J. London Math. Soc. (2) 83 (2011) 208–231 © 2011 London Mathematical Society
doi:10.1112/jlms/jdq074

Rings and ideals parameterized by binary n-ic forms

Melanie Matchett Wood

Abstract

The association of algebraic objects to forms has had many important applications in number theory. Gauss, over two centuries ago, studied composition of binary quadratic forms, which we now understand via Dedekind's association of ideal classes of quadratic rings to integral binary quadratic forms. Delone and Faddeev, in 1940, showed that cubic rings are parameterized by equivalence classes of integral binary cubic forms. Birch, Merriman, Nakagawa, del 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 paper, we show exactly what algebraic structures are parameterized by binary n-ic forms, for all n. The algebraic data associated to an integral binary n-ic form includes a ring isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$-module, an ideal class for that ring, and a condition on the ring and ideal class that comes naturally from geometry. In fact, we prove these parameterizations 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 give geometric constructions of the rings and ideals from the forms that parameterize them and a simple construction of the form from an appropriate ring and ideal.

1. *Introduction*

When one looks for a parameterizing 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 with rational coefficients 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 parameterization of orders in those number fields; $\mathrm{GL}_2(\mathbb{Z})$ classes of integral binary cubic forms are in bijection with isomorphism classes of cubic rings (see [**2**, **4**, **8**, **9**]). For other n, the space of binary n-ic forms parameterizes algebraic data that are more subtle than this. It has long been known that binary quadratic forms parameterize ideal classes in quadratic rings (originally in [**5**], see [**12**, **17**, **19**] for modern treatments). In this paper, we construct the algebraic data associated to a binary n-ic form, and determine what algebraic structures are in fact parameterized 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 [**6**]. They have also given a condition on the form equivalent to the p-maximality of the associated ring. Simon [**16**] uses the ring associated to a binary form to find a class group obstruction to equations of the form $Cy^d = f(x, z)$ having integral solutions (where f is the binary form). Work of the author finds an explicit moduli

Received 10 November 2009; published online 3 January 2011.

2000 *Mathematics Subject Classification* 11E76 (primary), 11R04 (secondary).

This work was done with the support of an NSF Graduate Fellowship, an NDSEG Fellowship, an AAUW Dissertation Fellowship, and a Josephine De Kármán Fellowship, an American Institute of Mathematics Five-Year Fellowship, and NSF Grant DMS-1001083.

space for ideal classes in the rings associated to binary n-ic forms [20]. Thus, we can work explicitly with these rings, prime splitting in them, and their ideal classes.

However, in addition to the ring that is canonically associated to a binary form, there is more associated data, including ideal classes of the ring. Some of these ideal classes have been constructed for irreducible primitive forms in [6, 15, 16]. In Section 2, we give the following 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 Lorentz Center Rings of Low Rank Workshop in 2006 about giving a basis-free description of the ring associated to a binary form. In the case $n = 3$, the geometric construction of (4) was originally given in a letter of Deligne [7]. 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 of a ring and ideal classes from a binary form is so simple that we give it here.

A binary n-ic form f 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 $-1 \leqslant k \leqslant n-1$, 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 classically associated to the binary quadratic form. (This construction gives an ideal even when f is reducible or non-primitive. See [19] for a complete description of the $n = 2$ case.) When $n = 3$, we expect to obtain canonical modules for the ring since we know that binary cubic forms parameterize 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 2.2). Thus from a binary form, we naturally construct a ring and several ideal classes. As we are interested in understanding exactly what data are parameterized by binary forms, the natural questions remaining are: are there more data naturally associated to the form; is some of the data we have already constructed redundant, in other words could it be constructed from other pieces of the data; and what rings and ideal classes actual arise from this construction?

First, we shall see that there is more important structure to the ring and ideal classes that we have constructed. Given a form f, let R be the associated ring, and I be the ideal from $k = n - 3$. From the exact sequences on $\mathbb{P}^1_{\mathbb{Z}}$

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

and

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

we obtain the exact sequences

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

and

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

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, 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

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

Note that 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 $H^0(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(n-3)) = \mathrm{Sym}^{n-3} V$, and $H^1(\mathbb{P}^1_{\mathbb{Z}}, \mathcal{O}(-3)) = V^*$.

In Section 4, we prove that the above algebraic data are precisely the data parameterized by binary n-ic forms.

THEOREM 1.1. *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 I have a $\mathbb{Z}$-module basis $\alpha_1, \alpha_2, \beta_1, \ldots, \beta_{n-2}$ such that*

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

The 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. So we see here that only one of the ideal classes constructed is really new data, since the binary form, and thus all its associated ideal classes, can be recovered from R, I, and the exact sequence above.

All of the work in the paper 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 $\mathcal{O}_S$ be its sheaf of regular functions. A *binary n-ic form* over S is a locally free rank 2 $\mathcal{O}_S$-module V, and a global section $f \in \mathrm{Sym}^n V$. An l-twisted binary n-ic form over S is a locally free rank 2 $\mathcal{O}_S$-module V, and a global section $f \in \mathrm{Sym}^n V \otimes (\wedge^2 V)^{\otimes l}$. 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, 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 4.

THEOREM 1.2. *For $n \geqslant 3$, 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 an isomorphism of the moduli stack of (-1)-twisted binary n-ic forms and the moduli stack of binary n-pairs.*

Analogs of Theorem 1.2 can be proved for l-twisted binary forms for all l. We have already given the idea of a geometric construction for one direction of the bijection in Theorem 1.2 (see Section 3 for the details), and we now give a simple construction of the other direction of the bijection. We can write the construction of a (-1)-twisted binary n-ic form from a binary n-pair as the evaluation

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

of the above 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 4.4).

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

2.1. *Concrete construction*

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

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

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

$$\begin{aligned}
\zeta_0 &= 1, \\
\zeta_1 &= f_0\theta, \\
\zeta_2 &= f_0\theta^2 + f_1\theta, \\
&\vdots \\
\zeta_k &= f_0\theta^k + \ldots + f_{k-1}\theta, \\
&\vdots \\
\zeta_{n-1} &= f_0\theta^{n-1} + \ldots + f_{n-2}\theta.
\end{aligned} \tag{2.1}$$

Since $f_0 \neq 0$, we have that R_f is a free rank n $\mathbb{Z}$-module, that is, *a rank n ring* in the terminology of Bhargava [**2**]. Birch and Merriman [**3**] studied this $\mathbb{Z}$-submodule of Q_f, and Nakagawa [**13**, 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:

$$\zeta_i\zeta_j = -\sum_{\max(i+j-n,1)\leqslant k\leqslant i} f_{i+j-k}\zeta_k + \sum_{j<k\leqslant\min(i+j,n)} f_{i+j-k}\zeta_k \quad \text{for } 1 \leqslant i,j \leqslant n-1, \tag{2.2}$$

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 2.2). We have the discriminant equality $\operatorname{Disc} R_f = \operatorname{Disc} f$ (see, for example, [**14**, Proposition 4]), which is a point of interest in R_f in previous works (for example, [**13**, **14**]).

Remark 1. Throughout this paper, it will be useful to also make the above construction with $\mathbb{Z}$ replaced by $\mathbb{Z}[f_0,\ldots,f_n]$, where the f_i are formal variables, and with $f = f_0x^n + \ldots + f_ny^n$, which we call the *universal form*. If K is the fraction field of $\mathbb{Z}[f_0,\ldots,f_n]$, we can then work in $K[\theta]/(f_0\theta^n + f_1\theta^{n-1} + \ldots + f_n)$ instead of $\mathbb{Q}[\theta]/(f_0\theta^n + f_1\theta^{n-1} + \ldots + f_n)$. The multiplication table in Equation (2.2) 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 2.3. (See also [**13**, Proposition 1.2] for a direct proof of the invariance of R_f, and [**14**, 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 $0 \leqslant k \leqslant n-1$:

$$I_f^k = \langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}\rangle_{\mathbb{Z}}, \tag{2.3}$$

where $\langle s_1, \ldots, s_n \rangle_R$ denotes the R-module generated by $s_1, \ldots, s_n$. Equivalently to Equation (2.3), we have, for $0 \leqslant k \leqslant n-1$,

$$I_f^k = \langle 1, \theta, \ldots, \theta^k, f_0\theta^{k+1}, f_0\theta^{k+2} + f_1\theta^{k+1}, \ldots, f_0\theta^{n-1} + f_1\theta^{n-2} + \ldots + f_{n-k-2}\theta^{k+1} \rangle_{\mathbb{Z}}. \quad (2.4)$$

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 A.1 in the Appendix (Section A) 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 actually ideals.

If we look at the $\mathbb{Z}$ bases of I_f^2, I_f^1, and I_f^0 given in Equation (2.4), they naturally lead to considering another $\mathbb{Z}$-module (given by Equation (2.4) when $k = -1$)

$$I_f^{\#} = \langle f_0, f_0\theta + f_1, \ldots, f_0\theta^{n-1} + f_1\theta^{n-2} + \ldots + f_{n-1} \rangle_{\mathbb{Z}}. \quad (2.5)$$

It turns out that $I_f^{\#}$ is an ideal of R_f, which is shown in Proposition A.3 in the Appendix (Section A). This ideal is studied in the case of f irreducible and primitive as $\mathfrak{b}$ in [**14**, **16**] and as $\mathfrak{B}$ in [**6**].

REMARK 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 $f = f_0x^n + \ldots + f_ny^n$, working in $K[\theta]/(f_0\theta^n + f_1\theta^{n-1} + \ldots + f_n)$. The ideals have $\mathbb{Z}[f_0, \ldots, f_n]$-module bases as given in Equations (2.3)–(2.5), 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 (proved in Proposition A.4 of the Appendix (Section A)). A form f is *primitive* if its coefficients generate the unit ideal in $\mathbb{Z}$.

PROPOSITION 2.1. *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 where f is primitive, $I_f^{-1} = I_f^{\#}$.*

When f is primitive, Simon [**15**, Proposition 3.2] proved that the ideal classes of what we call I_f and $I_f^{\#}$ are inverses. 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 3.7.

THEOREM 2.2. *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 [**16**, Proposition 14] independently discovered that when f is primitive and irreducible, $(I_f^{\#})^{2-n}$ is in the ideal class of the inverse different of R_f. In this paper, 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 the zero form! When $f \equiv 0$,

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.

COROLLARY 2.3. *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 2.1. □

REMARK 3. 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. Also, in this case $I_f^k \cong I_f^{\#} \cong R_f$ as R_f-modules.

2.2. *Explicit multiplication and action tables*

If a form $f = f_0x^n + f_1x^{n-1}y + \ldots + f_ny^n$ 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 can then 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 $f \equiv 0$.

Given a base ring B, if we form a rank n B-module $R = Br_1 \oplus \ldots \oplus Br_n$, 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 and associative, and e is a multiplicative identity (which is a question 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 $I = B\alpha_1 \oplus \ldots \oplus B\alpha_m$, 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 where 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 $f \equiv 0$ or to study the form $f = x^2y + xy^2$ when we replace $\mathbb{Z}$ with $\mathbb{Z}/2\mathbb{Z}$), we see that we can define a ring $\mathcal{R}_f$ from the multiplication table given in Equation (2.2). 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.

Equations (2.3) and (2.5) display $\mathbb{Z}$-module bases of I_f and $I_f^{\#}$, respectively. 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 A.1 and A.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 $1 \leqslant k \leqslant n-1$. We use the action table of I_f^k with the basis of Equation (2.3). 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 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.

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 where $f_0 = 0$ and see easily the $\mathrm{GL}_2(\mathbb{Z})$ invariance of our constructions. A binary n-ic form f describes a subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ that 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 2.4. *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 $1 \leqslant k \leqslant n-1$, 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 2.5. *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 $\sum_{i \geqslant -k} a_i x^{k+i} y^{-i} \mapsto 0$, with $a_i \in \mathbb{Z}$, then $\sum_{i \geqslant -k} a_i x^{k+i} y^{-i} = \sum_j d_j x^j y^{k-n-j} f$, where $d_j \in \mathbb{Z}$. Since $\sum_{i \geqslant -k} a_i x^{k+i} y^{-i}$ has no terms of negative degree in x and $f_n \neq 0$, we conclude that $d_j = 0$ for $j < 0$. Thus, $\sum_{i \geqslant -k} a_i x^{k+i} y^{-i}$ is 0 in $\Gamma(U_y, \mathcal{O}_{S_f}(k))$. □

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 $1 \leqslant m \leqslant n-k-1$, we have

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

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 $p = \sum_{i \geqslant -k} a_i x^{k+i} y^{-i} = \sum_{i \leqslant -k} b_i x^{-i} y^{k+i}$ with $a_i, b_i \in \mathbb{Z}$. If $a = \sum_{i \geqslant -k} a_i x^{k+i} y^{-i} \in \Gamma(U_y, \mathcal{O}_{S_f}(k))$ and $b = \sum_{i \leqslant 0} b_i x^{-i} y^{k+i} \in \Gamma(U_x, \mathcal{O}_{S_f}(k))$, then we

have a formal equality $a - b = \sum_i c_i x^i y^{k-i-n} f$ (in $\mathbb{Z}[x, x^{-1}, y, y^{-1}]$), where $c_i \in \mathbb{Z}$. We can assume without loss of generality that $c_i = 0$ for $i \geqslant 0$ because any $c_i x^i y^{k-i-n} f$, with i non-negative, we could just subtract from the representation a to obtain another such representation of p in $\Gamma(U_y, \mathcal{O}_{S_f}(k))$. Similarly, we can assume that $c_i = 0$ for $i \leqslant k - n$. 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 $x^k, x^{k-1}y, \ldots, y^k$ 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, $a \in \langle x^k, x^{k-1}y, \ldots, y^k, z_1, \ldots, z_{n-1-k} \rangle_{\mathbb{Z}}$.

For $k \geqslant 0$, when we map $\langle x^k, x^{k-1}y, \ldots, y^k, z_1, \ldots, z_{n-1-k} \rangle_{\mathbb{Z}}$ to Q_f via $x \mapsto \theta$ and $y \mapsto 1$, the image is the free rank n $\mathbb{Z}$-module $\langle 1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1} \rangle_{\mathbb{Z}}$. Thus, the map is an isomorphism of $\langle x^k, x^{k-1}y, \ldots, y^k, z_1, \ldots, z_{n-1-k} \rangle_{\mathbb{Z}}$, 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 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 although $\mathcal{O}_{S_f}(k)$ 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, for non-zero f and $1 \leqslant k \leqslant n-1$, that $\Gamma(\mathcal{O}_{S_f}(k))$ is an invertible $\Gamma(\mathcal{O}_{S_f})$-module exactly when f is primitive.

THEOREM 2.6. *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 2.4 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 2.1, if S_f is affine, then f is primitive. 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 (2.2)) that the fiber of a over (p) is the non-reduced n-dimensional point $\operatorname{Spec} \mathbb{Z}_{/(p)}[x_1, x_2, \ldots, x_{n-1}]/(x_i x_j)_{1 \leqslant i,j \leqslant n-1}$, 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 A.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 A.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 $a(x/y)^m = bu$. Thus,

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

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 y/x is 0 at p. Since in $\Gamma(U_y \cap U_x, \mathcal{O}_{S_f})$ we have $a = bu(y/x)^m$, this is also true in $\Gamma(U_x, \mathcal{O}_{S_f}) \cong \mathbb{Z}[y/x]/(f/x^n)$ (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 [**11**, 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 $\mathbb{P}^1_{\mathbb{Z}/p\mathbb{Z}}$, but $\operatorname{Spec} R_f$ has a non-reduced n-dimensional point. □

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 $f \equiv 0$. It may seem at first that $f \equiv 0$ is a pesky, uninteresting case, but we shall eventually want to reduce a form so that its coefficients are in $\mathbb{Z}/p\mathbb{Z}$, 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 by p, will give a rank n ring $\Gamma(\mathcal{O}_{S_f})$, but the reduction $\bar{f}$ of f to $\mathbb{Z}/p\mathbb{Z}$ would give $S_{\bar{f}} = \mathbb{P}^1_{\mathbb{Z}/p\mathbb{Z}}$ and thus a ring of global functions that is rank 1 over $\mathbb{Z}/p\mathbb{Z}$.

We can, however, make the following construction, which was given for $n = 3$ by Deligne in a letter [**7**] 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:

$$R = H^0 R\pi_* (\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}). \tag{2.6}$$

(Here we are taking the zeroth right hyper-derived functor of the pushforward by $\pi : \mathbb{P}^1_{\mathbb{Z}} \to \operatorname{Spec} \mathbb{Z}$ on this complex. Alternatively, we push forward 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 quasi-isomorphic to $\mathcal{O}/f(\mathcal{O}(-n)) \cong \mathcal{O}_{S_f}$ (as a chain complex in the zeroth degree). The quasi-isomorphism 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 $f \equiv 0$ we have

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

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 2.2, which used the coefficients of f to give a multiplication table for $\mathcal{R}_f$. So we see that 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 $f \equiv 0$.

THEOREM 2.7. *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 2.2.*)*

Proof. The proof of Theorem 2.4 shows that $\mathcal{R}_f \cong H^0 R\pi_* \left(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}\right)$ for the universal form $f = f_0 x^n + f_1 x^{n-1} y + \ldots + f_n y^n$ with coefficients in $\mathbb{Z}[f_0, \ldots, f_n]$. Since both the construction of $\mathcal{R}_f$ from the multiplication table in Section 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 shall see in Theorem 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 $\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)$:

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

where all maps are the natural ones.

THEOREM 2.8. *For all binary n-ic forms f and $-1 \leqslant k \leqslant n-1$, 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 the same as that of Theorem 2.7. □

We have the following nice corollary of Theorems 2.7 and 2.8.

COROLLARY 2.9. *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. *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 now develop our theory over an arbitrary base scheme S. When $S = \operatorname{Spec} B$, we sometimes say we are working over a base ring B and we 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 $\mathcal{H}om_{\mathcal{O}_S}(M, \mathcal{O}_S)$. 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 $f \in \mathrm{Sym}^n V$. 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 $\mathcal{O}_S x \oplus \mathcal{O}_S y$, then we call f a *free* binary form.

Given a binary form $f \in \mathrm{Sym}^n V$ over a base scheme S, the form f determines a subscheme S_f of $\mathbb{P}(V)$ (where we define $\mathbb{P}(V) = \mathrm{Proj}\,\mathrm{Sym}^* V$). 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

$$\mathcal{R}_f := H^0 R\pi_* \left(\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}\right), \tag{3.1}$$

where $\mathcal{O}(-n) \xrightarrow{f} \mathcal{O}$ is a complex in degrees -1 and 0. (In Section 2.4 this point of view is worked out in detail over $S = \mathrm{Spec}\,\mathbb{Z}$.) 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

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

as in Section 2.4. Similarly, we can define an $\mathcal{R}_f$-module

$$\mathcal{I}_{f\,k} := H^0 R\pi_* \left(\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)\right) \tag{3.2}$$

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 $\mathrm{Sym}^n V$. Again, when $\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)$ is injective, we have

$$\mathcal{I}_{f\,k} = \pi_*(\mathcal{O}_{S_f}(k))$$

for all $k \in \mathbb{Z}$.

Example 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 $\mathrm{Spec}\,\mathbb{Z}$ the form f cuts out $\mathrm{Spec}\,R_{p(f)}$, 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 $\mathrm{Spec}\,\mathbb{Z}$, 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 pushing forward $\mathcal{O}_{S_f}(k)$ to S, the constructions of $\mathcal{R}_f$ and $\mathcal{I}_{f\,k}$ for $-1 \leqslant k \leqslant n-1$ commute with base change.

Theorem 3.2. *Let $f \in \mathrm{Sym}^n V$ be a binary form over a base scheme S. The construction of $\mathcal{R}_f$ and $\mathcal{I}_{f\,k}$ for $-1 \leqslant k \leqslant n-1$ commutes with base change. More precisely, let $\phi : T \to S$ be a map of schemes. Let $\phi^* f \in \mathrm{Sym}^n \phi^* V$ be the pullback of f. Then the natural map from cohomology*

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

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

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

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 (3.6) in the next section. In particular, $\mathcal{C}(k)$ does not have any cohomology in degrees other than 0. Since $k \leqslant n-1$, we have that $H^0 R\pi_*(\mathcal{O}(-n+k)) = 0$ and thus $H^{-1} R\pi_*(\mathcal{C}(k)) = 0$. Since $k \geqslant -1$, we have that $H^1 R\pi_*(\mathcal{O}(k)) = 0$ and thus $H^1 R\pi_*(\mathcal{C}(k)) = 0$. Moreover, in Section 3.1, 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 [**10**, Corollaire 6.9.9], we have that cohomology and base change commute. □

In the case where 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 (2.2) and $\mathcal{I}_{f\,k}$ for $-1 \leqslant k \leqslant n-1$ as a free rank n $\mathcal{O}_S$-module using the action tables for the Equations (2.3) and (2.5) bases. (See Section 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 2.4 works over $\mathbb{Z}[f_0, \ldots, f_n]$) we see, as in Theorem 2.7, that, for free binary forms and $-1 \leqslant k \leqslant n-1$, 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

$$\mathcal{R}_f := H^0 R\pi_* \left(\mathcal{O}(-n) \otimes (\pi^* \wedge^2 V)^{\otimes -l} \xrightarrow{f} \mathcal{O}\right), \tag{3.3}$$

and

$$\mathcal{I}_{f\,k} := H^0 R\pi_* \left(\mathcal{O}(-n+k) \otimes (\pi^* \wedge^2 V)^{\otimes -l} \xrightarrow{f} \mathcal{O}(k)\right) \tag{3.4}$$

or

$$\mathcal{I}'_{f\,k} := H^0 R\pi_* \left(\mathcal{O}(-n+k) \otimes (\pi^* \wedge^2 V) \xrightarrow{f} \mathcal{O}(k) \otimes (\pi^* \wedge^2 V)^{\otimes l+1}\right). \tag{3.5}$$

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 3.2, we find that these constructions also commute with base change for $-1 \leqslant k \leqslant n-1$. 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 B.3 and B.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.

3.1. *Long exact sequence of cohomology*

In this section, we use the long exact sequence of cohomology to find the $\mathcal{O}_S$-module structures of the rings and modules we have constructed, and important relationships between these $\mathcal{O}_S$-module structures. From the short exact sequence of complexes in degrees -1 and 0

$$\begin{array}{ccc} & & \mathcal{O}(k) \\ & & \downarrow \\ \mathcal{O}(-n+k) & \xrightarrow{f} & \mathcal{O}(k) \\ \downarrow & & \\ \mathcal{O}(-n+k) & & \end{array} \tag{3.6}$$

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

$$\begin{aligned} H^0 R\pi_* \mathcal{O}(-n+k) \longrightarrow H^0 R\pi_* \mathcal{O}(k) \longrightarrow H^0 R\pi_* (\mathcal{O}(-n+k) \xrightarrow{f} \mathcal{O}(k)) \\ \longrightarrow H^1 R\pi_* \mathcal{O}\,(-n+k) \longrightarrow H^1 R\pi_* \mathcal{O}(k). \end{aligned}$$

For $k \leqslant n-1$, we have $H^0 R\pi_* \mathcal{O}(-n+k) = 0$ and for $k \geqslant -1$, we have $H^1 R\pi_* \mathcal{O}(k) = 0$. Also, $H^0 R\pi_* \mathcal{O}(k) = \operatorname{Sym}^k V$ and $H^1 R\pi_* \mathcal{O}(-n+k) = (\operatorname{Sym}^{n-k-2} V)^* \otimes (\wedge^2 V)^*$. Thus for $1 \leqslant k \leqslant$

$n-1$ and a binary form $f \in \mathrm{Sym}^n V$, we have the exact sequence

$$0 \longrightarrow \mathrm{Sym}^k V \longrightarrow \mathcal{I}_{f_k} \longrightarrow (\mathrm{Sym}^{n-k-2} V)^* \otimes (\wedge^2 V)^* \longrightarrow 0. \tag{3.7}$$

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 have

$$0 \longrightarrow \mathrm{Sym}^k V \longrightarrow \mathcal{I}_{f_k} \longrightarrow (\mathrm{Sym}^{n-k-2} V)^* \otimes (\wedge^2 V)^{\otimes -l-1} \longrightarrow 0 \tag{3.8}$$

or

$$0 \longrightarrow \mathrm{Sym}^k V \otimes (\wedge^2 V)^{\otimes l+1} \longrightarrow \mathcal{I}'_{f_k} \longrightarrow (\mathrm{Sym}^{n-k-2} V)^* \longrightarrow 0. \tag{3.9}$$

In Section 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 the concrete construction of $\mathcal{R}_f$ and $\mathcal{I}_{f_k}$ in Section 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 $Q_f := K[\theta]/(f_0\theta^n + f_1\theta^{n-1} + \ldots + f_n)$ and are given by Equations (2.1) and (2.3).

PROPOSITION 3.3. *For the universal form f, where V is a free module on x and y, in the exact sequence of Equation (3.8) or (3.9) (with $\wedge^2 V$ trivialized by the basis element $x \wedge y$) we have that*

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

and

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

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 $H^i R\pi_*$ with H^i since the base is affine. The short exact sequence of complexes in Equation (3.6) then simplifies to the short exact sequence of sheaves

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

which gives the same long exact sequence leading to Equation (3.7). The identification of $\mathcal{I}_{f_k}$ with global sections is at the end of proof of Theorem 2.4, 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 next 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 2.4, 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 (for example, in [**11**, 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 (3.8). 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, one could prove the following by computation.

PROPOSITION 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* (3.8) *is identified with the natural map* (*see Lemma* B.2 *in the Appendix*)

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

under the identification $R/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1}$ *of Equation* (3.8). *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* (3.9) *is identified with the natural map* (*see Lemma* B.2 *in the Appendix*)

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

under the identification $R/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} V^* \otimes (\wedge^2 V)^{\otimes -l-1}$ *of Equation* (3.8).

3.2. *Dual modules*

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

$$\mathcal{I}_{f_k}' \otimes \mathcal{I}_{f_{n-2-k}} \longrightarrow \mathcal{I}_{f_{n-2}}' \longrightarrow \mathcal{O}_S. \tag{3.10}$$

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 (3.9).

THEOREM 3.5. *The pairing in Equation* (3.10) *gives an* $\mathcal{O}_S$*-module map*

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

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 pullback from the universal form and these constructions commute with base change, the theorem will follow for all forms.

We use the construction of $\mathcal{R}_f$, $\mathcal{I}_{f_k}'$, and $\mathcal{I}_{f_{n-2-k}}$ in Section 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 quasi-isomorphic 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 2.1.

LEMMA 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* (2.4), *but reverse the order to obtain*

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

These are dual basis with respect to the pairing from Equation (3.10).

Proof. From Proposition 3.3, we know that the map $\phi : \mathcal{I}_{f}{}'_{n-2} \to \mathcal{O}_S$ in Equation (3.9) sends $\zeta_{n-1} \mapsto 1$ and $\theta^i \mapsto 0$ for $0 \leqslant i \leqslant n-2$. The proof of this lemma then has four cases.

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

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

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

Since $n-i-1+j+i-n = j-1 \leqslant n-2$, we see that

$$(\zeta_i + f_i)(f_0\theta^j + \ldots + f_{j+k+1-n}\theta^{n-k-1}) \overset{\phi}{\longmapsto} 0.$$

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

If $i+j \leqslant n-2$, then this maps to 0.

If $i+j = n-1$, then this maps to 1.

If $i+j \geqslant n$, then the product is

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

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

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

If $i+j \leqslant n-2$, then this maps to 0.

If $i+j = n-1$, then this maps to 1.

If $i+j \geqslant n$, then the product is $(\zeta_i + f_i)\theta^j = -f_{i+1}\theta^{j-1} - \ldots - f_n\theta^{i+j-n}$, and since $j-1 \leqslant n-2$ 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 3.7. *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 (3.9).

4. *Main theorem for (-1)-twisted binary forms*

In this section, we will see how a binary form is actually equivalent to a certain combination of the data we have constructed from it. 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 (3.8). So, $Q \cong V^*$. From Proposition 3.4, we know that the map $R/\mathcal{O}_S \otimes \mathrm{Sym}^{n-3} Q^* \to Q$ given by the action of R on I and the exact sequence of Equation (3.8) is identified with the natural map $\mathrm{Sym}_{n-2} Q \otimes \mathrm{Sym}^{n-3} Q^* \to Q$ under the identification $R/\mathcal{O}_S \cong \mathrm{Sym}_{n-2} Q$ of Equation (3.8).

Definition. 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 $\mathrm{Sym}_{n-2} Q \otimes \mathrm{Sym}^{n-3} Q^* \to Q$.

REMARK 4. 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 can conclude that a binary 3-pair is just equivalent to a cubic ring, that is, an $\mathcal{O}_S$-algebra R that is a locally free rank 3 $\mathcal{O}_S$-module.

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

PROPOSITION 4.1. *An $\mathcal{O}_S$-algebra R and R-module I are in 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 I has an $\mathcal{O}_S$-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 $\dot{y}$, then 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

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

We have $\zeta_j \in \mathrm{Sym}_{n-2} Q$ corresponding to $\mathrm{sym}(x^{n-j-1} y^{j-1})$, α_1 corresponding to y, 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 4.2. *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 binary pair if and only if*

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

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

Proposition 4.2 follows from the following lemma, proved in Lemma B.5 of the Appendix (Section B).

LEMMA 4.3. *If Q is any locally free rank 2 $\mathcal{O}_S$-module, then we have the exact sequence*

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

The following lemma is used to construct a (-1)-twisted binary form from a binary pair, and is proved in Lemma B.6 of the Appendix (Section B).

LEMMA 4.4. *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*

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

is the zero map, then

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

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 4.2, we see that $\mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q) \to \wedge^2 Q$ is always the zero map for a binary pair, and thus we can use Lemma 4.4 to construct a (-1)-twisted binary form in $\mathrm{Sym}^n Q^* \otimes \wedge^2 Q$ from a binary pair. We can write the map of Lemma 4.4 as the evaluation

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

of a degree n map $Q \to \wedge^2 Q$. Note that this coincides with the map $x \wedge x^2$ as described in the case of binary cubic forms in [1, Footnote 3].

THEOREM 4.5. *Let (V, f) be a (-1)-twisted binary form and (R, I) be its associated 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 is then a pullback from the universal form, we can just check the theorem on the universal form f over $B = \mathbb{Z}[f_0, \dots, f_n]$. 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

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

Thus, for $1 \leqslant k \leqslant n$, we have

$$\begin{aligned} \mathrm{sym}(x^k y^{n-k}) \longmapsto\ & x \wedge \phi(\mathrm{sym}(x^{k-2} y^{n-k}))x + x \wedge \phi(\mathrm{sym}(x^{k-1} y^{n-k-1}))y \\ & + y \wedge \phi(\mathrm{sym}(x^{k-1} y^{n-k-1}))x + y \wedge \phi(\mathrm{sym}(x^k y^{n-k-2}))y \\ =\ & (\dot{y}(\zeta_{n-k+1} x) + \dot{y}(\zeta_{n-k} y) - \dot{x}(\zeta_{n-k} x) - \dot{x}(\zeta_{n-k-1} y)) \otimes (x \wedge y), \end{aligned} \tag{4.1}$$

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 2.1 lie in $Q_f := K[\theta]/(f_0 \theta^n + f_1 \theta^{n-1} + \dots + f_n)$ and are given by Equations (2.1) and (2.3). From Proposition 3.3, we know that we 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 $1, \theta, \dots, \theta^{n-3}$ 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 (2.3) 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 they are being taken with respect to 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 Equation (2.2) to prove the proposition. □

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

THEOREM 4.6. *For $n \geqslant 3$ 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 an 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 $f \in \operatorname{Sym}^n V \otimes \wedge^2 V^*$ and $f' \in \operatorname{Sym}^n V' \otimes \wedge^2 (V')^*$ 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 the isomorphisms $R \cong R'$ and $I \cong I'$, and $Q \cong Q'$ that respect the exact sequence for I (and I') and the maps $R/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} Q$ and $R'/\mathcal{O}_S \cong \operatorname{Sym}_{n-2} Q'$.

See [**19**] for the full story for binary quadratic forms. In the $n = 3$ case, from Remark 4 we know that a binary 3-pair is equivalent to a *cubic ring*, an $\mathcal{O}_S$-algebra R such that R is a locally free rank 3 $\mathcal{O}_S$-module. Thus, we obtain the following corollary, given in [**7**] (see also [**21**] for a detailed exposition of this case).

COROLLARY 4.7. *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 an isomorphism of the moduli stack of (-1)-twisted binary n-ic forms and the moduli stack of cubic rings.*

To prove Theorem 4.6, we rigidify the moduli stacks, and thus we need to define based binary pairs.

4.1. *Based binary pairs*

A *based binary pair* is a 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 $K = (\operatorname{Sym}_{n-3} Q)^* = \ker(I \to Q)$, 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 pick these using certain normalizations.

Let $\zeta_i = \operatorname{sym}(x^{n-1-i} y^{i-1})$ for $1 \leqslant i \leqslant n-1$ be the given basis of $R/\mathcal{O}_S$ and let k_j for $1 \leqslant j \leqslant n-2$ be the given basis of K dual to the basis $\operatorname{sym} x^{j-1} y^{n-2-j}$ of $\operatorname{Sym}_{n-3} Q$. Let $\dot{x}, \dot{y} \in Q^*$ be a dual basis of x, y. (Recall that $\operatorname{sym}(w)$ for a word w is the sum of all distinct permutations of w.) Thus, from Proposition 4.1,

$$\text{the image of } \zeta_i k_j \text{ in } Q \text{ is } \begin{cases} x & \text{if } i+j = n-1, \\ y & \text{if } i+j = n, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

Equation (4.2) allows us to choose normalized lifts of x and y to elements of I, which form 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

$$\dot{y}(\zeta_i x) = 0 \quad \text{for } 2 \leqslant i \leqslant n-1 \tag{4.3}$$

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

$$\dot{x}(\zeta_i x) = 0 \quad \text{for } 1 \leqslant i \leqslant n-1 \tag{4.4}$$

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

$$\dot{y}(\zeta_i y) = 0 \quad \text{for } 2 \leqslant i \leqslant n-1 \tag{4.5}$$

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 shall refer to now simply as x, y, and ζ_i. We 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 pair.

There are only $n+1$ coordinates that we have not determined in the maps $\zeta_i : I \to Q$. Equation (4.2) 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 $1 \leqslant i \leqslant n-1$. Let $a_0 = \dot{y}(\zeta_1 x)$ and $a_1 = \dot{y}(\zeta_1 y)$. These a_i specify the map $\zeta_i : I \to Q$. We have carefully indexed and signed the a_i so that we have the following.

PROPOSITION 4.8. *The (-1)-twisted binary form associated to the above based binary pair is*

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

Proof. We use the formula from Equation (4.1). □

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

PROPOSITION 4.9. *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 entries of these matrices that are determined by the entries in the last two rows of the matrices as polynomials in the a_i (that is, the maps $\zeta_i : I \to Q$), as well 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 $1 \leqslant i \leqslant n-1$ and $1 \leqslant k \leqslant n$.

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

LEMMA 4.10. *We have*

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

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 4.11. *We have*

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

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 $1 \leqslant i \leqslant n-1$. 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 4.10, we see that that all matrix entries in the $n-1-i$th row are in $\mathcal{K}$. (If $i = 0$ this is from the definition of $\mathcal{K}$.) Using Lemma 4.11, then 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 (4.2), we see that since $n \geqslant 3$, 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 4.6.

Proof. The stack of binary n-pairs is the quotient of the stack of based binary n-pairs by the GL_2 action given by change of the basis for Q. Since a based 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 sections a_i (given by the corresponding binary form), the moduli space of based binary n-pairs is $\mathbb{Z}[a_0, \ldots, a_n]$, and there is a universal based binary n-pair.

We have maps between the stack of (-1)-twisted binary n-ic forms and binary n-pairs in both directions, which lift to the rigidified versions of these stacks, the stacks of corresponding based objects. Theorem 4.5 shows that the map from forms to pairs and 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 binary n-pair, Proposition 4.8 shows that the associated form is the universal binary n-ic form. From the universal binary n-ic form, we construct some based binary n-pair (R, I), and Proposition 4.9 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 binary n-pair and (R, I) both give the same form, by Proposition 4.9 they are the same. Thus, we have proved there is an isomorphism of the moduli stack of (-1)-twisted binary n-ic forms and the moduli stack of 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 that some of the constructions are more natural when working with $\mathcal{I}_{f'_{n-3}}$ and binary pairs, so we have used that version in this exposition.

One can prove analogs of Theorem 4.6 for all l-twisted binary forms. We define a *k-twisted binary n-pair* as 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 have an $(l+1)$-twisted binary pair from $\mathcal{R}_f$, $\mathcal{I}_{f'_{n-3}}$, and the exact sequence from Equation (3.9).

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 that I was a principal R-module in a binary 3-pair. So, we see that I is determined uniquely by R and Q. 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.

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 [**18**] 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 [**14**] asks which maximal orders are constructed 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. In general, it would be very interesting to understand which maximal orders are associated to binary forms.

Appendix A. Verifications of $\mathbb{Z}$ basis of I_f^k

PROPOSITION A.1. *For f with $f_0 \neq 0$ and $1 \leqslant k \leqslant n-1$, the R_f module I_f^k is a free rank n $\mathbb{Z}$-module on the basis given in Equation 2.3.*

LEMMA A.2. *We have*

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

for all $k \geqslant 1$.

Proof of Lemma A.2. We see that

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

and

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

□

Proof of Proposition A.1. So, as a $\mathbb{Z}$-module I_f^k is generated by $1, \theta, \ldots, \theta^k, \zeta_{k+1}, \ldots, \zeta_{n-1}$ for $k \geqslant 1$. If $k \leqslant n-1$, 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 A.3. *The $\mathbb{Z}$-module $I_f^{\#}$ defined by Equation (2.5) 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 (2.2), 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 $I_f^{\#}$ are ideals of R_f. □

PROPOSITION A.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 where 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 $x_i \in \mathbb{Z}$. 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 that 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 that $I_f^\#$ 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. □

Appendix B. Maps between locally free $\mathcal{O}_S$-modules

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

LEMMA B.1. *Let V be a locally free $\mathcal{O}_S$ module. We have $(\mathrm{Sym}_n V)^* \cong \mathrm{Sym}^n V^*$.*

LEMMA B.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*

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

which is injective.

LEMMA B.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 $\mathrm{Sym}^k(V \otimes L) \cong \mathrm{Sym}^k V \otimes L^{\otimes k}$.*

LEMMA B.4. *If V is a locally free $\mathcal{O}_S$-module of rank 2, then $V \otimes \wedge^2 V^* \cong V^*$.*

LEMMA B.5. *If Q is any locally free rank 2 $\mathcal{O}_S$-module, we have the exact sequence*

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

Proof. We can check that 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 $0 \leqslant k \leqslant n-1$. A basis for $Q \otimes \mathrm{Sym}_{n-2} Q$ is

given by

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

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 B.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*

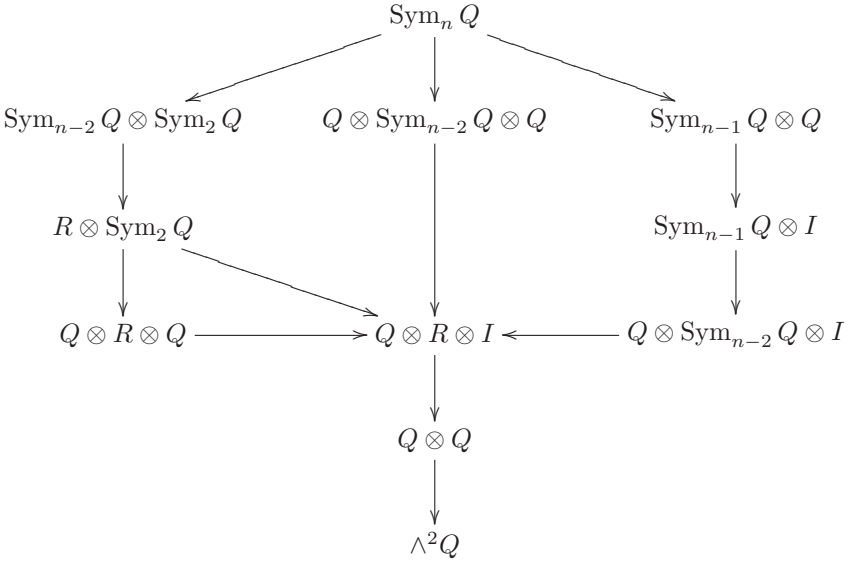
$$\begin{array}{ccc}\mathrm{Sym}_{n-1} Q \otimes \ker(I \to Q) & \longrightarrow & \wedge^2 Q\\ q_1 \dots q_{n-1} \otimes k & \longmapsto & q_1 \wedge \phi(q_2 \dots q_{n-1}) \circ k\end{array}$$

is the zero map, then

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

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 B.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.

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. □

Acknowledgements. The author would like to thank Manjul Bhargava for asking the questions that inspired this research, guidance along the way, and helpful feedback both on the ideas and the exposition in this paper. She would also like to thank Lenny Taelman and Keith Conrad for suggestions for improvements to the paper.

References

1. M. Bhargava, 'Higher composition laws. II. On cubic analogues of Gauss composition', *Ann. of Math.* (2) 159 (2004) 865–886.
2. M. Bhargava, 'Higher composition laws. III. The parametrization of quartic rings', *Ann. of Math.* (2) 159 (2004) 1329–1360.
3. B. J. Birch and J. R. Merriman, 'Finiteness theorems for binary forms with given discriminant', *Proc. London Math. Soc.* (3) 24 (1972) 385–394.
4. H. Davenport and H. Heilbronn, 'On the density of discriminants of cubic fields. II', *Proc. Roy. Soc. London Ser. A* 322 (1971) 405–420.
5. R. Dedekind, 'Supplement X', *Vorlesungen über Zahlentheorie* (ed. P. G. L. Dirichlet; Vieweg, 2nd edn, 1871).
6. I. Del Corso, R. Dvornicich and D. Simon, 'Decomposition of primes in non-maximal orders', *Acta Arith.* 120 (2005) 231–244.
7. P. Deligne, letter to W. T. Gan, B. Gross and G. Savin, November 13, 2000.
8. B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree* (American Mathematical Society, Providence, RI, 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).)
9. W. T. Gan, B. Gross and G. Savin, 'Fourier coefficients of modular forms on G_2', *Duke Math. J.* 115 (2002) 105–169.
10. A. Grothendieck, Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. II, Publ. Math. Inst. Hautes Études Sci. 17 (1963) 1–91.
11. R. Hartshorne, *Algebraic geometry* (Springer, New York, 1977).
12. M. Kneser, 'Composition of binary quadratic forms', *J. Number Theory* 15 (1982) 406–413.
13. J. Nakagawa, 'Binary forms and orders of algebraic number fields', *Invent. Math.* 97 (1989) 219–235.
14. D. Simon, 'The index of nonmonic polynomials', *Indag. Math. (N.S.)* 12 (2001) 505–517.
15. D. Simon, 'La classe invariante d'une forme binaire', *C. R. Math. Acad. Sci. Paris* 336 (2003) 7–10.
16. D. Simon, 'A "class group" obstruction for the equation $Cy^d = F(x, z)$', *J. Théor. Nombres Bordeaux* 20 (2008) 811–828.
17. J. Towber, 'Composition of oriented binary quadratic form-classes over commutative rings', *Adv. Math.* 36 (1980) 1–107.
18. M. M. Wood, 'Quartic rings associated to binary quartic forms', Preprint, arXiv:1007.5501v1, http://arxiv.org/abs/1007.5501.
19. M. M. Wood, 'Gauss composition over an arbitrary base', *Adv. Math.* 226 (2011) 1756-1771.
20. M. M. Wood, 'Parametrization of ideal classes in rings associated to binary forms', Preprint, arXiv:1008.4781v1, http://arxiv.org/abs/1008.4781.
21. M. M. Wood, 'Parametrizing quartic algebras over an arbitrary base', *Algebra & Number Theory*, to appear.

Melanie Matchett Wood
American Institute of Mathematics
360 Portage Ave
Palo Alto, CA 94306-2244
USA

and

Stanford University
Department of Mathematics
Building 380, Sloan Hall
Stanford, CA 94305
USA

mwood@math.stanford.edu