INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

Higher Composition Laws

Manjul Bhargava

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

June 2001

Bell & Howell Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

Abstract

The primary aim of this thesis is to derive higher analogues of Gauss's celebrated law of composition on the space of binary quadratic forms. Specifically, we show that Gauss's law is only one of at least ten such laws of composition that yield information on the class groups of algebraic number fields. We begin our investigation of higher composition laws by giving a new perspective on Gauss composition in a manner reminiscent of the group law on elliptic curves. We then proceed to derive new laws of composition on $2 \times 2 \times 2$ cubes, binary cubic forms, pairs of binary quadratic forms, $2 \times 3 \times 3$ boxes, and pairs of ternary quadratic forms. We show that the resulting groups in these spaces all have natural interpretations in terms of ideal classes of orders in algebraic number fields.

We also develop a theory of resolvent rings in order to explain how orders in number fields of low degree should be parametrized. The theory allows us, in particular, to obtain a new derivation of the Delone-Faddeev-Gross parametrization of cubic rings by means of binary cubic forms. More importantly, our perspective enables us to generalize the Delone-Faddeev-Gross result to the quartic case, yielding a parametrization of quartic rings by means of two ternary quadratic forms.

We use this new parametrization result for quartic rings, in the spirit of Davenport-Heilbronn, to compute the density of discriminants of S_4-quartic fields, thus resolving this long-standing problem. In addition, our methods allow us also to compute the mean value of the size of the 2-class group of cubic fields. This result confirms, for the first time, a case of the Cohen-Martinet heuristics, and implies that at least 75% of totally real cubic fields have odd class number.

Finally, we expect that the composition laws presented here will have many additional applications, e.g., to the theory of automorphic forms on exceptional groups. We outline a few of these potential applications to indicate directions for future work.

Acknowledgments

First and foremost, I would like to express my thanks to my advisor, Professor Andrew Wiles, for his constant encouragement, enthusiasm, and sound advice. I am also extremely grateful to Professor Peter Sarnak for his deep interest in my work, and for many wonderful and helpful conversations. In addition, I would like to thank Professor John Conway, who served as my first-year mentor and from whom I have learned a great deal.

My graduate work has also benefited due to conversations with a number of other mathematicians; in this regard, I would especially like to thank Professor Dick Gross, Johan deJong, Kiran Kedlaya, Lenny Ng, and Ravi Vakil.

I extend my gratitude to the Hertz Foundation for funding my graduate work and this project, and to the Clay Mathematics Institute (CMI) for their subsequent support. Additionally, I would like to thank the Princeton Mathematics Department for providing me an excellent environment in which to work, and MSRI for its hospitality during the summers of 1999 and 2000, where I found my first "higher composition law".

Finally, I want to thank all my friends and family for their love and support. I am especially grateful to my grandparents, my mother, and my uncle, for their constant interest in my progress, and their continuous encouragement.

To

my Nanaji and Naniji,

Ma, Mausi, Mamaji, and Mami,

Hansa, Mudita, Aparna Didis, and Nalin

Contents

Chapter 1

Introduction

Two centuries ago, in his celebrated work *Disquisitiones Arithmeticae* of 1801, Gauss laid down the beautiful law of composition of integral binary quadratic forms which would play such a critical role in number theory in the decades to follow. Even today, two hundred years later, this law of composition still remains one of the primary tools for understanding and computing with the class groups of quadratic orders.

It is thus only natural to ask whether higher analogues of this composition law might exist that could shed light on the structure of other algebraic number rings and fields. The primary objective of this dissertation is precisely to work towards such "higher composition laws." In fact, we show that Gauss's law of composition is only one of at least ten composition laws of its kind that yield information on number rings and their class groups.

In Chapter 2, we begin by examining the quadratic case more closely, and derive a general law of composition on $2 \times 2 \times 2$ cubes of integers, from which we obtain Gauss's law as a simple special case in a manner reminiscent of the group law on elliptic curves. We also obtain from this general law on $2 \times 2 \times 2$ cubes two further new laws of composition, one defined on the space of binary cubic forms, and the other on pairs of binary quadratic forms.

These composition laws all turn out to have natural interpretations in terms of ideal classes of quadratic rings. We prove that the law of composition on $2 \times 2 \times 2$ cubes gives rise to groups isomorphic to $\mathrm{NCl}(S) \times \mathrm{NCl}(S)$, where $\mathrm{NCl}(S)$ denotes the narrow class group of the quadratic order S. This interpretation of the space of $2 \times 2 \times 2$ cubes then specializes to give the narrow class group in Gauss's case and in the case of pairs of binary quadratic forms, and yields roughly the 3-part of the narrow class group in the case of binary cubic forms.

In Chapter 3, we look for the cubic analogue of the $2 \times 2 \times 2$ cube. Interestingly, it is not the $3 \times 3 \times 3$ cube as one might first guess, but is rather the $2 \times 3 \times 3$ box. The space of $2 \times 3 \times 3$ boxes of integers turns out to be exactly what is needed for a cubic analogue of Gauss's theory; indeed, there is again a natural composition law on this space, and we prove that the groups obtained via this law of composition are isomorphic to the class groups of cubic orders.

Specializing this general cubic law, we then also obtain a law of composition on pairs of ternary quadratic forms. We show that the corresponding groups turn out to equal roughly the 2-parts of the ideal class groups of cubic rings.

Very helpful in discovering the above cubic composition laws was the parametrization of cubic rings due to Delone-Faddeev and Gross, who showed that cubic rings correspond naturally to integral binary cubic forms. Parametrizations of this kind have not been known to exist for rings of higher rank. In Chapter 4, we derive such a parametrization result for quartic rings. We begin by developing a theory of resolvent rings, which allows us to give a new, purely ring-theoretic interpretation of the Delone-Faddeev-Gross parametrization of cubic rings. We are then able to generalize this perspective to rings of rank 4, and prove that the correct objects parametrizing quartic rings are pairs of integral ternary quadratic forms.

One of the most stellar applications of the parametrization of cubic orders is the well-known work of Davenport and Heilbronn [11], who used this parametrization to

compute the asymptotic density of discriminants of cubic fields. Having obtained a parametrization for quartic orders (Chapter 4), it is natural to ask whether similar density theorems could now be proven for quartic fields. We accomplish this in Chapter 5. As a by-product, we also obtain the mean value of the size of the 2-class group of cubic fields; our result verifies, for the first time, a case of the Cohen-Martinet heuristics, and implies, in particular, that at least 75% of totally real cubic fields have odd class number.

We note that many of the spaces we have derived here over $\mathbb{Z}$ were previously considered over the rational numbers in the work of Wright-Yukie [25], who showed that generic rational orbits in these spaces correspond to étale extensions of $\mathbb{Q}$ of degree 2, 3, 4, or 5. One of the motivations for their work was to apply an adelic version of Sato and Shintani's zeta function theory [23], developed by Datskovsky and Wright [8], to obtain density theorems for field extensions. In the case of pairs of ternary quadratic forms over $\mathbb{Q}$, the corresponding global adelic zeta function was treated in the treatise of Yukie [26], who showed that the rightmost pole of this zeta function is of order 2. The double pole, however, poses some significant difficulties in obtaining a density of discriminants result for quartic fields, because the necessary "filtering process" does not apply in its usual form (see [8], [26]). As these difficulties have not been overcome, the long-standing question on the density of discriminants of quartic fields has remained open. We resolve this problem by using the rich structure over $\mathbb{Z}$ to cut directly to (the orders in) S_4-quartic fields, eliminating altogether the undesirable dominant term corresponding to reducible rings. The problem then is eventually reduced to a simple volume computation which we carry out explicitly.

Regarding our result on the density of discriminants of quartic fields, we should also like to mention the recent announcement of Cohen-Diaz-Olivier [5], who have obtained by very different methods the correct order of growth cX for the number of S_4-quartic fields of absolute discriminant at most X. Their methods do not, however,

yield any information on the value of the constant c. Our approach leads naturally to the explicit determination of c, which is important in the applications.

We end this introduction with two remarks on generality. First, since there is always a unique ring homomorphism $\mathbb{Z} \to T$, the parametrization and composition laws defined in this thesis over $\mathbb{Z}$ are in fact valid over any base ring T. However, as it is our main case of interest, we always take the base ring T to be $\mathbb{Z}$. Second, the parametrization results obtained in this thesis may be extended in a natural way to "orders" in non-étale extensions of $\mathbb{Q}$. Although not of essential interest here from the perspective of higher composition, class groups, and density theorems, such generalizations to discriminant zero rings may prove important in the study of automorphic forms on exceptional groups, and will be treated more fully in subsequent work.

Chapter 2

Quadratic composition laws

In this chapter, we begin our study of higher composition by taking a closer look at the quadratic case. We find that the fundamental object of quadratic composition is the space of $2 \times 2 \times 2$ integer cubes, which has on it a natural composition law. Our perspective of $2 \times 2 \times 2$ cubes leads in particular to a very simple and elegant description of the composition law of Gauss, and additionally, yields new composition laws on binary cubic forms and on pairs of binary quadratic forms. These four laws of composition are discussed in Section 2.1.

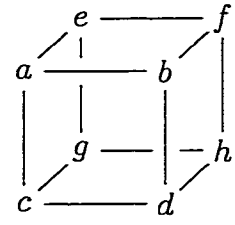
In Section 2.2, we then show how the groups resulting from these composition laws may naturally be interpreted in terms of the ideal class groups of quadratic orders.

2.1 On $2 \times 2 \times 2$ cubes of integers

In this section, we examine the natural action of $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ on the space $C_2 = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ of $2 \times 2 \times 2$ cubical integer matrices.

2.1.1 The fundamental slicings

A cube of integers $A \in \mathcal{C}_2$ may be partitioned into two 2×2 matrices in three essentially different ways, corresponding to the three possible slicings of a cube—along its three planes of symmetry—into two congruent parallelopipeds. More precisely, the integer cube



can be partitioned into the 2×2 matrices

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \; N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

or into

$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix}, \; N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}$$

or

$$M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix}, \; N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}.$$

Our action of Γ is defined so that, for any $1 \leq i \leq 3$, an element $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ in the ith factor of $SL_2(\mathbb{Z})$ acts on the cube A by replacing (M_i, N_i) by $(rM_i + sN_i, tM_i + uN_i)$.

For each such i, let us construct a quadratic form Q_i, by defining

$$-Q_i(x, y) = \mathrm{Det}(M_i x - N_i y).$$

Then note that the form Q_1 is invariant under the action of the subgroup $\{e\} \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \subset \Gamma$. The remaining factor of $SL_2(\mathbb{Z})$ acts in the standard way on Q_1, and it is well-known that over $\mathbb{C}$ this action has exactly one invariant, namely the discriminant $\mathrm{Disc}(Q_1)$ of Q_1. Thus the unique invariant for the action of $SL_2(\mathbb{C}) \times SL_2(\mathbb{C}) \times SL_2(\mathbb{C})$ on its representation $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ is given simply by $\mathrm{Disc}(Q_1)$. Of course, by the same reasoning, $\mathrm{Disc}(Q_2)$ and $\mathrm{Disc}(Q_3)$ must also be equal to this same invariant up to scalar factors. A quick calculation shows that in fact $\mathrm{Disc}(Q_1) = \mathrm{Disc}(Q_2) = \mathrm{Disc}(Q_3)$; we denote this common value simply by $\mathrm{Disc}(A)$.

2.1.2 Gauss's law revisited

We have seen that every cube A in $\mathcal{C}_2$ gives three integral binary quadratic forms Q_1, Q_2, Q_3, all having the same discriminant. Let us define an addition law on binary quadratic forms by declaring that, for all such triplets Q_1, Q_2, Q_3 arising from a cube A,

The Cube Law. *The sum of Q_1, Q_2, Q_3 is zero.**

The Cube Law has some interesting consequences. First, suppose that $\gamma = \gamma_1 \times e \times e \in \Gamma$, and that A gives rise to the three quadratic forms Q_1, Q_2, Q_3. Then $A' = \gamma A$ gives rise to the three quadratic forms Q_1', Q_2, Q_3, where $Q_1' = \gamma_1 Q_1$. It follows immediately from the Cube Law that $SL_2(\mathbb{Z})$-equivalent forms correspond to the same element.

For quadratic forms Q_1, Q_2, Q_3 associated to a cube A we shall write $[Q_1] + [Q_2] + [Q_3] = 0$, where $[Q]$ is used to denote the $SL_2(\mathbb{Z})$-equivalence class of Q. When

*The analogy with elliptic curves is evident.

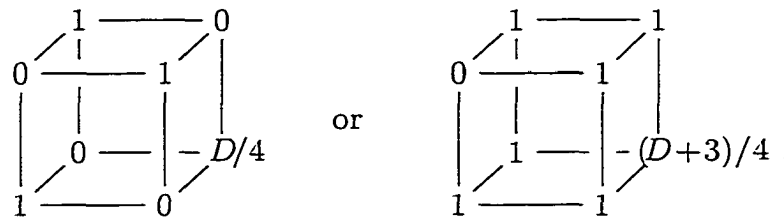
this law is then restricted to the set of all (equivalence classes of) primitive binary quadratic forms of a given discriminant D, and an identity element is chosen, we find

Theorem 2.1 *This defines a group law!*

For the identity, we may take any binary quadratic form Q such that $[Q]+[Q]+[Q] = 0$. The most natural choice of identity is

$$O_D = [x^2 - \frac{D}{4}y^2] \quad \text{or} \quad O_D = [x^2 - xy + \frac{1-D}{4}y^2] \tag{2.1}$$

in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$. That $[O_D] + [O_D] + [O_D] = 0$ follows from the cubes



(2.2)

whose three associated quadratic forms are all given by O_D (as defined by (2.1)).

More formally, the group referred to in Theorem 2.1 is obtained by considering the free abelian group generated by all primitive quadratic forms of a given discriminant D, and quotienting by O_D and by all relations of the form $Q_1 + Q_2 + Q_3 = 0$, where $\{Q_1, Q_2, Q_3\}$ is a triplet of quadratic forms arising from a cube A of discriminant D.

Assuming the Cube Law, we find that its converse must then also be true:

Theorem 2.2 *If* $[Q_1]+[Q_2]+[Q_3] = 0$, *then there exists a cube* $A \in \mathcal{C}_2$ *such that the three associated quadratic forms are* Q_1, Q_2, Q_3 *respectively.*[†]

We denote the set of primitive binary quadratic forms of discriminant D, equipped with the above group structure, by $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z})^*; D\big)$. Indeed, this group structure on

[†]We note again the analogy with elliptic curves.

integral binary quadratic forms turns out to be equivalent to that defined by Gauss. We give a proof of this equivalence, and of Theorems 2.1 and 2.2, in Section 2.2 using the language of ideal classes. An alternate proof not using ideal classes is given in the Appendix.

2.1.3 Composition of $2 \times 2 \times 2$ cubes

Having defined a law of composition on the quadratic forms arising from a cube, we may now define a law of composition on the cubes themselves. First, let us make a definition.

Definition 2.3 A $2\times2\times2$ cube A is said to be *projective* if each of the three quadratic forms Q_1, Q_2, Q_3 associated to A is primitive.

Now let A and B be any two projective cubes in $\mathcal{C}_2$ having the same discriminant D, and let Q_1, Q_2, Q_3 and R_1, R_2, R_3 be their associated triples of primitive quadratic forms. Then since $[Q_1] + [Q_2] + [Q_3] = 0$ and $[R_1] + [R_2] + [R_3] = 0$, we must have $([Q_1]+[R_1])+([Q_2]+[R_2])+([Q_3]+[R_3]) = 0$; hence by Theorem 2, there exists a cube $C \in \mathcal{C}_2$ whose three associated quadratic forms are (up to equivalence) $[Q_1] + [R_1]$, $[Q_2] + [R_2]$, and $[Q_3] + [R_3]$. We define the composition of A and B by declaring that $[A] + [B] = [C]$.

That this is a group law on the set of Γ-equivalence classes of projective cubes having the same fixed discriminant D follows immediately from Theorems 1 and 2. Furthermore, the identity in this group is given as in (2.2) in accordance with whether $D \equiv 0$ or $1 \pmod 4$.

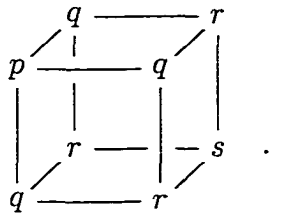
We denote the set of equivalence classes of projective binary cubic forms of discriminant D equipped with the above group structure by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$.

2.1.4 Composition of binary cubic forms

The above law of composition on cubes also leads naturally to a law of composition on $SL_2(\mathbb{Z})$-equivalence classes of integral binary cubic forms $px^3 + 3qx^2y + 3rxy^2 + sy^3$. For just as one frequently associates to a binary quadratic form $px^2 + 2qxy + ry^2$ the symmetric 2×2 matrix

$$\begin{bmatrix} p & q \\ q & r \end{bmatrix},$$

one may naturally associate to a binary cubic form $px^3 + 3qx^2y + 3rxy^2 + sy^3$ the symmetric $2 \times 2 \times 2$ matrix



It is easily checked that within the group defined on equivalence classes of projective cubes, the set of classes containing a symmetric cube forms a subgroup. Therefore, by restriction, we obtain a natural group law on the space of projective binary cubic forms of fixed discriminant D. The identity elements of course correspond to those indicated in the case of cubes (2.2), and are given by

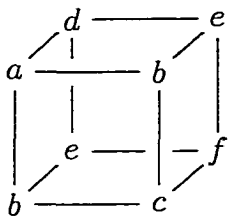
$$[3x^2y + Dy^3] \quad \text{or} \quad [3x^2y + 3xy^2 + \left(\frac{D+3}{4}\right)y^3] \tag{2.3}$$

in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$.

We denote the set of equivalence classes of projective binary cubic forms of discriminant D equipped with the above group structure by $\mathrm{Cl}(\mathrm{Sym}^3\mathbb{Z}^2; D)$.

2.1.5 Composition of pairs of binary quadratic forms

The group law on binary cubic forms of discriminant D was obtained by imposing a symmetry condition on the group of $2 \times 2 \times 2$ cubes of discriminant D, and checking that this symmetry was indeed preserved under the group law. Rather than imposing a threefold symmetry, one may instead impose only a twofold symmetry. This leads to cubes taking the form



That is, these cubes can be sliced (along a certain fixed plane) into two 2×2 symmetric matrices. It is again easily checked that such a symmetry is preserved under the quadratic forms having a fixed discriminant D. We denote the latter group by $\mathrm{Cl}(\mathbb{Z}^2 \otimes_{\mathrm{ary}} \mathrm{Sym}^2\mathbb{Z}^2; D)$.

quadratic forms having a fixed discriminant D. We denote the latter group by $\mathrm{Cl}(\mathbb{Z}^2 \otimes$ $\mathrm{Sym}^2\mathbb{Z}^2; D)$.

The groups $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D)$, however, are not new. Indeed, we have imposed our symmetry condition on cubes so that, for such a cube $A \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$, the last two associated quadratic forms Q_2 and Q_3 are equal, while the first, Q_1, is (possibly) different. Therefore the map

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D) \to \mathrm{Cl}((\mathrm{Sym}^2\mathbb{Z}^2)^*; D),$$

taking twofold symmetric projective cubes $A \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$ to their third associated quadratic form Q_3, yields an isomorphism of groups.[‡]

[‡]That these two spaces $(\mathrm{Sym}^2\mathbb{Z})^*$ and $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$ carry similar information may be a reflection of the fact that, in the language of prehomogenous vector spaces, $\mathrm{Sym}^2\mathbb{Z}$ is a *reduced form* of the space $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$.

In summary, we have the natural inclusions

$$\mathrm{Sym}^3\mathbb{Z}^2 \;\to\; \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2 \;\to\; \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \tag{2.4}$$

leading to natural group homomorphisms

$$\mathrm{Cl}(\mathrm{Sym}^3\mathbb{Z}^2; D) \;\to\; \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D) \;\to\; \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \tag{2.5}$$

where we have shown that the center group, $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D)$, is isomorphic to $\mathrm{Cl}\left((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\right)$.

2.2 Relations with ideal classes in quadratic orders

The integral orbits of the four spaces discussed in the previous section each have natural interpretations in terms of quadratic orders.

2.2.1 The parametrization of quadratic rings

It is elementary and well-known that a ring having finite rank as a $\mathbb{Z}$-module must have discriminant congruent to 0 or 1 (mod 4). Conversely, given any integer $D \equiv 0$ or 1 (mod 4) there is a unique quadratic ring $S(D)$ of discriminant D, given by

$$S(D) = \begin{cases} \mathbb{Z}[x]/(x^2) & \text{if } D = 0, \\ \mathbb{Z} \oplus \mathbb{Z} & \text{if } D = 1, \\ \mathbb{Z}[(D + \sqrt{D})/2] & \text{otherwise;} \end{cases} \tag{2.6}$$

explicitly, the ring $S(D)$ has $\mathbb{Z}$-basis $< 1, \tau >$ where multiplication is determined by the law

$$\tau^2 = \frac{D}{4} \tag{2.7}$$

or

$$\tau^2 = \frac{D-1}{4} + \tau \tag{2.8}$$

in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$.

Therefore, if we denote by $\tilde{\mathbb{Z}}$ the elements of $\mathbb{Z}$ that are congruent to 0 or 1 (mod 4), we may say that the isomorphism classes of quadratic rings are parametrized by $\tilde{\mathbb{Z}}$.

Theorem 2.4 *There is a one-to-one correspondence between the set of elements of $\tilde{\mathbb{Z}}$ and the set of isomorphism classes of quadratic rings, by the association*

$$D \leftrightarrow S(D)\,,$$

where $D = \mathrm{Disc}(S(D))$.

2.2.2 The case of binary quadratic forms

As is well-known, the group $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$ is almost, but not quite the same as, the ideal class group of the unique quadratic order S of discriminant D. To make up for the slight discrepancy, it is necessary to introduce the notion of *narrow class group*, which may be defined as the group $\mathrm{NCl}(S)$ of *oriented ideal classes*. More precisely, an *oriented ideal* is a pair (I, ϵ), where I is an ideal, and $\epsilon = \pm 1$ gives the *orientation* of I. Multiplication of oriented ideals is defined componentwise, and the norm of an oriented ideal (I, ϵ) is defined to be $N(I)\epsilon$. For an element $\kappa \in S$, $\kappa \cdot (I, \epsilon)$ is defined to be $(\kappa I, \mathrm{sgn}(N(\kappa))\epsilon)$. With these notions, the narrow class group can then be defined as the group of invertible oriented ideals modulo multiplication by nonzero scalars $\kappa \in S$ (equivalently, modulo the subgroup consisting of invertible *principal oriented ideals* $((\kappa), 1)$). In practice, we shall denote an oriented ideal (I, ϵ)

simply by I, with the orientation $\epsilon = \epsilon(I)$ on I being understood.[§]

We may now state the precise relation between equivalence classes of binary quadratic forms and ideal classes of quadratic orders.

Theorem 2.5 *There is a bijection between the set of $SL_2(\mathbb{Z})$-equivalence classes of binary quadratic forms of discriminant D, and the set of pairs (S, I), where S is a quadratic ring of discriminant D and I is a (not necessarily invertible) narrow ideal class of S.*

Restricting the above result to the set of primitive quadratic forms, we obtain the following group isomorphism.

Theorem 2.6 *The bijection of Theorem 2.5 restricts to a correspondence*

$$\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big) \leftrightarrow \mathrm{NCl}(S(D));$$

this correspondence is in fact an isomorphism of groups.

Theorem 2.5 is known in the indefinite case, while the general definite case follows easily from the known case of positive definite quadratic forms. We will give proofs of Theorems 2.1 and 2.2 in a more general context in the next section.

2.2.3 The case of $2 \times 2 \times 2$ cubes

We now turn to the general case of $2 \times 2 \times 2$ cubes. Before stating the result, we make some definitions. Let S be the quadratic ring of discriminant D. If $D > 0$ (resp. $D < 0$), we say three ideals (resp. oriented ideals) I_1, I_2, I_3 of S are *collinear* if there exists an element $\delta \in S$ such that $N(I_1)N(I_2)N(I_3) = N(\delta)$ and $I_1I_2I_3 \subseteq (\delta)$.

[§]Traditionally, the narrow class group is considered only for quadratic orders S of positive discriminant D, and is defined as the group of invertible ideals of S modulo the subgroup of invertible principal ideals that are generated by elements of positive norm. We prefer our definition here since it gives the correct notion also when $D \leq 0$.

Also, we define two collinear triples (I_1, I_2, I_3) and (I_1', I_2', I_3') of ideals (resp. oriented ideals) of S to be *equivalent* if $I_1 = \kappa_1 I_1'$, $I_2 = \kappa_2 I_2'$, $I_3 = \kappa_3 I_3'$ for some elements $\kappa_1, \kappa_2, \kappa_3$ of positive norm in the ring of quotients of S. (In particular, we must have $\kappa_1\kappa_2\kappa_3 = 1$.) For example, if S is Dedekind, then an equivalence class of collinear triples means simply a triple of narrow ideal classes whose product is the principal class.

Theorem 2.7 *There is a bijection, to be given below, between the set of* Γ*-orbits on the space of* $2 \times 2 \times 2$ *integer cubes, and the set of pairs* $(S, (I_1, I_2, I_3))$*, where* S *is a quadratic ring and* (I_1, I_2, I_3) *is a collinear triple of narrow ideal classes of* S*.*

Proof: Given a collinear triple (I_1, I_2, I_3) of ideals of a quadratic order S, where δ is an element such that $I_1I_2I_3 \subseteq (\delta)$ and $N(\delta) = N(I_1I_2I_3)$, we first show how to construct a corresponding $2 \times 2 \times 2$ cube. In accordance with whether $D = \mathrm{Disc}(S)$ is congruent to 0 or 1 (mod 4), let τ be an element of S satisfying $\tau^2 - \frac{D}{4} = 0$ or $\tau^2 - \tau + \frac{1-D}{4} = 0$ respectively. Then as a $\mathbb{Z}$-module, S has basis $< 1, \tau >$. Let $< \alpha_1, \alpha_2 >$, $< \beta_1, \beta_2 >$, and $< \gamma_1, \gamma_2 >$ denote $\mathbb{Z}$-bases of the ideals I_1, I_2, and I_3 respectively, where the basis for each I_j is chosen to be oriented the same as or different than $< 1, \tau >$ precisely in accordance with whether $\epsilon(I_j) = +1$ or -1. Since by hypothesis the product $I_1I_2I_3$ is contained in δS, we may write

$$\begin{aligned} \alpha_1\beta_1\gamma_1 &= \delta\,(\,c_{111} + a_{111}\tau\,) \\ \alpha_1\beta_1\gamma_2 &= \delta\,(\,c_{112} + a_{112}\tau\,) \\ &\vdots \\ \alpha_2\beta_2\gamma_2 &= \delta\,(\,c_{222} + a_{222}\tau\,) \end{aligned} \tag{2.9}$$

for some set of sixteen integers a_{ijk} and c_{ijk} $(1 \le i, j, k \le 2)$. Then $A = (a_{ijk})$ is our desired $2 \times 2 \times 2$ cube.

It is clear from construction that changing $< \alpha_1, \alpha_2 >$, $< \beta_1, \beta_2 >$, $< \gamma_1, \gamma_2 >$ to some other set of (appropriately oriented) bases for I_1, I_2, I_3, via an element $T \in \Gamma$, would simply transform A into an equivalent cube via that same element T. Hence the Γ-equivalence class of A is independent of our choice of bases for I_1, I_2, and I_3. Furthermore, it is clear that if the collinear triple (I_1, I_2, I_3) is replaced by an equivalent triple, our cube A does not change. Hence we have a well-defined map from collinear triples of narrow ideal classes in a quadratic ring to Γ-orbits in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$.

It remains to show that this mapping $(S, (I_1, I_2, I_3)) \to A$ is in fact a bijection; that is, we wish to show that for any given cube A there is *exactly one* pair $(S, (I_1, I_2, I_3))$ up to equivalence that yields the element A via the above map.

To this end, let us fix a cube $A = (a_{ijk})$ of discriminant D, and consider the system (2.9), which currently consists mostly of indeterminates. We show that all these indeterminates are in fact essentially determined by A.

First, we claim that the ring S is determined by A. It suffices to show that $\mathrm{Disc}(S)$ is determined. Writing out $\alpha_i, \beta_i, \gamma_i$ $(1 \leq i \leq 3)$ and δ in terms of the basis $< 1, \tau >$ of S (with indeterminate coefficients), and using the relations (2.9), a large but beautiful calculation shows that

$$\mathrm{Disc}(A) = N(I_1)N(I_2)N(I_3)N(\delta)^{-1} \cdot \mathrm{Disc}(S).$$

But by assumption $N(I_1)N(I_2)N(I_3) = N(\delta)$, so

$$\mathrm{Disc}(A) = \mathrm{Disc}(S), \tag{2.10}$$

and therefore S is indeed determined by A.

Now by the associativity and commutativity of S, we must have

$$\alpha_i\beta_j\gamma_k \cdot \alpha_{i'}\beta_{j'}\gamma_{k'} = \alpha_{i'}\beta_j\gamma_k \cdot \alpha_i\beta_{j'}\gamma_{k'} = \alpha_i\beta_{j'}\gamma_k \cdot \alpha_{i'}\beta_j\gamma_{k'} = \alpha_i\beta_j\gamma_{k'} \cdot \alpha_{i'}\beta_{j'}\gamma_k \quad (2.11)$$

for all $1 \leq i, i', j, j', k, k' \leq 2$. Expanding out these identities using (2.9), and then equating all coefficients of 1 and τ, yields 18 (linear and quadratic) equations in the eight variables c_{ijk} in terms of the a_{ijk}. We find that this system, together with the condition $N(I_1)N(I_2)N(I_3) > 0$, has a unique solution, given by

$$c_{111} = (a_{111}^2 a_{222} + 2a_{112}a_{121}a_{211} - a_{111}a_{112}a_{221} - a_{111}a_{121}a_{212} - a_{111}a_{122}a_{211})/2$$

or by

$$c_{111} = (a_{111}^2 a_{222} + 2a_{112}a_{121}a_{211} - a_{111}a_{112}a_{221} - a_{111}a_{121}a_{212} - a_{111}a_{122}a_{211} - a_{111})/2,$$

in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$, with symmetrically obtained expressions for the other c_{ijk}. A quick congruence check shows that the solutions for the c_{ijk} are necessarily integral! Therefore, the c_{ijk}'s in (2.9) are also uniquely determined by the cube A.

We must still determine the existence of $\alpha_i, \beta_j, \gamma_k \in S$ yielding the desired a_{ijk} and c_{ijk}'s in (2.9). It is clear that the pair (α_1, α_2) (similarly (β_1, β_2), (γ_1, γ_2)) is uniquely determined—up to nonzero scaling factors in S—by the equations (2.9). For example, given any fixed $1 \leq j, k \leq 2$, we have

$$\alpha_1\beta_j\gamma_k(c_{2jk} + a_{2jk}\tau) = \alpha_2\beta_j\gamma_k(c_{1jk} + a_{1jk}\tau),$$

so the ratio $\alpha_1 : \alpha_2$ is determined, and we may let, e.g., $\alpha_1 = c_{1jk} + a_{1jk}\tau$ and $\alpha_2 = c_{2jk} + a_{2jk}\tau$. That this choice of (α_1, α_2) is independent of i, j (up to a constant

factor) follows from the associative laws (2.11) that have been forced upon the system (2.9).

Thus we must show only that the $\mathbb{Z}$-modules $I_1 =< \alpha_1, \alpha_2 >$, $I_2 =< \beta_1, \beta_2 >$, $I_3 =< \gamma_1, \gamma_2 >$ as determined above actually form ideals in S. In fact, it is possible to determine the precise S-module structures of I_1, I_2, I_3. Let Q_1, Q_2, Q_3 be the three quadratic forms associated to A as in Section 2.1.2, where we write $Q_i = p_i x^2 + q_i xy + r_i y^2$. Then a short calculation using the explicit expressions for $\alpha_i, \beta_j, \gamma_k$ as above shows that

$$\begin{aligned} 1 \cdot \alpha_1 &= \alpha_1 \\ 1 \cdot \alpha_2 &= \alpha_2 \\ \tau \cdot \alpha_1 &= \tfrac{q_1}{2} \cdot \alpha_1 + p_1 \cdot \alpha_2 \\ -\tau \cdot \alpha_2 &= r_1 \cdot \alpha_1 + \tfrac{q_1}{2} \cdot \alpha_2 \end{aligned} \tag{2.12}$$

or

$$\begin{aligned} 1 \cdot \alpha_1 &= \alpha_1 \\ 1 \cdot \alpha_2 &= \alpha_2 \\ \tau \cdot \alpha_1 &= \tfrac{q_1+1}{2} \cdot \alpha_1 + p_1 \cdot \alpha_2 \\ -\tau \cdot \alpha_2 &= r_1 \cdot \alpha_1 + \tfrac{q_1-1}{2} \cdot \alpha_2 \end{aligned} \tag{2.13}$$

in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$, where the module structures of $I_2 =< \beta_1, \beta_2 >$ and $I_3 =< \gamma_1, \gamma_2 >$ are given analogously in terms of the forms Q_2 and Q_3 respectively. In particular, we see that I_1, I_2, I_3 are indeed ideals of S.

We have now determined all the indeterminates in (2.9), having started only with the value of the cube A. It follows that there is exactly one pair $(S, (I_1, I_2, I_3))$ up to equivalence which yields the cube A under the mapping $(S, (I_1, I_2, I_3)) \to A$; this completes the proof. □

Note that the above discussion makes the bijection of Theorem 2.7 very precise. Given a quadratic ring S and a collinear triple (I_1, I_2, I_3) of ideals in S, the corresponding cube $A = (a_{ijk})$ is obtained from equations (2.9). Conversely, given a cube $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, the ring S is determined by (2.10); bases for the ideal classes I_1, I_2, I_3 in S are obtained from (2.9), and the S-module structures of I_1, I_2, and I_3 are given by (2.12) and (2.13).

Finally, define a collinear triple (I_1, I_2, I_3) of ideals of S to be *projective* if I_1, I_2, I_3 are projective as S-modules. Then there is a natural group law on the set of projective collinear triples of ideals of a ring S. Namely, for any two such collinear triples (I_1, I_2, I_3) and (I_1', I_2', I_3'), define their composition to be the (collinear) triple $(I_1 I_1', I_2 I_2', I_3 I_3')$. This group of projective collinear triples is naturally isomorphic to $\mathrm{NCl}(S) \times \mathrm{NCl}(S)$, via the map $(I_1, I_2, I_3) \to (I_1, I_2)$.

Restricting Theorem 2.7 to the set of projective elements of C_2, and noting that projective cubes give rise to projective collinear triples of ideals, yields the following group isomorphism.

Theorem 2.8 *The bijection of Theorem 2.7 restricts to a correspondence*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \leftrightarrow \mathrm{NCl}(S(D)) \times \mathrm{NCl}(S(D));$$

this correspondence is in fact an isomorphism of groups.

That primitive binary quadratic forms and projective ideal classes are in one-to-one correspondence (the case of Gauss) is of course recovered as a special case. Indeed, a short calculation shows that the norm forms of I_1, I_2, I_3 as given by Theorem 2.7 are simply Q_1, Q_2, Q_3, where Q_1, Q_2, Q_3 are the three quadratic forms associated to A. Thus we have also proven Theorems 2.1, 2.2, 2.5, and 2.6.

2.2.4 The case of binary cubic forms

In this section, we obtain the analogue of Theorem 2.7 for binary cubic forms.

Theorem 2.9 *There is a bijection, to be given below, between the set of $SL_2(\mathbb{Z})$-orbits on the space $\mathrm{Sym}^3\mathbb{Z}^2$, and the set of equivalence classes of triples (S, I, δ), where S is a quadratic ring, I is an ideal of S, and δ is an element of I^3 such that $N(\delta) = N(I)^3$. (Here two triples (S, I, δ) and (S, I', δ') are equivalent if there exists a nonzero element κ in the ring of quotients of S such that $I' = \kappa I$ and $\delta' = \kappa^3\delta$.)*

Proof: Given a triple (S, I, δ) as in the theorem, we first show how to construct the corresponding binary cubic form $f(x, y)$. Let again $S = \mathbb{Z} + \mathbb{Z}\tau$, and let $I = \mathbb{Z}\alpha + \mathbb{Z}\beta$ with α, β positively oriented. In analogy with (2.9), we may write

$$\begin{aligned} \alpha^3 &= \delta\,(c_0 + a_0\tau) \\ \alpha^2\beta &= \delta\,(c_1 + a_1\tau) \\ \alpha\beta^2 &= \delta\,(c_2 + a_2\tau) \\ \beta^3 &= \delta\,(c_3 + a_3\tau) \end{aligned} \tag{2.14}$$

for some eight integers a_i and c_i. Then $f(x, y) = a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3$ is our desired binary cubic form.

It is easily verified that changing $< \alpha, \beta >$ to some other basis for I, via an element $T \in SL_2(\mathbb{Z})$, simply changes $f(x, y)$ (via the natural $SL_2(\mathbb{Z})$-action on $\mathrm{Sym}^3\mathbb{Z}^2$) by that same element T. Hence the $SL_2(\mathbb{Z})$-equivalence class of $f(x, y)$ is independent of our choice of basis for I. Conversely, any binary cubic form $SL_2(\mathbb{Z})$-equivalent to $f(x, y)$ can be obtained from (S, I, δ) in the manner described above simply by changing the basis for I appropriately. Finally, it is clear that triples equivalent to (S, I, δ) yield the identical cubic forms $f(x, y)$ under the above map.

It remains to show that this map from the set of equivalence classes of triples (S, I, δ) to the set of equivalence classes of binary cubic forms $f(x, y)$ is in fact a

bijection.

To this end, fix a binary cubic form $f(x, y)$, and consider the system (2.14), which again consists mostly of indeterminates. We show that these indeterminates are essentially determined by the form $f(x, y)$.

First, the ring S is completely determined. To see this, we write out $\alpha, \beta \in S$ in terms of the basis $< 1, \tau >$ of S (with indeterminate coefficients); using the relations (2.14), a calculation shows that

$$\mathrm{Disc}(f) = N(I)^3 N(\delta)^{-1} \cdot \mathrm{Disc}(S).$$

By assumption, $N(\delta) = N(I)^3$, so

$$\mathrm{Disc}(f) = \mathrm{Disc}(S). \tag{2.15}$$

Thus $\mathrm{Disc}(S)$, and hence the ring S itself, is determined by A.

The associativity and commutativity of S implies $(\alpha^2\beta)^2 = \alpha^3 \cdot \alpha\beta^2$ and $(\alpha\beta^2)^2 = \alpha^2\beta \cdot \beta^3$. Expanding these identities out using (2.14), we obtain two linear and two quadratic equations in c_0, c_1, c_2, c_3. Assuming the basis $< \alpha, \beta >$ of I has positive orientation, we find that this system of four equations for the c_i has exactly one solution, given by

$$\begin{aligned} c_0 &= -(2a_1^3 - 3a_0a_1a_2 + a_0^2a_3)/2 \\ c_1 &= -(a_1^2a_2 - 2a_0a_2^2 + a_0a_1a_3)/2 \\ c_2 &= (a_1a_2^2 - 2a_1^2a_3 + a_0a_2a_3)/2 \\ c_3 &= (2a_2^3 - 3a_1a_2a_3 + a_0a_3^2)/2. \end{aligned}$$

(Again, the solutions for the $\{c_i\}$ are necessarily integral.) Thus the c_i's in (2.14) are also uniquely determined by the binary cubic form f.

An examination of the system (2.14) shows that we must have

$$\alpha : \beta = c_1 + a_1\tau : c_2 + a_2\tau \tag{2.16}$$

in S, and hence α, β are uniquely determined up to scalar factors in S. Regardless of how α, β are scaled, this then determines δ uniquely up to the cube of an element in S. Thus we have produced the unique triple up to equivalence that yields the form f under the mapping $(S, I, \delta) \to f(x, y)$.

To see that this object (S, I, δ) is a valid triple in the sense of Theorem 2.9, we must only check that I, currently given as a $\mathbb{Z}$-module, is actually an ideal of S. In fact, one can calculate the module structure of I explicitly in terms of f; it is given by (2.12) or (2.13) in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$, where we set

$$p_1 = b^2 - ac, \quad q_1 = ad - bc, \quad r_1 = c^2 - bd. \tag{2.17}$$

This completes the proof. □

The above discussion gives very precise information about the bijection of Theorem 2.9. Given a triple (S, I, δ), the corresponding cubic form $f(x, y)$ is obtained from equations (2.14). Conversely, given a cubic form $f(x, y) \in \mathrm{Sym}^3\mathbb{Z}^2$, the ring S is determined by (2.15); a basis for the ideal class I is obtained from (2.16), and the S-module structure of I is given by (2.12), (2.13), and (2.17).

Restricting Theorem 2.9 to the set of projective classes of binary cubic forms now yields the following group isomorphism; here, we use $\mathrm{Cl}_3(S(D))$ to denote the group of ideal classes of order dividing 3 in $\mathrm{Cl}(S(D))$.

Theorem 2.10 *Let $S(D)$ denote the quadratic ring of discriminant D. Then there*

is a natural surjective group homomorphism

$$\mathrm{Cl}(\mathrm{Sym}^3\mathbb{Z}^2; D) \to \mathrm{Cl}_3(S(D))$$

which sends a binary cubic form f to the $S(D)$-module I, where $(S(D), I, \delta)$ is a triple corresponding to f as in Theorem 2.9. Moreover, the cardinality of the kernel of this homomorphism is precisely $|U/U^3|$, where U denotes the group of units in the normalization of $S(D)$.

The special case where D corresponds to the ring of integers in a quadratic number field deserves special mention.

Corollary 2.11 *Suppose D is the discriminant of a quadratic number field K. Then there is a natural surjective homomorphism*

$$\mathrm{Cl}(\mathrm{Sym}^3\mathbb{Z}^2; D) \to \mathrm{Cl}_3(K),$$

where $\mathrm{Cl}_3(K)$ denotes the 3-part of the ideal class group of the ring of integers in K. The cardinality of the kernel is equal to

$$\begin{cases} 3 & \text{if } D < 0; \text{ and} \\ 1 & \text{if } D \geq 0. \end{cases}$$

2.2.5 The case of pairs of binary quadratic forms

Just as the case of binary cubic forms was treated by imposing a threefold symmetry on collinear triples (I_1, I_2, I_3) of a quadratic ring S, the case of pairs of binary quadratic forms can be handled by imposing a twofold symmetry. The method of proof is similar; we simply state the result.

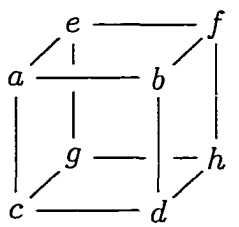
Theorem 2.12 *There is a bijection between the set of $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$-orbits on the space $\mathrm{Sym}^2\mathbb{Z} \otimes \mathbb{Z}^2$, and the set of pairs $(S, (I_1, I_2, I_3))$, where S is a quadratic ring and (I_1, I_2, I_3) is a collinear triple of narrow ideal classes of S such that $I_2 = I_3$.*

The map taking a collinear triple (I_1, I_3, I_3) to the third ideal I_3 corresponds to the isomorphism of groups stated at the end of Section 2.1.5. In particular, the theorem stated for $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$ in Section 2.2.2 holds also for $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D)$ with no other changes.

Appendix: Equivalence of the Cube Law and Gauss composition

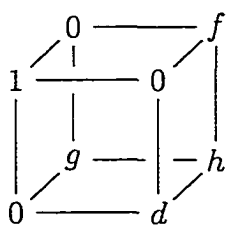
The most elementary way to see the equivalence of the Cube Law and Gauss composition is probably via the definition of Gauss composition due to Dirichlet. In this Appendix, we show how Dirichlet composition can be derived in a very natural and simple manner from the Cube Law.

Suppose we have a projective cube



(2.18)

Since the cube is projective, the greatest common divisors of the entries of the cube is 1. Therefore, by applying elements of $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$, we may obtain an entry "1" in the $(1,1,1)$ position; that is, we may find an equivalent cube with $a = 1$ in (2.18). This "1" entry can then be used to clear out the three adjacent entries in the cube, i.e., we may arrange for $b = c = e = 0$. Thus we see that any projective cube can be transformed by an element of Γ to some cube of the form



(2.19)

Let us write down the three quadratic forms Q_1, Q_2, Q_3 associated to the cube (2.19).

We have

$$\begin{aligned} Q_1 &= -dx^2 + hxy + fgy^2 \\ Q_2 &= -gx^2 + hxy + dfy^2 \\ Q_3 &= -fx^2 + hxy + dgy^2. \end{aligned} \tag{2.20}$$

Now the cube law declares that $[Q_1] + [Q_2] = -[Q_3]$, and therefore

$$[-dx^2 + hxy + fgy^2] + [-gx^2 + hxy + dfy^2] = [dgx^2 + hxy - fy^2].$$

This is precisely Dirichlet composition.

Chapter 3

Cubic composition laws

In this chapter, we develop the cubic analogue of the theory of quadratic composition presented in Chapter 2. Recall that the fundamental object in our treatment of quadratic composition was the $2 \times 2 \times 2$ integer cube, from which all our quadratic composition laws were derived. To proceed with the cubic case, we must first ponder the following question: what are the correct objects on which to define composition laws, so that the resulting groups yield information on the class groups of cubic fields?

Based on our study of the quadratic case in Chapter 2, our first inclination might be to examine $3 \times 3 \times 3$ cubes of integers. A $3 \times 3 \times 3$ cube C can be sliced (in three different ways) into three 3×3 matrices L_i, M_i, N_i $(i = 1, 2, 3)$. We may therefore obtain from C three ternary cubic forms $f_1(x, y, z), f_2(x, y, z), f_3(x, y, z)$ by setting

$$f_i(x, y, z) = -\mathrm{Det}(L_i x + M_i y + N_i z).$$

Again, we may declare a cubic analogue of the "Cube Law" of the previous chapter by demanding that $[f_1] + [f_2] + [f_3] = 0$.

This procedure does in fact yield a law of composition on ternary cubic forms, and gives the desired group structure on the norm forms of ideal classes in cubic rings. The only problem is that it gives us a bit more than we want, for the norm form of

an ideal class in a cubic ring is always a *decomposable form*, i.e., one that decomposes into linear factors over $\bar{\mathbb{Q}}$. On the other hand, our group law arising from $3 \times 3 \times 3$ cubes gives a law of composition not just on decomposable forms, but on general ternary cubic forms. Since our interest in composition laws here is primarily for their connection with class groups, we should like to "slice away" a part of the space of $3 \times 3 \times 3$ cubes somehow so as to extract only the part of the space we are interested in.

How this slicing should occur becomes apparent upon examination of how cubic rings are parametrized. Since cubic rings do not correspond to ternary cubic forms, but rather to binary cubic forms (as was shown by Delone-Faddeev and Gross), this indicates that we should perhaps slice away one layer of the $3 \times 3 \times 3$ cube to retain only a $2 \times 3 \times 3$ box of integers, so that the one $SL(3) \times SL(3)$-invariant is a binary cubic form, while the other two dimensions might then give ideal classes in the associated cubic ring. This is precisely what we determine in the next section.

3.1 On $2 \times 3 \times 3$ boxes of integers

In this section we discover that, just as the basic building blocks for understanding the quadratic case were $2 \times 2 \times 2$ integer cubes, the building blocks in the cubic case are $2 \times 3 \times 3$ integer boxes. As such boxes have a bit less symmetry, there is essentially only one slicing of interest, namely, the one which splits a $2 \times 3 \times 3$ box into two 3×3 submatrices. Hence we shall identify the space $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ of $2 \times 3 \times 3$ integer boxes with the space of pairs (A, B) of 3×3 integer matrices. Note that the group $\bar{\Gamma} = GL_2(\mathbb{Z}) \times GL_3(\mathbb{Z}) \times GL_3(\mathbb{Z})$ then acts in the natural way on the space $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$.

3.1.1 The unique Γ-invariant $\mathrm{Disc}(A, B)$

In studying the orbits of $\bar{\Gamma} = GL_2(\mathbb{Z}) \times GL_3(\mathbb{Z}) \times GL_3(\mathbb{Z})$ on pairs (A, B) of 3×3 matrices, it suffices to restrict the $\bar{\Gamma}$-action to the subgroup $\Gamma = GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$, since $(-I_2, -I_3) \in \bar{\Gamma}$ acts trivially on all pairs (A, B). Moreover, unlike $\bar{\Gamma}$, Γ acts without stabilizer.

Over $\mathbb{C}$, we find that the action of $SL_2(\mathbb{C}) \times SL_3(\mathbb{C}) \times SL_3(\mathbb{C})$ on its 18-dimensional representation $V = \mathbb{C}^2 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ has just a single invariant. This may be seen as follows. First, the action of $SL_3(\mathbb{C}) \times SL_3(\mathbb{C})$ on V has four independent invariants, namely the coefficients of the cubic form $f(x, y) = \mathrm{Det}(Ax - By)$, for it is readily seen that the cubic form f completely specifies the $SL_3(\mathbb{C}) \times SL_3(\mathbb{C})$-orbit of the pair (A, B). Now $SL_2(\mathbb{C})$ acts on the cubic form $f(x, y)$, and it is well-known that the latter action has exactly one invariant, namely the discriminant $\mathrm{Disc}(f)$ of f. Thus the unique $SL_2(\mathbb{C}) \times SL_3(\mathbb{C}) \times SL_3(\mathbb{C})$-invariant on V is given by $\mathrm{Disc}(\mathrm{Det}(Ax - By))$, which we denote simply by $\mathrm{Disc}(A, B)$.

3.1.2 The parametrization of cubic rings

The parametrization of cubic orders by integral binary cubic forms was first discovered by Delone and Faddeev in their famous treatise on cubic irrationalities [12]; this parametrization was refined recently to general cubic rings by Gross [17]. Their construction is as follows. Given a cubic ring R (i.e., any ring free of rank 3 as a $\mathbb{Z}$-module), let $< 1, \omega, \theta >$ be a $\mathbb{Z}$-basis for R. Translating ω, θ by the appropriate elements of $\mathbb{Z}$, we may assume that $\omega \cdot \theta \in \mathbb{Z}$. We call a basis satisfying the latter condition *normalized*, or simply *normal*. If $< 1, \omega, \theta >$ is a normal basis, there exist

constants $a, b, c, d, \ell, m, n \in \mathbb{Z}$ such that

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m + b\omega - a\theta \\ \theta^2 &= \ell + d\omega - c\theta. \end{aligned} \tag{3.1}$$

To the cubic ring R, associate the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Conversely, given a binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, form a potential cubic ring having multiplication laws (3.1). The values of ℓ, m, n are subject to the associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega \cdot \omega\theta$, which when multiplied out using (3.1), yield a system of equations which possess a unique solution for n, m, ℓ, namely

$$\begin{aligned} n &= -ad \\ m &= -ac \\ \ell &= -bd. \end{aligned} \tag{3.2}$$

If follows that any binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, via the recipe (3.1) and (3.2), leads to a unique cubic ring $R = R(f)$.

Lastly, one observes by an explicit calculation that changing the $\mathbb{Z}$-basis $< \omega, \theta >$ of $R/\mathbb{Z}$ by an element of $GL_2(\mathbb{Z})$, and then renormalizing the basis in R, transforms the resulting binary cubic form $f(x, y)$ by that same element of $GL_2(\mathbb{Z})$. Hence an isomorphism class of cubic ring determines a binary cubic form uniquely up to the action of $GL_2(\mathbb{Z})$. It follows that isomorphism classes of cubic rings are parametrized by integral binary cubic forms modulo integer equivalence.

One finds by a further calculation that the discriminant of a cubic ring $R(f)$ is precisely the discriminant of the binary cubic form f. We summarize this discussion as follows:

Theorem 3.1 ([12],[17]) *There is a one-to-one correspondence between the set of equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings, by the association*

$$f \leftrightarrow R(f).$$

Moreover, $\mathrm{Disc}(f) = \mathrm{Disc}(R(f))$.

3.1.3 Cubic rings and $2 \times 3 \times 3$ boxes of integers

In this section we determine as promised the Γ-orbits on $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ in terms of ideal classes of cubic rings. Before stating the result, we make a definition. Let us say two ideals I, I' in a cubic ring R are *weakly inverse* in R if there exists an element $\delta \in R$ such that $II' \subseteq (\delta)$ and $N(I)N(I') = N(\delta)$. (If R is a Dedekind domain, the notion of "weakly inverse" coincides with the usual notion of "inverse".)

Theorem 3.2 *There is a bijection, to be given below, between the set of Γ-orbits on the space $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$, and the set of pairs $(R, (I, I'))$, where R is a cubic ring, and (I, I') is a pair of weakly inverse ideals in R.*

Proof: Given ideals I and I' of a cubic ring R with $N(I)N(I') = N(\delta)$ and $II' \subseteq (\delta)$, we first show how to construct a corresponding pair (A, B) of 3×3 integer matrices. Let $< 1, \omega, \theta >$ denote a normal basis of R, and let $< \alpha_1, \alpha_2, \alpha_3 >$ and $< \beta_1, \beta_2, \beta_3 >$ denote $\mathbb{Z}$-bases for the ideals I and I' having the same orientation as $< 1, \omega, \theta >$. Then since $II' \subseteq (\delta)$, we must have

$$\begin{aligned} \alpha_1\beta_1 &= \delta\,(c_{11} + b_{11}\omega + a_{11}\theta\,) \\ \alpha_1\beta_2 &= \delta\,(c_{12} + b_{12}\omega + a_{12}\theta\,) \\ &\vdots \\ \alpha_3\beta_3 &= \delta\,(c_{33} + b_{33}\omega + a_{33}\theta\,) \end{aligned} \tag{3.3}$$

for some set of twenty-seven integers a_{ij}, b_{ij}, and c_{ij} $(1 \leq i \leq j \leq 3)$. Let A and B denote the 3×3 matrices (a_{ij}) and (b_{ij}) respectively. Then $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ is our desired pair of 3×3 matrices.

By construction, it is clear that changing $< \alpha_1, \alpha_2, \alpha_3 >$ and $< \beta_1, \beta_2, \beta_3 >$ to some other bases of I and I', via an element $T \in SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$, would simply transform (A, B) by that same element T. Similarly, a change of the basis $< 1, \omega, \theta >$ to another normal basis $< 1, \omega', \theta' >$ of R is completely determined by the element $\begin{pmatrix} r & s \\ u & v \end{pmatrix} \in SL_2(\mathbb{Z})$, where

$$\begin{aligned} \omega' &= q + r\omega + s\theta \\ \theta' &= t + u\omega + v\theta. \end{aligned}$$

Again, it is easily checked that this change of basis transforms (A, B) by the same element $\begin{pmatrix} r & s \\ u & v \end{pmatrix} \in SL_2(\mathbb{Z})$. Along the same lines, if δ is replaced in (3.3) by some other generator $u\delta$ of the ideal (δ), where u is a unit of positive norm, then this simply transforms (A, B) by $T_u \in SL_3(\mathbb{Z})$ (or, equivalently, by $T'_u \in SL_3(\mathbb{Z})$), where T_u (resp. T'_u) denotes the multiplication-by-u operator on $I =< \alpha_1, \alpha_2, \alpha_3 >$ (resp. on $I' =< \beta_1, \beta_2, \beta_3 >$). We conclude that the Γ-equivalence class of (A, B) is independent of our initial choice of bases for R, I, and I', and of our choice of δ. Conversely, any pair of 3×3 matrices in the same Γ-orbit as (A, B) can actually be obtained from (R, I, I') in the manner described above, simply by changing the bases for R, I, and I' appropriately.

Next, suppose J and J' are ideals of R such that I, J and I', J' correspond to the same ideal classes. Then there exists a nonzero element κ in the ring of quotients of R such that $J = \kappa I$ and $J' = \kappa' I'$. If we choose bases for I, I', J, J' to take the form $< \alpha_1, \alpha_2, \alpha_3 >$, $< \beta_1, \beta_2, \beta_3 >$, $< \kappa\alpha_1, \kappa\alpha_2, \kappa\alpha_3 >$, and $< \kappa'\beta_1, \kappa'\beta_2, \kappa'\beta_3 >$ respectively, it is immediate from (3.3) that (R, I, I') and (R, J, J') (where δ is then

replaced by $\kappa\kappa'\delta$) will give rise to identical elements (A, B) in $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$. It follows that the association $(R, I, I') \to (A, B)$ is a well-defined map even on the level of ideal classes.

It remains to show that our mapping $(R, (I, I')) \to (A, B)$ from the set of pairs $(R, (I, I'))$ to the space $(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3)/\Gamma$ is in fact a bijection.

To this end, fix 3×3 symmetric matrices $A = (a_{ij})$ and $B = (b_{ij})$, and consider the system (3.3), which at this point consists almost entirely of indeterminates. Contrary to how it might look, we show in several steps that these indeterminates are in fact essentially determined by the pair (A, B).

First, we claim that the ring structure of R is completely determined. Indeed, let us write

$$\begin{aligned} \omega\theta &= -ad \\ \omega^2 &= -ac + b\omega - a\theta \\ \theta^2 &= -bd + d\omega - c\theta, \end{aligned} \tag{3.4}$$

and let f be the corresponding binary cubic form given by

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Writing out the seven elements $\alpha_i, \beta_j, \delta \in R$ in terms of the basis $1, \omega, \theta$ of R (with indeterminate coefficients), and using the relations (3.3), a rather large but beautiful calculation (best suppressed here) shows that

$$\mathrm{Det}(Ax - By) = N(I)N(I')N(\delta)^{-1} \cdot (ax^3 + bx^2y + cxy^2 + dy^3). \tag{3.5}$$

But by assumption, $N(I)N(I') = N(\delta)$, so

$$\mathrm{Det}(Ax - By) = f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3, \tag{3.6}$$

and therefore the ring $R = R(f)$ is indeed determined.

Next, we show that the quantities c_{ij} in (3.3) are also completely determined. By the associative law in R, we have nine equations of the form

$$(\alpha_i\beta_j)(\alpha_{i'}\beta_{j'}) = (\alpha_i\beta_{j'})(\alpha_{i'}\beta_j), \tag{3.7}$$

for $1 \le i, i', j, j' \le 3$. Expanding these out using (3.3), (3.4), and (3.6), and then equating the coefficients of 1, ω, and θ, yields a system of 18 linear and 9 quadratic (!) equations in the 9 indeterminates c_{ij}. Although it seems that this system may be a bit overdetermined, we find (by another large calculation) that it has exactly one (quite pretty) solution, given by

$$\begin{aligned} c_{11} \;=\; & \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{13} \\ b_{31} & b_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix} \\ & - \begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{13} \\ b_{21} & b_{23} \end{vmatrix} - \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} \\ b_{31} & b_{32} \end{vmatrix}, \end{aligned} \tag{3.8}$$

where the values of the other c_{ij} are symmetrically obtained. (Note that the solutions for the $\{c_{ij}\}$ are necessarily integral, since they are polynomials in the a_{ij} and b_{ij}!) Thus the c_{ij}'s are also uniquely determined by the pair of matrices (A, B).

We still must determine the existence of $\alpha_i, \beta_j, \delta \in R$ yielding the desired a_{ij}, b_{ij}, and c_{ij}'s in (3.3). An examination of this system (3.3) shows that we must have, for any $1 \le j \le 3$,

$$\alpha_1 : \alpha_2 : \alpha_3 = c_{1j} + b_{1j}\omega + a_{1j}\theta : c_{2j} + b_{2j}\omega + a_{2j}\theta : c_{3j} + b_{3j}\omega + a_{3j}\theta \;; \tag{3.9}$$

that the ratio on the right hand side of (3.9) is independent of the choice of j follows from the identities (3.7) that we have forced on the system (3.3). Thus the triple

$(\alpha_1, \alpha_2, \alpha_3)$ is uniquely determined up to factors in R. Similarly, the triple $(\beta_1, \beta_2, \beta_3)$ is so determined. Regardless of how $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ are scaled, this then determines δ uniquely up to a unit of positive norm in R.

To see that this object $(R, (I, I'))$ forms a valid pair in the sense of Theorem 3.2, we must only check that I and I', currently given only as $\mathbb{Z}$-modules, actually form ideals of R. In fact, one can calculate the exact R-module structures of I' and I explicitly in terms of (A, B), which are too beautiful to be left unmentioned. Given a matrix M, let us use M^i to denote the ith column of M and $|M|$ denote the determinant of M. Then the R-module structure of I' is given by

$$\begin{aligned}
-\omega \cdot \alpha_1 &= |B^1\ A^2\ A^3| \cdot \alpha_1 + |A^1\ B^1\ A^3| \cdot \alpha_2 + |A^1\ A^2\ B^1| \cdot \alpha_3 \\
-\omega \cdot \alpha_2 &= |B^2\ A^2\ A^3| \cdot \alpha_1 + |A^1\ B^2\ A^3| \cdot \alpha_2 + |A^1\ A^2\ B^2| \cdot \alpha_3 \\
-\omega \cdot \alpha_3 &= |B^3\ A^2\ A^3| \cdot \alpha_1 + |A^1\ B^3\ A^3| \cdot \alpha_2 + |A^1\ A^2\ B^3| \cdot \alpha_3 \\
-\theta \cdot \alpha_1 &= |A^1\ B^2\ B^3| \cdot \alpha_1 + |B^1\ A^1\ B^3| \cdot \alpha_2 + |B^1\ B^2\ A^1| \cdot \alpha_3 \\
-\theta \cdot \alpha_2 &= |A^2\ B^2\ B^3| \cdot \alpha_1 + |B^1\ A^2\ B^3| \cdot \alpha_2 + |B^1\ B^2\ A^2| \cdot \alpha_3 \\
-\theta \cdot \alpha_3 &= |A^3\ B^2\ B^3| \cdot \alpha_1 + |B^1\ A^3\ B^3| \cdot \alpha_2 + |B^1\ B^2\ A^3| \cdot \alpha_3,
\end{aligned} \tag{3.10}$$

where the R-module structure of I is given analogously in terms of the rows of A and B rather than the columns. This concludes the proof of Theorem 3.2. □

Note that our discussion makes the bijection of Theorem 3.2 very precise. Given a cubic order R and a weakly inverse pair (I, I') of ideals in R, the corresponding element $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ is obtained from equations (3.3). Conversely, given an element $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$, the ring R is determined by (3.4) and (3.6); bases for the ideal classes I and I' of R may be obtained from (3.9), and the R-module structures of I and I' are given by (3.10). Finally, we note that equation (3.6) implies that if (A, B) corresponds to $(R, (I, I'))$, then $\mathrm{Disc}(A, B) = \mathrm{Disc}(R)$; thus the bijection of Theorem 3.2 preserves discriminants.

3.1.4 Cubic rings and pairs of ternary quadratic forms

Just as we were able to put a symmetry condition on $2 \times 2 \times 2$ matrices to obtain information on the 3-parts of class groups of quadratic rings, we can impose a symmetry condition on $2 \times 3 \times 3$ matrices to obtain information on the 2-parts of class groups of cubic rings. The "symmetric" elements in $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ are precisely the elements of $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$, i.e., pairs (A, B) of symmetric 3×3 integer matrices, which may be viewed as pairs (A, B) of integral ternary quadratic forms. The group $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ acts in the natural way on $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$, and the precise correspondence between pairs of ternary quadratic forms and ideal classes "of order 2" in cubic rings is given by the following theorem.

Theorem 3.3 *There is a bijection, to be given below, between the set of $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$-orbits on the space $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$, and the set of equivalence classes of triples (R, I, δ), where R is a cubic ring, I is an ideal of R, and δ is an element of I^2 such that $N(\delta) = N(I)^2$. (Here two triples (R, I, δ) and (R, I', δ') are equivalent if there exists a nonzero element κ in the ring of quotients of R such that $I' = \kappa I$ and $\delta' = \kappa^2\delta$.)*

Proof: For a triple (R, I, δ) as above, we first show how to construct a corresponding pair (A, B) of ternary quadratic forms. Let $< 1, \omega, \theta >$ denote a normal basis of R, and let $< \alpha_1, \alpha_2, \alpha_3 >$ denote a $\mathbb{Z}$-basis of the ideal I having the same orientation as $< 1, \omega, \theta >$. Since by hypothesis I is an ideal whose square contains the element $\delta \in R$, we must have

$$\alpha_i\alpha_j = \delta\,(\,c_{ij} + b_{ij}\omega + a_{ij}\theta\,) \tag{3.11}$$

for some set of integers a_{ij}, b_{ij}, and c_{ij}. Let A and B denote the 3×3 symmetric matrices (a_{ij}) and (b_{ij}) respectively. Then the ordered pair $(A, B) \in V(\mathbb{Z})$ is our desired pair of ternary quadratic forms.

The matrices A and B can naturally be viewed as quadratic forms on the lattice $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$. Hence changing $< \alpha_1, \alpha_2, \alpha_3 >$ to some other basis of I, via an element $T \in SL_3(\mathbb{Z})$, would simply transform (A, B) (via the natural $SL_3(\mathbb{Z})$-action) by that same element T. Also, just as in Theorem 3.2, a change of the basis $< 1, \omega, \theta >$ to another normal basis by an element of $GL_2(\mathbb{Z})$ transforms (A, B) by that same element. We conclude that our map from equivalence classes of triples (R, I, δ) to equivalence classes of pairs (A, B) of ternary quadratic forms is well-defined.

To show that this map is a bijection, we fix the pair $A = (a_{ij})$ and $B = (b_{ij})$ of ternary quadratic forms, and then show that these values determine all the indeterminates in the system (3.11). First, to show that the ring R is determined, we assume (3.4), and derive from (3.11) the identity

$$\begin{aligned} \mathrm{Det}(Ax - By) &= N(I)^2 N(\delta)^{-1}(ax^3 + bx^2y + cxy^2 + dy^3) \\ &= ax^3 + bx^2y + cxy^2 + dy^3, \end{aligned} \tag{3.12}$$

where we have used the hypothesis that $N(\delta) = N(I)^2$. It follows, as in the proof of Theorem 3.2, that the ring R is determined by the pair (A, B).

Next we use the associative law in R to show that the constants c_{ij} in the system (3.11) are uniquely determined. We have three identities of the form $(\delta^{-1}\alpha_1^2)(\delta^{-1}\alpha_2^2) = (\delta^{-1}\alpha_1\alpha_2)^2$, and three more of the form $(\delta^{-1}\alpha_1^2)(\delta^{-1}\alpha_2\alpha_3) = (\delta^{-1}\alpha_1\alpha_2)(\delta^{-1}\alpha_1\alpha_3)$. Expanding out all six of these using (3.4) and (3.11), and then equating the coefficients of 1, ω, and θ, yields a system of 18 linear and quadratic equations in the six indeterminates $c_{11}, c_{22}, c_{33}, c_{12}, c_{13}, c_{23}$. This system in the c_{ij} has a unique solution, given again by (3.8), with symmetrically obtained solutions for the other c_{ij}.

An examination of the system (3.11) shows that we must have, for any $1 \leq j \leq 3$,

$$\alpha_1 : \alpha_2 : \alpha_3 = c_{1j} + b_{1j}\omega + a_{1j}\theta : c_{2j} + b_{2j}\omega + a_{2j}\theta : c_{3j} + b_{3j}\omega + a_{3j}\theta\ , \tag{3.13}$$

and the latter ratio is independent of the choice of j. Thus the triple $(\alpha_1, \alpha_2, \alpha_3)$ is uniquely determined up to factors in R. Regardless of how the triple $(\alpha_1, \alpha_2, \alpha_3)$ is scaled, this then determines δ uniquely up to a square factor in R. Thus we have produced the unique triple, up to equivalence, that yields the form f under the mapping $(R, I, \delta) \to (A, B)$.

To see that this object (R, I, δ) is really a valid triple in the sense of Theorem 3.3, we must only check that I is an ideal of R. Again, the R-module structure of I can be determined explicitly in terms of (A, B), and is given by (3.10). This completes the proof of Theorem 3.3. □

The proof gives very precise information about the bijection of Theorem 3.3. Given a triple (R, I, δ), the corresponding pair (A, B) of ternary quadratic forms is obtained from equations (3.11). Conversely, given an element $(A, B) \in \mathrm{Sym}^3\mathbb{Z}^2 \otimes \mathbb{Z}^2$, the ring R is determined by (3.4) and (3.12); a basis for the ideal class I may be obtained from (3.13), and the R-module structure of I is given by (3.10). We should point out again that by (3.12), if (A, B) corresponds to (R, I, δ), then $\mathrm{Disc}(A, B) = \mathrm{Disc}(R)$; that is, the correspondence of Theorem 3.3 is discriminant-preserving.

3.2 Resulting composition laws

In this section, we describe natural composition laws on $2 \times 3 \times 3$ boxes of integers and on pairs of integral ternary quadratic forms. These composition laws may be viewed as cubic analogues of the composition laws presented in Chapter 2.

3.2.1 Composition of $2 \times 3 \times 3$ integer matrices

Define a pair of ternary quadratic forms $(A, B) \in (\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3)/\Gamma$ to be *projective* if in the corresponding pair $(R, (I, I'))$ (as in Section 3.1), the ideals I and I' are projective as R-modules. For a given binary cubic form f, let $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$ denote the set of

all elements $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ such that $\mathrm{Det}(Ax - By)$ is $GL_2(\mathbb{Z})$-equivalent to $f(x, y)$.

The purpose of this section is to note that, for a given cubic form f, there is a natural group law on the set of projective elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)/\Gamma$. This law of composition is most easily defined as follows. Let (A, B) and (A', B') be any two elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)/\Gamma$, and let $(R, (I_1, I_2))$ and $(R, (I_1', I_2'))$ be the corresponding pairs as constructed in Section 3.1 (here R can be chosen to be the same in both pairs, since they correspond to equivalent cubic forms). Define then the composition of (A, B) and (A', B') to be the pair (A'', B'') of ternary quadratic forms corresponding to the pair $(R, (I_1 I_1', I_2 I_2'))$. It is not hard to see that this does in fact yield a group law on the desired set. We denote the resulting group by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f)$.

If $R(f)$ denotes the cubic ring corresponding to a cubic form f, then the group $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f)$ is closely related to the ideal class group $\mathrm{Cl}(R(f))$ of $R(f)$. To be precise,

Theorem 3.4 *There is a natural group isomorphism*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f) \leftrightarrow \mathrm{Cl}(R(f)),$$

which sends an element $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$ to the ideal class I in the cubic ring $R(f)$, where $(R(f), (I, I'))$ is the pair corresponding to (A, B) as in Theorem 3.2.

The whole situation may thus be viewed as a cubic analogue of Gauss's theory of composition for binary quadratic forms and its relation to ideal classes of quadratic

orders. Indeed, the analogy is quite strong:

- In the case of binary quadratic forms, the unique $SL(2)$-invariant is the discriminant D, which classifies orders in quadratic fields. The primitive classes having a fixed value of D form a group under a certain natural composition law. This group is naturally isomophic to the narrow class group of the corresponding quadratic order.

- In the case of $2 \times 3 \times 3$ integer boxes, the unique $SL(3) \times SL(3)$-invariant is the cubic form f, which classifies orders in cubic fields. The projective classes having a fixed value of f form a group under a certain natural composition law. This group is naturally isomorphic to the ideal class group of the corresponding cubic order.

If $f(x,y) = ax^3+bx^2y+cxy^2+dy^3$ is a given cubic form, then the identity element of $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f)$ (i.e., the *principal class*) is given by

$$\left(\begin{bmatrix} & & 1 \\ & -a & \\ 1 & & -c \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & b & \\ & & d \end{bmatrix} \right),$$

as may be seen from the multiplication laws for R as given by (3.4). It is interesting to check that indeed $\mathrm{Det}(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3$ for this pair (A, B).

3.2.2 Composition of pairs of ternary quadratic forms

We may restrict the group law on pairs of 3×3 matrices defined in the previous section to symmetric pairs (A, B) of 3×3 matrices, i.e., pairs (A, B) of ternary quadratic forms. Again, this set is easily verified to be preserved under the group law. We denote the resulting groups by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f)$, where f denotes again the binary cubic form invariant.

As in the quadratic case, we find that the restriction to symmetric classes isolates a certain arithmetic part of the ideal class group of the corresponding order. In the current case, if $R(f)$ is the cubic ring corresponding to the cubic form f, then there is a natural map from $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f)$ onto the 2-class group $\mathrm{Cl}_2(R)$ of R. To be more precise,

Theorem 3.5 *There is a natural surjective group homomorphism*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f) \to \mathrm{Cl}_2(R),$$

which takes a pair (A, B) of ternary quadratic forms to the R-module I; here (R, I, δ) is a triple corresponding to (A, B) as in Theorem 3.3. Moreover, the cardinality of the kernel of this homomorphism is precisely $|U/\{U^2, \pm 1\}|$, where U denotes the group of units of R.

The special case where f corresponds to the ring of integers in a number field deserves special mention.

Corollary 3.6 *Suppose f corresponds to the ring of integers in a cubic field K. Then there is a natural surjective homomorphism*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f) \to \mathrm{Cl}_2(K),$$

where $\mathrm{Cl}_2(K)$ denotes the 2-class group of the ring of integers R in K. The cardinality of the kernel is equal to 2 if $R \otimes \mathbb{R} \cong \mathbb{R} \oplus \mathbb{C}$, and is equal to 4 if $R \otimes \mathbb{R} \cong \mathbb{R}^3$.

Chapter 4

The parametrization of quartic rings

The parametrizations of quadratic and cubic orders presented in Sections 2.2.1 and 3.1.2 are at once both beautiful and simple, and have enjoyed numerous applications both within this thesis and elsewhere (see e.g., [11], [12], [13], [17], [20]). It is therefore only natural to ask whether analogous parametrizations might exist for orders in number fields of degree $k > 3$. In this chapter, we show how such a parametrization can also be achieved for quartic orders (i.e., the case $k = 4$).

In classifying quartic rings, the first approach (as in the cases $k = 2$ and $k = 3$) might be simply to write out the multiplication laws for a rank 4 ring in terms of an explicit basis, and examine the transformation properties of the structure coefficients under change of basis. However, since the jump in complexity from $k = 3$ to $k = 4$ is so large, this idea goes astray very quickly (yielding a huge mess!), and it becomes necessary to have a new perspective in order to make any further progress.

In Section 4.1, we give such a new perspective on the case $k = 3$ in terms of what we call *resolvent rings*. The notion of quadratic resolvent ring, defined in 4.1.2, immediately yields the Delone-Faddeev parametrization of cubic orders from a purely

ring-theoretic viewpoint. Generalizing this notion to $k = 4$ then indicates that the analogous objects parametrizing quartic orders should be pairs of ternary quadratic forms.

Section 4.2 is dedicated to proving this assertion. The proof is accomplished in several steps, and the main result on parametrization is achieved in Subsection 4.2.5. In the five remaining subsections of Section 4.2, we investigate how cubic resolvents, maximality and splitting of primes manifest themselves in terms of pairs of ternary quadratic forms; this may have future computational applications, and will also be important to us in Chapter 5 in obtaining results on the density of discriminants of quartic fields.

4.1 Resolvent rings and parametrizations

Before introducing the notion of resolvent ring, it is necessary first to understand the notion of "Galois closure" (specifically, "S_k-closure") at the level of rings, which we turn to first.

4.1.1 The S_k-closure of a ring of rank k

Let R be any ring of rank k (i.e., any ring having rank k when viewed as a $\mathbb{Z}$-module), and let $\mathrm{Tr}(\cdot)$ denote the trace form on R. Let $R^{\otimes k}$ denote the kth tensor power

$$R^{\otimes k} = R \otimes_{\mathbf{Z}} R \otimes_{\mathbf{Z}} \cdots \otimes_{\mathbf{Z}} R$$

of R, and let I_R denote the ideal in $R^{\otimes k}$ generated by all elements in $R^{\otimes k}$ of the form

$$(x \otimes 1 \otimes \cdots \otimes 1) + (1 \otimes x \otimes \cdots \otimes 1) + \cdots + (1 \otimes 1 \otimes \cdots \otimes x) - \mathrm{Tr}(x)(1 \otimes 1 \otimes \cdots \otimes 1)$$

for $x \in R$.

Definition 4.1 *The S_k-closure $\bar{R}$ of a ring R of rank k is the ring extension $\bar{R}$ of R given by $R^{\otimes k}/I_R$.*

The notion of S_k-closure is precisely the analogue of "Galois closure" we seek. We may write $\mathrm{Gal}(\bar{R}/R) = S_k$, since the symmetric group S_k acts naturally as a group of automorphisms on $\bar{R}$; furthermore, it is clear that $\bar{R}^{S_k}$, the subring invariant under this action, is simply $\mathbb{Z} \otimes \mathbb{Z} \otimes \cdots \otimes \mathbb{Z} \cong \mathbb{Z}$.

For example, if R is an order in an number field K of degree k such that $\mathrm{Gal}(K/\mathbb{Q}) = S_k$, then $\bar{R}$ is simply the $\mathbb{Z}$-algebra generated by all the Galois conjugates of elements of R, i.e.,

$$\bar{R} = \mathbb{Z}[\{\alpha : \alpha \ S_k\text{-conjugate to some element of } R\}].$$

The S_k-closure may similarly be described for any ring of rank k having nonzero discriminant. If R has nonzero discriminant, then $K = R \otimes \mathbb{Q}$ is étale over $\mathbb{Q}$ and hence is the direct sum $\oplus K_i$ of algebraic number fields. Let G_i denote the Galois group of K_i over $\mathbb{Q}$; then $G = \prod G_i$ may be viewed as a group of automorphisms of K over $\mathbb{Q}$ in the natural way. Let $\tilde{R}$ denote the ring in K generated by all G-conjugates of elements of R in K, i.e., let

$$\tilde{R} = \mathbb{Z}[\{\alpha : \alpha \ G\text{-conjugate to some element of } R\}],$$

and finally set $\bar{R}$ to be the direct sum of $k!/|G|$ copies of $\tilde{R}$. Then $\bar{R}$ is clearly a ring of rank $k!$, and it is the S_k-closure of R.

To fix notation, we always assume a fixed embedding of R into $\bar{R}$. In the next two sections, we use the notion of S_k-closure to attach rings of lower rank to orders in cubic and quartic fields.

4.1.2 The quadratic resolvent of a cubic ring

Given a cubic ring, there is a natural way to associate to R a quadratic ring S, namely the unique quadratic ring S having the same discriminant as R. Since the discriminant $D = \mathrm{Disc}(R)$ of R is necessarily congruent to 0 or 1 modulo 4, the quadratic ring $S(D)$ of discriminant D always exists; we call $S = S(D)$ the *quadratic resolvent ring* of R.

Definition 4.2 For a cubic ring R, the *quadratic resolvent* of R is the unique quadratic ring S such that $\mathrm{Disc}(R) = \mathrm{Disc}(S)$.

Given a cubic ring R, there is a natural map from R to its quadratic resolvent ring S that preserves discriminants. Indeed, for an element $x \in R$, let x, x', x'' denote the S_3-conjugates of x in a fixed S_3-closure $\bar{R}$ of R. Then the element

$$\phi_{3,2}(x) = \frac{[(x-x')(x'-x'')(x''-x)]^2 + (x-x')(x'-x'')(x''-x)}{2} \tag{4.1}$$

is contained in some quadratic ring, and it has the same discriminant as x. In fact, all the elements $\phi_{3,2}(x)$ may be viewed as lying in a single ring $S^{\mathrm{inv}}(R)$ naturally associated to R, namely the quadratic subring of $\bar{R} \otimes \mathbb{Q}$ defined by

$$S^{inv}(R) = \mathbb{Z}[\{\phi_{3,2}(x) : x \in R\}]. \tag{4.2}$$

This ring is quadratic since it is fixed under the natural action of the alternating group on the rank 6 ring $\bar{R} \otimes \mathbb{Q}$. We call $S^{inv}(R)$ the *quadratic invariant ring* of R.

How is $S^{inv}(R)$ related to the quadratic resolvent ring $S = S^{res}(R)$? To answer this question, we observe that forming $\phi_{3,2}(x)$ for $x \in R$ involves taking a square root of the discriminant of x in $\bar{R}$. Since $\mathrm{Disc}(x)$ is equal to $r^2\mathrm{Disc}(R)$ for some integer r, $\phi_{3,2}(x)$ is naturally an element of the quadratic resolvent S for all $x \in R$, so that $S^{inv}(R)$ is naturally a subring of S. In particular, the map $\phi_{3,2} : R \to S^{inv}(R)$ may

also be viewed as a (discriminant-preserving) map

$$\phi_{3,2} : R \to S. \tag{4.3}$$

When does $S^{inv}(R) = S$? As we shall prove in the next chapter, the answer is that $S^{inv}(R) = S$ precisely when R is Gorenstein. Thus for most nice cubic rings R, $S^{inv}(R) = S$.

Let us now examine the implication of our construction for the parametrization of cubic rings. Suppose R is a cubic ring and S is the quadratic resolvent ring of R, and let $\phi_{3,2} : R \to S$ be the natural map given by (4.1). Then observe that $\phi_{3,2}(x) = \phi(x + c)$ for any $c \in \mathbb{Z}$; hence $\phi_{3,2} : R \to S$ actually descends to a map

$$\bar{\phi}_{3,2} : R/\mathbb{Z} \to S/\mathbb{Z}. \tag{4.4}$$

As a map of $\mathbb{Z}$-modules, $\bar{\phi}_{3,2}$ is a cubic map from $\mathbb{Z}^2$ to $\mathbb{Z}$, and thus corresponds to an integral binary cubic form, well-defined up to $GL_2(\mathbb{Z}) \times GL_1(\mathbb{Z})$-equivalence.

To produce explicitly a binary cubic form corresponding to the cubic ring R as above, we compute the discriminant of $x\omega + y\theta \in R$, where R is spanned by $< 1, \omega, \theta >$ and multiplication is defined by (3.1). An explicit calculation shows that

$$\mathrm{Disc}(x\omega + y\theta) = D\,(ax^3 + bx^2y + cxy^2 + dy^3)^2.$$

Since $S/\mathbb{Z}$ is generated by $(D + \sqrt{D})/2$, it is clear that the binary cubic form corresponding to the map $\bar{\phi}_{3,2}$ is given by

$$\frac{\sqrt{\mathrm{Disc}(x\omega + y\theta)}/2}{\sqrt{D}/2} = ax^3 + bx^2y + cxy^2 + dy^3.$$

Thus we have obtained a concrete ring-theoretic interpretation of the Delone-Faddeev-Gross parametrization of cubic rings.

4.1.3 Cubic resolvents of a quartic ring

Let Q be a *quartic ring*, i.e., any ring of rank 4 over $\mathbb{Z}$. Developing the quartic analogue of the work of the previous section is the key to determining what the corresponding parametrization of quartic rings should be. To accomplish this task, we must in particular determine the correct notions of a cubic resolvent ring R of Q, a cubic invariant ring $R^{inv}(Q)$ of Q, and a map

$$\phi_{4,3} : Q \to R.$$

As it turns out, the notion of what the cubic resolvent ring R should be is not quite as immediate and clear cut as was the concept of quadratic resolvent ring in the cubic case. Thus, we turn first to the map $\phi_{4,3}$ and to the cubic invariant ring $R^{inv}(Q)$, which are easier to define.

In analogy with the cubic case of the previous section, we should like $\phi_{4,3}$ to be a polynomial function that associates to any x in a quartic ring a natural element of the same discriminant in a cubic ring. Such a map does indeed exist: if $\bar{Q}$ denotes the S_4-closure of Q, and x, x', x'', x''' denote the conjugates of x in $\bar{Q}$, then define $\phi_{4,3}(x)$ by the following well-known expression:

$$\phi_{4,3}(x) = xx' + x''x'''. \tag{4.5}$$

It is known from the classical theory of solving the quartic that $\phi_{4,3}$ is discriminant-preserving; it is also clear that $\phi_{4,3}(x)$ lies in a cubic ring, having exactly three S_4-conjugates in $\bar{Q}$. In fact, all elements $\phi_{4,3}(x)$ for $x \in Q$ are seen to lie in a single cubic ring, namely, the cubic subring of $\bar{R}$ fixed under the action of a fixed dihedral

subgroup $D_4 \subset S_4$ of order 8. Following the example of the previous section, define

$$R^{inv}(Q) = \mathbb{Z}[\{\phi_{4,3}(x) : x \in Q\}]. \tag{4.6}$$

We call $R^{inv}(Q)$ the *cubic invariant ring* of Q. Thus we have a natural, discriminant-preserving map

$$\phi_{4,3} : Q \to R^{inv}(Q).$$

Let us return to the notion of cubic resolvent of Q. In analogy again with the cubic-quadratic case, we should like to define the cubic resolvent of Q to be a cubic ring R that has the same discriminant as Q and that contains $R^{inv}(Q)$. However, there may actually be many such rings, and no single one naturally lends itself to being distinguished from the others. Thus we ought to allow any such ring to be called a cubic resolvent ring of Q.

Definition 4.3 Let Q be a quartic ring, and $R^{inv}(Q)$ its cubic invariant ring. A *cubic resolvent ring* of Q is a cubic ring R such that $\mathrm{Disc}(Q) = \mathrm{Disc}(R)$ and $R \supset R^{inv}(Q)$.

In the next section we will see that all quartic rings have at least one cubic resolvent, and moreover, for Gorenstein quartic rings the cubic resolvent is in fact unique. Thus cubic resolvents exist, and given any cubic resolvent R of Q, we may then of course speak of the natural map

$$\phi_{4,3} : Q \to R.$$

Following the cubic case, let us see what implications our construction of cubic resolvents has for the parametrization of quartic rings. Suppose Q is a quartic ring, R is its cubic resolvent ring, and $\phi_{4,3} : Q \to R$ is the natural map as defined by (4.5).

Then observe that for any $c \in \mathbb{Z}$,

$$\phi_{4,3}(x+c) = (x+c)(x'+c) + (x''+c)(x'''+c) = \phi(x) + d$$

for some $d \in \mathbb{Z}$, namely $d = c\,\mathrm{Tr}(x) + 2c^2$. Hence $\phi_{4,3} : Q \to R$ descends naturally to a map

$$\bar{\phi}_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}. \tag{4.7}$$

As a map between $\mathbb{Z}$-modules, this map is a quadratic map from $\mathbb{Z}^3$ to $\mathbb{Z}^2$, and thus corresponds to a pair of integral ternary quadratic forms, well-defined up to $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$-equivalence.

As the reader will have noticed, the analogy with the cubic case up to this point is very remarkable, and if it is to continue, it suggests that *isomorphism classes of quartic rings should be parametrized roughly by pairs of integral ternary quadratic forms, up to integer equivalence.*

On the other hand, proving the latter statement, or even just determining the pair of ternary quadratic forms attached to a given quartic ring Q, is not quite as easy as the corresponding calculation was in the cubic case. The difference lies in the fact that, in the case of cubic rings, one could completely describe the quadratic resolvent ring, so $\bar{\phi}_{3,2}$ could also be described explicitly. For quartic rings, however, it is difficult to say anything a priori about the cubic resolvent ring other than that it is a ring of rank 3 and certain discriminant D; more structural information is not forthcoming without some additional work, which we carry out in Section 4.2.

4.2 Quartic rings and pairs of ternary quadratic forms

Given a quartic ring Q, and a cubic resolvent R of Q, we have shown that there is a pair of integral ternary quadratic forms (A, B) associated to (Q, R), determined by the natural map

$$\bar{\phi}_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}. \tag{4.8}$$

However, even when we are given explicitly a pair of rings (Q, R), it is not immediate how to produce explicitly the pair (A, B) of integral ternary quadratic forms corresponding to (Q, R). Hence our strategy in this chapter is to work the other way around: given a pair (A, B) of integral ternary quadratic forms, we determine the possible structures that the rings Q and R can have.

It is necessary first to understand some of the basic invariant theory of pairs of ternary quadratic forms. This is summarized briefly in Section 4.2.1. In Sections 4.2.1-4.2.4, we gather structural information on the rings Q and R, using only the data (A, B) corresponding to the map (4.8). In Section 4.2.5, we present our main theorem on the parametrization of quartic rings and their cubic resolvents. In Section 4.2.6–4.2.7, we study an invariant of rank k rings that we call the *content*, and show that the content of a quartic ring Q is related in a precise way to the number of cubic resolvents of Q. Finally, in Sections 4.2.8–4.2.10, we use this notion of content to determine the precise relationship between quartic rings and pairs of integral ternary quadratic forms.

4.2.1 The fundamental invariant $\mathrm{Disc}(A, B)$

In studying a pair (A, B) of ternary quadratic forms representing the map $\phi_{4,3}$ as in (4.8), we may change the basis of $Q/\mathbb{Z}$ or $R/\mathbb{Z}$ by elements of $GL_3(\mathbb{Z})$ or $GL_2(\mathbb{Z})$

respectively. This reflects the fact that the group $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$ acts on the space of pairs (A, B) of integral ternary quadratic forms in a natural way; namely, if $(A, B) \in V_{\mathbb{Z}}$ is a pair of ternary quadratic forms (which we write as a pair of symmetric 3×3 matrices), then an element $(g_2, g_3) \in G$ operates by sending (A, B) to

$$(g_2, g_3) \cdot (A, B) = (r \cdot g_3 A g_3^t + s \cdot g_3 B g_3^t, t \cdot g_3 A g_3^t + u \cdot g_3 B g_3^t), \tag{4.9}$$

where we have written g_2 as $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL(2)$.

Over $\mathbb{C}$, the representation $V = \mathrm{Sym}^2 \mathbb{C}^3 \otimes \mathbb{C}^2$ of $SL_3(\mathbb{C}) \times SL_2(\mathbb{C})$ has just one fundamental invariant. To see this, notice first that the action of $SL_3(\mathbb{C})$ on V has four independent invariants, namely the coefficients a, b, c, d of the cubic form $f(x, y) = 4 \cdot \mathrm{Det}(Ax - By)$, for it is easily seen that the cubic form f completely specifies the $SL_3(\mathbb{C})$-orbit of the pair (A, B). Next, $SL_2(\mathbb{C})$ acts on the cubic form $f(x, y)$, and it is well-known that this action has exactly one invariant, namely the discriminant $\mathrm{Disc}(f)$ of f. Thus the unique $SL_2(\mathbb{C}) \times SL_3(\mathbb{C})$-invariant on V is $\mathrm{Disc}(4 \cdot \mathrm{Det}(Ax - By))$. We call this fundamental invariant the *discriminant* $\mathrm{Disc}(A, B)$ of the pair (A, B). (The factor 4 has been included to insure that any pair of integral ternary quadratic forms has integral discriminant.)

4.2.2 How much of the structure of Q is determined by (A, B)?

The only fact we have so far relating the structures of Q, R, and the map $\phi_{4,3}$ is that $\phi_{4,3}$ is discriminant-preserving as a map from Q to R. However, this fact alone yields little information on the nature of Q and R. Thus the following lemma on $\phi_{4,3}$ plays an invaluable role in determining the multiplicative structure of Q.

To state the lemma, we use the notation $\mathrm{Ind}_M(v_1, v_2, \ldots, v_k)$ to denote the index of the lattice spanned by $\{v_1, v_2, \ldots, v_k\}$ in the rank k $\mathbb{Z}$-module M.

Lemma 4.4 *If Q is a quartic ring, and R is a cubic resolvent of Q, then*

$$\mathrm{Ind}_Q(1, x, y, xy) = \pm \mathrm{Ind}_R(1, \phi_{4,3}(x), \phi_{4,3}(y)). \tag{4.10}$$

Proof: Since $\mathrm{Disc}(Q) = \mathrm{Disc}(R)$, the assertion of the lemma is equivalent to the following identity:

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ x & x' & x'' & x''' \\ y & y' & y'' & y''' \\ xy & x'y' & x''y'' & x'''y''' \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ xx' + x''x''' & xx'' + x'x''' & xx''' + x'x'' \\ yy' + y''y''' & yy'' + y'y''' & yy''' + y'y'' \end{vmatrix}.$$

The identity may be verified by direct calculation. □

The sign in expression (4.10) of course depends on how Q and R are oriented. To fix the orientations on Q and R once and for all, let $< 1, \alpha, \beta, \gamma >$ and $< 1, \omega, \theta >$ be bases for Q and R respectively such that the map $\bar{\phi}_{4,3}$ is given by

$$\phi_{4,3}(r\alpha + s\beta + t\gamma) = A(r, s, t)\omega + B(r, s, t)\theta.$$

Then we fix the orientations on Q and R so that $\mathrm{Ind}_Q(1, \alpha, \beta, \gamma) = \mathrm{Ind}_R(1, \omega, \theta) = 1$.

We may make one additional assumption about the basis $< 1, \alpha, \beta, \gamma >$ without any harm. By translating α, β, γ by appropriate constants in $\mathbb{Z}$, we may arrange for the coefficients of α and β in $\alpha\beta$, together with the coefficient of α in $\alpha\gamma$, to each equal zero. We call a basis $< 1, \alpha, \beta, \gamma >$ satisfying the latter condition a *normal basis* for R.

Assuming our basis $< 1, \alpha, \beta, \gamma >$ has been normalized, let us write out the mul-

tiplication laws for Q explicitly as

$$\begin{aligned}
\alpha^2 &= h_{11} + g_{11}\alpha + f_{11}\beta + e_{11}\gamma \\
\beta^2 &= h_{22} + g_{22}\alpha + f_{22}\beta + e_{22}\gamma \\
\gamma^2 &= h_{33} + g_{33}\alpha + f_{33}\beta + e_{33}\gamma \\
\alpha\beta &= h_{12} + g_{12}\alpha + f_{12}\beta + e_{12}\gamma \\
\alpha\gamma &= h_{13} + g_{13}\alpha + f_{13}\beta + e_{13}\gamma \\
\beta\gamma &= h_{23} + g_{23}\alpha + f_{23}\beta + e_{23}\gamma,
\end{aligned} \tag{4.11}$$

where $h_{ij}, g_{ij}, f_{ij}, e_{ij} \in \mathbb{Z}$ are constants. The condition that the basis $< 1, \alpha, \beta, \gamma >$ is normal is then equivalent to

$$g_{12} = g_{13} = f_{12} = 0.$$

We use Lemma 4.4 as follows. Let $x = r_1\alpha + r_2\beta + r_3\gamma$, $y = s_1\alpha + s_2\beta + s_3\gamma$ be general elements of Q, where $r_i, s_i, t_i \in \mathbb{Z}$. Then using (4.11), we find that

$$xy = c + t_1\alpha + t_2\beta + t_3\gamma,$$

where $c \in \mathbb{Z}$ and

$$\begin{aligned}
t_1 &= r_1s_1g_{11} + r_1s_2g_{12} + r_1s_3g_{13} + r_2s_1g_{12} + r_2s_2g_{22} + r_2s_3g_{23} + r_3s_1g_{13} \\
&\quad + r_3s_2g_{23} + r_3s_3g_{33} \\
t_2 &= r_1s_1f_{11} + r_1s_2f_{12} + r_1s_3f_{13} + r_2s_1f_{12} + r_2s_2f_{22} + r_2s_3f_{23} + r_3s_1f_{13} \\
&\quad + r_3s_2f_{23} + r_3s_3f_{33} \\
t_3 &= r_1s_1e_{11} + r_1s_2e_{12} + r_1s_3e_{13} + r_2s_1e_{12} + r_2s_2e_{22} + r_2s_3e_{23} + r_3s_1e_{13} \\
&\quad + r_3s_2e_{23} + r_3s_3e_{33},
\end{aligned} \tag{4.12}$$

so that

$$\mathrm{Ind}_Q(1,x,y,xy) = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & r_1 & r_2 & r_3 \\ 0 & s_1 & s_2 & s_3 \\ 0 & t_1 & t_2 & t_3 \end{vmatrix}. \tag{4.13}$$

The right side of (4.13) is a polynomial of degree 4 in the variables r_1, r_2, r_3, s_1, s_2, s_3, and we denote it by $p(r_1, r_2, r_3, s_1, s_2, s_3)$.

Similarly,

$$\mathrm{Ind}_R(1, \phi_{4,3}(x), \phi_{4,3}(y)) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & A(r_1,r_2,r_3) & B(r_1,r_2,r_3) \\ 0 & A(s_1,s_2,s_3) & B(s_1,s_2,s_3) \end{vmatrix}. \tag{4.14}$$

The right side of (4.14) is also a polynomial of degree 4 in the variables r_1, r_2, r_3, s_1, s_2, s_3, and we denote it by $q(r_1, r_2, r_3, s_1, s_2, s_3)$. (Note that the multiplicative structure of R was not needed for computing the polynomial q.)

By Lemma 4.4, we conclude that for all integers $r_1, r_2, r_3, s_1, s_2, s_3$,

$$p(r_1, r_2, r_3, s_1, s_2, s_3) = q(r_1, r_2, r_3, s_1, s_2, s_3).$$

As they take equal values at all integer arguments, the polynomials p and q must in fact be identical. Equating coefficients of like terms yields a system containing numerous linear and quadratic equations in the 15 variables g_{ij}, f_{ij}, e_{ij} in terms of the coefficients of the quadratic forms A and B. Solving (which takes some work!) this overdetermined system, we find that, rather miraculously, there is exactly one solution for these 15 variables.

The values of g_{ij}, f_{ij}, e_{ij} are given as follows. Writing out the pair (A, B) of ternary

quadratic forms (viewed again as symmetric matrices) in the form

$$2 \cdot (A, B) = \left(\begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}, \begin{bmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{bmatrix} \right), \tag{4.15}$$

define the 15 constants $\lambda^{ij}_{k\ell} = \lambda^{ij}_{k\ell}(A, B)$ by

$$\lambda^{ij}_{k\ell}(A, B) = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{k\ell} & b_{k\ell} \end{vmatrix}, \tag{4.16}$$

where $1 \leq i \leq j \leq 3$, $1 \leq k \leq \ell \leq 3$, and $(1,1) \leq (i,j) < (k,\ell) \leq (3,3)$ in the lexicographic ordering. Then we find that the unique solution to the system $p = q$ is given by

$$\begin{aligned}
&g_{11} = \lambda^{11}_{23} + \lambda^{12}_{13},\ g_{22} = \lambda^{22}_{23},\ g_{33} = \lambda^{23}_{33},\ g_{12} = 0,\ g_{13} = 0,\ g_{23} = \lambda^{22}_{33},\\
&f_{22} = \lambda^{13}_{22} - \lambda^{12}_{23},\ f_{11} = -\lambda^{11}_{13},\ f_{33} = -\lambda^{13}_{33},\ f_{12} = 0,\ f_{13} = -\lambda^{11}_{33},\ f_{23} = -\lambda^{12}_{33},\\
&e_{33} = \lambda^{11}_{23} + \lambda^{12}_{13},\ e_{11} = \lambda^{11}_{12},\ e_{22} = \lambda^{12}_{22},\ e_{12} = \lambda^{11}_{22},\ e_{13} = \lambda^{11}_{23},\ e_{23} = \lambda^{13}_{22},
\end{aligned} \tag{4.17}$$

where the h_{ij} are still undetermined. However, it turns out that the associative law for Q now uniquely determines the h_{ij}! Namely, we use (4.11) and (4.17) to expand out the identities

$$\begin{aligned}
&\alpha^2 \cdot \beta = \alpha \cdot \alpha\beta,\quad \alpha \cdot \beta^2 = \alpha\beta \cdot \beta,\quad \alpha^2 \cdot \gamma = \alpha \cdot \alpha\gamma,\\
&\alpha \cdot \gamma^2 = \alpha\gamma \cdot \gamma,\quad \beta^2 \cdot \gamma = \beta \cdot \alpha\gamma,\quad \beta \cdot \gamma^2 = \beta\gamma \cdot \gamma;
\end{aligned} \tag{4.18}$$

equating coefficients of $1, \alpha, \beta, \gamma$, we obtain a system of several linear and quadratic equations in the h_{ij}. By another miracle, these equations also possess a unique

solution, namely,

$$\begin{aligned}
h_{11} &= -\lambda_{22}^{11}\lambda_{33}^{11} - \lambda_{13}^{11}\lambda_{23}^{12} + \lambda_{13}^{11}\lambda_{22}^{13} + \lambda_{12}^{11}\lambda_{33}^{12} \\
h_{22} &= \lambda_{22}^{11}\lambda_{33}^{22} - \lambda_{13}^{12}\lambda_{23}^{22} - \lambda_{23}^{11}\lambda_{23}^{22} \\
h_{33} &= -\lambda_{33}^{11}\lambda_{33}^{22} - \lambda_{13}^{12}\lambda_{33}^{23} \\
h_{12} &= -\lambda_{13}^{11}\lambda_{23}^{22} + \lambda_{12}^{11}\lambda_{33}^{22} \\
h_{13} &= -\lambda_{13}^{11}\lambda_{33}^{22} + \lambda_{12}^{11}\lambda_{33}^{23} \\
h_{23} &= -\lambda_{33}^{11}\lambda_{23}^{22} - \lambda_{13}^{12}\lambda_{33}^{22}.
\end{aligned} \tag{4.19}$$

Thus we have completely determined the ring structure of Q; it is given in sum by (4.11), (4.17), and (4.19).

It is interesting to ask what the discriminant of the resulting quartic ring $Q = Q(A, B)$ is in terms of the pair of ternary quadratic forms (A, B). As an explicit calculation shows, the answer is happily that $\mathrm{Disc}(Q(A, B)) = \mathrm{Disc}(A, B)$.

Notice that all the structure coefficients of Q are given in terms of the quantities $\lambda_{k\ell}^{ij}(A, B)$, which are $SL(2)$-invariants of the space of pairs (A, B) of ternary quadratic forms. This should be expected since $SL(2)$ acts only on the basis of the cubic ring R and does not affect Q or the chosen basis of Q. We study the $SL(2)$-invariants $\lambda_{k\ell}^{ij}(A, B)$ in more detail in Section 4.2.7.

4.2.3 How much of the structure of R is determined by (A, B)?

Having found that the structure of Q is uniquely determined from the data (A, B), it may come as little surprise that the cubic ring R is also determined by (A, B).

We may guess what this ring R should be as follows. Suppose multiplication in R is given by (3.1). We have seen in Chapter 2 that as $GL_2(\mathbb{Z})$ acts on the chosen basis $< \omega, \theta >$ of $R/\mathbb{Z}$, the quantities a, b, c, d change according to the action of $GL_2(\mathbb{Z})$ on the binary cubic form $g(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, where $\mathrm{Disc}(g) = \mathrm{Disc}(R)$.

On the other hand, as observed in Subsection 4.2.1, changing basis in $R/\mathbb{Z}$ results also in an action of $SL_2(\mathbb{Z})$ on the binary cubic form $f(x,y) = 4 \cdot \mathrm{Det}(Ax - By) = a'x^3 + b'x^2y + c'xy^2 + d'y^3$, and again, $\mathrm{Disc}(f) = \mathrm{Disc}(R)$. Hence we expect that $g = f$, i.e., $a = a'$, $b = b'$, $c = c'$, $d = d'$.

To prove the latter assertion, we may simply use the relation

$$\mathrm{Ind}_Q(1, x, x^2, x^3) = \mathrm{Ind}_R(1, \phi_{4,3}(x), \phi_{4,3}(x)^2), \tag{4.20}$$

since the multiplicative structure of Q is now in place. Let $x = r_1\alpha + r_2\beta + r_3\gamma \in Q$. Then

$$\mathrm{Ind}_Q(1, x, x^2, x^3) = p(r_1, r_2, r_3)$$

and

$$\mathrm{Ind}_R(1, \phi_{4,3}(x), \phi_{4,3}(x)^2) = q(r_1, r_2, r_3),$$

where p and q are determinantal expressions similar to (4.13) and (4.14), but quite a bit larger and thus best left suppressed. As before, we argue that the polynomials p and q must take the same values for all integer choices of r_1, r_2, r_3, and consequently are identical. Equating coefficients of like terms, we obtain several linear and quadratic equations in a, b, c, d. Solving these equations for a, b, c, d, we find that there is a unique solution, and it is indeed given by $a = a'$, $b = b'$, $c = c'$, $d = d'$, i.e.,

$$4 \cdot \mathrm{Det}(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3, \tag{4.21}$$

and we have determined the structure of R.

4.2.4 Is R the cubic resolvent of Q?

It remains only to verify that the unique pair (Q, R) of rings we have obtained from (A, B) satisfy the conditions we require of them, namely, that R is a cubic resolvent of Q and that (A, B) describes the map

$$\bar{\phi}_{4,3} : Q/\mathbb{Z} \to R/\mathbb{Z}.$$

We have already seen that $\mathrm{Disc}(Q) = \mathrm{Disc}(R)$. Hence it suffices just to show that: if $F_{w,x,y,z}$ is the characteristic polynomial of a general element $w + x\alpha + y\beta + z\gamma \in Q$ (acting on Q by multiplication), then there exists a constant $c \in \mathbb{Z}$ such that the characteristic polynomial $G_{w,x,y,z,c}$ of the element $c + A(x, y, z)\omega + B(x, y, z)\theta \in R$ (acting on R by multiplication) is the cubic resolvent of $F_{w,x,y,z}$.*

To prove the latter assertion, we use (4.11), (4.17) and (4.19) to determine the action of $w + x\alpha + y\beta + z\gamma$ on Q explicitly, allowing us to compute $F_{w,x,y,z}$. Similarly, we use (3.1) and (3.2) to explicitly compute $G_{w,x,y,z,c}$. These (somewhat lengthy) computations then show that there is a certain polynomial c, in the entries of A and B, such that $G_{w,x,y,z,c}$ is the cubic resolvent of $F_{w,x,y,z}$, as desired.

4.2.5 The main result

We have completed the proof of the following theorem:

Theorem 4.5 *There is a bijection between the set of $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$-equivalence classes of pairs of integral ternary quadratic forms, and pairs (Q, R), where Q is an isomorphism class of quartic ring and R is a cubic resolvent ring of Q. Moreover, this bijection is discriminant-preserving, i.e.,* $\mathrm{Disc}((A, B)) = \mathrm{Disc}(Q) = \mathrm{Disc}(R)$.

*The cubic resolvent of a quartic polynomial $F(t) = x^4 + px^3 + qx^2 + rx + s$ is given by the expression $G(t) = x^3 - qx^2 + (pr - 4s)x - p^2s + 4qs - r^2$. If the roots of F are denoted $\kappa, \kappa', \kappa'', \kappa'''$, then the roots of G are $\kappa\kappa' + \kappa''\kappa'''$, $\kappa\kappa'' + \kappa'\kappa'''$, $\kappa\kappa''' + \kappa'\kappa''$.

Notice that in the statement of the theorem we do not say "isomorphism class of cubic ring". This is because, for certain rings Q of discriminant zero, a cubic ring R may arise as a cubic resolvent of Q in more than one way which is not accounted for by any automorphism of $\bar{Q}$. This phenomenon does not occur for rings of nonzero discriminant (e.g., for orders in number fields), but in general, when writing a pair (Q, R), R is implied to be not just an isomorphism class of cubic ring, but rather an explicit overring of $R^{inv}(Q)$ such that $\mathrm{Disc}(R) = \mathrm{Disc}(Q)$.

It may seem slightly disconcerting at first to see that pairs of integral ternary quadratic forms do not precisely parametrize rings, but rather pairs of rings! But the situation is still very analogous to the case for cubic rings (Theorem 3.1), for binary cubic forms parametrize pairs (R, S), where R is a cubic ring and S is a quadratic resolvent. However, since one finds that the quadratic resolvent S is unique for all cubic rings R, the parametrization becomes a bijection on cubic rings.

This leads to the question: for which quartic rings Q is the cubic resolvent unique? More generally, given a quartic ring Q, how can we determine the number of cubic resolvents of Q? To answer this question, it is necessary to introduce the notion of *content* of a ring, which we discuss in the next section.

4.2.6 The content of a ring

In addition to the discriminant, rings of rank k possess another very important invariant which we call the *content*.

Definition 4.6 *Let $\mathcal{R}$ be a ring of rank k. The content* $\mathrm{ct}(\mathcal{R})$ *of $\mathcal{R}$ is defined to be*

$$\mathrm{ct}(\mathcal{R}) = \max\{n : \exists\, \tilde{\mathcal{R}} \text{ of rank } k \text{ such that } \mathcal{R} = \mathbb{Z} + n\tilde{\mathcal{R}}\},$$

if the latter maximum exists; otherwise, the content is said to be ∞.

For example, the quadratic ring $\mathbb{Z}[x]/(x^2)$ of discriminant 0 has content ∞, since it is equal to $\mathbb{Z} + nS_n$, where $S_n = \mathbb{Z}[x_n]/(x_n^2)$ and $x = nx_n$. For other quadratic rings, the content coincides with what is usually called the *conductor*.

The content of a cubic ring $R = R(f)$ is equal to the content of the corresponding binary cubic form f (in the usual sense, i.e., the greatest common divisor of its coefficients). Indeed, the correspondence $f \leftrightarrow R(f)$ given by (3.1) implies that

$$R(nf) = \mathbb{Z} + nR(f)$$

for all n and f, so that a ring corresponding to a cubic form of content n has content at least n, and, conversely, a cubic form corresponding to a cubic ring of content n must be a multiple of n.

One finds using the same reasoning and formulas (4.11), (4.17), and (4.19) that the content of a quartic ring $Q = Q(A, B)$ is equal to the greatest common divisor of the fifteen $SL(2)$-invariants $\lambda_{k\ell}^{ij}(A, B)$. It is thus natural to define the *content* $\mathrm{ct}(A, B)$ of a pair (A, B) of integral ternary quadratic forms to be the content of the corresponding quartic ring, i.e.,

$$\mathrm{ct}(A, B) = \mathrm{ct}(Q(A, B)) = \gcd\{\lambda_{k\ell}^{ij}(A, B)\}.$$

Most "nice" rings have content 1. For example, it is easy to see that any Gorenstein ring $\mathcal{R}$ of rank at least 3 must have content 1; for if $\mathcal{R}$ did not have content 1, then there would exist a prime p such that

$$\mathcal{R}/(p) \cong \mathbb{F}_p[x_1, x_2, \ldots, x_{k-1}]/(x_1, x_2, \ldots, x_{k-1})^2,$$

and the latter is clearly not Gorenstein if $k > 2$. Gross [17] has shown that in the rank 3 case, the notions of Gorenstein and content 1 actually coincide. This,

however, does not hold true for higher rank, as the non-Gorenstein content 1 ring $\mathbb{Z} \oplus \mathbb{Z}[x,y]/(x^2, xy, y^2)$ illustrates.

Like the discriminant, the content gives important structural information about a ring of rank k. Our motivation for introducing the content arises from its close relation to resolvent rings. In the case of cubic rings, the notion of content is exactly what is needed to answer the question posed at the end of Section 3.3: when is the quadratic invariant ring of a cubic ring equal to its quadratic resolvent ring?

Theorem 4.7 *Let R be a cubic ring, and let $S^{inv}(R)$ denote the quadratic invariant ring of R and S the quadratic resolvent ring of R. Then $S^{inv}(R) = S$ if and only if R has content* 1.

Proof: We observe that, by definition, the quadratic invariant ring $S^{inv}(R)$ is the smallest ring containing the image of the mapping $\phi_{3,2} : R \to S$, and any subring of S takes the form $\mathbb{Z}+rS$, for some nonnegative integer r. In the case of $S^{inv}(R) \subset S$, this number is simply the smallest nonnegative integer r such that $\bar{\phi}_{3,2}(x)$ is a multiple of r in $S/\mathbb{Z}$ for all $x \in R/\mathbb{Z}$.

However, $\bar{\phi}_{3,2}$ is given by a binary cubic form, and the greatest common divisor of the values taken by a cubic form is given simply by the greatest common divisor of its coefficients. Therefore, we have $r = 1$ if and only if some (any) binary cubic form corresponding to R is primitive. On the other hand, we have seen that f is primitive if and only if R has content 1. This is the desired conclusion. □

The analogue of Theorem 4.7 also remains true for quartic rings: the cubic invariant ring $R^{inv}(Q)$ of a quartic ring Q forms the unique cubic resolvent ring if and only if $\mathrm{ct}(Q) = 1$. To prove this statement, and its generalizations, it is necessary to better understand the $SL(2)$-related invariant theory of pairs of ternary quadratic forms. This is carried out in the next section.

4.2.7 Invariant theory of pairs of ternary quadratic forms II

We observed in Section 4.1 that the $SL_3(\mathbb{C})$-invariants on the space $V = \mathbb{C}^2 \otimes \mathrm{Sym}^2\mathbb{C}^3$ of pairs (A, B) of ternary quadratic forms are given by the four coefficients of the binary cubic form $f(x, y) = 4 \cdot \mathrm{Det}(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3$. Moreover, the unique $SL(2) \times SL(3)$ invariant on V is given simply by $\mathrm{Disc}(A, B) = \mathrm{Disc}(4 \cdot \mathrm{Det}(Ax - By))$.

In this section, we examine more closely the $SL_2(\mathbb{C})$-invariants on V, as these are precisely the quantities that determine the structure of the quartic rings corresponding to points in V. If we write out again the element $(A, B) \in V$ as

$$2 \cdot (A, B) = \left(\begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}, \begin{bmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{bmatrix} \right), \tag{4.22}$$

then we observed earlier that the $SL_2(\mathbb{C})$-invariants are given by

$$\lambda^{ij}_{k\ell}(A, B) = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{k\ell} & b_{k\ell} \end{vmatrix}, \tag{4.23}$$

where $1 \le i \le j \le 3$, $1 \le k \le \ell \le 3$, and $(1, 1) \le (i, j) < (k, \ell) \le (3, 3)$ in the lexicographic ordering. This yields a total of 15 invariants. However, unlike the case of the four $SL(3)$-invariants a, b, c, d, these 15 $SL(2)$-invariants are not independent, but are related by the fifteen syzygies

$$\lambda^{gh}_{k\ell}(A, B)\, \lambda^{ij}_{mn}(A, B) = \lambda^{gh}_{ij}(A, B)\, \lambda^{k\ell}_{mn}(A, B) + \lambda^{gh}_{mn}(A, B)\, \lambda^{ij}_{k\ell}(A, B), \tag{4.24}$$

where $(1, 1) \le (g, h) < (i, j) < (k, \ell) < (m, n) \le (3, 3)$, again in the lexicographic ordering.[†]

[†]These fifteen syzygies are also not independent, but this does not matter for our purposes.

Conversely, given any set of 15 constants $\{\lambda_{k\ell}^{ij}\}$ satisfying the fifteen relations (4.24), there is always an $SL_2(\mathbb{C})$-orbit in V possessing these 15 constants as the $SL(2)$-invariants. In fact, something stronger is true; namely, if these 15 constants $\lambda_{k\ell}^{ij}$ are actually integers, then there exists an integer point in V possessing these 15 constants as the $SL(2)$-invariants. We state this more precisely in the following lemma.

Lemma 4.8 *For any 15 constants $\lambda_{k\ell}^{ij} \in \mathbb{C}$ satisfying the relations* (4.24)*, there exists an irreducible $SL_2(\mathbb{C})$-orbit $W \subset V$ such that*

$$\lambda_{k\ell}^{ij}(W) = \lambda_{k\ell}^{ij} \text{ for all } i \leq j,\ k \leq \ell,\ (i,j) < (k,\ell).$$

If the 15 constants $\lambda_{k\ell}^{ij}$ are not all equal to zero, then W is uniquely determined, and if furthermore all the $\lambda_{k\ell}^{ij}$ are integers, then the variety W contains an integer point $(A,B) \in V_{\mathbb{Z}}$.

Proof: It is easy to see that all invariants $\lambda_{k\ell}^{ij}(A,B)$ are equal to zero if and only if $\{A,B\}$ spans a zero or one-dimensional space in V. There are of course (infinitely) many such points (A,B), both in V/G as well as in $V_{\mathbb{Z}}/G_{\mathbb{Z}}$.

We therefore proceed to the case where not all invariants are zero; without loss of generality, we may assume $\lambda_{12}^{11} \neq 0$. Applying the appropriate transformation in $SL_2(\mathbb{C})$, we may assume then that $a_{11} = 1$, $b_{11} = 0$, $a_{12} = 0$, and $b_{12} = \lambda_{12}^{11} \neq 0$.

With these assumptions, the definition (4.23) of $\lambda_{k\ell}^{ij}$ for $(i,j) = (1,1)$ and $(1,2)$ immediately imply that $b_{k\ell} = \lambda_{k\ell}^{11}$ for all k,ℓ, and that $a_{k\ell} = \lambda_{k\ell}^{12}/b_{12}$ for all $(k,\ell) \neq (1,1)$. Six of the equations in (4.23) remain unused, but they, when expanded out, turn out to be equivalent to the six of the syzygies in (4.24). Therefore, if the 15 invariants $\lambda_{k\ell}^{ij}$ are fixed, not all zero, and satisfy the syzygies (4.24), then there is a unique solution for (A,B) of the above type, and so a unique $SL_2(\mathbb{C})$-orbit W having the prescribed set of invariants.

Assume now that the 15 constants $\lambda_{k\ell}^{ij}$ are also integral. Then, by the above discussion, the quantities $b_{ij} = \lambda_{ij}^{11}$ are themselves forced to be integers, while the quantities $a_{ij} = \lambda_{ij}^{12}/b_{12}$ are all integer multiples of $1/b_{12}$. Consider the pair of integral forms $(b_{12}A, B) \in V_{\mathbb{Z}}$, whose λ-invariants are all multiples of b_{12}. By the theory of elementary divisors, there exists an $SL_2(\mathbb{Z})$-transformation (A', B') of $(b_{12}A, B)$ such that A' is a multiple of n_1 and B' is a multiple of n_2, where n_1, n_2 are integers such that $n_1 n_2 = n$. It follows that $(A'/n_1, B'/n_2) \in V_{\mathbb{Z}}$ is $SL_2(\mathbb{Q})$-equivalent to (A, B), and is therefore an integer point of W. $\square$

Lemma 4.8 implies that if the $\lambda_{k\ell}^{ij}$'s are integers satisfying (4.24), then there exists at least one $G_{\mathbb{Z}}$-orbit on $V_{\mathbb{Z}}$ having those integers as the $SL(2)$-invariants. The next lemma strengthens this, by giving the exact number of $G_{\mathbb{Z}}$-orbits on $V_{\mathbb{Z}}$ having a prescribed set of (integral) $SL(2)$-invariants.

Lemma 4.9 *Let $\lambda_{k\ell}^{ij} \in \mathbb{Z}$ be any 15 integers satisfying the relations* (4.24). *Then the number of $G_{\mathbb{Z}}$-orbits $W_{\mathbb{Z}}$ in $V_{\mathbb{Z}}$ such that*

$$\lambda_{k\ell}^{ij}(W_{\mathbb{Z}}) = \lambda_{k\ell}^{ij} \text{ for all } i \le j,\ k \le \ell,\ (i,j) < (k,\ell)$$

is equal to the number of index n sublattices of $\mathbb{Z}^2$, where

$$n = \gcd\{\lambda_{k\ell}^{ij} : (i,j) < (k,\ell)\}.$$

Proof: The lemma is true when all the $SL(2)$-invariants $\lambda_{k\ell}^{ij}$ are zero (i.e., $n = \infty$), so we assume the integers $\lambda_{k\ell}^{ij}$ are not all equal to zero.

Clearly, the set of integers $\{\lambda_{k\ell}^{ij}/n\}$ also satisfy the syzygies (4.24); hence, by Lemma 4.8, there is exactly one $SL_2(\mathbb{C})$-orbit W in V having $\{\lambda_{k\ell}^{ij}/n\}$ as the $SL(2)$-invariants, and W contains an integral point (A, B). Let $X \subset \mathrm{Sym}^2\mathbb{C}^3$ denote the two-dimensional $\mathbb{C}$-vector space of ternary quadratic forms spanned by A and B

(equivalently, X is the vector space spanned by A_0, B_0 for any point $(A_0, B_0) \in W$), and let $X_{\mathbf{Z}}$ denote the (unique) maximal lattice in X consisting of integral ternary quadratic forms. Since $\gcd\{\lambda_{k\ell}^{ij}(A,B)\} = 1$, it must be that A, B span a maximal integral lattice in X, so A, B actually form a $\mathbb{Z}$-basis for $X_{\mathbf{Z}}$.

Define $W_{\mathbf{Z}}$ by

$$W_{\mathbf{Z}} = \{(A,B) : \{A,B\} \text{ spans } X_{\mathbf{Z}} \text{ as a } \mathbb{Z}\text{-module}\}.$$

Then $W_{\mathbf{Z}} \subset W$, $W_{\mathbf{Z}}$ forms a single $SL_2(\mathbb{Z})$-orbit, and any integral point $(A,B) \in W$ must lie in $W_{\mathbf{Z}}$. Hence $W_{\mathbf{Z}}$ is the unique $SL_2(\mathbb{Z})$-orbit in $V_{\mathbf{Z}}$ having $\lambda_{k\ell}^{ij}/n$ as the $SL(2)$-invariants.

Similarly, if $W'_{\mathbf{Z}}$ is an $SL_2(\mathbb{Z})$-orbit $V_{\mathbf{Z}}$ having $SL(2)$-invariants $\lambda_{k\ell}^{ij}$, then for any $(A',B') \in W'_{\mathbf{Z}}$, A, B span a lattice L in $X_{\mathbf{Z}}$, and we may define $W'_{\mathbf{Z}}$ by

$$W'_{\mathbf{Z}} = \{(A,B) : \{A,B\} \text{ spans } L \text{ as a } \mathbb{Z}\text{-module}\}. \tag{4.25}$$

Moreover, $\gcd\{\lambda_{k\ell}^{ij}(A,B)\} = n$ implies that this sublattice L has index n in $X_{\mathbf{Z}}$. Conversely, given any index n sublattice L of $X_{\mathbf{Z}}$, let $W'_{\mathbf{Z}}$ be defined by (4.25). Then $W'_{\mathbf{Z}}$ is an $SL_2(\mathbb{Z})$-orbit with the desired invariants. Thus the $SL_2(\mathbb{Z})$-orbits in $V_{\mathbf{Z}}$ having $SL(2)$-invariants $\lambda_{k\ell}^{ij}$ are in one-to-one correspondence with the index n sublattices of $X_{\mathbf{Z}} \cong \mathbb{Z}^2$. This implies the lemma. □

4.2.8 Isolating Q

Given a quartic ring Q, and given the structure coefficients of Q with respect to a normal basis $< 1, \alpha, \beta, \gamma >$ of Q, the relations (4.17) and (4.19) completely determine the values of the 15 constants $\lambda_{k\ell}^{ij}$. Indeed, only the coefficients of α, β, and γ in (4.17) are needed in order to determine the values of $\lambda_{k\ell}^{ij}$. The associative law in Q

then does two things. First, as we have observed earlier, it implies that the values of the constant coefficients h_{ij} must then be as given in (4.19). Second, it implies that the syzygies (4.24) must hold among the $\lambda_{k\ell}^{ij}$. By Lemma 4.8, it follows that there exists an integer orbit $\bar{x} \in V_{\mathbb{Z}}/G_{\mathbb{Z}}$ such that $Q(\bar{x}) = Q$ and $\mathrm{Disc}(Q(\bar{x})) = \mathrm{Disc}(x)$. Combined with Theorem 4.5, we have shown:

Theorem 4.10 *The map $\bar{x} \to Q(\bar{x})$ is a discriminant-preserving surjection from the set $V_{\mathbb{Z}}/G_{\mathbb{Z}}$ onto the set of isomorphism classes of quartic rings. The number of preimages in $V_{\mathbb{Z}}/G_{\mathbb{Z}}$ of a given quartic ring Q is equal to the number of index $\mathrm{ct}(Q)$ sublattices of $\mathbb{Z}^2$.*

Corollary 4.11 *Every quartic ring has at least one cubic resolvent.*

Corollary 4.12 *The cubic resolvent ring of a quartic ring Q is unique if and only if the quartic ring has content 1; in that case, the cubic resolvent ring R is equal to the cubic invariant ring $R^{inv}(Q)$.*

Thus Theorem 4.10 shows that the map $\bar{x} \to Q(\bar{x})$ is a genuine bijection on quartic rings having content 1 (and hence on all Gorenstein rings).

An important class of rings on which Theorem 4.10 gives a bijective correspondence are the maximal orders in quartic number fields. These, of course, are the quartic rings of greatest interest to algebraic number theorists. It may therefore be desirable to understand those pairs (A, B) of integral ternary quadratic forms that correspond to maximal orders in quartic fields, and to understand the splitting behavior of primes in those fields in terms of the corresponding pairs (A, B). This is the goal of the next two sections.

4.2.9 Local behaviour

In this section, we consider pairs (A, B) of ternary quadratic forms over the p-adic ring $\mathbb{Z}_p$ and over its residue field $\mathbb{Z}/p\mathbb{Z}$.

Let (A, B) be an element of $V_{\mathbb{Z}}$ (resp. of $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$). Over the residue field $\mathbb{F}_p$, (A, B) determines two conics on $\mathbb{P}^2_{\mathbb{F}_p}$, which, aside from certain degenerate cases, intersect each other in exactly four points (counting multiplicities). For such nondegenerate pairs (A, B), define the symbol $((A, B), p)$ by putting

$$((A, B), p) = (f_1^{e_1} f_2^{e_2} \cdots),$$

where the f_i's indicate the degrees of the residue fields at the points of intersection, and the e_i's indicate the respective multiplicities. There are thus eleven possible values for the symbol $((A, B), p)$, namely, (1111), (112), (13), (4), (22), $(1^2 11)$, $(1^2 2)$, $(1^3 1)$, (1^4), $(1^2 1^2)$, and (2^2). (As is customary, we suppress exponents that are equal to one.)

It is clear that if two points x, y in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$), are equivalent under a transformation in $GL_2(\mathbb{Z})$ (resp. $GL_2(\mathbb{Z}_p)$, $GL_2(\mathbb{F}_p)$), then $(x, p) = (y, p)$. By $T_p(1111), T_p(112)$, etc., denote the set of x such that $(x, p) = (1111)$, $(x, p) = (112)$, etc.

By the definition of $Q(A, B)$, the ring structure of the quotient ring $Q(A, B)/(p)$ depends only on the $GL_2(\mathbb{F}_p)$-orbit of the pair (A, B) modulo p; thus the symbol $((A, B), p)$ should indicate something about the structure of the ring $Q(A, B)$ when reduced modulo p. In fact, a direct calculation shows that

$$(A, B) \in T_p(f_1^{e_1} f_2^{e_2} \cdots) \tag{4.26}$$

if and only if

$$Q(A, B)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \cdots, \tag{4.27}$$

except in the case $T_p(1^4)$, where the ring $Q(A, B)/(p)$ might also take the form

$\mathbb{F}_p[x,y]/(x^2,y^2)$. It is hence natural to divide $T_p(1^4)$ into two further sets: $T_p^{(1)}(1^4)$, consisting of the pairs (A,B) such that $Q(A,B)/(p) \cong \mathbb{F}_p[t]/(t^4)$, and $T_p^{(2)}(1^4)$, consisting of the pairs (A,B) such that $Q(A,B)/(p) \cong \mathbb{F}_p[x,y]/(x^2,y^2)$.

For any set S in $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Z}_p}$, $V_{\mathbb{F}_p}$) that is definable by congruence conditions, denote by $\mu(S) = \mu_p(S)$ the p-adic density of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure μ on V so that $\mu(V_{\mathbb{Z}_p}) = 1$. The following lemma determines the p-adic densities of the sets $T_p(\cdot)$.

Lemma 4.13 *We have*

$$\begin{aligned}
\mu(T_p(1111)) &= \tfrac{1}{24}(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(112)) &= \tfrac{1}{4}(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(13)) &= \tfrac{1}{3}(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(22)) &= \tfrac{1}{8}(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(4)) &= \tfrac{1}{4}(p-1)^4\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(1^211)) &= \tfrac{1}{2}(p-1)^3\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(1^22)) &= \tfrac{1}{2}(p-1)^3\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(1^21^2)) &= \tfrac{1}{2}(p-1)^2\,p^4\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(2^2)) &= \tfrac{1}{2}(p-1)^3\,p^4\,(p+1)\;\;(p^2+p+1)\,/\,p^{12}\\
\mu(T_p(1^31)) &= \;\;(p-1)^3\,p^3\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p^{(1)}(1^4)) &= \;\;(p-1)^3\,p^2\,(p+1)^2\,(p^2+p+1)\,/\,p^{12}\\
\mu(T_p^{(2)}(1^4)) &= \;\;(p-1)^2\,p^3\,(p+1)\;\;(p^2+p+1)\,/\,p^{12}\,.
\end{aligned}$$

Proof: Since the criteria for membership of (A,B) in a $T_p(\cdot)$ depend only the residue class of (A,B) modulo p, it suffices to consider the situation over $\mathbb{F}_p$.

We examine first $\mu(T_p(1111))$. An elementary count shows that the number of unordered quadruples of points in $\mathbb{P}^2_{\mathbb{F}_p}$, such that no three are collinear, is $\frac{1}{24}(p^2+p+1)(p^2+p)(p^2)(p^2-2p+1)$. Furthermore, given such a quadruple of points, there is a two-dimensional family of conics passing through those four points; that is, there are

$(p^2-1)(p^2-p)$ ordered pairs (A,B) of ternary quadratic forms over $\mathbb{F}_p$ having those four points as common zeros. Since the total number of pairs of ternary quadratic forms over $\mathbb{F}_p$ is p^{12}, it follows that

$$\mu(T_p(1111)) = \frac{1}{24}\left[(p^2+p+1)(p^2+p)(p^2)(p^2-2p+1)^4\right] \cdot \left[(p^2-1)(p^2-p)\right] / p^{12},$$

as given by the lemma.

The other parts may be handled similarly. □

It can be seen by a direct calculation that a pair (A,B) has nonzero discriminant modulo p if and only if it is in $T_p(1111), T_p(112), T_p(13), T_p(4)$, or $T_p(22)$ (i.e., if and only if (A,B) intersect in four distinct points as conics over $\bar{\mathbb{F}}_p$).

4.2.10 Maximal quartic rings

A quartic ring having nonzero discriminant is said to be *maximal* if it is not a subring of any other quartic ring. In this section, we determine necessary and sufficient conditions on $(A,B) \in V_{\mathbb{Z}}$ for $Q(A,B)$ to be a maximal quartic ring.

By the theory of algebraic numbers, a maximal ring R of nonzero discriminant is a direct sum of Dedekind domains. In particular, a prime p factorizes uniquely in Q as a product of prime ideals of Q. If $p = P_1^{e_1}P_2^{e_2}\cdots$ is the factorization of p into prime ideals of $Q(A,B)$, where $Q/P_i \cong \mathbb{F}_{p^{f_i}}$, define the symbol (Q,p) by setting

$$(Q,p) = (f_1^{e_1}f_2^{e_2}\cdots).$$

Suppose now $(A,B) \in V_{\mathbb{Z}}$ is such that $Q(A,B)$ is maximal. If $(Q,p) = (f_1^{e_1}f_2^{e_2}\cdots)$, then clearly

$$Q(A,B)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \mathbb{F}_{p^{f_2}}[t_2]/(t_2^{e_2}) \oplus \cdots,$$

so that by (4.26), $(A,B) \in T_p(f_1^{e_1} f_2^{e_2} \cdots)$. Therefore, if the ring $Q(A,B)$ is maximal for an element $(A,B) \in V_{\mathbb{Z}}$, then (A,B) is contained in one of the $T_p(\cdot)$'s as defined in the previous section, and

$$((A,B),p) = (Q(A,B),p).$$

Now a quartic ring Q is maximal if and only if the $\mathbb{Z}_p$-algebra $Q_p = Q \otimes \mathbb{Z}_p$ is maximal for every p, in the sense that Q_p is not contained in any other quartic $\mathbb{Z}_p$-algebra over $\mathbb{Z}_p$. As a quartic ring Q with discriminant prime to p is necessarily maximal at p, $Q(A,B)$ is automatically maximal at p for any (A,B) in $T_p(1111), T_p(112), T_p(13), T_p(4)$, or $T_p(22)$.

In order to understand the other $T_p(\cdot)$'s with regard to maximality, we require the following lemma.

Lemma 4.14 *If Q is not a maximal ring at p, then there exists a $\mathbb{Z}$-basis $1, \alpha, \beta, \gamma$ of Q, such that at least one of the following is true:*

- $\mathbb{Z} + \mathbb{Z} \cdot (\alpha/p) + \mathbb{Z} \cdot \beta + \mathbb{Z} \cdot \gamma$ *forms a ring*
- $\mathbb{Z} + \mathbb{Z} \cdot (\alpha/p) + \mathbb{Z} \cdot (\beta/p) + \mathbb{Z} \cdot \gamma$ *forms a ring*
- $\mathbb{Z} + \mathbb{Z} \cdot (\alpha/p) + \mathbb{Z} \cdot (\beta/p) + \mathbb{Z} \cdot (\gamma/p)$ *forms a ring.*

Proof: Let Q' be a maximal ring at p containing Q, and let $Q_1 = Q'' \cap Q_p$. Then the ring Q_1 also strictly contains Q, and moreover, the index of Q in Q_1 is a power of p. By the theory of elementary divisors, there exist nonnegative integers $i \geq j \geq k$ and a basis $< \alpha, \beta, \gamma >$ of Q such that

$$Q_1 = \mathbb{Z} + \mathbb{Z}(\alpha/p^i) + \mathbb{Z}(\beta/p^j) + \mathbb{Z}(\gamma/p^k). \tag{4.28}$$

If $i = 1$, then we are done. Hence we assume $i > 1$.

Suppose the multiplicative structure of Q with respect to the basis $< \alpha, \beta, \gamma >$ is given by (4.11). That the right side of (4.28) is a ring then translates into the following congruence conditions on the structure coefficients:[‡]

$$\begin{array}{lll} g_{11} \equiv 0 \pmod{p^i}, & f_{11} \equiv 0 \pmod{p^{2i-j}}, & e_{11} \equiv 0 \pmod{p^{2i-k}}, \\ g_{22} \equiv 0 \pmod{p^{2j-i}}, & f_{22} \equiv 0 \pmod{p^j}, & e_{22} \equiv 0 \pmod{p^{2j-k}}, \\ g_{33} \equiv 0 \pmod{p^{2k-i}}, & f_{33} \equiv 0 \pmod{p^{2k-j}}, & e_{33} \equiv 0 \pmod{p^k}, \\ g_{12} \equiv 0 \pmod{p^j}, & f_{12} \equiv 0 \pmod{p^i}, & e_{12} \equiv 0 \pmod{p^{i+j-k}}, \\ g_{13} \equiv 0 \pmod{p^k}, & f_{13} \equiv 0 \pmod{p^{i+k-j}}, & e_{13} \equiv 0 \pmod{p^i}, \\ g_{23} \equiv 0 \pmod{p^{j+k-i}}, & f_{23} \equiv 0 \pmod{p^k}, & e_{23} \equiv 0 \pmod{p^j}, \end{array} \tag{4.29}$$

If $j = k = 0$, then a quick check shows that replacing (i, j, k) by $(i-1, j, k)$ maintains the truth of the above congruences, and so Q' as defined by (4.28) remains a ring. Similarly, if $k = 0$ and $j > 0$, then we may replace (i, j, k) by $(i-1, j-1, k)$, and if $k > 0$, then we may replace (i, j, k) by $(i-1, j-1, k-1)$. Thus by a finite sequence of such moves we arrive at $i = 1$, the desired conclusion. □

For an $(A, B) \in V_{\mathbb{Z}}$, using the multiplication laws of $Q(A, B)$ as given in (4.11) the conditions itemized above translate into the following conditions respectively on the λ-invariants of (A, B):

- $\lambda_{22}^{11}, \lambda_{23}^{11}, \lambda_{33}^{11}, \lambda_{13}^{12}$, and $\lambda_{12}^{11}, \lambda_{13}^{11}$, are multiples of p^2
- $\lambda_{13}^{11}, \lambda_{23}^{11}, \lambda_{13}^{12}, \lambda_{23}^{12}, \lambda_{22}^{13}, \lambda_{23}^{22}$ are all multiples of p, and $\lambda_{12}^{11}, \lambda_{22}^{11}, \lambda_{22}^{12}$ are multiples of p^2
- all the $\lambda_{k\ell}^{ij}$'s are multiples of p

Recall that the third condition is equivalent to A, B spanning a rank zero or one space over $\mathbb{F}_p$.

[‡]We follow here the convention that, for $e \leq 0$, we have $a \equiv 0 \pmod{p^e}$ for any integer a.

Assume now that A, B span a two-dimensional space of conics over $\mathbb{F}_p$. Then condition (i) occurs if and only if $a_{11} \equiv b_{11} \equiv 0 \pmod{p}$ and the vector $(a_{11}/p, a_{12}, a_{13})$ is a multiple of $(b_{11}/p, b_{12}, b_{13})$ modulo p. By a transformation in $GL_2(\mathbb{Z})$, we may then assume in sum that

$$a_{11} \equiv b_{12} \equiv b_{13} \equiv 0 \pmod{p}, \text{ and } b_{11} \equiv 0 \pmod{p^2}. \tag{4.30}$$

Then we see that $(1,0,0)$ is a double intersection point when A, B are viewed as two conics in $\mathbb{P}^2_{\bar{\mathbb{F}}_p}$. It follows that (A, B) must be in $T_p(1^2 11), T_p(1^2 2), T_p(1^3 1), T_p^{(1)}(1^4)$, or $T_p(1^2 1^2)$.

On the other hand, any element (A, B) of $T_p(1^2 11), T_p(1^2 2), T_p(1^3 1), T_p^{(1)}(1^4)$, or $T_p(1^2 1^2)$ can be brought into the form

$$a_{11} \equiv b_{12} \equiv b_{13} \equiv 0 \pmod{p}, \text{ and } b_{11} \equiv 0 \pmod{p}$$

by sending a double point of intersection of (A, B) in $\mathbb{P}^2_{\bar{\mathbb{F}}_p}$ to $(1,0,0)$, via an element of $SL_3(\mathbb{Z})$, and then using an $GL_2(\mathbb{Z})$ transformation to insure that B becomes a double line through $(1,0,0)$ modulo p. Of all (A, B) in $T_p(1^2 11), T_p(1^2 2), T_p(1^3 1), T_p^{(1)}(1^4)$, or $T_p(1^2 1^2)$ rendered in such a form, a proportion of $1/p$ actually satisfy (4.30). Therefore, if we denote by $U_p(\cdot) \subset V_{\mathbb{Z}}$ the elements of $T_p(\cdot)$ which correspond to rings maximal at p, then $\mu(U_p(1^2 11)) = \frac{p-1}{p}\mu(T_p(1^2 11))$.

One proceeds similarly with $T_p(1^2 1^2)$ and $T_p(2^2)$.

We have proven the following.

Lemma 4.15 *We have*

$$\begin{aligned}
\mu(U_p(1111)) &= (p-1)^4\, p^4\, (p+1)^2\, (p^2+p+1)/24 \\
\mu(U_p(112)) &= (p-1)^4\, p^4\, (p+1)^2\, (p^2+p+1)/4 \\
\mu(U_p(13)) &= (p-1)^4\, p^4\, (p+1)^2\, (p^2+p+1)/3 \\
\mu(U_p(22)) &= (p-1)^4\, p^4\, (p+1)^2\, (p^2+p+1)/8 \\
\mu(U_p(4)) &= (p-1)^4\, p^4\, (p+1)^2\, (p^2+p+1)/4 \\
\mu(U_p(1^2 11)) &= (p-1)^4\, p^3\, (p+1)^2\, (p^2+p+1)/2 \\
\mu(U_p(1^2 2)) &= (p-1)^4\, p^3\, (p+1)^2\, (p^2+p+1)/2 \\
\mu(U_p(1^2 1^2)) &= (p-1)^4\, p^2\, (p+1)^2\, (p^2+p+1)/2 \\
\mu(U_p(2^2)) &= (p-1)^4\, p^2\, (p+1)^2\, (p^2+p+1)/2 \\
\mu(U_p(1^3 1)) &= (p-1)^4\, p^2\, (p+1)^2\, (p^2+p+1) \\
\mu(U_p(1^4)) &= (p-1)^4\, p\ \ (p+1)^2\, (p^2+p+1).
\end{aligned}$$

Let $\mathcal{U}_p$ denote the union of the eleven $U_p(\cdot)$'s in $V_{\mathbb{Z}}$. Then Lemma 4.15 implies that

$$\mu(\mathcal{U}_p) = (p-1)^4\, p\, (p+1)^2\, (p^2+p+1)(p^3+p^2+2p+1). \tag{4.31}$$

Regarding maximality, we have shown:

Theorem 4.16 *Let $(A, B) \in V_{\mathbb{Z}}$. Then $Q(A, B)$ is a maximal ring if and only if $(A, B) \in \mathcal{U}_p$ for all primes p.*

Chapter 5

The density of discriminants of quartic rings and fields

The primary purpose of this chapter is to prove the following theorem.

Theorem 5.1 *Let $N_4(\xi, \eta)$ denote the number of totally real S_4-quartic fields K such that $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$\lim_{X\to\infty} \frac{N_4(0,X)}{X} = \frac{1}{48}\prod_p (1+p^{-2}-p^{-3}-p^{-4}).$$

Three further results are obtained as by-products. First, our methods enable us to count all orders in S_4-quartic fields.

Theorem 5.2 *Let $M_4(\xi, \eta)$ denote the number of quartic orders $\mathcal{O}$ contained in totally real S_4-quartic fields such that $\xi < \mathrm{Disc}(\mathcal{O}) < \eta$. Then*

$$\lim_{X\to\infty} \frac{M_4(0,X)}{X} = \frac{\zeta(2)^2\zeta(3)}{48\,\zeta(5)}.$$

Second, the proof of Theorem 5.1 involves a determination of the densities of various splitting types of primes in S_4-quartic fields. If K is an S_4-quartic field and

K_{24} denotes the Galois closure of K, then the Artin symbol (K_{24}/p) is defined as a conjugacy class in S_4, its values being $\langle e\rangle$, $\langle(12)\rangle$, $\langle(123)\rangle$, $\langle(1234)\rangle$, or $\langle(12)(34)\rangle$, where $\langle x\rangle$ denotes the conjugacy class of x in S_4. It follows from the Cebotarev density theorem that for fixed K and varying p (unramified in K), the values $\langle e\rangle$, $\langle(12)\rangle$, $\langle(123)\rangle$, $\langle(1234)\rangle$, and $\langle(12)(34)\rangle$ occur with relative frequency $1:6:8:6:3$. We prove the following complement to Cebatorev density:

Theorem 5.3 *Let p be a fixed prime, and let K run through the totally real quartic fields in which p does not ramify, the fields being ordered by the size of the discriminants. Then the Artin symbol (K_{24}/p) takes the values $\langle e\rangle$, $\langle(12)\rangle$, $\langle(123)\rangle$, $\langle(1234)\rangle$, and $\langle(12)(34)\rangle$ with relative frequency $1:6:8:6:3$.*

Actually, we do a little more: we determine for each prime p the density of quartic fields K in which p has the various possible ramification types.

Lastly, using the duality between quartic fields and 2-class groups of cubic fields, we obtain the mean value of the size of the 2-class group of totally real cubic fields. More precisely, we prove

Theorem 5.4 *For a totally real cubic field F, let $h_2^*(F)$ denote the size of the 2-class group of F. Then*

$$\lim_{X\to\infty} \frac{\sum_F h_2^*(F)}{\sum_F 1} = 5/4, \tag{5.1}$$

where the sums range over all totally real cubic fields F of discriminant less than X.

It is natural to compare the value $5/4$ obtained in our theorem with the corresponding value predicted by the Cohen-Martinet heuristics (the analogues of the Cohen-Lenstra heuristics for noncyclic, higher degree fields). There has been much recent skepticism surrounding these heuristics (even by Cohen-Martinet themselves; see [7]), since at

the prime $p = 2$ they do not seem to agree with current computational data*. In light of this situation, it is interesting to note that our Theorem 5.4 *agrees exactly* with the (original) prediction of the Cohen-Martinet heuristics [6]. In particular, Theorem 5.4 is a strong indication that, in the language of [6], the prime $p = 2$ is indeed "good", and the fact that Theorem 5.4 does not agree well with existing computations is due only to the extremely slow convergence of the limit (5.1).

The cubic analogues of Theorems 5.1, 5.3, and 5.4 for cubic fields were obtained in the well-known work of Davenport-Heilbronn [11]. Their methods relied heavily on the remarkable discriminant-preserving correspondence between cubic orders and equivalence classes of integral binary cubic forms, established by Delone-Faddeev [12]. It seems, however, that Davenport-Heilbronn were not aware of the work in [12], and derived the same correspondence for maximal orders independently; had they known the general form of the Delone-Faddeev parametrization, it would have been possible for them (using again the results of Davenport [10]) simply to read off also the cubic analogue of Theorem 5.2.†

The key ingredient that allows us to extend the latter results to the quartic case is a parametrization of quartic orders by means of two integral ternary quadratic forms, which we established in Chapter 4. The proofs of Theorems 5.1–5.4 thus reduce to counting integer points in certain fundamental regions. We carry out this counting in a manner similar to that of Davenport [10], although our case is a good deal more involved since the dimension is now 12 instead of 4. The necessary point-counting is

*A computation of all cubic fields of discriminant less than 100000 ([14]) shows that $(\sum_{0<\mathrm{Disc}(F)<100000} h_2^*(F))/(\sum_{0<\mathrm{Disc}(F)<100000} 1)$ equals about 1.08, a good deal less than 5/4!

†We note the result here, since it seems not to have been stated previously in the literature. Let $M_3(\xi, \eta)$ denote the number of cubic orders $\mathcal{O}$ such that $\xi < \mathrm{Disc}(\mathcal{O}) < \eta$. Then

$$\lim_{X\to\infty} \frac{M_3(0,X)}{X} = \pi^2/108,$$

$$\lim_{X\to\infty} \frac{M_3(-X,0)}{X} = \pi^2/12.$$

accomplished in Section 5.1, and forms the bulk of this chapter. This counting result, together with the results of Chapter 4, immediately yields the asymptotic density of discriminants of pairs (Q, R), where Q is an order in a totally real S_4-quartic field and R is a cubic resolvent of Q. Obtaining Theorems 5.1–5.4 from this general density result then requires a simple sieve which we carry out in Section 2.

We remark that the analogous counting results for mixed and totally complex quartic fields should be obtainable by similar techniques. For the purposes of this chapter, though, we concentrate on the totally real case.

5.1 On the class numbers of pairs of ternary quadratic forms

Say a pair (A, B) of integral ternary quadratic forms is *absolutely irreducible* if

- A and B do not have a common zero in $\mathbb{P}^2(\mathbb{Q})$; and
- the binary cubic form $f(x, y) = \mathrm{Det}(Ax - By)$ is irreducible over $\mathbb{Q}$.

We write pairs (A, B) of ternary quadratic forms as pairs of 3×3 symmetric matrices as follows:

$$2 \cdot (A, B) = \left(\begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}, \begin{bmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{bmatrix} \right), \tag{5.2}$$

Thus a pair (A, B) is *integral* if, in this matrix representation, A and B have integer diagonal entries and half-integer off-diagonal entries.

The group $G = GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ acts naturally on the space V of pairs of ternary quadratic forms, and preserves the integral elements $V_{\mathbf{Z}}$. The aim of this section is to count the number of G-equivalence classes of pairs $(A, B) \in V_{\mathbf{Z}}$ having absolute

discriminant at most X. At the moment, we restrict ourselves to counting only the totally real elements $(A, B) \in V_{\mathbb{Z}}$, where (A, B) is said to be *totally real* if it possesses four zeros in $\mathbb{P}^2(\mathbb{R})$. Specifically, we prove the following theorem.

Theorem 5.5 *Let $N(\xi, \eta; V_{\mathbb{Z}})$ denote the number of G-equivalence classes of absolutely irreducible, totally real elements $(A, B) \in V_{\mathbb{Z}}$ satisfying $\xi < \mathrm{Disc}(A, B) < \eta$. Then*

$$\lim_{X \to \infty} \frac{N(0, X; V_{\mathbb{Z}})}{X} = \frac{\zeta(2)^2 \zeta(3)}{48}.$$

Notation. We use ϵ to denote any positive real number. Thus we say "$f(X) = O(X^{1+\epsilon})$" if $f(X) = O(X^{1+\epsilon})$ for any $\epsilon > 0$.

5.1.1 Reduction theory

Let $V_{\mathbb{R}}$ denote the space of pairs of ternary quadratic forms over the reals.

We say an element (A, B) of positive discriminant in $V_{\mathbb{R}}$ is $GL_2(\mathbb{Z})$-*reduced* if the binary cubic covariant

$$f(x, y) = \mathrm{Det}(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3$$

is $GL_2(\mathbb{Z})$-reduced in the sense of Hermite, i.e., if

$$|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd. \tag{5.3}$$

Next, given a pair $(A, B) \in V_{\mathbb{Z}}$, let $Q = Q(A, B)$ be the corresponding quartic ring, and let $\mathcal{Q}$ denote the ternary quadratic form $\mathrm{Tr}(x^2)$ on Q restricted to the hyperplane $\mathrm{Tr}(x) = 0$. Then $\mathcal{Q}$ is an $SL_3(\mathbb{Z})$-covariant of (A, B), and is a positive definite ternary quadratic form for all totally real (A, B). Call a totally real element

(A, B) in $V_{\mathbb{R}}$ $SL_3(\mathbb{Z})$-*reduced* if this quadratic covariant $\mathcal{Q} = (q_{ij})$ is $SL_3(\mathbb{Z})$-reduced in the sense of Minkowskii (see, e.g., Cassels [2]), i.e.,

$$\begin{gathered} 0 < q_{11} \leq q_{22} \leq q_{33}, \\ |q_{12}| \leq q_{11}, \ |q_{13}| \leq q_{11}, \ |q_{23}| \leq q_{22} \\ |q_{12} \pm q_{13} \pm q_{23}| \leq q_{22}. \end{gathered} \tag{5.4}$$

(The coefficients of the form $\mathcal{Q} = (q_{ij})$ are given in the Appendix.)

We say a totally real element (A, B) in $V_{\mathbb{R}}$ is *G-reduced* (or simply *reduced*) if it is both $GL_2(\mathbb{Z})$-reduced and $SL_3(\mathbb{Z})$-reduced. Let $\mathcal{F}$ denote the region in $V_{\mathbb{R}}$ consisting of totally real reduced elements (A, B), and let $\mathcal{F}_X$ denote the subset of $\mathcal{F}_X$ consisting of those elements having discriminant less than X. Finally, let $\mathcal{F}_X(\mathbb{Z})$ denote the set of integer points in $\mathcal{F}_X$. Our task is to understand the number of points in $\mathcal{F}_X(\mathbb{Z})$.

We note that $\mathcal{F}_X$ is contained in the image of a standard Siegel set, i.e.,

$$\mathcal{F}_X \subset X^{\frac{1}{12}} \cdot \bar{N}' A' K v$$

for some fixed $v \in V_{\mathbb{R}}$; here

$$K = \{\text{orthogonal transformations in } G_{\mathbb{R}}\}; \tag{5.5}$$

$$A' = \{a(s,t) : 0 < |s_1| \leq c|s_2|, \ 0 < |t_1| \leq c|t_2| \leq c|t_3|\}, \tag{5.6}$$

$$\text{where } a(s,t) = \left(\begin{pmatrix} s_1 & & \\ & s_2 & \end{pmatrix}, \begin{pmatrix} t_1 & & \\ & t_2 & \\ & & t_3 \end{pmatrix} \right); \tag{5.7}$$

$$\bar{N}' = \{n(u) : |u|, |u_1|, |u_2|, |u_3| \leq c\}, \tag{5.8}$$

$$\text{where } n(u) = \left(\begin{pmatrix} 1 & u \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & u_1 & u_2 \\ & 1 & u_3 \\ & & 1 \end{pmatrix} \right), \tag{5.9}$$

and c is an absolute constant.

5.1.2 Some further notation

Let $R_1(y,z)$, $R_2(x,z)$, $R_3(x,y)$ denote the resultants of the two quadratic forms $A(x,y,z)$ and $B(x,y,z)$ with respect to the variables x,y,z respectively. (The R_i's are thus binary quartic forms.)

Next, denote by $A_{12}(x,y)$, $A_{13}(x,z)$, $A_{23}(y,z)$ the binary quadratic forms obtained from $A(x,y,z)$ by setting z,y,x equal to zero respectively. Define $B_{12}(x,y)$, $B_{13}(x,z)$, and $B_{23}(y,z)$ analogously.

Associate with these pairs (A_{12},B_{12}), (A_{13},B_{13}), (A_{23},B_{23}) of binary quadratic forms their discriminant invariants D_{12}, D_{13}, D_{23} as defined in Chapter 2. Equivalently, D_{ij} is the resultant of the binary forms $A_{ij}(x,y)$ and $B_{ij}(x,y)$ with respect to y, divided by x^4. The discriminants D_{ij} are forms of degree four in the entries of (A,B). We note also that D_{12} is the coefficient of x^4 in $R_2(x,z)$ and of y^4 in $R_1(y,z)$, with the analogous interpretations for D_{13} and D_{23}.

5.1.3 Preliminary estimates

We begin with some estimates that must be satisfied by the coefficients of any reduced element $(A,B) \in V_{\mathbb{R}}$.

Lemma 5.6 *Let $(A,B) \in \mathcal{F}_X$ have entries given by (5.2), and let S be a multiset consisting solely of elements of the form a_{ij} or b_{ij}. Let m denote the number of a's which occur in S, and let $n = |S| - m$ denote the number of b's; let i, j, and $k = 2|S| - i - j$ denote the number of indices in S equal to 1, 2, and 3 respectively. If $m \geq n$, $2i \geq j + k$, and $i + j \geq k$, then*

$$\prod_{s \in S} s = O(X^{|S|/12}).$$

Proof: As noted in Subsection 5.1.1, $\mathcal{F}_X \subset X^{\frac{1}{12}} \cdot \bar{N}'A'Kv$ for some fixed vector $v \in V_{\mathbb{R}}$, where $\bar{N}'$ and A' are as in (5.5). Given S as in the lemma, it is clear that

the value of $f = \prod_{s \in S} s$ is bounded on Kv, since K is compact. Next, the values of f on $A'Kv$ are simply $s_1^m s_2^n t_1^i t_2^j t_3^k$ times the values of f on Kv. If $m \geq n$, $2i \geq j + k$, and $i + j \geq k$, then it is clear that $s_1^m s_2^n t_1^i t_2^j t_3^k$ is absolutely bounded, and hence the values of f on $A'Kv$ are also bounded. Finally, $\bar{N}'$ is compact, and it acts by upper triangular transformations; thus f also takes bounded values on $\bar{N}'A'Kv$, and so the values of f on $X^{\frac{1}{12}} \cdot \bar{N}'A'Kv$ are at most $O(X^{|S|/12})$ in size. This is the desired conclusion. □

Lemma 5.6 gives those inequalities which follow immediately from the fact that $\mathcal{F}$ is contained in a Siegel set. When we wish to use the inequalites (5.3) and (5.4) more precisely, the following two lemmas will be useful. The first of these is due to Davenport [9]. Given a region $\mathcal{R} \subset \mathbb{R}^n$, let $\mathrm{Vol}(\mathcal{R})$ denote its Euclidean volume.

Lemma 5.7 *The number of integer points in a compact region $\mathcal{R} \subset \mathbb{R}^n$ enclosed by a bounded number of algebraic surfaces of bounded degree is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\bar{\mathcal{R}}), 1\}),$$

where $\mathrm{Vol}(\bar{\mathcal{R}})$ denotes the maximum of the volumes of the projections of $\mathcal{R}$ onto smaller-dimensional coordinate hyperplanes.

The second lemma states that in controlling certain one-variable inequalities, it suffices to consider only the leading term.

Lemma 5.8 *Let $P(x)$ be a polynomial of degree n over $\mathbb{R}$ in one variable, with leading term $c_0 x^n$. Let X be any large real number. Then there exists a subset $U \subset \mathbb{R}$, consisting of at most n intervals and of total length at most $n(|c_0|X|)^{1/n}$, such that if $|P(\alpha)| < X$ $(\alpha \in \mathbb{R})$, then $\alpha \in U$.*

Proof: Write $P(x)$ as a product over its roots r_i (taken with multiplicity):

$$P(x) = c_0 \prod_{i=1}^{n} (x - r_i).$$

Set

$$U = \{\alpha \in \mathbb{R} : |\alpha - r_i|^n < X/c_0\}.$$

Then U satisfies the desired property. □

5.1.4 Estimates on reducible pairs (A, B)

Lemma 5.9 *The number of absolutely irreducible elements $(A, B) \in \mathcal{F}_X(\mathbb{Z})$ with $a_{11} = 0$ is $O(X^{191/192+\epsilon})$.*

Therefore, for the purposes of Theorem 5.5, we may assume that $a_{11} \neq 0$.

(We postpone the proof of Lemma 5.9 to Subsection 5.1.6.)

Lemma 5.10 *The number of $(A, B) \in \mathcal{F}_X(\mathbb{Z})$ with $a_{11} \neq 0$ and $a \neq 0$, for which $f(x, y) = \mathrm{Det}(Ax - By)$ is reducible, is $O(X^{101/108+\epsilon})$.*

Proof: Any cubic ring $R = R(f)$ of discriminant n such that $f(x, y)$ is a reducible cubic form must sit in a unique cubic $\mathbb{Q}$-algebra $K = \mathbb{Q} \oplus F$, where F is a certain quadratic $\mathbb{Q}$-algebra (indeed, F depends only on the squarefree part of n). Write $\mathrm{Disc}(R) = k^2\mathrm{Disc}(K)$. Then the number of quartic $\mathbb{Q}$-algebras L having discriminant dividing $\mathrm{Disc}(R) = k^2\mathrm{Disc}(K)$, and such that the cubic resolvent of L is K, is $O(h_2^*(K)\mathrm{Disc}(R)^\epsilon)$ by the work of Baily [1].[‡] Since K is of the form $\mathbb{Q} \oplus F$, where F is a quadratic $\mathbb{Q}$-algebra, we have $h_2^*(K) = O(\mathrm{Disc}(K)^\epsilon)$ by genus theory. Hence

[‡]Although Baily states all results for "cubic fields", it is clear that his arguments hold also when every occurrence of "field" is replaced by "étale $\mathbb{Q}$-algebra".

the total number of possibilities for the quartic $\mathbb{Q}$-algebra L, given $R = R(f)$, is $O(\mathrm{Disc}(R)^\epsilon)$.

Now any quartic ring Q such that the cubic resolvent ring of Q is R must be an order in such an L, and the index of this order in $\mathcal{O}_L$ (the ring of integers of L) must divide k, since $\mathrm{Disc}(Q) = \mathrm{Disc}(R) = k^2\mathrm{Disc}(K) \leq k^2\mathrm{Disc}(L)$. In particular, for a fixed choice of L the number of $Q \subseteq L$ with $R^{res}(Q) = R(f)$ is at most the number of orders of index k in $\mathcal{O}_L$. For any integer $k > 0$, let $\mathrm{EP}(k)$ denote the product of all factors p^e occurring in the prime power decomposition of k such that $e \geq 8$. Then it follows from a result of Nakagawa [19, Theorem 1] that the number of orders of index k in an étale quartic $\mathbb{Q}$-algebra L is at most $O(\mathrm{EP}(k)^{1/2+\epsilon})$, independent of L.

Let $s = 20/27$. We divide the set S of reducible cubic forms $f(x, y)$ into two sets: S_1, the set of all reducible cubic forms f with $\mathrm{EP}(\mathrm{Disc}(f)) \geq \mathrm{Disc}(f)^s$, and S_2, the set of all reducible cubic forms f with with $\mathrm{EP}(\mathrm{Disc}(f)) < \mathrm{Disc}(f)^s$.

We treat first the number of $(A, B) \in \mathcal{F}_X$ with $f(x, y) \in S_1$. It is a standard fact that the number of positive integers n such that $EP(n) > n^\delta$ is $O(X^{1-\frac{7}{8}\delta+\epsilon})$. Furthermore, it is easy to see (see e.g., Datskovsky-Wright [8], Nakagawa [20]) that the number of orders of a given index k in the maximal order of a cubic $\mathbb{Q}$-algebra K is at most $O(k^{1/3+\epsilon})$, independent of K; it follows that the number of reducible $f(x, y)$ with a given discriminant n is at most $O(n^{1/3+\epsilon})$. Hence the total number of reducible cubic forms $f \in S_1$ of discriminant less than X is at most

$$O(X^{1-\frac{7}{8}\delta+\epsilon} \cdot X^{\frac{1}{3}}).$$

Finally, given an $f \in S_1$ with $0 < \mathrm{Disc}(f) < X$, the number of quartic $\mathbb{Q}$-algebras L of discriminant at most $\mathrm{Disc}(R(f))$, such that the cubic resolvent of L is $K = R(f) \otimes \mathbb{Q}$, is $O(\mathrm{Disc}(f)^\epsilon) = O(X^\epsilon)$; and the maximal number of orders Q of index k in $\mathcal{O}_L$ is at most $O(\mathrm{EP}(k)^{1/2+\epsilon}) = O(X^{1/4+\epsilon})$. We conclude that the total number of $(A, B) \in \mathcal{F}_X$

with $f(x,y) \in S_1$ is at most

$$O(X^{1-\frac{7}{8}\delta+\epsilon} \cdot X^{\frac{1}{3}} \cdot X^{\epsilon} \cdot X^{1/4+\epsilon}) = O(X^{101/108+\epsilon}).$$

To treat the number of $(A,B) \in \mathcal{F}_X$ with $f(x,y) \in S_2$, we may invoke a result of Davenport [10, Lemma 3], which states that the total number of reduced binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ with $0 < \text{Disc}(f) < X$ and $a \neq 0$ is at most $O(X^{3/4+\epsilon})$. In particular, the total number of cubic forms $f \in S_2$ is at most $O(X^{3/4+\epsilon})$. Again, given an $f \in S_2$, the number of quartic $\mathbb{Q}$-algebras L having discriminant at most $\text{Disc}(R(f))$, such that the cubic resolvent of L is $K = R(f) \otimes \mathbb{Q}$, is $O(\text{Disc}(f)^{\epsilon}) = O(X^{\epsilon})$; and the maximal number of orders Q of index k in $\mathcal{O}_L$ is at most $O(\text{EP}(k)^{1/2+\epsilon}) = O(k^{\frac{1}{2}\delta+\epsilon}) = O(X^{\frac{1}{4}s+\epsilon})$. Therefore, the total number of $(A,B) \in \mathcal{F}_X$ with $f(x,y) \in S_2$ is at most

$$O(X^{\frac{3}{4}+\epsilon} X^{\frac{1}{4}\delta+\epsilon}) = O(X^{101/108+\epsilon}),$$

as desired. □

Let T denote the set of twelve variables $\{a_{ij}, b_{ij}\}$. Note that $a_{11} \neq 0$ together with the estimate $a_{11}^2 t = O(X^{1/3})$ for $t \in T$ (Lemma 5.6) shows that

$$t = O(X^{1/3})$$

for all $t \in T$.

Lemma 5.11 *The number of $(A,B) \in \mathcal{F}_X(\mathbb{Z})$ with $a_{11} \neq 0$ and $a \neq 0$ such that A and B have a common zero in $\mathbb{P}^2(\mathbb{Q})$ is $O(X^{47/48+\epsilon})$.*

Proof: Let (A,B) be an element in $\mathcal{F}_Z(\mathbb{Z})$ having a common rational zero $(r,s,t) \in \mathbb{P}^2(\mathbb{Q})$, where r,s,t are integers having no common factor. (If there is choice, we pick

as many of the r, s, t to be zero as possible.) Write $r = (r,s)(r,t)r_0$, $s = (r,s)(s,t)s_0$, $t = (r,t)(s,t)t_0$ (set $(x,0) = (0,x) = 1$ for convenience).

We consider first the case where $rst \neq 0$ (so A and B have no common rational point in $\mathbb{P}^2$ with a coordinate equal to zero.) To bound the number of possibilities for (A,B) in this case, we examine the discriminants D_{12}, D_{13}, D_{23}.

If any of these discriminants, say D_{12}, is equal to zero, then the corresponding pair of quadratic forms (A_{12}, B_{12}) must have a common zero (r', s') in $\mathbb{P}_1$. By assumption, this zero cannot be rational, for otherwise $(r', s', 0)$ would be a common rational zero of (A,B) having a zero coordinate. Therefore, if $D_{12} = 0$, then A_{12}, B_{12} possess the same pair of conjugate zeros (defined over some quadratic extension of $\mathbb{Q}$), and thus A_{12} and B_{12} are scalar multiples of each other. Pick $u, v \in \mathbb{Z}$ such that $uA_{12} - vB_{12} = 0$. Then clearly $f(u,v) = \mathrm{Det}(uA - vB) = 0$, so that $f(x,y)$ is reducible over $\mathbb{Q}$. Such elements (A,B) with $f(x,y)$ reducible have already been handled, by Lemma 5.10.

We may therefore assume that $D_{12} \neq 0$, $D_{13} \neq 0$, and $D_{23} \neq 0$. If all a_{ij}, b_{ij} aside from possibly b_{23} are nonzero, then the inequality (Lemma 5.6)

$$\prod_{t \in T \setminus \{b_{23}\}} t = O(X^{11/12}) \tag{5.10}$$

implies that the number of nonzero choices for the variables in $T \setminus \{b_{23}\}$ is $O(X^{11/12+\epsilon})$. If some elements of $T \setminus b_{23}$ are equal to 0, we may replace those variables in (5.10) by a_{11}, and the inequality remains true by Lemma 5.6. Thus the number of choices for the remaining nonzero variables in T is still $O(X^{11/12+\epsilon})$.

Once the variables in $T \setminus \{b_{23}\}$ have been chosen, they also determine the quantities D_{12} and D_{13}, which by assumption are nonzero. Since the coefficients of x^4 in $R_3(x,y)$ and $R_2(x,z)$ are D_{12} and D_{13} respectively, and $R_3(r,s) = R_2(r,t) = 0$, it follows that t_0 and s_0 divide D_{12} and D_{13} respectively. Thus the number of possibilities for s_0 and t_0 are bounded by the number of factors of D_{12} and D_{13} respectively. Since

$D_{12}D_{13} = O(X^{2/3})$ by Lemma 5.6, the number of possibilities for s_0, t_0 is at most $O(X^\epsilon)$. Now r divides (the nonzero quantity) $A_{23}(s,t)$, and as $A_{23}(s,t)$ is clearly at most $O(X^2)$ in absolute value, the number of choices for r is also at most $O(X^\epsilon)$. The factors (r,s), (r,t), and (s,t) are also determined up to $O(X^\epsilon)$ choices, as they are factors of r, r, and a_{11} respectively. Finally, since $B(r,s,t) = 0$, b_{23} is uniquely determined by $T\backslash\{b_{23}\}$, r, s, and t. Hence the number of choices for b_{23}, given $T\backslash b_{23}$, is at most $O(X^\epsilon)$, and so the total number of choices for T is $O(X^{11/12+\epsilon})$.

We consider next the cases where exactly one of r, s, t is equal to zero (so A and B do not have a common rational point in $\mathbb{P}^2$ with two coordinates equal to zero).

If $r = 0$ and $st \neq 0$, then

$$A_{23}(s,t) = B_{23}(s,t) = 0. \tag{5.11}$$

We can assume that at least one of a_{22}, b_{22} (say b_{22}) and at least one of a_{33}, b_{33} (say b_{33}) is nonzero, for otherwise $(0,1,0)$ or $(0,0,1)$ would be a rational zero of (A,B) with two zero coordinates. Since

$$\prod_{t \in T\backslash\{a_{23},b_{23}\}} t = O(X^{10/12}) \tag{5.12}$$

(where as before zero variables are replaced by a_{11}), we see that the number of choices for $T \setminus \{a_{23}, b_{23}\}$ is bounded by $O(X^{10/12+\epsilon})$. Once these choices are made, (5.11) implies that s divides b_{33} and t divides b_{22}; hence the number of possibilities for s and t is bounded by the number of factors of b_{33} and b_{22} respectively, so s and t can take at most $O(X^\epsilon)$ values (since b_{22} and b_{33} are both $O(X^{1/3})$). The values of a_{23} and b_{23} are then determined by $T \setminus \{a_{23}, b_{23}\}$, r, s, and t. Thus the total number of possibilities for (A,B) in this case is $O(X^{10/12+\epsilon})$.

The case $s = 0$, $rt \neq 0$ is handled similarly; the equation (5.12) is simply changed to

$$a_{11} \prod_{t \in T \setminus \{a_{13}, b_{13}\}} t = O(X^{11/12}), \tag{5.13}$$

and we find in conclusion that there are at most $O(X^{11/12+\epsilon})$ choices for (A, B) in this case.

The case $t = 0$, $rs \neq 0$ is a bit more difficult. Proceeding in the same manner, we find a_{12} and b_{12} are determined up to $O(X^{\epsilon})$ possibilities once a_{11}, a_{22}, b_{11}, and b_{22} are fixed. However, equation (5.13) now becomes

$$a_{11}^2 \prod_{t \in T \setminus \{a_{12}, b_{12}\}} t = O(X^{12/12}), \tag{5.14}$$

which does not yield a satisfactory estimate. Thus we must instead appeal to the inequalities (5.4).

If $a_{13} = 0$, then (5.14) becomes

$$a_{11}^2 \prod_{t \in T \setminus \{a_{12}, a_{13}, b_{12}\}} t = O(X^{11/12}), \tag{5.15}$$

and again the number of choices for the remaining variables in T is at most $O(X^{11/12+\epsilon})$. We therefore assume that $a_{13} \neq 0$, and examine the coefficients q_{11} and q_{13} of Q. Since by (5.4), $|q_{13}| < q_{11}$, and by Lemma 5.6,

$$|a_{11}|^{5/2} a_{13} q_{11} \prod_{T \setminus \{a_{13}, b_{23}, a_{12}, b_{12}\}} t^2 = O(X^{23.5/12}) \tag{5.16}$$

(where again all variables equal to zero are replaced with a_{11}), we conclude

$$|a_{11}|^{5/2} a_{13} q_{13} \prod_{T \setminus \{a_{13}, b_{23}, a_{12}, b_{12}\}} t^2 = O(X^{23.5/12}). \tag{5.17}$$

Now q_{13}, when viewed as a polynomial in b_{23}, has leading term $a_{11} a_{13} b_{23}^2$. It follows from Lemma 5.8 that, once all variables in $T \setminus \{b_{23}\}$ are fixed (we recall a_{12} and b_{12} are determined by $a_{11}, a_{13}, b_{11}, b_{13}$), the number of possibilities for b_{23} is at most

$$O\left(X^{23.5/24} / (a_{11}^{7/4} \prod_{T \setminus \{a_{12}, b_{12}\}}) \right).$$

Summing the latter expression over the variables in $T \setminus \{a_{12}, b_{12}\}$, we see that (A, B) can take at most $O(X^{23.5/24+\epsilon})$ values in this case.

Finally, we consider the cases where exactly two of r, s, t are equal to 0. This condition implies that either $a_{11} = b_{11} = 0$ (which does not occur by hypothesis), $a_{22} = b_{22} = 0$, or $a_{33} = b_{33} = 0$.

If $a_{33} = b_{33} = 0$, then the inequality

$$\prod_{t \in T \setminus \{a_{33}, b_{33}\}} t < O(X^{10/12}) \tag{5.18}$$

(again with variables equal to zero replaced by a_{11}) shows that there are at most $O(X^{10/12+\epsilon})$ possibilities for the variables in T.

Finally, suppose $a_{22} = b_{22} = 0$. Again, if $a_{13} = 0$, then

$$a_{11}^2 \prod_{t \in T \setminus \{a_{13}, a_{22}, b_{22}\}} t = O(X^{11/12}) \tag{5.19}$$

(Lemma 5.6) shows that (A, B) can take at most $O(X^{11/12+\epsilon})$ values. Thus we assume $a_{13} \neq 0$, and again consider $|q_{13}| < q_{11}$. The same reasoning as in (5.16) and

(5.17) (but with $\{a_{22}, b_{22}\}$ and $\{a_{12}, b_{12}\}$ interchanged) shows that there are at most $O(X^{23.5/24+\epsilon})$ values for (A, B) in this case as well. □

5.1.5 Cutting the cusps

Let $\delta = 1/192$.

Lemma 5.12 *The number of absolutely irreducible* $(A, B) \in \mathcal{F}_X(\mathbb{Z})$ *with* $0 < a_{11} < X^\delta$ *is* $O(X^{\frac{49}{50}+\frac{6}{25}\delta+\epsilon})$.

Proof: Let us consider first the case where $a_{13} = 0$. If, in addition,

$$a_{22}b_{33} - 2a_{23}b_{23} - a_{33}b_{22} = 0, \tag{5.20}$$

then since at least one of a_{22}, a_{23}, a_{33} must be nonzero ($\mathrm{Det}(A) \neq 0$), one of b_{22}, b_{23}, b_{33}, say b_{22}, is completely determined by the other variables. Lemma 5.6 then implies

$$a_{11}^{1/2} \prod_{t \in T \setminus \{a_{13}, b_{22}} t = O(X^{10.5/12}),$$

and therefore the number of absolutely irreducible $(A, B) \in \mathcal{F}_X$ satisfying (5.20) and $a_{13} = 0$ is only $O(X^{10.5/12+\epsilon})$. We may therefore assume $\lambda = a_{22}b_{33} - 2a_{23}b_{23} - a_{33}b_{22} = 0 \neq 0$. Similarly, we may also assume $\lambda' = -a_{11}b_{33} + 2a_{13}b_{13} - a_{33}b_{11} \neq 0$ (otherwise b_{33} is determined by the other variables) and $\lambda'' = -a_{11}b_{22} + 2a_{12}b_{12} - a_{22}b_{11} \neq 0$ (otherwise b_{22} is determined by the other variables).

Now the leading coefficient of $bc - 9ad$, as a polynomial in b_{11}, b_{22}, b_{33}, b_{12}, b_{13}, or b_{23} respectively is given by $(a_{23}^2 - a_{22}a_{33})\lambda$, $(a_{13}^2 - a_{11}a_{33})\lambda'$, $(a_{12}^2 - a_{11}a_{22})\lambda''$, $2a_{33}(a_{13}a_{23} - a_{12}a_{33})$, $2a_{22}(a_{12}a_{23} - a_{13}a_{22})$, or $2a_{11}(a_{11}a_{23} - a_{12}a_{13})$ respectively. If $\mathrm{Det}(A) \neq 0$, then at least one of these leading coefficients must be nonzero; let us assume, say, that the leading coefficient $(a_{23}^2 - a_{22}a_{33})\lambda$ is nonzero (the other cases can be dealt with analogously).

From Lemma 5.6, we have

$$a_{11}^3 a_{12}^2 a_{22} a_{23} a_{33} b_{12}^2 b_{13}^2 b_{22}^2 b_{23} b_{33}^2 \ (b^2 - 3ac) = O(X^{23/12}).$$

Since $|bc - 9ad| < b^2 - 3ac$,

$$a_{11}^3 a_{12}^2 a_{22} a_{23} a_{33} b_{12}^2 b_{13}^2 b_{22}^2 b_{23} b_{33}^2 \ (bc - 9ad) = O(X^{23/12}).$$

Since the leading coefficient of $(bc - 9ad)$ as a polynomial in b_{11} is $(a_{23}^2 - a_{22}a_{33})\lambda b_{11}^2$, it follows from Lemma 5.8 that b_{11} can take at most

$$O(X^{11.5/12}/(a_{11}^{3/2} a_{12} a_{22}^{1/2} a_{23}^{1/2} a_{33}^{1/2} b_{12} b_{13} b_{22} b_{23}^{1/2} b_{33} \ (a_{23}^2 - a_{22}a_{33})^{1/2} \lambda^{1/2})) \qquad (5.21)$$

values when all other variables are held fixed. Summing (5.21) over the variables b_{23}, a_{33}, and then over the remaining variables yields

$$O(X^{11.5/12+\epsilon});$$

thus, the number of absolutely irreducible $(A, B) \in \mathcal{F}_X$ with $a_{11} \neq 0$ and $a_{13} = 0$ is $O(X^{23/24})$.

The identical arguments show that the number of absolutely irreducible $(A, B) \in \mathcal{F}_X$ with $a_{11} \neq 0$ and $a_{23} = a_{12}a_{13}/a_{11}$ is $O(X^{23/24})$. Therefore, to prove the theorem, we may assume $a_{13} \neq 0$ and $a_{11}a_{23} - a_{12}a_{13} \neq 0$.

By Lemma 5.6, we know

$$a_{11}^8 a_{13}^{14} a_{12}^{22} \ q_{11}^8 (b^2 - 3ac) \prod_{t \in T \setminus \{a_{11}, a_{12}, a_{13}, b_{23}\}} t^{25} = O(X^{294/12}).$$

The inequality $|q_{13}| < q_{11}$ and $|bc - 9ad| \leq b^2 - 3ac$ then implies

$$a_{11}^8 a_{13}^{14} a_{12}^{22}\ q_{13}^8 (bc - 9ad) \prod_{t \in T \setminus \{a_{11}, a_{12}, a_{13}, b_{23}\}} t^{25} = O(X^{294/12}). \tag{5.22}$$

The leading term of $q_{13}^8(bc - 9ad)$, viewed as a polynomial in b_{23}, is $a_{11}^{11} a_{13}^8 (a_{11}a_{23} - a_{12}a_{13})^3 b_{23}^{25}$. Hence by Lemma 5.8, if all other variables are held fixed, b_{23} can take at most

$$O\left(X^{49/50} / (a_{11}^{19/25} a_{12}^{22/25} a_{13}^{22/25} (a_{11}a_{23} - a_{12}a_{13})^{3/25} \prod_{t \in T \setminus \{a_{11}, a_{12}, a_{13}, b_{23}\}} t) \right) \tag{5.23}$$

values. Summing the latter over a_{13}, and then over the remaining variables in $T \setminus \{a_{11}, a_{13}, b_{23}\}$, we obtain

$$O(X^{49/50+\epsilon} / a_{11}^{19/25}).$$

Finally, summing over a_{11} $(1 \leq a_{11} \leq X^{\delta})$, we get

$$O(X^{\frac{49}{50} + \frac{6}{25}\delta + \epsilon})$$

as desired. □

Lemma 5.13 *The number of elements $(A, B) \in \mathcal{F}_X(\mathbb{Z})$ with $|a_{11}| > X^{\delta}$ is*

$$\mathrm{Vol}(\mathcal{F}_1) \cdot X + o(X),$$

where $\mathrm{Vol}(\mathcal{F}_X)$ denotes the Euclidean volume of the region $\mathcal{F}_X$.

Proof: Let $\mathcal{F}_X'$ denote the region $\mathcal{F}_X \cap \{|a_{11}| > X^{\delta}\}$. The region $\mathcal{F}_X'$ is bounded; indeed, $a_{11} > X^{\delta}$ and $a_{11}^3 t = O(X^{1/3})$ implies $t = O(X^{1/3 - 3\delta})$ for all $t \in T$. Further-

more, the boundary of $\mathcal{F}'_X$ consists of a bounded number of algebraic surfaces. Thus the number of integer points in $\mathcal{F}'_X$ is

$$\mathrm{Vol}(\mathcal{F}'_X) + O(\bar{V}_X) \tag{5.24}$$

where $\bar{V}_X$ denotes the greatest m-dimensional volume of a projection of $\mathcal{F}'_X$ onto any of the m-dimensional coordinate hyperplanes ($1 \leq m \leq 11$).

Let T' be any proper subset of T, and consider the projection of $\mathcal{F}'_X$ onto the coordinate hyperplane $H_{T'}$ given by

$$H_{T'} = \{t = 0 : t \in T \setminus T'\}.$$

We know by Lemma 5.6 that for $(A, B) \in \mathcal{F}'_X$,

$$a_{11}^{12-|T'|} \left| \prod_{T'} t \right| < C_1 X$$

for some constant C_1. Since $a_{11} > X^\delta$, and $12 - |T'| \geq 1$, it follows that

$$\left| \prod_{t \in T'} t \right| < C_1 X^{1-\delta}. \tag{5.25}$$

Furthermore, we have seen that $|a_{11}| > X^\delta$ implies that for any $t \in T'$,

$$|t| < C_2 X^{1/3} \tag{5.26}$$

for some constant C_2. Thus the projection of $\mathcal{F}'_X$ onto $H_{T'}$ is contained in the $|T'|$-dimensional region defined by (5.25) and (5.26). This region is seen to have volume at most

$$O(X^{1-\delta+\epsilon}),$$

for any proper subset $T' \subset T$.

Therefore, (5.24) implies that the number of integer points in $\mathcal{F}'_X$ is given by

$$\mathrm{Vol}(\mathcal{F}'_X) + o(X). \tag{5.27}$$

By Lemma 5.12, this also gives the number of integer points in $\mathcal{F}_X$.

Finally, it follows from homogeneity considerations that

$$\mathrm{Vol}(\mathcal{F}_X) = \mathrm{Vol}(\mathcal{F}_1) \cdot X,$$

and that

$$\mathrm{Vol}(\mathcal{F}'_X) = \mathrm{Vol}(\mathcal{F}_X) + o(X).$$

This proves the lemma. □

5.1.6 Proof of Lemma 5.9

We may divide the proof into two cases, namely the case where $a_{11} = 0$, $a_{12} \neq 0$, and the case where $a_{11} = a_{12} = 0$. Of these, the second is by far the more difficult. Since the first case can be treated in a similar (and much easier) fashion, we proceed directly to the second case and assume $a_{11} = a_{12} = 0$. This is the worst case scenario, since absolute irreducibility implies that a_{13}, a_{22}, and b_{11} must then be nonzero. In particular, all variables in T remain bounded by some constant power of X; for example, the estimate

$$|a^{1/3} a_{22} b_{11} b_{33}| = O(X^{1/3}) \tag{5.28}$$

shows that b_{33} is bounded by $O(X^{1/3})$.

We begin with a simple argument that yields $O(X^{1+\epsilon})$ for the number of possibilities for (A, B) of this type. First, we observe that if $a_{11} = a_{12} = 0$, then q_{12} does not depend on b_{33}. By (5.4) and Lemma 5.6,

$$|q_{12}a_{23}b_{23}| \leq |q_{11}a_{23}b_{23}| = O(X^{6/12}).$$

Since the leading term of $q_{12}a_{23}b_{23}$ as a polynomial in b_{13} is $-a_{13}a_{23}a_{22}b_{12}b_{23}b_{13}$, it follows that the number of choices for b_{13}, once all variables outside b_{13} and b_{33} have been fixed, is

$$O(X^{\frac{1}{2}}/(a_{13}a_{22}b_{12}a_{23}b_{23})). \tag{5.29}$$

Similarly, by (5.4) and Lemma 5.6 again,

$$|q_{13}a_{33}b_{22}| \leq |q_{11}a_{33}b_{22}| = O(X^{6/12});$$

since the leading coefficient of $q_{13}a_{33}b_{22}$ as a polynomial in b_{33} is $2a_{13}a_{22}b_{11}a_{33}b_{22}b_{33}$, the number of choices for b_{33} once b_{13} has also been fixed is

$$O(X^{\frac{1}{2}}/(a_{13}a_{22}b_{11}a_{33}b_{22})). \tag{5.30}$$

Multiplying (5.29) and (5.30), we see that the total number of choices for b_{13} and b_{33}, once all other variables have been fixed, is

$$O(X/(a_{13}^2a_{22}^2a_{23}a_{33}b_{11}b_{12}b_{22}b_{23})). \tag{5.31}$$

Summing (5.31) over all variables outside b_{13} and b_{33} yields $O(X^{1+\epsilon})$.

Note that if $|a_{13}a_{22}| \geq X^{\delta}$ then the number of possibilities for $(A, B) \in \mathcal{F}_X(\mathbb{Z})$ is then $O(X^{1-\delta+\epsilon})$. Hence we may assume that a_{13} and a_{22} are small, i.e., $|a_{13}a_{22}| < X^{\delta}$.

Similarly, suppose $a_{23}b_{23}$ and $a_{33}b_{22}$ differ by a factor of more than X^{δ}. Without loss of generality, assume $a_{23}b_{23} \geq a_{33}b_{22} \cdot X^{\delta}$. Then applying the above argument using the estimate $q_{13}a_{23}b_{23} = O(X^{6/12})$ (instead of $q_{13}a_{33}b_{22} = O(X^{6/12})$) shows that the number of choices for b_{13} and b_{33}, once all other variables have been fixed, is

$$O(X/(a_{13}^2 a_{22}^2 a_{23}^2 b_{11} b_{12} b_{23}^2)) = O(X^{1-\delta}/(a_{13}^2 a_{22}^2 a_{23} a_{33} b_{11} b_{12} b_{22} b_{23})); \tag{5.32}$$

summing the latter over all variables outside b_{13} and b_{33} yields $O(X^{1-\delta+\epsilon})$. Hence we may assume that $a_{23}b_{23}$ and $a_{33}b_{22}$ are close to each other within a factor of X^{δ}.

Let us suppose now that b_{13} is also small, say $|b_{13}| < X^{1/48}$. An upper bound for the number of choices for b_{33}, when all other variables have been fixed, is given by (5.30). In addition, by Lemma 5.6,

$$|a^{1/3} b_{11}^{1/2} a_{13} a_{23} b_{12} b_{23}| = O(X^{5.5/12}). \tag{5.33}$$

This shows that (5.30) is less than

$$O(X^{11.5/12}/(a^{1/3} a_{13}^2 a_{22} a_{23} a_{33} b_{11}^{3/2} b_{12} b_{22} b_{23})).$$

Summing the above over all variables in $T \setminus \{b_{33}\}$ yields $O(X^{11.5/12+\epsilon} \cdot X^{1/48}) = O(X^{47/48+\epsilon})$. Thus it suffices to assume that $|b_{13}| > X^{1/48}$.

Almost the identical reasoning (using the inequality $a_{23}b_{23}q_{13} = O(X^{8/12})$ instead of $a_{33}b_{22}q_{13} = O(X^{8/12})$) shows that the number of (A, B) with $|b_{22}| < X^{1/48}$ is also $O(X^{47/48+\epsilon})$. Hence we may assume in addition that $|b_{22}| > X^{1/48}$.

Next, let

$$\beta = |b_{11} b_{12} b_{13} b_{22} b_{23} b_{33}|^{1/6},$$

where nonzero variables are replaced by b_{11} to assure $\beta \neq 0$. Suppose $|\beta| < X^{1/12+\delta/2}$. Then the total number of choices for B is $O(X^{6/12+3\delta+\epsilon})$. On the other hand, by Lemma 5.6,

$$|b_{11}^{3/2} a_{22} a_{23} a_{33}| < X^{4.5/12},$$

and so the total number of choices for A is $X^{4.5/12+\delta+\epsilon}$. The total number of choices for (A, B) is therefore $O(X^{10.5/12+4\delta+\epsilon}) = O(X^{11/12})$.

Now suppose $\gamma = -3a_{13}^2 a_{23}^2 b_{11}^2 - 3a_{13}^2 a_{22} a_{33} b_{11}^2 + 4a_{13}^3 a_{23} b_{11} b_{12} - a_{13}^4 b_{12}^2 = 0$, so that a_{33} is determined by a_{23}, b_{11}, a_{22}, b_{12}, a_{13}. As in (5.29), the number choices for b_{13}, when all variables outside b_{13} and b_{33} are held fixed, is

$$O(X^{\frac{1}{2}}/(a_{13} a_{22} b_{12} a_{23} b_{23})). \tag{5.34}$$

The leading coefficient of $\beta^2(bc - 9ad)$, taken as a linear polynomial in b_{33}, is $\beta^2\kappa$, where κ is given by

$$\kappa = a_{22} a_{23}^2 b_{11}^2 - a_{22}^2 a_{33} b_{11}^2 - 2a_{13} a_{22} a_{23} b_{11} b_{12} + 9a_{13}^2 a_{22} b_{12}^2 + 2a_{13} a_{22}^2 b_{11} b_{13} - 8a_{13}^2 a_{22} b_{11} b_{22}.$$

If in addition $\kappa = 0$, then b_{22} is uniquely determined by the other variables; Lemma 5.6 implies

$$|a^{2/3} a_{13} a_{22}^{3/2} a_{23} b_{11}^{3/2} b_{12} b_{13} b_{23} b_{33}| = O(X^{11/12}),$$

and hence the total number of choices for (A, B) if $\kappa = 0$ is $O(X^{11/12+\epsilon})$. Thus we may assume that $\kappa \neq 0$. It follows from the estimate

$$(bc - 9ad)\beta^2 = O(X^{8/12})$$

that the total number of choices for b_{13} and b_{33}, once all other variables have been fixed, is

$$O(X^{14/12}/(a_{13}a_{22}b_{12}a_{23}b_{23}\beta^2\kappa)).$$

But since $\beta^2 > X^{2/12+\delta}$, the above is

$$O(X^{1-\delta}/(a_{13}a_{22}b_{12}a_{23}b_{23}\kappa)).$$

Summing first over b_{22} and then over the remaining variables shows that the number of choices for (A, B) when $\gamma = 0$ is at most $O(X^{1-\delta})$. Hence we may assume also that $\gamma \neq 0$.

We consider now the region S in $\mathbb{R}^{10}$ defined by the conditions of Lemma 5.6 and the inequalities

$$|q_{12}| \leq q_{11} \tag{5.35}$$

$$|q_{13}| \leq q_{11} \tag{5.36}$$

$$|q_{23}| \leq q_{22} \tag{5.37}$$

$$|bc - 9ad|b_{13}b_{22}^{1/2} = O(X^{7.5/12}) \tag{5.38}$$

$$|a_{13}a_{22}| < X^{\delta} \tag{5.39}$$

$$X^{-\delta}|a_{33}b_{22}| < |a_{23}b_{23}| < X^{\delta}|a_{33}b_{22}| \tag{5.40}$$

$$|b_{13}| > X^{1/48} \tag{5.41}$$

$$|b_{22}| > X^{1/48} \tag{5.42}$$

$$\beta \geq X^{1/12+\delta/2} \tag{5.43}$$

$$|\gamma| \geq 1. \tag{5.44}$$

We estimate the number of integral choices for b_{13}, b_{22}, b_{23} and b_{23} satisfying the above

inequalities when all other variables have been fixed. By Lemma 5.8, this quantity is approximated by the volume of the four-dimensional region R (R is dependent on the set of variables outside b_{13}, b_{22}, b_{23} and b_{23}) cut out by the inequalities (5.35)-(5.44). The error is at most

$$O(\sum_{\bar{R}} \mathrm{Vol}(\bar{R})),$$

where $\bar{R}$ ranges over the various projections of R onto smaller dimensional coordinate hyperplanes. The total number of integral points satisfying inequalities (5.35)-(5.44), where all 10 variables are allowed to vary, is therefore

$$O\left(\max_{\bar{R}}\left\{\sum \mathrm{Vol}(\bar{R})\right\}\right),$$

where $\bar{R}$ ranges over all projections of R onto four- and smaller-dimensional coordinate hyperplanes, and the inside sums are taken over all values of the variables in $T \setminus \{b_{13}, b_{22}, b_{23}, b_{33}\}$. We estimate each of the latter sums in turn.

We begin by estimating $\sum \mathrm{Vol}(R)$. We divide into two cases. First suppose

$$|a_{13}^2 a_{22}^4 b_{22}^9| < X^{15/12+9\delta}. \tag{5.45}$$

Then note that the inequalites (5.36) and (5.37) are linear in the variables b_{22} and b_{33}. The two-dimensional volume cut out by these two inequalities, when all variables outside b_{22} and b_{33} are fixed, is

$$O(q_{11}q_{22}/\lambda), \tag{5.46}$$

where

$$\lambda = -3a_{13}a_{22}a_{23}a_{33}b_{11}^2 + 3a_{13}^2 a_{22}a_{33}b_{11}b_{12} - 2a_{13}^2 a_{22}a_{23}b_{11}b_{13} + 2a_{13}^3 a_{22}b_{11}b_{23}.$$

We may assume $\lambda \neq 0$ for the same reason we assumed $\gamma \neq 0$ (b_{23} is uniquely determined by the rest). By Lemma 5.6,

$$q_{11}q_{22}/\lambda = O(X^{10.5/12}/(a_{33}b_{13}a_{22}^{1/4}b_{22}^{1/4}\lambda));$$

thanks to (5.45), this in turn is at most

$$O(X^{47/48+3\delta/4}/(a_{13}^{1/6}a_{33}b_{13}a_{22}^{7/12}b_{22}\lambda)),$$

and since $|a_{33}b_{22}| \leq |a_{23}b_{23}| \cdot X^{\delta}$ by (5.40), it is at most

$$O(X^{47/48+7\delta/4}/(a_{13}^{1/6}a_{23}b_{13}a_{22}^{7/12}b_{23}\lambda)).$$

Integrating now over b_{13} and b_{23}, then summing over the remaining variables, we obtain

$$\sum \mathrm{Vol}(R) = O(X^{47/48+7\delta/4+\epsilon}).$$

Suppose next that the negation of (5.45) holds. Then note that the first two inequalities (5.35) and (5.36) are linear in the three variables b_{13}, b_{22}, and b_{23}. We make the change of variables

$$\begin{aligned} x &= q_{12}. \\ y &= q_{13}. \end{aligned}$$

Solving for b_{23} and b_{22} in terms of x and y (simultaneous linear equations), and substituting these values into the left side of the third inequality (5.37), we obtain an

inequality of the form

$$p(x, y, b_{13}) = O(X^{7.5/12}).$$

If we treat $p(x, y, b_{13})$ as a polynomial of degree 4 in b_{13}, then the leading coefficient of p is given by

$$-72a_{13}^9 a_{22}^4 a_{33}^2 b_{11}^4 b_{22}^{1/2} \gamma^2 / \gamma^4$$

and hence b_{13} is restricted to lie in an interval of length

$$O(X^{7.5/48} / (a_{13}^{9/4} a_{22} a_{33}^{1/2} b_{11} b_{22}^{1/8} \gamma^{1/2} / \gamma))$$

once x and y have been fixed. Taking into account the Jacobian of the transformation $(x, y, b_{13}) \to (b_{23}, b_{22}, b_{13})$ (a quick computation shows that the Jacobian of the map $(x, y) \to (b_{23}, b_{22})$ is γ), we see that the three-dimensional volume of R''—the cross section of R at the given value of b_{33}—is bounded above by

$$O(X^{7.5/48} q_{11}^2 / (a_{13}^{9/4} a_{22} a_{33}^{1/2} b_{11} b_{22}^{1/8} \gamma^{1/2})).$$

By Lemma 5.6, q_{11}^2 is bounded above by $O(X/(a_{22}^{1/2} a_{23} a_{33}^{1/2} b_{22} b_{33}))$. Thus $\mathrm{Vol}(R'')$ is bounded by

$$O(X^{55.5/48} / (a_{13}^{9/4} a_{22}^{3/2} a_{23} a_{33} b_{11} b_{22}^{9/8} b_{33} \gamma^{1/2})),$$

which by assumption is less than

$$O(X^{1-\delta} / (a_{13}^2 a_{22} a_{23} a_{33} b_{11} b_{33} \gamma^{1/2})).$$

Integrating over b_{33}, then summing over b_{12}, and finally summing over the remaining variables, we obtain $O(X^{1-\delta})$.

Next, we consider the volumes of the smaller-dimensional projections $\bar{R}$ of R, which correspond to the error in our estimate for the number of integer points in R. To improve our estimate for this error, we perform a piecewise linear change-of-variable by replacing b_{33} by b'_{33}, where

$$b'_{33} = b_{33} - \left\lfloor \frac{q_{13} - 2a_{13}a_{22}b_{11}b_{33}}{2a_{13}a_{22}b_{11}} \right\rfloor .$$

This transformation evidently preserves the integer lattice as well as the volume form on $\mathbb{R}^{10}$, and is therefore harmless. The inequality (5.36) thus becomes

$$|2a_{13}a_{22}b_{11}b'_{33} + \mu| \leq q_{11},$$

where μ is some integer with $0 \leq \mu < 2a_{13}a_{22}b_{11}$.

It will suffice to estimate the projections of the larger region R' defined only by the inequalities (5.35) and (5.36). We have already seen that the volume of this region R', when summed over the variables in $T \setminus \{b_{13}, b_{22}, b_{23}\}$, is $O(X^{1+\epsilon})$.

Let us examine the projection of R' onto $b_{13} = 0$. When all other variables are fixed, the number of choices for b_{13}, as we have seen, is

$$O(X^{\frac{1}{2}}/(a_{13}a_{22}b_{12}a_{23}b_{23})). \tag{5.47}$$

By Lemma 5.6,

$$a_{13}^2|b_{11}b_{22}|^{1/2}b_{12}a_{23}b_{23} = O(X^{1/2});$$

it follows from (5.39) and (5.42) that

$$a_{13}a_{22}b_{12}a_{23}b_{23} = O(X^{47/96+\delta}).$$

Therefore, (5.47) is at least $cX^{1/96-\delta}$ for some $c > 0$, and so the region R' has b_{13}-thickness at least $X^{1/96-\delta}$ everywhere; hence the volume of the projection of R' onto $b_{13} = 0$, summed over all variables in $T \setminus \{b_{13}, b_{22}, b_{23}\}$, is at most $X^{95/96+\delta+\epsilon}$. The projections onto $b_{22} = 0$, $b_{23} = 0$, and $b'_{33} = 0$ are similar (but easier) to handle, and the same estimate is obtained.

The one- and smaller-dimensional projections are even easier. We simply observe that by Lemma 5.6,

$$a_{13}a_{22}^{5/2}a_{23}a_{33}b_{11}^{5/2}b_{12}b_{23}b_{33} = O(X^{11/12});$$

thus the volume of the projection of R onto $b_{13} = b_{22} = 0$, summed over all variables in $T \setminus \{b_{13}, b_{22}, b_{23}\}$, is at most $O(X^{11/12+\epsilon})$. Similar estimates hold for the other one-dimensional projections.

We conclude finally that the number of $(A, B) \in \mathcal{F}_X(\mathbb{Z})$ with $a_{11} = a_{12} = 0$ is at most $O(X^{191/192+\epsilon})$, as desired.

5.1.7 Computation of the fundamental volume

To prove Theorem 5.5, it remains only to compute $\mathrm{Vol}(\mathcal{F}_X)$. Before performing this computation, we state first some propositions regarding the group $G = GL_2 \times SL_3$ and its 12-dimensional representation V.

Let $V^{(1)}$ denote the $G_{\mathbb{R}}$-orbit in $V_{\mathbb{R}}$ consisting of the totally real elements.

Proposition 5.14 *The group $G_{\mathbb{R}}$ acts transitively on $V^{(1)}$, and the isotropy groups for $x \in V^{(1)}$ are isomorphic to the symmetric group S_4.*

Now define the usual subgroups K, A_+, N, and $\bar{N}$ of $G_{\mathbb{R}}$ as follows:

$$
\begin{aligned}
K &= \{\text{orthogonal transformations in } G_{\mathbb{R}}\};\\
A_+ &= \{a(t) : t \in \mathbb{R}_+^{\times 4}\}, \text{ where } a(t) = \left(\begin{pmatrix} t_1 & \\ & t_2 \end{pmatrix}, \begin{pmatrix} t_3 & & \\ & t_4 & \\ & & (t_3t_4)^{-1} \end{pmatrix} \right);\\
N &= \{n(u) : u \in \mathbb{R}^4\}, \text{ where } n(u) = \left(\begin{pmatrix} 1 & \\ u_1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ u_2 & 1 & \\ u_3 & u_4 & 1 \end{pmatrix} \right);\\
\bar{N} &= \{\bar{n}(x) : x \in \mathbb{R}^4\}, \text{ where } \bar{n}(x) = \left(\begin{pmatrix} 1 & x_1 \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & x_2 & x_3 \\ & 1 & x_4 \\ & & 1 \end{pmatrix} \right).
\end{aligned}
$$

It is well-known that the natural product map $K \times A_+ \times N \to G_{\mathbb{R}}$ is an analytic diffeomorphism. In fact, for any $g \in G_{\mathbb{R}}$, there exist unique $k \in K$, $a = a(t_1, \ldots, t_4) \in A_+$, and $n = n(u_1, \ldots, u_4) \in N$ such that $g = k\,a\,n$. In particular, the element $\bar{n}(x) \in \bar{N}$ can also be factored uniquely in this way; the corresponding value of a is provided in the following proposition.

Proposition 5.15 *Let $\bar{n}(x_1, \ldots, x_4) \in \bar{N}$. Set*

$$q = 1 + x_1^2, \;\; r = 1 + x_2^2 + (x_2x_4 - x_3)^2, \;\; s = 1 + x_3^2 + x_4^2.$$

Then $\bar{n} = k\,a(t_1, t_2, t_3, t_4)\,n$, where

$$t_1 = 1/\sqrt{q}, \;\; t_2 = \sqrt{q}, \;\; t_3 = 1/\sqrt{r}, \;\; t_4 = \sqrt{r}/\sqrt{s}.$$

Define an invariant measure dg on G as follows. Choose an invariant measure dk on

K so that $\int_K 1\,dk = 1$, and define

$$\begin{aligned}\int_G f(g)dg &= \int_K \int_{\mathbb{R}^4} \int_{\mathbb{R}_+^{\times 4}} f(kna) d^\times t\, du\, dk \\ &= \int_K \int_{\mathbb{R}^4} \int_{\mathbb{R}_+^{\times 4}} t_1^{-1} t_2 t_3^{-4} t_4^{-2} f(kan) d^\times t\, du\, dk.\end{aligned}$$

Let $dy = dy_1\, dy_2 \cdots dy_{12}$ be the standard Euclidean measure on $V_{\mathbb{R}}$.

Proposition 5.16 *For any $f \in L^1(G)$,*

$$\int_G f(g)dg = \frac{1}{32\pi^3} \int_{\mathbb{R}^{\times 4}} \int_{\mathbb{R}^4} \int_{\mathbb{R}^4} f(\bar{n}(x)n(u)a(t))dx\, du\, d^\times t.$$

Proof: Use Proposition 5.15. □

Proposition 5.17 *Let $f \in C_0(V^{(1)})$, and let y denote any element of $V^{(1)}$. Then*

$$\int_G f(g \cdot y)dg = \frac{4}{\pi^3} \int_{V^{(1)}} P(x)^{-1} f(x)\, dx.$$

Proof: It suffices to prove the equality for

$$y = \left(\begin{bmatrix} 1 & & & \\ & -1 & & \\ & & & \end{bmatrix}, \begin{bmatrix} & -1 & & \\ & & & \\ & & 1 & \end{bmatrix} i \right) \in V^{(1)}.$$

Put

$$(z_1, \ldots, z_{12}) = \bar{n}(x)n(u)a(t) \cdot y.$$

Then the form $P(z)^{-1} dz_1 \wedge \cdots \wedge dz_{12}$ is a G-invariant measure, and so we must have

$$P(z)^{-1} dz_1 \wedge \cdots \wedge dz_{12} = c\, dx \wedge du \wedge d^\times t$$

for some constant factor c. An explicit calculation shows that $c = -3/16$. By Proposition 5.14, G is a 24-fold covering of $V^{(i)}$ via the map $g \to g \cdot y$. Hence

$$\int_G f(g \cdot y)dg = 24 \cdot \frac{1}{32\pi^3} \cdot \frac{16}{3} \int_{V^{(1)}} P(x)^{-1} f(x)dx = \frac{24}{6\pi^3} \int_{V^{(1)}} P(x)^{-1} f(x)dx,$$

as desired. □

Finally, we obtain using Proposition 5.17 that

$$\mathrm{Vol}(\mathcal{F}_X) = \frac{\pi^3}{4} \int_0^{X^{1/6}} t^6 d^\times t \int_{G_{\mathbf{Z}} \backslash G^1_{\mathbf{R}}} dg = \frac{\pi^3}{4} \cdot \frac{X}{6} \cdot \frac{\zeta(2)}{\pi} \cdot \frac{\zeta(2)\zeta(3)}{2\pi^2} = \frac{\zeta(2)^2\zeta(3)}{48} X.$$

This concludes the proof of Theorem 5.5.

5.2 Pairs of ternary quadratic forms and Theorems 5.1–5.4

Theorem 4.5 of Chapter 4 together with Theorem 5.5 of the previous section now immediately imply the following.

Theorem 5.18 *Let $M_4^*(\xi, \eta)$ denote the number of pairs (Q, R) where Q is a quartic order in a totally real S_4-quartic field, R is a cubic resolvent ring of Q, and $\xi <$ $\mathrm{Disc}(Q) < \eta$. Then*

$$\lim_{X \to \infty} \frac{M_4^*(0, X)}{X} = \frac{\zeta(2)^2\zeta(3)}{48}.$$

To obtain finer asymptotic information on the distribution of quartic rings (in particular, without the weighting by the number of cubic resolvents), we need to be able to count absolutely irreducible equivalence classes in $V_{\mathbf{Z}}$ lying in certain subsets $S \subset V_{\mathbf{Z}}$. If S is defined, say, by *finitely many* congruence conditions, then this can

easily be done; we have

$$\lim_{X\to\infty} \frac{N(0,X;S)}{X} = \frac{\zeta(2)^2\zeta(3)}{48} \prod_p \mu_p(S). \tag{5.48}$$

This refinement of Theorem 5.5 is proven in exactly the same way as the original theorem.

We recall from Section 4.10, however, that the set $\mathcal{U} = \cap_p \mathcal{U}_p$ of elements $(A, B) \in V_{\mathbb{Z}}$ corresponding to maximal orders is defined by infinitely many congruence conditions. To prove that (5.48) still holds for such a set, we require a uniform estimate on the error term when only finitely many factors are taken in (5.48). This estimate is provided in Section 5.2.2. In Section 5.2.3, we then use this estimate to complete the proofs of Theorems 5.1–5.4.

5.2.1 Nowhere overramified quartic fields

Let Q be an order in an S_4-quartic field, and let $p \in \mathbb{Z}$ be a prime such that Q is maximal at p. We say p is *overramified* in Q if (p) factors into primes in Q as P^4, P^2, or $P_1^2P_2^2$; we say a quartic maximal order Q (or the quartic field K_4 in which it lies) is *nowhere overramified* if no prime in $\mathbb{Z}$ is overramified in Q.

The significance of being "nowhere overramified" is as follows. Given an S_4-quartic field K_4, let K_{24} denote its Galois closure. Let K_3 denote a cubic field contained in K_{24} (the "cubic resolvent field"), and let K_6 be the unique quadratic extension of K_3 such that the Galois closure of K_6 over $\mathbb{Q}$ is precisely K_{24}. Then one checks that the quadratic extension K_6/K_3 is unramified precisely when the quartic field K_4 is nowhere overramified. Conversely, if K_3 is a noncyclic cubic field, and K_6 is an unramified quadratic extension of K_3, then the Galois closure of K_6 is an S_4-extension K_{24} which contains up to conjugacy a unique, nowhere overramified quartic extension K_4.

5.2.2 A uniformity estimate

Let us denote by $\mathcal{V}_p$ the set of all $(A, B) \in V_{\mathbb{Z}}$ corresponding to quartic orders Q that are maximal at p and in which p is not overramified. Let $\mathcal{W}_p = V_{\mathbb{Z}} - \mathcal{V}_p$. In order to apply a simple sieve to obtain Theorems 5.1–5.4, we require the following proposition, analogous to Proposition 1 in [11] (though our proof is significantly simpler).

Proposition 5.19 *$N(0, X; \mathcal{W}_p) = O(X/p^2)$, where the implied constant is independent of p.*

Proof: The set $\mathcal{W}_p$ may be naturally partitioned into two subsets: $\mathcal{W}_p^{(1)}$, the set of points $(A, B) \in V_{\mathbb{Z}}$ corresponding to quartic rings not maximal at p; and $\mathcal{W}_p^{(2)}$, the set of points $(A, B) \in V_{\mathbb{Z}}$ corresponding to quartic rings that are maximal at p but also overramified at p. We treat first $\mathcal{W}_p^{(1)}$.

Lemma 5.20 *Let Q be a maximal quartic ring of nonzero discriminant. Then Q has at most 6 subrings of index p.*

Proof: Let $< 1, \alpha, \beta, \gamma >$ be a normal basis for Q corresponding to an element $(A, B) \in V_{\mathbb{Z}}$. Any $\mathbb{Z}$-submodule Q' of index p in Q containing $\mathbb{Z}$ is spanned by 1, $p\alpha$, $p\beta$, $p\gamma$, and two additional elements $\xi_1 = x_1\alpha + y_1\beta + z_1\gamma$ and $\xi_2 = x_1\alpha + y_1\beta + z_1\gamma$, where ξ_1, ξ_2 span a sublattice in Q well-defined modulo p. Let L be the line in $\mathbb{P}^2_{\mathbb{F}_p}$ passing through the two points (x_1, y_1, z_1) and (x_2, y_2, z_2). Then one checks that Q' is a ring if and only if L intersects A and B (viewed as conics in $\mathbb{P}^2_{\bar{\mathbb{F}}_p}$) in the same two points. Since A and B intersect in four points (counting multiplicities), there are at most $6 = \binom{4}{2}$ possible lines that L could be. This is the desired conclusion. □

Lemma 5.21 *Let Q be a maximal quartic ring of nonzero discriminant. Then there are at most 4 index p^2 subrings of Q containing $\mathbb{Z} + pQ$.*

Proof: Let $< 1, \alpha, \beta, \gamma >$ be a normal basis for Q corresponding to to an element $(A, B) \in V_{\mathbf{Z}}$. A $\mathbb{Z}$-submodule Q' of index p^2 in Q containing $\mathbb{Z} + pQ$ is spanned by 1, $p\alpha$, $p\beta$, $p\gamma$, and an additional element $\xi = x\alpha + y\beta + z\gamma$, where ξ is well-defined modulo p up to multiplication by scalars. One checks that Q' forms a ring if and only if (x, y, z) is a common zero of the quadratic forms A and B. Since A and B intersect in at most four points as conics in $\mathbb{P}^2_{\mathbb{F}_p}$, there are at most 4 values that (x, y, z) could take (as an element of $\mathbb{P}^2_{\mathbb{F}_p}$). This is the desired conclusion. □

For general index p^k subalgebras of Q not containing $\mathbb{Z}+pQ$, much cruder estimates will suffice. First, we recall that, by Lemma 4.14, any index p^k subring of a maximal order Q contains some proper subring Q' of Q such that $\mathbb{Z}+pQ \subseteq Q'$. In addition, the number of such subrings Q' of index p, p^2, or p^3 in Q is at most 6, 4, or 1 respectively, by Lemmas 5.20 and 5.21.

Now the set of index p^k subrings of Q is contained in the set of index p^k $\mathbb{Z}$-submodules of Q containing $\mathbb{Z}$, or equivalently, the index p^k $\mathbb{Z}$-submodules of $Q/\mathbb{Z}$. Furthermore, any index p^k submodule of $Q/\mathbb{Z}$ is an index p submodule of some index p^{k-1} submodule of $Q/\mathbb{Z}$. Since any rank 3 $\mathbb{Z}$-module has exactly $p^2 + p + 1$ index p submodules, we have by Lemmas 5.20 and 5.21, and induction, that there are at most $6(p^2+p+1)^{k-1} + 4(p^2+p+1)^{k-2} + (p^2+p+1)^{k-3} \leq 11(p^2+p+1)^{k-1}$ index p^k subrings of Q.

Next, given any index p^k subring Q'' of Q, by Lemma 4.10 there are at most $(p+1)^{\lfloor k/6 \rfloor}$ points $x \in \mathcal{W}_p$ with $Q(x) = Q''$. It follows that

$$N(X; \mathcal{W}_p) < \sum_{k=1}^{\infty} \frac{11(p^2+p+1)^{k-1}(p+1)^{\lfloor k/6 \rfloor}}{p^{2k}} X = O(X/p^2),$$

as desired.

We turn next to $\mathcal{W}_p^{(2)}$. Let us say a quadratic extension K_6 of a non-cyclic cubic field K_3 is *acceptable* if the Galois closure of K_6 over $\mathbb{Q}$ has Galois group a subgroup

of S_4. For a fixed K_3, let $g(n)$ denote the number of acceptable quadratic extensions whose conductor has absolute norm n. To estimate $g(n)$, we require two lemmas. The first lemma is due to Baily:

Lemma 5.22 (Baily) *K_6 is an acceptable quadratic extension of K_3 if and only if $N_{K_3/\mathbb{Q}}\mathrm{Disc}(K_6/K_3)$ is the square of an ideal in $\mathbb{Z}$.*

The second lemma gives an upper bound on the sum of $h_2^*(F)$ over all cubic fields F of discriminant at most X.

Lemma 5.23 *We have*

$$\sum_F h_2^*(K_3) = O(X), \tag{5.49}$$

where the sum ranges over all totally real cubic fields K_3 of discriminant less than X.

Lemma 5.23 follows from Theorem 5.5 as Theorem 5.4 will follow from Theorem 5.1.

Now for any $s > 1$, it is an easy consequence of Lemma 5.22 that

$$\sum_{n=1}^{\infty} g(n)n^{-s} < \kappa\, h_2^*(K_3) \prod_p (1 + 3p^{-2s}) = \kappa\, h_2^*(K_3) \sum_{n=1}^{\infty} 3^{\tau(n)} n^{-2s}, \tag{5.50}$$

where $\tau(n)$ denotes the number of prime factors of n, and κ is a constant bounded independently of K_3 (it corresponds to the even and infinite places; see [1] for details). Lemma 5.23 and (5.50) now imply that, for some constant c',

$$\begin{aligned}
N(X; \mathcal{W}_p^{(2)}) &\leq \kappa \sum_{K_3} \sum_{\substack{p \mid n \\ n^2 \mathrm{Disc}(K_3) < X}} 3^{\tau(n)} h_2^*(K_3) \\
&\leq 3\kappa \sum_{p^2 n^2 < X} 3^{\tau(n)} \sum_{\mathrm{Disc}(K_3) < X/(p^2n^2)} h_2^*(K_3) \\
&\leq 3\kappa c' \frac{X}{p^2} \sum_{p^2n^2 < X} \frac{3^{\tau(n)}}{n^2} \\
&< 3\kappa c' \frac{X}{p^2} \sum_{n} \frac{3^{\tau(n)}}{n^2}.
\end{aligned}$$

As the last sum converges absolutely, this concludes the proof of the lemma. □

5.2.3 Proofs of Theorems 5.1–5.4

Proof of Theorem 5.1: Suppose Y is any positive integer. It follows from Theorem 4.15 and (5.48) that

$$\lim_{X\to\infty} \frac{N(0,X;\cap_{p<Y}\mathcal{U}_p)}{X} = \frac{\zeta(2)^2\zeta(3)}{48}\prod_{p<Y}[p^{-12}p\,(p^2-1)^2(p^3-1)(p^4+p^2-p-1)].$$

Letting Y tend to ∞, we obtain immediately that

$$\begin{aligned}\limsup_{X\to\infty} \tfrac{N(0,X;\mathcal{U})}{X} &\leq \tfrac{\zeta(2)^2\zeta(3)}{48}\textstyle\prod_{p<Y}[p^{-12}p\,(p^2-1)^2(p^3-1)(p^4+p^2-p-1)] \\ &= \tfrac{\zeta(2)^2\zeta(3)}{48}\textstyle\prod_{p}[(1-p^{-2})^2\,(1-p^{-3})(1+p^{-2}-p^{-3}-p^{-4})]. \\ &= \tfrac{1}{48}\textstyle\prod_{p}(1+p^{-2}-p^{-3}-p^{-4}).\end{aligned}$$

To obtain a lower bound for $N(0,X;\mathcal{U})$, we note that

$$\bigcap_{p<Y}\mathcal{U}_p \subset (\mathcal{U}\cup\bigcup_{p\geq Y}\mathcal{W}_p).$$

Hence by Proposition 5.19,

$$\lim_{X\to\infty}\frac{N(0,X;\mathcal{U})}{X} \geq \frac{\zeta(2)^2\zeta(3)}{48}\prod_{p<Y}[p^{-12}p\,(p^2-1)^2(p^3-1)(p^4+p^2-p-1)] - O(\sum_{p\geq Y}p^{-2}).$$

Letting Y tend to infinity completes the proof of Theorem 5.1. □

Proof of Theorem 5.2: We first prove the analogue of Theorem 5.2 for S_4-quartic orders of content 1; on such quartic rings the correspondence of Theorem 4.5 is bijective. Let $\mathcal{S}_p$ denote the set of elements $(A,B)\in V_{\mathbb{Z}}$ having content prime to p, and let $\mathcal{S}=\cup_p\mathcal{S}_p$. Then note that an element $(A,B)\in V_{\mathbb{F}_p}$ has nonzero content if

and only if A and B are linearly independent over $\mathbb{F}_p$. It follows that

$$\mu_p(S_p) = (p^6 - 1)(p^6 - p)/p^{12}.$$

The same argument as in the proof of Theorem 5.1 then shows that

$$\lim_{X\to\infty} \frac{N(0, X; \mathcal{S})}{X} = \frac{\zeta(2)^2\zeta(3)}{48} \prod_p (1 - p^{-5})(1 - p^{-6}) = \frac{\zeta(2)^2\zeta(3)}{48\zeta(5)\zeta(6)}. \tag{5.51}$$

To obtain Theorem 5.2 from (5.51), we observe that every content 1 ring Q_1 contains the content n ring $Q_n = \mathbb{Z} + nQ_1$, and conversely, every content n ring Q_n arises from a unique content 1 ring Q_1 in this way. Furthermore, if Q_1 has discriminant D then Q_n has discriminant $n^6 D$. It follows that

$$\lim_{X\to\infty} \frac{M_4(0, X)}{X} = \sum_{n=1}^{\infty} \frac{1}{n^6} \frac{\zeta(2)^2\zeta(3)}{48\zeta(5)\zeta(6)} = \frac{\zeta(2)^2\zeta(3)}{48\zeta(5)},$$

as desired. □

Proof of Theorem 5.3: It is known that the Artin symbol (K_{24}/p) equals $\langle e \rangle$, $\langle (12) \rangle$, $\langle (123) \rangle$, $\langle (1234) \rangle$, and $\langle (12)(34) \rangle$ precisely when (Q, p) equals (1111), (112), (13), (4), or (22) respectively, where Q denotes the ring of integers in K_4. The set of all $(A, B) \in V_{\mathbb{Z}}$ corresponding to maximal quartic rings Q with a given value σ of (Q, p) is given by $\mathcal{U} \cap T_p(\sigma)$; hence by the same argument as in the proof of Theorem 5.1, we have

$$\lim_{X\to\infty} N(0, X; \mathcal{U} \cap T_p(\sigma)) = \mu_p(T_p(\sigma)) \prod_{q\neq p} \mu_q(U_q).$$

On the other hand, an examination of Theorem 4.15 immediately shows that the values of $\mu_p(T_p(\sigma))$ for σ = (1111), (112), (13), (4), or (22) occur in the ratio 1:6:8:6:3 for any value of p; this is the desired result. □

Proof of Theorem 5.4: Let $\mathcal{V} = \cap_p \mathcal{V}_p$ be the set of all $(A, B) \in V_{\mathbb{Z}}$ corresponding to nowhere overramified maximal quartic rings. Using Theorem 4.15 and the fact that V_p is simply the union of all $U_p(\sigma)$'s where $\sigma \neq (1^4)$, (2^2), or $(1^2 1^2)$, we obtain

$$\mu(\mathcal{V}_p) = p^{-12}\, p^2\, (p^2-1)^2\, (p^3-1)^2. \tag{5.52}$$

By the same argument as in Theorem 5.1, we therefore get

Lemma 5.24 *Let $L_4(\xi, \eta)$ denote the number of nowhere overramified totally real S_4-quartic fields K such that $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$\lim_{X\to\infty} \frac{L_4(0,X)}{X} = \frac{\zeta(2)^2\zeta(3)}{48} \prod_p \mu_p(\mathcal{V}_p) = \frac{\zeta(2)^2\zeta(3)}{48} \zeta(2)^{-2}\zeta(3)^{-2} = 1/(48\zeta(3)).$$

On the other hand, given a nowhere overramified S_4-quartic field K_4 with Galois closure K_{24}, we have observed earlier that in K_{24} is contained a unique (up to conjugacy) cubic field K_3 and a unique unramified extension K_6 of K_3. In addition, the discriminant of K_4 is equal to the discriminant of K_3, and the number of quadruplets of quartic fields K_4 corresponding to a given K_3 in this way equals $h_2^*(K_3) - 1$ (see Heilbronn [18] for full details). Therefore,

$$\sum_{\substack{K_3 \\ 0<\mathrm{Disc}(K_3)<X}} (h_2^*(K_3) - 1) = L_4(0, X). \tag{5.53}$$

Since Davenport and Heilbronn [11] have shown that

$$\lim_{X\to\infty} \frac{\sum_{0<\mathrm{Disc}(K_3)<X} 1}{X} = 1/(12\zeta(3)), \tag{5.54}$$

we conclude

$$\lim_{X\to\infty} \frac{\sum_{0<\mathrm{Disc}(K_3)<X} h_2^*(K_3)}{\sum_{\substack{K_3 \\ 0<\mathrm{Disc}(K_3)<X}} 1} = \lim_{X\to\infty} \frac{L_4(0,X)+1}{\sum_{0<\mathrm{Disc}(K_3)<X} 1} = 1 + \frac{1/(48\zeta(3))}{1/(12\zeta(3))} = \frac{5}{4}.$$

□

Appendix: The quadratic covariant $\mathcal{Q}$

The space $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$ of pairs (A, B) of integral ternary quadratic forms has an integral ternary quadratic SL_3-covariant $\mathcal{Q}$ of degree 4. Below we give the coefficients $\{q_{ij}\}_{1\le i\le j\le 3}$ of this covariant $\mathcal{Q}$ in terms of the coefficients of the quadratic forms $A = (a_{ij})$ and $B = (b_{ij})$.

$$\begin{aligned}
q_{11} &= a_{23}^2b_{11}^2 - a_{22}a_{33}b_{11}^2 - 2a_{13}a_{23}b_{11}b_{12} + 2a_{12}a_{33}b_{11}b_{12} + 3a_{13}^2b_{12}^2 - 2a_{11}a_{33}b_{12}^2 \\
&\quad + 2a_{13}a_{22}b_{11}b_{13} - 2a_{12}a_{23}b_{11}b_{13} - 6a_{12}a_{13}b_{12}b_{13} + 4a_{11}a_{23}b_{12}b_{13} + 3a_{12}^2b_{13}^2 \\
&\quad - 2a_{11}a_{22}b_{13}^2 - 2a_{13}^2b_{11}b_{22} + a_{11}a_{33}b_{11}b_{22} + 2a_{11}a_{13}b_{13}b_{22} + 4a_{12}a_{13}b_{11}b_{23} \\
&\quad - 2a_{11}a_{23}b_{11}b_{23} - 2a_{11}a_{13}b_{12}b_{23} - 2a_{11}a_{12}b_{13}b_{23} + a_{11}^2b_{23}^2 - 2a_{12}^2b_{11}b_{33} \\
&\quad + a_{11}a_{22}b_{11}b_{33} + 2a_{11}a_{12}b_{12}b_{33} - a_{11}^2b_{22}b_{33}
\end{aligned}$$

$$\begin{aligned}
q_{12} &= a_{23}^2b_{11}b_{12} - a_{22}a_{33}b_{11}b_{12} + a_{13}a_{23}b_{12}^2 - a_{13}a_{22}b_{12}b_{13} - a_{12}a_{23}b_{12}b_{13} + a_{12}a_{22}b_{13}^2 \\
&\quad - 3a_{13}a_{23}b_{11}b_{22} + 2a_{12}a_{33}b_{11}b_{22} + a_{13}^2b_{12}b_{22} - a_{11}a_{33}b_{12}b_{22} - a_{12}a_{13}b_{13}b_{22} \\
&\quad + 3a_{11}a_{23}b_{13}b_{22} + 3a_{13}a_{22}b_{11}b_{23} - a_{12}a_{23}b_{11}b_{23} - a_{12}a_{13}b_{12}b_{23} - a_{11}a_{23}b_{12}b_{23} \\
&\quad + a_{12}^2b_{13}b_{23} - 3a_{11}a_{22}b_{13}b_{23} + a_{11}a_{12}b_{23}^2 - a_{12}a_{22}b_{11}b_{33} + 2a_{11}a_{22}b_{12}b_{33} \\
&\quad - a_{11}a_{12}b_{22}b_{33}
\end{aligned}$$

$$\begin{aligned}
q_{13} &= a_{13}a_{33}b_{12}^2 + a_{23}^2b_{11}b_{13} - a_{22}a_{33}b_{11}b_{13} - a_{13}a_{23}b_{12}b_{13} - a_{12}a_{33}b_{12}b_{13} + a_{12}a_{23}b_{13}^2 \\
&\quad - a_{13}a_{33}b_{11}b_{22} + 2a_{11}a_{33}b_{13}b_{22} - a_{13}a_{23}b_{11}b_{23} + 3a_{12}a_{33}b_{11}b_{23} + a_{13}^2b_{12}b_{23} \\
&\quad - 3a_{11}a_{33}b_{12}b_{23} - a_{12}a_{13}b_{13}b_{23} - a_{11}a_{23}b_{13}b_{23} + a_{11}a_{13}b_{23}^2 + 2a_{13}a_{22}b_{11}b_{33} \\
&\quad - 3a_{12}a_{23}b_{11}b_{33} - a_{12}a_{13}b_{12}b_{33} + 3a_{11}a_{23}b_{12}b_{33} + a_{12}^2b_{13}b_{33} - a_{11}a_{22}b_{13}b_{33} \\
&\quad - a_{11}a_{13}b_{22}b_{33}
\end{aligned}$$

$$\begin{aligned}
q_{22} &= 3a_{23}^2b_{12}^2 - 2a_{22}a_{33}b_{12}^2 - 2a_{22}a_{23}b_{12}b_{13} + a_{22}^2b_{13}^2 - 2a_{23}^2b_{11}b_{22} + a_{22}a_{33}b_{11}b_{22} \\
&\quad - 2a_{13}a_{23}b_{12}b_{22} + 2a_{12}a_{33}b_{12}b_{22} - 2a_{13}a_{22}b_{13}b_{22} + 4a_{12}a_{23}b_{13}b_{22} + a_{13}^2b_{22}^2 \\
&\quad - a_{11}a_{33}b_{22}^2 + 2a_{22}a_{23}b_{11}b_{23} + 4a_{13}a_{22}b_{12}b_{23} - 6a_{12}a_{23}b_{12}b_{23} - 2a_{12}a_{22}b_{13}b_{23} \\
&\quad - 2a_{12}a_{13}b_{22}b_{23} + 2a_{11}a_{23}b_{22}b_{23} + 3a_{12}^2b_{23}^2 - 2a_{11}a_{22}b_{23}^2 - a_{22}^2b_{11}b_{33} \\
&\quad + 2a_{12}a_{22}b_{12}b_{33} - 2a_{12}^2b_{22}b_{33} + a_{11}a_{22}b_{22}b_{33}
\end{aligned}$$

$$
\begin{aligned}
q_{23} &= a_{23}a_{33}b_{12}^2 + a_{23}^2 b_{12}b_{13} - 3a_{22}a_{33}b_{12}b_{13} + a_{22}a_{23}b_{13}^2 - a_{23}a_{33}b_{11}b_{22} - a_{13}a_{23}b_{13}b_{22} \\
&\quad + 3a_{12}a_{33}b_{13}b_{22} + 2a_{22}a_{33}b_{11}b_{23} - a_{13}a_{23}b_{12}b_{23} - a_{12}a_{33}b_{12}b_{23} - a_{13}a_{22}b_{13}b_{23} \\
&\quad - a_{12}a_{23}b_{13}b_{23} + a_{13}^2 b_{22}b_{23} - a_{11}a_{33}b_{22}b_{23} + a_{12}a_{13}b_{23}^2 - a_{22}a_{23}b_{11}b_{33} \\
&\quad + 3a_{13}a_{22}b_{12}b_{33} - a_{12}a_{23}b_{12}b_{33} - 3a_{12}a_{13}b_{22}b_{33} + 2a_{11}a_{23}b_{22}b_{33} + a_{12}^2 b_{23}b_{33} \\
&\quad - a_{11}a_{22}b_{23}b_{33}
\end{aligned}
$$

$$
\begin{aligned}
q_{33} &= a_{33}^2 b_{12}^2 - 2a_{23}a_{33}b_{12}b_{13} + 3a_{23}^2 b_{13}^2 - 2a_{22}a_{33}b_{13}^2 - a_{33}^2 b_{11}b_{22} + 2a_{13}a_{33}b_{13}b_{22} \\
&\quad + 2a_{23}a_{33}b_{11}b_{23} - 2a_{13}a_{33}b_{12}b_{23} - 6a_{13}a_{23}b_{13}b_{23} + 4a_{12}a_{33}b_{13}b_{23} + 3a_{13}^2 b_{23}^2 \\
&\quad - 2a_{11}a_{33}b_{23}^2 - 2a_{23}^2 b_{11}b_{33} + a_{22}a_{33}b_{11}b_{33} + 4a_{13}a_{23}b_{12}b_{33} - 2a_{12}a_{33}b_{12}b_{33} \\
&\quad + 2a_{13}a_{22}b_{13}b_{33} - 2a_{12}a_{23}b_{13}b_{33} - 2a_{13}^2 b_{22}b_{33} + a_{11}a_{33}b_{22}b_{33} - 2a_{12}a_{13}b_{23}b_{33} \\
&\quad + 2a_{11}a_{23}b_{23}b_{33} + a_{12}^2 b_{33}^2 - a_{11}a_{22}b_{33}^2
\end{aligned}
$$

Chapter 6

Conclusion

During the past two centuries, Gauss's law of composition has been of central importance in algebraic and analytic number theory, and has enjoyed numerous applications. It is our hope that the composition laws presented in this thesis might similarly enjoy many additional applications in the future.

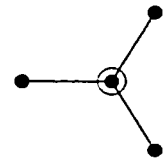
In this final chapter, we outline just a few of these potential applications, and indicate directions for future work.

6.1 Higher composition laws and exceptional groups

The higher composition laws we have presented in this thesis turn out to be closely related to the exceptional Lie groups. To be precise, let G be an exceptional Lie group, and let P be a certain maximal parabolic of G. Write $P = LU$, where L is the Levi factor and U is the unipotent radical at P. Then the group L acts naturally (by conjugation) on the abelianized unipotent radical $W = U/[U, U]$; for appropriate choices of G and P, we find that we obtain precisely the spaces W underlying our composition laws.

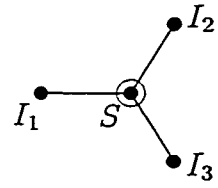
For example, the first case we considered in Chapter 2 was the space of $2 \times 2 \times 2$ cubes. Let G denote the exceptional Lie group of type D_4, and let P denote the

maximal parabolic corresponding to the central vertex of D_4:



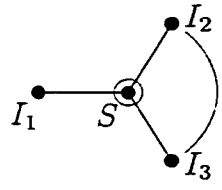
When this central vertex is removed, what remains are three isolated vertices, and hence the Levi L at P is $L = SL_2 \times SL_2 \times SL_2$. In addition, a calculation shows that W, the abelianized unipotent radical at P, is precisely the space of $2 \times 2 \times 2$ cubes.

As we discovered in Chapter 2, the three factors of SL_2 in L act on the bases of three ideals I_1, I_2, and I_3 respectively in some quadratic order S (where the three ideals sum to zero). This suggests that we ought to label the vertices of the Dynkin diagram of D_4 in the following manner:

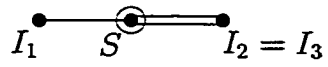


In particular, we see that the outer automorphisms of D_4 act by permuting the triple (I_1, I_2, I_3) of ideals in S.

Next, let us see what happens when we impose certain symmetry conditions, as we did in Chapter 2. First, we would like to impose the symmetry condition that identifies I_2 with I_3, so that $I_2 = I_3$. On the level of Dynkin diagrams, then, we perform the identification

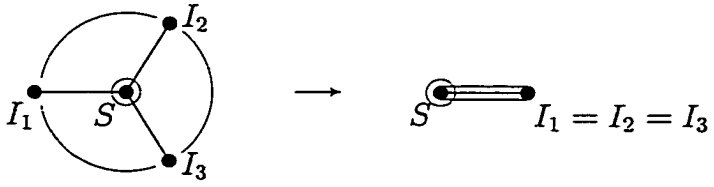


to yield



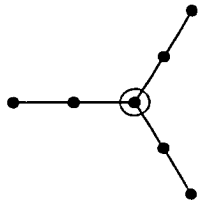
and we have obtained the Dynkin diagram C_3. Thus the composition law corresponding to pairs of binary quadratic forms, as discussed in Section 2.1.5, arises from the group C_3, where the parabolic P corresponds again to the central vertex.

Finally, let us identify all three ideals I_1, I_2, I_3. This corresponds, on the level of Dynkin diagrams, to the identification



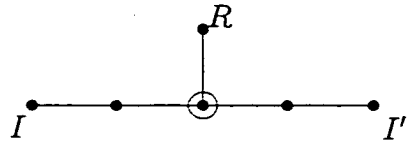
yielding the Dynkin diagram G_2. Thus the composition law on binary cubic forms, discussed in Section 2.1.4, arises in this sense from G_2.

The above discussion shows that quadratic composition essentially stems from the triply-symmetric Dynkin diagram of D_4. To obtain a theory of cubic composition, we then might want a Dynkin diagram of the form

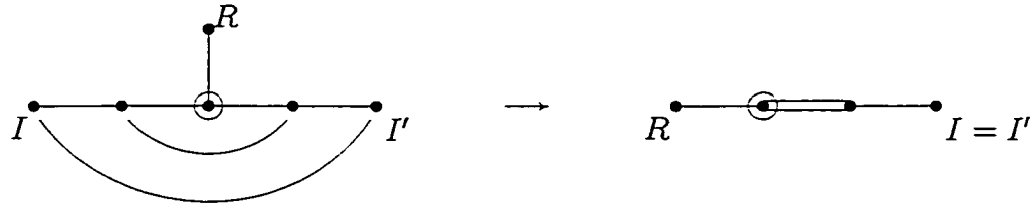


Unfortunately, a group with the above Dynkin diagram does not exist. However, if we cut short one of the legs of this diagram, we do obtain a genuine Dynkin diagram, namely that of the group E_6. (This corresponds to the "slicing" we performed at the start of Chapter 3). Taking again the parabolic P of E_6 corresponding to the central vertex, we find the Levi factor is $L = GL_2 \times GL_3 \times GL_3$, and the abelianized unipotent radical W is the space of $2 \times 3 \times 3$ boxes, the subject of Chapter 3.

We have shown in Chapter 3 that the GL_2 factor of L acts on the basis of a cubic ring R, while the two SL_3 factors act on bases of ideals I and I' of R (where I and I' sum to zero). Thus suggests we may label the Dynkin diagram of E_6 as follows:



As with the quadratic case, we may impose a symmetry condition on the situtation, and identify the ideals I and I'; this corresponds to the identification



yielding the Dynkin diagram for F_4. Thus the composition law on pairs of ternary quadratic forms, discussed in Section 3.2.2, arises in this sense from the exceptional group F_4.

6.2 Modular forms on exceptional groups

The connections between composition laws and exceptional groups outlined in the previous section may play an important role in understanding automorphic forms on the exceptional Lie groups, particularly in developing notions of "Fourier expansion" for these groups. In the case of the exceptional group G_2, such a theory of Fourier coefficients was recently obtained by Gross [17] and Gan-Gross-Savin [15]. We suspect that our work in Chapters 2, 3, and 4 should additionally yield a theory of Fourier

coefficients for modular forms on each of the exceptional groups C_3, D_4, F_4, E_6, E_7, and (possibly) E_8. We hope that this will be worked out more precisely in the near future.

6.3 Higher composition laws and prehomogeneous vector spaces

The work we have described here also has a natural interpretation in terms of the theory of prehomogeneous vector spaces. Following Sato, a *prehomogeneous vector space* is a vector space having a Zariski open orbit under the action of a reductive group. Over fields, such group representations have been studied by Wright and Yukie [25], who determined when generic rational orbits of such representations correspond to field extensions. Our approach differs from theirs in that we consider *integral* orbits rather than rational ones—as we have seen, the integral orbits have an extremely rich structure, and allow a direct extraction of arithmetic information on orders and their class groups by purely elementary means.

There are three spaces arising in Wright and Yukie's classification, however, that we have not considered in this thesis, and they correspond (from the point of view of Lie groups) to D_5, E_7, E_8 respectively. Again, it is interesting to ask whether the integer orbits in these spaces too might have intrinsic interpretations. We believe, in fact, that the integer orbits in these spaces should correspond to quadratic ideal classes, cubic rings, and quintic rings, respectively. We hope to treat these cases more carefully in a future article.

In 1974, Sato and Shintani [23] developed, for prehomogeneous vector spaces, a theory of zeta functions defined as certain sums over integer orbits. It may be interesting from the point of view of prehomogeneous vector spaces to ask how arithmetic interpretations of integer orbits, such as those given here, might correspond to

data (special values, functional equations, etc.) of the associated Sato-Shintani zeta functions.

6.4 Computational applications

As we stated at the outset, Gauss's law of composition is still the best known way for performing computations in the class group of quadratic fields; similarly, the Delone-Faddeev parametrization still gives the best known methods for computing cubic fields.* It is our hope that the higher composition laws presented here will additionally yield the best known algorithms for computing the class groups of cubic fields, the 3-parts of the class groups of quadratic fields, the 2-parts of the class groups of cubic fields, as well as quartic fields.

*Optimized implementations of these algorithms, due to Shanks and Belabas respectively, may be found in [3] and [4] respectively.

Summary of Higher Composition Laws				
Space	Group acting	Parametrizes	Dim.	Lie G.
$\{0\}$	-	Linear rings	0	-
$\tilde{\mathbb{Z}}$	$SL_1(\mathbb{Z})$	Quadratic rings	1	A_1
$(\mathrm{Sym}^2\mathbb{Z}^2)^*$ (GAUSS'S LAW)	$SL_2(\mathbb{Z})$	Ideal classes in quadratic rings	3	B_2
$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$	$SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$	Ideal classes in quadratic rings	6	C_3
$\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$	$SL_2(\mathbb{Z}) \times GL_4(\mathbb{Z})$	Ideal classes in quadratic rings	12	D_5
$\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$	$SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ $\times SL_2(\mathbb{Z})$	Pairs of ideal classes in quadratic rings	8	D_4
$\mathrm{Sym}^3\mathbb{Z}^2$	$SL_2(\mathbb{Z})$	Order 3 ideal classes in quadratic rings	4	G_2
$(\mathrm{Sym}^3\mathbb{Z}^2)^*$	$GL_2(\mathbb{Z})$	Cubic rings	4	G_2
$\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$	$SL_2(\mathbb{Z}) \times GL_6(\mathbb{Z})$	Cubic rings	12	E_7
$\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$	$GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ $\times SL_3(\mathbb{Z})$	Ideal classes in in cubic rings	18	E_6
$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$	$GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$	Order 2 ideal classes in cubic rings	12	F_4
$(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3)^*$	$GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$	Quartic rings	12	F_4
$\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$	$SL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$	Quintic rings[†]	40	E_8

[†]Conjectural.

Bibliography

[1] A. M. Baily, On the density of discriminants of quartic fields, *J. Reine Angew. Math.* **315** (1980), 190–210.

[2] J.W.S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, Academic Press, Inc., London, 1978.

[3] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1993.

[4] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics **193**, Springer-Verlag, New York, 2000.

[5] H. Cohen, Diaz, and Olivier, Counting Discriminants of Number Fields of Degree up to Four, *Algorithmic Number Theory*, Berlin, 2000, 269–283.

[6] H. Cohen and J. Martinet, Étude heuristique des groupes de classes des corps de nombres, *J. Reine Angew. Math.* **404** (1990), 39–76.

[7] H. Cohen and J. Martinet, Heuristics on class groups: some good primes are not too good, *Math. Comp.* **63** (1994), no. 207, 329–334.

[8] B. Datskovsky and D. J. Wright, The adelic zeta function associated to the space of binary cubic forms II. Local theory, *J. Reine Angew. Math.* **367** (1986), 27–75.

[9] H. Davenport, On a principle of Lipshitz, *J. London Math. Soc.* **26** (1951), 179–183.

[10] H. Davenport, On the class-number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.

[11] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.

[12] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.

[13] P.G.L. Dirichlet, *Zahlentheorie*, 4th. edition, Vieweg Brunswick, 1894.

[14] V. Ennola, Veikko and R. Turunen, On totally real cubic fields, *Math. Comp.* **44** (1985), no. 170, 495–518.

[15] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, preprint.

[16] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[17] B. H. Gross, Fourier coefficients for G_2, preprint.

[18] H. Heilbronn, On the 2-Classgroup of Cubic Fields, *Studies in Pure Math.* (1971), 117–119.

[19] J. Nakagawa, Orders of a quartic field, *Mem. Amer. Math. Soc.* **122** (1996), no. 583.

[20] J. Nakagawa, On the relations among the class numbers of binary cubic forms, *Invent. Math.* **134** (1998), no. 1, 101–138.

[21] Y. Ohno, A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms, *Amer. J. Math.* **119** (1997), no. 5, 1083–1094.

[22] M. Sato and T. Kimura, A classification of irreducible prehomogeneous vector spaces and their relative invariants, *Nagoya Math. J.* **65** (1977), 1–155.

[23] M. Sato and T. Shintani, On zeta functions associated with prehomogeneous vector spaces, *Ann. of Math.* (2) **100** (1974), 131–170.

[24] E. B. Vinberg, On the classification of the nilpotent elements of graded Lie algebras, *Soviet Math. Dokl.* **16** (1975), 1517–1520.

[25] D. J. Wright and A. Yukie, Prehomogeneous vector spaces and field extensions, *Invent. Math.* **110** (1992), 283–314..

[26] A. Yukie, *Shintani zeta functions*, London Mathematical Society Lecture Note Series **183**, Cambridge University Press, Cambridge, 1993.