The Equidistribution of Lattice Shapes of Rings of Integers of Cubic, Quartic, and Quintic Number Fields: an Artist's Rendering

Based on the original story by Manjul Bhargava and Piper Harron

Piper Alexis Harron

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 2016

Abstract

A fascinating tale of mayhem, mystery, and mathematics. Attached to each degree n number field is a rank $n-1$ lattice called its shape. This thesis shows that the shapes of S_n-number fields (of degree $n = 3, 4$, or 5) become equidistributed as the absolute discriminant of the number field goes to infinity. The result for $n = 3$ is due to David Terr. Here, we provide a unified proof for $n = 3, 4$, and 5 based on the parametrizations of low rank rings due to Bhargava and Delone–Faddeev. We do not assume any of those words make any kind of sense, though we do make certain assumptions about how much time the reader has on her hands and what kind of sense of humor she has.

Acknowledgements

In the early 1800s when this journey first began, I was but a young and naive graduate student. Centuries later, I am a wife, mother of two, and dare I say, mathematician.

I would like to thank my advisor, Manjul Bhargava, for being in the graduate lounge for Must See TV, for giving me this problem to work on, for guidance, and, of course, patience. I would also like to thank Melanie Matchett Wood for being my local, informal advisor, without whom my thesis may never have survived my relocation and new-motherhood.

Along the way, I've also had helpful math conversations with Wei Ho, Elena Fuchs, Lillian Pierce, and Jordan Ellenberg, and much thesis-related-non-mathematical help from Sarah LeMieux, Amy Lee, and Arielle Henderson. Special mention goes to Amanda Town and David Ellwood for providing re-inspiration at a particularly vulnerable stage.

More important than the math, though, was probably my sanity, kept up by various friends, family, and while at Princeton, a certain underground establishment of distilled and fermented beverages. Though I can't trace it back to them, I'd like to thank my parents, Lois and Arthur, for giving me whatever random assortment of qualities led to my commitment to honesty-in-math which explains the somewhat silly, as in unserious yet mathematically sound, nature of this thesis.

Finally, I'd like to thank my husband, Robert Harron, for always being at the aforementioned underground establishment, for being a night owl, for being a number theorist, for being an informal advisor, for being an unpaid copy-editor, for increasing the amount of truth in my thesis, and all sorts of help with everything. (I would thank the children, but frankly, they've been no help.)

To Alex and Julien who were born (three years apart) during the making of this.

Contents

Prologue

Respected research math is dominated by men of a certain attitude. Even allowing for individual variation, there is still a tendency towards an oppressive atmosphere, which is carefully maintained and even championed by those who find it conducive to success. As any good grad student would do, I tried to fit in, mathematically. I absorbed the atmosphere and took attitudes to heart. I was miserable, and on the verge of failure. The problem was not individuals, but a system of self-preservation that, from the outside, feels like a long string of betrayals, some big, some small, perpetrated by your only support system. When I physically removed myself from the situation, I did not know where I was or what to do. First thought: FREEDOM!!!! Second thought: but what about the others like me, who don't do math the "right way" but could still greatly contribute to the community? I combined those two thoughts and started from zero on my thesis. What resulted was a thesis written for those who do not feel that they are encouraged to be themselves. People who, for instance, try to read a math paper and think, "Oh my goodness what on earth does any of this mean why can't they just say what they mean????" rather than, "Ah, what lovely results!" (I can't even pretend to know how "normal" mathematicians feel when they read math, but I know it's not how I feel.) My thesis is, in many ways, not very serious, sometimes sarcastic, brutally honest, and very me. It is my art. It is myself. It is also as mathematically complete as I could honestly make it.

I'm unwilling to pretend that all manner of ways of thinking are equally encouraged, or that there aren't very real issues of lack of diversity. It is not my place to make the system comfortable with itself. This may be challenging for happy mathematicians to read through; my only hope is that the challenge is accepted.

Chapter 1

I will always be honest with you.

Introduction

1.1 Notes to My Dear Reader(s)

1.1.1 The Layperson: Math 101

The hardest part about math is the level of abstraction required. We have innate logical abilities, but they are based in context. If you give people a scenario of university students drinking beverages at a bar and give them information either about the person's age or about the person's beverage, most people know instinctively which students' drinks or IDs need to be checked to avoid underaged drinking (i.e., if the person's 22 you don't care what they're drinking, but if the person has a vodka tonic, you need to know their age). Take the logically equivalent situation of cards with a color on one side and a number on the other. Suddenly it takes some work to figure out which cards have to be turned over to satisfy a given condition (say, all even numbers have red on the back). Just one level of abstraction and the untrained, but educated, person will have a good amount of difficulty even understanding the situation. Now try doing Number Theory.

I like to imagine abstraction (abstractly ha ha ha) as pulling the strings on a marionette. The marionette, being "real life," is easily accessible. Everyone understands the marionette whether it's walking or dancing or fighting. We can see it and it makes sense. But watch instead the hands of the puppeteers. Can you look at the hand movements of the puppeteers and know what the marionette is doing? A puppeteer walks up to you and says "I'm really excited about figuring out Fermat's Last Thumb Bend!" You say, "huh?" The puppeteer responds, "Oh, well, it's simply a matter of realizing that the main thumb joint has several properties that distinguish it from..." You're already starting to fantasize about the Zombie Apocalypse. Imagine it gets worse. Much, much worse. Imagine that the marionettes we see are controlled by marionettoids we don't see which are in turn controlled by pre-puppeteers which are finally controlled by actual puppeteers. NEVER HAVE A CONVERSATION WITH THESE FICTIONAL ACTUAL PUPPETEERS ABOUT THEIR WORK!

I spent years trying to fake puppeteer lingo, but I have officially given up. My goal here is to write something that I can understand and remember and talk about with my non-puppeteer friends and family, which will allow me to speak my own language to the puppeteers. To you, the lay reader, I recommend reading this introduction and then starting each subsection of laysplanations (the .1s) and reading until you hit your mathiness threshold (stopping to think or write something down is encouraged; even math you know won't necessarily make sense at the speed at which you can read and understand non-math), then skim/skip to the next lay portion. Depending on how you feel with that, you should look at the math parts (the .2s) which will look familiar if you were able to finish the lay sections. I can't promise they'll make sense, but things should be vaguely readable. Maybe. The weeds (the .3s) contain extra information (some lay, some math) and calculations, more for answering questions than for reading. Enter at your own peril.

1.1.2 The Initiated

Welcome mathy friend! Depending on the extent of your initiation (and your sense of humor), this thesis may be exactly what you've always wanted to read! Skim the laysplanations (.1s), but if they are too math-less for you, it's okay to only read the math sections (.2s) and just go back to the lay stuff if necessary (several things are introduced/motivated in the laysplanations, including explanations of my Formula in the .1.1s). You may also be interested in the weeds (.3s) which are appendices with things that weren't strictly necessary to get through the proof of the Main Theorem, but were necessary personally for me to get a hold of things. The weeds aren't to be read straight through, but you might find an explicit calculation or extra explanation there.

1.1.3 The Mathematician

Dear Professor, thank you for showing interest in my thesis! Your introduction awaits at §1.3. For results, however, you may find the fluffless arxived original [BH13] easier to read (certainly quicker!) than this thesis.

1.2 This Thesis (Problem) 101: A Mostly Layscape

Every thesis is a question and (very long) answer. My question in layspeak is: “How many” “shapes” of certain degree n “number fields” are there?

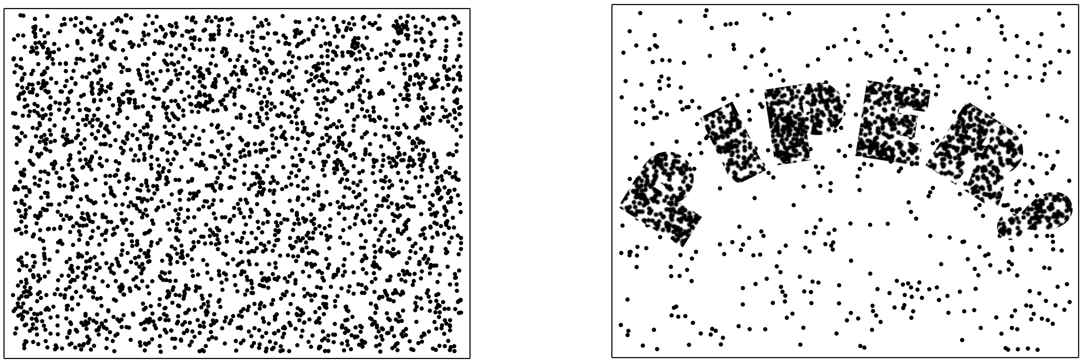
The naive short answer is: Infinitely many! But of course, though true, that is not nearly enough information. What we will show is that the infinitely many shapes we find are actually “equidistributed” with respect to the “space of shapes.” In other words, if you think of the collection of possible shapes as being a blob (a “space”), then wherever you look in this blob, you will find shapes of number fields in equal quantity.

Equivalently, though somewhat less to my liking, a thesis is a claim and a (very long) proof. My equivalent claim in layspeak is: “Shapes” of certain degree n “number fields” become “equidistributed” when ordered by “absolute discriminant.”

In what follows I hope to do enough “**laysplanations**” to make the whole argument approximately readable by approximately anyone. Approximately. In addition to laysplaining and “**mathsplaining**,” I will also, where appropriate and not too horrifying, have some “**weedsplanations**” where I wade into the weeds with examples and explicit calculations, sometimes with extra laysplanations that were not strictly necessary to the main argument.

1.2.1 How many (and Equidistribution)

As I mentioned, we aren’t merely counting things. There are infinitely many number fields, and the aforementioned “equal quantity” of shapes anywhere in our blob of shapes is also infinite, but this tells us little. In general, “infinity” is considered a rather crappy answer to the question of “how many?” You know what “equals” infinity? $\infty, \infty^2, \infty^{10}, ..., \infty^{\infty}$! Or maybe there’s secret information contained inside your ∞. Maybe “how many” is actually related to some X which just happens to be going to infinity. Then your “how many” may look like X or X^2 or (SPOILER ALERT) $KX + o(X)$ as $X \to \infty$, for example. This tells you how quickly “how many” goes to infinity. Additionally, if what you are counting looks like points in a blob, you may also be able to tell whether the points are equidistributed (i.e., if you look at half the blob by volume, have you gotten half the points? And is this true for any sized subregion?). So when we ask “how many?” we really mean “how many, and how?”



(a) Equidistributed.

(b) Not equidistributed!

Figure 1.1: Equidistribution versus non-equidistribution (with respect to the normal measure you put on a two-dimensional sheet of paper).

1.2.2 Shapes of S_n-Number Fields

How many (and how) whats? Shapes of S_n-number fields of fixed degree $n = 3$, 4, or 5. What a number field is doesn’t matter so much right now, but it is an extension (of degree n) of the rational numbers. For instance, the rational numbers with the square root of 3 added to it is a degree 2 number field (by which I mean that in the rational numbers you’re allowed to add and subtract, multiply and divide, and now you’re also allowed to multiply things by root 3 and then also add and subtract, multiply and divide). There’s a way in which you can “act” on a number field by a specific group and they will tell you this is related to its “symmetry” and expect you to understand immediately what that means. I am not a fan of allusions to abstract “symmetry,” but at any rate, S_n is the largest and least “symmetric” such group.

We don’t use any aspect of S_n-ness here, so it’s okay if you don’t understand its precise definition, which is as follows: a number field is called an S_n-number field if its Galois closure has Galois group S_n (as opposed to it being a subgroup of S_n which would imply potential “extra symmetry.”) In the case of $n = 4$ it is actually important that we restrict ourselves to “S_4-quartic rings”. For $n = 3, 5$ it doesn’t matter either way, so altogether we'll say we're looking at "S_n" number fields. For what it's worth, I know I'm not being informative right now.

Moving on. Given a number field, K, of degree n, let's look at its unique maximal order $\mathcal{O}_K$, its ring of integers. Regardless of what any of that means, $\mathcal{O}_K$ can be viewed as a lattice (dots evenly spaced in each direction, very orderly, a repeated pattern), and as such, we can talk about the shape of this repeated pattern (and the shape of a number field will be defined to be the shape of its ring of integers). In fact any "non-degenerate" (non-useless) "rank n ring" is a lattice for which we may define a shape, and that's what we'll actually be looking at. A subring of a (number) field may or may not be a rank n ring, and a rank n ring may or may not be an order in a number field, but at the end of the day we'll have used rank n rings to get information on maximal orders in number fields, and thus the number fields themselves.

Getting back to lattices and shapes, let's look at a two-dimensional lattice generated by vectors **u** and **v**.

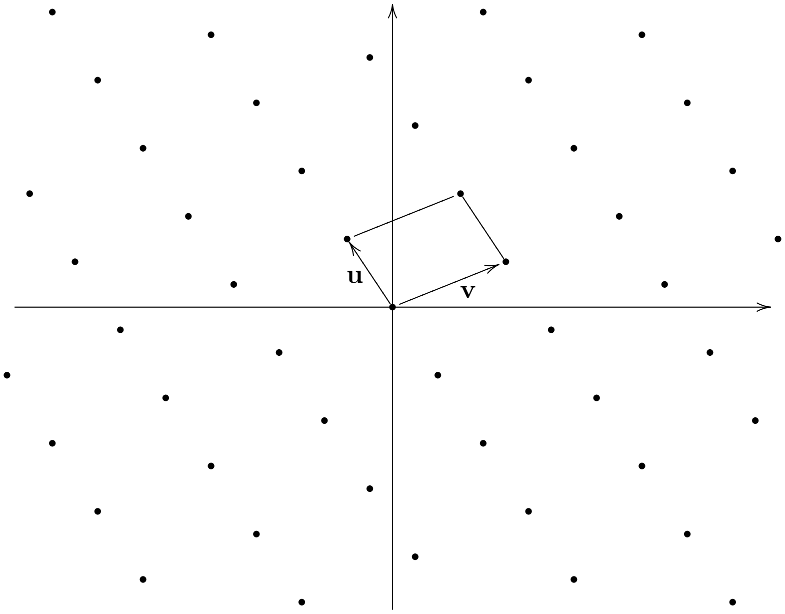


Figure 1.2: A two-dimensional lattice generated by vectors **u** and **v**.

Our first notion of shape would then be to describe the fundamental domain, i.e., the parallelogram determined by **u** and **v**. It might be square, rectangular with a specific height:width ratio, or just some other parallelogram. Now, we know that two squares have the same shape (square!) no matter their size, whether we look directly or at a reflection, and if we ignore the word "diamond" we know that a rotated square is still a square. So when we are counting shapes, we will ignore shapes that differ from ones we've counted only because of scaling, rotation, or reflection. We will also ignore shapes from rings that we know to be "equivalent" to rings already accounted for.

Since we are looking at orders and not just lattices, we have one more piece of information to throw away. Namely, all of our orders will have a $\mathbb{Z}$ component, i.e., as lattices they all have a common generator: the number $\mathbf{1}$. No good can come from keeping this around, so we will get rid of it by "projecting onto the orthogonal complement of $\mathbf{1}$." This will give us an $(n-1)$-dimensional lattice we can then find the shape of. If you use the fact that you can put generating vectors into a matrix that then represents that lattice, it makes sense that projecting and modding out by things still leaves us with a (now $(n-1) \times (n-1)$) matrix. (This matrix will often be represented by a symmetric matrix if written explicitly, for convenience/math reasons, but that is not to say that the shape "is" a symmetric matrix.) If all we had to go on were the words "square," "this kind of rectangle," and "that other kind of rectangle" we would be out of luck trying to learn anything about the number or frequency of shapes, let alone figuring out what "distribution" would mean. Since we can define the shape as a matrix (or a form) though, this means we have a space of shapes in which we can take volumes and count points. The shapes we care about will be some collection of points, so you can imagine a blob in $\mathbb{R}^2$ and counting points there.

In real life, the shape is an associated, restricted form do-hickey viewed as living in a doubly quotiented matrix group, which is more mathy, but far less motivating to those who don't already know this stuff. (And I assume anyone who already knows this stuff is not reading this section too closely, unless explicitly requested by me (Thanks!!!).)

1.2.3 Volume

To make sense of equidistribution we will need a notion of size. For our space of shapes, we will have something called a "measure," and for the regions where we will be doing our counting, we will have our more normal understanding of volume. The measure on our space of shapes is the one that makes sense, and it gives us that the space of shapes has a finite measure.

1.2.4 I said, Hey, What's Going On?

Fix $n = 3, 4$, or 5. We have infinitely many isomorphism classes of S_n-number fields of degree n. To each isomorphism class of number fields, we associate a point in the space, $\mathcal{S}_{n-1}$, of shapes. We order everything with respect to the "absolute discriminant" (meaning, we impose the condition that the absolute value of the discriminant be less than a bound, X) and we want to see how the shapes are distributed. To prove equidistribution, we will need to show that if you take any "nice" region W of $\mathcal{S}_{n-1}$, then

$$\frac{\#\text{ of fields with shape in } W}{\text{total }\#\text{ of fields (so shape is anywhere in } \mathcal{S}_{n-1})} = \frac{\text{size of } W}{\text{size of } \mathcal{S}_{n-1}} \text{ as } X \to \infty.$$

In other words, if you look at a region W of the blob $\mathcal{S}_{n-1}$, the number of points in W only depends on how big W is, not where it is or what it looks like.

1.3 In Mathiness We Trust

From [BH13], the goal of this thesis is to prove the following:

Theorem 1. *For $n = 3$, 4, and 5, when isomorphism classes of S_n-number fields of degree n are ordered by their absolute discriminants, the lattice shapes of the rings of integers in these fields become equidistributed in the space of shapes as the discriminant goes to infinity.*

Let's define all the terms. A number field is called an S_n-number field if its associated Galois group is S_n (you look at the Galois group of the Galois closure of the number field; it is either all of S_n or a subgroup of S_n). For a lattice, L, in Euclidean space $\mathbb{R}^n$, you can explicitly define its shape to be in $\mathrm{GL}_n(\mathbb{Z})\backslash \mathrm{GL}_n(\mathbb{R})/\mathrm{GO}_n(\mathbb{R})$, by taking a basis of L and putting those vectors as the rows of a matrix B, then forming the double-coset $\mathrm{GL}_n(\mathbb{Z})B\,\mathrm{GO}_n(\mathbb{R})$. (This makes sense because $\mathrm{GL}_n(\mathbb{Z})$ takes care of changing the basis of the lattice, and we only care about the lattice shape up to scaling by $\mathbb{R}^\times$, rotations and reflections.) Given a number field, K, use Minkowski theory to embed K into real space, $j : K \hookrightarrow \mathbb{R}^n$. Then $j(\mathcal{O}_K)$ is now a lattice in Euclidean space whose first component is determined by $j(1)$. Projecting onto the orthogonal complement of $j(1)$ gets rid of that first component all rings of integers have in common, and we're left with $j(\mathcal{O}_K)^\perp$ which is a lattice in $\mathbb{R}^{n-1}$. We define the shape of K to be the shape of $\mathcal{O}_K^\perp$ (suppressing the j notation). The space of shapes is thus $\mathcal{S}_{n-1} := \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathrm{GO}_{n-1}(\mathbb{R})$. There is a natural measure, μ, on $\mathcal{S}_{n-1}$ obtained from the Haar measure on $\mathrm{GL}_{n-1}(\mathbb{R})$ and $\mathrm{GO}_{n-1}(\mathbb{R})$, and it is a classical result of Minkowski that $\mu(\mathcal{S}_{n-1})$ is finite. (Alternatively, you can get the shape by taking the natural quadratic form on $\mathcal{O}_K$, $q(x) := \langle j(x), j(x)\rangle$, and restricting q to $\{x \in \mathbb{Z} + n\mathcal{O}_K : \mathrm{Tr}_{\mathbb{Q}}^{K}(x) = 0\}$.)

The theorem, more precisely and directly from [BH13], says that for $n = 3$, 4, or 5, let $N_n^{(i)}(X)$ denote the number of isomorphism classes of n-ic fields having i pairs of complex embeddings, associated Galois group S_n, and absolute discriminant less than X. Also, for a measurable subset $W \subseteq \mathcal{S}_{n-1}$ whose boundary has measure 0, let $N_n^{(i)}(X, W)$ denote the number of isomorphism classes of n-ic fields having i pairs of complex embeddings, associated Galois group S_n, absolute discriminant less than X, and ring of integers with shape in W. Then, we prove that

$$\lim_{X\to\infty} \frac{N_n^{(i)}(X, W)}{N_n^{(i)}(X)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}. \tag{1.1}$$

The condition that the associated Galois group be S_n may be dropped in Theorem 1 in the cases $n = 3$ and $n = 5$, since 100% of all cubic fields (resp. quintic fields), when ordered by discriminant, have associated Galois group S_3 (resp. S_5). However, the condition is needed in the case $n = 4$, as the Galois group S_4 does *not* occur with density 1 among all quartic fields when ordered by discriminant. Indeed, about 9.356% of all quartic fields have associated Galois group D_4 rather than S_4, and the lattice shapes of the rings of integers in D_4-quartic fields cannot be equidistributed, as is easily seen. For example, note that if K is a D_4-quartic field, then K has a nontrivial automorphism of order 2 which means that $\mathcal{O}_K$ does too, as does its underlying lattice. It is an interesting problem to determine the distribution of lattice shapes for n-ic number fields having a given non-generic (i.e., non-S_n) associated Galois group, even heuristically. For the simple answer in the case of C_3-cubic number fields, and related results, see [BS14]. In the general case of associated Galois group S_n, we naturally conjecture that Theorem 1 is true for all values of n.

1.4 Very Interesting, Or Is It?

What I wanted for this section was to explain why mathematicians might find this interesting. Am I not a mathematician? Could I not simply tell you why I find it interesting? Well... people tell me I'm weird, and I believe them because I put a comic strip in my math thesis. For me to find something interesting, I have to have prior knowledge of it or something related. I just don't have the necessary experience with math, outside of this thesis, to find abstract research-level math "interesting." So, I had to ask around.

This thesis is about number fields. Number fields count as Amazingly Interesting (to number theorists). Anytime you can prove something about number fields, there's a very good chance it will be considered at least somewhat interesting, so, already we're off to a good start. But what do we prove? That shapes are equidistributed. Hmm, what? The shape of a number field is some kind of fundamental description of the structure (the look, if you will) of its underlying (maximal) lattice. Saying shape is equidistributed is like saying it's totally random. Other than the potential for tweeting "S_n # fields = soooo #Random!! #Shapes #NailedIt," why do we care? As my husband says, it means there's nothing going on. Now, when I heard that, I thought he was telling me my result wasn't interesting at all, but proving that nothing else is going on with S_n-number fields is not nothing. Indeed it can be interpreted as a quantitative statement of the qualitative feeling that S_n-number fields are in fact sooo random. #OohThatISInteresting!

1.5 The Proof 101 (Structure of Thesis Paper)

How we do this is a whole nother (sic) thing!

1.5.1 Historical Truths and That Time I Was Wrong

A first question to be asked might be "What has already been done?" Without the shape condition, the question of "how many (and how)" S_n-number fields are there (ordered by discriminant) has already been answered for $n = 3, 4, 5$. In each case, the first step was a parametrization that allows you to look at forms instead of number fields [DF64, Bha04, Bha08]. Counting results were done in [Dav51b, Dav51c, DH71, Bha05, Bha10]. With the shape condition, the question was answered in [Ter97] for $n = 3$. (I should also note that in [BST13] they rewrite things we need for $n = 3$ from [Dav51b, Dav51c, DH71, DF64] in an easier-to-use way so I often use that reference for myself.)

What does that give us? Well, first, I thought I was supposed to read Terr's thesis [Ter97] and magically generalize it to $n = 4$ (the case I worked on). This was folly. Then, I thought I was supposed to rewrite [Bha05] adding "and shape in W" everywhere. This is what I did and I alternated between feeling the task was impossibly hard and trivially, plagiarizingly easy (common feelings for grad students). And then one day (and we won't say which day), my advisor tells me I should just "use" what is known and "make an argument" to prove my result. MIND = BLOWN.

1.5.2 A Map of the Math

What we want is to count number fields (ordered by discriminant, subject to certain conditions). Each number field has a unique maximal order (with same conditions). A maximal order is a rank n ring and we have nice discriminant-preserving parametrizations (Chapter 2) which allow us to look at forms instead of rank n rings (all conditions still hold). The parametrization doesn't keep track just of rings, but of rings paired with secondary rings ("resolvents") which will mess up our count, but the maximal orders we're interested in have unique resolvent rings anyway. What we need then (and what we have because otherwise, hello, we wouldn't be here) is a way to see the "corresponds to a maximal ring" condition on the forms side (Chapter 5), and also a way to count just these forms (Chapters 3 and 4), and for the count to work (Chapter 5). Each of these counts will lead us to volumes of specific regions which we will then have to calculate and relate to sizes inside the space of shapes (Chapter 6).

The Formula

I wanted to be able to put everything into one formula to see how the sections fit together, but the fact is, they don't. This is a formula for the proof, which is essentially Chapter 5, but you'll see in the breakdown that other work goes into it. (I did create a formula that went out of its way to incorporate all the sections but it was longer and not necessarily illuminating.)

$$\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)} = \frac{\lim\limits_{Y\to\infty} N^{(i)}\left(\bigcap\limits_{p<Y} U_p; X, W\right)}{\lim\limits_{Y\to\infty} N^{(i)}\left(\bigcap\limits_{p<Y} U_p; X\right)} \xrightarrow[X\to\infty]{} \frac{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)}$$

$$= \frac{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)} = \frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$$

This formula is for a fixed $n = 3, 4, 5$. We use $N^{(i)}(\cdot)$ to indicate a count of isomorphism classes of S_n-rings or equivalence classes of irreducible forms (where the i indicates signature or orbit), and X or X, W

is used to indicate the conditions that the absolute discriminant is less than X with or without the additional condition that the shape is in W. Whenever there's a letter U, there's something maximal going on, and $\mathcal{R}$ is a region in the space of forms. The denominators are all already known and known to be equal (up to suppressed constants which cancel in the ratios). The formula will be repeated each chapter with the relevant terms defined.

The Outline

How it's gonna go down:

Ch. 2: Set up the parametrizations which allow us to look at forms in a vector space $V_{\mathbb{R}}$ instead of willy-nilly rank n rings. Add shape condition giving: $\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)}$.

Ch. 3: Set up our counting environment using fundamental domains and Iwasawa decomposition. Add shape condition. Get shape count for forms: $\frac{N(V_{\mathbb{Z}}^{(i)};\, X,W)}{N(V_{\mathbb{Z}}^{(i)};\, X)} \underset{X\to\infty}{\longrightarrow} \frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)}$, which is used implicitly any time we get an answer in terms of volumes. Get shape equidistribution result if we presume the postponed volume calculation that $\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$.

Ch. 4: Do analogous work for subsets of forms satisfying finitely many congruence conditions modulo prime powers (because that's step one to translating results to maximal orders and thus number fields). Get shape result for such sets (again presuming a volume calculation):

$$\frac{N^{(i)}(S;X,W)}{N^{(i)}(S;X)} = \frac{N(\bigcup_{j=1}^{k}(m\cdot V_{\mathbb{Z}}^{(i)});\, X,W)}{N(\bigcup_{j=1}^{k}(m.V_{\mathbb{Z}}^{(i)});\, X)} = \frac{\prod_p \mu_p(S)\cdot N(V_{\mathbb{Z}}^{(i)};\, X,W)}{\prod_p \mu_p(S)\cdot N(V_{\mathbb{Z}}^{(i)};\, X)} \underset{X\to\infty}{\longrightarrow} \frac{\prod_p \mu_p(S)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod_p \mu_p(S)\cdot \mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$$

Ch. 5: Use results over p plus a sieve to get shape result for maximal orders. Get main result (presuming the volume calculation):

$$\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)} = \frac{\lim_{Y\to\infty} N^{(i)}(\bigcap_{p<Y} U_p;X,W)}{\lim_{Y\to\infty} N^{(i)}(\bigcap_{p<Y} U_p;X)} \underset{X\to\infty}{\longrightarrow} \frac{\lim_{Y\to\infty}\prod_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\lim_{Y\to\infty}\prod_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)} = \frac{\prod_p \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod_p \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)}$$
$$= \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}.$$

Ch. 6: Calculate the volume already! $\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$.

Whatever any of that means!

[Editor's note: The author throws in many phrases that seem to indicate uncertainty; please know that this does not represent *mathematical* uncertainty, but is meant to relay the following to student readers: 1) you are not expected to understand every word as you read it, 2) you can successfully use math before you've successfully understood it, and 3) it has to be okay to be honest about your understanding. The author refused to sacrifice these messages or what she called her "integrity" for the sake of what we saw as very important mathematical credibility.]

Chapter 2

When darkness falls
And all that's known is still
When heartbeats fade
And warmth gives way to chill
Who will be left to sing?
The things, of course, the things!

Defining the Things

$$\boxed{\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)}} = \frac{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X, W)}{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X)} \underset{X\to\infty}{\longrightarrow} \frac{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)}$$

$$= \frac{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)} = \frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$$

2.1 The Layscape: Oh the Things You Will Know

Here's what I don't like about this chapter. In this chapter we introduce a **parametrization** and **group action** which keep track of conditions we will be looking at, **equivalence**, **S_n**-ness, **shape** and **discriminant**. Since we're all about counting, what I'd like to be able to tell you is that this parametrization allows us to count Something-We-Can-Count instead of What-We-Want-To-Count, but that's only almost true. Instead this parametrization allows us to count Something-We-Can-Count (Chapter 3) which is bigger than What-We-Want-To-Count and whose result we don't even use, per se. Instead we use the set up to count Other-Things-We-Can-Count which will then be whittled down (or sieved) to What-We-Want-To-Count (Chapter 5). Whew.

Each degree n number field has a unique maximal order which is a **ring of rank n**. Our parametrization relates rings of rank n to certain lattice points in a **vector space** (vector spaces being happy spaces for counting). We will be able to count the relevant vectors, but that will actually give us a number larger than the number of rank n rings, which itself is more than the number of maximal orders in number fields.

Here's what my husband doesn't like about this chapter. It's long. Long, long, long, long.

2.1.1 The Formula

What we want to count is isomorphism classes of S_n-number fields of degree n, with absolute discriminant bounded by X and with shape in W, and we will have to restrict ourselves to one "signature" at a time. For a fixed n, this is denoted in The Formula as $N^{(i)}(X; W)$ where the i keeps track of the signature. (The total count will just be the sum of the counts per signature.) For equidistribution results, this number must be compared with the count where all shapes are allowed, $N^{(i)}(X; \mathcal{S}_{n-1})$, which we denote $N^{(i)}(X)$.

Our parametrization in this section will give a bijection between isomorphism classes of rank n rings paired with a resolvent ring (of rank r) and equivalence classes of forms $v \in V_{\mathbb{Z}}$. Signatures on the rings side corresponds to "orbits" on the forms side. The nice thing about maximal rings (aside from corresponding to what we want to count) is that they have unique resolvent rings, so we can actually count them using our parametrization (provided we find a way to get to them). In Chapter 5, we define U to be the set of $v \in V_{\mathbb{Z}}$ such that the corresponding ring R is maximal. Thus, $N^{(i)}(U; \cdot)$ is the number of inequivalent forms, per orbit, corresponding to maximal orders (with discriminant and possibly shape conditions imposed) which will be equal to $N^{(i)}(\cdot)$.

2.1.2 So What If This Were All Just About Unicycles?

Parametrization and Group Work

Since having a toddler, I've found myself doing things I never used to do (because I would've found them boring) and discovering it's not always so easy. When your kid asks you to count the cars (by saying "dix! quatre!") it is not always obvious which cars to count, for instance (and don't get me started on what is a car and what is a truck). But my real problem comes when trying to count bicycles parked at a bicycle stand. Every time I count, I get a different number because it's hard for me to tell which parts belong to the bikes I've already counted. One possible solution would be to pick one easy-to-see bicycle part and only count that. Obvious choices would be handlebars, wheels, or seats. Imagine you had a way of seeing only the wheels or only the seats (I don't like handlebars; doesn't matter why), maybe because you have some really awesome spy computer sunglasses.

Okay, so you're undercover posing as a "natural mama" with your bilingual robot baby in the baby carrier when you have to stop and count bicycles. You press the screen of your spy phone (I almost said "on your watch" LOL) and now you see a black screen with a bunch of blue circles, each representing a wheel. A swipe of your screen puts all the circles in a row for easy counting. You count fifteen. Uh-oh! You look back at the actual bicycles and realize that they're not all bicycles! Not all of the things you want to count have exactly two wheels. So fifteen doesn't tell you anything. What about the seats? You inspect and find that yes, each ...cycle has exactly one seat. Okay, going back to your spy screen you switch to view red ovals that represent seats and you count seven. Seven something-cycles! In other words, for our purposes, cycles can be parametrized by seats. To understand the parametrizations, though, we're still missing some more information.

I had to manipulate my ovals in order to count them. In this case, that was certainly fine because all we cared about was the number and the number didn't change. If, for example, I wanted to keep track of how many wheels each velocipede (yes, there's a word for bicycle-oid) had, I could turn on the wheels screen and the seat screen at the same time and include little lines that connected each seat to the right number of wheels. Now if I mess with the seats in my screen by moving them around, I need to make sure the wheels move around too and are still connected in the right way. Otherwise, the information is lost. When dealing with only abstract objects, this manipulation might be a "group action" and making sure information doesn't get lost just amounts to being careful and having lots of definitions on hand.

But Can You Make This Ridiculous and Feature Unicycles??

Alright, let's get ridiculous. You live in a town where there's an annual Cycling Clown-Capades Rally. From all around the region, troupes of cycling clowns show up to put on a cycling show using bicycles, tricycles, bicycles with training wheels, and unicycles. When the clowns are not performing, their velocipedes are kept in a high-tech warehouse with useful sensors and a computer that keeps track of data. Of course. The night before the big event you enter the warehouse to get the final numbers and everything is an absolute mess and your computer has crashed and is generally unhappy.

Your first constructive thought is to check the inventory. You turn on your computer in Safe Mode (does that still exist?) and you only have access to some of your systems. You can pull up a screen that shows you one blue circle for each wheel in the room in its present location, but you can't get the seats to load. No chance of counting the inventory. Then you remember that each troupe has exactly one unicycle, so if you can find a way to just count unicycles, this will at least tell you whether all the clown troupes had arrived. You ask the computer to load whatever data hasn't been corrupted and you find that you can access the diameter of each wheel, and some numerical rating system you're not totally sure of called "clown points."

Immediately overwhelmed, you check Facebook to help you think. When you look up, someone is moving some of the bikes! Frantically you check your computer, but you see all the data is moving together and the clown points of the moved items aren't changing. "Whew!" you say, "I'm so glad clown points are invariant under relocation!" Now it's time to count. First, you decide to count all the wheels, just to check your count program is still working. A pop-up window opens and tells you that to count the velocipedes, you need to order them first and it asks with respect to what data you want to order them. You choose clown points. The program works and tells you there are 144 velocipedes. Now to get to the unicycles. Your program has a Sift button which can identify (using some data about the diameters) wheels not connected to any other wheels. Sift! Count! Boom! Twelve unicycles! Twelve clown troupes! Hooray!

Mapping The Analogy

What we had in real life (velocipedes) were our **rank n rings**, in the clown example the wheels were **resolvent rings**. On the screen we were looking at the **parametrization** of velocipedes by icons representing

vectors. Moving things around was a **group action** and in the clown analogy, the clown points were **discriminants** which we use to order our count and are **invariant** under a group action. The clown troupes we wanted to count were our **$\mathbf{S_n}$-number fields**, each of which contains a unique unicycle (**maximal order**). Maximal orders have unique resolvents, so isolating them in our parametrization gives us the count we need (if we had been counting wheels that belonged to non-unicycles, we wouldn't have known how many velocipedes we'd counted). The computer had a sift button (sift is just another word for **sieve**) which isolated the circles corresponding to unicycles based on certain available data (**congruence conditions**), thus allowing our count. There are many other concepts of course not included here, but I don't think we could reasonably (or even ridiculously) go any further.

This chapter is just about the parametrization. In some sense it's just the background (turning on the computer program), but without it, nothing else would work. In order to understand what the parametrization is, we need to talk about **rank n rings** and **vector spaces** (on either end of the parametrization), the **group action** that is compatible with the parametrization, and the various bits of information we will keep track of (**discriminant, shape, equivalence/isomorphism, irreducibility/S_n-ness**). Doing the actual counts and sieve will come later.

2.1.3 Background Galore: Rings and Spaces and Groups, Oh my!

Rank n Rings, Briefly

Knowing what a rank n ring is is not going to tell you why we're doing any of this, nor is it necessary for following the first bit of work that needs to be done. Still, I think it would be weird not to at least mention something about them here.

The basic example of a ring is $\mathbb{Z}$, the set of integers (positive and negative counting numbers and zero), and $\mathbb{Z}$ is the only rank 1 ring. You can add or subtract any two integers and get another integer, there's an additive identity (i.e., $k+0 = k$, for all $k \in \mathbb{Z}$), every non-zero element has an additive inverse ($k+-k = 0$, for all $k \in \mathbb{Z}$), and you can multiply any two integers together and get another integer. There's a multiplicative identity, 1, but notice that you don't have multiplicative inverses ($2^{-1} = \frac{1}{2} \notin \mathbb{Z}$). Two rings are called **isomorphic** if they are pretty much the same ring (they could be exactly the same ring, or just satisfy all the same properties/relationships but technically look different because of how you're writing them).

You could "adjoin" an element α to $\mathbb{Z}$, giving $\mathbb{Z}[\alpha]$, which would mean allowing for integer multiples of powers of α. Instead of just having $0, \pm 1, \pm 2$, etc, you'd also have $\pm\alpha, \pm 2\alpha, ..., \pm\alpha^2, ...$ and sums like $1+\alpha, 1+2\alpha, ...$ etc. If α is the zero for some monic polynomial (meaning the leading coefficient is 1) with integer coefficients, you've just created a rank n ring for some n. Congratulations! If $\alpha = i = \sqrt{-1}$, then $\mathbb{Z}[i] = \{a+bi, a, b \in \mathbb{Z}\}$. This is a rank 2 ring because "as $\mathbb{Z}$-modules" (i.e., ignoring multiplication rules) $\mathbb{Z}[i] \cong \mathbb{Z} \times i\mathbb{Z} \cong \mathbb{Z}^2$. A rank 3 ring looks like $\mathbb{Z}^3$ and a rank 4 ring looks like $\mathbb{Z}^4$.

This doesn't say why we care, and it won't be used yet, but there it is.

The Rings You'll See

Our rank n rings are usually called R and you will often see them paired up with another ring S (of rank r) called a resolvent. One side of our parametrization will be pairs (R, S), and any given R may have more than one resolvent.

Vector Spaces, Even More Briefly

A finite-dimensional real vector space consists of linear combinations of basis vectors where the scalars are real numbers. The 1-dimensional vector space $\mathbb{R}$ can be written as $\{c_0 \cdot \mathbf{1} : c_o \in \mathbb{R}\} = \{c_0\}$, the 2-dimensional vector space $\mathbb{R}^2$ can be written as $\{c_0 \cdot (1,0) + c_1 \cdot (0,1) : c_0, c_1 \in \mathbb{R}\} = \{(c_0, c_1)\}$, etc. Vectors can be scaled and added together, but not multiplied. You can think of elements of a vector space in terms of their "tuples," meaning their ordered coefficients where you suppress the actual basis elements. Vector spaces are nice, and you should usually accept an invitation to go to a party at a vector space.

The Vectors You'll See

Our pairs (R, S) will be parametrized by elements $v \in V_{\mathbb{Z}}$ which are the integral points of the real vector space $V_{\mathbb{R}}$.

Groups (of Matrices)

A group is an all inclusive set and operation package. You have a bunch of group elements, you have an operation, your elements operate on each other giving more elements and these operations can be undone via inverses. The integers make an additive group because you can add and subtract integers to get more integers. They do not make a multiplicative group because most integers do not have integer multiplicative inverses. The real numbers don't make a multiplicative group either, but if you remove the 0, they do (this is called $\mathbb{R}^\times$).

A matrix is a two-dimensional array of numbers, and a square matrix is one with the same number of rows as columns. Matrices can be easily added together, entry-by-entry, and can less easily be multiplied together via "matrix multiplication." (Helpful, yes?) The set of $n \times n$ matrices with entries in $\mathbb{R}$ (or $\mathbb{Z}$) is an additive group, an n^2-dimensional real vector space (or $\mathbb{Z}$-module), and for that matter it is also a ring (if you believe in non-commutative rings). None of these is what we'll use though. We want multiplicative groups of matrices, therefore we have to restrict ourselves to the invertible matrices. For a real number x its inverse x^{-1} is whichever element gives the multiplicative identity, 1, when the two are multiplied together ($xx^{-1} = 1$); for matrices, you have $AA^{-1} = I$, the identity matrix which has 1s down the diagonal and 0s elsewhere. In order to understand which matrices are invertible, we'll need to see the "determinant."

To any square matrix you can assign/calculate a number called its determinant. The absolute value of the determinant is kind of like a size and its sign is sort of like an orientation. Determinants multiply ($\det(AB) = \det(A)\det(B)$, and thus $\det(A) = \det(AI) = \det(A)\det(I)$ which means the identity matrix I has determinant 1), so invertible matrices must have invertible determinant, which over $\mathbb{R}$ just means non-zero determinant ($1 = \det(I) = \det(A)\det(A^{-1})$ so $\det(A^{-1}) = (\det(A))^{-1} \neq 0$). In order to have a multiplicative group, we need every element to have an inverse, so our groups $\mathrm{GL}_{\mathrm{whatever}}(\mathbb{NUMBERS})$ represent invertible matrices (i.e., matrices with determinant having an inverse in $\mathbb{NUMBERS}$) whose size is whatever by whatever and with entries in $\mathbb{NUMBERS}$. We could also look at $\mathrm{SL}_{\mathrm{whatever}}(\mathbb{NUMBERS})$ which is the subgroup of $\mathrm{GL}_{\mathrm{whatever}}(\mathbb{NUMBERS})$ of matrices with determinant 1. For example, $\begin{pmatrix} 2 & -1 \\ -2 & 3 \end{pmatrix}$ is an element of $\mathrm{GL}_2(\mathbb{R})$ with determinant equal to 4. We can rewrite it as $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & -\frac{1}{2} \\ -1 & \frac{3}{2} \end{pmatrix}$ where now $\begin{pmatrix} 1 & -\frac{1}{2} \\ -1 & \frac{3}{2} \end{pmatrix}$ is an element of $\mathrm{SL}_2(\mathbb{R})$. One thing I often forget is that whereas "invertible" means non-zero over $\mathbb{R}$, ±1 are the only invertible integers, so $\mathrm{GL}_2(\mathbb{Z})$ is the set of two by two matrices with integer coefficients whose determinant is equal to ±1. Thus any element of $\mathrm{GL}_2(\mathbb{Z})$ may be written as an element of $\mathrm{SL}_2(\mathbb{Z})$ times $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or times $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Scalar multiplication comes when our matrix is a scalar matrix, which means it's just a number times the identity matrix. The 2×2 scalar matrix for multiplying by 3 is $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = 3 \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 3I_2$, where I_2 is the 2×2 identity matrix. The determinant of the $d \times d$ scalar matrix, λI_d, is just λ^d, the product of the diagonal coefficients.

Most matrices are, of course, not scalar matrices, but you can take any matrix and factor out the dth root of (the absolute value of) its determinant. This separates out the part of the matrix that acts like scalar multiplication from the part which does whatever else it does (basically rotating, reflecting, and "shearing" which is math for slanting). The remaining matrix can have determinant ± 1. In a recent example above, we saw a 2×2 matrix with determinant 4 and we pulled out a 2 in order to create a matrix of determinant 1.

The Matrix Groups You'll See

Mentioned throughout will be GLs and SLs and pairs of these. In particular, we'll have $G_{\mathbb{NUMBERS}} = \mathrm{GL}_{n-1}(\mathbb{NUMBERS}) \times \mathrm{GL}_{r-1}(\mathbb{NUMBERS})$ with or without a superscript indicating some type of restriction. Other groups we'll see include "scalar multiplication" represented by $\mathbb{G}_m$, "orthogonal matrices" represented by O, and $\mathrm{GO} \cong \mathbb{R}^{\times}\mathrm{O}$.

2.1.4 Group Action Intro

What connects our rings and our forms is a natural group action on our forms that also makes sense to our rings and preserves important information. What might this action look like? For an element $v \in V_{\mathbb{Z}}$, we will see in the next section that this v is really a collection of (possibly only one) specific polynomial(s). There are two ways to act on a collection of polynomials; you can either treat the polynomials as objects, which for us will mean creating linear combinations of them (scaling them and/or adding them together), or else you can act on each polynomial individually by modifying the coefficients. If I have a pair of polynomials (A, B) in three variables, I can act on it by $g_2 = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$ to get $(A + 2B, -B)$, or I can act on it by g_3 (which is secretly a 3×3 matrix) and get $(g_3 A g_3^T, g_3 B g_3^T)$, where that means whatever it means but involves messing with coefficients individually.

Each of these actions is represented by invertible matrices of distinct sizes, so they cannot be confused when you put the two actions together. We should note that there is one action that these two potentially have in common, scalar multiplication. I can accomplish scalar multiplication either by treating the polynomials as objects that I scale, i.e., $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \cdot (A, B) = (4A, 4B)$, or by creating an action on the coefficients that just happens to only scale the whole thing, i.e., $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot (A, B) = (2A2, 2B2) = (4A, 4B)$.

What You'll See

Our forms live in a space $V_{\mathbb{Z}} \subset V_{\mathbb{R}}$ and we have a group $G_{\mathbb{Z}} \leq G_{\mathbb{R}}$ acting on it. Saying that a group acts on a set implies that for each element of your group, you know what that element "does" to each element of your set (which element of the set it gets sent to). For $g \in G_{\mathbb{Z}}$ and $v \in V_{\mathbb{Z}}$, $g \cdot v$ is also an element of $V_{\mathbb{Z}}$. If two forms differ only by an element of $G_{\mathbb{Z}}$, we say that they are ($G_{\mathbb{Z}}$-)**equivalent**. We will be acting on all of $V_{\mathbb{R}}$ by $G_{\mathbb{R}}$ in fact and looking at "integral points" (those in $V_{\mathbb{Z}}$) up to $G_{\mathbb{Z}}$-equivalence.

Equivalence

$G_{\mathbb{Z}}$-equivalent forms in $V_{\mathbb{Z}}$ correspond to isomorphic rings. We are interested in isomorphism classes of rings and thus equivalence classes of forms (in each case this just means we only want rings and forms that are meaningfully different from each other; we'll count one from each class rather than keep track of how many versions, if you will, there are). When we talk about "modding out" by something or you see groups with slashes or backslashes between them, this is a way of saying we will only count one version from each class of possibilities, where the specifics, of course, depend on the situation. We'll be looking at $G_{\mathbb{Z}} \backslash G_{\mathbb{R}}$ and $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ (modding out by $G_{\mathbb{Z}}$ on the left) for instance.

2.1.5 Invariance (Discriminant and Shape)

Discriminant

For any polynomial, there is a specific function on the coefficients of the polynomial which satisfies properties and is called the discriminant (note: like age or years spent in graduate school, the discriminant of a polynomial is just a number). Every number field also has a number associated with it called its discriminant, and you can turn our collection of forms into a polynomial and find its discriminant and this will give you the same number as the discriminant of the associated number field. It is common to throw out items with discriminant 0, because they don't adhere to the normal rules and/or because they would uselessly and unhelpfully skew data. For us, rings and forms which have discriminant zero will be called "degenerate," which my husband points out "colloquially certainly means something you don't want to hang around with." One major flaw of such degenerates is that they have no shape. In what follows will we restrict ourselves only to non-degenerate rings and forms.

People really like discriminants, like really. What's so great about discriminants? Sometimes they let you in on secrets, also they are "invariant" which means messing with your polynomial (in specific ways) won't change the discriminant. This can be useful. In fact, for us, the only time the discriminant changes is when we act by scalar multiplication. Or, more truthfully, the only part of the matrix that matters is the determinant.

What You'll See

You will see the absolute value of the discriminant of a vector (or g acting on a vector) all over the place. You will also see X everywhere. To accomplish anything we will have to have some kind of order and for that we use the absolute discriminant. We will always be restricting ourselves to situations in which $|\operatorname{Disc}(\cdot)| < X$ and our main results will only be true as we let X go to infinity. With respect to the group action, the important thing to know is that for $g \in G_{\mathbb{Z}}$ and $v \in V_{\mathbb{R}}$, then $\operatorname{Disc}(gv) = \operatorname{Disc}(v)$, meaning that for all $g \in G_{\mathbb{Z}}$, the condition that $|\operatorname{Disc}(g \cdot v)| < X$ is equivalent to the condition that $|\operatorname{Disc}(v)| < X$.

Shape

Right now all we know of the shape is that it is some kind of thing that is vaguely related to what you'd think "shape" should mean. Great, but what *is* it? For me, the shape has always been a symmetric matrix, probably because that's what it was for Terr in [Ter97]. Shapes live in the space of shapes $\mathcal{S}_{n-1} := \operatorname{GL}_{n-1}(\mathbb{Z})\backslash \operatorname{GL}_{n-1}(\mathbb{R})/\operatorname{GO}_{n-1}(\mathbb{R})$, which I'm finding need not have anything to do with symmetric matrices. We won't need to be able to calculate any shapes explicitly, luckily, because things get a bit out of control for $n = 4$ and I have no desire to find out how ridiculous it is for $n = 5$. In general you can write an $(n-1)$-dimensional lattice as an $(n-1) \times (n-1)$ matrix using the basis vectors, and you can turn it into a symmetric matrix by multiplying it by its "transpose." This new matrix contains inner products of pairs of basis elements, and as such encodes the magnitudes of the basis elements and the angles between them. In the case of $n = 3$, the 2×2 symmetric matrix given by the basis elements gives you as entries: the square of the length of each basis vector, and the product of the lengths times the cosine of the angle between them, which is enough to determine the fundamental parallelogram of the lattice. When writing the shape explicitly, we'll factor out the top left entry, since we don't care about scaling. I say this merely to point out that what you'll see of shapes in the weeds does make some sense potentially. When we actually use the shape in our calculation, we will not be first turning it into a symmetric matrix.

What You'll See

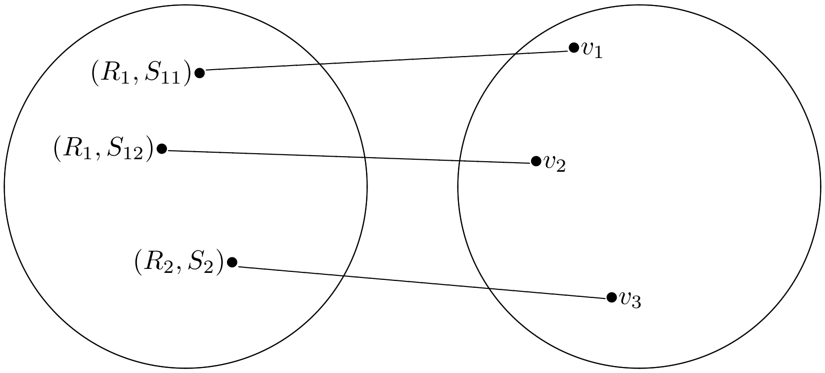
All the new results involve adding the condition that forms (or rings) have shape in some not terrible region W of $\mathcal{S}_{n-1}$. We don't really use anything about the shape (except that it doesn't ruin previous results) until the end. At that point we will need the fact that for $g \in G_{\mathbb{R}}$, $\mathrm{Sh}(g \cdot v) = g \cdot \mathrm{Sh}(v)$ and that both $G_{\mathbb{Z}}$ and $\mathrm{GL}_{r-1}(\mathbb{R})$ leave the shape unchanged. (If we're talking about $\mathrm{Sh}(v) \in \mathcal{S}_{n-1}$, as opposed to its representation as a symmetric matrix, then $g \cdot \mathrm{Sh}(v) = g\,\mathrm{Sh}(v)$, where the operation on the right-hand side is matrix multiplication.) This means that for $g \in G_{\mathbb{Z}}$ or $g \in \mathrm{GL}_{r-1}(\mathbb{R})$, the condition that $\mathrm{Sh}(g \cdot v) \in W$ is the same as the condition that $\mathrm{Sh}(v) \in W$, and importantly, if $\mathrm{Sh}(v) = I$ then $g \cdot \mathrm{Sh}(v) = g$, for all $g \in G_{\mathbb{R}}$.

2.1.6 Simply Irreducible (S_n)

Another piece of data we will keep track of is S_n-ness of number fields. This is important because our methods only tell us about S_n-number fields (number fields with no special symmetries, which is most number fields). We will not need any information on the forms side in terms of how to see irreducibility; we just use that for $n = 3, 4, 5$ reducible points have been shown to be negligible. If you want to know more, however, check out [Dav51b, p. 183], [Bha05, p. 1037], [Bha10, p. 1583] (in the first two sources, A_n fields are also included, but there are very few of those so it doesn't matter). It should be noted that for $n = 3, 5$ you can forget to say S_n and not be lying about the result because S_3-number fields and S_5-number fields make up essentially all of the number fields of rank 3 and 5. For $n = 4$ however a positive proportion of number fields are not S_4 so the distinction becomes important.

2.1.7 Summary

We have a parametrization that gives us a "canonical bijection" (non-weird matching-up-type correspondence) between pairs (R, S) of rank n rings R together with a resolvent ring S of rank r and forms $v \in V_{\mathbb{Z}}$. In this bijection, isomorphism corresponds to $G_{\mathbb{Z}}$-equivalence, S_n-ness corresponds to irreducibility, the discriminant of the ring equals the discriminant of the corresponding form, and similarly for the shape. If we keep track of the bases of R and S (actually we'll keep track of $\alpha_\perp$ and $\beta_\perp$ which are bases for $R/\mathbb{Z}$ and $S/\mathbb{Z}$), then we have a natural action on $(\alpha_\perp, \beta_\perp)$ by $G_{\mathbb{Z}}$ which preserves the discriminant and shape.



$\mathrm{Disc}(R_1) = \mathrm{Disc}(v_1) = \mathrm{Disc}(v_2)$ $\mathrm{Sh}(R_1) = \mathrm{Sh}(v_1) = \mathrm{Sh}(v_2)$
$\mathrm{Disc}(R_2) = \mathrm{Disc}(v_3)$ $\mathrm{Sh}(R_2) = \mathrm{Sh}(v_3)$

Figure 2.1: The parametrization between pairs of rings and forms. Note that on the left we only have two distinct rank n rings, whereas on the right we have three distinct forms.

I should also say that all of this extends (with some work) to $\mathbb{R}$, i.e., we will want to look at $G_{\mathbb{R}}$ acting on $V_{\mathbb{R}}$ to get our results, but this won't correspond to rank n rings anymore, instead it will just correspond to things that look like copies of $\mathbb{R}$ times copies of $\mathbb{C}$. (For example, $\mathbb{Z} \times \sqrt{2}\mathbb{Z}$ and $\mathbb{Z} \times \sqrt{3}\mathbb{Z}$ are two different rank 2 rings, whereas $\mathbb{R} \times \sqrt{2}\mathbb{R}$ and $\mathbb{R} \times \sqrt{3}\mathbb{R}$ are both just $\mathbb{R}^2$.) In particular, we haven't defined the shape of an arbitrary element of $V_{\mathbb{R}}$, but have no fear, it all works the way you'd want it to, though our action will now scale the discriminant and act on the shape.

2.2 The Mathscape

...scrambling in the dark, for anything, anything at all, even just a memory. No, not a memory. If any part of her thought about where she was or how she got there or where in existence there could ever be such thick, tangible darkness, she would surely lose her mind. If she hadn't already, that is. Breath. Feel around the cool ground beneath you. Stone? Are there walls? Somehow she finds herself praying there are walls. Nothing. Nothing at all. Think. Then from deep within the nothingness a voice rings clear in her skull, "In your own words, please."

You know the old saying, "The key algebraic ingredient in proving Theorem 1 for cubic, quartic, and quintic fields is the parametrization of cubic, quartic, and quintic orders in [DF64, Bha04, Bha08]" [BH13]? Well, in this section we'll define all the necessary pieces to understanding these parametrizations.

2.2.1 Pairs (R, S)

Let R be a rank n ring (i.e., a ring that is isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$-module). Then there exist maps from R to some number of "resolvent rings," S, of rank $r = r(n) = 2, 3, 6$ for $n = 3, 4, 5$, respectively. We don't need to know anything about these resolvent rings, but for our parametrization rather than dealing just with rings R we will have pairs (R, S). (For more information on resolvents, see [Bha04, Bha08].)

The discriminant of R is defined in terms of its basis as a $\mathbb{Z}$-module. The shape of R is defined in terms of the $n-1$ basis elements of $R/\mathbb{Z}$, viewed as the matrix of these basis elements, up to $\mathrm{GL}_{n-1}(\mathbb{Z})$ (change of basis) on the left and $\mathrm{GO}_{n-1}(\mathbb{R})$ (scaling, rotating, and reflecting) on the right. Alternatively, you could view the shape as this matrix times its transpose (factoring out the top left entry) to get a matrix of ratios of inner products of pairs of basis elements. This symmetric matrix is nice when dealing with things explicitly, but for our calculations, we'll take the non-symmetric matrices, and so we'll define the space of shapes, $\mathcal{S}_{n-1}$, to be the double coset space $\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/ \mathrm{GO}_{n-1}(\mathbb{R})$.

2.2.2 Forms

If we let $n = 3, 4, 5$ be the rank of the rings we want to study (we can only do one rank at a time), then for each n we will have a corresponding space of forms (with integer coefficients), $V_{\text{integers}} = V_{\mathbb{Z}}$. More specifically,

$$V_{\mathbb{Z}} = \begin{cases} \text{the space of integral binary cubic forms} & \text{for } n = 3, \\ \text{the space of pairs of integral ternary quadratic forms} & \text{for } n = 4, \text{ and} \\ \text{the space of quadruples of integral alternating quinary 2-forms} & \text{for } n = 5. \end{cases}$$

The discriminant of an element $v \in V_{\mathbb{Z}}$ is a “homogeneous” polynomial of degree d in the coefficients of v, where $d = 4, 12, 40$ for $n = 3, 4, 5$, respectively [SK77]. Note that d is also the rank of $V_{\mathbb{Z}}$ as a $\mathbb{Z}$-module (used in §3.3.3).

Examples

What are any of these forms? Well, examples of binary cubic forms (over the integers) would be $v_1 = 4x^3 - 7x^2y + 3xy^2 + y^3$ and $v_2 = x^3 + xy^2$, and examples of integral ternary quadratic forms would be $v_3 = x^2 + 11y^2 - z^2 - xy + 6xz + yz$ and $v_4 = 2x^2 - 25z^2$. So v_1 and v_2 are elements of $V_{\mathbb{Z}}$ for $n = 3$, and $v = (v_3, v_4)$ would be an example of an element of $V_{\mathbb{Z}}$ for $n = 4$. But when we talk about it, except when getting into the ickiness, we'll just talk about forms $v \in V_{\mathbb{Z}}$ and it won't really matter what they look like but you'll want to remember they are collections of specific polynomials.

“Alternating quinary 2-forms” is a bit more complicated. An example of one in polynomial form would be $v_5 = x_1x_2 - x_2x_1 + 3x_2x_5 - 3x_5x_2$. You might notice that this polynomial is equal to zero, since $x_ix_j = x_jx_i$. This may look silly, but we could rewrite all of the canceling terms into new variables, so that $x_1x_2 - x_2x_1 = x_{12}$ and $x_2x_5 - x_5x_2 = x_{25}$, then v_5 could be rewritten as $x_{12} + 3x_{25}$, which is less silly and we needn't tell anyone all our variables are secretly zero. At any rate, people don't really write them out this way, instead they think of them as matrices (which aren't at all zero), but I like saying that my forms are just like polynomials. So, that's what I'm doing.

We can also define the d-dimensional vector space, $V_{\mathbb{R}}$, which is $V_{\mathbb{Z}}$ but where you allow real number coefficients, instead of restricting to integral coefficients. For example, $v_6 = \pi x^3 + \sqrt{2}x^2y - \frac{5}{3}xy^2 - y^3 \in V_{\mathbb{R}}$ for $n = 3$.

2.2.3 Group Action Outro

Which of these groups acts on our forms? For $n = 3$, we have that $\mathrm{GL}_2(\mathbb{Z})$ acts on integral binary cubic forms; for $n = 4$, $\mathrm{SL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ acts on pairs of integral ternary quadratic forms; and for $n = 5$, $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ acts on quadruples of alternating quinary 2-forms [DF64], [Bha04], [Bha08]. In the cases of $n = 4, 5$, the group is made up of two different groups put together, but the action is just the same as if you acted by each one individually: we have that $(g, h) \cdot v = g \cdot h \cdot v = h \cdot g \cdot v$, and thus you just need to know what the individual groups do. (I've heard rumors that it's even more specific if you want to take a more robust approach, if you will, but we won't, so we're alright.)

This is great and all, but we're trying to be cool and do everything at once, so what we'll say instead is that the group $G_{\mathbb{Z}}$ acts on our forms $V_{\mathbb{Z}}$, and we'll define $G_{\mathbb{Z}}$ to be $\mathrm{GL}_{n-1}(\mathbb{Z}) \times \mathrm{GL}_{r-1}(\mathbb{Z})$, where r is defined to be 2,3, or 6 respectively corresponding to $n = 3, 4, 5$ (and this r is in fact the same as the rank of the resolvent ring). What does this mean? This means that

$$G_{\mathbb{Z}} = \begin{cases} \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z}) \text{ instead of just } \mathrm{GL}_2(\mathbb{Z}) & \text{for } n = 3, \\ \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}) \text{ instead of just } \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}) & \text{for } n = 4, \text{ and} \\ \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z}) \text{ instead of just } \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z}) & \text{for } n = 5. \end{cases}$$

We may again define $G_{\mathbb{R}}$ by replacing our integers with real numbers as entries in our matrices. Then, $G_{\mathbb{R}}$ acts on $V_{\mathbb{R}}$ just as $G_{\mathbb{Z}}$ acts on $V_{\mathbb{Z}}$.

Is having a new-fangled $G_{\mathbb{Z}}$ okay??

Yes and no. It is okay in that it acts the way we want it to, and so what we're talking about in this section all makes sense (say I anyway). When we actually try to *count* things, however, we will run into problems and we'll have to change things up a bit.

Acting on Discriminant and Shape

When $G_{\mathbb{Z}}$ acts on $V_{\mathbb{R}}$, it does not affect the shape or discriminant ($\mathrm{Disc}(g \cdot v) = \mathrm{Disc}(v)$ and $\mathrm{Sh}(g \cdot v) = \mathrm{Sh}(v)$ for all $g \in G_{\mathbb{Z}}$, $v \in V_{\mathbb{R}}$). When $G_{\mathbb{R}}$ acts on $V_{\mathbb{R}}$, the discriminant is scaled by factors related to the determinants of the two components. If $g = (g_{n-1}, g_{r-1}) \in G_{\mathbb{R}}$ such that $|\det g_{n-1}| = |\det g_{r-1}| = 1$, then

$\mathrm{Disc}(g \cdot v) = \mathrm{Disc}(v)$ for $v \in V_{\mathbb{R}}$. The action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ is compatible with taking the shape, in that $\mathrm{Sh}(g \cdot v) = g \cdot \mathrm{Sh}(v)$ and in the case of non-symmetric $\mathrm{Sh}(v) \in \mathcal{S}_{n-1}$, $g \cdot \mathrm{Sh}(v)$ is just matrix multiplication.

Acting on Rings

We've only talked about $G_{\mathbb{Z}}$ acting on our forms, but of course there is also an action on our corresponding pairs (R, S). For R a rank n ring, let $1, \alpha_1, \alpha_2, ..., \alpha_{n-1}$ be an integral basis for R. Similarly, we can let $1, \beta_1, \beta_2, ..., \beta_{r-1}$ be an integral basis for a rank r resolvent ring S corresponding to R. We don't care about the $\mathbb{Z}$ component, so we do a projection and end up with $\alpha_{1\perp}, \alpha_{2\perp}, ..., \alpha_{n-1\perp}$, an integral basis for $R/\mathbb{Z}$ and $\beta_{1\perp}, \beta_{2\perp}, ..., \beta_{r-1\perp}$, an integral basis for $S/\mathbb{Z}$. If this makes any kind of sense to you, then you should readily see that $\mathrm{GL}_{n-1}(\mathbb{Z})$ acts on $R/\mathbb{Z}$ by sending each basis element to some linear combination of the basis elements, and again we'd have the same for $\mathrm{GL}_{r-1}(\mathbb{Z})$ acting on $S/\mathbb{Z}$. Since $G_{\mathbb{Z}}$ only changes the bases of $R/\mathbb{Z}$ and $S/\mathbb{Z}$, we see why $G_{\mathbb{Z}}$ does not affect the discriminant or shape at all ($\mathrm{Disc}(g \cdot v) = \mathrm{Disc}(v)$ and $\mathrm{Sh}(g \cdot v) = \mathrm{Sh}(v)$ for $g \in G_{\mathbb{Z}}$), and in fact we will be modding out by $G_{\mathbb{Z}}$ the whole time.

What happens if we look at $G_{\mathbb{R}}$? It doesn't act on our integral forms or rings, because it can send a rank n ring R and corresponding element of $V_{\mathbb{Z}}$ to an "$\mathbb{R}$-algebra" corresponding to a form with non-integral coefficients in $V_{\mathbb{R}}$. We can still talk about $G_{\mathbb{R}}$ acting on $V_{\mathbb{R}}$ of course, and on the rings side, $G_{\mathbb{R}}$ will still act on $\alpha_{\perp}$ and $\beta_{\perp}$. It turns out we can get one more piece of information by looking at how the different components act on the basis elements. If we look at $\mathrm{GL}_{r-1}(\mathbb{R})$ it sends $S/\mathbb{Z}$ who knows where, but only scales $R/\mathbb{Z}$. Since shape has nothing to do with S and isn't affected by scaling, we see that the action of $\mathrm{GL}_{r-1}(\mathbb{R})$ on (R, S) doesn't affect the shape of R at all.

2.2.4 Theorems

That rings (together with resolvents, keeping track of bases) can be parametrized by forms with integer coefficients:

Theorem 2. *Take all your non-isomorphic (not essentially the same) rank n rings, R, picking for each a specific integral basis, $\alpha_{\perp}$, of $R/\mathbb{Z}$ (more in the weeds), and getting rid of any with discriminant 0. Each R may have more than one "resolvent ring," S (of rank r). Form pairs $(R, S) = ((R, \alpha_{\perp}), (S, \beta_{\perp}))$ where again $\beta_{\perp}$ is a specified integral basis of $S/\mathbb{Z}$. Keeping track of all this data is exactly the same as keeping track of elements of $V_{\mathbb{Z}}$ with non-zero discriminant, and the discriminant of R is equal to the discriminant of* *any of its corresponding $v \in V_{\mathbb{Z}}$. The action of $G_{\mathbb{Z}} = \mathrm{GL}_{n-1}(\mathbb{Z}) \times \mathrm{GL}_{r-1}(\mathbb{Z})$ on $V_{\mathbb{Z}}$ corresponds to an action on $(\alpha_\perp, \beta_\perp)$ so that $g \in G_{\mathbb{Z}}$ sends (R, S) corresponding to $v \in V_{\mathbb{Z}}$ to the the pair (R', S') corresponding to $v' = gv$. Maximal rings R have unique resolvents, S, so counting (R, S) where R is maximal is the same as counting maximal rings (to be defined later).*

To do what we need to do, though, we'll need to know our parametrization is still meaningful over $\mathbb{R}$.

Theorem 3. *If we replace all our $\mathbb{Z}$s with $\mathbb{R}$s, we still have a bijective correspondence between pairs $((R, \alpha_\perp), (S, \beta_\perp))$ and elements of $V_{\mathbb{R}}$. Again, the action of $G_{\mathbb{R}} = \mathrm{GL}_{n-1}(\mathbb{R}) \times \mathrm{GL}_{r-1}(\mathbb{R})$ on $V_{\mathbb{R}}$ corresponds to an action on $(\alpha_\perp, \beta_\perp)$ so that $g \in G_{\mathbb{R}}$ sends (R, S) corresponding to $v \in V_{\mathbb{R}}$ to the the pair (R', S') corresponding to $v' = gv$. Over $\mathbb{R}$, it turns out that each R has a unique S, just FYI.*

The proof of Theorem 2 is found in [DF64, §15], [Bha04, Corollary 5], [Bha08, Corollary 3]: (one for each n). The proof of Theorem 3 is based on the the proof of Theorem 2 with some additional explanation (see [BH13]).

2.2.5 So......? Some True Things

We want to count the number of non-isomorphic S_n-number fields of degree n (for one n at a time) with bounded absolute discriminant (meaning the absolute value of the discriminant is less than some number, X), and with shape in some nice pre-determined region W. We know that each number field has a unique maximal order, which is a ring of rank n, therefore we start by attempting to get a hold of those.

Through a nice parametrization, we decide to start by looking at rings with their resolvents and bases (counting $((R, \alpha_\perp), (S, \beta_\perp))$ instead of R) which now correspond to elements in $V_{\mathbb{Z}}$. For $v \in V_{\mathbb{Z}}$ and $R(v)$ its associated ring, we have that $\mathrm{Disc}(v) = \mathrm{Disc}(R(v))$ and $\mathrm{Sh}(v) := \mathrm{Sh}(R(v))$. (The parametrization gives explicit relationships between the multiplication table of $R(v)$ and the coefficients of v in general for each n, so it is sometimes possible to write $\mathrm{Sh}(v)$ explicitly.) A form in $V_{\mathbb{Z}}$ will be called irreducible if it corresponds to a ring R in an S_n-field (a number field whose Galois closure has Galois group S_n), therefore we will restrict ourselves to counting irreducible forms. (Okay, if we're keeping it 100, a form is called irreducible if we want to count it, and corresponding to an S_n-field is a sufficient condition which works with our methods. For the individual cases, irreducibility was defined (and sometimes named) somewhat differently. See [Dav51b, p. 183], [Bha05, p. 1037], [Bha10, p. 1583].)

The action by $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ is compatible with taking the discriminant and shape. If the determinants of the components of $g \in G_{\mathbb{R}}$ are ±1, then $\mathrm{Disc}(g \cdot v) = \mathrm{Disc}(v)$ and $\mathrm{Sh}(g \cdot v) = \mathrm{Sh}(v)$ (so this goes for all of $G_{\mathbb{Z}}$ and some other elements of $G_{\mathbb{R}}$ as well). Additionally, since $\mathrm{GL}_{r-1}(\mathbb{R})$ doesn't affect the shape of R, we know it mustn't affect the shape of v either. Forms that are equivalent under the action of $G_{\mathbb{Z}}$ correspond to isomorphic rings, therefore we will only look at $V_{\mathbb{Z}}$ up to $G_{\mathbb{Z}}$-equivalence.

The next step will be to count equivalence classes of irreducible forms in $V_{\mathbb{Z}}$ with imposed shape and discriminant conditions. This doesn't give us exactly what we want, but we will be able to modify the count in subsequent chapters to eventually reach our goal.

In the following sections all of our counts will be of irreducible forms.

2.3 The Weedscape

She had never cared for art or museums. Stolen art on white walls. Detached yet still condescending. No, thank you. Whenever these trips were forced upon her ("let's go, girl, your teen vamps can wait"), she would inevitably find herself sitting alone, finally able to retrieve her current not-always-about-teenaged-vampires novel from her bag. This trip was no different, though something had caught her eye. A large painting (oil? That was a thing, right?) that had a whole wall to itself. Empty landscape, setting sun, single tree on a hill, quaint village in a valley. Vaguely bleak, though not overly so. But in the distance, the only person, a young woman, with her face close to the ground, searching. Digging. The blurb for the painting said it was called Answers. It all made a sort of sense to her; the truth is always under the dirt.

Okay, time to wade into the weeds with some details. These details will likely not be particularly illuminating, unless you've understood the rest enough to need to see it explicitly to check your understanding. Enter at your own peril.

This section is about explicit facts concerning the parametrization and shapes, grouped by $n = 3, 4, 5$. Note that some general explanations are included in the $n = 3$ section. The calculations included represent what I needed to get an understanding of things. I did the most work for $n = 3$, and essentially no work for

$n = 5$ where things were so complicated it seemed doubtful explicit work would actually give me any warm and fuzzies. As you may have guessed, $n = 4$ is somewhere in between.

2.3.1 $n = 3$

Parametrization

A rank n ring can be written as $\mathbb{Z} \times \alpha_1\mathbb{Z} \times ... \times \alpha_{n-1}\mathbb{Z}$, with a multiplication table that tells you what happens when you multiply two α_i together. Since every element of the ring can be written as a linear combination of basis elements, the same is true for $\alpha_i\alpha_j$ for $i, j = 0, 1, ..., n-1$ and therefore we know there must exist $c_{ij}^k \in \mathbb{Z}$ such that

$$\alpha_i\alpha_j = c_{ij}^0 + c_{ij}^1\alpha_1 + ... + c_{ij}^{n-1}\alpha_{n-1}.$$

The c_{ij}^k are thus the coefficients in the multiplication table, and they will turn (somehow) into the coefficients of the corresponding element of $V_{\mathbb{Z}}$.

The discriminant of the ring with integral basis $\alpha_0 = 1, \alpha_1, \alpha_2..., \alpha_{n-1}$ is the determinant of the matrix whose entries are given by the "trace" of $\alpha_i\alpha_j$, for $0 \leq i, j \leq n-1$, and this will equal the discriminant of any of the corresponding elements in $V_{\mathbb{Z}}$. We'll do discriminants later with the shapes of rings because the work is overlapping.

From [BST13], we have a bijective correspondence between $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of integral binary cubic forms and rank 3 rings as follows.

Let $v = ax^3 + bx^2y + cxy^2 + dy^3$, then the corresponding ring, $R(v)$, can be written as $\mathbb{Z} \times \alpha\mathbb{Z} \times \beta\mathbb{Z}$ with the following **multiplication table**:

$$\alpha\beta = -ad$$

$$\alpha^2 = -ac + b\alpha - a\beta$$

$$\beta^2 = -bd + d\alpha - c\beta.$$

The **discriminant** of $R(v)$ is $\begin{vmatrix} 1 & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\beta) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha\beta) \\ \mathrm{Tr}(\beta) & \mathrm{Tr}(\alpha\beta) & \mathrm{Tr}(\beta^2) \end{vmatrix}$ and will turn out to be equal to

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

which is precisely the formula for the discriminant of $v = ax^3 + bx^2y + cxy^2 + dy^3$.

Example

If you start with a form, say $v = x^3 - 2xy^2 + y^3$ that means that $(a, b, c, d) = (1, 0, -2, 1)$ so the multiplication table you get is:

$$\alpha\beta = -1$$

$$\alpha^2 = 2 - \beta$$

$$\beta^2 = \alpha + 2\beta.$$

Now figuring out what α, β give those equations is not necessarily fun or satisfying, but if you give me any two elements from the ring, I can add, subtract, and multiply them, so that's good enough to know the ring. Starting with a ring is somewhat more difficult because you first have to change bases until you get $\alpha\beta$ to be an integer. From there, you can read off all the coefficients for the corresponding form. (If you must know, α satisfies $\alpha^3 - 2\alpha + 1 = 0$, and β satisfies $\beta^3 - 2\beta^2 + 1 = 0$, and the internet can help you solve those cubics. I got those equations from the multiplication table, but you can also start from the original form $v = x^3 - 2xy^2 + y^3$ and find α, β such that $(\alpha, 1)$ and $(1, \beta)$ are roots of v, meaning they send v to 0.)

Shapes

We know that we have some theoretical matrix element called a shape which is somehow related to the ideas we want to encompass in the word, but what does it actually look like? Whenever we write a shape explicitly, we'll view it as a symmetric matrix (called the Gram matrix of the lattice, I'm told), because it looks nicer.

First, we start with a rank n ring $R = \mathbb{Z} \times \alpha_1\mathbb{Z} \times ... \times \alpha_{n-1}\mathbb{Z}$ and its associated form $v \in V_{\mathbb{Z}}$. They share information in that the coefficients of v form the coefficients of the multiplication table of R (though not necessarily in a straightforward way). So we'll have two routes for finding their shape. Our motivation comes from the ring side. We have to "project onto the orthogonal complement of $\mathbf{1}$" in order to find $R_\perp$ which gets rid of that first $\mathbb{Z}$ component that all our rings will have in common which would skew our distribution of shapes. Finding a basis for this space gives us $R_\perp = \alpha_{1\perp}\mathbb{Z} \times \alpha_{2\perp}\mathbb{Z}...\alpha_{n-1\perp}\mathbb{Z}$, and we can find $R_\perp$ explicitly in terms of the coefficients of v basically by looking inside $\mathbb{Q} \times \alpha_1\mathbb{Q} \times \alpha_2\mathbb{Q} \times ... \times \alpha_{n-1}\mathbb{Q}$ for elements with "trace" equal to zero. Our basis for these trace zero elements will give us the $\alpha_{i\perp}$. From there, our shape will be a symmetric matrix of ratios of products of pairs of $\alpha_{i\perp}$. If all of our α_i give off the impression that they belong in $\mathbb{R}$ (if all their embeddings into $\mathbb{C}$ land in $\mathbb{R}$), we are in the totally real case, and our inner products are given by the trace function, so we can find the shape fairly easily. When we're not in the totally real case, the trace (isn't an inner product and thus) doesn't behave in the way we need for it to give us the shape, and finding the inner product without the trace is a drag.

Trace

For a square matrix, A, you can find its trace, $\mathrm{Tr}(A)$, by summing up the diagonal entries. The trace of the $k \times k$ identity matrix is k, the dimension of the space. We'll be finding the trace of ring elements, which are not square matrices. Our ring R has an integral basis given by $\{1, \alpha_1, \alpha_2, ..., \alpha_{n-1}\}$. Since we can actually multiply our elements together, we can consider each element as a "linear operator" on R. Once you have a linear operator, you can view it as a matrix, and then you can find its trace. For example, the matrix of multiplication by i in $\mathbb{Z}[i]$ is given by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ in the basis $(1, i)$. The columns of this matrix are the vectors representing i times the basis elements $1, i$. If you rewrite $a + bi$ as $\begin{bmatrix} a \\ b \end{bmatrix}$, then $i \cdot 1 = i = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, the first column of the matrix, and $i \cdot i = -1 = \begin{bmatrix} -1 \\ 0 \end{bmatrix}$, the second column. The trace of i is thus $\mathrm{Tr}(i) = 0 + 0 = 0$. Two important properties of the trace are that $\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$ and that $\mathrm{Tr}(kA) = k\,\mathrm{Tr}(A)$. In the case of operators $1, \alpha_1$ this looks like $\mathrm{Tr}(k_0 + k_1\alpha_1) = k_0\,\mathrm{Tr}(1) + k_1\,\mathrm{Tr}(\alpha_1)$.

Calculating Shapes of Cubic Rings

We again start with $R = \mathbb{Z}\times\alpha\mathbb{Z}\times\beta\mathbb{Z}$ with corresponding $f(x, y) = ax^3+bx^2y+cxy^2+dy^3$ and multiplication table

$$\alpha\beta = -ad$$

$$\alpha^2 = -ac + b\alpha - a\beta$$

$$\beta^2 = -bd + d\alpha - c\beta.$$

To find $R_\perp = \alpha_\perp\mathbb{Z} \times \beta_\perp\mathbb{Z}$, we first take the traces of the basis elements of R, then we can find a formula for elements which have trace 0.

$$\mathrm{Tr}(1) = 3$$

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}\begin{pmatrix} 0 & -ac & -ad \\ 1 & b & 0 \\ 0 & -a & 0 \end{pmatrix} = b$$

$$\mathrm{Tr}(\beta) = \mathrm{Tr}\begin{pmatrix} 0 & -ad & -bd \\ 0 & 0 & d \\ 1 & 0 & -c \end{pmatrix} = -c$$

For an element $k_1 + k_2\alpha + k_3\beta \in \mathbb{Q} \times \alpha\mathbb{Q} \times \beta\mathbb{Q}$ to have trace zero, that means that

$$0 = \mathrm{Tr}(k_1 + k_2\alpha + k_3\beta) = k_1\,\mathrm{Tr}(1) + k_2\,\mathrm{Tr}(\alpha) + k_3\,\mathrm{Tr}(\beta) = 3k_1 + bk_2 - ck_3.$$

If we solve for k_1 (which happily does not involve dividing by an unknown) we get a formula for the elements of $R_\perp$. Since $k_1 = -k_2\frac{b}{3} + k_3\frac{c}{3}$, we have that $R_\perp = \{(-k_2\frac{b}{3} + k_3\frac{c}{3}) + k_2\alpha + k_3\beta\} = \{k_2(\alpha - \frac{b}{3}) + k_3(\beta + \frac{c}{3})\}$ and we see that our new basis elements are $\alpha_\perp = \alpha - \frac{b}{3},\ \beta_\perp = \beta + \frac{c}{3}$.

The shape of R (defined to be the shape of $R_\perp$) is then given by:

$$\mathrm{Sh}(R) = \begin{pmatrix} 1 & \frac{\alpha_\perp \cdot \beta_\perp}{\alpha_\perp \cdot \alpha_\perp} \\ \frac{\alpha_\perp \cdot \beta_\perp}{\alpha_\perp \cdot \alpha_\perp} & \frac{\beta_\perp \cdot \beta_\perp}{\alpha_\perp \cdot \alpha_\perp} \end{pmatrix}$$

In the totally real case, we can find the shape explicitly somewhat easily, by using the fact that the inner product $u \cdot v$ is given by $\mathrm{Tr}(uv)$.

$$\alpha_\perp \cdot \alpha_\perp = \mathrm{Tr}(\alpha_\perp^2) = \mathrm{Tr}((\alpha - \frac{b}{3})(\alpha - \frac{b}{3})) = \mathrm{Tr}(\alpha^2 - \frac{b}{3}\alpha - \frac{b}{3}\alpha_\perp).$$

This is not the normal way to expand the product, but it's useful since the trace is additive and $\alpha_\perp, \beta_\perp$ have trace zero, so that $\mathrm{Tr}(u + k\alpha_\perp) = \mathrm{Tr}(u)$. Remembering that $\alpha^2 = -ac + b\alpha - a\beta$ we get

$$\alpha_\perp \cdot \alpha_\perp = \mathrm{Tr}(-ac + \frac{2b}{3}\alpha - a\beta) = -ac\,\mathrm{Tr}(1) + \frac{2b}{3}\,\mathrm{Tr}(\alpha) - a\,\mathrm{Tr}(\beta) = -3ac + \frac{2b^2}{3} + ac = -2ac + \frac{2b^2}{3}.$$

$$\alpha_\perp \cdot \beta_\perp = \mathrm{Tr}(\alpha_\perp \beta_\perp) = \mathrm{Tr}((\alpha - \frac{b}{3})(\beta + \frac{c}{3})) = \mathrm{Tr}(\alpha\beta - \frac{b}{3}\beta + \frac{c}{3}\alpha_\perp) = \mathrm{Tr}(-ad - \frac{b}{3}\beta) = -3ad + \frac{bc}{3}.$$

$$\beta_\perp \cdot \beta_\perp = \mathrm{Tr}(\beta_\perp^2) = \mathrm{Tr}((\beta + \frac{c}{3})^2) = \mathrm{Tr}(\beta^2 + \frac{c}{3}\beta + \frac{c}{3}\beta_\perp) = \mathrm{Tr}(-bd + d\alpha - \frac{2c}{3}\beta) = -2bd + \frac{2c^2}{3}.$$

The shape is thus (clearing the denominators)

$$\mathrm{Sh}(R) = \begin{pmatrix} 1 & \frac{bc - 9ad}{2(b^2 - 3ac)} \\ \frac{bc - 9ad}{2(b^2 - 3ac)} & \frac{c^2 - 3bd}{b^2 - 3ac} \end{pmatrix}.$$

Extra Fun For $n = 3$ Only

There's another way to get the formula on the form side. Start with $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ and find its "Hessian," which is the quadratic form you get when you compute $H(f) = \begin{vmatrix} f_{xx} & f_{xy} \\ f_{xy} & f_{yy} \end{vmatrix}$. In this case, we use calculus to get

$$H(f) = \begin{vmatrix} 6ax + 2by & 2bx + 2cy \\ 2bx + 2cy & 2cx + 6dy \end{vmatrix} = -4[(b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 + 3bd)y^2].$$

If we set $P = b^2 - 3ac, Q = bc - 9ad, R = c^2 - 3bd$, then $H(f) = -4(Px^2 + Qxy + Ry^2)$ and

$$\mathrm{Sh}(f) = \mathrm{Sh}(R) = \begin{pmatrix} 1 & \frac{Q}{2P} \\ \frac{Q}{2P} & \frac{R}{P} \end{pmatrix}.$$

Those of you who know binary quadratic forms will recognize that the shape is the matrix associated with $H(f)$ scaled to get a 1 in the first entry. (Note: I'm using Bhargava's multiplication table [Bha04], which is slightly different from Terr's, so my Q is -1 times Terr's Q.)

Discriminants of Cubic Rings

The discriminant of R is given by the determinant of the 3×3 matrix whose entries are $\mathrm{Tr}(\alpha_i\alpha_j)$, remembering we're setting $\alpha_0 = 1$. We know that $\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\alpha) = b$, and $\mathrm{Tr}(\beta) = -c$, then from the multiplication table, we see that $\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(-ac + b\alpha - a\beta) = b^2 - 2ac$, $\mathrm{Tr}(\beta^2) = c^2 - 2bd$, and $\mathrm{Tr}(\alpha\beta) = -3ad$. Now we see that

$$\mathrm{Disc}(R) = \begin{vmatrix} 3 & b & -c \\ b & b^2 - 2ac & -3ad \\ -c & -3ad & c^2 - 2bd \end{vmatrix} = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

In terms of P, Q, R from the Hessian, $\mathrm{Disc}(R) = \mathrm{Disc}(f) = \frac{4PR - Q^2}{3}$. We also have that $\mathrm{Disc}(H(f)) = -16(4PR - Q^2)$ and the determinant of the shape matrix is $\frac{4PR-Q^2}{4P^2}$.

Group Action

We want to see what it actually looks like when $G_{\mathbb{Z}}$ acts on $V_{\mathbb{Z}}$, and to see whether and how the discriminant and shape are affected. Here, $G_{\mathbb{Z}} = \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z})$ and $V_{\mathbb{Z}} = \{ax^3 + bx^2y + cxy^2 + dy^3 : \ a, b, c, d \in \mathbb{Z}\}$.

For

$$g = (g_2, g_1) = \left(\begin{pmatrix} r & s \\ t & u \end{pmatrix}, \lambda_1 \right) \in G_{\mathbb{Z}} \text{ (or } G_{\mathbb{R}})$$

and $f(x, y) \in V_{\mathbb{Z}}$ (or $V_{\mathbb{R}}$), we have

$$g \cdot f(x, y) = \lambda_1 f(rx + ty, sx + uy),$$

and also

$$\operatorname{Disc}(g \cdot f(x, y)) = (\lambda_1)^4 (\det g_2)^6 \operatorname{Disc}(f(x, y)).$$

We see that any $g \in G_{\mathbb{R}}$ such that λ_1 and $\det g_2$ are ± 1 leaves the discriminant unchanged (this includes all of $G_{\mathbb{Z}}$). We also note that if $g \in G_{\mathbb{R}}$ and $g_2 = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, then

$$g \cdot f(x, y) = \lambda_1 f(\lambda_2 x, \lambda_2 y) = \lambda_1 \lambda_2^3 f(x, y).$$

By definition, $\mathrm{GL}_1(\mathbb{R})$ does not act on the shape of $f(x, y)$, so $\operatorname{Sh}(g \cdot f(x, y)) = \operatorname{Sh}(g_2 \cdot f(x, y))$, which turns out to be equivalent to $g_2 \cdot \operatorname{Sh}(f(x, y))$, whether $g_2 \cdot \operatorname{Sh}(f(x, y)) = g_2 \operatorname{Sh}(f(x, y)) g_2^T$ when dealing with symmetric matrices, or whether $g_2 \cdot \operatorname{Sh}(f(x, y)) = g_2 \operatorname{Sh}(f(x, y))$, representing matrix multiplication, in the case of our chosen space of shapes.

Let $g = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$, then for $v = \langle a, b, c, d \rangle$, $g \cdot v = v' = \langle a', b', c', d' \rangle$, and the ring associated with v' is R' with basis $1, \alpha', \beta'$, and the shape will come from ratios of dot products of $\alpha'_\perp, \beta'_\perp$. Here are some things I've calculated:

$$g \cdot v = \langle a, b, c, d \rangle = \langle ar^3 + br^2 s + crs^2 + ds^3,\ 3ar^2 t + 2brst + cs^2 t + br^2 u + 2crsu + 3ds^2 u,$$

$$3art^2 + 2brtu + bst^2 + cru^2 + 2cstu + 3dsu^2,\ at^3 + bt^2 u + ctu^2 + du^3 \rangle,$$

$$\alpha' = (r\alpha + s\beta)(ru - st) + s(brt + dsu) + r(art + csu),$$

$$\beta' = (t\alpha + u\beta)(ru - st) - u(brt + dsu) - t(art + csu),$$

$$\alpha'_\perp = (r\alpha_\perp + s\beta_\perp)(ru - st),$$

$$\beta'_\perp = (t\alpha_\perp + u\beta_\perp)(ru - st),$$

$$\mathrm{Sh}(g \cdot v) = \begin{pmatrix} 1 & \frac{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(t\alpha_\perp \cdot + u\beta_\perp)}{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(r\alpha_\perp \cdot + s\beta_\perp)} \\ \frac{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(t\alpha_\perp \cdot + u\beta_\perp)}{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(r\alpha_\perp \cdot + s\beta_\perp)} & \frac{(t\alpha_\perp \cdot + u\beta_\perp)\cdot(t\alpha_\perp \cdot + u\beta_\perp)}{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(r\alpha_\perp \cdot + s\beta_\perp)} \end{pmatrix},$$

$$g \cdot \mathrm{Sh}(v) = \frac{(r\alpha_\perp \cdot + s\beta_\perp) \cdot (r\alpha_\perp \cdot + s\beta_\perp)}{\alpha_\perp \cdot \alpha_\perp} \begin{pmatrix} 1 & \frac{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(t\alpha_\perp \cdot + u\beta_\perp)}{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(r\alpha_\perp \cdot + s\beta_\perp)} \\ \frac{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(t\alpha_\perp \cdot + u\beta_\perp)}{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(r\alpha_\perp \cdot + s\beta_\perp)} & \frac{(t\alpha_\perp \cdot + u\beta_\perp)\cdot(t\alpha_\perp \cdot + u\beta_\perp)}{(r\alpha_\perp \cdot + s\beta_\perp)\cdot(r\alpha_\perp \cdot + s\beta_\perp)} \end{pmatrix},$$

(Remember, when shape is not a symmetric matrix, the action is simply normal matrix multiplication and is compatible with the action on $V_{\mathbb{R}}$.)

$$H(g \cdot f) = -4(ru - st)^2[(b^2 - 3ac)(rx + sy)^2 + (bc - 9ac)(rx + sy)(tx + uy) + (c^2 - 3bd)(tx + uy)^2].$$

The action on $\alpha_\perp, \beta_\perp$ can be seen if you view them as the basis of a vector space and write $\alpha_\perp$ as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, and $\beta_\perp$ as $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Then $g \cdot v = (\det g)gv$.

2.3.2 $n = 4$

Parametrization of Quartic Rings

From [Bha04, §3], we have a bijective correspondence between (isomorphism classes of) pairs (R, S) of quartic rings and their cubic resolvents and ($G_{\mathbb{Z}}$-equivalence classes of) pairs of integral ternary quadratic forms.

Let $R = \mathbb{Z} \times \mathbb{Z}\alpha \times \mathbb{Z}\beta \times \mathbb{Z}\gamma$ be a quartic ring, it can be arranged that its multiplication table will look like

$$\alpha^2 = h_{11} + g_{11}\alpha + f_{11}\beta + e_{11}\gamma$$

$$\beta^2 = h_{22} + g_{22}\alpha + f_{22}\beta + e_{22}\gamma$$

$$\gamma^2 = h_{33} + g_{33}\alpha + f_{33}\beta + e_{33}\gamma$$

$$\alpha\beta = h_{12} + e_{12}\gamma$$

$$\alpha\gamma = h_{13} + f_{13}\beta + e_{13}\gamma$$

$$\beta\gamma = h_{23} + g_{23}\alpha + f_{23}\beta + e_{23}\gamma,$$

for some integers $h_{ij}, g_{ij}, e_{ij}, f_{ij}$.

If $v = (A, B)$ is the pair

$$(a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + a_{12}xy + a_{13}xz + a_{23}yz,\ b_{11}x^2 + b_{22}y^2 + b_{33}z^2 + b_{12}xy + b_{13}xz + b_{23}yz) \in V_{\mathbb{Z}},$$

define $\lambda^{ij}_{kl} = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{kl} & b_{kl} \end{vmatrix}$. Then the coefficients for the **multiplication table** of R are:

$$g_{11} = \lambda^{11}_{23} + \lambda^{12}_{13},\ g_{22} = \lambda^{22}_{23},\ g_{23} = \lambda^{22}_{33},\ g_{33} = \lambda^{23}_{33},$$

$$f_{11} = -\lambda^{11}_{13},\ f_{13} = -\lambda^{11}_{33},\ f_{22} = -\lambda^{12}_{23} + \lambda^{13}_{22},\ f_{23} = -\lambda^{12}_{33},\ f_{33} = -\lambda^{13}_{33},$$

$$e_{11} = \lambda^{11}_{12},\ e_{12} = \lambda^{11}_{22},\ e_{13} = \lambda^{11}_{23},\ e_{22} = \lambda^{12}_{22},\ e_{23} = \lambda^{13}_{22},\ e_{33} = -\lambda^{12}_{33} + \lambda^{13}_{23}$$

$$h_{11} = e_{12}f_{13} - f_{11}f_{22} - e_{11}f_{23} = -\lambda^{11}_{22}\lambda^{11}_{33} - \lambda^{11}_{13}\lambda^{12}_{23} + \lambda^{11}_{13}\lambda^{13}_{22} + \lambda^{11}_{12}\lambda^{12}_{33},$$

$$h_{12} = f_{11}g_{22} + e_{11}g_{23} = -\lambda^{11}_{13}\lambda^{22}_{23} + \lambda^{11}_{12}\lambda^{22}_{33},$$

$$h_{13} = f_{11}g_{23} + e_{11}g_{33} = -\lambda^{11}_{13}\lambda^{22}_{33} + \lambda^{11}_{12}\lambda^{23}_{33},$$

$$h_{22} = g_{23}e_{12} - g_{11}g_{22} = \lambda^{11}_{22}\lambda^{22}_{33} - \lambda^{11}_{23}\lambda^{22}_{23} - \lambda^{12}_{13}\lambda^{22}_{23},$$

$$h_{23} = g_{22}f_{13} + e_{22}f_{33} - e_{23}f_{23} = -\lambda^{11}_{33}\lambda^{22}_{23} - \lambda^{12}_{13}\lambda^{22}_{33},$$

$$h_{33} = f_{13}g_{23} + e_{13}g_{33} - g_{11}g_{33} = -\lambda^{11}_{33}\lambda^{22}_{33} - \lambda^{12}_{13}\lambda^{23}_{33}.$$

The **discriminant** of (A, B) is defined to be $\mathrm{Disc}(4\det(Ax+By))$. If that looks funny, remember A and B are 3×3 symmetric matrices, so $Ax + By$ is, too. The determinant (and four times it) will then be a binary cubic form, so it makes sense to talk about a discriminant. This will turn out to be equal to

$$\mathrm{Disc}(R) = \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\beta) & \mathrm{Tr}(\gamma) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha\beta) & \mathrm{Tr}(\alpha\gamma) \\ \mathrm{Tr}(\beta) & \mathrm{Tr}(\alpha\beta) & \mathrm{Tr}(\beta^2) & \mathrm{Tr}(\beta\gamma) \\ \mathrm{Tr}(\gamma) & \mathrm{Tr}(\alpha\gamma) & \mathrm{Tr}(\beta\gamma) & \mathrm{Tr}(\gamma^2) \end{vmatrix}.$$

Shapes of Quartic Rings

We start with $R = \mathbb{Z} \times \mathbb{Z}\alpha \times \mathbb{Z}\beta \times \mathbb{Z}\gamma$ and associated $(A, B) = (a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + a_{12}xy + a_{13}xz + a_{23}yz, b_{11}x^2 + b_{22}y^2 + b_{33}z^2 + b_{12}xy + b_{13}xz + b_{23}yz)$. We again have a multiplication table, the coefficients denoted by $g_{ij}, e_{ij}, f_{ij}, h_{ij}$ where $1 \leq i \leq j \leq 3$. These coefficients are related to the coefficients of (A, B) via the determinants $\lambda^{ij}_{kl} = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{kl} & b_{kl} \end{vmatrix}$.

To find $R_\perp = \alpha_\perp\mathbb{Z} \times \beta_\perp\mathbb{Z} \times \gamma_\perp\mathbb{Z}$, we first take the traces of the basis elements of R, then we can find a formula for elements which have trace 0.

$$\mathrm{Tr}(1) = 4$$

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}\begin{pmatrix} & h_{11} & h_{12} & h_{13} \\ 1 & g_{11} & & \\ & f_{11} & & f_{13} \\ & e_{11} & e_{12} & e_{13} \end{pmatrix} = g_{11} + e_{13}$$

$$\mathrm{Tr}(\beta) = \mathrm{Tr}\begin{pmatrix} & h_{12} & h_{22} & h_{23} \\ & & g_{22} & g_{23} \\ 1 & & f_{22} & f_{23} \\ & e_{12} & e_{22} & e_{23} \end{pmatrix} = f_{22} + e_{23}$$

$$\mathrm{Tr}(\gamma) = \mathrm{Tr}\begin{pmatrix} & h_{13} & h_{23} & h_{33} \\ & & g_{23} & g_{33} \\ & f_{13} & f_{23} & f_{33} \\ 1 & e_{13} & e_{23} & e_{33} \end{pmatrix} = f_{23} + e_{33}$$

For an element $k_1 + k_2\alpha + k_3\beta + k_4\gamma \in \mathbb{Q} \times \alpha\mathbb{Q} \times \beta\mathbb{Q} \times \gamma\mathbb{Q}$ to have trace zero, we must have

$$0 = \mathrm{Tr}(k_1 + k_2\alpha + k_3\beta + k_4\gamma) = 4k_1 + k_2(g_{11} + e_{13}) + k_3(f_{22} + e_{23}) + k_4(f_{23} + e_{33}).$$

Solving that $k_1 = -\frac{1}{4}(k_2(g_{11} + e_{13}) + k_3(f_{22} + e_{23}) + k_4(f_{23} + e_{33}))$ we get that

$$R_\perp = \{k_2(\alpha - \frac{g_{11} + e_{13}}{4}) + k_3(\beta - \frac{f_{22} + e_{23}}{4}) + k_4(\gamma - \frac{f_{23} + e_{33}}{4})\}$$

and thus

$$\alpha_\perp = \alpha - \frac{1}{4}(g_{11} + e_{13}),$$

$$\beta_\perp = \beta - \frac{1}{4}(f_{22} + e_{23}),$$

$$\gamma_\perp = \gamma - \frac{1}{4}(f_{23} + e_{33}).$$

The shape of R is given by:

$$\mathrm{Sh}(R) = \begin{pmatrix} 1 & \frac{\alpha_\perp \cdot \beta_\perp}{\alpha_\perp \cdot \alpha_\perp} & \frac{\alpha_\perp \cdot \gamma_\perp}{\alpha_\perp \cdot \alpha_\perp} \\ \frac{\alpha_\perp \cdot \beta_\perp}{\alpha_\perp \cdot \alpha_\perp} & \frac{\beta_\perp \cdot \beta_\perp}{\alpha_\perp \cdot \alpha_\perp} & \frac{\beta_\perp \cdot \gamma_\perp}{\alpha_\perp \cdot \alpha_\perp} \\ \frac{\alpha_\perp \cdot \gamma_\perp}{\alpha_\perp \cdot \alpha_\perp} & \frac{\beta_\perp \cdot \gamma_\perp}{\alpha_\perp \cdot \alpha_\perp} & \frac{\gamma_\perp \cdot \gamma_\perp}{\alpha_\perp \cdot \alpha_\perp} \end{pmatrix}.$$

We calculate this explicitly in the totally real case again using the trace function.

$$\alpha_\perp \cdot \alpha_\perp = Tr((\alpha_\perp)^2) = Tr((\alpha - \frac{1}{4}(g_{11} + e_{13}))^2)$$

$$= Tr(\alpha^2 - \frac{1}{4}(g_{11} + e_{13})\alpha - \frac{1}{4}(g_{11} + e_{13})\alpha_\perp)$$

$$= Tr(h_{11} + g_{11}\alpha + f_{11}\beta + e_{11}\gamma) - \frac{1}{4}(g_{11} + e_{13})Tr(\alpha)$$

$$= 4h_{11} + \frac{1}{4}(3g_{11} - e_{13})(g_{11} + e_{13}) + f_{11}(f_{22} + e_{23}) + e_{11}(f_{23} + e_{33})$$

$$\alpha_\perp \cdot \beta_\perp = Tr(\alpha\beta) - \frac{1}{4}(g_{11} + e_{13})Tr(\beta)$$

$$= 4h_{12} - \frac{1}{4}(g_{11} + e_{13})(f_{22} + e_{23}) + e_{12}(f_{23} + e_{33})$$

$$\alpha_\perp \cdot \gamma_\perp = Tr(\alpha\gamma) - \frac{1}{4}(g_{11} + e_{13})Tr(\gamma)$$

$$= 4h_{13} + f_{13}(f_{22} + e_{23}) - \frac{1}{4}(g_{11} - 3e_{13})(f_{23} + e_{33})$$

$$\beta_\perp \cdot \beta_\perp = Tr(\beta^2) - \frac{1}{4}(f_{22} + e_{23})Tr(\beta) = 4h_{22} + g_{22}(g_{11} + e_{13}) + \frac{1}{4}(3f_{22} - e_{23})(f_{22} + e_{23}) + e_{22}(f_{23} + e_{33})$$

$$\beta_\perp \cdot \gamma_\perp = Tr(\beta\gamma) - \frac{1}{4}(f_{22} + e_{23})Tr(\gamma) = 4h_{23} + g_{23}(g_{11} + e_{13}) + f_{23}(f_{22} + e_{23}) - \frac{1}{4}(f_{22} - 3e_{23})(f_{23} + e_{33})$$

$$\gamma_\perp \cdot \gamma_\perp = Tr(\gamma^2) - \frac{1}{4}(f_{23} + e_{33})Tr(\gamma) = 4h_{33} + g_{33}(g_{11} + e_{13}) + f_{33}(f_{22} + e_{23}) - \frac{1}{4}(f_{23} - 3e_{33})(f_{23} + e_{33})$$

Set Q_{ij} as follows:

$$Q_{11} = 4(\alpha_\perp \cdot \alpha_\perp) = 16h_{11} + (3g_{11} - e_{13})(g_{11} + e_{13}) + 4f_{11}(f_{22} + e_{23}) + 4e_{11}(f_{23} + e_{33})$$

$$Q_{12} = 4(\alpha_\perp \cdot \beta_\perp) = 16h_{12} - (g_{11} + e_{13})(f_{22} + e_{23}) + 4e_{12}(f_{23} + e_{33})$$

$$Q_{13} = 4(\alpha_\perp \cdot \gamma_\perp) = 16h_{13} + 4f_{13}(f_{22} + e_{23}) - (g_{11} - 3e_{13})(f_{23} + e_{33})$$

$$Q_{22} = 4(\beta_\perp \cdot \beta_\perp) = 16h_{22} + 4g_{22}(g_{11} + e_{13}) + (3f_{22} - e_{23})(f_{22} + e_{23}) + 4e_{22}(f_{23} + e_{33})$$

$$Q_{23} = 4(\beta_\perp \cdot \gamma_\perp) = 16h_{23} + 4g_{23}(g_{11} + e_{13}) + 4f_{23}(f_{22} + e_{23}) - (f_{22} - 3e_{23})(f_{23} + e_{33})$$

$$Q_{33} = 4(\gamma_\perp \cdot \gamma_\perp) = 16h_{33} + 4g_{33}(g_{11} + e_{13}) + 4f_{33}(f_{22} + e_{23}) - (f_{23} - 3e_{33})(f_{23} + e_{33}).$$

Then $\mathrm{Sh}(\mathcal{O}) = \begin{pmatrix} 1 & \frac{Q_{12}}{Q_{11}} & \frac{Q_{13}}{Q_{11}} \\ \frac{Q_{12}}{Q_{11}} & \frac{Q_{22}}{Q_{11}} & \frac{Q_{23}}{Q_{11}} \\ \frac{Q_{13}}{Q_{11}} & \frac{Q_{23}}{Q_{11}} & \frac{Q_{33}}{Q_{11}} \end{pmatrix}$.

On the forms side, to each pair (A, B) of ternary quadratic forms, we may associate the SL_3-covariant we will call its shape given by:

$$\mathrm{Sh}(A, B) = \begin{pmatrix} 1 & \frac{Q_{12}}{Q_{11}} & \frac{Q_{13}}{Q_{11}} \\ \frac{Q_{12}}{Q_{11}} & \frac{Q_{22}}{Q_{11}} & \frac{Q_{23}}{Q_{11}} \\ \frac{Q_{13}}{Q_{11}} & \frac{Q_{23}}{Q_{11}} & \frac{Q_{33}}{Q_{11}} \end{pmatrix}$$

where

$$Q_{11} = 4a_{23}^2b_{11}^2 - 16a_{22}a_{33}b_{11}^2 - 4a_{13}a_{23}b_{11}b_{12} + 8a_{12}a_{33}b_{11}b_{12} + 3a_{13}^2b_{12}^2 - 8a_{11}a_{33}b_{12}^2 + 8a_{13}a_{22}b_{11}b_{13}$$

$$-4a_{12}a_{23}b_{11}b_{13} - 6a_{12}a_{13}b_{12}b_{13} + 8a_{11}a_{23}b_{12}b_{13} + 3a_{12}^2b_{13}^2 - 8a_{11}a_{22}b_{13}^2 - 8a_{13}^2b_{11}b_{22} + 16a_{11}a_{33}b_{11}b_{22}$$

$$+8a_{11}a_{13}b_{13}b_{22} + 8a_{12}a_{13}b_{11}b_{23} - 8a_{11}a_{23}b_{11}b_{23} - 4a_{11}a_{13}b_{12}b_{23} - 4a_{11}a_{12}b_{13}b_{23} + 4a_{11}^2b_{23}^2 - 8a_{12}^2b_{11}b_{33}$$

$$+16a_{11}a_{22}b_{11}b_{33} + 8a_{11}a_{12}b_{12}b_{33} - 16a_{11}^2b_{22}b_{33}$$

$$Q_{22} = 4a_{13}^2b_{22}^2 - 16a_{11}a_{33}b_{22}^2 - 4a_{13}a_{23}b_{12}b_{22} + 8a_{12}a_{33}b_{12}b_{22} + 3a_{23}^2b_{12}^2 - 8a_{22}a_{33}b_{12}^2 + 8a_{11}a_{23}b_{22}b_{23}$$

$$-4a_{12}a_{13}b_{22}b_{23} - 6a_{12}a_{23}b_{12}b_{23} + 8a_{13}a_{22}b_{12}b_{23} + 3a_{12}^2b_{23}^2 - 8a_{11}a_{22}b_{23}^2 - 8a_{23}^2b_{11}b_{22} + 16a_{22}a_{33}b_{11}b_{22}$$

$$+8a_{22}a_{23}b_{11}b_{23} + 8a_{12}a_{23}b_{13}b_{22} - 8a_{13}a_{22}b_{13}b_{22} - 4a_{22}a_{23}b_{12}b_{13} - 4a_{12}a_{22}b_{13}b_{23} + 4a_{22}^2b_{13}^2 - 8a_{12}^2b_{22}b_{33}$$

$$+16a_{11}a_{22}b_{22}b_{33} + 8a_{12}a_{22}b_{12}b_{33} - 16a_{22}^2b_{11}b_{33}$$

$$Q_{33} = 4a_{12}^2b_{33}^2 - 16a_{11}a_{22}b_{33}^2 - 4a_{12}a_{23}b_{13}b_{33} + 8a_{13}a_{22}b_{13}b_{33} + 3a_{23}^2b_{13}^2 - 8a_{22}a_{33}b_{13}^2 + 8a_{11}a_{23}b_{23}b_{33}$$

$$-4a_{12}a_{13}b_{23}b_{33} - 6a_{13}a_{23}b_{13}b_{23} + 8a_{12}a_{33}b_{13}b_{23} + 3a_{13}^2b_{23}^2 - 8a_{11}a_{33}b_{23}^2 - 8a_{23}^2b_{11}b_{33} + 16a_{22}a_{33}b_{11}b_{33}$$

$$+8a_{23}a_{33}b_{11}b_{23}+8a_{13}a_{23}b_{12}b_{33}-8a_{12}a_{33}b_{12}b_{33}-4a_{23}a_{33}b_{12}b_{13}-4a_{13}a_{33}b_{12}b_{23}+4a_{33}^2b_{12}^2-8a_{13}^2b_{22}b_{33}$$

$$+16a_{11}a_{33}b_{22}b_{33}+8a_{13}a_{33}b_{13}b_{22}-16a_{33}^2b_{11}b_{22}$$

$$Q_{12}=2a_{23}^2b_{11}b_{12}-8a_{22}a_{33}b_{11}b_{12}+a_{13}a_{23}b_{12}^2-2a_{13}a_{22}b_{12}b_{13}-a_{12}a_{23}b_{12}b_{13}+2a_{12}a_{22}b_{13}^2-12a_{13}a_{23}b_{11}b_{22}$$

$$+16a_{12}a_{33}b_{11}b_{22}+2a_{13}^2b_{12}b_{22}-8a_{11}a_{33}b_{12}b_{22}-2a_{12}a_{13}b_{13}b_{22}+12a_{11}a_{23}b_{13}b_{22}+12a_{13}a_{22}b_{11}b_{23}-2a_{12}a_{23}b_{11}b_{23}$$

$$-a_{12}a_{13}b_{12}b_{23}-2a_{11}a_{23}b_{12}b_{23}+a_{12}^2b_{13}b_{23}-12a_{11}a_{22}b_{13}b_{23}+2a_{11}a_{12}b_{23}^2-8a_{12}a_{22}b_{11}b_{33}+16a_{11}a_{22}b_{12}b_{33}$$

$$-8a_{11}a_{12}b_{22}b_{33}$$

$$Q_{13}=2a_{23}^2b_{11}b_{13}-8a_{22}a_{33}b_{11}b_{13}+a_{12}a_{23}b_{13}^2-2a_{12}a_{33}b_{12}b_{13}-a_{13}a_{23}b_{12}b_{13}+2a_{13}a_{33}b_{12}^2-12a_{12}a_{23}b_{11}b_{33}$$

$$+16a_{13}a_{22}b_{11}b_{33}+2a_{12}^2b_{13}b_{33}-8a_{11}a_{22}b_{13}b_{33}-2a_{12}a_{13}b_{12}b_{33}+12a_{11}a_{23}b_{12}b_{33}+12a_{12}a_{33}b_{11}b_{23}-2a_{13}a_{23}b_{11}b_{23}$$

$$-a_{12}a_{13}b_{13}b_{23}-2a_{11}a_{23}b_{13}b_{23}+a_{13}^2b_{12}b_{23}-12a_{11}a_{33}b_{12}b_{23}+2a_{11}a_{13}b_{23}^2-8a_{13}a_{33}b_{11}b_{22}+16a_{11}a_{33}b_{13}b_{22}$$

$$-8a_{11}a_{13}b_{22}b_{33}$$

$$Q_{23}=2a_{13}^2b_{22}b_{23}-8a_{11}a_{33}b_{22}b_{23}+a_{12}a_{13}b_{23}^2-2a_{12}a_{33}b_{12}b_{23}-a_{13}a_{23}b_{12}b_{23}+2a_{23}a_{33}b_{12}^2-12a_{12}a_{13}b_{22}b_{33}$$

$$+16a_{11}a_{23}b_{22}b_{33}+2a_{12}^2b_{23}b_{33}-8a_{11}a_{22}b_{23}b_{33}-2a_{12}a_{23}b_{12}b_{33}+12a_{13}a_{22}b_{12}b_{33}+12a_{12}a_{33}b_{13}b_{22}-2a_{13}a_{23}b_{13}b_{22}$$

$$-a_{12}a_{23}b_{13}b_{23}-2a_{13}a_{22}b_{13}b_{23}+a_{23}^2b_{12}b_{13}-12a_{22}a_{33}b_{12}b_{13}+2a_{22}a_{23}b_{13}^2-8a_{23}a_{33}b_{11}b_{22}+16a_{22}a_{33}b_{11}b_{23}$$

$$-8a_{22}a_{23}b_{11}b_{33}$$

Note:

$$Q_{11}=-16\lambda_{22}^{11}\lambda_{33}^{11}-4\lambda_{13}^{11}\lambda_{23}^{12}+8\lambda_{13}^{11}\lambda_{22}^{13}-4\lambda_{12}^{11}\lambda_{23}^{13}+8\lambda_{12}^{11}\lambda_{33}^{12}+4\lambda_{23}^{11}\lambda_{23}^{11}+3\lambda_{13}^{12}\lambda_{13}^{12}$$

$$=4(\alpha_\perp\cdot\alpha_\perp)$$

$$Q_{22}=16\lambda_{22}^{11}\lambda_{33}^{22}-4\lambda_{13}^{12}\lambda_{23}^{22}-8\lambda_{23}^{11}\lambda_{23}^{22}-4\lambda_{22}^{12}\lambda_{23}^{13}-8\lambda_{22}^{12}\lambda_{33}^{12}+4\lambda_{22}^{13}\lambda_{22}^{13}+3\lambda_{23}^{12}\lambda_{23}^{12}$$

$$= 4(\beta_\perp \cdot \beta_\perp)$$

$$Q_{33} = -16\lambda_{33}^{11}\lambda_{33}^{22} - 4\lambda_{13}^{12}\lambda_{33}^{23} + 8\lambda_{23}^{11}\lambda_{33}^{23} - 4\lambda_{23}^{12}\lambda_{33}^{13} - 8\lambda_{33}^{13}\lambda_{22}^{13} + 4\lambda_{33}^{12}\lambda_{33}^{12} + 3\lambda_{23}^{13}\lambda_{23}^{13}$$

$$= 4(\gamma_\perp \cdot \gamma_\perp)$$

$$Q_{12} = 8\lambda_{12}^{11}\lambda_{33}^{22} - 8\lambda_{33}^{11}\lambda_{22}^{12} - 12\lambda_{13}^{11}\lambda_{23}^{22} + 2\lambda_{23}^{11}\lambda_{23}^{12} - 2\lambda_{13}^{12}\lambda_{22}^{13} + \lambda_{13}^{12}\lambda_{23}^{12}$$

$$= 4(\alpha_\perp \cdot \beta_\perp)$$

$$Q_{13} = -8\lambda_{13}^{11}\lambda_{33}^{22} - 8\lambda_{22}^{11}\lambda_{33}^{13} + 12\lambda_{12}^{11}\lambda_{33}^{23} + 2\lambda_{23}^{11}\lambda_{23}^{13} + 2\lambda_{13}^{12}\lambda_{33}^{12} - \lambda_{13}^{12}\lambda_{23}^{13}$$

$$= 4(\alpha_\perp \cdot \gamma_\perp)$$

$$Q_{23} = 8\lambda_{22}^{11}\lambda_{33}^{23} - 8\lambda_{33}^{11}\lambda_{23}^{22} - 12\lambda_{22}^{12}\lambda_{33}^{13} + 2\lambda_{23}^{12}\lambda_{33}^{12} + 2\lambda_{22}^{13}\lambda_{23}^{13} + \lambda_{23}^{12}\lambda_{23}^{13}$$

$$= 4(\beta_\perp \cdot \gamma_\perp)$$

so the shape of (A, B) is equal to the shape of the associated quartic order.

Discriminant

The discriminant of R is $\frac{Q_{11}^3}{16}\det(\mathrm{Sh}(R)) = 4(\frac{Q_{11}}{4})^3\det(\mathrm{Sh}(R))$.

Acting on Quartic Rings

Here $G_{\mathbb{Z}} = \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ and $V_{\mathbb{Z}} = \{(A, B) = (a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + a_{12}xy + a_{13}xz + a_{23}yz, b_{11}x^2 + b_{22}y^2 + b_{33}z^2 + b_{12}xy + b_{13}xz + b_{23}yz)\}$. In order to see the group action, it's easier to view (A, B) as a pair of symmetric 3×3 matrices,

$$(A, B) = \left(\begin{pmatrix} a_{11} & a_{12}/2 & a_{13}/2 \\ a_{12}/2 & a_{22} & a_{23}/2 \\ a_{13}/2 & a_{23}/2 & a_{33} \end{pmatrix}, \begin{pmatrix} b_{11} & b_{12}/2 & b_{13}/2 \\ b_{12}/2 & b_{22} & b_{23}/2 \\ b_{13}/2 & b_{23}/2 & b_{33} \end{pmatrix} \right).$$

Then for $g \in G_{\mathbb{Z}}$ (or $G_{\mathbb{R}}$), $g = (g_3, g_2) = \left(g_3, \begin{pmatrix} r & s \\ t & u \end{pmatrix} \right)$,

$$g \cdot (A, B) = (r \cdot g_3 A g_3^T + s \cdot g_3 B g_3^T, t \cdot g_3 A g_3^T + u \cdot g_3 B g_3^T).$$

Note if

$$g = \left(\begin{pmatrix} \lambda_3 & 0 & 0 \\ 0 & \lambda_3 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}, \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2 \end{pmatrix} \right),$$

then $g \cdot (A, B) = \lambda_2 \lambda_3^2 (A, B)$.

We also have that for $g = (g_3, g_2) = \left(g_3, \begin{pmatrix} r & s \\ t & u \end{pmatrix} \right)$,

$$\operatorname{Disc}(g \cdot (A, B)) = (\det g_3)^8 (\det g_2)^6 \operatorname{Disc}((A, B)).$$

If we define $f_{(A,B)}(x, y) = 4 \cdot |Ax + By|$, then

$$f_{(g \cdot (A,B))}(x, y) = (\det g_3)^2 \cdot g_2 \cdot f_{(A,B)}(x, y) = (\det g_3)^2 f_{(A,B)}(rx + ty, sx + uy).$$

We see that only the determinants of $\mathrm{GL}_2(\mathbb{R})$ and $\mathrm{GL}_3(\mathbb{R})$ affect the discriminant, and in fact $G_{\mathbb{Z}}$ fixes the discriminant.

Again, $\mathrm{GL}_2(\mathbb{R})$ does not affect the shape at all (it scales each Q_{ij} by $(\det g_2)^2$), and $\mathrm{GL}_3(\mathbb{R})$ acts by conjugation on the symmetric matrix form of the shape: $\mathrm{Sh}(g_3 \cdot v) = g_3 \cdot \mathrm{Sh}(v) = g_3 \, \mathrm{Sh}(v) g_3^T$ (equality as equivalence classes, or else after you factor out the top left entry). Again in the non-symmetric matrix form, the action is simply matrix multiplication, and $\mathrm{Sh}(g \cdot v) = g \cdot \mathrm{Sh}(v) = g \, \mathrm{Sh}(v)$.

It may be worth noting that g_2 sends $\lambda_{kl}^{ij} = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{kl} & b_{kl} \end{vmatrix}$ to $(\det g_2) \lambda_{kl}^{ij}$ which means that in the multiplication table, g_2 scales non-constant coefficients by its determinant and constant coefficients by its determinant squared.

2.3.3 $n = 5$

Parametrization

From [Bha08], we have a bijective correspondence between pairs (R, S) of quintic rings and sextic resolvents and quadruples of skew-symmetric 5×5 matrices.

Again you have a ring with a multiplication table, and again the parametrization involves relating the coefficients in the multiplication table with the coefficients of our forms. But now things are much, much worse. Our multiplication table has 50 potential spots for coefficients (as opposed to 9 for $n = 3$, or 24 for $n = 4$), and our forms have 40 coefficients. So even if things were straightforward, they'd be tough, but things are not at all straightforward.

If you're still here, you're making a fairly large life mistake, though you're better off than I am. The situation for $n = 5$ is a fricking mess. If I make it through here without my head exploding, please send me your congratulations – if your head has also not exploded, that is.

Seriously, the appropriate response is "Oh my goodness what *is* any of this??"

Moving on. Okay, it starts simple enough. $R = \mathbb{Z} \times \alpha_1\mathbb{Z} \times ... \times \alpha_4\mathbb{Z}$ and it corresponds to $v = A = (A_1, A_2, A_3, A_4) \in V_{\mathbb{Z}}$. Do I know what these are? Yes, though I didn't when I started writing this section. The A_i are 5×5 "skew-symmetric" matrices. The transpose of a matrix is what you get when you switch the rows for the columns. A skew-symmetric matrix is one whose negative is its transpose, i.e., $B = -B^T$. In particular, the diagonals are always zero (since they are fixed under transpose). Looking at 3×3 matrices, the transpose of $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ is $\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$. An example of a skew-symmetric 3×3 matrix is $\begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{pmatrix}$.

From there we need to define a few things before we can make sense of the coefficients for the multiplication table. The terms are so long, we'll just have to be happy with formulas.

First thing to learn is the "Pfaffian." I don't know what kind of life you have to lead to have heard of a Pfaffian, but I had to look it up on Wikipedia. You take a skew-symmetric matrix and find its determinant, this happens to be equal to the square of a polynomial in the entries of the matrix. That polynomial is the Pfaffian and it is apparently zero whenever the original matrix had an odd number of rows and columns.

Some determinants:

$$\begin{vmatrix} 0 & a \\ -a & 0 \end{vmatrix} = a^2.$$

$$\begin{vmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{vmatrix} = 0.$$

$$\begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix} = (cd - be + af)^2.$$

The respective Pfaffians would then be $a, 0$, and $af - be + cd$.

The Pfaffian is not necessarily zero for a $2k \times 2k$ skew-symmetric matrix, in which case it is a degree k polynomial over the coefficients of the original matrix.

In particular, taking the Pfaffian of our A_i will just give us zero, which is not very useful. We have to get more creative (er, not we, we're just reading someone else's work). For any 5×5 skew-symmetric matrix X, we will define a vector $Q(X)$, using the Pfaffian as follows:

Let

$$X = \begin{pmatrix} 0 & x_{12} & x_{13} & x_{14} & x_{15} \\ -x_{12} & 0 & x_{23} & x_{24} & x_{25} \\ -x_{13} & -x_{23} & 0 & x_{34} & x_{35} \\ -x_{14} & -x_{24} & -x_{34} & 0 & x_{45} \\ -x_{15} & -x_{25} & -x_{35} & -x_{45} & 0 \end{pmatrix}.$$

Define Q_i to be $(-1)^{i+1}$ times the "4×4 sub-Pfaffian" (i.e., the Pfaffian of the submatrix) of the 4×4 skew-symmetric matrix obtained by removing the ith row and column of X. (If you know how to find the determinant of X, it's similar, but we're going down the diagonal instead of along a row or column.)

For example, for Q_1, we remove the first row and first column and get $\begin{pmatrix} 0 & x_{23} & x_{24} & x_{25} \\ -x_{23} & 0 & x_{34} & x_{35} \\ -x_{24} & -x_{34} & 0 & x_{45} \\ -x_{25} & -x_{35} & -x_{45} & 0 \end{pmatrix}$. Calculating the Pfaffian (we saw the Pfaffian of 4×4 skew-symmetric matrices above), and multiplying by $(-1)^{i+1} = 1$ we get that $Q_1 = x_{25}x_{34} - x_{24}x_{35} + x_{23}x_{45}$. Doing this for $i = 1, 2, 3, 4, 5$ we can now define the vector

$$Q(X) = \begin{bmatrix} Q_1 \\ Q_2 \\ Q_3 \\ Q_4 \\ Q_5 \end{bmatrix} = \begin{bmatrix} x_{25}x_{34} - x_{24}x_{35} + x_{23}x_{45} \\ -x_{15}x_{34} + x_{14}x_{35} - x_{13}x_{45} \\ x_{15}x_{24} - x_{14}x_{25} + x_{12}x_{45} \\ -x_{15}x_{23} + x_{13}x_{25} - x_{12}x_{35} \\ x_{14}x_{23} - x_{13}x_{24} + x_{12}x_{34} \end{bmatrix}$$

Now for Y another 5×5 skew-symmetric matrix (written the same way as X with coefficients y_{ij}) we can define $Q(X, Y) = Q(X + Y) - Q(X) - Q(Y)$ which (if you care) looks like

$$Q(X, Y) = \begin{bmatrix} x_{45}y_{23} - x_{35}y_{24} + x_{34}y_{25} + x_{25}y_{34} - x_{24}y_{35} + x_{23}y_{45} \\ -x_{45}y_{13} + x_{35}y_{14} - x_{34}y_{15} - x_{15}y_{34} + x_{14}y_{35} - x_{13}y_{45} \\ x_{45}y_{12} - x_{25}y_{14} + x_{24}y_{15} + x_{15}y_{24} - x_{14}y_{25} + x_{12}y_{45} \\ -x_{35}y_{12} + x_{25}y_{13} - x_{23}y_{15} - x_{15}y_{23} + x_{13}y_{25} - x_{12}y_{35} \\ x_{34}y_{12} - x_{24}y_{13} + x_{23}y_{14} + x_{14}y_{23} - x_{13}y_{24} + x_{12}y_{34} \end{bmatrix}.$$

Alright, already, am I right? Let's get to the **multiplication table**! Formulas! (Remember, what we're looking for when we say "coefficients for the multiplication table" are the coefficients of the α_i when we multiply the α_i together.)

For $1 \leq i \leq j \leq 4$, we're looking for the c_{ij}^0 and c_{ij}^k found in

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{4} c_{ij}^k \alpha_k.$$

First, we have some terms which are zero:

$$c_{12}^1 = c_{12}^2 = c_{34}^3 = c_{34}^4 = 0.$$

We also have a straightforward (if not simple) formula for the constant coefficents:

$$c_{ij}^0 = \sum_{r=1}^{4} (c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k).$$

Now things get a bit icky. For $i, j, k, l, m \in \{1, 2, 3, 4\}$ define $\{ijklm\} = Q(A_i, A_j)^T \cdot A_k \cdot Q(A_l, A_m)$. Then, for (i, j, k, l) any permutation of $(1, 2, 3, 4)$ (noting the sign of the permutation as indicated by the ± below), close your eyes and do this:

$$c_{ij}^k = \pm\{iiljj\}/4$$

$$c_{ii}^j = \pm\{liiik\}$$

$$c_{ij}^j - c_{ik}^k = \pm\{jklii\}/2$$

$$c_{ii}^i - c_{ij}^j - c_{ik}^k = \pm\{ijlki\}.$$

If you do actually attempt to figure out the coefficients, you'll find some redundancies, because for instance $\{kiiil\} = -\{liiik\}$. You'll also curse me for posting a logic puzzle if you forget that you already know certain coefficients are 0.

The discriminant of A is defined to be the discriminant of the corresponding ring $R(A)$ in terms of the above multiplication table. It's degree 40, so, you know, good luck with that.

Shapes of Quintic Rings

Let $n = 5$. We start with $R = \mathbb{Z} \times \alpha_1\mathbb{Z} \times ... \times \alpha_4\mathbb{Z}$ and its associated $A = (A_1, A_2, A_3, A_4) \in V_{\mathbb{Z}}$, where the A_i are 5×5 skew-symmetric matrices with integer coefficients. To write out a basis for $R_\perp$ and to write the shape explicitly in the totally real case, would take a long time and is not necessarily useful... So, all I can say at the moment is that the shape is still

$$\mathrm{Sh}(R) = \begin{pmatrix} 1 & \frac{\alpha_{1\perp}\cdot\alpha_{2\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{1\perp}\cdot\alpha_{3\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{1\perp}\cdot\alpha_{4\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} \\ \frac{\alpha_{1\perp}\cdot\alpha_{2\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{2\perp}\cdot\alpha_{2\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{2\perp}\cdot\alpha_{3\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{2\perp}\cdot\alpha_{4\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} \\ \frac{\alpha_{1\perp}\cdot\alpha_{3\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{2\perp}\cdot\alpha_{3\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{3\perp}\cdot\alpha_{3\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{3\perp}\cdot\alpha_{4\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} \\ \frac{\alpha_{1\perp}\cdot\alpha_{4\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{2\perp}\cdot\alpha_{4\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{3\perp}\cdot\alpha_{4\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} & \frac{\alpha_{4\perp}\cdot\alpha_{4\perp}}{\alpha_{1\perp}\cdot\alpha_{1\perp}} \end{pmatrix}$$

Acting on Quintic Rings

Here $G_{\mathbb{Z}} = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$ and $V_{\mathbb{Z}} = \{(A_1, A_2, A_3, A_4) : A_i$ are 5×5 skew-symmetric matrices over $\mathbb{Z}\}$.

For $g = (g_4, g_5) \in G_{\mathbb{Z}}$,

$$g \cdot (A_1, A_2, A_3, A_4) = \left(g_4 \begin{pmatrix} g_5 A_1 g_5^T \\ g_5 A_2 g_5^T \\ g_5 A_3 g_5^T \\ g_5 A_4 g_5^T \end{pmatrix} \right)^T .$$

Acting by scalar matrices looks like

$$(\lambda_4 I_4, \lambda_5 I_5) \cdot (A_1, A_2, A_3, A_4) = \lambda_4 \lambda_5^2 (A_1, A_2, A_3, A_4).$$

The discriminant of $(g_4, g_5) \cdot (A_1, A_2, A_3, A_4)$ is equal to $(\det g_4)^{10} (\det g_5)^{16} \operatorname{Disc}(A_1, A_2, A_3, A_4)$.

Chapter 3

Q: What you're doing is weird; you know that, right?

A: It's not normal.

Q: It's more than not normal. It's weird. Some would say unnecessary, risky, maybe even self-destructive.

A: Sure...

Q: I mean, did you ask anyone's advice before you started? What if you fail? What if you fail specifically because you made the totally unnecessary choice to be weird?

A: Look, it's not a choice. Maybe it would be better if it were, I don't know, but I did try on several occasions to do things the right way. I'd think I was writing down, you know, definitions and lemmas and theorems and proofs, that I was doing real math. But if I set it down for more than a day, when I came back to it, I'd find it wholly incomprehensible. And when I look at math that I wrote years ago, it is so clearly full of lies and nonsense that it makes me angry. It makes me actually angry to see my name printed as the author of complete and utter [...] no matter how mathematically proper it looks. The emperor was naked, and so is this.

Counting

$$\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)} = \frac{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X, W)}{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X)} \xrightarrow[X\to\infty]{} \frac{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)}$$

$$= \frac{\prod_p \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod_p \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_1)} \boxed{= \frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)}} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$$

3.1 Laysplaining the Count: One, Two, Three Ha Ha Ha

Pretend, if you will, that we only have ten points to count: $v_1, v_2, ..., v_{10}$. One way to do this, of course, is to line them up and count. Each v_i is the ith in your count. If only it were so simple for what we want to do! Pretend further that we have a lot of trouble counting ten v_i for whatever reason. What if, instead, we had a group G that acted on our v_i so that $g_j v_i = v_{j+i}$. So $g_0 v_1 = v_1, g_1 v_1 = v_2$, etc. (I haven't said what happens if $i + j > 10$, but never mind for now.) This means that each v_i is actually equal to $g_j v_1$ for $j = i - 1$. In other words, our list to count $v_1, v_2, ..., v_{10}$ is the same as the list $g_0 v_1, g_1 v_1, ..., g_9 v_1$. As far as counting is concerned, that list is just the same as $g_0, g_1, ..., g_9$. In other words, under these conditions, counting v_i is the same as instead counting g_j. Similarly, instead of scrambling around trying to get a handle on $V_{\mathbb{Z}}$, we will use our group action which will allow us to focus more on elements of $G_{\mathbb{R}}$ which just happen to be easier to deal with.

Actually we will need to switch to a **new group**, $G'_{\mathbb{R}}$, because of problems mentioned previously with our chosen $G_{\mathbb{R}}$. We don't want to count forms which are equivalent to forms we've already counted, so we'll be looking at $G'_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$, which will require **fundamental domains**, and we won't be able to deal with $G'_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$ all at once because of something called **orbits**. That's just the organizational stuff, though. I spend a lot of time there because I find it confusing and hard to keep track of. The important part is what happens next, though, because even after we're organized, we're not actually going to have something we can just count. We will be forced to **set up the count** by defining a region whose irreducible lattice points are precisely those we wish to count, and we'll **argue a proof** of the count by looking at the relationship between the volume of that region and the number of irreducible lattice points it contains (namely that one approximates the other).

3.1.1 The Formula

In this chapter, we'll find $N(V_{\mathbb{Z}}^{(i)}; X, W)$, the number of inequivalent, irreducible points in $V_{\mathbb{Z}}^{(i)}$ (which is $V_{\mathbb{Z}}$ intersected with a $G_{\mathbb{R}}$-orbit of $V_{\mathbb{R}}$) with the usual discriminant and shape conditions, by defining a region $\mathcal{R}_{X,W}$ and counting points there. The "W" is omitted from our notation in the instance where $W = \mathcal{S}_{n-1}$. We get that $\frac{N(V_{\mathbb{Z}}^{(i)}; X,W)}{N(V_{\mathbb{Z}}^{(i)}; X)} \underset{X\to\infty}{\longrightarrow} \frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)}$. Within the space of shapes, size is denoted by μ and by presuming a postponed calculation (giving $\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$), we'll note the equidistribution result for forms that $\frac{N(V_{\mathbb{Z}}^{(i)}; X,W)}{N(V_{\mathbb{Z}}^{(i)}; X)} \underset{X\to\infty}{\longrightarrow} \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$. Of course, $N(V_{\mathbb{Z}}^{(i)}; X, W)$, is nowhere to be found in the formula, because as was stated at the start of Chapter 2, we use the work of setting up this count and not really the actual result.

3.1.2 Orbits, Stabilizers, and Multisets

Picture yourself in a room full of children (with tangerine trees and marmalade skies?), now ask them to stand in a circle (hopefully you're imagining well-behaved children). Time to play the game $\mathbb{Z}$ Action! For any integer n you give them, the children will move clockwise n positions. If each child started out in front of a chair with his/her name on it, then you can easily determine what each integer does on the set of children. In this case we say that the group acts "transitively" on the children in that there is only one orbit (one circle of kids). If there are 20 children, then any integer that is a multiple of 20 will actually fix the circle (no, it's not broken; I mean that the circle stays fixed in that the end result is the same as the start). The "stabilizer" of any given child is the set of elements of the group that fix the child. In this case, for each child, the stabilizer is $20\mathbb{Z}$ or more generally $(\#\{kids\})\mathbb{Z}$. When you're talking about finite groups, it turns out that the number of elements in an orbit is equal to the number of elements in the group divided by the number of elements in the stabilizer of an element of the orbit. Here, that would look like $20 = \#\mathbb{Z}/\#20\mathbb{Z}$ which is illegal but true-ish in that the twenty children could be representatives of $\mathbb{Z}/20\mathbb{Z}$.

Now let's break the kids up into a few circles of different sizes, say, $4, 6,$ and 10. Now again when you give a number, the children move clockwise, but they have to stay in their own circles. This means that no matter how large of a number you give, a child in the 4-circle will never make it to a spot in the 10-circle. We say, then, that there are three orbits (circles of kids), and it is easy to see that the stabilizer of each child depends on which circle s/he belongs to.

Again let's get unnecessarily weird about things. Suppose we are bizarrely unable to count under normal conditions. Form a circle of ten kids in ten spots and give the teacher the set of numbers 0 through 19. When the teacher calls a number, the children move that number of spaces around the circle. That shows you what a particular group element does to the whole set. Since there is only one orbit, that means that we can get to each child's spot just by acting on a single child. Pick that lucky child and have the teacher call out all the numbers one at a time (allowing the child to return to the original position each time; what's 240 moves between friends?), what does that tell us? Since we do actually have a group action in this setup, we can count group elements, find the stabilizer, and figure out the size of our orbit. Since both 0 and 10 send the child back to the original position, the stabilizer has size 2. We know the group has 20 elements, and thus we have that our orbit has $20/2 = 10$ elements. We just counted our ten children/spots using group action!

If we call our group $G = \{g_j\}_{j=0}^{19}$ and our children $V = \{v_j\}_{j=1}^{10}$, then we saw that $\#G = 20$, $\#V = 10$, $\#Gv_1 = 10$, and $\#\text{stab } v_1 = 2$, and we found that $\#V = \#Gv_1$ (because there's only one orbit) $= \#G/\#\text{stab } v_1$. Since we will be counting by keeping track of group elements, it will sometimes be more helpful to us if by $\#Gv_1$ we actually meant $\#G$, and we get this if we view Gv_1 as a "multiset" rather than as a set. As a multiset, $G \cdot v_1$ gives $\{v_1, v_2, ..., v_{10}, v_1, v_2, ..., v_{10}\}$ even though as a set it is only $\{v_1, v_2, ..., v_{10}\}$ (see Figure 3.1(b)). As a multiset, then, acting on a child with the whole group gives two copies of the orbit of children, and that two comes from the size of the stabilizer.

At any rate, none of this is exactly our situation, obviously, because math. Our group $G_{\mathbb{R}}$ doesn't actually act on $V_{\mathbb{Z}}$ (it sends an element of $V_{\mathbb{Z}}$ to some element of $V_{\mathbb{R}}$ which may or may not have integer coefficients). It would be as though our group could send a child to anywhere in the circle of chairs, not just from one chair to another. Then our Gv isn't ten spots (or two copies of ten spots), but a full circle (or two copies of a full circle), and instead of talking about the number of points in Gv we will talk about its volume (in this case, the circumference of the circle). The basic ideas of orbits, stabilizers, and multisets still apply, but it won't be so straightforward figuring out how to only count integer points (children). We'll end up using additional information we have about the relationship between the size of a region and the number of integer points inside.

When we want to count points in $V_{\mathbb{Z}}$, as mentioned above, we will try to look at $G_{\mathbb{R}}v$ instead, allowing us to focus more on individual group elements rather than individual vectors. We won't be able to look inside $V_{\mathbb{R}}$ all at once like that, though, because $G_{\mathbb{R}}$ does not act transitively on $V_{\mathbb{R}}$; there are in fact $\lfloor n/2 \rfloor + 1$ orbits for $n = 3, 4, 5$. We'll denote an orbit of $V_{\mathbb{R}}$ by $V_{\mathbb{R}}^{(i)}$, and in general an i index will keep track of orbits, so $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$, and $N^{(i)}(\cdot)$ will denote a count of some specified subset of $V_{\mathbb{Z}}^{(i)}$. The cardinality of (which means the number of elements in) the stabilizer of any $v \in V_{\mathbb{R}}^{(i)}$ will be denoted n_i, and $G_{\mathbb{R}}v$ will be viewed as a multiset giving n_i copies of $V_{\mathbb{R}}^{(i)}$. You will see a lot of dividing by n_i around as we attempt to use our group action to count subsets of our orbits $V_{\mathbb{R}}^{(i)}$.

3.1.3 A Brave New Group

In [BST13], [Bha04], [Bha08], the group "$G_{\mathbb{R}}$" is defined so that only one component has scalar multiplication, but which component has it depends on n. Thus, to write it all as one, we've overdone things. We've allowed for both components to have scalar multiplication. This change is not without negative consequences! Remember, the stabilizer is the set of group elements which send a set member to itself. Remember also that if we have a non-trivial stabilizer (more than just the identity element), then the size of the stabilizer tells you how many times we overcount elements of our set when we instead count group elements. We divide by the order of the stabilizer, so in order for things to remain meaningful, a finite stabilizer is of utmost importance. In [BST13], [Bha05], [Bha10], the fundamental domain used overcounted by a factor of n_i, but things will get worse when we use our group.

For example, in the case $n = 4$, we saw above that $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \cdot (A, B) = (4A, 4B)$, and that $\begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \cdot$ $(A, B) = (\frac{1}{4}A, \frac{1}{4}B)$. This means that

$$\left(\begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \right) \cdot (A, B) = (4 \cdot \frac{1}{4}A, 4 \cdot \frac{1}{4}B) = (A, B).$$

In fact, for any $\lambda > 0, (\lambda I_2, \lambda^{-\frac{1}{2}} I_3)$ will send (A, B) to itself. Since there are infinitely many positive real numbers to choose from, we have an infinite stabilizer, which totally ruins everything.

All should not be lost, though. We know we can do what we want to do because it's already been done before. We just need to recover the nice properties of the group action from when there's only one scalar component, but in a way that's related to the group we've chosen to work with.

We might wonder if the solution could be in “factoring out” scalar multiplication from both components, since that’s where the trouble begins. Suppose we look at a group called $G'_{\mathbb{R}}$ which will now have three components: scalar multiplication, $\mathrm{GL}_{n-1}(\mathbb{R})$ restricted to determinant ±1, and $\mathrm{GL}_{r-1}(\mathbb{R})$ restricted to determinant ±1. We’ll write it as $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}^{\pm1}_{n-1}(\mathbb{R}) \times \mathrm{GL}^{\pm1}_{r-1}(\mathbb{R})$.

We should also take a quick look at $G'_{\mathbb{Z}}$. Our original $G_{\mathbb{Z}}$ consisted of restricting $G_{\mathbb{R}}$ to invertible matrices over the integers. Invertibility in this case now means having determinant ±1. Pulling out scalar multiplication, then gives us $\mathbb{G}_m(\mathbb{Z}) \times \mathrm{GL}^{\pm1}_{n-1}(\mathbb{Z}) \times \mathrm{GL}^{\pm1}_{r-1}(\mathbb{Z}) = \{\pm1\} \times G_{\mathbb{Z}}$.

Ideally, $G'_{\mathbb{R}}$ will be essentially the same as $G_{\mathbb{R}}$, but what does that mean and how do we know? We would like the action on $V_{\mathbb{R}}$ to be the same, but with a now finite stabilizer. We need the orbits to be the same. We get these by defining a nice map from our old group to our new group that sends our infinite stabilizer to the kernel of the action on $V_{\mathbb{R}}$. In other words, we’ll send (g_{n-1}, g_{r-1}) to $(\lambda, g'_{n-1}, g'_{r-1})$ in such a way that “up to scalar multiplication” the action on $V_{\mathbb{R}}$ will be the same, and so that any element of $G_{\mathbb{R}}$ that stabilized v gets sent to the identity element in $G'_{\mathbb{R}}$ (accomplished via the “up to scalar multiplication” stipulation which will allow us to make sure that we don’t get canceling scalars out of our two main actions). Sending all of the bad elements to the identity means we get back our finite stabilizer. Since we can write a scalar matrix in terms of its determinant (if $g = \lambda I_d$, then $\det g = \lambda^d$, and so we can also write it as $g = (\det g)^{\frac{1}{d}} I_d$ for $\lambda > 0$, or $g = -|\det g|^{\frac{1}{d}} I_d$ for $\lambda < 0$), we can write formulas for λ which depend on n and give us exactly what we need. For example, the action we’ve been using comes from $n = 4$ in which case we send (g_3, g_2) to $(|\det g_3|^{\frac{2}{3}} |\det g_2|^{\frac{1}{2}}, g'_3, g'_2)$, where $g_k = |\det g_k|^{1/k} g'_k$. This map would send

$$\left(\begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \right) \quad \text{to} \quad (\frac{1}{4} \cdot 4, I_2, I_3) = (1, I_2, I_3).$$

That the orbits remain the same comes from the fact that we’ve kept the same actions, just cut out some of the redundancy.

We got rid of the infinite stabilizer, but we still have some extra stabilizing elements. We factored out scalar multiplication, but only mostly. Each component is still potentially able to scale by -1, which means that they can cancel each other to stabilize an element. For each $n = 3, 4, 5$, the number of extra stabilizing elements is 4, so when we look at $G'_{\mathbb{R}}$ acting on a $v^{(i)} \in V^{(i)}_{\mathbb{R}}$, we’ll get $4n_i$ copies of $V^{(i)}_{\mathbb{R}}$. These four stabilizing elements, however, are all in $G'_{\mathbb{Z}}$ so when we look at a "fundamental domain" for $G'_{\mathbb{R}}$ up to $G'_{\mathbb{Z}}$ and act on $v^{(i)}$ we'll only be overcounting by n_i (which is what our sources had with their versions of $G_{\mathbb{R}}$).

Fixing n, for each $i \in \{0, 1, \ldots, \lfloor n/2 \rfloor\}$, we will pick $v^{(i)} \in V_{\mathbb{R}}^{(i)}$ such that $|\operatorname{Disc}(v^{(i)})| = 1$ and $\operatorname{Sh}(v^{(i)})$ is $\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$. When we act on $v^{(i)}$ by $g \in G_{\mathbb{R}}$, the discriminant will thus be determined only by the scalar component of g and the shape will be the image of g in the space of shapes. This will again allow us to focus only on group elements for counting rather than specific forms, even as we keep track of data that have nothing to do with the group elements themselves.

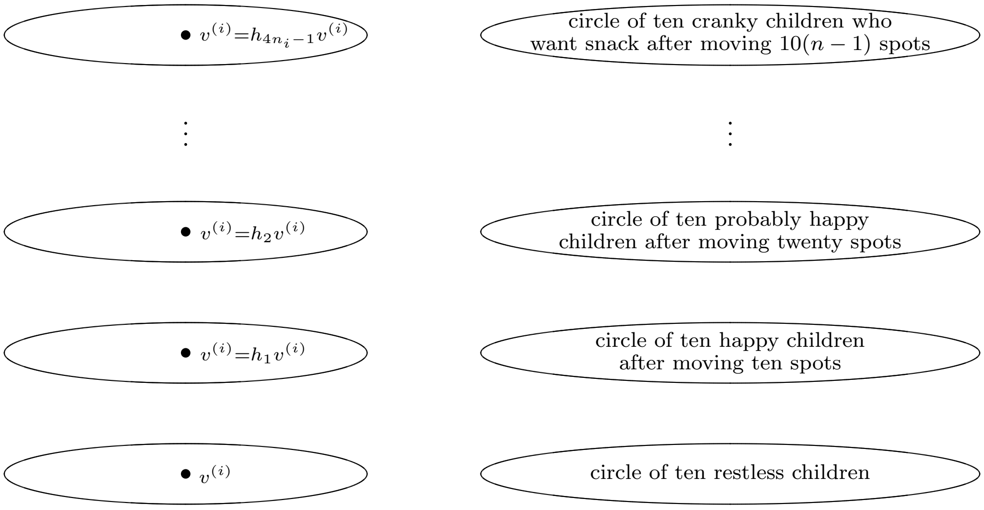
I should also mention that on the rings side of things, these orbits correspond to how the ring splits into real and complex embeddings. Not that I have ever knowingly used this, but you'll see the language around in mathier write-ups.

3.1.4 Fundamental Domains

We've seen that studying $V_{\mathbb{R}}$ can be accomplished by using the group $G'_{\mathbb{R}}$ and looking at how it acts on $V_{\mathbb{R}}$. We saw that when using group actions, we have to count one orbit at a time and keep track of stabilizers. In order to count points in $V_{\mathbb{R}}^{(i)}$, then, we use our nice $v^{(i)} \in V_{\mathbb{R}}^{(i)}$ and act on it by all of $G'_{\mathbb{R}}$. This will give us our whole orbit, and if things were finite, we could say truthfully that the size of our orbit was equal to the size of our group divided by n_i, the size of the stabilizer. We're headed in the right direction, however, we haven't addressed the issue of equivalence at all. Remember, we only want to count equivalence classes mod $G'_{\mathbb{Z}}$ (which corresponds to only counting isomorphism classes of rings and resolvents). How we deal with this extra issue is by looking at fundamental domains.

A fundamental domain is a nice, complete set of representatives. The elements of the group $\mathbb{Z}/10\mathbb{Z}$ are $0+10\mathbb{Z}, 1+10\mathbb{Z}, 2+10\mathbb{Z}, ..., 9+10\mathbb{Z}$, but if we choose a set of representatives, we can instead consider $\mathbb{Z}/10\mathbb{Z}$ to simply be 0, 1, 2, ..., 9. (We have to use the phrase "choose a set of representatives" because as obvious as 0, 1, 2, ..., 9 is, we could also have chosen 10, 11, 12, ..., 19, or worse, we could have chosen 0, 11, 22, ..., 99.) If we have a group acting on a set we can also have a fundamental domain for the set with respect to that action. Two elements of our set are said to be "equivalent" or "G-equivalent" if they differ only by an element of your group, G (notice then that orbits are equivalence classes). Let's go back to our children. Let's say we have one circle of twenty children. Then two children are "$10\mathbb{Z}$-equivalent" if they differ by (a multiple of) ten places (for twenty kids, this means if there are nine children between them, or if they are the same child). A fundamental domain of $10\mathbb{Z}$ acting on 20 kids would be a set of ten inequivalent children, which you can get by taking any ten consecutive kids.

Where oh where to begin? Our goal is to define $\mathcal{F}$ as a fundamental domain for $G'_{\mathbb{Z}}$ acting on $G'_{\mathbb{R}}$, see that $\mathcal{F}v^{(i)}$ is n_i copies of a fundamental domain of $G'_{\mathbb{Z}}$ acting on $V_{\mathbb{R}}^{(i)}$, and to have any of those words make sense. I'm going to start with our nice $v^{(i)} \in V_{\mathbb{R}}^{(i)}$ (which has absolute discriminant 1 and shape the identity matrix) and look at $G'_{\mathbb{R}}v^{(i)}$ as a multiset. You can picture this by picturing a blob representing the orbit $V_{\mathbb{R}}^{(i)}$ and then putting several identical blobs on top of it, for a total of $4n_i$ copies of the same blob. Put a dot for $v^{(i)}$ in each blob and remember each blob is a subset of $G'_{\mathbb{R}}$ acting on that one $v^{(i)}$. If H' is the stabilizer of $v^{(i)}$ in $G'_{\mathbb{R}}$, then you can index the blobs by elements of H' and think of each $v^{(i)}$ as actually being $hv^{(i)}$ for each $h \in H'$.


$v^{(i)}=h_{4n_i-1}v^{(i)}$
$v^{(i)}=h_2v^{(i)}$
$v^{(i)}=h_1v^{(i)}$
$v^{(i)}$
circle of ten cranky children who want snack after moving $10(n-1)$ spots
circle of ten probably happy children after moving twenty spots
circle of ten happy children after moving ten spots
circle of ten restless children

(a) $4n_i$ copies of $V_{\mathbb{R}}^{(i)}$

(b) n copies of a circle of ten kids

Figure 3.1: How to view $G \cdot v$ as a multiset.

Now we need to mod out by $G'_{\mathbb{Z}}$. First of all, we know that this reduces our blob count from $4n_i$ to just n_i copies (where n_i is the size of H, the stabilizer of $v^{(i)}$ in $G_{\mathbb{R}}$). Next, we know that inside $G'_{\mathbb{R}}$ there is a fundamental domain, $\mathcal{F}$, for the action of $G'_{\mathbb{Z}}$. If we look inside $V_{\mathbb{R}}^{(i)}$, $\mathcal{F}v^{(i)}$ is thus a fundamental domain for the action of $G'_{\mathbb{Z}}$ on $V_{\mathbb{R}}^{(i)}$ (since $G'_{\mathbb{R}}v^{(i)}$ gives all of $V_{\mathbb{R}}^{(i)}$). We want to keep track of the number of elements in $\mathcal{F}$, though, so we will view $\mathcal{F}v^{(i)}$ as a multiset, which means we'll have a copy of a fundamental domain for $G'_{\mathbb{Z}}$ acting on $V_{\mathbb{R}}^{(i)}$ in each of our n_i copies of $V_{\mathbb{R}}^{(i)}$. If you wanted to, you could define the set $\mathcal{F}v^{(i)}$ to be equal to $fv^{(i)}$ for an appropriate $f \subset \mathcal{F}$ and then view $\mathcal{F}$ as fH. The important part is that what we want to count can be found inside $\mathcal{F}v^{(i)}$ and since this is viewed as a multiset, we will have to divide by n_i to find the number we actually want.

Omitting discriminant and shape conditions to save room, we have:

$$\begin{aligned}
&\#\text{we want} = \#\{S_n\text{-number fields}\} \\
&\text{which is related to } \#\{\text{pairs } ((R,\alpha_\perp),(S,\beta_\perp)) \text{ up to } G_{\mathbb{Z}}\text{-equivalence}\} \\
&\qquad = \#\{\text{irred. points in } V_{\mathbb{Z}} = V_{\mathbb{R}} \cap V_{\mathbb{Z}} \text{ up to } G_{\mathbb{Z}}\text{-equivalence}\} \\
&\qquad = \#\{\text{irred. points in } \bigcup_{i=0}^{i=\lfloor n/2 \rfloor} V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}} \text{ up to } G_{\mathbb{Z}}\text{-equivalence}\} \\
&\qquad = \sum_{i=0}^{i=\lfloor n/2 \rfloor} \frac{1}{n_i} \times \#\{\text{irred. points in } \mathcal{F}v^{(i)} \cap V_{\mathbb{Z}}\}.
\end{aligned}$$

3.1.5 Setting up the Count

This is where I mentioned mind-blowing-ness earlier. In the sources, you will see a lot more than is about to happen here. Somehow, we don't actually have to calculate any integrals or make any estimates. We can just argue.

I find it helpful to constantly remind myself what on Earth I'm doing and why. For a given $n = 3, 4$, or 5, we want to look at how shapes of number fields of degree n are distributed with respect to their discriminant. As a first step, we will pick a nice region, W, in our space of shapes, $\mathcal{S}_{n-1}$, and count the non-isomorphic ring-pairs whose shapes are in W and whose absolute discriminant is less than X, and then let X go to infinity. We're not counting points in W! We're counting ring-pairs with corresponding points in W. (How many forms correspond to a given shape? Hmm? Does it depend on the shape? Hmm? Rather than answer those questions, we'll just stick to not counting points in W, though for $n = 3$, [BS14] answered this in the "totally real" case.)

Counting ring-pairs, however, is like herding cats (here ring-pair ring-pair ring-pair, here ring-pair ring-pair ring-pair) so instead we look at our forms which are points in $V_{\mathbb{Z}}$, which is a lattice in $V_{\mathbb{R}}$. Our goal for this section will be to prove our equidistribution result for $V_{\mathbb{Z}}$, that the ratio of (certain) points in $V_{\mathbb{Z}}$ with or without a restriction on the shape is equal to a ratio of sizes in the space of shapes.

But, what do we actually do? For each orbit, indexed by i, we want to count irreducible, inequivalent points in $V_{\mathbb{Z}}^{(i)}$ with shape in some nice W in the space of shapes $\mathcal{S}_{n-1}$. We will order our count with respect to the discriminant X which amounts to setting the condition that $|\operatorname{Disc}(x)| < X$ and eventually letting $X \to \infty$. We start by picking a $v^{(i)} \in V_{\mathbb{R}}^{(i)}$ such that its shape in the space of shapes is $\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$, and such that $|\operatorname{Disc}(v^{(i)})| = 1$. Next we need to set up our fundamental domain and define notation to make things easier to talk about.

For any subset $S \subset V_{\mathbb{Z}}$, let $N(S; X, W) = N^{(i)}(S; X, W)$ be the number of irreducible points in $\mathcal{F}v^{(i)} \cap S$ with absolute discriminant less than X and shape in W. This means that the number of equivalence classes of irreducible points in $V_{\mathbb{Z}}$ with absolute discriminant bounded by X and shape in W is equal to

$$\sum_{i=0}^{i=\lfloor n/2 \rfloor} \frac{1}{n_i} N(V_{\mathbb{Z}}^{(i)}; X, W).$$

Setting $W = \mathcal{S}_{n-1}$ is the same as removing the shape condition altogether, and in that case we will suppress the W and use the notation $N^{(i)}(S; X)$.

The points we'll be counting will be elements of $\mathcal{F}v^{(i)} \cap V_{\mathbb{Z}}$, which are all lattice points, but we'd also like to be able to talk about the regions those points live in, namely $\mathcal{F}v^{(i)}$, and we'd like to be able to restrict the discriminant and shape. To help with this, we'll define

$$\mathcal{R}_{X,W} := \{x \in \mathcal{F}v^{(i)} : |\operatorname{Disc}(x)| < X \text{ and } \operatorname{Sh}(x) \in W\},$$

where again we define $\mathcal{R}_X := \mathcal{R}_{X,\mathcal{S}_{n-1}}$. We'll also let $\operatorname{Vol}(\mathcal{R}_{X,W})$ denote the "Euclidean" (i.e., usual) volume of $\mathcal{R}_{X,W}$ as a multiset.

What We Have

There are two different spaces we are dealing with. Our space of shapes, and then our forms $V_{\mathbb{Z}}$ inside the space $V_{\mathbb{R}}$. Whenever you have a "space," you can actually "picture" it. So let's draw our two spaces, and let's go ahead and restrict ourselves to forms with absolute discriminant less than X. (Discriminant is somewhat related to a "size," but it's not something that's going to affect your mental picture.) Rather than picturing all of $V_{\mathbb{R}}$ let's do one orbit at a time and just stick with our fundamental domain, $\mathcal{F}v^{(i)}$, since that's where we'll be counting points. (I prefer to draw it as n_i fundamental domains, since we'll have a bunch of n_i's floating around and it's good to remember why.)

Let's start with the forms we want to count. Since $V_{\mathbb{Z}}$ is a lattice inside $V_{\mathbb{R}}$, you can draw the points we want to count inside $\mathcal{F}v^{(i)}$ as lattice points. Now, each of these points has a corresponding point in the space of shapes. Draw dots representing all the points which actually correspond to points in $V_{\mathbb{Z}}$ (most points in the space of shapes don't).

Let's draw a nice region W inside of our space of shapes, where nice will mean measurable and whose boundary has measure zero. (Measurable is just mathspeak for reasonable. For an example of a measurable subset of $V_{\mathbb{R}}$, picture the blob $V_{\mathbb{R}}$ and then picture any subregion. Unless you are experienced and successful at being mathematically difficult, your subregion is most assuredly measurable. Similarly, the boundary of anything you can picture has measure zero.) The "pre-image" of a dot in the space of shapes is the set of vectors which correspond to it. The pre-image of all the dots is all of $V_{\mathbb{Z}}$ (or in our case, looking only up to $G_{\mathbb{Z}}$-equivalence, the pre-image is all of $\mathcal{F}v^{(i)} \cap V_{\mathbb{Z}}$ (unioned over i)). The pre-image of W inside $V_{\mathbb{R}}$ will also be a nice region (not obvious from what I've said, but basically the shape function is "nice enough"), so go ahead and draw the pre-image. (If you're keeping track of the multiple fundamental domains, you'll have a region in each.) Since we have bounded discriminant, our whole picture of $\mathcal{F}v^{(i)}$ is actually our $\mathcal{R}_X$ defined above, and the pre-image of W again with the discriminant condition gives us $\mathcal{R}_{X,W}$. Then we have that $N(V_{\mathbb{Z}}^{(i)};X)$ is the number of lattice points in $\mathcal{R}_X$ (this count has already been done by others) and $N(V_{\mathbb{Z}}^{(i)};X,W)$ is the number of lattice points in $\mathcal{R}_{X,W}$.

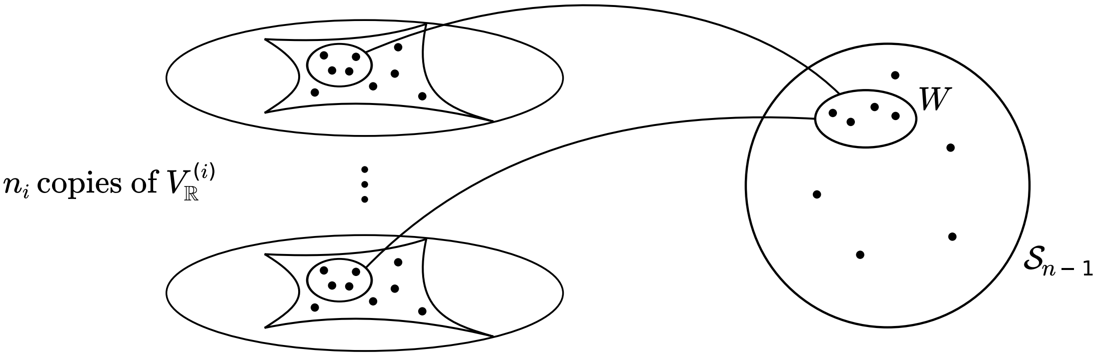


Figure 3.2: On the left, n_i copies of $V_{\mathbb{R}}^{(i)}$, each with a set of points in the soon-to-be-seen-as-cusp-y $\mathcal{F}v^{(i)}$ and the pre-image of W. On the right, $\mathcal{S}_{n-1}$ and a nice region W.

What we want to show is that

$$\frac{N(V_{\mathbb{Z}}^{(i)};X,W)}{N(V_{\mathbb{Z}}^{(i)};X)} = \frac{\text{size of } W}{\text{size of whole space of shapes}} \qquad \text{as } X \to \infty.$$

Where Would We Even Begin

We want to count lattice points in a region. Let's start with just lattice points in a disk in the plane. This is "Gauss's Circle Problem" and it turns out that it is in fact the case that the number of lattice points inside a disk is approximately the area of the disk.

If you let things get a bit more complicated, we have a lemma from Davenport [Dav51a] which gives the same result for a closed and bounded region $\mathcal{R}$ which is allowed to be funkier than a disk in the plane.

What's The Catch?

As it turns out, $\mathcal{R}_X$ is neither a disk in the plane nor a Davenport-lemma-appropriate reigion, and $\mathcal{R}_{X,W}$ could be even worse. What is $\mathcal{R}_X$'s problem anyway? Unbounded-cusp-i-ness. Bounded means essentially that you can draw a circle (if we're in the plane) that contains your region (and if you liked it, then you should've drawn a ring around it). If you had a region that went off to infinity in one direction, you would not be able to enclose it inside any circle/sphere/what-have-you. This region could still have finite volume, though, so even though it is not technically bounded, you might suspect Davenport's lemma to hold, and in fact it does! (With some work.)

Our goal for $\mathcal{R}_{X,W}$ is the same as the goal had been for $\mathcal{R}_X$ which is the same as for Gauss's Circle Problem. You want to show that # pts $\approx$ vol. It's been shown for $\mathcal{R}_X$ but that doesn't automatically make it true for $\mathcal{R}_{X,W}$. We need to look at why it's true for $\mathcal{R}_X$ to see if the same reasoning applies or which elements of the proof can be borrowed and perhaps modified for our needs.

You can think of $\mathcal{R}_X$ as being something nice, but with cusps off to infinity. What is a cusp? Imagine a long thin region going off forever and getting thinner and thinner as it goes, approaching an asymptote from two sides (and in fact, the region gets so thin so fast, the volume is finite). If the asymptote coincides with a line of lattice points, you automatically get infinitely many points. If the asymptote stays between the lattice points, you could pick up zero points. Either way, the volume of the cusp will mess things up if you have to include it.

Let's break up $\mathcal{R}_X$ into $\mathcal{R}_X^{\text{good}}$ and $\mathcal{R}_X^{\text{bad}}$ where Davenport's lemma will hold for $\mathcal{R}_X^{\text{good}}$ and the cusps are contained in $\mathcal{R}_X^{\text{bad}}$. Davenport tells us that the number of points in $\mathcal{R}_X^{\text{good}}$ is approximately the volume, or slightly more precisely,

$$\#\text{ points in } \mathcal{R}_X^{\text{good}} = \text{Vol}(\mathcal{R}_X^{\text{good}}) + E_X,$$

where E_X is an error term related to X. (In the weeds (3.3.4) we'll define the error term $o(X)$ which will replace E_X in the mathsplanations.) To get that # points in $\mathcal{R}_X = \text{Vol}(\mathcal{R}_X) + E_X$, we need both the number of points and the volume of $\mathcal{R}_X^{\text{bad}}$ to be contained in the error term E_X. Getting the volume right is just a matter of splitting up $\mathcal{R}_X$ properly in the first place. The number of points in $\mathcal{R}_X^{\text{bad}}$ is a problem, though, as we already saw it could have infinitely many points. This is where we need to remember that in our case, we are not counting all lattice points. Instead, we're counting certain irreducible points and it will turn out that there are very few of those in the cusps.

3.1.6 Arguing a Proof

What do we know about $\mathcal{R}_{X,W}$ and how can we use what we know about $\mathcal{R}_X$? Before we do anything, we can switch from thoughts of $\mathcal{R}_X$ and $\mathcal{R}_{X,W}$ to thoughts of $\mathcal{R}_1$ and $\mathcal{R}_{1,W}$. We know that this is just shrinking everything by a factor of X (see §3.3.3), so this is an easy simplification. Now, in order to use Davenport, and break up $\mathcal{R}_{1,W}$ into its good and bad components, we'd really have to, as I said, get into the weeds of it all. What we need is something Davenporty enough, but that incorporates our specific situation. Namely, that the number of irreducible lattice points in a bounded subregion of $V_{\mathbb{R}}$ is approximately equal to its volume (as we let its size grow to infinity). This is Lemma 6, and its proof does require going into the weeds for each case to see what happens to the reducible points (postponed until Chapter 5).

Once we know that our # pts $\approx$ vol result holds for nice, bounded regions of $\mathcal{R}_1$ we can think about $\mathcal{R}_{1,W}$. Now we know $\mathcal{R}_{1,W}$ is not necessarily bounded, but we can always create a nice bounded subregion. How do we do that? By definition! We create $\mathcal{R}'_{1,W}$ a bounded subset of $\mathcal{R}_{1,W}$ which is almost the whole thing by volume. We then do the exact same thing for $\mathcal{R}_{1,\overline{W}}$. Making clever (or mundane, depending on your expertise) use of an epsilon, we'll get clever/mundane inequalities for our result for $\mathcal{R}_{1,W}$ and $\mathcal{R}_{1,\overline{W}}$ and use the fact that we have the result for $\mathcal{R}_1 = \mathcal{R}_{1,W} + \mathcal{R}_{1,\overline{W}}$ to prove equality.

3.2 How Mathematicians Count

3.2.1 Definitions

In the laysplanations, we introduced the following definitions and facts, which come from [BST13], [Bha04], [Bha05], [Bha08], [Bha10]. We defined $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R}) \times \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})$ and $G'_{\mathbb{Z}} = \{\pm 1\} \times G_{\mathbb{Z}}$. Under the action of $G'_{\mathbb{R}}$, $V_{\mathbb{R}}$ breaks up into $\lfloor n/2 \rfloor + 1$ orbits we'll call $V^{(i)}_{\mathbb{R}}$, and any Subset$^{(i)}$ will be that Subset $\cap V^{(i)}_{\mathbb{R}}$. We picked $v^{(i)} \in V^{(i)}_{\mathbb{R}}$ to have the nice properties that $|\operatorname{Disc}(v^{(i)})| = 1$ and $\operatorname{Sh}(v^{(i)})$ is $\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix}$, and we stated that the cardinality of the stabilizer of $v^{(i)}$ in $G'_{\mathbb{R}}$ was $4n_i$ which was 4 times the size of the stabilizer of $v^{(i)}$ in $G_{\mathbb{R}}$. We defined $\mathcal{F}$ to be a fundamental domain for $G'_{\mathbb{Z}}$ acting on $G'_{\mathbb{R}}$ and stated that this meant that $\mathcal{F}v^{(i)}$ as a multiset was n_i copies of a fundamental domain for the action of $G'_{\mathbb{Z}}$ on $V^{(i)}_{\mathbb{R}}$.

For any $S \subset V_{\mathbb{Z}}$ and for $W \subset \mathcal{S}_{n-1}$ measurable and with a measure zero boundary, we also let $N^{(i)}(S; X, W)$ be the number of irreducible points in $\mathcal{F}v^{(i)} \cap S$ with absolute discriminant less than X and with shape in W. The W will be suppressed whenever there is no restriction on shape, and the i will be suppressed whenever it is still clear that we'll be counting per orbit.

We saw that counting points in $\mathcal{F}v^{(i)}$ takes care of our "up to $G'_{\mathbb{Z}}$ equivalence" condition and gives us n_i times the number we actually want. We also motivated the need to define

$$\mathcal{R}_{X,W} := \{x \in \mathcal{F}v^{(i)} : |\operatorname{Disc}(x)| < X \text{ and } \operatorname{Sh}(x) \in W\},$$

where we would use $\operatorname{Vol}(\mathcal{R}_{X,W})$ to denote the Euclidean volume of $\mathcal{R}_{X,W}$ as a multiset. Again $\mathcal{R}_X$ is just $\mathcal{R}_{X,W}$ where all shapes are allowed.

3.2.2 Theorems

Theorem 4 ([Dav51b, p. 183], [Bha05, p. 1037], [Bha10, p. 1583])**.** *For $n = 3, 4, 5$, the number of inequivalent, irreducible points in $V^{(i)}_{\mathbb{Z}}$ with absolute discriminant bounded by X, denoted $N(V^{(i)}_{\mathbb{Z}}; X)$, is approximately equal to (i.e., up to $o(X)$) the volume of $\mathcal{R}_X$ divided by n_i, which in turn is equal to $\dfrac{1}{n_i}\operatorname{Vol}(\mathcal{R}_1) \cdot X + o(X)$.*

Actually there are tons and tons of lattice points in $\mathcal{R}_X$! Way more than its volume! This is due to its unbounded-cusp-ness, which in our case picks up all of the points. The great news, though, is these excess points are essentially all reducible. Once we restrict ourselves only to irreducible points, we start getting the results we want.

The main work of this section is to use Theorem 4 to prove the shape version of that result:

Theorem 5. *For $n = 3, 4, 5$, the number of inequivalent, irreducible points in $V_{\mathbb{Z}}^{(i)}$ with absolute discriminant bounded by X and shape in a nice region W, denoted $N(V_{\mathbb{Z}}^{(i)}; X, W)$, is approximately equal (up to $o(X)$) to the volume of $\mathcal{R}_{X,W}$ divided by n_i, which in turn is equal to $\frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X)$.*

The Davenporty lemma we need to prove this is the following. (Recall that for $n = 3, 4, 5$, the discriminant of $v \in V_{\mathbb{R}}$ is a homogeneous polynomial of degree $d = 4, 12, 40$, respectively, in the coefficients of v, and that d is also the dimension of $V_{\mathbb{R}}$.)

Lemma 6. *For H any bounded, measurable set in $V_{\mathbb{R}}$, scale H by a real number z and let z go to infinity. Looking at lattice points in zH, we get that the number of irreducible lattice points in zH is $\operatorname{Vol}(zH) + o(z^d)$ as $z \to \infty$ (i.e., the number of irreducible points is essentially equal to the volume).*

Proof. We already know from Davenport [Dav51a] that the number of lattice points (reducible and irreducible combined) in a region is essentially the volume of the region, as your parameter goes to infinity, so the main point of this lemma is that the number of reducible lattice points in zH becomes negligible as z goes to infinity.

There are (at most) two ways to bound reducible points in $\mathcal{R}_X$ based on the information bestowed to us by our sources.

1. For $n = 3, 4, 5$, using an argument from [Bha10, §3.2], we can see that reducible rings must satisfy certain congruence conditions (more in the weeds, §5.3.4), and thus we can bound the number of reducible points based on the relevant densities given in [BST13], [Bha04], [Bha08].

2. For $n = 3, 5$ [Dav51b], [Dav51c], and [Bha10] provide bounds for reducible points without using congruence conditions.

Either way we get that the number of reducible points in $\mathcal{R}_X$ is at most $o(X)$ as X goes to infinity, now we just need to relate that to zH.

For any $v \in V_{\mathbb{R}}$, we can define $\mathcal{R}_X(v) := \{x \in \mathcal{F}v : |\operatorname{Disc}(x)| < X\}$, where $\mathcal{F}v$ is still n_i copies of a fundamental domain for the action of $G'_{\mathbb{Z}}$ on $V_{\mathbb{R}}^{(i)}$. Our set H may not be contained in $\mathcal{F}v$ for any given $v \in V_{\mathbb{R}}$, but because H is bounded, it will be contained in at most finitely many such fundamental domains.

What happens when we scale H by z? Well, since $\mathcal{F}$ contains scalar multiplication (by positive real numbers), zH will still be contained in the same finite set of fundamental domains. Now things are starting to approach something we know (others know) how to count. Again because H is bounded, there exists an X such that all points in H have absolute discriminant bounded by X, therefore zH will be contained in a finite union of $\mathcal{R}_X(v)$. This is happy news because we have estimates on the number of reducible points in any such $\mathcal{R}_X(v)$. Scaling H by z scales our discriminant by z^d, therefore we'll be looking for points in a finite union of $\mathcal{R}_{z^d X}(v)$. In the sources you can see the specific estimates for each $n = 3, 4, 5$, but at the end what we get is that the number of reducible lattice points in zH is $o(z^d X) = o(z^d)$ (see §3.3.4). □

3.2.3 Proof of Theorem 5

We want to prove that

$$N(V_{\mathbb{Z}}^{(i)}; X, W) = \frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_{X,W}) + o(X),$$

which, as we see in §3.3.3, is equal to

$$\frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X).$$

This is the same thing as saying that the number of irreducible integral points in $\mathcal{R}_{X,W}$ is approximately equal to its volume. Since this is actually n_i copies of the same thing, we have to divide by n_i to get what we want to know about our forms, namely $N(V_{\mathbb{Z}}^{(i)}; X, W)$. We already know this result for $\mathcal{R}_X$, that

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_X) + o(X) = \frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_1) \cdot X + o(X).$$

Proof of Theorem 5. Start with W, a nice but not necessarily bounded subset of the space of shapes. Let $\mathcal{R}'_{1,W}$ be a bounded, measurable subset of $\mathcal{R}_{1,W}$ whose volume is almost the same as that of $\mathcal{R}_{1,W}$. More precisely, for any $\epsilon > 0$, we have that $\operatorname{Vol}(\mathcal{R}_{1,W'}) \geq \operatorname{Vol}(\mathcal{R}_{1,W}) - \epsilon$.*

*Laysterisk: For instance, if $\mathcal{R}_{1,W}$ has volume 10 (whatever that means), and ϵ is 1, then choose $\mathcal{R}'_{1,W}$ to have volume 9.5 and you get that the volume of the smaller region is greater than the volume of the bigger region less ϵ, i.e., $9.5 \geq 10 - 1$.

Since $\mathcal{R}'_{1,W}$ is bounded our Davenporty lemma 6 says that the number of irreducible lattice points in

$\mathcal{R}'_{X,W} := X^{1/d} \cdot \mathcal{R}_{1,X}$ is equal to $\dfrac{1}{n_i}\operatorname{Vol}(\mathcal{R}'_{1,W}) \cdot X + o(X)$ (remembering that $\mathcal{R}_{1,W}$ is a multiset). The number we want to find is $N(V_{\mathbb{Z}}^{(i)}; X, W)$ and we know that there will be more points in $\mathcal{R}_{X,W}$ than in a subset, so we know

$$N(V_{\mathbb{Z}}^{(i)}; X, W) \geq \ \#\{\text{irred lattice pts in } \mathcal{R}'_{X,W}\} = \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}'_{1,W}) \cdot X + o(X) \geq \frac{1}{n_i}(\operatorname{Vol}(\mathcal{R}_{1,W}) - \epsilon) \cdot X + o(X).$$

Funny thing about ϵ is that if this is true for all ϵ, as it is, then it must be true without the ϵ as well. (Otherwise, there would be an ϵ that didn't work.) This means that

$$N(V_{\mathbb{Z}}^{(i)}; X, W) \geq \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X).$$

In other words, the number we want to find is greater than or equal to what we want to prove the number is. That's math for you. Now let's do it again, but looking at $\overline{W}$.

Let $\overline{W}$ be the complement of W in the space of shapes. Then running the exact same argument as above, what we get is that

$$N(V_{\mathbb{Z}}^{(i)}; X, \overline{W}) \geq \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,\overline{W}}) \cdot X + o(X).$$

Since the space of shapes is equal to the union of W and $\overline{W}$ (and there's no overlap), we know that $\operatorname{Vol}(\mathcal{R}_1) = \operatorname{Vol}(\mathcal{R}_{1,W}) + \operatorname{Vol}(\mathcal{R}_{1,\overline{W}})$, and that $N(V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X, W) + N(V_{\mathbb{Z}}^{(i)}; X, \overline{W})$. Adding up our two inequalities, then, we get

$$N(V_{\mathbb{Z}}^{(i)}; X, W) + N(V_{\mathbb{Z}}^{(i)}; X, \overline{W}) \geq \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X + \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,\overline{W}}) \cdot X + o(X),$$

i.e.,

$$N(V_{\mathbb{Z}}^{(i)}; X) \geq \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_1) \cdot X + o(X).$$

Of course, we already know that $N(V_{\mathbb{Z}}^{(i)}; X)$ is exactly (ha) equal to $\dfrac{1}{n_i}\operatorname{Vol}(\mathcal{R}_1) \cdot X + o(X)$, therefore our inequalities about W and $\overline{W}$ must actually be equalities. In other words, we have just shown that the number of irreducible points with bounded absolute discriminant and shape in W is approximately equal to the volume of the region these points live in (remembering that $\mathcal{R}_{X,W}$ overcounted things by a factor of n_i), or, mathily:

$$N(V_{\mathbb{Z}}^{(i)}; X, W) = \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X).$$

□

3.2.4 $N(V_{\mathbb{Z}}^{(i)}; X, W)$ Ain't Nothin' But a Number a.k.a. How's That Distributing For Ya?

At the end of the day we will want to show that the number of degree n number fields with shape in a nice W is proportional to the size of W when ordered by discriminant, which is what it means to say the shapes are equidistributed. We will get that by counting the number of fields with the shape condition imposed and dividing by the total number of fields and seeing that as the discriminant goes to infinity, this ratio is equal to the ratio of the size of W to the size of the whole space of shapes. We will get a few preliminary counts before we get to number fields, though, and for each of those counts we will also have such an equidistribution result, presuming the following from Chapter 6:

Theorem 7. $\dfrac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_1)} = \dfrac{\textit{size of } W}{\textit{size of the space of shapes}}.$

Above, we just learned that $N(V_{\mathbb{Z}}^{(i)}; X, W) = \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X)$, and we already knew that $N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_1) \cdot X + o(X)$. Another way to write this is to say that

$$\lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X, W)}{X} = \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,W})$$

and similarly,

$$\lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X} = \frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_1).$$

Now let's take a ratio:

$$\lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X, W)/X}{N(V_{\mathbb{Z}}^{(i)}; X)/X} = \frac{\frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,W})}{\frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_1)}.$$

In other words, we have that

$$\lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X, W)}{N(V_{\mathbb{Z}}^{(i)}; X)} = \frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_1)}.$$

Theorem 7 is thus precisely what we need to have equidistribution for our forms with bounded discriminant and shape in W (when ordered by discriminant):

Corollary 7.1. $\lim_{X\to\infty} \dfrac{N(V_{\mathbb{Z}}^{(i)}; X, W)}{N(V_{\mathbb{Z}}^{(i)}; X)} = \dfrac{\textit{size of } W}{\textit{size of the space of shapes}}.$

3.3 The Counting Weeds

This section is organized by topic and walks you through the new group, fundamental domains, and a bit about the region $\mathcal{R}_{X,W}$.

3.3.1 New Group Action

$n = 3$

Non-degenerate cubic rings R can be embedded into one of two possible ring structures on $\mathbb{R}^3$, namely $\mathbb{R}^3$ and $\mathbb{R} \times \mathbb{C}$. For $i = 0, 1$, if $v \in V_{\mathbb{Z}}^{(i)}$ corresponds to (R, S), then $R \otimes \mathbb{R}$ is isomorphic to $\mathbb{R}^{3-2i} \times \mathbb{C}^i$. This happens to correspond with the sign of the discriminant, with positive discriminants corresponding to $i = 0$, the totally real case, and negative discriminants corresponding to $i = 1$.

The action of $G_{\mathbb{R}} = \mathrm{GL}_2(\mathbb{R}) \times \mathrm{GL}_1(\mathbb{R})$ on $V_{\mathbb{R}}$ has infinite kernel, therefore we instead use $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}_2^{\pm 1}(\mathbb{R}) \times \mathrm{GL}_1^{\pm 1}(\mathbb{R})$ (where the $^{\pm 1}$ denotes the restriction to elements with determinant equal to ± 1, and $\mathrm{GL}_1^{\pm 1}(\mathbb{R})$ is simply $\{\pm 1\}$). The action of $G'_{\mathbb{R}}$ on $V_{\mathbb{R}}$ is essentially the same, producing the same orbits, but now scalar multiplication occurs in a separate component, $\mathbb{G}_m(\mathbb{R})$, and the only scaling that can come from the other two components is a possible -1 factor. If $g' = (\lambda, g'_2, g'_1) \in G'_{\mathbb{R}}$, then $(g'_2, g'_1) \in G_{\mathbb{R}}$ and $(\lambda, g'_2, g'_1) \cdot v$ is just λ times whatever $(g'_2, g'_1) \cdot v$ was. To see that things are essentially the same, we notice that the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ "factors through" that of $G'_{\mathbb{R}}$ via the map which sends (g_2, g_1) to $\big(|\det g_2|^{3/2} |\det g_1|,\ g'_2,\ g'_1\big)$, where $g_k = |\det g_k|^{1/k} g'_k$.

Important to note is that for $g' = (\lambda, g'_2, g'_1) \in G'_{\mathbb{R}}$, we have $\mathrm{Disc}(g' \cdot v) = \lambda^4 \,\mathrm{Disc}(v)$ where the exponent comes from the dimension of $V_{\mathbb{R}}$, and $\mathrm{Sh}(g' \cdot v) = g'_2 \cdot \mathrm{Sh}(v)$ where the action on the shape depends on how we're viewing the shape. For the purposes of our calculation in Chapter 6, the action will just be matrix multiplication, as we will not consider the symmetric matrix representation. The size of the stabilizer in $G'_{\mathbb{R}}$ of any $v^{(i)} \in V^{(i)}$ is $4n_i$ where $n_0 = 6$ and $n_1 = 2$ are the sizes of the stabilizers of $v^{(i)}$ in $G_{\mathbb{R}}$ and the extra factor of 4 comes from extra stabilizing elements inside $G'_{\mathbb{Z}}$, namely $(1, I_2, 1), (-1, -I_2, 1), (-1, I_2, -1), (1, -I_2, -1)$.

Restricting to integers gives $G'_{\mathbb{Z}} = \mathbb{G}_m(\mathbb{Z}) \times \mathrm{GL}_2^{\pm 1}(\mathbb{Z}) \times \mathrm{GL}_1^{\pm 1}(\mathbb{Z})$, where $\mathbb{G}_m(\mathbb{Z})$ and $\mathrm{GL}_1^{\pm 1}(\mathbb{Z})$ are both just $\{\pm 1\}$.

$n = 4$

Non-degenerate quartic rings R can be embedded into one of three possible ring structures on $\mathbb{R}^4$, namely $\mathbb{R}^4$, $\mathbb{R}^2 \times \mathbb{C}$, and $\mathbb{C}^2$. For $i = 0, 1, 2$, if $v \in V_{\mathbb{Z}}^{(i)}$ corresponds to (R, S), then $R \otimes \mathbb{R}$ is isomorphic to $\mathbb{R}^{4-2i} \times \mathbb{C}^i$.

The action of $G_{\mathbb{R}} = \mathrm{GL}_3(\mathbb{R}) \times \mathrm{GL}_2(\mathbb{R})$ on $V_{\mathbb{R}}$ has infinite kernel, therefore we instead use $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}_3^{\pm 1}(\mathbb{R}) \times \mathrm{GL}_2^{\pm 1}(\mathbb{R})$ (where the ${}^{\pm 1}$ denotes the restriction to elements with determinant equal to ± 1). The action of $G'_{\mathbb{R}}$ on $V_{\mathbb{R}}$ is essentially the same, producing the same orbits, but now scalar multiplication occurs in a separate component, $\mathbb{G}_m(\mathbb{R})$, and the only scaling that can come from the other two components is a possible -1 factor from the $\mathrm{GL}_2(\mathbb{R})$ component ($\mathrm{GL}_3(\mathbb{R})$ acts by the fake-transpose-conjugation action given by $g \cdot A = gAg^T$). If $g' = (\lambda, g'_3, g'_2) \in G'_{\mathbb{R}}$, then $(g'_3, g'_2) \in G_{\mathbb{R}}$ and $(\lambda, g'_3, g'_2) \cdot v$ is just λ times whatever $(g'_3, g'_2) \cdot v$ was. To see that things are essentially the same, we notice that the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ "factors through" that of $G'_{\mathbb{R}}$ via the map which sends (g_3, g_2) to $\big(|\det g_3|^{2/3} |\det g_2|^{1/2},\ g'_3,\ g'_2\big)$, where $g_k = |\det g_k|^{1/k} g'_k$.

Important to note is that for $g' = (\lambda, g'_3, g'_2) \in G'_{\mathbb{R}}$, we have $\mathrm{Disc}(g' \cdot v) = \lambda^{12} \mathrm{Disc}(v)$ where the exponent comes from the dimension of $V_{\mathbb{R}}$, and $\mathrm{Sh}(g' \cdot v) = g'_3 \cdot \mathrm{Sh}(v)$ where the action on the shape depends on how we're viewing the shape. For the purposes of our calculation in Chapter 6, the action will just be matrix multiplication, as we will not consider the symmetric matrix representation.

The size of the stabilizer in $G'_{\mathbb{R}}$ of any $v^{(i)} \in V^{(i)}$ is $4n_i$ where $n_0 = 24, n_1 = 4$, and $n_2 = 8$ are the sizes of the stabilizers of $v^{(i)}$ in $G_{\mathbb{R}}$ and the extra factor of 4 comes from extra stabilizing elements inside $G'_{\mathbb{Z}}$, namely $(1, I_3, I_2), (1, -I_3, I_2), (-1, I_3, -I_2), (-1, -I_3, -I_2)$.

Restricting to integers gives $G'_{\mathbb{Z}} = \mathbb{G}_m(\mathbb{Z}) \times \mathrm{GL}_3^{\pm 1}(\mathbb{Z}) \times \mathrm{GL}_2^{\pm 1}(\mathbb{Z})$, where $\mathbb{G}_m(\mathbb{Z})$ is just $\{\pm 1\}$.

$n = 5$

Non-degenerate quintic rings R can be embedded into one of three possible ring structures on $\mathbb{R}^5$, namely $\mathbb{R}^5$, $\mathbb{R}^3 \times \mathbb{C}$, and $\mathbb{R} \times \mathbb{C}^2$. For $i = 0, 1, 2$, if $v \in V_{\mathbb{Z}}^{(i)}$ corresponds to (R, S), then $R \otimes \mathbb{R}$ is isomorphic to $\mathbb{R}^{5-2i} \times \mathbb{C}^i$.

The action of $G_{\mathbb{R}} = \mathrm{GL}_4(\mathbb{R}) \times \mathrm{GL}_5(\mathbb{R})$ on $V_{\mathbb{R}}$ has infinite kernel, therefore we instead use $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times$

$\mathrm{GL}_4^{\pm 1}(\mathbb{R}) \times \mathrm{GL}_5^{\pm 1}(\mathbb{R})$ (where the $^{\pm 1}$ denotes the restriction to elements with determinant equal to ±1). The action of $G'_{\mathbb{R}}$ on $V_{\mathbb{R}}$ is essentially the same, producing the same orbits, but now scalar multiplication occurs in a separate component, $\mathbb{G}_m(\mathbb{R})$, and the only scaling that can come from the other two components is a possible -1 factor from the $\mathrm{GL}_4(\mathbb{R})$ component ($\mathrm{GL}_5(\mathbb{R})$ acts by the fake-transpose-conjugation action given by $g \cdot A = gAg^T$). If $g' = (\lambda, g'_4, g'_5) \in G'_{\mathbb{R}}$, then $(g'_4, g'_5) \in G_{\mathbb{R}}$ and $(\lambda, g'_4, g'_5) \cdot v$ is just λ times whatever $(g'_4, g'_5) \cdot v$ was. To see that things are essentially the same, we notice that the action of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$ "factors through" that of $G'_{\mathbb{R}}$ via the map which sends (g_4, g_5) to $\left(|\det g_4|^{1/4} |\det g_5|^{2/5},\ g'_4,\ g'_5\right)$, where $g_k = |\det g_k|^{1/k} g'_k$.

Important to note is that for $g' = (\lambda, g'_4, g'_5) \in G'_{\mathbb{R}}$, we have $\mathrm{Disc}(g' \cdot v) = \lambda^{40} \mathrm{Disc}(v)$ where the exponent comes from the dimension of $V_{\mathbb{R}}$, and $\mathrm{Sh}(g' \cdot v) = g'_4 \cdot \mathrm{Sh}(v)$ where the action on the shape depends on how we're viewing the shape. For the purposes of our calculation in Chapter 6, the action will just be matrix multiplication, as we will not consider the symmetric matrix representation.

The size of the stabilizer in $G'_{\mathbb{R}}$ of any $v^{(i)} \in V^{(i)}$ is $4n_i$ where $n_0 = 120, n_1 = 12$, and $n_2 = 8$ are the sizes of the stabilizers of $v^{(i)}$ in $G_{\mathbb{R}}$ and the extra factor of 4 comes from extra stabilizing elements inside $G'_{\mathbb{Z}}$, namely $(1, I_4, I_5), (1, I_4, -I_5), (-1, -I_4, I_5), (-1, -I_4, -I_5)$.

Restricting to integers gives $G'_{\mathbb{Z}} = \mathbb{G}_m(\mathbb{Z}) \times \mathrm{GL}_4^{\pm 1}(\mathbb{Z}) \times \mathrm{GL}_5^{\pm 1}(\mathbb{Z})$, where $\mathbb{G}_m(\mathbb{Z})$ is just $\{\pm 1\}$.

3.3.2 Fundamental Domains

We need a fundamental domain $\mathcal{F} \subset G'_{\mathbb{R}}$ for the left action of $G'_{\mathbb{Z}}$ on $G'_{\mathbb{R}}$. Since $G'_{\mathbb{R}}$ is made up of $\mathrm{GL}_k(\mathbb{R})$ components, we can start with the Iwasawa decomposition:

$$\mathrm{GL}_k(\mathbb{R}) = N'AK,$$

where K is the orthogonal matrices, A is positive diagonal matrices, and N is lower triangular matrices with 1's down the diagonal.

Since we are modding out by $G'_{\mathbb{Z}}$ which has positive and negative determinant, we need only consider elements of $\mathrm{GL}_k(\mathbb{R})$ with positive determinant for our fundamental domain. We can factor out that positive determinant giving:

$$\mathrm{GL}_k^+(\mathbb{R}) = N'AK\Lambda,$$

with K, A, and N' as above but with determinant 1, and with Λ equal to scalar matrices. (Whether we can factor out all determinants or just positive determinants depends on the size of the matrices.)

Finding the actual fundamental domain inside $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R}) \times \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})$ is not something I know how to do. I tried vaguely and decided it must require "math" as opposed to just kind of falling nicely out of explicit calculations. For $n = 3$, we know the fundamental domain for $\mathrm{GL}_2(\mathbb{Z})$ acting on $\mathrm{GL}_2(\mathbb{R})$ because of Gauss (so they tell me), but for $n = 4, 5$, we'll have to use a "Siegel set" which will be slightly too big, but suits our needs just fine. Either way, it amounts to finding bounds for the coordinates in our Iwasawa decomposition and taking into account our new-fangled-ness.

$n = 3$

Let $\mathcal{F}$ be the fundamental domain of the action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathrm{GL}_2(\mathbb{R})$, then we have

$$\mathcal{F} = \{nak\lambda : n \in N'(a), a \in A', k \in K, \lambda \in \Lambda\}$$

$$N'(a) = \left\{ \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} : n \in \nu(a) \right\}, \quad A' = \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \geq \sqrt[4]{3}/\sqrt{2} \right\}$$

$$\Lambda = \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0 \right\}, \quad K = \mathrm{SO}_2(\mathbb{R})$$

Apparently, $\nu(a)$ is the union of either one or two subintervals of $[\frac{-1}{2}, \frac{1}{2}]$ depending only on the value of $a \in A'$, where $\nu(a)$ is all of $[\frac{-1}{2}, \frac{1}{2}]$ whenever $t \geq 1$ [BST13].

For any element of $\mathrm{GL}_2(\mathbb{R})$ then, we have the following decomposition.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}, \quad ad - bc > 0.$$

We can switch λ and k since λ is just scalar multiplication. Then,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \alpha & \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where

$$\alpha = \sqrt{a^2+b^2}, \quad \gamma = \frac{c}{a}\sqrt{a^2+b^2} + \frac{b(ad-bc)}{a\sqrt{a^2+b^2}}, \quad a \neq 0, \quad \delta = \frac{ad-bc}{\sqrt{a^2+b^2}}$$

and

$$\gamma = \frac{d}{b}\sqrt{a^2+b^2} - \frac{a(ad-bc)}{b\sqrt{a^2+b^2}}, \quad b \neq 0, \quad a \text{ and } b \text{ can't both be } 0$$

also

$$\cos\theta = \frac{a}{\sqrt{a^2+b^2}}, \quad \sin\theta = \frac{-b}{\sqrt{a^2+b^2}}.$$

Then,

$$\begin{pmatrix} \alpha & \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix},$$

where

$$n = \frac{\gamma}{\alpha}, \quad t = \sqrt{\frac{\delta}{\alpha}}, \quad \lambda = \sqrt{\alpha\delta}.$$

What we need though is a fundamental domain for $G'_{\mathbb{Z}} = \{\pm 1\} \times \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z})$ acting on $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}_2^{\pm 1}(\mathbb{R}) \times \mathrm{GL}_1^{\pm 1}(\mathbb{R})$. The first component will be a fundamental domain for $\{\pm 1\}$ acting on $\mathbb{G}_m$ (which is just scalar multiplication). Since ± 1 acts on the sign of the scalar, we get that each orbit is of the form $\{\pm\lambda\}$ for some scalar λ. Thus a fundamental domain is just scalar multiplication by positive scalars (which is our Λ above). Next we need to figure out what the restricted determinant does to our $\mathcal{F}$. The only difference is that we pulled out the determinant, which means we have the $\mathcal{F}$ without the Λ which we just happened to pick up anyway from our first component. Lastly we have $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$ acting on $\mathrm{GL}_1^{\pm 1}(\mathbb{R}) = \{\pm 1\}$ which gives us just $\{1\}$. So, our fundamental domain has not changed, and $\mathcal{F}$ is just what we want. Hooray!

$n = 4$

From Minkowski via [Bha05], we have a fundamental domain for $\mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ acting on $\mathrm{GL}_3(\mathbb{R}) \times \mathrm{GL}_2(\mathbb{R})$ contained in a Siegel set, $\mathcal{F}_0 \subset N'A'K\Lambda_0$, where

$$K = \mathrm{SO}_3(\mathbb{R}) \times \mathrm{SO}_2(\mathbb{R})$$

;

$$A' = \{a(t_1,t_2,t_3) : 0 < t_1^{-1} \leq c_1 t_1,\ 0 < (t_2t_3)^{-1} \leq c_1 t_2 \leq c_1^2 t_3\},$$

$$\text{where } a(t_1,t_2,t_3) = \left(\begin{pmatrix} (t_2t_3)^{-1} & & \\ & t_2 & \\ & & t_3 \end{pmatrix}, \begin{pmatrix} t_1^{-1} & \\ & t_1 \end{pmatrix} \right);\ \text{or}$$

$$A' = \{a(s_1,s_2,s_3) : s_1 \geq 1/\sqrt{c_1},\ s_2,s_3 \geq 1/\sqrt[3]{c_1}\},$$

$$\text{where } a(s_1,s_2,s_3) = \left(\begin{pmatrix} s_2^{-2}s_3^{-1} & & \\ & s_2 s_3^{-1} & \\ & & s_2 s_3^2 \end{pmatrix}, \begin{pmatrix} s_1^{-1} & \\ & s_1 \end{pmatrix} \right);$$

$$N' = \{n(u_1,u_2,u_3,u_4) : |u_1|,|u_2|,|u_3|,|u_4| \leq c_2\},$$

$$\text{where } n(u_1,u_2,u_3,u_4) = \left(\begin{pmatrix} 1 & & \\ u_2 & 1 & \\ u_3 & u_4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ u_1 & 1 \end{pmatrix} \right);$$

$$\Lambda_0 = \{\lambda_1, \lambda_2 : \lambda_1, \lambda_2 > 0\},$$

$$\text{where } \lambda_i \text{ act by } \left(\begin{pmatrix} \lambda_2 & & \\ & \lambda_2 & \\ & & \lambda_2 \end{pmatrix}, \begin{pmatrix} \lambda_1 & \\ & \lambda_1 \end{pmatrix} \right),$$

where $c_1 = 2/\sqrt{3}$ and $c_2 = 1/2$.

What about $G'_{\mathbb{Z}} = \{\pm 1\} \times \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z})$ acting on $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}_3^{\pm 1}(\mathbb{R}) \times \mathrm{GL}_2^{\pm 1}(\mathbb{R})$? Once again, all that happens is we pull out two copies of scalar multiplication and replace it with a single one. This time however, our scalar multiplication will not be exactly our Λ_0 above. Instead we'll just leave it as $\mathcal{F} \subset N'A'K\Lambda$ where N', A', K are as above and

$$\Lambda = \{ \text{ scalar multiplication by } \lambda : \lambda > 0\}.$$

$n = 5$

From [Bha10], we have that the fundamental domain for $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$ acting on $\mathrm{GL}_4(\mathbb{R}) \times \mathrm{GL}_5(\mathbb{R})$ is of the form $\mathcal{F}_0 \subset N'A'K\Lambda$, where

$$K = \mathrm{SO}_4(\mathbb{R}) \times \mathrm{SO}_5(\mathbb{R});$$

$$A' = \{a(s_1, s_2, ..., s_7) : s_1, s_2, ..., s_7 \geq c\}, \text{ where}$$

$$a(s) = \left(\begin{pmatrix} s_1^{-3}s_2^{-1}s_3^{-1} & & & \\ & s_1 s_2^{-1} s_3^{-1} & & \\ & & s_1 s_2 s_3^{-1} & \\ & & & s_1 s_2 s_3^3 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} s_4^{-4}s_5^{-3}s_6^{-2}s_7^{-1} & & & & \\ & s_4 s_5^{-3} s_6^{-2} s_7^{-1} & & & \\ & & s_4 s_5^2 s_6^{-2} s_7^{-1} & & \\ & & & s_4 s_5^2 s_6^3 s_7^{-1} & \\ & & & & s_4 s_5^2 s_6^3 s_7^4 \end{pmatrix} \right);$$

$$N' = \{n(u_1, u_2, ..., u_{16}) : u = (u_1, u_2, ..., u_{16}) \in \nu(a)\}, \text{ where}$$

$$n(u) = \left(\begin{pmatrix} 1 & & & \\ u_1 & 1 & & \\ u_2 & u_3 & 1 & \\ u_4 & u_5 & u_6 & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & & \\ u_7 & 1 & & & \\ u_8 & u_9 & 1 & & \\ u_{10} & u_{11} & u_{12} & 1 & \\ u_{13} & u_{14} & u_{15} & u_{16} & 1 \end{pmatrix} \right);$$

$$\Lambda_0 = \{\lambda_1, \lambda_2 : \lambda_1, \lambda_2 > 0\},$$

$$\text{where } \lambda_i \text{ act by } \left(\begin{pmatrix} \lambda_1 & & & \\ & \lambda_1 & & \\ & & \lambda_1 & \\ & & & \lambda_1 \end{pmatrix}, \begin{pmatrix} \lambda_2 & & & & \\ & \lambda_2 & & & \\ & & \lambda_2 & & \\ & & & \lambda_2 & \\ & & & & \lambda_2 \end{pmatrix} \right);$$

where c is an absolute constant (i.e., not dependent on any of the variables) and $\nu(a)$ is an absolutely bounded measurable subset of $\mathbb{R}^{16}$ dependent only on the value of $a \in A'$ (so they say).

Just like in the previous case, the fundamental domain for $G'_{\mathbb{Z}} = \{\pm 1\} \times \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$ acting on $G'_{\mathbb{R}} = \mathbb{G}_m(\mathbb{R}) \times \mathrm{GL}_4^{\pm 1}(\mathbb{R}) \times \mathrm{GL}_5^{\pm 1}(\mathbb{R})$ is $\mathcal{F} \subset N'A'K\Lambda$ where N', A', K are as above and $\Lambda = \{$ scalar multiplication by $\lambda : \lambda > 0\}$.

3.3.3 $\mathcal{R}_{X,W}$

Let $v^{(i)}$ be an element of $V_{\mathbb{R}}^{(i)}$ such that $|\operatorname{Disc}(v^{(i)})| = 1$ and $\operatorname{Sh}(v^{(i)})$ is the identity matrix. We know we can find such a $v^{(i)}$ because for any element w of $V_{\mathbb{R}}^{(i)}$, let $\lambda = |\operatorname{Disc}(w)|^{-1/d}$, then $|\operatorname{Disc}(\lambda w)| = \lambda^d |\operatorname{Disc}(w)| = |\operatorname{Disc}(w)|^{-1} |\operatorname{Disc}(w)| = 1$. Next we know that for $g_{n-1} \in \mathrm{GL}_{n-1}(\mathbb{R})$, $\operatorname{Sh}(g_{n-1} \cdot w) = g_{n-1} \operatorname{Sh}(w)$ so if we let $g_{n-1} = \operatorname{Sh}(\lambda w)^{-1}$, then $\operatorname{Sh}(g_{n-1} \cdot \lambda w) = g_{n-1} \operatorname{Sh}(\lambda w) = \operatorname{Sh}(\lambda w)^{-1} \operatorname{Sh}(\lambda w) = I_{n-1}$. I'm being a little loose with my terms here. Let's stick to $G'_{\mathbb{R}}$, so by "λ" I mean $(\lambda, I_{n-1}, I_{r-1})$ and by "g_{n-1}" I mean $(|\det g_{n-1}|^e, |\det g_{n-1}|^{-1/n-1} g_{n-1}, I_{r-2})$ where the exponent e depends on n and is given by the maps from $G_{\mathbb{R}}$ to $G'_{\mathbb{R}}$ mentioned above.

Taking our fundamental domain $\mathcal{F}$, we now create $\mathcal{F}v^{(i)}$ and view it as a multiset. In order to proceed we will want to define the region of (n_i copies of) $V_{\mathbb{R}}^{(i)}$ which is in $\mathcal{F}v^{(i)}$ but has discriminant and shape restrictions imposed. We have $\mathcal{R}_{X,W} = \{x \in \mathcal{F}v^{(i)}$ such that $|\operatorname{Disc}(x)| < X$, and $\operatorname{Sh}(x) \in W\}$. We want to see how $\mathcal{R}_{X,W}$ and $\mathcal{R}_{1,W}$ are related. For any $y \in \mathcal{F}v^{(i)}$, and $\lambda \in \mathbb{R}$, λy is also in $\mathcal{F}v^{(i)}$, $|\operatorname{Disc}(\lambda y)| = |\lambda|^d |\operatorname{Disc}(y)|$, and $\operatorname{Sh}(\lambda y) = \operatorname{Sh}(y)$ (as equivalence classes). Therefore if we scale $\mathcal{R}_{X,W}$ by λ what we get is $\{x \in \mathcal{F}v^{(i)}$, such that $|\operatorname{Disc}(x)| < |\lambda|^d X$, and $\operatorname{Sh}(x) \in W\}$ which is equal to $\mathcal{R}_{|\lambda|^d X,W}$. In particular, $\mathcal{R}_{X,W} = X^{1/d} \mathcal{R}_{1,W}$, which means that $\operatorname{Vol}(\mathcal{R}_{X,W}) = \operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X$ because you get a power of the scalar ($X^{1/d}$) for each dimension d (for example, if you doubled each side of a square, you'd get a square with four times the area).

What's It Look Like?

From [Bha06], we have a nice summary of the region. For $n = 3$, $\mathcal{R}_{X,W}$ is four-dimensional, with a single cusp containing mostly reducible points (corresponding to $\mathbb{Q}$ plus a quadratic field). In the case $n = 4$, $\mathcal{R}_{X,W}$ is twelve-dimensional, with three major cusps in several dimensions. Essentially all points in the first cusp are reducible (corresponding to two quadratic fields). It's the same for the second cusp ($\mathbb{Q}$ plus a cubic field or "etale cubic algebra"). The third cusp contains mostly D_4 points (this is why we actually need the S_n condition for $n = 4$). Lastly for $n = 5$, $\mathcal{R}_{X,W}$ is forty dimensions of awesome with ridiculous cusps. Bhargava identified some 160ish sub-cusps each of which has either negligible points or is almost all points which are considered reducible in some way.

3.3.4 Big O Little O, What the Heck is O?

All of our results have the error term $o(X)$, whereas if you go to the sources, you're likely to see error terms that look like $O(X^{\text{fraction less than 1}})$, and yet elsewhere you might see no error term at all, but the word "asymptotically" or else X will be in the denominator. What's going on?

Suppose you want to approximate $x^3 + x^2 + x + 1$. We can say it's approximately $x^3 + x^2 + x$ which is a pretty good approximation, but probably not useful since you're not sparing yourself much calculation. You could also say it's approximately $x^3 + x^2$ or even just x^3. Each of these is a reasonable approximation, but you also want to keep track of how wrong you are. That's where fancy notation comes in. Also keep in mind sometimes, as in our case, you don't actually know the full answer. The $x^3 + x^2 + x + 1$ is secret and our methods give us that it's approximately x^3 with fancy error term notation. Keeping track of errors helps you know whether your approximation is meaningful.

The rules are we take x to infinity and in the limit (by which I really mean for sufficiently large x), our error is bounded in some way, and that's what our notation tells us. Let's start with little o since that's what we've been using.

Little-Oh

For a positive function, $f(x)$, and $g(x)$ assumed to be positive for sufficiently large x, we say $f(x) = o(g(x))$ ("f of x is little-oh of g of x") as $x \to \infty$ if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

When we approximate one function $f_1(x)$ with another $f_2(x)$ and say that $f_1(x) = f_2(x) + o(g(x))$ what we're saying is that the new function $f(x) = f_1(x) - f_2(x)$ is little-oh of $g(x)$. Our error is precisely $f_1(x) - f_2(x)$ and its size is $o(g(x))$. For our polynomials, if we approximate x^3+x^2+x+1 by x^3+x^2+x then our error term is just 1, which is $o(x^e)$ for what e? If we take the limit of $\frac{1}{x^e}$ as x goes to infinity, we get 0 for any value of $e > 0$. Making our approximation a bit weaker, we see that $x^3 + x^2 + x + 1 = x^3 + x^2 + o(x^{1+e})$ where again e is any positive number (including teeny tiny fractions). Lastly, $x^3 + x^2 + x + 1 = x^3 + o(x^{2+e})$ for any $e > 0$.

Taking the ratio of two functions and seeing what its limit goes to tells you how the two functions behave in comparison to each other. If they tend to zero, then you know that the function on the bottom gets bigger faster than the function on top. If they tend to a non-zero constant, this tells you they grow at the same rate, with the size of the bottom function being approximately the limit times the size of the top function. If we say some function, F, is $x^3 + o(x^{2.1})$, then we know that $\lim_{x\to\infty} \frac{F}{x^3} = 1$ (if you divide something which is $o(x^{2.1})$ by $x^{2.1}$ and take the limit you get zero, so the same is true for any exponent greater than 2.1), which says that in the limit, F behaves like x^3 (or mathily, F grows asymptotically like x^3).

One important property, used in the proof of Lemma 6, is that scaling does not affect the little-oh-ness of things. Since $k \cdot 0 = 0$ for all constants, k, we know that if $f(x) = o(g(x))$, then $f(x)$ is also $o(kg(x))$ for any positive constant k.

Our results all look like $N(\cdot) = KX + o(X)$ as X goes to infinity (where K is the volume of a region), which means that our approximation (KX) is off by an error that grows more slowly than X. We could be off by a constant (which doesn't grow at all), or a power of X which is less than 1, or some other type of function which is slower than X (like $X\log(X)$). More importantly it means that our error is not swallowing up our main term. You can see this by dividing by X and taking the limit. $N(\cdot) = KX + o(X)$ becomes

$$\lim_{X\to\infty} \frac{N(\cdot)}{X} = \lim_{X\to\infty} \frac{KX + o(X)}{X} = K + \lim_{X\to\infty} \frac{o(X)}{X} = K.$$

Big-Oh

Another way of talking about errors uses big-oh notation. We say $f(x) = O(g(x))$ if there exists a positive real constant, M, and real number, x_0, such that

$$|f(x)| \leq M|g(x)| \text{ for all } x \geq x_0.$$

Big-oh gives a more precise upper bound (of sorts), though it does not guarantee you know how the function behaves. When the limit of $\frac{f(x)}{g(x)}$ actually exists and is positive, then this implies that $f(x) = O(g(x))$, and you know the two functions grow together, which is more than you get with little-oh. In our example above, $x^3 + x^2 + x + 1 = x^3 + O(x^2)$, and if $F = x^3 + O(x^2)$ then we know that $\lim_{x\to\infty} \frac{F}{x^3} = 1$ because anything $O(x^2)$ will be less than some constant when divided by x^2 so if you divide by anything larger and take the limit, it will go to zero.

If you look at various sources, you'll find

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_1) \cdot X + O(X^{\frac{15}{16}}), \text{ for } n = 3$$

from [Dav51b],[Dav51c] (or the same thing with $O(X^{5/6})$ in [BST13]). In [Bha05], you get

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_1) \cdot X + O(X^{23/24+\epsilon}), \text{ for any } \epsilon > 0, \text{ for } n = 4.$$

Lastly, in [Bha10] you find

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_1) \cdot X + O(X^{39/40} - o(X)), \text{ for } n = 5$$

combining both notations!

Chapter 4

Mathematics, let us in
Let us welcome in the sun!
Let us open the doors and clear the way;
Our work is far from done.

And all the underrepresented minority women sing
"Doo do-doo do-doo doo do-doo..."

Congruence Conditions

$$\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)} = \frac{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p;X,W)}{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p;X)} \xrightarrow[X\to\infty]{} \frac{\lim\limits_{Y\to\infty} \boxed{\prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}}{\lim\limits_{Y\to\infty} \boxed{\prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1})}}$$

$$= \frac{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1})} = \frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_{1})} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$$

4.1 Laysplaining Congruences: What Up, p?

We have our equidistribution result now for irreducible forms in $V_{\mathbb{Z}}$ (up to $G_{\mathbb{Z}}$-equivalence), but how does this help us count number fields? Our bijection says that counting forms in $V_{\mathbb{Z}}$ is the same as counting pairs

(R, S) where R is a rank n ring and S is its resolvent. To figure out how to get to number fields we'll have to go on something of a detour.

In Chapter 5, we will see that counting maximal rings is precisely what we need to be able to count number fields, and that counting maximal rings will involve looking at everything modulo prime powers. In the meantime, what we need is to see that our equidistribution result holds for sets defined by finitely many congruence conditions. Our goal then is to understand how to count points in such sets, using **p-adic density**.

4.1.1 The Formula

Given a subset $S \subset V_{\mathbb{Z}}$ defined by finitely many congruence conditions modulo prime powers, we will count the number of irreducible points in S in a fixed fundamental domain subject to the usual discriminant and shape conditions, denoted $N^{(i)}(S; X, W)$. We will see that we can view S as k translates of the scaled lattice $m \cdot V_{\mathbb{Z}}$ (for some integers k and m) and thus our previous counting work holds for each scaled $V_{\mathbb{Z}}$, and it's just a matter of finding $\sum_{j=1}^{k} N(m \cdot V_{\mathbb{Z}}^{(i)}; X, W)$. It will turn out that we get our previous count, $N(V_{\mathbb{Z}}^{(i)}; X, W)$, but now scaled by a product of "p-adic densities," $\prod_p \mu_p(S)$.

You may have noticed that the work of this section has nothing to do with the main formula, and that's true. A formula for this section would be:

$$\frac{N^{(i)}(S; X, W)}{N^{(i)}(S; X)} = \frac{N^{(i)}(\bigcup_{j=1}^{k}(m \cdot V_{\mathbb{Z}}); X, W)}{N^{(i)}(\bigcup_{j=1}^{k}(m.V_{\mathbb{Z}}; X)} = \frac{\prod_p \mu_p(S) \cdot N(V_{\mathbb{Z}}^{(i)}; X, W)}{\prod_p \mu_p(S) \cdot N(V_{\mathbb{Z}}^{(i)}; X)} \xrightarrow[X \to \infty]{} \frac{\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$$

In Chapter 5, we will define U_p to be the set of forms in $V_{\mathbb{Z}}$ corresponding to rings which are "maximal at p." These U_p will satisfy our conditions for S in this section, as will their finite intersection, $\bigcap_{p<Y} U_p$. When we replace S with that finite intersection, the product of p-adic densities we get out looks like $\prod_{p<Y} \mu_p(U_p)$, hence why I highlighted

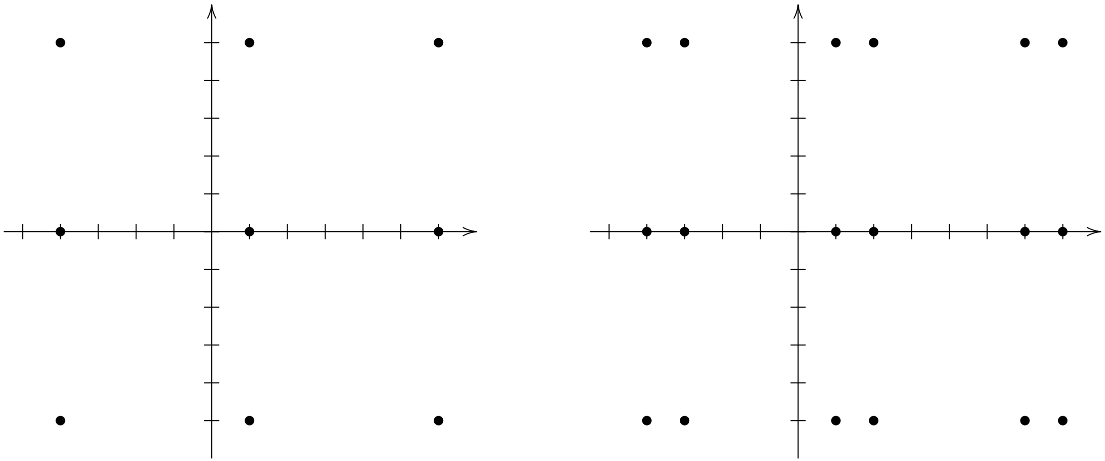
$$\frac{\lim\limits_{Y \to \infty} \prod\limits_{p<Y} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\lim\limits_{Y \to \infty} \prod\limits_{p<Y} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_1)}$$

as coming from this section.

4.1.2 p-adic density

Ignoring the maximality issues for now, let's just deal with how we'll count subsets of $V_{\mathbb{Z}}$ defined by congruence conditions.

We're still just counting lattice points. What happens if we set congruence conditions on lattice points? If we have the lattice for $\mathbb{Z}[i]$ and look only at points that are 1 mod $5\mathbb{Z}[i]$, we get a different lattice made up of $\{a+bi \text{ such that } a \equiv 1 \bmod 5, b \equiv 0 \bmod 5\}$. If we look at points that are 1 or 2 mod $5\mathbb{Z}[i]$, we don't get a (translate of a) lattice, but we do get the union of two (translates of) lattices. It takes more work, but this is a clue that the work that was necessary to prove equidistibution results will still hold, but the count will of course change as you scale and sum up lattices.


(a) 1 (mod $5\mathbb{Z}[i]$)

(b) 1 or 2 (mod $5\mathbb{Z}[i]$)

Figure 4.1: Congruence conditions as unions of translates of lattices.

How would you count points in a sublattice? For there to be any meaning to the count, it makes sense to refer to the number of points in some fundamental region of the sublattice, because otherwise you'll always just say there are infinitely many points. If we look at $\mathbb{Z}[i]$, all integer points in the plane are in the lattice, and a fundamental region could be the unit square with lower-left-hand corner at the origin. In order for our count to be nicely additive, we will not use the top or right boundaries in our count. Instead we'll take our unit square to be $s_1 = \{(x, y) : 0 \leq x < 1, 0 \leq y < 1\}$. That way the unit square contains just one lattice point, the origin, and if you scale each side by 2 to get $s_2 = \{(x, y) : 0 \leq x < 2, 0 \leq y < 2\}$, which is the sum of four unit squares, you'll count that it has four points $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$. On the other hand, if you had said the fundamental region also contained the top point and right point, and hence had 4 points, then you'd get that scaling each side by 2 gave you 9 points, which would be weird for life.

If we look at points that are 1 or 2 mod $5\mathbb{Z}[i]$, the fundamental region would be $s_5 = \{(x, y) : 0 \leq x < 5, 0 \leq y < 5\}$ which contains 25 points (from the main lattice) of which only 2 are in our union of sublattices. It would make sense then if its "density" were 2/25. This incidentally is equal to 2/5 (the proportion of integral points of the x-axis in our lattice) times 1/5 (the proportion of integral points of the y-axis in our lattice). Actually finding the "5-adic density" is slightly more complicated, though in this simple example the answer is the same.

We'll do examples in the weeds, but if you have a set $S \subset V_{\mathbb{Z}}$ which is defined by imposing finitely many congruence conditions modulo powers of p on the coefficients of the forms, then the p-adic density of S, $\mu_p(S)$, is given by the number of points in S when looking mod p^k for the biggest k necessary divided by the total number of forms mod p^k (i.e., p^k to the number of coefficients your forms have). For example, if you're looking at binary quadratic forms whose y^2 coefficient is 2 or 4 mod 5, this is the set $\{ax^2 + bxy + cy^2,$ such that $a, b, c \in \mathbb{Z}/5\mathbb{Z}; c \equiv 2$ or 4 mod $5\}$, and it contains $5 \times 5 \times 2 = 50$ points. The total number of quadratic forms mod 5 is $5 \times 5 \times 5 = 125$ so the 5-adic density of this set is $50/125 = 2/5$.

If we have conditions for more than one prime p, then we multiply the densities together. When you see $\Pi_p \mu_p(S)$ in an equation this is the product of p-adic densities. If we have finitely many congruence conditions, almost all of the densities will be 1.

4.2 Getting Mathy With It

Should we happen to have a subset $S \subset V_{\mathbb{Z}}$ defined by finitely many congruence conditions modulo prime powers, let $\prod_p \mu_p(S)$ be the product of its p-adic densities. Then, others found that for $n = 3, 4, 5$, the number of certain integer points in S (per orbit), with absolute discriminant bounded by X, is approximately $\prod_p \mu_p(S)$ times the volume of the region containing our points before imposing congruence conditions, where we also must divide by n_i because our region was a multiset.

To prove the result with the shape condition added, we look back and see we need a p-adic version of Lemma 6 for counting points in $S \cap zH$ where H is a bounded measurable subset of $V_{\mathbb{R}}$ and z goes to infinity. This is Lemma 9, and its proof is simple once you see, in the weeds (§4.3.1), that S is just a finite union of scaled and translated lattices, so our previous proof translates easily. After that, our equidistribution result for S with imposed shape condition follows as before.

4.2.1 Theorems

From [DH71, Bha05, Bha10], we have a congruence version of our # pts ≈ vol result for any $S \subset V_{\mathbb{Z}}$ defined by finitely many congruence conditions modulo prime powers.

Theorem 8. *For $n = 3, 4, 5$, the number of irreducible points in $S \cap V_{\mathbb{Z}}^{(i)}$ in a fixed fundamental domain (with S defined by finitely many congruence conditions and thus the union of finitely many lattices), is approximately equal to the volume of $\mathcal{R}_X$ scaled by the product over p of its p-adic densities and divided by n_i, which gives the formula*

$$N^{(i)}(S; X) = \frac{1}{n_i} \prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_1) \cdot X + o(X).$$

In order to get a congruence version that includes the shape condition, we'll need a congruence version of our Davenporty lemma. The proof is simple after some weedwork, so will be saved for the weeds (§4.3.2).

Lemma 9. *For H a bounded, measurable subset of $V_{\mathbb{R}}$, scale H by a real number z and let z go to infinity. Then we have that the number of irreducible lattice points in $S \cap zH$ is $\prod_p \mu_p(S) \cdot \mathrm{Vol}(zH) + o(z^d)$ as $z \to \infty$.*

In Chapter 3, we prove Theorem 5 from Theorem 4 using Lemma 6 by defining a nice, bounded subset of W with a slightly smaller volume, for which Lemma 6 holds. We also look at $\overline{W}$, the complement of W in the space of shapes and see that Lemma 6 also applies there. This sets us up with some inequalities. Using that by Theorem 4, we know the result for the whole space of shapes (or rather, the set of forms with shape anywhere in the space of shapes), we find our inequalities are actually equality. This gives Theorem 5. We can do the exact same thing here, replacing Theorem 4 and Lemma 6 with their congruence versions Theorem 8 and Lemma 9. This argument gives the proof for Theorem 10 (or you can see it all written out in §4.3.3).

Theorem 10. *For $n = 3, 4, 5$, the number of irreducible, integral points in S in a fixed fundamental domain with absolute discriminant bounded by X and shape in a nice region W is approximately equal to the volume* *of $\mathcal{R}_{X,W}$ scaled by the product over p of its p-adic desnities and divided by n_i, which in turn gives*

$$N^{(i)}(S;X,W) = \frac{1}{n_i}\prod_p \mu_p(S)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X). \tag{4.1}$$

Again, using Theorem 7 we get our congruence version of the equidistribution result for our forms in S with bounded discriminant and shape in W (when ordered by discriminant) :

Corollary 10.1. $\lim\limits_{X\to\infty}\dfrac{N^{(i)}(S;X,W)}{N^{(i)}(S;X)} = \dfrac{\textit{size of } W}{\textit{size of the space of shapes}}.$

4.3 p Weeds Playhouse!

This section gives a laysplanation of p-adic density (with examples!), and proofs of Lemma 9 and Theorem 10.

4.3.1 p-adic Density

Let's start with $S\subset V_{\mathbb{Z}}$ which is defined by finitely many congruence conditions. What might that look like? I found this a little confusing, and I wasn't sure what adding the words "modulo prime powers" changed. What follows is how I figured it out.

When I think of "finitely many congruence conditions" I think of, well, finitely many congruence conditions. I think of any finite combination of congruence conditions on any number of coordinates in $V_{\mathbb{Z}}$ (and remember we're just thinking of $V_{\mathbb{Z}}$ as a lattice, as in $\mathbb{Z}^d$).

Let's do some examples, starting with various ways to combine congruence conditions on a single coordinate a of $(a,b)\in\mathbb{Z}\times\mathbb{Z}$.

1. Suppose $S^{(1)}\subset\mathbb{Z}\times\mathbb{Z}$ is defined by $a\equiv 1$ or 2 mod 3. Then $S^{(1)}$ is the union of the lattice $a\equiv 1$ mod 3 and $a\equiv 2$ mod 3, each of which is a translate of (i.e., an integer plus) the lattice $3\mathbb{Z}\times\mathbb{Z}$ (where $a\equiv 0$ mod 3). The lattice $3\mathbb{Z}\times\mathbb{Z}$ in turn is the union of three translates of the lattice $3\mathbb{Z}\times 3\mathbb{Z} = 3\cdot(\mathbb{Z}\times\mathbb{Z})$. Thus, $S^{(1)}$ is the union of six translates of $3\cdot(\mathbb{Z}\times\mathbb{Z})$.

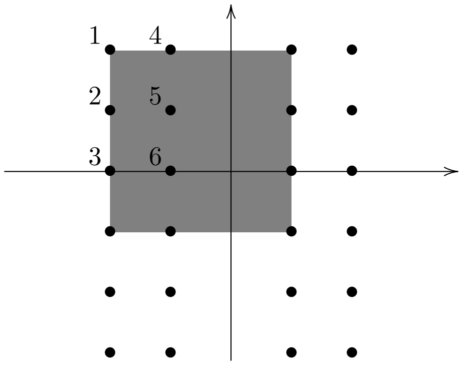


Figure 4.2: The set $S^{(1)}$, a union of six translates of $3 \cdot (\mathbb{Z} \times \mathbb{Z})$. The points labelled 1–6 are from different translates. A fundamental parallelogram for the lattice containing point number 1 is shaded.

2. Suppose $S^{(2)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1 \bmod 3$ and 4 mod 5. When does this happen? We know that $a \equiv 1 \bmod 3$ means $a = 1 + 3k$ for some $k \in \mathbb{Z}$ and $a \equiv 4 \bmod 5$ means $a = 4 + 5l$ for some $l \in \mathbb{Z}$. We can find solutions (k, l) such that $1 + 3k = 4 + 5l$ and use that to find a which are 1 mod 3 and 4 mod 5 (for example, $a = 4$ and 19 work; you could also find them just by listing all the numbers satisfying each condition and finding overlap). If you want to look for all solutions, notice that the condition $a \equiv 1 \bmod 3$ happens every 3 spots (..., 1, 4, 7, 10, 13, ...) and $a \equiv 4 \bmod 5$ happens every 5 spots (..., 4, 9, 14, 19, ...) and they overlap every $\text{lcm}(3, 5) = 15$ spots, where lcm is the least common multiple. In other words, $S^{(2)}$ is the set of (a, b) such that $a \equiv 4 \bmod 15$ which is the union of 15 translates of the lattice $15 \cdot (\mathbb{Z} \times \mathbb{Z})$.

3. Suppose $S^{(3)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1 \bmod 4$ and 3 mod 6. We again look or solve for a solution and find that 9 works. To find all solutions, we see that the least common multiple of 4 and 6 is 12, so $S^{(3)}$ is given by (a, b) with $a \equiv 9 \bmod 12$ which is the union of 12 translates of the lattice $12 \cdot (\mathbb{Z} \times \mathbb{Z})$. Actually, you can rewrite the conditions instead as $a \equiv 1 \bmod 4$ and 0 mod 3. I think this has something to do with "Chinese Remainder Theorem," but I figured it out by just seeing that 9 mod 12 worked.

4. Suppose $S^{(4)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1 \bmod 4$ and 2 mod 6. Numbers that are 1 mod 4 are all odd, whereas numbers which are 2 mod 6 are all even, thus we have no solutions and $S^{(4)}$ is the empty set. What went wrong? Trying to solve $1+4k = 2+6l$ we see that this can never happen because if we rearrange things a bit, we get that $1 = 2(1 - 2k + 3l)$ in other words, we'd need some integer m such that $1 = 2m$ and no such m exists. We will get no solution whenever the greatest common divisor of the integers we're modding out by divides one of our conditions but not the other. In other words the problem was that $\gcd(4, 6) = 2$

divided 2 (the condition mod 6) but not 1 (the condition mod 4).

5. Suppose $S^{(5)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1$ or 2 mod 3 and 2 mod 6. This is the same as saying $a \equiv$ 1 mod 3 and 2 mod 6 or else $a \equiv 2$ mod 3 and 2 mod 6. In either case we have the $\gcd(3, 6) = 3$ and the lcm(3,6)=6. If we look at the second option everything 2 mod 6 is also 2 mod 3, so $a \equiv 2$ mod 3 and 2 mod 6 is the same as just saying $a \equiv 2$ mod 6. Similarly, nothing that is 2 mod 6 is also 1 mod 3, so we get no solution for that option. Whenever you have that one modulus (the modding integer) divides the other, you can easily read off that there is either no solution or that the conditions are the same as what's defined for the larger modulus. If you wanted to see the no solution thing similarly to the previous example, try to solve $1 + 3k = 2 + 6l$. There's nothing obviously wrong with having $\gcd(3, 6) = 3$ but you'll see that we must have $-1 = 3(-k + 2l)$ which can never happen. Again the issue is that we can factor out the gcd and it will have to satisfy an equation in integers that may not be possible. At any rate, $S^{(5)}$ will be given by (a, b) with $a \equiv 2$ mod 6 which is the union of six translates of the lattice $6 \cdot (\mathbb{Z} \times \mathbb{Z})$.

Adding the second component, let's see two more examples.

6. Suppose $S^{(6)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1$ or 2 mod 4, and $b \equiv 0$ mod 2 and 3 mod 5. The least common multiple of our moduli is 20, so we'll have the union of k lattices which are translates of $20 \cdot (\mathbb{Z} \times \mathbb{Z})$. We find k by counting the number of values of a and b mod 20 and multiplying the two numbers together. Since a has two solutions mod 4, we know that it will have 10 solutions mod 20. Similarly b will have 2 solutions mod 20, and we get that $k = 20$. (You can also just list all numbers from 0 to 19 that satisfy the necessary conditions and count them.)

7. Suppose $S^{(7)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1$ or 2 mod 3 and 4 mod 5, $b \equiv 1$ mod 2 or 3 mod 5. The least common multiple of our moduli is 30, so we will have the union of k lattices which are translates of $30 \cdot (\mathbb{Z} \times \mathbb{Z})$. We find that a will have $(1 + 1) \times 2 = 4$ values because you add up "or" conditions within the same modulus and multiply "and" conditions across moduli to get the number of solutions mod the least common multiple of the two moduli (we get 2 values mod 15), then you multiply by 2 to find out that you get 4 values mod 30. (It turns out the conditions on a give that $a \equiv 4$ or 14 mod 15.) For b, to count the number of solutions mod 10, you add up that there are 5 numbers which are 1 mod 2 and 2 numbers which are 3 mod 5, but then you have to subtract the unique solution mod 10, giving 6 values mod 10 and 18 values mod 30. Therefore we end up that $S^{(7)}$ is the union of $k = 4 \times 18 = 72$ translates of the lattice $30 \cdot (\mathbb{Z} \times \mathbb{Z})$.

In general, if S is defined by finitely many congruence conditions, then there are some integers k, m, and d such that S is the union of k translates of the lattice $m \cdot \mathbb{Z}^d$ (remember m scales each factor, as in $2 \cdot (\mathbb{Z} \times \mathbb{Z})$ is $2\mathbb{Z} \times 2\mathbb{Z}$). How does the number of points in S compare to the number of points in $\mathbb{Z}^d$ (as in the proportion; they're both infinite, but not the same infinity)? The lattice $m\mathbb{Z}$ has $1/m$ the number of points in $\mathbb{Z}$. Scaling each factor of $\mathbb{Z}^d$ means that $m \cdot \mathbb{Z}^d$ has $1/m^d$ the number of points of $\mathbb{Z}^d$, then summing over all k translates gives you that S has km^{-d} times the points as $\mathbb{Z}^d$.

Now let's find the p-adic densities of our examples. The p-adic density of S is the proportion of points in $(\mathbb{Z}/p^n\mathbb{Z})^d$ which are also in S, where n is the largest number necessary to capture the relevant congruence conditions. We saw that S was the union of translates of $m \cdot \mathbb{Z}^d$ where m was the least common multiple of all the moduli in the defining congruence conditions. This means that we only have to worry about p^n dividing m. If q is a prime which does not divide m, then $\mu_q(S)$, the q-adic density of S, will be equal to 1. This seems reasonable, but to actually understand why this is, when you try to do it yourself, requires knowing things I don't know. Barring that, one way to look at it is by remembering that you can choose your representatives however you like. For example, if you want to find the 5-adic density of a set defined by the condition $a \equiv 1 \bmod 2$ (which means that a is odd), you might find it disconcerting pretending that 0, 2, or 4 are 1 mod 2. They're not. However, viewing $\mathbb{F}_5$ as $\{0, 1, 2, 3, 4\}$ is just one choice. Remembering that $0 \equiv 5, 2 \equiv 7$, and $4 \equiv 9$, you could also write $\mathbb{F}_5$ as $\{1, 3, 5, 7, 9\}$ and now it starts to make more sense that "all" points in $\mathbb{F}_5$ "are" 1 mod 2. (I'm told it's actually something like any element of $\mathbb{Z}_5$ can be approximated arbitrarily well by an integer which is 1 mod 2, if you know what that means. You needn't.) After we find the p-adic densities for p dividing m, we can find the product $\prod_p \mu_p(S) = \prod_{p|m} \mu_p(S)$.

1. We had that $S^{(1)} \subset \mathbb{Z} \times \mathbb{Z}$ was defined by $a \equiv 1$ or $2 \bmod 3$, and we found that $S^{(1)}$ was the union of six translates of $3 \cdot (\mathbb{Z} \times \mathbb{Z})$, meaning that $k = 6, m = 3, d = 2$, and $km^{-d} = 2/3$. The 3-adic density is the number of possible values mod 3 for each a and b divided by the total number of points possible mod 3. We get $2/3$ for a and $3/3$ for b which tells us that $\mu_3(S^{(1)}) = 2/3$. This means that $\prod_p \mu_p(S^{(i)}) = 2/3$ gives us the proportion of points in $\mathbb{Z} \times \mathbb{Z}$ which are in $S^{(1)}$.

2. We had that $S^{(2)} \subset \mathbb{Z} \times \mathbb{Z}$ was defined by $a \equiv 1 \bmod 3$ and $4 \bmod 5$, and we found that $S^{(2)}$ was the union of 15 translates of $15 \cdot (\mathbb{Z} \times \mathbb{Z})$, meaning that $k = 15, m = 15, d = 2$, and $km^{-d} = 1/15$. We have that $\mu_3(S^{(2)}) = 1/3 \times 3/3 = 1/3$ and $\mu_5(S^{(2)}) = 5/5 \times 1/5 = 1/5$. Since 3 and 5 are the only primes dividing $m = 15$, we know that $\prod_p \mu_p(S^{(2)}) = 1/3 \times 1/5 = 1/15$ gives us the proportion of points in $\mathbb{Z} \times \mathbb{Z}$ which are in $S^{(2)}$.

3. We had that $S^{(3)} \subset \mathbb{Z} \times \mathbb{Z}$ turned out to be defined by $a \equiv 1$ mod 4 and 0 mod 3, and we found that $S^{(3)}$ was the union of 12 translates of $12 \cdot (\mathbb{Z} \times \mathbb{Z})$, meaning that $k = 12, m = 12, d = 2$, and $km^{-d} = 1/12$. To find the 2-adic density, we have to look mod 4, and we get that $\mu_2(S^{(3)}) = 1/4$. Since $\mu_3(S^{(3)}) = 1/3$, and 2 and 3 are the only primes dividing $m = 12$, we get that $\prod_p \mu_p(S^{(3)}) = 1/12$ gives the proportion of points in $\mathbb{Z} \times \mathbb{Z}$ which are in $S^{(3)}$.

4. We had that $S^{(4)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1$ mod 4 and 2 mod 6, and we found that $S^{(4)}$ was the empty set, so $k = 0 = km^{-d}$ and our relevant densities will also be 0.

5. We had that $S^{(5)} \subset \mathbb{Z} \times \mathbb{Z}$ turned out to be defined by $a \equiv 2$ mod 6, and we found that $S^{(5)}$ was the union of 6 translates of $6 \cdot (\mathbb{Z} \times \mathbb{Z})$, meaning $k = 6, m = 6, d = 2$, and $km^{-d} = 1/6$. To find the 2-adic and 3-adic densities, we can rewrite our condition mod 2 and mod 3. We find that saying $a \equiv 2$ mod 6, is the same as saying $a \equiv 0$ mod 2 and 2 mod 3. Now we see that $\mu_2(S^{(5)}) = 1/2$, $\mu_3(S^{(5)}) = 1/3$, and $\prod_p \mu_p(S^{(5)}) = 1/6$ gives the proportion of points in $\mathbb{Z} \times \mathbb{Z}$ which are in $S^{(5)}$.

6. We had that $S^{(6)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1$ or 2 mod 4, and $b \equiv 0$ mod 2 and 3 mod 5, and we found that $S^{(6)}$ was the union of 20 translates of $20 \cdot (\mathbb{Z} \times \mathbb{Z})$, meaning $k = 20, m = 20, d = 2$, and $km^{-d} = 1/20$. Now we have that $\mu_2(S^{(6)}) = 2/4 \times 1/2 = 1/4$, and $\mu_5(S^{(6)}) = 1/5$, which means that $\prod_p \mu_p(S^{(6)}) = 1/20$ gives the proportion of points in $\mathbb{Z} \times \mathbb{Z}$ which are in $S^{(6)}$.

7. We had that $S^{(7)} \subset \mathbb{Z} \times \mathbb{Z}$ is defined by $a \equiv 1$ or 2 mod 3 and 4 mod 5, $b \equiv 1$ mod 2 or 3 mod 5, and we found that $S^{(7)}$ was the union of 72 translates of $30 \cdot (\mathbb{Z} \times \mathbb{Z})$, meaning $k = 72, m = 30, d = 2$, and $km^{-d} = 2/25$. For the b coordinate, we have to keep in mind that the "or" condition means that no condition need be satisfied mod 2 (or mod 5), so the 2-adic density (or the 5-adic density) will actually be 1. Or, to view it the way we stated earlier, having b being either 0 or 1 mod 2 will "satisfy" the 3 mod 5 condition, if you choose your representatives carefully. At any rate, $\mu_2(S^{(7)}) = 1, \mu_3(S^{(7)}) = 2/3, \mu_5(S^{(6)}) = 1/5$, and now we see that $\prod_p \mu_p(S^{(7)}) = 2/15$ which is *not* the proportion of points in $\mathbb{Z} \times \mathbb{Z}$ which are in $S^{(7)}$. We're off by a factor of 6/10 which is what the density "should" be for the b coordinate. In other words p-adic density doesn't give us the right information if we allow for "or" across different moduli.

If $S \subset V_{\mathbb{Z}}$ is defined by finitely many congruence conditions, then you'd expect the number of points in S to be km^{-d} times the number of points in $V_{\mathbb{Z}}$. If S is defined by finitely many congruence conditions *modulo prime powers* (which says implicitly that you have "and" across your moduli), then $km^{-d} = \prod_p \mu_p(S)$. This does not negate the option of having congruence conditions modulo not necessarily prime integers, but if this produces a non-empty subset of $V_{\mathbb{Z}}$, then the conditions can be rewritten modulo prime powers.

4.3.2 Proof of Lemma 9

Lemma 9 says:

For $S \subset V_{\mathbb{Z}}$ defined by finitely many congruence conditions modulo prime powers, and for H any bounded, measurable set in $V_{\mathbb{R}}$, scale H by a positive real number z and let z go to infinity. Looking at lattice points in $S \cap zH$, we get that the number of irreducible lattice points in $S \cap zH$ is $\prod_p \mu_p(S) \cdot \mathrm{Vol}(zH) + o(z^d)$ as $z \to \infty$ (i.e., the number of irreducible points is essentially equal to the volume).

Proof. We know from Davenport that the number of lattice points in $V_{\mathbb{Z}} \cap zH$ is $\mathrm{Vol}(zH) + o(z^d)$, and we saw that for S defined by finitely many congruence conditions, S is the union of k translates of the lattice $m \cdot V_{\mathbb{Z}}$. This means that the number of lattice points in $S \cap zH$ is $km^{-d} \cdot \mathrm{Vol}(zH) + o(z^d)$. We also saw that if S is defined modulo prime powers, then $km^{-d} = \prod_p \mu_p(S)$. As in the proof of Lemma 6, we have $\mathcal{R}_X(v) = \{x \in \mathcal{F}v : |\,\mathrm{Disc}(x)| < X\}$, where $\mathcal{F}v$ is still n_i copies of a fundamental domain for the action of $G'_{\mathbb{Z}}$ on $V_{\mathbb{R}}^{(i)}$, and we know that the number of reducible points in $\mathcal{R}_z^d X(v)$ is $o(z^d)$ as $z \to \infty$. Since this is still true when we look at $S \subset V_{\mathbb{Z}}$, the result holds.

□

4.3.3 Proof of Theorem 10

We want to prove that if $S \subset V_{\mathbb{Z}}$ is defined by finitely many congruence conditions, then

$$N^{(i)}(S; X, W) = \frac{1}{n_i} \prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{X,W}) + o(X)$$

which happens to equal $\dfrac{1}{n_i} \displaystyle\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X)$. This is like saying that the number of irreducible integral points in $\mathcal{R}_{X,W}$ that are in S is approximately the volume of $\mathcal{R}_{X,W}$ scaled by the proportion of $V_{\mathbb{Z}}$ in S. Since this is actually n_i copies of the same thing, we again have to divide by n_i to get what we want to know about our forms, namely $N^{(i)}(S; X, W)$. We already know this result for $\mathcal{R}_X$ corresponding to S, that

$$N^{(i)}(S; X) = \frac{1}{n_i} \prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_X) + o(X) = \frac{1}{n_i} \prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_1) \cdot X + o(X).$$

Proof. Start with W, a nice but not necessarily bounded subset of the space of shapes. Let W' be a similarly nice, but bounded subset of W whose volume is almost the same as that of W. More precisely, we choose W' such that $\mathrm{Vol}(\mathcal{R}_{1,W'}) \geq \mathrm{Vol}(\mathcal{R}_{1,W}) - \epsilon$.

Since W' is bounded, so is $\mathcal{R}_{1,W'}$, and by our Davenporty Lemma 9, we get that for $S \subset V_{\mathbb{Z}}$ defined by finitely many congruence conditions, $N^{(i)}(S; X, W')$, the number of irreducible lattice points in $\mathcal{R}_{X,W'}$ that are in S, is equal to $\dfrac{1}{n_i}\displaystyle\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{1,W'}) \cdot X + o(X)$. The number we want to find is $N^{(i)}(S; X, W)$ and we know that there will be more points with shape in W than with shape in the smaller region W', so we know

$$N^{(i)}(S; X, W) \geq N^{(i)}(S; X, W') = \frac{1}{n_i}\prod_p \mu_p(S)\cdot\mathrm{Vol}(\mathcal{R}_{1,W'})\cdot X + o(X) \geq \frac{1}{n_i}\prod_p \mu_p(S)\cdot(\mathrm{Vol}(\mathcal{R}_{1,W}) - \epsilon)\cdot X + o(X).$$

This is true for all ϵ, thus

$$N^{(i)}(S; X, W) \geq \frac{1}{n_i}\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X).$$

Let $\overline{W}$ be the complement of W in the space of shapes. Then $\overline{W}$ is also a nice, not necessarily bounded, region of the space of shapes and we can do the exact same thing we just did for W. What we get is that

$$N^{(i)}(S; X, \overline{W}) \geq \frac{1}{n_i}\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{1,\overline{W}}) \cdot X + o(X).$$

Since the space of shapes is equal to W plus $\overline{W}$ (and that there's no overlap), we know that $\mathrm{Vol}(\mathcal{R}_1) = \mathrm{Vol}(\mathcal{R}_{1,W}) + \mathrm{Vol}(\mathcal{R}_{1,\overline{W}})$, and that $N^{(i)}(S; X) = N^{(i)}(S; X, W) + N^{(i)}(S; X, \overline{W})$. Adding up our two inequalities, then, we get

$$N^{(i)}(S; X, W) + N^{(i)}(S; X, \overline{W}) \geq \frac{1}{n_i}\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + \frac{1}{n_i}\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_{1,\overline{W}}) \cdot X + o(X),$$

i.e.,

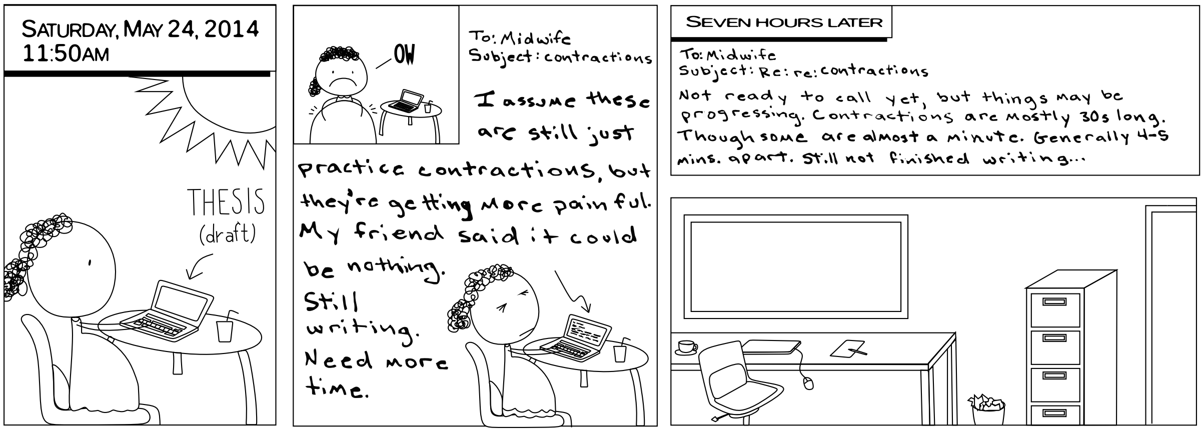
$$N^{(i)}(S; X) \geq \frac{1}{n_i}\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_1) \cdot X + o(X).$$

We already know that $N^{(i)}(S; X) = \dfrac{1}{n_i}\displaystyle\prod_p \mu_p(S) \cdot \mathrm{Vol}(\mathcal{R}_1) \cdot X + o(X)$, therefore our inequalities about

W and $\overline{W}$ must actually be equalities.

$\square$

Chapter 5


SATURDAY, MAY 24, 2014
11:50AM
THESIS
(draft)
OW
To: Midwife
Subject: contractions
I assume these are still just practice contractions, but they're getting more painful. My friend said it could be nothing. Still writing. Need more time.
SEVEN HOURS LATER
To: Midwife
Subject: Re: re: contractions
Not ready to call yet, but things may be progressing. Contractions are mostly 30s long. Though some are almost a minute. Generally 4-5 mins. apart. Still not finished writing...

Maximality

$$\boxed{\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)} = \frac{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X, W)}{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X)} \underset{X\to\infty}{\longrightarrow} \frac{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)}}$$

$$\boxed{= \frac{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod\limits_{p} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_1)} = \frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)}} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$$

5.1 Laysplanus Maximus: Turning it up to 11

Here things should hopefully start to come together. We've seen that in order to count **number fields**, we will need to count **maximal orders**, but this only works if we can actually see maximality on the forms side of things. Luckily maximality is a local condition, which means we can look at our **parametrization** and **group action** over $\mathbb{Z}_p$ instead of over $\mathbb{Z}$ and find congruence conditions on our forms which correspond to maximal rings. Then it's just a matter of **sieving** to actually get the number we want.

5.1.1 The Formula

As we mentioned in §4.1.1, U_p is the set of forms in $V_{\mathbb{Z}}$ which correspond to rings which are maximal at p. The set of forms corresponding to maximal rings will then be $U = \bigcap_p U_p$. This chapter gives the whole formula except the last equality which happens in Chapter 6.

5.1.2 We're Counting Rings, Fields, Huh, What?

I often felt like I was confusingly going between counting "rings" (or "orders") and "number fields." In case you feel this way, too, let's take a step back. First, we should note that a number field is *not* a rank n ring. A rank n ring "looks like" $\mathbb{Z}^n$ ("as a $\mathbb{Z}$-module") by which I mean, an element can be written as an element of $\mathbb{Z} \times a_1\mathbb{Z} \times a_2\mathbb{Z} \times ... \times a_{n-1}\mathbb{Z}$. One rank 2 ring is $\mathbb{Z}[i]$ which is the "ring of integers" of the degree 2 number field $\mathbb{Q}(i)$. Any element of $\mathbb{Z}[i]$ looks like $a + bi$ with $a, b \in \mathbb{Z}$, so $\mathbb{Z}[i]$ looks like $\mathbb{Z} \times i\mathbb{Z}$. In contrast, $\mathbb{Q}$ (and thus $\mathbb{Q}(i)$) cannot be formed with any finite number of copies of $\mathbb{Z}$. Degree n number fields, being finite (n-dimensional) extensions of $\mathbb{Q}$, are not rank n rings, but each does contain a unique maximal order called its "ring of integers" which is a rank n ring.

5.1.3 Number fields

Let's see why degree n number fields aren't rank n rings. Any finite set of rational non-integers (i.e., fractions) you might choose will not be enough to build $\mathbb{Q}$. If we start with linear combinations of $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}\}$ we still can't get $\frac{1}{17}$, for example. Also note that adjoining a finite number of rational non-integers to $\mathbb{Z}$ will also not give you a ring. If you take $\frac{1}{2} \in M = \mathbb{Z} \times \frac{1}{2}\mathbb{Z} \times \frac{1}{3}\mathbb{Z} \times \frac{1}{4}\mathbb{Z} \times \frac{1}{5}\mathbb{Z}$, then among other things, for M to be a ring you would need all powers of $\frac{1}{2}$ to be in M, but it is easy to see this will not be the case.

A basic example of a field is $\mathbb{Q}$, the field of rational numbers. Nice field-y things that happen inside $\mathbb{Q}$ are $q_1 + q_2 = q_2 + q_1 \in \mathbb{Q}$, $q_1 q_2 = q_2 q_2 \in \mathbb{Q}$, $0, 1 \in \mathbb{Q}$ such that $q + 0 = q$, $q \cdot 1 = q$, $-q, q^{-1} \in \mathbb{Q}$ such that $q + (-q) = 0$ and for non-zero q_3, $q_3 \cdot q_3^{-1} = 1$, if $q_1 q_2 = 0$ then $q_1 = 0$ or $q_2 = 0$, and these things are true for all $q, q_1, q_2 \in \mathbb{Q}$, and non-zero $q_3 \in \mathbb{Q}$. What separates the field $\mathbb{Q}$ from the ring $\mathbb{Z}$ is the multiplicative inverse. In $\mathbb{Z}$ only ± 1 are invertible, whereas in $\mathbb{Q}$ every non-zero element is invertible.

A number field is a finite extension of $\mathbb{Q}$ meaning you start with $\mathbb{Q}$ but you also allow additional real or complex numbers which satisfy a finite relationship, if you will, over $\mathbb{Q}$. By that I mean that if you add $\alpha \in \mathbb{C}$, you need for α^n to be contained in $\mathbb{Q} \times \alpha\mathbb{Q} \times \alpha^2\mathbb{Q} \times ... \times \alpha^{n-1}\mathbb{Q}$ for some n (and thus all numbers greater than n). Generally you say that α must be the root of a polynomial with rational coefficients. So if you start with $\mathbb{Q}$ and you add $\sqrt[3]{2+i}$, you know this gives a finite extension because $\overline{\sqrt[3]{2+i}}^6 = 4\overline{\sqrt[3]{2+i}}^3 - 5$ which is the same as saying it satisfies the polynomial $x^6 - 4x^3 + 5 = 0$. If on the other hand, you tried to add π, you'd create an infinite extension because π does not satisfy any polynomial over $\mathbb{Q}$, so each power of π would add a new dimension to the extension.

How do we count them? Every degree n number field has a unique maximal order which is a rank n ring, its ring of integers. Therefore, counting number fields with a certain property will amount to counting maximal rank n rings with that property. In our parametrization, a ring may have multiple resolvent rings and our count only sees pairs (R, S). If we have points v_1, v_2, and v_3 corresponding to $(R_1, S_{11}), (R_2, S_{21})$, and (R_3, S_{31}), that's fine, but we could also have v_4 corresponding to (R_2, S_{22}) and v_5 corresponds to (R_3, S_{32}). In other words, the fact that we only have three distinct rings R_1, R_2, and R_3 gets lost because we count five points corresponding to five pairs. Awesomely, maximal orders have unique resolvent rings, so if we restrict to those rings, our count will be accurate. This ability to count maximal orders is the good news that allows us to count number fields, and number theorists rejoice because they (we?) love number fields. We get that the number of $G_{\mathbb{Z}}$-equivalence classes of irreducible integral forms corresponding to maximal rings with absolute discriminant less than X and shape in W (i.e., $\sum_{i=0}^{\lfloor n/2 \rfloor} N^{(i)}(U; X, W)$) is equal to the number of isomorphism classes of S_n-number fields with absolute discriminant less than X and shape in W. What we need is a way to see the maximality of rings on our forms side somehow, and we do this by looking at everything mod p.

5.1.4 Maximal Orders via Sublattices a.k.a. What's p Got To Do, Got To Do With It?

Why should we be able to see anything useful looking at things mod p? Let's go back to orders again and remember we can view them as lattices. We want to figure out what makes a maximal order and how this could ever be related to prime numbers. A maximal order is an order not contained in any other order, so let's start by looking at sublattices.

Start with the lattice in the plane corresponding to $\mathbb{Z} \times \mathbb{Z}$ so that lattice points are all (a, b) with a and b integers. Then if you imagine an arrow (vector), $\mathbf{u_1}$, going from $(0, 0)$ to $(1, 0)$ and another, $\mathbf{v_1}$, going from (0,0) to (0,1), then we have that every point of the lattice can be gotten to using a linear combination of $\mathbf{u_1}$ and $\mathbf{v_1}$. For example, the point (4,3) is 4 times (1,0) plus 3 times (0,1), i.e., you go over 4 (in the direction of $\mathbf{u_1}$) and up 3 (in the direction of $\mathbf{v_1}$). The parallelogram determined by $\mathbf{u_1}$ and $\mathbf{v_1}$ is the square with vertices {(0,0), (0,1), (1,0), (1,1)}. Let's call this set of vertices f_1, the fundamental region of our lattice, since the lattice is just a bunch of copies of this region.

What would a sublattice look like? What was not obvious to me from the picture is that a sublattice must be a subset of the containing lattice. You can't add points, only take them away. One sublattice of $\mathbb{Z} \times \mathbb{Z}$ would be $2\mathbb{Z} \times \mathbb{Z}$ where you only take even x-coordinates.

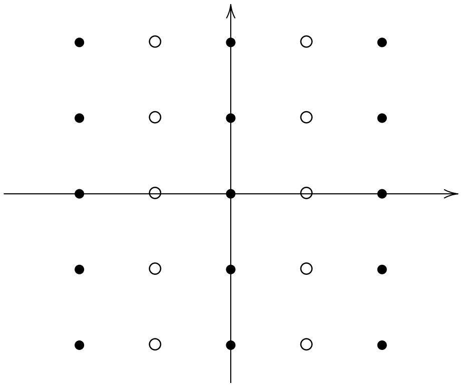


Figure 5.1: The sublattice $2\mathbb{Z} \times \mathbb{Z}$ in $\mathbb{Z} \times \mathbb{Z}$.

This lattice is generated by $\mathbf{u_2} = 2\mathbf{u_1}$, the vector going from $(0, 0)$ to $(0, 2)$, and $\mathbf{v_2} = \mathbf{v_1}$. Notice that the fundamental region, f_2, of $2\mathbb{Z} \times \mathbb{Z}$ is bigger than f_1, that of $\mathbb{Z} \times \mathbb{Z}$. In fact the area of f_2 is twice that of f_1 and we say that the index of $2\mathbb{Z} \times \mathbb{Z}$ in $\mathbb{Z} \times \mathbb{Z}$ is two.

If we start with a lattice, though, how do we know whether it is a sublattice of an allowed lattice? We're only interested in lattices which correspond to orders in number fields. Our lattices aren't actually rings yet, so let's look at $\mathbb{Z}[qi]$ for $q \in \mathbb{Q}$, which gives the same lattice as $\mathbb{Z} \times q\mathbb{Z}$. If $q = 1$, we know $\mathbb{Z}[i]$ is a ring, and in fact it is a maximal one. If $q = 2$, we also have a ring, $\mathbb{Z}[2i]$, but this time it is a suborder of $\mathbb{Z}[i]$. On the other hand, if $q = 1/2$, then we do not have a ring, and thus we don't have an order in a number field. So the question is how can we tell the difference between the lattices $2\mathbb{Z} \times \mathbb{Z}, \mathbb{Z} \times \mathbb{Z}$, and $\frac{1}{2}\mathbb{Z} \times \mathbb{Z}$? How can we see that $\mathbb{Z}[2i]$ is a suborder of $\mathbb{Z}[i]$ which is maximal despite being contained in the lattice corresponding to $\mathbb{Z}[\frac{i}{2}]$ which is not a ring? This is where things get complicated.

5.1.5 $\mathbb{Z}_p$

Now there's this thing called $\mathbb{Z}_p$, and it's a little weird. Instead of telling you what $\mathbb{Z}_p$ is, I'll tell you what $\mathbb{Z}_{(p)}$ is and though they are NOT THE SAME AT ALL, it's okay here if you think of them as the same. Like I said, $\mathbb{Z}_p$ is weird and doesn't live inside any set of numbers you've ever heard of if you don't already know what $\mathbb{Z}_p$ is. So instead we'll look at $\mathbb{Z}_{(p)}$ which is what happens when you intersect $\mathbb{Z}_p$ with the rational numbers, $\mathbb{Q}$ (this intersection must take place inside something called $\mathbb{Q}_p$).

Start with the integers, $\mathbb{Z}$, and fix a prime p. We "localize" $\mathbb{Z}$ at the ideal $(p) = p\mathbb{Z}$ by allowing fractions $\frac{r}{s}$ with $r, s \in \mathbb{Z}$ but where $s \notin (p)$. (When you see "local" talk in number theory it means p stuff.) In other words, all integers are now invertible except those divisible by p. This property is exactly what we need from $\mathbb{Z}_p$, so it's what I think of, but in real life $\mathbb{Z}_p$ is much weirder (now with more infinity!).

If we take our order and "tensor with $\mathbb{Z}_p$" (replace $\mathbb{Z}$ with $\mathbb{Z}_p$) then we say the original order is "maximal at p" if this new $\mathbb{Z}_p$ order is maximal. An order in a number field is maximal if and only if it is maximal at p for all p. Could this make sense? Sure. Let's look back to the lattice $2\mathbb{Z} \times \mathbb{Z}$ associated with the ring $\mathbb{Z}[2i]$. We saw that the ring was not maximal because it was contained in $\mathbb{Z}[i]$ which was maximal. Tensor with $\mathbb{Z}_p$ and you get $\mathbb{Z}_p[2i]$ which, as a lattice, looks like $2\mathbb{Z}_p \times \mathbb{Z}_p$. If we let p be any prime not equal to 2, then 2 is invertible which means that $2\mathbb{Z}_p = \mathbb{Z}_p$. (Let $p = 3$, then look at $\mathbb{Z}_3[2i]$. Since 2 is not divisible by 3, 2 is invertible (that's the only property of $\mathbb{Z}_3$ we know, in fact). This means that $2^{-1} \in \mathbb{Z}_3$ which means that $1 = 2 \cdot 2^{-1} \in 2\mathbb{Z}_3$ which in turn gives us that $2\mathbb{Z}_3 = \mathbb{Z}_3$, and so $\mathbb{Z}_3[2i] = \mathbb{Z}_3[i]$.) We now see that for $p \neq 2, \mathbb{Z}_p[2i] = \mathbb{Z}_p[i]$ which I'm telling you is maximal. But if you let $p = 2$, you have $\mathbb{Z}_2[2i] \subsetneq \mathbb{Z}_2[i]$, so it is not maximal. This shows that $\mathbb{Z}[2i]$ is not maximal at 2 and is thus not maximal. (Looking at $\mathbb{Z}_p[\frac{i}{2}]$, you see that for $p \neq 2$ this is just $\mathbb{Z}_p[i]$, but that $\mathbb{Z}_2[\frac{i}{2}]$ is not even a ring, so the fact that $\mathbb{Z}_p[i] \subset \mathbb{Z}_p[\frac{i}{2}]$ doesn't affect its maximality.) This may seem a ridiculous way to go about things, but it's the fact that we can see maximality at p on the forms side that makes things nice.

In what follows, we will want to look at conditions mod p, except that p won't always be enough. We might need to look mod p^2 or even higher powers. The advantage of talking about $\mathbb{Z}_p$ is that it allows you to see things modulo powers of p without having to pick one in advance. Once you figure out what's going on, you can go back to finite things like $\mathbb{F}_p$ or $\mathbb{Z}/p^k\mathbb{Z}$ for whatever k.

5.1.6 $G_{\mathbb{F}_p}$ acting on $V_{\mathbb{Z}_p}$ mod $G_{\mathbb{Z}_p}$

This is number theory, so obviously things won't be super duper nice, by my reckoning anyway. While it's true we will be looking at sets defined by finitely many congruence conditions modulo prime powers, they won't be defined nicely in ways I can hold in my head. The reason for this is that we aren't just looking at forms mod p, but we want to know about equivalence classes of forms.

What happens to our group action when we look mod p? If $v \equiv 0$ mod p, then $gv \equiv 0$ mod p, and in the weeds, we'll look at how forms factor mod p and that will be unaffected by our group action, but in general I can't tell you much about the coefficients of gv when $v \not\equiv 0$ mod p.

So rather than having some nice conditions for our forms and counting how many points this gives us, we'll end up calculating the proportion of forms which can be transformed into forms known to be (non-) maximal based on congruence conditions. This is fine (if a bit icky) though because all we need is to know proportions mod p (or p-adic densities), thanks to the niceness of lattices.

5.1.7 Locating Those Maximal Rings

Let U_p be the set of $v \in V_{\mathbb{Z}}$ such that v corresponds to $(R(v), S)$ with $R(v)$ maximal at p. Then what we want to count will be the number of forms in $U = \bigcap_p U_p$ which will give us all the forms corresponding to rings that are maximal at p for all p, otherwise known as maximal rings.

For $n = 3, 4$, [BST13] and [Bha04] tell you how to find U_p. For $n = 5$ [Bha08] instead gives a formula for counting points in U_p. We'll see a bit more in the weeds (§5.3.4).

Basically, if $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is not maximal, then that means that one or more of your basis elements α_i have a p in them, such that if you divided that component by p, you would still have a ring. (In our example above, we saw that $\mathbb{Z}[2i] \cong \mathbb{Z} \times 2i\mathbb{Z}$ was not maximal; in that case you divide the second component by 2 and end up with $\mathbb{Z} \times i\mathbb{Z} \cong \mathbb{Z}[i]$ which is a ring.) Working this out in the multiplication tables gives you conditions for the coefficients of the corresponding v. These conditions are not necessarily mod p, but they will be mod p^k for some k. Forms v which satisfy these conditions form a set $U'_{p,non\text{-}max}$ defined by finitely many congruence conditions mod p^k. Let $W_p = U_{p,non\text{-}max}$ be all $v \in V_{\mathbb{Z}}$ such that $\gamma v \in U'_{p,non\text{-}max}$ for some $\gamma \in G_{\mathbb{Z}}$. Then W_p is the set of $v \in V_{\mathbb{Z}}$ which are equivalent to forms satisfying conditions for non-maximality at p, which means it's the set of forms corresponding to rings not maximal at p. The complement of this set is thus the set of forms equivalent to rings maximal at p, which is U_p.

Is U_p defined by finitely many congruent conditions mod powers of p? Yes! We know that $U'_{p,non\text{-}max}$ is defined by finitely many congruence conditions mod p^k for some k. This means that we can reduce everything mod p^k and just look at $G_{\mathbb{Z}/p^k\mathbb{Z}}$-equivalence in $V_{\mathbb{Z}/p^k\mathbb{Z}}$. Since both of these are finite, we are necessarily defining U_p by finitely many congruence conditions, no matter how bad things get.

So we know that the work in the previous section gives us a count for forms in U_p, or for a finite intersection of U_p. This section will prove that things stay nice even as we take the number of primes we consider to infinity to get the infinite intersection $\bigcap_p U_p = U$.

5.1.8 The First Rule of Giving a Definition of Sieving is You Do Not Give a Definition of Sieving

A sieve used to be a process of counting or identifying numbers via systematically crossing things out. Abstractifying this has lead to many different procedures all called sieves for reasons that, as of this printing, elude me. It seems as though you are trying to get a grasp of how many (and how) numbers or elements of a set subject to congruence conditions where what you're counting is taken to infinity. Counting something mod p is generally doable, but it takes a little bit of work to count modulo a bunch of p's and it certainly takes work to let the number of conditions go to infinity. For each finite count you'll be off by an error, and an important aspect of the sieve is that this error term is less than your main term, otherwise your answer would be useless ("the answer is 100 plus or minus 100"). I GUESS.

We want to count (certain) elements in $U = \bigcap_p U_p$ defined by infinitely many congruence conditions. In order to be in U, you have to be in U_p for all p. If we define W_p to be the complement of U_p in $V_{\mathbb{Z}}$ (so that you're either in U_p or else you're in W_p), then as soon as you're in W_p we can cross you off the list of possible candidates for U. In that way, counting U is inherently "sievey."

Our finite count (of a finite intersection of U_p's) is easy after the work in Chapter 4, but you could also use "Inclusion–Exclusion," common to sieves, to count the union of the W_p's. This would give the size of the complement of U, but that's okay since we have a count for $V_{\mathbb{Z}}$ already. This method would give us a sum that fancy math would show is equal to a product of proportions with lots of p's around in the numerator and denominator. Another bit of "sieviness."

Finally, we will see that this actually works to give us our answer, that our estimates are good enough. Because apparently it isn't sieving unless it works.

5.2 Mathsplanus Maximus: The Proof You've Been Waiting For!

Some definitions! Let's let U be the subset of elements of $V_{\mathbb{Z}}$ corresponding to pairs (R, S) where R is a maximal ring of rank n. (Remember, this will mean that R has unique resolvent S, so these points actually correspond just to maximal rings R.) Let U_p be the set of elements in $V_{\mathbb{Z}}$ which correspond to pairs (R, S) where R is maximal at p. We know that R is maximal (and thus corresponding to a $v \in U$) if and only if it is maximal at p for all p (and thus corresponding to a v which is in U_p for all p), so this tells us that $U = \bigcap_p U_p$, and that U is given by infinitely many congruence conditions (modulo prime powers).

We know our # pts $\approx$ vol result for the following sets: all of $V_{\mathbb{Z}}$, $V_{\mathbb{Z}}$ with restrictions on the shape, a subset $S \subset V_{\mathbb{Z}}$ defined by finitely many congruence conditions, and such an S with restrictions on the shape. We now want to show the result for U which is given by infinitely many congruence conditions.

Let's recap the equations of what we know:

The number of irreducible, $G_{\mathbb{Z}}$-inequivalent, integer points in $V_{\mathbb{Z}}^{(i)}$, with absolute discriminant bounded by X and shape in W, $N(V_{\mathbb{Z}}^{(i)}; X, W)$, is given by

$$N(V_{\mathbb{Z}}^{(i)}; X, W) = \frac{1}{n_i} \operatorname{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X).$$

The number of irreducible integer points in a subset $S \subset V_{\mathbb{Z}}$ (in a fixed fundamental domain) given by finitely many congruence conditions modulo prime powers, with absolute discriminant bounded by X and shape in W (counting one orbit at a time), $N^{(i)}(S; X, W)$, is given by

$$N^{(i)}(S;X,W) = \frac{1}{n_i}\prod_p \mu_p(S)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X).$$

Okay, everyone, this is it! This is where we prove* The Main Theorem Of Everything**!!!!

*some restrictions may apply; namely, we still have to go through Chapter 6 before it's official.

**in this case "Everything" means "This Thesis."

Namely, we will prove Theorem 1 that for $n = 3$, 4, and 5, when isomorphism classes of S_n-number fields of degree n are ordered by their absolute discriminants, the lattice shapes of the rings of integers in these fields become equidistributed in the space of lattices.

Since counting S_n-number fields is the same as counting irreducible forms $v \in V_{\mathbb{Z}}$ corresponding to maximal rings (up to $G'_{\mathbb{Z}}$ equivalence), we first count points in U and find

Theorem 11. $N^{(i)}(U;X,W) = \frac{1}{n_i}\prod_p \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X)$

Note that proving this will also tell us that

$$N^{(i)}(U;X) = N^{(i)}(U;X,\mathcal{S}_{n-1}) = \frac{1}{n_i}\prod_p \mu_p(U_p)\cdot\mathrm{Vol}(\mathcal{R}_{1,\mathcal{S}_{n-1}})\cdot X + o(X) = \frac{1}{n_i}\prod_p \mu_p(U_p)\cdot\mathrm{Vol}(\mathcal{R}_1)\cdot X + o(X),$$

because removing the shape condition is the same thing as letting W equal the whole space of shapes.

Proof. To prove things for U, let's start by looking at a subset that is related to U, but is only defined by finitely many congruence conditions. For Y any positive integer, let's take the finite intersection $\bigcap_{p<Y} U_p$. Letting $S = \bigcap_{p<Y} U_p$ we see that (or we sieve that, if you will)

$$N(\bigcap_{p<Y} U_p;X,W) = \frac{1}{n_i}\prod_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X).$$

(In case you're wondering, $\mu_p(U_p \cap U_q) = \mu_p(U_p)$, which seems weird to me when I look at it, but it's inherent in the definition of p-adic density.) Our set U is actually smaller than this $\bigcap_{p<Y} U_p$ so

$$N^{(i)}(U;X,W) \leq \frac{1}{n_i}\prod_{p<Y} \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X)$$

for all Y. Letting Y go to infinity gives us

$$N^{(i)}(U;X,W) \leq \frac{1}{n_i}\prod_p \mu_p(U_p)\cdot \mathrm{Vol}(\mathcal{R}_{1,W})\cdot X + o(X).$$

What we want, though, is equality. We need to find a clever (or mundane) way of writing things so that we get $N(U;X,W)$ is greater than or equal to the right-hand side, and then those two statements together will give us equality. (If $x \leq 1$ and $x \geq 1$, then $x = 1$.) We need an expression that says $N(U;X,W)$ is greater than something involving $N^{(i)}(\bigcap_{p<Y} U_p; X, W)$, since the latter expression is our key to the right-hand side of the equation. Hopefully, we can write $\bigcap_{p<Y} U_p$ as being contained in U plus something whose size we have a handle on (remember U is smaller than $\bigcap_{p<Y} U_p$).

A natural way to relate U and $\bigcap_{p<Y} U_p$ is to write $U = \left(\bigcap_{p<Y} U_p\right) \cap \left(\bigcap_{p\geq Y} U_p\right)$. Then we can see that $\bigcap_{p<Y} U_p$ is contained in the union of U and the complement of $\bigcap_{p\geq Y} U_p$ in $V_{\mathbb{Z}}$, or in symbols

$$\bigcap_{p<Y} U_p \subset U \cup \overline{\bigcap_{p\geq Y} U_p}.$$

Or in pictures!

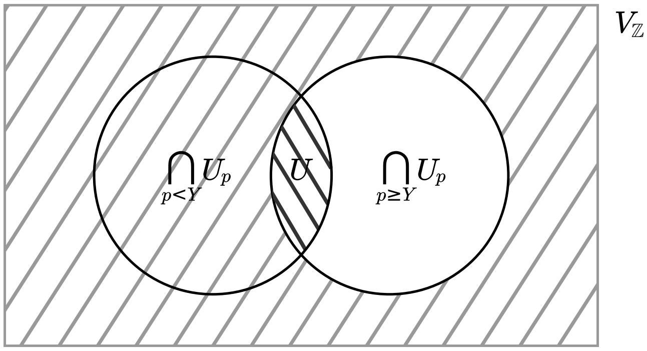


Figure 5.2: A child's proof.

Does that help us? First let's define W_p to be the complement of U_p in $V_{\mathbb{Z}}$. Since the complement of the intersection is the union of the complements, we have that $\overline{\bigcap_{p\geq Y} U_p} = \bigcup_{p\geq Y} \overline{U_p} = \bigcup_{p\geq Y} W_p$, meaning

$$\bigcap_{p<Y} U_p \subset U \cup \bigcup_{p\geq Y} W_p.$$

The number of elements in a union of sets is less than or equal to the sum of the number of elements in each set, thus we get that

$$N^{(i)}(\bigcap_{p<Y} U_p; X, W) \leq N^{(i)}(U; X, W) + \sum_{p \geq Y} N^{(i)}(W_p; X, W)$$

so that

$$N^{(i)}(U; X, W) \geq N^{(i)}(\bigcap_{p<Y} U_p; X, W) - \sum_{p \geq Y} N^{(i)}(W_p; X, W).$$

This is useful because of the following lemma which is [DH71, §4, Proposition 1], [Bha05, Proposition 23], [Bha10, Proposition 19]

Lemma 12. $N(W_p; X) = O(X/p^2)$.

This implies that $N^{(i)}(W_p; X, W) = O(X/p^2)$. This together with Theorem 10 gives

$$N^{(i)}(U; X, W) \geq \frac{1}{n_i} \prod_{p<Y} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X) - \sum_{p \geq Y} O(X/p^2)$$

To sum the infinite error, we use that $O(x/p^2) = O(X) \cdot 1/p^2$, and get via calculus that

$$\sum_{p \geq Y} O(X/p^2) = O(X) \cdot \sum_{p \geq Y} 1/p^2 < O(X) \cdot \frac{\text{some constant}}{Y} = O(X/Y)$$

.

Now we have

$$N^{(i)}(U; X, W) \geq \frac{1}{n_i} \prod_{p<Y} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X) + O(X/Y).$$

If we let Y go to infinity, we get the inequality we were looking for

$$N^{(i)}(U; X, W) \geq \frac{1}{n_i} \prod_{p<Y} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_{1,W}) \cdot X + o(X),$$

which then proves the theorem. □

This combined with Theorem 7 gives

Corollary 12.1. $\lim_{X\to\infty} \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)} = \frac{\textit{size of } W}{\textit{size of the space of shapes}}$.

This corollary is actually our Main Theorem 1 since counting points in U is precisely counting number fields.

5.3 Weeds!

This section gives background information that explains where things come from, but is not strictly necessary for following the work in this chapter. In order to see what it means for maximality to be a "local condition" (why and how p has shown up), we'll need to see what happens when we look at things mod p. We will see that maximality and S_n-ness on the rings side correspond to congruence conditions on the forms side (needed to obtain the bounds for the proof of Lemma 6).

5.3.1 Forms and Orders mod p

Remember a number field K may look like $\mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$ where we have a polynomial $f(x)$, irreducible in $\mathbb{Q}$, with $f(\alpha) = 0$. The ring of integers $\mathcal{O}_K$ may or may not look like $\mathbb{Z}[\alpha]$ but at any rate, the order $\mathbb{Z}[\alpha]$ is at least a subring of $\mathcal{O}_K$. We can learn things about $\mathbb{Z}[\alpha]$ by looking at $f(x)$ mod p and by looking at $\mathbb{Z}[\alpha]/(p) = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$. Given a $v \in V_{\mathbb{Z}}$, we'll have a ring $R(v)$ (with potentially many resolvent rings) and we can look at $R(v)/(p)$, but our v is usually not the $f(x)$ which defines our field (in fact, for $n = 4, 5$, v isn't even a single polynomial).

Motivating (we hope) Examples

Okay, now we're ready to look mod p. What happens to our forms and our orders? Let's start by looking at some specific orders and seeing how their corresponding polynomials behave mod p. For any number field, we may find an associated irreducible polynomial such that our number field comes from adding a root to $\mathbb{Q}$. For any number field we may also find its ring of integers (in theory; in practice our first guess is probably a nonmaximal order). What we want to see is the relationship between these two when we look mod p.

Let's start with $\mathbb{Z}[i]$ and $x^2 + 1$ which are both associated to the degree 2 number field $\mathbb{Q}(i)$. What does it mean to look at $\mathbb{Z}[i]$ mod p? As $\mathbb{Z}$-modules, $\mathbb{Z}[i]$ is just $\mathbb{Z} \times i\mathbb{Z}$ and $(p) = p\mathbb{Z}[i]$ is just $p\mathbb{Z} \times ip\mathbb{Z}$ so $\mathbb{Z}[i]/(p)$ is just $\mathbb{Z}/p\mathbb{Z} \times i\mathbb{Z}/p\mathbb{Z}$. This tells you how many elements there are and what addition looks like. It also tells you that $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a rank 2 extension of $\mathbb{Z}/p\mathbb{Z}$, and we write this as $[\mathbb{Z}[i]/p\mathbb{Z}[i] : \mathbb{Z}/p\mathbb{Z}] = 2$. As rings, though, we know nothing because we have no sense of the multiplication. In fact, the multiplicative structure (and thus the ring structure) will depend on p (and actually it will never have the same multiplication as $\mathbb{Z}/p\mathbb{Z} \times i\mathbb{Z}/p\mathbb{Z}$ because $1 \times i = i$, whereas $(1, 0) \times (0, 1)$ ought to be $(0, 0)$).

Some examples!

Let $p = 2$, then let's try to understand $\mathbb{Z}[i]/2\mathbb{Z}[i] = \{0, 1, i, i + 1\}$. One question to ask would be what happens when we take powers of i and $i + 1$? We get $i^2 \equiv 1$ and $(i + 1)^2 = 2i \equiv 0$. The fact that $i + 1$ is nilpotent (has a power that equals zero) means that this is not a field, so we know we're not looking at $\mathbb{F}_4$. Beyond that, though, it's hard to tell. Let's switch now and instead look at $x^2 + 1$ mod 2, this is equivalent to $x^2 - 1 = (x + 1)(x - 1) \equiv (x + 1)^2$, and in fact if we plug in i for x into the factored polynomial we see that $(i + 1)^2 = 2i$. This is how we find out how a rational prime splits (factors) in a field extension. (Don't worry, I also see the i in my $2i$ that I seem to be saying is just a 2. Since i is invertible in $\mathbb{Z}[i]$, we don't care if it lurks. It's like factoring a negative number into prime factors; the -1 doesn't matter. And okay actually we're factoring ideals anyway, not numbers, and the ideal $(2i)$ is exactly the ideal (2) again because i is invertible.) In order to see what $\mathbb{Z}[i]/2\mathbb{Z}[i]$ actually is, we view $\mathbb{Z}[i]$ as $\mathbb{Z}[x]/(x^2 + 1)$ and turn to the third isomorphism theorem and see (with some thought) that $\mathbb{Z}[i]/2\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1, 2) = (\mathbb{Z}[x]/2\mathbb{Z}[x])/(x^2+1) \cong ((\mathbb{Z}/2\mathbb{Z})[x])/(x^2+1) = (\mathbb{Z}/2\mathbb{Z})[x+1]/(x+1)^2$ which we write as $\mathbb{F}_2[t]/(t^2)$. (Well, what I see is that $\mathbb{Z}[i]/2\mathbb{Z}[i]$ must be $(\mathbb{Z}/2\mathbb{Z})[i]$ just from looking at its elements, and then since $(i+1)^2 \equiv 0$, it ought to be the same as $(\mathbb{Z}/2\mathbb{Z})[i+1]/(i+1)^2$, but I'm not sure this is mathy enough.)

Let's also look briefly at $\mathbb{Z}[i]/(i+1)\mathbb{Z}[i]$. It's not immediately obvious what this looks like. To start with, it's less obvious what $(i+1)\mathbb{Z}[i]$ even consists of. As it turns out, $(i+1)\mathbb{Z}[i] = \{a+bi,\ \text{such that } a \equiv b \bmod 2\}$. In other words, we just have two equivalence classes (evens and odds) and so $\mathbb{Z}[i]/(i + 1)\mathbb{Z}[i] \cong \mathbb{Z}/2\mathbb{Z}$ and $[\mathbb{Z}[i]/(i + 1)\mathbb{Z}[i] : \mathbb{Z}/2\mathbb{Z}] = 1$.

Let $p = 3$, then let's look at $\mathbb{Z}[i]/3\mathbb{Z}[i] = \{0, 1, 2, i, i + 1, i + 2, 2i, 2i + 1, 2i + 2\}$. If we again, take powers of $i, i + 1$, and $i + 2$, we see that $i^4 = 1, (i + 1)^8 \equiv 1$, and $(i + 2)^8 \equiv 1$. Since $\mathbb{Z}[i]/3\mathbb{Z}[i]$ only has 8 non-zero elements anyway, we see (if you look at all the powers) that $i + 1$ actually generates the multiplicative group $\mathbb{Z}[i]/3\mathbb{Z}[i]^\times$. That tells us that the quotient is indeed a field, and we are looking at $\mathbb{F}_9$. If we instead look at $x^2 + 1$ mod 3, we find that it is irreducible (since our polynomial is quadratic, if it factored it would split into linear factors so you can just test $x = 0, 1, 2$ and see if you get 0 mod 3; you don't). In other words the ideal (3) remains prime in $\mathbb{Z}[i]$ and thus it seems to make sense that $\mathbb{Z}[i]/3\mathbb{Z}[i]$ is the field $\mathbb{F}_9$.

Let $p = 5$, and again let's see the quotient $\mathbb{Z}[i]/5\mathbb{Z}[i] = \{0, 1, 2, 3, 4, i, i+1, i+2, ..., 4i+4\}$, and again let's take powers of $i, i+1, i+2, i+3, i+4$. We have that $i^4 \equiv 1, (i+1)^4 \equiv 1, (i+2)^3 \equiv i+2, (i+3)^2 \equiv i+3, (i+4)^4 \equiv 1$. This is not looking like either of our previous cases because we don't have any powers going to zero, we don't have any element generating the multiplicative group, and we've discovered a new feature. The element $i+3$ is called idempotent because it squared is itself (and this thus holds for all higher powers as well). It should not surprise you, therefore, to find that x^2+1 has a new behavior mod 5; it splits into $(x-2)(x+2)$. Again we plug in i and see that $(i-2)\mathbb{Z}[i] \cdot (i+2)\mathbb{Z}[i] = -5\mathbb{Z}[i] = 5\mathbb{Z}[i]$, so by Chinese Remainder Theorem, $\mathbb{Z}[i]/5\mathbb{Z}[i] \cong \mathbb{Z}[i]/(i+2)\mathbb{Z}[i] \times \mathbb{Z}[i]/(i-2)\mathbb{Z}[i]$. Each piece is a degree 1 extension over $\mathbb{Z}/5\mathbb{Z}$ and we have that $\mathbb{Z}[i]/5\mathbb{Z}[i] \cong \mathbb{F}_5 \times \mathbb{F}_5$.

One more example, now showing how lack of maximality can change things. Let's look at $\mathbb{Z}[3i]$ and $f(x) = x^2+9$, and let's have $p = 3$. In our previous examples, looking at the polynomial mod p or the ring mod p or seeing how p split seemed to confer the same information, which in turn seemed related to the decomposition of the field mod p. In our previous examples, though, our field was maximal at each chosen p. In this case, $\mathbb{Z}[3i]$ is not maximal at 3. If you work it out, $\mathbb{Z}[3i]/3\mathbb{Z}[3i]$ turns out to be a degree 2 extension of $\mathbb{F}_3$ isomorphic to $\mathbb{F}_3[t]/(t^2)$. The function $f(x) = x^2+9$ is clearly congruent to x^2 mod 3, but what happens to 3? It actually remains prime in $\mathbb{Z}[3i]$. More on this later.

5.3.2 Types of Math and Things Interlude

There will be two approaches to what follows, the **arithmetic** approach and the **geometric** approach. Let's say a little bit about these things first.

Arithmetic, Not Your Grandma's

Arithmetic is what most people think math is ("you must be great at calculating tip!") and it's certainly what people tend to assume number theory is ("what, did you like invent a new number or something?"). And, okay, number theorists will tell you what they do is arithmetic, but they aren't talking about the arithmetic you learned in school. Arithmetic is the study of numbers and their properties. The work we just did in our hopefully motivating examples was looking at (algebraic) things arithmetically (prime factorization).

Geometry

When I think of geometry, I think of triangles and angles and distances. I think of shapes in the plane and things you can do to shapes in the plane, and things you can prove about them given just enough information. I don't think of "curves," but I'm told I should. By a curve I mean what I think of as a function (which I'm supposed to call a "graph"). Whatever you call $y = f(x)$ when you plot it in the plane, that is a curve, and curves are part of geometry. My hang-up is that when I think of curves (which I still call functions), I think of calculus. The problem is that whereas geometry is a type of math, calculus is merely a collection of methods. If you agree that curves are geometric (and we needn't be in the plane, of course, we can be in n-dimensional space), then it stands to reason that points of intersection of multiple curves are also geometric. This also includes looking at zeroes or other particular values of a given curve. In fact we won't just be looking in the plane, or in space, but in "projective space."

Projective Space: The Final Frontier

Generally speaking, it's better if you can make (true!) statements that don't require too many exceptions. If you're trying to prove something, it would be great not to have to break it up into every possibility taking into account a bunch of exceptions. For example, if you are used to drawing lines in planes, you should be comfortable with the notion that two lines intersect in exactly one point... except parallel lines. We would prefer a world in which any two distinct lines intersect in exactly one point. That world is called the "projective plane." In that world, parallel lines intersect at infinity. More specifically, if you take a degree n polynomial and a degree m polynomial, they will intersect in exactly nm points, including multiplicity, in the appropriate projective space over an "algebraically closed field."

I'm being advised not to try to learn all about projective space in order to describe it here, but to instead say that what we care about is having a consistent count of points of intersection, and the way to do that is to be in projective space. The details don't matter. MAYBE, MAYBE NOT.

UPDATE: For a great laysplanation of projective space, check out [Ell14, Ch. 13].

5.3.3 A Symbol for That

The first step to getting a handle of things mod p will be to partition our forms or rings based on their structure/behavior mod p and this is something that will hold even when we act by $G_{\mathbb{Z}}$. We will define the symbol $(\cdot, p)$ for rings and for forms using two different approaches. Let's start with the arithmetic side and define the symbol for rings.

(R, p), Arithmetically

From [DH71], [Bha04], [Bha08], we have the following definition: for a rank n ring, R, and for each prime p, we define (R, p) to be $(f_1^{e_1} f_2^{e_2} \ldots f_g^{e_g})$ where f_i, e_i, g are defined as below by looking at how pR factors. (Note that there is no explicit symbol defined in the sources for $n = 3$, but the information is there.)

Let K be a number field of degree n and let $R = \mathcal{O}_K$ be its ring of integers. If we take a prime $p \in \mathbb{Z}$ we can ask how it behaves in K, as in does $p\mathcal{O}_K$ remain prime or factor, and if it factors, what does that look like. We saw three examples above of different behaviors. When $K = \mathbb{Q}(i)$ we saw that $2\mathcal{O}_K = \mathfrak{P}^2, 3\mathcal{O}_K = \mathfrak{P}$, and $5\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$. In general, for a prime $p \in \mathbb{Z}$, $p\mathcal{O}_K = \Pi_{i=1}^{g} \mathfrak{P}_i^{e_i}$. Notice that when we look at factoring polynomials, we have conservation of degree. A degree 2 polynomial can split into two, possibly identical, linear (degree 1) factors as was the case with $p = 2, 5$ or it can remain an irreducible degree 2 polynomial. In either case you have that the sum of the degrees of the factors add to 2. Looking at the prime decompositions though we appear to lose this degree information; we can't tell that the primes that make up (2) or (5) are any different or smaller than the one prime $\mathfrak{P} = (3)$. We can recover this information, however, if we look at $\mathcal{O}_K/\mathfrak{P}_i$ and how it relates to $\mathbb{Z}/p\mathbb{Z}$.

Specifically, we define $f_i = [\mathcal{O}_K/\mathfrak{P}_i : \mathbb{Z}/p\mathbb{Z}]$, and now we will have that $\Sigma_{i=1}^{g} e_i f_i = n$, where n is the degree of K over $\mathbb{Q}$. Another way to look at it is that $\mathcal{O}_K/\mathfrak{P}_i \cong \mathbb{F}_{p^{f_i}}$. Looking at that equation, you can see that for $n = 2$ there are only three options: $g = 1, e_1 = 1, f_1 = 2$ is the case for $p = 3$ ($g = 1$ means there's only one prime, $e_1 = 1$ means that prime has exponent 1); $g = 1, e_1 = 2, f_1 = 1$ is the case for $p = 2$; and $g = 2, e_1 = e_2 = f_1 = f_2 = 1$ is the case for $p = 5$.

What does the symbol actually look like? If $n = 2$ the only possibilities are $(1^2), (11), (2)$. Looking at our examples, we have $(\mathbb{Z}[i], 2) = (1^2), (\mathbb{Z}[i], 3) = (2)$, and $(\mathbb{Z}[i], 5) = (11)$, which corresponded with our polynomial factorizations. In general, though, R need not be maximal. As we saw with $R = \mathbb{Z}[3i], (\mathbb{Z}[3i], 3) = (2)$, even though the corresponding polynomial did not remain irreducible. If R is maximal, it is a theorem of Dedekind [Neu99, Proposition I.8.3] that you can find (R, p) by factoring some relevant polynomial mod p. Otherwise you have some work to do.

(v, p), **Geometrically**

On the forms side, let $v \in V_{\mathbb{Z}}$, and fix a prime p, then (v, p) is again defined to be $(f_1^{e_1} f_2^{e_2} ... f_g^{e_g})$ but our f_i, e_i, g are defined differently in terms of their geometry.

We can apparently view our correspondence with (R, S) as being geometric. I didn't understand whether that sentence was true when I typed it, but then I made the most amazing discovery! (And by "amazing discovery" I mean that I finally took in the meaning of a collection of words I'd already attempted to read several times before.)

From [Bha08, §2]: "In this section, we wish to understand the parametrization of rings of small rank via a natural mapping that associates, to any nondegenerate R of rank n, a set X_R of n points in an appropriate projective space." And then things happen that I don't currently totally understand. Point being, there is some geometric way of viewing elements of $V_{\mathbb{Z}}$ that involves points in space.

I'm venturing a bit into the unknown(-by-me), but I don't want to just leave things there. Within geometry, there is algebraic geometry. Algebraic geometry is the sort of thing that makes me feel like the interpretation button in my brain is broken. Unfortunately, that's where we've ended up. Start with $v \in V_{\mathbb{Z}}$, then this defines n points in the "projective space" $\mathbb{P}^{n-2}$ by looking at points of intersection of various things. For $n = 3$, it's just zeroes (where v intersects with the curve $y = 0$), and for $n = 4$, $v = (A, B)$ and you look at the points of intersection of the curves $A = 0$ and $B = 0$. For $n = 5$, the five 4×4 sub-Pfaffians define five "quadric surfaces" in $\mathbb{P}^3$ that intersect in five points. After you get those points, according to algebraic geometry, it makes sense to talk about "degrees of residue fields" with "multiplicity." I don't totally get it, but it seems like perhaps if you find the points of intersection over $\mathbb{F}_p$ you will end up in a similar situation as above where you can read of degrees and multiplicities. Hopefully I'll know more by the end of this, and can edit this section appropriately.

At any rate, you can usually get the data for (v, p) by looking at the decomposition of $R(v)/(p)$ where $R(v)$ is the rank n ring associated to v (where $R(v)/(p) = \bigoplus_{j=1}^{g} \mathbb{F}_{p^{f_i}}[t_i]/t_i^{e_i}$).

5.3.4 Symbol Outro: What Is It Good For? Maximality and Reducibility

Okay, what have we? We have rings R, forms v, and a correspondence $R(v) \sim v$. Looking mod p, we have a symbol $(\cdot, p) = (\sigma)$. Now we have to figure out what this can tell us.

Start on the forms side and define (v, p) in terms of the geometry (residue fields and multiplicities at points of intersection). We can also see the data (almost always) by saying $(v, p) = (f_1^{e_1} f_2^{e_2} \dots f_g^{e_g})$ where $R(v)/(p) = \bigoplus_{j=1}^{g} \mathbb{F}_{p^{f_i}}[t_i]/t_i^{e_i}$. For $n = 3$, the symbol (v, p) is simply taken from factoring v mod p, as we did in our examples.

Next we partition our forms in terms of this symbol by defining $T_p(\sigma)$ to be the set of $v \in V_{\mathbb{Z}}$ such that $(v, p) = (\sigma)$. This partition is stable under the action by $G_{\mathbb{Z}}$, so it is actually a partition of equivalence classes of forms. In [BST13] and [Bha04], we see p-adic densities for the $T_p(\sigma)$.

Maximality

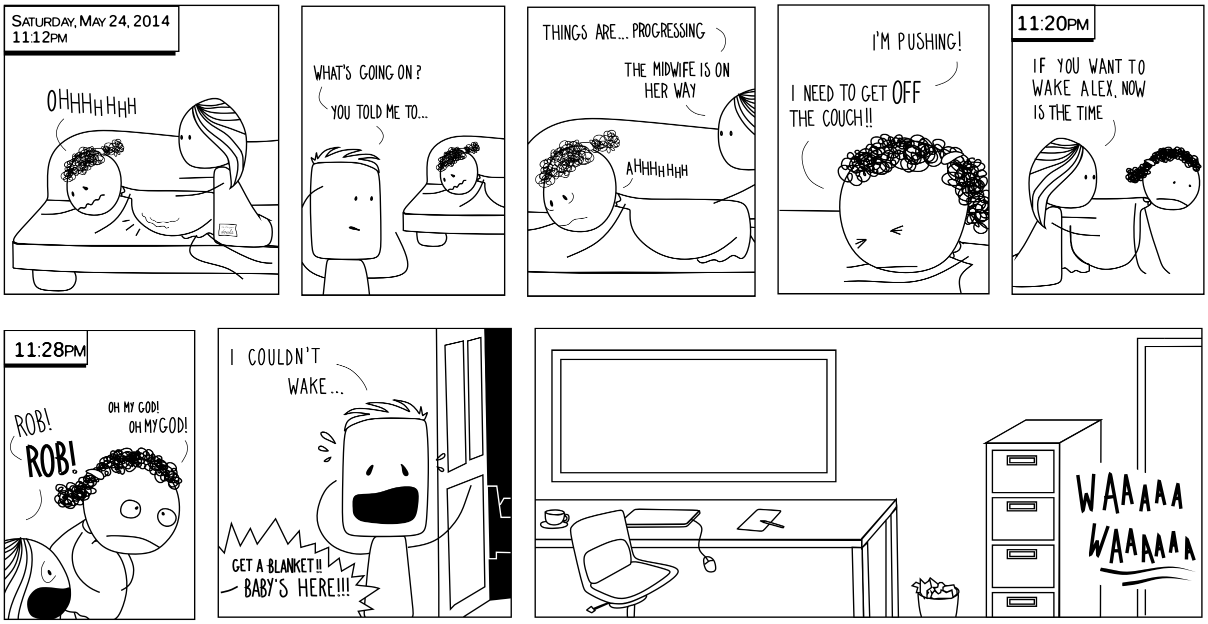
Now look at rings and define the symbol (R, p) in terms of the arithmetic, with $(R, p) = (f_1^{e_1} f_2^{e_2} \dots f_g^{e_g})$ where $pR = \Pi_{i=1}^{g} \mathfrak{P}_i^{e_i}$ and $R/\mathfrak{P}_i \cong \mathbb{F}_{p^{f_i}}$. For v corresponding to maximal rings $R(v)$, we have that $(R(v), p) = (v, p)$, and we define $U_p(\sigma)$ to be the set of $v \in T_p(\sigma)$ such that $R(v)$ is maximal. It is known that any form corresponding to a non-maximal ring will have "ramification" which means an $e_i > 1$, so right away we have that $T_p(\sigma) = U_p(\sigma)$ for all σ for which $e_i = 1$ for all i (in other words, (111), (12), (3), (1111), (112), (13), (4), etc).

The first goal is to count the number of forms in, or rather get a p-adic density of, $U_p = \bigcup_{\sigma} U_p(\sigma)$. For $n = 3, 4$ we can count the T_p's by looking at possible combinations for points of intersection over $\mathbb{F}_p$ (no idea) which automatically gives us the "unramified" $U_p(\sigma)$, and then for the rest we can find the proportion of points in $T_p(\sigma)$ which will correspond to maximal forms. For $n = 5$ we have a formula to get us the densities for $U_p(\sigma)$ without going through T_p (this formula gives the right answer for $n = 3, 4$, but I don't have a proof for it). The actual p-adic densities are not very illuminating, to me anyway, but can be found in [BST13], [Bha04], and [Bha08]. These densities were used to find $N^{(i)}(U; X)$ explicitly for $n = 3, 4, 5$, but since we only care about ratios, we don't need to know the value of the scaling factor $\prod_p \mu(U_p)$.

Reducibility

From there, you can get a bound on reducible points by knowing things I don't really know, but read about in [Bha10, §3.2]. Namely, that you can tell something about the elements of a ring's Galois group by looking at its symbols over all primes. In fact, there are symbols (σ) and (τ), for each n, such that if R is in both $T_p(\sigma)$ and $T_q(\tau)$ for primes p, q, then R is necessarily S_n. It turns out that the f_i's in (R, p) tell you a cycle type that's necessarily contained in the ring's Galois group. Having symbol (n) means containing an n-cycle, and having the symbol $(11...1k)$ means containing a k-cycle. Since S_3 is generated by a transposition and a 3-cycle, we know that any reducible cubic ring cannot have both (12) and (3). By the same rationale, reducible quartic rings cannot have both (13) and (4), and reducible quintic rings cannot have both (1112) and (5). Once you know that constraint on reducible forms, you can use the p-adic densities to get an upper bound on the number of reducible points. If you know how to take limits of products, then you see this ends up being $o(X)$. This bound was the missing information in the proof of Lemma 6.

Chapter 6



VOLUME

$$\frac{N^{(i)}(X,W)}{N^{(i)}(X)} = \frac{N^{(i)}(U;X,W)}{N^{(i)}(U;X)} = \frac{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X,W)}{\lim\limits_{Y\to\infty} N^{(i)}(\bigcap\limits_{p<Y} U_p; X)} \xrightarrow[X\to\infty]{} \frac{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\lim\limits_{Y\to\infty} \prod\limits_{p<Y} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_1)}$$

$$= \frac{\prod\limits_{p} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_{1,W})}{\prod\limits_{p} \mu_p(U_p) \cdot \mathrm{Vol}(\mathcal{R}_1)} = \boxed{\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}}$$

6.1 Laysplaining Volume Calculation: How Do I Enter Matrix Groups Into My TI-82?

Several times we came up with a count-is-almost-volume result which we claimed would lead directly to the desired equidistribution result but for a volume calculation. What's that about?

The equidistribution result we want says that the proportion of (certain) points with shape in W is given by the proportion of W's size compared to the whole space of shapes, $\mathcal{S}_{n-1}$. We have equidistribution if we can show that

$$\frac{N(\,\cdot\,;X,W)}{N(\,\cdot\,;X)} = \frac{\text{size of } W}{\text{size of } \mathcal{S}_{n-1}}.$$

What we have so far, for instance for $V_{\mathbb{Z}}^{(i)}$, is that

$$\frac{N(V_{\mathbb{Z}}^{(i)};X,W)}{N(V_{\mathbb{Z}}^{(i)};X)} = \frac{\frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1,W})\cdot X + o(X)}{\frac{1}{n_i}\operatorname{Vol}(\mathcal{R}_{1})\cdot X + o(X)}$$

.

Dividing top and bottom by X gives us that

$$\lim_{X\to\infty}\frac{N(V_{\mathbb{Z}}^{(i)};X,W)}{N(V_{\mathbb{Z}}^{(i)};X)} = \frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_{1})},$$

and we also get this same ratio if we replace $V_{\mathbb{Z}}$ with S or U. Our goal here is to prove Theorem 7 showing that

$$\frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_{1})} = \frac{\text{size of } W}{\text{size of entire space of shapes}}.$$

How do we calculate the **volumes** and show the two ratios are equal? First, we need to know about **integrals** and how to set them up for volume calculations. In our case, we're also going to need to actually (finally) use some of the properties we've mentioned about our group action, plus a few other details to interpret our integrals. Then it will just be a matter of writing things nicely so the answer falls out.

6.1.1 The Formula

In the case of our space of shapes, size is denoted by μ so this section finishes our formula, finding that

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}.$$

6.1.2 Integrals

In order to understand our volume calculation, you will need to know what an integral is. An integral is whatever you want it to be (certain terms and restrictions apply; read the fine print, not provided here). It's notation. It's metaphor. It's an allusion. I taught Calc 2 repeatedly, so when I see an integral, I always see the Calc 2 integral, but that's just one small part of the story.

An integral looks like this: $\displaystyle\int_R f(A)dM$, where A is any set of variables and M is a metaphor.

1. $\int$ is a stretched out s for funky sum. An integral is a funky sort of summation of some values (under some weighting system) given some indexing set. A normal sum looks like

$$\sum_{n=1}^{5} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5}.$$

   The values we sum are given by $\frac{1}{n}$ (i.e., 1, $\frac{1}{2}$, ..., $\frac{1}{5}$), our indexing set is $\{1, 2, 3, 4, 5\}$, and each value is given equal weight (and that weight is simply 1). We could write this as $\int_{x\in\{1,2,3,4,5\}} \frac{1}{x} dC$, where C represents "counting". The funkiness comes in when you try to add up infinitely many values (more than that, really) of infinitely small (or metaphorical) weighting. Using an integral to calculate a volume amounts to having a formula for the volume of tiny pieces of the region and then funky-summing them up.

2. R is some region of some space. If $R \subset \mathbb{R}^n$, we are most likely doing calculus, and if we're finding a volume, it's the Euclidean volume which is what you'd get if you used an appropriately scaled tape measure. If R is a line segment in $\mathbb{R}$, say $R = \{x \in \mathbb{R},$ such that $a \leq x \leq b\}$, then we can write $\int_a^b$ instead of $\int_R$. If R is more than one dimension, you might see more than one $\int$ sign, and the goal is generally to integrate one dimension at a time. Another way to write $\int_R$ is to define the characteristic function of R. If $R \subset V$, then define $\chi_R(A)$ to be the function which for any point $A \in V$ returns the

answer to the question "Is this point in R?" In other mathy words,

$$\chi_R(A) = \begin{cases} 1 \text{ if } A \in R \\ 0 \text{ if } A \notin R. \end{cases}$$

Then instead of $\int_R f(A)dM$ we can write $\int_V \chi_R(A)f(A)dM$.

3. $f(A)$ is a function of potentially multiple variables. There is always a function being integrated even if the function is just 1, as in $\int_R dM$ which equals $\int_R 1dM$.

4. dM. Ah. This. Often you will see dx or dy or $d\lambda$ or dt and this tells you what variable you are integrating with respect to. Examples:

$$\int 1dx = x + C, \quad \int 1dy = y + C, \quad \int xdx = \frac{1}{2}x^2 + C, \quad \int xdy = x\int dy = xy + Cx.$$

In the calculus case of integration, in $\mathbb{R}^n$, we are measuring things in a fairly standard way, and the $d$variable doesn't really do much more than name the variable. It can be useful to view it as an infinitesimal width when attempting to set up an integral from a picture or word problem, but it is otherwise pretty meaningless. Example: Finding the area under the curve, somehow you'd like to sum up a bunch of rectangles that are super duper thin whose heights are $f(x)$ evaluated at various (evenly spaced out) points:

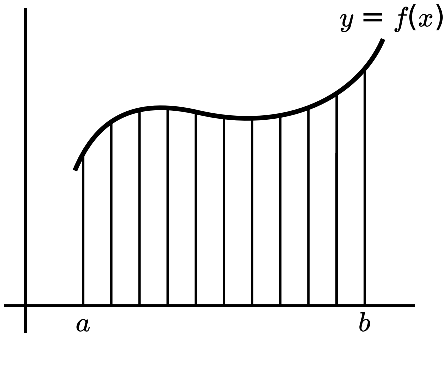


Figure 6.1: Area under the curve $y = f(x)$ between $x = a$ and $x = b$.

How we teach you to set up the integral which calculates the area under the curve from $x = a$ to $x = b$

is by drawing a “slice” (a single such thin rectangle).

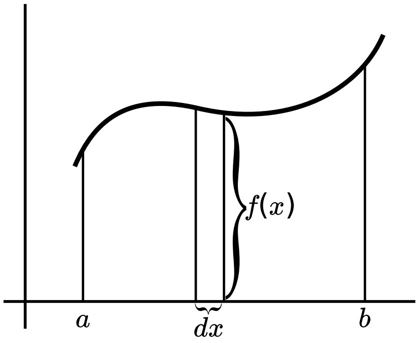


Figure 6.2: Using a “slice” to set up the integral which calculates the area under the curve.

Though we draw it big (so we can see it), it represents something infinitely thin. It sits on the point x, its height is $f(x)$, and its width is defined to be dx. Thus, the area of the slice is $f(x)dx$ and to get the area under the curve, we funky-sum it over allowable values of x, i.e., $\int_a^b f(x)dx$. Area is just the volume of a two dimensional region, so it makes sense to start there. Calculating a three dimensional volume in calculus is essentially the same, but harder to draw.

And if we’re not in Calculus class? The integration one learns in Calc class relies on certain properties that aren’t always available to us, so we turn to something else called a measure.

If calculus is like using a tape measure to figure out how big a table is, measure theory is like setting up rules for quantifying other qualities, like how good a table is, or how successful a person is. How successful are you? In order to answer that, you need to “pick a measure.” Are you more successful if you have more money? If you make more money? If you have more friends? A bigger family? If you’re happy? A measure tells you (in a sense) how various values are weighted since we can’t just break out the ruler.

Fortunately, we don’t have to know too much about measures to get through this section. When it comes to actually integrating, we will have formulas for translating our $d$measures into calc style $d$metaphors. There is a notion of a measure being “natural” in some way, and sometimes translating a measure into metaphorical calculus notation involves an extra function. For instance, $dV = |\operatorname{Disc}(v)||^{-1}dv$ is a natural measure on $V_{\mathbb{R}}$ and $d\Lambda = d^{\times}\lambda = \lambda^{-1}d\lambda$ is a natural measure on $\mathbb{G}_m(\mathbb{R})$.

Integrating dv, say, means integrating with respect to v and means your integral ends in dv.

6.1.3 Volumes

We saw one way to set up an integral in calculus to find the area under the curve. Let's revisit that. To find the volume of the two-dimensional region $R_{(2)}$ given by $\{(x, y) \in \mathbb{R}^2$ such that $a \leq x \leq b$ and $0 \leq y \leq f(x)\}$ (i.e., the area under $f(x)$ above the line segment on the x-axis, L, from $x = a$ to $x = b$), we set up the integral $\int_a^b f(x)dx = \int_L f(x)dx$. This is assigning a value to each line segment from the x-axis to $f(x)$ and summing them up. Alternatively, we could assign a value to each *point* of $R_{(2)}$ and sum that up. That integral looks like $\int_{R_{(2)}} 1dxdy$.

For a three-dimensional region, $R_{(3)}$, the following integrals are equal to the volume, though perhaps only one is actually possible to write down and calculate:

$$\mathrm{Vol}(R_{(3)}) = \int_{(x,y,z)\in R_{(3)}} dxdydz = \int_{(x,y)\in B_2, \text{ the ``shadow'' of } R_{(3)}} f_{\text{height}}(x, y)dxdy = \int_{x\in L, \text{ a line in } B_2} f_{\text{area}}(x)dx.$$

When we're dealing with measures instead of calculus, we talk about the measure of a region instead of its volume, and a safe place to start is measure$(R) = \int_R d$measure.

6.1.4 Relating g and v, a Proposition

When we do actually go to integrate, we will have an integral over g on the one hand and v on the other, and we'll need a way to relate the two. We have just the proposition we need in:

Proposition 13. *For $i \in \{0, 1, \ldots, \lfloor n/2 \rfloor\}$, let f be a Lebesgue-integrable function on $V_{\mathbb{R}}^{(i)}$. Then there exist nonzero rational constants c_i such that*

$$\int_{v\in V_{\mathbb{R}}^{(i)}} f(v)dv \;=\; c_i^{-1} \cdot \int_{g\in \text{``}G_{\mathbb{R}}\text{''}} f(\text{``}g\text{''} \cdot v^{(i)}) \mid \mathrm{Disc}(\text{``}g\text{''} \cdot v^{(i)}) \mid d\text{``}g\text{''}.$$

This doesn't work with our original $G_{\mathbb{R}}$ because we're off by a factor of infinity, but If we replace "$G_{\mathbb{R}}$" with our new $G'_{\mathbb{R}}$, this proposition holds for us.

Okay, but what is the proposition about anyway? What we want to be able to do is make a "change of variables" from v to g. On the left-hand side, we are funky-summing $f(v)$ for all v in an orbit of $V_{\mathbb{R}}$. We know that looking at $f(v)$ for all v in an orbit is the same as looking at $f(g \cdot v^{(i)})$ for all $g \in G'_{\mathbb{R}}$ multiple times according to the size of the stabilizer. Assuming a finite stabilizer, this tells us to expect a constant out front when we funky-sum over g instead of v. The next question is how do the values of $f(v)$ or $f(g \cdot v^{(i)})$ get weighted differently depending on whether we integrate dg or dv. The answer to that is in the above proposition, that we need a factor of the discriminant inside our integral to make things make sense (and another constant; the c_i is not simply n_i from the stabilizer, but also another constant depending only on n).

6.2 Calculating the Volume, with Math

Okay, let's do this!! So we want to show that $\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$. We can start simply enough:

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{\mathcal{R}_{1,W}} d\text{metaphor}}{\displaystyle\int_{\mathcal{R}_1} d\text{metaphor}}, \quad \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})} = \frac{\displaystyle\int_W d\mu}{\displaystyle\int_{\mathcal{S}_{n-1}} d\mu}.$$

Once we figure out our variables on the left, we'll be able to fill in our "metaphors." On the right, we need to know the measure. To show both sides are equal we will use our proposition relating our metaphors and our measures.

d what?

Recall that $\mathcal{R}_{1,W}$ (and thus $\mathcal{R}_1$) consists of elements of $V_{\mathbb{R}}^{(i)}$, an orbit of our space of forms. Since our forms are essentially just the tuples of their coefficients, this is just $\mathbb{R}^d$. This is why we get to think Euclid and deal in metaphors. To start, we will just integrate with respect to v in subsets of (or all of) $V_{\mathbb{R}}^{(i)}$, which means we'll be integrating dv. On the other hand we have that $W \subset \mathcal{S}_{n-1} = \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/ \mathrm{GO}_{n-1}(\mathbb{R})$ which is sort of contained in $\mathrm{GL}_{n-1}(\mathbb{R})$. So to start we will be integrating dg, the $\mathrm{GL}_{n-1}(\mathbb{R})$-invariant measure induced from the Haar measure, on the right-hand side.

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{\mathcal{R}_{1,W}} dv}{\displaystyle\int_{\mathcal{R}_1} dv}, \quad \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})} = \frac{\displaystyle\int_W dg}{\displaystyle\int_{\mathcal{S}_{n-1}} dg}.$$

Regions of Integration

The proposition we plan on using relates integrals over $G'_{\mathbb{R}}$ to integrals over all of $V_{\mathbb{R}}^{(i)}$, so on the dv side, we want to use characteristic functions to rewrite our integral over the whole orbit. On the right-hand side we can remember that $\mathcal{S}_{n-1} = \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathrm{GO}_{n-1}(\mathbb{R})$, and also use a characteristic function for W:

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{v\in V_{\mathbb{R}}^{(i)}} \chi_{\mathcal{R}_{1,W}}(v)dv}{\displaystyle\int_{v\in V_{\mathbb{R}}^{(i)}} \chi_{\mathcal{R}_1}(v)dv}, \quad \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})} = \frac{\displaystyle\int_{\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathrm{GO}_{n-1}(\mathbb{R})} \chi_W(g)dg}{\displaystyle\int_{\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/\mathrm{GO}_{n-1}(\mathbb{R})} dg}.$$

Change of Variables

At this point we need to start thinking about how to go from dv to dg (or vice versa, whichever is easier).

We return to our Proposition 13 which follows from [Shi72, Proposition 2.4], [Bha05, Proposition 21], [Bha10, Proposition 16] (follows using an application of Lebesgue's dominated convergence theorem and the density of the bounded continuous functions in the integrable ones, if you must know) which we looked at in the laysplanations. The proposition says that for $i \in \{0, 1, \ldots, \lfloor n/2 \rfloor\}$, and f a Lebesgue-integrable function on $V_{\mathbb{R}}^{(i)}$, then there exist nonzero rational constants c_i such that

$$\int_{v\in V_{\mathbb{R}}^{(i)}} f(v)dv \;=\; c_i^{-1} \cdot \int_{g\in G'_{\mathbb{R}}} f(g\cdot v^{(i)}) \mid \mathrm{Disc}(g\cdot v^{(i)}) \mid dg.$$

It's starting to look like maybe we want to turn our dv integral into a dg one (which makes sense if you remember that I keep talking about how somehow the groupiness makes things easier). From now on we will work just with the $\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)}$ equation until we can see that it's equal to the $\frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}$ equation.

If we let $f(v)$ equal $\chi_{\mathcal{R}_{1,W}}(v)$ above and $\chi_{\mathcal{R}_1}(v)$ below, we now have that

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{c_i^{-1}\cdot \displaystyle\int_{g\in G'_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)}) \mid \mathrm{Disc}(g\cdot v^{(i)}) \mid dg}{c_i^{-1}\cdot \displaystyle\int_{g\in G'_{\mathbb{R}}} \chi_{\mathcal{R}_1}(g\cdot v^{(i)}) \mid \mathrm{Disc}(g\cdot v^{(i)}) \mid dg} = \frac{\displaystyle\int_{g\in G'_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)}) \mid \mathrm{Disc}(g\cdot v^{(i)}) \mid dg}{\displaystyle\int_{g\in G'_{\mathbb{R}}} \chi_{\mathcal{R}_1}(g\cdot v^{(i)}) \mid \mathrm{Disc}(g\cdot v^{(i)}) \mid dg}.$$

Actual Conditions of Integration

Now we need to figure out what these conditions mean to work out how to manipulate the integrals into something we can work with.

First off, we need to remember what $\mathcal{R}_{1,W}$ is. The set of g for which $\chi_{\mathcal{R}_{1,W}}(g \cdot v^{(i)}) \neq 0$ will be the set $\{g \in G'_{\mathbb{R}}$ such that $g \cdot v^{(i)} \in \mathcal{F}v^{(i)},\ |\operatorname{Disc}(g \cdot v^{(i)})| < 1$ and $\operatorname{Sh}(g \cdot v^{(i)}) \in W\}$. That means there are three conditions we need to keep track of: fundamental domain, discriminant, and shape.

Fundamental Domain

Super easy is the first condition. Replacing $g \in G'_{\mathbb{R}}$ with $g \in \mathcal{F}$ changes nothing in our integrals because this condition is already implied in the characteristic function (which determines the region of integration) and we already know that whether you mod out by $G'_{\mathbb{Z}}$ has no effect on the shape or discriminant. Writing this in terms of our actual groups will make things easier, so we'll use $g \in G'_{\mathbb{Z}} \backslash G'_{\mathbb{R}}$ as our region of integration, though this is simply defined to mean take g in $\mathcal{F}$.

$$\frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{g \in G'_{\mathbb{Z}} \backslash G'_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g \cdot v^{(i)})\ |\operatorname{Disc}(g \cdot v^{(i)})\ |\ dg}{\displaystyle\int_{g \in G'_{\mathbb{Z}} \backslash G'_{\mathbb{R}}} \chi_{\mathcal{R}_1}(g \cdot v^{(i)})\ |\operatorname{Disc}(g \cdot v^{(i)})\ |\ dg}.$$

Discriminant

Now we have integrals which only care about when the absolute discriminant is less than 1. What is the discriminant of $g \cdot v^{(i)}$? Let's write $g = (\lambda, g')$ where $\lambda \in \mathbb{G}_m(\mathbb{Z}) \backslash \mathbb{G}_m(\mathbb{R}) = \mathbb{G}_m^+(\mathbb{R})$ (the positive real numbers), and $g' \in G''_{\mathbb{Z}} \backslash G''_{\mathbb{R}} := \operatorname{GL}_{n-1}(\mathbb{Z}) \backslash \operatorname{GL}_{n-1}^{\pm 1}(\mathbb{R}) \times \operatorname{GL}_{r-1}(\mathbb{Z}) \backslash \operatorname{GL}_{r-1}^{\pm 1}(\mathbb{R})$. Then

$$|\operatorname{Disc}(g \cdot v^{(i)})| = |\operatorname{Disc}(\lambda v^{(i)})| = |\lambda^d \operatorname{Disc}(v^{(i)})| = \lambda^d$$

where d is the dimension of $V_{\mathbb{R}}$ (if you don't remember why that's true, we have that only the scalar part affects the discriminant, λ in this case is positive, and we'd picked $v^{(i)}$ to have discriminant 1). In other words $|\operatorname{Disc}(g \cdot v^{(i)})|$ is constant on $G''_{\mathbb{Z}} \backslash G''_{\mathbb{R}}$ and if we rewrite our integral in terms of $\mathbb{G}_m^+$ and $G''_{\mathbb{Z}} \backslash G''_{\mathbb{R}}$, we can hope to separate out the $\mathbb{G}_m^+(\mathbb{R})$ part.

$$\begin{aligned}\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} &= \frac{\displaystyle\int_{\lambda\in\mathbb{G}_m^+(\mathbb{R})}\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}((\lambda,g')\cdot v^{(i)})\lambda^d dg' d^\times\lambda}{\displaystyle\int_{\lambda\in\mathbb{G}_m^+(\mathbb{R})}\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_1}((\lambda,g')\cdot v^{(i)})\lambda^d dg' d^\times\lambda} \\ &= \frac{\displaystyle\int_{\lambda\in\mathbb{G}_m^+(\mathbb{R})}\lambda^d\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}((\lambda,g')\cdot v^{(i)}) dg' d^\times\lambda}{\displaystyle\int_{\lambda\in\mathbb{G}_m^+(\mathbb{R})}\lambda^d\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_1}((\lambda,g')\cdot v^{(i)}) dg' d^\times\lambda}.\end{aligned}$$

Furthermore, we know that the integral is only non-zero if the absolute discriminant is less than 1, therefore we can bound λ to being between 0 and 1.

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_0^1\lambda^d\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}((\lambda,g')\cdot v^{(i)}) dg' d^\times\lambda}{\displaystyle\int_0^1\lambda^d\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_1}((\lambda,g')\cdot v^{(i)}) dg' d^\times\lambda}.$$

Now that our absolute discriminant is always less than 1, we have that $\mathcal{R}_1((\lambda,g')\cdot v^{(i)}) = 1$ for all $g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}$ and $\mathcal{R}_{1,W}((\lambda,g')\cdot v^{(i)}) = \mathcal{R}_{1,W}(g'\cdot v^{(i)})$ since scaling doesn't affect whether the shape is in W. Thus,

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_0^1\lambda^d\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g'\cdot v^{(i)}) dg' d^\times\lambda}{\displaystyle\int_0^1\lambda^d\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} dg' d^\times\lambda}.$$

Now on top and bottom the dg' integrands have no λ whatsoever and are thus constants with respect to $d^\times\lambda$, so we can pull out that whole integral and get the product of two distinct integrals.

$$\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_0^1\lambda^d d^\times\lambda\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g'\cdot v^{(i)}) dg'}{\displaystyle\int_0^1\lambda^d d^\times\lambda\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} dg'} = \frac{\displaystyle\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} \chi_{\mathcal{R}_{1,W}}(g'\cdot v^{(i)}) dg'}{\displaystyle\int_{g'\in G''_{\mathbb{Z}}\backslash G''_{\mathbb{R}}} dg'}.$$

Shape

Now we want to understand when $\chi_{\mathcal{R}_{1,W}}(g' \cdot v^{(i)})$ is non-zero, which happens only when the shape of $g' \cdot v^{(i)}$ is in W. Again we ask what is the shape of $g' \cdot v^{(i)}$ and again we will rewrite our group element this time as $g' = (g'_{n-1}, g'_{r-1}) \in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R}) \times \mathrm{GL}_{r-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})$. We know that g'_{r-1} does not affect the shape, therefore $\mathrm{Sh}(g' \cdot v^{(i)}) = \mathrm{Sh}(g'_{n-1} \cdot v^{(i)})$, and so $\chi_{\mathcal{R}_{1,W}}(g' \cdot v^{(i)}) = \chi_{\mathcal{R}_{1,W}}(g'_{n-1} \cdot v^{(i)})$ is constant on $\mathrm{GL}_{r-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})$. Thus,

$$\begin{aligned}
\frac{\mathrm{Vol}(\mathcal{R}_{1,W})}{\mathrm{Vol}(\mathcal{R}_1)} &= \frac{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})} \int_{g'_{r-1}\in \mathrm{GL}_{r-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g'_{n-1}\cdot v^{(i)}) dg'_{r-1} dg'_{n-1}}{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})} \int_{g'_{r-1}\in \mathrm{GL}_{r-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})} dg'_{r-1} dg'_{n-1}} \\
&= \frac{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g'_{n-1}\cdot v^{(i)}) dg'_{n-1} \int_{g'_{r-1}\in \mathrm{GL}_{r-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})} dg'_{r-1}}{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})} dg'_{n-1} \int_{g'_{r-1}\in \mathrm{GL}_{r-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{r-1}(\mathbb{R})} dg'_{r-1}} \\
&= \frac{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g'_{n-1}\cdot v^{(i)}) dg'_{n-1}}{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})} dg'_{n-1}}.
\end{aligned}$$

Destination Space of Shapes

Let's not forget that ultimately we want to get to our space of shapes which we're writing as $\mathcal{S}_{n-1} = \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/ \mathrm{GO}_{n-1}(\mathbb{R})$. Right now we're looking at $\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})$. Are they related? Certainly you can send any equivalence class $\mathrm{GL}_{n-1}(\mathbb{Z})g'_{n-1} \in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})$ to $\mathrm{GL}_{n-1}(\mathbb{Z})g'_{n-1}\, \mathrm{GO}_{n-1}(\mathbb{R}) \in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/ \mathrm{GO}_{n-1}(\mathbb{R})$, but what is the kernel of that map? It's not $\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GO}_{n-1}(\mathbb{R})$, as we'd need for isomorphism, because that allows for any determinant over $\mathbb{R}$ so is not contained in $\mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})$, however if we just impose our ±1 condition on the determinants, we're good to go. Indeed, we get that $\mathcal{S}_{n-1} = \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}_{n-1}(\mathbb{R})/ \mathrm{GO}_{n-1}(\mathbb{R}) \cong \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})/ \mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})$, and now we have hope of finishing.

Integrating Quotient Groups

Fun fact: [Liu65] For G a group and $H, K \leq G$, and whatever measure stuff you need,

$$\int_{H\backslash G/K} f(g)dg \int_K f(k)dk = \int_{H\backslash G} f(g)dg.$$

Which means we now have:

$$\frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})/\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g'_{n-1}\cdot v^{(i)})dg'_{n-1} \int_{\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(k\cdot v^{(i)})dk}{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})/\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} dg'_{n-1} \int_{\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} dk}.$$

I had a bit of a crisis over whether my characteristic function was still okay after messing around with the GOs, because I worried we weren't still in the right fundamental domain. Fortunately $\mathcal{F}$ was chosen to be GO-stable, so everything is fine.

The discriminant and shape are constant on $\mathrm{GO}^{\pm 1}_{n-1}$, so we have that

$$\int_{\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(k\cdot v^{(i)})dk = \int_{\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} dk,$$

giving:

$$\frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})/\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g'_{n-1}\cdot v^{(i)})dg'_{n-1} \int_{\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} dk}{\displaystyle\int_{g'_{n-1}\in \mathrm{GL}_{n-1}(\mathbb{Z})\backslash \mathrm{GL}^{\pm 1}_{n-1}(\mathbb{R})/\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} dg'_{n-1} \int_{\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} dk}$$

Since $\int_{\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})} dk$ is finite (because $\mathrm{GO}^{\pm 1}_{n-1}(\mathbb{R})$ is compact and dk is nice), this is cool, and we may cancel. Let's also replace our new space with the now isomorphic space of shapes.

$$\frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{g\in \operatorname{GL}_{n-1}(\mathbb{Z})\backslash \operatorname{GL}_{n-1}(\mathbb{R})/\operatorname{GO}_{n-1}(\mathbb{R})} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)})dg}{\displaystyle\int_{g\in \operatorname{GL}_{n-1}(\mathbb{Z})\backslash \operatorname{GL}_{n-1}(\mathbb{R})/\operatorname{GO}_{n-1}(\mathbb{R})} dg}$$

$$= \frac{\displaystyle\int_{g\in\mathcal{S}_{n-1}} \chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)})dg}{\displaystyle\int_{g\in\mathcal{S}_{n-1}} dg}.$$

Shape in W

The last step is to look at the shape of $g\cdot v^{(i)}$, where now $g\in\mathcal{S}_{n-1}$. Since $\operatorname{Sh}(v^{(i)}) = I$, we know that $\operatorname{Sh}(g\cdot v^{(i)}) = g\operatorname{Sh}(v^{(i)}) = g$. Therefore, the set of $g\in\mathcal{S}_{n-1}$ such that $\operatorname{Sh}(g\cdot v^{(i)})\in W$ is the same as the set of $g\in\mathcal{S}_{n-1}$ such that $g\in W$. If we define $\chi_W(g)$ to be the characteristic function of $W\subset\mathcal{S}_{n-1}$ then we have $\chi_{\mathcal{R}_{1,W}}(g\cdot v^{(i)}) = \chi_W(g)$ for all $g\in\mathcal{S}_{n-1}$.

In other words,

$$\frac{\operatorname{Vol}(\mathcal{R}_{1,W})}{\operatorname{Vol}(\mathcal{R}_1)} = \frac{\displaystyle\int_{g\in\mathcal{S}_{n-1}} \chi_W(g)dg}{\displaystyle\int_{g\in\mathcal{S}_{n-1}} dg} = \frac{\displaystyle\int_W dg}{\displaystyle\int_{\mathcal{S}_{n-1}} dg} = \frac{\mu(W)}{\mu(\mathcal{S}_{n-1})}.$$

HOORAY!!!

6.3 Light Weeding

In the making of this, I found it vaguely annoying that in the sources I was using the “volume” factor was often written explicitly (in numbers or “numbers”), so I had to actually read something to know that it was there. Just for reference, I’ll include the actual volumes here, but mostly this is a weedless chapter.

$n = 3$

From [BST13], $c_i = \frac{2\pi}{n_i}$ in our Proposition 13, and $\operatorname{Vol}(\mathcal{R}_1(v^{(i)})) = \dfrac{\pi^2}{12}$.

$n = 4$

From [Bha05], $c_i = \frac{n_i}{6\pi^3}$ and $\mathrm{Vol}(\mathcal{R}_1(v^{(i)})) = \dfrac{\zeta(2)^2\zeta(3)}{2}$.

$n = 5$

From [Bha10], $c_i = \frac{n_i}{20}$ and $\mathrm{Vol}(\mathcal{R}_1(v^{(i)})) = \dfrac{\zeta(2)^2\zeta(3)^2\zeta(4)^2\zeta(5)}{2}$.

THE END

You're still here? Oh, I guess I should tell you math papers generally don't have what you or I might call a "conclusion." They just sort of stop.

So, yeah, you can, um, go now. But, cheers!

Seriously, it’s over.

Bibliography

[BH13] M. Bhargava and Piper H., *The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields*, preprint, arXiv:1309.2025, 2013.

[Bha04] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Annals of Mathematics, Second Series **159** (2004), no. 3, 1329–1360.

[Bha05] ———, *The density of discriminants of quartic rings and fields*, Annals of Mathematics, Second Series **162** (2005), no. 2, 1031–1063.

[Bha06] ———, *Higher composition laws and applications*, Proceedings of the International Congress of Mathematician (M. Sanz-Sol, J. Soria, J. L. Varona, and J. Verdera, eds.), vol. 2, EMS, 2006.

[Bha08] ———, *Higher composition laws IV: The parametrization of quintic rings*, Annals of Mathematics, Second Series **167** (2008), no. 1, 53–94.

[Bha10] ———, *The density of discriminants of quintic rings and fields*, Annals of Mathematics, Second Series **172** (2010), no. 3, 1559–1591.

[BS14] M. Bhargava and A. Shnidman, *On the number of cubic orders of bounded discriminant having automorphism group C_3, and related problems*, Algebra & Number Theory **8** (2014), no. 1, 53–88.

[BST13] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport–Heilbronn theorems and second order terms*, Inventiones mathematicae **193** (2013), no. 2, 439–499.

[Dav51a] H. Davenport, *On a principle of Lipschitz*, Journal of the London Mathematical Society, Second Series **26** (1951), 179–183.

[Dav51b] ______, *On the class-number of binary cubic forms I*, Journal of the London Mathematical Society, Second Series **26** (1951), 183–192.

[Dav51c] ______, *On the class-number of binary cubic forms II*, Journal of the London Mathematical Society, Second Series **26** (1951), 192–198.

[DF64] B. N. Delone and D. K. Fadeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, AMS, 1964.

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proceedings of the Royal Society. London. Series A. Mathematical, Physical and Engineering Sciences **322** (1971), no. 1551, 405–420.

[Ell14] J. Ellenberg, *How not to be wrong*, The Penguin Press, 2014, A The New York Times Best Seller!

[Liu65] T. Liu, *Invariant measures on double coset spaces*, Journal of the Australian Mathematical Society **5** (1965), 495–505.

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, 1999, Translated from the German by N. Schappacher.

[Shi72] T. Shintani, *On Dirichlet series whose coefficients are class numbers of integral binary cubic forms*, Journal of the Mathematical Society of Japan **24** (1972), 132–188.

[SK77] M. Sato and T. Kimura, *A classification of irreducible prehomogeneous vector spaces and their relative invariants*, Nagoya Mathematical Journal **65** (1977), 1–155.

[Ter97] D. Terr, *The distribution of shapes of cubic orders*, Ph.D. thesis, University of California, Berkeley, 1997.