) = C \prod_{p < Y} \mu_p(S_p) + O(X^{-1/12} m).$$

But the condition of being maximal at p is a congruence condition modulo p^2 , so here $m = \prod_{p < Y} p^2$ by the Chinese Remainder Theorem. For *fixed* Y , this allowed us to immediately take the limit. But if Y is varying, then in order to obtain uniformity in the error term, we must have that $\prod_{p < Y} p^2 = o(X^{1/12})$.

But we know that the Chebyshev function $\left| \sum_{p < Y} \log(p) - Y \right| \ll Y/\log(Y)$, and so in particular, we know that

$$\prod_{p < Y} p = \exp[(1 + o(1))Y].$$

So in order that $m = \prod_{p < Y} p^2 = o(X^{1/12})$ we would need to take $Y \ll \log(X)$, which is in particular strictly smaller than $\log^{2+\delta'}(X)$.

So in order to continue with this method of simply using worst case bounds, we would either have to improve estimates on the number of everywhere primitive rings which are nonmaximal at p or we would have to improve Sands bound.

For the latter point, there is some chance that the $\sqrt{\log \log X}$ could be saved. But the bound without the $\sqrt{\log \log X}$ is exactly Siegel's version of Sands' theorem when $\mathcal{O}$ is maximal, so we probably should not hope for much.

As to improving the number of everywhere primitive rings which are nonmaximal at p , we note that Proposition 15 of [19] tells us that if $\mathcal{O}$ corresponds to the binary cubic form $f \not\equiv 0 \pmod{p}$, then the total number of subrings of $\mathcal{O}$ is the total number of roots of f modulo p . So the total number of primitive rings which are nonmaximal at p with discriminant at most X is bounded *below* by the total number of *maximal* rings with discriminant at most X/p^2 which do have splitting type (3) at p . But we have already seen in the proof of Lemma 83 $\mu_p((\mathcal{O}_p)^\times) = 2/3 + O(1/p)$ as $p \rightarrow \infty$. Hence, we have a lower bound of $\Omega(X/p^2)$.

Average case methods

In this section, we obtain bounds for $\mathcal{Z}_p^{(2)}$ based on some analytic techniques. These are a preview of Chapter 4.

First, by partial summation⁹ we have already shown in this chapter that

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{\Delta(\mathcal{O}) < X} L(\mathcal{O}, 1) = C \quad (2.32)$$

where the sum is over all orders in number fields with $\Delta(\mathcal{O}) < X$ and C is a finite, nonzero constant. Moreover, by the same partial summation computation, to show that $N(\mathcal{Z}_p^{(2)}; X) \ll X/p^2$, we need only show that

$$\sum_{\substack{\Delta(\mathcal{O}) < X \\ (\mathcal{O}, (I, I')) \in \mathcal{Z}_p^{(2)}}} L(\mathcal{O}, 1) \ll X/p^2 \quad (2.33)$$

where the implied constant is independent of p .

Now for any triple $(\mathcal{O}, (I, I'))$ corresponding to points in $\mathcal{Z}_p^{(2)}$ we have that $\mathcal{O}$ is non-maximal at p . Thus, we may invoke the Davenport-Heilbronn correspondence of Lemma 71. Since $\mathcal{O}$ is primitive, we know that we must be in case (i). So $[\mathcal{O}' : \mathcal{O}] = p$.

Let us compare the L -functions of $\mathcal{O}$ and $\mathcal{O}'$ at 1. Note that $L_q(\mathcal{O}, s) = L_q(\mathcal{O}', s)$ for all primes $q \neq p$ since $\mathcal{O}'_q = \mathcal{O}_q$. So the only thing left to compare is $L_p(\mathcal{O}, 1)$ and $L_p(\mathcal{O}', 1)$.

Lemma 96. *Let $\mathcal{O}$ be an order in a cubic number field which is nonmaximal at p . Then $L_p(\mathcal{O}, 1) = 1$.*

Proof. There are only six possible values of $\mathcal{O} \otimes \mathbb{F}_p$. Of these, four imply that the discriminant of $\mathcal{O}$ is divisible by at most one power of p , which is not possible since $\Delta(\mathcal{O}) = p^2 \Delta(\mathcal{O}')$. The two remaining possibilities are $\mathbb{F}_p[x]/(x^3)$ and $\mathbb{F}_p[x]/(x, y)^2$. In either case, it is easy to calculate that $L_p(\mathcal{O}, 1) = 1$. □

⁹See Section 4.2.1 for details.

Lemma 97. *For $\mathcal{O}$ an order in a cubic number field, $L_p(\mathcal{O}, 1) \geq 1$ unless $\mathcal{O} \otimes \mathbb{F}_p$ is a field.*

Proof. This is a simple calculation. See Table 4.2 for the exact values. $\square$

So now we are in a position to compute (2.33). To do so, we divide $\mathcal{Z}_p^{(2)}$ into two sets: either $\mathcal{O}'$ is primitive or it is not. We call the first set $\mathcal{Z}_p^{(2\text{prim})}$ and the second set $\mathcal{Z}_p^{(2\text{imp})}$. In both cases we proceed much like our computations for $\mathcal{Z}_p^{(3)}$.

Lemma 98. *We have that $N(\mathcal{Z}_p^{(2\text{prim})}; X) \ll X/p^2$.*

Proof. By Lemma 30 of [19], we know that $\mathcal{O}'$ has at most 3 subrings of index p . Also, we note that if $\mathcal{O}' \otimes \mathbb{F}_p$ is a field, then Lemma 96 and Table 4.2 imply that

$$L_p(\mathcal{O}, 1) = \frac{p^2 + p + 1}{p^2} L(\mathcal{O}', 1).$$

Combining all these facts with Lemma 97 we find that

$$\sum_{\substack{\Delta(\mathcal{O}) < X \\ \mathcal{O}' \text{ primitive}}} L(\mathcal{O}, 1) \ll \sum_{\substack{\Delta(\mathcal{O}') < X/p^2 \\ \tau(\mathcal{O}') \neq (3)}} L(\mathcal{O}', 1) + \frac{p^2 + p + 1}{p^2} \sum_{\substack{\Delta(\mathcal{O}') < X/p^2 \\ \tau(\mathcal{O}') = (3)}} L(\mathcal{O}', 1).$$

Allowing both sums to range over *all* orders in number fields with norm discriminant less than X/p^2 allows us to apply (2.32), which says that both sums are $\ll X/p^2$. But then arithmetic tells us that the right hand side is $\ll X/p^2$. $\square$

Lemma 99. *We have that $N(\mathcal{Z}_p^{(2\text{imp})}; X) \ll X/p^{4-\varepsilon}$.*

Proof. In this case, $\mathcal{O}'$ has $O(p^2)$ subrings of index p . So as in the previous lemma, we may write

$$\sum_{\substack{\Delta(\mathcal{O}) < X \\ \mathcal{O}' \text{ is imprimitive}}} L(\mathcal{O}, 1) \ll p^2 \sum_{\substack{\Delta(\mathcal{O}') < X/p^2 \\ \mathcal{O}' \text{ imprimitive}}} L(\mathcal{O}', 1).$$

Note that we do not have to separate the sum by the splitting type of $\mathcal{O}'$ since $\mathcal{O}'$ is imprimitive, hence nonmaximal, and hence Lemma 96 applies. But now by partial summation

and Lemma 91 we know that the sum on the right is $O(X/p^{6-\epsilon})$. So by multiplying by p^2 , we arrive at the statement of the lemma. $\square$

2.A Appendix: Comment on Conjecture 65

In this appendix, we address a problem with extending Conjecture 65 to local almost trivial local specifications when the degree d of the order is sufficiently large. In fact, we show

Proposition 100. *For $d \gg 0$ we have that $c(\Sigma)$ is infinite, where Σ is the trivial collection of local specifications.*

The proof begins with two simple lemmas.

Lemma 101. *Suppose that B is a commutative ring and that S is a B algebra. Suppose further that $b \in B$. Then $R = B + bS$ is a B subalgebra of S .*

Proof. Since any two elements of R can be written as $a_i + bs_i$ with $i = 1, 2$, we see that $(a_1 + bs_1) + (a_2 + bs_2) = (a_1 + a_2) + b(s_1 + s_2)$. But $a_1 + a_2 \in B$ since B is a ring and $s_1 + s_2 \in S$ since S is a B module. Hence the lemma. $\square$

Lemma 102. *Suppose that B , S , and b are as in Lemma 101. Now suppose that $R \subseteq B + bS$ is some B submodule of S , i.e., it is closed under addition. If we further have that $B + b^2S \subseteq R$ then R is actually a subalgebra of S , i.e., it is closed under multiplication.*

Proof. Let $a_i + bs_i \in R$ with $i = 1, 2$ and $a_i \in B$ and $s_i \in S$. Then $(a_1 + bs_1)(a_2 + bs_2) = a_1a_2 + b(a_1s_2 + a_2s_1) + b^2s_1s_2$. Since $a_1, a_2 \in B$ we know that $a_1(a_2 + bs_2) + a_2(a_1 + bs_1) = 2a_1a_2 + b(a_1s_2 + a_2s_1) \in R$, and since $a_1a_2 \in B$ we know that $a_1a_2 + b(a_1s_2 + a_2s_1) \in R$. So it suffices to show that $b^2s_1s_2 \in R$. But $b^2s_1s_2 \in b^2S \subseteq R$ by assumption. $\square$

To examine the consequences of Lemmas 101 and 102, fix $\mathcal{O}_p$ a nondegenerate, unramified¹⁰ degree d extension of $\mathbb{Z}_p$ for some prime p . That is, $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$ for the ring of

¹⁰These restrictions are not necessary for our analysis to go through, but they make some computations easier.

integers $\mathcal{O}$ of some degree d number field unramified at p . Then according to the lemmas, every sublattice R of $\mathcal{O}_p$ such that

$$\mathbb{Z}_p + p^2\mathcal{O}_p \subseteq R \subseteq \mathbb{Z}_p + p\mathcal{O}_p$$

is actually a subring.

Now the number of automorphisms of R is bounded above by the number of automorphisms of $k_p = \mathcal{O}_p \otimes \mathbb{Q}_p$ since any automorphism of R must extend to an automorphism of k_p . So let us further fix k_p to be the *cyclic* field extension of $\mathbb{Q}_p$ so that the number of automorphisms of R is bounded above by d .

Further, we know that if R' is another lattice between $\mathbb{Z}_p + p^2\mathcal{O}_p$ and $\mathbb{Z}_p + p\mathcal{O}_p$ such that there exists an abstract isomorphism $\varphi : R \rightarrow R'$ of $\mathbb{Z}_p$ algebras, then φ extends to an abstract *automorphism* of $R \otimes \mathbb{Q}_p = R' \otimes \mathbb{Q}_p = k_p$ via the inclusion mappings. Hence, there are at most d distinct sublattices between $\mathbb{Z}_p + p^2\mathcal{O}_p$ and $\mathbb{Z}_p + p\mathcal{O}_p$ which are isomorphic to R .

Now recall that $c(\Sigma)$ was defined as

$$c(\Sigma) = \left(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{\# \text{Aut}_{\mathbb{R}}(R)} \right) \prod_{p \text{ finite}} \frac{p-1}{p} \sum_{R \in \Sigma_p} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}(R/\mathbb{Z}_p)}. \quad (2.34)$$

So by combining the two previous paragraphs, we know that the sum in (2.34) for a fixed finite p is bounded below by

$$\sum_{\substack{[R] \text{ an isomorphism class of} \\ \mathbb{Z}_p + p^2\mathcal{O}_p \subseteq R \subseteq \mathbb{Z}_p + p\mathcal{O}_p}} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\text{Aut}(R)} \geq \frac{1}{d^2} \sum_{\mathbb{Z}_p + p^2\mathcal{O}_p \subseteq R \subseteq \mathbb{Z}_p + p\mathcal{O}_p} \frac{1}{\text{Disc}_p(R)}, \quad (2.35)$$

where the first sum is over a set of representatives of isomorphism classes of such R .

But $\text{Disc}_p(R) = n^2 \text{Disc}_p(\mathcal{O}_p)$ where¹¹ $n = [\mathcal{O}_p : R]$ is the index of R in $\mathcal{O}_p$. Since we

¹¹This relies on the fact that we are concerned here with the absolute discriminant over $\mathbb{Z}_p$, for it relies

have assumed that $\mathcal{O}_p$ is unramified, we know that $\text{Disc}_p(R) = n^2$. But the index of R in $\mathcal{O}_p$ is p^{d-1} times the index of the *image* of R in $(\mathbb{Z}_p + p\mathcal{O}_p)/(\mathbb{Z}_p + p^2\mathcal{O}_p) \cong (\mathbb{Z}/p\mathbb{Z})^{d-1}$. Moreover, R is determined by its image. As such, we know that the right hand side of (2.35) is equal to

$$\frac{1}{d^2} \sum_{r=0}^{d-1} \frac{\# \text{Gr}(r, d-1; p)}{p^{2(d-1+r)}} \quad (2.36)$$

where $\text{Gr}(r, d-1; p)$ is the Grassmannian of r planes in $d-1$ space over $\mathbb{F}_p$.

Now the Grassmannian $\text{Gr}(r, m; p)$ is a homogenous space for $\text{GL}_m(\mathbb{F}_p)$ whose stabilizing parabolic consists of matrices of the form

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

where $A \in \text{GL}_r(\mathbb{F}_p)$ and the matrix as a whole is invertible. This leads to the well-known formula for the order of the Grassmannian

$$\begin{aligned} \# \text{Gr}(r, m; p) &= \frac{(p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})}{(p^r - 1)(p^r - p) \cdots (p^r - p^{r-1})(p^m - p^r)(p^m - p^{r+1}) \cdots (p^m - p^{m-1})} \\ &= \frac{(p^m - 1) \cdots (p^m - p^{r-1})}{(p^r - 1) \cdots (p^r - p^{r-1})} \\ &= \frac{(p^m - 1) \cdots (p^{m-r+1} - 1)}{(p^r - 1) \cdots (p - 1)}. \end{aligned} \quad (2.37)$$

This is in turn at least

$$\frac{(p^m - 1) \cdots (p^{m-r+1} - 1)}{p^{\binom{r+1}{2}}}.$$

Consider then the case when $r = \lfloor d/2 \rfloor$. Then as $d \rightarrow \infty$ we have that

$$\# \text{Gr}(r, d-1; p) \geq \frac{(p^{d-1} - 1) \cdots (p^{d-r} - 1)}{p^{\binom{r+1}{2}}} \sim p^{(d-1)+(d-2)+\cdots+\lfloor d/2 \rfloor - \binom{\lfloor d/2 \rfloor + 1}{2}}$$

on the structure theorem of modules over PIDs like $\mathbb{Z}_p$.

The total in the exponent of p in the above is asymptotically $d^2/4$. But the exponent of the denominator of the $r = \lfloor d/2 \rfloor$ th term of the sum in (2.36) is *linear* in d . As such, the quotient

$$\frac{\# \text{Gr}(\lfloor d/2 \rfloor, d-1; p)}{p^{2(d-1+\lfloor d/2 \rfloor)}}$$

grows much faster than d^2 , and hence the p th factor of (2.34) eventually becomes strictly greater than 3. In fact, if this is true for $p = 2$, then it is true for *all* primes. Then

$$\frac{p-1}{p} \sum_{R \in \Sigma_p} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}(R)}$$

is bounded away from 1 for all p , and hence the product in (2.34) is infinite.

Chapter 3

Asymptotics of the Square of the Class Number Times the Regulator of Quadratic Fields and Orders

3.1 Introduction

In Chapter 2, we used the geometry of numbers to give asymptotics for the sum

$$\sum_{\Delta(\mathcal{O}) < X} h(\mathcal{O}) \operatorname{Reg}(\mathcal{O}) \tag{3.1}$$

where $\mathcal{O}$ ran over (subsets of) cubic rings with $\Delta_{\mathcal{O}} = |\operatorname{Disc}(\mathcal{O})|$ is the absolute discriminant of $\mathcal{O}$, $h(\mathcal{O})$ is the ideal class number of $\mathcal{O}$, and $\operatorname{Reg}(\mathcal{O})$ is its regulator. This method was analogous to the work of Siegel [101] using binary quadratic forms to compute the same number for orders in quadratic fields.

In that chapter, we also computed the sum (3.1) when the class number was replaced by the total number of *proper* ideal classes. In this chapter, we see in Section 3.4 that for quadratic rings, an ideal is proper if and only if it is invertible. So this distinction will be

meaningless.

There is one more prehomogeneous vector space known whose integral orbits correspond to ideals in orders in number fields. This is the space of $2 \times 2 \times 2$ boxes, which corresponds roughly to pairs of ideals in quadratic orders (see Section 3.3 or [9] for the original reference). As such, we should be able to compute

$$\sum_{\Delta(\mathcal{O}) < X} h(\mathcal{O})^2 \text{Reg}(\mathcal{O})^2 \quad (3.2)$$

as $\mathcal{O}$ ranges over (some nice subsets of) orders in quadratic number fields. This we accomplish in Section 3.6 and Section 3.7. Our result is the following, which the reader should compare to the main theorem of Chapter 2.

Theorem 103. *Let $M^\pm(X)$ be the sum*

$$M^\pm(X) = \sum_{0 < \pm \text{Disc}(\mathcal{O}) < X} h(\mathcal{O})^2 \text{Reg}(\mathcal{O})^2 \quad (3.3)$$

be the sum of the square of the class number times the regulator of quadratic orders with $0 < \pm \text{Disc}(\mathcal{O}) < X$. Then

$$M^\pm(X) \sim X^2 \frac{\zeta(2)^2}{2n_\pm} \prod_p (1 - 3p^{-3} - p^{-4} + 4p^{-5} - p^{-7})$$

Similarly, if $N^\pm(X)$ is (3.3) restricted to maximal orders, then

$$N^\pm(X) \sim X^2 \frac{\zeta(2)^3}{2n_\pm} \prod_p (1 - p^{-2} - 3p^{-3} + 2p^{-4} + 4p^{-5} - 3p^{-6} - p^{-7} + p^{-8})$$

3.2 Points in Products of Projective Spaces

In [14, Section 2], Bhargava points out that the parameterization of rank n étale $\mathbb{Q}$ algebras amounts to finding a parameterization of all the dimension 0 subschemes of $\mathbb{P}_{\mathbb{Q}}^{n-2}$ such that geometrically the scheme consists of n distinct points in linearly general position¹. For $n = 3$, such points are cut out by a single binary cubic form. For $n = 4$, such points are the complete intersection of two ternary quadratic forms. Finally, for $n = 5$, the famous structure theorem of Buchsbaum–Eisenbud [25] implies that they are cut out by the Pfaffians of a 5×5 skew-symmetric matrix of linear forms on $\mathbb{P}^3$.

In fact, each of these parameterizations comes from looking at the minimal free resolution of the points. Indeed, each of these minimal free resolutions has a canonical multiplicative structure (for $n = 3, 4$ it is the Koszul complex; for $n = 5$ it is the Buchsbaum–Eisenbud multiplication) from which you can recover the ring structure Bhargava explicitly writes down in [11, 14]. Wood worked out the details over an arbitrary base for $n = 3, 4$ in her thesis [114, 113], and the present author has made some strides toward the general theory for $n = 5$ (see Chapters 5 and 7).

But the present chapter is about *ideals* in rank n rings. When a rank n ring over $\mathbb{Z}$ is maximal, then fractional ideal classes are the same as line bundles on $\mathrm{Spec} R \rightarrow \mathrm{Spec} \mathbb{Z}$. But line bundles on $\mathrm{Spec} R$ give embeddings into projective space, specifically $\mathbb{P}_{\mathbb{Z}}^{n-1}$. More generally, m -tuples $(I_1, \dots, I_m)$ of line bundles give embeddings of $\mathrm{Spec} R$ into $(\mathbb{P}_{\mathbb{Z}}^{n-1})^m$. So if we want parameterizations of m -tuples of ideals of rank n rings, we should be trying to determine the minimal free resolution of sets of n general points in $(\mathbb{P}_k^{n-1})^m$ over a field k and hope that we can extend that insight to work over $\mathbb{Z}$.

The structure theory of codimension $d > 2$ schemes in $\mathbb{P}^n$ is very complicated. However, when $d = 1, 2$, it is very well-known. But then there are only three cases we could hope to cover: 2 points in $\mathbb{P}^1$, 3 points in $\mathbb{P}^2$, or 2 points in $\mathbb{P}^1 \times \mathbb{P}^1$.

¹This means that no $n - 2$ points lie on a hyperplane.

Well, 2 points in $\mathbb{P}^1$ are cut out by binary quadratic forms. Indeed, this yields a parameterization of the ideal classes in quadratic rings first noticed by Gauss (his so-called *Gauss composition*). In the case of 3 points in $\mathbb{P}^2$, we may apply the Hilbert-Burch theorem [46, Theorem 3.1] to see that such points are cut out by the 2×2 minors of a 3×2 matrix of linear forms on $\mathbb{P}^2$. That is, ideals in cubic rings should correspond to equivalence classes of $2 \times 3 \times 3$ boxes. This theory over $\mathbb{Z}$ is the content of [10] which we have discussed in Chapter 2.

Finally we come to the case of concern in this chapter: 2 points in $\mathbb{P}^1 \times \mathbb{P}^1$. Suppose that $X \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ is a pair of points. We will write the points of X as (x^i, y^i) where $i = 1, 2$ and $x^i = [x_0^i : x_1^i]$ and $y^i = [y_0^i : y_1^i]$. We say a pair of points X is *general* if $x^1 \neq x^2$ and $y^1 \neq y^2$. Then immediately we see that this precludes either a $(1, 0)$ or a $(0, 1)$ form from vanishing on X .

On the other hand, we see that a pair of $(1, 1)$ forms *do* vanish on X . Specifically, let f_x^i be the linear form cutting out $x^i \in \mathbb{P}^1$ and let f_y^i be the linear form cutting out $y^i \in \mathbb{P}^1$. Then the pair of forms $f_x^1 f_y^2$ and $f_x^2 f_y^1$ will be $(1, 1)$ forms which cut out *precisely* X .

In the other direction, a pair (f, g) of $(1, 1)$ forms on $\mathbb{P}^1 \times \mathbb{P}^1$ will cut out two points when the projections to each $\mathbb{P}^1$ factor consist of two distinct points. Indeed, viewing the pencil (f, g) as a pair of 2×2 matrices A, B , we see that the degenerate forms are precisely $rf - sg$ where (r, s) satisfies $\det(Ar - Bs) = 0$. Now in $\mathbb{P}^1 \times \mathbb{P}^1$, a degenerate $(1, 1)$ form gives precisely $x \times \mathbb{P}^1$ and $\mathbb{P}^1 \times y$. In particular, we see that a pair of $(1, 1)$ forms will cut out a pair of generic points precisely when $\det(Ar - Bs)$ has two *distinct* zeros. But this occurs precisely when the *discriminant* of $\det(Ar - Bs)$ is nonzero. Such a pair we call *nondegenerate*. This is exactly the invariant that we will describe in Section 3.3 when we discuss Bhargava's parameterization of pairs of ideal classes.

So we have seen that a pair of nondegenerate points in $\mathbb{P}^1 \times \mathbb{P}^1$ is cut out by a pair of $(1, 1)$ forms with nonzero discriminant. After choosing bases, we may identify such pairs with

elements of $V_k = k^2 \otimes k^2 \otimes k^2$. Moreover, since these two points are a complete intersection, we know that the two points determine the ideal and vice-versa. In particular, if we consider *equivalence classes* of pairs of points in $\mathbb{P}^1 \times \mathbb{P}^1$, i.e., pairs of points up to the action of $\mathrm{GL}_2(k) \times \mathrm{GL}_2(k)$, then we see the set of all pairs of $(1, 1)$ forms which cut out those equivalence classes form a single orbit in $k^2 \otimes k^2 \otimes k^2$ under the action of $\bar{G}(k) = \mathrm{GL}_2(k) \times \mathrm{GL}_2(k) \times \mathrm{GL}_2(k)$.

In fact, we readily see that this construction is Galois invariant. In particular, if $X \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ is a codimension 2 degree 2 subscheme which geometrically consists of a pair of general points, then X is the complete intersection of a pair of $(1, 1)$ forms. This implies the following theorem.

Theorem 104. *Let k be a field with separable closure $\bar{k}$. Then there is a canonical bijection between $\bar{G}(k)$ orbits on V_k and codimension 2, degree 2 subschemes of $\mathbb{P}_k^1 \times \mathbb{P}_k^1$ which over $\bar{k}$ consist of two distinct points.*

Translating this theorem to work over $\mathbb{Z}$ is the topic of the next section.

3.3 Gauss–Bhargava Composition

In this section, we review Gauss’s correspondence between the class groups of quadratic fields and equivalence classes of binary quadratic forms with integer coefficients. Since Gauss, this theory has been developed to much greater lengths by several authors, of late by M. Bhargava [9] and his student M.M. Wood [114, 112]. We will follow Bhargava’s description over $\mathbb{Z}$ as the general case handled by Wood requires extremely careful definitions.

Throughout, $V = V_{\mathbb{Z}} = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \times \mathbb{Z}^2$, the space of $2 \times 2 \times 2$ *boxes*. We regard $v \in V$ as a pair (A_i, B_i) of 2×2 matrices over $\mathbb{Z}$ in three different ways, corresponding to the three factors of $\mathbb{Z}^2$. Then we write $\det_i(v) = \det(A_i x - B_i y)$. Each of these binary quadratic forms $\det_i(v) = a_i x^2 + b_i xy + c_i y^2$ has a discriminant $\mathrm{Disc}_i(f) = b_i^2 - 4a_i c_i$. Regarded as a polynomial function in the entries of A_i and B_i , this discriminant has degree 4.

Moreover, $\mathrm{SL}_2 \mathbb{C} \times \mathrm{SL}_2 \mathbb{C} \times \mathrm{SL}_2 \mathbb{C}$ acts on $V_{\mathbb{C}}$, and one readily computes that V has a unique polynomial invariant of degree 4 and each $\mathrm{Disc}_i(v)$ is a polynomial invariant of degree 4. Then $\mathrm{Disc}_i(v) = c_{ij} \mathrm{Disc}_j(v)$ for some $c_{ij} \in \{\pm 1\}$ for all i, j . But one may check any particular box, say

$$A_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \quad B_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

to see that $c_{ij} = 1$ for all i, j . As such, for any $v \in V$, we denote $\mathrm{Disc}(v) = \mathrm{Disc}_i(v)$ for all $i = 1, 2, 3$.

Recall that to every $D \equiv 0, 1 \pmod{4}$ there is a unique quadratic ring over $\mathbb{Z}$ of discriminant D . If $D = m^2 D'$ where D' is a fundamental discriminant, then $R = \mathbb{Z} + m\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D'})$ and $\mathcal{O}_K$ is K 's ring of integers. If D is 0, then $R = \mathbb{Z}[x]/(x^2)$. If $D = m^2$ is a square, then $R = \mathbb{Z} + m(\mathbb{Z} \oplus \mathbb{Z})$.

Definition 105. To any $v \in V_{\mathbb{Z}}$, let $R(v)$ denote the quadratic ring over $\mathbb{Z}$ with $\mathrm{Disc}(R(v)) = \mathrm{Disc}(v)$. We say that v is *nodegenerate* if and only if $R(v)$ is nondegenerate if and only if $\mathrm{Disc}(v) \neq 0$.

Let G' be the algebraic group whose B points are $G'(B) = \mathrm{GL}_2(B) \times \mathrm{GL}_2(B) \times \mathrm{GL}_2(B) / \{(r, s, t) \in (B^\times)^3 : rst = 1\}$ PID B . Here, by $(B^\times)^3 \subseteq (\mathrm{GL}_2 B)^3$ we mean the multiplicative groups embedded diagonally. In particular, this is the kernel of the canonical action of GL_2^3 on V .

Now the work above shows that the quadratic ring associated to $\det_i(v)$ is the same for each i . Then Gauss gave a method of constructing for every binary quadratic form an ideal in the quadratic ring $R(v)$. As such, to a $2 \times 2 \times 2$ box, we get a quadratic ring R and three ideal classes I_1, I_2, I_3 . In [9], Bhargava shows that when v is nondegenerate we have

- $I_1 I_2 I_3 \subseteq R$, and
- $\mathfrak{N}(I_1) \mathfrak{N}(I_2) \mathfrak{N}(I_3) = 1$,

where $\mathfrak{N}(I)$ is the norm of the ideal I . We call such a triple of ideals *balanced*.

Moreover, we know that every quadratic ring $R(v)$ is monogenic, i.e., may be written as $R(v) = \mathbb{Z}[x]$ for some $x \in R$. Using this, for any triple of ideals I_1, I_2, I_3 satisfying these conditions, Bhargava recovers a $2 \times 2 \times 2$ box (a_{ijk}) where the a_{ijk} are given by

$$\alpha_{1i}\alpha_{2j}\alpha_{3k} = c_{ijk} + a_{ijk}x$$

where α_{i1}, α_{i2} is a basis of I_i .

There is an obvious action of $\mathrm{GL}_2 \mathbb{Z}$ on each of the I_i by change of basis, and Bhargava demonstrates that if we consider *equivalence classes* of triples I_1, I_2, I_3 , then the natural action of $(\mathrm{GL}_2 \mathbb{Z})^3$ descends to a natural action of $G'(\mathbb{Z})$. Here two triples $(I_1, I_2, I_3) \sim (I'_1, I'_2, I'_3)$ are equivalent if there are some $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in R \otimes \mathbb{Q}$ such that $I_i = \varepsilon_i I'_i$ and $\mathfrak{N}(\varepsilon_1 \varepsilon_2 \varepsilon_3) = 1$.

Theorem 106 ([9]). *There is a one-to-one correspondence between pairs $(R, (I_1, I_2, I_3))$ of nondegenerate quadratic rings R over $\mathbb{Z}$ and equivalence classes of balanced triples (I_1, I_2, I_3) and $G'(B)$ orbits on V_B .*

In fact, as a corollary of the construction, we may in fact determine the stabilizer of $v \in V_{\mathbb{Z}}$, at least when I_1, I_2 , and I_3 are invertible R ideals and v is nondegenerate.

Corollary 107. *Suppose that $v \in V_{\mathbb{Z}}$ corresponds to $(R, (I_1, I_2, I_3))$ and suppose further that each I_i is invertible and R is nondegenerate. Then the stabilizer of $v \in G'(\mathbb{Z})$ is isomorphic to*

$$\mathrm{Aut}(R) \ltimes (R^\times / \mathbb{Z}^\times)^2$$

Proof. When I_1 and I_2 are projective, then the balancing condition implies that I_3 is as well. In particular, $\mathrm{End}(I_1) = \mathrm{End}(I_2) = \mathrm{End}(I_3) = R$ and so $\mathrm{Aut}(I_1) = \mathrm{Aut}(I_2) = \mathrm{Aut}(I_3) = R^\times$. Now for any $r, s \in R^\times$, we see that the triple $(rI_1, sI_2, (rs)^{-1}I_3)$ is equivalent to (I_1, I_2, I_3) .

Further, $rI_1 = I_1$, so r acts on the basis α_{11}, α_{12} and we procure a matrix in $A \in \mathrm{GL}_2 \mathbb{Z}$. Similarly, $sI_2 = I_2$ and $(rs)^{-1}I_3 = I_3$ so we procure matrices $B, C \in \mathrm{GL}_2 \mathbb{Z}$ corresponding to each of these transformations. Moreover, if $r \in \mathbb{Z}^\times$ then $A \in \mathbb{Z}^\times \subseteq \mathrm{GL}_2 \mathbb{Z}$, so is trivial in $G'(\mathbb{Z})$. As such, we have an injective map $(R^\times/\mathbb{Z}^\times)^2 \rightarrow G'_v(\mathbb{Z})$.

So far, the triples of matrices listed have determinants whose products is $+1$. But those are not the only matrices in $G'_v(\mathbb{Z})$. In particular, one sees that the map $\det : G'(\mathbb{Z}) \rightarrow \{\pm 1\}$ is surjective and what we have described is precisely the kernel. The other elements correspond to those we have just named twisted by the automorphism group of R . $\square$

Remark 108. In fact, the entire discussion above makes sense for quadratic rings over any PID, in particular $\mathbb{Z}_p$ and $\mathbb{F}_p$. The discussion goes through entirely unchanged for $\mathbb{Z}_p$. For $\mathbb{F}_p$, the norm condition becomes vacuous except to guarantee that the I_i are line bundles as opposed to simply ideals. For the most general case, please consult [112].

3.4 Some remarks on invertibility

Suppose that R is a rank n ring. Then if I_1 and I_2 are invertible R -ideals, then so is I_1I_2 and $\mathfrak{N}(I_1I_2) = \mathfrak{N}(I_1)\mathfrak{N}(I_2)$. Moreover, if I_3 is an R -ideal with $\mathfrak{N}(I_1)\mathfrak{N}(I_2)\mathfrak{N}(I_3) = 1$ and $I_1I_2I_3 \subseteq R$, then $I_3 = (I_1I_2)^{-1}$.

Now we would like to repeat ourselves from Section 2 of Chapter 2 for the convenience of the reader. Recall that to any rank n ring R over a PID B we may define the *dual module* of an R -module M to be $\mathrm{Hom}(M, B)$. We say that the ring R is *Gorenstein* when $R^\vee$ is a projective R -module, or what is the same, when R is an injective R -module. The importance of this property is captured in the following lemma.

Lemma 109. *An order $\mathcal{O}$ in a number field is Gorenstein if and only if every proper ideal is invertible.*

Proof. It follows from [56, Lemma 5.4] that every proper ideal in a Gorenstein order is

invertible. For the other direction, note that $\text{Hom}(\mathcal{O}, \mathbb{Z})$ is always proper. For if $x/p \in (\mathcal{O}^\vee : \mathcal{O}^\vee)$ with $1, x, x_2, \dots, x_{d-1}$ a basis of $\mathcal{O}$, then for *every* $\varphi \in \text{Hom}(\mathcal{O}, \mathbb{Z})$ and $y \in \mathcal{O}$ we must have that $\varphi(xy) \in p\mathbb{Z}$. But in particular, if φ is the map which sends x to 1 and x_i and 1 to 0, then $\varphi(x \cdot 1) = 1$. $\square$

Now we turn our attention to quadratic rings. We begin with a very general lemma.

Lemma 110. *Every monogenic order in a number field is Gorenstein.*

Proof. A map $\mathbb{Z}[x] \rightarrow \mathbb{Z}$ is determined by the images of $1, x, x^2, \dots, x^{n-1}$, and so $\text{Hom}(\mathbb{Z}[x], \mathbb{Z})$ is generated by the map which sends $1 \mapsto 1$ and $x^i \mapsto 0$ for all $1 \leq i < n$. Hence $\text{Hom}(\mathbb{Z}[x], \mathbb{Z})$ is free and thus projective. $\square$

Corollary 111. *Every nondegenerate quadratic ring is Gorenstein.*

Proof. If $\mathcal{O}$ is the order of discriminant D in a quadratic number field, then $\mathcal{O} = \mathbb{Z}[x]$ where

$$x = \begin{cases} \sqrt{D} & D \equiv 0 \pmod{4} \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \pmod{4}. \end{cases}$$

Finally, $\mathbb{Z} + m(\mathbb{Z} \oplus \mathbb{Z}) \cong \mathbb{Z}[x]/(x^2 - mx)$. $\square$

In particular, unlike the cubic case, we will not have to worry about noninvertible proper ideals.

3.5 Local Densities for Maximal Rings and Invertible Ideals

Whether or not a ring is maximal and whether or not a ring is invertible are *local* conditions. As such, slightly abusing notation, let MAX_p denote either the subset of $V_{\mathbb{Z}}$ whose elements

correspond to quadruples $(R, (I_1, I_2, I_3))$ such that $R \otimes \mathbb{Z}_p$ is maximal, or this set's closure in $V_{\mathbb{Z}_p}$. Similarly, let INV_p be the same, except demanding that I_1 and I_2 (and hence I_3) be invertible at p .

3.5.1 A Mass Formula

To any free $\mathbb{Z}_p$ module W , let μ_W be the additive Haar probability measure on $\mathbb{Z}_p$. If R is a quadratic ring over $\mathbb{Z}_p$, let $\text{Disc}_p(R)$ be the discriminant of R as a power of p and let $\text{Reg}_p(R) = \mu_R(R^\times) / \mu_{\mathbb{Z}_p}(\mathbb{Z}_p^\times)$. Then we have the following mass formula.

Proposition 112. *Let R be a nondegenerate quadratic ring over $\mathbb{Z}_p$ and let I_1 and I_2 be invertible ideals of R . Then the p -adic density of all elements in $V_{\mathbb{Z}_p}$ corresponding to the tuple $(R, (I_1, I_2, (I_1 I_2)^{-1}))$ is*

$$\frac{\#G'(\mathbb{F}_p)}{p^{10}} \cdot \frac{1}{\#\text{Aut}(R)} \cdot \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\text{Reg}_p(R)^2}$$

Proof. Since I_1 and I_2 are invertible, they are principal, and hence $(R, (I_1, I_2, I_3)) \cong (R, (R, R, R))$, so we need only handle this case. Now there are only a finite number of quadratic rings over $\mathbb{Z}_p$ with a fixed nonzero discriminant, so there is some large n such that the structure of R is determined by the ring structure modulo p^n , i.e., $R/p^n R$ determines R . On the other hand, the parameterization of Theorem 106 is compatible with base change since all the structure coefficients are polynomials with integral coefficients. So if two $v, v' \in V_{\mathbb{Z}_p}$ lie in the same $G'_{\mathbb{Z}_p}$ orbit, then they lie in the same $G'_{\mathbb{Z}/p^n\mathbb{Z}}$ orbit and vice-versa.

But now that we have a finite group, we may employ the orbit-stabilizer theorem. According to Corollary 107 reduced modulo p^n , we have that the stabilizer of v in $G'_{\mathbb{Z}/p^n\mathbb{Z}}$

has order

$$\begin{aligned}\#G'_{v, \mathbb{Z}/p^n \mathbb{Z}} &= \# \operatorname{Aut}(R/p^n R) \cdot \left[\#(R/p^n R)^\times / \#(\mathbb{Z}_p/p^n \mathbb{Z}_p)^\times \right]^2 \\ &= (\# \operatorname{Aut}(R) \operatorname{Disc}_p(R)) \cdot (p^{2n} \operatorname{Reg}_p(R)^2).\end{aligned}$$

So the total density of point $v \in V_{\mathbb{Z}_p}$ corresponding to $(R, (R, R, R))$ is the proportion of points $v \in V_{\mathbb{Z}/p^n \mathbb{Z}}$ corresponding to $(R/p^n R, (R/p^n R, R/p^n R, R/p^n R))$, which is

$$\frac{1}{p^{8n}} \cdot \frac{\#G'_{\mathbb{Z}/p^n \mathbb{Z}}}{p^{2n} \cdot \# \operatorname{Aut}(R) \cdot \operatorname{Disc}_p(R) \cdot \operatorname{Reg}_p(R)^2} = \frac{p^{10(n-1)} \cdot \#G'(\mathbb{F}_p)}{p^{10n} \cdot \# \operatorname{Aut}(R) \cdot \operatorname{Disc}_p(R) \cdot \operatorname{Reg}_p(R)^2}$$

□

3.5.2 Maximal Rings

First note that for any rank n ring R over $\mathbb{Z}_p$, we have that $\operatorname{Reg}_p(R)$ is determined by R/pR .

In particular, an element of R is a unit if and only if it is a unit modulo p . As such,

$$\operatorname{Reg}_p(R) = \frac{\#(R/pR)^\times}{\#(R/pR)} \cdot \frac{p}{p-1} = \frac{\#(R/pR)^\times}{p(p-1)}$$

Now there are three possible reductions of a maximal quadratic ring R over $\mathbb{Z}_p$ modulo p corresponding to the three possible splitting types of a prime in $\mathbb{Z}$. We denote these splitting types (11), (2), and (1^2) , where R/pR is isomorphic to $\mathbb{F}_p^2$, $\mathbb{F}_{p^2}$, and $\mathbb{F}_p[x]/(x^2)$, respectively. We will typically denote the splitting type of an object by τ , e.g., $\tau(\mathbb{Z}_p \oplus \mathbb{Z}_p) = (11)$. Now we have the following table tabulating the values of $\operatorname{Reg}_p(R)$ by splitting type: So we have

Table 3.1: Local regulators for quadratic rings by splitting type

Splitting type	(11)	(2)	(1^2)
Reg_p	$\frac{p-1}{p}$	$\frac{p+1}{p}$	1

that

$$\sum^{\max} \frac{1}{\# \text{Aut}(R)} \cdot \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\text{Reg}_p(R)^2} = \sum_{\tau} \frac{1}{\text{Reg}_p(\tau)^2} \sum_{\tau(R/pR)=\tau}^{\max} \frac{1}{\# \text{Aut}(R)} \cdot \frac{1}{\text{Disc}_p(R)}. \quad (3.4)$$

Here the superscript max means the sum is over *maximal* quadratic rings.

Now we know that there are four maximal quadratic rings over $\mathbb{Z}_p$ for $p > 2$ corresponding to the four square classes of $\mathbb{Q}_p^\times$. Of these, one is split (11), one is inert (2), and two are ramified (1^2). Each has automorphism group S_2 . As such, the sum (3.4) becomes

$$\frac{p^2}{(p-1)^2} \cdot \frac{1}{2} \cdot 1 + \frac{p^2}{(p+1)^2} \cdot \frac{1}{2} \cdot 1 + 1 \cdot \left(\frac{1}{2} \cdot \frac{1}{p} + \frac{1}{2} + \frac{1}{p} \right) = \frac{p^5 + p^4 + p^3 - 2p^2 + 1}{p(p-1)^2(p+1)^2}.$$

Combining this we the fact that

$$\#G'_{\mathbb{F}_p} = \frac{1}{(p-1)^2} [(p^2-1)(p^2-p)]^3 = p^3(p-1)^4(p+1)^3 \quad (3.5)$$

we arrive at

$$\mu_{\mathbb{Z}_p}(\text{MAX}_p) = \frac{p^8 - p^6 - 3p^5 + 2p^4 + 4p^3 - 3p^2 - p + 1}{p^8}. \quad (3.6)$$

3.5.3 Invertible Ideals

If we instead want to count *invertible* ideals, then we should no longer restrict ourselves to maximal quadratic rings over $\mathbb{Z}_p$. But we know that every quadratic ring over $\mathbb{Z}_p$ may be written as $R = \mathbb{Z}_p + p^d R'$ for some $d \geq 0$ and some maximal R' .

Suppose that $d > 0$. Then we see that the splitting type of R is (1^2) and so $\text{Reg}_p(R) = 1$. Moreover, $\text{Disc}_p(R) = p^{2d} \text{Disc}_p(R')$. Finally, it remains true that $\# \text{Aut}(R) = 2$. As such, when we take the sum (3.4) to be over *all* quadratic rings, we see that it becomes the sum

(3.4) with the additional terms

$$\sum_{d \geq 1} \frac{1}{2} \cdot \frac{1}{p^{2d}} + \sum_{d \geq 1} \frac{1}{2} \cdot \frac{1}{p^{2d}} + \sum_{d \geq 1} \frac{1}{2} \cdot \frac{1}{p^{2d+1}} + \sum_{d \geq 1} \frac{1}{2} \cdot \frac{1}{p^{2d+1}}.$$

Here the first sum corresponds to subrings of the split maximal ring, the second to subrings of the inert maximal ring, and the final two to subrings of the two ramified rings. So in total, this yields an additional

$$\frac{p}{p-1} - 1 - \frac{1}{p} = \frac{1}{p(p-1)}. \quad (3.7)$$

Combining (3.4) with (3.7) and (3.5) and applying Proposition 112 we arrive at

$$\mu_{V_{\mathbb{Z}_p}}(\text{INV}_p) = (p^7 - 3p^4 - p^3 + 4p^2 - 1)/p^7.$$

3.6 A Geometry of Numbers Argument

Let $V = V_{\mathbb{R}}$ be the vector space of boxes over $\mathbb{R}$. Then the action of $G'(\mathbb{R})$ has two nondegenerate orbits, viz. V^+ consisting of elements with positive discriminant, and V^- consisting of elements with negative discriminant. In this section, we will get a handle on the total

$$N(V^{\pm}; X) = \sum \text{Reg}(v)$$

where the sum is over $G'(\mathbb{Z})$ orbits represented by v in $V_{\mathbb{Z}}$ lying in $V^{\pm}$ and having absolute discriminant at most X and such that $\det(v)$ is irreducible over $\mathbb{Q}$. That is, we are summing the regulator of ideal classes of *orders* in quadratic fields.

3.6.1 Reduction Theory

Over $\mathbb{R}$, we note that $G'(\mathbb{R}) \cong \mathrm{GL}_2(\mathbb{R}) \times \mathrm{SL}_2^\pm(\mathbb{R}) \times \mathrm{SL}_2^\pm(\mathbb{R})$ where $\mathrm{SL}_2^\pm(\mathbb{R})$ consists of 2×2 matrices with determinant ± 1 . On the other hand, we note that a fundamental domain $\mathcal{F}$ for the action of $G'(\mathbb{Z})$ on $G'(\mathbb{R})$ is *also* a fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$ where $G = \mathrm{GL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2 \subseteq G'$. As we will be counting integral points in a single $\mathbb{R}$ -orbit in $V_{\mathbb{R}}$, we will from now on work with the group G .

We may express elements of $G(\mathbb{R})$ via the Iwasawa decomposition $NAK\Lambda$ where N consists of triples of lower triangular matrices, A consists of triples of diagonal matrices of determinant one, $K = \mathrm{O}_2 \times \mathrm{SO}_2 \times \mathrm{SO}_2$ is the maximal compact, and Λ consists of positive scalar matrices in $\mathrm{GL}_2(\mathbb{R})$. Let $\mathcal{F}$ be a fundamental domain for the action of $G(\mathbb{Z})$ on $G(\mathbb{R})$. Then according to Minkowski's theory of such fundamental domains, we may take $\mathcal{F} = \{nak\lambda : n \in N'(a), a \in A', K \in K, \lambda \in \Lambda\}$ where

$$\begin{aligned} N'(a) &= \left[\begin{pmatrix} 1 & \\ n_1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ n_2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ n_3 & 1 \end{pmatrix} \right] \\ A' &= \left[\begin{pmatrix} s_1^{-1} & \\ & s_1 \end{pmatrix}, \begin{pmatrix} s_2^{-1} & \\ & s_2 \end{pmatrix}, \begin{pmatrix} s_3^{-1} & \\ & s_2 \end{pmatrix} \right] \end{aligned}$$

where $s_1, s_2, s_3 \geq \sqrt[4]{3}/\sqrt{2}$, and $n_j \in \tau_j(a) \subseteq [-1/2, 1/2]$ for each $a \in A'$. The exact values of $\tau_j(a)$ will not matter for us, only that they are bounded independent of a .

In these coordinates, a Haar measure dg on G is given by

$$dg = dn s_1^{-2} d^\times s_1 s_2^{-2} d^\times s_2 s_3^{-2} d^\times s_3 dk d^\times \lambda$$

where $d^\times$ denotes the usual multiplicative Haar measure $d^\times t = dt/t$.

3.6.2 An Averaging Argument

Let $B = B(C) = \{v \in V_{\mathbb{R}} : \|v\| \leq C\}$ where $\|v\|$ denotes the usual Euclidean norm. For what we do now, $C = 100$ will suffice. Moreover, the main features of B that we will use is that it is bounded, has positive volume in V , and that it is K invariant. Then as v ranges over $B \cap V^{\pm}$ we know that

$$\sum_{\substack{f \in \mathcal{F}v \cap V_{\text{irr}}^{\pm} \\ |\text{Disc}(f)| < X}} \text{Reg}(v)$$

is *constant* and is equal to $N(V^{\pm}; X)$. Then

$$N(V^{\pm}; X) = \frac{\int_{v \in B \cap V_{\text{irr}}^{\pm}} \sum_{\substack{f \in \mathcal{F}v \cap V^{\pm} \\ |\text{Disc}(f)| < X}} \text{Reg}(f) |\text{Disc}(v)|^{-2} dv}{\int_{v \in B \cap V^{\pm}} |\text{Disc}(v)|^{-2} dv} \quad (3.8)$$

where $V_{\text{irr}}^{\pm} \subseteq V^{\pm}$ consists of those orbits which are irreducible. Note that we choose the measure $|\text{Disc}(v)|^{-2} dv$ precisely because it is a G -invariant measure on V .

More generally, for any $G_{\mathbb{Z}}$ invariant subset $S \subseteq V_{\mathbb{Z}}^{\pm}$ let $N(S, X)$ be defined the same way as $N(V^{\pm}, X)$. That is, if $M_{\pm}(C)$ is the denominator of (3.8), then define

$$N(S; X) = \frac{1}{M_{\pm}(C)} \int_{v \in B \cap S} \sum_{\substack{f \in \mathcal{F}v \cap S_{\text{irr}} \\ |\text{Disc}(f)| < X}} \text{Reg}(f) |\text{Disc}(v)|^{-2} dv \quad (3.9)$$

Similarly, define $N^*(S, X)$ to be the same sum but *not* restricted to irreducible orbits.

Now as in the previous chapter, we may make the manipulations

$$N(S; X) = \frac{c_{\pm}}{M_{\pm}(C)} \int_{g \in \mathcal{F}} \#\{f \in V_{\text{irr}} \cap Bg : |\text{Disc}(f)| < X\} dg \quad (3.10)$$

where $\#$ means counted with weight $\#\text{Aut}(R(f))$, which in every instance for us is 2, so we shall ignore this henceforth. Moreover, recall that $c_{\pm}$ is the Jacobian of the change of variables divided by $\#\text{Aut}(f_{\mathbb{R}})$.

As before, in order to make these manipulations, we will need to demand that $a_{11} \neq 0$. As we shall see, this bounds the elements of the fundamental region $\mathcal{F}$ which could possibly yield integral points, and so the above manipulation is valid. But as before, we will need the following lemma, whose proof we delay.

Lemma 113. *Let $V(a_{11} = 0)$ be the set of all points in V with $a_{11} = 0$. Then $N(V(a_{11} = 0); X) = O(X^{7/4})$.*

Also as before, we would like to make our lives easier by showing that we can, instead of considering only *irreducible* boxes in (3.10) instead consider *all* boxes. The following lemma allows us to do so.

Lemma 114. *The difference $N^*(V(a_{11} \neq 0); X) - N(V(a_{11} \neq 0); X) = o(X^2)$.*

Finally, we rewrite (3.10) in a more convenient form incorporating Lemmas 113 and 114 and the K -invariance of B :

$$N(S; X) = \frac{c_{\pm}}{M_{\pm}(C)} \int_{g \in N'(a)A'\Lambda} \#\{f \in S \cap B(u, s, \lambda, X)\} dn s_1^{-2} d^{\times} s_1 s_2^{-2} d^{\times} s_2 s_3^{-2} d^{\times} \lambda + o(X^2) \quad (3.11)$$

where $B(u, s, \lambda, X) = n(u)a(s)\lambda B \cap \{f \in V_{\mathbb{R}}^{\pm} : |\text{Disc}(f)| < X\}$. Note that $N^*(S; X)$ is the same with $o(X^2)$ replace by $O(X^{7/4})$ as we do not have to apply Lemma 114.

Note that $\text{Disc}(nak\lambda v) = \lambda^4 \text{Disc}(v)$ and so in the integral (3.11), we know that $\lambda \leq X^{1/4}$.

3.6.3 A Lemma from the Geometry of Numbers

In later sections, we will need to estimate the number of lattice points in $B(u, s, \lambda, X)$, which we will do using the following elementary proposition due to Davenport [38].

Proposition 115. *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ which is defined by finite number of polynomial inequalities². Let $\mathcal{R}'$ be the image of $\mathcal{R}$ under any (upper or lower) triangular unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points contained in the region $\mathcal{R}'$ is*

$$\text{vol}(\mathcal{R}) + O(\max\{\text{vol}(\bar{\mathcal{R}}), 1\})$$

where $\text{vol}(\bar{\mathcal{R}})$ is the greatest d -dimensional volume ($1 \leq d \leq n - 1$) of any projection of $\mathcal{R}$ onto a coordinate subspace, i.e., by setting $n - d$ coordinates to 0. The implied constant depends only on n , the total number of defining polynomials, and their maximum degree.

Although Davenport states the above lemma only for compact semi-algebraic sets $\mathcal{R} \subseteq \mathbb{R}^n$, his proof adapts essentially without change to the above proposition.

3.6.4 A More General Regulator

For any $v \in B$, let $\mathcal{R}_X(v) = \mathcal{F}v$ be the orbit of $\mathcal{F}$ acting on v . Then we may define the *regulator* of a point $gv \in \mathcal{R}_X(v)$ to be

$$\text{Reg}(f) = \int_{h \in G_{f, \mathbb{R}}} 1_{\mathcal{F}}(gh) dh.$$

Now we would like to consider $\mathcal{R}_X(v)$ as a weighted set, with each point weighted by its regulator. Then its volume would be

$$\text{Vol}(\mathcal{R}_X(v)) = \int_{f \in \mathcal{R}_X(v)} \text{Reg}(f) df.$$

Note that for any $v \in B$, this volume is constant as we are dealing everywhere with unimodular Haar measures!

²For any property (P) of a set, we extend its meaning to multisets by saying a multiset $\mathcal{R}$ has property (P) if and only if $\mathcal{R}_k$ has property (P) for all k . Here $\mathcal{R}_k$ is the set of all $x \in \mathcal{R}$ with weight k .

3.6.5 The main term

Combining Proposition 115 with (3.11), we see that it suffices to compute the Euclidean volume of $B(u, s, \lambda, X)$ for every u, s, λ, X and then to show that none of its projections are too terribly large.

For the first task, we note simply that

$$c_{\pm} \int_{g \in \mathcal{F}} B(u, s, \lambda, X) dg = \int_{v \in B \cap V^{\pm}} \text{Vol}(\mathcal{R}_X(v)) |\text{Disc}(v)|^{-2} dv.$$

(Recall from (3.10) that $c_{\pm}$ is the Jacobian of the change of variables.) Since $\text{Vol}(\mathcal{R}_X(v))$ is constant, this yields a total of $M_{\pm}(C) \cdot \text{Vol}(\mathcal{R}_X(v))$.

For the second part, note that in order for a point in $V(a_{11} \neq 0)$ to be an integer point, $|a_{11}| \geq 1$. From Proposition 115, we may consider this only for $u = 1$. This in turn implies, from the boundedness of B , that

$$\lambda(s_1 s_2 s_3)^{-1} \gg 1 \tag{3.12}$$

where the implied constant is dependent only on C . Since the s_i are bounded below, (3.12) implies that the s_i are $\ll \lambda$. Now $\text{Vol}(B(1, s, \lambda, X)) \leq \lambda^8 \text{Vol}(B)$ and (3.12) implies the projection to the coordinate axis $a_{11} = 0$ must have volume at most a constant times

$$\lambda^8 s_1 s_2 s_3 / \lambda. \tag{3.13}$$

So the error term in Proposition 115 coming from this projection is at most a constant times

$$\int_{\lambda \gg 1}^{X^{1/4}} \int_{s_i \gg 1} \int_u \lambda^7 du d^{\times} s d^{\times} \lambda \ll X^{7/4+\varepsilon}.$$

Now we will see in the proof of Lemma 113 that after projecting to any coordinate

after a_{11} that this error term can be no bigger. But in the terms of that proof, a_{11} has minimal weight, and so projecting onto no other coordinate can yield a larger error term.

Finally, we note from [84, Proposition 20] that if we take instead dg to be the volume on $G(\mathbb{R})$ arising from the $NA\bar{N}\Lambda$ decomposition that the volume of $G^1(\mathbb{Z})\backslash G^1(\mathbb{R})$ is $\zeta(2)^3$ where $G^1(\mathbb{R}) = (\mathrm{SL}_2 \mathbb{R})^3 \subseteq G(\mathbb{R})$. Using this fact, our computation of the stabilizers of points, the change of variables formula, and finally the indispensable help of [105], we arrive at the formula

$$\mathrm{Vol}(\mathcal{R}_X(v)) = \frac{4}{n_{\pm}} \int_0^{X^{1/4}} t^8 d^{\times} t \int_{G_{\mathbb{Z}} \backslash G_{\mathbb{R}}^1} dg = \frac{\zeta(2)^3}{2n_{\pm}} X^2.$$

Here $n_{\pm}$ is given by $n_+ = 8$ and $n_- = 2\pi^2$.

3.6.6 Congruence Conditions

We can also prove a version of Theorem 103 for a set in $V^{\pm}$ defined by any finite number of congruence conditions. Specifically,

Theorem 116. *Suppose that $S \subseteq V_{\mathbb{Z}}^{\pm}$ is defined by finitely many congruence conditions. Then we have*

$$\lim_{X \rightarrow \infty} \frac{N(S \cap V^{\pm}; X)}{X} = \frac{\zeta(2)^3}{2n_{\pm}} \prod_p \mu_p(S),$$

where $\mu_p(S)$ denotes the p -adic density of S in $V_{\mathbb{Z}}$ and $n_+ = 8$ and $n_- = 2\pi^2$.

Proof. Suppose that S is defined by congruence conditions modulo m . Then S can be viewed as the union of (say) k translates $L_1, \dots, L_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each such lattice L_j we may compute $N(L_j; X)$ using Proposition 115 but where each d -dimensional volume is scaled by a factor of $1/m^d$ since our new lattice has been scaled by a factor of m . So,

$$N(L_j; X) = m^{-8} \mathrm{vol}(\mathcal{R}_X(v)) + O(m^{-7} X^{7/4})$$

with $v \in V^{\pm}$ and the implied constant *independent* of m provided that $m \ll X^{1/4}$. Summing

over j and noting that $km^{-8} = \prod_p \mu_p(S)$ we obtain the theorem. $\square$

3.6.7 Controlling the Error: Proofs of Lemmas 113 and 114

Finally, we come back to the proof of Lemmas 113 and 114. We begin with the proof of Lemma 113, but to do so, we need a sufficient condition for the reducibility of boxes.

Lemma 117. *Let $(A, B) \in V_{\mathbb{Z}}$ be a box. Then if any of the following sets of coordinates simultaneously vanish, then the box is reducible.*

- $\{a_{11}, a_{12}\},$
- $\{a_{11}, a_{21}\},$ or
- $\{a_{11}, b_{11}\}.$

Proof. In cases (i) and (ii), $\det(A) = 0$ and hence $\det(Ax - By)$ has x^2 coefficient 0 and so is certainly reducible. In case (iii), either a_{12} or b_{12} is 0, or a_{12} can be made 0 through a rational linear combination of A and B , in which case we are back to case (i). $\square$

Proof of Lemma 113. Recall that we are setting $a_{11} = 0$, and so the previous lemma implies that a_{12} , a_{21} , and b_{11} all must be nonzero and hence must have absolute value at least 1. On the other hand, examining how $g \in G(\mathbb{R})$ acts on (A, B) , we see that

$$\begin{aligned} \lambda s_1^{-1} s_2^{-1} s_3 &\gg a_{12} \gg 1, \\ \lambda s_1^{-1} s_2 s_3^{-1} &\gg a_{21} \gg 1, \text{ and} \\ \lambda s_1 s_2^{-1} s_3^{-1} &\gg b_{11} \gg 1. \end{aligned} \tag{3.14}$$

Now again examining the action of G on V , we see, exploiting Proposition 115 and especially its claim that we may ignore the action by unipotents as well as the averaging trick to ignore

the compact, we find

$$N(V(1); X) \ll \int_c^{X^{1/4}} \int_{s_1, s_2, s_3=c}^{\infty} (\lambda^7 s_1 s_2 s_3) s_1^{-1} s_2^{-2} s_3^{-2} d^\times s_1 d^\times s_2 d^\times s_3 d^\times \lambda.$$

Restricting our range of integration using (3.14), we find that this integral is $\ll X^{7/4}$. $\square$

Proof of Lemma 114. First, note that the statement of Theorem 116 if we replace $N(S \cap V^\pm; X)$ with $N^*(S \cap V(a_{11} \neq 0); X)$ is still true by the same proof. Indeed, Lemma 113 removes $(a_{11} \neq 0)$ and this is the crucial lemma to saying $N(S \cap V^\pm; X) \sim N^*(S \cap V^\pm)$.

In order to prove the lemma, then, we need only show that the set of reducible boxes in $V(a_{11} \neq 0)$ is contained in some S defined by congruence conditions such that

$$\prod_p \mu_p(S) = 0$$

for then

$$\limsup_{X \rightarrow \infty} \frac{N(S \cap V^\pm; X)}{X^2} = \frac{\zeta(2)^3}{2n_\pm} \prod_p \mu_p(S) = 0.$$

Now every reducible box cannot have splitting type $(2) \bmod p$ for *any* p . So let $(\chi)_p$ be the subset of $V_\mathbb{Z}$ which does *not* have splitting type $(2) \bmod p$ and let $(\chi) = \bigcap_p (\chi)_p$. Then from Section 3.5, we know that

$$\mu_p((\chi)_p) = \frac{1}{2} + O\left(\frac{1}{p}\right)$$

and hence the product of all such densities is 0, completing the lemma. $\square$

3.7 A Sieve and the Proof of the Main Theorem

So far we have shown how to compute the sum $N(S; X)$ for S defined by a *finite* number of congruence conditions. Of most interest to us are those congruence conditions which define

the maximality of an order at a given prime, for if S corresponds to *maximal* quadratic orders, then $N(S; X)$ is precisely the second moment of the class number times the regulator. However, this S is defined by an *infinite* number of congruence conditions, so we must show that the error is not too great.

3.7.1 The error from nonmaximal orders

To do so, let $\mathcal{Z}_p$ denote the sublattice of $V_{\mathbb{Z}}$ corresponding to orders which are *not* maximal at p . We show that

Proposition 118. $N(\mathcal{Z}_p; X) = O(X^2/p^2)$.

Proof. We simply note that $v \in V_{\mathbb{Z}}$ corresponds to a maximal ring if and only if it is primitive. That is, if and only if $\det(Ax - By)$ has coefficients which are mutually relatively prime. But in that case, we note that $\det(A)$ is the coefficient of x^2 and $\det(B)$ is the coefficient of y^2 . This implies that if v is imprimitive then $\det(A) \equiv \det(B) \equiv 0 \pmod{p}$.

The density of solutions to these congruences in $V_{\mathbb{Z}_p}$ is bounded above by the proportion of $v \in V_{\mathbb{F}_p}$ which are solutions to these equations. However, the total proportion of such solutions is

$$\left[1 - \frac{\#\mathrm{GL}_2(\mathbb{F}_p)}{p^4}\right]^2 = \left[\frac{p^2 + p - 1}{p^3}\right]^2 = O(p^{-2}).$$

Applying Theorem 116 implies the proposition. $\square$

3.7.2 Proof of the Main Theorem

We now have enough information to prove Theorem 103. We let $\mathrm{MAX} = \cap_p \mathrm{MAX}_p$ be the set of all $v \in V_{\mathbb{Z}}$ corresponding to maximal quadratic rings $R(v)$. By (3.6), the p -adic density of MAX_p is $\mu(\mathrm{MAX}_p) = \frac{p^8 - p^6 - 3p^5 + 2p^4 + 4p^3 - 3p^2 - p + 1}{p^8}$. From Theorem 116, we then know that

$$\lim_{X \rightarrow \infty} \frac{N(V^{\pm} \cap_{p < Y} \mathrm{MAX}_p; X)}{X^2} = \frac{\zeta(2)^3}{2n_{\pm}} \prod_{p < Y} \frac{p^8 - p^6 - 3p^5 + 2p^4 + 4p^3 - 3p^2 - p + 1}{p^8}.$$

Letting Y go to ∞ , we immediately obtain the result

$$\limsup_{X \rightarrow \infty} \frac{N(V^\pm \text{MAX}; X)}{X^2} = \frac{\zeta(2)^3}{2n_\pm} \prod_p \frac{p^8 - p^6 - 3p^5 + 2p^4 + 4p^3 - 3p^2 - p + 1}{p^8}.$$

It remains to compute the $\liminf$. To do so, note that $\cap_{p < Y} \text{MAX}_p \subseteq (\text{MAX} \cup_{p \geq Y} \mathcal{Z}_p)$, and so

$$\begin{aligned} \liminf_{X \rightarrow \infty} \frac{N(V^\pm \cap \text{MAX}; X)}{X^2} &\geq \frac{\zeta(2)^3}{2n_\pm} \prod_{p < Y} \frac{p^8 - p^6 - 3p^5 + 2p^4 + 4p^3 - 3p^2 - p + 1}{p^8} + O\left(\sum_{p \geq Y} p^{-2}\right). \end{aligned}$$

Letting Y run to ∞ completes the proof.

The sieve when restricting only to invertible ideals in all rings is exactly the same. For if $\mathcal{Y}_p \subseteq V_{\mathbb{Z}}$ is the sublattice corresponding to triples $(R, (I_1, I_2, I_3))$ such that one of I_1, I_2, I_3 is not invertible, then $\mathcal{Y}_p \subseteq \mathcal{Z}_p$ and so Proposition 118 implies that $N(\mathcal{Y}_p; X) = O(X^2/p^2)$ as well.

Part II

Analytic Number Theory

Chapter 4

$L(1, k)$ Behaves Like a Random Euler Product

4.1 Introduction

In this chapter, we continue our work in Chapter 2 and in particular provide our second proof of Theorem 40. In this method of proof, we will average the value of $L(\mathcal{O}, 1)$ where $L(\mathcal{O}, s)$ is the L -function we described in Section 2.3 attached to an order $\mathcal{O}$ in a cubic (resp. quartic) number field. This averaging takes place in Sections 4.2 and 4.3. From Dirichlet's Class Number Formula, this result is related to Theorem 40 via partial summation, as explained in Section 4.2.

In fact, this second method of proof allows us to compute asymptotics for $\sum L(\mathcal{O}, 1)^m$ for all integral $m \geq 1$ as $\mathcal{O}$ runs through orders in cubic and quartic number fields. Moreover, it gives us a beautiful interpretation of the Euler product in Theorem 40 along the lines of [13]. Let us set a little notation. If $R/\mathbb{Z}_p$ is a rank d ring, then we define $\text{Disc}_p(R)$ to be the discriminant of $R/\mathbb{Z}_p$ as a power of p . Moreover, let $\text{Aut}_{\mathbb{Z}_p}(R)$ be the group of automorphisms of $R/\mathbb{Z}_p$. Finally, if M is any free module over $\mathbb{Z}_p$ of rank d , let μ_M be the additive Haar probability measure on M . Note in particular that $\mu_{\mathbb{Z}_p}(\mathbb{Z}_p^\times) = (p-1)/p$. Define the *local*

regulator of R to be $\text{Reg}_p(R) = \mu_R(R^\times) / \mu_{\mathbb{Z}_p}(\mathbb{Z}_p^\times)$.

In fact, we are also able to place finitely many congruence conditions on the orders $\mathcal{O}$ and *still* obtain the asymptotics of the moments of $L(\mathcal{O}, 1)$. As such, a *local condition at a finite prime p* is a collection Σ_p of degree d free $\mathbb{Z}_p$ algebras. A local condition at $p = \infty$ is a collection of degree d étale algebras over $\mathbb{R}$. Let $\Sigma^{\max} = \{\Sigma_p^{\max}\}$ be the collection of local conditions which at every p consists precisely of the *maximal orders* in degree d étale extensions $k/\mathbb{Q}_p$, and let $\Sigma^{\text{triv}} = \{\Sigma_p^{\text{triv}}\}$ be such that Σ_p^{triv} consists of all the localizations of all orders in any degree d number field. A collection of local conditions is *almost maximal* (resp. *almost trivial*) whenever Σ_p differs from $\Sigma_p^{\max}$ (resp. Σ_p^{triv}) for at most a finite number of p . For any collection of local conditions, let $\mathcal{F}_\Sigma(X)$ be the collection of all orders $\mathcal{O}$ in a degree d number field $k/\mathbb{Q}$ with Galois group S_d such that $\mathcal{O} \otimes \mathbb{Z}_p \in \Sigma_p$ for all p . Then we have the following theorem.

Theorem 119. *Suppose $d \leq 4$ and Σ is an almost maximal or almost trivial collection of local conditions, then*

$$\begin{aligned} & \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} L(\mathcal{O}, 1)^m \\ &= \left(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{\# \text{Aut}_{\mathbb{R}}(R)} \right) \left(\prod_{p \text{ finite}} \frac{p-1}{p} \sum_{R \in \Sigma_p} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}_{\mathbb{Z}_p}(R)} \cdot \frac{1}{\text{Reg}_p(R)^m} \right) \end{aligned}$$

By partial summation, we obtain

Theorem 120. *Suppose $d \leq 4$ and Σ is an almost maximal or almost trivial collection of*

local conditions such that $\Sigma_\infty = \{\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}\}$ is a singleton set, then

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{1}{X^{m/2+1}} \sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} h(\mathcal{O})^m \text{Reg}(\mathcal{O})^m \\ = \left(\frac{2}{2^{r_1} (2\pi)^{r_2}} \right)^m \left(\frac{2}{m+2} \right) \left(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{\# \text{Aut}_{\mathbb{R}}(R)} \right) \\ \times \left(\prod_{p \text{ finite}} \frac{p-1}{p} \sum_{R \in \Sigma_p} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}_{\mathbb{Z}_p}(R)} \cdot \frac{1}{\text{Reg}_p(R)} \right). \end{aligned}$$

Remark 121. Unlike the geometry of numbers method, the analytic method currently only allows us to recover information about *invertible* ideals in orders. To extend this method, we would have to extend the definition of the L -function to include noninvertible ideals. Many people have studied this object and have found it to have many pathologies, e.g., B. Green's work on its functional equation [62]. Any attempt to extend this method to invertible ideals would have to confront these pathologies.

Two major ingredients in our proof are the Strong Artin Conjecture for L -functions attached to number fields, and the Number of Number Fields Conjecture (NNF) (Conjecture 65), which gives asymptotics (with a power saving error term) for the number of S_d number fields of discriminant at most X . The Strong Artin Conjecture is known for all solvable groups [85, 107], and hence for all S_d with $d \leq 4$. The NNF Conjecture is known by [40, 12, 6] and could probably be proved with great effort by combining the techniques of [6] and [15] for the case $d = 5$. We have not attempted that here. More general d seem far out of reach. Still, combining these two conjectures, we arrive at the following conjecture.

Conjecture 122. *For any d and Σ an almost maximal collection of local conditions, we have*

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} L(\mathcal{O}, 1)^m = c(\Sigma)$$

where

$$c(\Sigma) = \left(\frac{1}{2} \sum_{R \in \Sigma_\infty} \frac{1}{\# \text{Aut}_{\mathbb{R}}(R)} \right) \left(\prod_{p \text{ finite}} \frac{p-1}{p} \sum_{R \in \Sigma_p} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}_{\mathbb{Z}_p}(R)} \cdot \frac{1}{\text{Reg}_p(R)^m} \right).$$

Remark 123. One major topic of [13] is that for any almost maximal set of local specifications, we have $0 < c(\Sigma) < \infty$ whenever $d \geq 2$. However, it is *not* known whehter $c(\Sigma)$ is finite for any almost trivial collection of local specifications when $d > 4$ and in fact in the appendix to Chapter 2 we saw that it is infinite for d sufficienly large. As such, while we will *prove* Conjecture 122 when $d \leq 4$ for any almost trivial collection of local specifications, we will not make the conjecture when $d > 4$.

In Section 4.4, much like Barban [4] and Elliot [52], we apply the method of moments to recover the *distribution* of $L(\mathcal{O}, 1)$. We show that they behave like *random Euler products*, as stipulated below.

Definition 124. For each p and each rank d ring $R/\mathbb{Z}_p$ let the *mass of $\mathcal{O}$ relative to Σ* be $\mu^\Sigma(R) = c(\Sigma')/c(\Sigma)$ where $\Sigma'_q = \Sigma_q$ for all primes $q \neq p$ and $\Sigma'_p = \{\mathcal{O}\}$.

Theorem 125. *For $d \leq 4$ let Σ be an almost maximal or almost trivial collection of local conditions. The limit*

$$F(z) = \lim_{X \rightarrow \infty} \frac{\#\{\mathcal{O} \in \mathcal{F}_X(\Sigma) : L(\mathcal{O}, 1) < z\}}{c(\Sigma)X}$$

exists and is a continuous distribution function. The probability space on $\mathbb{R}$ which it defines is the same as that defined by the product $\prod X_p$ of random variables, where for each prime p , X_p takes on the value $\text{Reg}(R)^{-1}$ with probability $\mu^\Sigma(R)$ for each R in Σ_p .

Remark 126. Assuming Conjecture 122 for any particular d , our methods yield Theorem 125's conclusion for almost maximal collections of local specifications.

4.2 A false—but instructive—proof

In this section, we relate the moments of $h(k) \text{Reg}(k)$ to average values of $L(k, 1)$ via partial summation, that is, we derive Theorem 120 from Theorem 119. We also compute the constants stated in Theorem 120.

Remark 127. Throughout this and the next section, we will often make reference to Conjecture 65, but remember that this is Theorem 66 when $d \leq 4$.

4.2.1 From Special Values to Class Number and Regulator

In this section, we would like to demonstrate how to translate between Theorem 119 and Theorem 120. As such, we focus for now on $G = S_d$. From Section 2.3, we know that

$$L(k, 1) = \frac{\pi^\sigma h(k) \text{Reg}(k)}{w_k \sqrt{\Delta(k)}}$$

for number fields k . Now if k is an S_d field and $d > 2$, then $w_k = 2$. For if not, then k contains a root of unity $\zeta \neq \pm 1$ and so $\mathbb{Q}(\zeta) \subseteq k$. As $\mathbb{Q}(\zeta)$ is an abelian field, this shows that k would contain a proper subfield if $d > 2$, which is impossible for an S_d field.

On the other hand, if $d = 2$, then there are precisely 2 fields which contain a nontrivial root of unity, viz. $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive 3rd root of unity. As such, they only contribute a finite number of terms to the sum in Theorem 120, so we can ignore them and the theorem remains true.

In fact, a similar argument shows that there are a finite number of *orders* in S_d fields which contain nontrivial roots of unity. As such, if Σ is almost maximal or almost trivial Σ_∞ is a singleton, we have that

$$\sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} [h(\mathcal{O}) \text{Reg}(\mathcal{O})]^m = \sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} \left(\frac{2}{\pi^\sigma} \right)^m \Delta(\mathcal{O})^{m/2} L^m(\mathcal{O}, 1) + O(1).$$

By partial summation, we see that the sum is

$$\begin{aligned} & \sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} \left(\frac{2}{\pi^\sigma} \right)^m \Delta_{\mathcal{O}}^{m/2} L^m(\mathcal{O}, 1) \\ &= \left(\frac{2}{\pi^\sigma} \right)^m \left[X^{m/2} \sum_{\mathcal{O} \in \mathcal{F}_\Sigma(X)} L^m(\mathcal{O}, 1) - \left(\frac{m}{2} \right) \int_1^X x^{m/2-1} \sum_{k \in \mathcal{F}_x(\Sigma)} L^m(\mathcal{O}, 1) dx \right] \quad (4.1) \end{aligned}$$

Let $C_m = C_m(\Sigma)$ be as in Theorem 119. Then (4.1) becomes

$$\begin{aligned} & \left(\frac{2}{\pi^\sigma} \right)^m \left[X^{m/2} \sum_{\mathcal{O} \in \mathcal{F}_X} L^m(\mathcal{O}, 1) - \left(\frac{m}{2} \right) \int_1^X x^{m/2-1} \sum_{\mathcal{O} \in \mathcal{F}_x} L^m(\mathcal{O}, 1) dx \right] \\ & \sim \left(\frac{2}{\pi^\sigma} \right)^m \left[C_m X^{m/2+1} - \left(\frac{m}{2} \right) \int_1^X C_m x^{m/2} dx \right] = C_m \left(\frac{2}{\pi^\sigma} \right)^m \left(\frac{2}{m+2} \right) X^{m/2+1} \end{aligned}$$

4.2.2 The False Proof

So we have reduced Theorem 120 to Theorem 119. In the coming sections, we compute the constants C_m . Begin by writing $L^m(k, s) = \sum a_k^{(m)}(n) n^{-s}$ with each

$$a_k^{(m)}(n) = \sum_{\substack{xy=n \\ x, y \geq 1}} a_k^{(m-1)}(x) a_k^{(1)}(y).$$

This converges absolutely for $\Re(s) > 1$ and converges conditionally to $L^m(k, 1)$ when $s = 1$. Moreover, it is not hard to see that the $a_k^{(m)}(n)$ are multiplicative in the sense that $a_k^{(m)}(x) a_k^{(m)}(y) = a_k^{(m)}(xy)$ when x and y are coprime.

As usual, we then try to switch the order of summation by letting $0 < N_X \leq X$ and

saying

$$\begin{aligned} \sum_{k \in \mathcal{F}_\Sigma(X)} \sum_{n=0}^{\infty} \frac{a_k^{(m)}(n)}{n} &= \sum_{k \in \mathcal{F}_\Sigma(X)} \left[\sum_{n=0}^{N_X} \frac{a_k^{(m)}(n)}{n} + \sum_{n=N_X+1}^{\infty} \frac{a_k^{(m)}(n)}{n} \right] \\ &= \left(\sum_{n=0}^{N_X} \sum_{k \in \mathcal{F}_\Sigma(X)} \frac{a_k^{(m)}(n)}{n} \right) + \left(\sum_{k \in \mathcal{F}_\Sigma(X)} \sum_{n=N_X+1}^{\infty} \frac{a_k^{(m)}(n)}{n} \right) \quad (4.2) \end{aligned}$$

The first term here would be the main term and the second term would be the error.

Let us begin with the main term in (4.2). We note that noting that the prime power coefficients $a_k^{(m)}(p^e)$ depend only on the splitting type of p in $\mathcal{O}$, i.e., on the isomorphism class of $\mathcal{O} \otimes \mathbb{F}_p$. If (τ) is a splitting type, we will thus denote the relevant coefficient by $a_\tau^{(m)}(p^e)$. As such, if we knew the proportion of rings in Σ_p with splitting type τ up to discriminant N_X , then we could compute the first summand at prime power coefficients over fields with a fixed splitting type. But this is precisely what Conjecture 65 tells us.

As such, for each integer n , let $b^{(m)}(n) = \sum_{\tau} \mu(\tau) \prod_{p^e \parallel n} a_{\tau_p}^{(1)}(p^e)$ where the sum is over all splitting types τ of n and the product is over all p^e exactly dividing n . Here we mean $\tau = \{\tau_p\}_{p|n}$ is a collection of splitting types for each prime p dividing n , and $\mu(\tau) = c(\Sigma')/c(\Sigma)$ where Σ' differs from Σ at those primes dividing n , in which case Σ_p is the set of all $R/\mathbb{Z}_p$ with splitting type τ_p . Note that $\mu(\tau)$ is a multiplicative function in the sense that if τ and τ' are supported on a disjoint set of primes, then $\mu(\tau \cup \tau') = \mu(\tau)\mu(\tau')$.

Since the $a_\tau^{(m)}(p^e)$ are multiplicative functions and $\mu(\tau)$ is multiplicative, we see that $b^{(m)}(n)$ is multiplicative. Then if we could control the error coming from Conjecture 65, we would see that (4.2) was asymptotic to

$$c(\Sigma)X \sum_{n=1}^{\infty} \frac{b^{(m)}(n)}{n}, \quad (4.3)$$

assuming of course that $\sum b^{(m)}(n)/n$ converges (which we will see that it does).

At this point, one could try to prove (4.3) for cubic fields using just Theorem 66. To

do so, one would have to bound the tail sum in (4.2) uniformly in the discriminant as in (2.3). As such, if we want that the sum over $k \in \mathcal{M}_X$ is $o(X)$, we would need to choose $N_X \gg X^{3/4}$.

However, the state-of-the-art error term in Theorem 66 for cubic fields is $O(n^{4/5}X^{2/3})$, as explicated in [21]. Summing this over n up to N_X we get a total $\ll N_X^{9/5}X^{2/3}$. As such, we must take $N_X \ll X^{5/27}$, so this method cannot at the moment yield a small enough error term.

4.2.3 The Constants

We will now compute the $b^{(m)}(n)$ and the sum $\sum b^{(m)}(n)/n$. Of course, $b^{(m)}(n)/n$ is a multiplicative function, so if it converges absolutely, then it should have an Euler product. We will prove this for $2 \leq d \leq 4$ in the following examples.

$$G = S_2$$

The relevant constants for this case appear in Table 4.1. Note that we have abbreviated

$$\Sigma^{\max}(\tau) = \sum_{\mathcal{O} \in \Sigma_p^{\max}(\tau)} \frac{1}{\text{Disc}_p(\mathcal{O})} \cdot \frac{1}{\# \text{Aut}(\mathcal{O})}.$$

Then we quickly see that

$$b^{(1)}(p^e) = \begin{cases} 0 & e \text{ odd} \\ \frac{p-1}{p} & e \text{ nonzero and even} \\ 1 & e = 0 \end{cases}$$

From this characterization, it is clear that $b^{(1)}(n) \neq 0$ only if n is a square. Since $0 \leq b^{(1)}(n) \leq 1$, this implies that $\sum b^{(1)}(n)/n$ converges absolutely. Then

$$\sum \frac{b^{(1)}(p^e)}{p^e} = \frac{1}{p+1} + \frac{p}{p+1}(1-p^{-2})^{-1} = 1 + \frac{p}{p^3+p^2-p-1}.$$

$$G = S_3$$

The relevant constants again appear in Table 4.2. Then some addition reveals that for $e > 0$

$$b^{(1)}(p^e) = \frac{p}{p^2+p+1} + \frac{p^2}{6(p^2+p+1)} \begin{cases} e+6 & e \equiv 0 \pmod{6} \\ e-1 & e \equiv 1 \pmod{6} \\ e+4 & e \equiv 2 \pmod{6} \\ e+3 & e \equiv 3 \pmod{6} \\ e+2 & e \equiv 4 \pmod{6} \\ e+1 & e \equiv 5 \pmod{6} \end{cases}$$

Then after some algebra, we arrive at

$$\sum \frac{b^{(1)}(p^e)}{p^e} = 1 + \frac{2p^5 - 2p^3 - 2p^2 + 1}{(p^3-1)(p^2-1)(p^2+p+1)}.$$

Since this sum is $1 + O(p^{-2+\varepsilon})$ and the $b^{(1)}(n)$ are multiplicative, we see that $\sum b^{(1)}(n)/n$ converges absolutely and that

$$\sum \frac{b^{(1)}(n)}{n} = \prod_p \sum_{e \geq 0} \frac{b^{(1)}(p^e)}{p^e}$$

τ	$\mu^{\max}(\tau)$	$\text{Reg}_p(\tau)$	$\sum^{\max}(\tau)$	$a_{p^e}(\tau)$
(11)	$\frac{p}{2(p+1)}$	$\frac{p-1}{p}$	$\frac{1}{2}$	1
(2)	$\frac{p}{2(p+1)}$	$\frac{p+1}{p}$	$\frac{1}{2}$	$(-1)^e$
(1 ²)	$\frac{1}{p+1}$	1	$\frac{1}{p}$	1 when $e = 1$ 0 otherwise

Table 4.1: $G = S_2$

τ	$\mu^{\max}(\tau)$	$\text{Reg}_p(\tau)$	$\sum^{\max}(\tau)$	$a_{p^e}(\tau)$
(111)	$\frac{1}{6} \cdot \frac{p^2}{p^2+p+1}$	$\frac{(p-1)^2}{p^2}$	$\frac{1}{6}$	$e + 1$
(12)	$\frac{1}{2} \cdot \frac{p^2}{p^2+p+1}$	$\frac{p^2-1}{p^2}$	$\frac{1}{2}$	1 when e is even 0 when e is odd
(3)	$\frac{1}{3} \cdot \frac{p^2}{p^2+p+1}$	$\frac{p^2+p+1}{p^2}$	$\frac{1}{3}$	1 when $e \equiv 0 \pmod{3}$ -1 when $e \equiv 1 \pmod{3}$ 0 when $e \equiv 2 \pmod{3}$
(1 ² 1)	$\frac{p}{p^2+p+1}$	$\frac{p-1}{p}$	$\frac{1}{p}$	1
(1 ³)	$\frac{1}{p^2+p+1}$	1	$\frac{1}{p^2}$	1 when $e = 0$ 0 otherwise

Table 4.2: $G = S_3$

$G = S_4$

A similar (and even more tedious) computation yields in the quartic case that

$$\sum_{e \geq 0} \frac{b^{(1)}(p^e)}{p^e} = 1 + \frac{2p^{10} + 4p^9 + 4p^8 - p^7 - 4p^6 - 6p^5 - 3p^4 + p^3 + 2p^2 + 2p}{(p^3 - 1)(p^2 - 1)^2(p^2 + 1)(p^3 + p^2 + 2p + 1)}.$$

4.2.4 Invertible Ideals

If instead we work with *invertible ideals* instead of maximal rings, there is no general conjecture for the relevant asymptotic constant like [13] provides for the maximal rings. However, in the case $d = 2$, we may simply work by hand, and in the case $d = 3$, we may use the computations of [19, Lemma 11] to compute these constants when $d = 3$. In either case, we arrive at the constants stated in Theorem 36 and Theorem 40, and which we have already computed in Chapter 2.

Unfortunately, if we instead work with $d = 4$, then the computations become much more unwieldy due essentially to the number of isomorphism classes of quartic algebras over $\mathbb{F}_p$. As such, we will not compute the appropriate factor here, as we will give a much more satisfying answer in Theorem 120.

4.2.5 Higher Moments

In this section, using Theorem 66 for $d \leq 4$ and Conjecture 65 when $d \geq 5$, we compute $\sum b^{(m)}(p^e)/p^e$. We begin with a lemma about the size of the $b^{(m)}(p^e)$.

Lemma 128. *We have that $b_1^m = 1$ for all m and that $b^{(m)}(p) = O(p^{-1+\varepsilon})$ for all primes p and all m , with the implied constant independent of p . For all $e \geq 2$, we have that $b^{(m)}(p^e) = O(p^{\varepsilon e})$.*

Proof. That $b^{(m)}(1) = 1$ follows from the fact that $a_\tau^{(1)}(1) = 1$ for all τ , and hence $a_\tau^{(m)}(1) = 1$ for all m . Applying the fact that $\sum \mu(\tau) = 1$, finishes the proof. That $b^{(m)}(p^e) = O(p^{\varepsilon e})$ for $e \geq 2$ follows from the fact that $a_\tau^{(m)}(p^e) = O(p^\varepsilon)$ for all m and all τ .

For the statement at primes, first note that $a_\tau^{(m)}(p) = m a_\tau^{(1)}(p)$. For this is certainly true for $m = 1$. And we know that

$$a_\tau^{(m)}(p) = a_\tau^{(m-1)}(1) a_\tau^{(1)}(p) + a_\tau^{(m-1)}(p) a_\tau^{(1)}(1) = a_\tau^{(1)}(p) + (m-1) a_\tau^{(1)}(p) = m a_\tau^{(1)}(p).$$

So to compute

$$b^{(m)}(p) = \sum_{\tau} \mu(\tau) a_\tau^{(m)}(p)$$

it suffices to compute $b^{(1)}(p)$.

From Conjecture 62 we know that

$$\sum_{\tau \text{ unramified}} = \frac{\sum_{R \in \Sigma_p^{\text{unr}}} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}(R/\mathbb{Z}_p)}}{\sum_{R \in \Sigma_p} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}(R/\mathbb{Z}_p)}}$$

where Σ_p^{unr} consists of all unramified splitting types over p . Both the numerator and denominator were computed in [13, Proposition 2.2] and the ratio is easily seen to be

$$u(p) = \frac{p^{d-1}}{p^{d-1} + p^{d-2} + \dots + 1}$$

Then Conjecture 62 implies that

$$\mu(\tau) = \frac{u(p)}{\#\text{Aut}(\tau)}.$$

Now we break the sum defining $b^{(1)}(p)$ into its unramified and ramified parts:

$$b^{(1)}(p) = \sum_{R \in \Sigma_p^{\text{unr}}} \frac{u(p)}{\#\text{Aut}(\tau)} a_\tau^{(1)}(p) + \sum_{R \in \Sigma_p - \Sigma_p^{\text{unr}}} \mu(\tau) a_\tau^{(1)}(p).$$

For ramified splitting types we know that $\mu(\tau) \leq 1 - u(p) = O(p^{-1+\varepsilon})$ and $a_\tau^{(1)}(p) = O(1)$, so this conforms with the statement of the lemma.

As for the *unramified* portion, we will show that

$$\sum_{\tau \in \Sigma_p^{\text{unr}}} \frac{a_\tau^{(1)}(p)}{\#\text{Aut}(\tau)} = 0.$$

To do so, we easily see from Lemma 55 that

$$a_\tau^{(1)}(p) = \frac{c_1(\tau) - 1}{p}$$

where $c_1(\tau)$ is the number of 1's (split places) appearing in τ . Then we are left to show that

$$\sum_{\tau \in \Sigma_p^{\text{unr}}} \frac{c_1(\tau) - 1}{\#\text{Aut}(\tau)} = 0$$

Again according to [13, Proposition 2.2], we have that

$$\sum_{\tau \text{ unramified}} \frac{1}{\# \text{Aut}(\tau)} = 1, \quad (4.4)$$

so we only need to handle the sum of the $c_1(\tau)$'s. If τ contains a split place, let τ' be the splitting type which is the same as τ but with one split place removed. Then $\# \text{Aut}(\tau') = c_1(\tau) \cdot (\# \text{Aut}(\tau'))$. Moreover, the collection of τ' is in one-to-one correspondence with the splitting types of degree $d - 1$. Hence, using the base case of $d = 2$ for which the claim is easily shown, we have that the sum

$$\sum_{\tau \text{ unramified}} \frac{c_1(\tau)}{\# \text{Aut}(\tau)} = \sum_{\tau' \text{ unramified}} \frac{1}{\# \text{Aut}(\tau')} = 1$$

by (4.4). □

This lemma implies in particular that

$$\sum_{e \geq 0} \frac{b^{(m)}(p^e)}{p^e} = 1 + O(p^{-2+\varepsilon}) \quad (4.5)$$

which combined with the multiplicativity of $b^{(m)}(n)$ in n , we see that

$$\sum_{n \geq 1} \frac{b^{(m)}(n)}{n} = \prod_p \sum_{e \geq 0} \frac{b^{(m)}(p^e)}{p^e}.$$

Finally, employing the estimate $a_\tau^{(m)}(p^e) = O(p^{\varepsilon e})$, we may switch the finite sum defining

$b^{(m)}(p^e)$ and the infinite sum in e , we find using Conjecture 62 that

$$\begin{aligned} c(\Sigma^{\max}) \cdot \sum_{n \geq 1} \frac{b^{(m)}(n)}{n} \\ = \left(\frac{1}{2} \sum_{R \in \Sigma_{\infty}^{\max}} \frac{1}{\# \text{Aut}_{\mathbb{R}}(R)} \right) \prod_{p \text{ finite}} \frac{p-1}{p} \sum_{R \in \Sigma_p^{\max}} \frac{1}{\text{Disc}_p(R)} \cdot \frac{1}{\# \text{Aut}(R/\mathbb{Z}_p)} \cdot \frac{1}{\text{Reg}(R)^m} \end{aligned}$$

4.2.6 Double Checking

In order to double check our computations, we used Sage [105] along with tables of cubic fields compiled by G. Malle¹. For totally real cubic fields, the tables extend to $\Delta(k) < 10^8$ and our asymptotics agree with the tables only up to 2 decimal places. For not totally real cubic fields, the tables only extend to $\Delta(k) < 10^6$, and again the agreement is only to two decimal places. This strongly indicates the presence of second order terms, a la [19, 106]. We will return to this in Section 4.5.

4.3 An Actual Proof

Now that we have given an “almost proof”, we give an actual proof of Theorem 119 employing smoothing techniques and Tauberian theorems. We note that our method is inspired particularly by [89], whose method carries over rather nicely to our case. The main new difficulty for us is dealing invertible ideals in orders, which we handle in Section 6.3, as well as the computation in Lemma 128.

To begin we note that in order to prove Theorem 120, it suffices to consider smooth sums. By a standard Tauberian theorem [64, Theorem 8], proving Theorem 120 is the same as proving

$$\sum_{k \in \mathcal{M}} L^m(k, 1) \exp(-\Delta_k/X) \sim CX \left(\sum_{n=1}^{\infty} \frac{b^{(m)}(n)}{n} \right). \quad (4.6)$$

¹These tables are available at <http://www.mathematik.uni-kl.de/~numberfielddtables/> and represent the work of many researchers. Please see there for a more detailed bibliography.

Here $\mathcal{M}$ is the set of all S_d number fields with a fixed signature at ∞ .

Using the Mellin inversion formula, for any $x > 1$ we have that

$$\frac{1}{2\pi i} \int_{\Re(s)=c} L^m(k, s+1) \Gamma(s) x^s ds = \sum_{n \geq 1} \frac{a_k^{(m)}(n)}{n} \exp(-n/x).$$

Shifting the contour to $\Re(s) = \gamma$ for some $-1 < \gamma < 0$, we pick up the pole at $s = 0$ with residue $L^m(k, 1)$ to obtain

$$L^m(k, 1) = \sum_{n \geq 1} \frac{a_k^{(m)}(n)}{n} \exp(-n/x) - \frac{1}{2\pi i} \int_{\Re(s)=\gamma} L^m(k, s+1) \Gamma(s) x^s ds$$

Let

$$I_k = I_k(x, \gamma) = \frac{1}{2\pi i} \int_{\Re(s)=\gamma} L^m(k, s+1) \Gamma(s) x^s ds.$$

Then the sum in (4.6) becomes

$$\sum_{k \in \mathcal{M}} L^m(k, 1) \exp(-\Delta_k/X) = \sum_{k \in \mathcal{M}} \sum_n \frac{\exp(-n/x)}{n} a_k^{(m)}(n) \exp(-\Delta_k/X) - \sum_{k \in \mathcal{M}} I_k \exp(-\Delta_k/X) \quad (4.7)$$

$$= \sum_n \frac{\exp(-n/x)}{n} \sum_{k \in \mathcal{M}} a_k^{(m)}(n) \exp(-\Delta_k/X) - \sum_{k \in \mathcal{M}} I_k \exp(-\Delta_k/X) \quad (4.8)$$

Here we justify switching the summation since we know that each $a_k^{(m)}(n) = O(n^\varepsilon)$ and that there are $O(X)$ fields of any given discriminant from Conjecture 65. So the exponential decays quickly enough to make the sums converge absolutely, and so we may switch their order.

Siegel showed in [100] that

$$L(k, 1) = O(\Delta(k)^\varepsilon) \quad (4.9)$$

where the constant depends only on $d = [k : \mathbb{Q}]$. Moreover, for $\Re(s)$ very close to 1,

$$L(k, s) = O((\Delta(k)|\Im(s)|)^\varepsilon) \quad (4.10)$$

where the range of s and the implied constant are dependent on ε . As such, for $x \ll X$ and $\Re(\gamma)$ very small, we have

$$|I_k| \ll (\Delta_k X)^\varepsilon \quad (4.11)$$

With (4.11), we note that by expanding in dyadic sums and taking X sufficiently large we have

$$\begin{aligned} \sum_{\Delta_k > X \log^2 X} I_k \exp(-\Delta_k/X) &= \sum_{n=0}^{\infty} \sum_{\Delta_k=2^n X \log^2 X}^{2^{n+1} X \log^2 X} I_k \exp(-\Delta_k/X) \\ &\ll X^\varepsilon \sum_{n=0}^{\infty} \sum_{\Delta_k=2^n X \log^2 X}^{2^{n+1} X \log^2 X} \Delta_k^\varepsilon \exp(-\Delta_k/X) \\ &\ll X^\varepsilon \sum_{n=0}^{\infty} 2^n X \log^2 X (2^{n+1} X \log^2 X)^\varepsilon \exp(-2^n \log^2 X) \\ &\ll X^{1+\varepsilon} \sum_{n=0}^{\infty} (2^{1+\varepsilon})^n \exp(-2^n \log^2 X) \\ &\ll X^{1+\varepsilon-\log X} + X^{1+\varepsilon} \sum_{n=1}^{\infty} \frac{3^n}{X^{2^n}} \\ &\ll X^{-2} + X^{1+\varepsilon} \lim_{N \rightarrow \infty} \left[\sum_{n=1}^N X^{-2^n} - \sum_{j=1}^{N-1} 2 \cdot 3^j \sum_{k=1}^{\infty} X^{-2^k} \right] \\ &\ll X^{-2} + X^{-2} + X^{-4} \\ &\ll X^{-2}, \end{aligned}$$

where, as usual, ε may become smaller from line-to-line. So (4.8) is equal to

$$\sum_n \frac{\exp(-n/x)}{n} \sum_{k \in \mathcal{M}} a_k^{(m)}(n) \exp(-\Delta(k)/X) - \sum_{\Delta(k) < X \log^2 X} I_k \exp(-\Delta(k)/X) + O(X^{-2}) \quad (4.12)$$

4.3.1 The main term

In this section, we consider the first term of (4.12). First, break the inner sum of the main term into splitting types as in the last section:

$$\sum_{k \in \mathcal{M}} a_k^{(m)}(n) \exp(-\Delta(k)/X) = \sum_{\tau} a_{\tau}^{(m)}(n) \sum_{\substack{k \in \mathcal{M} \\ \tau(k) = \tau}} \exp(-\Delta(k)/X) \quad (4.13)$$

Now the inner sum here is, by definition and partial summation

$$\begin{aligned} \sum_{\substack{k \in \mathcal{M} \\ \tau(k) = \tau}} \exp(-\Delta(k)/X) &= \lim_{T \rightarrow \infty} \sum_{\substack{k \in \mathcal{M}_T \\ \tau(k) = \tau}} \exp(-\Delta(k)/X) \\ &= \lim_{T \rightarrow \infty} \left[\exp(-T/X) \sum_{\substack{k \in \mathcal{M}_T \\ \tau(k) = \tau}} 1 + \frac{1}{X} \int_1^T \exp(-j/X) \sum_{\substack{k \in \mathcal{M}(j) \\ \tau(k) = \tau}} 1 \, dj \right] \end{aligned}$$

Of course, by Conjecture 65 we know that the sum in the first summand is $O(X)$ and so as $T \rightarrow \infty$ the first summand goes to 0. Hence, the final statement is

$$\sum_{\substack{k \in \mathcal{M} \\ \tau(k) = \tau}} \exp(-\Delta(k)/X) = \frac{1}{X} \int_1^{\infty} \exp(-j/X) \sum_{\substack{k \in \mathcal{M}(j) \\ \tau(k) = \tau}} 1 \, dj \quad (4.14)$$

Now according to Conjecture 65 we know that the inner sum in (4.14) is

$$c(\Sigma^{\max}) \mu(\tau) j + O(n^{\gamma} j^{1-\delta}).$$

Then we note that

$$\int_1^\infty \exp(-j/X) j^\beta dj = X^{\beta+1} \int_{1/X}^\infty \exp(-j) j^\beta dj = \Gamma\left(\beta + 1, \frac{1}{X}\right) X^{\beta+1}$$

where $\Gamma(\beta + 1, 1/X)$ is the *incomplete* Γ *function*, whose definition is precisely the integral in the previous expression. Then (4.14) becomes

$$c(\Sigma^{\max}) \mu(\tau) \Gamma\left(2, \frac{1}{X}\right) X + O\left(n^\gamma \Gamma\left(2 - \delta, \frac{1}{X}\right) X^{1-\delta}\right). \quad (4.15)$$

As $X \rightarrow \infty$, we have $\Gamma(a, 1/X) \rightarrow \Gamma(a)$. Of course, $\exp(-t)$ is bounded above by 1 on the interval $[0, 1/X]$, and for $\beta > 0$ we have $t^{\beta-1}$ is bounded above by $X^{1-\beta}$. So

$$\Gamma(\beta) - \Gamma\left(\beta, \frac{1}{X}\right) = \int_0^{1/X} \exp(-t) t^{\beta-1} dt \leq X^{-\beta},$$

and so (4.15) becomes

$$c(\Sigma^{\max}) \mu(\tau) X + O(n^\gamma X^{1-\delta}). \quad (4.16)$$

Now we can plug (4.16) into (4.13) in order to get the expression

$$\sum_{k \in \mathcal{M}} a_k^{(m)}(n) \exp(-\Delta(k)/X) \sim \sum_{\tau} a_\tau^{(m)}(n) [c(\Sigma^{\max}) \mu(\tau) X + O(n^\gamma X^{1-\delta})]$$

whose main term is exactly the same expression as in the previous section. In particular, we have that the main term in (4.12) is

$$\sum_n \frac{\exp(-n/x)}{n} [c(\Sigma^{\max}) b^{(m)}(n) X + O(n^{\gamma+\varepsilon} X^{1-\delta})]. \quad (4.17)$$

Then suppose that $x = X^\xi$ for some $\xi > 0$. Consider first the error term, viz.

$$\begin{aligned} X^{1-\delta} \sum_n \frac{\exp(-n/X^\xi)}{n} n^\gamma &= X^{1-\delta} \sum_n \exp(-n/X^\xi) n^{\gamma-1} \\ &\ll X^{1-\delta} \int_1^\infty \exp(-n/X^\xi) n^{\gamma-1} dn = X^{\gamma\xi+1-\delta} \Gamma\left(\gamma, \frac{1}{X}\right) \ll X^{\gamma\xi+1-\delta}. \end{aligned} \quad (4.18)$$

As for the main term, we may deduce from (4.5) that $\sum (b^{(m)}(n))^2 / n^{1/2+\varepsilon}$ converges, and so Cauchy-Schwarz implies, for example, that

$$\sum \frac{b^{(n)}(m)}{n} \exp(-n/x) = \sum \frac{b^{(n)}(m)}{n} + O(x^{-1/5+\varepsilon}).$$

And so we have that the main term is as claimed!

4.3.2 The Error Term

In this section, we handle the error term of (4.12). That is, we are worried about the order of magnitude of

$$\sum_{\Delta(k) < X \log^2 X} I_k \exp(-\Delta(k)/X)$$

We follow the method of many others in using a large sieve type zero density result to avoid an application of the Riemann Hypothesis². In particular, if the Riemann Hypothesis were true, then would could immediately apply the following lemma to finish the proof. Let

$$\Omega(\alpha, T) = \{z \in \mathbb{C} : \Re(z) \geq \alpha \text{ and } |\Im(z)| \leq T\}$$

Lemma 129. *Let $0 < \eta < 1/2$. Further, suppose that $L(k, s)$ (with $\Delta(k) \leq X \log^2 X$) has no zero in the domain $\Omega(1 - \eta, \log^3 X)$. Then in domain $\Omega(1 - \eta/2, \log^2 X)$ we have*

²B. Hough has pointed out to us that our method is perhaps over-powerful to attain the requisite bounds we need. However, he points out that if we wish to recover more than just the integral moments, we will need to work with the Euler product instead of the Dirichlet series, in which case, our method is the appropriate starting point. We intend to explore this in future work, see Section 4.5.

$$L(k, s) \ll X^\varepsilon.$$

Proof. This proof is standard, but we include it for completeness. The version presented is basically that presented in [89]. Consider the principal value of $\log L(k, s)$ when $L(k, s) \neq 0$. Then recall the Borel-Carathéodory Theorem: for any analytic function $f(z)$ on a closed disc of radius R with center z_0 , we have for any $r < R$ that

$$M(r) \leq \frac{2r}{R-r} \max_{|z-z_0|=r} \Re(f(z)) + \frac{R+r}{R-r} |f(z_0)| \quad (4.19)$$

where $M(r) = \max_{|z-z_0|=r} |f(z)|$.

We will center our circles at $z_0 = 2+it$ for $|t| \leq \log^3 X - 2$ and we will let $R = 1+\eta-\delta\eta$ and $r = 1 + \eta - 2\delta\eta$ for some small positive δ . But on the larger circle, by the convexity bound we have

$$\Re(\log L(k, s)) = \log |L(k, s)| \ll \log X$$

where the implied constant of course depends on η and δ but *not* on k . Now $|L(k, z_0)| \ll L(k, 2) \ll \sum_{n=1}^{\infty} \frac{1}{n^{2-\varepsilon}} = O(1)$ independent of k . So the previous paragraph, (4.19), and the maximum modulus principle together imply that for all $\sigma \geq 1 - \eta + 2\delta\eta$ and $|t| \leq \log^2 X - 2$ that

$$|\log L(k, s)| \ll \log X. \quad (4.20)$$

Putting this altogether, we have that (4.20) holds for *any* $s = \sigma + it$ with $|t| \leq \log^3 X - 2$ and $\sigma \geq 1 - (1 - 2\delta)\eta$.

Next recall that Hadamard's Three Circles Theorem states that if $f(z)$ is analytic on an open disc centered at z_0 of radius R and $0 < r_1 < r_2 < r_3 < R$ then

$$M(r_2) \leq \frac{\log(r_3/r_2)}{\log(r_3/r_1)} \log M(r_1) + \frac{\log(r_2/r_1)}{\log(r_3/r_1)} \log M(r_3)$$

Now we use the observation that for $X > 1$ and $\sigma \geq 1 + \eta/2$ and $|t| \leq \log^2 X$ that

for every $\varepsilon > 0$ we have

$$|\log L(k, s)| \ll \varepsilon \log X.$$

Then by the Three Circles Theorem with

- center $z_0 = 2 + it$ and $|t| \leq \log^2 X$,
- $r_1 = 1 - \eta/3$,
- $r_2 = 2 - \sigma$, and
- $r_3 = 1 - \eta + 2\delta\eta$

we have

$$M(r_2) \leq M(r_1)^{1-a} M(r_3)^a \ll \varepsilon^{1-a} \log X,$$

with

$$a = \frac{\log(r_2/r_1)}{\log(r_3/r_1)} < 1.$$

Exponentiating yields $M(L(k, s); r_2) \ll X^{\varepsilon^{1-a}} = X^\varepsilon$. □

Now we divide $\mathcal{M}_{X \log^2 X}$ into two sets: $\mathcal{M}_1$ consisting of all $k \in \mathcal{M}_{X \log^2 X}$ such that $L(k, s)$ has no zero in $\Omega(\eta, \log^3 X)$ and its complement $\mathcal{M}_2$. If the Generalized Riemann Hypothesis were true, then we could take $\eta = 1/2 + \varepsilon$ and then $\mathcal{M}_2 = \emptyset$. However, we will need to know an upper bound on the size of $\mathcal{M}_2$. For this, we recall a theorem of Kowalski and Michel. Fix $n \geq 1$. Then for each $q \geq 1$, let $S(q)$ be a (possibly empty) set of cuspidal automorphic representations of $\mathrm{GL}(n)/\mathbb{Q}$ such that

- the forms $f \in S(q)$ satisfy the Ramanujan-Petersson conjecture at all finite places, i.e., the local components f_p of f are tempered,
- there is some $A > 0$ such that for all $f \in S(q)$ the conductor of f is $\leq q^A$,

- there is some $B > 0$ such that $\#S(q) \ll q^B$ for all q , where the constant depends only on the family $\{S(q)\}_q$ and *not* on q , and
- all $f \in S(q)$ have the same archimedean component.

In particular, if we assume the Strong Artin conjecture that $L(k, s)$ is automorphic for all S_d number fields (a theorem for S_3 and S_4 number fields!), then we may take $S(q) = \mathcal{M}_q(d, S_d, \sigma)$ to be the set of all (automorphic representations associated with all) fields of degree d , Galois group S_d and signature σ . Checking point-by-point,

- the Ramanujan-Petersson conjecture may be checked explicitly: if $L(k, s) = \sum a_k^{(1)}(n)n^{-s}$ for $\Re(s) > 1$, then $a_k^{(1)}(p) = O(1)$ for all primes p and with the constant independent of k ;
- the conductor of the form is precisely the discriminant of the number field, so this condition is trivial with $A = 1$;
- this is simply a bound on the total number of number fields of fixed degree and signature up to a given discriminant, the classical bounds toward which satisfy this condition (see [50] for an overview and the best known bounds); and
- this is precisely a stipulation of the signature of the fields we are considering.

Now define $N(f; \alpha, T) = \#\{z \in \Omega(\alpha, T) : L(f, z) = 0\}$ where the zeros are counted with multiplicity.

Theorem 130 ([73, Theorem 2]). *Let $S(q)$ with $q \geq 1$ be as above and let $\alpha \geq 3/4$ and $T \geq 2$. Then there exists some $c > 0$ and $B \geq 0$ depending only on the family such that*

$$\sum_{f \in S(q)} N(f; \alpha, T) \ll T^B q^{c(1-\alpha)/(2\alpha-1)}$$

where the implied constant depends only on the choice of c .

In our definition of $\mathcal{M}_2$, we took $\alpha = 1 - \eta$ and $T = \log^3 X$, so we have that

$$\#\mathcal{M}_2 \ll X^{c\eta/2(\eta+1)} \log^{3B} X \ll X^{c\eta/(1-2\eta)+\varepsilon}$$

Combining this with (4.11) we have

$$\sum_{k \in \mathcal{M}_2} |I_k \exp(-\Delta(k)/X)| \ll X^{c\eta/(1-2\eta)+\varepsilon}. \quad (4.21)$$

If we take $k \in \mathcal{M}_1$, then we may break the integral $I_k = I_k(x, -\eta/2)$ into two parts, viz. $|\Im(s)| \leq \log^2 X$ and $|\Im(s)| \geq \log^2 X$. In the first part of the integral, Lemma 129 says that $|L(k, s)| \ll X^\varepsilon$, and recall that $x \ll X$, we have that the first part of the integral is $\ll X^\varepsilon x^{-\eta/2}$. For the second part of the integral, we may apply Stirling's formula and (4.10) to see that the second part of the integral is $\ll X^{-A}$ for any $A > 0$. So in total, we have that for $k \in \mathcal{M}_1$ that

$$|I_k| \ll X^\varepsilon x^{-\eta/2} + X^{-A}.$$

Once again, using Conjecture 65 we see that

$$\sum_{k \in \mathcal{M}_1} I_k \ll X^{1+\varepsilon} x^{-\eta/2} \quad (4.22)$$

Then supposing $0 < \eta \ll 1$ and $x = X^\xi$ we may combine (4.22) and (4.21) to get

$$\sum_{\Delta(k) < X \log^2 X} I_k \exp(-\Delta(k)/X) \ll X^{1-\xi\eta/2+\varepsilon} + X^{c\eta/2(\eta+1)+\varepsilon} \quad (4.23)$$

So for any positive ξ and η and ε sufficiently small, we have that (4.23) is $o(X)$. Combining this with the previous section, we have proved Theorem 119 in the field case.

4.3.3 Invertible Ideals and Congruence Conditions

In fact, this proof technique allows us to handle not just ideal classes in number fields, but also *invertible* ideals in *orders* in number fields. Recall from Section 2.3 that we may define the ζ function of an order $\mathcal{O}$ in a number field to be (for $\Re(s) > 1$)

$$\zeta_{\mathcal{O}}(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O} \\ \mathfrak{a} \text{ invertible}}} = \mathfrak{N}(\mathfrak{a})^{-s}$$

and the L -function of $\mathcal{O}$ is $\zeta_{\mathcal{O}}/\zeta$ has an easily defined Euler product expression for its value at $s = 1$:

$$L(\mathcal{O}, 1) = \prod_{q \text{ prime}} \frac{1}{\text{Reg}_q(\mathcal{O})}$$

where $\text{Reg}_q(\mathcal{O}) = \mu_{\mathcal{O}_q}(\mathcal{O}_q^\times) / \mu_{\mathbb{Z}_q}(\mathbb{Z}_q^\times)$. Moreover, $\text{Reg}_q(\mathcal{O})$ depended only on the splitting type of $\mathcal{O}$ at q , and so we might hope to use the NNF Conjecture in order to average L -values in orders subject to certain congruence conditions.

Using the computations of Section 4.2, we see that all of the math in Section 6.1 still carries through. What remains is to handle the error term which arises in Section 6.2. Due to certain technical complications³, while the previous theorems were proven only assuming the Strong Artin Conjecture and the NNF Conjecture, we will from now on assume that $d = [k : \mathbb{Q}] \leq 4$.

Indeed, $L(\mathcal{O}, 1)$ differs from $L(k, 1)$ for the number field $\mathcal{O} \otimes \mathbb{Q}$ in a finite number of Euler factors. Since we are only interested in $L(\mathcal{O}, 1)$, we may in fact modify its definition slightly. Specifically, we will define $L'_p(\mathcal{O}, s)$ to be the Euler factor associated to the splitting type of p in $\mathcal{O}$, with $L'_p(\mathcal{O}, s) = 1$ if $\mathcal{O}/p\mathcal{O}$ is not the reduction of any maximal ring. In particular, $L'_p(\mathcal{O}, s) = L_p(\mathcal{O}, s)$ for all but at most the finitely many primes where $\mathcal{O}$ is nonmaximal, and $L'_p(\mathcal{O}, 1) = \text{Reg}_p(\mathcal{O})^{-1}$. However, we know the exact Euler product of

³Specifically, we will need to know a bound on the total number of suborders of bounded discriminant in the maximal order in a number field.

$L'(\mathcal{O}, s)$, whereas it is potentially rather complicated for $L(\mathcal{O}, s)$.

Since we are changing the definition of $L(\mathcal{O}, s)$ by a finite number of Euler factors, it is not hard to see that L' has an analytic continuation and a Siegel bound, as well as a functional equation. These together give us a convexity bound in the critical strip. Finally, it is easy to see that $L'(\mathcal{O}, s) = 0$ for s in the critical strip if and only if $L(\mathcal{O} \otimes \mathbb{Q}, s) = 0$ as well. And so our math in the previous subsection all goes through for $\mathcal{F}_1$, the set of all orders with discriminant at most $X \log^2 X$ and which do not have a zero in $\Omega(\eta, \log^3 X)$. What is left is to handle its complement, $\mathcal{F}_2$.

For this, it suffices to bound the total number of suborders of discriminant at most X in $\mathcal{O}_k$ for each $k \in \mathcal{M}_2$. At this point, we will begin to treat the cases $d = 3$ and $d = 4$ separately.

In the cubic case, we note that every suborder $\mathcal{O}$ of $\mathcal{O}_k$ is a sublattice of $\mathcal{O}_k$. Moreover, the image of $\mathcal{O}/\mathbb{Z} \subseteq \mathcal{O}_k/\mathbb{Z}$ determines the order $\mathcal{O}$. (Proof: Every cubic order has a basis $(1, \omega, \theta)$.) Now a suborder of index n in $\mathcal{O}_k$ has discriminant $n^2 \Delta(k)$, so we need only count the suborders of $\mathcal{O}_k$ of index at most $\sqrt{X/\Delta(k)}$. However, Datskovsky and Wright [37] proved that

$$\eta_k(s) = \sum_{\mathcal{O} \subseteq \mathcal{O}_k} [\mathcal{O}_k : \mathcal{O}]^{-s}$$

converges absolutely for $\Re(s) > 1$ and that this may be meromorphically continued to the whole complex plane such that

$$\eta_k(s) = \frac{\zeta_k(s)}{\zeta_k(2s)} \zeta(2s) \zeta(3s - 1).$$

Then Perron's formula implies that the total number of suborders in $\mathcal{O}_k$ of index bounded by $\sqrt{X/\Delta(k)}$ is $O(X^{1/2+\varepsilon})$. We combine this with the bound on $\#\mathcal{M}_2$ in the field case to see that

$$\sum |I_k \exp(-\Delta(k)/X)| \ll X^{1/2+c\eta/(1-2\eta)+\varepsilon} = o(X)$$

in the error term.

In the quartic case, Nakagawa [92] shows that the total number of suborders of index $d = \prod p_i^{e_i}$ in $\mathcal{O}_k$ for k a quartic field is $O\left(\prod p_i^{(2+\varepsilon)(\lfloor e_i/4 \rfloor)}\right) = O(n^{1/2+\varepsilon})$. Here $\prod p_i^{e_i}$ is the prime factorization of n . So the total number of orders in $\mathcal{O}_k$ of discriminant at most X is at most a constant times

$$\sum_{n < \sqrt{X/\Delta(k)}} n^{1/2+\varepsilon} \ll X^{3/4+\varepsilon}$$

and so the total to the error term

$$\sum |I_k \exp(-\Delta(k)/X)| \ll X^{3/4+c\eta/(1-2\eta)+\varepsilon} = o(X)$$

for η sufficiently small, which is all that we need.

4.3.4 Stepping Back

In the previous subsection, we completed the proof of Theorem 119 when Σ is either submaximal or subtrivial. But in fact, the results of the previous subsection are easily seen to imply that we may take Σ to be any collection of local conditions which differs from these at a finite number of places. Hence, we have proved the full force of Theorem 119 and hence completed the proof of Theorem 120.

4.4 From moments to a distribution

In this section, we prove Theorem 125. To begin, we recall the following fact.

Lemma 131 ([4, Lemma 6]). *Suppose that $\alpha_0 = 1, \alpha_1, \alpha_2, \dots$ are finite real numbers which are the positive integral moments some probability measure μ on $\mathbb{R}$. Set*

$$f(t) = \sum_{k=0}^{\infty} \frac{\alpha_k}{k!} (it)^k. \tag{4.24}$$

If $f(t_0)$ converges absolutely for some $t_0 > 0$, then μ is the unique probability measure with moments α_k and its characteristic function coincides with $f(t)$ for $|t| < t_0$.

Now define

$$F(z) = \lim_{X \rightarrow \infty} \frac{\#\{k \in \mathcal{F}_X(\Sigma) : L(k, 1) < z\}}{c(\Sigma)X}$$

which exists by Conjecture 122 (or Theorem 66). By the same conjecture, this is a distribution function. Its moments are given by $\alpha_m = c_m(\Sigma)/c(\Sigma)$ where $c_m(\Sigma)$ is leading term in the statement of Conjecture 122.

Next note that from Section 4.2.5 we know that $\sum b^{(m)}(p^e)/p^e = 1 + O(mp^{-2})$. By taking logs and looking at the Taylor series expansion, we see that

$$\sum_m \frac{c_m(\Sigma)}{c(\Sigma)} \cdot t^m \ll \sum \left(\frac{A}{m}\right)^m$$

for some constant A dependent on t . As such, (4.24) converges absolutely for any $t > 0$ and so from the lemma, we see that $F(z)$ defines the unique probability measure with moments α_m .

On the other hand, let X_p be the random variable which takes on the value $\text{Reg}_p(\tau)$ with probability $\mu^{\max}(\tau)$ where τ ranges over the splitting types of p . Then define $X = \prod X_p$, which converges almost surely. It is rather clear that the moments of X are precisely the α_m . Hence, we have completed the proof of Theorem 125.

4.5 Future Work

There are several possible avenues for generalization. For instance, [19, 106] have proven second order main terms for the count of cubic fields up to discriminant X . As such, one can immediately conjecture that there is a second order main term for *every* moment $L(k, 1)^m$, not just when $m = 0$. Indeed, Goldfeld–Hoffstein already discovered this phenomenon for

quadratic fields when they proved Theorem 120 in the case $d = 2$ in [58]. As we noted in Section 4.3, current technology is not quite strong enough to prove second order main terms.

Another direction for generalization is to generalize these results to larger base fields. In this case, the NNF conjecture is available in the abelian cases due to work of Wright [115] and in case of S_d number fields ($d \leq 5$) due to work of Shankar in his forthcoming thesis. However, Shankar currently does not have a power saving error term as in the NNF Conjecture, but this seems likely to arrive soon. Moreover, the Strong Artin Conjecture is available for G nilpotent and for $G = S_4$. We note also that Theorem 130 extends to automorphic forms attached to these field extension through Weil restriction to $\mathbb{Q}$.

As for the geometric side, we give an explanation in Chapter 3 as to why we should not expect any more prehomogeneous vector spaces which would yield parameterizations of ideal classes. However, one may, in the spirit of Chapter 5 still produce varieties whose integral points correspond to ideal classes. Unfortunately, counting integer points on varieties is extremely difficult and any progress in this area would be considered a major advance.

Finally, there are two other parameters which can be varied: m and s . Specifically, we could instead of considering integral moments consider more general *complex* moments. Through the method of moments, we could then get a better handle on extreme behavior of the product of the class number and regulator much as [60] did for quadratic characters. Finally, we could use these methods to compute averages $L(k, s)$ for s close to 1, much as Goldfeld and Hoffstein did in [58] for quadratic characters. We plan to attack these ideas in the near future.

Part III

Commutative Algebra and the Symmetric Group

Chapter 5

Multiplicative Structures on the Free Resolution of n Points in $\mathbb{P}^{n-2}$

5.1 Introduction

In [25], Buchsbaum and Eisenbud make the following conjecture:

Conjecture 132 ([25]). *If R is a local ring, then the minimal free resolution of a cyclic R module possesses a nontrivial commutative, associative, differential graded algebra (ACDGA) structure.*

Remark 133. For the definition and basic properties of differential graded algebras, please see Section 1.2.2 of Chapter 1.

Buchsbaum and Eisenbud were led to make this conjecture from their observations about the Koszul complex and their construction in [25] of such a structure on the free resolution on the free resolution of cyclic codimension 3 Gorenstein modules. Indeed, they even showed that an *a priori* commutative DGA structure exists. However, as they note in the same paper, the conjecture as stated is false. In this chapter, we provide several more cases in which it is true, and extend Buchsbaum and Eisenbud's construction to higher

codimensions.

Theorem 134. *Let k be an algebraically closed field of characteristic 0. Then the minimal free resolution of $n \geq 3$ general points in $\mathbb{P}_k^{n-2}$ admits a nontrivial ACDGA structure.*

Perhaps the most striking aspect of our proof is the role of the representation theory of finite groups. Similar multiplicative structures, reviewed below, tend to rely on the presence of a reductive automorphism group (usually GL_n). In the cases we handle, the relevant stabilizer is S_n . In fact, while our first results concern algebraically closed fields, where the representation theory of S_n is clear, we may push our results to non-closed fields.

Theorem 135. *Let k be a field of characteristic 0. Let $X \subseteq \mathbb{P}_k^{n-2}$ be a dimension 0 subscheme of degree $n \geq 3$ which is geometrically n points in linearly general position¹. Then the minimal free resolution of X admits a canonical associative, commutative differential graded algebra structure. In particular, if we require the resolution to be S_n -equivariant, then this resolution is unique up to unique isomorphism.*

Such strong canonicity in these multiplicative structures has been implicitly used by many authors. For instance, Wright and Yukie [116] implicitly used this structure to parameterize rank n rings over $\mathbb{Q}$. And Bhargava also implicitly relied on a much stronger canonicity (over $\mathbb{Z}$) in structuring his Higher Composition Laws [9, 10, 11, 14]. Perhaps the place where the idea of using such canonical multiplicative structures was first developed was in Deligne’s letter to Bhargava [41] which inspired Wood’s vast generalization in her thesis [114, 113, 112] extending Bhargava’s quadratic, cubic, and quartic Higher Composition Laws to arbitrary base schemes. As a first step in generalizing these results, we also prove the following theorem.

Theorem 136. *Let $\pi : X \rightarrow Y$ be a Gorenstein cover of schemes of degree $n \geq 3$ with Y integral whose generic point $\eta \in Y$ has characteristic 0. Moreover, suppose that X is*

¹This means that no $n - 2$ points lie on a hyperplane.

generically étale in the sense that the fiber $X_\eta \rightarrow \eta$ is an étale cover of degree n . Then X admits a minimal free resolution, and this resolution has a canonical ACDGA structure.

One striking feature of the codimension one, two, and three cases of Theorem 134 (which were known before this work) is that they also produce series of moduli spaces for codimension ≤ 3 Gorenstein ideals which take the form of a quotient of a vector space by the linear action of a reductive group. There is ample evidence that any more general structure theorems cannot be this simple. For instance, n distinct points in $\mathbb{P}^{n-2}$ form an arithmetically Gorenstein scheme. However, over an algebraically closed field, all n -tuples of general points in $\mathbb{P}^{n-2}$ lie in the same PGL_{n-1} orbit. As such, if there were to exist a vector space parameterizing such ideals, then it would necessarily be *prehomogeneous*, i.e., have a single open Zariski dense orbit under the action of some group which would presumably be reductive. But there is a finite list [97] of irreducible prehomogeneous vector spaces attached to reductive groups². Moreover, Bhargava has given arithmetic interpretations for most of these vector spaces, making it unlikely that any more will be found. Of course, perhaps the relevant vector spaces are actually attached to *nonreductive groups*, but there prehomogeneous vector spaces are no longer guaranteed to have a single invariant, which would also be contrary to our expectation that the unique invariant should be the discriminant of the associated ring. However, we should not completely rule out this possibility, as Bhargava and Shnidman’s work [20] for counting A_3 extensions of $\mathbb{Q}$ indicates.

However, using the ideas of Wood’s thesis and an irreducibility result of Poonen’s [95], one may give an inexplicit proof of Bhargava’s Higher Composition Laws. Using Theorem 136 and similar ideas, we may parameterize rank n rings over $\mathbb{Z}$, but not by the integer orbits on a vector space, but rather by the integer orbits on a certain orbit of a complex Lie group. The proof of this fact does not appear in this thesis, but shall be the topic of future work of

²This is actually up to “castling”. Without this qualification, there are actually an *infinite* number of such spaces and so one might suspect that you could find parameterizations of these ideals among them. However, a short study of how the castling transformation affects these vector spaces, specifically which groups can appear, seems to indicate the contrary.

ours. Moreover, we can obtain extensions to higher dimensions similar to those of [16, 67]. In particular, we expect if one could count the number of integer orbits in the spaces we enumerate, one could prove bounds on the average size of the n -Selmer groups of elliptic curves a la [17, 18]. These results are far out of reach for the moment, but are areas of active interest.

Before moving on, we would like to give a little more historical context to this result. Much work has been done to construct moduli spaces of algebro-geometric objects, for instance, in finding appropriate ways to deal with the inevitable singularities of the spaces. This work often falls under the heading of noncommutative geometry, and one of the objects which is often promoted for this purpose is dg-schemes, where the sheaf of algebras is replaced by a sheaf of differential graded algebras. This approach to deformation theory has appeared in works by Kontsevich [71], Ciocan-Fontanine–Kapranov [34], and others. Moreover, it figures into Kuznetsov’s notion of homological projective duality [81], with which he hopes to prove general statements about the rationality of cubic fourfolds. We hope that our work will shed light on some of their more canonical constructions. More generally, dg-categories (i.e., categories enriched over complexes of modules for some commutative ring) provide the first example of A_∞ categories [72] at the heart of much recent work, for instance, in trying to determine what exactly is the Fukaya-category of a symplectic manifold [99].

As to simultaneous associativity and commutativity, it turns out that the Leibniz rule is actually a rather restrictive condition. In terms of general results, Buchsbaum and Eisenbud showed in [25] that every minimal free resolution of a cyclic R module admits a commutative but not necessarily associative DGA structure through a trick which will be integral to our work. For specific cases, suppose that $m \geq n$ and I is generated by the maximal minors of a generic³ $m \times n$ matrix M of elements of $\mathfrak{m}$. Then the minimal free resolution of R/I is given by the Eagon–Northcott complex [43]. In her thesis, Srinivasan [103]

³Here this means that the grade of the ideal I is $m - n + 1$, the greatest possible value.

showed that if R contains $\mathbb{Q}$ the rational numbers, then this minimal free resolution admits an ACDGA structure. Following up, Pelikaan [94] gave an associative but not necessarily commutative structure on this resolution even when R did not contain the rationals. He showed that it was also commutative when $n \leq m \leq n + 1$.

More generally, there are resolutions (not necessarily minimal) of R/I when I is generated by the nonmaximal minors of M . These are the *Buchsbaum-Rim complexes* [26]. Gover [59] produced an associative DGA structure on these complexes such that those associated to nonmaximal minors were modules over the complex associated to the maximal minors.

Similarly, Schur complexes as developed by Akin, Buchsbaum and Weyman [1] come equipped with a natural multiplicative structure, of which the Koszul complex is the most accessible example.

After Buchsbaum and Eisenbud, there has not been too much work on nondeterminantal ideals of a given codimension. Indeed, neither the Cohen-Macaulay nor the Gorenstein condition is enough to guarantee existence of an ACDGA structure, as Hinic [2] and Avramov [3] point out in the Cohen-Macaulay and Gorenstein cases, respectively. There has been some work on the codimension four case, due to Kustin and Miller [75]. We should also mention that these two authors have given many examples of multiplicative structures on other resolutions [77, 79] and have found applications to build an “almost generic” resolution for codimension four Gorenstein ideals [78, 76] and to classify their Tor algebras [80].

This chapter is organized as follows. In Section 5.2, we prove that the minimal free resolution of X admits an action by S_n which in turn gives it a very nice structure. In fact, by working with a particular set of points, we give a structure which is actually defined over $\mathbb{Z}$. In Section 5.3 we further exploit the representation theory of S_n to show that the resolution of X also admits an ACDGA structure. In Section 5.4, we descend our results from an algebraically closed field to *any* field of characteristic 0. Finally, in Section 5.5, we prove Theorem 136 exploiting our work in Section 5.4 and the hard work of Section 5.2

giving us at least one $\mathbb{Z}$ structure.

Remark 137. Starting in the next section we will ignore the case $n = 3$ as it does not fit into our scheme of proof. But this case is obvious: In $\mathbb{P}^1$, any dimension 0 subscheme is cut out by a (unique up to scalars) binary form of degree equal to the degree of the subscheme. So the resolution of X is given by

$$R(-3) \xrightarrow{f} R$$

where f is the form cutting out X and $R = k[x_0, x_1]$ is the homogeneous coordinate ring of $\mathbb{P}^1$. The multiplication table is then determined by the canonical maps:

$$\begin{aligned} R \otimes R &\rightarrow R \\ R \otimes R(-3) &\rightarrow R(-3) \\ R(-3) \otimes R(-3) &\rightarrow 0 \end{aligned}$$

The resulting structure is obviously an ACDGA.

Acknowledgments

For this chapter, we are particularly indebted to V.V. Shende for his comments and advice.

5.2 An S_n -equivariant resolution of X

Throughout this section, we will work over an algebraically closed field k of characteristic 0. We let $X \subseteq \mathbb{P}^{n-2}$ be a collection of $n \geq 4$ points in linearly general position. Since all sets of n points in $\mathbb{P}^{n-2}$ are conjugate under the action of PGL_{n-1} , we may assume without loss

of generality $X = \{p_0, \dots, p_{n-1}\}$ where $p_i = [p_{i0} : p_{i1} : \dots : p_{i,n-2}]$ with

$$p_{ij} = \begin{cases} \delta_{ij} & i \neq n-1 \\ 1 & i = n-1 \end{cases}$$

Let $R = k[x_0, \dots, x_{n-2}]$ and let $I \subseteq R$ be the ideal which cuts out X . Then we have the following theorem.

Theorem 138. *The minimal free resolution of $X \subseteq \mathbb{P}^{n-2}$ has the shape:*

$$R(-n) \rightarrow R(-n+2)^{b_{n-3}} \rightarrow R(-n+3)^{b_{n-4}} \rightarrow \dots \rightarrow R(-2)^{b_1} \rightarrow R$$

where for $1 \leq i \leq n-3$ we have

$$b_i = n \binom{n-2}{i} - \binom{n}{i+1}. \quad (5.1)$$

Remark 139. Note that b_i actually depends on n as well. If we need to emphasize the role played by n , we will denote this by $b_{i,n}$.

Proof. There are several potential proofs of Theorem 138, and in fact we provide a slightly novel one in Chapter 6. Schenzel [98] and Hoa [68] have given direct proofs of this fact. Another possible proof which gives all but the last Betti number is the work of Green and Lazarsfeld on their property (N_p) [63]. Another direction is to embed $\mathbb{P}^{n-2} \subseteq \mathbb{P}^{n-1}$ as a hyperplane and to show that the p_i live on an elliptic normal curve, which is a variety of almost minimal degree and as such has a known minimal free resolution (e.g., [46, Chapter 6]). Coupled with the fact that varieties of almost minimal degree are always arithmetically Cohen-Macaulay so that generic hyperplane sections have the same Betti numbers, we arrive at the result. $\square$

Corollary 140. *The subscheme X is arithmetically Gorenstein.*

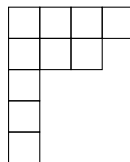
Proof. The Betti numbers of X are symmetric in the sense of Theorem 24 of the introduction to this thesis. Moreover, it is not hard to show (using, say, the cohomological description of [5, Section 1]) that X is at least arithmetically Cohen-Macaulay. Putting these facts together, we arrive at the assertion. $\square$

Remark 141. In fact, one may show that the points are in general position if and only if they are arithmetically Gorenstein, see e.g. [69, Theorem C.ii].

Recall that over an algebraically closed field of characteristic 0 there is a canonical bijection between the irreducible representations of S_n and the partitions of the number n . We will often write partitions as Young diagrams, using the British convention, or as a sorted multiset. For instance, the partition $5 = 3 + 2$ may be written as $\{3, 2\}$ or as

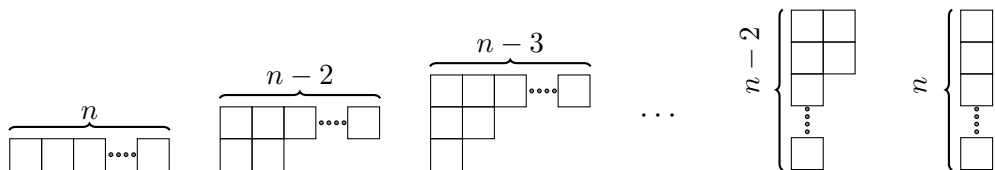


and the partition $10 = 4 + 3 + 1 + 1 + 1$ may be written as $\{4, 3, 1, 1, 1\}$ or as



For more information, see Chapter 6 or [54, Chapter 6].

Lemma 142. *The numbers b_i from Theorem 138 are the dimensions of certain irreducible representations of S_n , namely, $b_0, b_1, b_2, \dots, b_{n-2}$ are precisely the dimensions of the representations*



In words, the first representation is the trivial representation, the last the alternating representation. The second has $n - 2$ boxes on the first row and two boxes on the second. Subsequent partitions move a single box from the first row to the first column until the penultimate partition is reached.

Proof. Let F_i represent both the i th Young diagram listed and the corresponding representation of S_n over k . Then F_0 and F_{n-2} are the trivial and alternating representations of S_n , respectively, both of which have dimension $1 = b_0 = b_{n-2}$.

Our proof is by induction on n . We note that the case $n = 4$ is trivial, as $b_{1,4} = 2$ and $\dim F_1 = 2$. In order to perform the inductive step, we recall the branching law for representations of S_n (cf. e.g. [108]). Recall that S_n is defined as the automorphisms of the set $\{1, \dots, n\}$. Then the stabilizer of any $i \in \{1, \dots, n\}$ is some $S_{n-1} \subseteq S_n$. Since the action of S_n on $\{1, \dots, n\}$ is transitive, all such S_{n-1} are conjugate. We call these the *standard* S_{n-1} 's in S_n . If $n > 6$, then these are in fact the *only* S_{n-1} 's in S_n .

Now suppose that $\lambda = \{\lambda_1, \lambda_2, \dots\}$ is a partition of n . Then we say that a partition $\mu = \{\mu_1, \mu_2, \dots\}$ of $n - 1$ is a *restriction of λ* if $\mu_i \leq \lambda_i$ for all i . Stated less formally, μ has Young diagram which is the same as λ , except one row has one fewer box.

Theorem 143 (Branching Law). *The restriction to a standard S_{n-1} of the representation of S_n associated to λ is isomorphic to the direct sum of the representations associated to all μ partitions of $n - 1$ which are restrictions of λ .*

Remark 144. Stated less formally, each irreducible component of the restriction of the representation associated to λ to a standard S_{n-1} appears precisely once. Moreover, the irreducible representations that appear differ from λ by removing a single box such that the resulting diagram remains the Young diagram of a partition.

We now show $b_{1,n} = \dim F_1$ for all $n \geq 5$. Consider the restriction of F_1 to a standard

S_{n-1} . Then the branching law implies that the resulting representation splits as

$$\overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & & \\ \hline \end{array}}^{n-1} \oplus \overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \end{array}}^{n-2}.$$

The dimensions of these representations are $n-2$ and $b_{1,n-1}$, the second fact being by induction. According to Theorem 138, we know that $b_{1,n} = n(n-2) - \binom{n}{2}$. On the other hand,

$$(n-2) + b_{1,n-1} = (n-2) + (n-1)(n-3) - \binom{n-1}{2} = n(n-2) - \binom{n-1}{1} - \binom{n-1}{2},$$

and so by Pascal's identity we have the claim.

We now show that $b_i = \dim F_i$ for all other i . By symmetry, we know that $b_{n-3} = \dim F_{n-3} = \dim F_1 = b_1$, so we may assume $1 < i < n-3$. Thus, upon restricting to S_{n-1} , we find that V_i splits as

$$i \left\{ \overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \square & & \\ \hline \vdots & & \\ \hline \square & & \end{array}}^{n-i-1} \oplus 1 \left\{ \overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \square & & \\ \hline \vdots & & \\ \hline \square & & \end{array}}^{n-i-1} \oplus 1 \left\{ \overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \square & & \\ \hline \vdots & & \\ \hline \square & & \end{array}}^{n-i-2} \right. \right.$$

(Note that we have used here that $1 < i < n-3$ as there would otherwise have only been *two* terms in the decomposition.) So it suffices to show

$$b_{i,n} = b_{i,n-1} + \binom{n-2}{i} + b_{i-1,n-1} = n \binom{n-2}{i} - \binom{n}{i+1}.$$

This is just a simple computation. Hence we are done. $\square$

It turns out that this is not a coincidence. By definition, PGL_{n-1} acts on $\mathbb{P}^{n-2}$. Let

$G \subseteq \mathrm{PGL}_{n-1} k$ be the stabilizer of X . Then G actually *permutes* the points p_i , i.e., there is a surjection $G \twoheadrightarrow S_n$. Moreover, this is actually an *isomorphism*. For if the points $p_i \in \mathbb{P}_k^{n-2}$ are fixed, then the *lines* in $\mathbb{A}_k^{n-1}$ they correspond to are *also* fixed. That is, if $q_0, \dots, q_{n-1}$ are lifts of the p_i , and $g \in \ker(G \twoheadrightarrow S_n)$ then $g(q_i) = a_i q_i$ for some $a_i \in k$. But we note that one choice of lifts is $q_i = (q_{i0}, \dots, q_{i,n-1})$ with

$$q_{ij} = \delta_{ij} \text{ when } i \neq n-1$$

and $q_{n-1} = -(q_0 + \dots + q_{n-2})$. Then

$$g(q_{n-1}) = a_{n-1} q_{n-1} = -(a_0 q_0 + \dots + a_{n-2} q_{n-2} = a_{n-1} q_0 + \dots + a_{n-1} q_{n-2}).$$

Hence, $a_i = a_{n-1}$ for all i . That is, g is a multiple of the identity matrix and hence trivial in $\mathrm{PGL}_{n-1}(k)$.

Moreover, we see that the group $G \subseteq \mathrm{PGL}_{n-1}$ has a lift to GL_{n-1} . Consider the permutation representation of S_n on k^n , say with basis vectors $e_1, \dots, e_n$. Then let $V = k^n / (e_1 + \dots + e_n)$ be the standard representation of S_n . Fix as a basis of V the reductions $\bar{e}_1, \dots, \bar{e}_{n-1}$, so $\bar{e}_n = -(\bar{e}_1 + \dots + \bar{e}_{n-1})$. Identifying $\mathbb{P}V = \mathbb{P}^{n-2}$ by $k\bar{e}_i = p_i$ for all i , we see that the actions of S_n on $\mathbb{P}V$ and $\mathbb{P}^{n-2}$ coincide. That is, letting $\tilde{G}$ be the preimage of G in GL_{n-1} , we see that the exact sequence

$$0 \rightarrow \mathbb{G}_m \rightarrow \tilde{G} \rightarrow S_n \rightarrow 0 \tag{5.2}$$

splits. In particular, since $\mathbb{G}_m$ is central, we see that $\tilde{G} \cong \mathbb{G}_m \times S_n$.

Lemma 145. *There are precisely two splittings of (5.2). In both, the image of $S_n \subseteq \mathrm{GL}_{n-1}$ is an irreducible representation. One lift corresponds to the partition $\{n-1, 1\}$ and the other to the partition $\{2, 1, 1, \dots, 1\}$.*

Proof. A choice of $S_n \subseteq \tilde{G}$ is determined by a choice of Coxeter generators, i.e., elements $s_i \in \tilde{G}$ with $1 \leq i \leq n-1$, $s_i^2 = 1$ for all i and $(s_i s_j)^{m_{ij}} = 1$ where $m_{i,i\pm 1} = 3$ and all other $m_{ij} = 2$. Moreover, all ordered sets of Coxeter generators are conjugate and any set of elements satisfying these relations will generate S_n .

Now start with a splitting $\tilde{G} \cong \mathbb{G}_m \times S_n$. Then any choice of Coxeter generators $s_i = (\mu_i, t_i) \in \mathbb{G}_m \times S_n$ will have t_i as Coxeter generators of our chosen S_n since they satisfy the Coxeter relations. Since all Coxeter relations are conjugate and $\mathbb{G}_m$ is central, we may as well assume $t_i = ((i)(i+1))$ is the usual Coxeter generator.

Then the Coxeter relations imply $\mu_i^2 = 1$, i.e., $\mu_i = \pm 1$ for all i . Then the relation $(\mu_i \mu_{i+1})^3 = 1$ implies that $\mu_i = \mu_{i+1}$ for all i . Moreover, it is easy to see that the elements $(-1, t_i)$ satisfy the Coxeter relations, and hence generate S_n .

For the final statement of the theorem, note that we have already shown that one lift is the standard representation $\{n-1, 1\}$ of S_n . Then the other lift has Coxeter generators $(-1, (i(i+1)))$. But the trace of the matrix in GL_{n-1} corresponding to $(-1, (i(i+1)))$ is the negative of the trace of the matrix corresponding to $(1, (i(i+1)))$. From character theory, this means that the representation is the standard representation twisted by the alternating representation and as such has partition $\{2, 1, 1, \dots, 1\}$. $\square$

Since these two lifts give different representations when $n \geq 5$, there is a canonical choice of lift, which we will take to be the standard representation $S_n \subseteq \mathrm{GL}(V)$.

Let $R = k[x_0, \dots, x_{n-2}] = \mathrm{Sym}^\bullet V^\vee$ be the homogeneous coordinate ring of $\mathbb{P}^{n-2} = \mathbb{P}V$ and let $I = I_X \subseteq R$ be the ideal of X and $S = R/I$ be the homogeneous coordinate ring of X . As noted in Corollary 140, S is Gorenstein. Moreover, let I_2 be the subspace of I consisting of forms of degree 2.

According to Theorem 138, $I = (I_2)$, i.e., I is generated by quadrics. In fact, we may write these quadrics down.

Lemma 146. *For distinct $i, j, k \in \{0, \dots, n_2\}$, let $f_{i,jk} = x_i(x_j - x_k) \in R$. The $f_{i,jk}$ span I_2 .*

Proof. That the f_{ijk} all vanish on X is evident. Moreover, it is not hard to see that in fact they do not vanish at any other point. Finally, the ideal $J = (f_{ijk})$ is saturated, or else its saturation I would have to contain a linear form, which contradicts the assumption that the points are in general position. Hence, $I = J$ and we have proved the lemma. $\square$

Remark 147. For notational convenience, we define $f_{i,jk} = 0$ whenever two of i, j, k are equal.

Now S_n acts on V , and hence on $V^\vee$ and thus on $R = \text{Sym}^\bullet(V^\vee)$. This action is degree preserving. Moreover, since S_n preserves X , it must also preserve I , and hence I_2 since it preserves degrees. We can then ask *which* representation of S_n is given by I_2 . We can then decompose $\text{Sym}^2(V^\vee)$ using character theory and the fact that all representations of S_n are self-dual, and we find that it is isomorphic to

$$\overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \end{array}}^n \oplus \overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & & \end{array}}^{n-1} \oplus \overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \end{array}}^{n-2}.$$

The trivial representation is the span of $x_0^2 + \cdots + x_{n-2}^2 + (x_0 + \cdots + x_{n-2})^2$, which is not in the span of the f_{ijk} since every monomial of f_{ijk} is squarefree. Similarly, the standard representation is spanned by $\{x_i(x_0 + \cdots + x_{n-2}) : 0 \leq i \leq n-2\}$, which also contains non-squarefree monomials. So we are left only with rightmost Young diagram and the nonobvious lemma:

Lemma 148. I_2 is the irreducible S_n representation

$$\overbrace{\begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & & \end{array}}^{n-2}.$$

We will now collect some facts about the action S_n on the $f_{i,jk}$. It suffices to determine the action of transpositions (ℓ, m) for $0 \leq \ell, m \leq n-1$.

Lemma 149. *If $0 \leq \ell, m < n - 1$, then the action of (ℓ, m) on $f_{i,jk}$ is the usual permutation action on the i, j, k . If $m = n - 1$, then*

$$(\ell, n - 1)f_{i,jk} = \begin{cases} f_{i,jk} - f_{\ell,jk} & \ell \neq i, j, k, \\ -f_{\ell,jk} & \ell = i, \\ f_{i,jk} - f_{j,ik} & \ell = j, \text{ and} \\ f_{i,jk} - f_{k,ji} & \ell = k. \end{cases}$$

Proof. All of these are simple computations, but just to set ideas, we prove the third line of the displayed relations.

$$\begin{aligned} (j, n - 1)f_{i,jk} &= (j, n - 1)[x_i(x_j - x_k)] \\ &= (x_i - x_j)[-x_j - (x_k - x_j)] \\ &= x_jx_k - x_ix_k \\ &= x_jx_k - x_ix_k + (x_ix_j - x_ix_j) \\ &= x_i(x_j - x_k) - x_j(x_i - x_k) \\ &= f_{i,jk} - f_{j,ik}. \end{aligned}$$

□

This is the first step of the proof of the following theorem:

Theorem 150. *The minimal free resolution of X has an S_n -equivariant expansion which has shape*

$$F_{n-2} \otimes R(-n) \rightarrow F_{n-3} \otimes R(-n+2) \rightarrow \cdots \rightarrow F_1 \otimes R(-2) \rightarrow F_0 \otimes R,$$

where the F_i are as in Lemma 142.

From Theorem 138 and Lemma 142, we know that if $\mathbb{K}_\bullet$ is the minimal free resolution of S , then $\mathbb{K}_m \cong E_m \otimes R(-a_m)$ where E_m is a vector space with $\dim_k E_m = \dim_k F_m$. Notably, it is also an S_n representation since it will inductively be the kernel of an S_n equivariant map. Our strategy of proof will be for each E_m to find a subrepresentation $W \subseteq E_m$ which is isomorphic to F_m , and thus by dimension considerations, $E_m = W \cong F_m$.

We begin with the case $n = 4$. In this case, we are almost done with the proof, since $E_0 \cong F_0$ is obvious, and $E_1 \cong F_1$ was Lemma 148. Moreover, Theorem 138 implies we only need to show that $E_2 \subseteq F_1 \otimes \text{Sym}^2 V^\vee$ is the alternating representation of S_4 .

We know that $\dim E_1 = 2$, and so in particular it is generated by

$$\begin{aligned} f_{012} &= x_0(x_1 - x_2) \text{ and} \\ f_{120} &= x_1(x_2 - x_0). \end{aligned}$$

To distinguish between elements of R and elements of, say, $F_1 \otimes \text{Sym}^2 V^\vee$, we denote by $s_{i,jk}^1 \in F_1$ the element corresponding to $f_{i,jk} \in \text{Sym}^2 V^\vee$. In this notation, $s_{0,12}^1$ and $s_{1,20}^1$ admit a quadratic syzygy, namely:

$$f_{012}s_{120}^1 - f_{120}s_{012}^1. \tag{5.3}$$

Since E_2 is a one-dimensional S_n representation, it is either the trivial or the alternating representation. In fact, we see that

$$(01) \cdot (f_{0,12}s_{1,20}^1 - f_{1,20}s_{0,12}^1) = f_{1,02}s_{0,21}^1 - f_{0,21}s_{1,02}^1 = -(f_{0,12}s_{1,20}^1 - f_{1,20}s_{0,12}^1).$$

Thus, the action of S_4 on E_2 is nontrivial and so is necessarily the alternating action.

From now on, we assume that $n \geq 5$. We begin with a definition, which will turn out

to give us an explicit realization of the m -syzygies in Theorem 138. Let $1 \leq m \leq n-3$ be an integer and let I denote an ordered m -tuple of distinct integers in $[0, n-1]$. Let $J = (j_1, j_2)$ be an ordered pair of distinct integers in $[0, n-1]$ disjoint from I . Denote by I_k the k th element of I and J_k the k th element of J . Similarly, denote by I^k the ordered $(m-1)$ -tuple which is $(I_1, \dots, \hat{I}_k, \dots, I_m)$. For $\sigma \in S_m = \text{Aut}(I)$, let $\varepsilon(\sigma)$ denote the sign of the permutation. Finally, for $m \geq 2$, define

$$s_{I,J}^m = \frac{1}{(m-1)!} \sum_{\sigma \in S_m} \varepsilon(\sigma) x_{\sigma(I)_1} s_{\sigma(I)^1, J}^{m-1}. \quad (5.4)$$

Remark 151. Note that for any permutation $\sigma \in \text{Aut}(I)$ we have that $s_{I,J}^m = \varepsilon(\sigma) s_{\sigma(I), J}^m$, so in particular, this definition makes sense over $\mathbb{Z}$.

As it stands, this definition actually only makes sense for the case $m = 2$ as we defined $s_{i,jk}^1 \in F_1$ above, presuming that Theorem 134 has been shown for all pairs (m_0, n_0) such that either $n_0 < n$ or $n_0 = n$ and $m_0 < m$. Then the $s_{I,J}^m \in V^\vee \otimes F_{m-1}$.

Let W be the span of the $s_{I,J}^m$. Since W is a subspace of an S_n representation, it is acted on by S_n . For transpositions (k, ℓ) with $0 \leq k, \ell < n-1$, we see by induction on m that S_n acts in the obvious way on indices. For transpositions $(k, n-1)$, we have the following lemma.

Lemma 152. *The action of (k, ℓ) on $s_{I,J}^m$ is given as follows:*

$$(k, n-1)s_{I,J}^m = \begin{cases} s_{I,J}^m - \sum_{i=1}^m s_{I \overset{i}{\leftrightarrow} k, J}^m & k \notin I \cup J, \\ -s_{I,J}^m & k \in I, \\ s_{I,J}^m - \sum_{i=1}^m s_{I \overset{i}{\leftrightarrow} k, ij_2}^m & k = j_1, \text{ and} \\ s_{I,J}^m - \sum_{i=1}^m s_{I \overset{i}{\leftrightarrow} k, j_1 i}^m & k = j_2. \end{cases}$$

Here the notation $I \overset{i}{\leftrightarrow} k$ means the ordered m -tuple $(I_1, \dots, I_{i-1}, k, I_{i+1}, \dots, I_m)$.

Proof. We note that we have already shown the $m = 1$ case of this lemma: it was Lemma 149. For larger m , the computation gets a bit messy, so for clarity, we first make the computation for $m = 2$. Here

$$s_{ij,\ell m}^2 = x_i s_{j,\ell m}^1 - x_j s_{i,\ell m}^1.$$

We first take $k \notin I \cup J$. Then acting by $(k, n - 1)$ gives

$$\begin{aligned} & (x_i - x_k)(s_{j,\ell m}^1 - s_{k,\ell m}^1) - (x_j - x_k)(s_{i,\ell m}^1 - s_{k,\ell m}^1) \\ &= [x_i s_{j,\ell m}^1 - x_j s_{i,\ell m}^1] - [x_k s_{j,\ell m}^1 - x_j s_{k,\ell m}^1] + [x_k s_{i,\ell m}^1 - x_i s_{k,\ell m}^1] + [x_k s_{k,\ell m}^1 - x_k s_{k,\ell m}^1] \\ &= s_{ij,\ell m}^2 - s_{kj,\ell m}^2 - s_{ik,\ell m}^2. \end{aligned}$$

If $k \in I$, then we assume $k = i$, so we act by $(i, n - 1)$ on $s_{ij,\ell m}^2$ and get

$$-x_i(s_{j,\ell m}^1 - s_{i,\ell m}^1) - (x_j - x_i)(-s_{i,\ell m}^1) = -(x_i s_{j,\ell m}^1 - x_j s_{i,\ell m}^1) + [x_i s_{i,\ell m}^1 - x_i s_{i,\ell m}^1] = -s_{ij,\ell m}^2.$$

If $k \in J$, then we may as well assume $k = \ell$ and we get

$$\begin{aligned} & (x_i - x_\ell)(s_{j,\ell m}^1 - s_{\ell,jm}^1) - (x_j - x_\ell)(s_{i,\ell m}^1 - s_{\ell,im}^1) \\ &= [x_i s_{j,\ell m}^1 - x_j s_{i,\ell m}^1] + [x_j s_{\ell,im}^1 - x_i s_{\ell,jm}^1] + x_\ell (s_{i,\ell m}^1 - s_{j,\ell m}^1 + s_{\ell,jm}^1 - s_{\ell,im}^1). \end{aligned}$$

The first bracketed expression is $s_{ij,\ell m}^2$. Working inside of $F_1 \subseteq \text{Sym}^2 V^\vee$, we see that the last bracketed expression is $s_{m,ji}^1$. Now we add and subtract $x_\ell(s_{j,im}^1 + s_{i,mj}^1)$ and we come to the expression

$$s_{ij,\ell m}^2 - s_{\ell j,im}^2 - s_{i\ell,jm}^2 + x_\ell(s_{j,im}^1 + s_{i,mj}^1 + s_{m,ji}^1).$$

However, we may again work in $F_1 \subseteq \text{Sym}^2 V^\vee$ in order to show that the bracketed expression on the right is 0. Hence, we arrive at the lemma.

For larger $m > 2$, the calculations become much more arduous. But the results remain

the same. Let us begin by assuming $k \notin I \cup J$. Then the effect of applying $(k, n-1)$ on $s_{I,J}^m$ is

$$\begin{aligned}
& \sum_{\sigma \in S_m} \varepsilon(\sigma) (x_{\sigma(I)_1} - x_k) (s_{\sigma(I)^1, J}^{m-1} - \sum_{i=1}^{m-1} s_{\sigma(I)^1 \overset{i}{\leftrightarrow} k, J}^{m-1}) \\
&= \sum_{\sigma \in S_m} \varepsilon(\sigma) x_{\sigma(I)_1} s_{\sigma(I)^1, J}^{m-1} - \sum_{\sigma \in S_m} \varepsilon(\sigma) x_k s_{\sigma(I)^1, J}^{m-1} \\
&\quad - \sum_{\sigma \in S_m} \varepsilon(\sigma) x_{\sigma(I)_1} \sum_{i=1}^{m-1} s_{\sigma(I)^1 \overset{i}{\leftrightarrow} k, J}^{m-1} + x_k \sum_{\sigma \in S_m} \varepsilon(\sigma) \sum_{i=1}^{m-1} s_{\sigma(I)^1 \overset{i}{\leftrightarrow} k, J}^{m-1}. \quad (5.5)
\end{aligned}$$

The first summand of (5.5) is visibly $s_{I,J}^m$. We now analyze the other summands.

We begin by showing the last summand of (5.5) is 0. Note that for all σ, i , there is another $\sigma' = (1i)\sigma \in S_m$ such that $\sigma'(I)^1 \overset{i}{\leftrightarrow} k = \sigma(I)^1 \overset{i}{\leftrightarrow} k$. As S_m is a group and $(1i)$ is an involution, this partitions S_m . Moreover, $\varepsilon(\sigma) = -\varepsilon(\sigma')$. Hence, the last term is 0.

Now we need to show that the middle two terms are $-\sum_{p=1}^m s_{I \overset{p}{\leftrightarrow} k, J}^m$. Let's expand this sum:

$$\sum_{p=1}^m \sum_{\sigma \in S_m} \varepsilon(\sigma) x_{\sigma(I \overset{p}{\leftrightarrow} k)_1} s_{\sigma(I \overset{p}{\leftrightarrow} k)^1, J}^{m-1} = \sum_{\sigma \in S_m} \sum_{p=1}^m \varepsilon(\sigma) x_{\sigma(I \overset{p}{\leftrightarrow} k)_1} s_{\sigma(I \overset{p}{\leftrightarrow} k)^1, J}^{m-1}.$$

For a fixed $\sigma \in S_m$, let $q = \sigma^{-1}(1)$. Then the q th term of the inside sum is $x_k s_{\sigma(I)^1, J}^{m-1}$. This is the second summand in (5.5).

As for the sum over the other p 's, it is easy to see that it is precisely

$$\sum_{i=1}^{m-1} \varepsilon(\sigma) x_{\sigma(I)_1, J} s_{\sigma(I)^1 \overset{i}{\leftrightarrow} k, J}^{m-1}.$$

which is the third term in (5.5). Hence, we have equality.

Let us now assume that $k \in I$. Note that for $\tau \in \text{Aut}(I)$ that $s_{\tau(I), J}^m = \varepsilon(\tau) s_{I, J}^m$, which follows immediately from the definition. Thus, we may assume without loss of generality that $k = i_1$.

Let $G \cong S_{m-1} \subseteq S_m$ be the subgroup fixing the first index of I . Let $G_p = G(1p)$

be the coset of elements taking the p th index to the first. Then action of the transposition $(i_1(n-1))$ on $s_{I,J}^m$ breaks up as:

$$\begin{aligned} & \sum_{\sigma \in G} \varepsilon(\sigma)(-x_{I_1})(s_{I,J}^m - \sum_{i=1}^m x_{\sigma(I)^1 \xrightarrow{i} I_1, J}) + \sum_{p=2}^m \sum_{\sigma \in G} -\varepsilon(\sigma)(x_{I_p} - x_{I_1})(-s_{\sigma(1p)(I)^1, J}^{m-1}) \\ = & -s_{I,J}^m + x_{I_1} \sum_{\sigma \in G} \varepsilon(\sigma) \sum_{i=1}^{m-1} s_{\sigma(I)^1 \xrightarrow{i} I_1, J}^{m-1} + x_{I_1} \sum_{p=2}^m \sum_{\sigma \in G} -\varepsilon(\sigma) s_{\sigma(1p)(I)^1, J}^{m-1}. \end{aligned}$$

So we need to show that the last two summands sum to 0. We note that given $\sigma \in G$ and $1 \leq i \leq m-1$ that $\sigma(I)^1 \xrightarrow{i} I_1 = \sigma(1(i+1))(I)^1$. This pairs up elements of the two double sums so that the two elements of the pair are the same except they have opposite sign. Hence, the total is 0.

Finally, suppose that $k \in J$. Here the calculations become so unwieldy (as witnessed in the $m=2$ case) that we change our method of proof.

Let $G_p \subseteq S_n$ be the stabilizer of $0 \leq p \leq n-1$, so $G_p \cong S_{n-1}$ and is generated by the transpositions $(01), (12), \dots, ((p-1)(p+1)), ((p+1)(p+2)), \dots, ((n-2)(n-1))$. Suppose for the moment that $m < n-3$. Let W_p be the span of the $s_{I,J}^m$ such that $p \notin I \cup J$. Since $m < n-3$, we have that $W_p \neq 0$. Moreover, we see by induction that W_p is an irreducible G_p representation, and in particular is the vector space of m -syzygies of $(n-1)$ points in $\mathbb{P}^{n-3}$.

Since $k \in J$ we have that $|\{k\} \cup I \cup J| < n-1$. Hence, there is some index $0 \leq p \leq n-1$ such that $p \notin I \cup J$ and $p \neq k$. Then $s_{I,J}^m \in W_p$, and by induction we know how $(k, n-1)$ acts on $s_{I,J}^m$, and it is exactly as in the statement of the lemma.

Finally, we must consider the case $m = n-3$.

$$\begin{aligned}
& \sum_{\sigma \in S_n} \varepsilon(\sigma) (x_{\sigma(I)_1} - x_{J_1}) (s_{\sigma(I)^1, J}^{m-1} - \sum_{i=1}^m s_{\sigma(I)^1 \dot{\leftrightarrow} k, I_i J_2}^{m-1}) \\
&= \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{\sigma(I)_1} s_{\sigma(I)^1, J}^{m-1} - \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{\sigma(I)_1} \sum_{i=1}^{m-1} s_{\sigma(I)^1 \dot{\leftrightarrow} k, I_i J_2}^{m-1} \\
&\quad + \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{J_1} \sum_{i=1}^{m-1} s_{\sigma(I)^1 \dot{\leftrightarrow} k, I_1 J_2}^{m-1} - \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{J_1} s_{\sigma(I)^1, J}^{m-1}.
\end{aligned}$$

The first summand on the right hand side is visibly $s_{I,J}^m$. The rest of the lemma is similar to the previous parts. □

But why are these objects even of interest? The answer is contained in

Lemma 153. *For all m, I, J , the $s_{I,J}^m \in E_m$, i.e., they are syzygies.*

Proof. First apply d_m to $s_{I,J}^m$ and get

$$\sum_{\sigma \in S_m} \varepsilon(\sigma) x_{\sigma(I)_1} \sum_{\tau \in S_{m-1}} \varepsilon(\tau) x_{\tau(\sigma(I)^1)_1} s_{\tau(\sigma(I)^1)^1, J}^{m-2}. \tag{5.6}$$

We would like to show that this is 0. We note that this sum may be rewritten as a sum

$$\sum_{i < j \in I} \chi_{ij} x_i x_j s_{I^{ij}, J}^{m-2}$$

where I^{ij} is $(m-2)$ -tuple with i and j removed and the χ_{ij} is some integer. We assume without loss of generality that $I = (1, 2, \dots, m)$ and that $i = 1$ and $j = 2$. We now compute χ_{ij} .

In the sum (5.6), there are two ways that an addend can contribute to χ_{12} : either $\sigma(I)_1 = 1$ and $\tau(\sigma(I)^1)_1 = 2$ or vice-versa. So we search for the terms which fix 1 and 2. Let $G \subseteq S_m$ be the subgroup fixing 1. For $\sigma \in G$, $H = H_\sigma \subseteq S_{m-1}$ be the subgroup fixing 2

in $\sigma(I)^1$ and let $\gamma_\sigma \in S_{m-1}$ be the transposition swapping 2 and $(\sigma(I)^1)_1$. Then for $\sigma \in G$, $\tau \in H$, we have $\gamma_\sigma \tau$ fixes 1 and 2 in I . Moreover, these yield *precisely* the terms in (5.6) which fix both 1 and 2. But each of these terms contributes

$$\varepsilon(\sigma)\varepsilon(\gamma_\sigma\tau)\varepsilon(\gamma_\sigma\tau\sigma) = 1$$

to the sum (5.6).

On the other hand, we seek the terms which *transpose* 1 and 2. These will be the exact same terms except they should first transpose 1 and 2. So each term contributes

$$\varepsilon(\sigma(12))\varepsilon(\gamma_\sigma\tau)\varepsilon(\gamma_\sigma\tau\sigma) = -1$$

to (5.6). Hence, $\chi_{12} = 0$. □

Let W be the span of the $s_{I,J}^m$, which we know is an S_n representation which consists of syzygies. We now ask *which* representation it is. What follows now are four lemmas on how the representation W of S_n breaks up into irreducible representations of $S_{n-1} \subseteq S_n$, where the particular S_{n-1} we choose is the stabilizer of p_0 , i.e., the subgroup generated by the transpositions $(12), (23), \dots, ((n-2)(n-1))$. These four lemmas combined with the branching law for S_n (Theorem 143) and dimension considerations (Theorem 138 and Lemma 142) will be sufficient to prove Theorem 134 when $m < n - 3$. When $m = n - 3$, Lemma 157 will finish the proof. Finally, we consider $m = n - 2$ in Lemma 158.

Lemma 154. *Suppose $2 \leq m < n - 3$. Let $S_{n-1} \subseteq S_n$ be the subgroup fixing p_0 , i.e., that which is generated by the transpositions $(12), (23), \dots, ((n-2)(n-1))$. Then W contains a copy W_1 of the representation $F_{m,n-1}$.*

Proof. Let $W_1 \subseteq W$ be the span of $s_{I,J}^m$ such that $0 \notin I \cup J$. (Note that since $|I \cup J| = m + 2$ we have already used the assumption $m < n - 3$.) Then from Lemma 152 we see that W_1 is

an S_{n-1} subrepresentation. Moreover, it is evident from Lemma 152 and induction that the action of S_{n-1} on W_1 is the same as the action on $E_{m,n-1} = F_{m,n-1}$. $\square$

Let $2 \leq m \leq n-3$ and let $S_{n-1} \subseteq S_n$ be the subgroup generated by the transpositions $(01), (12), \dots, ((n-3)(n-2))$. Then $V^\vee$ restricts to the permutation representation of $x_0, \dots, x_{n-2}$. In particular, it breaks up as a trivial representation spanned by $x_0 + x_1 + \dots + x_{n-2}$ and a standard representation $V_{n-1}^\vee$ spanned by the differences $x_i - x_j$ for all $0 \leq i, j \leq n-2$. Consider the S_{n-1} -equivariant projection

$$p : F_{m-1,n} \otimes V^\vee \rightarrow F_{m-1,n} \otimes V^\vee / V_{n-1}^\vee.$$

Then we denote the image of each $x_i \in V^\vee / V_{n-1}^\vee$ as x_0 .

Lemma 155. *The image $p(W)$ contains a copy W_2 of the S_{n-1} representation $F_{m-1,n-1}$ as an S_{n-1} representation.*

Proof. From the definition (5.6) of the $s_{I,J}^m$, we see that

$$p(s_{I,J}^m) = x_0 \sum_{k=1}^m (-1)^{m-1} s_{I^k,J}^{m-1}.$$

Since $|I \cup J| \leq n-1$, we can find all $s_{I,J}^{m-1}$ in the image. In particular, using Lemma 152 we get the claim. where I' is some ordering of the set $I - \{0\}$. Moreover, we know that $V^\vee / V_{n-1}^\vee$ is a trivial representation and is spanned by x_0 . Hence, after sending $x_0 \mapsto 1 \in k$, we are left with a surjective map which lands in $E_{m-1,n}$. Hence the lemma. $\square$

Lemma 156. *There is an irreducible S_n subrepresentation $W_3 \subseteq W$ containing both the representations described in the previous two lemmas.*

Proof. Consider $I = (1, 2, \dots, m)$ and $J = (n-3, n-2)$. Then $s_{I,J}^m \in W_1$, the irreducible S_{n-1} representation from Lemma 154. Let $I' = (0, 2, 3, \dots, m)$ and $J = (n-3, n-2)$.

Then $(01)s_{I,J}^m = s_{I',J}^m$. Since $p(s_{I',J}^m) \neq 0$, we have that W_2 and W_1 must belong to the same irreducible S_n subrepresentation of W . $\square$

Lemma 157. *Let $2 \leq m \leq n - 3$ and let $S_m \subseteq S_n$ be the subgroup generated by the transpositions $(01), (12), \dots, ((m-2)(m-1))$. Then W contains a copy of the alternating representation of S_m .*

Proof. Let $I = (0, 1, \dots, m-1)$ and let $J = (n-3, n-2)$. Then according to Lemma 152, $ks_{I,J}^m$ is an S_m representation, specifically, the alternating representation. $\square$

This is now sufficient to prove Theorem 134 for $m < n - 3$. For according to Lemma 156, we know that W_1 and W_2 from Lemmas 154 and 155 belong to the same irreducible S_n subrepresentation of W . However, it is not hard to see that the only Young diagram of which both $F_{m,n-1}$ and $F_{m-1,n-1}$ are *both* restrictions is $F_{m,n}$.

Finally, we come to the case $m = n - 3$. As noted above, Lemma 154 only makes sense for $m < n - 3$, so we no longer have W_1 . However, we still have W_2 . For $n = 5$ (resp. $n \geq 6$) there are only 2 (resp., 3) Young diagrams of which $F_{m-1,n-1}$ is a restriction, namely,

$$\begin{array}{ccc}
 n-3 & \left\{ \begin{array}{c} \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \square & & \\ \hline \vdots & & \\ \hline \square & & \end{array} \\ \end{array} \right. & n-3 & \left\{ \begin{array}{c} \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \square & \square \\ \hline \square & \square & \\ \hline \vdots & & \\ \hline \square & & \end{array} \\ \end{array} \right. & n-2 & \left\{ \begin{array}{c} \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \square & \\ \hline \vdots & \\ \hline \square & \end{array} \\ \end{array} \right.
 \end{array} \quad (5.7)$$

(The middle diagram only makes sense for $n \geq 6$.)

These representations have dimensions, respectively,

$$\alpha_n = \frac{n(n-2)(n-4)}{3} \quad \beta_n = \frac{n(n-1)(n-5)}{6} \quad b_{n-3} = \frac{n(n-3)}{2}.$$

But $\alpha_n > b_{n-3}$ when $n \geq 6$, and $\beta_n > b_{n-3}$ whenever $n \geq 7$. So we need only concern ourselves with the cases $n = 5, 6$.

Note that $\alpha_5 = b_{2,5} = 5$, so we already know that W is irreducible. Thus, in order to determine W , we need only distinguish between these two. One notable feature of the rightmost representation in (5.7) is that it contains a copy of the alternating representation of S_3 . Hence, Lemma 157 takes care of the case $n = 5$.

For the case $n = 6$, we note that the rightmost representation is again distinguished by containing an alternating representation of S_4 . Again, Lemma 157 saves the day.

Finally, to finish the proof of Theorem 134, we need the following lemma.

Lemma 158. *The representation E_{n-2} is the alternating representation.*

Proof. We already know that $\dim E_{n-2} = 1$ from Theorem 138 and Lemma 142, so it is only necessary to show that S_n does not act *trivially* on E_{n-2} . In fact, we will show that the trivial representation does not even appear in $F_{n-3} \otimes \text{Sym}^2 V^\vee$.

We know that $E_{n-2} \subseteq F_{n-3,n} \otimes \text{Sym}^2 V^\vee$. Moreover, we saw above that $\text{Sym}^2 V^\vee \cong k \oplus V \otimes F_{1,n}$ where k is the trivial representation. Now $F_{n-3,n} \otimes k \cong F_{n-3,n}$ certainly does not contain a trivial representation.

As we will see in our discussion of the Littlewood-Richardson rule in the next section, to show that the trivial representation does not appear in $F_{n-3} \otimes V$, it suffices to show that the restriction of the trivial representation to S_{n-1} does not appear in the restriction of F_{n-3} to S_{n-1} . However, this is obvious from the branching law.

Finally, to see that the trivial representation does not appear in $F_{n-3} \otimes F_1$, it suffices to show that the trivial representation does not appear in $\text{Res}_{S_{n-2} \times S_2}^{S_n} F_{n-3}$. But then it suffices to show that the trivial representation does not appear in $\text{Res}_{S_{n-2}}^{S_n} F_{n-3}$. This is again obvious for $n \geq 5$. $\square$

Thus, we have completed the proof of Theorem 134.

Remark 159. We used heavily the already known dimensions of the various syzygy modules in this proof, and we will again use this method of proof in Chapter 6. This begs the question

of whether or not there is a *direct* method of proof of the fact that the syzygy modules are irreducible representations.

5.3 An ACDGA structure for the Resolution of X

In fact, we can use equivariance of the resolution proved in Theorem 150 in order to put an ACDGA structure on that resolution. To begin with, we more closely examine the known examples of ACDGA resolutions of $n \geq 4$ points in $\mathbb{P}^{n-2}$, i.e., $n = 4, 5$.

In the case $n = 4$, the minimal free resolution of X is a Koszul resolution, since X is the complete intersection of 2 quadrics f, g :

$$R(-4) \begin{bmatrix} g \\ -f \end{bmatrix} \longrightarrow R(-2)^2 \begin{bmatrix} f & g \end{bmatrix} \longrightarrow R.$$

Viewing $R^{b_i} \cong \wedge^i R^2 \cong F_i \otimes R$ as R modules, there is a natural differential graded multiplication map, which is given by $x \cdot y = x \wedge y$ for $x \in \wedge^i R^2$ and $y \in \wedge^j R^2$.

There is in fact another way to think of this exterior product. Specifically, consider that as *representations* of S_n , $\wedge^i F_1 \cong F_i$. So we get an ACDGA multiplication $(\wedge^i F_1 \otimes R) \otimes (\wedge^j F_1 \otimes R) \rightarrow \wedge^{i+j} F_1 \otimes R$ which is S_n -equivariant.

Now consider the case $n = 5$. We recall the construction of Buchsbaum and Eisenbud [25]. Let $\mathbb{K}$ be the minimal free resolution of X constructed in Theorem 150. Then consider the symmetric square

$$\mathrm{Sym}^2(\mathbb{K}) = \mathbb{K} \otimes \mathbb{K} / M$$

where M is the graded submodule of $\mathbb{K} \otimes \mathbb{K}$ given by

$$\{f \otimes g - (-1)^{ij} g \otimes f : f \in \mathbb{K}_i, g \in \mathbb{K}_j\}.$$

Then

$$\mathrm{Sym}^2(\mathbb{K})_k \cong \left(\sum_{i+j=k, i < j} \mathbb{K}_i \otimes \mathbb{K}_j \right) + \begin{cases} 0 & k \equiv 1 \pmod{2}, \\ \wedge^2 \mathbb{K}_{k/2} & k \equiv 2 \pmod{4}, \text{ and} \\ \mathrm{Sym}^2(\mathbb{K}_{k/2}) & k \equiv 0 \pmod{4}. \end{cases}$$

The decomposition is also seen to be S_n equivariant. So in particular, $\mathrm{Sym}^2(\mathbb{K})$ consists of projective R modules and is isomorphic to $\mathbb{K}$ in degrees 0 and 1. Note further that M is closed under the action of S_n . Hence $\mathrm{Sym}^2(\mathbb{K})$ inherits an S_n -equivariant structure. We recall the following:

Theorem 160. *If $\mathbb{K}_\bullet$ and $\mathbb{L}_\bullet$ are two projective resolutions in an abelian category and there are maps*

$$\begin{array}{ccc} \mathbb{K}_1 & \longrightarrow & \mathbb{K}_0 \\ \downarrow & & \downarrow \\ \mathbb{L}_1 & \longrightarrow & \mathbb{L}_0 \end{array}$$

with the vertical maps isomorphisms then these maps may be extended to maps of complexes $\mathbb{K} \rightarrow \mathbb{L}$:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{K}_2 & \longrightarrow & \mathbb{K}_1 & \longrightarrow & \mathbb{K}_0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \cdots & \longrightarrow & \mathbb{L}_2 & \longrightarrow & \mathbb{L}_1 & \longrightarrow & \mathbb{L}_0. \end{array}$$

Buchsbaum and Eisenbud use this theorem to put an *a priori* commutative DGA structure on the resolution of codimension 3 arithmetically Gorenstein schemes. They then note that there is only one associativity relation that needs to be checked, specifically, that $(ab)c = a(bc)$ for $a, b, c \in \mathbb{K}_1$. But $(ab)c, a(bc) \in \mathbb{K}_3$. Since d_3 is injective, it suffices to show that $d_3((ab)c) = d_3(a(bc))$. After applying the DGA rules and the known cases, both turn out to be equal to

$$d_1(a) \cdot b \cdot c - a \cdot d_1(b) \cdot c + a \cdot b \cdot d_1(c).$$

This technique of proof of course fails for higher codimension, where the length of the resolution is strictly greater than 3. However, we know the resolution to be S_n equivariant, and the category of S_n equivariant R modules is *also* abelian. Moreover, we have seen in Chapter 1 that for any finite dimensional representation W of S_n that $W \otimes R$ is a projective equivariant R module. Hence, the same trick used by Buchsbaum and Eisenbud may be used to put a CDGA structure on $\mathbb{K}$ which respects the S_n structure.

Now to show that the multiplication is *associative*, it would suffice to show that the image of the multiplication maps and the kernels of the various d maps belong to disjoint isotypical components. In fact, since both multiplication and the d maps are R -linear, it suffices to show that no two elements of *ordinary* degree 0 multiply to an element of the kernel of the relevant d map. This is what we endeavor to show.

Remark 161. Recall from Section 1.3.7 of Chapter 1 that our complexes are equipped with two natural gradings: the *homological* degree and the *ordinary* degree. The first is the grading of the complex and runs from 0 to $n - 2$. The latter arises from the grading on R . Thus, an element of $F_1 \otimes \text{Sym}^5(V^\vee)$ has homological degree 1 and ordinary degree 5.

To this effect, we introduce some notation for this section. Suppose $a \in \mathbb{K}$ is homogeneous in the homological (resp., ordinary) degree. Then denote by $|a|$ (resp., $\delta(a)$) its homological (resp., ordinary) degree. We say a is homogeneous provided that it is homogeneous with respect to both the homological and ordinary degrees.

Lemma 162. *Suppose $a, b \in \mathbb{K}$ are homogeneous with $0 \leq |a|, |b| \leq n - 2$. Then with respect to any differential graded multiplication on $\mathbb{K}$ we have*

$$\delta(ab) = \delta(a) + \delta(b) + p_{|a|, |b|}$$

where

$$p_{|a|,|b|} = \begin{cases} 0 & |a| = 0, \\ 0 & |b| = 0, \\ 0 & |a| + |b| = n - 2, \text{ and} \\ 1 & \text{otherwise.} \end{cases}$$

Remark 163. If $|a| + |b| > n - 2$, then $\mathbb{K}_{|a|+|b|} = 0$, so we ignore these cases.

Proof. The case $|a| = 0$ is obvious. Also, we note that $\delta(ab) = \delta(ba)$ by the commutativity of our DGA. Also, note that for all i, j , we have that $p_{ij} = p_{ji}$. Hence, we may assume without loss of generality that $1 \leq |a| \leq |b| \leq n - 2 - |a|$. All other calculations are based on the following equality:

$$\begin{aligned} \delta(ab) &= \delta(d(ab)) - \delta(d_{|a|+|b|}) \\ &= \delta[d(a) \cdot b \pm a \cdot d(b)] - \delta(d_{|a|+|b|}) \\ &= \max\{\delta(d(a) \cdot b), \delta(a \cdot d(b))\} - \delta(d_{|a|+|b|}) \\ &= \max\{\delta(d(a)) + \delta(b) + p_{|a|+1,|b|}, \delta(a) + \delta(d(b)) + p_{|a|,|b|+1}\} - \delta(d_{|a|+|b|}) \\ &= \delta(a) + \delta(b) - \delta(d_{|a|+|b|}) + \max\{\delta(d_{|a|} + p_{|a|+1,|b|}), \delta(d_{|b|} + p_{|a|,|b|+1})\}, \end{aligned}$$

where $\delta(d_i) = \delta(d_i(a)) - \delta(a)$ for any $a \in \mathbb{K}_i$. So we see that

$$p_{|a|,|b|} = \max\{\delta(d_{|a|} + p_{|a|+1,|b|}), \delta(d_{|b|} + p_{|a|,|b|+1})\} - \delta(d_{|a|+|b|}).$$

We consider separately the case $|a| = |b| = 1$. If $n = 4$, then the above expression is obviously 0. If $n \geq 5$, then we fill in the expression above as

$$\max\{2 + 0, 2 + 0\} - 1 = 1.$$

If $|a| = 1 < |b| < n - 2$, then (using the previous computation) it is filled in as

$$\max \{2 + 0, 1 + 1\} - 1 = 1.$$

Finally, if $|a| = 1$ and $|b| = (n - 2) - 1$, then it becomes

$$\max \{2 + 0, 1 + 1\} - 2 = 0.$$

The calculations for $|a| > 1$ are similar. □

Combining Lemma 162 with Theorem 150 shows that we only need to check that F_{i+j+1} does not appear in $F_i \otimes F_j$ with $1 \leq i \leq j \leq (n - 2 - i) - 2$. Note that if $j = n - 2 - i$ then there is nothing to check since d_{n-2} is injective. If $j = (n - 2 - i) - 1$, then there is also nothing to check since d_{n-2+1} is injective in ordinary degree 1, where Lemma 162 tells us the image of $F_i \otimes F_{(n-2-i)-1}$ must lie.

Thankfully, checking whether a given irreducible representation of S_n appears in a tensor product of irreducible representations is well-studied. We use the techniques outlined in [54, §4.3].

We want to show that the multiplicity of F_{i+j+1} is 0 in $F_i \otimes F_j$. Let G_m be the subgroup of S_n which preserves the rows of the standard tableau on F_m . Then F_m is in $U_m = \text{Ind}_{S_m}^{S_n} k$, the induction of the trivial representation on S_m , by [54, Exercise 4.39]. So it suffices to show that F_{i+j+1} does not appear in

$$F_j \otimes \text{Ind}_{G_i}^{S_n} \text{Res}_{G_i}^{S_n} k \cong \text{Ind}_{G_i}^{S_n} \text{Res}_{G_i}^{S_n} F_j.$$

Then Frobenius reciprocity says that it is enough to check that none of the irreducible representations in $\text{Res}_{G_i}^{S_n} F_{i+j+1}$ appears in $\text{Res}_{G_i}^{S_n} F_j$.

As a first step, we consider the case of $i = 1$, so $G_1 = S_{n-2} \times S_2$. Then the Littlewood-

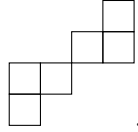
Richardson Rule [54, pg. 58] states that

$$\text{Res}_{G_1}^{S_n} F_j = \sum N_{\lambda\nu j} V_\lambda \boxtimes V_\nu$$

where the sum runs over all partitions λ of $n - 2$ and ν of 2 and the symbol $\boxtimes$ means the “external” tensor product. The numbers $N_{\lambda\nu j}$ can be computed as the number of Littlewood-Richardson tableau of shape F_j/λ of weight ν .

Definition 164. Let $m \leq n$ and let λ (resp. η) be a partition of m (resp. n). Suppose further that $\eta_i \leq \lambda_i$ for all i . Then the *skew Young diagram of shape η/λ* is the Young diagram of η with the Young diagram of λ removed.

Example 165. Let $\lambda = \{3, 2\}$ and $\eta = \{4, 4, 2, 1\}$. Then η/λ is the diagram



Definition 166. Let λ, ν, η be partitions of $d, m, d + m$, respectively. Then a *Littlewood-Richardson tableau of shape η/λ and weight ν* is a skew Young tableau for the diagram η/λ containing ν_i copies of the number i which is column strict and row standard, i.e., has strictly increasing column entries and weakly increasing row entries, and which has the additional property that if we write the entries of the tableau from right-to-left then top-to-bottom, then for all $1 \leq j \leq |\nu|$, every initial segment of the resulting word has at least as many j 's as it does $(j + 1)$'s.

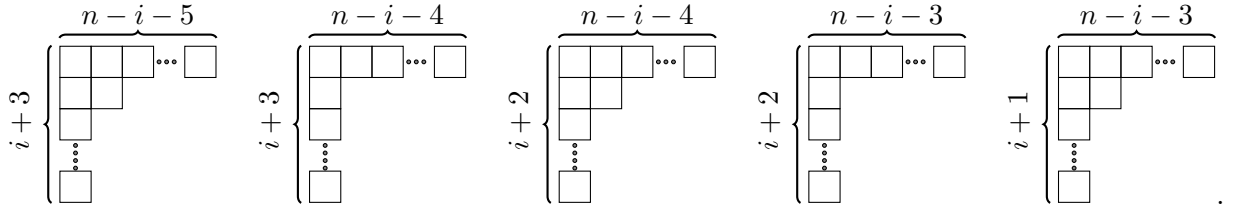
Another way to picture this definition is as follows: Given a Young diagram λ , first add ν_1 boxes containing 1s, no more than one per column; then add ν_2 boxes containing 2s, no more than one per column; continue and make sure the extra condition of Definition 166 is satisfied. When we want to refer to this picture, we will say this is a *strict ν extension of*

λ of shape η .

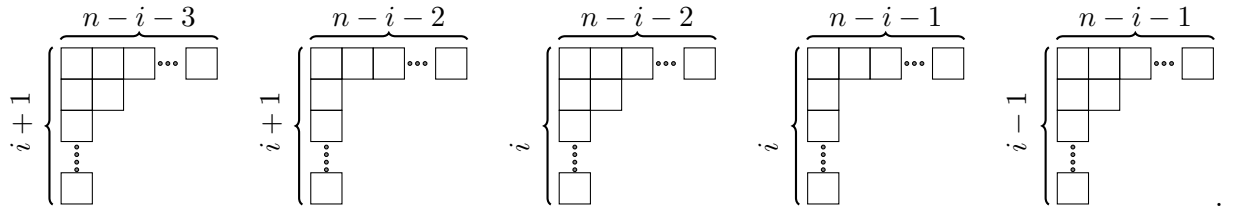
Now we consider our particular case, where $|\nu| = 2$, so the only possibilities for ν are:



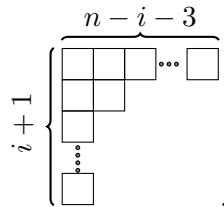
Moreover, the only diagrams λ to which we can add two boxes to obtain F_{i+2} are



Similarly, the only diagrams to which we can add two boxes to obtain F_i are



There is precisely one diagram in common:



But we cannot extend this diagram by $\nu = \square\square$ in order to obtain F_{i+2} . Similarly, we cannot extend this diagram by $\nu = \square$ in order to obtain F_i . Hence, whenever $N_{\lambda\nu, i+2} \neq 0$, we have that $N_{\lambda\nu, i} = 0$. Thus, our theorem is verified in the case $j = 1$.

For $j > 1$, we see that the group $G_j = S_{n-j-1} \times S_2 \times S_1 \times \cdots \times S_1$ where $j - 1$ copies of S_1 appear. But the functor

$$\text{Res}_{G_j}^{S_n} = \text{Res}_{S_{n-j+1} \times S_2 \times S_1 \times \cdots \times S_1}^{S_{n-j+3} \times S_1 \times \cdots \times S_1} \circ \text{Res}_{S_{n-j+3} \times S_1 \times \cdots \times S_1}^{S_{n-j+4} \times S_1 \times \cdots \times S_1} \circ \cdots \circ \text{Res}_{S_{n-1} \times S_1}^{S_n}.$$

At the very last step, we are confronted directly with the Littlewood-Richardson Rule. As we saw in the case $j = 1$, the only way one of the irreducible representations of $\text{Res}_{S_{n-j-1} \times S_2}^{S_{n-j+1}} V_\lambda$ could possibly show up in $\text{Res}_{S_{n-j-1} \times S_2}^{S_{n-j+1}} V_\mu$ is if we could get from the Young diagram λ to the Young diagram μ by subtracting two boxes from λ to obtain another Young diagram and then put them back in a different place to get μ .

In our case, the irreducible representations showing up in $\text{Res}_{S_{n-j+1}}^{S_n} V_\lambda$ are those corresponding to diagrams μ which are λ with any $j - 1$ boxes removed. Now the first column of F_i has height $i + 1$ and the first column of F_{i+j+1} has height $i + j + 2$, so the only irreducible representation appearing in $\text{Res}_{S_{n-j+1}}^{S_n} F_{i+j+1}$ which might possibly intersect $\text{Res}_{S_{n-j+1}}^{S_n} F_i$ is

$$(i+1)+2 \left\{ \begin{array}{c} \overbrace{\begin{array}{cccc} \square & \square & \square & \cdots & \square \end{array}}^{n-(i+j+1)-1} \\ \square \\ \square \\ \vdots \\ \square \end{array} \right.$$

which corresponds to removing all $j - 1$ boxes from the first column of F_{i+j+1} . The corresponding diagram for F_i is attained by removing $j - 1$ boxes from the first row to get

$$i+1 \left\{ \begin{array}{c} \overbrace{\begin{array}{cccc} \square & \square & \square & \cdots & \square \end{array}}^{n-(i+j+1)-j} \\ \square \\ \square \\ \vdots \\ \square \end{array} \right. .$$

But this is just the $j = 1$ case for S_{n-j+1} , and we have already shown that these two representations do not intersect. Hence, our theorem is proved!

In fact, the same proof as above proves the following lemma, which will be important to us in the next chapter.

Lemma 167. *Suppose that $\lambda = \{\lambda_1, \lambda_2, \dots, \lambda_\ell\}$ and $\mu = \{\mu_1, \mu_2, \dots, \mu_m\}$ be partitions of n with ℓ and m rows respectively. Further, suppose that $\lambda_i = \mu_j = 1$ for all $i, j \geq 3$. Then for all irreducible representations ν in $\lambda \otimes \mu$, ν has at most $\ell + m - 1$ rows.*

5.4 A Remark on Canonicity and Smaller Fields

An important point is that after an S_n -equivariant resolution $\mathbb{K}$ of X is chosen, we note that there is a *unique* ACDGA structure on $\mathbb{K}$ which respects the S_n action. We begin with a lemma.

Lemma 168. *The representation E_i appears with multiplicity one in $F_{i-1} \otimes V$ when $1 < i < n - 2$.*

Proof. First, we see that the multiplicity of E_i is *at most* one. For if you restrict to S_{n-1} then the branching law says that you are taking the tensor product

$$\left(\begin{matrix} i-1 \\ \left\{ \begin{matrix} \overbrace{\square \square \square \dots \square}^{n-i} \\ \square \square \square \dots \square \\ \square \square \square \dots \square \\ \vdots \\ \square \end{matrix} \right\} \oplus \cdot \left\{ \begin{matrix} \overbrace{\square \square \square \dots \square}^{n-i} \\ \square \square \square \dots \square \\ \square \square \square \dots \square \\ \vdots \\ \square \end{matrix} \right\} \oplus \cdot \left\{ \begin{matrix} \overbrace{\square \square \square \dots \square}^{n-i-1} \\ \square \square \square \dots \square \\ \square \square \square \dots \square \\ \vdots \\ \square \end{matrix} \right\} \end{matrix} \right) \otimes \left(\begin{matrix} \overbrace{\square \square \square \dots \square}^{n-1} \oplus \cdot \overbrace{\square \square \square \dots \square}^{n-2} \end{matrix} \right).$$

A similar argument to the previous section demonstrates the 6 terms in the expansion of

this tensor product, only one of

$$\begin{array}{c} \sim \end{array} \left\{ \begin{array}{c} \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-i-1} \dots \square \\ \square \\ \vdots \\ \square \end{array} \right\} \otimes \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-2} \dots \square \quad \text{or} \quad \begin{array}{c} \sim \end{array} \left\{ \begin{array}{c} \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-i} \dots \square \\ \square \\ \vdots \\ \square \end{array} \right\} \otimes \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-2} \dots \square \quad (5.8)$$

could possibly contain a representation whose first column has height $i + 1$. By induction (the base case can be $n = 6$ and checked using Magma's character manipulation features [23]), the first of these has exactly *one* copy of $E_{i,n-1}$, which is a restriction of $E_{i,n}$, and so we see that $F_{i-1} \otimes V$ has at most one copy of E_i arising from the left hand side of (5.8)

So for the upper bound we are reduced to showing that the second of the representations in (5.8) does not contain $E_{i,n-1}$. Suppose first that $i < n - 3$. Then to show that $E_{i,n-1}$ does not appear in the the right hand side of (5.8) it suffices to show that $E_{i,n-2}$ does not appear when we restrict the right hand side to S_{n-2} . But $\{n - 2, 1\}$ breaks up into a trivial representation and a standard representation $\{n - 3, 1\}$ when restricted to S_{n-2} . So it suffices to show that $E_{i,n-2}$ does not appear in

$$\begin{array}{c} \sim \end{array} \left\{ \begin{array}{c} \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-i-1} \dots \square \\ \square \\ \vdots \\ \square \end{array} \right\} \otimes \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-3} \dots \square \quad \text{or} \quad \begin{array}{c} \sim \end{array} \left\{ \begin{array}{c} \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-i} \dots \square \\ \square \\ \vdots \\ \square \end{array} \right\} \otimes \overbrace{\begin{array}{ccc} \square & \square & \square \end{array}}^{n-3} \dots \square .$$

Induction rules out the left hand tensor product. To rule out the right hand tensor product simply note that the computations of the previous section imply that any representation appearing in the right hand tensor product must have first column with height $\leq i$, which is less than the requisite $i + 1$.

On the other hand, we know that $E_i \cong F_i \subseteq F_{i-1} \otimes V$. Hence, the lemma is proven

when $i < n - 3$.

Finally, we are in the case $i = n - 3$. Then we need to show that

$$\left\{ \begin{array}{c} \square \square \square \\ \square \square \square \\ \square \square \square \\ \vdots \\ \square \end{array} \right\}^{n-2} \cup \left\{ \begin{array}{c} \square \square \square \square \\ \square \square \square \square \\ \square \square \square \square \\ \vdots \\ \square \end{array} \right\}^{n-3} \otimes \overbrace{\begin{array}{c} \square \square \square \square \dots \square \\ \square \square \square \square \end{array}}^{n-1}$$

appears with multiplicity at most 1, or what is the same, that the representation $\{n - 2, 2\}$ appears with multiplicity at most 1 in $\{n - 3, 2, 1\} \otimes \{n - 1, 1\}$. These diagrams, however, are simple enough that the Littlewood-Richardson Rule may be easily applied. And so the lemma is proved. $\square$

Now F_0 is the trivial representation, so there is a canonical isomorphism $F_0 \otimes F_i \rightarrow F_i$. Now the previous lemma allows us a unique splitting of the d map $F_{i+j+1} \hookrightarrow F_{i+j} \otimes V^\vee$ and so there is a unique equivariant lift of $d(a) \cdot b \pm a \cdot d(b) \in F_{i+j-1}$ to the complement of $F_{i+j+1} \subseteq F_{i+j}$ defined by this splitting. By induction, then, this says that *if* an S_n -equivariant multiplicative structure exists, then it is *unique*. As such, we immediately obtain the following theorem.

Theorem 169. *The $\text{Aut}(X)$ -equivariant DGA minimal free resolution of X is unique up to unique isomorphism. Moreover, it is necessarily associative and commutative.*

Proof. We have seen that X has a minimal free resolution which admits an $\text{Aut}(\bar{X}) \cong S_n$ equivariant structure. Then Schur's lemma and Lemma 168 implies that this resolution is unique up to a homothety in every homological degree. But then the commutativity of the diagram defining an isomorphism of complexes would inductively imply that the homothety in each degree is determined by the homothety in degree 0. But here the identity (which we know exists and is identified uniquely by the DGA structure) must go to the identity. The remark right before this theorem finishes the proof. $\square$

Finally, this allows us to push our work to smaller fields. For suppose that k is *not* algebraically closed and $X \subseteq \mathbb{P}_k^{n-2}$ is some dimension 0 reduced subscheme of degree n which is *geometrically* a set $\bar{X}$ of n points in linearly general position. *A priori*, the minimal free resolution X exists over k , but the action of S_n may not be defined over this smaller field. But we do not need the *action* of S_n to be defined over the smaller fields, only the canonical equivariant *splittings* that the action yields.

But there is a continuous homomorphism $G_k = \text{Gal}(\bar{k}/k) \rightarrow \text{Aut}(\bar{X} \subseteq \mathbb{P}_{\bar{k}}^{n-2})$. But as discussed above, any automorphism of $\bar{X}$ determines a unique automorphism of $\mathbb{P}_{\bar{k}}^{n-2}$. So as before, we may lift the action of G_k on $\mathbb{P}_{\bar{k}}^{n-2}$ to $\text{GL}_{n-1} \bar{k}$, and the image lives in the same S_n we have been discussing. That is, G_k acts via the S_n representations we've been discussing.

Now recall the proof that every subrepresentation of a finite group over a field of characteristic 0 has a canonical, equivariant splitting: One averages a nondegenerate bilinear form over the group to obtain a G -invariant bilinear form, and the perp space of the subspace yields a canonical complement. But for us, since $G_k \rightarrow S_n$, we see that the bilinear form is also Galois-equivariant, and hence the splittings we've been discussing are *also* defined over k . And so we have the following theorem.

Theorem 170. *Let k be a field of characteristic 0 and let $X \subseteq \mathbb{P}_k^{n-2}$ be a reduced, dimension 0 subscheme which is geometrically a set of n linearly general points. Then there is a unique up to unique isomorphism ACDGA free resolution of X which is geometrically equivariant under the action of $\text{Aut}(\bar{X})$.*

5.5 A Remark on Integrality

Now we would like to go a little bit further than Theorem 170 and address the question of integrality. In particular, we would like to know when the multiplicative structure on the minimal free resolution appearing in Theorem 170 is actually defined over $\mathbb{Z}$.

To begin, recall the following theorem of Casnati and Ekedahl⁴. Recall that to a map of schemes $\rho : X \rightarrow Y$, we have the structure map $\rho^\sharp : \mathcal{O}_Y \rightarrow \rho_*\mathcal{O}_X$. If ρ is a Gorenstein cover of degree d , then $\check{\mathcal{E}} = \text{coker } \rho^\sharp$ is a locally free $\mathcal{O}_Y$ sheaf of rank $d - 1$ called the *Tschirnhausen module* of ρ .

Theorem 171 ([30, Theorem 2.1],[31]). *Let X and Y be schemes with Y integral and suppose that $\rho : X \rightarrow Y$ is a Gorenstein cover of degree $d \geq 3$. Then there exists a unique $\mathbb{P}^{d-2}$ bundle $\pi : \mathbb{P} \rightarrow Y$ and an embedding $i : X \hookrightarrow \mathbb{P}$ with $\rho = \pi \circ i$. Moreover, the fibers $X_y \subseteq \mathbb{P}_y^{d-2}$ are all arithmetically Gorenstein subschemes for each $y \in Y$. Additionally,*

1. $\mathbb{P} \cong \mathbb{P}(\mathcal{E})$ with $\check{\mathcal{E}}$ the Tschirnhausen module of ρ ,
2. the composition $\varphi : \rho^*\mathcal{E} \rightarrow \rho^*\rho_*\omega_{X|Y} \rightarrow \omega_{X|Y}$ is surjective and the ramification divisor satisfies $\mathcal{O}_X(R) \cong \omega_{X|Y} \cong \mathcal{O}_X(1) = i^*\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$,
3. There is an exact sequence $\mathcal{N}_*$ of locally free $\mathcal{O}_{\mathbb{P}}$ sheaves

$$0 \rightarrow \mathcal{N}_{d-2}(-d) \xrightarrow{\alpha_{d-2}} \mathcal{N}_{d-3}(-d+2) \xrightarrow{\alpha_{d-3}} \cdots \xrightarrow{\alpha_3} \mathcal{N}_1(-2) \xrightarrow{\alpha_1} \mathcal{O}_{\mathbb{P}} \rightarrow \mathcal{O}_X \rightarrow 0$$

unique up to unique isomorphism and whose restriction to the fiber $\mathbb{P}_y$ over $y \in Y$ is a minimal free resolution of the structure sheaf of X_y (in particular $\mathcal{N}_i$ is fiberwise trivial),

4. the rank of $\mathcal{N}_i$ is given by b_i as in (5.1),
5. $\pi^*\pi_*\mathcal{N}_* \cong \mathcal{N}_*$ and $\mathcal{H}om_{\mathcal{O}_{\mathbb{P}}}(\mathcal{N}_*, \mathcal{N}_{d-2}(-d)) \cong \mathcal{N}_*$, and
6. If $\mathbb{P} \cong \mathbb{P}(\mathcal{E}')$ then $\mathcal{E}' \cong \mathcal{E}$ if and only if $\mathcal{N}_{d-2} \cong \pi^*\det \mathcal{E}'$ in the above resolution computed with respect to the polarization $\mathcal{O}_{\mathbb{P}(\mathcal{E}')} (1)$.

⁴The statement of the theorem we give appears in [30], however the proof appears in [31]. The statement of the theorem in [31], as noted in [30, Remark 2.2], is not correct as written.

Since Y is integral, any affine open subset $\text{Spec } Z$ must contain the generic point and hence the generic fiber. According to our uniqueness Theorem 169, there is a unique isomorphism between any two ACDGA structures on minimal free resolutions at the generic point which respect an S_n -equivariant structure. As such, as long as the isomorphism between the minimal free resolutions and the multiplicative structure itself is defined over the base ring Z , then we will be able to glue any two ACDGA structures together in a canonical way. But the isomorphism of minimal free resolutions we constructed above is guaranteed to be defined over Z by the uniqueness in part (3) of the above theorem.

Finally, we need to show that the multiplicative structure is defined over Z , an integral domain with field of fractions $Q = \text{Frac}(Z)$. As such, let R be some Gorenstein ring of rank n over Z . In addition to the condition that R be a Gorenstein ring, we also restrict ourselves to the case when X is *generically étale*, i.e., $R \otimes Q$ is an étale algebra over Q . Then Theorem 170 yields a multiplicative structure on the free resolution $\pi_*(\mathcal{N} \otimes Q)$, and hence by part (5) of the above theorem, on $\pi^*(\pi_*(\mathcal{N} \otimes Q)) = \mathcal{N} \otimes Q$. But note that according to the proof of Theorem 169, this only relied on the various splittings defined there to be defined over Q .

Now over $\bar{Q}$, the algebraic closure of Q , every set of n points in linear general position in $\mathbb{P}_{\bar{Q}}^{n-2}$ are conjugate to each other under the action of $\text{PGL}_{n-1}(\bar{Q})$. Moreover, from the uniqueness of the minimal free resolution, we know that any minimal free resolution of any n points in $\mathbb{P}_{\bar{Q}}^{n-2}$ must be conjugate to the minimal free resolution described in the preceding sections.

Moreover, note that any conjugate of a minimal free resolution will take the above splittings we described above to splittings of the conjugate resolution. After choosing bases, the matrix of a splitting is a pseudoinverse of the projection map. As such, examining the formula for the pseudoinverse, we see that if *any one of* the conjugates and their splittings were defined over Z , then all conjugates which were defined over Z would also have their splittings defined over Z . In the next chapter, we will work with Specht modules and in doing

so we will construct one such resolution and its splittings over $\mathbb{Z}$, and so by base change over Z .

On the other hand, the existence of the resolution defined over Z is taken care of by Theorem 171. Since all minimal free resolutions are conjugate, we have proved Theorem 136.

Chapter 6

Free Resolutions and Multiplicative Structures Thereon Attached to Two-Rowed Specht Ideals

6.1 Introduction

In Chapter 5, we built a multiplicative structure on the minimal free resolution of n general points in $\mathbb{P}^{n-2}$. One of the critical elements of the proof was that the resolution was *pure*, i.e. had Betti numbers b_{ij} such that for every i there was at most one j such that $b_{ij} \neq 0$. Or said more colloquially, if we wrote each d map as a matrix, its entries would be forms of a single degree. There has been a recent resurgence in interest in such resolutions as they form the basis of *Boij-Söderberg Theory* [22, 49, 48]. Usually pure resolutions are constructed from the representation theory of the general linear group, but in Chapter 5 we constructed pure resolutions from the representation theory of the symmetric group. In this note we continue this theme.

Recall that for every irreducible representation V of S_n over an algebraically closed

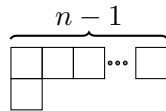
field of characteristic 0, there is an N such that V may be realized as a subrepresentation of $\text{Sym}^N \mathcal{P}$. Here $\mathcal{P}$ is the permutation representation. Taking the ideal of $\text{Sym}^\bullet \mathcal{P}$ generated by this subrepresentation, we obtain what we call a *Specht ideal*. In fact, Specht showed that these representations, and hence these modules, could be realized over $\mathbb{Z}$. Let $R = \mathbb{Z}[x_1, \dots, x_n] = \text{Sym}^\bullet \mathcal{P}$ over $\mathbb{Z}$ and for any field k , let $R_k = R \otimes_{\mathbb{Z}} k$. These concepts will be reviewed in Section 6.2, but first let us state our theorem:

Theorem 172. *The free resolutions of two-rowed Specht ideals over $\mathbb{Z}$ are pure and have a canonical S_n -equivariant structure so that for any field k the nontrivial $\text{Tor}_i^R(R/I, \mathbb{Z})_j$ are isomorphic to Specht modules for all i and j .*

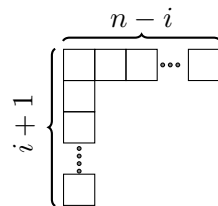
To elucidate this theorem, let us consider some more well-known examples. Consider the sequence of elements $x_1 - x_2, x_1 - x_3, \dots, x_1 - x_n \in R$. This is a regular sequence and so the ideal I generated by them has the Koszul complex as a minimal free resolution:

$$\wedge^{n-1} V \otimes R(-(n-1)) \rightarrow \wedge^{n-2} V \otimes R(-(n-2)) \rightarrow \cdots \rightarrow V \otimes R(-1) \rightarrow R \rightarrow R/I.$$

Here V is the subspace of the degree one part R_1 of R generated by $x_i - x_j$ for all i, j and $I = RV$. But note if we regard $R_1 = \mathcal{P}$ as the permutation representation of the symmetric group, then $V \subseteq R_1$ is the Specht representation associated to the *standard representation*



of S_n . Then $\wedge^i V$ is the representation



of S_n . Moreover, note that this resolution has a canonical multiplicative structure on it coming from the exterior algebra structure of $\wedge^\bullet V$.

Next consider the case of Chapter 5. Here we notice that n generic points in $\mathbb{P}^{n-2}$ are cut out by the ideal I generated by V spanned by quadrics $(x_i - x_j)(x_k - x_\ell)$. Moreover, the resolution has Betti numbers given by the Betti table

	0	1	2	$\cdots$	$n-3$	$n-2$
0	1					
1		β_{12}^n	β_{23}^n	$\cdots$	$\beta_{n-3,n-2}^n$	
2						1

where β_{ij}^n may be defined recursively as

$$\beta_{ij}^n = \beta_{i-1,j-1}^{n-1} + \beta_{ij}^{n-1} + \binom{n-1}{i+1}$$

with $\beta_{12}^2 = 2$. Using the branching law for irreducible representations of S_n , we showed in the previous chapter that these were the dimensions of the representations

$$1 + \left\{ \begin{array}{c} \overbrace{\begin{array}{|c|c|c|c|} \hline \square & \square & \square & \cdots & \square \\ \hline \square & \square & \square & & \\ \hline \square & \square & & & \\ \hline \vdots & & & & \\ \hline \square & & & & \end{array}}^{n-i-1} \end{array} \right.$$

of S_n . Using this fact we put an S_n -equivariant structure on this resolution and from this deduced a canonical multiplicative structure.

The common feature of these two representations that we will be using is that the

partitions have *two rows*. Stated informally, this means that their Young diagrams



have two rows. Stated formally, a partition $\lambda = \{\lambda_1, \lambda_2, \dots\}$ has r rows if $\lambda_i = 0$ for all $i > r$. Our main theorem shows that this is not an isolated fact. In particular, we will show that the Betti table of R/I where I is associated to the partition $\lambda = \{n - c, c\}$ is

	0	1	2	...	$n - 2c + 1$	$n - 2c + 2$	$n - 2c + 3$	...	$n - c$
0	1								
1									
$\vdots$									
$c - 2$									
$c - 1$		$\{n - c, c\}$	$\{n - c - 1, c, 1\}$	...	$\{c, c, 1, 1, \dots, 1\}$				
c						$\{c - 1, c - 1, 1, 1, \dots, 1\}$	$\{c - 1, c - 2, 1, 1, \dots, 1\}$	...	$\{c - 1, 1, 1, \dots, 1\}$

(6.1)

In words, one moves a box from the right-hand side of the top row to the bottom of the first column until doing so would make the first row shorter than the second. This ends this strand of the resolution. The next strand (the strand for the regularity of R/I) then begins by moving the last column of the partition to the first column. Then boxes are removed from the second row one at a time until no more can be removed.

In the spirit of Chapter 5, we prove the following Corollary in Section 6.5.

Corollary 173. *The free resolution of Theorem 172 admits a canonical S_n -equivariant associative, commutative, differential graded algebra structure.*

In Section 6.4, we actually write down the maps in the resolution. These maps turn out to be defined *over* $\mathbb{Z}$. Then to show that the purported maps actually yield an exact sequence over $\mathbb{Z}$, we may show injectivity over $\mathbb{C}$ (since everything in sight is free). We show surjectivity through explicit manipulations¹.

In [68], Hoa computed the Betti numbers for the Specht ideal associated to $\lambda =$

¹Perhaps there is some simpler high brow method involving the dual picture, but we have not found it.

$\{n-2, 2\}$. One could use a similar approach combining it with the techniques of Green and Lazarsfeld in [63], and indeed this was our original proof. However, it turns out that these ideals are what Kumar, Singh and Kumar [74] call *nearly extremal* ideals for which, using the ideas of [98], they have already computed the Betti numbers. The bulk of this chapter is concerned with proving that these ideals are indeed nearly extremal. We then prove *a posteriori* with the Littlewood–Richardson Rule and a dimension count that the various Tor modules are indeed *irreducible* S_n representations. One could deduce Theorem 172 from this irreducibility, but a direct proof escapes us.

Before beginning our proof, we note that this fact does not generalize to Specht ideals with more than two rows. In fact, already for $n = 4$, the Specht ideal associated to the partition $\{2, 1, 1\}$ does *not* have a pure resolution. In particular, Macaulay2 [61] immediately tells us that the resolution has Betti numbers

	0	1	2
0	1		
1			
2		3	1
3			1

On the other hand, this is not a property which characterizes two-rowed Specht representations. In particular, Macaulay2 immediately tells us that the resolution of the representation $\{2, 2, 1\}$ of S_5 has Betti numbers

	0	1	2
0	1		
1			
2			
3		5	4

So we are left wondering, What exactly about *two-rowed* representations is so special? In forthcoming work, we hope to give some hint by exhibiting a connection with (certain homogeneous spaces of) the group $\mathrm{Sp}_{2n}(\mathbb{C})$ of symplectic automorphisms of a $2n$ -dimensional vector space.

The rest of this chapter is outlined as follows. In Section 6.2, we set the notation for the rest of the chapter, taking the opportunity to review the construction and properties of Specht representations. In Section 6.3 we prove that these ideals are Cohen-Macaulay. This fact will allow us to take linear sections of our resolutions in order to compute their Betti numbers. In particular, we compute the regularity c of these ideals and show that $\beta_{ij} = 0$ whenever $i > 0$ and $j - i < c$ or $j - i > c + 1$. In Section 6.4, we use the theory of [74] in order to show that these resolutions are pure. In Section 6.4.1, we will demonstrate that the various Tor modules are either irreducible representations of S_n or trivial and will write down *which* irreducible representations they are. Finally, in Section 6.5, we follow the technique of Chapter 5 to put a canonical associative, commutative, differential graded algebra structure on these resolutions.

6.2 Notation

This section is divided into two parts. The first recalls the representation theory of the symmetric group, in particular we recall the construction of the Specht representations of S_n . The second part recalls some basic notions of commutative algebra, notably the (*Castelnuovo-Mumford*) *regularity* of an R -module.

6.2.1 The Representation Theory of the Symmetric Group

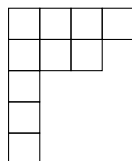
Throughout let k be a field, $n \geq 2$ and S_n the symmetric group on n letters. It is well known that when k is algebraically closed and of characteristic 0 (or at least characteristic $p \gg n$),

the irreducible representations of S_n are in canonical one-to-one correspondence with the partitions of n , i.e., the sequences of numbers $\lambda = \{\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0\}$ such that $\sum \lambda_i = n$ [54, Lecture 4].

We will often denote partitions by their *Young diagrams*. These will be drawings which will consist of left-justified rows of boxes. We will number the rows top-to-bottom, i.e., we take the British convention. So in particular, the partition $5 = 3 + 2$ corresponds to the diagram



and the partition $10 = 4 + 3 + 1 + 1 + 1$ corresponds to the diagram



Usually, the irreducible representations of S_n are constructed as the *image* of a map $c_\lambda : k[G] \rightarrow k[G]$ where $k[G]$ is the *group ring* associated to G , which, as a G -module, is the *regular representation* of G . The map c_λ is called the *Young symmetrizer* of shape λ [54, pg. 46]. However, this method has the disadvantage of only working in certain characteristics (in particular, it does not work for every λ when $\text{char}(k) \leq n$).

In order to overcome this deficiency, Specht found a different way to construct these irreducible representations which, in fact, works over $\mathbb{Z}$ [102]. These have become known as the *Specht representations*, or sometimes, the *Specht realizations*. Here we recall their construction, which appears as [54, Problem 4.47].

Suppose we have a partition λ represented as a Young diagram. Then a labeling of boxes of λ with the numbers $\{1, \dots, n\}$ we will call a (*Young*) *tableau* T of shape λ . We denote the label in row i and column j of T by T_{ij} . We say a Young tableau is *standard* if the labels are increasing along both the rows and columns of T . Formally stated, this means

$T_{ij} \leq T_{IJ}$ for all $i \leq I, j \leq J, i \leq \lambda_i, J \leq \lambda_j$. For example,

$$\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & \\ \hline 6 & & \\ \hline \end{array} \quad (6.2)$$

is a standard tableau of shape $6 = 3 + 2 + 1$ whereas

$$\begin{array}{|c|c|c|} \hline 5 & 2 & 3 \\ \hline 4 & 1 & \\ \hline \end{array} \quad (6.3)$$

is a tableau which is *nonstandard* of shape $5 = 3 + 2$.

Of course, S_n acts in the obvious way on the vector space spanned by tableau T of shape λ . Given a tableau T of shape λ , let $R_T \subseteq S_n$ be the subgroup which fixes the *rows* of T , similarly $C_T \subseteq S_n$ is the subgroup which fixes the *columns*. We say that two tableaux T and T' are *row-equivalent* if $R_T = R_{T'}$, or what is the same, the same numbers appear in the same rows of T and T' . An equivalence class of row-equivalent tableaux is called a *tabloid*. For instance, there are 6 tableaux of shape $\{2, 1\}$ and they break up into 3 tabloids:

$$\begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline \end{array} \sim \begin{array}{|c|c|} \hline 2 & 1 \\ \hline 3 & \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 2 & 3 \\ \hline 1 & \\ \hline \end{array} \sim \begin{array}{|c|c|} \hline 3 & 2 \\ \hline 1 & \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \end{array} \sim \begin{array}{|c|c|} \hline 3 & 1 \\ \hline 2 & \\ \hline \end{array}$$

where $\sim$ indicates row-equivalence. Let M_λ be the free module over $\mathbb{Z}$ spanned by the tabloids. There is an evident action of S_n on M_λ . As an example, it is not hard to see that if $\lambda = \{n - c, c\}$ is a two-rowed partition, then $M_\lambda = \text{Sym}^c \mathcal{P}$ where $\mathcal{P}$ is the permutation representation of S_n .

Now to any tableau T of shape λ , let

$$E_T = \sum_{\sigma \in C_T} (-1)^\sigma \sigma([T]) \in M_\lambda$$

where $[T]$ denotes the tabloid associated to T . Then let $W_\lambda \subseteq M_\lambda$ be the submodule spanned

by the E_T .

Theorem 174. [102] *The module W_λ is a representation of S_n defined over $\mathbb{Z}$, and $V_\lambda \otimes \mathbb{C}$ is irreducible with associated partition λ . The E_T with T standard form a basis of V_λ .*

Given a tableau T of shape λ we may form the polynomial

$$f_T = \prod (x_a - x_b)$$

where a appears above b as labels in the *same column* of the tableau T . For instance, if T is as in (6.2), then $f_T = (x_1 - x_4)(x_1 - x_6)(x_4 - x_6)(x_2 - x_5)$, and if T is as in (6.3), then $f_T = (x_5 - x_4)(x_2 - x_1)$. Let $N = \deg(f_T)$ and let V_λ be the subspace of $\text{Sym}^N \mathcal{P}$ spanned by all f_T where T ranges over all tableaux of shape λ .

Theorem 175. *The representation V_λ is isomorphic to W_λ . Moreover, there is no $M < N$ such that V_λ appears as a subrepresentation of $\text{Sym}^M \mathcal{P}$.*

Now $V_\lambda \subseteq R = \text{Sym}^\bullet \mathcal{P}$, and so generates an *ideal* I_λ . The rest of this chapter concerns these ideals, and the quotients $S_\lambda = R/I_\lambda$. As a final bit of notation, we will often suppress the partition λ whenever the context is clear. For instance, $I = I_\lambda$, $V = V_\lambda$ and $S = S_\lambda$.

6.2.2 Some Commutative Algebra

The purpose of this section is to set notation. As such, we refer the reader to [46] for a more thorough discussion of the commutative algebra involved, particularly Chapter 4.

Let k be a field and let $R = k[x_1, \dots, x_n]$ be a polynomial ring. This ring has a natural *grading* $R = \bigoplus_{i \geq 0} R_i$ where R_i is spanned by the monomials of degree i . An R -module M is called *graded* whenever $M = \bigoplus_{i \in \mathbb{Z}} M_i$ and $R_i M_j \subseteq M_{i+j}$. We may *twist* a graded R -module M by any $t \in \mathbb{Z}$, denoting the twisted module $M(t) = \bigoplus M(t)_i$ where $M(t)_i = M_{i+t}$. All modules in this note are finitely-generated.

Let $\mathfrak{m} = (x_1, \dots, x_n) \subseteq R$ be the ideal of positively graded elements. If M is an R -module, we say that the *dimension of M* $\dim M$ is the Krull dimension of the ring $R/\text{Ann}(M)$ where $\text{Ann}(M) = \{r \in R : rM = 0\}$ is the *annihilator of M* . We say a sequence $f_1, \dots, f_r \in \mathfrak{m}$ is *regular for M* if f_i is not a zerodivisor of $M/(f_1, \dots, f_{i-1})M$. The *depth* of M is the maximal length of a regular sequence for M . We say a module is *Cohen-Macaulay* if its depth is equal to its dimension.

Any (finitely-generated) module M over R admits a free resolution $F_\bullet$, i.e., a sequence of free modules $F_i = \bigoplus_j R(-a_j)$ for $i \geq 0$ and maps $d_i : F_i \rightarrow F_{i-1}$ for $i \geq 1$ such that the cokernel of $d_1 : F_1 \rightarrow F_0$ is isomorphic to M and the homology $H_i(F_\bullet) = \ker(d_i)/\text{im}(d_{i+1}) = 0$ for all $i \geq 1$. Such a free resolution is *minimal* if $d_i(x) \subseteq \mathfrak{m}F_{i-1}$ for all $i \geq 1$ and $x \in F_i$. Minimal resolutions are unique up to isomorphism, so we will usually refer to *the* minimal resolution of a module M . The length of the minimal resolution, i.e., $\max\{i : F_i \neq 0\}$ is called the *projective dimension* of M , denoted $\text{pd } M$. For Cohen-Macaulay modules M , the Auslander-Buchsbaum Theorem [45, Theorem 19.9] states that

$$\text{pd } M + \dim M = \dim R.$$

As such, the minimal free resolution of a Cohen-Macaulay module has length $\dim R - \dim M = \text{codim } M$.

If $\dim M = 0$, then we define the *regularity of M* to be $\text{reg } M = \max\{c : M_c \neq 0\}$. If M is Cohen-Macaulay², then there is a regular sequence $f_1, \dots, f_r \in \mathfrak{m}$ for M so that $M' = M/(f_1, \dots, f_r)M$ has dimension 0. In this case we define $\text{reg } M = \text{reg } M'$.

Recall that there is a polynomial $H(M, t)$ in t such that $H(M, t) = \dim M_t$ for all $t \gg 0$. This is the *Hilbert polynomial* of M . Finally, the generating series of the dimensions M_i is denoted by $F(M, t) = \sum_{i=0}^{\infty} \dim(M_i)t^i$ and is called the *Hilbert series* of M . For us,

²Since all the modules we study are Cohen-Macaulay, we will not need the more general definition of regularity in terms of local cohomology, which may be found in [46, Chapter 4].

the most important property of regularity will be the following.

Theorem 176 ([46, Theorems 4.2 and 4.3]). *If M is a Cohen-Macaulay R -module with regularity c , then $\beta_{ij} = 0$ for all $j > c + i$. Moreover, $H(M, t) = \dim M_t$ for all $t \geq c + \text{pd}(M) - \dim(R) + 1$ and $H(M, t) \neq \dim M_t$ for all other t .*

6.3 Two-rowed Specht Ideals are Cohen-Macaulay

In this section, we work over an algebraically closed field k of arbitrary characteristic. The purpose of this section is to prove the following proposition.

Proposition 177. *If $\lambda = \{n - c, c\}$ is a two-rowed partition with $c \geq 2$ (and hence $n \geq 4$), then $\text{depth}(S_\lambda) = \dim(S_\lambda) = \text{reg}(S_\lambda) = c$. In particular, S_λ is Cohen-Macaulay.*

The main tool in our proof is the following geometric description of the Specht ideals. For $J \subseteq \{1, \dots, n\}$, let P_J be the ideal generated by the differences $x_i - x_j$ for $i, j \in J$.

Lemma 178. *If $|J| = n - c + 1$, then $P_J \in \text{Ass}(I_\lambda)$. Conversely, for every associated prime $P \in \text{Ass}(I_\lambda)$, there exists $J \subseteq \{1, \dots, n\}$ with $|J| = n - c + 1$ such that $P = P_J$.*

Proof. The Specht ideal I_λ is generated by f_T for T tableaux of shape λ . But f_T is the product of c differences $x_i - x_j$. So for none of these pairs $\{i, j\}$ to live in J , J could have at most $n - c$ elements. So P_J contains I_λ .

On the other hand, running this argument in reverse shows that every prime containing I_λ must contain some P_J . For if it did not, then we could find a tableau T of shape λ and i, j such that $(x_i - x_j) \nmid f_T$ and $f_T / (x_i - x_j)$ did not belong to the prime. $\square$

In fact, we can show that I_λ is *radical*. Indeed, the Specht polynomials f_T as T runs over all tableaux of shape λ form a Gröbner basis of I_λ for any lexicographic ordering on the variables. But the leading terms of each of the f_T is squarefree, and hence the ideal itself must be radical. From this we obtain the corollary

Corollary 179. *The degree of R/I_λ is $\binom{n}{c-1}$.*

We may now calculate the dimension and depth of S_λ . Note that if $|J| = m$ then we may order its elements $j_1 < \cdots < j_m$. Then P_J is generated by $x_{j_\ell} - x_{j_{\ell+1}}$ for $1 \leq \ell < m$. Moreover, this is a *regular sequence*, so we know that $\dim R/P_J = n - (m - 1)$. Applying this to $P_J \in \text{Ass}(I_\lambda)$, so $|J| = n - c + 1$, we see that $\dim R/I_\lambda = n - (n - c) = c$.

On the other hand, since we are working over an algebraically closed field, we know that the maximal prime ideals of R are precisely the ideals of points in affine space. Since the P_J cut out linear spaces, this immediately implies that the maximal ideals of R/P_J have depth equal to their height. But the maximal ideals of R/I consist of the images of the maximal ideals of R/P_J in R/I . This pullback by definition does not change the height of the ideal, and it is easily seen that the depth is at least the depth in R/P_J . However, the depth of an ideal cannot exceed its height, and so we have shown that R/I is unmixed, hence Cohen-Macaulay.

So all that's left is to compute the regularity of S_λ . By taking $c - 1$ linear sections of variety that I_λ cuts out in $\mathbb{P}^{n-1}$, we have $\binom{n}{c-1}$ points by Corollary 179. We call the set of these points X . The homogeneous coordinate ring of the $\mathbb{P}^{n-c}$ on which they lie shall be called R' , and their associated ring we shall call $S_X = R'/I_X$. Since our module is Cohen-Macaulay, if we take sufficiently general sections then $\text{reg}_{R'}(S_X) = \text{reg}_R(S_\lambda)$.

Now the regularity of X is the smallest integer d such that the space of forms vanishing on the points has codimension $\deg(X)$. This is a special case of the latter half of Theorem 176. But we note that I_X is generated in degree c so $\text{reg}(S_X) \geq c$. On the other hand, R' is generated by $n - c + 1$ transcendentals, so $\dim R'_c = \binom{n}{c}$. But as we will see in Lemma 183, $\dim(I_X)_c = \binom{n}{c} - \binom{n}{c-1}$. Hence the theorem.

6.4 Purity of the resolution

In this section, we recall the theory of [98, 74] and use it to compute the Hilbert functions of our Specht ideals. Suppose then that I is any homogeneous ideal of $R = k[x_1, \dots, x_n]$ such that $S = R/I$ is a Cohen-Macaulay R module. The *initial degree* of I is $\min\{\deg(f) : f \in I, f \neq 0\}$. We denote this by $\text{init}(I)$.

Let $H(S, t)$ be the *Hilbert polynomial* S , i.e., $H(S, t)$ is the polynomial such that $\dim S_t = H(S, t)$ for $t \gg 0$. Let $i(S) = \min\{t : H(S, t) = \dim S_t\}$. Then Schenzel showed in [98] that $\text{init}(I) \leq i(S) + \dim(R)$ when S is Cohen-Macaulay. He called ideals I for which the equality actually held *extremal*. Also in [98], he explicitly wrote down Hilbert series $F(S, t) = \sum_{i=0}^{\infty} \dim(S_i)t^i$ for such ideals.

When $\text{init}(I) + 1 = i(S) + \dim(R)$ and I is Cohen-Macaulay, we say that I is *nearly extremal*. It follows immediately from the second half of Theorem 176 and Proposition 177 that our two-rowed ideals are nearly extremal. Applying the first half of Theorem 176, we note that $\beta_{ij} = 0$ unless $j - i \in \{\text{init}(I) - 1, \text{init}(I)\}$. Then Kumar, Singh, and Kumar proved the following (translated to our case and making use of Lemma 183).

Theorem 180 ([74, Theorem 2.2]). *If I is a two-rowed Specht ideal with c columns, then we have that*

$$\beta_{i, c+i-1}(c) = \binom{n-1}{c+i-1} \binom{c+i-2}{i-1} + \binom{n-c}{i-1} \left[\binom{n}{c} - \binom{n}{c-1} - \binom{n-1}{c} \right] + \beta_{i-1, c+i-1}(c)$$

Note as well that we have shown that the Hilbert polynomial of S_λ is *independent* of the characteristic of k . As such, if we instead take $\mathcal{P}$ to be the permutation representation of S_n defined over $\mathbb{Z}$ and take $I_\lambda \subseteq R = \text{Sym}^\bullet \mathcal{P} = \mathbb{Z}[x_1, \dots, x_n]$, then we have the following corollary.

Corollary 181. *The ring $S_\lambda = \mathbb{Z}[x_1, \dots, x_n]/I_\lambda$ is flat over $\mathbb{Z}$.*

Proof. For any connected noetherian scheme T , a scheme $X \subseteq \mathbb{P}_T^M$ is flat if and only if the Hilbert polynomial of the fibers X_t ($t \in T$) is independent of t [66, Theorem 9.9]. But $\text{Spec } \mathbb{Z}$ is certainly a connected noetherian scheme, and so we have the corollary. $\square$

Note also that Theorem 180 implies that if any numbers b_{ij} satisfy the relation of the theorem, then the actual Betti numbers $\beta_{i,c+i-1} = b_{i,c+i-1} + C$ and $\beta_{i-1,c+i-1} = b_{i-1,c+i-1} + C$ for some integer C . In particular, if $\beta_{i,c+i-1} = b_{i,c+i-1}$, then $\beta_{i-1,c+i-1} = b_{i-1,c+i-1}$ and vice-versa.

In the next subsection, we verify that the dimensions claimed in (6.1) satisfy the relation of Theorem 180. Then in the following subsection, we explicitly construct the maps of the free resolution in for the $(c-1)$ strand. We show inductively that the $\beta_{i,c+i-1}$ are as claimed in (6.1) for $i \leq n-2c+1$. Combining this with a lemma of Green and Lazarsfeld, we will then have shown that the dimensions are as claimed.

6.4.1 Some Combinatorics

In this section, we verify that the dimensions claimed in (6.1) satisfy (180). We will be making constant use of the branching law for representations of the symmetric group. For any partition λ , let $|\lambda| = \sum \lambda_i$. Then for two partitions λ, μ we say that $\mu \leq \lambda$ whenever $|\mu| \leq |\lambda|$ and $\mu_i \leq \lambda_i$ for all i . We say that μ is a *restriction* of λ whenever $\mu \leq \lambda$ and $|\mu| = |\lambda| - 1$.

To see why we use this terminology, note that S_n by definition acts on the set $\{1, \dots, n\}$. Then the stabilizer of 1 (or, just as well, any $1 \leq i \leq n$) is a subgroup $S_{n-1} \subseteq S_n$. These are the *canonical* S_{n-1} 's in S_n . (These are in fact the *only* S_{n-1} 's in S_n for $n \geq 7$, but there are a few exceptions for $n \leq 6$.) Then the *branching law* for S_n states that

$$\text{Res}_{S_{n-1}}^{S_n} V_\lambda = \bigoplus V_\mu$$

where Res means *restriction* and the sum is over all μ which are restrictions of λ .

Example 182. For instance, the restriction V_λ for $\lambda = \{3, 3, 1\}$ is given by

$$\begin{array}{|c|c|c|} \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array} \oplus \begin{array}{|c|c|c|} \hline & & \\ \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array}$$

As an example of why this is useful, we show the following lemma.

Lemma 183. *The dimension of $V_{\{n-c,c\}}$ is $\binom{n}{c} - \binom{n}{c-1}$.*

Proof. The proof is by induction employing the branching law. We note that $\dim V_{\{n-1,1\}} = n - 1 = \binom{n}{1} - \binom{n}{0}$. This completes the case $n = 3$, so we induct on n and for each case induct on c . Then $\dim V_{\{n-c,c\}} = \dim V_{\{n-c-1,c\}} + \dim V_{\{n-c,c-1\}}$ whenever $1 < n/2 < c$. Then by induction

$$\dim V_{\{n-c-1,c\}} + \dim V_{\{n-c,c-1\}} = \binom{n-1}{c} - \binom{n-1}{c-1} + \binom{n-1}{c-1} - \binom{n-1}{c-2} = \binom{n}{c} - \binom{n}{c-1}$$

Finally, in the case $n = 2c$, we have that

$$\dim V_{\{c,c\}} = \dim V_{\{c,c-1\}} = \binom{n-1}{c-1} - \binom{n-1}{c-2}$$

Then since $n - 1 = (c - 1) + c$, adding and subtracting $\binom{n-1}{c-1} = \binom{n-1}{c}$ yields

$$\binom{n-1}{c-1} + \binom{n-1}{c} - \binom{n-1}{c-1} - \binom{n-1}{c-2} = \binom{n}{c} - \binom{n}{c-1}$$

□

Note that since $\beta_{0,c} = 0$, this lemma is consistent with Theorem 180.

To make everything more readable, we let $b_i^n(c) = \beta_{i,c+i-1}^n(c)$ and $c_i^n(c) = \beta_{i,c+i}^n(c)$ be the two (potentially) nonzero entries in the i th column of (6.1). Then Theorem 172 asserts

that for $1 \leq i \leq n - 2c + 1$ we have $c_i^n(c) = 0$ whereas for $i > n - 2c + 1$ we have $b_i^n(c) = 0$.

Let $1 < i < n - 2c + 1$ and let $\lambda = \{n - c - (i - 1), c, 1, \dots, 1\}$. Then the restrictions of λ are

$$\begin{aligned}\mu_1 &= \{n - c - (i - 1), c, 1, \dots\} &= \{(n - 1) - c - i, c, 1, \dots\} \\ \mu_2 &= \{n - c - (i - 1), c - 1, 1, \dots\} &= \{n - (c - 1) - i, c - 1, 1, \dots\} \\ \mu_3 &= \{n - c - i, c, 1, \dots\} &= \{(n - 1) - c - (i - 1), c, 1, \dots\}\end{aligned}$$

By induction, we know that these have dimensions

$$\begin{aligned}\dim \mu_1 &= b_{i-1}^{n-1}(c) \\ \dim \mu_2 &= b_i^{n-1}(c - 1) \\ \dim \mu_3 &= b_i^{n-1}(c)\end{aligned}$$

Now by induction again, we have that $c_{i-1}^{n-1}(c) = c_i^{n-1}(c - 1) = c_i^{n-1}(c) = 0$. So Theorem 180 implies

$$\begin{aligned}\dim \lambda &= \binom{n-2}{c+i-2} \binom{c+i-3}{i-2} + \binom{n-c-1}{i-2} \left[\binom{n-1}{c} - \binom{n-1}{c-1} - \binom{n-2}{c} \right] \\ &\quad \binom{n-2}{c+i-2} \binom{c+i-3}{i-1} + \binom{n-c}{i-1} \left[\binom{n-1}{c-1} - \binom{n-1}{c-2} - \binom{n-2}{c-1} \right] \\ &\quad \binom{n-2}{c+i-1} \binom{c+i-2}{i-1} + \binom{n-c-1}{i-1} \left[\binom{n-1}{c} - \binom{n-1}{c-1} - \binom{n-2}{c} \right]\end{aligned}$$

Then after applying Pascal's identity four times, we arrive at the claim.

The next case is when $i = n - 2c + 1$ so that there are only two restrictions of λ . The proof in this case is functionally identical, just with fewer terms. For $i > n - 2c + 1$ the proof is substantially similar, except now we need to use the realization of $\dim \lambda$ in terms of the c^{n-1} 's. The proof, though, is functionally identical.

Altogether, we have shown that the dimensions listed in (6.1) satisfy the relation of Theorem 180. In the next two subsections, we show that there are no extra components of the resolution.

6.4.2 Some Equivariant Maps: The $(c - 1)$ Strand

In this section, we construct the $(c - 1)$ -strand of the resolution of $S_\lambda = R/I_\lambda$ where $\lambda = \{n - c, c\}$ over $\mathbb{Z}$ as promised in the introduction. To begin, we construct some maps between tensor products of Specht modules.

To simplify notation, in this section we will never write the second row of any tableau. But note that it *always* has c boxes. Moreover, if two tableaux appear in the same equation, all ellipses will indicate the same number of columns or rows. In particular, we will be constructing a map

$$\begin{array}{c} \square \square \square \dots \square \\ \vdots \\ \square \\ \blacksquare \end{array} \longrightarrow \begin{array}{c} \square \square \square \dots \square \blacksquare \\ \vdots \\ \square \end{array} \otimes \mathcal{P} \quad (6.4)$$

where the diagram on the right has one fewer row and one more column than the diagram on the left. That is, the marked box moved. Let λ be the shape of the left-hand diagram, μ the shape of the right-hand diagram. If T is a tableau of shape λ , let T' be the tableau of shape μ and let t be the entry of the marked box. Then to a tabloid $[T]$ let $\varphi([T]) = [T'] \otimes x_t$. Since t is in an isolated row, this is well-defined and S_n -equivariant. It gives a map $M_\lambda \rightarrow M_\mu \otimes \mathcal{P}$.

Proposition 184. *The map φ is injective on $V_\lambda \subseteq M_\lambda$ and has image in $V_\mu \otimes \mathcal{P} \subseteq M_\mu \otimes \mathcal{P}$.*

Proof. Since all the modules in sight are free $\mathbb{Z}$ modules they are in particular torsion free. As such, it suffices to prove injectivity over $\mathbb{C}$ instead of $\mathbb{Z}$. Then since V_λ is irreducible, it suffices to show that $\varphi(v) \neq 0$ for *any* $v \in V_\lambda$. This is then easy to see by filling in λ left-to-right top-to-bottom with the numbers $1, \dots, n$. Then we may examine term-by-term the image

$$\varphi(E_T) = \sum_{\sigma \in C_T} \sigma([T])' \otimes x_t. \quad (6.5)$$

Fixing $t \in \{1, \dots, n\}$, look at the terms $\sigma([T])' \otimes x_t$ which appear in $\varphi(E_T)$.

A moment's thought shows that each tabloid in (6.5) is *distinct*. Indeed, by design, every tabloid the expansion of E_T is distinct, and if $[\sigma_1(T)'] = [\sigma_2(T)']$ for $\sigma_i \in C_T$, then

necessarily σ_1 and σ_2 must have the *same* action on all columns but the first. On the first column, the two permutations must differ at most by a final transposition of the first and last rows. But then their image in $\varphi(E_T)$ is differentiated by the $\otimes x_t$.

For the claim that $\varphi(V_\lambda) \subseteq V_\mu \otimes \mathcal{P}$, we again gather our terms according to the extra $\otimes x_t$. Note that $C_{T'}$ differs from C_T only in that elements of the first column are not allowed to be swapped with the marked box. Now it becomes obvious that the terms with $\otimes x_t$ come together to form $\pm E_{U'} \otimes x_t$ where U is the same as T except t and the final box of the first column have been switched. To compute the sign, note that $[U']$ appears with a positive sign in $E_{U'}$ but since U and T differ by a transposition, $[U']$ appears with a negative sign in $\varphi(E_T)$. More generally, if $\sigma \in C_T$ is any permutation swapping t and the marked box in (6.4), then the $\otimes x_t$ part of $\varphi(E_T)$ is $(-1)^\sigma E_{\sigma(T')} \otimes x_t$. $\square$

The reason that this map is important for us is the following proposition. Let λ and μ be as above and let ν be the partition which moves one more box from the first column to the first row, assuming that μ does not already have either two rows (so ν does not exist) or two columns (so λ does not exist). Let $\varphi_\lambda, \varphi_\mu$ be the maps described in (6.4). Then there is a map $\psi : V_\mu \otimes \mathcal{P} \rightarrow V_\nu \otimes \text{Sym}^2 \mathcal{P}$.

Proposition 185. *The kernel of ψ is precisely $\varphi(V_\lambda)$.*

Proof. To show that $\varphi(V_\lambda)$ is in the kernel of ψ it suffices to show that a single nonzero vector in $\varphi(V_\lambda)$ goes to 0 since everything in sight is free and so we may work over $\mathbb{C}$ where the representation in question is irreducible! So fix the usual tableau T of shape λ . We again break up the image by the basis vector $x_s x_t$ of $\text{Sym}^2 \mathcal{P}$.

Now $\psi(\varphi(E_T))$ cannot have any x_t^2 since T is a tableau, so we assume that $s < t$. Moreover, we know that $x_s x_t$ can only appear if s and t are in the first column of T . Then as in the previous proof, we know that the term involving $\otimes x_s$ in $\varphi(E_T)$ is $(-1)^\sigma E_{\sigma(T')} \otimes x_s$ where $\sigma \in C_T$ is any permutation taking the marked box of (6.4) to the box containing s . Similarly for $\otimes x_t$.

So the term involving $\otimes x_s x_t$ in $\psi(\varphi(E_T))$ must be $[(-1)^\sigma + (-1)^\tau] E_U \otimes x_s x_t$. Here $\sigma \in C_T$ takes s to the penultimate box in the first column and t to the last box. Then τ does the same, but reverse s and t . Here U is $\sigma(T)''$ is the tableau given by moving first t then s to the top row. Note that while $\tau(T)'' \neq \sigma(T)''$ we have $E_{\tau(T)''} = E_{\sigma(T)''}$ since the *tabloids* are the same and the differing columns are only one row high. But σ and τ have different signs, so this expression is 0. So we have shown this half of the claim.

To see that this is exactly the kernel is a little harder. Consider first the case when $\otimes x_1$ appears in an element of the kernel. Then since the E_U where U runs over standard tableaux is a basis of V_μ , we may write this part of the element as $(\sum a_U E_U) \otimes x_1$ with 1 in the top-left corner of U . Then applying ψ , we see that if $E_U \otimes x_1$ appears, then so must $E_{\sigma(U)} \otimes x_s$ where s is the bottom left entry of U . Quickly we find that we may subtract off elements of $\varphi(V_\lambda)$ and no $\otimes x_1$'s remain.

Note that if the top right box were not there, then it quickly becomes clear that in order to cancel out the $\otimes x_1^2$ terms in the image in ψ , one must have both $E_U \otimes x_1$ and $E_{\sigma(U)} \otimes x_1$ for some $\sigma \in C_U$ which does *not* permute the first column, both appearing with positive sign. However, $E_{\sigma(U)} = -E_U$ and so this means that our original element is 0.

So now we have a hope of applying induction. Changing the ordering of the numbers $1, \dots, n$, we may assume that they are ordered $2, 3, \dots, n, 1$. Then the standard tableaux all have 2 in the top left box and a similar argument allows us to expunge all $\otimes x_2$ entries. $\square$

As a corollary of the proof, we arrive at:

Proposition 186. *Suppose that λ has only two columns. Then the map $\psi : V_{\{c, c, 1, \dots, 1\}} \otimes \mathcal{P} \rightarrow V_{\{c+1, c, 1, \dots, 1\}} \otimes \text{Sym}^2 \mathcal{P}$ is injective.*

Since we have hit a 0 in the $(c-1)$ strand of the resolution, we know that the rest of the strand must also be 0. So Theorem 180 and Section 6.4.1 imply that we have computed all of the Betti numbers in any characteristic. As such, we need only determine the maps in the c strand.

6.4.3 Some More Equivariant Maps: The c Strand

Finally, as promised in Section 6.1, we write down the maps in the c strand of the resolution (6.1) and show that they are defined over $\mathbb{Z}$. Moreover, employing the Betti numbers we computed in the last two subsections, we show that the maps we write down are *injective* in every characteristic, and hence describe the resolution in every characteristic.

The maps that we are trying to describe are from $V_\mu \rightarrow V_\nu \otimes \mathcal{P}$ where μ and ν have shapes $\{c-1, c-i-2, 1, \dots, 1\}$ and $\{c-1, c-i-1, 1, \dots, 1\}$ where $0 \leq i \leq c-3$. That is, they have the same first row and differ by a single box in the second row.

But now the map is obvious. For a tableau T of shape μ we send the tabloid $[T]$ to the tabloid $[T']$ of shape ν where we have moved the bottom left entry t of T to the second row of T' . Then to get a map $V_\mu \rightarrow V_\nu \otimes \mathcal{P}$ we take $[T] \mapsto [T'] \otimes x_t$.

For example, we have the map

$$\begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 & & \\ \hline 7 & & & \\ \hline 8 & & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 8 & \\ \hline 7 & & & \\ \hline \end{array} \otimes x_8 \quad (6.6)$$

A similar argument as in the previous section shows that $\varphi(V_\lambda) \subseteq V_\mu \otimes \mathcal{P}$ is the kernel of $V_\mu \otimes \mathcal{P} \rightarrow V_\nu \otimes \text{Sym}^2 \mathcal{P}$ when $\mu_2 < \mu_1$.

To see that the map $V_\lambda \rightarrow V_\mu \otimes \mathcal{P}$ is injective, we may determine the inclusion matrix with the left hand side having basis the standard tableaux. As for the left hand side, we take a basis of elementary tensors $T(i, j) \otimes x_j$ where as i ranges, $T(i, j)$ runs through the standard tableaux under the ordering $1 < 2 < \dots < \hat{j} < \dots < n < j$. Now the inclusion matrix consists of blocks of identity matrices, and so it is clear that this map is injective in any characteristic.

There is but one more map remaining to define. Specifically, let λ, μ be as in Proposition 186. Then we know that $V_\lambda \otimes \mathcal{P} \rightarrow V_\mu \otimes \text{Sym}^2 \mathcal{P}$ is injective. But by our Betti number

computation $V_\lambda \otimes \text{Sym}^2 \mathcal{P} \rightarrow V_\mu \otimes \text{Sym}^3 \mathcal{P}$ is *not*.

Recall that $\lambda = \{c, c, 1, 1, \dots, 1\}$. Then let $\xi = \{c-1, c-1, 1, \dots, 1\}$. Then there is a map from tabloids of shape ξ to tabloids of shape λ by moving the bottom *two* boxes to the first two rows. Attaching $\otimes x_s x_t$ to the tabloid and making similar arguments, we see that V_ξ is exactly the kernel of this map!

Just to clarify this last map, we have the following example:

$$\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline 7 & & \\ \hline 8 & & \\ \hline 9 & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 8 \\ \hline 4 & 5 & 6 & 9 \\ \hline 7 & & & \\ \hline \end{array} \otimes x_8 x_9$$

6.5 A Multiplicative Structure

Finally in this section we build a multiplicative structure on the free resolutions constructed in the previous sections. We follow the generic outline of Chapter 5.

To begin, we recall from Chapter 5 the construction of the symmetric square

$$\text{Sym}^2(\mathbb{K}) = \mathbb{K} \otimes \mathbb{K} / M$$

of the resolution $\mathbb{K}$, where M is the graded submodule of $\mathbb{K} \otimes \mathbb{K}$ given by

$$\{f \otimes g - (-1)^{ij} g \otimes f : f \in \mathbb{K}_i, g \in \mathbb{K}_j\}.$$

Then

$$\text{Sym}^2(\mathbb{K})_k \cong \left(\sum_{i+j=k, i < j} \mathbb{K}_i \otimes \mathbb{K}_j \right) + \begin{cases} 0 & k \equiv 1 \pmod{2} \\ \wedge^2 \mathbb{K}_{k/2} & k \equiv 2 \pmod{4} \\ \text{Sym}^2(\mathbb{K}_{k/2}) & k \equiv 0 \pmod{4}. \end{cases}$$

In our case, when we have an S_n equivariant structure on the free resolution, the decomposition is also seen to be S_n equivariant. So in particular, $\text{Sym}^2(\mathbb{K})$ consists of projective R modules and is isomorphic to $\mathbb{K}$ in degrees 0 and 1. Note further that M is closed under the action of S_n . Hence $\text{Sym}^2(\mathbb{K})$ inherits an S_n -equivariant structure. We recall the following:

Theorem 187. *If $\mathbb{K}_\bullet$ and $\mathbb{L}_\bullet$ are two projective resolutions in an abelian category and there are maps*

$$\begin{array}{ccc} \mathbb{K}_1 & \longrightarrow & \mathbb{K}_0 \\ \downarrow & & \downarrow \\ \mathbb{L}_1 & \longrightarrow & \mathbb{L}_0 \end{array}$$

with the vertical maps isomorphisms then these maps may be extended to maps of complexes $\mathbb{K} \rightarrow \mathbb{L}$:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{K}_2 & \longrightarrow & \mathbb{K}_1 & \longrightarrow & \mathbb{K}_0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \cdots & \longrightarrow & \mathbb{L}_2 & \longrightarrow & \mathbb{L}_1 & \longrightarrow & \mathbb{L}_0 \end{array}$$

Using this theorem, we may, as Buchsbaum and Eisenbud did in [25], put an *a priori* CDGA structure on our resolutions, which also respects the S_n equivariant structure. In Buchsbaum and Eisenbud's case, their resolutions had length 3, and so to check associativity, they need only check one associativity relation: $(ab)c = a(bc)$ for $a, b, c \in \mathbb{K}_1$. But $(ab)c, a(bc) \in \mathbb{K}_3$. Since d_3 is injective, it suffices to show that $d_3((ab)c) = d_3(a(bc))$. After applying the DGA rules and the known cases, both turn out to be equal to

$$d_1(a) \cdot b \cdot c - a \cdot d_1(b) \cdot c + a \cdot b \cdot d_1(c).$$

Our free resolutions, on the other hand, can be arbitrarily long. As such, this proof technique is no longer valid. However, we may exploit the S_n equivariant structure as we did in Chapter 5. Specifically, we show that the kernels of the transition maps and the images

of multiplication belong to disjoint isotypical components. In fact, since both multiplication and the d maps are R -linear, it suffices to show that no two elements of *ordinary* degree 0 multiply to an element of the kernel of the relevant d map. This is what we endeavor to show. We begin with a lemma.

Lemma 188. *For $a \in \mathbb{K}_i$ and $b \in \mathbb{K}_j$, the ordinary degree of ab is 1 more than the sum of the ordinary degrees of a and b unless $i = 0$, $j = 0$, or $i + j = n - 2c + 2$, in which case the ordinary degree of ab is just the sum of the ordinary degrees of a and b .*

Proof. First we note that since $\mathbb{K}_0 = R$ that there is a canonical multiplication $\mathbb{K}_0 \otimes \mathbb{K}_i \rightarrow \mathbb{K}_i$ simply given by multiplication by multiplication by R . As such, there is no adjustment to the ordinary degree necessary.

Now we proceed by induction. For instance, suppose that $a, b \in \mathbb{K}_1$. Then $d(ab) = a \cdot d(b) \pm d(a) \cdot b$. If $n \neq 2c$, then the ordinary degree of $d(ab)$ is one more than the ordinary degree of ab . On the other hand, $d(a)$ has ordinary degree 2 more than a and the same is true of $d(b)$. But $d(a), d(b) \in \mathbb{K}_0$, so multiplication by them causes no adjustment in the ordinary degree. As such, when $n \neq 2c$, the ordinary degree of ab must be one more than the sum of the ordinary degrees of a and b .

Similarly, if $a \in \mathbb{K}_1$ but $b \in \mathbb{K}_i$ for any i , then the Leibniz rule and the fact that we are searching for a homogeneous multiplicative structure implies that $a \cdot d(b)$ must have the same ordinary degree as $d(a) \cdot b$, which is two more than the sum of the ordinary degrees of a and b . So, if $b \in \mathbb{K}_{n-2c+2}$, then there is no need for an adjustment to the ordinary degree. Otherwise, we must add 1 whenever we multiply $c \in \mathbb{K}_{i-1}$ and $a \in \mathbb{K}_1$.

We may continue in this combinatorial manner noting that if $a \in \mathbb{K}_2$, then $d(a) \cdot b$ has a total of 2 added to the ordinary degree unless $b \in \mathbb{K}_{n-2c+1}$. And this tells us that $a \cdot d(b)$ has two added to the ordinary degree unless $d(b) \in \mathbb{K}_{n-2c}$.

This argument continues to show that unless the homological degrees of a and b sum to $n - 2c + 2$ or unless the homological degree of a or b is 0, then multiplying a and b together

yields an element of ordinary degree 1 more than the sum of the ordinary degrees of a and b . □

As the trick of Buchsbaum and Eisenbud has already allowed us to put an S_n -equivariant commutative differential graded algebra structure on our free resolution over a field of characteristic 0, we will now demonstrate that this structure is associative. To do so, we simply show that the kernel of d_{i+j} does *not* appear in any isotypical component of $F_i \otimes F_j$.

When $i+j = n-2c+2$, then the preceding lemma implies that if a, b have ordinary degree 0, then so does ab . But in ordinary degree 0, our computation of the minimal free resolution shows that the kernel is trivial in this ordinary degree.

When $i+j < n-2c+2$, then Lemma 167 of Chapter 5 implies that every representation in $F_i \otimes F_j$ has at most $i+j+1$ rows, whereas the kernel has $i+j+2$ rows. So this must appear in a disjoint isotypical component.

Finally, when $i+j > n-2c+2$, the same lemma implies that $F_i \otimes F_j$ has again at most $i+j+1$ rows whereas the kernel has $i+j+2$ rows. This completes the proof of Corollary 173.

6.6 Conclusions and Future Work

From here there are several directions for future work. For instance, can other Weyl groups than S_n be exploited to produce pure resolutions, especially ones with multiplicative structures? How are these pure resolutions related to Boij-Söderberg Theory? Do they fit together with the so-called *tensor complexes* [7] or are they a new phenomenon?

We also find it odd that there would be no *a priori* proof that $\mathrm{Tor}_i^R(k, S)_j$ is an irreducible representation for every i and j when S is the ring associated to a two-rowed Specht ideal. We wonder if there is another approach which would yield this fact.

Finally, we are also curious as to what these multiplicative structures mean. In Chapter 5, the fact that the final Betti number of S was 1 and the multiplicative structure gave the self-duality of the free resolution. Is there some similar notion of duality for free resolutions with ACDGA structures when the final Betti number is not 1?

Chapter 7

Sextic Resolvents of Quintic Fields and the Representation Theory of S_5

7.1 Introduction

Recall that an n -ic ring over a (commutative, associative, unital) base ring B is a B -algebra R such that R/B is a free R -module of rank $n - 1$. In [14], Bhargava introduced a new notion of a *sextic resolvent ring* S of a quintic ring R over $\mathbb{Z}$. This in turn was a case of a larger program of Higher Composition Laws which yielded parameterizations for quadratic [9], cubic [10] and quartic [11] rings with some extra data over $\mathbb{Z}$. Wood, starting from an idea of Deligne [41], subsequently generalized these parameterizations in her thesis [111] to apply over an arbitrary base scheme.

This, however, leads to the question of how to generalize the quintic construction to an arbitrary base. We have not been entirely successful in accomplishing this task, and in this chapter, we try to give a sense of why.

In the previous chapters of this thesis, we have seen that there is a fundamental link between certain representations of the symmetric group on n letters and Bhargava's parameterizations of rank n rings. In particular, they were linked by the minimal free resolution of

n points in $\mathbb{P}^{n-2}$. We saw that the points themselves define a standard representation of S_n on V where $\mathbb{P}^{n-2} = \mathbb{P}V$. And we saw that the equations cutting out these n points (when $n \geq 4$) was an S_n subrepresentation of $\text{Sym}^2 V^\vee$ whose associated Young diagram is

$$\begin{array}{c} \overbrace{\begin{array}{|c|c|c|c|} \hline & & & \\ \hline & & & \\ \hline \end{array}}^{n-2} \\ \begin{array}{|c|c|} \hline & \\ \hline & \\ \hline \end{array} \end{array} . \quad (7.1)$$

In the case $n = 4$, the double transpositions form a normal Klein four subgroup $V_4 \subseteq S_4$ and S_4/V_4 is noncommutative and has order 6 and so must be isomorphic to S_3 . In fact, V_4 acts trivially on (7.1), and hence is canonically an S_3 representation. In particular, it is the *standard* S_3 representation. But a standard S_3 representation yields a set of 3 points in some $\mathbb{P}^2$, which in turn yields a cubic ring. This ring is precisely the cubic resolvent of the quartic ring!

In Section 7.2, we find that the representation theory connecting S_5 and S_6 also connects quintic fields to their traditional *sextic* resolvent in the same manner. In Section 7.3, we use this insight to define a sextic resolvent ring of $\mathbb{Z}^5$. In particular, we find

Proposition 189. *The sextic resolvent ring of $\mathbb{Z}^5$ has discriminant 4. Moreover, for any definition of a sextic resolvent which is compatible with base change and compatible with the representation theory of Section 7.2, the discriminant of the sextic resolvent must be divisible by 4.*

This result differs from Bhargava's result in Equation (33) of [14], which yields a sextic resolvent ring of discriminant $4096 = 2^{12}$ for $\mathbb{Z}^5$. We have not yet extended our method to all quintic rings over $\mathbb{Z}$, and perhaps we will find in future work that these extra 2s are necessary for the theory to work for all quintic rings. But either way, these results indicate that extending the theory of sextic resolvents of quintic rings to arbitrary base rings will be rather difficult unless at least 2 is invertible. We hope to pursue this avenue of work in the

future.

7.2 The Representation Theory of S_5 and S_6

We begin this section with some elementary facts about the symmetric groups S_5 and S_6 . The unusual nature of these groups and the connections between them underlies our whole program.

7.2.1 The Transitive S_5 in S_6

To begin, recall that for all $m < n$, there are many copies of $S_m \subseteq S_n$. In particular, there are many copies of $S_{n-1} \subseteq S_n$. The most readily apparent $S_{n-1} \subseteq S_n$ is the stabilizer of some letter. This subgroup, however, is not transitive. In fact, it is known that for $n > 6$, there are no copies of S_{n-1} which live in S_n as a transitive subgroup. Here we construct a transitive subgroup of S_6 which is isomorphic to S_5 .

Note that S_5 has $4! = 24$ five-cycles, and hence has 6 cyclic subgroups C_5 of order 5. But the 5-part of $5!$ is 5, so these are in fact the *Sylow* 5-subgroups. Now any group G acts on its set of Sylow p -subgroups *transitively* under conjugation, so by labelling the five-cycles, we obtain a map $S_5 \rightarrow S_6$ whose image is a transitive subgroup. It suffices to show that this map is *injective*.

But S_5 has three normal subgroups: the trivial group, the whole group, and the alternating group A_5 . As noted, S_5 acts transitively, so in particular nontrivially, on its Sylow 5-subgroups, so the kernel cannot be the whole group. Similarly, $[S_5 : A_5] = 2$, and since there are $6 > 2$ 5-Sylow subgroups, if the kernel were A_5 then S_5 would again be unable to act transitively. So the morphism *must* be injective.

Recall that the inner automorphisms of S_n can be viewed as the automorphisms which permute the names of the n letters. As such, we immediately see that our single copy of S_5

has 720 conjugates. In fact, these are the only transitive S_5 's living in S_6 , a fact which may be obtained, for instance, by asking Magma [23] to enumerate the subgroups of S_6 .

Lemma 190. *The group S_6 has precisely $6! = 720$ transitive subgroups isomorphic to S_5 . They are all conjugate to each other.*

Remark 191. This transitive S_5 in S_6 has many realizations in (algebraic) combinatorics. For some other beautiful descriptions of it, see, e.g., [14, 70]

7.2.2 Some Special Representations of S_5 and S_6

Next we recall that the irreducible representations of S_n over $\mathbb{C}$ are in one-to-one correspondence with the *partitions* $\lambda = \{\lambda_i\}$ of n , i.e., sets of numbers $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$ such that $\sum \lambda_i = n$. We will often refer to a specific partition by its Young diagram without further comment. Moreover, if it is necessary, we will refer to the irreducible representation associated to λ by V_λ , and if it is further necessary to emphasize n , we shall write V_λ^n . For further information on this correspondence, see [54, Problem 4.47], [108] or Chapter 6.

For the “usual” copies of $S_{n-1} \subseteq S_n$, i.e., those copies which are the stabilizers of a letter, we know the so-called “branching law”, i.e., how an irreducible representation V of S_n breaks up into irreducible components when restricted to S_{n-1} . Specifically, for any partition λ , let $|\lambda| = \sum \lambda_i$. Then for two partitions λ, μ we say that $\mu \leq \lambda$ whenever $|\mu| \leq |\lambda|$ and $\mu_i \leq \lambda_i$ for all i . We say that μ is a *restriction* of λ whenever $\mu \leq \lambda$ and $|\mu| = |\lambda| - 1$.

To see why we use this terminology, note that S_n by definition acts on the set $\{1, \dots, n\}$. Then the stabilizer of 1 (or, just as well, any $1 \leq i \leq n$) is a subgroup $S_{n-1} \subseteq S_n$. These are the *canonical* S_{n-1} 's in S_n . (These are in fact the *only* S_{n-1} 's in S_n for $n \geq 7$, but there are a few exceptions for $n \leq 6$.) Then the *branching law* for S_n states that

$$\text{Res}_{S_{n-1}}^{S_n} V_\lambda = \bigoplus V_\mu$$

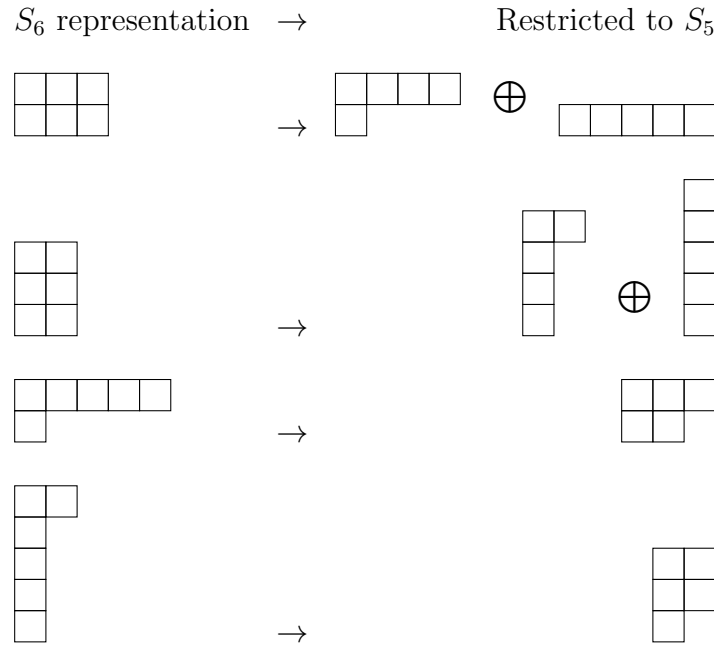
where Res means *restriction* and the sum is over all μ which are restrictions of λ .

Example 192. For instance, the restriction V_λ for $\lambda = \{3, 3, 1\}$ is given by

$$\begin{array}{|c|c|c|} \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array} \oplus \begin{array}{|c|c|c|} \hline & & \\ \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array}$$

The branching law behaves differently for our transitive $S_5 \subseteq S_6$. We will, in particular, be interested in the 5-dimensional representations of S_6 , of which there are four. One can compute using character theory how these representations break up when restricted to the transitive S_5 . This is drawn in Figure 7.1.

Figure 7.1: Restrictions of the 5-dimensional representations of S_6 to S_5



We have arrived at a situation we have seen before. Recall that to every rank n étale algebra R over a field k , Bhargava constructed in [14, Section 2] a Galois-invariant set of n points in $\mathbb{P}_{k^{sep}}^{n-2}$ whose global sections over k were precisely R . So the governing philosophy is that rank n rings should correspond to (Galois-invariant) sets of n (geometric) points in

$\mathbb{P}_k^{n-2}$. This is explicated more thoroughly in Chapter 3.

In what follows, we recapitulate briefly the contents of Section 2 of Chapter 5. A set of n linearly general¹ points in $\mathbb{P}^{n-2} = \mathbb{P}V$ is acted on transitively by $\mathrm{PGL}_{n-1}(k)$. (This is a generalization of the fact that three points in $\mathbb{P}^1$ can be sent to any three other points by fractional linear transformations.) In fact, the subgroup of $\mathrm{PGL}_{n-1}(k)$ which leaves this set of points fixed is isomorphic to S_n . One sees (as in Chapter 5) that there are precisely *two* lifts of this subgroup to $\mathrm{GL}_{n-1}(k)$. One of these is the standard representation of S_n , and the other of these is the twist of the standard representation by the alternating character, i.e., its next-to-top wedge power. From now on, we forget the alternating twist and instead consider V equipped with the standard representation.

It turns out that if $n \geq 4$, then the n points in $\mathbb{P}^{n-2}$ are cut out by quadrics², and it is obvious that the subspace of quadrics in $\mathrm{Sym}^2 V^\vee$ should be a *subrepresentation* of S_n . We saw in Chapter 5 that $\mathrm{Sym}^2 V^\vee$ broke up into a trivial representation, a standard representation, and one corresponding to the partition $\{n-2, 2\}$. This latter representation is precisely the linear system of quadrics cutting out our n points.

In the case $n = 6$, we have seen that the restriction of $V_{\{5,1\}}^6$ to a transitive S_5 is the $V_{\{3,2\}}^5$. That is, we expect there to be a relation between sextic and quintic rings. Indeed, this is the same type of relation which gives rise to the quadratic resolvents of cubic rings and the cubic resolvents of quartic rings, which is again explicated in Chapter 5. We explore this further in the next subsection.

¹This means that no $n-1$ of them lie on a hyperplane.

²This is an instance of a much more general fact due to Green and Lazarsfeld [63], though it may also be proven directly.

7.2.3 The Representation-Theoretic Sextic Resolvent of a Quintic Ring

Fix a particular labelling of the five-cycles of S_5 , i.e., fix a transitive embedding $S_5 \hookrightarrow S_6$. In this section, we show that there is a *unique* map $S_6 \rightarrow \mathrm{GL}_5$ extending the representation $V_{\{3,2\}}$ of S_5 to the representation $V_{\{5,1\}}$ of S_6 . Let's first give the intuitive, geometric construction³. In the next section, we will show that this construction is universal, in an appropriate sense. But for now, let the base field $k = \bar{k}$ be an algebraically closed field of characteristic 0.

For any $(\sigma) \subseteq S_5$ isomorphic to C_5 , we note that σ acts *nontrivially* on the set of 5-Sylow subgroups. Extending this to the rational permutation representation, we see that this action has a *unique* fixed point, for the only nontrivial rational 5-dimensional representation of C_5 is the regular representation. Indeed, more generally, we have

Lemma 193. *The cyclic group C_p of p prime elements has precisely 2 (isomorphism classes of) irreducible finite-dimensional representations over $\mathbb{Q}$: the trivial representation and the regular representation modulo the trivial representation.*

Proof. Over an algebraically closed field $\bar{k}$ of arbitrary characteristic, the irreducible representations of C_p are precisely the characters $C_p \rightarrow \bar{k}^\times$. Any representation over $\mathbb{Q}$ must break into a direct sum of these characters. By fixing an element $1 \in C_p$ (i.e., fixing an isomorphism $\mathbb{Z}/p\mathbb{Z} \cong C_p$), we may detect how a representation V of C_p breaks up over $\bar{\mathbb{Q}}$ by asking what the eigenvalues of the action of $1 \in C_p$ are. But if a nontrivial root of unity is an eigenvalue, then since they are all Galois-conjugate over $\mathbb{Q}$, the other nontrivial roots of unity must also appear. However, the span of the Galois orbit of an eigenvector is obviously a subrepresentation of V defined over $\mathbb{Q}$. This leads to the theorem. $\square$

Now restricting the action of S_5 on $V_{\{3,2\}}$ to (σ) , the same argument implies that there is a unique trivial subrepresentation. In fact, we can say something much stronger:

³I originally learned this idea from a letter of Edixhoven to Bhargava [44], but did not realize its connection to the quirks of the representation theory of S_5 and S_6 until much later.

Let $(\sigma_1), \dots, (\sigma_6)$ be the six copies of C_5 in S_5 and let $\ell_1, \dots, \ell_6$ be their respective trivial subrepresentations.

Lemma 194. (σ_i) acts transitively on $\{\ell_1, \dots, \ell_6\} - \{\ell_i\}$.

Proof. Consider the case $i = 1$. All other cases are essentially the same. Now (σ_1) acts on the set $\{(\sigma_2), \dots, (\sigma_6)\}$ by conjugation. A quick computation shows that it acts nontrivially on σ_2 , and hence, since C_5 has prime order, the orbit-stabilizer theorem says that it must act transitively.

But $\sigma_1^i \ell_j$ is stabilized by $\sigma_1^i(\sigma_j)\sigma_1^{-i}$. But the ℓ_j 's were the *unique* trivial subrepresentation for the associated cyclic group. Hence the lemma. $\square$

If $\ell_i = \ell_j$ for $i \neq j$, then the above lemma combined with the orbit-stabilizer theorem would then imply that *all* the ℓ_i are equal. This would consequently imply that all the Sylow 5-subgroups of S_5 act trivially on ℓ_1 . But the Sylow 5-subgroups of S_5 *generate* S_5 , and hence $V_{\{3,2\}}$ would contain a trivial representation, which of course is ludicrous.

Finally, we see that $\{\ell_1, \dots, \ell_6\}$ is a linearly general set of points in $\mathbb{P}V_{\{3,2\}}$. To see this, it suffices to show that any subset of 5 elements spans all of $V_{\{3,2\}}$. To do this, we note that there is a representation of S_5 which is defined over $\mathbb{Q}$ which is isomorphic to $V_{\{3,2\}}$ over k , the so-called *Specht representation*. Then we may once again use the fact that any nontrivial five-dimensional representation of C_5 over $\mathbb{Q}$ is the regular representation, and so Lemma 194 yields the result.

Thus, we have 6 linearly general *points* in $\mathbb{P}V_{\{3,2\}}$. From our previous discussion, this implies that there is a subgroup $S_6 \subseteq \mathrm{PGL}(V_{\{3,2\}})$ acting on these points, and that there is a unique lift to $\mathrm{GL}(V_{\{3,2\}})$ which is the standard representation.

Theorem 195. *This representation of S_6 restricts to the original representation $V_{\{3,2\}}$ of S_5 . Moreover, this is the unique such extension.*

Proof. That this restricts to the same representation on S_5 is obvious from the construction. To see that this is the unique such extension, we recall from Section 2 of Chapter 5 that a standard representation of S_n on an $(n - 1)$ -dimensional vector space V is determined by n points in linearly general position in $\mathbb{P}V$, or, what is the same, by n “basic lines” $\ell_1, \dots, \ell_n \subseteq V$ such that any $(n - 1)$ of them span V .

In particular, these basic lines can be determined by noting that by the usual branching law for S_n , we have that $\text{Res}_{S_{n-1}}^{S_n} V_{std}^n = V_{std}^{n-1} \oplus V_{triv}^{n-1}$. The n basic lines are the n trivial representations that arise from the n nontransitive S_{n-1} ’s in S_n .

In our case, one way to rephrase the above lemmas is that the six nontransitive S_5 ’s in S_6 each contain a *unique* Sylow 5-subgroup of the (fixed!) transitive S_5 . Moreover, the restriction to this cyclic subgroup *already* picks out the trivial representation. But this is exactly the process we used to construct the extension. Hence, we have shown uniqueness. $\square$

7.2.4 Galois Invariance

In this section, we demonstrate that the constructions of the previous section are *Galois invariant*. In particular, we construct in a representation theoretic manner the sextic resolvent of a quintic algebra over *any* field k of characteristic 0. Let $G = \text{Gal}(\bar{k}/k)$ be the absolute Galois group of k and let $X \subseteq \mathbb{P}W = \mathbb{P}_k^3$ be reduced subscheme of dimension 0 and degree 5 which is linearly general, i.e., $\bar{X} = X \times \bar{k}$ consists of 5 points in linearly general position.

Remark 196. Another way to state the condition of linear generality which doesn’t rely on the geometric picture is to say that any hyperplane section of X must have degree at most 3. For if the five points of $\bar{X}$ span a linear subspace, this linear subspace would be defined over k and this linear subspace would be contained in a hyperplane defined over k . If only four points in $\bar{X}$ lived on a hyperplane, then the Galois conjugates of those four points would also have to live on a hyperplane. So either $\bar{X}$ breaks up into two Galois conjugate sets of

points (four points on a hyperplane defined over k and one point off it) in which case we are done, *or* each Galois conjugate pair of hyperplanes has three points in common. Then if no three of our original four points are collinear, this would imply that the fifth point already lay on the original hyperplane (since three noncollinear points define a plane). If three of our original four points were collinear, then the Galois conjugates of that set of points must *also* be collinear. But any conjugate of this set must have at least one point in common. If ever there are two in common, then since we've assumed the points are distinct, there are *four* points lying on a line, and the fifth point at most defines a hyperplane. If there is always at most *one* point in common, then we procure two Galois conjugate lines, which in turn define a hyperplane defined over k .

By tensoring up to $\bar{k}$, we see that X is cut out by a five-dimensional space of quadrics $V \subseteq \text{Sym}^2 W^\vee$. Working over $\bar{V} = V \otimes \bar{k}$, we may find six lines $\ell_1, \dots, \ell_6$ by the procedure of the previous section. We wish to show that these lines are Galois conjugate, and thus we will obtain a linearly general set of six (geometric) points in $\mathbb{P}V$. The ring of functions on this set of points is thus a sextic algebra over k .

That the 5 points in X are Galois conjugate means that there is a map $G \rightarrow \text{PGL}(\bar{W})$ whose image lies in the S_5 leaving $\bar{X}$ fixed. That is, acting by G amounts to executing an *inner* automorphism of S_5 on the representation $S_5 \rightarrow \text{GL}(\bar{V})$. In particular, this does not change the image of S_5 in $\text{GL}(\bar{V})$. But the ℓ_i were defined as the fixed lines of the Sylow 5-subgroups of the *image* of S_5 in $\text{GL}(\bar{V})$. That is, the set of ℓ_i is not effected by inner automorphisms of S_5 , though the labelling might be.

In particular, this implies that the points $\ell_i \in \mathbb{P}\bar{V}$ form a Galois invariant set.

7.3 A Specific Case

In this section, we give an example of the extension of the representation $V_{\{3,2\}}$ we constructed in the last section to a representation of S_5 . In particular, we will work with the Specht

realization of $V_{\{3,2\}}$ as detailed in Chapter 6. We will see that while the extension described in the previous section is *not* the Specht realization of $V_{\{5,1\}}$, it is still a representation defined over $\mathbb{Z}$.

In what follows, all computations were done in Sage [105], especially relying on F. Salicrú's implementation of the Specht representations, which were in turn based off of the outline in Lascoux's notes [86].

To begin, we construct the Specht representation $\rho : S_5 \rightarrow \mathrm{GL}_5(\mathbb{Z})$ associated to $\{3, 2\}$. We then construct representatives of each of the six 5-Sylow subgroups of S_5 and ask Sage to compute the right eigenvectors of these transformations. As we proved, precisely one eigenvector has eigenvalue one. These are given by the columns of the following matrix.

$$\begin{bmatrix} 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 \\ 0 & 0 & 0 & -2 & 2 & 0 \end{bmatrix} \quad (7.2)$$

Note that each row sums to 0. In fact there are only two choices of signs among the $2^6 = 64$ possibilities making this true: the stated one and the one given by the negative of the matrix (7.2). In Bhargava's construction of Section 2 of [14], the discriminant of the ring R associated to these six points in $\mathbb{P}_{\mathbb{Z}}^4$ is $\pm\sqrt{|\det(M)|}$ where M is any 5×5 submatrix of (7.2). Each such M has $|\det(M)| = 16$ and hence $\mathrm{Disc}(R) = \pm 4$.

Now the sextic resolvent ring we have described over $\mathbb{Z}$ is necessarily a subring of the sextic resolvent ring over $\mathbb{Q}$. But this ring is the ring of functions on the six points in (7.2), which is $\mathbb{Q}^6$. So $\mathrm{Disc}(R) = 4$ since $\mathbb{Q}^6$ is totally real.

Finally, to identify R , we note that $R \subseteq \mathbb{Z}^6$ must have index 2 since $\mathrm{Disc}(R) = [\mathbb{Z}^6 : R]^2 \mathrm{Disc}(\mathbb{Z}^6) = [\mathbb{Z}^6 : R]^2$. But then combining the fact that 2 is prime and the fact that Smith

Normal Form exists, we know that all such R are conjugate. Explicitly, one representative of this isomorphism class is the span of $(2e_1, e_2, e_3, e_4, e_5, e_1 + e_2 + \cdots + e_6)$ where $e_1, e_2, \dots, e_6$ is a set of orthongonal idempotents of $\mathbb{Z}^6$ and $e_1 + \cdots + e_6$ is the multiplicative identity element of $\mathbb{Z}^6$.

So from this we begin to see perhaps the largest problem with extending the theory of the sextic resolvent to arbitrary base schemes: in order to be compatible with base change, a nondegenerate algebra $\mathbb{F}_2^6$ over $\mathbb{F}_2$ must have a sextic resolvent which is degenerate! Specifically, $(2e_1)^2 = 0$ modulo 2, and so $R \otimes \mathbb{F}_2 \cong \mathbb{F}_2[x]/(x^2) \oplus \mathbb{F}_2^4$.

We have not been able to work out the most general theory of the sextic resolvent from this perspective. In particular, we are not sure if the methods of this section can be extended to all quintic rings over $\mathbb{Z}$, much less those over an arbitrary base scheme. We hope to answer this question in future work, and in doing so resolve the discrepancy between Bhargava's discriminant for the sextic resolvent of $\mathbb{Z}^6$ (which yields 4096) and ours (which yields 4).

Finally, as promised, we note that we may build the standard representation of S_6 associated with R as follows. Let

$$M = \begin{bmatrix} 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & -2 & 2 \end{bmatrix} \quad (7.3)$$

be the first five columns of (7.2). If $i < 5$, let $(i, i+1) \in \text{GL}_5(\mathbb{Z})$ be the permutation matrix which is the identity matrix except for the 2×2 block between rows and columns i and $i+1$,

in which case it has the form

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

Then let $(4, 5)$ be the matrix which is the identity matrix except the last column consists entirely of -1 . Each of these matrices is easily seen to have determinant -1 and hence lives in $\mathrm{GL}_5 \mathbb{Z}$. Moreover, they satisfy the Coxeter relations for S_6 and hence generate S_6 . In fact, they form the Specht realizations of the standard representation $V_{\{5,1\}}$ of S_6 .

Then the eigenvectors (7.2) yield a standard representation with the generators

$$M \cdot (i, i+1) \cdot M^{-1}. \tag{7.4}$$

Of course, $\det(M) = 16$ and so *a priori* these involutions only live in $\mathrm{GL}_5 \mathbb{Q}$. However, Sage quickly tells us that they actually live in $\mathrm{GL}_5 \mathbb{Z}$.

We note, however, that this method once highlights the problem at 2: $\det(M) = 16$ implies that the change of variables (7.4) is not defined over $\mathbb{F}_2$. As such, we would once again expect a degenerate ring to be the sextic resolvent of $\mathbb{Z}^5$.

To finish off the proof of Proposition 189, we note that compatibility with the representation theory of the previous section means that a sextic resolvent R for $\mathbb{Z}^5$ must be an order in the $\mathbb{Q}^6$ which is the ring of functions for the six points in (7.2) in $\mathbb{P}_{\mathbb{Q}}^4$. But the *span* of these points is determined by the representation theory, any other realizations of these points must be constant multiples of the points given. But since these points contain ± 1 , they cannot be multiplied by any number to reduce the determinant of a 5×5 minor of (7.2). As such, we see that any definition of the sextic resolvent compatible with the representation theory outlined must have discriminant divisible by 4.

Bibliography

- [1] K. Akin, D. Buchsbaum, and J. Weyman. Schur functors and Schur complexes. *Adv. in Math.*, 44(3):207–278, 1982.
- [2] L.L. Avramov. On the Hopf algebra of a local ring with an appendix by V. Hinič. *Math. USSR-Izv.*, 8:259–284, 1974.
- [3] L.L. Avramov. Obstructions to the existence of multiplicative structures on minimal free resolutions. *Amer. J. Math.*, 103:1–31, 1981.
- [4] M.B. Barban. Linnik’s “great sieve” and a limit theorem for the class number of ideals of an imaginary quadratic field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 26:573–580, 1962.
- [5] A. Beauville. Determinantal hypersurfaces. *Michigan Math. J.*, 48(1):39–64, 2000.
- [6] K. Belabas, M. Bhargava, and C. Pomerance. Error estimates for the Davenport–Heilbronn theorems. *Duke Math. J.*, 153(1):173–210, 2010.
- [7] C. Berkesch, D. Erman, M. Kummini, and S. Sam. Tensor complexes: Multilinear free resolutions constructed from higher tensors. *J. European Math. Soc.*, 2012, math.AC/1101.4604. To appear.
- [8] M. Bhargava. Higher Composition Laws V. In preparation.
- [9] M. Bhargava. Higher Composition Laws I: A new view on Gauss composition, and quadratic generalizations. *Ann. Math. (2)*, 159(1):217–250, 2004.

- [10] M. Bhargava. Higher Composition Laws II: On cubic analogues of Gauss composition. *Ann. Math. (2)*, 159(2):865–886, 2004.
- [11] M. Bhargava. Higher Composition Laws III: The parameterization of quartic rings. *Ann. Math. (2)*, 159(3):1329–1360, 2004.
- [12] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. Math. (2)*, 162(2):1031–1063, 2005.
- [13] M. Bhargava. Mass formulae for extensions of local fields, and conjectures on the densities of discriminants of number fields. *Int. Math. Res. Not.*, (17), 2007.
- [14] M. Bhargava. Higher Composition Laws IV: The parameterization of quintic rings. *Ann. Math. (2)*, 167(1):53–94, 2008.
- [15] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. Math. (2)*, 172(3):1559–1591, 2010.
- [16] M. Bhargava and W. Ho. Coregular spaces and curves. In preparation.
- [17] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. 2010, arXiv:math-NT/1006.1002v2.
- [18] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. 2010, arXiv:math-NT/1007.0052.
- [19] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorem and second order terms. 2010, arXiv:math-NT/1005.0672v3.
- [20] M. Bhargava and A. Shnidman. On the number of cubic orders of bounded discriminant having automorphism group C_3 , and related problems. 2012, arXiv:math-NT/1206.4746.

- [21] M. Bhargava, T. Taniguchi, and F. Thorne. Secondary terms in counting functions for cubic fields, II. 2012, In preparation.
- [22] M. Boij and J. Söderberg. Graded Betti numbers of Cohen-Macaulay modules and the multiplicity conjecture. *J. London Math. Soc. (2)*, 78(1):78–101, 2008.
- [23] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [24] R. Brauer. On the Zeta-Function of Algebraic Number Fields. *Amer. J. Math.*, 69:243–250, 1947.
- [25] D. Buchsbaum and D. Eisenbud. Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3. *Amer. J. Math.*, 99(3):447–485, 1977.
- [26] D.A. Buchsbaum and D. Rim. A generalized Koszul complex II. Depth and multiplicity. *Trans. Amer. Math. Soc.*, 111:197–224, 1964.
- [27] C.J. Bushnell and I. Reiner. Zeta functions of arithmetic orders and Solomon’s Conjecture. *Math. Z.*, 173:135–161, 1980.
- [28] C.J. Bushnell and I. Reiner. L -functions of arithmetic orders and asymptotic distribution of ideals. *J. Reine Angew. Math.*, 327:156–183, 1981.
- [29] C.J. Bushnell and I. Reiner. A survey of analytic methods in noncommutative number theory. In *Orders and their applications*, volume 1142 of *Lecture Notes in Math.*, pages 50–87, Oberwolfach (1984), 1985.
- [30] G. Casnati. Covers of algebraic varieties IV. A Bertini theorem for scandinavian covers. *Forum Math.*, pages 21–36, 2001.

- [31] G. Casnati and T. Ekedahl. Covers of algebraic varieties I. A general structure theorem, covers of degree 3,4 and Enriques' surfaces. *J. Algebraic Geom.*, 5:439–460, 1996.
- [32] K. Chandrasekharan and R. Narasimhan. On Hecke's functional equation. *Bull. Amer. Math. Soc.*, 67(2):182–185, 1961.
- [33] K. Chanrasekharan and R. Narasimhan. Functional equations with multiple gamma factors and the average order of arithmetical functions. *Ann. Math. (2)*, 76:93–136, 1962.
- [34] I. Ciocan-Fontanine and M. Kapranov. Derived Hilbert Schemes. *J. Amer. Math. Soc.*, 15(4):787–815, 2002.
- [35] H. Cohn. *Advanced Number Theory*. Dover, 1980.
- [36] D.A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, 1989.
- [37] B. Datskovsky and D.J. Wright. Density of discriminants of cubic extensions. *J. Reine Angew. Math.*, 386:116–138, 1988.
- [38] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, s1-26(3), 1951.
- [39] H. Davenport. On the class-number of binary cubic forms I and II. *J. Lon. Math. Soc.*, 26:183–198, 1951.
- [40] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields II. *Proc. Roy. Soc. Lon. Ser. A*, 322(1551):405–420, 1971.
- [41] P. Deligne. Letter to M. Bhargava, March 2004.
- [42] B.N. Delone and D.K. Fadeev. *The Theory of Irrationalities of the Third Degree*. Number 10 in Translations of Mathematical Monographs. A.M.S., 1964.

- [43] J.A. Eagon and D.G. Northcott. Ideals defined by matrices and a certain complex associated with them. *Proc. Royal Soc. A*, 269:188–204, 1962.
- [44] B. Edixhoven. Letter to M. Bhargava, 2006, <http://www.math.leidenuniv.nl/~jbrakenh/lowrank/6points.pdf>.
- [45] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Number 150 in Graduate Texts in Mathematics. Springer, 1995.
- [46] D. Eisenbud. *The Geometry of Syzygies*, volume 229 of *Graduate Texts in Mathematics*. Springer, 1 edition, 2005.
- [47] D. Eisenbud and J. Harris. On varieties of minimal degree, 1987.
- [48] D. Eisenbud and F.-O. Schreyer. Betti numbers of graded modules and cohomology of vector bundles. *J. Amer. Math. Soc.*, 22(3):859–888, 2009.
- [49] D. Eisenbud, G. Fløystad, and J. Weyman. The existence of equivariant pure free resolutions. *Ann. Inst. Fourier*, 61(3), 2011.
- [50] J. Ellenberg and A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, pages 723–741, 2006.
- [51] J. Ellenberg and A. Venkatesh. Statistics of number fields and function fields. In *Proceedings of the ICM*, 2010.
- [52] P.D.T.A. Elliot. The distribution of the quadratic class number. *Livotsk. Mat.Sb.*, 10:189–197, 1970.
- [53] T. Fujita. Classification of projective varieties of Δ -genus one. *Proc. Japan Acad. Ser. A Math. Sci.*, 58(3):113–116, 1982.
- [54] W. Fulton and J. Harris. *Representation Theory: A First Course*. Number 129 in Graduate Texts in Mathematics. Springer, 1991.

- [55] W.-T. Gan, B.H. Gross, and G. Savin. Fourier coefficients of modular forms on G_2 . *Duke Math. J.*, 115:105–169, 2002.
- [56] X. Gao. On the zeta function associated with module classes of a number field. *J. Number Theory*, 131:994–1019, 2011.
- [57] D. Garton. *Random matrices and the Cohen–Lenstra heuristics*. PhD thesis, University of Wisconsin–Madison, 2012.
- [58] D. Goldfeld and J. Hoffstein. Eisenstein series of $\frac{1}{2}$ -integral weight and the mean value of real Dirichlet series. *Invent. Math.*, 80(2):185–208, 1985.
- [59] E.H. Gover. Multiplicative Structures of generalized Koszul complexes. *Trans. Amer. Math. Soc.*, 185:287–307, 1973.
- [60] A. Granville and K. Soundararajan. The distribution of values of $L(1, \chi_d)$. *Geom. funct. anal.*, 13:992–1028, 2003.
- [61] Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at <http://www.math.uiuc.edu/Macaulay2/>.
- [62] B. Green. Functional equations for zeta functions of non-Gorenstein orders in global fields. *Manuscripta Math.*, 64(4):485–502, 1989.
- [63] M. Green and R. Lazarsfeld. Some results on the syzygies of finite sets and algebraic curves. *Composito Math.*, 67(3):301–314, 1988.
- [64] G.H. Hardy. *Divergent Series*. American Mathematical Society, 2 edition, 1992.
- [65] R. Hartshorne. Complete intersections and connectedness. *Amer. J. Math.*, 84(3):497–508, 1962.
- [66] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

- [67] W. Ho. *Orbit Parameterizations of Curves*. PhD thesis, Princeton University, 2009.
- [68] L.T. Hoa. On minimal free resolutions of projective varieties of degree = codimension +2. *J. Pure Appl. Algebra*, 87(3):241–250, 1993.
- [69] L.T. Hoa, J. Stückrad, and W. Vogel. Towards a structure theory for projective varieties of degree = codimension +2. *J. Pure and Appl. Algebra*, 71:203–231, 1991.
- [70] B. Howard, J. Millson, A. Snowden, and R. Vakil. A description of the outer automorphism of S_6 , and the invariants of six points in projective space. *J. Combin. Theory Ser. A*, 115:1296–1303, 2008.
- [71] M. Kontsevich. Enumeration of rational curves via torus actions. In R. Dijkgraaf, C. Faber, and G. van der Geer, editors, *The Moduli Space of Curves*, pages 335–368. Birkhauser, 1995.
- [72] M. Kontsevich and Y. Soibelman. Notes on A_∞ -algebras, A_∞ -categories, and Non-Commutative Geometry. In *Homological Mirror Symmetry*, volume 757/2009 of *Lecture Notes in Physics*, pages 1–67. Springer, 2009, arXiv:math.RA/0606241v2.
- [73] E. Kowalski and P. Michel. Zeros of families of automorphic L -functions close to 1. *Pacific J. Math.*, (2):411–431, 2002.
- [74] C. Kumar, P. Singh, and A. Kumar. Nearly extremal Cohen–Macaulay and Gorenstein algebras. *Bull. Austral. Math. Soc.*, 75:211–220, 2007.
- [75] A.R. Kustin and M. Miller. Algebra structures on minimal resolutions of Gorenstein rings of embedding codimension four. *Math. Z.*, 173(2):171–184, 1980.
- [76] A.R. Kustin and M. Miller. A general resolution for grade four Gorenstein ideals. *Manuscripta Math.*, 35(1–2):221–269, 1981.

- [77] A.R. Kustin and M. Miller. Algebra structures on minimal resolutions of Gorenstein rings. In *Commutative algebra*, volume 68 of *Lect. Notes in Pure and Appl Math.*, pages 45–65, Fairfax, Va. (1979), 1982. Dekker.
- [78] A.R. Kustin and M. Miller. Structure theory for a class of grade four Gorenstein ideals. *Trans. Amer. Math. Soc.*, 270(1):287–307, 1982.
- [79] A.R. Kustin and M. Miller. Multiplicative structure on resolutions of algebras defined by Herzog ideals. *J. London Math. Soc. (2)*, 28(2):247–260, 1983.
- [80] A.R. Kustin and M. Miller. Classification of the Tor-algebras of codimension four Gorenstein local rings. *Math. Z.*, 190(3):341–355, 1985.
- [81] A. Kuznetsov. Homological Projective Duality. *Publ. Math.*, 105(1):157–220, 2007.
- [82] E. Landau. Zur analytischen Zahlentheorie der definiten quadratischen Formen. (Über die Gitterpunkte in einem mehrdimensionalen Ellipsoid.). *Berliner Akademieberichte*, pages 458–476, 1915.
- [83] S. Mac Lane. *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. 2 edition, 1998.
- [84] R. Langlands. The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups. In *Algebraic Subgroups and Discontinuous Subgroups*, Proceedings of Symposia in Pure Mathematics IX, pages 143–148. American Mathematical Society, 1966.
- [85] R. Langlands. *Base change for $GL(2)$* , volume 96 of *Ann. Math. Studies*. Princeton University Press, 1980.
- [86] A. Lascoux. Young’s representations of the symmetric groups. 2000, <http://phalanstere.univ-mlv.fr/~al/ARTICLES/ProcCrac.ps.gz>.

- [87] A.F. Lavrik. The Siegel-Brauer Theorem concerning parameters of algebraic number fields. *Math. Notes*, pages 615–617, 1971.
- [88] F. Levi. Kubische Zahlkörper und binre kubische Formenklassen. *Leipz. Ber.*, 66:26–37, 1914.
- [89] W. Luo. Values of symmetric square L -functions at 1. *J. reine angew. Math.*, 506:215–235, 1999.
- [90] G. Malle. On the distribution of Galois groups II. *Experiment. Math.*, 13:129–135, 2004.
- [91] F. Mertens. Über einige asymptotische Gesetze der Zahlentheorie. *J. reine angew. Math.*, 77:289–338, 1874.
- [92] J. Nakagawa. *Orders of a Quartic Field*, volume 122 of *Mem. Amer. Math. Soc.* American Mathematical Society, 1996.
- [93] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1999.
- [94] R. Pelikaan. Multiplicative structures on the resolution of determinantal rings. *Proc. Konink. Ned. Ac. Wetens. A*, 92:471–478, 1989.
- [95] B. Poonen. The moduli space of commutative algebras of finite rank. *J. Euro. Math. Soc.*, 10(3):817–836, 2008.
- [96] J.W. Sands. Generalization of a theorem of Siegel. *Acta Arith.*, 58(1):47–57, 1991.
- [97] M. Sato and T. Kimura. A classification of irreducible prehomogeneous vector spaces and their relative invariants. *Nagoya Math Journal*, 65:1–155, 1977.
- [98] P. Schenzel. Über die Freien Auflösungen extremaler Cohen–Macaulay-Ringe. *J. Algebra*, 64:93–101, 1980.

- [99] P. Seidel. *Fukaya Categories and Picard-Lefschetz Theory*. Zurich Lectures in Advanced Mathematics. European Math. Soc., 2008.
- [100] C.L. Siegel. Abschätzung von Einheiten. *Ges. Abh. IV*, pages 66–81.
- [101] C.L. Siegel. The average measure of quadratic forms with given determinant and signature. *Ann. Math. (2)*, 45(4):667–685, 1944.
- [102] W. Specht. Die irreduziblen Darstellungen der symmetrischen Gruppe. *Math. Z.*, 39(1):696–711, 1935.
- [103] H. Srinivasan. Algebra structures on some canonical resolutions. *J. Algebra*, 122(1):150–187, 1989.
- [104] R. Stanley. Hilbert Functions of Graded Algebras. *Adv. Math.*, 28:57–83, 1978.
- [105] W. A. Stein et al. *Sage Mathematics Software (Version 5.0.0)*. The Sage Development Team, 2012. <http://www.sagemath.org>.
- [106] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. 2011, arXiv:math-NT/1102.2914.
- [107] J. Tunnell. Artin’s conjecture for representations of octahedral type. *Bull. American Math. Soc.*, 5:173–175, 1981.
- [108] A.M. Vershik and A.Yu. Okounkov. A new approach to the representation theory of the symmetric groups. II. *Zap. Nauchn. Sem. POMI*, 307:57–98, 2004.
- [109] A. Walfisz. Über die Koeffizientensummen einiger Modulformen. *Math. Ann.*, 108:75–90, 1933.
- [110] C. Weibel. *An Introduction to Homological Algebra*. Cambridge University Press, 1995.

- [111] Melanie Wood. *Moduli Spaces for Rings and Ideals*. PhD thesis, Princeton University, 2009.
- [112] M.M. Wood. Parametrization of ideal classes in rings associated to binary forms. 2010, arXiv:math-NT/1008.4781.
- [113] M.M. Wood. Quartic Rings Associated to Binary Quartic Forms. *Int. Math. Res. Not.*, 2011.
- [114] M.M. Wood. Rings and ideals parametrized by binary n -ic forms. *J. Lon. Math. Soc. (2)*, 83:208–231, 2011.
- [115] D.J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58:17–50, 1989.
- [116] D.J. Wright and A. Yukie. Prehomogeneous vector spaces and field extensions. *Invent. Math.*, 110:283–314, 1992.