Moduli Spaces for Rings and Ideals

Melanie Eggers Matchett Wood

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
by the Department of
Mathematics
Adviser: Manjul Bhargava

June 2009

Abstract

The association of algebraic objects to forms has had many important applications in number theory. Gauss, over two centuries ago, studied quadratic rings and ideals associated to binary quadratic forms, and found that ideal classes of quadratic rings are exactly parametrized by equivalence classes of integral binary quadratic forms. Delone and Faddeev, in 1940, showed that cubic rings are parametrized by equivalence classes of integral binary cubic forms. Recently, Bhargava has showed that quartic rings (with cubic resolvents) are parametrized by classes of pairs of integral ternary quadratic forms, and that quintic rings (with sextic resolvents) are parametrized by quadruples of integral alternating quinary forms. Bhargava has also studied ideals in quadratic and cubic rings, and found that they are associated to pairs of 2 by 2 and 3 by 3 integral matrices. Birch, Merriman, Nakagawa, Corso, Dvornicich, and Simon have all studied rings associated to binary forms of degree n for any n, but it has not previously been known which rings, and with what additional structure, are associated to binary forms.

In this thesis, we explain exactly what algebraic structures are parametrized by binary n-ic forms, for all n. The algebraic data associated to an integral binary n-ic form includes a rank n ring, an ideal class for that ring, and a condition on the ring and ideal class that comes naturally from geometry. We also give a different story for what is parametrized by integral binary quartic forms, namely, binary quartic forms parametrize quartic rings with a monogenic cubic resolvent. We further show that classes of pairs of n by n matrices parametrize the ideal classes of rings associated to binary n-ic forms.

In fact, we prove these parametrizations when any base scheme replaces the integers, and show that the correspondences between forms and the algebraic data are functorial in the base scheme. We also give geometric constructions of the rings and ideals from the forms that parametrize them. This geometric approach allows us to also give a statement of Gauss composition, the parametrization of ideal classes of quadratic rings by binary quadratic forms, over an arbitrary base scheme. We give an analog of Bhargava's parametrization of quartic rings over an arbitrary base scheme, including a geometric construction of a quartic ring from a pair of ternary quadratic forms that works even in degenerate cases and commutes with base change. We also give a subspace of pairs of ternary quadratic forms that parametrizes quartic rings with quadratic subrings, which includes orders in quartic fields whose Galois closure has Galois group D_4.

Acknowledgements

I would like to thank my advisor, Manjul Bhargava, for asking so many wonderful questions that led me into the mathematics in this thesis and elsewhere, and for helpful conversations while I was pursing the answers. I would also like to thank him for his support, encouragement, and advice throughout my years as a graduate student. I would like to thank the mathematicians who have answered my many algebraic geometry questions, in particular, Vivek Shende, Rahul Pandharipande, Max Lieblich, Barbara Fantechi, and Bhargav Bhatt. Thank you to Manjul Bhargava, Christopher Skinner, Lenny Taelman, and Asher Auel for comments on earlier drafts of this thesis that led to many improvements and far fewer typos. I am grateful for the financial support of the National Science Foundation Graduate Fellowship, the National Defense Science and Engineering Graduate Fellowship, the Josephine De Kármán Fellowship, and the American Association of University Women Dissertation Fellowship. Finally, I would like to thank Andrew Wiles and Peter Sarnak for helpful conversations about my work as I prepare for the next stage of my mathematical career, and for serving on my thesis defense committee.

Contents

Chapter 1

Introduction

There has been a long history of studying algebraic objects associated to forms. Gauss [25], over two centuries ago, studied quadratic rings and ideals associated to binary quadratic forms, and found that ideal classes of quadratic rings are exactly parametrized by equivalence classes of integral binary quadratic forms. Birch and Merriman [8] and Nakagawa [35] studied rank n rings (rings isomorphic to $\mathbb{Z}^n$ as $\mathbb{Z}$-modules) associated to integral binary forms of degree n. These rings have further been studied by Del Corso, Dvornicich, and Simon [18], who determined the splitting of the prime p in such a ring in terms of the factorization of the binary n-ic form modulo p^k. In [38], Simon constructed an ideal class of the associated ring from a binary n-ic form, and in [37] this ideal class was applied to study integer solutions to equations of the form $Cy^d = F(x, z)$, where F is a binary form. Bhargava [4, 5] studied ideals in quadratic and cubic rings, and found that they are associated to pairs of 2 by 2 and 3 by 3 integral matrices. Through these associations he found another parametrization of ideal classes of quadratic rings (different from, but related to Gauss's) and a new parametrization of ideal classes in cubic rings. Morales [34, 33] studied ideal classes in rank n rings that are associated to pairs of symmetric n by n matrices, and found a relation to the 2-part of the class group of the rings. Bhargava obtained a similar but more exact relation between pairs of symmetric n by n integral matrices and the 2-part of the class group of rank n rings in the cases $n = 2$ and 3.

Parametrizations of, or moduli spaces for, rings of low rank have also been found among forms. Delone and Faddeev [21] showed that cubic rings are parametrized by equivalence classes of integral binary cubic forms (see also the work of Davenport and Heilbronn [17] and Gan, Gross, and Savin [24]). Bhargava [6, 7] showed that quartic rings (with cubic resolvents) are parametrized by classes of pairs of integral ternary quadratic forms, and that quintic rings (with sextic resolvents) are parametrized by quadruples of integral alternating quinary forms.

Binary forms have played an important role in the above story. In this thesis, we explain exactly what algebraic structures are parametrized by binary n-ic forms, for all n (Chapter 3). The algebraic data associated to an integral binary n-ic form includes a rank n ring, an ideal class for that ring, and a condition on the ring and ideal class that comes naturally from geometry. We also give a different story for what is parametrized by binary quartic forms. Integral binary quartic forms parametrize

quartic rings with a monogenic cubic resolvent. We use a geometric point of view to relate these two stories (Chapter 4). We further find a space that parametrizes all the ideal classes of rings associated to binary n-ic forms (Chapter 5).

We can think of these orbit spaces that parametrize algebraic structures geometrically. For example, GL_2 classes of binary cubic forms are the space $\mathbb{A}^4/\mathrm{GL}_2$. One approach is to then use a fundamental domain over $\mathbb{Z}$ to associate the algebraic objects of interest with lattice points in a region. From this point of view, geometry of numbers can sometimes be applied to count the associated algebraic objects. This approach has been applied successfully by Davenport and Heilbronn [17] to count the density of discriminants of cubic fields (the number of cubic fields of discriminant X asymptotically in X). Bhargava [2, 3] used this approach to count the density of discriminants of quartic and quintic fields whose Galois closure has group S_4 or S_5, respectively.

One can also use a reduction theory to choose representative lattice points for each algebraic object. This has been very useful for doing computations with the algebraic objects in the parametrization. Binary quadratic forms, with their reduction theory, have long been the basis of computations made about ideal classes in quadratic rings (see [16]). Binary cubic forms are also used to make computations with cubic rings and fields, such as tables of all cubic fields up to some large discriminant (see [1]).

We can also take a more abstract geometric view of the orbit spaces that parametrize algebraic objects. For example, the stack $[\mathbb{A}^4/\mathrm{GL}_2]$ is isomorphic to the moduli stack of cubic rings over a base scheme. From this point of view, these parametrization spaces are like moduli spaces in geometry, except that their points correspond to algebraic objects. One naturally then works over an arbitrary base scheme S, and then looks for a geometric representation of a functor that gives certain algebraic data over S (for example, a locally free $\mathcal{O}_S$-algebra of rank n, a module for that algebra, and perhaps some other data). This is the point of view we take in this thesis. We prove results mostly over an arbitrary base scheme S that are functorial in the base. We also give geometric constructions of the algebraic objects from their associated forms.

The results described above about the rings and ideal classes parametrized by binary n-ic forms and the parametrization of all ideal classes in rings associated to binary n-ic forms are proven over a general base scheme S. Our geometric approach allows us to give a totally general statement of Gauss composition, the parametrization of ideal classes in quadratic rings by binary quadratic forms, over any base scheme (Chapter 2). It also allows us to generalize Bhargava's parametrization of quartic rings to a moduli space for locally free $\mathcal{O}_S$-algebras of rank 4, along with cubic resolvent algebras, over a base scheme S (Chapter 6). Casnati and Ekedahl [13] have given a parametrization of Gorenstein degree 4 covers of an integral base scheme, and Deligne [20] has given a parametrization of "aligned" degree 4 covers of an arbitrary base scheme. The work of Chapter 6 generalizes these parametrizations to degree four covers with cubic resolvents over an arbitrary base, and proves that these constructions are the same as Bhargava's. We also investigate where special quartic algebras lie in this moduli space, in particular the ones with quadratic subalgebras. Over $\mathbb{Z}$, we see that any quartic order in a field whose Galois closure has

group D_4 will have a quadratic subring, and thus we have a parametrization of such D_4 rings (Chapter 7).

Each chapter in this thesis has a long introduction to orient the reader to the work of that chapter. The chapters can be read independently, but contain many references to work in other chapters.

Chapter 2

Gauss composition over an arbitrary base

2.1 Introduction

The classical theorems relating binary quadratic forms $ax^2+bxy+cy^2$ with $a, b, c \in \mathbb{Z}$ and ideal classes in quadratic rings have seen tremendous application. In this chapter, we give a generalization of those theorems when $\mathbb{Z}$ is replaced by an arbitrary base ring or scheme (Theorems 2.1.3, 2.5.1, and 2.5.2). We state the classical theorems now in a modern language.

Theorem 2.1.1. *There is a bijection*

$$\left\{\begin{array}{l}\textit{twisted } \mathrm{GL}_2(\mathbb{Z})\textit{-equivalence classes}\\ \textit{of non-degenerate binary quadratic}\\ \textit{forms}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C, I),\\ \textit{with } C \textit{ a non-degenerate oriented}\\ \textit{quadratic ring, and } I \textit{ a full ideal}\\ \textit{class of } C\end{array}\right\}.$$

This bijection is discriminant preserving, i.e. if $f \leftrightarrow (C, I)$ *then* $\operatorname{disc} f = \operatorname{disc} C$.

A *quadratic ring* is a ring that is a free rank 2 $\mathbb{Z}$-module under addition. An ideal I of a quadratic ring is *full* if it is rank 2 as a $\mathbb{Z}$-module. (When C is a domain, full is equivalent to non-zero.) A form or ring is *non-degenerate* if its discriminant is non-zero. An *oriented quadratic ring* is a quadratic ring R with a choice of generator of $R/\mathbb{Z}$ (there are two choices), and an isomorphism of oriented quadratic rings must preserve this generator. The most subtle issue in Theorem 2.1.1 is the $\mathrm{GL}_2(\mathbb{Z})$ action. An element $g = \left(\begin{smallmatrix} k & \ell \\ m & n \end{smallmatrix}\right)$ acts on a form $f(x, y) = ax^2 + bxy + cy^2$ by

$$g \circ f = \frac{1}{\det g} f(kx + \ell y, mx + ny).$$

We will call this the *twisted* $\mathrm{GL}_2(\mathbb{Z})$ action on binary quadratic forms.

It is interesting to note that quadratic rings are in bijection with integers D congruent to 0 or 1 modulo 4; the bijection is given by the discriminant of the quadratic ring. The condition that the quadratic ring is *oriented* may seem unnatural, and if we wish to remove it, we obtain the following theorem.

Theorem 2.1.2. *There is a bijection*

$$\left\{\begin{array}{l}\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z}) \text{ equivalence} \\ \text{classes of non-degenerate binary} \\ \text{quadratic forms}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{isomorphism classes of } (C, I), \text{ with} \\ C \text{ a non-degenerate quadratic ring} \\ \text{and } I \text{ a full ideal class of } C\end{array}\right\}.$$

This isomorphism is discriminant preserving.

In this theorem, $\mathrm{GL}_1(\mathbb{Z})$ acts on a form by $(k) \circ f = kax^2 + kbxy + kcy^2$. This allows multiplication of the form by -1. When we also act by $\mathrm{GL}_1(\mathbb{Z})$, we can change the $\mathrm{GL}_2(\mathbb{Z})$ action by any twist without changing the equivalence classes, and so here we may as well consider the most natural (non-twisted) $\mathrm{GL}_2(\mathbb{Z})$ action

$$g \circ f = f(ax + by, cx + dy).$$

Given that we can remove the oriented condition and use a more natural $\mathrm{GL}_2(\mathbb{Z})$ action, Theorem 2.1.2 seems the more natural theorem. In this chapter we will see how both of these theorems fit into a larger framework, and we will remove the non-degeneracy condition (see Theorem 2.4.3 over $\mathbb{Z}$).

Theorems 2.1.1 and 2.1.2 are called *Gauss composition* because they give a composition law on binary quadratic forms with the same discriminant, given by multiplication of ideal classes. Classically, such as in Gauss's original work [25], it was more common to work with an $\mathrm{SL}_2(\mathbb{Z})$ action, but the theorems were similar. When one works with the $\mathrm{SL}_2(\mathbb{Z})$ actions (see for example [16, Section 5.2]) then one has to make adjustments such as only working with the narrow class group or only working with positive definite quadratic forms (in the definite case). Given this beautiful and extremely useful correspondence over the integers, one naturally wonders what happens when the integers are replaced by other rings, or if one is inclined to think geometrically, when the integers are replaced by the sheaf of functions on another scheme. In this chapter, we give the Gauss composition correspondence over an arbitrary base scheme S. In the case $S = \operatorname{Spec} R$, we have the correspondence over an arbitrary base ring R.

We now give the definitions necessary to work over an arbitrary scheme. The most important change from $\mathbb{Z}$ to a scheme S is that previously we allowed the quadratic form to have variables x and y which generate a free rank 2 $\mathbb{Z}$-module and thus were acted on by $\mathrm{GL}_2(\mathbb{Z})$. Over an arbitrary scheme S, we allow the variables of the binary form to be in a locally free rank 2 $\mathcal{O}_S$-module instead of just a free module. (Over $\mathbb{Z}$ all locally free modules are free.) A *binary quadratic form* over S is a locally free rank 2 $\mathcal{O}_S$-module V and a global section $f \in \operatorname{Sym}^2 V$. (See the Notation section at the end of this introduction for some remarks on the notion of *locally free*.) Isomorphisms of binary quadratic forms (V, f) and (V', f') are given by isomorphisms $V \to V'$ that send f to f'. The notion of isomorphism classes of binary quadratic forms replaces $\mathrm{GL}_2(\mathbb{Z})$-equivalence. Over $\mathbb{Z}$, isomorphism classes of binary quadratic forms correspond exactly to non-twisted $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of binary quadratic forms.

Now, we take a different point of view on our above $\mathrm{GL}_1(\mathbb{Z})$ action. We could consider a form $f = ax^2z + bxyz + cy^2z$ and then view our above $\mathrm{GL}_1(\mathbb{Z})$ action as the

invertible changes of coordinates in the z variable (which over $\mathbb{Z}$ are just multiplication by ± 1). Then analogously to our above transition to an arbitrary scheme S, we make the following definition. A *linear binary quadratic form* over S is a locally free rank 2 $\mathcal{O}_S$-module V, a locally free rank 1 $\mathcal{O}_S$-module L, and a global section $f \in \operatorname{Sym}^2 V \otimes L$. Isomorphisms are given by isomorphisms $V \to V'$ and $L \to L'$ that send $f \mapsto f'$. Over $\mathbb{Z}$, isomorphism classes of linear binary quadratic forms correspond exactly to the $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z})$ equivalence classes described in Theorem 2.1.2. A *quadratic algebra* C over S is a locally free rank 2 $\mathcal{O}_S$-algebra. A C-module M is *traceable* if M is a locally free rank 2 $\mathcal{O}_S$-module and if C and M give the same trace map $C \to \mathcal{O}_S$. We now are ready to give the main theorem of Gauss composition over an arbitrary base.

Theorem 2.1.3. *There is a bijection*

$$\left\{\begin{array}{l}\textit{isomorphism classes of linear bi-}\\ \textit{nary quadratic forms/}S\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C,M),\\ \textit{with } C \textit{ a quadratic algebra/}S\textit{, and}\\ M \textit{ a traceable } C\textit{-module}\end{array}\right\}.$$

Given (C, M) and a corresponding $f \in \operatorname{Sym}^2 V \otimes L$, we have $M \cong V$ as $\mathcal{O}_S$-modules and

$$C/\mathcal{O}_S \cong \wedge^2 V^* \otimes L^*$$

as $\mathcal{O}_S$-modules. An isomorphism of pairs (C, M) and (C', M') is given by an isomorphism $C \cong C'$ of $\mathcal{O}_S$-algebras, and an isomorphism $M \cong M'$ as $\mathcal{O}_S$-modules that respects the C (or C') module structure.

In the case when $S = \operatorname{Spec} \mathbb{Z}$ and we consider only non-degenerate objects, we recover the classical Theorem 2.1.2. We give a simple and concrete proof of Theorem 2.1.3 in Section 2.2. We also reinterpret the proof in terms of moduli stacks. Theorem 2.1.3 comes from an isomorphism of moduli stacks parametrizing linear binary quadratic forms on the one hand and parametrizing quadratic algebras and their traceable modules on the other. The content of the "isomorphism of moduli stacks" result is that the bijection of Theorems 2.1.3 commutes with base change of the scheme S or ring R (when $S = \operatorname{Spec} R$). Moreover, we give explicit descriptions of the bijection maps in terms of bases for the ring and module (which describe the map locally on the base scheme) as well as global descriptions of the bijection, both geometric and algebraic (see Section 2.3).

There has been previous work done to generalize Gauss composition (see [12], [15], [29], [40]), usually with conditions on the base ring (for example, that it is a Bezout domain or that 2 is not a zero-divisor), with conditions on the forms and modules (for example, free, primitive, invertible), or with orientations of the rings or modules. In this work we are able to give a complete theorem without any such conditions. The closest previous work is that of Kneser [30], who works over an arbitrary ring and gives a construction of quadratic algebras and modules from quadratic maps using Clifford algebras. Kneser mainly studies composition of two modules and does not formulate a theorem in the style of this work. Lenstra has given a talk [31] based on Kneser's work in which he suggested theorems for primitive forms and invertible

modules in the style of this work. In Section 2.6, we give a closer comparison of our terminology and results to those of Kneser. Our work introduces definitions and a framework that are used to study binary forms of degree n in Chapter 3, which gives bijection theorems in the style of Theorem 2.1.3 for binary forms of degree n. The global geometric and algebraic constructions of this chapter can be generalized to binary forms of degree n and are critical to the study of such forms in Chapter 3. Besides its independent interest, this chapter is an introduction to and motivation for the results of Chapter 3.

A linear binary quadratic form is *primitive* if everywhere locally where V and L are free (and x, y is a basis for V and z is a basis for L), f can be written as $ax^2z + bxyz + cy^2z$, where a, b, c generate the unit ideal in $\mathcal{O}_S$. A form over $\mathbb{Z}$ is *primitive* if its coefficients generate the unit ideal in $\mathbb{Z}$, and over $\mathbb{Z}$, primitive forms correspond exactly to the invertible ideal classes. We can understand precisely which modules primitive forms correspond to in general.

Theorem 2.1.4. *In the bijection of Theorem 2.1.3, primitive linear binary quadratic forms correspond to (C, M) for which M is a locally free C-module of rank 1, i.e. an invertible C-module. If C is a quadratic $\mathcal{O}_S$-algebra and M is a locally free C-module of rank 1, then M is traceable.*

Note that if M is *locally on S* a free C-module of rank 1, then M is *locally on C* a free C-module of rank 1. It turns out that the converse is true. If M is *locally on C* a free C-module of rank 1, then M is *locally on S* a free C-module of rank 1.

We can also talk about discriminants of quadratic algebras and linear binary quadratic forms over S. The discriminant of a quadratic $\mathcal{O}_S$-algebra C is a global section of $(\wedge^2 C)^{\otimes -2} \cong (C/\mathcal{O}_S)^{\otimes -2}$ given by the determinant of the trace map $C \otimes C \to \mathcal{O}_S$. The discriminant of a linear binary quadratic form $f \in \operatorname{Sym}^2 V \otimes L$ is a global section of $(\wedge^2 V \otimes L)^{\otimes 2}$ which is given locally where V and L are free by $ax^2z + bxyz + cy^2z$ has discriminant $(b^2 - 4ac)((x \wedge y) \otimes z)^2$. We can view the discriminant (in either case) as a pair (N, d), where N is a locally free $\mathcal{O}_S$-module of rank 1 and $d \in N^{\otimes 2}$, with isomorphisms given by isomorphisms $N \cong N'$ sending d to d'.

Theorem 2.1.5. *In the bijection of Theorem 2.1.3, the isomorphism $C/\mathcal{O}_S \cong \wedge^2 V^* \otimes L^*$ gives a map $(C/\mathcal{O}_S)^{\otimes -2} \cong (\wedge^2 V \otimes L)^{\otimes 2}$ which maps the discriminant of (C, M) to the discriminant of f. In other words, the bijection of Theorem 2.1.3 is discriminant preserving.*

We can specialize Theorem 2.1.3 by specifying the locally free rank 1 module L (see Section 2.5). This allows us to give a correspondence for binary quadratic forms over an arbitrary scheme and modules of quadratic algebras. As another specialization, we get a version of Theorem 2.1.1 over an arbitrary base.

Theorem 2.1.3 parametrizes traceable modules for quadratic rings over some base, but the original theorems of Gauss composition are about ideal classes. We can compare traceable modules and ideal classes. To do this we work over an integral domain D. An ideal I of a quadratic D-algebra C is *full* if it is a locally free rank 2

D-module. Two ideals I and I' are *equivalent* if there are non-zero-divisors $c, c' \in C$ such that $cI = c'I'$, and this equivalence defines ideal classes. Over a domain, an object is *degenerate* if its discriminant is zero.

Proposition 2.1.6. *When D is a domain, and C is a non-degenerate quadratic D-algebra, all traceable C-modules are realized as full ideals of C and all full ideals of C are traceable C-modules. Two full ideals of C are in the same ideal class if and only if they are isomorphic as modules.*

Corollary 2.1.7. *When D is a domain, there is a discriminant preserving bijection*

$$\left\{\begin{array}{l}\textit{isomorphism classes of non-}\\ \textit{degenerate linear binary quadratic}\\ \textit{forms/}D\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C,I),\\ \textit{with } C \textit{ a non-degenerate quadratic}\\ \textit{algebra/}D\textit{, and } I \textit{ a full ideal class}\\ \textit{of } C\end{array}\right\}.$$

Note that we do not require C to be a domain. When C is a degenerate quadratic D-algebra, there are traceable modules which do not occur as ideals of C. However, since these modules do correspond to linear binary quadratic forms we see that traceable modules are naturally included in the most complete theorem.

2.1.1 Outline of the chapter

In Section 2.2, we prove Theorems 2.1.3, 2.1.4, and 2.1.5 and give a local explicit description of the bijection of Theorem 2.1.3. In Section 2.3, we give a global geometric construction of (C, M) from a linear binary quadratic form and a global algebraic construction of a linear binary quadratic form from a pair (C, M). In Section 2.4, we relate traceable modules to ideals in order to understand Theorem 2.1.3 in terms of ideals when the base is an integral domain. We also give Theorem 2.1.3 over $\mathbb{Z}$ and see that not all the modules in the theorem are realizable as ideals. In Section 2.5, we specialize Theorem 2.1.3 to forms $f \in \operatorname{Sym}^2 V \otimes L$ with a given L, and recover a version of Theorem 2.1.1 over an arbitrary scheme. Finally, in Section 2.6 we relate our terminology and results to those of Kneser [30], who worked on Gauss composition over an arbitrary base ring.

Notation. Given an $\mathcal{O}_S$-module P, we let P^* denote the $\mathcal{O}_S$-module $\mathcal{H}om(P, \mathcal{O}_S)$, even when P is also a module for some other $\mathcal{O}_S$-algebra. Given a sheaf $\mathcal{G}$ on S, we write $x \in \mathcal{G}$ to denote that x is a global section of $\mathcal{G}$. We use $\operatorname{Sym}_k V$ to denote the submodule of $V^{\otimes k}$ that is fixed by the S_k action, and we use $\operatorname{Sym}^k V$ to denote the usual quotient of $V^{\otimes k}$. We use $\mathbb{P}(V)$ to denote $\operatorname{Proj} \operatorname{Sym}^* V$.

Normally, in the language of algebra, one says that an R-module M is locally free of rank n if for all prime ideals $\wp$ of R, the localization $M_\wp$ is free of rank n; in the geometric language we would describe this situation as "M is free in every stalk." However, if we have a scheme S and an $\mathcal{O}_S$-module M, we normally say that M is locally free of rank n if on some open cover of S it is free of rank n; in the algebraic language this is equivalent to saying that for every prime ideal $\wp$ of R, there is an $f \in R \setminus \wp$ such that the localization M_f is free of rank n. It turns out that over a

ring, the geometric condition of locally free of rank n is equivalent to being finitely generated and having the algebraic condition of locally free of rank n ([10, II.5.3, Theorem 2]). In this thesis, we use the geometric notion of locally free of rank n, even when working over a ring.

2.2 Proof of Theorem 2.1.3

We give a simple proof of Theorem 2.1.3.

Key Construction. Given a linear binary quadratic form $f \in \operatorname{Sym}^2 V \otimes L$, we we construct C and M as $\mathcal{O}_S$-modules as follows:

$$C = \mathcal{O}_S \oplus \wedge^2 V^* \otimes L^* \qquad M = V. \tag{2.1}$$

Next, we need to specific the algebra and C-module structure of C and M respectively. First, consider the case then V and L are free such that $V = \mathcal{O}_S x \oplus \mathcal{O}_S y$ and $L = \mathcal{O}_S z$. We rename $(1,0)$ and $(0,(x^* \wedge y^*) \otimes z^*)$ of C to 1 and τ. Suppose $f = ax^2z + bxyz + cy^2z$. Now we let 1 be the multiplicative identity of C, and let the rest of the algebra and module structures be as follows:

$$\tau^2 = -b\tau - ac \qquad \tau x = -cy - bx \qquad \tau y = ax$$

This gives M the structure of a traceable C-module. Also note that $\operatorname{disc} f = (b^2 - 4ac)((x \wedge y) \otimes z)^2 = \operatorname{disc} C$.

For a general f, we need to specify the algebra and module structures of C and M by giving $C \otimes C \to C$ and $C \otimes M \to M$ satisfying the axioms of rings and modules. Since the module of such homomorphisms is a sheaf, it suffices to give the algebra and module structures locally when V and L are free, which is what we have done above. To see that the local definitions agree on overlaps, we just check that if we had chosen different bases for the free V and L that we would have gotten the same algebra and module structure on C and M. This is a simple computation. Also note that $\operatorname{disc} f$ and $\operatorname{disc} C$ correspond in the isomorphism $(\wedge^2 V \otimes L)^{\otimes 2} \cong (C/\mathcal{O}_S)^{\otimes -2}$ because they correspond locally.

Given a quadratic $\mathcal{O}_S$-algebra C and a traceable C-module M we can construct $\mathcal{O}_S$-modules $V = M$ and $L = \wedge^2 V^* \otimes (C/\mathcal{O}_S)^*$. In the case that C and M are free $\mathcal{O}_S$-modules, we can choose bases for $1, \tau$, and x, y for C and M respectively, such that

$$\tau x = -cy - bx \quad \text{and} \quad \tau y = ax$$

for some $a, b, c \in \mathcal{O}_S$. (Shifting τ by an element of $\mathcal{O}_S$ if necessary, we can ensure that τy is a multiple of a and we call such a basis $1, \tau$ *normalized*.) If $\tau^2 = -q\tau - r$ with $q, r \in \mathcal{O}_S$, then the traceability condition tells us that $q = b$ and the condition that $\tau^2 = -q\tau - r$ tells us that $r = ac$. From this (C, M) we can construct a form $ax^2z + bxyz + cy^2z$, where $z = x^* \wedge y^* \otimes \bar{\tau}^*$ and $\bar{\tau}$ is the image of τ in $C/\mathcal{O}_S$.

Now for an arbitrary (C, M), this construction specifies $f \in \mathrm{Sym}^2 V \otimes L$ locally on S where C and M are free $\mathcal{O}_S$-modules. To see that the local definitions of f agree on overlaps, we can do a simple computation to see that if we had chosen a different basis for M, and a different normalized basis for C, we would get the same form.

The constructions of the above two paragraphs are inverse to each other, because we see they are locally inverse by construction. Thus we have proved the bijection of Theorem 2.1.3, as well as Theorem 2.1.5 which says that Theorem 2.1.3 is discriminant preserving.

2.2.1 Primitive forms

If we had a form such that V and L were free as above and $f = ax^2z+bxyz+cy^2z$ with a, b, c generating $\mathcal{O}_S$ as an $\mathcal{O}_S$-module, then we also have $a, a+b+c, c$ generating $\mathcal{O}_S$ as an $\mathcal{O}_S$-module. We can cover S by subsets D_a, D_{a+b+c}, D_c on which $a, a+b+c, c$ are invertible respectively. By changing the basis of V on D_{a+b+c} and D_c we can assume that a is invertible in each open subset. By changing the basis of V again, we can assume that $a = 1$. When $a = 1$, we see that M, as given by the Key Construction, is a free rank 1 C-module.

On the other hand, if C is a free $\mathcal{O}_S$-module and if M is a free C-module of rank 1, then we can choose a $\mathcal{O}_S$-module basis x and y of M and a $\mathcal{O}_S$-module basis $1, \tau$ of C such that

$$\tau^2 = -b\tau - c, \quad \tau x = -cy - bx \quad \text{and} \quad \tau y = x$$

with $b, c \in \mathcal{O}_S$. Such a (C, M) gives a form $x^2z + bxyz + cy^2z$, which is primitive. So we see that in the bijection of Theorem 2.1.3, primitive forms correspond exactly to (C, M) such that locally on S, we have M a free C-module of rank 1. Note that any module which is locally on S a free C-module of rank 1 is traceable. Thus we conclude that in the bijection of Theorem 2.1.3, primitive forms correspond to M which are locally on S free C-modules of rank 1, proving Theorem 2.1.4

2.2.2 Moduli stacks

Another way to see the proof of Theorem 2.1.3 is as follows.

Theorem 2.2.1. *There is an equivalence of moduli stacks between the moduli stack of linear binary quadratic forms and the moduli stack of pairs (C, M) where C is a quadratic algebra and M is a traceable C-module.*

Proof. This is just another way of formalizing the above argument. We can rigidify the two moduli problems of the theorem. We have that $\mathbb{A}^3$ is the moduli scheme $\mathcal{F}_B$ of linear binary quadratic forms (V, L, f) on S with given $V \cong {\mathcal{O}_S}^2$ and $L \cong \mathcal{O}_S$. This is parametrizing linear binary forms with V and L free and with chosen bases. Also, we saw above that $\mathbb{A}^3$ is the moduli scheme $\mathcal{M}_B$ of pairs (C, M) where C is a quadratic $\mathcal{O}_S$-algebra, M is a traceable C-module, and we have given isomorphisms $C/\mathcal{O}_S \cong \mathcal{O}_S$ and $M \cong {\mathcal{O}_S}^2$. This is parametrizing quadratic $\mathcal{O}_S$-algebras C with

traceable modules M, with $C/\mathcal{O}_S$ and M free and with chosen bases. An element $g \in \mathrm{GL}_2$ acts on the isomorphisms of M and V with ${\mathcal{O}_S}^2$ by composing with g and acts on the isomorphism $C/\mathcal{O}_S \cong \mathcal{O}_S$ by composing with $\det g^{-1}$. An element $g \in \mathrm{GL}_1$ acts on the isomorphism $C/\mathcal{O}_S \cong \mathcal{O}_S$ by composing with g^{-1}. This gives an action of the group scheme $\mathrm{GL}_2 \times \mathrm{GL}_1$ on both of the rigidified moduli spaces. The Key Construction of (C, M) from the universal form gives us $\mathcal{F}_B \cong \mathcal{M}_B$ which is equivariant for the $\mathrm{GL}_2 \times \mathrm{GL}_1$ actions. Thus we have an equivalence of the quotient stacks by $\mathrm{GL}_2 \times \mathrm{GL}_1$, which are the moduli stacks in this theorem. □

The bijection of Theorem 2.1.3 is a corollary of this theorem by comparing S points of the two moduli stacks.

2.3 Global descriptions of the bijection

We have proven Theorem 2.1.3, and the maps in the bijection are given locally in a simple and completely explicit form by the Key Construction. We wish now to give global descriptions of the maps in each direction in our bijections.

A linear binary quadratic form f over S defines a closed subscheme S_f of $\mathbb{P}(V)$. We let $\mathcal{O}(k)$ denote the usual sheaf on $\mathbb{P}(V)$ and let $\mathcal{O}_{S_f}(k)$ denote the pullback of $\mathcal{O}(k)$ to S_f. The global functions of S_f give an $\mathcal{O}_S$-algebra and the global sections of $\mathcal{O}_{S_f}(1)$ give a module for that algebra. Whenever $S = \operatorname{Spec} R$ and f is not a zero-divisor, this algebra and module are the (C, M) given locally by the Key Construction. When, for example, $f = 0$, the global functions of S_f are $\mathcal{O}_S$, which is not a quadratic $\mathcal{O}_S$-algebra. In order to extend these simple and natural constructions of C and M to f that may be zero or zero divisors, we use cohomology. In the case of binary cubic forms, such a construction of the ring C was given by Deligne in a letter to Gan, Gross, and Savin [19].

Global Construction of Ring and Ideal. Let $\pi : \mathbb{P}(V) \to S$. We can construct

$$C := H^0 R\pi_* \left(\mathcal{O}(-2) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O} \right), \tag{2.2}$$

and

$$M := H^0 R\pi_* \left(\mathcal{O}(-1) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O}(1) \right). \tag{2.3}$$

Above we are taking the hypercohomology of complexes with terms in degrees -1 and 0. *When f is not a zero-divisor, Equations* (2.2) *and* (2.3) *just say that C is the pushforward of the functions of S_f, the subscheme of $\mathbb{P}(V)$ cut out by f, to S. Also, in this case, M is the pushforward of $\mathcal{O}_{S_f}(1)$ to S.* This is because when the map $\mathcal{O}(k) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O}(k+2)$ is injective, the complex $\mathcal{O}(k) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O}(k+2)$ is chain homotopic to $\mathcal{O}(k+2)/f(\mathcal{O}(k) \otimes \pi^* L^*) \cong \mathcal{O}_{S_f}(k)$ (as a chain complex in the 0th degree). Thus when f is not a zero-divisor, we have $C \cong \pi_*(\mathcal{O}_{S_f})$ and $M \cong \pi_*(\mathcal{O}_{S_f}(1))$.

We see that there is an associative product on the complex $\mathcal{O}(-2) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O}$ given by the action of $\mathcal{O}$ on $\mathcal{O}(-2)$, which gives C the structure of a ring. The map of

$\mathcal{O}$ as a complex in degree 0 to the complex $\mathcal{O}(-2) \xrightarrow{f} \mathcal{O}$ induces $\mathcal{O}_S \cong R^0\pi_*(\mathcal{O}) \to C$, which makes C into an $\mathcal{O}_S$-algebra. The C-module structure on M is given by the following action of the complex $\mathcal{O}(-2) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O}$ on the complex $\mathcal{O}(-1) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O}(1)$:

$$\mathcal{O} \otimes (\mathcal{O}(-1) \otimes \pi^* L^*) \to \mathcal{O}(-1) \otimes \pi^* L^* \quad \mathcal{O} \otimes (\mathcal{O}(-1) \otimes \pi^* L^*) \to \mathcal{O}(-1) \otimes \pi^* L^*$$
$$(\mathcal{O}(-2) \otimes \pi^* L^*) \otimes \mathcal{O}(1) \to \mathcal{O}(-1) \otimes \pi^* L^* \quad (\mathcal{O}(-2) \otimes \pi^* L^*) \otimes (\mathcal{O}(-1) \otimes \pi^* L^*) \to 0,$$

where all maps are the natural ones.

From the short exact sequence of complexes in degrees -1 and 0

$$\begin{array}{ccc} & & \mathcal{O}(k+2) \\ & & \downarrow \\ \mathcal{O}(k) \otimes \pi^* L^* & \xrightarrow{f} & \mathcal{O}(k+2) \\ \downarrow & & \\ \mathcal{O}(k) \otimes \pi^* L^* & & \end{array} \tag{2.4}$$

(where each complex is on a horizontal line and $k = -1$ or -2), we can apply the long exact sequence of cohomology to obtain the exact sequences

$$0 \to \mathcal{O}_S \to C \to (\wedge^2 V^*) \otimes L^* \to 0$$
$$0 \to V \to M \to 0.$$

Thus we have natural isomorphisms of $\mathcal{O}_S$-modules

$$C/\mathcal{O}_S \cong (\wedge^2 V^*) \otimes L^* \quad \text{and} \quad V \cong M \tag{2.5}$$

as claimed in Theorem 2.1.3. So C and M constructed here have the same $\mathcal{O}_S$-module structure as given in the Key Construction, and we can further see that the algebra and C-module structures are also the same.

Proposition 2.3.1. *The constructions of C and M from a form f given in the Global Construction commute with base change and are the same as the Key Construction.*

Proof. They key to this proof is to compute all cohomology of the pushforward of the complex $\mathcal{C}(k) : \mathcal{O}(k-2) \otimes \pi^* L^* \xrightarrow{f} \mathcal{O}(k)$ for $k = 0, 1$. This can be done using the long exact sequence of cohomology from the short exact sequence of complexes given in Equation (2.4) above. In particular, $\mathcal{C}(k)$ does not have any cohomology in degrees other than 0. Since $k \leq 1$, we have that $H^0 R\pi_*(\mathcal{O}(-2+k)) = 0$ and thus $H^{-1} R\pi_*(\mathcal{C}(k)) = 0$. Since, $k \geq -1$ we have that $H^1 R\pi_*(\mathcal{O}(k)) = 0$ and thus $H^1 R\pi_*(\mathcal{C}(k)) = 0$. Moreover, we saw above that $H^0 R\pi_*(\mathcal{C}(k))$ is locally free. Thus since all $H^i R\pi_*(\mathcal{C}(k))$ are flat, by [26, Corollaire 6.9.9], we have that cohomology and base change commute. Base change respects the induced maps between cohomology

sheaves that gave C and M algebra and module structures, respectively, as well as the maps in Equation (2.5).

As in the Key Construction of (C, M) from a form, this construction lifts, using Equation (2.5), to a map $\mathcal{F}_B \to \mathcal{M}_B$ of the rigidified moduli spaces. This is because Equation (2.5) gives a basis for $C/\mathcal{O}_S$ and M from a basis of V and L. So, it suffices to check that on the universal linear binary quadratic form this construction gives the universal pair (C, M). This is proven more generally in an analogue for binary forms of degree n in Chapter 3. □

Global Construction of Form. We now give a global construction of a linear binary quadratic form from quadratic ring and module. Let C be a quadratic $\mathcal{O}_S$-algebra and M be a traceable C-module. There is a natural map

$$\begin{array}{ccc} C/\mathcal{O}_S \otimes \wedge^2_{\mathcal{O}_S} M & \longrightarrow & \operatorname{Sym}^2 M \\ \gamma \otimes m_1 \wedge m_2 & \mapsto & \gamma m_1 \otimes m_2 - \gamma m_2 \otimes m_1 \end{array}.$$

We define $V = M$ and $L = (C/\mathcal{O}_S \otimes \wedge^2_{\mathcal{O}_S} M)^*$ and then the map above gives us an element $f \in \operatorname{Sym}^2 V \otimes L$.

Remark 2.3.2. We can rewrite this construction as

$$\begin{array}{ccc} C/\mathcal{O}_S \otimes \operatorname{Sym}_2 M & \longrightarrow & \wedge^2_{\mathcal{O}_S} M \\ \gamma \otimes m_1 m_2 & \mapsto & \gamma m_1 \wedge m_2 \end{array}.$$

Using the isomorphism $\operatorname{Sym}_2 M^* \otimes \wedge^2 M \cong \operatorname{Sym}_2 M \otimes \wedge^2 M^*$, this gives a binary form of the required form, which one can check is equivalent to the one given above.

This construction clearly commutes with base change. Also, it gives a map $\mathcal{F}_B \to \mathcal{M}_B$ of the moduli space of forms with V and L free with chosen basis to the moduli space of quadratic algebras and traceable modules with C and M free with chosen basis. We can easily check that on the universal (C, M), this construction gives the universal linear binary quadratic form, and thus is inverse to the Key Construction.

2.4 Ideals and modules

We now relate traceable modules to ideals. Recall that an ideal I of a quadratic $\mathcal{O}_S$-algebra C is *full* if it is a locally free rank 2 $\mathcal{O}_S$-module. Two ideals I and I' are *equivalent* if there are non-zero-divisors $c, c' \in C$ such that $cI = c'I'$, and this equivalence defines ideal classes. Over a domain, an object is *degenerate* if its discriminant is zero. We prove the following proposition given in the introduction.

Proposition 2.4.1 (Proposition 2.1.6)**.** *When D is a domain, and C is a non-degenerate quadratic D-algebra, all traceable C-modules are realized as full ideals of C and all full ideals of C are traceable C-modules. Two full ideals of C are in the same ideal class if and only if they are isomorphic as modules.*

Proof. Let K be the fraction field of D. We have that $C \otimes_D K$ is a 2 dimensional K-algebra, generated by 1 and τ. If M is a traceable C-module, then $M \otimes_D K$ is a 2 dimensional K vector space and a $C \otimes_D K$-module. We can put the action of τ on $M \otimes_D K$ into rational normal form. An easy calculation shows that if C is non-degenerate then τ does not have any repeated eigenvalues, and so we can assume that τ acts on $M \otimes_D K$ by $\left(\begin{smallmatrix} 0 & r \\ 1 & q \end{smallmatrix}\right)$ and $\tau^2 = -s\tau - t$ with $q, r, s, t \in K$. Since M is traceable, we have $q = -s$ and since τ^2 must act on M in the same way as $-s\tau - t$ we have $r = -t$. Thus, as $(C \otimes_D K)$-modules, $M \otimes_D K \cong C \otimes_D K$. Since $M \subset M \otimes_D K$, we have realized M as a C-submodule of $C \otimes_D K$. Since M is finitely generated as a C-module, for some non-zero $d \in D$, we have $dM \subset C$. This realizes M as a full ideal of C.

Let I be a full ideal of C. By definition I is a locally free rank 2 D-module. We have that $I \otimes_D K \subset C \otimes_D K$, and since both are two dimensional K vector spaces, we must have equality. So $I \otimes_D K$ and $C \otimes_D K$ give the same trace map from $C \otimes_D K$ to K, which when restricted to C gives the trace maps that I and C give from C to D. Thus I is traceable.

Clearly two ideals in the same ideal class are isomorphic as modules. Suppose we have a module isomorphism of two full ideals $\phi : I \to J$. Since $I \otimes_D K \cong C \otimes_D K$, there is some nonzero element $d \in D \subset C$ such that $d \in I$. We claim that as subsets of C, $\phi(d)I = dJ$. Suppose we have an element $\phi(d)x \in \phi(d)I$ with $x \in I$. We have $\phi(d)x = \phi(dx) = d\phi(x)$ since ϕ is a C-module homomorphism. Thus, $\phi(d)x \in dJ$. Similarly we see that $dJ \subset \phi(d)I$. Thus I and J are in the same ideal class. □

This allows us to deduce Corollary 2.1.7, which presents the bijection of Gauss composition in terms of ideals instead of traceable modules. If we further require our base D to be a Dedekind domain and that C be a domain, then all non-zero ideals of C are full. When D is a domain with fraction field K, it is easy to check that C is a domain if and only if f is irreducible over K. Thus we deduce the following corollary.

Corollary 2.4.2. *When D is a Dedekind domain with fraction field K, there is a discriminant preserving bijection*

$$\left\{\begin{array}{l}\textit{isomorphism classes of non-}\\ \textit{degenerate linear binary quadratic}\\ \textit{forms/}D\textit{ that are irreducible over}\\ K\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C, I),\\ \textit{with } C \textit{ a non-degenerate quadratic}\\ \textit{algebra/}D\textit{ and a domain, and } I \textit{ a}\\ \textit{non-zero ideal class of } C\end{array}\right\}.$$

2.4.1 Theorem 2.1.3 over $\mathbb{Z}$

In Theorem 2.1.3, we remove the condition of non-degeneracy seen in the classical theorems in order to give the most complete theorem. Over $\mathbb{Z}$, there is only one degenerate quadratic ring, but over an arbitrary base, especially one with 0-divisors, much more can occur in the degenerate locus. Moreover, one may want to study quadratic rings and their ideal classes under base change, in which case non-degenerate objects may become degenerate. Over $\mathbb{Z}$, however, when we include the degenerate case, we are already forced to include a module which is not realized as an ideal. We give here

Theorem 2.1.3 and its specialization, Theorem 2.5.2, which will be proven in the next section, when considered over $\mathbb{Z}$.

Theorem 2.4.3. *There are discriminant preserving bijections*

$$\left\{\begin{array}{l}\textit{twisted } \mathrm{GL}_2(\mathbb{Z}) \textit{ equivalence classes}\\ \textit{of binary quadratic forms over } \mathbb{Z}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C,M),\\ \textit{with } C \textit{ a oriented quadratic}\\ \textit{ring/}\mathbb{Z}\textit{, and } M \textit{ a } C\textit{-module that is}\\ \textit{a free rank 2 } \mathbb{Z}\textit{-module such that}\\ C \textit{ and } M \textit{ give the same trace map}\\ C \to R\end{array}\right\}$$

and

$$\left\{\begin{array}{l}\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z}) \textit{ equivalence}\\ \textit{classes of binary quadratic forms}\\ \textit{over } \mathbb{Z}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C,M),\\ \textit{with } C \textit{ a quadratic ring over } \mathbb{Z},\\ \textit{and } M \textit{ a } C\textit{-module which is a free}\\ \textit{rank 2 } \mathbb{Z}\textit{-module such that } C \textit{ and}\\ M \textit{ give the same trace map } C \to R\end{array}\right\}.$$

The 0 form corresponds to the ring $\mathbb{Z}[\tau]/\tau^2$ and the module $\mathbb{Z}x \oplus \mathbb{Z}y$ where τ annihilates x and y. This module cannot be realized as an ideal of $\mathbb{Z}[\tau]/\tau^2$, and so even when the base is $\mathbb{Z}$ we see that we must consider modules and not just ideals to get the most complete theorem.

2.5 Other kinds of binary quadratic forms

We can specialize Theorem 2.1.3 by specifying the locally free rank 1 module L. The linear binary quadratic forms with a given L correspond to (C, M) as above with

$$C/\mathcal{O}_S \cong \wedge^2_{\mathcal{O}_S} M^* \otimes L^*$$

as $\mathcal{O}_S$-modules. This can be thought us as an L-type orientation of (C, M). For example, we can fix $L = \mathcal{O}_S$ to get binary quadratic forms (as defined in Section 2.1), the analog of binary quadratic forms over $\mathbb{Z}$ up to non-twisted $\mathrm{GL}_2(\mathbb{Z})$-equivalence.

Theorem 2.5.1. *There is a discriminant preserving bijection*

$$\left\{\begin{array}{l}\textit{isomorphism classes of binary}\\ \textit{quadratic forms/}S\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C,M),\\ \textit{with } C \textit{ a quadratic algebra/}S\textit{, } M\\ \textit{a traceable } C\textit{-module, and } C/\mathcal{O}_S \cong\\ \wedge^2_{\mathcal{O}_S} M^*\end{array}\right\}.$$

Isomorphisms of (C, M) are required to commute with the isomorphism $C/\mathcal{O}_S \cong \wedge^2_{\mathcal{O}_S} M^*$.

Another useful choice is $L = \wedge^2 V^*$, which is not fixed but rather depends of the V of the form. A *twisted binary quadratic form* over S is a locally free rank 2 $\mathcal{O}_S$-module V and a global section $f \in \mathrm{Sym}^2 V \otimes \wedge^2 V^*$. Isomorphisms of binary quadratic

forms are given by isomorphisms $V \to V'$ that preserve the section. This allows us to specialize to Theorem 2.1.1 because isomorphism classes of twisted binary quadratic forms over $\mathbb{Z}$ correspond exactly to the twisted $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of binary quadratic forms of Theorem 2.1.1.

Theorem 2.5.2. *There is a discriminant preserving bijection*

$$\left\{\begin{array}{l}\textit{isomorphism classes of twisted bi-}\\ \textit{nary quadratic forms/}S\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (C,M),\\ \textit{with } C \textit{ a quadratic algebra/}S,\ M\\ \textit{a traceable } C\textit{-module, and } C/\mathcal{O}_S \cong\\ \mathcal{O}_S\end{array}\right\}.$$

Isomorphisms of (C, M) are required to commute with the isomorphism $C/\mathcal{O}_S \cong \mathcal{O}_S$.

The isomorphism $C/\mathcal{O}_S \cong \mathcal{O}_S$ is an orientation of C, and over $\mathbb{Z}$ is exactly the orientation we defined above. So when $S = \operatorname{Spec}\mathbb{Z}$, Theorem 2.5.2 gives us the first bijection of Theorem 2.4.3, and when we consider only non-degenerate objects we recover the classical Theorem 2.1.1. Of course, we could get similar theorems by choosing some other L, either fixed or as a function of V, such as $(\wedge^2 V)^{\otimes k}$.

The proofs of Theorems 2.5.1 and 2.5.2 are completely analogous to that of Theorem 2.1.3. Moreover, we have global descriptions of the bijections which can be read off from the Global Constructions in Section 2.3. For completeness, we give the moduli stack version of the proofs of the above theorems.

Theorem 2.5.3. *There is an equivalence of moduli stacks between the moduli stack of binary quadratic forms on S and the moduli stack of pairs (C, M) where C is a quadratic $\mathcal{O}_S$-algebra, M is a traceable C-module, and $C/\mathcal{O}_S \cong \wedge^2_{\mathcal{O}_S} M^*$ is given.*

Proof. We can rigidify the two moduli problems of the theorem. We have that $\mathbb{A}^3$ is the moduli scheme ${\mathcal{F}'}_B$ of binary quadratic forms (V, f) on S with given $V \cong {\mathcal{O}_S}^2$. Also, from Section 2.2 we know that $\mathbb{A}^3$ is the moduli scheme ${\mathcal{M}'}_B$ of pairs (C, M) where C is a quadratic $\mathcal{O}_S$-algebra, M is a traceable C-module, and we have given isomorphisms $C/\mathcal{O}_S \cong \wedge^2_{\mathcal{O}_S} M^*$ and $M \cong {\mathcal{O}_S}^2$. An element of $g \in \mathrm{GL}_2$ acts on the isomorphisms of M and V with ${\mathcal{O}_S}^2$ by composing with g and acts on the isomorphism $C/\mathcal{O}_S \cong \mathcal{O}_S$ by composing with $\det g^{-1}$. This gives an action of the group scheme GL_2 on both of these rigidifies moduli spaces. The Key Construction of (C, M) from the universal form gives us ${\mathcal{F}'}_B \cong {\mathcal{M}'}_B$ which is equivariant for the GL_2 actions. Thus we have an equivalence of the quotient stacks by GL_2, which are the moduli stacks in this theorem. □

Theorem 2.5.4. *There is an equivalence of moduli stacks between the moduli stack of twisted binary quadratic forms on S and the moduli stack of pairs (C, M) where C is a quadratic $\mathcal{O}_S$-algebra, M is a traceable C-module, and $C/\mathcal{O}_S \cong \mathcal{O}_S$ is given.*

Proof. We can rigidify the two moduli problems of the theorem. We have that $\mathbb{A}^3$ is the moduli scheme ${\mathcal{F}''}_B$ of twisted binary quadratic forms (V, f) of S with given $V \cong {\mathcal{O}_S}^2$. Also, from Section 2.2 we know that $\mathbb{A}^3$ is the moduli scheme ${\mathcal{M}''}_B$ of pairs (C, M) where C is a quadratic $\mathcal{O}_S$-algebra, M is a traceable C-module, and we

have given isomorphisms $C/\mathcal{O}_S \cong \mathcal{O}_S$ and $M \cong {\mathcal{O}_S}^2$. An element of $g \in \mathrm{GL}_2$ acts on the isomorphisms of M and V with ${\mathcal{O}_S}^2$ by composing with g, which gives an action of the group scheme GL_2 on both of these rigidified moduli spaces. The construction of (C, M) from the universal form gives us ${\mathcal{F}''}_B \cong {\mathcal{M}''}_B$ which is equivariant for the GL_2 actions. Thus we have an equivalence of the quotient stacks by GL_2, which are the moduli stacks in this theorem. □

2.6 Relationship to work of Kneser

In this section, we relate the work of this chapter to the work of Kneser [30] on Gauss composition over an arbitrary base, First we reconcile our terminology with his. Kneser works over an arbitrary ring R, so throughout this section our base with always be a ring R.

Kneser works with *quadratic maps* $q : M \to N$, i.e set maps from M, a locally free rank 2 R-module, to N, a locally free rank 1 R-module, such that for all $r \in R$ and $m \in M$, we have $q(rm) = r^2 q(m)$ and $q(x + y) - q(x) - q(y)$ is a bilinear form on $M \times M$.

Proposition 2.6.1. *Quadratic maps $q : M \to N$ in the sense of Kneser described above are in bijection with linear binary quadratic forms $f \in \mathrm{Sym}^2 M^* \otimes N$, where M and N are R-modules locally free of ranks 2 and 1 respectively.*

Proof. Given an $f \in \mathrm{Sym}^2 M \otimes N$, we naturally obtain a homomorphism from $(\mathrm{Sym}^2 M^*)^* \cong \mathrm{Sym}_2 M$ to N which we call Q. Given $m \in M$ we can define $q(m) = Q(m \otimes m)$. We see that for $r \in R$, we have $q(rm) = Q(rm \otimes rm) = r^2 q(m)$. Also, $q(x + y) - q(x) - q(y) = Q(xy + yx)$ which is bilinear in x and y. Thus q is a quadratic map in Kneser's sense.

Now suppose we have a quadratic map $q : M \to N$ in the sense of Kneser. First assume that M is a free R-module generated by m_1 and m_2. Then we know that $q(r_1 m_1 + r_2 m_2) = r_1^2 q(m_1) = r_2^2 q(m_2) + r_1 r_2 B(m_1, m_2)$, where $B(x, y) = q(x + y) - q(x) - q(y)$ and $r_i \in R$. We can give a map $\mathrm{Sym}_2 M \to N$ by sending $m_i \otimes m_i$ to $r_i^2(q(m_i)$ and $m_1 \otimes m_2 + m_2 \otimes m_1$ to $B(m_1, m_2)$. It is easily checked that the map $\mathrm{Sym}_2 M \to N$ does not depend on the choice of basis of M. Now if M is a locally free R-module, this defines a map $\mathrm{Sym}_2 M \to N$ by defining it on local patches where M is free.

An easy computation for free M shows that these two constructions are inverses locally on R and thus inverses. □

One advantage of the $\mathrm{Sym}^2 M \otimes N$ point of view that we take in this thesis is that it makes it clearer how to base change a form.

Kneser says that a quadratic map is *primitive* if $q(M)$ generates N as an R-module. (Kneser actually only gives this definition for $N = R$.) We can see that primitivity of a quadratic map is a local condition on R. When M is free with basis m_1, m_2, then $q(c_1 m_1 + c_2 m_2) = q(m_1)c_1^2 + (q(m_1 + m_2) - q(m_1) - q(m_2))c_1 c_2 + q(m_2)c_2^2$. If $q(M)$ generates N then $q(m_1), q(m_1 + m_2) - q(m_1) - q(m_2), q(m_2)$ must generate

N as an R-module. Conversely, if $q(m_1), q(m_1+m_2)-q(m_1)-q(m_2), q(m_2)$ generate N, then $q(m_1), q(m_1+m_2), q(m_2)$ and thus $q(M)$ generate N as an R-module. The corresponding linear binary quadratic form (of Proposition 2.6.1) is primitive if and only if $q(m_1), q(m_1+m_2)-q(m_1)-q(m_2), q(m_2)$ generate N, which is also a local condition on R. Thus we conclude the following.

Proposition 2.6.2. *A quadratic map in the sense of Kneser is primitive if and only if the corresponding linear binary quadratic form is primitive.*

Kneser works for most of his paper with quadratic maps $q : M \to R$, which correspond to our binary quadratic forms $f \in \operatorname{Sym}^2 V$. Kneser gives a global algebraic construction, using Clifford algebras, of a quadratic R-algebra C and a C-module M from a quadratic map $q : M \to R$. He sees that primitive maps give invertible C-modules. He shows this function from quadratic maps to pairs (C, M) is neither injective nor surjective and he finds the structure of the kernel and image. In a talk [31], Lenstra suggested that Kneser's construction could be used to given a theorem about quadratic maps along the lines of Theorem 2.5.1 restricted to primitive non-degenerate forms, where the traceable condition does not apepar.

Kneser further gives a global algebraic construction of quadratic maps (corresponding to our linear binary quadratic forms) from (C, M) with M an invertible C-module. Lenstra [31] suggested an algebraic construction of (C, M) from a quadratic map which should provide an inverse construction and thus suggested a theorem along the lines of Theorem 2.1.3 restricted to primitive forms. Lenstra also gave a construction of a quadratic map from (C, M) similar to ours in Section 2.3.

In this chapter we have removed the conditions of primitivity and non-degeneracy to give a bijection for all linear binary quadratic forms which required us to consider non-invertible ideals and introduce the idea of traceable modules. We have given a geometric description of the construction of (C, M). We have provided a new framework of linear binary quadratic forms as elements of $\operatorname{Sym}^2 V \otimes L$ which later in Chapter 3 allows us to study binary forms of degree n over an arbitrary base. Finally, we have given proofs of theorems of Gauss composition over an arbitrary base.

Chapter 3

Rings and ideals parametrized by binary n-ic forms

3.1 Introduction

When one looks for a parametrizing space for degree n number fields, binary n-ic forms are a natural guess. It turns out that for $n = 3$ this guess is correct. We have that $\mathrm{GL}_2(\mathbb{Q})$ classes of binary cubic forms are in bijection with isomorphism classes of cubic $\mathbb{Q}$-algebras and irreducible forms correspond to cubic number fields. Moreover, an analogous result allows the parametrization of orders in those number fields; $\mathrm{GL}_2(\mathbb{Z})$ classes of binary cubic forms are in bijection with isomorphism classes of cubic rings ([21], see also [17], [24], and [6]). For other n, the space of binary n-ic forms parametrizes algebraic data that is more subtle than this. It has long been known that binary quadratic forms parametrize ideal classes in quadratic rings ([25], or see Chapter 2 for a treatment that covers all binary quadratic forms). In this chapter, we construct the algebraic data associated to a binary n-ic form, and determine what algebraic structures are in fact parametrized by binary n-ic forms for all n.

Every binary n-ic form with integral coefficients does have an associated ring. The rings that come from binary n-ic forms are interesting for many reasons in their own right, in particular because we have several other tools to understand these rings. Del Corso, Dvornicich, and Simon have viewed the rings associated to binary n-ic forms as a generalization of monogenic rings and have described how a prime splits in a ring associated to a binary n-ic form in terms of the factorization of the form modulo the prime [18]. They have also given a condition on the form equivalent to the p-maximality of the associated ring. Simon [37] uses the ring associated to a binary form to find a class group obstruction equations of the form $Cy^d = f(x, y)$ having integral solutions (where f is the binary form). Chapter 5 of this thesis finds an explicit moduli space for ideal classes in the rings associated to binary n-ic forms. Thus, we can work explicitly with these rings, prime splitting in them, and their ideal classes.

However, there is more data than the associated ring that is canonically associated

to a binary form, including ideal classes of the ring. Some of these ideal classes have been constructed for irreducible, primitive forms in [38], [18], and [37]. In Section 3.2, we give four different ways to construct the associated ring and ideal classes from a binary form 1) explicitly as a subring of a $\mathbb{Q}$-algebra, 2) by giving the multiplication and action tables, 3) via a simple geometric construction that works when $f \not\equiv 0$, and 4) via a more complicated geometric construction that works in all cases. The geometric constructions answer a question posed by Lenstra at the Rings of Low Rank Workshop in 2006 about giving a basis-free description of the ring associated to a binary form. The final geometric construction was originally given in a letter of Deligne [19] in the case $n = 3$. We see that for $n \neq 2$ the ring associated to a form is Gorenstein if and only if the form is primitive. Also, the ideal classes associated to the form are invertible if and only if the form is primitive. The geometric construction is so simple that we give it here.

A binary n-ic form with integer coefficients describes a subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ which we call S_f. Let $\mathcal{O}(k)$ denote the usual sheaf on $\mathbb{P}^1_{\mathbb{Z}}$ and let $\mathcal{O}_{S_f}(k)$ denote its pullback to S_f. Also, for a sheaf $\mathcal{F}$, let $\Gamma(\mathcal{F})$ be the global sections of $\mathcal{F}$. When $f \not\equiv 0$, the ring associated to the binary n-ic form f is simply the ring of global functions of S_f. The global sections $\Gamma(\mathcal{O}_{S_f}(k))$ have an $\Gamma(\mathcal{O}_{S_f})$-module structure, and for a binary form $f \not\equiv 0$ and $-1 \leq k \leq n-1$, the global sections $\Gamma(\mathcal{O}_{S_f}(k))$ give a module of the ring associated to f which is realizable as an ideal class. When $n = 2$, taking $k = 1$ we obtain the ideal associated to the binary quadratic form in Gauss composition. (This construction gives an ideal even when f is reducible or non-primitive. See Chapter 2 for a complete description of the $n = 2$ case.) When $n = 3$, we expect to obtain canonical modules for the ring since we know binary cubic forms parametrize exactly cubic rings. When $n = 3$, by taking $k = 1$ we obtain the inverse different of the ring associated to the binary cubic form, and in general taking $k = n-2$ gives the inverse different (see Theorem 3.2.4).

Given a form f, let R be the associated ring, and I the ideal from $k = n-3$. From the exact sequences on $\mathbb{P}^1_{\mathbb{Z}}$

$$0 \to \mathcal{O}(-n) \xrightarrow{f} \mathcal{O} \to \mathcal{O}/f(\mathcal{O}(-n)) \to 0$$

and

$$0 \to \mathcal{O}(-3) \xrightarrow{f} \mathcal{O}(n-3) \to \mathcal{O}(n-3)/f(\mathcal{O}(-3)) \to 0$$

we obtain exact sequences

$$0 \to \mathbb{Z} \to R \to H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-n)) \to 0$$

and

$$0 \to H^0(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(n-3)) \to I \to H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-3)) \to 0.$$

We have a map $R \otimes I \to I$ from the action of the ring on the ideal, and thus a map $\phi : R/\mathbb{Z} \otimes H^0(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(n-3)) \to H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-3))$. It is easy to see that with the identification of $R/\mathbb{Z}$ with $H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-n))$, that ϕ is the same as the natural map

$$H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-n)) \otimes H^0(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(n-3)) \to H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-3)).$$

Note if we write $V = \mathbb{Z}^2$, then we have $H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-n))) = \mathrm{Sym}_{n-2} V^*$, and also $H^0(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(n-3)) = \mathrm{Sym}^{n-3} V$, and $H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-3)) = V^*$.

In Section 3.4, we prove that the above algebraic data is precisely the data parametrized by binary n-ic forms. Given a ring R and an R-module I, we have that R and I are associated to a binary n-ic form if and only if we can write $R/\mathbb{Z} = \mathrm{Sym}_{n-2} V^*$ and an exact sequence $0 \to \mathrm{Sym}^{n-3} V \to I \to V^* \to 0$ such that the map $\mathrm{Sym}_{n-2} V^* \otimes \mathrm{Sym}^{n-3} V \to V^*$ given by the action of R on I is the same as the natural map between those $\mathbb{Z}$-modules. It is equivalent to require that R have a $\mathbb{Z}$-module basis $\zeta_0 = 1, \zeta_1, \ldots, \zeta_{n-1}$ and and I have a $\mathbb{Z}$-module basis $\alpha_1, \alpha_2, \beta_1, \ldots, \beta_{n-2}$ such that

$$\text{the } \alpha_i \text{ coefficient of } \zeta_j \beta_k \text{ is } \begin{cases} 1 & \text{if } i+j+k = n+1 \\ 0 & \text{otherwise.} \end{cases}$$

(This equivalence can be computed by working out the natural map $\mathrm{Sym}_{n-2} V^* \otimes \mathrm{Sym}^{n-3} V \to V^*$ in terms of an explicit basis.) It is easy to see that when $n = 3$ this condition requires that I is isomorphic to R as an R-module. All of the work in the chapter can be done with an arbitrary base scheme (or ring) replacing $\mathbb{Z}$ in the above, and we now state a precise theorem capturing the above claims over an arbitrary base.

Let S be a scheme, and $\mathcal{O}_S$ its sheaf of regular functions. A *binary n-ic form* over S is a locally free rank 2 $\mathcal{O}_S$-module V, and an element $f \in \mathrm{Sym}^n V$. An l-twisted binary n-ic form over S is a locally free rank 2 $\mathcal{O}_S$-module V, and an element $f \in \mathrm{Sym}^n V \otimes (\wedge^2 V)^{\otimes l}$. A *binary n-pair* is an $\mathcal{O}_S$-algebra R, an R-module I, an exact sequence $0 \to \mathrm{Sym}^{n-3} Q^* \to I \to Q \to 0$ such that Q is a locally free rank 2 $\mathcal{O}_S$-module, and an isomorphism $R/\mathcal{O}_S \cong \mathrm{Sym}_{n-2} Q$ that identifies the map $R/\mathcal{O}_S \otimes \mathrm{Sym}^{n-3} Q^* \to Q$ induced from the action of R on I with the natural map $\mathrm{Sym}_{n-2} Q \otimes \mathrm{Sym}^{n-3} Q^* \to Q$. In Section 3.3, we give a geometric construction of rings and modules from (twisted) binary n-ic forms over a scheme S, motivated by the geometric description given above over $\mathbb{Z}$. Our main theorem is the following, proved in Section 3.4.

Theorem 3.1.1. *For $n \geq 3$, we have a bijection between (-1)-twisted binary n-ic forms over S and binary n-pairs over S, and the bijection commutes with base change in S. In other words, we have a isomorphism of the moduli stack of (-1)-twisted binary n-ic forms and the moduli stack of binary n-pairs.*

Analogs of Theorem 3.1.1 can be proven for l-twisted binary forms for all l. In Section 6.2 we give a simple, self-contained proof for -1-twisted cubic forms to show that over an arbitrary base, binary cubic forms are in correspondence with cubic rings. We can write the construction of a (-1)-twisted binary n-ic form from a (-1)-twisted binary n-pair as the evaluation

$$x \mapsto x \wedge \phi(x^{n-2}) x$$

of a degree n map $Q \to \wedge^2 Q$, where ϕ is the isomorphism $\mathrm{Sym}_{n-2} Q \cong R/\mathcal{O}_S$ and we lift x to the ideal I to act on it by R and then take the quotient to Q. It is not clear a priori that this map is even well-defined, but that will follow from the definition of a binary n-pair (Lemma 3.4.5).

3.2 Constructing a ring and modules from a binary n-ic form over $\mathbb{Z}$

3.2.1 Concrete construction

In this section we will explicitly realize the ring and ideals associated to a binary n-ic form inside a $\mathbb{Q}$-algebra. Given a *binary n-ic form*,

$$f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n \quad \text{with} \quad f_i \in \mathbb{Z},$$

such that $f_0 \neq 0$, we can form a ring R_f as a subring of $Q_f := \mathbb{Q}(\theta)/(f_0\theta^n + f_1\theta^{n-1} + \cdots + f_n)$ with $\mathbb{Z}$-module basis

$$\begin{aligned} \zeta_0 &= 1 \\ \zeta_1 &= f_0\theta \\ \zeta_2 &= f_0\theta^2 + f_1\theta \\ &\vdots \\ \zeta_k &= f_0\theta^k + \cdots + f_{k-1}\theta \\ &\vdots \\ \zeta_{n-1} &= f_0\theta^{n-1} + \cdots + f_{n-2}\theta. \end{aligned} \tag{3.1}$$

Since $f_0 \neq 0$, we have that R_f is a free rank n $\mathbb{Z}$-module, i.e. *a rank n ring* in the terminology of Bhargava [6]. Birch and Merriman [8] studied this $\mathbb{Z}$-submodule of Q_f, and Nakagawa [35, Proposition 1.1] proved that this $\mathbb{Z}$-submodule is a ring (though Nakagawa worked only with irreducible f, his proof makes sense for all f). Nakagawa writes down the multiplication table of R_f explicitly as follows:

$$\zeta_i\zeta_j = -\sum_{\max(i+j-n,1)\leq k\leq i} f_{i+j-k}\zeta_k + \sum_{j<k\leq \min(i+j,n)} f_{i+j-k}\zeta_k \quad \text{for } 1 \leq i,j \leq n-1, \tag{3.2}$$

where $\zeta_n := -f_n$. If $f_0 = 0$, we could still use the above multiplication table to define a rank n ring (see Section 3.2.2). We have the discriminant equality $\operatorname{Disc} R_f = \operatorname{Disc} f$ (see, for example, [39, Proposition 4]), which is a point of interest in R_f in previous works (e.g. [35], [39]).

Remark 3.2.1. Throughout this chapter, it will be useful to also make the above construction with $\mathbb{Z}$ replaced by $\mathbb{Z}[f_0, \dots f_n]$, where the f_i are formal variables, and with $f = f_0x^n + + \cdots + f_ny^n$, which we call the *universal form.* If K is the fraction field of $\mathbb{Z}[f_0, \dots f_n]$, we can then work in $K(\theta)/(f_0\theta^n + f_1\theta^{n-1} + \cdots + f_n)$ instead of $\mathbb{Q}(\theta)/(f_0\theta^n + f_1\theta^{n-1} + \cdots + f_n)$. The multiplication table in Equation (3.2) still holds, as Nakagawa's proof can also be interpreted in this context.

When $f_0 \neq 0$, we can also form a fractional ideal $I_f = (1, \theta)$ of R_f (lying in Q_f). There is a natural $\mathrm{GL}_2(\mathbb{Z})$ action on binary forms, and the ring R_f and the ideal class of I_f are invariant under this action The invariance will follow from our geometric

construction of this ideal in Section 3.2.3. (See also [35, Proposition 1.2] for a direct proof of the invariance of R_f, and [39, Théorème 3.4] which, in the case when f is irreducible and primitive, considers a sequence of ideals $\mathfrak{J}_j$, all in the ideal class of I_f, and proves that this ideal class is SL_2 invariant.) The powers of I_f give a sequence of ideals ${I_f}^0, {I_f}^1, \ldots, {I_f}^{n-1}, \ldots$ whose classes are each $\mathrm{GL}_2(\mathbb{Z})$ invariant. We can write down the following explicit $\mathbb{Z}$-module bases for ${I_f}^k$ for $0 \leq k \leq n-1$:

$$ {I_f}^k = \langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1} \rangle_{\mathbb{Z}}, \tag{3.3} $$

where $\langle s_1, \ldots, s_n \rangle_R$ denotes the R-module generated by $s_1, \ldots, s_n$. Equivalently to Equation (3.3), we have for $0 \leq k \leq n-1$

$$ {I_f}^k = \langle 1, \theta, \ldots, \theta^k, f_0\theta^{k+1}, f_0\theta^{k+2} + f_1\theta^{k+1}, \ldots, f_0\theta^{n-1} + f_1\theta^{n-2} + \cdots + f_{n-k-2}\theta^{k+1} \rangle_{\mathbb{Z}}. \tag{3.4} $$

To be clear, we give the boundary cases explicitly:

$$ {I_f}^{n-2} = \langle 1, \theta, \ldots, \theta^{n-2}, f_0\theta^{n-1} \rangle_{\mathbb{Z}} $$
$$ {I_f}^{n-1} = \langle 1, \theta, \ldots, \theta^{n-1} \rangle_{\mathbb{Z}}. $$

Proposition 3.6.1 in the Appendix (Section 3.6) shows that the $\mathbb{Z}$-modules given above are equal to the ideals we claim. Clearly, the given $\mathbb{Z}$-modules are subsets of the respective ideals and contain the ideal generators, and so it only remains to check that the given $\mathbb{Z}$-modules are themselves ideals.

If we look at the $\mathbb{Z}$ bases of ${I_f}^2$, ${I_f}^1$, and ${I_f}^0$ given in Equation (3.4), they naturally lead to considering another $\mathbb{Z}$-module (given by Equation (3.4) when $k = -1$)

$$ {I_f}^{\#} = \langle f_0, f_0\theta + f_1, \ldots, f_0\theta^{n-1} + f_1\theta^{n-2} + \cdots + f_{n-1} \rangle_{\mathbb{Z}}. \tag{3.5} $$

It turns out that ${I_f}^{\#}$ is an ideal of R_f (Proposition 3.6.3). This ideal is studied in the case of f irreducible and primitive as $\mathfrak{b}$ in [39] and [37] and as $\mathfrak{B}$ in [18].

Remark 3.2.2. Similarly, we can form the fractional ideals I_f^k and $I_f^{\#}$ over the base ring $\mathbb{Z}[f_0, \ldots f_n]$ and with $f = f_0x^n + + \cdots + f_ny^n$, working in $K(\theta)/(f_0\theta^n + f_1\theta^{n-1} + \cdots + f_n)$. The ideals have $\mathbb{Z}[f_0, \ldots f_n]$-module bases as given in Equations (3.3), (3.4), and (3.5), and these $\mathbb{Z}[f_0, \ldots f_n]$-modules are R ideals by the same proofs as in the $\mathbb{Z}$ case.

Given the sequence ${I_f}^2, {I_f}^1, {I_f}^0$ that led us to define ${I_f}^{\#}$ one might expect that ${I_f}^{\#}$ is the same as ${I_f}^{-1}$. However, it turns out that I_f is not always invertible. We do have the following proposition (proven in Proposition 3.6.4 in the Appendix). A form f is *primitive* if its coefficients generate the unit ideal in $\mathbb{Z}$.

Proposition 3.2.3. *For $f \not\equiv 0$, the ideal class of I_f is invertible if and only if the form f is primitive. Also, the ideal class of ${I_f}^{\#}$ is invertible if and only if the form f is primitive. In the case that f is primitive, ${I_f}^{-1} = {I_f}^{\#}$.*

When f is primitive, Simon [38, Proposition 3.2] proved that the ideal classes of what we call I_f and ${I_f}^{\#}$ are inverses. Note an invertible fractional ideal is invertible as a module [10, II.5.6, Proposition 11]). Since I_f is finitely generated, if it has a

module inverse then it is projective of rank 1 ([10, II.5.4, Theorem 3]), and since I_f is a fractional ideal containing 1, if I_f is projective of rank 1 then it is an invertible fractional ideal ([10, II.5.6, Theorem 4]). Of course, for any $k > 0$, we have ${I_f}^k$ is invertible if and only if I_f is. Some of the ideal classes ${I_f}^k$ are particularly interesting. For example, we have the following result which we prove in Corollary 3.3.7.

Theorem 3.2.4. *The class of ${I_f}^{n-2}$ is the class of the inverse different of R_f. In other words, as R_f modules, ${I_f}^{n-2} \cong \mathrm{Hom}_{\mathbb{Z}}(R_f, \mathbb{Z})$.*

Simon [37, Proposition 14] independently discovered that when f is primitive and irreducible that $({I_f}^{\#})^{2-n}$ is in the ideal class of the inverse different of R_f. In this chapter, we find that while $({I_f}^{\#})^{2-n}$ is not naturally constructed as a module, ${I_f}^{n-2}$ can be naturally constructed and is always the inverse different, even when f is reducible, primitive, or even the zero form! When $f = 0$, we construct ${I_f}^{n-2}$ as a module and the above theorem holds, but the module is not realizable as a fractional ideal of R_f.

Theorem 3.2.4 holds even when the inverse different is not invertible. (Recall the inverse different can be defined as the R_f-module $\mathrm{Hom}_{\mathbb{Z}}(R_f, \mathbb{Z})$, which, when the trace form on Q_f is nondegenerate or equivalently the discriminant of f is nonzero, is realized as the fractional ideal $\{x \in Q_f | \ \mathrm{Tr}(xR_f) \subset \mathbb{Z}\}$.) When the form f is primitive, then $[({I_f}^{\#})^{n-2}]$ is the ideal class of the different of R_f.

Corollary 3.2.5. *For $n \neq 2$ and $f \not\equiv 0$, the ring R_f is Gorenstein if and only if the form f is primitive.*

Proof. It is known that for rank n rings, the condition of Gorenstein is equivalent to the inverse different being invertible. For the ring R_f, the inverse different is in the same ideal class as ${I_f}^{n-2}$ and thus this follows from Proposition 3.2.3. □

For maximal orders in number fields, the inverse different is always a square in the class group [28, Theorem 176]. For the rings R_f, whether they are maximal or not, the inverse different is always an $(n-2)$th power in the class group. For example, for quartic rings R_f arising from binary quartic forms the inverse different is always a square in the class group, even in the case when R_f is non-maximal or does not lie in a number field. Even for maximal quintic orders in number fields, the inverse different is not always a cube in the class group. However, for R_f from binary quintic forms, the inverse different is always a cube in the class group.

Remark 3.2.6. When we have a binary form with $f_0 = \pm 1$, then $R_f = \mathbb{Z}[\theta]/f(\theta)$. Such rings, generated by one element, are called *monogenic*. We see that all monogenic rings are R_f for some binary form f (made by homogenizing the minimal polynomial of the generating element) . Also, in this case ${I_f}^k \cong I_f^{\#} \cong R_f$ as R_f-modules. In particular, it follows from Theorem 3.2.4 that the inverse different of any monogenic ring R is isomorphic to R as an R-module, and thus principal when it is realized as a fractional ideal (this is proven in [36, III, Proposition 2.4] for maximal monogenic domains.)

3.2.2 Explicit multiplication and action tables

If a form $f = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$ has $f_0 = 0$, but $f \not\equiv 0$, then we can act by $\mathrm{GL}_2(\mathbb{Z})$ to take f to a form f' with $f'_0 \neq 0$. We then can define the ring R_f and the R_f ideal classes I_f and ${I_f}^{\#}$ using f'. Since the ring and ideal classes are $\mathrm{GL}_2(\mathbb{Z})$ invariants, it does not matter which f' we use. In this section, we give a more systematic way to define the rings R_f and ideal classes I_f that works even when $f = 0$.

Given a base ring B, if we form a rank n B-module $R = Br_1 \oplus \ldots Br_n$, we can specify a B-bilinear product on R by letting

$$r_ir_j = \sum_{k=1}^{n} c_{i,j,k}r_k \quad \text{for } c_{i,j,k} \in B,$$

and $e = \sum_{k=1}^{n} e_kr_k$ for some $e_k \in B$. If this product is commutative, associative, and e is a multiplicative identity (which is a queston of certain polynomial equalities with integer coefficients being satisfied by the $c_{i,j,k}$ and e_k) then we call the $c_{i,j,k}$ and e_k a *multiplication table*. A multiplication table gives a ring R with a specified B-module basis.

Similarly, we can form a free rank m B-module $I = B\alpha_1 \oplus \ldots B\alpha_m$, where usually m is a multiple of n. Then we can specify a B-bilinear product $R \times I \to B$ by

$$r_i\alpha_j = \sum_{k=1}^{m} d_{i,j,k}\alpha_k \quad \text{for } d_{i,j,k} \in B.$$

That this product gives an R-module action on I is a question of certain polynomial equalities with integer coefficients being satisfied by the $d_{i,j,k}$, $c_{i,j,k}$ and e_k, and in the case they are satisfied we call the $d_{i,j,k}$ an *action table*. An action table gives an R-module I with a specified B-module basis.

If we want to work directly with forms with $f_0 = 0$ (for example, to deal with the form $f = 0$ or to study the form $f = x^2y + xy^2$ when we replace $\mathbb{Z}$ with $\mathbb{Z}/(2)$), we see that we can define a ring $\mathcal{R}_f$ from the multiplication table given in Equation (3.2). The conditions of commutativity and associativity on this multiplication table are polynomial identities in the f_i since the construction of R can also be made with the universal form. The isomorphism class of the ring $\mathcal{R}_f$ is a $\mathrm{GL}_2(\mathbb{Z})$ invariant of the form f.

Equations (3.3) and (3.5) display $\mathbb{Z}$-module bases of I_f and ${I_f}^{\#}$. The action of elements of R_f on these $\mathbb{Z}$-module bases is given by an action table of polynomials in the f_i with $\mathbb{Z}$ coefficients. (We can see this, for example, because the proofs of Propositions 3.6.1 and 3.6.3 work over the base ring $\mathbb{Z}[f_0, \ldots, f_n]$.) These polynomials in the f_i formally give an action table because they give an action table over the base ring $\mathbb{Z}[f_0, \ldots, f_n]$. Thus, we can construct $\mathcal{R}_f$-modules $\mathcal{I}_f$ and ${\mathcal{I}_f}^{\#}$ first as rank n $\mathbb{Z}$-modules and then give them an $\mathcal{R}_f$ action by the same polynomials in the f_i that make the action tables for I_f and ${I_f}^{\#}$ respectively.

We can also form versions of the powers of I_f this way, which are $\mathcal{R}_f$-modules that we call $\mathcal{I}_{f_k}$ for $1 \leq k \leq n-1$. We use the action table of ${I_f}^k$ with the basis

of Equation (3.3). The action table has entries that are integer polynomials in the f_i for the same reasons as above. We only have defined the $\mathcal{I}_{f_k}$ as $\mathcal{R}_f$-modules and not as fractional ideals of $\mathcal{R}_f$. Whenever $f \not\equiv 0$, however, we have also given a a realization of the $\mathcal{I}_{f_k}$ as the ideal class I_f^k (or $I_f^\#$ when $k = -1$). Let $\mathcal{I}_{f_{-1}} := \mathcal{I}_f{}^\#$ and $\mathcal{I}_f := \mathcal{I}_{f_1}$. We do not put the k in the exponent because even when f is non-zero but non-primitive, it is not clear that the module $\mathcal{I}_{f_k}$ is a power of the module $\mathcal{I}_f$. When f is primitive, since I_f is invertible, its ideal class powers are the same as its module powers.

Whenever R_f and $I_f{}^k$ are defined (i.e. when $f \not\equiv 0$), we have the ring isomorphism $R_f \cong \mathcal{R}_f$, the R_f-module isomorphism $I_f{}^k \cong \mathcal{I}_{f_k}$ for $1 \leq k \leq n-1$, and the R_f-module isomorphism $I_f{}^\# \cong \mathcal{I}_f{}^\#$. This is because $\mathcal{R}_f$, $\mathcal{I}_{f_k}$, and $\mathcal{I}_f{}^\#$ are defined by the multiplication tables and action tables of R_f, $I_f{}^k$, and $I_f{}^\#$ respectively. The ring $\mathcal{R}_f$ and the modules $\mathcal{I}_{f_k}$ are $\mathrm{GL}_2(\mathbb{Z})$ invariants of the form f (which will be clear, for example, from our geometric construction in Section 3.2.3).

3.2.3 Simple geometric construction

For many reasons, we desire a canonical, basis free description of the ring $\mathcal{R}_f$ and $\mathcal{R}_f$-modules $\mathcal{I}_{f_k}$. We would like to deal more uniformly with the case that $f_0 = 0$ and see easily the $\mathrm{GL}_2(\mathbb{Z})$ invariance of our constructions. We would also like to prepare to give these results over arbitrary base where we will have locally free modules over the base which are not free. A binary n-ic form f describes a subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ which we call S_f. Let $\mathcal{O}(k)$ denote the usual sheaf on $\mathbb{P}^1_{\mathbb{Z}}$ and let $\mathcal{O}_{S_f}(k)$ denote its pullback to S_f. Also, for a sheaf $\mathcal{F}$, let $\Gamma(U, \mathcal{F})$ be sections of $\mathcal{F}$ on U and let $\Gamma(\mathcal{F})$ be the global sections of $\mathcal{F}$.

Theorem 3.2.7. *For a binary form $f \not\equiv 0$, the ring $\Gamma(\mathcal{O}_{S_f})$ of global functions of S_f is isomorphic to R_f. The global sections $\Gamma(\mathcal{O}_{S_f}(k))$ have an $\Gamma(\mathcal{O}_{S_f})$-module structure, and since $R_f \cong \Gamma(\mathcal{O}_{S_f})$, this gives $\Gamma(\mathcal{O}_{S_f}(k))$ an R_f-module structure. For, $1 \leq k \leq n-1$, the global sections $\Gamma(\mathcal{O}_{S_f}(k))$ are isomorphic to $I_f{}^k$ as an R_f-module. The global sections $\Gamma(\mathcal{O}_{S_f}(-1))$ are isomorphic to $I_f{}^\#$ as an R_f-module.*

Proof. We can act by $\mathrm{GL}_2(\mathbb{Z})$ so that $f_0 \neq 0$ and $f_n \neq 0$. Then if we write $\mathbb{P}^1_{\mathbb{Z}} = \operatorname{Proj} \mathbb{Z}[x, y]$, we can cover $\mathbb{P}^1_{\mathbb{Z}}$ with the open subsets U_y and U_x where y and x are invertible, respectively.

Lemma 3.2.8. *If $f_n \neq 0$, then the restriction map*

$$\Gamma(U_y, \mathcal{O}_{S_f}(k)) \to \Gamma(U_y \cap U_x, \mathcal{O}_{S_f}(k))$$

is injective.

Proof. If $\sum_{i \geq -k} a_i x^{k+i} y^{-i} \mapsto 0$, with $a_i \in \mathbb{Z}$, then $\sum_{i \geq -k} a_i x^{k+i} y^{-i} = \sum_j d_j x^j y^{k-n-j} f$, where $d_j \in \mathbb{Z}$. Since $\sum_{i \geq -k} a_i x^{k+i} y^{-i}$ has no terms of negative degree in x and $f_n \neq 0$, we conclude that $d_j = 0$ for $j < 0$. Thus, $\sum_{i \geq -k} a_i x^{k+i} y^{-i}$ is 0 in $\Gamma(U_y, \mathcal{O}_{S_f}(k))$. $\square$

Similarly, since $f_0 \neq 0$, we have that $\Gamma(U_x, \mathcal{O}_{S_f}(k)) \to \Gamma(U_y \cap U_x, \mathcal{O}_{S_f}(k))$ is an injection.

So we wish to determine the elements of $\Gamma(U_y \cap U_x, \mathcal{O}_{S_f}(k))$ that are in the images of both $\Gamma(U_x, \mathcal{O}_{S_f}(k))$ and $\Gamma(U_y, \mathcal{O}_{S_f}(k))$ First, note that $x^k, x^{k-1}y, \ldots, y^k$ are in the images of both restriction maps. In $\Gamma(U_y \cap U_x, \mathcal{O}_{S_f}(k))$ for $1 \leq m \leq n-k-1$, we have

$$f_0 x^{k+m} y^{-m} + \cdots + f_{k+m-1} x y^{k-1} = -f_{k+m} y^k - \cdots - f_n x^{k+m-n} y^{n-m},$$

and thus $z_m := f_0 x^{k+m} y^{-m} + \ldots f_{k+m-1} x y^{k-1}$ is in the images of both $\Gamma(U_x, \mathcal{O}_{S_f}(k))$ and $\Gamma(U_y, \mathcal{O}_{S_f}(k))$.

Now, let p be in both images so that $p = \sum_{i \geq -k} a_i x^{k+i} y^{-i} = \sum_{i \leq -k} b_i x^{-i} y^{k+i}$ with $a_i, b_i \in \mathbb{Z}$. If $a = \sum_{i \geq -k} a_i x^{k+i} y^{-i} \in \Gamma(U_y, \mathcal{O}_{S_f}(k))$ and $b = \sum_{i \leq 0} b_i x^{-i} y^{k+i} \in \Gamma(U_x, \mathcal{O}_{S_f}(k))$, then we have a formal equality $a - b = \sum_i c_i x^i y^{k-i-n} f$ (in the ring $\mathbb{Z}[x, x^{-1}, y, y^{-1}]$) where $c_i \in \mathbb{Z}$. We can assume without loss of generality that $c_i = 0$ for $i \geq 0$ because any $c_i x^i y^{k-i-n} f$ with i non-negative we could just subtract from the representation a to get another such representation of p in $\Gamma(U_y, \mathcal{O}_{S_f}(k))$. Similarly, we can assume that $c_i = 0$ for $i \leq k-n$. From the equality $a - b = \sum_{i=-n+k+1}^{-1} x^i y^{k-i-n} f$, we can conclude that a is a linear combination of the monomials $x^k, x^{k-1}y, \ldots, y^k$ plus all the terms $\sum_{i=-n+k+1}^{-1} x^i y^{k-i-n} f$ of positive degree in x, and b is that same linear combination minus all the terms of $\sum_{i=-n+k+1}^{-1} x^i y^{k-i-n} f$ of positive degree in x. The terms of positive degree in x of $x^i y^{k-i-n} f$ sum to z_{n+i-k}. Thus, $a \in \left\langle x^k, x^{k-1}y, \ldots, y^k, z_1, \ldots, z_{n-1-k} \right\rangle_{\mathbb{Z}}$.

For $k \geq 0$, when we map $\left\langle x^k, x^{k-1}y, \ldots, y^k, z_1, \ldots, z_{n-1-k} \right\rangle_{\mathbb{Z}}$ to Q_f via $x \mapsto \theta$ and $y \mapsto 1$, the image is the free rank n $\mathbb{Z}$-module $\left\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1} \right\rangle_{\mathbb{Z}}$. Thus, the map is an isomorphism of $\left\langle x^k, x^{k-1}y, \ldots, y^k, z_1, \ldots, z_{n-1-k} \right\rangle_{\mathbb{Z}}$, the global sections of $\mathcal{O}_{S_f}(k)$, onto ${I_f}^k$. Clearly the $\Gamma(\mathcal{O}_{S_f})$-module structure on $\Gamma(\mathcal{O}_{S_f}(k))$ is the same as the the R_f-module structure on ${I_f}^k$ (including the $k = 0$ case, which gives the ring isomorphism $R_f \cong \Gamma(\mathcal{O}_{S_f})$). When $k = -1$, when we map $\langle z_1, \ldots, z_n \rangle_{\mathbb{Z}}$ to Q_f via $x \mapsto \theta$ and $y \mapsto 1$, the image is the free rank n $\mathbb{Z}$-module ${I_f}^{\#}$. Similarly we conclude the theorem for ${I_f}^{\#}$. □

Note that though $\mathcal{O}_{S_f}(k)$ is always an invertible $\mathcal{O}_{S_f}$-module, when S_f is not affine, the global sections $\Gamma(\mathcal{O}_{S_f}(k))$ are not necessarily an invertible $\Gamma(\mathcal{O}_{S_f})$-module. In fact, we know that for nonzero f and $1 \leq k \leq n-1$ that $\Gamma(\mathcal{O}_{S_f}(k))$ is an invertible $\Gamma(\mathcal{O}_{S_f})$-module exactly when f is primitive.

Theorem 3.2.9. *Let f be a binary form with non-zero discriminant. The scheme S_f is affine if and only if f is primitive.*

Proof. From Theorem 3.2.7 we see that if S_f is affine, then since $\Gamma(\mathcal{O}_{S_f}(1)) \cong I_f$ and $\mathcal{O}_{S_f}(1)$ is invertible we must have that I_f is an invertible R_f-module. Thus by Proposition 3.2.3, if S_f is affine then f is primitive. To see the picture more concretely, consider the map $a : \operatorname{Spec} R_f \to \operatorname{Spec} \mathbb{Z}$. Since $R_f/\wp$ is finite for any prime $\wp$ of R_f that contains a prime p of $\mathbb{Z}$, we have that all points in the fiber of a

over (p) are closed. However if $p \mid f$, then the fiber of S_f over (p) is $\mathbb{P}^1_{\mathbb{Z}/(p)}$ which has a non-closed point. We see that S_f has a vertical fiber over (p) when $p \mid f$. Moreover, when $p \mid f$ we see from the multiplication table (Equation (3.2)) that the fiber of a over (p) is the non-reduced n-dimensional point $\operatorname{Spec} \mathbb{Z}_{/(p)}[x_1, x_2, \ldots, x_{n-1}]/(x_i x_j)_{1 \le i,j \le n-1}$ which does not embed into $\mathbb{P}^1_{\mathbb{Z}}$.

Now suppose that f is primitive and has non-zero discriminant. We can change variables so that $f_0 \neq 0$ and $f_n \neq 0$. From the standard open affine cover of $\mathbb{P}^1_{\mathbb{Z}}$, we have that S_f is covered by affine opens $U_y = \operatorname{Spec} \mathbb{Z}[x/y]/(f/y^n)$ and $U_x = \operatorname{Spec} \mathbb{Z}[y/x]/(f/x^n)$. Since R_f is a finitely generated $\mathbb{Z}$-module inside Q_f (which is a product of number fields), we know that the class group of R_f is finite. So, let m be such that $({I_f}^{\#})^m$ is principal. (Note that by Proposition 3.6.4 we know that $({I_f}^{\#})$ is an invertible R_f-module.) Let $J = \theta {I_f}^{\#}$ which is an integral R_f-ideal. Let $J^m = (b)$ and $({I_f}^{\#})^m = (a)$, with $a, b \in R_f$. As in the computation in the proof of Proposition 3.6.4, we see that ${I_f}^{\#} + J = (1)$ and thus there exists $\alpha, \beta \in R_f$ such that $\alpha a + \beta b = 1$. We claim that $(S_f)_a = U_y$ as open subschemes of S_f, where $(S_f)_a$ denotes the points of S_f at which a is non-zero.

In the ring Q_f we have that $a\theta^m = bu$, where u is a unit in R_f. In $\Gamma(U_y \cap U_x, \mathcal{O}_{S_f}) \cong Q_f$ this translates to $a(\frac{x}{y})^m = bu$ Thus

$$a(\alpha + \frac{\beta}{u}\left(\frac{x}{y}\right)^m) = \alpha a + \beta \frac{a}{u}\left(\frac{x}{y}\right)^m = \alpha a + \beta b = 1$$

in $\Gamma(U_y, \mathcal{O}_{S_f})$ (which injects into $\Gamma(U_y \cap U_x, \mathcal{O}_{S_f}) \cong Q_f$). Therefore a is not zero at any point of U_y, and so $U_y \subset (S_f)_a$. Suppose that we have a point $p \notin U_y$ so that $\frac{y}{x}$ is 0 at p. Since in $\Gamma(U_y \cap U_x, \mathcal{O}_{S_f})$ we have $a = bu(\frac{y}{x})^m$, this is also true in $\Gamma(U_x, \mathcal{O}_{S_f}) \cong \mathbb{Z}[y/x]/F(y/x)$ (which injects into $\Gamma(U_y \cap U_x, \mathcal{O}_{S_f})$). Since we have $p \in U_x$, then a is also 0 at p and so $p \notin (S_f)_a$ and we conclude $(S_f)_a \subset U_y$. We have shown $(S_f)_a = U_y$ and by switching x and y we see similarly that $(S_f)_b = U_x$. Since (a, b) is the unit ideal in $\Gamma(S_f, \mathcal{O}_{S_f}) \cong R_f$, and $(S_f)_a$ and $(S_f)_b$ are each affine, we have that S_f is affine ([27, Exercise 2.17(b)]).

We could similarly argue over a localization of $\mathbb{Z}$, and thus localizing away from the $\mathbb{Z}$ primes that divide f, the scheme S_f is the same as $\operatorname{Spec} R_f$. Over the primes of $\mathbb{Z}$ that divide f, S_f has vertical fibers isomorphic to $\mathbb{P}^1_{\mathbb{Z}/(p)}$ but $\operatorname{Spec} R_f$ has a non-reduced n-dimensional point. □

When f is primitive and has non-zero discriminant, then the affineness of S_f and the invertibility of $\mathcal{O}_{S_f}(1)$ implies the invertibility of I_f, which we knew for primitive f from Proposition 3.2.3.

3.2.4 Geometric construction by hypercohomology

The description of R_f as the global functions of the subscheme given by f is very satisfying as a coordinate-free, canonical and simple description of R_f, but still does not take care of the form $f = 0$. It may seem at first that $f = 0$ is a pesky, uninteresting case, but we will eventually want to reduce a form so that its coefficients

are in $\mathbb{Z}/(p)$, in which case many of our non-zero forms will go to 0. In general we may want to base change, and the formation of the ring $\Gamma(\mathcal{O}_{S_f})$ does not commute with base change. For example, a non-zero binary n-ic all of whose coefficients are divisible p will give a rank n ring $\Gamma(\mathcal{O}_{S_f})$ but the reduction $\bar{f}$ of f to $\mathbb{Z}/(p)$ would give $S_{\bar{f}} = \mathbb{P}^1_{\mathbb{Z}/(p)}$ and thus a ring of global functions that is rank 1 over $\mathbb{Z}/(p)$.

We can, however, make the following construction, which was given for $n = 3$ by Deligne in a letter [19] to Gan, Gross, and Savin. On $\mathbb{P}^1_{\mathbb{Z}}$ a binary n-ic form f gives $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$, whose image is the ideal sheaf of S_f. We can consider $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ as a complex in degrees -1 and 0, and then take the hypercohomology of this complex:

$$R = H^0 R\pi_* \left(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O} \right). \tag{3.6}$$

(Here we are taking the 0th right hyper-derived functor of the pushforward by $\pi : \mathbb{P}^1_{\mathbb{Z}} \to \operatorname{Spec} \mathbb{Z}$ on this complex. Alternatively, we pushforward the complex in the derived category and then take H^0. We take hypercohomology since we are applying the functor to a complex of sheaves and not just a single sheaf.) There is a product on the complex $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ given as $\mathcal{O} \otimes \mathcal{O} \to \mathcal{O}$ by multiplication, $\mathcal{O} \otimes \mathcal{O}(-n) \to \mathcal{O}(-n)$ by the $\mathcal{O}$-module action, and $\mathcal{O}(-n) \otimes \mathcal{O}(-n) \to 0$. This product is clearly commutative and associative, and induces a product on R. The map of complexes

$$\begin{array}{ccc} & & \mathcal{O} \\ & & \downarrow \\ \mathcal{O}(-n) & \longrightarrow & \mathcal{O} \end{array}$$

induces $\mathbb{Z} \to R$. (Of course, $H^0 R\pi_*(\mathcal{O})$ is just $\pi_*(\mathcal{O}) \cong \mathbb{Z}$.) It is easy to see that $1 \in H^0 R\pi_*(\mathcal{O})$ acts as the multiplicative identity.

When $f \not\equiv 0$, the map $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ is injective, and thus the complex $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ is chain homotopy equivalent to $\mathcal{O}/f(\mathcal{O}(-n)) \cong \mathcal{O}_{S_f}$ (as a chain complex in the 0th degree). The chain homotopy equivalence also respects the product structure on the complexes. Thus when $f \not\equiv 0$, we have $R \cong \pi_*(\mathcal{O}_{S_f})$, and since $\operatorname{Spec} \mathbb{Z}$ is affine we can consider $\pi_*(\mathcal{O}_{S_f})$ simply as a $\mathbb{Z}$-module isomorphic to $\Gamma(\mathcal{O}_{S_f}) \cong R_f$. When $f = 0$ we get

$$R = H^0 R\pi_*(\mathcal{O}) \oplus R^1 \pi_*(\mathcal{O}(-n)) \cong \mathbb{Z} \oplus \mathbb{Z}^{n-1}$$

as a $\mathbb{Z}$-module and with multiplication given by $(1, 0)$ acting as the multiplicative identity and $(0, x)(0, y) = 0$ for all $x, y \in \mathbb{Z}^{n-1}$. This agrees with the definition of $\mathcal{R}_0$ given in Section 3.2.2 that used the coefficients of f to give a multiplication table for $\mathcal{R}_f$. So we see this definition of R is a natural extension to all f of the construction $\Gamma(\mathcal{O}_{S_f})$ for non-zero f, especially since R gives a rank n ring even when $f = 0$.

Theorem 3.2.10. *For all binary n-ic forms f, we have*

$$\mathcal{R}_f \cong H^0 R\pi_* \left(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O} \right)$$

as rings. (Note that $\mathcal{R}_f$ is defined in Section 3.2.2.)

Proof. The proof of Theorem 3.2.7 shows that $\mathcal{R}_f \cong H^0 R\pi_* \left(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}\right)$ for the universal form $f = f_0 x^n + f_1 x^{n-1} y + \cdots + f_n y^n$ with coefficients in $\mathbb{Z}[f_0, \ldots, f_n]$. Since both the construction of $\mathcal{R}_f$ from the multiplication table in Section 3.2.2 and the formation of $H^0 R\pi_* \left(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}\right)$ commute with base change (as we will see in Theorem 3.3.2), and every form f is a base change of the universal form, the theorem follows. □

We have a similar description of the $\mathcal{R}_f$ ideal classes (or modules) $\mathcal{I}_{f_k}$. We can define $\mathcal{R}_f$-modules for all $k \in \mathbb{Z}$:

$$H^0 R\pi_* \left(\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)\right).$$

(Here, $\mathcal{O}(k)$ is in degree 0 in the above complex.) The $\mathcal{R}_f$-module structure on

$$H^0 R\pi_* \left(\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)\right)$$

is given by the following action of the complex $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ on the complex $\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)$:

$$\begin{array}{cc} \mathcal{O} \otimes \mathcal{O}(k) \to \mathcal{O}(k) & \mathcal{O} \otimes \mathcal{O}(-n+k) \to \mathcal{O}(-n+k) \\ \mathcal{O}(-n) \otimes \mathcal{O}(k) \to \mathcal{O}(-n+k) & \mathcal{O}(-n) \otimes \mathcal{O}(-n+k) \to 0, \end{array}$$

where all maps are the natural ones.

Theorem 3.2.11. *For all binary n-ic forms f and $-1 \leq k \leq n-1$ we have*

$$\mathcal{I}_{f_k} \cong H^0 R\pi_* \left(\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)\right)$$

as $\mathcal{R}_f$-modules.

Proof. The proof is that same as that of Theorem 3.2.10. □

We have only defined the $\mathcal{I}_{f_k}$ for $-1 \leq k \leq n-1$, though for $f \not\equiv 0$ we have defined ${I_f}^k$ for all $k \geq 0$. For $f \not\equiv 0$, we have that the $\mathcal{R}_f$-module isomorphism $\mathcal{I}_f \cong \Gamma(\mathcal{O}_{S_f}(1))$ implies ${\mathcal{I}_f}^{\otimes k} \cong \Gamma(\mathcal{O}_{S_f}(1))^{\otimes k}$ for all $k \geq 0$. Further, if f is primitive, then I_f is an invertible ideal and thus ${I_f}^k \cong {\mathcal{I}_f}^{\otimes k} \cong \Gamma(\mathcal{O}_{S_f}(1))^{\otimes k} \cong \Gamma(\mathcal{O}_{S_f}(k))$. The first isomorphism is because ${I_f}^k$ is invertible, the second isomorphism is always true, and the third isomorphism is because S_f is affine. When f is not primitive, however, for $k > n-1$ it is not clear how to relate ${I_f}^k$ to $\Gamma(\mathcal{O}_{S_f}(k))$.

We have the following nice corollary of Theorems 3.2.10 and 3.2.11.

Corollary 3.2.12. *The ring $\mathcal{R}_f$ and the $\mathcal{R}_f$-module $\mathcal{I}_f$ are $\mathrm{GL}_2(\mathbb{Z})$ invariants of binary n-ic forms f.*

3.3 Constructing rings and modules from a binary form over an arbitrary base

So far, we have mainly considered binary forms with coefficients in $\mathbb{Z}$. We will now develop our theory over an arbitrary base scheme S. When $S = \operatorname{Spec} B$ we will sometimes say we are working over a base ring B and we will replace $\mathcal{O}_S$-modules with their corresponding B-modules.

Notation. For an $\mathcal{O}_S$-module M, we write M^* to denote the $\mathcal{O}_S$ dual module $\mathcal{H}om_{\mathcal{O}_S}(M, \mathcal{O}_S)$. If $\mathcal{F}$ is a sheaf, we use $s \in \mathcal{F}$ to denote that s is a global section of $\mathcal{F}$. We use $\operatorname{Sym}^n M$ to denote the usual quotient of $M^{\otimes n}$, and $\operatorname{Sym}_n M$ to denote the submodule of symmetric elements of $M^{\otimes n}$. We have $(\operatorname{Sym}_n M)^* \cong \operatorname{Sym}^n M^*$ for locally free $\mathcal{O}_S$-modules M.

A *binary n-ic form* over S is a pair (f, V) where V is a locally free $\mathcal{O}_S$-module of rank 2 and $f \in \operatorname{Sym}^n V$. An isomorphism of binary n-ic forms (f, V) and (f, V') is given by an $\mathcal{O}_S$-module isomorphism $V \cong V'$ which takes f to f'. We call f a *binary form* when n is clear from context or not relevant. If V is the free $\mathcal{O}_S$-module $\mathcal{O}_S x \oplus \mathcal{O}_S y$ we call f a *free* binary form.

Given a binary form $f \in \operatorname{Sym}^n V$ over a base scheme S, the form f determines a subscheme S_f of $\mathbb{P}(V)$ (where we define $\mathbb{P}(V) = \operatorname{Proj} \operatorname{Sym}^* V$). Let $\pi : \mathbb{P}(V) \to S$. Let $\mathcal{O}(k)$ denote the usual sheaf on $\mathbb{P}(V)$ and $\mathcal{O}_{S_f}(k)$ denote the pullback of $\mathcal{O}(k)$ to S_f. Then we can define the $\mathcal{O}_S$-algebra

$$\mathcal{R}_f := H^0 R\pi_* \left(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O} \right), \tag{3.7}$$

where $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ is a complex in degrees -1 and 0. (In section 3.2.4 this point of view is worked out in detail over $S = \operatorname{Spec} \mathbb{Z}$.) The product of $\mathcal{R}_f$ is given by the natural product of the complex $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ with itself and the $\mathcal{O}_S$-algebra structure is induced from the map of $\mathcal{O}$ as a complex in degree 0 to the complex $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$.

When $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ is injective, we have

$$\mathcal{R}_f = \Gamma(\mathcal{O}_{S_f}),$$

i.e. $\mathcal{R}_f$ is the ring of global functions of S_f, as in Section 3.2.4. Similarly, we can define an $\mathcal{R}_f$-module

$$\mathcal{I}_{f_k} := H^0 R\pi_* \left(\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k) \right), \tag{3.8}$$

for all $k \in \mathbb{Z}$. Let $\mathcal{I}_f{}^{\#} := \mathcal{I}_{f_{-1}}$ and $\mathcal{I}_f := \mathcal{I}_{f_1}$. Clearly $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ are invariant under the $\mathrm{GL}(V)$ action on forms in $\operatorname{Sym}^n V$. Again, when $\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)$ is injective, we have

$$\mathcal{I}_{f_k} = \Gamma(\mathcal{O}_{S_f}(k))$$

for all $k \in \mathbb{Z}$. The constructions of $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ as $\Gamma(\mathcal{O}_{S_f}(k))$ are simpler than the hypercohomological approach, and these constructions give the desired ring and modules on a large locus of nice forms f.

Example 3.3.1. *If $B = \mathbb{Z} \oplus \mathbb{Z}$ and $(f_i) = \mathbb{Z} \oplus \{0\}$, then in $\mathbb{P}^1_{\mathbb{Z}\oplus\mathbb{Z}}$ over the first* $\operatorname{Spec}\mathbb{Z}$ *the form f cuts out* $\operatorname{Spec} R_{p(f)}$*, where $p(f)$ is the projection of f onto the first factor of $(\mathbb{Z} \oplus \mathbb{Z})[x, y]$. Over the second copy of* $\operatorname{Spec}\mathbb{Z}$*, the form f is 0 and cuts out all of $\mathbb{P}^1_{\mathbb{Z}}$. Here $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ is not injective because f is a 0 divisor. Thus the ring $\mathcal{R}_f := H^0 R\pi_*(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O})$ is not just the global functions of S_f but also has a contribution from* $\ker(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O})$.

Unlike the global sections construction, the constructions of $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ for $-1 \leq k \leq n-1$ commutes with base change.

Theorem 3.3.2. *Let $f \in \operatorname{Sym}^n V$ be a binary form over a base scheme S. The construction of $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ for $-1 \leq k \leq n-1$ commutes with base change. More precisely, let $\phi : T \to S$ be a map of schemes. Let $\phi^* f \in \operatorname{Sym}^n \phi^* V$ be the pullback of f. Then the natural map from cohomology*

$$\mathcal{R}_f \otimes \mathcal{O}_T \to \mathcal{R}_{\phi^* f}$$

is an isomorphism of $\mathcal{O}_T$-algebras. Also, for $-1 \leq k \leq n-1$, the natural map from cohomology

$$\mathcal{I}_f \otimes \mathcal{O}_T \to \mathcal{I}_{\phi^* f}$$

is an isomorphism of $\mathcal{R}_{\phi^* f}$-modules (where the $\mathcal{R}_{\phi^* f}$-module structure on $\mathcal{I}_f \otimes \mathcal{O}_T$ comes from the $(\mathcal{R}_f \otimes \mathcal{O}_T)$-module structure.

Proof. The key to this proof is to compute all cohomology of the pushforward of the complex $\mathcal{C}(k) : \mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)$. This can be done using the long exact sequence of cohomology from the short exact sequence of complexes given in Equation (3.12) in the next section. In particular, $\mathcal{C}(k)$ does not have any cohomology in degrees other than 0. Since $k \leq n-1$, we have that $H^0 R\pi_*(\mathcal{O}(-n+k)) = 0$ and thus $H^{-1} R\pi_*(\mathcal{C}(k)) = 0$. Since, $k \geq -1$ we have that $H^1 R\pi_*(\mathcal{O}(k)) = 0$ and thus $H^1 R\pi_*(\mathcal{C}(k)) = 0$. Moreover, in Section 3.3.1, we see that $H^0 R\pi_*(\mathcal{C}(k))$ is locally free. Thus since all $H^i R\pi_*(\mathcal{C}(k))$ are flat, by [26, Corollaire 6.9.9], we have that cohomology and base change commute. □

In the case that f is a free form, we could have defined $\mathcal{R}_f$ as a free rank n $\mathcal{O}_S$-module using the multiplication table given by Equation (3.2) and $\mathcal{I}_{f_k}$ for $-1 \leq k \leq n-1$ as a free rank n $\mathcal{O}_S$-module using the action tables for the Equation (3.3) and (3.5) bases. (See Section 3.2.2 for more details.) Both the constructions from hypercohomology described above and from the multiplication and action tables commute with base change. Thus by verification on the universal form (the proof of Theorem 3.2.7 works over $\mathbb{Z}[f_0, \ldots, f_n]$) we see, as in Theorem 3.2.10, that for free binary forms and $-1 \leq k \leq n-1$, these two definitions of $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ agree.

For any l, we can also formulate this theory for *l-twisted binary forms* $f \in \operatorname{Sym}^n V \otimes (\wedge^2 V)^{\otimes l}$, where

$$\mathcal{R}_f := H^0 R\pi_* \left(\mathcal{O}(-n) \otimes (\pi^* \wedge^2 V)^{\otimes -l} \xrightarrow{f} \mathcal{O} \right), \tag{3.9}$$

and

$$\mathcal{I}_{f_k} := H^0 R\pi_* \left(\mathcal{O}(-n+k) \otimes (\pi^* \wedge^2 V)^{\otimes -l} \xrightarrow{f} \mathcal{O}(k) \right) \tag{3.10}$$

or

$$\mathcal{I}'_{f_k} := H^0 R\pi_* \left(\mathcal{O}(-n+k) \otimes (\pi^* \wedge^2 V) \xrightarrow{f} \mathcal{O}(k) \otimes (\pi^* \wedge^2 V)^{\otimes l+1} \right). \tag{3.11}$$

By the projection formula, $\mathcal{I}'_{f_k} = \mathcal{I}_{f_k} \otimes (\wedge^2 V)^{\otimes l+1}$. By an argument analogous to that of Theorem 3.3.2 we find that these constructions also commute with base change for $-1 \leq k \leq n-1$. In the l-twisted case, we can define S_f as the subscheme of $\mathbb{P}^1(V)$ defined by the ideal sheaf that is the image of $\mathcal{O}(-n) \otimes (\pi^* \wedge^2 V)^{\otimes -l} \xrightarrow{f} \mathcal{O}$. Note that since $\operatorname{Sym}^n V \otimes (\wedge^2 V)^{\otimes l} \cong \operatorname{Sym}^n V^* \otimes (\wedge^2 V^*)^{\otimes -n-l}$ (see Lemmas 3.7.3 and 3.7.4 in the Appendix), the theory of l-twisted binary n-ic forms is equivalent to the theory of $(-n-l)$-twisted binary n-ic forms.

3.3.1 Long exact sequence of cohomology

From the short exact sequence of complexes in degrees -1 and 0

$$\begin{array}{ccc} & & \mathcal{O}(k) \\ & & \downarrow \\ \mathcal{O}(-n+k) & \xrightarrow{f} & \mathcal{O}(k) \\ \downarrow & & \\ \mathcal{O}(-n+k) & & \end{array} \tag{3.12}$$

(where each complex is on a horizontal line), we have the long exact sequence of cohomology

$$H^0 R\pi_* \mathcal{O}(-n+k) \to H^0 R\pi_* \mathcal{O}(k) \to H^0 R\pi_* \left(\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k) \right) \\ \to R^1 \pi_* \mathcal{O}(-n+k) \to R^1 \pi_* \mathcal{O}(k).$$

For $k \leq n-1$, we have $H^0 R\pi_* \mathcal{O}(-n+k) = 0$ and for $k \geq -1$ we have $R^1 \pi_* \mathcal{O}(k) = 0$. Also, $H^0 R\pi_* \mathcal{O}(k) = \operatorname{Sym}^k V$ and $R^1 \pi_* \mathcal{O}(-n+k) = (\operatorname{Sym}^{n-k-2} V)^* \otimes (\wedge^2 V)^*$. Thus for $1 \leq k \leq n-1$ and a binary form $f \in \operatorname{Sym}^n V$, we have the exact sequence

$$0 \to \operatorname{Sym}^k V \to \mathcal{I}_{f_k} \to (\operatorname{Sym}^{n-k-2} V)^* \otimes (\wedge^2 V)^* \to 0. \tag{3.13}$$

Thus $\mathcal{I}_{f_k}$ has a canonical rank $k+1$ $\mathcal{O}_S$-module inside of it (coming from the global sections $x^k, x^{k-1}y, \ldots, y^k$ of $\mathcal{O}(k)$), and a canonical rank $n-k-1$ $\mathcal{O}_S$-module quotient.

So we see, for example, that as an $\mathcal{O}_S$-module

$$\mathcal{R}_f/\mathcal{O}_S \cong (\mathrm{Sym}^{n-2} V)^* \otimes (\wedge^2 V)^*.$$

Note that if we make the corresponding exact sequence for an l-twisted binary form $f \in \mathrm{Sym}^n V \otimes (\wedge^2 V)^{\otimes l}$ we get

$$0 \to \mathrm{Sym}^k V \to \mathcal{I}_{f_k} \to (\mathrm{Sym}^{n-k-2} V)^* \otimes (\wedge^2 V)^{\otimes -l-1} \to 0 \tag{3.14}$$

or

$$0 \to \mathrm{Sym}^k V \otimes (\wedge^2 V)^{\otimes l+1} \to \mathcal{I}'_{f_k} \to (\mathrm{Sym}^{n-k-2} V)^* \to 0. \tag{3.15}$$

In Section 3.2.1 we have given a multiplication table for an explicit basis of $\mathcal{R}_f$ and an (implicit) action table for an explicit basis of $\mathcal{I}_{f_k}$. One naturally wonders how those bases relate to the exact sequences that we have just found. Consider the universal form f over the base ring $B = \mathbb{Z}[f_0, \ldots, f_n]$. We can use a concrete construction of $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ in Section 3.2.1. If K is the fraction field of B, then the concrete constructions of $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ lie in $Q_f := K(\theta)/(f_0\theta^n + f_1\theta^{n-1} + \cdots + f_n)$ and are given by Equations (3.1) and (3.3).

Proposition 3.3.3. *For the universal form f, where V is a free module on x and y, in the exact sequence of Equation* (3.14) *or Equation* (3.15) *(with $\wedge^2 V$ trivialized by the basis element $x \wedge y$) we have that*

$$x^i y^{k-i} \in \mathrm{Sym}^k V \text{ is identified with } \theta^i \in \mathcal{I}_{f_k} \text{ for } 0 \le i \le k$$

and

$$\text{the dual basis to } x^{n-k-i-1}y^{i-1} \in \mathrm{Sym}^{n-k-2} V \text{ is identified with } \zeta_{k+i} \in \mathcal{I}_{f_k}$$

for $1 \le i \le n-k-1$.

Proof. For the universal form, the cohomological construction simplifies. We can replace the complex $\mathcal{O}(-n+k) \to \mathcal{O}(k)$ on $\mathbb{P}^1_B$ with the single sheaf $\mathcal{O}(k)/f(\mathcal{O}(-n+k))$. We can then replace $\mathbf{R}^i\pi_*$ with H^i since the base is affine. The short exact sequence of complexes in Equation (3.12) then simplifies to the short exact sequence of sheaves

$$0 \to \mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k) \to \mathcal{O}(k)/f(\mathcal{O}(-n+k)) \to 0,$$

which gives the same long exact sequence leading to Equation (3.13). The identification of $\mathcal{I}_{f_k}$ with global sections is at the end of proof of Theorem 3.2.7, and from that it is easy to see that the map $H^0(\mathbb{P}^1_B, \mathcal{O}(k)) \to H^0(\mathbb{P}^1_B, \mathcal{O}(k)/f(\mathcal{O}(-n+k))) = \mathcal{I}_{f_k}$ sends $x^i y^{k-i} \mapsto \theta^i$. To compute the δ map $\mathcal{I}_{f_k} \to H^1(\mathbb{P}^1_B, \mathcal{O}(-n+k))$, we use Cech cohomology for the usual affine cover of $\mathbb{P}^1$ and the δ map is the snake lemma map between rows of the Cech complexes.

In the notation of Theorem 3.2.7, the element ζ_{k+i} is identified with the global section z_i. The global function z_i pulls back to $z_i \in \Gamma(U_x, \mathcal{O}(k)) \times \Gamma(U_y, \mathcal{O}(k))$ which maps to $f/(x^{n-k-i}y^i) \in \Gamma(U_x \cap U_y, \mathcal{O}(k))$. This pulls back to $1/(x^{n-k-i}y^i) \in \Gamma(U_x \cap U_y, \mathcal{O}(-n+k))$, which in the standard pairing of the cohomology of projective space (e.g. in [27, III, Theorem 5.1]) pairs with $x^{n-k-i-1}y^{i-1} \in H^0(\mathbb{P}^1_B, \mathcal{O}(n-k-2)) \cong \mathrm{Sym}_{n-k-2} V$. □

Since the ring $\mathcal{R}_f$ acts on $\mathcal{I}_{f_k}$, it is natural to want to understand this action in terms of the exact sequences of Equation (3.14). We have the following description, which can be proved purely formally by the cohomological constructions of everything involved. Alternatively, with the concrete description of the basis elements in Proposition 3.3.3, one could prove the following by computation.

Proposition 3.3.4. *The map $\mathcal{R}_f/\mathcal{O}_S \otimes \operatorname{Sym}^k V \to \operatorname{Sym}_{n-k-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1}$ given by the action of $\mathcal{R}_f$ on $\mathcal{I}_{f_k}$ and the exact sequence of Equation (3.14) is identified with the natural map (see Lemma 3.7.2 in the Appendix)*

$$\operatorname{Sym}_{n-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1} \otimes \operatorname{Sym}^k V \to \operatorname{Sym}_{n-k-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1}$$

under the identification $R/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1}$ of Equation (3.14). The map $\mathcal{R}_f/\mathcal{O}_S \otimes \operatorname{Sym}^k V \otimes (\wedge^2 V)^{\otimes l+1} \to \operatorname{Sym}_{n-k-2} V^*$ given by the action of $\mathcal{R}_f$ on $\mathcal{I}'_{f_k}$ and the exact sequence of Equation (3.15) is identified with the natural map (see Lemma 3.7.2 in the Appendix)

$$\operatorname{Sym}_{n-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1} \otimes \operatorname{Sym}^k V \otimes (\wedge^2 V)^{\otimes l+1} \to \operatorname{Sym}_{n-k-2} V^*$$

under the identification $R/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1}$ of Equation (3.14).

3.3.2 Dual modules

For $-1 \leq k \leq n-1$ we have a map

$$\mathcal{I}'_{f_k} \otimes \mathcal{I}_{f_{n-2-k}} \to \mathcal{I}'_{f_{n-2}} \to \mathcal{O}_S. \tag{3.16}$$

The first map is induced from the map from the product of the complexes used to define $\mathcal{I}'_{f_k}$ and $\mathcal{I}_{f_{n-2-k}}$ to the complex used to define $\mathcal{I}'_{f_{n-2}}$. The second map comes from Equation (3.15).

Theorem 3.3.5. *The pairing in Equation (3.16) gives an $\mathcal{O}_S$-module map*

$$\mathcal{I}'_{f_k} \to \mathcal{I}^*_{f_{n-2-k}},$$

and this map is an $\mathcal{R}_f$-module isomorphism.

Proof. We will show that this map is an $\mathcal{R}_f$-module isomorphism, by checking on the universal form. Since all forms are locally a pull-back from the universal form and these constructions commute with base change, the theorem will follow for all forms.

We use the construction of $\mathcal{R}_f$ and $\mathcal{I}'_{f_k}$ and $\mathcal{I}_{f_{n-2-k}}$ in Section 3.2.1. (Note that for the universal form, we trivialize all $\wedge^2 V$ with the basis $x \wedge y$ and so $\mathcal{I}'_{f_k} = \mathcal{I}_{f_k}$.) Since the complex used to define $\mathcal{I}_{f_i}$ is chain homotopy equivalent to the sheaf $\mathcal{O}(i)/f(\mathcal{O}(i-n))$, we see that the map $\mathcal{I}'_{f_k} \otimes \mathcal{I}_{f_{n-2-k}} \to \mathcal{I}'_{f_{n-2}}$ is just the multiplication of global sections of $\mathcal{O}(k)_{S_f}$ and $\mathcal{O}(n-2-k)_{S_f}$ to obtain a global section of $\mathcal{O}(n-2)_{S_f}$. This can be realized by multiplication of elements of the fractional ideals $\mathcal{I}_{f_k}$, $\mathcal{I}_{f_{n-2-k}}$, and $\mathcal{I}_{f_{n-2}}$ in Section 3.2.1.

Lemma 3.3.6. *Consider the $\mathcal{O}_S$-module basis*

$$1, \theta, \ldots, \theta^k, \zeta_{k+1} + f_{k+1}, \ldots, \zeta_{n-1} + f_{n-1}$$

for $\mathcal{I}'_{f_k}$. For $\mathcal{I}_{f_{n-2-k}}$, consider the $\mathcal{O}_S$-module basis of Equation (3.4)*, but reverse the order to obtain*

$$f_0\theta^{n-1} + f_1\theta^{n-2} + \cdots + f_k\theta^{n-k-1}, \ldots, f_0\theta^{n-k} + f_1\theta^{n-k-1}, f_0\theta^{n-k-1}, \theta^{n-2-k}, \ldots, \theta, 1.$$

These are dual basis with respect to the pairing from Equation (3.16)*.*

Proof. From Proposition 3.3.3, we know that the map $\phi : \mathcal{I}'_{f_{n-2}} \to \mathcal{O}_S$ in Equation (3.15) sends $\zeta_{n-1} \mapsto 1$ and $\theta^i \mapsto 0$ for $0 \leq i \leq n-2$. The proof of this lemma then has four cases.

Case 1: We see that $\theta^i\theta^j \overset{\phi}{\mapsto} 0$ if $0 \leq i \leq k$ and $0 \leq j \leq n-2-k$.

Case 2: We compute the image of $(\zeta_i + f_i)(f_0\theta^j + \cdots + f_{j+k+1-n}\theta^{n-k-1})$ under ϕ for $k+1 \leq i \leq n-1$ and $n-k-1 \leq j \leq n-1$. We have

$$\begin{aligned}
&(\zeta_i + f_i)(f_0\theta^j + \cdots + f_{j+k+1-n}\theta^{n-k-1}) \\
=&(\zeta_i\theta^{n-i} + f_i\theta^{n-i})(f_0\theta^{j+i-n} + \cdots + f_{j+k+1-n}\theta^{i-k-1}) \\
=&(-f_{i+1}\theta^{n-i-1} - \cdots - f_n)(f_0\theta^{j+i-n} + \cdots + f_{j+k+1-n}\theta^{i-k-1}).
\end{aligned}$$

Since $n-i-1+j+i-n = j-1 \leq n-2$, we see that $(\zeta_i + f_i)(f_0\theta^j + \cdots + f_{j+k+1-n}\theta^{n-k-1}) \overset{\phi}{\mapsto} 0$.

Case 3: We compute the image of $\theta^i(f_0\theta^j + \cdots + f_{j+k+1-n}\theta^{n-k-1})$ under ϕ for $0 \leq i \leq k$ and $n-k-1 \leq j \leq n-1$.

- If $i + j \leq n-2$, this maps to 0.
- If $i + j = n-1$, this maps to 1.
- If $i + j \geq n$, the product is

  $$f_0\theta^{j+i} + \cdots + f_{j+k+1-n}\theta^{n-k-1+i} = -f_{j+k+2-n}\theta^{n-k-2+i} - \cdots - f_n\theta^{i+j-n},$$

  and since $n-k-2+i \leq n-2$ it maps to 0.

Case 4: We compute the image of $(\zeta_i + f_i)\theta^j$ under ϕ for $k+1 \leq i \leq n-1$ and $0 \leq j \leq n-2-k$.

- If $i + j \leq n-2$, this maps to 0.
- If $i + j = n-1$, this maps to 1.
- If $i + j \geq n$, the product is $(\zeta_i + f_i)\theta^j = -f_{i+1}\theta^{j-1} - \cdots - f_n\theta^{i+j-n}$, and since $j - 1 \leq n-2$ it maps to 0.

□

Finally, it is easy to see in the universal case that the pairing gives an $\mathcal{R}_f$-module homomorphism $\mathcal{I}'_{f_k} \to \mathcal{I}^*_{f_{n-2-k}}$, since the pairing factors through multiplication of the fractional ideal elements.

□

Corollary 3.3.7. *Let f be an l-twisted binary n-ic form over a base scheme S. Then we have an isomorphism of $\mathcal{R}_f$-modules*

$$\mathcal{I}'_{f_{n-2}} \cong \mathcal{H}om_{\mathcal{O}_S}(\mathcal{R}_f, \mathcal{O}_S)$$

given by $j \mapsto (r \mapsto \phi(rj))$ where $\phi : \mathcal{I}_{f_{n-2}} \to \mathcal{O}_S$ is the map from Equation (3.15).

3.4 Main Theorem for (-1)-twisted binary forms

Let f be a (-1)-twisted binary form over a base scheme S. Let $R = \mathcal{R}_f$, let $I = \mathcal{I}_{f_{n-3}}$, and let $I \to Q$ be the canonical quotient of $\mathcal{I}_{f_{n-3}}$ from Equation (3.14). So, $Q \cong V^*$. From Proposition 3.3.4, we know that the map $R/\mathcal{O}_S \otimes \operatorname{Sym}^{n-3} Q^* \to Q$ given by the action of R on I and the exact sequence of Equation (3.14) is identified with the natural map $\operatorname{Sym}_{n-2} Q \otimes \operatorname{Sym}^{n-3} Q^* \to Q$ under the identification $R/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} Q$ of Equation (3.14).

Definition. A *binary n-pair* is an $\mathcal{O}_S$-algebra R, an R-module I, an exact sequence $0 \to \operatorname{Sym}^{n-3} Q^* \to I \to Q \to 0$ such that Q is a locally free rank 2 $\mathcal{O}_S$-module, and an isomorphism $R/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} Q$ that identifies the map $R/\mathcal{O}_S \otimes \operatorname{Sym}^{n-3} Q^* \to Q$ induced from the action of R on I with the natural map $\operatorname{Sym}_{n-2} Q \otimes \operatorname{Sym}^{n-3} Q^* \to Q$.

Remark 3.4.1. When $n = 3$, we have that $\ker(I \to Q) \cong \mathcal{O}_S$ and the map $Q \otimes \mathcal{O}_S \to Q$ given by the ring action $R/\mathcal{O}_S \otimes \ker(I \to Q) \to Q$ is just the natural one. We can tensor the exact sequence $0 \to \mathcal{O}_S \to R \to R/\mathcal{O}_S \to 0$ with $\ker(I \to Q)$ to show that $R \cong I$ as R-modules. We first obtain the action sequence

$$0 \to \mathcal{O}_S \otimes \ker(I \to Q) \to R \otimes \ker(I \to Q) \to R/\mathcal{O}_S \otimes \ker(I \to Q) \to 0.$$

The action of R on I gives a map from that sequence to

$$0 \to \ker(I \to Q) \to I \to Q \to 0,$$

and since the outside maps are isomorphisms, by the 5-Lemma we have $R \otimes \ker(I \to Q) \cong I$. If k is a basis element for $\ker(I \to Q)$, then we have the map $R \to I$ given by $r \mapsto rk$ is an isomorphism of $\mathcal{O}_S$-modules. Moreover, since $r'r \mapsto r'rk = r'(rk)$, this is also an isomorphism of R-modules. Moreover, the map of complexes above shows that in this isomorphism $\mathcal{O}_S \xrightarrow{\sim} \ker(I \to Q)$ and $R/\mathcal{O}_S \xrightarrow{\sim} Q$. We can conclude that a twisted binary setup is just equivalent to a cubic ring, i.e. an $\mathcal{O}_S$-algebra R such that $R/\mathcal{O}_S$ is a locally free rank 2 $\mathcal{O}_S$-module.

There are two equivalent formulations of the definition of a twisted binary pair that can be useful.

Proposition 3.4.2. *An $\mathcal{O}_S$-algebra R and and R-module I are in a a binary pair with Q a free $\mathcal{O}_S$-module if and only if R has a $\mathcal{O}_S$-module basis $\zeta_0 = 1, \zeta_1, \ldots, \zeta_{n-1}$ and and I has a $\mathcal{O}_S$-module basis $\alpha_1, \alpha_2, \beta_1, \ldots, \beta_{n-2}$ such that*

$$\text{the } \alpha_i \text{ coefficient of } \zeta_j\beta_k \text{ is } \begin{cases} 1 & \text{if } i+j+k = n+1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If Q is free with basis x, y and dual basis $\dot{x}$ and $\dot{y}$, we can explicitly calculate the natural map $\mathrm{Sym}_{n-2} Q \otimes \mathrm{Sym}^{n-3} Q^* \to Q$. Let $\mathrm{sym}(w)$ of a word w be the sum of all distinct permutations of w. We have that

$$\mathrm{sym}(x^i y^{n-2-i}) \otimes \dot{x}^j \dot{y}^{n-3-j} \mapsto \begin{cases} x & \text{if } i = j+1 \\ y & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

We have $\zeta_j \in \mathrm{Sym}_{n-2} Q$ corresponding to $\mathrm{sym}(x^{n-j-1}y^{j-1})$, and α_1 corresponding to y and α_2 corresponding to x, and β_k corresponding to $\dot{x}^{k-1}\dot{y}^{n-2-k}$, and we obtain the proposition. □

Proposition 3.4.3. *An $\mathcal{O}_S$-algebra R, an R-module I, a locally free rank 2 $\mathcal{O}_S$-module Q that is a quotient of I, and an isomorphism of $\mathcal{O}_S$-modules $\phi : \mathrm{Sym}_{n-2} Q \cong R/\mathcal{O}_S$ are in twisted binary pair if and only if*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sym}_{n-1} Q & \longrightarrow & Q \otimes \mathrm{Sym}_{n-2} Q & \longrightarrow & (\ker(I \to Q))^* \otimes \wedge^2 Q & \longrightarrow & 0 \\ & & q_1 q_2 \cdots q_{n-1} & \mapsto & q_1 \otimes q_2 \cdots q_{n-1} & \mapsto & & & \\ & & & & q \otimes q_1 \cdots q_{n-2} & \mapsto & (k \mapsto q \wedge \phi(q_1 \cdots q_{n-2}) \circ k) & & \end{array}$$

is an exact sequence, where $\circ$ denotes the action of R on I followed by the quotient to Q..

Proposition 3.4.3 follows from the following Lemma, proven in Lemma 3.7.5 in the Appendix (Section 3.7).

Lemma 3.4.4. *If Q is any locally free rank 2 $\mathcal{O}_S$-module, we have the exact sequence*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sym}_{n-1} Q & \longrightarrow & Q \otimes \mathrm{Sym}_{n-2} Q & \longrightarrow & \mathrm{Sym}_{n-3} Q \otimes \wedge^2 Q & \longrightarrow & 0. \\ & & q_1 q_2 \cdots q_{n-1} & \mapsto & q_1 \otimes q_2 \cdots q_{n-1} & \mapsto & q_2 \cdots q_{n-2} \otimes (q_{n-1} \wedge q_1) & & \end{array}$$

The following lemma is used to construct a (-1)-twisted binary form from a binary pair, and is proven in Lemma 3.7.6 in the Appendix (Section 3.7).

Lemma 3.4.5. *Let R be an $\mathcal{O}_S$-algebra, I be an R-module, Q be a locally free rank 2 $\mathcal{O}_S$-module quotient of I, and ϕ be an isomorphism of $\mathcal{O}_S$-modules $\phi : \mathrm{Sym}_{n-2} Q \cong R/\mathcal{O}_S$. If*

$$\begin{array}{ccc} \mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q) & \longrightarrow & \wedge^2 Q \\ q_1 \cdots q_{n-1} \otimes k & \mapsto & q_1 \wedge \phi(q_2 \cdots q_{n-1}) \circ k \end{array}$$

is the zero map, then

$$\begin{array}{ccc} \mathrm{Sym}_n Q & \longrightarrow & \wedge^2 Q \\ q_1 \cdots q_n & \mapsto & q_1 \wedge \phi(q_2 \cdots q_{n-1}) \circ \tilde{q_n} \end{array}$$

is well-defined. Here the $\circ$ denotes the action of R on I followed by the quotient to Q and $\tilde{q}$ denotes a fixed splitting $Q \to I$. In particular the map $\mathrm{Sym}_n Q \to \wedge^2 Q$ does not depend on the choice of this splitting.

By Proposition 3.4.3, we see that $\mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q) \to \wedge^2 Q$ is always the zero map for a twisted binary pair, and thus we can use Lemma 3.4.5 to construct a (-1)-twisted binary form in $\mathrm{Sym}^n Q^* \otimes \wedge^2 Q$ from a twisted binary pair. We can write the map of Lemma 3.4.5 as the evaluation

$$x \mapsto x \wedge \phi(x^{n-2})x$$

of a degree n map $Q \to \wedge^2 Q$. Note this coincides with the map $x \wedge x^2$ as described in the case of binary cubic forms in [5, Footnote 3].

Remark 3.4.6. For $n = 2$, note that $\phi(1)$ is *not* $1 \in R$ but rather a generator of $R/\mathcal{O}_S$.

Theorem 3.4.7. *Let (V, f) be a (-1)-twisted binary form and (R, I) be its associated twisted binary pair. The (-1)-twisted binary form constructed from (R, I) is $f \in \mathrm{Sym}^n V \otimes \wedge^2 V$.*

Proof. First we note that the (-1)-twisted binary form constructed from (R, I) is a global section of $\mathrm{Sym}^n V \otimes \wedge^2 V$. Then, we can check the theorem locally on S, so we can assume that f is a free form. Since f then is a pull-back from the universal form, we can just check the theorem on the universal form f over $B = \mathbb{Z}[f_0, \ldots, f_n]$. Let x, y be the basis of $Q \cong V^*$ and $\dot{x}, \dot{y}$ be a corresponding dual basis.

The (-1)-twisted binary n-ic form associated to our binary n-pair is given by

$$\begin{array}{ccc} \mathrm{Sym}_n Q & \longrightarrow & \wedge^2 Q \\ q_1 \cdots q_n & \mapsto & q_1 \wedge \phi(q_2 \cdots q_{n-1}) \circ \tilde{q_n} \end{array}.$$

Thus for $1 \leq k \leq n$ we have

$$\begin{aligned} \mathrm{sym}(x^k y^{n-k}) \mapsto\ & x \wedge \phi(\mathrm{sym}(x^{k-2} y^{n-k}))x + x \wedge \phi(\mathrm{sym}(x^{k-1} y^{n-k-1}))y \\ & + y \wedge \phi(\mathrm{sym}(x^{k-1} y^{n-k-1}))x + y \wedge \phi(\mathrm{sym}(x^k y^{n-k-2}))y \\ =\ & (\dot{y}(\zeta_{n-k+1}x) + \dot{y}(\zeta_{n-k}y) - \dot{x}(\zeta_{n-k}x) - \dot{x}(\zeta_{n-k-1}y)) \otimes (x \wedge y) \end{aligned} \tag{3.17}$$

where by convention $\mathrm{sym}(x^a y^b)$ is zero if either a or b is negative and $\zeta_i = 0$ if $i < 1$ or $i > n - 1$. If K is the fraction field of B, then the concrete constructions of $\mathcal{R}_f$ and $\mathcal{I}_{f_{n-3}}$ from Section 3.2.1 lie in $Q_f := K(\theta)/(f_0\theta^n + f_1\theta^{n-1} + \cdots + f_n)$ and are given by Equations (3.1) and (3.3). From Proposition 3.3.3, we know we can can identify x with the image of ζ_{n-2} and y with the image of ζ_{n-1} in the concrete construction of $\mathcal{I}_{f_{n-3}}$. We can further identify $1, \theta, \ldots, \theta^{n-3}$ with the kernel $\mathrm{Sym}^{n-3} Q^*$ of $I \to Q$. Using the basis ζ_i of $\mathcal{R}_f$ and the basis from Equation (3.3) for $\mathcal{I}_{f_{n-3}}$,

we have that the ζ_{n-1} and ζ_{n-2} coordinates of elements in $\mathcal{R}_f$ and $\mathcal{I}_{f_{n-3}}$ do not depend on whether taken in the $\mathcal{R}_f$ basis or $\mathcal{I}_{f_{n-3}}$ basis. We can thus compute the expressions $\dot{y}(\zeta_{n-k+1}x), \dot{y}(\zeta_{n-k}y), \dot{x}(\zeta_{n-k}x), \dot{x}(\zeta_{n-k-1}y)$ from Equations (3.2) to prove the proposition. We have

$$\dot{y}(\zeta_{n-k}y) = \begin{cases} -f_{n-k} & \text{if } k = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\dot{y}(\zeta_{n-k+1}x) = \begin{cases} f_{n-k} & \text{if } 3 \leq k \leq n \\ 0 & \text{otherwise} \end{cases}$$

$$\dot{x}(\zeta_{n-k-1}y) = \begin{cases} -f_{n-k} & \text{if } 0 \leq k \leq 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\dot{x}(\zeta_{n-k}x) = \begin{cases} -f_{n-k} & \text{if } 1 \leq k \leq 2 \\ 0 & \text{otherwise.} \end{cases}$$

□

In fact, we have the following theorem, which shows that (-1)-twisted binary forms exactly parametrize twisted binary pairs.

Theorem 3.4.8. *For $n \geq 3$, we have a bijection between (-1)-twisted binary n-ic forms over S and binary n-pairs over S, and the bijection commutes with base change in S. In other words, we have a isomorphism of the moduli stack of (-1)-twisted binary n-ic forms and the moduli stack of binary n-pairs.*

An isomorphism of two (-1)-twisted binary n-ic forms $f \in \mathrm{Sym}^n V \otimes \wedge^2 V^*$ and $f' \in \mathrm{Sym}^n V' \otimes \wedge^2 (V')^*$ is an isomorphism $V \cong V'$ that preserves f. An isomorphism of two binary n-pairs R, I, Q and R', I', Q' is given by isomorphisms $R \cong R'$, and $I \cong I'$, and $Q \cong Q'$ that respect the exact sequence for I (and I') and the maps $R/\mathcal{O}_S \cong \mathrm{Sym}_{n-2} Q$ and $R'/\mathcal{O}_S \cong \mathrm{Sym}_{n-2} Q'$.

See Chapter 2 for the full story for binary quadratic forms. In the $n = 3$ case, from Remark 3.4.1 we know that a twisted binary 3-pair is equivalent to a *cubic ring*, an $\mathcal{O}_S$-algebra R such that $R/\mathcal{O}_S$ is a locally free rank 2 $\mathcal{O}_S$-module. Thus we obtain the following corollary, given in [19] (see also Chapter 6 for a detailed exposition of this case).

Corollary 3.4.9. *We have a bijection between (-1)-twisted binary cubic forms over S and cubic rings over S, and the bijection commutes with base change in S. In other words, we have a isomorphism of the moduli stack of (-1)-twisted binary n-ic forms and the moduli stack of cubic rings.*

To prove Theorem 3.4.8 we will rigidify the moduli stacks, and thus we will need to define based twisted binary pairs.

3.4.1 Based twisted binary pairs

A *based twisted binary pair* is twisted binary pair R, I, Q and a choice of basis x, y of Q such that Q is the free $\mathcal{O}_S$-module on x and y. This gives a natural basis of $R/\mathcal{O}_S$ as a free rank $(n-1)$ $\mathcal{O}_S$-module, and thus R is a free rank n $\mathcal{O}_S$-module. Let $K = (\mathrm{Sym}_{n-3} Q)^* = \ker(I \to Q)$, and so we have a natural basis for K as a free rank $n-2$ $\mathcal{O}_S$-module. Thus I is a free rank n $\mathcal{O}_S$-module. However, we do not yet have canonical bases for R and I as $\mathcal{O}_S$-modules. We will pick these using certain normalizations.

Let $\zeta_i = \mathrm{sym}(x^{n-1-i}y^{i-1})$ for $1 \leq i \leq n-1$ be the given basis of $R/\mathcal{O}_S$ and let k_j for $1 \leq j \leq n-2$ be the given basis of K dual to the basis $\mathrm{sym}\, x^{j-1}y^{n-2-j}$ of $\mathrm{Sym}_{n-3} Q$. Let $\dot{x}, \dot{y} \in Q^*$ be a dual basis of x, y. (Recall that $\mathrm{sym}(w)$ for a word w is the sum of all distinct permutations of w.) Thus from Proposition 3.4.2,

$$\text{the image of } \zeta_i k_j \text{ in } Q \text{ is } \begin{cases} x & \text{if } i+j = n-1 \\ y & \text{if } i+j = n \\ 0 & \text{otherwise.} \end{cases} \tag{3.18}$$

Remark 3.4.10. For $n = 3$, here we see that $\zeta_1 k_1 = x$ and $\zeta_2 k_1 = y$, and thus I is a principal ideal generated by k_1. Moreover, this determines the sequence $K \to I \to Q$ is just $\mathcal{O}_S k_1 \to R k_1 \to R k_1/\mathcal{O}_S k_1$. Therefore a based twisted binary 3 setup is just a cubic ring with a given basis of $R/\mathcal{O}_S$.

Equation (3.18) allows us to choose normalized lifts of x and y to elements of I that forms a basis along with the given basis of K, and normalized lifts of the ζ_i to R to form a basis along with 1. We choose these lifts so that

$$\dot{y}(\zeta_i x) = 0 \text{ for } 2 \leq i \leq n-1 \tag{3.19}$$

by changing the lift x by an appropriate multiple of k_{n-i}. We then specify that

$$\dot{x}(\zeta_i x) = 0 \text{ for } 1 \leq i \leq n-1 \tag{3.20}$$

by changing the lift of ζ_i by an appropriate multiple of 1. Finally, we specify that

$$\dot{y}(\zeta_i y) = 0 \text{ for } 2 \leq i \leq n-1 \tag{3.21}$$

by changing the lift of y by an appropriate multiple of k_{n-i}. These specifications determine a unique lift of x and y to I, and unique lifts of the ζ_i to R, which we will refer to now as simply x, y, and ζ_i. We will now see that with these choices of normalized bases for R and I, we can determine the action of R and I in terms of a small number of variables, and these variables will in fact be the coefficients of the binary form associated to this binary setup.

There are only $n+1$ coordinates we have not determined in the maps $\zeta_i : I \to Q$. Equation (3.18) gives $\zeta_i : K \to Q$. Our choice of normalization gives all but the following. Let $-a_{i+1} = \dot{x}(\zeta_i y)$ for $1 \leq i \leq n-1$. Let $a_0 = \dot{y}(\zeta_1 x)$ and $a_1 = \dot{y}(\zeta_1 y)$.

These a_i specify the map $\zeta_i : I \to Q$.

	$\zeta_k x$	$\zeta_k y$
x coordinate	0 for $1 \leq k \leq n-1$	$-a_{k+1}$ for $1 \leq k \leq n-1$
y coordinate	a_0 for $k = 1$ 0 for $2 \leq k \leq n-1$	a_1 for $k = 1$ 0 for $2 \leq k \leq n-1$

We have carefully indexed and signed the a_i so that we have the following.

Proposition 3.4.11. *The (-1)-twisted binary form associated to the above based twisted binary setup is*

$$\begin{array}{ccc} \mathrm{Sym}_n Q & \longrightarrow & \wedge^2 Q \\ \mathrm{sym}(x^k y^{n-k}) & \mapsto & a_{n-k} x \wedge y \end{array}.$$

Proof. We use the formula

$$\mathrm{sym}(x^k y^{n-k}) \mapsto (\dot{y}(\zeta_{n-k+1} x) + \dot{y}(\zeta_{n-k} y) - \dot{x}(\zeta_{n-k} x) - \dot{x}(\zeta_{n-k-1} y)) \otimes (x \wedge y)$$

from Equation (3.17) , where $\dot{x}$ and $\dot{y}$ denote the x and y coordinates respectively . □

Moreover, we find that the coefficients of the associated (-1)-twisted binary form determine the based twisted binary pair.

Proposition 3.4.12. *The maps $\zeta_i : R \to I$ and $\zeta_i : R \to R$ are determined by the maps $\zeta_i : I \to Q$ and the commutativity relations on the ζ_i. Each coordinate of the action and multiplication maps is as a polynomial in the a_i with integral coefficients.*

Proof. We view each map $\zeta_i : R \to I$ as an n by n matrix Z_i. We write $Z_i(a, b)$ for the a, b entry of Z_i, which is the k_a coordinate of $\zeta_i k_b$, where by convention $k_{n-1} = x$ and $k_n = y$. We let $\mathcal{K}$ be the set of all of entries of these matrices that are determined by the entries in the last two rows of the matrices as polynomials in the a_i (i.e. the maps $\zeta_i : I \to Q$), as well as as all polynomial combinations of the matrix entries which are so determined. We will show that the systems of equations given by commutativity of the ζ_i determine all the matrix entries from the last two rows. So, by definition we have $Z_i(n-1, k), Z_i(n, k) \in \mathcal{K}$ for $1 \leq i \leq n-1$ and $1 \leq k \leq n$.

We have two tools that we use to solve for more and more matrix entries.

Lemma 3.4.13. *We have*

$$Z_i(n-1-\ell, k) - Z_\ell(n-1-i, k) \in \mathcal{K}, \quad \text{for } 1 \leq i \leq n-1 \text{ and } 1 \leq \ell \leq n-1$$

Proof. Consider the $n-1$st rows (x coordinates) of $Z_i Z_\ell$ and $Z_\ell Z_i$. Equating the jth entries in both these rows gives the lemma, where by convention $Z_i(0, k) = 0$. □

Lemma 3.4.14. *We have*

$$Z_i(n-\ell, k) - Z_\ell(n-i, k) \in \mathcal{K}, \quad \text{for } 1 \leq \ell \leq n-1 \text{ and } 1 \leq i \leq n-1.$$

Proof. Consider the nth rows (y coordinates) of Z_iZ_ℓ and $Z_\ell Z_i$. Equating the jth entries in both these rows gives the lemma. □

We prove, by induction, that all the entries of Z_i are in $\mathcal{K}$ for $1 \leq i \leq n-1$. We can use $i = 0$ as the (trivial) base case. Assuming that all the entries of Z_i are in $\mathcal{K}$, we will now show that the entries of Z_{i+1} are in $\mathcal{K}$. Using Lemma 3.4.13, we see that that all matrix entries in the $n-1-i$th row are in $\mathcal{K}$. (If $i = 0$ this is by from the definition of $\mathcal{K}$.) Using Lemma 3.4.14, we conclude all the entries of Z_{i+1} are in $\mathcal{K}$, which completes the induction.

This shows the proposition for the maps $\zeta_i : R \to I$. From Equation (3.18), we see that since $n \geq 3$, each Z_i has a 1 in a matrix entry for which all z_j for $j \neq i$ have entry 0. Thus, the action of R on I gives an injection of R into the space on n by n matrices. To find the ζ_k coordinate of $\zeta_i\zeta_j$, we just have to look at the matrix entry of Z_iZ_j where Z_k has a 1 and all Z_ℓ for $\ell \neq k$ have a zero. This shows the proposition for the maps $\zeta_i : R \to I$. □

Now we prove Theorem 3.4.8.

Proof. The stack of twisted binary n-pairs is the quotient of the stack of based twisted binary n-pairs by the GL_2 action given by change of the basis for Q. Since a based twisted binary n-pair is given by $a_0, \ldots, a_n \in \mathcal{O}_S$, and we have one such binary pair for every choice of a_i's (given by the corresponding binary form), the moduli space of based twisted binary n-pairs is $\mathbb{Z}[a_0, \ldots, a_n]$, and there is a universal based twisted binary n-pair.

We have maps between the stack of (-1)-twisted binary n-ic forms and twisted binary n-pairs in both directions, which lift to the rigidified versions of these stacks, the stacks of corresponding based objects. Theorem 3.4.7 shows that the map from forms to pairs back to forms is the identity. We will show that the other composition of these constructions is the identity by verifying it on the rigidified stacks. If we start with the universal based twisted binary n-pair, Proposition 3.4.11 shows that the associated form is the universal binary n-ic form. From the universal binary n-ic form we construct some based twisted binary n-pair (R, I), and Proposition 3.4.12 shows that (R, I) is determined from the binary form constructed from it–which is just the universal binary form (since we know going from forms to pairs to forms is the identity). Since the universal based twisted binary n-pair and (R, I) both give the same form, by Proposition 3.4.12 they are the same. Thus, we have prove there is an isomorphism of the moduli stack of (-1)-twisted binary n-ic forms and the moduli stack of twisted binary n-pairs. □

We could have done all the work in this section with $\mathcal{I}_{f_1}$, the dual of $\mathcal{I}_{f'_{n-3}}$, and considered analogs of binary pairs where the conditions on the module would be $\mathcal{O}_S$-dual to the conditions on I in a binary pair. It turns out some of the constructions are more natural when working with $\mathcal{I}_{f'_{n-3}}$ and binary pairs, so we have chosen to exposit that version.

One could prove analogs of Theorem 3.4.8 for all l-twisted binary forms. We define an *k-twisted binary n-pair* is an $\mathcal{O}_S$-algebra R, an R-module I, an exact sequence

$0 \to \mathrm{Sym}^{n-3} Q^* \otimes (\wedge^2 Q)^{\otimes -k} \to I \to Q \to 0$ such that Q is a locally free rank 2 $\mathcal{O}_S$-module, and an isomorphism $R/\mathcal{O}_S \cong \mathrm{Sym}_{n-2} Q \otimes (\wedge^2 Q)^{\otimes k}$ that identifies the map $R/\mathcal{O}_S \otimes \mathrm{Sym}^{n-3} Q^* \otimes (\wedge^2 Q)^{\otimes -k} \to Q$ induced from the action of R on I with the natural map $\mathrm{Sym}_{n-2} Q \otimes (\wedge^2 Q)^{\otimes k} \otimes \mathrm{Sym}^{n-3} Q^* \otimes (\wedge^2 Q)^{\otimes -k} \to Q$. Given an l-twisted binary n-ic form, we get an $(l+1)$-twisted binary pair from $\mathcal{R}_f$, $\mathcal{I}_{f\,n-3}'$, and the exact sequence from Equation (3.15).

For example, in a k-twisted binary 3-pair we can see that $I \cong R \otimes \wedge^2 Q^{\otimes -k}$, by the same argument that we used to see I was a principal R-module in a binary 3-pair. So, we see that I is determined uniquely by R. However, since we have that $R/\mathcal{O}_S \cong Q \otimes (\wedge^2 Q)^{\otimes k}$, we see that not all cubic algebras will appear as k-twisted binary 3-pairs.

3.5 Further questions

For simplicity, we ask further questions over the base $\mathbb{Z}$. One naturally wonders which rank n rings appear in a binary pair. In other words, which rank n rings have modules satisfying the conditions of a binary pair? When $n = 3$, we saw that the answer is all cubic rings, and each has a unique module and exact sequence that makes a binary pair. For $n = 4$, there is another characterization of the answer. In Chapter 4 it is shown that the quartic rings associated to binary quartic forms are exactly the quartic rings with monogenic cubic resolvents. The cubic resolvent is a certain integral model of the classical cubic resolvent field. Are there such connections with resolvents for higher n?

Simon [39] asks which maximal orders are realized from binary n-ic forms. He defines the *index* of a form to be the index of its ring in the maximal order. He begins a program to compute all forms with a given index. For example, in the quartic case he uses elliptic curves to compute the forms of index 1 and a certain I and J ($\mathrm{GL}_2(\mathbb{Z})$ invariants of a binary quartic form). Simon also shows that there are no index 1 forms with a root generating a cyclic extension of prime degree at least 5.

3.6 Appendix I: Verifications of $\mathbb{Z}$ basis of ${I_f}^k$

Proposition 3.6.1. *For f with $f_0 \neq 0$ and $1 \leq k \leq n-1$, the R_f module ${I_f}^k$ is a free rank n $\mathbb{Z}$-module on the basis given in Equation 3.3.*

Lemma 3.6.2. *We have*

$$R_f \theta^k \subset \left\langle R_f, \theta, \theta^2, \ldots, \theta^k \right\rangle_{\mathbb{Z}}$$

for all $k \geq 1$.

Proof ofLemma 3.6.2. We see that

$$\zeta_i \theta^k = f_0 \theta^{k+i} + \cdots + f_{i-1} \theta^{k+1} \quad \text{if } k + i \leq n - 1$$

and

$$\begin{aligned}\zeta_i\theta^k =& \theta^{k+i-n}(f_0\theta^n + \cdots + f_{i-1}\theta^{n-i+1}) \quad \text{if } k+i \geq n\\ =& -\theta^{k+i-n}(f_i\theta^{n-i} + \cdots + f_n)\\ =& -(f_i\theta^k + \cdots + f_n\theta^{k+i-n}).\end{aligned}$$

□

Proof of Proposition 3.6.1. So, as a $\mathbb{Z}$-module ${I_f}^k$ is generated by the elements

$$1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots \zeta_{n-1}$$

for $k \geq 1$. If $k \leq n-1$, then since $f_0 \neq 0$, we have that $1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots \zeta_{n-1}$ generate a free $\mathbb{Z}$-module, and thus are a $\mathbb{Z}$-module basis for ${I_f}^k$. □

Proposition 3.6.3. *The $\mathbb{Z}$-module ${I_f}^\#$ defined by Equation* (3.5) *is an ideal.*

Proof. Let $J = \theta{I_f}^\# = \langle \zeta_1, \zeta_2, \ldots, \zeta_{n-1}, -f_n\rangle_{\mathbb{Z}}$. From the multiplication table given in Equation (3.2) we see that $\langle \zeta_1, \ldots, \zeta_{n-1}\rangle_{\mathbb{Z}} \cdot \langle \zeta_1, \ldots, \zeta_{n-1}\rangle_{\mathbb{Z}} \subset J$. Thus, $R_f J \subset J$ and so J and thus ${I_f}^\#$ are ideals of R_f. □

Proposition 3.6.4. *Let f be a non-zero binary n-ic form. Then, the fractional ideal I_f is invertible if and only if the form f is primitive. Also, the fractional ideal ${I_f}^\#$ is invertible if and only if the form f is primitive. We always have that ${I_f}^\# = (R_f : I_f)$, where $(A : B) = \{x \in Q_f |\, xB \subset A\}$. In the case that f is primitive, ${I_f}^{-1} = {I_f}^\#$.*

Proof. First, we act by $\mathrm{GL}_2(\mathbb{Z})$ so that we may assume $f_0 \neq 0$. Since ${I_f}^\# \subset R_f$ and $\theta{I_f}^\# = \langle \zeta_1, \zeta_2, \ldots, \zeta_{n-1}, -f_n\rangle_{\mathbb{Z}} \subset R_f$, we have $I_f{I_f}^\# \subset R_f$. More specifically, we see that

$$\begin{aligned}I_f{I_f}^\# =& \langle f_0, \zeta_1 + f_1, \ldots, \zeta_{n-1} + f_{n-1}, \zeta_1, \zeta_2, \ldots, \zeta_{n-1}, -f_n\rangle_{\mathbb{Z}}\\ =& \langle f_0, f_1, \ldots, f_n, \zeta_1, \zeta_2, \ldots, \zeta_{n-1}\rangle_{\mathbb{Z}},\end{aligned}$$

which is equal to R_f if and only if the form f is primitive.

Let $x \in (R_f : I_f)$. Since $1 \in I_f$, we have $x \in R_f$. Write $x = x_0 + \sum_{i=0}^{n-1} x_i(\zeta_i + f_i)$ where the $x_i \in \mathbb{Z}$. Also, $\theta x \in R_f$, and $\theta x = x_0\theta + \sum_{i=0}^{n-1} x_i\zeta_{i+1}$. Thus $f_0 \mid x_0$, which implies $x \in {I_f}^\#$. We conclude ${I_f}^\# = (R_f : I_f)$.

Suppose I_f is invertible. Then, its inverse is $(R_f : I_f) = {I_f}^\#$, which implies $I_f{I_f}^\# = R_f$ and the form f is primitive. Suppose $I_f^\#$ is invertible, then the norm of $I_f{I_f}^\#$ is the product of the norms of I_f and ${I_f}^\#$, which is 1. Since $I_f{I_f}^\# \subset R_f$, we have that $I_f{I_f}^\# = R_f$ and the form f is primitive. □

3.7 Appendix: Maps of locally free $\mathcal{O}_S$-modules

Let S be a scheme. In this appendix we will give several basic facts about maps between locally free $\mathcal{O}_S$-modules.

Lemma 3.7.1. *Let V be a locally free $\mathcal{O}_S$ module. We have $(\mathrm{Sym}_n V)^* \cong \mathrm{Sym}^n V^*$.*

Proof. We give a map from $\mathrm{Sym}^n V^*$ to $(\mathrm{Sym}_n V)^*$ as follows

$$\mathcal{V}_1\mathcal{V}_2\cdots\mathcal{V}_n \mapsto (v_1\otimes\cdots\otimes v_n \mapsto \mathcal{V}_1(v_1)\mathcal{V}_2(v_2)\cdots\mathcal{V}_n(v_n)).$$

If we permute the $\mathcal{V}_i$ factors, we see the result does not change because the elements of $\mathrm{Sym}_n V$ that we evaluate on are invariant with respect to this permutation. When V is free, we see that $\check{e_{i_1}}\check{e_{i_2}}\cdots\check{e_{i_n}}$ is the dual of $\mathrm{sym}(i_1,\ldots,i_n)\in\mathrm{Sym}_n V$. In this case this map is an isomorphism and thus it is an isomorphism for all locally free V. □

Lemma 3.7.2. *Let V be a locally free $\mathcal{O}_S$ module. Inside of $V^{\otimes a+b}$ the submodule $\mathrm{Sym}_{a+b} V$ is a submodule of $\mathrm{Sym}_a V\otimes\mathrm{Sym}_b V$. Thus we have a natural map*

$$\mathrm{Sym}_{a+b} V \to \mathrm{Sym}_a V\otimes\mathrm{Sym}_b V,$$

which is injective.

Proof. We can check locally where V is free that $\mathrm{Sym}_{a+b} V$ is a submodule of $\mathrm{Sym}_a V\otimes\mathrm{Sym}_b V$. The natural map sends $v_1\cdots v_{a+b}$ to $v_1\cdots v_a\otimes v_{a+1}\cdots v_{a+b}$. This is just the dual of the natural map $\mathrm{Sym}^a V^*\otimes\mathrm{Sym}^b V^*\to\mathrm{Sym}^{a+b} V^*$. □

Lemma 3.7.3. *If L is a locally free rank 1 $\mathcal{O}_S$-module and V is a locally free rank n $\mathcal{O}_S$-module, then $\mathrm{Sym}^k(V\otimes L)\cong\mathrm{Sym}^k V\otimes L^{\otimes k}$.*

Proof. We have the canonical map

$$\begin{array}{ccc}\mathrm{Sym}^k(V\otimes L) & \longrightarrow & \mathrm{Sym}^k V\otimes\mathrm{Sym}^k L\\ (v_1\otimes\ell_1)\cdots(v_k\otimes\ell_k) & \mapsto & v_1\cdots v_k\otimes\ell_1\cdots\ell_k\end{array},$$

which we can check is an isomorphism on free modules and thus is an isomorphism on locally free modules. Moreover, we have that $L^{\otimes k}\cong\mathrm{Sym}^k L$. We have the canonical quotient map $L^{\otimes k}\to\mathrm{Sym}^k L$ which is clearly an isomorphism for L free of rank 1 and thus locally free of rank 1. □

Lemma 3.7.4. *If V is a locally free $\mathcal{O}_S$-module of rank two then $V\otimes\wedge^2 V^*\cong V^*$.*

Proof. We can define the canonical map which is an isomorphism for free and thus locally free modules of rank 2.

$$\begin{array}{ccc}V\otimes\wedge^2 V^* & \longrightarrow & V^*\\ v\otimes(\mathcal{V}_1\wedge\mathcal{V}_2) & \mapsto & \mathcal{V}_1(v)\mathcal{V}_2-\mathcal{V}_2(v)\mathcal{V}_1\end{array}$$

□

Lemma 3.7.5. *If Q is any locally free rank 2 $\mathcal{O}_S$-module, we have the exact sequence*

$$\begin{array}{ccccccccc}0 & \longrightarrow & \mathrm{Sym}_{n-1} Q & \longrightarrow & Q\otimes\mathrm{Sym}_{n-2} Q & \longrightarrow & \mathrm{Sym}_{n-3} Q\otimes\wedge^2 Q & \longrightarrow & 0.\\ & & q_1q_2\cdots q_{n-1} & \mapsto & q_1\otimes q_2\cdots q_{n-1} & \mapsto & q_2\cdots q_{n-2}\otimes(q_{n-1}\wedge q_1) & & \end{array}$$

Proof. We can check this sequence is exact and thus on free Q generated by x and y. For a word w in x and y, let $\mathrm{sym}(w)$ denote the sum of all distinct permutations of w. Then, a basis for $\mathrm{Sym}_{n-1} Q$ is $\alpha_k = \mathrm{sym}(x^k y^{n-1-k})$ for $0 \leq k \leq n-1$. A basis for $Q \otimes \mathrm{Sym}_{n-2} Q$ is given by

$$\begin{aligned}
\beta_0 &= y \otimes \mathrm{sym}(y^{n-2}) \\
\beta_k &= x \otimes \mathrm{sym}(x^{k-1} y^{n-1-k}) + y \otimes \mathrm{sym}(x^k y^{n-2-k}) \text{ for } 1 \leq k \leq n-2 \\
\beta_{n-1} &= x \otimes \mathrm{sym}(x^{n-2}) \\
\gamma_\ell &= x \otimes \mathrm{sym}(x^\ell y^{n-2-\ell}) \text{ for } 0 \leq \ell \leq n-3.
\end{aligned}$$

We see that in the sequence of the proposition, $\alpha_i \mapsto \beta_i$ and the γ_ℓ map to a basis of $\mathrm{Sym}_{n-3} Q \otimes \wedge^2 Q$. □

Lemma 3.7.6. *Let R be an $\mathcal{O}_S$-algebra, I be an R-module, Q be a locally free rank 2 $\mathcal{O}_S$-module quotient of I, and ϕ be an isomorphism of $\mathcal{O}_S$-modules $\phi : \mathrm{Sym}_{n-2} Q \cong R/\mathcal{O}_S$. If*

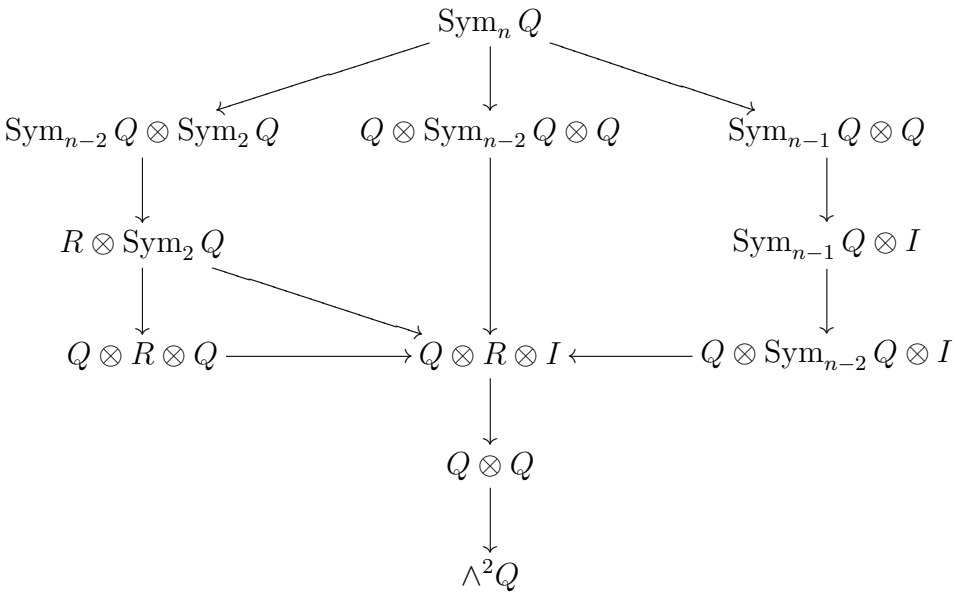
$$\begin{array}{ccc}
\mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q) & \longrightarrow & \wedge^2 Q \\
q_1 \cdots q_{n-1} \otimes k & \mapsto & q_1 \wedge \phi(q_2 \cdots q_{n-1}) \circ k
\end{array}$$

is the zero map, then

$$\begin{array}{ccc}
\mathrm{Sym}_n Q & \longrightarrow & \wedge^2 Q \\
q_1 \cdots q_n & \mapsto & q_1 \wedge \phi(q_2 \cdots q_{n-1}) \circ \tilde{q_n}
\end{array}$$

is well-defined. Here the $\circ$ denotes the action of R on I followed by the quotient to Q and $\tilde{q}$ denotes a fixed splitting $Q \to I$. In particular the map $\mathrm{Sym}_n Q \to \wedge^2 Q$ does not depend on the choice of this splitting.

Proof. Since $\mathrm{Sym}_{n-1} Q \subset Q \otimes \mathrm{Sym}_{n-2} Q$ as submodules of $Q^{\otimes n}$ (see Lemma 3.7.2), the first map $\mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q) \to \wedge^2 Q$ is well-defined. For a given choice of splittings $\mathrm{Sym}_{n-2} Q \to R$ and $Q \to I$, consider the following commutative diagram.



To investigate the effect of a different splitting $Q \to I$ on the map $\mathrm{Sym}_n Q \to \wedge^2 Q$, we take the route on the right hand side of the diagram. The difference between the composite maps from two different splittings will land in the submodule $\mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q)$ of the $\mathrm{Sym}_{n-1} Q \otimes I$ term, and thus be zero in the final map by the hypothesis of the lemma. In the diagram, let the maps $\mathrm{Sym}_{n-1} Q \otimes Q \to \mathrm{Sym}_{n-1} Q \otimes I$ given by the two different splittings be g_1 and g_2, and let f be the composite map $\mathrm{Sym}_{n-1} Q \otimes I \to \wedge^2 Q$. For $x \in \mathrm{Sym}_{n-1} Q \otimes Q$, we consider $f \circ g_1(x) - f \circ g_2(x) = f(g_1(x) - g_2(x))$. Since $g_1(x) - g_2(x) \in \mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q)$, we have $f(g_1(x) - g_2(x)) = 0$ by the hypothesis of the lemma, and therefore the composite map $\mathrm{Sym}_n Q \to \wedge^2 Q$ does not depend on the choice of splitting $Q \to I$.

To investigate the effect of a different splitting $\mathrm{Sym}_{n-2} Q \cong R/\mathcal{O}_S \to R$ on the map $\mathrm{Sym}_n Q \to \wedge^2 Q$, we take the route on the left hand side of the diagram. The difference between the maps from the different splittings will land in the submodule $\mathcal{O}_S \otimes \mathrm{Sym}_2 Q$ of the $R \otimes \mathrm{Sym}_2 Q$ term, and it is easy to see that the difference will be zero in the composite map. Let k_1 and k_2 be the maps $\mathrm{Sym}_{n-2} Q \otimes \mathrm{Sym}_2 Q \to R \otimes \mathrm{Sym}_2 Q$ given by two different splittings, and let h be the composite map $R \otimes \mathrm{Sym}_2 Q \to \wedge^2 Q$. For $x \in \mathrm{Sym}_{n-2} Q \otimes \mathrm{Sym}_2 Q$, we consider $h \circ k_1(x) - h \circ k_2(x) = h(k_1(x) - k_2(x))$. We have that $k_1(x) - k_2(x) \in \mathcal{O}_S \otimes \mathrm{Sym}_2 Q \subset R \otimes \mathrm{Sym}_2 Q$, and clearly $h(\mathcal{O}_S \otimes \mathrm{Sym}_2 Q) = 0$. Therefore, the composite map $\mathrm{Sym}_n Q \to \wedge^2 Q$ does not depend on the choice of splitting $\mathrm{Sym}_{n-2} Q \cong R/\mathcal{O}_S \to R$. $\square$

Chapter 4

Quartic rings associated to binary quartic forms

4.1 Introduction

Algebraic objects associated to binary forms have long been studied. Gauss associated a quadratic ring and ideal class to every binary quadratic form in what is called Gauss composition. He found that, in fact, binary quadratic forms exactly parametrize ideal classes of quadratic rings (see [25] for the original source, [16, Section 5.2], and [30] for more modern treatments, and Chapter 2 for an extremely modern point of view, which includes all binary quadratic forms, even the zero form!). In 1940, Delone and Faddeev associated cubic rings to binary cubic forms and found that binary cubic forms exactly parametrize cubic rings (see [21] for the original, and [24] for a modern point of view treating all binary cubic forms).

In fact, one can associate a rank n ring (a ring isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$ module) to a binary n-ic form for any n. These rings have been studied by Birch and Merriman [8] and Nakagawa [35]. In [18], Del Corso, Dvornicich, and Simon determine the splitting of the prime p in such a ring in terms of the factorization of the binary n-ic form modulo p^k. In [38], Simon associates an ideal class of the associated ring to a binary n-ic form, and in [37] this ideal class is applied to study integer solutions to equations of the form $Cy^d = F(x, z)$, where F is a binary form. In Chapter 3, it is determined exactly what algebraic structures are parametrized by binary n-ic forms, for all n. This structure is a rank n ring and an ideal class for that ring, such that the action of the ring on the ideal class satisfies a certain exact sequence (which comes naturally from geometry). When $n = 2$, the exact sequence condition is vacuous, and when $n = 3$ the condition forces the ideal class to be the unit ideal. In this chapter we give a different point of view (from Chapter 3) on the algebraic data parametrized by binary quartic forms. We prove the following main theorem.

Theorem 4.1.1. *There is a bijection between* $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes of binary quartic forms and isomorphism classes of pairs* (Q, C) *where* Q *is a quartic ring and* C *is a monogenic cubic resolvent of* Q *(where isomorphisms are required to preserve the generator of* C *modulo* $\mathbb{Z}$*).*

A binary quartic form is $f = f_0x^4 + f_1x^3y + f_2x^2y^2 + f_3xy^3 + f_4y^4$ with $f_i \in \mathbb{Z}$. We can represent a pair of ternary quadratic forms by a pair of matrices (A, B) such that

$$A = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \frac{a_{13}}{2} \\ \frac{a_{12}}{2} & a_{22} & \frac{a_{23}}{2} \\ \frac{a_{13}}{2} & \frac{a_{23}}{2} & a_{33} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & \frac{b_{12}}{2} & \frac{b_{13}}{2} \\ \frac{b_{12}}{2} & b_{22} & \frac{b_{23}}{2} \\ \frac{b_{13}}{2} & \frac{b_{23}}{2} & b_{33} \end{pmatrix}$$

with $a_{ij}, b_{ij} \in \mathbb{Z}$. We have a map

$$\Psi : \{\text{binary quartic forms}\} \longleftrightarrow \{\text{pairs of ternary quadratic forms}\}.$$

which sends $f = f_0x^4 + f_1x^3y + f_2x^2y^2 + f_3xy^3 + f_4y^4$ to (A_0, B_f), where

$$A_0 = \begin{pmatrix} 0 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad B_f = \begin{pmatrix} f_4 & 0 & \frac{f_3}{2} \\ 0 & f_0 & \frac{f_1}{2} \\ \frac{f_3}{2} & \frac{f_1}{2} & f_2 \end{pmatrix}$$

One then naturally puts an equivalence on pairs of ternary quadratic forms such that $(A, B) \sim (A, B + nA)$ for $n \in \mathbb{Z}$, and we can also consider

$$\bar{\Psi} : \{\text{binary quartic forms}\} \longrightarrow \{\text{binary quartic forms}\} / \sim .$$

which sends f to $(A_0, B_f + \mathbb{Z}A_0)$. Note that $\bar{\Psi}$ is injective and its image is all classes of pairs (A_0, B).

From the theory of binary n-ic forms, we know that the form f gives a based quartic ring R_f over $\mathbb{Z}$. From Bhargava's parametrization of quartic rings [6], we know that a pair of ternary quadratic forms gives a based quartic ring Q and a based cubic resolvent C for that quartic ring. The map Ψ (and also $\bar{\Psi}$) has been constructed so as to respect these constructions of based quartic rings.

Lemma 4.1.2. *If a based quartic ring Q is associated to the pair $\Psi(f) = (A_0, B_f)$ or any element of the class $\bar{\Psi}(f) = (A_0, B_f + \mathbb{Z}A_0)$, then $R_f = Q$.*

Note that when we have based rings, it makes sense to talk about equality and not just isomorphism. All of the elements in the class $(A_0, B_f + \mathbb{Z}A_0)$ give the same based quartic ring and the same cubic resolvent, but with different bases for the cubic resolvent. Lemma 4.1.2 will be proven in Section 4.7.1. The question remaining is which quartic rings are associated to binary quartic forms. In Chapter 3, we saw that one could understand the answer in terms of the existence of a certain kind of ideal for the quartic ring. In this chapter, we will give another point of view in terms of cubic resolvents. We will see in Section 4.5, when we give the geometric perspective on these results, that the two points of views are connected.

The based cubic resolvent associated to a pair (A, B) is given by the binary cubic form $4\,\mathrm{Det}(Ax - By)$. Since $4\det(A_0) = -1$, any element of $\bar{\Psi}(f)$ has a based cubic ring given by a cubic form with coefficient -1 of x^3. In particular if the cubic ring C has normalized basis $1, \omega, \theta$, we have that $\omega^2 = -c + b\omega + \theta$ with $b, c \in \mathbb{Z}$, and thus $1, \omega, \omega^2$ is a (not necessarily normalized) $\mathbb{Z}$-module basis of C. We call a ring *monogenic* if it is generated by one element as a $\mathbb{Z}$-algebra. A *monogenized cubic ring*

is a cubic ring C and an element $\omega \in C/\mathbb{Z}$ such that $C = \mathbb{Z}[\omega]$. (Note this condition does not depend on the lift of ω to C.) An isomorphism of monogenized cubic rings must preserve the element of $C/\mathbb{Z}$. A *monogenized based cubic ring* is a based cubic ring C with basis $1, \omega, \theta$, such that $1, \omega, \omega^2$ is a (not necessarily normalized) $\mathbb{Z}$-module basis for the ring *of the same orientation as* $1, \omega, \theta$, or equivalently that corresponds to a binary cubic form with x^3 coefficient -1.

Proposition 4.1.3. *Any element of $\bar{\Psi}(f)$ corresponds to a quartic ring with a monogenized based cubic resolvent.*

Corollary 4.1.4. *Any ring R_f from a binary quartic form has a monogenic cubic resolvent.*

Most surprisingly, we will see that the converse is true.

Theorem 4.1.5. *If a quartic ring Q has a monogenic resolvent R, then there exist normalized bases of Q and R such that the based pair (Q, R) corresponds to (A_0, B) in the parametrization of quartic rings.*

Proof. Recall that $g \in \mathrm{SL}_3(\mathbb{Z})$ acts on A by sending it to gAg^t. We prove in Lemma 4.7.1 that there is only one $\mathrm{SL}_3(\mathbb{Z})$ class of ternary quadratic forms with determinant $-1/4$. Then we can conclude that all such forms are in the $\mathrm{SL}_3(\mathbb{Z})$ class of A_0. If we have a pair (A, B) corresponding to a quartic ring Q with a monogenic cubic resolvent C, we can choose a monogenized basis of C (perhaps changing the basis of Q to preserve the isomorphism of orientations) so that we can assume $\mathrm{Det}(A) = -1/4$. Then we can act by an element $g \in \mathrm{SL}_3(\mathbb{Z})$ so that we obtain $A = A_0$. □

Corollary 4.1.6. *All quartic rings with monogenic resolvents are the ring R_f constructed from some binary quartic form f.*

In Section 4.2 we see how the $\mathrm{GL}_2(\mathbb{Z})$ action on binary quartic forms interacts with the construction Ψ. This will allow us to prove Theorem 4.1.1 in Section 4.4, after recording some preliminaries about monogenized cubic rings in Section 4.3. In Section 4.5, we explain the results of this chapter from a geometric point of view. In Section 4.6, we see how the $\mathrm{GL}_2(\mathbb{Z})$ invariants of a binary quartic form are related to the monogenized cubic resolvent ring of the associated quartic ring.

4.2 GL action on forms

There is a natural (left) $\mathrm{GL}_2(\mathbb{Z})$ action on binary quartic forms. Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\mathrm{GL}_2(\mathbb{Z})$ and $f = F(x, y)$ be a binary quartic form. Then $g \circ f = F(ax + cy, bx + dy)$. Note that this action has a kernel of ± 1.

There is also the natural (left) $\mathrm{SL}_3(\mathbb{Z})$ action on pairs of ternary quadratic forms, given by $(A, B) \mapsto (gAg^t, gBg^t)$.

Theorem 4.2.1. *The map*

$$\begin{array}{ccc} \rho : \mathrm{GL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SL}_3(\mathbb{Z}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \frac{1}{ad-bc}\begin{pmatrix} d^2 & c^2 & dc \\ b^2 & a^2 & ab \\ 2bd & 2ac & ad+bc \end{pmatrix} \end{array}$$

is a homomorphism, and gives gives a $\mathrm{GL}_2(\mathbb{Z})$ *action on pairs of ternary quadratic forms for which* $\bar{\Psi}$ *is equivariant. We have* $\mathrm{im}(\rho) \subset \mathrm{Stab}(A_0)$.

Proof. It is easy to compute that ρ is a homomorphism, and it can also can be realized as the representation of $\mathrm{GL}_2(\mathbb{Z})$ on binary quadratic forms (up to a twist by the determinant). We can check the equivariance of $\bar{\Psi}$ by computation (which simplifies on generators $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of $\mathrm{GL}_2(\mathbb{Z})$). Let

$$Y = \begin{pmatrix} d^2 & c^2 & dc \\ b^2 & a^2 & ab \\ 2bd & 2ac & ad+bc \end{pmatrix},$$

and $Y' = \frac{1}{ad-bc}Y$. We can compute formally that $Y'A_0(Y')^t = A_0$. We can also compute formally that Y gives the right action on $B + A_0\mathbb{Z}$ exactly; if $\Psi(f) = (A_0, B)$ and $\Phi(g \circ f) = (A_0, B')$, then $Y(B + A_0\mathbb{Z})Y^t = B' + A_0\mathbb{Z}$. Since $ad - bc = \pm 1$, we have that $Y(B + A_0\mathbb{Z})Y^t = Y'(B + A_0\mathbb{Z})(Y')^t$. □

The following Lemma, proven in Section 4.7.3, will be crucial to our main theorem.

Lemma 4.2.2. *We have* $\mathrm{im}(\rho) = \mathrm{Stab}(A_0)$.

4.3 Monogenized cubic rings

Recall that binary cubic forms are in bijection with normalized based cubic rings [24]. (A normalized basis $1, \omega, \theta$ of a cubic ring is a $\mathbb{Z}$-module basis such that $\omega\theta \in \mathbb{Z}$. The bijection between binary cubic forms and normalized based cubic rings is equivariant under a $\mathrm{GL}_2(\mathbb{Z})$ action that we specify here. Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\mathrm{GL}_2(\mathbb{Z})$ and $f = F(x, y)$ be a binary cubic form. Then $g \circ f = \frac{1}{ad-bc}F(ax + cy, bx + dy)$. If ω, θ is a basis of $C/\mathbb{Z}$, then after action by g, the new basis of $C/\mathbb{Z}$ is ω', θ', where $\left[\begin{smallmatrix} \omega' \\ \theta' \end{smallmatrix}\right] = g\left[\begin{smallmatrix} \omega \\ \theta \end{smallmatrix}\right]$.

We define N to be the subgroup $\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)$ of $\mathrm{GL}_2(\mathbb{Z})$. Note that N acts on binary cubic forms, and fixes the x^3 coefficients. Moreover, N acts on normalized based cubic rings and fixes their first basis element. We also have that N acts on pairs of ternary quadratic forms, and fixes the first form in the pair. (Recall the action of $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ on a pair (A, B) of ternary quadratic forms takes (A, B) to $(aA + bB, cA + dB)$.)

Proposition 4.3.1. *We have that* N *classes of binary cubic forms with* x^3 *coefficient* -1 *are in bijection with monogenized cubic rings.*

Proof. We have that binary cubic forms with x^3 coefficient -1 are in bijection with normalized based cubic rings in which $1, \omega, \omega^2$ is a basis of the same orientation as the given basis $1, \omega, \theta$. When we pass to N classes of forms, the correspondence is to cubic rings with a choice of $\omega \in C/\mathbb{Z}$ and $\theta \in C/(\mathbb{Z} \oplus \omega\mathbb{Z})$ such that $1, \omega, \omega^2$ is a basis of the same orientation as $1, \omega, \theta$. However, given ω, the only such choice of $\theta \in C/(\mathbb{Z} \oplus \omega\mathbb{Z})$ is $\theta = \omega^2$. □

4.4 Main Theorem

In this section, we prove the main theorem of this chapter.

Theorem 4.1.1. *There is a bijection between* $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes of binary quartic forms and isomorphism classes of pairs* (Q, C) *where* Q *is a quartic ring and* C *is a monogenized cubic resolvent of* Q*.*

An isomorphism of a pair (Q, C) where C is monogenized, is just an isomorphism of the underlying pair of quartic ring and cubic resolvent such that the isomorphism between cubic rings preserves the chosen generator modulo $\mathbb{Z}$.

Proof. So far, we have established a bijection

$$\{\text{binary quartic forms}\} \longleftrightarrow \left\{\begin{matrix} N \text{ classes of pairs } (A_0, B) \text{ of ternary} \\ \text{quadratic forms} \end{matrix}\right\},$$

where A_0 is the fixed form defined in the Introduction, and B is any ternary quadratic form. From the parametrization of quartic rings [6], we know that N classes of pairs (A_0, B) of ternary quadratic forms are in bijection with (Q, C), where Q is a based quartic ring, C is an N class of based cubic resolvent rings, and the resolvent map is given by (A_0, B). Since $4\,\mathrm{Det}(A_0) = -1$, the N class of bases of C exactly corresponds to a monogenization of C. Thus we have a bijection

$$\{\text{binary quartic forms}\} \longleftrightarrow \left\{\begin{matrix} (Q, C), \text{ where } Q \text{ is a based quartic} \\ \text{ring, } C \text{ is a monogenized cubic re-} \\ \text{solvent ring, and the resolvent map} \\ \text{is given by } (A_0, B) \end{matrix}\right\}.$$

We know that in this map the $\mathrm{GL}_2(\mathbb{Z})$ action on binary quartic forms just corresponds to a $\mathrm{SL}_3(\mathbb{Z})$ change of basis of Q, and thus gives the same isomorphism class of (Q, C). Thus the map from $\mathrm{GL}_2(\mathbb{Z})$ classes of binary quartic forms to isomorphism classes of (Q, C) is well-defined. We know the map is surjective by Theorem 4.1.5. To show it is injective, suppose we have two pairs (Q, C) and (Q', C') of quartic rings with monogenized cubic resolvents. We can choose bases for the quartic rings so that the resolvent maps are given by $(A_0, B + A_0\mathbb{Z})$ and $(A_0, B' + A_0\mathbb{Z})$. If we have an isomorphism of the pairs (Q, C) and (Q', C'), it must come from an element $(g, h) \in \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ with $\det(g)\det(h) = 1$. Since g fixes ω and the orientation of the cubic ring (as both cubic forms have x^3 coefficient -1), it must be an element of N. Then $\det(h) = 1$, and we see that the isomorphism comes from an element

of $\mathrm{SL}_3(\mathbb{Z})$ that fixes A_0. By Lemma 4.2.2, such an element is in the image of the ρ of Theorem 4.2.1, and thus $(A_0, B + A_0\mathbb{Z})$ and $(A_0, B' + A_0\mathbb{Z})$ come from the same $\mathrm{GL}_2(\mathbb{Z})$ class of binary quartic forms. □

A quartic ring might have multiple cubic resolvents, only some of which are monogenic. In our bijection, the quartic ring appears once for each monogenized resolvent. If it has a cubic resolvent monogenic in two different ways then it will appear for each of those monogenizations of the cubic ring. Also, note that the binary quartic form $-x^3y + bx^2y^2 + cxy^3 + dy^4$ maps to (A_0, B) with determinant $-x^3 + bx^2y + cxy^2 + dy^3$. Thus every monogenized cubic ring appears as a resolvent of some quartic ring.

4.5 Geometric interpretation

We can give a geometric description of the main theorem, though it still relies on the same key lemmas. We have a map $\mathbb{P}^1_{\mathbb{Z}} \to \mathbb{P}^2_{\mathbb{Z}}$ given by the rational normal curve, or $[u : v] \mapsto [v^2 : u^2 : uv]$. Note that A_0 gives a quadratic form on $\mathbb{P}^2_{\mathbb{Z}}$, and the scheme cut out by this form is the rational normal curve specified above. If we have a pair (A, B) of ternary quadratic forms, they cut out a subscheme of $\mathbb{P}^2_{\mathbb{Z}}$. In nice cases, the ring of regular functions of this scheme is the quartic ring associated to the pair (and in general the quartic ring is given by a hypercohomology construction from the pair, see Chapter 6). When (A, B) is a sufficiently nice pair (e.g. the schemes cut out by each do not share a component over $\mathbb{Q}$), then it makes sense to talk about the $\mathbb{P}^1_{\mathbb{Z}}$ (pencil) of conics through A and B. The cubic resolvent ring associated to (A, B) is the cubic ring associated to the binary cubic form $4\,\mathrm{Det}(Ax - By)$. This is the form that cuts out the singular locus of the pencil of conics through A and B. So the cubic ring will be given by the regular functions on the subscheme of singular conics in the $\mathbb{P}^1_{\mathbb{Z}}$ of conics through A and B.

A conic given by a symmetric matrix A is singular in a fiber if and only if $4\,\mathrm{Det}(A)$ is 0 in that fiber. To form the matrix A from the conic, we must use $1/2$, but then $D = 4\,\mathrm{Det}(A)$ is a polynomial with integer coefficients in the coefficients of the form defining the conic. Even in characteristic 2, the polynomial D gives the exact condition for singularity. If we have a pair (A_0, B) (with B not a multiple of A_0), then the conic given by A_0 in the pencil is not singular in any fiber. Thus, the cubic ring is given by the ring of regular functions of a closed subscheme of $\mathbb{P}^1 \setminus \{A_0\} \cong \mathbb{A}^1$, and thus is monogenic.

Conversely, if the cubic resolvent ring associated to a nice (as above) pair (A, B) is monogenic, then that means that the subscheme of singular conics in the $\mathbb{P}^1_{\mathbb{Z}}$ of conics through A and B is disjoint from some particular conic defined over $\mathbb{Z}$, and we can change basis of the pencil so that it is disjoint from A. (We can see from the parametrization of cubic rings that whenever a cubic ring is monogenic, in its realization as the global functions of a subscheme of $\mathbb{P}^1_{\mathbb{Z}}$, that subscheme actually sits inside an $\mathbb{A}^1 \subset \mathbb{P}^1_{\mathbb{Z}}$.) This means that A is non-singular. From Lemma 4.7.1, we know that up to $\mathrm{GL}_3(\mathbb{Z})$ change of basis on $\mathbb{P}^2_{\mathbb{Z}}$, the only such conic is the one cut out by $\pm A_0$. So we see that pairs (A_0, B) correspond to pairs of quartic rings and cubic resolvents such that the resolvents are monogenic.

Moreover, if we have a pair (A_0, B), we can pull B back to a form on the $\mathbb{P}^1_{\mathbb{Z}}$ cut out by A_0 to obtain a binary quartic form (and we obtain the same binary quartic form with any element of $B + A_0\mathbb{Z}$). We can easily compute that every binary quartic form arises this way. In particular, if $B = b_{11}x^2 + b_{12}xy + b_{13}xz + b_{22}y^2 + b_{23}yz + b_{33}z^2$, we see it pulls back to the form $b_{11}v^4 + b_{12}u^2v^2 + b_{13}uv^3 + b_{22}u^4 + b_{23}u^3v + b_{33}u^2v^2$ (exactly inverse to the map Ψ defined in the introduction). The elements of $\mathrm{GL}_3(\mathbb{Z})$ that fix the $\mathbb{P}^1_{\mathbb{Z}}$ cut out by A_0 setwise restrict to elements of $\mathrm{GL}_2(\mathbb{Z})$ acting on that $\mathbb{P}^1_{\mathbb{Z}}$. This allows us to see the correspondence of the $\mathrm{GL}_2(\mathbb{Z})$ action on $\mathbb{P}^1_{\mathbb{Z}}$ and an action on $\mathbb{P}^2_{\mathbb{Z}}$ which fixes the rational normal curve.

If we have a primitive binary quartic form f, then the scheme S cut out by the form is Spec of the associated ring (Theorem 3.2.9). The ideal associated to the form gives a line bundle on this scheme, which is equivalent to the data of the map of S into $\mathbb{P}^1_{\mathbb{Z}}$. The scheme S is also a subscheme of $\mathbb{P}^2_{\mathbb{Z}}$ cut out by (A_0, B_f). We can see the relationship here between the ideal and the monogenic cubic resolvent. The ideal gives a map of S to $\mathbb{P}^1_{\mathbb{Z}}$, and then by composing with the rational normal curve map into $\mathbb{P}^2_{\mathbb{Z}}$ we see from the above story that the cubic resolvent is monogenic. Conversely, a monogenic cubic resolvent gives a smooth conic on which our degree four subscheme lies (as in the above story), and pulling back $\mathcal{O}(1)$ from this conic (which is isomorphic to $\mathbb{P}^1_{\mathbb{Z}}$) gives the ideal associated to the binary quartic form.

4.6 $\mathrm{GL}_2(\mathbb{Z})$ invariants of binary quartic forms and cubic resolvent rings

We have a canonical map Ψ' which sends $f = f_0x^4 + f_1x^3y + f_2x^2y^2 + f_3xy^3 + f_4y^4$ to

$$\left(A_0, \begin{pmatrix} f_4 & \frac{f_2}{6} & \frac{f_3}{2} \\ \frac{f_2}{6} & f_0 & \frac{f_1}{2} \\ \frac{f_3}{2} & \frac{f_1}{2} & \frac{2f_2}{3} \end{pmatrix}\right),$$

which is equivariant with respect the $\mathrm{GL}_2(\mathbb{Z})$ action on the binary quartic forms and the $\mathrm{GL}_2(\mathbb{Z})$ action on pairs of ternary quadratic forms given in Theorem 4.2.1. Our previous map Ψ was equivariant only as a map to N classes of pairs of ternary quadratic forms. However Ψ was defined over $\mathbb{Z}$, and Ψ' requires the use of $\frac{1}{3}$.

The determinant binary cubic of any element in the image of Ψ' has x^3y coefficient 0. If $3 \mid f_2$, then Ψ' has integral coefficients and its determinant is the unique binary cubic form to give a (normalized) basis $1, \omega, \theta$ such that $\omega^2 - \theta \in \mathbb{Z}$, where ω is the generator of the resolvent cubic associated to the form f. If $3 \nmid f_2$, then there is no (normalized) basis $1, \omega, \theta$ of the monogenized resolvent cubic C, ω such that $\omega^2 - \theta \in \mathbb{Z}$.

We define $N_{1/3}$ to be the group of matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$, where $n \in \frac{1}{3}\mathbb{Z}$.

Proposition 4.6.1. *The map from N classes of monogenic binary cubic forms to $N_{1/3}$ classes of binary cubic forms is injective.*

Proof. Consider the action of $\left(\begin{smallmatrix} 1 & \\ k/3 & 1 \end{smallmatrix}\right)$ (where $k \in \mathbb{Z}$) on the form $-x^3+bx^2y+cxy^2+dy^3$. The new coefficient of y^3 is $d - \frac{ck}{3} + \frac{bk^2}{9} - \frac{k^2}{27}$, which is only an integer if k is divisible by 3. □

The determinant of $\Psi'(f)$ is

$$-x^3 + \frac{I}{3}xy^2 - \frac{J}{27}y^3,$$

where I and J are generators for the $\mathrm{GL}_2(\mathbb{Z})$ invariants of binary quartic forms, given by

$$\frac{I}{3} = 4f_0f_4 - f_1f_3 + \frac{1}{3}f_2^2 \quad \text{and} \quad \frac{-J}{27} = \frac{-8}{3}f_0f_2f_4 + \frac{2}{27}f_2^3 + f_0f_3^2 + f_4f_1^2 - \frac{1}{3}f_1f_2f_3.$$

Given a binary quartic form, we have an associated quartic ring and a monogenized cubic resolvent C with generator ω. We can thus give the monogenized cubic resolvent canonically by saying it corresponds to the N class of binary cubic forms over $\mathbb{Z}$ in the $N_{1/3}$ class of $-x^3 + \frac{I}{3}xy^2 - \frac{J}{27}y^3$.

Let r be a root of $-x^3 + \frac{I}{3}x - \frac{J}{27}$. Then there is only one $\mathbb{Z}$ coset of algebraic integers in $r + \frac{1}{3}\mathbb{Z}$, and it is $\omega + \mathbb{Z}$. So, we have found a description for ω in terms of the $\mathrm{GL}_2(\mathbb{Z})$ invariants of the binary quartic form. (Note that even if $-x^3 + \frac{I}{3}x - \frac{J}{27}$ is reducible, we can still make sense of r as an element of $\mathbb{Q}(r)/(-r^3 + \frac{I}{3}r - \frac{J}{27})$ and there is only one $\mathbb{Z}$ coset in $r + \frac{1}{3}\mathbb{Z}$ whose elements generate algebras that are finitely generated $\mathbb{Z}$-modules.)

4.7 Proofs of key Lemmas

4.7.1 Proof of Lemma 4.1.2

Lemma 4.1.2. *If a based quartic ring Q is associated to the pair $\Psi(f) = (A_0, B_f)$ or any element of the class $\bar{\Psi}(f) = (A_0, B_f + \mathbb{Z}A_0)$, then $R_f = Q$.*

Proof. We have a basis $\zeta_1, \zeta_2, \zeta_3$ of the quartic ring associated to a binary quartic form as given in Chapter 3. We let $\zeta_3' = \zeta_3 + f_3$. From Equation (3.2), we have that

$$\begin{aligned}
\zeta_1^2 &= -f_1\zeta_1 + f_0\zeta_2 \\
\zeta_1\zeta_2 &= -f_2\zeta_1 + f_0\zeta_3' - f_0f_3 \\
\zeta_1\zeta_3' &= -f_0f_4 \\
\zeta_2\zeta_2 &= -f_3\zeta_1 - f_2\zeta_2 + f_1\zeta_3' - f_1f_3 - f_0f_4 \\
\zeta_2\zeta_3' &= -f_4\zeta_1 - f_1f_4 \\
(\zeta_3')^2 &= -f_4\zeta_2 + f_3\zeta_3' - f_3^2 - f_2f_4 \qquad .
\end{aligned}$$

We let $\alpha_1 = \zeta_3'$ and $\alpha_2 = \zeta_1$ and $\alpha_3 = \zeta_2$. We then see that the α_i satisfy the multiplication table given in [6, Equations (21) and (23)] for the pair (A_0, B_f). □

4.7.2 Proof of Lemma 4.7.1

Lemma 4.7.1. *There is only one* $\mathrm{SL}_3(\mathbb{Z})$ *class of ternary quadratic form such that* $\mathrm{Det}(A) = -1/4$.

Proof. Let

$$A = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \frac{a_{13}}{2} \\ \frac{a_{12}}{2} & a_{22} & \frac{a_{23}}{2} \\ \frac{a_{13}}{2} & \frac{a_{23}}{2} & a_{33} \end{pmatrix}$$

represent a ternary quadratic form, and assume $\mathrm{Det}(A) = -1/4$. We will now act on A by elements of $\mathrm{SL}_3(\mathbb{Z})$, and abuse notation by calling the resulting form A. As in [9, Section 5], we can find an $S \in \mathrm{SL}_3(\mathbb{Z})$ such that $S^t AS$ is semi-reduced, which in particular means that $|a_{11}| \leq \frac{4}{3}|\det A|^{1/3} < 1$ and $|a_{11}a_{22} - a_{12}^2/4| \leq \sqrt{4|a_{11}\,\mathrm{Det}(A)|}/3$. So, $a_{11} = 0$ and $a_{12} = 0$. Thus $-a_{13}^2 a_{22}/4 = -1/4$. Thus $a_{22} = 1$ and $a_{13} = \pm 1$. We can exchange the second and third rows and columns to obtain $a_{33} = 1$ and $a_{12} = \pm 1$, but that transformation has determinant -1 so we can then multiply the first row and column by $-(\pm 1)$ and the third row and column by ± 1 to obtain $a_{33} = 1$ and $a_{12} = -1$. We also have $a_{11} = 0$ and $a_{13} = 0$. If we let

$$J = \begin{pmatrix} 1 & a_{22} & a_{23} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

then $J^t AJ = A_0$. □

4.7.3 Proof of Lemma 4.2.2

Recall the map $\rho : \mathrm{GL}_2(\mathbb{Z}) \to \mathrm{SL}_3(\mathbb{Z})$ defined in Theorem 4.2.1.

Lemma 4.2.2. *We have* $\mathrm{im}(\rho) = \mathrm{Stab}(A_0)$.

Lemma 4.2.2 is like the classical fact that over an algebraically closed field, the elements of PGL_3 that fix the rational normal curve setwise are exactly a PGL_2 acting on the curve. However, for our application we need a precise statement over $\mathbb{Z}$ and in the nonprojectivized version.

Proof. Let

$$X = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} \in \mathrm{SL}_3(\mathbb{Z})$$

such that $XA_0X^t = A_0$. We obtain the following system of equations of the x_{ij}

$$\begin{aligned}
x_{13}^2 - x_{11}x_{12} &= 0 \\
x_{23}^2 - x_{11}x_{12} &= 0 \\
-\frac{x_{12}x_{21}}{2} - \frac{x_{11}x_{22}}{2} + x_{13}x_{23} &= -\frac{1}{2} \\
-\frac{x_{12}x_{31}}{2} - \frac{x_{11}x_{32}}{2} + x_{13}x_{33} &= 0 \\
-\frac{x_{22}x_{31}}{2} - \frac{x_{21}x_{32}}{2} + x_{23}x_{33} &= 0 \\
-x_{32}x_{31} + x_{33}^2 &= 1
\end{aligned}$$

Let u_1 be a square root of x_{11}, and $u_2 = x_{13}/u_1$ (which is a square root of x_{12}). Let u_3 be a square root of x_{21}, and $u_4 = x_{23}/u_3$ (which is a square root of x_{22}). We can then rearrange

$$-\frac{x_{12}x_{21}}{2} - \frac{x_{11}x_{22}}{2} + x_{13}x_{23} = -\frac{1}{2}$$

to

$$-u_2^2u_3^2 - u_1^2u_4^2 + 2u_1u_2u_3u_4 = -1$$

or

$$(u_2u_3 - u_1u_4)^2 = 1.$$

Given u_1, u_2, u_3, u_4, we have a system of two linear equations in the variables x_{31}, x_{32}, and x_{33}:

$$\begin{aligned}
-u_2^2x_{31} - u_1^2x_{32} + 2u_1u_2x_{33} &= 0 \\
-u_4^2x_{31} - u_3^2x_{32} + 2u_3u_4x_{33} &= 0
\end{aligned}$$

First, we will see that the above system cannot be rank 1. That would imply that $u_1u_2u_3^2 = u_1^2u_3u_4$ and thus unless $u_1 = 0$ or $u_3 = 0$, we have $u_2u_3 = u_1u_4$ which is impossible since $(u_2u_3 - u_1u_4)^2 = 1$. If $u_1 = 0$, we cannot have $u_2 = 0$ or $u_3 = 0$ since $(u_2u_3 - u_1u_4)^2 = 1$, and for the system to be rank 1, we would have $u_2^2u_3^2 = u_1^2u_4^2 = 0$, which is impossible. If $u_3 = 0$, we cannot have $u_1 = 0$ or $u_4 = 0$ since $(u_2u_3 - u_1u_4)^2 = 1$, and for the system to be rank 1, we would have $u_1^2u_4^2 = u_2^2u_3^2 = 0$, which is impossible.

Since the system is rank 2, there is one dimension of solutions in $\mathbb{C}^3$. We see that $[x_{31}, x_{32}, x_{33}] = [2u_1u_3, 2u_2u_4, u_1u_4 + u_2u_3]$ is a solution, and thus as long as it isn't the zero vector, all solutions are scalar multiples of this solution. If $[2u_1u_3, 2u_2u_4, u_1u_4 + u_2u_3]$ is zero, without loss of generality say $u_1 = 0$. That implies $u_2u_3 = 0$, which contradicts $(u_2u_3 - u_1u_4)^2 = 1$.

So we have $[x_{31}, x_{32}, x_{33}] = k[2u_1u_3, 2u_2u_4, u_1u_4 + u_2u_3]$. We can compute that the determinant of X is $k(u_1u_4 - u_2u_3)^3$. Thus if X has determinant 1, then

$k = u_1u_4 - u_2u_3$ (and $k^2 = 1$). We note that the final equation $-x_{32}x_{31} + x_{33}^2 = 1$ is always satisfied with the x_{ij} we have determined. So we have

$$X = \begin{pmatrix} u_1^2 & u_2^2 & u_1u_2 \\ u_3^2 & u_4^2 & u_3u_3 \\ 2(u_1u_4 - u_2u_3)u_1u_3 & 2(u_1u_4 - u_2u_3)u_2u_4 & (u_1u_4 - u_2u_3)(u_1u_4 + u_2u_3) \end{pmatrix}.$$

We now wish to show that the u_i are integral. Now, assume that X is not in the image of $\mathrm{GL}_2(\mathbb{Z})$ under ρ. Since $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ maps to

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

we can assume that x_{11} is non-negative and that x_{21} is non-negative. We see that the u_i are all algebraic integers; more precisely they are the square roots of integers. If $u_1 = 0$ (respectively, $u_4 = 0$), then u_2 and u_3 must be non-zero and $u_2u_3 = \pm 1$. Since u_3^2 is non-negative, we have that u_2 and u_3 are both integers. Since u_2u_4 (respectively, u_1u_3) is rational, this implies u_4 (respectively, u_1) is rational and thus an integer.

If $u_2 = 0$ (respectively, $u_3 = 0$), then u_1 and u_4 must be non-zero and $u_1u_4 = \pm 1$. Since u_1^2 is non-negative, we have that u_1 and u_4 are both integers. Since u_1u_3 (respectively, u_2u_4) is rational, this implies u_3 (respectively, u_2) is rational and thus an integer.

It remains to consider the case when all of the u_i are non-zero. Since u_1u_2, u_3u_4, u_1u_3, and u_2u_4 are all rational, we have that $Q(u_i)$ is the same for all i, say $Q(\sqrt{d})$ where d is a square free positive integer. Now the u_i are all square roots of integers, and thus $u_i = n_i\sqrt{d}$, where n_i is an integer. However, that implies that $(u_1u_4 - u_2u_3)$ is divisible by d. Thus $d = 1$, and all of the u_i are integral, and we see that X is in the image of $\mathrm{GL}_2(\mathbb{Z})$. (If $u_1u_4 - u_2u_3 = 1$, take $a = u_1$ and $b = -u_2$, and $c = -u_3$, and $d = u_4$. If $u_1u_4 - u_2u_3 = -1$, take $a = u_1$ and $b = -u_2$, and $c = u_3$, and $d = -u_4$.) $\square$

Chapter 5

Parametrization of ideal classes in rings associated to binary forms

5.1 Introduction

The goal of this chapter is to find a moduli space for ideal classes in the rings associated to binary n-ic forms. Every binary form of degree n has a ring of rank n (a ring isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$-module) associated to it ([35], [39], Chapter 3). For $n = 2$, the associated ring to a binary quadratic form is just the quadratic ring of the same discriminant used in Gauss composition, the parametrization of ideal classes of quadratic rings by binary quadratic forms. For $n = 3$, binary cubic forms parametrize cubic rings exactly ([21], [24]). See Chapters 3 and 4 for results on which rank n rings are associated to binary n-ic forms.

When $n = 2$, ideal classes of quadratic rings are parametrized by binary quadratic forms themselves. Bhargava [5] has found a moduli space for ideal classes of cubic rings. This is his space of 2 by 3 by 3 boxes, or classes of elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$. In this chapter, we find that classes of elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ parametrize ideal classes of the rings associated to binary n-ic forms for all n. When $n = 2, 3$, these are the results of Bhargava in [4], [5]. One can also study symmetric elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$, that is elements of $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$. These are related to the 2-part of the class group of rings associated to binary n-ic forms, just as in the cases $n = 2, 3$ in [4], [5]. Morales ([34], [33]) has also studied elements of $\mathbb{Z}^2 \otimes \mathrm{Sym}_2 \mathbb{Z}^n$ and associated modules to them, though he associates modules for a slightly different ring than in our work.

In addition, this chapter gives analogous results when the integers are replaced by an arbitrary base scheme S (or base ring when $S = \mathrm{Spec}\, R$), and so we generalize the results from [4] and [5] from the integers to an arbitrary base. Morales [34] replaces $\mathbb{Z}$ by an arbitrary maximal order in a number field in his constructions of modules from symmetric tensors. In this chapter, we give both algebraic and geometric constructions for the modules associated to an element of $\mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$.

5.1.1 Outline of results

We can represent an element of the space $\mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ as a pair $A = (A_1, A_2)$ of n by n matrices. Let f_A be the binary n-ic form $\mathrm{Det}(A_1 x + A_2 y)$. For a form f, let R_f be the ring associated to f as in Chapter 3. Let Γ be the subgroup of elements (g_1, g_2) of $\mathrm{GL}_n(\mathbb{Z}) \times \mathrm{GL}_n(\mathbb{Z})$ such that $\mathrm{Det}(g_1)\,\mathrm{Det}(g_2) = 1$. Over the integers, in the nicest cases, we have the following theorem.

Theorem 5.1.1. *For a primitive non-degenerate binary n-ic form f, there is a bijection between Γ classes $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ such that $f_A = f$ and (not necessarily invertible) ideal classes of R_f.*

If $f = F(x_1, x_2)$ is monic, then $R_f = \mathbb{Z}[\theta]/F(\theta, 1)$, and this generalizes the classical result that ideal classes of monogenic rings correspond to conjugacy classes in $\mathbb{Z}^n \otimes \mathbb{Z}^n$ whose characteristic polynomial is $F(t, -1)$. If f is monic, that implies that $\mathrm{Det}(A_1) = 1$. We can then act by an element of Γ so as to assume that A_1 is the identity matrix. Further Γ action fixing A_1 (the identity matrix) is just conjugation of A_2. So, we can view Theorem 5.1.1 as placing rings associated to binary forms in analogy with monogenic rings, as in [18] and [39].

In the case $n = 3$, Theorem 5.1.1 is slightly stronger than the corresponding version in [6], which gives a correspondence between A associated to invertible ideals and invertible ideal classes of R_f. As in [4, 5], we must define a notion of balanced to state a theorem that works over all forms. There are several equivalent ways to formulate the notion of balanced. For a non-zero form f, there is a naturally associated ideal class I_f of R_f, and a natural map $I_f \to \mathbb{Z}^2$. A *balanced pair of modules* for a non-zero form f is a pair of R_f-modules M and N, each a free rank n $\mathbb{Z}$-module, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathbb{Z}} N \to M \otimes_{R_f} N \to I_f \to V$ is written as a pair of matrices A_1 and A_2, we have $\det(A_1 x_1 + A_2 x_2) = \pm f$. Corollary 5.5.3 shows that when f is non-zero, every finitely generated invertible module (or invertible fractional ideal) has a balancing partner, and it is unique. In [6], Bhargava asks for an appropriate formula of balanced for degenerate forms so as to obtain a theorem such as the below. Our definition works for degenerate forms except for the zero form.

Theorem 5.1.2. *For every non-zero binary n-ic form f with coefficients in $\mathbb{Z}$, there is a bijection*

$$\left\{\begin{matrix}\textit{isomorphism classes of balanced}\\ \textit{pairs } (M,N) \textit{ of modules for } f\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\Gamma \textit{ classes of } A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n \textit{ with}\\ \det(A) = f\end{matrix}\right\}.$$

In order to prove Theorem 5.1.1 from Theorem 5.1.2, we prove that for non-degenerate f, all modules appearing in balanced pairs are realizable as fractional ideals (Propositions 5.5.1 and 5.5.4), and that for primitive and non-degenerate f, every fractional ideal has a unique balancing partner (Proposition 5.5.8). Theorem 5.1.2 is proven in Section 5.3.

We can also prove results for symmetric elements of $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$. For nice forms f we get the following, which follows from Theorems 5.4.1 and 5.5.9.

Theorem 5.1.3. *For every primitive non-degenerate binary n-ic form f with coefficients in $\mathbb{Z}$, there is a bijection*

$$\left\{\begin{array}{l}\text{classes of } (M,k) \text{ where } M \text{ is a}\\ \text{fractional } R_f\text{-ideal, } k \text{ is an invert-}\\ \text{ible element of } R_f \otimes_{\mathbb{Z}} \mathbb{Q}, \text{ and } M =\\ (I_f k : M)\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\mathrm{GL}_n(\mathbb{Z}) \text{ classes of } A \in \mathbb{Z}^2 \otimes\\ \mathrm{Sym}_2 \mathbb{Z}^n \text{ with } \det(A) = f\end{array}\right\},$$

where $\mathrm{Sym}_2 \mathbb{Z}^n$ *are symmetric n by n matrices, the action of $g \in \mathrm{GL}_n(\mathbb{Z})$ is by multiplication on the left by g and the right by g^t, and (M,k) and (M_1,k_1) are in the same class if $M_1 = \lambda M$ and $k_1 = \lambda^2 k$ for some invertible element $\lambda \in R_f \otimes_{\mathbb{Z}} \mathbb{Q}$, and $(I_f k : M)$ is the fractional ideal of elements x such that $xM \subset I_f k$.*

We give a version of the above in Theorem 5.4.1 for all non-zero forms f, which again uses the notion of balanced. If we restrict Theorem 5.1.3 to invertible modules M, then the condition $M = (I_f k : M)$ is replaced by $M^2 = I_f k$, and the restricted set is an extension of a torsor of the 2-part of the class group of R_f by R_f^*/R_f^2. (We say a torsor instead of a principal homogeneous space because I_f might not be a square in the class group and there would be no such M in that case.)

We have analogous results over an arbitrary base scheme S. We consider V, U, W, locally free $\mathcal{O}_S$-modules of ranks 2, n, and n, respectively. We then study global sections $p \in V \otimes U \otimes W$. We can construct $\det(p) \in \mathrm{Sym}^n V \otimes \wedge^n U \otimes \wedge^n W$, which is a binary n-ic form. Fix any f in $\mathrm{Sym}^n V \otimes L$, where L is a locally free rank 1 $\mathcal{O}_S$-module. A *balanced pair of modules* for a non-zero divisor f is a pair of R_f-modules M and N, each a locally free rank n $\mathcal{O}_S$-module such that $\wedge^n M \otimes \wedge^n N \cong L^*$, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathcal{O}_S} N \to M \otimes_{R_f} N \to I_f \to V$ is written as $A \in M^* \otimes N^* \otimes V$ we have $\det(A) = fu$, where u is a unit in $\mathcal{O}_S$. We have the following, proven in Theorem 5.6.2.

Theorem 5.1.4. *For every non-zero divisor binary n-ic form $f \in \mathrm{Sym}^n V \otimes L$, there is a bijection*

$$\left\{\begin{array}{l}\text{isomorphism classes of balanced}\\ \text{pairs } (M,N) \text{ of modules for } f\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{isomorphism classes of } A \in V \otimes\\ U \otimes W, \text{ where } U \text{ and } W \text{ are lo-}\\ \text{cally free rank } n \ \mathcal{O}_S\text{-modules with}\\ \text{an isomorphism } \wedge^n U \otimes \wedge^n W \cong L\\ \text{such that } \det(A) = f\end{array}\right\}.$$

From a $p \in V \otimes U \otimes W$ we give two constructions of the corresponding ideal classes or modules. The first construction (in Section 5.6) is algebraic and concrete and the second (in Section 5.8) is geometric and more intuitive. We give a heuristic description of the geometric construction here. If we have locally free $\mathcal{O}_S$-modules F and G, and $s \in F \otimes G$, then we can construct the k-minor $\wedge^k s \in \wedge^k F \otimes \wedge^k G$. If H is also a locally free $\mathcal{O}_S$-module, and we have $s \in F \otimes G \otimes H$, then we have a k-minor $\wedge^k_H s$ with H-coefficients in $\wedge^k F \otimes \wedge^k G \otimes \mathrm{Sym}^k H$. For $p \in V \otimes U \otimes W$, the n minor with coefficients in V defines a subscheme $T_p(V)$ in $\mathbb{P}(V)$, the 2 minor with coefficients in U defines a subscheme $T_p(U)$ in $\mathbb{P}(U)$, and the 2 minor with coefficients

in W defines a subscheme $T_p(W)$ in $\mathbb{P}(W)$. Abusing notation, we let π denote the map from all of these schemes to S. The *heuristic* definition of R_f is to take $\pi_*\mathcal{O}_{T_p(V)}$ (or $\pi_*\mathcal{O}_{T_p(U)}$ or $\pi_*\mathcal{O}_{T_p(W)}$–all the rings turns out to be the same), and $M = \pi_*\mathcal{O}_{T_p(U)}(1)$ and $N = \pi_*\mathcal{O}_{T_p(W)}(1)$ (where $\mathcal{O}(1)$ is as pulled back from the corresponding projective bundle). This construction does not work for all p (for example, it doesn't work for $p = 0$) and it is not functorial in S. As in the case of binary n-ic forms, we must use hypercohomology to make a construction that works in all cases and is functorial.

5.1.2 Outline of the chapter

In Section 5.2 we review the rings and ideals associated to binary n-ic forms. In Section 5.3, we prove Theorem 5.1.2. We first give the algebraic constructions of the modules from an element of $\mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ in Section 5.3.1. In Section 5.3.2 we prove Theorem 5.1.2 when the leading coefficient of f is not zero. In Section 5.3.3, we study the $\mathrm{GL}_2(\mathbb{Z})$ invariance of our construction of modules, and use this to finish the proof of Theorem 5.1.2. In Section 5.4 we give the general analogs of Theorem 5.1.2 for symmetric tensors.

In Section 5.5, we further study the notion of balanced pairs of modules, and show it is equivalent to a characteristic polynomial condition and an index condition (Proposition 5.5.1). In Section 5.5.1, we show that for non-degenerate binary n-ic forms all balanceable modules are fractional ideals (Proposition 5.5.4), and prove that in this case our definition of balanced is equivalent to a norm condition on fractional ideals (Theorem 5.5.5). This condition generalizes the definition of a balanced pair of fractional ideals in the cases $n = 2, 3$ in [4] and [5]. In Section 5.5.2, we specialize to the case of primitive non-degenerate forms, where we see that every fractional ideal has a unique balancing partner. This is the final step in the proof of Theorem 5.1.1. We can work similarly for symmetric tensors, and we find that Theorem 5.1.3 follows from Theorem 5.4.1 for general non-zero forms, and Theorem 5.5.9, which finds an equivalent condition for balanced in the primitive case.

In Section 5.6, we prove versions of these main theorems over an arbitrary base. In particular, we prove Theorem 5.1.4 (as Theorem 5.6.2) and a symmetric version. In Section 5.7, we give a geometric construction of the modules from the universal form and prove it is the same as the algebraic construction in Section 5.3.1. The main obstacle is that we give multiple ring constructions and we must show that they agree. The rings are given by global sections of different schemes, but the schemes themselves are not isomorphic. Finally, in Section 5.8, we give a geometric construction over arbitrary base of the modules from a triple tensor and prove that it commutes with base change (Corollary 5.8.3).

5.2 Binary forms, rings, and ideals

Given a binary n-ic form $f_0x_1^n + f_1x_1^{n-1}x_2 + \cdots + f_nx_2^n$ with $f_i \in \mathbb{Z}$, in Chapter 3 we have defined a rank n ring R_f and a sequence of R_f-modules. Here we review the facts about R_f and these modules that are necessary in this chapter, as well as make

some computations that will be critical in this work. We will eventually need these results over more general rings than $\mathbb{Z}$, so we will now work over an arbitrary ring B in place of $\mathbb{Z}$.

Let $f = f_0x_1^n + f_1x_1^{n-1}x_2 + \cdots + f_nx_2^n$ a binary n-ic form with coefficients $f_i \in B$ such that f_0 is not a zero divisor in B. We first give geometric constructions of a ring and ideals from f, as given in Chapter 3. We define R_f as the B-algebra of global sections of the regular functions of T_f, the subscheme of $\mathbb{P}^1_B$ defined by f. We have line bundles $\mathcal{O}_{T_f}(k)$ on T_f pulled back from $\mathcal{O}(k)$ on $\mathbb{P}^1_B$. We define I_f to be $\Gamma(\mathcal{O}_{T_f}(n-3))$ (i.e. the global sections of $\mathcal{O}_{T_f}(n-3)$), and J_f to be $\Gamma(\mathcal{O}_{T_f}(n-2))$. This gives I_f and J_f the structure of R_f-modules. Note that our I_f is the I_f^{n-3} or $\mathcal{I}_{f_{n-3}}$ of Chapter 3, and our J_f is the I_f^{n-2} or $\mathcal{I}_{f_{n-2}}$ of Chapter 3.

Equivalent, but more concrete, constructions of R_f, I_f, and J_f are also given in Chapter 3, and we give those now, as they will be easier to work with. Write $f = F(x,y)$. Let $B' = B_{f_0}$ (the ring B with f_0 inverted). We can also define the B-algebra R_f as the subring of $B'[\theta]/F(\theta,1)$ generated by $\zeta_0, \ldots, \zeta_{n-1}$ with

$$\zeta_0 = 1, \text{ and } \zeta_k = f_0\theta^k + \cdots + f_{k-1}\theta \text{ for } k > 1.$$

The ζ_k give a B-module basis of R_f, and it is shown in Chapter 3 that this definition of R_f agrees with the geometric one give above, and in particular that the B-module generated by the ζ_i is closed under multiplication. Note that if f_0 is a unit in B, then $R_f = B[\theta]/F(\theta,1)$. We can define I_f and J_f as sub-B-modules of $B'[\theta]/F(\theta,1)$, such that

$$\begin{aligned} I_f \text{ is the } B\text{-module generated by} \quad & 1, \theta, \theta^2, \ldots, \theta^{n-3}, \zeta_{n-2}, \zeta_{n-1} \text{ or} \\ \text{equiv. the } B\text{-module generated by} \quad & 1, \theta, \theta^2, \ldots, \theta^{n-3}, f_0\theta^{n-2}, f_0\theta^{n-1} + f_1\theta^{n-2} \\ J_f \text{ is the } B\text{-module generated by} \quad & 1, \theta, \theta^2, \ldots, \theta^{n-3}, \theta^{n-2}, \zeta_{n-1}. \end{aligned}$$

When $n = 2$, we use only the second description of I_f given above. In Chapter 3, it is shown that these definitions of I_f and J_f agree with the geometric ones given above, and in particular that I_f and J_f are closed under multiplication by elements of R_f. We have a map of R_f-modules $I_f \to J_f$ given by inclusion. This map is not canonical and does not arise geometrically, yet it will be important in our proofs.

The elements $f_0, \zeta_1, \ldots, \zeta_{n-1}$ are a B'-module basis of $B'[\theta]/F(\theta,1)$. Let $\check{\zeta}_i$ be the B'-module basis of $\mathrm{Hom}_{B'}(B'[\theta]/F(\theta,1), B')$ dual to the ζ_i. So $\check{\zeta}_i(\zeta_j) = \delta_{ij}$ for $j > 0$. Also, let $\check{\theta}_i$ be the B'-module basis of $\mathrm{Hom}_{B'}(B'[\theta]/F(\theta,1), B')$ dual to $1, \theta, \theta^2, \ldots, \theta^{n-1}$. We can apply these $\check{\zeta}_i$ and $\check{\theta}_i$ to elements in I and J since they lie in $B'[\theta]/F(\theta,1)$, but they are not necessarily dual to a B-module basis of I or J. The following are the key computations we will need.

Proposition 5.2.1. *For $r \in B'[\theta]/F(\theta,1)$ and $1 \le k \le n-1$,*

$$\check{\zeta}_{n-1}(\zeta_k r) = \check{\theta}_{n-1-k}(r) - f_k\check{\zeta}_{n-1}(r).$$

Proof. We will write out $\zeta_k r$ in terms of powers of θ and then read off the coefficient of θ^{n-1}. First, we write $r = \sum_{j=0}^{n-1} r_j\theta^j$ and so

$$\zeta_k r = (f_0\theta^k + \cdots + f_{k-1}\theta)(r_{n-1}\theta^{n-1} + \cdots + r_0).$$

To find the θ^{n-1} coefficient, we only have to look at terms of r with $j \geq n-1-k$. From the $r_{n-1-k}\theta^{n-1-k}$ term we get a θ^{n-1} coefficient of $r_{n-1-k}f_0$. From the remaining terms, we get the sum

$$\begin{aligned}\sum_{j=n-k}^{n-1} r_j\theta^j(f_0\theta^k + \cdots + f_{k-1}\theta) &= \sum_{j=n-k}^{n-1} r_j\theta^{j-(n-k)}(f_0\theta^n + \cdots + f_{k-1}\theta^{n-k+1}) \\ &= \sum_{j=n-k}^{n-1} -r_j\theta^{j-(n-k)}(f_k\theta^{n-k} + \cdots + f_n)\end{aligned}$$

and the only term of the final sum with a non-zero θ^{n-1} coefficient is the $j = n-1$ term which has a θ^{n-1} coefficient of $-r_{n-1}f_k$. So $\check{\theta}_{n-1}(r) = f_0\check{\theta}_{n-1-k}(r) - f_k\check{\theta}_{n-1}(r)$, and dividing by f_0 proves the proposition. □

Corollary 5.2.2. *For $r \in B'[\theta]/f(\theta, 1)$,*

$$\check{\zeta}_{n-1}(\theta r) = \check{\zeta}_{n-2}(r).$$

Proof. We have

$$\check{\zeta}_{n-1} := \frac{\check{\theta}_{n-1}}{f_0} \quad \text{and} \quad \check{\zeta}_{n-2} := \frac{\check{\theta}_{n-2} - \frac{f_1\check{\theta}_{n-1}}{f_0}}{f_0},$$

and thus this follows from the above proposition when $k = 1$. □

Lemma 5.2.3. *If we have a homomorphism ϕ of B-modules from some B-module P to J_f, then the image of ϕ is in I_f if and only if the image of $\check{\zeta}_{n-2}\phi$ is in B.*

Proof. The elements of I_f are just the elements $j \in J_f$ for which $\check{\zeta}_{n-2}(j) \in B$. □

Thus $\check{\zeta}_{n-1}$ and $-\check{\zeta}_{n-2}$ give two B-module maps from I_f to B, or a B-module map $I_f \to V = B^2$, where $(-1)^{i+1}\zeta_{n-i}$ gives the map into the ith coordinate of V. We choose the maps in such a way that the map $I_f \to V$ the canonical map given in Equations (3.14) and (3.15). This map is useful because it doesn't lose information about R_f-module maps. More formally, we have the following.

Proposition 5.2.4. *For any binary n-ic form f and any R_f-module P, composition with the map $I_f \to V$ gives an injection of R_f modules*

$$\mathrm{Hom}_{R_f}(P, I_f) \to \mathrm{Hom}_B(P, V).$$

Proof. Suppose, for the sake of contradiction, that we had a non-zero map $\phi \in \mathrm{Hom}_{R_f}(P, I_f)$ such that the image of ϕ was in the kernel of $I_f \to V$. Let r be a non-zero element of $\mathrm{im}(\phi)$. Then, by Proposition 5.2.1 we have

$$\check{\theta}_{n-1-k}(r) = \check{\zeta}_{n-1}(\zeta_k r) = 0$$

for $2 \leq k \leq n-1$. Thus, we see that $r = 0$. □

In Corollary 3.3.7, we see that as R_f modules, $J_f \cong \mathrm{Hom}_B(R_f, B)$, and thus we have the following proposition.

Proposition 5.2.5. *For any binary n-ic form f and any R_f-module P, composition with the map $\check{\zeta}_{n-1}\colon J_f \to B$ gives an isomorphism of R_f modules*

$$\mathrm{Hom}_{R_f}(P, J_f) \overset{\check{\zeta}_{n-1}}{\to} \mathrm{Hom}_B(P, B).$$

5.3 Main theorems

We write an element $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ as pair A_1, A_2 of $n \times n$ matrices. The *determinant* of A is the binary n-ic form $\det(A_1x_1 + A_2x_2)$. For binary form f with integer coefficients, we defined in Section 5.2 a rank n ring R_f and two modules I_f and J_f for that ring. Recall that we have a map $I_f \to V$ of abelian groups, where $V = \mathbb{Z}^2$. We will next define a notion of a balanced pair of R_f-modules. The idea is that the product of the pair should map to I_f, but that map should be constrained by the form f itself.

Definition. A *based balanced pair of modules* for f is a pair of R_f-modules M and N, a choice of basis $M \cong \mathbb{Z}^n$ and $N \cong \mathbb{Z}^n$, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathbb{Z}} N \to M \otimes_{R_f} N \to I_f \to V$ is written as a pair of matrices A_1 and A_2 (viewing elements of M as row vectors and elements of N as column vectors), we have $\det(A_1x_1 + A_2x_2) = f$. If v_i, m_j, and n_k are the bases of V, M, and N respectively indicated above, then the j,k entry of A_i is the coefficient of v_i in the image of $m_j \otimes n_k$, i.e. $(-1)^{i+1}\zeta_{n-i}(m_j \otimes n_k)$. We will often refer to the based balanced pair as M, N, with the bases and balancing map understood.

Definition. A *balanced pair of modules* for a non-zero form f is a pair of R_f-modules M and N, each a free rank n $\mathbb{Z}$-module, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathbb{Z}} N \to M \otimes_{R_f} N \to I_f \to V$ is written as a pair of matrices A_1 and A_2, we have $\det(A_1x_1 + A_2x_2) = \pm f$. Given a balanced pair of modules for a non-zero form f, there is a unique choice of generator χ of $\wedge^n M \otimes \wedge^n N$ such that $\det(A_1x_1 + A_2x_2) = f$ when choosing bases of M and N that give $\chi \in \wedge^n M \otimes \wedge^n N$, because $-\chi$ would give $\det(A_1x_1 + A_2x_2) = -f$. If we have based balanced pairs (M, N) and (M', N') such that the modules and balancing maps are the same and only the bases differ, then the change of bases must preserve χ since both based balanced pairs give $\det(A_1x_1 + A_2x_2) = f$.

In this section we prove the following theorem.

Theorem 5.3.1. *For every non-zero binary n-ic form f with coefficients in $\mathbb{Z}$, there is a bijection*

$$\left\{\begin{matrix}\textit{based balanced pairs } (M,N) \textit{ of} \\ \textit{modules for } f\end{matrix}\right\} \longleftrightarrow \{A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n \textit{ with } \det(A) = f\}.$$

Let Γ be the subgroup of $\mathrm{GL}_n(\mathbb{Z}) \times \mathrm{GL}_n(\mathbb{Z})$ of elements (g_1, g_2) with $\det(g_1)\det(g_2) = 1$. Then, Γ acts equivariantly in the above bijection (acting of the bases of M and N), and we obtain a bijection

$$\left\{\begin{matrix}\textit{isomorphism classes of balanced} \\ \textit{pairs } (M,N) \textit{ of modules for } f\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\Gamma \textit{ classes of } A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n \textit{ with} \\ \det(A) = f\end{matrix}\right\}.$$

It is easy to give a map ϕ from balanced based pairs to $\mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$. From the definition of a balanced based pair, we have the map of $\mathbb{Z}$-modules $M \otimes_{\mathbb{Z}} N \to M \otimes_{R_f} N \to I_f \to V$, which can be written as a pair of matrices A_1, A_2 as above. This pair of matrices is $\phi(M, N)$.

In Section 5.3.1 we construct a based balanced pair of modules from an $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$. Our construction is completely concrete, and we give formulas for the action of R_f on M and N. In Section 5.3.2, we prove that this construction gives an inverse to the map ϕ described above when $f_0 \neq 0$. In Section 5.3.3, we use the GL_2 equivariance of our construction to reduce to the case that $f_0 \neq 0$, which will prove Theorem 5.3.1.

5.3.1 Construction of balanced pair of modules

We are given $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$, which we can write as a pair A_1, A_2 of $n \times n$ matrices. Let f be the determinant of A. In this section, we will construct a based balanced pair (M, N) of modules for f. We begin by letting $M = \mathbb{Z}^n$ and $N = \mathbb{Z}^n$ as abelian groups. It remains to specify the R_f action on M and N and the map of R_f-modules $M \otimes_{R_f} N \to I_f$. We can write the elements of M as row vectors with entries in $\mathbb{Z}$ and the elements of N as column vectors with entries in $\mathbb{Z}$. Heuristically, the action of R_f will by given by θ acting on M on the right by $-A_2 A_1^{-1}$ and on N on the left by $-A_1^{-1} A_2$. The trouble with this construction is that θ is not an element of R_f (unless f_0, the x^n coefficient of f, is ± 1) and that A_1 is not necessarily invertible (it could be the zero matrix!). We could solve both of these problems by inverting f_0, but it is possible that $f_0 = 0$. So we will pass to a universal situation, where we can always invert f_0.

We replace $\mathbb{Z}$ by the ring $\Lambda = \mathbb{Z}[\{u_{ijk}\}_{1 \leq i \leq 2, 1 \leq j \leq n, 1 \leq k \leq n}]$ (the free polynomial algebra on $2n^2$ variables over $\mathbb{Z}$), and we replace A with the universal tensor $\mathcal{C}$ in $\Lambda^2 \otimes_\Lambda \Lambda^n \otimes_\Lambda \Lambda^n$, where $\mathcal{C}_i$ has j, k entry $u_{i,j,k}$. We have a binary n-ic form $c = \det(\mathcal{C}_1 x_1 + \mathcal{C}_2 x_2)$ with coefficients in Λ. We now let $M_{\mathcal{C}} = \Lambda^n$ and $N_{\mathcal{C}} = \Lambda^n$ as Λ-modules. We will give an action of the Λ-algebra R_c on $M_{\mathcal{C}}$ and $N_{\mathcal{C}}$ and then we will give a map of R_c-modules $M_{\mathcal{C}} \otimes_{R_c} N_{\mathcal{C}} \to I_c$. This construction will be equivariant for the Γ_Λ actions, where Γ_Λ is the subgroup of $\mathrm{GL}_n(\Lambda) \times \mathrm{GL}_n(\Lambda)$ of (g_1, g_2) such that $\det(g_1)\det(g_2) = 1$. To recover a construction over $\mathbb{Z}$, we can just specialize by letting the $u_{i,j,k} = a_{i,j,k}$ in our formulas.

R_c action

We will write elements of $M_{\mathcal{C}}$ as row vectors with entries in Λ and elements of $N_{\mathcal{C}}$ as column vectors with entries in Λ. We can write $c = c_0 x_1^n + c_1 x_1^{n-1} x_2 + \cdots + c_n x_2^n$. We

will invert c_0 and denote all of the corresponding objects with a $'$. For example, we have $\Lambda' = \Lambda_{c_0}$, the ring Λ with c_0 inverted. We also have $R_c' = R_c \otimes_\Lambda \Lambda'$, which is just the result of inverting c_0 in R_c. If we write $c = C(x_1, x_2)$, we know from Section 5.2 that $R_c' = \Lambda'[\theta]/C(\theta, 1)$. We have $M_\mathcal{C}' = M_\mathcal{C} \otimes_\Lambda \Lambda'$ and $N_\mathcal{C}' = N_\mathcal{C} \otimes_\Lambda \Lambda'$.

We define an action of R_c' on $M_\mathcal{C}'$ and $N_\mathcal{C}'$ (which we still view as row vectors and column vectors respectively, just now with entries in Λ') by having θ act like $-\mathcal{C}_2\mathcal{C}_1^{-1}$ (on the right) on the row vectors and $-\mathcal{C}_1^{-1}\mathcal{C}_2$ (on the left) on the column vectors. Since $\det(\mathcal{C}_1 x_1 + \mathcal{C}_2 x_2) = c$, the matrices $-\mathcal{C}_2\mathcal{C}_1^{-1}$ and $-\mathcal{C}_1^{-1}\mathcal{C}_2$ satisfy their (common) characteristic polynomial $C(t, 1)$. Thus we have given a well-defined action of $\Lambda'[\theta]/u(\theta, 1)$ on $M_\mathcal{C}'$ and $N_\mathcal{C}'$. This restricts to an action of R_c on $M_\mathcal{C}'$ and $N_\mathcal{C}'$, which we will now show is actually an action of R_c on $M_\mathcal{C}$ and $N_\mathcal{C}$.

Lemma 5.3.2. *For $1 \leq k \leq n-1$, the matrix*

$$c_0(-\mathcal{C}_1^{-1}\mathcal{C}_2)^k + c_1(-\mathcal{C}_1^{-1}\mathcal{C}_2)^{k-1} + \dots c_{k-1}(-\mathcal{C}_1^{-1}\mathcal{C}_2) \tag{5.1}$$

whose entries a priori are in $\mathbb{Q}(u_{i,j,k})$ (the fraction field of Λ) are actually in Λ.

Proof. Over the field $\mathbb{Q}(u_{i,j,k})$, since $-\mathcal{C}_1^{-1}\mathcal{C}_2$ satisfies its characteristic polynomial, we have

$$\begin{aligned} c_0(-\mathcal{C}_1^{-1}\mathcal{C}_2)^n &+ c_1(-\mathcal{C}_1^{-1}\mathcal{C}_2)^{n-1} + \dots c_{k-1}(-\mathcal{C}_1^{-1}\mathcal{C}_2)^{n-k+1} \\ &+ c_k(-\mathcal{C}_1^{-1}\mathcal{C}_2)^{n-k} + c_{k+1}(-\mathcal{C}_1^{-1}\mathcal{C}_2)^{n-k-1} + \dots c_n(-\mathcal{C}_1^{-1}\mathcal{C}_2)^0 = 0. \end{aligned}$$

Since $\mathcal{C}_1$ and $\mathcal{C}_2$ are invertible over the field $\mathbb{Q}(u_{i,j,k})$, the last equation is equivalent to

$$c_0(-\mathcal{C}_1^{-1}\mathcal{C}_2)^k + c_1(-\mathcal{C}_1^{-1}\mathcal{C}_2)^{k-1} + \dots c_{k-1}(-\mathcal{C}_1^{-1}\mathcal{C}_2) \tag{5.2}$$

$$= -\left(c_{k+1}(-\mathcal{C}_2^{-1}\mathcal{C}_1)^0 + \dots c_n(-\mathcal{C}_2^{-1}\mathcal{C}_1)^{n-k}\right). \tag{5.3}$$

If we view the matrix entries of the expressions in Equations (5.2) and (5.3) as reduced ratios of elements of the UFD Λ, the denominator of the left hand side can only involve u_{1jk} and the denominator of the right hand side can only involve u_{2jk}. Thus, the matrices $c_0(-\mathcal{C}_1^{-1}\mathcal{C}_2)^k + c_1(-\mathcal{C}_1^{-1}\mathcal{C}_2)^{k-1} + \dots c_{k-1}(-\mathcal{C}_1^{-1}\mathcal{C}_2)$ must have all their entries in Λ. □

By definition, the Λ-algebra R_c has a basis as a Λ-module given by $1, \zeta_1, \dots, \zeta_{n-1}$, where $\zeta_k = c_0\theta^k + \dots + c_{k-1}\theta \in \Lambda'[\theta]/c(\theta, 1)$. Thus ζ_k action on $N_\mathcal{C}'$ is given by a matrix whose coefficients are in Λ, and so it restricts to an action on $N_\mathcal{C}$. An analogous argument can be made for $M_\mathcal{C}$. This construction is clearly equivariant for the Γ_Λ actions.

Balancing Map

Now we will construct a map of R_c-modules $M_\mathcal{C} \otimes_{R_c} N_\mathcal{C} \to I_c$. The matrix $\mathcal{C}_1$ gives us an Λ-module pairing on $M_\mathcal{C}$ and $N_\mathcal{C}$ into Λ by $\alpha \star \beta = \alpha\mathcal{C}_1\beta$ for $\alpha \in M_\mathcal{C}$ and $\beta \in N_\mathcal{C}$. In other words, the matrix $\mathcal{C}_1$ which acts on $N_\mathcal{C}$ on the left as a Λ-module, gives n

homomorphisms of Λ-modules from $N_{\mathcal{C}}$ into Λ, one for each row of $\mathcal{C}_1$, and we map the ith basis element m_i of M to the Λ-module homomorphism of $N_{\mathcal{C}}$ into Λ given by the ith row of $\mathcal{C}_1$. This gives us a Λ-module map from $M_{\mathcal{C}}$ into $\mathrm{Hom}_\Lambda(N_{\mathcal{C}}, \Lambda)$ and we have $\mathrm{Hom}_\Lambda(N_{\mathcal{C}}, \Lambda) \cong \mathrm{Hom}_{R_c}(N, J_c)$, by Proposition 5.2.5. We use the symbol $\circ$ to denote the resulting pairing of $M_{\mathcal{C}}$ and $N_{\mathcal{C}}$ into J_c. Thus, $\check{\zeta}_{n-1}(\alpha \circ \beta) = \alpha \star \beta$. This pairing in J_c is clearly equivariant for the Γ_Λ actions.

Now we will show that $\circ$ gives a map of R_c-modules $M_{\mathcal{C}} \otimes_{R_c} N_{\mathcal{C}} \to I_c$. To see this, we extend our pairing $\circ$ to $M'_{\mathcal{C}} \otimes_{\Lambda'} N'_{\mathcal{C}} \to J'_c$, which is a R'_c module map for the R'_c action on $N_{\mathcal{C}}$. In fact, we can show that $\circ$ factors through $M'_{\mathcal{C}} \otimes_{R'_c} N'_{\mathcal{C}}$, i.e. $(\theta\alpha) \circ \beta = \alpha \circ (\theta\beta)$ for $\alpha \in M'_{\mathcal{C}}$ and $\beta \in N'_{\mathcal{C}}$. If we fix an α and let β vary over the elements of $N'_{\mathcal{C}}$, the expressions $(\theta\alpha) \circ \beta = \alpha \circ (\theta\beta)$ give two homomorphisms from $N'_{\mathcal{C}}$ into J'_c and we can check if they are the same by taking $\check{\zeta}_{n-1}$. Now, $\check{\zeta}_{n-1}((\theta\alpha) \circ \beta) = (\theta\alpha) \star \beta = \alpha(-\mathcal{C}_2\mathcal{C}_1^{-1})\mathcal{C}_1\beta$ and $\check{\zeta}_{n-1}(\alpha \circ (\theta\beta)) = \alpha\mathcal{C}_1(-\mathcal{C}_1^{-1}\mathcal{C}_2)\beta$, so we see that $\circ$ gives a map of R'_c modules $M'_{\mathcal{C}} \otimes_{R'_c} N'_{\mathcal{C}} \to J'_c$ and thus our original $\circ$ is a map of R_c-modules $M_{\mathcal{C}} \otimes_{R_c} N_{\mathcal{C}} \to J_c$.

We have an inclusion of R_c modules $I_c \subset J_c$ (given in Section 5.2), and we will use Lemma 5.2.3 to see that for all $\alpha \in M_{\mathcal{C}}$ and $\beta \in N_{\mathcal{C}}$, the element $\alpha \circ \beta$ is in I_c. Fix an $\alpha \in M_{\mathcal{C}}$. Then by Lemma 5.2.3, $\alpha \circ N_{\mathcal{C}} \subset I_c$ if and only if $\check{\zeta}_{n-2}(\alpha \circ N_{\mathcal{C}}) \subset \Lambda$. By Corollary 5.2.2 we see that $\check{\zeta}_{n-2}(\alpha \circ N_{\mathcal{C}}) = \check{\zeta}_{n-1}(\alpha \circ (\theta N_{\mathcal{C}})) = \alpha \star (\theta N_{\mathcal{C}})$. However, we have seen that the pairing $\alpha \star (\theta\beta)$ is given by the matrix $-\mathcal{C}_2$, and thus $\check{\zeta}_{n-2}(\alpha \circ N_{\mathcal{C}}) \subset \Lambda$. Thus we have given a map of R_c-modules $M_{\mathcal{C}} \otimes_{R_c} N_{\mathcal{C}} \to I_c$. Note that we have defined $\circ$ so that if m_j and n_k are the chosen bases of $M_{\mathcal{C}}$ and $N_{\mathcal{C}}$ respectively,

$$\check{\zeta}_{n-1}(m_j \circ n_k) = u_{1jk} \quad \text{and} \quad -\check{\zeta}_{n-2}(m_j \circ n_k) = u_{2jk}, \tag{5.4}$$

which makes $M_{\mathcal{C}}$ and $N_{\mathcal{C}}$ a based balanced pair of modules for c.

Back to $\mathbb{Z}$

Now given $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$, to find the action of R_f on M, we take the matrix by which ζ_k acted on $M_{\mathcal{C}}$ above, and substitute $a_{i,j,k}$ for the $u_{i,j,k}$, and similarly for N. Of course, the conditions for this to be a ring action will be satisfied since they are satisfied formally. Also, we have a map of $\mathbb{Z}$-modules $M \otimes_{\mathbb{Z}} N \to I_f$ given by specializing the formulas from the last section, and we can see that this factors through a map of R_f-modules $M \otimes_{R_f} N \to I_f$ because the conditions for the factorization and for the map to respect R_f-module structure are satisfied formally. Let $\psi(A) = (M, N)$.

5.3.2 Proof of Theorem 5.3.1 when $f_0 \neq 0$

Now we prove Theorem 5.3.1 by showing that ϕ and ψ are inverse constructions. Suppose we have $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$. Let $\psi(A) = (M, N)$, and let $A' = \phi(M, N)$. By Equation (5.4), we have that $A' = A$. Now, suppose we have (M, N), a based balanced pair of modules for f, and $\phi(M, N) = A$ and $\psi(A) = (M', N')$. We first check that the action of R_f is the same on M and M' (and N and N'), and then we will check that the balancing maps agree. We assume that $f_0 \neq 0$. In this case, we may invert f_0 as in Section 5.3.1, and obtain $\mathbb{Z}[\theta]/F(\theta, 1)$-modules M_{f_0} and N_{f_0}.

Proposition 5.3.3. *If we write elements of M_{f_0} as row vectors and elements of N_{f_0} as column vectors, then θ acts by $-A_2A_1^{-1}$ on the right on M_{f_0} and θ acts by $-A_1^{-1}A_2$ on the left on N_{f_0}.*

Proof. We let the map $M \otimes_{\mathbb{Z}} N \to I_f$ be denoted by $\circ$. We define $\alpha \star \beta$ to be $\check{\zeta}_{n-1}(\alpha \circ \beta)$. We fix a non-zero $\alpha \in M_{f_0}$ and suppose for the sake of contradiction that $\alpha \star N_{f_0} = 0$. Then $\alpha \circ N_{f_0} = 0$ by Proposition 5.2.5, and thus $\alpha A_1 = \alpha A_2 = 0$. Thus α is in the left kernel of $A_1x_1 + A_2x_2$ for formal x_i and so we obtain $f = \det(A_1x_1 + A_2x_2) = 0$, a contradiction. Therefore, if $\alpha \circ N_{f_0} = 0$, then $\alpha = 0$. We have$(\theta\alpha) \star \beta = \check{\zeta}_{n-2}(\alpha \circ \beta)$ by Corollary 5.2.2 and $\check{\zeta}_{n-2}(\alpha \circ \beta) = \alpha(-A_2)\beta = (\alpha(-A_2A_1^{-1}))A_1\beta$. We conclude that $\theta\alpha = \alpha(-A_2A_1^{-1})$. A similar argument can be made for N_{f_0}. □

This proposition shows that the pairs of modules (M, N) and (M', N') have the same R_f action. We know that the map $\mathrm{Hom}_{R_f}(M \otimes_{R_f} N, I) \to \mathrm{Hom}_{\mathbb{Z}}(M \otimes_{\mathbb{Z}} N, V)$ is injective (from Proposition 5.2.4), and thus since $\phi(M, N) = A$ and $\phi(M', N') = \phi(\psi(A)) = A$, we see that (M, N) and (M', N') have the same balancing map. Therefore, we have proven Theorem 5.3.1 when $f_0 \neq 0$. We will finish the proof at the beginning of the next section, by reducing to this case.

5.3.3 $\mathrm{GL}(V)$ invariance

Let $V = \mathbb{Z}^2$, and we have that $\mathrm{GL}_2(\mathbb{Z}) = \mathrm{GL}(V)$ acts on $V \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ and also on binary n-ic forms in $\mathrm{Sym}^n V$. The determinant map is equivariant for these actions. Let $g \in \mathrm{GL}(V)$, so that $g(A) = A'$ and $g(f) = f'$. Then we have (see Chapter 3) isomorphisms $R_f \cong R'_f$, and $I_f \cong I'_f$. In fact, g also gives a map $V \to V$ such that the diagram

$$\begin{array}{ccc} I_f & \xrightarrow{g} & I'_f \\ \downarrow & & \downarrow \\ V & \xrightarrow[g]{} & V \end{array}$$

commutes.

More concretely, consider $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. If $A = (A_1, A_2)$, then $g(A) = A' = (A'_1, A'_2) = (aA_1+bA_2, cA_2+dA_2)$. If $f = F(x, y)$, then $g(f) = f' = F(ax+cy, bx+dy)$. Write $f' = F'(x, y)$. If θ is a root of $F(x, 1)$, then $\theta' = \frac{d\theta-c}{-b\theta+a}$ is a root of $F'(x, 1)$. This induces the map $R'_f \cong R_f$. Note that $\theta = \frac{a\theta'+c}{b\theta'+d}$. We can view I_f and I'_f as fractional ideals in the same $\mathbb{Q}$-algebra. They are given as fractional ideals of different $\mathbb{Q}$-algebras, Q_f and Q'_f respectively, in Section 5.2, but the map $\theta' \mapsto \frac{d\theta-c}{-b\theta+a}$ gives an isomorphism of those $\mathbb{Q}$-algebras. Then the map $I_f \cong I'_f$ is given by

$$I_f \to Q_f \cong Q'_f \xrightarrow{\times(b\theta'+d)^{n-3}} Qf' \supset I'_f.$$

Note that $\frac{1}{b\theta'+d} = \frac{a-b\theta}{ad-bc}$.

Viewing $\check{\zeta}_{n-1}$,$\check{\zeta}_{n-2}$ and $\check{\zeta}'_{n-1}$,$\check{\zeta}'_{n-2}$ as maps of I_f and I'_f, respectively, we have that $I_f \cong I'_f$ induces

$$\check{\zeta}'_{n-1} \mapsto a\check{\zeta}_{n-1} - b\check{\zeta}_{n-2} \text{ and } -\check{\zeta}'_{n-2} \mapsto \check{\zeta}_{n-1} - d\check{\zeta}_{n-2},$$

which exactly gives that our construction of (A_1, A_2) from $\check{\zeta}_{n-1}$,$-\check{\zeta}_{n-2}$ is equivariant. We can check this on a basis of $\mathrm{GL}_2(\mathbb{Z})$, though it also follows from Proposition 3.3.3. If we write an element v of V as a column vector, then g acts on V by the standard left action. In the map from $I_f \to V$, an element $\alpha \in I_f$ maps to $\begin{bmatrix} \check{\zeta}'_{n-1}(\alpha) \\ -\check{\zeta}'_{n-2}(\alpha) \end{bmatrix}$.

Our constructions of M, N, and the balancing map are equivariant under this $\mathrm{GL}(V)$ action. More precisely, under the identifications $R_f \cong R'_f$ and $I_f \cong I'_f$ and the map $V \xrightarrow{g} V$, the based modules and balancing map we obtain from A are the same as the based modules and balancing map we obtain from A'. (This can easily be checked on a basis of $\mathrm{GL}_2(\mathbb{Z})$, or alternatively, it follows from the geometric versions of the constructions in Section 5.7. For example, if θ acts like $-A_2A_1^{-1}$ then $\theta' = \frac{d\theta - c}{-b\theta + a}$ will act like $(-dA_2A_1^{-1} - c)(bA_2A_1^{-1} + a)^{-1} = -(A'_2)(A'_1)^{-1}$.) Thus, to check that the R_f action and balancing map on pairs M, N and M', N' agree, we can check after a $\mathrm{GL}_2(\mathbb{Z})$ action on f so that $f_0 \neq 0$ (as long as $f \neq 0$). This proves Theorem 5.3.1.

5.4 Symmetric tensors

In the map

$$\left\{\begin{matrix}\text{based balanced pairs } (M,N) \text{ of} \\ \text{modules for } f\end{matrix}\right\} \longleftrightarrow \{A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n \text{ with } \det(A) = f\}.$$

of Theorem 5.3.1, it is easy to see from the construction that pairs where M and N are the same based module exactly correspond to A such that A_1 and A_2 are symmetric matrices.

Definition. A *self balanced module* for a non-zero form f is an R_f-module M, that is a free rank n $\mathbb{Z}$-module, and a map of R_f-modules $M \otimes_{R_f} M \to I_f$, such that when the composition $M \otimes_{\mathbb{Z}} N \to M \otimes_{R_f} N \to I_f \to V$ is written as a pair of matrices A_1 and A_2, we have $\det(A_1x_1 + A_2x_2) = \pm f$.

We easily conclude the following.

Theorem 5.4.1. *For every non-zero binary n-ic form f with coefficients in $\mathbb{Z}$, there is a bijection*

$$\left\{\begin{matrix}\textit{isomorphism classes self balanced} \\ \textit{modules } M \textit{ for } f\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\mathrm{GL}_n(\mathbb{Z}) \textit{ classes of } A \in \mathbb{Z}^2 \otimes \\ \mathrm{Sym}_2 \mathbb{Z}^n \textit{ with } \det(A) = f\end{matrix}\right\},$$

where $\mathrm{Sym}_2 \mathbb{Z}^n$ are symmetric n by n matrices, and the action of $g \in \mathrm{GL}_n(\mathbb{Z})$ is by multiplication on the left by g and the right by g^t.

5.5 Equivalent formulations of the balancing condition

In order to prove Theorems 5.1.1 and 5.1.3 in the Introduction, we will show that for primitive forms, modules that appear in balanced pairs have unique balance part-

ners, and that for non-degenerate forms, modules that appear in balanced pairs can be realized as fractional ideals. First, we will see an equivalent formulation of the definition of balanced.

We define a *characteristic R_f-module* M to be a R_f-module M which is a free rank n $\mathbb{Z}$-module such that for any element $\zeta \in R_f$ the action of ζ on M viewed as a $\mathbb{Z}$-module has the same characteristic polynomial as the action of ζ on R_f (by multiplication) viewed as a $\mathbb{Z}$-module. Fractional ideals of R_f are characteristic modules of R_f.

Given two based modules M and N with bases α_i and β_i respectively such that $M \subset N$, the *index* $[N : M]$ is the absolute value of the determinant of the matrix Q with entries in $\mathbb{Z}$ such that $[\alpha_1 \ \ \alpha_2 \ \ \dots \ \ \alpha_n] = [\beta_1 \ \ \beta_2 \ \ \dots \ \ \beta_n] \cdot Q$. Now we will see that our condition of balanced is equivalent to M characteristic and an index condition on the map $M \otimes_{R_f} N \to I$.

Proposition 5.5.1. *Consider a non-zero binary form f over $\mathbb{Z}$, and two R_f modules M and N, with a R_f-module map $M \otimes_{R_f} N \to I_f$, such that M and N are both free rank n $\mathbb{Z}$-modules. Then this data gives a balanced pair of modules for f if and only if $M \subset \mathrm{Hom}_{R_f}(N, I_f)$, and $[\mathrm{Hom}_{R_f}(N, J_f) : M] = [J_f : I_f]$ (with any inclusion of I_f in J_f as R_f-modules), and either M or N is characteristic.*

The equality of indexes does not depend on the choice of inclusion of I in J, because any two inclusions differ by multiplication by a non-zero divisor in $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. This multiplies both $[\mathrm{Hom}_{R_f}(N, J) : M] = [J : I]$ by the absolute value of the norm of that element.

Proof. We can act by $\mathrm{GL}_2(\mathbb{Z})$ so as to assume $f_0 \neq 0$. Then, we use the inclusion of I_f in J_f given in Section 5.2 and see that $[J_f : I_f] = f_0$.

Lemma 5.5.2. *Suppose we have two R_f modules M and N, with a map $M \otimes_{R_f} N \to I_f$, such that M and N are both free rank n $\mathbb{Z}$-modules, either M or N is characteristic, and $M \subset \mathrm{Hom}_{R_f}(N, I_f)$ such that $[\mathrm{Hom}_{R_f}(N, J_f) : M] = f_0$. Let A, as usual, denote the map $M \otimes_{\mathbb{Z}} N \to V$. We write elements of M as row vectors with entries in $\mathbb{Z}$. Then θ acts on $M' = M_{f_0}$ by $-A_2 A_1^{-1}$ on the right, and θ acts on $N' = N_{f_0}$ by $-A_1^{-1} A_2$ on the left. Also, $\mathrm{Det}(A_1 x_1 + A_2 x_2) = f$.*

Proof. We define $m \star n$ to be $\check{\zeta}_{n-1}(m \circ n)$. By Proposition 5.2.5, we see that $\star$ is faithful for both M and N if and only if $\circ$ is. We see that $\circ$ is faithful on M since the index of M in $\mathrm{Hom}_{R_f}(N, J_f)$ is not zero. If there were an $n \in N$ such that $M \circ n = 0$ for all n, then inverting f_0 we would find that $M_{f_0} \star n = 0$ but $M_{f_0} = \mathrm{Hom}_{\mathbb{Z}_{f_0}}(N_{f_0}, \mathbb{Z}_{f_0})$, and we obtain a contradiction since N_{f_0} is a free $\mathbb{Z}_{f_0}$-module and thus there is some homomorphism from N_{f_0} to $\mathbb{Z}_{f_0}$ which is non-zero on n. So, we fix an $\alpha \in M$ and let β vary in N. Then $\alpha\theta \star \beta = \check{\zeta}_{n-2}(\alpha \circ \beta) = -\alpha A_2 \beta = -\alpha A_2 A_1^{-1} A_1 \beta = (-\alpha A_2 A_1^{-1}) \star \beta$. We similarly obtain the action of θ on N.

We have that $|\mathrm{Det}(A_1)|$ is the index of M in $\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Z})$ or $\mathrm{Hom}_{R_f}(N, J_f)$, which is the index of I in J, i.e. $|f_0|$. Since M is characteristic, we know that θ and thus $-A_2 A_1^{-1}$ acts with characteristic polynomial $F(t, 1)/f_0$ on M_{f_0}. It follows that $\mathrm{Det}(A_1 x_1 + A_2 x_2) = \pm f$. We can argue similarly if N is characteristic. $\square$

Now, suppose that M, N are balanced. Then we know that M, N are constructed from an element $A \in Z^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ such that $\mathrm{Det}(A) = f$. We can see from the construction of the action of θ on M_{f_0} that M is characteristic. We have a map $M \to \mathrm{Hom}_{R_f}(N, I_f)$, and composition with $I_f \subset J_f$ gives $M \to \mathrm{Hom}_{R_f}(N, J_f) = \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Z})$. The map $M \to \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Z})$ is given by A_1, and thus $[\mathrm{Hom}_{R_f}(N, J) : M] = |f_0|$, which implies $M \subset \mathrm{Hom}_{R_f}(N, J_f)$, and thus the map $M \to \mathrm{Hom}_{R_f}(N, I_f)$ is injective as well. □

Corollary 5.5.3. *For a non-zero form f, if N is a finitely generated invertible module for R_f, then there exists a unique balancing partner M for N.*

Proof. If N is a finitely generated invertible module, then N can be realized an an invertible fractional ideal of R_f [10, II.5.7, Proposition 12]. Then $\mathrm{Hom}_{R_f}(N, J_f) = N^{-1}J_f$ and $\mathrm{Hom}_{R_f}(N, I_f) = N^{-1}I_f$. In that case, $[\mathrm{Hom}_{R_f}(N, J_f) : \mathrm{Hom}_{R_f}(N, I_f)] = [J_f : I_f]$ and for M to be balanced with N it is necessary and sufficient that $M = \mathrm{Hom}_{R_f}(N, I_f)$. □

5.5.1 Non-degenerate forms

When f is a non-degenerate binary n-ic form over $\mathbb{Z}$, we have the following.

Proposition 5.5.4. *If f is a non-degenerate binary n-ic form over $\mathbb{Z}$ (i.e. $\mathrm{disc}(f) \neq 0$), then all characteristic modules can be realized as fractional ideals. This gives a bijection between isomorphism classes of characteristic R_f-modules and fractional ideal classes of R_f.*

Proof. We assume $f_0 \neq 0$ by an action of $\mathrm{GL}_2(\mathbb{Z})$. Then, we see that we can put the action of θ on a characteristic module M in rational normal form over $\mathbb{Q}$, and since it acts with the same separable characteristic polynomial as the action of θ on $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$, in rational normal form these actions must be the same. Thus, we can view M as a $\mathbb{Z}$-submodule of $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$, or a fractional ideal. Clearly two fractional ideals in the same class give isomorphic modules. Moreover, a module homomorphism between two fractional ideals $I_1 \to I_2$ sends $q \in \mathbb{Q} \cap I_1$ to some element $k \in I_2$, and since the map is an R_f-module map, we see that it is multiplication by k/q. □

For a fractional ideal M, let $|M|$ denote the norm of M, given by the index $[R_f : M]$, which can be defined even if M is not a submodule of R_f, since they sit in a common $\mathbb{Q}$-vector space. Then, we can reformulate the balancing condition in terms of norms. This is the version of balanced used in [4] and [5].

Theorem 5.5.5. *For non-degenerate f, we have a bijection*

$$\left\{\begin{matrix}\textit{isomorphism classes of balanced}\\ \textit{pairs } (M,N) \textit{ of modules for } f\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\textit{classes of } (M,N) \textit{ where } M \textit{ and } N\\ \textit{are fractional } R_f\textit{-ideals, } MN \subset I_f\\ \textit{and } |M||N| = |I_f|\end{matrix}\right\},$$

where (M, N) and (M_1, N_1) are in the same class if $M_1 = \lambda M$ and $N_1 = \lambda^{-1}N$ for some invertible element $\lambda \in R_f \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proof. All modules that appear in balancing pairs are characteristic by Proposition 5.5.1, and thus can be realized as fractional ideals. For a balanced pair M, N of modules, we can take any fractional ideal representative of M, but then we choose the unique representative of N such that the map $M \otimes N \to I_f$ is just given by $M \otimes N \to MN \subset R_f \otimes_{\mathbb{Z}} \mathbb{Q}$ with image landing in $\mathcal{R}_f$. If M and N are fractional ideals of R_f, a map $M \otimes_{R_f} N \to I$ factors through MN.

We now argue that $\tau : MN \to I_f$ is injective. As usual, we assume $f_0 \neq 0$ by a $\mathrm{GL}_2(\mathbb{Z})$ action if necessary. We can detect the injectivity after tensoring with $\mathbb{Q}$ because $\mathbb{Q}$ is a flat $\mathbb{Z}$-module. Over $\mathbb{Q}$ we have that MN is at least rank n because it contains N and thus is rank n. We can take θ^k as a basis of MN, and we see where they map to in $I_f = J_f = \mathrm{Hom}(R, \mathbb{Q})$. Then $\tau(\theta^k)$ is the map in $\mathrm{Hom}(R, \mathbb{Q})$ that sends ζ_i to $\check{\zeta}_{n-1}(\zeta_i \theta^k)$. By Proposition 5.2.1, we have

$$\check{\zeta}_{n-1}(\zeta_i \theta^k) = \begin{cases} 1 & \text{if } k + i = n - 1 \text{ and } i > 0, \\ 1/f_0 & \text{if } k = n - 1 \text{ and } i = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we see that $\tau(MN) = \mathrm{Hom}(R, \mathbb{Q})$, when working over $\mathbb{Q}$, and therefore over $\mathbb{Z}$ we have that $MN \to I_f$ is injective.

A map $MN \to I_f$ is just multiplication by some element of $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. The element is not a zero-divisor since $MN \to I_f$ is injective, and thus it is invertible in $R_f \otimes_{\mathbb{Z}} \mathbb{Q}$. We can choose that element to be 1 by taking a different representative for N in its ideal class. If we had chosen a different representative for M, this would change the class of (M, N).

Suppose we have a balanced pair (M, N) realized as ideal classes with $MN \subset I$. We will show that the index condition for balanced is equivalent to the norm condition in the above theorem.

Proposition 5.5.6. *Let f be a non-zero form. If M and N are fractional ideals of R_f with $MN \subset I_f$, then $[\mathrm{Hom}_{R_f}(N, J_f) : M] = [J_f : I_f]$ if and only if $|M||N| = |I_f|$.*

Proof. We can act by $\mathrm{GL}_2(\mathbb{Z})$ so as to assume $f_0 \neq 0$. We claim that $|M||N|$ is the product of $|J_f|$ with the determinant of the pairing $\zeta_{n-1}(mn)$. When $M = R_f$ and $N = J_f$, we see from Proposition 5.2.1 that the determinant of the pairing is 1, and thus the claim is true. If we change $\mathbb{Q}$-bases from R_f, J_f to M, N, we change the determinant of the pairing by $N(M)N(N)/N(J_f)$ and thus the determinant of the pairing $\zeta_{n-1}(mn)$ is $|M||N|/|J_f|$.

The index of M in $\mathrm{Hom}_{R_f}(N, J_f)$ is just the index of M in $\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Z})$, which is giving by the pairing $\zeta_{n-1}(mn)$. Thus $[\mathrm{Hom}_{R_f}(N, J_f) : M] = |M||N|/|J_f|$. We see that $[\mathrm{Hom}_{R_f}(N, J_f) : M] = [J_f : I_f]$ if and only if $|M||N| = |I_f|$. □

The theorem now follows from the above proposition.

□

For symmetric tensors, we can make a similar argument to prove the following.

Theorem 5.5.7. *For non-degenerate f, we have a bijection*

$$\left\{\begin{array}{l}\text{isomorphism classes of self bal-}\\ \text{anced of modules } M \text{ for } f\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{classes of } (M,k) \text{ where } M \text{ is a}\\ \text{fractional } R_f\text{-ideal, } k \text{ is an in-}\\ \text{vertible element of } R_f \otimes_{\mathbb{Z}} \mathbb{Q}, \text{ and}\\ M^2 k \subset I_f \text{ and } |M|^2|(k)| = |I_f|\end{array}\right\},$$

where (M,k) and (M_1,k_1) are in the same class if $M_1 = \lambda M$ and $k_1 = \lambda^{-2}k$ for some invertible element $\lambda \in R_f \otimes_{\mathbb{Z}} \mathbb{Q}$.

5.5.2 Primitive forms

If f is primitive them I_f and J_f are invertible R_f modules (Proposition 3.6.4). For general non-zero forms, we saw in Corollary 5.5.3 that invertible ideals have unique balancing partners. For primitive f we have the following.

Proposition 5.5.8. *If f is a primitive non-degenerate form, and N is a characteristic R_f-module, then there exists a unique balancing partner M for N (i.e. an $\mathcal{R}_f$-module M and map $M \otimes_{R_f} N \to I_f$ that gives a balanced pair).*

Proof. In this case, we see that $[\mathrm{Hom}_{R_f}(N, J_f) : \mathrm{Hom}_{R_f}(N, I_f)] = [J_f : I_f]$. This is because $\mathrm{Hom}_{R_f}(N, J_f)$ and $\mathrm{Hom}_{R_f}(N, I_f)$ are naturally realized as fractional R_f ideals. Then we see that $\mathrm{Hom}_{R_f}(N, J_f)J_f^{-1}I_f \subset \mathrm{Hom}_{R_f}(N, I_f)$ and $\mathrm{Hom}_{R_f}(N, I_f)I_f^{-1}J_f \subset \mathrm{Hom}_{R_f}(N, J_f)$. Thus $\mathrm{Hom}_{R_f}(N, J_f) = \mathrm{Hom}_{R_f}(N, I_f)I_f^{-1}J_f$, and $[\mathrm{Hom}_{R_f}(N, J_f) : \mathrm{Hom}_{R_f}(N, I_f)]$ is the norm of $J_f I_f^{-1}$, which is $[J_f : I_f]$. Then, for M to be balanced with N it is necessary and sufficient that $M = \mathrm{Hom}_{R_f}(N, I_f)$. □

Theorem 5.1.1 now follows from Propositions 5.5.8 and 5.5.4 and Theorem 5.3.1. We can also apply Proposition 5.5.8 to symmetric tensors.

Theorem 5.5.9. *For non-degenerate primitive f, we have a bijection*

$$\left\{\begin{array}{l}\text{isomorphism classes of self bal-}\\ \text{anced of modules } M \text{ for } f\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{classes of } (M,k) \text{ where } M \text{ is a}\\ \text{fractional } R_f\text{-ideal, } k \text{ is an invert-}\\ \text{ible element of } R_f \otimes_{\mathbb{Z}} \mathbb{Q}, \text{ and } M =\\ (I_f k : M)\end{array}\right\},$$

where (M,k) and (M_1,k_1) are in the same class if $M_1 = \lambda M$ and $k_1 = \lambda^2 k$ for some invertible element $\lambda \in R_f \otimes_{\mathbb{Z}} \mathbb{Q}$, and $(I_f k : M)$ is the fractional ideal of elements x such that $xM \subset I_f k$.

5.6 Main theorem over an arbitrary base

The proof of Theorem 5.3.1 works over an arbitrary base with some modifications. Let S be a scheme. We consider binary n-ic forms with coefficients in $\mathcal{O}_S$, i.e. $f_0 x_1^n + f_1 x_1^{n-1} x_2 + \cdots + f_n x_2^n$ with $f_i \in \mathcal{O}_S$. We say such a form is a *zero-divisor* if it is a

zero divisor in the $\mathcal{O}_S$-algebra $\mathcal{O}_S[x,y]$, which means that for some open $\mathcal{U}$ of S, that f is zero divisor in $\mathcal{O}_S[x,y](\mathcal{U})$. We have constructions of R_f, $\mathcal{I}_f$, and J_f given in Chapter 3.

Definition. A *based balanced pair of modules* for f is a pair of R_f-modules M and N, a choice of basis $M \cong {\mathcal{O}_S}^n$ and $N \cong {\mathcal{O}_S}^n$, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathcal{O}_S} N \to M \otimes_{R_f} N \to I_f \to V$ is written as a pair of matrices A_1 and A_2, we have $\det(A_1 x_1 + A_2 x_2) = f$. A *balanced free pair of modules* for f is a pair of R_f-modules M and N, each a free rank n $\mathcal{O}_S$-module, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathcal{O}_S} N \to M \otimes_{R_f} N \to I_f \to V$ is written as a pair of matrices A_1 and A_2, we have $\det(A) = fu$, where u is a unit in $\mathcal{O}_S$. When f is not a zero-divisor, there is a unique choice of generator of $\wedge^n M \otimes \wedge^n N$ such that when bases of M and N are chosen with that orientation, we obtain $\det(A) = f$.

Theorem 5.6.1. *For every non-zero divisor binary n-ic form f with coefficients in $\mathcal{O}_S$, there is a bijection*

$$\left\{\begin{matrix}\text{based balanced pairs } (M,N) \text{ of} \\ \text{modules for } f\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}A \in {\mathcal{O}_S}^2 \otimes {\mathcal{O}_S}^n \otimes {\mathcal{O}_S}^n \text{ with} \\ \det(A) = f\end{matrix}\right\}.$$

Let Γ be the subgroup of $\mathrm{GL}_n(\mathcal{O}_S) \times \mathrm{GL}_n(\mathcal{O}_S)$ of pairs (g_1, g_2) with $\det(g_1)\det(g_2) = 1$. Then, Γ acts equivariantly in the above bijection (acting of the bases of M and N), and we obtain a bijection

$$\left\{\begin{matrix}\text{isomorphism classes of balanced} \\ \text{free pairs } (M,N) \text{ of modules for } f\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\Gamma \text{ classes of } A \in {\mathcal{O}_S}^2 \otimes {\mathcal{O}_S}^n \otimes {\mathcal{O}_S}^n \\ \text{with } \det(A) = f\end{matrix}\right\}.$$

Proof. To construct a based balanced pair of modules from $A \in {\mathcal{O}_S}^2 \otimes {\mathcal{O}_S}^n \otimes {\mathcal{O}_S}^n$, we can simply use the construction over the universal tensor and plug in the coefficients of A (and we call this construction ψ). Again, the balancing map composed with $I_f \to V$ gives the construction ϕ of an element of ${\mathcal{O}_S}^2 \otimes {\mathcal{O}_S}^n \otimes {\mathcal{O}_S}^n$ from a based balanced pair. Now, suppose we have (M,N), a based balanced pair of modules for f, and $\phi(M,N) = A$ and $\psi(A) = (M', N')$. We need to check that the action of R_f is the same on M and M' (and N and N'), and that the balancing maps agree. It suffices to check this everywhere locally over S, and so we can assume that S is affine, and $S = \operatorname{Spec} B$. Then, if suffices to check in a larger ring, so we let E be the ring obtained from inverting all the non-zero divisors in $B[x,y]$.

We have that $B[x,y] \subset E$. We see that x is not a zero divisor in $B[x,y]$, because $xg = 0$ implies that the leading coefficient of g is 0. We consider $G(t_1,t_2) = F(xt_1, yt_1 + \frac{1}{x}t_2)$. This is a binary n-ic form in variables t_i with coefficients in E. Over E we see it is a $\mathrm{GL}_2(E)$ transformation of f. We have that $G(1,0) = F(x,y)$, and thus f is the leading coefficient of the new form. However, f has an inverse in E and thus is not a zero divisor. By the GL_2 invariance of our constructions, we can reduce to checking in the case where f_0 is not a zero divisor. In this case we can prove Proposition 5.3.3 just as in the case of $\mathbb{Z}$. $\square$

In fact, we can consider a completely general binary n-ic form over S given by a locally free rank 2 $\mathcal{O}_S$-module V, a locally free rank 1 $\mathcal{O}_S$-module L, and a global section $f \in \operatorname{Sym}^n V \otimes L$. We can define R_f and I_f in this case as well. We define I_f to be $\mathcal{I}_{f_{n-3}} \otimes (\wedge^2 V)^{\otimes 2} \otimes L$ in the notation of Section 3.2. Then we have a natural map $I_f \to V^* \otimes \wedge^2 V \cong V$. We say a form f is a *zero-divisor* if it is a zero divisor on any open $\mathcal{U}$ of S on which V and L are free (and in this case the notion of zero-divisor is defined above). We now consider $A \in V \otimes U \otimes W$, where U and W are locally free rank n $\mathcal{O}_S$-modules with an orientation isomorphism $\wedge^n U \otimes \wedge^n W \cong L$. An isomorphism between $A \in V \otimes U \otimes W$ and $A' \in V \otimes U' \otimes W'$ is given by isomorphisms $U \cong U'$ and $W \cong W'$ that take A to A' and respect the orientations. We can still define the determinant of A in $\operatorname{Sym}^n V \otimes L$. We write W^* to denote $\mathcal{H}om(W, \mathcal{O}_S)$.

Definition. A *balanced pair of modules* for a non-zero divisor f is a pair of R_f-modules M and N, each a locally free rank n $\mathcal{O}_S$-module such that $\wedge^n M \otimes \wedge^n N \cong L^*$, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathcal{O}_S} N \to M \otimes_{R_f} N \to I_f \to V$ is written as $A \in M^* \otimes N^* \otimes V$ we have $\det(A) = fu$, where u is a unit in $\mathcal{O}_S$. When f is a non-zero divisor, given that $\wedge^n M \otimes \wedge^n N \cong L^*$, there is a unique choice of isomorphism so that $\det(A) = f$ and not some other multiple of f.

Theorem 5.6.2. *For every non-zero divisor binary n-ic form $f \in \operatorname{Sym}^n V \otimes L$, there is a bijection*

$$\left\{\begin{array}{l}\textit{isomorphism classes of balanced}\\ \textit{pairs } (M,N) \textit{ of modules for } f\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } A \in V \otimes\\ U \otimes W\textit{, where } U \textit{ and } W \textit{ are lo-}\\ \textit{cally free rank } n \textit{ } \mathcal{O}_S\textit{-modules with}\\ \textit{an orientation isomorphism } \wedge^n U \otimes\\ \wedge^n W \cong L\textit{, and } \det(A) = f\end{array}\right\}.$$

Proof. From A, we can construct R_f modules from U^* and W^* by giving the R_f action locally where U and W are free and we can chose bases, and then seeing that it is invariant under change of basis by elements of $\mathrm{GL}_n \times \mathrm{GL}_n$ that preserve the orientation. Similarly, we can construct the balancing map. Again, the construction of A from a balanced pair of modules just combines the balancing map with $I_f \to V$. To see that these constructions are inverse, it suffices to check locally on S, where we can assume V, U, and W are free. □

As when working over $\mathbb{Z}$, we can also get a version on the theorem for symmetric tensors.

Definition. A *self balanced module* for a non-zero divisor f is an R_f-modules M, that is a locally free rank n $\mathcal{O}_S$-module and such that $(\wedge^n M)^{\otimes 2}$ is isomorphic to L^*, and a map of R_f-modules $M \otimes_{R_f} N \to I_f$, such that when the composition $M \otimes_{\mathcal{O}_S} N \to M \otimes_{R_f} N \to I_f \to V$ is written as $A \in M^* \otimes N^* \otimes V$ we have $\det(A) = fu$, where u is a unit in $\mathcal{O}_S$.

Theorem 5.6.3. *For every non-zero divisor binary n-ic form $f \in \operatorname{Sym}^n V \otimes L$, there is a bijection*

$$\left\{\begin{array}{l}\textit{isomorphism classes of self bal-}\\ \textit{anced modules } M \textit{ for } f\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } A \in V \otimes\\ \operatorname{Sym}_2 U, \textit{ where } U \textit{ is a locally free}\\ \textit{rank } n \ \mathcal{O}_S\textit{-module with an orien-}\\ \textit{tation isomorphism } (\wedge^n U)^{\otimes 2} \cong L,\\ \textit{and such that } \det(A) = f\end{array}\right\}.$$

5.7 Geometric construction

Just as we have in Chapter 3 both concrete and geometric constructions of R_f, I_f, and J_f, we can also give geometric constructions of the R_f-modules M and N that were constructed explicitly from a $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$ above. We will give only a geometric construction of the modules M and N in $\psi(A)$, and not another construction of the balancing map $M \otimes_{R_f} N \to I_f$.

Notation. When we have an a matrix $M \in \mathbb{Z}^m \otimes \mathbb{Z}^n$, we can multiply M by vectors in two ways. We can multiply M by a length m vector on the left, and we can multiply M by a length n column vector on the right. When we have an element $A \in \mathbb{Z}^\ell \otimes \mathbb{Z}^m \otimes \mathbb{Z}^n$, we can multiply it by vectors in three different ways, and we realize that the "on the left" and "on the right" descriptions do not generalize appropriately for three dimensional tensors. We will need a new language. An element $A \in \mathbb{Z}^\ell \otimes \mathbb{Z}^m \otimes \mathbb{Z}^n$ is comprised of entries a_{ijk}, with $1 \leq i \leq \ell$, $1 \leq j \leq m$, and $1 \leq k \leq n$. We say that a_{ijk} is the entry in the ith *aisle*, jth *row*, and kth *column*. Note that aisle, row, and column denote two dimensional submatrices, i.e. codimension one slices of A. For $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$, the n by n matrix we called A_i above is the ith aisle of A. If we have a sequence $x_1, \ldots, x_\ell$, we can form it into a vector and combine it with A to get the m by n matrix we call $A(x, \cdot, \cdot)$ with j, k entry $\sum_i a_{ijk} x_i$. The dots indicate that we have not also multiplied by vectors in the other situations. For example, for $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$, the matrix $A(x, \cdot, \cdot)$ is what we have previously referred to as $A_1 x_1 + A_2 x_2$. Similarly, if we have a sequence $y_1, \ldots, y_m$, we can form a $2 \times n$ array $A(\cdot, y, \cdot)$ with i, k entry $\sum_j a_{ijk} y_j$. We could call this array a matrix, but it is more convenient to continue to refer to its aisles and columns. If we have a sequence $z_1, \ldots, z_n$, we can form a $2 \times m$ array $A(\cdot, \cdot, z)$ with i, j entry (in the ith aisle and jth row) $\sum_\ell a_{ijk} z_k$. In fact, we will always use a x variable in the first place, y in the second place, and a z in the third place, and thus we will use the short hand $A(x)$ for $A(x, \cdot, \cdot)$ and $A(y)$ for $A(\cdot, y, \cdot)$. We may refer to the j, k entry of $A(x)$ by $A(x)_{j,k}$ and the i, k entry of $A(y)$ by $A(y)_{i,k}$. We can also multiply A by more than one vector at a time. For example, $A(x, y, \cdot)$ (denoted by $A(x, y)$ for short) is a length n vector with ℓth entry $\sum_i \sum_j a_{ijk} x_i y_j$.

Given a 2-dimensional array A with entries in some ring, we can form the ideal $\mathcal{M}(A)$ of the determinants of its maximal minors. For example, for $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^n \otimes \mathbb{Z}^n$, we have that $\mathcal{M}(A(x)) = (\det(A_1 x_1 + A_2 x_2))$. We have previously called the subscheme of $\mathbb{P}^1$ defined by this ideal $T_{\det(A_1 x_1 + A_2 x_2)}$. Now, in order to emphasize certain

symmetries, we say that $\mathcal{M}(A(x))$ defines a subscheme $T_{A(x)} \subset \mathbb{P}^1$. Analogously, we have a subscheme $T_{A(y)} \subset \mathbb{P}^{n-1}$ cut out by the determinants of 2×2 minors of $A(y)$.

The scheme $T_{A(y)}$ has line bundles $\mathcal{O}_{T_{A(y)}}(k)$ pulled back from $\mathcal{O}(k)$ on $\mathbb{P}^{n-1}_{\mathbb{Z}}$. Heuristically, we would like to say that R_f is the ring of global functions of $T_{A(y)}$ and then we would have an R_f-module $\Gamma(\mathcal{O}_{T_{A(y)}}(1))$. However, we have already defined R_f, and so it would have to be proven that $\Gamma(\mathcal{O}_{T_{A(y)}})$ gives the same ring, and this is not always the case. For example, when $A = 0$, we have that $\Gamma(\mathcal{O}_{T_{A(y)}}) = \mathbb{Z}$, not even a rank n-ring. This is the same sort of problem that arose in the construction of rings and ideal from binary forms (Chapter 3) that allows us to use our simple geometric construction of R_f as the global functions on $T_{A(x)}$ only under some hypothesis such as $f \neq 0$, and requires us to use a more complicated geometric construction in general. For more discussion about the obstacle of using the simple construction, see Chapter 3.

We can, however, use a simple geometric construction of modules from sufficiently general $2 \times n \times n$ tensors, including from the the universal tensor of these dimensions. As in Section 5.3.1, we work over the ring $\Lambda = \mathbb{Z}[u_{ijk}]$ and with the universal box $\mathcal{C}$ in $\Lambda^2 \otimes_\Lambda \Lambda^n \otimes_\Lambda \Lambda^n$ with i, j, k entry $u_{i,j,k}$. We have a binary n-ic form $c = \det(\mathcal{C}(x))$ with coefficients in Λ.

Theorem 5.7.1. *The Λ-algebra $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}})$ is isomorphic to R_c.*

Proof. Recall that $R_c = \Gamma(\mathcal{O}_{T_{\mathcal{C}(x)}})$ since c is not a zero-divisor (see Chapter 3). So we need to show that we have an isomorphism of Λ-algebras $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}) \cong \Gamma(\mathcal{O}_{T_{\mathcal{C}(x)}})$. We might expect that this would follow because we had an isomorphism of Λ-schemes $T_{\mathcal{C}(y)} \cong T_{\mathcal{C}(x)}$, but that is not the case. However, restricted to a large open subscheme of $\operatorname{Spec}\Lambda$, we do get such an isomorphism. Let S' be the open subscheme of $S = \operatorname{Spec}\Lambda$ that is the complement of the closed subscheme Z (defined below). Let $T'_{\mathcal{C}(y)} = T_{\mathcal{C}(y)} \otimes_S S'$, which is an open subscheme of $T_{\mathcal{C}(y)}$. Similarly, let $T'_{\mathcal{C}(x)} = T_{\mathcal{C}(x)} \otimes_S S'$, which is an open subscheme of $T_{\mathcal{C}(x)}$. We will show in Lemma 5.7.6 that we have an isomorphism of S'-schemes $T'_{\mathcal{C}(y)} \cong T'_{\mathcal{C}(x)}$.

The subscheme Z of S will correspond to boxes that are very degenerate. Thus we can think of the box $\mathcal{C} \otimes_S S'$ over S' as the universal "not too degenerate" box. The $n-1$ minors of $\mathcal{C}(x)$ form a matrix $W(\{x_1^{n-1}, x_1^{n-2}x_2, \ldots, x_2^{n-1}\}, \cdot, \cdot)$. The i, j, k entry of $W \in \Lambda^n \otimes \Lambda^n \otimes \Lambda^n$ is $(-1)^{j+k}$ times the $x_1^{n-i}x_2^{i-1}$ coefficient of the determinant of the submatrix of $\mathcal{C}(x)$ obtained by deleting the jth row and kth column. We can form $\det(W(y))$, a degree n polynomial in the y_i, and form the ideal $\mathfrak{w}$ of Λ of its coefficients, with d_i the coefficient of y_i^n. If we do the analogous construction, starting with $\mathcal{C}(y)$, we see that the next-to-maximal minors of $\mathcal{C}(y)$ are the entries themselves. Then we can form $\det(\mathcal{C}(x)) = c$, and form the ideal $(c_0, \ldots, c_n)$ of its coefficients. Let Z be the subscheme of $S = \operatorname{Spec}\Lambda$ defined by the ideal $(c_0, \ldots, c_n)\mathfrak{w}$.

We will prove the theorem with the following lemmas.

Lemma 5.7.2. *The codimension of Z in S is at least 2.*

Proof. Suppose for the sake of contradiction that Z is codimension 1. Then either the subscheme of S defined by $(c_0, \ldots, c_n)$ or the subscheme defined by $\mathfrak{w}$ must be codimension 1 and thus given by a principal ideal. However, we note that c_0 and c_n

are expressions is disjoint sets of the u_{ijk}. In fact, c_0 only involves the u_{1jk} and c_n the u_{2jk}. Thus c_0 and c_n have no nontrivial divisor in the UFD Λ, and the subscheme cut out by $(c_0, \ldots, c_n)$ cannot be codimension 1. Similarly, d_j does not involve any u_{**j}. Thus a common divisor of $d_1, \ldots, d_n$ must be trivial, and so the subscheme cut out by $(d_1, \ldots, d_n)$ cannot be codimension 1. We conclude the subscheme cut out by $\mathfrak{w}$, which is contained in the subscheme cut out by $(d_1, \ldots, d_n)$, cannot be codimension 1. □

Lemma 5.7.3. *We have that the restriction map $\Gamma(\mathcal{O}_S) \to \Gamma(\mathcal{O}_{S'})$ is an isomorphism and thus $\Gamma(\mathcal{O}_{S'})$ is naturally isomorphic to Λ.*

Proof. Since S is normal and locally Noetherian, and Z is codimension at least 2, this is a basic fact in algebraic geometry. □

From this lemma we conclude that $\Gamma(\mathcal{O}_{T'_{\mathcal{C}(x)}})$ and $\Gamma(\mathcal{O}_{T'_{\mathcal{C}(y)}})$ are Λ-algebras.

Lemma 5.7.4. *The restriction map $\Gamma(\mathcal{O}_{T_{\mathcal{C}(x)}}) \to \Gamma(\mathcal{O}_{T'_{\mathcal{C}(x)}})$ is an isomorphism of Λ-algebras.*

Proof. Let $\pi : T_{\mathcal{C}(x)} \to S$. We will see in Theorem 5.8.4 that the sheaf $\pi_*(\mathcal{O}_{T_{\mathcal{C}(x)}})$ is locally free on S. We will show that $\pi_*(\mathcal{O}_{T_{\mathcal{C}(x)}})$ is isomorphic to the pushforward of $\pi_*(\mathcal{O}_{T'_{\mathcal{C}(x)}})$ to S, and then taking global sections will prove the lemma. We cover S with opens $\mathcal{U}_i$ that trivialize $\pi_*(\mathcal{O}_{T_{\mathcal{C}(x)}})$. Since S is irreducible, $\mathcal{U}_i$ is the same dimension as S. On each $\mathcal{U}_i$, we then have that $\mathcal{U}_i \cap Z$ is at least codimension 2 in $\mathcal{U}_i$. Thus, on $\mathcal{U}_i$, the sheaf $\pi_*(\mathcal{O}_{T_{\mathcal{C}(x)}})$ is isomorphic to $\mathcal{O}_S^{\oplus n}$, for which the restriction map to S' is an isomorphism by Lemma 5.7.3. This means that restricted to $\mathcal{U}_i$, we have that $\pi_*(\mathcal{O}_{T_{\mathcal{C}(x)}})$ is isomorphic to the pushforward of $\pi_*(\mathcal{O}_{T'_{\mathcal{C}(x)}})$ to S. □

Lemma 5.7.5. *The restriction map $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}) \to \Gamma(\mathcal{O}_{T'_{\mathcal{C}(y)}})$ is an isomorphism of Λ-algebras.*

Proof. The sheaf $\pi_*(\mathcal{O}_{T_{\mathcal{C}(y)}})$ is locally free on S by Theorem 5.8.4. We then use the same argument as in Lemma 5.7.4. □

Lemma 5.7.6. *We have an isomorphism of S'-schemes $T'_{\mathcal{C}(y)} \cong T'_{\mathcal{C}(x)}$.*

Proof. The idea is that we can define a correspondence between points of $T'_{\mathcal{C}(y)}$ and $T'_{\mathcal{C}(x)}$ by $\mathcal{C}(x, y) = 0$. For points in $T'_{\mathcal{C}(x)}$, we have $\det(\mathcal{C}(x)) = 0$, and thus there should be some values of y_j such that $\mathcal{C}(x, y) = 0$. For these y_j, we have that $\mathcal{C}(y)$ sends a non-trivial vector x to 0, and thus is rank 1. Conversely, for points in $T'_{\mathcal{C}(y)}$, we have that $\mathcal{C}(y)$ is rank 1, and thus should send a non-trivial vector x to zero, and $\mathcal{C}(x, y) = 0$ implies that $\mathcal{C}(x)$ has determinant zero. The first difficultly in making this idea rigorous is that the correspondence is only a bijection when $\mathcal{C}$ is sufficiently non-degenerate, which is why we have had to restrict to the base S'. Over S', we can use the above argument to get a bijection of field valued points of $T'_{\mathcal{C}(y)}$ and $T'_{\mathcal{C}(x)}$. Below, we must work a bit harder to get an actual isomorphism of schemes, as well as to see that the boxes parametrized by S' are in fact sufficiently non-degenerate.

First we give a map $T'_{\mathcal{C}(y)} \to T'_{\mathcal{C}(x)}$. We will give maps from open sets of $T'_{\mathcal{C}(y)}$ to $\mathbb{P}^1_{S'}$. We will then show that the open sets cover $T'_{\mathcal{C}(y)}$. We will then show that these maps agree on overlaps, and finally we will show that the image lands in $T'_{\mathcal{C}(x)}$. Given an $1 \leq i \leq n$, we map $T'_{\mathcal{C}(y)}$ to $\mathbb{P}^1_{S'}$ via $x_1 = -\sum_j u_{2jk}y_j$ and $x_2 = \sum_j u_{1jk}y_j$, which we can do on the open set $E_k \subset T'_{\mathcal{C}(y)}$ defined as the complement of the ideal $(\sum_j u_{1jk}y_j, \sum_j u_{2jk}y_j)$. Note that $\sum_j u_{ijk}y_j$ is the i,k entry of $\mathcal{C}(y)$, or of the next-to-maximal minor of $\mathcal{C}(y)$. Suppose there was a point of $T'_{\mathcal{C}(y)}$ not in any E_k. If we write y for the vector of the y_j's, then at this point we have $\mathcal{C}(y) = 0$, i.e. $\mathcal{C}_1(y) = 0$ and $\mathcal{C}_2(y) = 0$, and thus for formal x_i, we have $\mathcal{C}(x, y) = 0$, and thus $\det(\mathcal{C}(x)) = 0$ at this point, which contradicts our choice of S' to be in the complement of $(c_0, \ldots, c_n)$.

The fact that these maps agree on the intersection of E_k and E_ℓ is exactly given by the fact that on $T'_{\mathcal{C}(y)}$ the 2×2 minor of $\mathcal{C}(y)$ including rows k and ℓ is 0. To see that the image of our map lands in $T'_{\mathcal{C}(x)}$, we check on open P_i of $T'_{\mathcal{C}(y)}$, where y_i is non-zero. We have that $\mathcal{C}(x)$ on E_ℓ has j,k entry $-u_{1,j,k}\sum_a a_{2a\ell}y_a + u_{2,j,k}\sum_a a_{1a\ell}y_a$, and thus $\mathcal{C}(x, y)$ has kth entry

$$\begin{aligned}
&\sum_j y_j \left(-u_{1,j,k} \sum_a u_{2a\ell}y_a + u_{2,j,k} \sum_a u_{1a\ell}y_a \right) \\
=&\sum_j -u_{1,j,k}y_j \sum_a u_{2a\ell}y_a + \sum_j u_{2,j,k}y_j \sum_a u_{1a\ell}y_a \\
=&-\mathcal{C}(y)_{1,k}\mathcal{C}(y)_{2,\ell} + \mathcal{C}(y)_{2,k}\mathcal{C}(y)_{1,\ell},
\end{aligned}$$

which is zero by the definition of $T'_{\mathcal{C}(y)}$. On P_i we form the column vector y/y_i of regular functions, with jth entry y_j/y_i, and we see that $\mathcal{C}(x, y/y_i) = 0$. Thus we can write the ith row of $\mathcal{C}(x)$ as a linear combination of the other rows, and conclude that $\det(\mathcal{C}(x)) = 0$.

Next, we will give a map $T'_{\mathcal{C}(x)} \to T'_{\mathcal{C}(y)}$, which should be seen in analogy to the map $T'_{\mathcal{C}(y)} \to T'_{\mathcal{C}(x)}$. We will give maps from open sets of $T'_{\mathcal{C}(x)}$ to $\mathbb{P}^{n-1}_{S'}$, and show that the open sets cover $T'_{\mathcal{C}(y)}$. We will then show that these maps agree on overlaps, and finally we will show that the image lands in $T'_{\mathcal{C}(x)}$. Given an $1 \leq i \leq n$, we map $T'_{\mathcal{C}(x)}$ to $\mathbb{P}^{n-1}_{S'}$ by letting y_j equal the j,k minor of $\mathcal{C}(x)$, that is y_j equals $(-1)^{j+k}$ times the determinant of the submatrix of $\mathcal{C}(x)$ obtained by deleting the jth row and kth column. We have defined the y_j's to be a column of minors of $\mathcal{C}(x)$. This is a well-defined map to $\mathbb{P}^{n-1}$ on the open set $F_k \subset T'_{\mathcal{C}(x)}$ defined as the complement of the ideal of $n-1$ minors of $\mathcal{C}(x)$ for the kth column. Suppose there was a point of $T'_{\mathcal{C}(x)}$ not in any F_k, then at this point we have all minors of $\mathcal{C}(x)$ are 0. This means that $W(\{x_1^{n-1}, x_1^{n-2}x_2, \ldots, x_2^{n-1}\}, \cdot, \cdot) = 0$. Thus for formal y, we have $W(\cdot, y, \cdot)$ has a non-trivial kernel and thus $\det(W(y)) = 0$, which contradicts our choice of S' to be in the complement of $\mathfrak{w}$.

The fact that these maps agree on the intersection of F_k and F_ℓ is exactly given by the fact that the 2×2 minors of the classical adjoint matrix are divisible by the determinant of the original matrix. To see that the image of our map lands in $T'_{\mathcal{C}(y)}$, we check on opens P_i of $T'_{\mathcal{C}(x)}$, where x_i is non-zero. On P_i we form the column vector

x/x_i of regular functions, with jth entry x_j/x_i. Computing $\mathcal{C}(x,y)_\ell$ with the y_i's we have defined on F_k is the same as computing the determinant of $\mathcal{C}(x)$ with the kth column replaced by the ℓth column. Whether or not $k=\ell$, since $\det(\mathcal{C}(x))=0$, we obtain $\mathcal{C}(x,y)_\ell = 0$. Thus, $\mathcal{C}(x/x_i,y)=0$ and we can write the ith aisle of $\mathcal{C}(y)$ as multiple of the other aisle. We conclude that $\mathcal{C}(y)$ has all 2 by 2 minors 0.

Now we need to check that the maps we have just given are inverses one one another. We first check on the inverse image of E_k in F_ℓ. Here we start with x_i, we define new y_j, and then from the y_j we define new x_i'. We will compute $-x_1'x_2+x_2'x_1$. Since we have $x_1' = -\sum_j u_{2jk}y_j$ and $x_2' = \sum_j u_{1jk}y_j$, we have that

$$-x_1'x_2 + x_2'x_1 = \sum_j (u_{1jk}x_1 + u_{2jk}x_2)y_j.$$

We note that $u_{1jk}x_1 + u_{2jk}x_2 = \mathcal{C}(x)_{j,k}$, and that y_j is defined to be the j,ℓ minor of $\mathcal{C}(x)$. Thus $-x_1'x_2+x_2'x_1$ is the determinant of the matrix obtained from $\mathcal{C}(x)$ by replacing the ℓth column by the kth column, and is zero in any case on $T_{\mathcal{C}(x)}$. This shows that our maps compose to the identity on the inverse image of E_k in F_ℓ for all k and ℓ, and thus on $T_{\mathcal{C}(x)}$.

We now check on the inverse image of F_k in E_ℓ. Here we start with y_j, we define new x_i, and then from the x_i we define new y_j'. At first, we will use formal y_j (i.e. not assuming the relation in $T_{\mathcal{C}(y)}$). Then we will compute $y_j'y_m - y_m'y_j$ is in the ideal of relations $\mathcal{M}(\mathcal{C}(y))$ that cut out $T_{\mathcal{C}(y)}$. We can form an $n\times n$ matrix M with a,b entry $(-1)^a\mathcal{C}(x)_{a,b}y_a$ if $a=j,m$ and $\mathcal{C}(x)_{a,b}$ otherwise. Note that $(-1)^m y_j'y_m$ is the j,k minor of M and $(-1)^j y_j'y_m$ is the m,k minor of M. For any matrix N the difference of $(-1)^m$ times the j,k minor of N and $(-1)^j$ times the m,k minor of N is in the ideal generated by maximal minors of $\bar{N}$, which is obtained from N by deleting rows j and m and adding a row that is the jth row of N plus $(-1)^{j+m}$ times the mth row of N. The maximal minors of $\bar{M}$ are not changed if we add multiples of the original (non-deleted) rows of M to the new row of $\bar{M}$. We add $(-1)^j y_a$ times the original ath row of M to the new row of $\bar{M}$ to obtain $\bar{M}'$. The maximal minors of $\bar{M}'$ certainly lie in the ideal generated by the elements of its "new" row, and we claim these elements are in $\mathcal{M}(\mathcal{C}(y))$. In the bth column, the element in the new row of $\bar{M}'$ is is

$$\sum_{i,c} u_{icb}x_iy_c(-1)^j = \sum_{i,c,a}(-1)^{i+j}u_{icb}u_{(3-i)a\ell}y_ay_c = \sum_i (-1)^{i+j}\mathcal{C}(y)_{i,b}\mathcal{C}(y)_{3-i,\ell},$$

which is the b,ℓ minor of $\mathcal{C}(y)$ and thus in $\mathcal{M}(\mathcal{C}(y))$. This shows that our maps compose to the identity on $T_{\mathcal{C}(x)}$. □

Thus it follows that we have an isomorphism of Λ-algebras $R_c = \Gamma(\mathcal{O}_{T_{\mathcal{C}(x)}}) \cong \Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}})$. □

From Theorem 5.7.1, we have an R_c-module structure on $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}(1))$. We now see that it is related to the module $M_{\mathcal{C}}$ we constructed in Section 5.3.1 from the universal tensor.

Theorem 5.7.7. *We have an isomorphism of R_c-modules*

$$\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}(1)) \cong \mathcal{H}om_\Lambda(M_\mathcal{C}, \Lambda),$$

where $M_\mathcal{C}$ is as in the construction ψ of two R_c modules $M_\mathcal{C}$ and $N_\mathcal{C}$ given in Section 5.3.1.

Proof. We will see in Theorem 5.8.4 that $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}(1))$ is a free Λ-module with basis $y_1, \ldots, y_n$. Thus, it just suffices to check that the ζ_i acts on the y_j in a way corresponding to their action on $M_\mathcal{C}$. We know that ζ_i acts on the y_j by a matrix of elements of Λ, and thus it suffices to determine this action over the generic point of $\operatorname{Spec}\Lambda$, i.e. the fraction field of Λ. We have that $\mathcal{C}(x, y) = 0$ and thus $y\mathcal{C}_1 x_1 + y\mathcal{C}_2 x_2 = 0$, where y is a row vector of the y_i. Thus, where x_2 is invertible, $\frac{x_1}{x_2}$ acts like $-\mathcal{C}_2\mathcal{C}_1^{-1}$ on the right on the row vector y, and where x_1 is invertible, $\frac{x_2}{x_1}$ acts like $-\mathcal{C}_1\mathcal{C}_2^{-1}$ on the right on the row vector y. Thus $\frac{x_1}{x_2}$ acts like $-\mathcal{C}_2\mathcal{C}_1^{-1}$ on the left on elements of $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}(1))$ written as row vectors whose entries are the coefficients of the y_i in the element. We have that θ acts in elements of $M_\mathcal{C}$ by $(-\mathcal{C}_2\mathcal{C}_1^{-1})^t$ on the left. Since in the correspondence between the algebraic and geometric construction on R_c we have that θ corresponds to $\frac{x_1}{x_2}$, we see that the ζ_i act on $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}(1))$ as they act on $\mathcal{H}om_\Lambda(M_\mathcal{C}, \Lambda)$. □

We can of course get a completely analogous geometric construction of $N_\mathcal{C}$ as $\mathcal{H}om_\Lambda(\Gamma(\mathcal{O}_{T_{\mathcal{C}(z)}}(1)), \Lambda)$.

5.8 Geometric construction over an arbitrary base scheme

Notation. Given a scheme S and a locally free $\mathcal{O}_S$-module U, we let U^* denote the $\mathcal{O}_S$-module $\mathcal{H}\mathrm{om}_{\mathcal{O}_S}(U, \mathcal{O}_S)$, even if U is also a module for another sheaf of algebras.

Now we replace $\operatorname{Spec}\Lambda$ by an arbitrary scheme S, and we consider V, U, W, locally free $\mathcal{O}_S$-modules of ranks 2, n, and n, respectively. Let $p \in V \otimes U \otimes W$ denote a global section of $V \otimes U \otimes W$. We can construct $f = \det(p) \in \operatorname{Sym}^n V \wedge^n U \otimes \wedge^n W$. We have, in Section 5.6 constructed a balanced pair M, N of modules for f from p. In this section, we will give a geometric construction of those modules, or rather a geometric construction of M^* and N^* as we have done in the case of the universal form in Section 5.7.

As in Section 5.7, we can give a heuristic geometric construction that will work in most cases. First, we define some basic constructions on vector bundles. If we have locally free $\mathcal{O}_S$-modules F and G, and $s \in F \otimes G$, then we can construct the k-minor $\wedge^k s \in \wedge^k F \otimes \wedge^k G$. If H is also a locally free $\mathcal{O}_S$-module, and we have $s \in F \otimes G \otimes H$, then we have a k-minor $\wedge^k_H s$ with H-coefficients in $\wedge^k F \otimes \wedge^k G \otimes \operatorname{Sym}^k H$. For $p \in V \otimes U \otimes W$, the n minor with coefficients in V defines a subscheme $T_p(V)$ in $\mathbb{P}(V)$, the 2 minor with coefficients in U defines a subscheme $T_p(U)$ in $\mathbb{P}(U)$, and

the 2 minor with coefficients in W defines a subscheme $T_p(W)$ in $\mathbb{P}(W)$. Abusing notation, we let π denote the map from all of these schemes to S. The *heuristic* definition of R_f is $\pi_*\mathcal{O}_{T_p(V)}$ (or $\pi_*\mathcal{O}_{T_p(U)}$ or $\pi_*\mathcal{O}_{T_p(W)}$), and we also have heuristic definitions $M^* = \pi_*\mathcal{O}_{T_p(U)}(1)$ and $N^* = \pi_*\mathcal{O}_{T_p(W)}(1)$ (where $\mathcal{O}(1)$ is as pulled back from the corresponding projective bundle). This construction has the same problems and mentioned in Section 5.7. In particular, it does not work for $p = 0$ and it is not functorial in S.

We can, however, make a geometric construction of the modules M^* and N^* from $p \in V \otimes U \otimes W$ that will work for all p and be functorial in S, i.e. will commute with base change in S. On the universal box, this construction will agree with the heuristic geometric construction given just above and in Section 5.7, as well as with the algebraic construction given in Section 5.3.1.

The idea is to replace the schemes $T_p(V)$, $T_p(U)$, and $T_p(W)$ with complexes of sheaves. We will then replace π_* with the hypercohomology functors $H^0R\pi_*$. This has already been done for $T_p(V)$ in the construction of R_f and the module I_f in Chapter 3. We face some additional challenges in this chapter for $T_p(U)$ and $T_p(W)$. One can also interpret this work as a construction of dg-schemes $T_p(V)$, $T_p(U)$, and $T_p(W)$ instead of just a construction of schemes.

5.8.1 Arbitrary triple tensors

We now give a more general construction before specifying to the situation of interest in this chapter. Let S be an arbitrary scheme, and let $p \in V \otimes U \otimes W$, where U, V, W are locally free $\mathcal{O}_S$-modules of ranks r_U, r_V, and r_W respectively. Let $r = r_V$. We can view p as a map $W^* \to V \otimes U$, and take r_V minors of this map, with coefficients in U, to get $\wedge^r_U p : \wedge^r W^* \to \wedge^r V \otimes \operatorname{Sym}^r U$ or equivalently $\wedge^r_U p : \wedge^r W^* \otimes \wedge^r V^* \to \operatorname{Sym}^r U$.

Let $\pi : \mathbb{P}(U) \to S$ (where $\mathbb{P}(U) = \operatorname{Proj} \operatorname{Sym}^* U$). Let $\mathcal{O}(k)$ be the usual sheaf of $\mathbb{P}(U)$. Then since $\pi_*\mathcal{O}(r) = \operatorname{Sym}^r U$, by the adjointness of π_* and π^* we get a map

$$\wedge^r_U p : \pi^* \left(\wedge^r W^* \otimes \wedge^r V^*\right) \to \mathcal{O}(r)$$

or equivalently, for any k, we get

$$\wedge^r_U p : \pi^* \left(\wedge^r W^* \otimes \wedge^r V^*\right) \otimes_{\mathcal{O}_S} \mathcal{O}(k) \to \mathcal{O}(r+k).$$

It is an abuse of notation to call all these maps $\wedge^r_U p$, but it better than the alternative in which case we would run out of names for maps. Locally on S, where U, V, and W are free, the map $\wedge^r_U p : \pi^* \left(\wedge^r W^* \otimes \wedge^r V^*\right) \to \mathcal{O}(r)$ has image spanned by the $\binom{r_W}{r}$ r-by-r minors of the matrix of the map $W^* \to V \otimes U$, an r_V by r_W matrix with entries in U. The idea of our construction is to replace the sheaf $\mathcal{O}/\operatorname{im}(\wedge^r_U p)$ of regular functions of the subscheme of $\mathbb{P}(U)$ cut out by those r-by-r minors with complex that is generically a locally free resolution of the $\mathcal{O}/\operatorname{im}(\wedge^r_U p)$.

From the Eagon-Northcott complex, which resolves R modulo the ℓ by ℓ minors of a generic matrix (see [22]), we can construct a complex $\mathcal{C}(k)$ with $\mathcal{C}^{-1}(k) \to \mathcal{C}^0(k)$ given by

$$\wedge^r_U p : \pi^* \left(\wedge^r W^* \otimes \wedge^r V^*\right) \otimes_{\mathcal{O}_S} \mathcal{O}(k) \to \mathcal{O}(r+k),$$

and with $\mathcal{C}^i(k) = 0$ for $i > 0$ and $i \leq -|r_V - r_W| - 2$. For $-|r_V - r_W| - 1 \leq i \leq -2$, we have

$$\mathcal{C}^i(k) = \pi^*(\wedge^r V^* \otimes K_{-i}(r, W^*, V)) \otimes_{\mathcal{O}_S} \mathcal{O}(i + 1 + k),$$

where $K_{-i}(r, W^*, V)$ is the locally free $\mathcal{O}_S$-module built from V and W that is the ith term in the Eagon-Northcott complex for a map $\alpha : W^* \to V$ and d_i is canonically constructed from p (and explained in the next paragraph). Note that $K_{-i}(r, W^*, V)$ only depends on V and W and does not depend on α.

We now show how to construct the d_i. From the construction of the Eagon-Northcott complex, there is a map

$$\mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(W^*, V) \to \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(\wedge^r V^* \otimes K_{-i}(r, W^*, V), \wedge^r V^* \otimes K_{-i+1}(r, W^*, V))$$

that sends $\alpha \mapsto d_i$, where d_i is the map in the Eagon-Northcott complex for α. We can extend that linear map to

$$\mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(W^*, V) \otimes U \to \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(\wedge^r V^* \otimes K_{-i}(r, W^*, V), \wedge^r V^* \otimes K_{-i+1}(r, W^*, V)) \otimes_{\mathcal{O}_Y} U$$

to get the maps when there are coefficients. Let H_i be the $\mathcal{O}_Y$-module $\wedge^r V^* \otimes K_{-i}(r, W^*, V)$. We obtain $d_i : H_i \to H_{i+1} \otimes U$, or equivalently $d_i : H_i \otimes H_{i+1}^* \to U$. Using adjointness of π_* and π^*, this is equivalent to $d_i : \pi^*(H_i \otimes H_{i+1}^*) \to \mathcal{O}_U(1)$, which gives us $d_i : \pi^*(H_i) \otimes \mathcal{O}_U(i + 1 + k) \to \pi^*(H_{i+1}) \otimes \mathcal{O}_U(i + 2 + k)$.

The complex $\mathcal{C}(-r)$ of sheaves on $\mathbb{P}(U)$ has a homotopy-associative differential graded algebra structure from the homotopy-associative differential graded algebra structure on the Eagon-Northcott complex (which every resolution of a cyclic module has [11, Proposition 1.1]), and the complex $\mathcal{C}(-r + 1)$ is a differential graded module for $\mathcal{C}(-r)$. Now we make an important calculation about the cohomology of $\mathcal{C}(-r)$ and $\mathcal{C}(-r + 1)$.

Theorem 5.8.1. *Let $p \in V \otimes U \otimes W$, where U, V, W are locally free $\mathcal{O}_S$-modules of ranks r_U, r, and r_W respectively. Assume that $r \geq 2$ or that we have have either 1) $r_U = 2$ and $r = r_W$ or 2) both $r = 2$ and $r_U - r \geq |r - r_W|$. Then $R\pi_*\mathcal{C}(k)$ has no cohomology in any degree except 0 for $k = -r$ and $k = -r + 1$.*

Proof. Let $j \neq 0$, and we will compute that each term of the complex $\mathcal{C}(k)$ has trivial $R^j\pi_*$. By the projection formula, we can ignore the term that is pulled back from S. We have $R^j\pi_*$ of the ith term $i \leq -1$ of $\mathcal{C}(k)$, in the ith place, is $R^{j-i}\pi_*$ of $\mathcal{C}(k)^i$ viewed as a complex in the 0th place. We have that $R^{j-i}\pi_*\mathcal{O}(i + 1 + k) = 0$ unless either 1) $j = i$ and $i + 1 + k \geq 0$ or 2) $j - i = r_U - 1$ and $i + 1 + k \leq -r_U$. Since $i + 1 \leq 0$ and $k \leq -r + 1 \leq -1$, we can never have $i + 1 + k \geq 0$. We consider the two assumptions of the theorem in cases.

1. **Case I: $r = 2$ and $r_U - r \geq |r - r_W|$.** In this case, we have $i + 1 + k \geq -|r - r_W| + k \geq -|r - r_W| - r \geq -r_U$ and thus we can only have $i + 1 + k \leq -r_U$ if $i = -|r - r_W| - 1$, and $k = -r$, and $r_U - r = |r - r_W|$. However, that implies that $i = -r_U + 1$ and thus $j = 0$.

2. **Case II: $r_U = 2$ and $r = r_W$.** In this case, we only are considering $i = -1$, and thus $j - i = r_U - 1$ implies $j = 0$.

We now need to consider $R^j\pi_*$ of the 0th term of $\mathcal{C}(k)$ (for $j \neq 0$). We have that $R^j\pi_*\mathcal{O}(r+k) = 0$ unless 1)$j = 0$ and $r + k \geq 0$ or 2)$j = r_U - 1$ and $r + k \leq -r_U$. However, we are assuming $j \neq 0$ and $r + k \geq 0$, and thus this can never happen. Thus we conclude that for $k = -r$ and $k = -r + 1$, under our assumptions about r_U, r, and r_W, the complex $\mathcal{C}(k)$ has no cohomology in any degree except 0. □

Corollary 5.8.2. *Thus $\mathcal{R}_{\wedge^r_U p} = H^0 R\pi_*\mathcal{C}(-r)$ is a sheaf of algebras on S, and $\mathcal{I}_{\wedge^r_U p} = H^0 R\pi_*\mathcal{C}(-r+1)$ is a sheaf of $\mathcal{R}$-modules on S.*

Proof. Since $R\pi_*\mathcal{C}(-r)$ is equivalent to a single sheaf in degree 0, it has no non-trivial homotopies. Thus $H^0 R\pi_*\mathcal{C}(-r)$ has an $\mathcal{O}_S$-algebra structure that is associative on the nose. Since $\mathcal{C}(-r+1)$ is a module for $\mathcal{C}(-r)$, we have that $\mathcal{I}_{\wedge^r_U p} = H^0 R\pi_*\mathcal{C}(-r+1)$ is an $H^0 R\pi_*\mathcal{C}(-r)$-module. □

We can also view the construction of $\mathcal{R}_{\wedge^r_U p}$ as taking the pushforward of the regular functions on the dg-scheme given by our resolution of $\mathcal{O}/\operatorname{im}(\wedge^r_U p)$, instead of on the scheme cut out by $\wedge^r_U p$.

When p is the universal tensor (of any size), then the Eagon-Northcott complex, and thus $\mathcal{C}(k)$, is exact at every spot except the 0th. Thus, when p is the universal tensor, $\mathcal{C}(k)$ is quasi-isomorphic to $\mathcal{O}(k)/\operatorname{im}(\wedge^r_U p)$. The sheaf $\mathcal{O}(k)/\operatorname{im}(\wedge^r_U p)$ is supported on the scheme defined by the r-by-r minors in $\operatorname{im}(\wedge^r_U p)$, and is isomorphic on that scheme to the pullback of $\mathcal{O}(k)$ from $\mathbb{P}(U)$. Thus, when $\mathcal{C}$ is the universal tensor in $\Lambda^2 \otimes \Lambda^n \otimes \Lambda^n$, we have that $\mathcal{R}_{\wedge^r_U \mathcal{C}}$ is the sheaf of rings given by the global sections $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}})$ (as defined in Section 5.7), and $\mathcal{I}_{\wedge^r_U \mathcal{C}}$ is the $\mathcal{R}_{\wedge^r_U \mathcal{C}}$-module given by the global sections $\Gamma(\mathcal{O}_{T_{\mathcal{C}(y)}}(1))$.

Theorem 5.8.1 also allows us to see that the constructions of $\mathcal{R}_{\wedge^r_U p}$ and $\mathcal{I}_{\wedge^r_U p}$ commute with base change on S

Corollary 5.8.3. *Let $p \in V \otimes U \otimes W$, where U, V, W are locally free $\mathcal{O}_S$-modules of ranks r_U, r, and r_W respectively. Assume that $r \geq 2$ or that we have have either 1) $r_U = 2$ and $r = r_W$ or 2) both $r = 2$ and $r_U - r \geq |r - r_W|$. Then the constructions of $\mathcal{R}_{\wedge^r_U p}$ and $\mathcal{I}_{\wedge^r_U p}$ commute with base change. More precisely, let $\phi : S' \to S$ be a map of schemes. Let $p' \in \phi^*U \otimes \phi^*V \otimes \phi^*W$ be the pullback of p. Then the natural map from cohomology*

$$\mathcal{R}_{\wedge^r_U p} \otimes_{\mathcal{O}_S} \mathcal{O}_{S'} \to \mathcal{R}_{\wedge^r_{\phi^*U} p'}$$

is an isomorphism of $\mathcal{O}_{S'}$-algebras. Also, the natural map from cohomology

$$\mathcal{I}_{\wedge^r_U p} \otimes_{\mathcal{O}_S} \mathcal{O}_{S'} \to \mathcal{I}_{\wedge^r_{\phi^*U} p'}$$

is an isomorphism of $\mathcal{R}_{\wedge^r_{\phi^*U} p'}$-modules (where the $\mathcal{R}_{\wedge^r_{\phi^*U} p'}$-module structure on $\mathcal{I}_{\wedge^r_U p} \otimes_{\mathcal{O}_S} \mathcal{O}_{S'}$ comes from the $(\mathcal{R}_{\wedge^r_U p} \otimes_{\mathcal{O}_S} \mathcal{O}_{S'})$-module structure.

Proof. The key to this proof is to compute all cohomology of the pushforward of the complex $\mathcal{C}(k)$ for $k = -r$ and $k = -r + 1$. We already know from Theorem 5.8.1 that there is only cohomology in degree 0. Theorem 5.8.4 will tell us that $H^0 R\pi_*\mathcal{C}(k)$ is locally free for $k = -r$ and $k = -r + 1$. Thus since all $H^i R\pi_*(\mathcal{C}(k))$ are flat, by [26, Corollaire 6.9.9], we have that cohomology and base change commute. Note that the base change morphisms respect the algebra and module structures on $\mathcal{R}_{\wedge^r_U p}$ and $\mathcal{I}_{\wedge^r_U p}$, and thus since they are isomorphisms, they are algebra and module isomorphisms. □

5.8.2 $\mathcal{O}_S$-module structure of $\mathcal{R}_{\wedge^r_U p}$ and $\mathcal{I}_{\wedge^r_U p}$

Now we consider a base scheme S, and V, U, W locally free $\mathcal{O}_S$-modules of ranks 2, n, and n, respectively. In this case, we construct the $\mathcal{O}_S$-algebra and module pairs $\mathcal{R}_{\wedge^n_V p}$ and $\mathcal{I}_{\wedge^n_V p}$, $\mathcal{R}_{\wedge^2_U p}$ and $\mathcal{I}_{\wedge^2_U p}$, and $\mathcal{R}_{\wedge^2_W p}$ and $\mathcal{I}_{\wedge^2_W p}$. We will now find the $\mathcal{O}_S$-module structure of all of these constructions. This has already been done for the $\wedge^n_V p$ construction in Chapter 3, and so we consider here the $\wedge^2_U p$ (as the $\wedge^2_W p$ constructions will follow identically).

Theorem 5.8.4. *We have an exact sequence of $\mathcal{O}_S$-modules*

$$0 \to \mathcal{O}_S \to \mathcal{R}_{\wedge^2_U p} \to (\mathrm{Sym}^{n-2} V)^* \otimes \wedge^2 V^* \otimes \wedge^n W^* \otimes \wedge^n U^* \to 0,$$

and an $\mathcal{O}_S$-module isomorphism $\mathcal{I}_{\wedge^2_U p} \cong U$.

Proof. From Theorem 5.8.1, we know that for $k = -r$ and $k = -r+1$ $\mathcal{C}(k)$ has trivial $H^j R\pi_*$ for all $j \neq 0$, and all components $C(k)^i_i$ of the complex (the ith term of $C(k)$ sitting as a complex in the ith place) have $H^0 R\pi_*(C(k)^i_i) = 0$ except for possibly the two extremal terms $i = 0$ and $i = -n+1$. Thus, by the standard machinery of long exact sequences in cohomology, we have the exact sequences

$$0 \to H^0 R\pi_*(\mathcal{O}) \to \mathcal{R}_{\wedge^2_U p} \to H^{n-1} R\pi_*(\pi^*(\wedge^2 V^* \otimes K_{-n+1}(2, W^*, V)) \otimes_{\mathcal{O}_S} \mathcal{O}(-n)) \to 0$$

and

$$0 \to H^0 R\pi_*(\mathcal{O}) \to \mathcal{R}_{\wedge^2_U p} \to H^{n-1} R\pi_*(\pi^*(\wedge^2 V^* \otimes K_{-n+1}(2, W^*, V)) \otimes_{\mathcal{O}_S} \mathcal{O}(-n+1)) \to 0.$$

We see that

$$\begin{aligned} & H^{n-1} R\pi_*(\pi^*(\wedge^2 V^* \otimes K_{-n+1}(2, W^*, V)) \otimes_{\mathcal{O}_S} \mathcal{O}(-n)) \\ &= \wedge^2 V^* \otimes K_{-n+1}(2, W^*, V) \otimes_{\mathcal{O}_S} H^{n-1} R\pi_*(\mathcal{O}(-n)) \\ &= \wedge^2 V^* \otimes K_{-n+1}(2, W^*, V) \otimes_{\mathcal{O}_S} \wedge^n U^*. \end{aligned}$$

Since $K_{-n+1}(2, W^*, V) = (\mathrm{Sym}^{n-2} V)^* \otimes \wedge^n W^*$, we obtain the exact sequence desired. Also, note that $H^{n-1} R\pi_*(\mathcal{O}(-n+1)) = 0$. □

One naturally wonders whether the three $\mathcal{O}_S$-algebras constructed from a tensor $p \in V \otimes U \otimes W$ are isomorphic. In the case that V, U, and W are free, then p is a pull-back from the universal tensor, in which case we know the algebras are isomorphic from Theorem 5.7.1. If one checks that the algebra isomorphism given by Theorem 5.7.1 is canonical, that it doesn't depend on the choice of bases of V, U, and W, then that would show that the three $\mathcal{O}_S$-algebras constructed from a tensor $p \in V \otimes U \otimes W$ are all isomorphic because locally, V, U and W are free, and if the isomorphisms between algebras do not depend on the choice of bases, they will agree on overlaps. In fact, the constructions made in Lemma 5.7.6 to give the isomorphism of S'-schemes $T'_{\mathcal{C}(y)} \cong T'_{\mathcal{C}(x)}$ are all given by minors of matrices and in fact are canonical.

Chapter 6

Parametrizing quartic rings over an arbitrary base

6.1 Introduction

It has been known since the work of Delone and Faddeev [21] (see also [17], [24], and [6]) that cubic rings are parametrized by binary cubic forms. (A *cubic ring* is a ring whose additive structure is a free rank 3 $\mathbb{Z}$-module, and a *binary cubic form* is a polynomial $f = ax^3 + bx^2y + cxy^2 + dy^3$ with integral coefficients.) Cubic rings, up to isomorphism, are in natural bijection with $\mathrm{GL}_2(\mathbb{Z})$-classes of binary cubic forms (where $\mathrm{GL}_2(\mathbb{Z})$ acts by change of coordinates of x and y). If we prefer to think geometrically, a cubic ring is just a finite flat degree three cover of $\operatorname{Spec}\mathbb{Z}$. A parametrization similar to that of Delone and Faddeev [21] was proven by Miranda [32] for finite flat degree three covers of an irreducible scheme over an algebraically closed field of characteristic not 2 or 3. Though these correspondences were originally given by writing down a multiplication table for the cubic ring (or ring of global functions of the cubic cover), it is shown in Chapter 3 that when $f \neq 0$, the cubic ring corresponding to an integral binary cubic form is simply the ring of global functions of the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ cut out by f. (Casnati and Ekedahl [14] give this sort of geometric construction of finite flat degree three Gorenstein covers of an integral base scheme, and so in Chapter 3 we have also shown that their construction agrees with Miranda's.)

In this paper, we study quartic rings, or equivalently, finite flat degree four covers of a base scheme. Casnati and Ekedahl [13] parametrize finite flat degree four Gorenstein covers of an integral base scheme by global sections of certain locally free sheaves, with a codimension condition on the section at every point of the base. Casnati [14] also gives a construction of a finite flat degree three *discriminant cover* corresponding to a finite flat degree four Gorenstein cover of an integral scheme over an algebraically closed field of characteristic not equal to 2. Recently, quartic rings over $\mathbb{Z}$, or finite flat degree four covers of $\operatorname{Spec}\mathbb{Z}$, have been parametrized by Bhargava [6]. More precisely, isomorphism classes of pairs (Q, C), where Q is a quartic ring over $\mathbb{Z}$ and C is a resolvent ring of Q, are in natural bijection with $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$-

classes of pairs of integral ternary quadratic forms. Cubic resolvent rings will be defined in Section 6.3 as models of the classical cubic resolvent field of a quartic field. The definition will agree with the construction of Casnati in the cases studied in [14].

A pair of integral ternary quadratic forms can be represented by a pair of matrices (A, B), where

$$A = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \frac{a_{13}}{2} \\ \frac{a_{12}}{2} & a_{22} & \frac{a_{23}}{2} \\ \frac{a_{13}}{2} & \frac{a_{23}}{2} & a_{33} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & \frac{b_{12}}{2} & \frac{b_{13}}{2} \\ \frac{b_{12}}{2} & b_{22} & \frac{b_{23}}{2} \\ \frac{b_{13}}{2} & \frac{b_{23}}{2} & b_{33} \end{pmatrix}$$

with $a_{ij}, b_{ij} \in \mathbb{Z}$. Here A represents the form $\sum_{1 \le i \le j \le 3} a_{ij} x_i x_j$ and B represents $\sum_{1 \le i \le j \le 3} b_{ij} x_i x_j$. Then $\mathrm{GL}_3(\mathbb{Z})$ acts by conjugating the two matrices and $\mathrm{GL}_2(\mathbb{Z})$ acts on the pair by $\left(\begin{smallmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ sending (A, B) to $(g_{11}A + g_{12}B, g_{21}A + g_{22}B)$. Maximal quartic rings have a unique resolvent ring, and so at least for maximal rings, Bhargava's result can be seen as a parametrization of quartic rings over $\mathbb{Z}$.

Bhargava, in [6], describes the relationship between quartic rings with cubic resolvents and pairs of ternary quadratic forms by giving the multiplication tables for the quartic and cubic rings explicitly in terms of the coefficients of the forms. In this chapter, we give a geometric, coordinate-free description of a quartic ring Q given by a pair (A, B). For the nicest pairs (A, B), we have that A and B give a pencil of conics in $\mathbb{P}^2_{\mathbb{Z}}$ and the quartic ring is given by the global functions of the subscheme cut out by the pencil. Casnati and Ekedahl [13] give this construction in the case when the quartic ring is Gorenstein. Deligne, in a letter [20] to Bhargava, gives this construction when the generic conic in the pencil is non-singular (over each geometric point of $\operatorname{Spec} \mathbb{Z}$), and proves that it extends to all pairs of ternary quadratic forms. Our geometric description works for all pairs of ternary quadratic forms, and also explains what ring Q is even when it not given by the expected global functions, for example when all of the entries of A and B have a common factor, when the conics given by A and B share a component, or when A and B are both 0!

We prove that our geometric construction agrees with explicit description of Bhargava in [6] of a quartic ring Q given by formulas for a multiplication table with respect to basis elements of Q. Such a global geometric description (which works even when $f = 0$) has been given for rings from cubic forms in Chapter 3. In fact, Chapter 3 gives such a description of a ring from a binary form of any degree. As in the description of a ring from a binary cubic (or n-ic), the description of a quartic ring from a pair (A, B) uses hypercohomology, which is the cohomology of a complex of sheaves.

Our geometric construction of a quartic ring from a pair of ternary quadratic forms in fact works when $\mathbb{Z}$ is replaced by an arbitrary commutative base ring R, or even a scheme S. We prove that our geometric construction commutes with base change in the base scheme S. This allows us to give a parametrization of quartic rings (with cubic resolvents) over any scheme S, or in other words, determine the structure of the moduli stack of quartic rings with cubic resolvents.

Remark 6.1.1. Some of the geometric language of this chapter makes it more natural to work over a scheme S, but all of our work includes the case $S = \operatorname{Spec} R$, in which case we are simply working over a ring R. The reader mainly interested in a base ring can replace $\mathcal{O}_S$ with R and "global section" with "element" throughout the chapter.

The most important change from $\mathbb{Z}$ to a scheme S is that previously we considered quartic rings which were free rank 4 $\mathbb{Z}$-algebras, and a *quartic ring* Q over a scheme S is an $\mathcal{O}_S$-algebra such that $Q/\mathcal{O}_S$ is a locally free rank 3 $\mathcal{O}_S$-module (and in particular Q is a locally free rank 4 $\mathcal{O}_S$-module). Of course, over $\mathbb{Z}$ all locally free modules are free, and this definition over $\mathbb{Z}$ agrees with the earlier definition of a quartic ring. The forms we must consider change similarly. We could view a pair of ternary quadratic forms over $\mathbb{Z}$ as a single form $\sum_{1\le i\le j\le 3} a_{ij}x_ix_jy+\sum_{1\le i\le j\le 3} b_{ij}x_ix_jz$. Then we can view the $\mathrm{GL}_2(\mathbb{Z})$ action as a change of basis on the free $\mathbb{Z}$-module generated by y and z and the $\mathrm{GL}_3(\mathbb{Z})$ action as a change of basis on the free $\mathbb{Z}$-module generated by x_1, x_2, and x_3. We replace the free modules over $\mathbb{Z}$ with locally free modules over S and get the following definition. A *double ternary quadratic form* over S is a locally free rank 3 $\mathcal{O}_S$-module W, a locally free rank 2 $\mathcal{O}_S$-module U, and a global section $p \in \mathrm{Sym}^2 W \otimes U$, and an *orientation* isomorphism $\wedge^3 W \otimes \wedge^2 U \cong \mathcal{O}_S$. Certain double ternary quadratic forms are the objects that parametrize finite flat degree four Gorenstein covers of an integral base scheme in the work of Casnati and Ekedahl [13]. One reason to fix an orientation is so that double ternary quadratic forms won't have a GL_1 of automorphisms given by acting by $(\lambda^{-2}, \lambda) \in \mathrm{GL}_2 \times \mathrm{GL}_3$. The orientation is a phenomenon that it is hard to see over $\mathbb{Z}$ because $\mathrm{GL}_1(\mathbb{Z})$ is so small. An isomorphism of double ternary quadratic forms (W, U, p) and (W', U', p') is given by isomorphisms $W \cong W'$ and $U \cong U'$ that send p to p and respect the orientation. Since in this framework, we don't have a pair of anything, we change the terminology from "pair of" to "double," but a double ternary quadratic form over $\mathbb{Z}$ is the same as a pair of ternary quadratic forms over $\mathbb{Z}$. Moreover, isomorphism classes of double ternary quadratic forms over $\mathbb{Z}$ correspond exactly to $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$-classes of pairs of ternary quadratic forms over $\mathbb{Z}$. (More precisely, if Γ is the subgroup of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ of elements (g_1, g_2) such that $\det(g_1)\det(g_2) = 1$, then isomorphism classes of double ternary quadratic form over $\mathbb{Z}$ correspond exactly to Γ-classes of pairs of ternary quadratic forms over $\mathbb{Z}$. However, it turns out that since $-I \in \mathrm{GL}_3(\mathbb{Z})$ acts trivially on pairs of ternary quadratic forms, the Γ classes are the same as the $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ classes.

In Section 6.7, we prove the following theorem which generalizes the bijection [6, Theorem 1] from $\mathbb{Z}$ to an arbitrary base scheme and the bijection [13, Theorem 4.4] for finite flat degree four Gorenstein covers to all finite flat degree four covers with cubic resolvents and from an integral base scheme to an arbitrary base scheme.

Theorem 6.1.2. *Over a scheme S, there is a bijection between isomorphism classes of double ternary quadratic forms and pairs (Q, C) where Q is a quartic ring over S and C is a cubic resolvent of Q. This bijection is functorial in S. In other words, there is an isomorphism between the moduli stack of double ternary quadratic forms and the moduli stack of pairs (Q, C) where Q is a quartic ring and C is a cubic resolvent of Q.*

Resolvent rings are defined in Section 6.3; they are an analog over an arbitrary base of the classical cubic resolvent field of a quartic field.

This chapter gives two descriptions of the bijection in Theorem 6.1.2. In Section 6.4 we give a global, geometric, coordinate free description of (Q, C) from a

double ternary quadratic form, which in the nicest cases over a ring R says that Q is the global functions of the scheme cut out by the form. In Section 6.5, we give an explicit local description of (Q, C) in terms of bases and multiplication tables. Once Q and C have the correct module structure, the local multiplication tables can be read off from the formulas given in Bhargava's work [6].

The key idea in this chapter is the geometric construction over arbitrary base of a quartic ring from a double ternary quadratic form in Section 6.4. The geometric construction we give is similar to, but more complicated than, the construction of a rank n-ring from a binary n-ic form in Chapter 3. A binary n-ic form over S cuts out a subscheme of $\mathbb{P}^1_S$ and we can usually take the pushforward of the regular functions on that subscheme to be our rank n ring over S. To obtain a construction that works in all cases and is functorial in the base, we instead had to take the 0th hypercohomology of a complex given by the binary n-ic form. In fact, it was the Kozul complex, though since it only had two terms it was too simple to recognize as such. In general, a double ternary quadratic form, locally on the base, gives two conics in $\mathbb{P}^2$ which intersect to give a subscheme of $\mathbb{P}^2$. We wish, heuristically, to take the ring of regular functions of this subscheme. As in the case of binary n-ic forms, to get a construction that works in all cases and is functorial in the base, we take the 0th hypercohomology of the Kozul complex given by the double ternary quadratic form. This always gives a quartic algebra over the base.

In Section 6.2, we review the theorems about binary cubic rings over $\mathbb{Z}$ and an arbitrary base. This is not only motivation for our study of quartic rings, but also is important background for the results in this chapter because the resolvent C of a quartic ring Q is a cubic ring. In Section 6.3 we give the definition of a general cubic resolvent ring. In Section 6.6, we give the construction of a cubic resolvent ring from a double ternary quadratic form.

Notation. If $\mathcal{F}$ is a sheaf, we use $s \in \mathcal{F}$ to denote that s is a global section of $\mathcal{F}$. If V is a locally free $\mathcal{O}_S$-module, we use V^* to denote the $\mathcal{O}_S$-module $\mathcal{H}om_{\mathcal{O}_S}(V, \mathcal{O}_S)$. We use $\operatorname{Sym}^n V$ to denote the usual quotient of $V^{\otimes n}$, and $\operatorname{Sym}_n V$ to denote the submodule of symmetric elements of $V^{\otimes n}$.

Normally, in the language of algebra, one says that an R-module M is locally free of rank n if for all prime ideals $\wp$ of R, the localization $M_\wp$ is free of rank n. However, if we have a scheme S and an $\mathcal{O}_S$-module M, we normally say that M is locally free of rank n if on some open cover of S it is free of rank n; in the algebraic language this is equivalent to saying that for every prime ideal $\wp$ of R, there is an $f \in R \setminus \wp$ such that the localization M_f is free of rank n. In this thesis we shall use the geometric sense of the term *locally free of rank n*. The geometric condition of locally free of rank n is equivalent to being finitely generated and having the algebraic condition of locally free of rank n.

6.2 The parametrization of cubic rings

In this section, we review the parametrization of cubic rings. Over $\mathbb{Z}$, this was first worked out in [21] (see also [17] and [24]).

Given a base scheme S, a *cubic ring* C over S is a $\mathcal{O}_S$-algebra such that $C/\mathcal{O}_S$ is a locally free rank 2 $\mathcal{O}_S$-module. A *binary cubic form* is a locally free rank 2 $\mathcal{O}_S$-module V and an element $f \in \mathrm{Sym}^3 V \otimes \wedge^2 V^*$, and an isomorphism of binary cubic forms $(V, f) \cong (V, f')$ is given by an isomorphism $V \cong V'$ that takes f to f'. (Normally, we would call these *twisted binary cubic forms* but since they are the only binary cubic forms in this chapter, we will use the shorter name for simplicity.) Of course, if V is the free rank 2 $\mathcal{O}_S$-module $\mathcal{O}_S x \oplus \mathcal{O}_S y$, then the binary cubic forms $f \in \mathrm{Sym}^3 V \otimes \wedge^2 V^*$ are just polynomials $(ax^3 + bx^2y + cxy^2 + dy^3) \otimes (x \wedge y)^*$, where $a, b, c, d \in \mathcal{O}_S$.

Over an arbitrary base, Deligne wrote a letter ([19]) to the authors of [24] giving the following theorem.

Theorem 6.2.1. *Over a scheme S, there is a bijection between isomorphism classes of binary cubic forms and cubic rings. This bijection is functorial in S. If a cubic ring C corresponds to a binary cubic form (V, f), then as $\mathcal{O}_S$-modules, we have $C/\mathcal{O}_S \cong V^*$.*

Miranda [32] also gives this bijection over a base which is an irreducible scheme over an algebraically closed field of characteristic not equal to 2 or 3. This bijection is studied and proven as part of a series of bijections involving binary forms of any degree in Chapter 3. We give a simple proof here for completeness.

Proof. Given a cubic ring C, we can define an $\mathcal{O}_S$-module $V = (C/\mathcal{O}_S)^*$. Then, where C is a free $\mathcal{O}_S$-module, we can choose a basis $1, \omega, \theta$ for C and then shift ω and θ by elements of $\mathcal{O}_S$ so that $\omega\theta \in \mathcal{O}_S$. Then, the associative law implies that we have a multiplication table

$$\begin{aligned} \omega\theta &= -ad \\ \omega^2 &= -ac + b\omega - a\theta \\ \theta^2 &= -bd + d\omega - c\theta, \end{aligned} \tag{6.1}$$

where $a, b, c, d \in \mathcal{O}_S$. Let x, y be the basis of V dual to ω, θ. Then we can define a form $(ax^3 + bx^2y + cxy^2 + dy^3) \otimes (x \wedge y)^* \in \mathrm{Sym}^3 V \otimes \wedge^2 V^*$. We can check that if we pick another basis $1, \omega', \theta'$ (also normalized so that $\omega'\theta' \in \mathcal{O}_S$) and another corresponding x' and y' we would define the same form in $\mathrm{Sym}^3 V \otimes \wedge^2 V^*$. Thus the form is defined everywhere locally in a way that agrees on overlapping open sets, and we have constructed a global binary cubic form (V, f). Deligne in [19] gives a different, geometric construction in the case when C is Gorenstein and then argues that the construction extends across the non-Gorenstein locus.

In [5, Footnote 3], the following algebraic, global, coordinate free description of the construction is mentioned. Given an algebra C, we can define an $\mathcal{O}_S$-module $V = (C/\mathcal{O}_S)^*$, and an $\mathcal{O}_S$-module homomorphism $\mathrm{Sym}_3 C/\mathcal{O}_S \to \wedge^2 C/\mathcal{O}_S$ given by $xyz \mapsto x \wedge yz$. One can check that this map is well-defined, and so it gives a binary cubic form $f \in (\mathrm{Sym}_3 C/\mathcal{O}_S)^* \otimes \wedge^2 C/\mathcal{O}_S \cong \mathrm{Sym}^3 V \otimes \wedge^2 V^*$.

On the other hand, given a binary cubic form (V, f), we can construct an $\mathcal{O}_S$-module $C = \mathcal{O}_S \oplus V^*$. Then, everywhere locally where V is free on basis x and y, we can write $f = (ax^3 + bx^2y + cxy^2 + dy^3) \otimes (x \wedge y)^*$ where $a, b, c, d \in \mathcal{O}_S$. If we let ω and θ be a dual basis to x, y, then we can locally give C a multiplication table by

$$\begin{aligned} \omega\theta &= -ad \\ \omega^2 &= -ac + b\omega - a\theta \\ \theta^2 &= -bd + d\omega - c\theta, \end{aligned} \tag{6.2}$$

and $(1, 0) \in \mathcal{O}_S \oplus V^*$ is the multiplicative identity. We can check that if we chose another basis for V and corresponding basis for C, we would get the same ring structure on C. Thus, C is defined as a cubic ring everywhere locally in a way that agrees on overlapping open sets, and we have constructed a global cubic ring C.

These contructions are clearly inverses and functorial in S. □

In this proof, we have given the construction of the bijection locally in terms of bases with explicit formulas. However, it is hard to see where the formula for the multiplication table came from or why the local constructions are invariant under change of basis. The following global description is given by Deligne in his letter [19], and in Chapter 3 it is shown that this description is same as the explicit description given in the proof above. Given a binary form $f \in \operatorname{Sym}^3 V \otimes \wedge^2 V^*$ over a base scheme S, the form f determines a subscheme S_f of $\mathbb{P}(V)$ (where we define $\mathbb{P}(V) = \operatorname{Proj} \operatorname{Sym}^* V$). Let $\pi : \mathbb{P}(V) \to S$. Let $\mathcal{O}(k)$ denote the usual sheaf on $\mathbb{P}(V)$ and $\mathcal{O}_{S_f}(k)$ denote the pullback of $\mathcal{O}(k)$ to S_f. Then we can define the $\mathcal{O}_S$-algebra by the hypercohomology

$$C := H^0 R\pi_* \left(\mathcal{O}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathcal{O} \right), \tag{6.3}$$

where $\mathcal{O}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathcal{O}$ is a complex in degrees -1 and 0. The product on C is given by the natural product of the complex $\mathcal{O}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathcal{O}$ with itself and the $\mathcal{O}_S$-algebra structure is induced from the map of $\mathcal{O}$ as a complex in degree 0 to the complex $\mathcal{O}(-3) \xrightarrow{f} \mathcal{O}$. (Note that $R^0\pi_*(\mathcal{O}) = \mathcal{O}_S$.)

Given a map of schemes $X \xrightarrow{\pi} S$, the construction of global functions of X relative to S is just the pushforward $\pi_*(\mathcal{O}_X)$. So the natural notion of global functions of S_f relative to S would be π_* of $\mathcal{O}_{S_f}$. We have that $\mathcal{O}_{S_f} = \mathcal{O}_S / f(\mathcal{O}(-3) \otimes \pi^* \wedge^2 V)$. When f is injective, then $\mathcal{O}_{S_f} = \mathcal{O}_S / f(\mathcal{O}(-3) \otimes \pi^* \wedge^2 V)$ as a complex in degree 0 is homotopy equivalent to $\mathcal{O}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathcal{O}$ as a complex in degrees -1 and 0. Thus we see when f is injective that C is just $\pi_*(\mathcal{O}_{S_f})$. When f gives an injective map and $S = \operatorname{Spec} R$ then C is just the ring of global functions of S_f. Unfortunately, this simpler construction does not give a cubic algebra where $f = 0$. When $f = 0$, then $S_f = \mathbb{P}^1$ and the global functions are a rank 1 $\mathcal{O}_S$-algebra, i.e. $\mathcal{O}_S$ itself. Hypercohomology is exactly the machinery we need to naturally extend our construction to all f.

6.3 Cubic resolvent rings

Bhargava discovered that to obtain a nice parametrization of quartic rings, one must parametrize them along with their cubic resolvent rings. One could also take a similar point of view on cubic rings, but it turns out that every cubic ring has a unique quadratic resolvent ring and so the parametrization does not change from the above. All quartic rings over $\mathbb{Z}$ have at least one cubic resolvent, and many quartic rings (e.g. maximal quartic rings over $\mathbb{Z}$) have a unique cubic resolvent.

We now give the definition of a cubic resolvent ring, given in [6, Definition 20] over $\mathbb{Z}$. The definition might seem complicated at first, but we will explain each aspect of it.

Definition. Given a quartic ring Q over a base scheme S, a cubic resolvent C of Q is

- a cubic ring C over S (i.e. an $\mathcal{O}_S$-algebra such that $C/\mathcal{O}_S$ is a locally free rank 2 $\mathcal{O}_S$-module)
- a quadratic map $\phi : Q/\mathcal{O}_S \to R/\mathcal{O}_S$, and
- an orientation isomorphism $\delta : \wedge^4 Q \cong \wedge^3 C$ (or equivalently $\bar{\delta} : \wedge^3 Q/\mathcal{O}_S \cong \wedge^2 C/\mathcal{O}_S$)

such that

1. for any open set $U \subset S$ and for all $x, y \in Q(U)$, we have $\delta(1 \wedge x \wedge y \wedge xy) = 1 \wedge \phi(x) \wedge \phi(y)$
2. R is the cubic ring corresponding to $\mathrm{Det}(\phi)$.

A *quadratic map* from A to B is given by an $\mathcal{O}_S$-module homomorphism $\mathrm{Sym}_2 A \to B$ evaluated on the diagonal (see the Appendix Section 6.8.1). (In Chapter 2 it is shown this is equivalent to the more classical notion of a quadratic map.) The map ϕ models the map from quartic fields to their resolvent fields given by $x \mapsto xx' + x''x'''$, where x, x', x'', x''' are the conjugates of an element x. In [6, Lemma 9] it is shown that condition 1 above holds for such classical resolvent maps, and it turns out that condition 1 is the key property of resolvent maps that allows them to be useful in the parametrization of quartic rings. So our definition of resolvent allows all quadratic maps that have this key property.

Another important property of the cubic resolvent over $\mathbb{Z}$ is that the discriminant of the cubic resolvent is equal to the discriminant of the quartic ring. In [6], this is a crucial part of the definition of a cubic resolvent over the integers. With the above formulation of the definition of a cubic resolvent, the equality of discriminants follows as a corollary of properties 1 and 2. However, since the discriminant of a ring R of rank n lies in $(\wedge^n R)^{\otimes -2}$, we need the orientation isomorphism to even state the question of the equality of discriminants.

The quadratic map ϕ is equivalent to a double ternary quadratic form in the module $\mathrm{Sym}^2(Q/\mathcal{O}_S)^* \otimes R/\mathcal{O}_S$. The determinant of a double ternary quadratic form is given by a natural cubic map from $\mathrm{Sym}^2 W \otimes V$ to $(\wedge^3 W)^{\otimes 2} \otimes \mathrm{Sym}^3 V$. We have a natural cubic determinant map from $\mathrm{Sym}^2 W$ to $(\wedge^3 W)^{\otimes 2}$. For free W and an element of $\mathrm{Sym}^2 W$ represented by the matrix

$$A = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \frac{a_{13}}{2} \\ \frac{a_{12}}{2} & a_{22} & \frac{a_{23}}{2} \\ \frac{a_{13}}{2} & \frac{a_{23}}{2} & a_{33} \end{pmatrix},$$

the map is given by the polynomial $4\,\mathrm{Det}(A)$, and since this is invariant under GL_3 change of basis, it defines a determinant map for all locally free W. We can extend to a cubic determinant map from $\mathrm{Sym}^2 W \otimes V$ to $(\wedge^3 W)^{\otimes 2} \otimes \mathrm{Sym}^3 V$ by using the elements of V as coefficients (see Appendix Section 6.8.2). Thus the determinant of ϕ lies in $(\wedge^3 Q/\mathcal{O}_S)^{\otimes -2} \otimes \mathrm{Sym}^3(C/\mathcal{O}_S)$, which is isomorphic to $(\wedge^2 C/\mathcal{O}_S) \otimes \mathrm{Sym}^3(C/\mathcal{O}_S)^*$ by the orientation isomorphism and Corollary 6.8.1 in the Appendix (Section 6.8).

When we speak of a pair (Q, C) of a quartic ring Q and a cubic resolvent C of Q, the maps ϕ and δ are implicit. An isomorphism of pairs is given by isomorphisms of the respective rings that respect ϕ and δ.

6.4 The geometric construction

In this section, we will construct a quartic ring from a double ternary quadratic form $p \in \mathrm{Sym}^2 W \otimes U$ over a base S. We consider the map $\pi : \mathbb{P}(W) \to S$, and the usual line bundles $\mathcal{O}(k)$ on $\mathbb{P}(W)$. We can view p as a two dimensional family of quadratic forms on $\mathbb{P}(W)$ (the two dimensions being given by U). More precisely, since p is equivalent to a map $U^* \to \mathrm{Sym}^2 W$, we get a naturally induced map $\pi^* U^* \to \mathcal{O}(2)$, which is equivalent to a map $p_1 : \pi^* U^* \otimes \mathcal{O}(-2) \to \mathcal{O}$. The image of p_1 is functions that are zero on the space cut out by the forms of p. The regular functions on the scheme cut out by p are just given by $\mathcal{O}/\operatorname{im}(p_1)$. From p we can construct one more map to make the Kozul complex of p, given as follows

$$\mathcal{K}_p : \quad \wedge^2 \pi^* U^* \otimes \mathcal{O}(-4) \xrightarrow{p_2} \pi^* U^* \otimes \mathcal{O}(-2) \xrightarrow{p_1} \mathcal{O}.$$

The complex $\mathcal{K}_p$ has $\mathcal{O}$ in the 0th place, and the other two terms in places -1 and -2. We can construct p_2 similarly to p_1 since p is also equivalent to a map $\wedge^2 U^* \otimes U \to \mathrm{Sym}^2 W$. (Recall $\wedge^2 U^* \otimes U \cong U^*$; see Lemma 3.7.4.) One can read about the construction of all the maps in the Kozul complex in [23, Appendix A2H]. For sufficiently generic p the Kozul complex will be exact in all places except the last and thus give a resolution of $\mathcal{O}/\operatorname{im}(p_1)$. For example, this it true when p is the universal double ternary quadratic form over the polynomial ring in twelve variables. In the sufficiently generic case, p will cut out four (relative) points in $\mathbb{P}(W)$ (i.e. a finite flat degree four S-scheme) and the pushforward of the global functions of those points will give us a quadratic algebra over the base S.

Example 6.4.1. *Suppose U is free with basis x, y, and dual basis $\dot{x}$ and $\dot{y}$. Then we can write $p = f_1 \otimes x + f_2 \otimes y$. The map p_1 just sends $\dot{x} \otimes g \mapsto f_1 g$ and $\dot{y} \otimes g \mapsto f_2 g$. We can write how p_1 acts on a general element as $a \otimes g \mapsto gp(a)$, where p acts on an element of U^* by evaluating the U components of p at the given element of U^*. The map p_2 sends $\dot{x} \wedge \dot{y} \otimes g \mapsto g f_1 \otimes \dot{y} - g f_2 \otimes \dot{x}$. We can write how p_2 acts on a general element as $a \wedge b \otimes g \mapsto b \otimes gp(a) - a \otimes gp(b)$. From this we see that $\mathcal{K}_p$ is a complex.*

When p is not so generic, for example in the extreme case where $p = 0$, then the forms given by p will not cut out four points and thus the functions on the corresponding subscheme will not pushforward to a quartic algebra. So instead of taking the pushforward of the global functions of the scheme cut out by p, we will take the 0th hypercohomology of the complex $\mathcal{K}_p$. We define Q_p to be $H^0 R\pi_*(\mathcal{K}_p)$, where $R\pi_*$ denotes the pushforward of the complex in the derived category. Alternatively, we can view the construction as the hypercohomological derived functor of π_*, where the hypercohomology is necessary since we are operating on a complex and not just a single sheaf. If p is sufficiently generic, then $\mathcal{K}_p$ will be homotopy equivalent to the complex $\mathcal{O}/\operatorname{im}(p_1)$ in degree 0 and Q_p will just be $\pi_*(\mathcal{O}/\operatorname{im}(p_1))$. However, what is nice about the hypercohomology construction is that Q_p will be a quartic algebra even when p is not sufficiently generic (as we'll see in Section 6.4.2). So far we have constructed Q_p as an $\mathcal{O}_S$-module, However, the Kozul complex has a natural differential graded algebra structure, and that gives the cohomology an inherited algebra structure. Thus Q_p is naturally an $\mathcal{O}_S$-algebra.

Theorem 6.4.2. *The construction of Q_p commutes with base change in S.*

Proof. To prove this theorem, we need to compute all of the cohomology of $\mathcal{K}_p$. The complex $\mathcal{K}_p$ has no cohomology in degrees other than 0. We have $R^k(\mathcal{O}(-4)) = 0$ for $k \neq 2$, and $R^k\pi_*(\mathcal{O}(-2)) = 0$ for all k, and $R^k\pi_*(\mathcal{O}) = 0$ for $k \neq 0$. Thus $H^k R\pi_*(\mathcal{K}_p) = 0$ for $k \neq 0$. In Section 6.4.2, we will see that $H^0 R\pi_*(\mathcal{K}_p)$ is locally free. Thus since all $H^i R\pi_*(\mathcal{K}_p)$ are flat, by [26, Corollaire 6.9.9], we have that cohomology and base change commute. □

6.4.1 Comparing the cohomological construction and global functions

When constructing the cubic ring from a binary cubic form, we took

$$H^0 R\pi_*(\mathcal{O}(-3) \xrightarrow{f} \mathcal{O})$$

on $\mathbb{P}(V)$, which, as long as the cubic form f gives an injective map above is the same as $\pi_*(\mathcal{O}/\operatorname{im} f)$. For example, when the base S is integral, whenever $f \neq 0$ then $\mathcal{O}(-3) \xrightarrow{f} \mathcal{O}$ is injective. However, when $f = 0$, of course $\mathcal{O}(-3) \xrightarrow{f} \mathcal{O}$ is not injective, and $H^0 R\pi_*(\mathcal{O}(-3) \xrightarrow{f} \mathcal{O})$ is not the same as $\pi_*(\mathcal{O}/\operatorname{im} f)$. When $f = 0$, the latter is an $\mathcal{O}_S$-module of rank 1.

Again, when constructing our quartic ring as $H^0 R\pi_*(\mathcal{K}_p)$, if $p = 0$ the complex will not be a resolution and $H^0 R\pi_*(\mathcal{K}_p)$ won't agree with $\pi_*(\mathcal{O}/\operatorname{im} p_1)$. This is the

case when both "conics" are given by the 0 form. However, even over an integral base, there are now more situations on which the complex $\mathcal{K}_p$ is not a resolution. The geometric constructions of Casnati and Ekedahl [13] and Deligne [20] for certain nice quartic rings are in the case when $\pi_*(\mathcal{O}/\operatorname{im} p_1)$ simply gives the quartic ring.

Recall the case where U is free, considered in Example 6.4.1, and for simplicity we consider W free as well. If f_1 and f_2 have some common linear factor ℓ, then $\dot{y} \otimes f_1/\ell - \dot{x} \otimes f_2/\ell \in \pi^*U^* \otimes \mathcal{O}(-2)$ goes to 0 under p_1, but it is not in the image of p_2. This is the case when both conics are a pair of lines and they share a common line. If $f_1 = 0$, then $\dot{x} \otimes g \in \pi^*U^* \otimes \mathcal{O}(-2)$ goes to 0 under p_1 even though it isn't necessarily in the image of p_2. This is the case when one "conic" is given by the zero form, or more generally the case where the two conics are the same. So, there are now several ways in which the complex $\mathcal{K}_p$ might not be a resolution, and therefore the algebra Q_p won't just be $\pi_*(\mathcal{O}/\operatorname{im} p_1)$.

6.4.2 Module structure of Q_p

In this section, we determine the $\mathcal{O}_S$-module structure of Q_p. We consider the short exact sequence of complexes $O \to \mathcal{A} \to \mathcal{K}_p \to \mathcal{D} \to 0$, where

$$\begin{aligned}
\mathcal{A}: &\qquad 0 \longrightarrow \pi^*U^* \otimes \mathcal{O}(-2) \xrightarrow{p_1} \mathcal{O} \\
\mathcal{K}_p: &\qquad \wedge^2\pi^*U^* \otimes \mathcal{O}(-4) \xrightarrow{p_2} \pi^*U^* \otimes \mathcal{O}(-2) \xrightarrow{p_1} \mathcal{O} \\
\mathcal{B}: &\qquad \wedge^2\pi^*U^* \otimes \mathcal{O}(-4) \longrightarrow 0 \longrightarrow 0.
\end{aligned}$$

From this short exact sequence we get a long exact sequence of hypercohomology sheaves on S, of which we consider the following part

$$H^{-1}R\pi_*(\mathcal{B}) \longrightarrow H^0R\pi_*(\mathcal{A}) \longrightarrow \underset{\underset{Q_p}{\|}}{H^0R\pi_*(\mathcal{K}_p)} \longrightarrow H^0R\pi_*(\mathcal{B}) \longrightarrow H^1R\pi_*(\mathcal{A}).$$

This sequence will allow us the determine the modules structure of Q_p once we compute the other terms. It is natural to shift the term in $\mathcal{B}$ to the 0 place and obtain

$$\begin{array}{ccccccccc}
R^1\pi_*(\wedge^2\pi^*U^* \otimes \mathcal{O}(-4)) & \to & H^0R\pi_*(\mathcal{A}) & \to & Q_p & \to & R^2\pi_*(\wedge^2\pi^*U^* \otimes \mathcal{O}(-4)) & \to & H^1R\pi_*(\mathcal{A}). \\
\| & & & & & & \| & & \\
0 & & & & & & W^* \otimes \wedge^3W^* \otimes \wedge^2U^* & & \\
& & & & & & \downarrow\cong & & \\
& & & & & & W^* & &
\end{array}$$

We can analyze the $\mathcal{A}$ terms by putting the complex $\mathcal{A}$ in its own short exact sequence of complexes $0 \to \mathcal{D} \to \mathcal{A} \to \mathcal{E} \to 0$, given by the following

$$\begin{aligned}
\mathcal{D}: &\qquad 0 \longrightarrow \mathcal{O} \\
\mathcal{A}: &\qquad \pi^*U^* \otimes \mathcal{O}(-2) \xrightarrow{p_1} \mathcal{O} \\
\mathcal{E}: &\qquad \pi^*U^* \otimes \mathcal{O}(-2) \longrightarrow 0.
\end{aligned}$$

Taking the long exact sequence for this short exact sequence of complexes gives

$$H^{-1}R\pi_*(\mathcal{E}) \to H^0R\pi_*(\mathcal{D}) \to H^0R\pi_*(\mathcal{A}) \to H^0R\pi_*(\mathcal{E}) \\ \to H^1R\pi_*(\mathcal{D}) \to H^1R\pi_*(\mathcal{A}) \to H^1R\pi_*(\mathcal{E}),$$

or

$$\begin{array}{ccccccc} R^0\pi_*(\pi^*U^* \otimes \mathcal{O}(-2)) & \longrightarrow & R^0\pi_*(\mathcal{O}) & \longrightarrow & H^0R\pi_*(\mathcal{A}) & \longrightarrow & R^1\pi_*(\pi^*U^* \otimes \mathcal{O}(-2)) \\ \| & & \| & & & & \| \\ 0 & & \mathcal{O}_S & & & & 0 \end{array}$$

and

$$\begin{array}{ccccc} R^1\pi_*(\mathcal{O}) & \longrightarrow & H^1R\pi_*(\mathcal{A}) & \longrightarrow & R^2\pi_*(\pi^*U^* \otimes \mathcal{O}(-2)). \\ \| & & & & \| \\ 0 & & & & 0 \end{array}$$

Thus, we conclude that $H^0R\pi_*(\mathcal{A}) \cong \mathcal{O}_S$ and $H^1R\pi_*(\mathcal{A}) = 0$.

Going back to our original long exact sequence, we have

$$0 \to \mathcal{O}_S \to Q_p \to W^* \to 0.$$

This proves that Q_p is a locally free rank 4 $\mathcal{O}_S$-module. Also, it gives us the necessary map $\mathcal{O}_S \to Q_p$ for our algebra to have a unit. (We can check this map respects the algebra structures because it is induced from the map of complexes $\mathcal{D} \to \mathcal{K}_p$ that respects the differential graded algebra structures on $\mathcal{D}$ and $\mathcal{K}_p$.)

6.5 Local construction by multiplication table

Given a double ternary quadratic form $p \in \mathrm{Sym}^2 W \otimes U$ (with a given $\wedge^3 W \cong \wedge^2 U^*$), now that we know that there is a natural quartic algebra structure of $\mathcal{O}_S \oplus W^*$ we could define the structure locally by giving multiplication tables. For free W and U, we could define an algebra structure on $\mathcal{O}_S \oplus W^*$ in terms of the coefficients of p. Then, if we checked that this structure respected change of basis of W and U (at least those respecting the isomorphism $\wedge^3 W \cong \wedge^2 U^*$), we will have given a construction of a quartic algebra over S from any double ternary quadratic form $p \in \mathrm{Sym}^3 W \otimes U$. This local construction repsects base change almost by definition.

For a double ternary quadratic form over $\mathbb{Z}$ (and therefore with W and U necessarily free), Bhargava [6, Equations (15) and (21)] gives a ring structure on $\mathbb{Z}^4$ whose multiplication table is given in terms of the coefficients of p. Each entry in the multiplication table is a polynomial in the coefficients of p. This, of course, is the multiplication table we would impose for free W and U in the above local construction. We will now see that this local construction agrees with the geometric construction we have given in Section 6.4. We will show this by working over the universal ring $R = \mathbb{Z}[\{a_{ij}, b_{ij}\}_{1 \le i \le j \le 3}]$ for double ternary quadratic forms, and with the universal free form $u = \sum_{1 \le i \le j \le 3} a_{ij}x_ix_jy_1 + b_{ij}x_ix_jy_2$.

Theorem 6.5.1. *For the universal form u, the quartic algebra Q_u is isomorphic to the quartic ring over R that is constructed above using Bhargava's multiplication tables.*

In particular, since our geometric construction of Q_u is invariant under change of basis of W and U (respecting $\wedge^3 W \cong \wedge^2 U^*$), this gives a proof of the invariance of Bhargava's multiplication table under change of basis, as long as the correct $\mathrm{GL}_3 \times \mathrm{GL}_2$ action is used. Since all double ternary quadratic forms are locally pullbacks from the universal form, and both the local construction by multiplication tables and the global geometric construction of Section 6.4 respect base change, Theorem 6.5.1 implies that the two constructions of quartic algebras from double ternary quadratic forms agree. We now prove Theorem 6.5.1.

Proof. For the universal form u, the complex $\mathcal{K}_u$ used to define Q_u is exact, and therefore Q_u is just the global functions on the scheme S_u in $\mathbb{P}^2_R$ cut out by $A = \sum_{1\le i\le j\le 3} a_{ij}x_ix_j$ and $B = \sum_{1\le i\le j\le 3} b_{ij}x_ix_j$. (We can just work in terms of global functions instead of the pushforward to the base since the base $\operatorname{Spec} R$ is affine. Moreover, the multiplicative structure of the global functions of S_u is the same as the induced multiplicative structure on the hypercohomological construction of Q_u.) We cover S_u with open sets $\mathcal{U}_{x_i}$ coming from the usual open sets in $\mathbb{P}^2_R$. As a first step, we will find $(f,g) \in \Gamma(\mathcal{U}_{x_i}) \times \Gamma(\mathcal{U}_{x_j})$ such that $f = g$ in $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j})$. This will find all regular functions on $\mathcal{U}_{x_i} \cup \mathcal{U}_{x_j}$, and it will turn out that they all extend uniquely to global functions on S_u. Thus, we will have found all the regular functions on S_u. We will identify these regular functions with the basis in Bhargava's quartic ring construction, and then it can be checked that the multiplication tables agree.

Let i,j,k be some permutation of $1,2,3$. We have that

$$\Gamma(\mathcal{U}_{x_i}) = R[x_j/x_i, x_k/x_i]/(A/x_i^2, B/x_i^2),$$

and similarly for $\Gamma(\mathcal{U}_{x_j})$. Let I_i be the ideal $(A/x_i^2, B/x_i^2)$ of $R[x_j/x_i, x_k/x_i]$, and similarly for I_j. Also, $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j}) = R[x_j/x_i, x_k/x_i, x_i/x_j]/(A/x_i^2, B/x_i^2)$. If we have $(f,g) \in \Gamma(\mathcal{U}_{x_i}) \times \Gamma(\mathcal{U}_{x_j})$ such that $f = g$ in $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j})$, then f and g are represented by polynomials $\tilde{f} \in R[x_j/x_i, x_k/x_i]$ and $\tilde{g} \in R[x_i/x_j, x_k/x_j]$ such the element $\tilde{f} - \tilde{g} \in R[x_j/x_i, x_k/x_i, x_i/x_j]$ is in the ideal $I = (A/x_i^2, B/x_i^2)$. However, $\tilde{f} - \tilde{g}$ will not have any terms with an x_i and an x_j in the denominator. We define T_1 to be the sub R-module of I of elements that do not have any terms with both an x_i and an x_j in the denominator. The set T_1 gives all the relations between polynomials representing elements in $\Gamma(\mathcal{U}_{x_i})$ and polynomials representing elements in $\Gamma(\mathcal{U}_{x_j})$. We define T_2 to be the sub R-module of T_1 generated by the images of I_i and I_j under their natural inclusion into $R[x_j/x_i, x_k/x_i, x_i/x_j]$. The set T_2 gives all the relations of T_1 that come from relations already in $\mathcal{U}_{x_i}$ and already in $\mathcal{U}_{x_j}$. We now seek to determine T_1/T_2, which gives rise to all pairs $(f,g) \in \Gamma(\mathcal{U}_{x_i}) \times \Gamma(\mathcal{U}_{x_j})$ such that $f = g$ in $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j})$ that are not functions on the base $\operatorname{Spec} R$.

We first define some notation to help us write down elements of T_1/T_2. Let $A_{i^m j^n} = A\frac{x_k^{m+n-2}}{x_i^m x_j^n}$, where the subscript $i^m j^n$ is a product of formal symbols, where a missing exponent denotes an exponent of 1. We define $B_{i^m j^n}$ analogously.

Lemma 6.5.2. *Let $t \in T_1/T_2$. We can write*

$$t = \sum_{\substack{m,n\geq 1\\ m+n\leq 3}} c_{m,n}A_{i^m j^n} + d_{m,n}B_{i^m j^n} \qquad \text{with } c_{m,n}, d_{m,n} \in R.$$

Proof. Clearly we can write any t in I as such as sum over $m, n \in \mathbb{Z}$ with $m+n \geq 2$. Any term with $m \leq 0$ is in the image of I_j and thus in T_2, and any term with $n \leq 0$ is in the image of I_i and thus in T_2. It remains to show that we do not need terms with $m+n \geq 4$ in order to represent t.

We suppose for the sake of contradiction that a term with $m+n \geq 4$ was required, and we take a t with $m+n$ maximal for this condition, and m maximal given that. Then $c_{m,n}A_{i^m j^n}$ contributes a $x_k^{m+n}/x_i^m x_j^n$ term with coefficient $c_{m,n}a_{kk}$ and $d_{m,n}B_{i^m j^n}$ contributes $x_k^{m+n}/x_i^m x_j^n$ term with coefficient $d_{m,n}b_{kk}$. No other terms of the summand for t can contribute a term with $x_i^m x_j^n$ in the denominator, and so we must have $c_{m,n} = rb_{kk}$ and $d_{m,n} = -ra_{kk}$ for some element $r \in R$.

Now we claim we did not need to use the terms $rb_{kk}A_{i^m j^n} - ra_{kk}B_{i^m j^n}$ in the sum that represents t. To prove this claim, we use the following identity

$$\begin{aligned}
&b_{kk}A_{i^m j^n} - a_{kk}B_{i^m j^n}\\
=&-b_{ik}A_{i^{m-1}j^n} + a_{ik}B_{i^{m-1}j^n} - b_{jk}A_{i^m j^{n-1}} + a_{jk}B_{i^m j^{n-1}} + a_{ij}B_{i^{m-1}j^{n-1}}\\
&-b_{ij}A_{i^{m-1}j^{n-1}} - b_{jj}A_{i^m j^{n-2}} + a_{jj}B_{i^m j^{n-2}} - b_{i,i}A_{i^{m-2}j^n} + a_{ii}B_{i^{m-2}j^n}.
\end{aligned}$$

This proves the lemma. □

The above lemma tells us that every element of T_1/T_2 can be written as a R linear combination of $A_{ij}, B_{ij}, A_{i^2 j}, B_{i^2 j}, A_{ij^2}$, and B_{ij^2}. Since only $A_{i^2 j}$ and $B_{i^2 j}$ have terms with $x_i^2 x_j$ in the denominator, we must have that $A_{i^2 j}$ and $B_{i^2 j}$ appear with coefficients $c_{2,1}$ and $d_{2,1}$ so as to cancel those terms out. We can argue similarly for A_{ij^2} and B_{ij^2}. Thus, every element of T_1/T_2 can be written as a R linear combination of $A_{ij}, B_{ij}, b_{kk}A_{i^2 j} - a_{kk}B_{i^2 j}$, and $b_{kk}A_{ij^2} - a_{kk}B_{ij^2}$. We note that all four of $A_{ij}, B_{ij}, b_{kk}A_{i^2 j} - a_{kk}B_{i^2 j}$, and $b_{kk}A_{ij^2} - a_{kk}B_{ij^2}$ have terms with a $x_i x_j$ denominator.

We define some notation so we can write combinations of these elements down more easily. For $i < j$, let $a_{ji} = a_{ij}$. Let $\lambda_{\ell_3\ell_4}^{\ell_1\ell_2} = a_{\ell_1\ell_2}b_{\ell_3\ell_4} - b_{\ell_1\ell_2}a_{\ell_3\ell_4}$. We note that

$$\begin{aligned}
H_{i,j} =&b_{kk}A_{i^2 j} - a_{kk}B_{i^2 j} + b_{ik}A_{ij} - a_{ik}B_{ij}\\
=&\lambda_{kk}^{jj}x_j x_k/x_i^2 + \lambda_{kk}^{ij}x_k/x_i + \lambda_{kk}^{ii}x_k/x_j + \lambda_{kk}^{jk}x_k^2/x_i^2 + \lambda_{ik}^{jj}x_j/x_i\\
&+\lambda_{ik}^{ij} + \lambda_{ik}^{ii}x_i/x_j + \lambda_{ik}^{jk}x_k/x_i
\end{aligned}$$

and

$$H_{j,i} = b_{kk}A_{ij^2} - a_{kk}B_{ij^2} + b_{jk}A_{ij} - a_{jk}B_{ij}$$

do not have any terms with both x_i and x_j in the denominator. Every element of T_1/T_2 can be written as a R linear combination of $A_{ij}, B_{ij}, H_{i,j}$ and $H_{j,i}$, because this is just a unipotent triangular transformation of the last list of four generators. We have seen that $H_{i,j}$ and $H_{j,i}$ have no $x_k^2/x_i x_j$ terms, and A_{ij} and B_{ij} have $x_k^2/x_i x_j$

terms with coefficients a_{kk} and b_{kk} respectively. Since an element of t does not have a term with $x_i x_j$ in the denominator, it can be written as a linear combination of $H_{i,j}, H_{j,i}$ and $F_{ij} = F_{ji} = b_{kk}A_{ij} - a_{kk}B_{ij}$. Moreover, $H_{i,j}, H_{j,i}$ and F_{ij} are all in T_1. We now define $h_{\underline{i},j}$ to be the sum of terms in $H_{i,j}$ that do not have an x_j in the denominator, and $h_{i,\underline{j}} = H_{i,j} - h_{\underline{i},j}$. We define $f_{\underline{i}\underline{j}} = f_{\underline{j}\underline{i}}$ to be the sum of terms in F_{ij} with x_i in the denominator, so that $f_{\underline{i}\underline{j}} + f_{\underline{j}i} + \lambda_{kk}^{ij} = F_{ij}$.

We have now found that the pairs $(f, g) \in \Gamma(\mathcal{U}_{x_i}) \times \Gamma(\mathcal{U}_{x_j})$ such that $f = g$ in $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j})$ can be written in terms of four R-module generators:

$$(1,1), (h_{\underline{i},j}, -h_{i,\underline{j}}), (h_{j,\underline{i}}, -h_{\underline{j},i}), (f_{\underline{i}\underline{j}}, -f_{\underline{j}i} + \lambda_{ij}^{kk}).$$

Letting i and j vary, this information is enough to determine the global functions on S_u. In this case, it turns out that the regular functions on $\mathcal{U}_{x_i}$ that can be extended to $\mathcal{U}_{x_j}$ are exactly the same as the regular functions on $\mathcal{U}_{x_i}$ that can be extended to $\mathcal{U}_{x_k}$. In particular, in the polynomial ring $R[x_j/x_i, x_k/x_i]$, we can compute that

$$h_{\underline{i},j} + h_{\underline{i},k} = \lambda_{jk}^{ii} + a_{jk}B/x_i^2 - b_{jk}A/x_i^2$$

and

$$h_{j,\underline{i}} = -f_{\underline{i}k}.$$

Moreover, it will turn out that the extensions to $\mathcal{U}_{x_j}$ and $\mathcal{U}_{x_k}$ agree on their intersection. We see that the global functions of S_u are generated as a R-module by four generators $g_1, g_2, g_3, g_4 \in \Gamma(\mathcal{U}_{x_1}) \times \Gamma(\mathcal{U}_{x_2}) \times \Gamma(\mathcal{U}_{x_3})$, whose components are given in the below table.

	$\Gamma(\mathcal{U}_{x_1})$	$\Gamma(\mathcal{U}_{x_2})$	$\Gamma(\mathcal{U}_{x_3})$
g_1	1	1	1
g_2	$h_{\underline{1},2} = -h_{\underline{1},3} + \lambda_{23}^{11}$	$-h_{1,\underline{2}} = f_{\underline{2}3}$	$-f_{\underline{3}2} + \lambda_{23}^{11} = h_{1,\underline{3}} + \lambda_{23}^{11}$
g_3	$h_{2,\underline{1}} = -f_{\underline{1}3}$	$-h_{\underline{2},1} = h_{\underline{2},3} + \lambda_{22}^{13}$	$-h_{2,\underline{3}} + \lambda_{22}^{13} = f_{\underline{3}1} + \lambda_{22}^{13}$
g_4	$f_{\underline{1}2} = -h_{3,\underline{1}}$	$-f_{\underline{2}1} + \lambda_{12}^{33} = h_{3,\underline{2}} + \lambda_{12}^{33}$	$-h_{\underline{3},2} + \lambda_{12}^{33} = h_{\underline{3},1}$

We now show that the g_i are generators for a free R-module of rank 4. Suppose for the sake of contradiction that there was a relation among these generators. Then over the generic point of R the global functions of S_u would be a vector space of at most dimension 3. But we know from Section 6.4.2 that the global functions of S_u are locally free four dimensional R module, and thus will be a four dimensional vector space over the generic point of $\operatorname{Spec} R$.

To construct the multiplication table on our four generators g_i of the global functions on S_u, we can reduce to finding a multiplication table in the $\Gamma(\mathcal{U}_{x_1})$ component, since the g_i are R-linearly independent even in this component. We can further reduce to finding the multiplication table over the generic point of $\operatorname{Spec} R$. We first construct a multiplication table on $1, x_2/x_1, x_3/x_1, x_2x_3/x_1^2$ over the generic point of $\operatorname{Spec} R$. To do this, we replace A and B by linear combinations of A and B, one of which has no $(x_2/x_1)^2$ term, and one of which has no $(x_3/x_1)^2$ term. Then on $\mathcal{U}_{x_1}$ over the generic

point of $\operatorname{Spec} R$, we can write all functions in terms of $1, x_2/x_1, x_3/x_1, x_2x_3/x_1^2$. We can then also write the g_i in terms of $1, x_2/x_1, x_3/x_1, x_2x_3/x_1^2$, and just apply this change of basis to the multiplication table to get a multiplication table for the g_i. If we take $\alpha_1 = -g_2$, $\alpha_2 = -g_3$, and $\alpha_3 = -g_4$, we get exactly the multiplication tables given by Bhargava in [6, Equations (15) and (21)]. □

In Section 6.4.2, we found that $Q_p/\mathcal{O}_S$ is canonically isomorphic to W^*. However, we also have explicit basis for $Q_p/\mathcal{O}_S$ when we have a basis for W. We see how these bases are related.

Theorem 6.5.3. *For the universal form u, in the map $Q_p \to W^*$ from Section 6.4.2, we have*

$$\begin{aligned} g_2 &\mapsto x_1^* \\ g_3 &\mapsto x_3^* \\ g_4 &\mapsto x_2^*. \end{aligned}$$

Proof. We compute the map in two steps. We first find the map

$$R^0\pi_*(\mathcal{O}/u(\mathcal{O}(-2)^{\oplus 2})) \to R^1\pi_*(\mathcal{O}(-2)^{\oplus 2}/u(\mathcal{O}(-4)))$$

and then the map

$$R^1\pi_*(\mathcal{O}(-2)^{\oplus 2}/u(\mathcal{O}(-4))) \to R^2\pi_*(\mathcal{O}(-4)).$$

We compute each of the individual maps by using the snake lemma on the Cech complex with the usual affine cover of $\mathbb{P}^2$. We summarize the computation in the charts below, which should be read from upper right to lower left.

	$\mathcal{O}(-4)$	$\mathcal{O}(-2)^{\oplus 2}$	$\frac{\mathcal{O}(-2)^{\oplus 2}}{u(\mathcal{O}(-4))}$	$\mathcal{O}$	$\frac{\mathcal{O}}{u(\mathcal{O}(-2)^{\oplus 2})}$
$\Gamma(\mathcal{U}_{x_1})$				$h_{\underline{1},2}$	
$\times\Gamma(\mathcal{U}_{x_2})$				$-h_{1,\underline{2}}$	g_2
$\times\Gamma(\mathcal{U}_{x_3})$				$-f_{\underline{3},2}+\lambda_{23}^{11}$	
$\Gamma(\mathcal{U}_{x_1x_2})$			$(\frac{a_{33}x_3}{x_1^2x_2}+\frac{a_{13}}{x_1x_2},$	$h_{\underline{1},2}+h_{1,\underline{2}}=H_{1,2}$	
			$\frac{b_{33}x_3}{x_1^2x_2}+\frac{b_{13}}{x_1x_2})$		
$\times\Gamma(\mathcal{U}_{x_2x_3})$				$-h_{1,\underline{2}}+f_{\underline{3},2}-\lambda_{23}^{11}$	
				$=f_{\underline{2},3}+f_{\underline{3},2}-\lambda_{23}^{11}$	
			$(\frac{a_{11}}{x_2x_3},\frac{b_{11}}{x_2x_3})$	$=F_{23}$	
$\times\Gamma(\mathcal{U}_{x_3x_1})$				$h_{\underline{1},2}+f_{\underline{3},2}-\lambda_{23}^{11}$	
				$=-h_{\underline{1},3}-h_{1,\underline{3}}$	
				$+a_{23}\frac{B}{x_1^2}-b_{23}\frac{A}{x_1^2}$	
			$-(\frac{a_{22}x_2}{x_1^2x_3}+\frac{a_{12}}{x_1x_3},$	$=-H_{1,3}$	
			$\frac{b_{22}x_2}{x_1^2x_3}+\frac{b_{12}}{x_1x_3})$		
			$-(\frac{a_{23}}{x_1^2},\frac{b_{23}}{x_1^2})$	$+a_{23}\frac{B}{x_1^2}-b_{23}\frac{A}{x_1^2}$	
$\Gamma(\mathcal{U}_{x_1x_2x_3})$	$\frac{1}{x_1^2x_2x_3}$	$\frac{A+B}{x_1^2x_2x_3}$			

	$\mathcal{O}(-4)$	$\mathcal{O}(-2)^{\oplus 2}$	$\frac{\mathcal{O}(-2)^{\oplus 2}}{u(\mathcal{O}(-4))}$	$\mathcal{O}$	$\frac{\mathcal{O}}{u(\mathcal{O}(-2)^{\oplus 2})}$
$\Gamma(\mathcal{U}_{x_1})$				$h_{2,\underline{1}}$	
$\times\Gamma(\mathcal{U}_{x_2})$				$-h_{\underline{2},1}$	g_3
$\times\Gamma(\mathcal{U}_{x_3})$				$f_{\underline{3},1}+\lambda_{22}^{13}$	
$\Gamma(\mathcal{U}_{x_1x_2})$			$(\frac{a_{33}x_3}{x_1x_2^2}+\frac{a_{23}}{x_1x_2},$	$h_{2,\underline{1}}+h_{\underline{2},1}=H_{2,1}$	
			$\frac{b_{33}x_3}{x_1x_2^2}+\frac{b_{23}}{x_1x_2})$		
$\times\Gamma(\mathcal{U}_{x_2x_3})$				$-h_{\underline{2},1}-f_{\underline{3},1}-\lambda_{22}^{13}$	
				$=h_{\underline{2},3}+h_{2,\underline{3}}$	
				$-a_{13}\frac{B}{x_2^2}+b_{13}\frac{A}{x_2^2}$	
			$(\frac{a_{11}x_1}{x_3x_2^2}+\frac{a_{12}}{x_3x_2},$	$=H_{2,3}$	
			$\frac{b_{11}x_1}{x_3x_2^2}+\frac{b_{12}}{x_3x_2})$		
			$+(\frac{a_{13}}{x_2^2},\frac{b_{13}}{x_2^2})$	$-a_{13}\frac{B}{x_2^2}+b_{13}\frac{A}{x_2^2}$	
$\times\Gamma(\mathcal{U}_{x_3x_1})$				$h_{2,\underline{1}}-f_{\underline{3},1}-\lambda_{22}^{13}$	
				$=-f_{\underline{1},3}-f_{\underline{3},1}-\lambda_{22}^{13}$	
			$-(\frac{a_{22}}{x_1x_3},\frac{b_{22}}{x_1x_3})$	$=-F_{13}$	
$\Gamma(\mathcal{U}_{x_1x_2x_3})$	$\frac{1}{x_1x_2^2x_3}$	$\frac{A+B}{x_1x_2^2x_3}$			

	$\mathcal{O}(-4)$	$\mathcal{O}(-2)^{\oplus 2}$	$\frac{\mathcal{O}(-2)^{\oplus 2}}{u(\mathcal{O}(-4))}$	$\mathcal{O}$	$\frac{\mathcal{O}}{u(\mathcal{O}(-2)^{\oplus 2})}$
$\Gamma(\mathcal{U}_{x_1})$				$-h_{3,\underline{1}}$	
$\times\Gamma(\mathcal{U}_{x_2})$				$-f_{\underline{2},1}+\lambda_{12}^{33}$	g_4
$\times\Gamma(\mathcal{U}_{x_3})$				$h_{\underline{3},1}$	
$\Gamma(\mathcal{U}_{x_1x_2})$				$-h_{3,\underline{1}}+f_{\underline{2},1}-\lambda_{12}^{33}$	
				$=f_{\underline{2},1}+f_{\underline{1},2}+\lambda_{33}^{12}$	
			$(\frac{a_{33}}{x_1x_2},\frac{b_{33}}{x_1x_2})$	$=F_{12}$	
$\times\Gamma(\mathcal{U}_{x_2x_3})$				$-h_{\underline{3},1}-f_{\underline{2},1}+\lambda_{12}^{33}$	
				$=h_{\underline{3},2}+h_{2,\underline{3}}$	
				$-a_{12}\frac{B}{x_3^2}+b_{12}\frac{A}{x_3^2}$	
			$(\frac{a_{11}x_1}{x_1x_3^2}+\frac{a_{13}}{x_2x_3},$	$=H_{3,2}$	
			$\frac{b_{11}x_1}{x_1x_3^2}+\frac{b_{13}}{x_2x_3})$		
			$+(\frac{a_{12}}{x_3^2},\frac{b_{12}}{x_3^2})$	$-a_{12}\frac{B}{x_3^2}+b_{12}\frac{A}{x_3^2}$	
$\times\Gamma(\mathcal{U}_{x_3x_1})$			$-(\frac{a_{22}x_2}{x_3^2x_1}+\frac{a_{23}}{x_1x_3},$	$-h_{\underline{3},1}-h_{3,\underline{1}}=$	
			$\frac{b_{22}x_2}{x_3^2x_1}+\frac{b_{23}}{x_1x_3})$	$-H_{3,1}$	
$\Gamma(\mathcal{U}_{x_1x_2x_3})$	$\frac{1}{x_1x_2x_3^2}$	$\frac{A+B}{x_1x_2x_3^2}$			

□

6.6 Construction of the cubic resolvent

In Section 6.2, we have already given a geometric construction of a cubic ring from a binary cubic form. In Section 6.3, we defined the determinant of a double ternary quadratic form p to be a binary cubic form $\det(p) \in \mathrm{Sym}^3 U^* \otimes (\wedge^2 U)$. The cubic ring C of this binary cubic form can be constructed as described in Section 6.2, and is the desired cubic resolvent.

We can also give a more geometric version of the construction of the binary cubic form from p. We have a quadratic map from $\mathrm{Sym}^2 W$ (conic bundles in $\mathbb{P}(W)$ over S) to $(\wedge^3 W)^{\otimes 2}$ as described in Section 6.3. In geometric fibers, we have that this map is zero exactly when the conic fiber is non-smooth. Thus since p gives a map from U^* to $\mathrm{Sym}^2 W$, we can compose to get a cubic map from U^* to $(\wedge^3 W)^{\otimes 2}$. This, up to the orientation isomorphism, is the binary cubic form given by the double ternary quadratic form p. As long as this map is not the zero map, its zeroes cut out a subscheme of $\mathbb{P}(U)$, and the pushforward to S of the global functions of this

subscheme give the cubic ring over S. If the map given by p from U^* to $(\wedge^3 W)^{\otimes 2}$ is zero, then an analogous hypercohomological construction will still give the appropriate cubic ring. In other words, for nice forms, p gives a map from $\mathbb{P}(U)$ to the Hilbert scheme of conic bundles in $\mathbb{P}(W)$ over S, and when the image of this map is not contained in the singular locus, the pullback of the singular locus gives a subscheme of $\mathbb{P}(U)$, whose regular functions pushforward to the cubic resolvent ring.

We have $C/\mathcal{O}_S \cong U$ (see Chapter 3 for a similar, but simpler argument to the one in Section 6.4.2). Thus, p gives the required quadratic map from $Q/\mathcal{O}_S$ to $C/\mathcal{O}_S$. The orientation isomorphism $\delta : \wedge^3 Q/\mathcal{O}_S \cong \wedge^2 C/\mathcal{O}_S$ comes from the orientation on the double ternary quadratic form. On any open set, we can check that $\delta(x \wedge y \wedge xy) = p(x) \wedge p(y)$ by looking on a open subcover on which W and U are trivial and pulling back from the universal form on each open set in that subcover. It remains to check that $\delta(x \wedge y \wedge xy) = p(x) \wedge p(y)$ when p is the universal ternary quadratic form, which can be checked explicitly given the multiplication table of Q_p. In particular, at the end of the proof of the Main Theorem in Section 6.7, we lay out a plan to determine the multiplication table of Q_p in terms of p. The result agrees with the multiplication table given explicitly in [6, Equations (15) and (21)]. The expressions $\delta(x \wedge y \wedge xy)$ and $p(x) \wedge p(y)$ both represent linear maps from $\mathrm{Sym}_2(Q_p/\mathcal{O}_S) \otimes \mathrm{Sym}_2(Q_p/\mathcal{O}_S)$ to $\wedge^4 Q_p$. Thus it suffices to check that these maps agree on a basis of global sections of $\mathrm{Sym}_2(Q_p/\mathcal{O}_S) \otimes \mathrm{Sym}_2(Q_p/\mathcal{O}_S)$, since in this case $Q_p/\mathcal{O}_S$ is a free $\mathcal{O}_S$ module. This is easily checked, especially exploiting the symmetry of the situation.

6.7 Main Theorem

In this section, we prove the main theorem of this chapter.

Theorem 6.7.1. *Over a scheme S, there is a bijection between isomorphism classes of double ternary quadratic forms and pairs (Q, C) where Q is a quartic ring over S and C is a cubic resolvent of Q. This bijection is functorial in S. In other words, there is an isomorphism between the moduli stack of double ternary quadratic forms and the moduli stack of pairs (Q, C) where Q is a quartic ring over S and C is a cubic resolvent of Q.*

Proof. Given a double ternary quadratic form p over a base S, we have shown how to construct a pair (Q_p, C_p), and all aspects of the construction commute with base change in S. Given a pair (Q, C) over S, we can just take the quadratic map ϕ from $Q/\mathcal{O}_S$ to $C/\mathcal{O}_S$ to be our double ternary quadratic form with $W = (Q/\mathcal{O}_S)^*$ and $U = C/\mathcal{O}_S$ (using the orientation $\wedge^3 Q/\mathcal{O}_S \cong \wedge^2 C/\mathcal{O}_S$). This construction clearly commutes with base change.

It remains to prove that the compositions of these two constructions (in either order) are the identity. To prove this, we rigidify the moduli problems. A *based double ternary quadratic form* is a ternary quadratic form $p \in \mathrm{Sym}^2 W \otimes U$ and a choice of bases w_1, w_2, w_3 and u_1, u_2 for W and U respectively as free $\mathcal{O}_S$-modules, such that $(w_1 \wedge w_2 \wedge w_3) \otimes (u_1 \wedge u_2)$ corresponds to the identity under the orientation isomorphism. A *based pair (Q, C) of a quadratic ring and cubic resolvent* is a a pair

(Q, C) of quadratic ring and cubic resolvent and choices of basis q_1, q_2, q_3 and c_1, c_2 for $Q/\mathcal{O}_S$ and $C/\mathcal{O}_S$ as free $\mathcal{O}_S$-modules, such that $(q_1 \wedge q_2 \wedge q_3)$ corresponds to $(c_1 \wedge c_2)$ under the orientation isomorphism. We see that our constructions above extend to the moduli stacks for these rigidified moduli problems. In particular, we get a basis for $Q/\mathcal{O}_S$ as a dual basis for the basis of W and vice versa.

It now suffices to show that these constructions compose to the identity on the rigidified moduli stacks. If we start with a double ternary quadratic form $p \in \mathrm{Sym}^2 W \otimes U$, we get a pair (Q, C) whose quadratic map is given exactly by the form, and then the construction of a form from (Q, C) gives back exactly our original form. The choices of bases for W and U and the orientation are clearly preserved under this composition.

We can start with a based pair (Q, C), and then build another based pair (Q_ϕ, C_ϕ) from the quadratic map ϕ of (Q, C), and we wish to show that (Q, C) and (Q_ϕ, C_ϕ) are equal. (We can use the notion of equal instead of isomorphic since all of the objects are based.) We have that C and C_ϕ are both given as the cubic ring corresponding to $\mathrm{Det}(\phi)$ and thus are equal. The quadratic resolvent maps are the same, since ϕ carries through the two constructions. The orientation isomorphism are clearly the same since they also carry through the constructions. It remains to show that the multiplication on Q agrees with the multiplication on Q_ϕ. To do this, we will show that the condition $\delta(1 \wedge x \wedge y \wedge xy) = \phi(x) \wedge \phi(y)$ determines the multiplication table on Q from the resolvent map ϕ. Since Q and Q_ϕ have the same resolvent map, this will show that they are isomorphic as $\mathcal{O}_S$-algebras.

We let the quadratic map ϕ be written as $Ac_2 + Bc_1$, where $A = \sum_{1 \le i \le j \le 3} a_{ij} x_i x_j$, and $B = \sum_{1 \le i \le j \le 3} b_{ij} x_i x_j$, and the x_i are a dual basis for q_i in $Q/\mathcal{O}_S$. We recall the notation $\lambda_{\ell_3 \ell_4}^{\ell_1 \ell_2} = a_{\ell_1 \ell_2} b_{\ell_3 \ell_4} - b_{\ell_1 \ell_2} a_{\ell_3 \ell_4}$. We lift the basis q_i of $Q/\mathcal{O}_S$ to a basis of Q uniquely so that $q_1 q_2$ has no q_1 or q_2 term and so that $q_1 q_3$ has no q_1 term. Let m_{ij}^k be the coefficient of q_k in the $q_i q_j$. From Equation (23) in [6], we know that the constant coefficient of $q_i q_j$ in given as a polynomial in the various m coefficients. Thus, it remains to show that the m_{ij}^k are determined by ϕ. We plug various x and y into $\delta(1 \wedge x \wedge y \wedge xy) = \phi(x) \wedge \phi(y)$. In the below, we always let i, j, k be a permutation of $1, 2, 3$ and let $\pm$ be the sign of this permutation. First, letting $x = q_i$ and $y = q_j$ gives $m_{ij}^k = \pm \lambda_{ii}^{jj}$. Then, letting $x = q_i + q_j$ and $y = q_i$ gives $m_{ii}^k = \pm \lambda_{ii}^{ij}$. Next, letting $x = q_i + q_k$ and $y = q_j$ gives $m_{jk}^k - m_{ij}^i = \pm \lambda_{ik}^{jj}$. Using the choice of lift, which gives $m_{12}^1 = m_{21}^2 = m_{13}^1 = 0$, this determines all m_{ij}^i. Finally, letting $x = q_i + q_k$ and $y = q_i + q_j$ determines m_{ii}^i in terms of the λ's and the m's that we have already determined. $\square$

6.8 Appendix: Maps of locally free $\mathcal{O}_S$-modules

Let S be a scheme. We have the following corollary of Lemmas 3.7.3 and 3.7.4 which is used throughout this chapter.

Corollary 6.8.1. *If V is a locally free $\mathcal{O}_S$-module of rank two then*

$$\mathrm{Sym}^3 V \otimes (\wedge^2 V)^{\otimes -2} \cong \mathrm{Sym}^3 V^* \otimes (\wedge^2 V^*)^{\otimes -1}.$$

6.8.1 Degree k maps

Let M and N be locally free $\mathcal{O}_S$-modules. A linear map from M to R is equivalent to a global section of M^*. In other words, sections of M^* are the degree 1 functions on M. We define the *degree* n functions on M as the global sections of $\mathrm{Sym}^n M^*$, symmetric polynomials in linear functions on M.

Definition. A *degree* n map from M to N is a global section of

$$\mathrm{Sym}^n M^* \otimes N \cong \mathcal{H}om(\mathrm{Sym}_n M, N).$$

Note that the identity map on $\mathrm{Sym}_n M$ gives a canonical degree n map from M to $\mathrm{Sym}_n M$.

The language "degree n map from M to N" suggests that we should be able to evaluate such a thing on elements of M.

Definition. Given a degree n map from M to N as an element $f \in \mathrm{Hom}(\mathrm{Sym}_n M, N)$, the *evaluation* of f on an element of M is $f(m \otimes \cdots \otimes m)$.

When M is free, say with generators $m_1, \ldots, m_k$ and dual basis $\mathfrak{m}_1, \ldots \mathfrak{m}_k$ of M^*, then we defined a degree n function f from M to R to be a homogeneous polynomial of degree n in the $\mathfrak{m}_1, \ldots \mathfrak{m}_k$. If we evaluate f on $(c_1 m_1 + \cdots + c_k m_k)$ for arbitrary sections c_i of $\mathcal{O}_S$, we will get a degree n polynomial in the c_i. Replacing the c_i in this polynomial by $\mathfrak{m}_i$ we get the homogeneous polynomial of degree n in the $\mathfrak{m}_1, \ldots \mathfrak{m}_k$ which is the realization of f as an element of $\mathrm{Sym}^n M^*$.

When M is free, we may have a non-linear map $\rho : M \to \mathcal{O}_S$ (or $\rho : M \to N$, but we take $N = \mathcal{O}_S$ for simplicity) and wish to realize it as the evaluation of a degree n map. We can consider $\rho(c_1 m_1 + \cdots + c_k m_k)$ for arbitrary $c_i \in R$ and if $\rho(c_1 m_1 + \cdots + c_k m_k)$ is a degree n polynomial in the c_i, we have an $f \in \mathrm{Sym}^n M^*$ (given by replacing the c_i by $\mathfrak{m}_i$) of which ρ is the evaluation).

Since M is locally free, we locally get $f \in \mathrm{Sym}^n M^*$ and see that the above recipe is invariant under change of basis and so we get a global $f \in \mathrm{Sym}^n M^*$ (as long as everywhere locally where M is free $\rho(c_1 m_1 + \cdots + c_k m_k)$ is a degree n polynomial in the c_i).

As an example, we explicitly realize the determinant as a distinguished element of

$$\mathrm{Hom}(\mathrm{Sym}_n \mathrm{Hom}(M, N), \mathrm{Hom}(\wedge^n M, \wedge^n N)).$$

Let $\phi_1 \otimes \cdots \otimes \phi_n \in \mathrm{Hom}(M, N)^{\otimes n}$. Then we can map $\phi_1 \otimes \cdots \otimes \phi_n$ to the element of $\mathrm{Hom}(\wedge^n M, \wedge^n N)$ which sends $m_1 \wedge \cdots \wedge m_n$ to $\phi_1(m_1) \wedge \cdots \wedge \phi_n(m_n)$. This will not be well-defined for $\phi_1 \otimes \cdots \otimes \phi_n \in \mathrm{Hom}(M, N)^{\otimes n}$, but it will be well-defined when restricted to $\mathrm{Sym}_n \mathrm{Hom}(M, N)$.

$$\begin{array}{ccc} \mathrm{Sym}_n \mathrm{Hom}(M, N) & \longrightarrow & \mathrm{Hom}(\wedge^n M, \wedge^n N) \\ \phi_1 \otimes \cdots \otimes \phi_n & \mapsto & (m_1 \wedge \cdots \wedge m_n \mapsto \phi_1(m_1) \wedge \cdots \wedge \phi_n(m_n)) \end{array} \tag{6.4}$$

This is our realization of the determinant function (as opposed to the determinant of a specific homomorphism) as an element of $\mathrm{Hom}(\mathrm{Sym}_n \mathrm{Hom}(M, N), \mathrm{Hom}(\wedge^n M, \wedge^n N))$.

When we evaluate the determinant on a map $\phi \in \mathrm{Hom}(M, N)$, we get $\phi(m_1) \wedge \cdots \wedge \phi(m_n)$. For example, let N and M be free of rank 2. Evaluating our degree 2 determinant map on a generic element of $\mathrm{Hom}(M, N)$ that sends m_1 to $an_1 + cn_2$ and m_2 to $bn_1 + dn_2$, we see that we obtain the element of $\mathrm{Hom}(\wedge^2 M, \wedge^2 N)$ that sends $m_1 \wedge m_2$ to $(an_1 + cn_2) \wedge (bn_1 + dn_2) = (ad - bc)n_1 \wedge n_2$.

6.8.2 Degree k maps with coefficients

Recall that we have defined a degree k map from a locally free $\mathcal{O}_S$-module M to a locally free $\mathcal{O}_S$-module V to be a linear map from $\mathrm{Sym}_k M$ to V. This is equivalent to a global section of $\mathrm{Sym}^k M^* \otimes V$. We use the following proposition to show that we can "add coefficients" to a degree k map.

Proposition 6.8.2. *In the natural map*

$$\mathrm{Sym}_k(M \otimes N) \to M^{\otimes k} \otimes \mathrm{Sym}^k N,$$

the image of $\mathrm{Sym}_k(M \otimes N)$ *is inside* $\mathrm{Sym}_k M \otimes \mathrm{Sym}^k N$.

Proof. We prove this proposition by checking the statement locally where the modules are free. If we symmetrize a pure tensor of basis elements in $(M \otimes N)^{\otimes k}$, we see that when we forget the terms from N we still get an element of $\mathrm{Sym}_k M$. Since all of the terms in the symmetrization will have the same factor in $\mathrm{Sym}^k N$, this completes the proof. □

Thus, given a degree k map from M to V, we naturally obtain a degree k map from $M \otimes N$ to $V \otimes \mathrm{Sym}^k N$ (by composing $\mathrm{Sym}_k(M \otimes N) \to \mathrm{Sym}_k M \otimes \mathrm{Sym}^k N \to V \otimes \mathrm{Sym}^k N$). We call this construction *using* V *as coefficients*, because it is as if we treat the elements of V as formal ring elements.

Chapter 7

Quartic rings with quadratic subrings or cubic quotients

7.1 Introduction

Quartic rings, along with a cubic resolvent, are parametrized by pairs of ternary quadratic forms [6]. The cubic resolvent is an integral model of the classical resolvent field of a quartic field. This result is over $\mathbb{Z}$, but an analogous result can also be formulated over an arbitrary base scheme S. A *rank n ring* over S is an $\mathcal{O}_S$-algebra R such that $R/\mathcal{O}_S$ is a locally free rank $n-1$ $\mathcal{O}_S$-module. A *double ternary quadratic form* over S is a locally free rank 3 $\mathcal{O}_S$-module W, a locally free rank 2 $\mathcal{O}_S$-module U, a global section $p \in \operatorname{Sym}^2 W \otimes U$, and an orientation isomorphism $\wedge^3 W \otimes \wedge^2 U \cong \mathcal{O}_S$. Recall the following theorem from Chapter 6.

Theorem 6.1.2. *Over a scheme S, there is a bijection between isomorphism classes of double ternary quadratic forms and pairs (Q, C) where Q is a quartic ring over S and C is a cubic resolvent ring of Q. This bijection is functorial in S. In this bijection we have $Q/\mathcal{O}_S \cong W^*$ and $C/\mathcal{O}_S \cong U$.*

In this chapter we will investigate some special structures on quartic rings and what properties of double ternary quadratic forms $p \in \operatorname{Sym}^2 W \otimes U$ they correspond to. One main structure of interest is quartic rings with quadratic subrings. These occur, for example, in orders in quartic fields whose Galois closure has Galois group D_4. We will also study quartic rings with cubic ring quotients. These occur in orders in the product of a cubic field and $\mathbb{Q}$. We will define several properties of double ternary quadratic forms, and see how each property relates these special structures on quartic rings.

We can specialize the base scheme to $S = \operatorname{Spec} \mathbb{Z}$ to get a parametrization that includes orders in quartic fields. For example, consider the space $V_{\mathbb{Z}}$ of pairs of symmetric matrices

$$A_1 = \begin{pmatrix} a_{111} & \frac{a_{121}}{2} & \frac{a_{131}}{2} \\ \frac{a_{121}}{2} & a_{221} & \frac{a_{231}}{2} \\ \frac{a_{131}}{2} & \frac{a_{231}}{2} & a_{331} \end{pmatrix} \qquad A_2 = \begin{pmatrix} a_{112} & \frac{a_{122}}{2} & \frac{a_{132}}{2} \\ \frac{a_{122}}{2} & a_{222} & \frac{a_{232}}{2} \\ \frac{a_{132}}{2} & \frac{a_{232}}{2} & a_{332} \end{pmatrix},$$

with $a_{ijk} \in \mathbb{Z}$. We have an action of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ on these matrices. The action of $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ takes (A_1, A_2) to $(aA_1 + bA_2, cA_1 + dA_2)$. The $\mathrm{GL}_3(\mathbb{Z})$ action is given by $(A_1, A_2) \mapsto (gA_1g^t, gA_2g^t)$. Let G be the subgroup of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ of (g_1, g_2) such that $\det(g_1)\det(g_2) = 1$, and

$$g_1 = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}.$$

An element of $V_{\mathbb{Z}}$ is *degenerate* if the discriminant of $4\,\mathrm{Det}(A_1x_1 - A_2x_2)$ is zero. We then have a parametrization of quartic rings with quadratic subrings.

Theorem 7.1.1. *We have a bijection*

$$\left\{\begin{array}{l} G\text{-equivalence classes of non-} \\ \text{degenerate elements of } V_{\mathbb{Z}}, \text{ such} \\ \text{that } A_1 \text{ has top row zero and} \\ a_{112} \neq 0 \end{array}\right\} \longleftrightarrow \left\{\begin{array}{l} \text{isomorphism classes of } (Q, C, T) \\ \text{with } Q \text{ a non-degenerate quartic} \\ \text{ring, and } C \text{ a cubic resolvent, and} \\ T \text{ a primitive quadratic subalgebra} \\ \text{of } Q, \text{ such that } T \to T/\mathbb{Z} \text{ does not} \\ \text{have a splitting whose image is an} \\ \text{ideal of } Q \end{array}\right\}.$$

Notation. Throughout this chapter, we will work with a double ternary quadratic form $p \in \mathrm{Sym}^2 W \otimes U$ over a scheme S. For all of the properties we will study, we fix a locally free rank 1 quotient $W \to L$. We let K be the kernel of $W \to L$. If B is a locally free $\mathcal{O}_S$-module, we say that A is a *primitive* submodule of B if A is a submodule of B such that A and B/A are both locally free $\mathcal{O}_S$-modules.

7.2 Special double ternary quadratic forms and special quartic rings

We will now study special double ternary quadratic forms over an arbitrary base scheme S. For any element v in $V_1 \otimes V_2$, where the V_i are locally free $\mathcal{O}_S$-modules, we can take its two-by-two minor $\det_2(v) \in \wedge^2 V_1 \otimes \wedge^2 V_2$. Thus we get $\det_2(p) \in \wedge^2(\mathrm{Sym}^2 W) \otimes \wedge^2 U$. It will be more convenient for us to view $\wedge^2(\mathrm{Sym}^2 W) \subset (\mathrm{Sym}^2 W)^{\otimes 2}$ via the natural map $x \wedge y \mapsto x \otimes y - y \otimes x$. (This map $\wedge^2 V \to V \otimes V$ is just the dual of the usual map $V^* \otimes V^* \to \wedge^2 V^*$.)

Definition. The double ternary quadratic form p is *angled* with respect to L if $\det_2(p)$ maps to 0 in $(\mathrm{Sym}^2 W)^{\otimes 2} \otimes \wedge^2 U \to (\mathrm{Sym}^2 W/\mathrm{Sym}^2 K) \otimes \mathrm{Sym}^2 L \otimes \wedge^2 U$.

Formally, we define an angled double ternary quadratic form to be (W, U, L, p), such that we have a surjective map $W \to L$, and such that $p \in \mathrm{Sym}^2 W \otimes U$ is angled with respect to L. An isomorphism of two angled double ternary quadratic forms (W, U, L, p) and (W', U', L', p') consists of isomorphisms $W \cong W'$, and $U \cong U'$, and $L \cong L'$ that respect the maps $W \to L$ and $W' \to L'$ and take p to p'.

Theorem 7.2.1. *We have that p is angled with respect to L if and only if in the corresponding quartic ring Q, the kernel of $Q \to K^*$ is a subalgebra of Q. In other words, a primitive rank 2 submodule T of Q (with $\mathcal{O}_S \subset T$) is a sub-algebra if and only if a resolvent mapping ϕ of Q is angled with respect to the quotient $(Q/\mathcal{O}_S)^* \to (T/\mathcal{O}_S)^*$.*

Corollary 7.2.2. *We have an isomorphism between the stack of angled double ternary quadratic forms, and the stack of triples (Q, C, T), where Q is a quartic ring, C is a cubic resolvent, and T is a primitive quadratic subalgebra of Q.*

Proof. We can check both conditions locally on the base scheme S, and therefore we can assume U, L, and K are free. Let l be a basis element for l and let k_1, k_2 be basis elements for K, corresponding, respectively, to the basis w_1, w_2, w_3 of W. Let u_1, u_2 be a basis for U. Write $p = \sum a_{ijk} w_i w_j u_k$. Let $\lambda_{kl}^{ij} = a_{ij1}a_{kl2} - a_{ij2}a_{kl1}$. Then the condition that p is angled is equivalent to $\lambda_{12}^{11} = \lambda_{13}^{11} = 0$. We want to show that $\mathcal{O}_S \oplus L^*$ is a subalgebra of Q, or equivalently, that $(l^*)^2$ has no k_1^* or k_2^* coefficients. (This statement does not depend of the choices of lifts of l^*, k_1^*, k_2^* to Q to form a basis along with 1.) If we write $\alpha_1 = l^*$, and $\alpha_2 = k_1^*$, and $\alpha_3 = k_2^*$ (i.e. α_i are a dual basis to the w_i), then we know the multiplication table for the (normalized) α_i in terms of the a_{ijk} from [6, Equations (21) and (23)]. In particular, we know that the α_2 coefficient of α_1^2 is λ_{13}^{11} and the α_3 coefficient of α_1^2 is λ_{12}^{11}. Thus, $\mathcal{O}_S \oplus L^*$ is a subalgebra of Q if and only if $\lambda_{12}^{11} = \lambda_{13}^{11} = 0$. □

Definition. The double ternary quadratic form p is *crossed* with respect to L if p maps to 0 in the map $(\mathrm{Sym}^2 W)^{\otimes 2} \otimes \wedge^2 U \to (\mathrm{Sym}^2 W) \otimes \mathrm{Sym}^2 L \otimes \wedge^2 U$.

If p is crossed with repsect to L then it is also angled.

Theorem 7.2.3. *We have that p is crossed with respect to L if and only if the corresponding quartic ring Q has a cubic algebra quotient $Q \to R$ whose kernel maps to L^* in $Q/\mathcal{O}_S$. In other words, a quotient map $Q \to R$ from Q to a locally free rank 3 $\mathcal{O}_S$-module such that $\mathcal{O}_S$ maps injectively is a morphism of algebras (i.e. its kernel is an ideal) if and only if p is crossed with repsect to the dual of its kernel.*

Corollary 7.2.4. *We have an isomorphism between the stack of crossed double ternary quadratic forms, and the stack of triples (Q, C, R), where Q is a quartic ring, C is a cubic resolvent, and R is a cubic algebra quotient of Q.*

Proof. We can check both conditions locally on the base scheme S, and therefore we can assume U, L, and K are free. Let l be a basis element for l and let k_1, k_2 be basis elements for K, corresponding, respectively, to the basis w_1, w_2, w_3 of W. Let u_1, u_2 be a basis for U. Write $p = \sum a_{ijk} w_i w_j u_k$. Let $\lambda_{kl}^{ij} = a_{ij1}a_{kl2} - a_{ij2}a_{kl1}$. The the condition that p is crossed is equivalent to $\lambda_{12}^{11} = \lambda_{13}^{11} = \lambda_{23}^{11} = \lambda_{22}^{11} = \lambda_{33}^{11} = 0$. This implies that if we lift w_i^* to a normalized basis α_i (with 1), i.e. such that $\alpha_1\alpha_2$ has no α_1 or α_2 coefficient and $\alpha_1\alpha_3$ has no α_1 coefficient, then we can read the multiplication table from [6, Equations (21) and (23)], and see that α_1^2 has no α_2 or α_3 coefficients

(since $\lambda_{12}^{11} = \lambda_{13}^{11}$) and that $\alpha_1\alpha_2, \alpha_1\alpha_3 \in \mathcal{O}_S$ (since $\lambda_{22}^{11} = \lambda_{33}^{11} = \lambda_{23}^{11} = 0$). We write out here the constant coefficients of $\alpha_1\alpha_j$ for ease of reference:

$$c_{1j}^0 = \sum_r c_{j2}^r c_{r1}^2 - c_{1j}^r c_{r2}^2.$$

Note that $c_{r1}^2 = 0$ for all r, and c_{1j}^r is only non-zero for $j = r = 1$, in which case $c_{r2}^2 = 0$. Thus, α_1^2 is a multiple of α_1, and $\alpha_1\alpha_2 = \alpha_1\alpha_3 = 0$. We conclude that the $\mathcal{O}_S$-module generated by α_1 is an ideal of Q.

If Q has a cubic algebra quotient $Q \to R$, then we can let L^* be the image of its kernel in $Q/\mathcal{O}_S$, and L be the corresponding quotient of W. Then, locally on the base where all the involved modules are free, we can write everything in terms of bases as above. We have then that for some $k \in \mathcal{O}_S$, that $(\alpha_1 + k)\mathcal{O}_S$ is an ideal of Q. There can only be one such k since $(\alpha_1+k)\alpha_2-(\alpha_1+k')\alpha_2$ is only a multiple of α_1 if $k = k'$. In particular, it must be the k such that $(\alpha_1 + k)\alpha_2$ has no α_2 coefficient, and this is $k = 0$ since we chose the α_i normalized. Since α_1^2 has no α_3 or α_2 coefficient, we obtain that $\lambda_{12}^{11} = \lambda_{13}^{11} = 0$. Since $\alpha_1\alpha_2$ has no α_3 coefficient, we see that $\lambda_{22}^{11} = 0$. Since $\alpha_1\alpha_3$ has no α_3 or α_2 coefficient, we see that $\lambda_{23}^{11} = \lambda_{33}^{11} = 0$. Thus any p corresponding to Q is crossed with repsect to L. □

Since any crossed p is also angled, it is natural to ask what the quadratic subalgebra is, and from the above proof we see that the quadratic subalgebra is $\mathcal{O}_S \oplus \ker(Q \to R)$.

Definition. The double ternary quadratic form p is *pointed* with respect to L if p is in the kernel of the natural map $\operatorname{Sym}^2 W \otimes U \to \operatorname{Sym}^2 L \otimes U$.

It is not hard to see that if p is pointed with respect to L then p is crossed (and thus angled) with respect to L. (If we write $p = \sum a_{ijk} w_i w_j u_k$ as in the above proofs then p is pointed if and only if $a_{111} = a_{112} = 0$.)

Now we fix not only a rank 1 quotient $W \to L$, but also a rank 1 quotient $U^* \to M$. We can view p as a degree two map from W^* to U.

Definition. The double ternary quadratic form p is *oblique* with respect to L, M if over any open set $\mathcal{U}$ of the base we have that $p(q+L^*)-p(q) \in M^*$ for all $q \in W^*(\mathcal{U})$.

If we write $p = \sum a_{ijk} w_i w_j u_k$, where u_2 is a basis for M^*, then p is oblique if and only if $a_{111} = a_{121} = a_{131} = 0$. If p is oblique, then it is angled with respect to L.

7.3 Working over a principal ideal domain

Now we specialize to the case when $S = \operatorname{Spec} B$, where B is a principal ideal domain.

Theorem 7.3.1. *If p is angled with repsect to L and not pointed with respect to L, then it is oblique with respect to L and some M.*

In other words, over a PID angled and not pointed is equivalent to oblique and not pointed. This tells us that quartic rings with quadratic subalgebras not of the form $\mathcal{O}_S \oplus I$, (where I is an ideal of Q) correspond to oblique forms.

Proof. Let $p \in \operatorname{Sym}^2 W \otimes U$, and let L be a free rank 1 quotient of W. Since B is a PID, all locally free modules of finite rank are free and thus we write $p = \sum a_{ijk} w_i w_j u_k$. (Here, L is the quotient of W by w_2 and w_3.) We can do a $\mathrm{GL}_2(B)$ change of basis of u_1, u_2 so that we have $a_{111} = 0$.

Now supposed p is angled with respect to L. If p is not pointed, then a_{112} is not zero, and thus since $\lambda_{12}^{11} = \lambda_{13}^{11} = 0$ we have that $a_{111} = a_{121} = a_{131} = 0$, and that p is oblique with respect to L, M, where M is the quotient of U^* by u_1^*. We can also describe M more canonically: $p(L^*)$ lies in a unique primitive rank 1 B-sub-module M^* of U. □

Theorem 7.3.2. *When $S = \operatorname{Spec} B$, where B is a principal ideal domain, if p is crossed and not pointed for L then it has discriminant 0.*

Proof. We work as in the above proof, and with that notation. Then, since a_{112} is not zero, we have that $a_{ij1} = 0$ for all i and j. In particular, p has discriminant 0. □

Thus for nondegenerate (non-zero discriminant) double ternary quadratic forms, crossed and pointed for L are equivalent.

If we are interested in orders of quartic fields whose Galois closure has group D_4 we see that they are angled but not crossed (and thus oblique and not pointed). We now give bijections of B-orbits that in the case $B = \mathbb{Z}$ parametrize such orders. To work concretely, we represent our double ternary quadratic forms with pairs of symmetric matrices, which will require that B is not characteristic 2. We will consider the space V_B of pairs of symmetric matrices

$$A_1 = \begin{pmatrix} a_{111} & \frac{a_{121}}{2} & \frac{a_{131}}{2} \\ \frac{a_{121}}{2} & a_{221} & \frac{a_{231}}{2} \\ \frac{a_{131}}{2} & \frac{a_{231}}{2} & a_{331} \end{pmatrix} \qquad A_2 = \begin{pmatrix} a_{112} & \frac{a_{122}}{2} & \frac{a_{132}}{2} \\ \frac{a_{122}}{2} & a_{222} & \frac{a_{232}}{2} \\ \frac{a_{132}}{2} & \frac{a_{232}}{2} & a_{332} \end{pmatrix},$$

with $a_{ijk} \in B$. We have an action of $\mathrm{GL}_2(B) \times \mathrm{GL}_3(B)$ on these matrices. The action of $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(B)$ takes (A_1, A_2) to $(aA_1 + bA_2, cA_1 + dA_2)$. The $\mathrm{GL}_3(B)$ action is given by $(A_1, A_2) \mapsto (gA_1g^t, gA_2g^t)$. Let G be the subgroup of $\mathrm{GL}_2(B) \times \mathrm{GL}_3(B)$ of (g_1, g_2) such that $\det(g_1)\det(g_2) = 1$, and

$$g_1 = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}.$$

We then have a theorem for oblique forms, essentially from the definition.

Theorem 7.3.3. *Let B be a principal ideal domain of characteristic not equal to 2. We have a bijection*

$$\left\{\begin{array}{l}\text{G-equivalence classes of elements}\\ \text{of } V_B, \text{ such that } A_1 \text{ has top row}\\ \text{zero}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{isomorphism classes of}\\ (Q, C, L^*, M^*) \text{ with } Q \text{ a quar-}\\ \text{tic ring over } B, \text{ and } C \text{ a cubic}\\ \text{resolvent, and } L^* \text{ and } M^* \text{ primi-}\\ \text{tive, rank 1 } B\text{-submodules of } Q/B\\ \text{and } R/B \text{ respectively, such that}\\ \phi(x + L^*) - \phi(x) \in M^* \text{ for all}\\ x \in Q\end{array}\right\}$$

An isomorphism of (Q, R, L^*, M^*) and $(Q', R', L^{*\prime}, M^{*\prime})$ is an isomorphism of (Q, R) to (Q', R') that takes L^* to $L^{*\prime}$ and takes M^* to $M^{*\prime}$. If ϕ is not pointed with respect to $(\alpha_1\mathcal{O}_S)^*$, then $\phi(L^*)$ is not 0, and M^* is the unique primitive rank 1 module containing $\phi(L^*)$. We thus have a theorem for oblique, non-pointed forms, which follows by restricting the above bijection to the case that $\phi(L^*) \neq 0$.

Theorem 7.3.4. *Let B be a principal ideal domain of characteristic not equal to 2. We have a bijection*

$$\left\{\begin{array}{l}\text{G-equivalence classes of elements}\\ \text{of } V_B, \text{ such that } A_1 \text{ has top row}\\ \text{zero and } a_{112} \neq 0\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{isomorphism classes of } (Q, C, L^*)\\ \text{with } Q \text{ a quartic ring over } B, \text{ and}\\ C \text{ a cubic resolvent, and } L^* \text{ a prim-}\\ \text{itive rank 1 submodule of } Q/B\\ \text{such that } \phi(L^*) \neq 0 \text{ and } \phi(x +\\ L^*) - \phi(x) \text{ lies in the primitive rank}\\ 1 \text{ module containing } \phi(L^*) \text{ for all}\\ x \in Q\end{array}\right\}.$$

However, a pair (A_1, A_2) of ternary quadratic forms, such that A has no terms involving x_1 and $b_{11} \neq 0$, is equivalent to a pair (A_1, A_2) such that $a_{11} = 0$ and $b_{11} \neq 0$ and $\lambda_{12}^{11} = \lambda_{13}^{11} = 0$, which is equivalent to a pair (A_1, A_2) such that $a_{11} = 0$ which is angled but not pointed (or, equivalently for non-degenerate pairs, not crossed) in the first coordinate. We thus have theorems for angled, non-pointed and angled, non-crossed forms.

Theorem 7.3.5. *Let B be a principal ideal domain of characteristic not equal to 2. We have a bijection*

$$\left\{\begin{array}{l}\text{G-equivalence classes of elements}\\ \text{of } V_B, \text{ such that } A_1 \text{ has top row}\\ \text{zero and } a_{112} \neq 0\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{isomorphism classes of } (Q, C, S)\\ \text{with } Q \text{ a quartic ring over } B, \text{ and}\\ C \text{ a cubic resolvent, and } T \text{ a primi-}\\ \text{tive quadratic subalgebra of } Q, \text{ such}\\ \text{that } \phi(T) \neq 0\end{array}\right\}$$

Theorem 7.3.6. *Let B be a principal ideal domain of characteristic not equal to 2. We have a bijection*

$$\left\{\begin{array}{l}\textit{G-equivalence classes of non-}\\ \textit{degenerate elements of } V_B, \textit{ such}\\ \textit{that } A_1 \textit{ has top row zero and}\\ a_{112} \neq 0\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\textit{isomorphism classes of } (Q, C, T)\\ \textit{with } Q \textit{ a non-degenerate quartic}\\ \textit{ring over } B, \textit{ and } C \textit{ a cubic resol-}\\ \textit{vent, and } T \textit{ a primitive quadratic}\\ \textit{subalgebra of } Q, \textit{ such that } T \to\\ T/B \textit{ does not have a splitting}\\ \textit{whose image is an ideal of } Q\end{array}\right\}.$$

The nice thing about Theorem 7.3.6 is that the conditions only depend on Q and not the choice of cubic resolvent. In particular, a maximal D_4 order (maximal order in a quartic number field whose Galois closure has Galois group D_4) has a unique resolvent [6] and a unique primitive quadratic subring. Moreover, a D_4 order has no rank 1 ideals. Therefore, each isomorphism class of D_4 orders appears exactly once in the bijection of Theorem 7.3.6.

7.4 Relating to Galois Groups

Let K be a field and consider a double ternary quartic form p over $\operatorname{Spec} K$. For the rest of this section, we assume $\operatorname{Disc}(p) \neq 0$. Then we have that p corresponds to an étale quartic K-algebra Q, which is just a direct product of field extensions of K. We list the possibilities here.

1. L_4, a quartic number field
2. $K \times L_3$, with L_3 a cubic extension
3. $L_2 \times M_2$, with L_2, M_2 quadratic extensions
4. $L_2 \times L_2$, with L_2 a quadratic extension
5. $K \times K \times L_2$, with L_2 a quadratic extension
6. $K \times K \times K \times K$

If p is angled, then Q has a quadratic subalgebra T. We have $\alpha_1 \in Q$, which in each projection to a field is of degree at most 2. In particular, α_1 must satisfy the same quadratic equation in each projection to a field. Also, $\alpha_1 \notin K$. If the minimal polynomial of α_1 is reducible, then in each projection α_1 must map to one of the two K-rational roots of the polynomial, and it cannot always map to the same rational root. This is possible in all but case 1 above. If the minimal polynomial for α_1 is irreducible, α_1 must map to a root of that polynomial in each projection onto a field, and that is possible in only cases 1 and 4 above. In case 1, it is only possible when K_4 has a quadratic subfield, which is when the Galois closure of K_4 over K has Galois group D_4, V_4, or C_4. If p is crossed, then Q has a cubic algebra quotient. This is possible exactly in cases 2, 5, and 6 above.

Similarly, we can consider the case of a non-degenerate double ternary quadratic form over a domain B. Let K be the fraction field of B. If $\mathrm{Disc}(p) \neq 0$, the corresponding Q is an order in a K-algebra of one of the above types. If a non-degenerate p is angled with corresponding subalgebra T, then Q must be an order in a quartic field (whose Galois closure over K has Galois group D_4, V_4, or C_4) or an order in an algebra which is not a field.

In Theorem 7.3.6, in which we assume that B is a PID, the only quartic rings over B that can appear are subrings of quartic extensions of K (whose Galois closure over K has Galois group D_4, V_4, or C_4) and subrings in K-algebras of types 3, 4, 5, or 6 above. For subrings of K-algebras of type 2 above, the quadratic subalgebra T is such that $T/\mathbb{Z}$ has a lift to an ideal of Q whose elements have projection 0 in L_3.

Bibliography

[1] K. Belabas, On quadratic fields with large 3-rank, Math. Comp. **73** (2004), no. 248, 2061–2074 (electronic).

[2] M. Bhargava, The density of discriminants of quartic rings and fields, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.

[3] M. Bhargava, The density of discriminants of quintic rings and fields, Ann. of Math., to appear.

[4] M. Bhargava, Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations, Ann. of Math. (2) **159** (2004), no. 1, 217–250.

[5] M. Bhargava, Higher composition laws. II. On cubic analogues of Gauss composition, Ann. of Math. (2) **159** (2004), no. 2, 865–886.

[6] M. Bhargava, Higher composition laws. III. The parametrization of quartic rings, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360.

[7] M. Bhargava, Higher composition laws. IV. The parametrization of quintic rings, Ann. of Math. (2) **167** (2008), no. 1, 53–94.

[8] B. J. Birch and J. R. Merriman, Finiteness theorems for binary forms with given discriminant, Proc. London Math. Soc. (3) **24** (1972), 385–394.

[9] W. Bosma and P. Stevenhagen, On the computation of quadratic 2-class groups, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 283–313.

[10] N. Bourbaki, *Elements of mathematics. Commutative algebra*, Translated from the French, Hermann, Paris, 1972

[11] D. A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3, Amer. J. Math. **99** (1977), no. 3, 447–485.

[12] H. S. Butts and G. Pall, Modules and binary quadratic forms, Acta Arith. **15** (1968), 23–44.

[13] G. Casnati and T. Ekedahl, Covers of algebraic varieties. I. A general structure theorem, covers of degree 3, 4 and Enriques surfaces, J. Algebraic Geom. **5** (1996), no. 3, 439–460.

[14] G. Casnati, Covers of algebraic varieties. III. The discriminant of a cover of degree 4 and the trigonal construction, Trans. Amer. Math. Soc. **350** (1998), no. 4, 1359–1378.

[15] B. J. Dulin and H. S. Butts, Composition of binary quadratic forms over integral domains, Acta Arith. **20** (1972), 223–251.

[16] H. Cohen, *A course in computational algebraic number theory*, Springer, Berlin, 1993.

[17] 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.

[18] I. Del Corso, R. Dvornicich and D. Simon, Decomposition of primes in non-maximal orders, Acta Arith. **120** (2005), no. 3, 231–244.

[19] P. Deligne, letter to W. T. Gan, B. Gross and G. Savin, November 13, 2000.

[20] P. Deligne, letter to M. Bhargava, March 5, 2004.

[21] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Amer. Math. Soc., Providence, R.I., 1964. (translation of B. N. Delone and D. K. Faddeev, Theory of Irrationalities of Third Degree, Acad. Sci. URSS. Trav. Inst. Math. Stekloff, **11** (1940).)

[22] D. Eisenbud, *Commutative algebra*, Springer, New York, 1995.

[23] D. Eisenbud, *The geometry of syzygies*, Springer, New York, 2005.

[24] W. T. Gan, B. Gross and G. Savin, Fourier coefficients of modular forms on G_2, Duke Math. J. **115** (2002), no. 1, 105–169.

[25] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[26] A. Grothendieck, Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. II, Inst. Hautes Études Sci. Publ. Math. No. 17 (1963), 91 pp.

[27] R. Hartshorne, *Algebraic geometry*, Springer, New York, 1977.

[28] E. Hecke, *Lectures on the theory of algebraic numbers*, Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen, Springer, New York, 1981.

[29] I. Kaplansky, Composition of binary quadratic forms, Studia Math. **31** (1968), 523–530.

[30] M. Kneser, Composition of binary quadratic forms, J. Number Theory **15** (1982), no. 3, 406–413.

[31] H. Lenstra, *Gauss composition over an arbitrary commutative ring,* talk at Stieltjes Onderwijsweek: Rings of Low Rank, Lorentz Center, June 2006.

[32] R. Miranda, Triple covers in algebraic geometry, Amer. J. Math. **107** (1985), no. 5, 1123–1158.

[33] J. Morales, The classification of pairs of binary quadratic forms, Acta Arith. **59** (1991), no. 2, 105–121.

[34] J. Morales, On some invariants for systems of quadratic forms over the integers, J. Reine Angew. Math. **426** (1992), 107–116.

[35] J. Nakagawa, Binary forms and orders of algebraic number fields, Invent. Math. **97** (1989), no. 2, 219–235.

[36] J. Neukirch, *Algebraic number theory*, Translated from the 1992 German original and with a note by Norbert Schappacher, Springer, Berlin, 1999.

[37] D. Simon, A "class group" obstruction for the equation $Cy^d = F(x, z)$, preprint (2008).

[38] D. Simon, La classe invariante d'une forme binaire, C. R. Math. Acad. Sci. Paris **336** (2003), no. 1, 7–10.

[39] D. Simon, The index of nonmonic polynomials, Indag. Math. (N.S.) **12** (2001), no. 4, 505–517.

[40] J. Towber, Composition of oriented binary quadratic form-classes over commutative rings, Adv. in Math. **36** (1980), no. 1, 1–107.