Binary Forms, Quintic Rings & Sextic Resolvents

Dan Fess

16th April 2021

Chapter 1

Introduction

By a construction of Birch and Merriman, we can attach to a binary quintic form f a quintic ring R_f. Not all quintic rings are produced this way; the forms describe a certain subclass of quintic rings. What is special about this subclass? Which quintic rings are these? We can also associate to a quintic ring a sextic resolvent ring; perhaps there is something special about the sextic resolvent?

Another problem we can hope to understand is the number of $GL_2(\mathbb{Z})$-classes of binary quintic forms of bounded discriminant. The collection of all quintic rings is described by the space $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, which naturally has an action of $\Gamma = GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$. If we can find a discriminant-preserving, orbit-preserving map from binary quintic forms to this space, then we can hope to translate our knowledge of orbits in $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ to study classes of binary quintics.

1.1 Results

Denote a generic element $f \in (Sym^5\mathbb{Z}^2)^*$ by $f = f_0x^5 + f_1x^4y + f_2x^3y^2 + f_3x^2y^3 + f_4xy^4 + f_5y^5$.

Theorem 1. *There is a map $\Phi : (Sym^5\mathbb{Z}^2)^* \to \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ which respects the two constructions of quintic rings. Furthermore, it is discriminant- and orbit-preserving. Explictly:*

$$\Phi(f) = \begin{pmatrix} 0 & t_3 & -t_2 & t_1 & 0 \\ -t_3 & 0 & -f_0t_1 - f_1t_2 & -f_2t_2 - f_3t_3 & -t_4 \\ t_2 & f_0t_1 + f_1t_2 & 0 & -f_4t_3 - f_5t_4 & t_3 \\ -t_1 & f_2t_2 + f_3t_3 & f_4t_3 + f_5t_4 & 0 & -t_2 \\ 0 & t_4 & -t_3 & t_2 & 0 \end{pmatrix}$$

For $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, denote the associated based quintic ring by $R(A)$ and the based sextic resolvent ring by $S(A)$. This theorem tells us that $R_f = R(\Phi(f))$, but the more interesting ramification is that it gives us access to the sextic resolvent ring $S(\Phi(f))$, which we denote by S_f. We can explicitly compute its multiplicative structure, and find out that the sextic resolvent rings coming from binary quintic forms have the following unusual structure:

Definition 1.1.1. *Let (R, S) be a quintic ring / sextic resolvent pair, with both rings of non-zero discriminant. Consider S as a based ring, with basis denoted by $\{1, \beta_1, \ldots, \beta_5\}$. Denote the dual basis with respect to the trace pairing by $\{\beta_0^*, \beta_1^*, \ldots, \beta_5^*\}$, i.e. $\beta_i^* \in S \otimes \mathbb{Q}$ such that $Tr(\beta_i^* \beta_j) = \delta_{ij}$.*

Then, we say that the based ring S is dual-digenic *if it has the following property:*

$$(\beta_2, \beta_3, \beta_4) \equiv 8\, Disc(R) \cdot ((\beta_1^*)^2, 2\beta_1^*\beta_5^*, (\beta_5^*)^2)\ mod\ \mathbb{Q} \tag{1.1}$$

This can also be rephrased in terms of $Disc(S)$ using $Disc(S) = (16 \cdot Disc(R))^3$.

We also define a (non-based) ring S to be dual-digenic if it has a basis in which it is dual-digenic.

Theorem 2. *Let f be a binary quintic form of non-zero discriminant $\Delta(f)$. Then, the based ring S_f is dual-digenic.*

Nakagawa proved that if f and g are $GL_2(\mathbb{Z})$-equivalent binary quintic forms, their associated quintic rings R_f and R_g are isomorphic, but have different canonical bases; the $GL_2(\mathbb{Z})$ action induces this change of basis of the quintic ring, and can equally be viewed as a $GL_2(\mathbb{Z})$ action on $R_f/\mathbb{Z} \simeq \mathbb{Z}^4$. Similarly, in the sextic resolvent ring, the $GL_2(\mathbb{Z})$ action induces a change of basis and a corresponding change of dual basis, which respect the special property of dual-digenicity.

Theorem 3. *Let f, g be binary quintic forms with $\gamma \in GL_2(\mathbb{Z})$ such that $g = \gamma \cdot f$. Then, S_f and S_g have different canonical bases but are isomorphic in a way that respects dual-digenicity, i.e. γ acts linearly on $sp\{\beta_1^*, \beta_5^*\}$ and quadratically on $sp\{\beta_2, \beta_3, \beta_4\}$.*

We would like to exactly pin down the quintic ring / sextic resolvent pairs (R, S) given by binary quintics. Thus, we need to know if this property is sufficient for the pair to have come from a binary quintic. With an extra condition on the alternating matrix A, there is indeed a basis of R such that it comes from a binary quintic form:

Theorem 4. *Let (R, S) be a quintic ring / sextic resolvent pair, basis-free, of non-zero discriminant, with fundamental alternating map $\phi : \wedge^2 \tilde{S} \to \tilde{R}$. Then, (R, S) arise from some binary quintic form if and only if the following two conditions hold:*

- *S has a basis $\{1, \beta_1, \ldots, \beta_5\}$ in which it is dual-digenic*
- *The associated dual basis has the property $\phi(\beta_1^*, \beta_5^*) = 0$*

By studying the action of various groups involved in this picture, we can upgrade this theorem so that it concerns classes of binary quintic forms. This theorem involves the notion of a choice of dual-digenization, which will be defined later, in Section 5; in short, it recognises the different ways in which a sextic ring can have a dual-digenic basis. Similarly, we shall later define a dual-digenic isomorphism; roughly speaking, this is an isomorphism of dual-digenic sextic rings, which respects their dual-digenizations.

Theorem 5. *There is a bijection between the following two sets:*

$$GL_2(\mathbb{Z})\backslash(Sym^5\mathbb{Z}^2)^* \leftrightarrow \left\{ \begin{array}{l} (R,S), R \textit{ basis-free} \\ S \textit{ dual-digenic with a} \\ \textit{fixed dual-digenization} \\ \textit{and } \phi(\beta_1^*, \beta_5^*) = 0 \end{array} \right\} / \sim \tag{1.2}$$

given by $f \mapsto$ the class of (R_f, S_f), where the $\sim$ denotes isomorphism of R and dual-digenic isomorphism of S, and where ϕ is the fundamental alternating map $\wedge^2\tilde{S} \to \tilde{R}$.

The other direction in which we would like to take this work is to count classes of binary quintic forms of bounded discriminant. The number of Γ-orbits in $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ of bounded discriminant is understood, and the map Φ is discriminant- and orbit-preserving, so if we understand Φ well then we can count classes of binary quintics. Specifically, we need to know how many classes of binary quintics can possibly land in one Γ-orbit in $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. The following result goes some way towards this:

Theorem 6. *Let $A \in \mathbb{Z}^5 \otimes \wedge^2\mathbb{Z}^5$. There are two-dimensional varieties $W_{A,1}, W_{A,-1} \subseteq \mathbb{A}^{10}$, given by explicit equations and having finitely many integral points, such that:*

$$\frac{1}{2}(\#W_{A,1}(\mathbb{Z}) + \#W_{A,-1}(\mathbb{Z}) - 2) = \sum_{\{f \, mod \, GL_2(\mathbb{Z}) : \Phi(f) \in \Gamma \cdot A\}} \frac{\#Aut(A)}{\#Aut(f)} \tag{1.3}$$

In particular, the left side of this equation bounds $\#\{f \, mod \, GL_2(\mathbb{Z}) : \Phi(f) \in \Gamma \cdot A\}$.

Chapter 2

Preliminaries

An n-ic ring is a ring which is isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$-module. The canonical example is an order in a degree n number field. In this chapter, we recap some key constructions of and relating to n-ic rings. One of the fundamental constructions is of resolvent rings and resolvent maps; these are ring-theoretic extensions of the classical resolvent polynomials which were used to solve cubic and quartic equations.

2.1 n-ic rings

Definition 2.1.1. *A based n-ic ring is an n-ic ring R with a fixed basis of $R/\mathbb{Z}$.*

The usual definitions of trace and discriminant apply to n-ic rings, and are denoted by $Tr(-)$ and $Disc(-)$ respectively. If an n-ic ring R has non-zero discriminant, we can define the dual basis as follows:

Definition 2.1.2. *Let R be a based n-ic ring, with basis $\mathfrak{B} = \{1, \alpha_1, \ldots, \alpha_{n-1}\}$. If $Disc(R) \neq 0$, the trace pairing on $R \otimes \mathbb{Q}$ is non-degenerate and we can define the dual basis $\mathfrak{B}^* = \{\alpha_0^*, \alpha_1^*, \ldots, \alpha_{n-1}^*\} \subseteq R \otimes \mathbb{Q}$ with respect to this pairing.*

In other words, the α_j^* are uniquely determined by the conditions:

$$Tr(\alpha_i \alpha_j^*) = \delta_{ij} \tag{2.1}$$

where $\alpha_0 = 1$.

Note that $\{\alpha_0^*, \ldots, \alpha_{n-1}^*\}$ spans $R^* = \{z \in R \otimes \mathbb{Q} : Tr(zw) \in \mathbb{Z} \, \forall \, w \in R\}$ and that $\{\alpha_1^*, \ldots, \alpha_{n-1}^*\}$ spans $\tilde{R} = \{z \in R^* : Tr(z) = 0\}$, which can be identified with $(R/\mathbb{Z})^* = Hom(R/\mathbb{Z}, \mathbb{Z})$.

Also note that if we translate α_i by $a_i \in \mathbb{Z}$ for $i \neq 0$, this perturbs only α_0^*, because $0 = Tr(\alpha_0 \alpha_j^*) = Tr(\alpha_j^*)$ for $j \neq 0$. Hence, for a based n-ic ring R, the tuple $(\alpha_1^*, \ldots, \alpha_{n-1}^*)$ is well-defined.

If $Disc(R) \neq 0$, R is an order in an etale algebra and there are n homomorphisms $\rho : R \otimes \mathbb{Q} \to \mathbb{C}$. Applying these homomorphisms to the dual basis enables us to associate to a based n-ic ring R a well-defined set of n points $X_R \subseteq \mathbb{P}^{n-2}$:

Definition 2.1.3. *Let R be a based n-ic ring, with basis $\mathfrak{B}$ and corresponding dual basis $\mathfrak{B}^*$ as above. Denote the n homomorphisms $\rho : R \otimes \mathbb{Q} \to \mathbb{C}$ by $\rho^{(1)}, \ldots, \rho^{(n)}$. Let $P_k = (\rho^{(k)}(\alpha_1^*), \ldots, \rho^{(k)}(\alpha_{n-1}^*))$ for $1 \leq k \leq n$. Then we define $X_R = \{P_1, \ldots, P_n\} \subseteq \mathbb{P}^{n-2}$.*

The lemma below shows that $P_k \neq (0, \ldots, 0)$, so these genuinely define points in $\mathbb{P}^{n-2}$.

Lemma 2.1.4. *$P_k \neq (0, \ldots, 0)$ for any k, and furthermore they lie in general position in the sense that no $n-1$ of them lie on a hyperplane.*

Proof. We use the shorthand $\alpha^{(k)}$ to mean $\rho^{(k)}(\alpha)$.

Define the matrix

$$D = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1^{(1)} & \alpha_1^{(2)} & \ldots & \alpha_1^{(n)} \\ \ldots & & & \ldots \\ \alpha_{n-1}^{(1)} & \alpha_{n-1}^{(2)} & \ldots & \alpha_{n-1}^{(n)} \end{pmatrix} \tag{2.2}$$

Note that $\det(D)^2 = \det(DD^t) = Disc(R) \neq 0$, so D is invertible. In fact, D^{-1} has to do with the dual basis:

$$(D^t)^{-1} = \begin{pmatrix} (\alpha_0^*)^{(1)} & (\alpha_0^*)^{(2)} & \ldots & (\alpha_0^*)^{(n)} \\ (\alpha_1^*)^{(1)} & (\alpha_1^*)^{(2)} & \ldots & (\alpha_1^*)^{(n)} \\ \ldots & & & \ldots \\ (\alpha_{n-1}^*)^{(1)} & (\alpha_{n-1}^*)^{(2)} & \ldots & (\alpha_{n-1}^*)^{(n)} \end{pmatrix} \tag{2.3}$$

If we add all the columns to the last one, because $Tr(\alpha_i^*) = 0$ for all $i \neq 0$ and $Tr(\alpha_0^*) = 1$, we obtain the following matrix:

$$\begin{pmatrix} (\alpha_0^*)^{(1)} & (\alpha_0^*)^{(2)} & \ldots & (\alpha_0^*)^{(n-1)} & 1 \\ (\alpha_1^*)^{(1)} & (\alpha_1^*)^{(2)} & \ldots & (\alpha_1^*)^{(n-1)} & 0 \\ \ldots & & & \ldots & \\ (\alpha_{n-1}^*)^{(1)} & (\alpha_{n-1}^*)^{(2)} & \ldots & (\alpha_{n-1}^*)^{(n-1)} & 0 \end{pmatrix} \tag{2.4}$$

This matrix is invertible, its determinant that of the $(1, n)$-th minor, from which we see that $\{P_1, \ldots, P_{n-1}\}$ is linearly independent.

Applying this trick to each of the columns in turn results in the statement of the lemma. □

We will shortly discuss the theory of rings of small rank n - namely, cubic, quartic and quintic rings. A key component of this theory is that these rings all have an associated resolvent ring which lies inside the Galois closure of $K = R \otimes \mathbb{Q}$, at least when K is a field and has Galois group S_n. In the general case, the resolvent ring lies in what Bhargava calls the "S_n-closure of R". We provide his definition here, followed by some key properties highlighted in Higher Composition Laws IV. More detail is present in that paper.

Definition 2.1.5. *Let R be a ring of rank n having non-zero discriminant, and let $R^{\otimes n}$ denote the n-th tensor power $R^{\otimes n} = R \otimes_{\mathbb{Z}} R \otimes_{\mathbb{Z}} \ldots \otimes_{\mathbb{Z}} R$ of R. Then $R^{\otimes n}$ is a ring of rank n^n in which $\mathbb{Z}$ lies naturally as a subring via the mapping $m \mapsto m(1 \otimes 1 \otimes \ldots \otimes 1)$.*

Denote by I_R the ideal in $R^{\otimes n}$ generated by all elements of the form

$$(x \otimes 1 \otimes \ldots \otimes 1) + (1 \otimes x \otimes \ldots \otimes 1) + \ldots + (1 \otimes 1 \otimes \ldots \otimes x) - Tr(x) \tag{2.5}$$

for $x \in R$. Let J_R denote the $\mathbb{Z}$-saturation of the ideal I_R; i.e. let

$$J_R = \{r \in R^{\otimes n} : mr \in I_R \text{ for some } m \in \mathbb{Z}\} \tag{2.6}$$

The S_n-closure of R is then the ring $\bar{R} = R^{\otimes n}/J_R$.

The ring $\bar{R}$ is of rank $n!$, and S_n acts naturally as a group of automorphisms on $\bar{R}$. Furthermore, $\bar{R}^{S_n} = \mathbb{Z}$. We view R as a subring of $\bar{R}$ via the mapping $\alpha \mapsto \alpha \otimes 1 \otimes \ldots \otimes 1$.

The elements $\{(\alpha \otimes 1 \otimes \ldots \otimes 1), (1 \otimes \alpha \otimes \ldots \otimes 1), \ldots, (1 \otimes 1 \otimes \ldots \otimes \alpha)\}$ are called the S_n-conjugates of α in $\bar{R}$ and behave as we would expect conjugates to. More precisely, if the characteristic polynomial of α in R is $F_\alpha(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \ldots \pm a_n$ with $a_i \in \mathbb{Z}$, then the i-th elementary symmetric polynomial in the S_n-conjugates of α will be congruent to a_i mod J_R.

For instance, if $k = 2$ and $\alpha \in R$ has $F_\alpha(x) = x^2 - a_1 x + a_2$, then $\alpha \otimes \alpha = a_2$ in $\bar{R}$ because:

$$\begin{aligned} 2\alpha \otimes \alpha &= (\alpha \otimes 1 + 1 \otimes \alpha)^2 - (\alpha^2 \otimes 1 + 1 \otimes \alpha^2) && (2.7)\\ &\equiv Tr(\alpha)^2 - Tr(\alpha^2) \bmod I_R && (2.8)\\ &= 2a_2 \bmod I_R && (2.9) \end{aligned}$$

When $K = R \otimes \mathbb{Q}$ is a number field with Galois group S_n and Galois closure N, the ring $\bar{R}$ is isomorphic to the ring generated by all the Galois conjugates of elements of R in N, i.e. $\bar{R}$ is an order in N given by $\bar{R} = \mathbb{Z}[\alpha : \alpha \text{ is } S_n\text{-conjugate to some element of } R]$.

When K is a number field whose Galois group has index k in S_n, the "S_n-closure" of K will be a direct sum of k copies of the Galois closure of K, and the ring $\bar{R}$ will be a subring of this having rank $n!$.

2.2 n-ic rings from binary n-ic forms

Birch and Merriman were the first to study $GL_2(\mathbb{Z})$-classes of binary n-ic forms, and they proved that there are only finitely many such classes of fixed discriminant. Key to the proof of this result was their construction of a based n-ic ring from a binary n-ic form. This construction is a key foundational component in the new work in later chapters of this thesis. We describe the construction below.

Denote the space of integral binary n-ic forms by $(Sym^n\mathbb{Z}^2)^*$.

Definition 2.2.1 (Birch-Merriman)**.** *Let $f = f_0x^n + f_1x^{n-1}y + \ldots + f_ny^n \in (Sym^n\mathbb{Z}^2)^*$ with $f_0 \neq 0$. Let $K = \mathbb{Q}[x]/(f(x,1))$ and let θ be the image of x in K. Define the $\mathbb{Z}$-module $R_f = \mathbb{Z}\{1, \alpha_1, \ldots, \alpha_{n-1}\} \subseteq K$ as follows:*

$$\alpha_1 = f_0\theta \tag{2.10}$$

$$\alpha_2 = f_0\theta^2 + f_1\theta \tag{2.11}$$

$$\ldots$$

$$\alpha_{n-1} = f_0\theta^{n-1} + f_1\theta^{n-2} + \ldots + f_{n-2}\theta \tag{2.12}$$

Then, R_f is in fact a ring. We consider it as a based n-ic ring.

An alternative way of defining R_f is via its multiplication table, whose entries are integer polynomials in the f_i. This definition extends immediately to the case $f_0 = 0$.

A key property of this construction, proved by Birch and Merriman, is the following:

Lemma 2.2.2 (Birch-Merriman)**.** *$Disc(R_f) = Disc(f)$*

This construction also behaves well with respect to the action of $GL_2(\mathbb{Z})$ on the space of binary n-ic forms, which is defined as usual by:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2.13}$$

$$(\gamma \cdot f)(x,y) = f(ax + cy, bx + dy) \tag{2.14}$$

To explain how R_f and $R_{\gamma \cdot f}$ are related, we first need the following homomorphism:

Definition 2.2.3. *Let $\rho_r : GL_2(\mathbb{Z}) \to GL_{r+1}(\mathbb{Z})$ be given by the standard action on degree r monomials, i.e. if $f(x,y) = \sum f_i x^{r-i}y^i$ and $(\gamma \cdot f)(x,y) = \sum g_i x^{r-i}y^i$, then*

$$\begin{pmatrix} g_0 \\ g_1 \\ \ldots \\ g_r \end{pmatrix} = \rho_r(\gamma) \begin{pmatrix} f_0 \\ f_1 \\ \ldots \\ f_r \end{pmatrix} \tag{2.15}$$

More explicitly, the map looks like:

$$\rho_r(\gamma) = \begin{pmatrix} a^r & a^{r-1}b & \ldots & b^r \\ ra^{r-1}c & \ldots & \ldots & rb^{r-1}d \\ \ldots & \ldots & \ldots & \ldots \\ c^r & \ldots & \ldots & d^r \end{pmatrix} \tag{2.16}$$

Theorem 7 (Nakagawa, (+ Wood for f_0 non-zero?))**.** *Let f be a binary n-ic form, $\gamma \in GL_2(\mathbb{Z})$ and $g = \gamma \cdot f$. Denote the basis of R_f by $\{1, \alpha_{1,f}, \ldots, \alpha_{n-2,f}\}$, and denote the basis of R_g analogously.*

Then, there exists an isomorphism $\sigma : R_f \to R_g$, with the property:

$$\begin{pmatrix} \alpha_{1,g} \\ \alpha_{2,g} \\ \cdots \\ \alpha_{n-1,g} \end{pmatrix} \equiv \det(\gamma)\, \rho_{n-2}(\gamma) \begin{pmatrix} \sigma(\alpha_{1,f}) \\ \sigma(\alpha_{2,f}) \\ \cdots \\ \sigma(\alpha_{n-1,f}) \end{pmatrix} \quad mod\ \mathbb{Z} \tag{2.17}$$

2.3 Quadratic rings

Quadratic rings are of the form $R = \mathbb{Z}\{1, \alpha\}$. Necessarily, α is quadratic over $\mathbb{Z}$, and $Disc(\alpha) = Disc(R) = D$. By translating it by an element of $\mathbb{Z}$, we may assume that its characteristic polynomial is in one of the following two forms:

$$F_\alpha(x) = x^2 - \frac{D}{4} \tag{2.18}$$

$$F_\alpha(x) = x^2 - x + \frac{1-D}{4} \tag{2.19}$$

which correspond respectively to $D \equiv 0, 1 \bmod 4$.

By checking cases, it follows that R is determined by its discriminant and comes in the following flavours:

$$R(D) = \begin{cases} \mathbb{Z}[x]/(x^2) & \text{if } D = 0 \\ \mathbb{Z} \cdot (1,1) + \sqrt{D}(\mathbb{Z} \oplus \mathbb{Z}) & \text{if } D \geq 1 \text{ is a square} \\ \mathbb{Z}[\frac{D+\sqrt{D}}{2}] & \text{otherwise} \end{cases} \tag{2.20}$$

So, quadratic rings are parameterised by the set $\mathbb{D} = \{D \in \mathbb{Z} : D \equiv 0, 1 \bmod 4\}$.

2.4 Cubic rings and cubic forms

Key work on cubic rings by Delone-Faddeev, Davenport-Heilbronn and Bhargava-Shankar-Tsimerman all rely on a parameterisation of the space of cubic rings. Birch and Merriman's construction of a cubic ring from a binary cubic form in fact provides a bijection between based cubic rings and binary cubic forms.

Theorem 8 (Delone-Faddeev, Gan-Gross-Savin)**.** *There is a bijection between the following two sets:*

$$(Sym^3\mathbb{Z}^2)^* \leftrightarrow \{Based\ cubic\ rings\}/\sim \tag{2.21}$$

given by Birch & Merriman's construction, where $\sim$ denotes isomorphism of based rings, i.e. an isomorphism which respects bases mod $\mathbb{Z}$.

Furthermore, this bijection descends to the following bijection:

$$GL_2(\mathbb{Z})\backslash(Sym^3\mathbb{Z}^2)^* \leftrightarrow \{Cubic\ rings\}/\sim \tag{2.22}$$

where $\sim$ here denotes isomorphism of rings.

From Theorem 7, we see that the action of $\gamma \in GL_2(\mathbb{Z})$ on binary cubic forms corresponds to the action of $\det(\gamma) \cdot \gamma$ on the basis of the cubic ring, so it makes sense that quotienting by $GL_2(\mathbb{Z})$ results in a basis-free correspondence.

There is an alternative way to view this parameterisation of cubic rings: via resolvent rings and resolvent maps.

Let R be a non-degenerate cubic ring. Recall the definition of the S_3-closure of R from Definition 2.1.5. An element $\alpha \in R$ has S_3-conjugates $\alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}$ in $\bar{R}$. There is a classical resolvent map, key in the solution of the cubic equation, which appears here as $\phi : R \to \bar{R}$:

$$\phi(\alpha) = \frac{Disc(\alpha) + \sqrt{Disc(\alpha)}}{2} \tag{2.23}$$

where $\sqrt{Disc(\alpha)} = (\alpha^{(1)} - \alpha^{(2)})(\alpha^{(2)} - \alpha^{(3)})(\alpha^{(3)} - \alpha^{(1)})$.

The image of this map is invariant under the action of A_3, so it lands in a quadratic subring of $\bar{R}$. In fact, it lands in a quadratic subring S with $Disc(S) = Disc(R)$, which exists because $Disc(R) \equiv 0, 1 \bmod 4$.

Definition 2.4.1. *The quadratic resolvent ring of a cubic ring R is the unique quadratic ring S with $Disc(S) = Disc(R)$.*

The map ϕ reduces to a map $\bar{\phi} : R/\mathbb{Z} \mapsto S/\mathbb{Z}$, because $\sqrt{Disc(\alpha)}$ is invariant mod $\mathbb{Z}$. It is worth noting that $\bar{\phi}$ is discriminant-preserving. Upon fixing bases of $R/\mathbb{Z}$ and $S/\mathbb{Z}$, we can view $\bar{\phi}$ as a map $f : \mathbb{Z}^2 \to \mathbb{Z}$. It is cubic, because $\sqrt{Disc(\alpha)}$ is cubic, and so it is a binary cubic form! Of course, this is exactly the binary cubic form appearing in the Delone-Faddeev correspondence!

Note that, because each cubic ring R has precisely one quadratic resolvent S, we could also package S in the correspondences of Theorem 8; i.e., so the correspondences involve pairs (R, S) of cubic rings and quadratic resolvent rings.

We have seen here an example of how a space of rings is parameterised by resolvent maps. This viewpoint is key to understanding the parameterisations of quartic and quintic rings.

Another interesting property of this parameterisation relates the binary cubic form f to the set of 3 points X_{R_f}, defined in Definition 2.1.3:

Lemma 2.4.2. *Let $f \in (Sym^3\mathbb{Z}^2)^*$ be of non-zero discriminant. Then $X_{R_f} \subseteq \mathbb{P}^1$ is precisely the set of roots of f.*

2.5 Quartic rings

Let Q be a non-degenerate quartic ring. The classical resolvent map for the solution of the quartic equation is the map $\phi : Q \to \bar{Q}$:

$$\phi : \alpha \mapsto \alpha^{(1)}\alpha^{(2)} + \alpha^{(3)}\alpha^{(4)} \tag{2.24}$$

where the $\alpha^{(i)}$ are the S_4-conjugates of α in $\bar{Q}$.

The map ϕ lands in the subring of $\bar{Q}$ fixed by the subgroup $\langle (12), (34), (13)(24) \rangle$ which is of index 3 in S_4. Thus, it lands in a cubic ring. This leads to the following definition:

Definition 2.5.1. *Let Q be a non-degenerate quartic ring, and $\phi : Q \to \bar{Q}$ the resolvent map. A cubic resolvent ring of Q is a cubic ring $R \subseteq \bar{Q} \otimes \mathbb{Q}$ such that $\phi(Q) \subseteq R$ and $Disc(Q) = Disc(R)$.*

The following is proven in Higher Composition Laws III:

Theorem 9 (Bhargava: HCL III Corollary 5)**.** *Every quartic ring has a cubic resolvent ring.*

Let (Q, R) be a quartic ring / cubic resolvent ring pair. The resolvent map $\phi : Q \to R$ descends to a map $\bar{\phi} : Q/\mathbb{Z} \to R/\mathbb{Z}$. When we fix bases of $Q/\mathbb{Z}$ and $R/\mathbb{Z}$, we can view $\bar{\phi}$ as a quadratic map $\mathbb{Z}^3 \to \mathbb{Z}^2$; in other words, as a pair of ternary quadratic forms. We denote the space of integral ternary quadratic forms by $\mathbb{Z}^2 \otimes (Sym^2\mathbb{Z}^3)^*$. Elements of this space can be viewed as a pair of symmetric 3×3 matrices (A, B).

How does changing bases of $Q/\mathbb{Z}$ and $R/\mathbb{Z}$ affect the pair of matrices (A, B)? Changing basis of $Q/\mathbb{Z}$ corresponds to an action of $GL_3(\mathbb{Z})$ given by $g \cdot (A, B) = (gAg^t, gBg^t)$. Changing basis of $R/\mathbb{Z}$ corresponds to an action of $GL_2(\mathbb{Z})$ given by:

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2.25}$$

$$h \cdot (A, B) = (aA + bB, cA + dB) \tag{2.26}$$

Theorem 10 (Bhargava: HCL III Theorem 1)**.** *There is a bijection between the following two sets:*

$$\mathbb{Z}^2 \otimes (Sym^2\mathbb{Z}^3)^* \leftrightarrow \left\{ \begin{array}{c} (Q,R),\ \ Q \textit{ based quartic ring,} \\ R \textit{ based cubic resolvent ring} \end{array} \right\} / \sim \tag{2.27}$$

where $\sim$ represents isomorphism of based rings respecting the resolvent map.

Furthermore, this bijection descends to the following bijection:

$$GL_2(\mathbb{Z}) \times GL_3(\mathbb{Z}) \backslash \mathbb{Z}^2 \otimes (Sym^2\mathbb{Z}^3)^* \leftrightarrow \left\{ \begin{array}{c} (Q,R),\ \ Q \textit{ quartic ring,} \\ R \textit{ cubic resolvent ring} \end{array} \right\} / \sim \tag{2.28}$$

where $\sim$ represents isomorphism of rings respecting the resolvent map.

These bijections are totally explicit, in the sense that it is possible to explicitly construct multiplication tables of the based rings Q and R from (A, B). In particular, describing the cubic resolvent ring is very simple:

Theorem 11 (Bhargava)**.** *Let $(A, B) \in \mathbb{Z}^2 \otimes (Sym^2\mathbb{Z}^3)^*$ and let $R(A, B)$ be the associated based cubic resolvent ring. Then, $R(A, B)$ is given in the Delone-Faddeev correspondence of Theorem 8 by the binary cubic form $4 \cdot \det(xA - yB)$.*

The action of $GL_2(\mathbb{Z}) \times GL_3(\mathbb{Z})$ on the space $\mathbb{Z}^2 \otimes (Sym^2\mathbb{Z}^3)^*$ has a unique polynomial invariant, which is called the discriminant and denoted by $Disc((A, B))$. The bijections in theorem 10 are discriminant-preserving.

Analogously to the case of cubic rings, the set X_Q has a nice description in terms of (A, B):

Lemma 2.5.2. *Let $(A, B) \in \mathbb{Z}^2 \otimes (Sym^2\mathbb{Z}^3)^*$ be non-degenerate and let $Q = Q(A, B)$. Then the vanishing locus $V(A, B)$ is precisely $X_Q \subseteq \mathbb{P}^2$. Furthermore, $\{A, B\}$ is a basis for the space of quadrics vanishing on X_Q.*

2.6 Quartic rings from binary quartic forms

Unlike in the case of cubic rings, binary n-ic forms do not parameterise the space of all n-ic rings when $n = 4$. However, due to Wood, we understand precisely which quartic rings are described by binary quartic forms.

We first remark that a monogenic ring R is a ring generated by one element, i.e. $R = \mathbb{Z}[\alpha]$. In this case, we call α a monogenizer of R. If α is a monogenizer, then any $\mathbb{Z}$-translate of α is also a monogenizer. Therefore, we define a monogenization of R to be a $\mathbb{Z}$-class of monogenizers.

Theorem 12 (Wood). *There is a bijection between the following two sets:*

$$GL_2(\mathbb{Z})\backslash(Sym^4\mathbb{Z}^2)^* \leftrightarrow \left\{ \begin{array}{l} (Q, R),\ \ Q \textit{ quartic ring,} \\ R \textit{ monogenic cubic resolvent} \\ \textit{with a fixed monogenization} \end{array} \right\} / \sim \tag{2.29}$$

where $\sim$ represents isomorphism of rings respecting the resolvent map and the monogenization of the cubic resolvent.

The proof relies upon the following map from binary quartics to pairs of ternary quadratic forms, which respects the two constructions of quartic rings (i.e. Birch-Merriman's construction and Bhargava's construction):

$$\Psi : f \mapsto [A_0, B_f] = \left[\begin{pmatrix} & & -\frac{1}{2} \\ & 1 & \\ -\frac{1}{2} & & \end{pmatrix}, \begin{pmatrix} f_0 & \frac{f_1}{2} & \\ \frac{f_1}{2} & f_2 & \frac{f_3}{2} \\ & \frac{f_3}{2} & f_4 \end{pmatrix} \right] \tag{2.30}$$

where $f(x, y) = f_0x^4 + f_1x^3y + \ldots + f_4y^4$.

Bhargava's construction of cubic resolvents shows that (A, B) gives rise to a based cubic resolvent $R = \mathbb{Z}\{1, \omega, \theta\}$ with ω a monogenizer of R if and only if $4 \cdot \det(A) = \pm 1$. We can act by $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ to assume that $4 \cdot \det(A) = -1$, and then apply the reduction theory of ternary quadratic forms to see that A is $GL_3(\mathbb{Z})$-equivalent to A_0.

To understand the quotient by $GL_2(\mathbb{Z})$ on the side of binary quartic forms, Wood proves that if f, g are $GL_2(\mathbb{Z})$-equivalent, then $\Psi(f)$ and $\Psi(g)$ are (essentially) $GL_3(\mathbb{Z})$-equivalent; hence, there is a change of basis in the quartic ring but no change of monogenizer in the cubic resolvent.

2.7 Quintic rings

The parameterisation of quintic rings again stems from a fundamental resolvent map. This time, the relevant resolvent map is an alternating map between a quintic ring and its sextic resolvent ring.

Let R be a non-degenerate quintic ring, denote its S_5-closure as usual by $\bar{R}$ and let $K = R \otimes \mathbb{Q}$. There are six special conjugate index 6 subgroups $M^{(1)}, \ldots, M^{(6)} \subseteq S_5$, called the metacyclic subgroups. The sextic resolvent ring S will be a non-degenerate subring of the sextic resolvent algebra $L = (\bar{R} \otimes \mathbb{Q})^{M^{(1)}}$. We will make reference to the sextic resolvent ring S before we have defined it, in the hope that it has certain properties, and then we'll see that such S does exist.

There is some well-known, beautiful combinatorics associated with the metacyclic subgroups. Although it is not relevant for quintic rings, one interesting application of the combinatorics is in constructing the unique outer automorphism of S_6. In the theory of quintic rings, the combinatorics motivates the definition of the upcoming resolvent map. More details can be found in Higher Composition Laws IV. [Add source for outer automorphism of S_6?]

The fundamental resolvent map is actually an alternating map between dual spaces: $\phi : \wedge^2 \tilde{S} \to \tilde{R}$, where the following dual spaces are defined with respect to trace pairings.

$$R^* = \{x \in K : Tr_K(xy) \in \mathbb{Z} \quad \forall y \in R\} \tag{2.31}$$

$$S^* = \{z \in L : Tr_L(zw) \in \mathbb{Z} \quad \forall w \in S\} \tag{2.32}$$

$$\tilde{R} = \{x \in R^* \subset K : Tr_K(x) = 0\} \tag{2.33}$$

$$\tilde{S} = \{z \in S^* \subset L : Tr_L(z) = 0\} \tag{2.34}$$

Definition 2.7.1. *The fundamental resolvent map $\phi : \wedge^2 \tilde{S} \to \tilde{R}$ is given by:*

$$\phi(u, v) = \frac{\sqrt{Disc(S)}}{48 \cdot Disc(R)} \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ u^{(1)} + u^{(2)} & u^{(3)} + u^{(6)} & u^{(4)} + u^{(5)} \\ v^{(1)} + v^{(2)} & v^{(3)} + v^{(6)} & v^{(4)} + v^{(5)} \end{pmatrix} \tag{2.35}$$

where $\beta^{(i)}$ denotes the i-th conjugate of $\beta \in \tilde{S}$.

Note: $\sqrt{Disc(S)}$ is computed in a canonical way, so it is defined on the nose and not up to sign.

Properties of ϕ:

- The combinatorics associated with the metacyclic subgroups is tied to the Galois theory of K and L, and shows that this map lands in K.

- ϕ lands in the trace-zero subspace of K.

- One of our conditions on S will be that this map lands not just in K but in $\tilde{R}$.

- Upon choosing bases for $\tilde{S}, \tilde{R}$, we get ϕ as a linear map $A : \wedge^2 \mathbb{Z}^5 \to \mathbb{Z}^4$: a quadruple of bilinear alternating maps, i.e. $A \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$. More explicitly, if $\tilde{S}$ has basis $\{\beta_1^*, \ldots, \beta_5^*\}$ and $\phi(\beta_i^*, \beta_j^*) = a_{1ij}\alpha_1^* + a_{2ij}\alpha_2^* + a_{3ij}\alpha_3^* + a_{4ij}\alpha_4^*$, then we get four 5×5 skew-symmetric matrices, one for each α_k^*.

- There is an action of $GL_4(\mathbb{Z})\times SL_5(\mathbb{Z})$ on this space, which corresponds to changing bases in $\tilde{R}, \tilde{S}$. Via the respective trace pairings, these correspond to dual changes of basis in $R/\mathbb{Z}$ and $S/\mathbb{Z}$.

Definition 2.7.2. *Let R be a quintic ring. Then a sextic resolvent ring S of R is a subring of $L = (\bar{R}\otimes\mathbb{Q})^{M^{(1)}}$ such that:*

- *$\phi(x\wedge y)\in\tilde{R}$ for all $x, y\in\tilde{S}$*
- *$Disc(S) = (16\cdot Disc(R))^3$*

Remark: The action of $GL_4(\mathbb{Z})\times SL_5(\mathbb{Z})$ on the space $\mathbb{Z}^4\otimes\wedge^2\mathbb{Z}^5$ has a unique polynomial invariant, which we denote by $Disc(A)$.

Theorem 13 (Bhargava)**.** *There is a bijection between the following two sets:*

$$\mathbb{Z}^4\otimes\wedge^2\mathbb{Z}^5 \leftrightarrow \left\{\begin{array}{l} (R,S),\ \textit{R based quintic ring,} \\ \textit{S based sextic resolvent ring,} \\ \textit{R, S similarly oriented} \end{array}\right\}/\sim \qquad (2.36)$$

where $\sim$ represents isomorphism of based rings respecting the resolvent map, and the condition "similarly oriented" is a technical condition on the bases of R and S.

If (R,S) corresponds to A, then $Disc(A) = Disc(R)$.

Furthermore, this bijection descends to the following bijection:

$$GL_4(\mathbb{Z})\times SL_5(\mathbb{Z})\backslash(\mathbb{Z}^4\otimes\wedge^2\mathbb{Z}^5) \leftrightarrow \left\{\begin{array}{l} (R,S),\ \textit{R quintic ring,} \\ \textit{S sextic resolvent ring} \end{array}\right\}/\sim \qquad (2.37)$$

Just like the previous parameterisations, these bijections are also totally explicit in the sense that the multiplication tables of the based rings R and S can be explicitly constructed from A.

Note: The impact of the technical condition "similarly oriented" is that an element of $GL_4(\mathbb{Z})\times SL_5(\mathbb{Z})$ will induce changes of bases of R and S of the same determinant; in more detail, $(\tau,\gamma)\in GL_4(\mathbb{Z})\times SL_5(\mathbb{Z})$ induces a change of basis of $R/\mathbb{Z}$ given by τ and a change of basis of $S/\mathbb{Z}$ given by $\det(\tau)\cdot(\gamma^{-1})^t$. This reflects the fact that $-I_5$ acts trivially on $\mathbb{Z}^4\otimes\wedge^2\mathbb{Z}^5$, so not every pair of changes of basis would be attainable from $GL_4(\mathbb{Z})\times GL_5(\mathbb{Z})$.

The key result which shows that this theory includes all quintic rings is the following:

Theorem 14 (Bhargava)**.** *Every quintic ring has at least one sextic resolvent, and maximal quintic rings have a unique sextic resolvent.*

Bhargava's fundamental map is a relatively recent discovery. However, prior to this, one of the key tools in the study of the quintic was the Cayley-Klein resolvent map, $F : R/\mathbb{Z}\to L$, given by:

$$\begin{aligned} F(\alpha) = \frac{1}{\sqrt{Disc(R)}}(&\alpha^{(1)}\alpha^{(2)}+\alpha^{(2)}\alpha^{(3)}+\alpha^{(3)}\alpha^{(4)}+\alpha^{(4)}\alpha^{(5)}+\alpha^{(5)}\alpha^{(1)} \\ &-\alpha^{(1)}\alpha^{(3)}-\alpha^{(3)}\alpha^{(5)}-\alpha^{(5)}\alpha^{(2)}-\alpha^{(2)}\alpha^{(4)}-\alpha^{(4)}\alpha^{(1)}) \end{aligned} \qquad (2.38)$$

The precise ordering of the conjugates is once again reflected by the combinatorics associated to the metacyclic subgroups, and ensures that the map does indeed land in the sextic resolvent algebra L.

Why was this map important in the study of quintics? The key fact is that a quintic equation is solvable precisely when its Galois group is contained in one of the metacyclic subgroups. The characteristic polynomial of $F(\alpha)$ is a degree 6 equation and its roots are fixed by conjugate metacyclic subgroups, so when the Galois group is solvable, this sextic will have a rational root.

If $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ truly captures the quintic ring / sextic resolvent pair (R, S), then it must surely encode the Cayley-Klein resolvent map somehow. We describe below a natural quadratic construction in the entries of A.

Definition 2.7.3. *Let* $B = \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{pmatrix}$ *be a skew-symmetric* 4×4 *matrix. The pfaffian of* B *is a canonical square root of* $\det B$ *and is defined by Pfaff*$(B) = af - be + dc$.

Any odd dimension skew-symmetric matrix has determinant 0, so $\det(A) = 0$. But, we can obtain 4×4 skew-symmetric submatrices, by removing the same row and column from A, and taking the pfaffian of these will in general be nonzero. Define the i-th signed sub-pfaffian Q_i to be $(-1)^{i+1}$ times the pfafffian of the 4×4 principal submatrix obtained from A by removing the i-th row and column.

Theorem 15 (Bhargava). *Let* (R, S) *correspond to* A. *Then the classical Cayley-Klein resolvent map* $F : R/\mathbb{Z} \to L$ *lands in* $\tilde{S}$, *and is given in terms of the associated bases of* $R/\mathbb{Z}$ *and* $\tilde{S}$ *by* $4 \cdot (Q_1, \ldots, Q_5)$.

The action of $GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ on the signed sub-pfaffians will be good to know:

Lemma 2.7.4 (Bhargava). *Let* $(\tau, \gamma) \in GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$, $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ *and* $A' = (\tau, \gamma) \cdot A)$. *Denote the signed sub-pfaffians of* A *by* $(Q_1, \ldots, Q_5)$ *and those of* A' *by* $(Q_1', \ldots, Q_5')$. *Then:*

$$\begin{pmatrix} Q_1' \\ Q_2' \\ Q_3' \\ Q_4' \\ Q_5' \end{pmatrix} = (\gamma^{-1})^t \begin{pmatrix} \tau Q_1 \tau^t \\ \tau Q_2 \tau^t \\ \tau Q_3 \tau^t \\ \tau Q_4 \tau^t \\ \tau Q_5 \tau^t \end{pmatrix} \tag{2.39}$$

Finally, analogous to the cubic and quartic cases, the set of 5 points $X_{R(A)} \subseteq \mathbb{P}^3$ can be understood geometrically via A as follows:

Proposition 2.7.5 (Bhargava). *Let* $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ *be non-degenerate and let* $R = R(A)$. *The vanishing locus of the signed sub-pfaffians* $\{Q_1, \ldots, Q_5\}$ *of* A *is precisely the set of 5 points* $X_R \subseteq \mathbb{P}^3$. *Furthermore,* $\{Q_1, \ldots, Q_5\}$ *is a basis for the space of quadrics vanishing on* X_R.

Chapter 3

New results on binary n-ic forms and n-ic rings

Here we collect a few new and useful results on the based rings coming from binary n-ic forms.

Throughout this section, let $R = \mathbb{Z}\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ be a based n-ic ring, denote the based n-ic ring coming from a binary n-ic form f by R_f, and denote a generic element $\gamma \in GL_2(\mathbb{Z})$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

3.1 An identity of the index form

The form f is encoded in the index form of R_f in the following way:

Theorem 16. *In the based ring R_f, let $\alpha_f(x, y) = \sum_{i=0}^{n-2} x^{n-2-i} y^i \alpha_i$. Denote the index form in R_f by I_f. Then:*

$$I_f(\alpha_f(x, y)) = f(x, y)^{\frac{(n-1)(n-2)}{2}} \tag{3.1}$$

Proof. First, we claim that both sides of this equation transform in the same way under the action of $\gamma \in SL_2(\mathbb{Z})$. Let $g = \gamma \cdot f$. From Theorem 7, the bases of $R_f/\mathbb{Z}$ and $R_g/\mathbb{Z}$ are related by $\rho_{n-2}(\gamma) \in SL_{n-1}(\mathbb{Z})$. Hence, $\alpha_g(x, y) = \alpha_f(ax + cy, bx + dy)$. There is no change of orientation, so $I_f = I_g$ and both sides transform linearly in the same way under the action of γ.

Now, we shall apply a well-chosen element of $SL_2(\mathbb{Z})$ to reduce the proof to a simple case.

Suppose (x, y) are coprime. Choose an element $\gamma \in SL_2(\mathbb{Z})$ mapping $(1, 0)^t$ to $(x, y)^t$. Let $g = \gamma^t \cdot f$. Then the first basis element of $R_g/\mathbb{Z}$ will be $\alpha_g(1, 0) = \alpha_f(x, y)$ and $I_f = I_g$, i.e. no orientation change. So, proving $I_f(\alpha_f(x, y)) = f(x, y)^{\frac{(n-1)(n-2)}{2}}$ amounts to proving $I_g(\alpha_g(1, 0)) = g(1, 0)^{\frac{(n-1)(n-2)}{2}}$.

When (x, y) are not coprime, we can still choose an element $\gamma \in SL_2(\mathbb{Z})$ mapping $(z, 0)^t$ to $(x, y)^t$ for $z = gcd(x, y)$. In this case, proving $I_f(\alpha_f(x, y)) =$

$f(x,y)^{\frac{(n-1)(n-2)}{2}}$ amounts to proving $I_g(\alpha_g(z,0)) = g(z,0)^{\frac{(n-1)(n-2)}{2}}$. This is the simple case we shall prove directly:

With explicit calculation using Theorem 7, the element $\alpha_g(z,0) = z^{n-2}\alpha_1$ has $I_g(z^{n-2}\alpha_1) = z^{\frac{n(n-1)(n-2)}{2}} g_0^{\frac{(n-1)(n-2)}{2}} = (g_0 z^n)^{\frac{(n-1)(n-2)}{2}} = g(z,0)^{\frac{(n-1)(n-2)}{2}}$.

□

3.2 Binary n-ic forms and the rational normal curve

Given an n-ic ring R of non-zero discriminant, recall that we can associate to R a set of n points $X_R \subseteq \mathbb{P}^{n-2}$, defined in Definition 2.1.3.

Definition 3.2.1. *Denote the rational normal curve in $\mathbb{P}^{n-2}$ by V_{n-2}, i.e. $V_{n-2} = \{(\lambda^{n-2} : \lambda^{n-3}\mu : \ldots : \mu^{n-2}) : (\lambda : \mu) \in \mathbb{P}^1\}$.*

The main result we have on n-ic rings coming from binary n-ic forms is:

Theorem 17. *For $n \geq 3$, a based n-ic ring R of non-zero discriminant is given by a binary n-ic form if and only if X_R is contained in the rational normal curve $V_{n-2} \subseteq \mathbb{P}^{n-2}$.*

Furthermore, we can be more precise about the set X_{R_f}:

Definition 3.2.2. *Let $q_r : \mathbb{C}^2 \to \mathbb{C}^{r+1}$ be given by*

$$\begin{pmatrix} u \\ v \end{pmatrix} \mapsto \begin{pmatrix} u^r \\ u^{r-1} \\ \ldots \\ v^r \end{pmatrix} \tag{3.2}$$

so that $q_r(u,v)$ is a generic element of V_r.

Theorem 18. *Let f be a binary n-ic form of non-zero discriminant. Then $X_{R_f} = \{q_{n-2}(\lambda,\mu) : f(\lambda,\mu) = 0\}$, and in particular $X_{R_f} \subseteq V_{n-2}$.*

We will first prove Theorem 18 and thus the forward direction of Theorem 17. The converse of Theorem 17 will require more work. Our plan of attack will be to reduce these results to the special case of a ring given by a binary n-ic form f with $f_0 \neq 0$, because in this case we have an explicit basis of R_f. We will use $SL_2(\mathbb{Z})$ to make this reduction.

We set to work proving Theorem 18 in this special case:

Lemma 3.2.3. *Let f be a binary n-ic form of non-zero discriminant with $f_0 \neq 0$. Then $X_{R_f} = \{q_{n-2}(\lambda,\mu) : f(\lambda,\mu) = 0\}$. In particular, $X_{R_f} \subseteq U_{n-2} := \{(x_0, x_1, \ldots, x_{n-2} : x_{n-2} \neq 0\} \subseteq \mathbb{P}^{n-2}$.*

Proof. R can be described as the subring of $\mathbb{Q}[x]/(f(x,1))$ with the following basis, where θ is the image of x:

$$\begin{aligned}
\alpha_0 &= 1 && (3.3)\\
\alpha_1 &= f_0\theta && (3.4)\\
\alpha_2 &= f_0\theta^2 + f_1\theta && (3.5)\\
&\dots \\
\alpha_{n-1} &= f_0\theta^{n-1} + f_1\theta^{n-2} + \ldots + f_{n-2}\theta && (3.6)
\end{aligned}$$

We now prove that $\alpha_j^* = \alpha_{j+1}^*\theta$ for $1 \leq j \leq n-2$. First, note that $Tr(\alpha_0 \cdot \alpha_{j+1}^*\theta) = Tr(\frac{1}{f_0}\alpha_1 \cdot \alpha_{j+1}^*) = 0$ for $j \neq 0$. Now, for $1 \leq i, j \leq n-2$, note that:

$$\begin{aligned}
Tr(\alpha_i \cdot \alpha_{j+1}^*\theta) &= Tr(\theta\alpha_i \cdot \alpha_{j+1}^*) && (3.7)\\
&= Tr((\alpha_{i+1} - f_i\theta) \cdot \alpha_{j+1}^*) && (3.8)\\
&= \delta_{ij} && (3.9)
\end{aligned}$$

Hence, $\alpha_j^* = \alpha_{j+1}^*\theta$ for $1 \leq j \leq n-2$, so $(\alpha_1^* : \ldots : \alpha_{n-1}^*) = (\theta^{n-2}\alpha_{n-1}^* : \theta^{n-3}\alpha_{n-1}^* : \ldots : \alpha_{n-1}^*)$, and $\rho^{(k)}(\alpha_1^* : \ldots : \alpha_{n-1}^*) = (\theta_k^{n-2} : \theta_k^{n-3} : \ldots : 1) \in V_{n-2}$, where $\theta_1, \ldots, \theta_n$ are the roots of $f(x,1) = 0$. (Note that $\rho^{(k)}(\alpha_{n-1}^*) \neq 0$ for all k; otherwise, for some k, $\rho^{(k)}(\alpha_j^*) = 0$ for all j, but this is outlawed by Lemma 2.1.4.) □

We will use $SL_2(\mathbb{Z})$ to reduce to this special case, which means that we need to understand how X_{R_f} and X_{R_g} are related for equivalent forms f, g.

Lemma 3.2.4. *Let $\gamma \in SL_2(\mathbb{Z})$, f be a binary n-ic form of non-zero discriminant and $g = \gamma \cdot f$. Then $X_{R_f} = \rho_{n-2}(\gamma)^t X_{R_g}$.*

Proof. By Theorem 7, to get from the basis of R_g to the basis of R_f, we apply $\rho_{n-2}(\gamma^{-1})$. Hence, the relation between the dual bases is given by the transpose inverse of this matrix, namely $\rho_{n-2}(\gamma)^t$. The sets X_{R_f} and X_{R_g} come from the dual bases of the rings, and the lemma follows. □

Lemma 3.2.5. *$\rho_r(\gamma)^t q_r(u,v) = q_r((u,v)\gamma)$, and so $\rho_r(\gamma)^t$ stabilises V_r.*

Proof. From the definition of $\rho_r(\gamma)$:

$$\begin{pmatrix} g_0 \\ g_1 \\ \dots \\ g_r \end{pmatrix} = \rho_r(\gamma) \begin{pmatrix} f_0 \\ f_1 \\ \dots \\ f_r \end{pmatrix} \qquad (3.10)$$

We calculate:

$$
\begin{aligned}
q_r(u,v)^t \rho_r(\gamma) \begin{pmatrix} f_0 \\ f_1 \\ \cdots \\ f_r \end{pmatrix} &= q_r(u,v)^t \begin{pmatrix} g_0 \\ g_1 \\ \cdots \\ g_r \end{pmatrix} && (3.11)\\
&= g(u,v) && (3.12)\\
&= f((u,v)\gamma) && (3.13)\\
&= q_r((u,v)\gamma)^t \begin{pmatrix} f_0 \\ f_1 \\ \cdots \\ f_r \end{pmatrix} && (3.14)
\end{aligned}
$$

This holds identically in the f_i, so

$$\rho_r(\gamma)^t q_r(u,v) = q_r((u,v)\gamma) \tag{3.15}$$

□

Proof of Theorem 18. The form $f \neq 0$, so there exists $\gamma \in SL_2(\mathbb{Z})$ such that $(\gamma \cdot f)(1,0) \neq 0$. Let $g = \gamma \cdot f$. Then by Lemma 3.2.3, X_{R_g} is of the required form, and by Lemma 3.2.5:

$$
\begin{aligned}
X_{R_f} &= \rho_{n-2}(\gamma)^t X_{R_g} && (3.16)\\
&= \rho_{n-2}(\gamma)^t \cdot \{q_{n-2}(\lambda,\mu) : g(\lambda,\mu) = 0\} && (3.17)\\
&= \rho_{n-2}(\gamma)^t \cdot \{q_{n-2}(\lambda,\mu) : f((\lambda,\mu)\gamma) = 0\} && (3.18)\\
&= \{q_{n-2}((\lambda,\mu)\gamma) : f((\lambda,\mu)\gamma) = 0\} && (3.19)\\
&= \{q_{n-2}(\lambda,\mu) : f(\lambda,\mu) = 0\} && (3.20)
\end{aligned}
$$

□

This deals with the forward direction of Theorem 17 too. Now, we set about proving that if $X_R \subseteq V_{n-2}$ then $R = R_f$ for some f. Again, we reduce to the case $f_0 \neq 0$ first.

Definition 3.2.6. *Let R be a based n-ic ring with basis $\{1, \alpha_1, \ldots, \alpha_{n-1}\}$ and $\gamma \in GL_2(\mathbb{Z})$. We define $\gamma \cdot R$ to be the based n-ic ring with the following basis mod $\mathbb{Z}$:*

$$\begin{pmatrix} \alpha'_1 \\ \alpha'_2 \\ \cdots \\ \alpha'_{n-1} \end{pmatrix} \equiv \det(\gamma)\, \rho_{n-2}(\gamma) \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_{n-1} \end{pmatrix} \ \textit{mod}\ \mathbb{Z} \tag{3.21}$$

Corollary 3.2.7. $\gamma \cdot R_f = R_{\gamma \cdot f}$

Proof. Evident from Theorem 7. □

Corollary 3.2.8. *The statement of Theorem 17 is $GL_2(\mathbb{Z})$-invariant. In other words:*

(i) A based n-ic ring R is given by a binary n-ic form if and only if $\gamma \cdot R$ is.

(ii) $X_R \subseteq V_{n-2}$ if and only if $X_{\gamma \cdot R} \subseteq V_{n-2}$

Proof. (i) Suppose $R = R_f$, then Theorem 7 tells us that $\gamma \cdot R = R_{\gamma \cdot f}$. The converse holds by applying γ^{-1} and using the same argument.

(ii) The bases of R and $\gamma \cdot R$ are related by $\det(\gamma)\rho_{n-2}(\gamma)$, and so their dual bases are related by $\det(\gamma)(\rho_{n-2}(\gamma)^t)^{-1}$. Hence, the sets of points X_R and $X_{\gamma \cdot R}$ in $\mathbb{P}^{n-2}$ are related by $(\rho_{n-2}(\gamma)^t)^{-1}$, which stabilises V_{n-2} as proven in Lemma 3.2.5. □

Lemma 3.2.9. *Suppose $X_R \subseteq V_{n-2}$. Then there exists $\gamma \in SL_2(\mathbb{Z})$ such that $X_{\gamma \cdot R} \subseteq V_{n-2} \cap U_{n-2}$.*

Proof. Let $X_R = \{q_{n-2}(\lambda_i, \mu_i) : 1 \leq i \leq n\}$. By Lemma 3.2.5 and the proof of Corollary 3.2.8 (ii), $X_{\gamma \cdot R} = \{q_{n-2}((\lambda_i, \mu_i)\gamma^{-1}) : 1 \leq i \leq n\}$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the condition that $X_{\gamma \cdot R} \subseteq U_{n-2}$ amounts to $-b\lambda_i + a\mu_i \neq 0$ for all i. This outlaws at most 2 coprime tuples (a, b) for each (λ_i, μ_i), leaving infinitely many γ to choose from which will satisfy our condition. □

The above results enable us to reduce the proof of the backward direction of Theorem 17 to the following result:

Proposition 3.2.10. *Let R be a based n-ic ring ($n \geq 3$) with $X_R \subseteq V_{n-2} \cap U_{n-2}$. Then $R = R_f$ for some f with $f_0 \neq 0$.*

Proof. Denote the homomorphisms $\rho : R \to \mathbb{C}$ by $\rho^{(1)}, \ldots, \rho^{(n)}$. Because of the assumption on X_R, we can let $X_R = \{P_1, \ldots, P_n\}$ with $P_k = (\theta_k^{n-2} : \ldots : \theta_k : 1)$. Hence, $\rho^{(k)}(\alpha_{n-1}^*) \neq 0$ for all k, and so $\alpha_{n-1}^* \in (R \otimes \mathbb{Q})^*$. We also see that $\rho^{(k)}(\alpha_j^*) = \rho^{(k)}(\alpha_{j+1}^*)\theta_k$ for $1 \leq j \leq n-2$, which in particular tells us $\rho^{(k)}(\alpha_{n-2}^*) = \rho^{(k)}(\alpha_{n-1}^*)\theta_k$. Let $\theta = \frac{\alpha_{n-2}^*}{\alpha_{n-1}^*} \in R \otimes \mathbb{Q}$. Then $\rho^{(k)}(\theta) = \theta_k$ for all k, so $\rho^{(k)}(\alpha_j^*) = \rho^{(k)}(\alpha_{j+1}^*\theta)$ for all k and $1 \leq j \leq n-2$. The n homomorphisms $\rho^{(k)} : R \otimes \mathbb{Q} \to \mathbb{C}$ separate points, so we actually have $\alpha_j^* = \alpha_{j+1}^*\theta$ for $1 \leq j \leq n-2$.

With the aim of showing that $\{\alpha_1, \ldots, \alpha_{n-1}\}$ takes the special form given by a binary n-ic form, we consider $\theta\alpha_i - \alpha_{i+1}$. For $1 \leq j \leq n-2$ and $0 \leq i \leq n-2$:

$$\begin{aligned} Tr((\theta\alpha_i - \alpha_{i+1}) \cdot \alpha_{j+1}^*) &= Tr(\alpha_i \cdot \alpha_j^*) - Tr(\alpha_{i+1} \cdot \alpha_{j+1}^*) && (3.22) \\ &= \delta_{ij} - \delta_{ij} && (3.23) \\ &= 0 && (3.24) \end{aligned}$$

Hence, $\theta\alpha_i - \alpha_{i+1} \in \mathbb{Q}\{1, \alpha_1\}$ for $0 \leq i \leq n-2$. The $i = 0$ case tells us that $\theta = a + b\alpha_1$ for some $a, b \in \mathbb{Q}$. To ensure linear independence of $\{\alpha_1^*, \ldots, \alpha_{n-1}^*\}$, we cannot have $\theta \in \mathbb{Q}$ (at least if $n \geq 3$, as we assume), so $b \neq 0$. Hence, we have $\mathbb{Q}\{1, \alpha_1\} = \mathbb{Q}\{1, \theta\}$, which together with $\theta\alpha_i - \alpha_{i+1} \in \mathbb{Q}\{1, \alpha_1\}$ implies

$\mathbb{Q}\{1, \alpha_1, \ldots, \alpha_{i+1}\} = \mathbb{Q}\{1, \theta, \ldots, \theta^{i+1}\}$ for all i. It follows that θ is of degree n over $\mathbb{Q}$ and that $\mathbb{Q}[\theta] = R \otimes \mathbb{Q}$.

Let $f(x, y) \in \mathbb{Z}[x, y]$ be a binary n-ic form such that $f(\theta, 1) = 0$. Note that $f_0 \neq 0$, since θ is of degree n over $\mathbb{Q}$. Let $R' = R_f$ with basis $\{\beta_0 = 1, \beta_1, \ldots, \beta_{n-1}\}$. Then $R' \subseteq \mathbb{Q}[\theta] = R \otimes \mathbb{Q}$. We will show that the change of basis from $R/\mathbb{Z}$ to $R'/\mathbb{Z}$ is by $u \in \mathbb{Q}$, and then that $R = R_{u^{-1} \cdot f}$.

Let $M \in GL_{n-1}(\mathbb{Q})$ such that the following holds:

$$\begin{pmatrix} 1 \\ \beta_1 \\ \ldots \\ \beta_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \ldots 0 \\ * & \\ \ldots & M \\ * & \end{pmatrix} \begin{pmatrix} 1 \\ \alpha_1 \\ \ldots \\ \alpha_{n-1} \end{pmatrix} \tag{3.25}$$

This induces the following relation between the two dual bases, where $N = (M^t)^{-1}$:

$$\begin{pmatrix} \beta_0^* \\ \beta_1^* \\ \ldots \\ \beta_{n-1}^* \end{pmatrix} = \begin{pmatrix} 1 & * \ldots * \\ 0 & \\ \ldots & N \\ 0 & \end{pmatrix} \begin{pmatrix} \alpha_0^* \\ \alpha_1^* \\ \ldots \\ \alpha_{n-1}^* \end{pmatrix} \tag{3.26}$$

We know from our earlier work that there exists $s = \alpha_{n-1}^*$ such that $\alpha_i^* = \theta^{n-1-i}s$ for $i \neq 0$. From the proof of Lemma 3.2.3, we similarly know that $\beta_i^* = \theta^{n-1-i}r$ for $i \neq 0$, where $r = \beta_{n-1}^*$. Furthermore, we noted that r, s are invertible. Upon writing $t = rs^{-1}$, we get:

$$\begin{pmatrix} \theta^{n-2}t \\ \ldots \\ t \end{pmatrix} = N \begin{pmatrix} \theta^{n-2} \\ \ldots \\ 1 \end{pmatrix} \tag{3.27}$$

The bottom equation tells us $t \in \mathbb{Q}\{1, \theta, \ldots, \theta^{n-2}\}$. We prove by induction that $t \in \mathbb{Q}$. For $0 \leq j \leq n-2$, let $S_j = \mathbb{Q}\{1, \theta, \ldots, \theta^j\}$. Suppose that $t \in S_j$ for some $1 \leq j \leq n-2$. We claim that $t \in S_{j-1}$:

Consider $\theta^{n-1-j}t$. If $t \in S_j$ then $\theta^{n-1-j}t \in T_j := \mathbb{Q}\{\theta^{n-1-j}, \theta^{n-j}, \ldots, \theta^{n-1}\}$. Looking at the j-th row of N, we also see that $\theta^{n-1-j}t \in S_{n-2}$. By linear independence of $\{1, \theta, \ldots, \theta^{n-1}\}$, $T_j \cap S_{n-2} = \mathbb{Q}\{\theta^{n-1-j}, \theta^{n-j}, \ldots, \theta^{n-2}\}$, so $\theta^{n-1-j}t \in \mathbb{Q}\{\theta^{n-1-j}, \theta^{n-j}, \ldots, \theta^{n-2}\}$ and indeed $t \in S_{j-1}$.

Hence, $t \in \mathbb{Q}$ and it follows that $N = tI_{n-1}$, $M = t^{-1}I_{n-1}$. We need a little extra work to confirm that $R = R_{t \cdot f}$. There exist $b_k \in \mathbb{Q}$ such that $\alpha_k = t\beta_k + b_k$ for $1 \leq k \leq n-1$. We need to show $b_k \in \mathbb{Z}$ for all k and that $t \cdot f \in \mathbb{Z}[x, y]$.

In Nakagawa's paper he proves the following formula. For $1 \leq i \leq j \leq n-1$ and with $\beta_n = -f_n$:

$$\beta_i \beta_j = \sum f_{i+j-k}\beta_k - \sum f_{i+j-k}\beta_k \tag{3.28}$$

where the first sum is over all k with $j < k \leq min(i+j, n)$ and the second sum is over all k with $max(i+j-n, 1) \leq k \leq i$.

We will use some special forms of this general equation. First, note that if $1 < j < n-1$, $\beta_1\beta_j = f_0\beta_{j+1} - f_j\beta_1$ and $\beta_1\beta_{n-1} = -f_0f_n - f_{n-1}\beta_1$. Secondly, note that β_j^2 has β_j coefficient equal to $-f_j$, i.e. $Tr(\beta_j^2\beta_j^*) = -f_j$.

We now calculate $\alpha_1\alpha_j$ and α_j^2. For $1 < j < n-1$:

$$\begin{aligned}
\alpha_1\alpha_j &= (t\beta_1 + b_1)(t\beta_j + b_j) && (3.29)\\
&= t^2(f_0\beta_{j+1} - f_j\beta_1) + b_1\alpha_j + b_j\alpha_1 - b_1b_j && (3.30)\\
&\equiv tf_0\alpha_{j+1} + b_1\alpha_j + (b_j - tf_j)\alpha_1 \bmod \mathbb{Q} && (3.31)\\
\alpha_1\alpha_{n-1} &= (t\beta_1 + b_1)(t\beta_{n-1} + b_{n-1}) && (3.32)\\
&= t^2(-f_0f_n - f_{n-1}\beta_1) + b_1\alpha_{n-1} + b_{n-1}\alpha_1 - b_1b_{n-1} && (3.33)\\
&\equiv b_1\alpha_{n-1} + (b_{n-1} - tf_{n-1})\alpha_1 \bmod \mathbb{Q} && (3.34)
\end{aligned}$$

Since R is closed under multiplication, this tells us $tf_0, b_1, b_j - tf_j \in \mathbb{Z}$ for $1 < j \leq n-1$.

Now, consider α_j^2 for $1 \leq j \leq n-1$, and recall that $\beta_j^* = t\alpha_j^*$:

$$\begin{aligned}
\alpha_j^2 &= (t\beta_j + b_j)^2 && (3.35)\\
&= t^2\beta_j^2 + 2b_j\alpha_j - b_j^2 && (3.36)\\
\mathbb{Z} \ni Tr(\alpha_j^2\alpha_j^*) &= Tr(t^2\beta_j^2\alpha_j^*) + 2b_j && (3.37)\\
&= Tr(t\beta_j^2\beta_j^*) + 2b_j && (3.38)\\
&= -tf_j + 2b_j && (3.39)
\end{aligned}$$

Bringing this all together, we have $tf_0, b_1, b_j - tf_j \in \mathbb{Z}$ for $1 < j \leq n-1$ and $2b_j - tf_j \in \mathbb{Z}$ for $1 \leq j \leq n-1$, so $tf_j, b_j \in \mathbb{Z}$ for all j. This means that, as a based ring, $R = \mathbb{Z}\{1, t\beta_1, \ldots, t\beta_{n-1}\} = R_{t\cdot f}$, with $t \cdot f \in \mathbb{Z}[x, y]$ and $t \cdot f_0 \neq 0$, as we aimed to show. □

We give below an alternative, related characterisation of based n-ic rings of non-zero discriminant which come from binary n-ic forms. The point of this corollary is that, not only can we ask that the n points of X_R are of the form $(x^{n-2}, x^{n-3}y, \ldots, y^{n-2})$, we can actually ask for the dual basis to essentially be of this form, which is a priori a stronger condition:

Corollary 3.2.11. *For $n \geq 3$, a based n-ic ring R of non-zero discriminant, with basis $\{\alpha_0 = 1, \alpha_1, \ldots, \alpha_{n-1}\}$, is given by a binary n-ic form if and only if the dual basis $\{\alpha_0^*, \alpha_1^*, \ldots, \alpha_{n-1}^*\}$ is of the form $\alpha_i^* = \lambda^{n-1-i}\mu^{i-1}r$ for $1 \leq i \leq n-1$, for some $\lambda, \mu, r \in R \otimes \mathbb{Q}$. Furthermore, $r \in (R \otimes \mathbb{Q})^\times$.*

Proof. The forward direction follows from the proof of Lemma 3.2.3, upon noting that the statement of this corollary is $GL_2(\mathbb{Z})$-invariant. The reverse direction follows from Theorem 17.

If $r \notin (R \otimes \mathbb{Q})^\times$, there exists a homomorphism $\rho : R \otimes \mathbb{Q} \to \mathbb{C}$ with $\rho(r) = 0$. Then $\rho(\alpha_i^*) = 0$ for all $1 \leq i \leq n-1$, contradicting Definition 2.1.4. □

3.3 Quadrics vanishing on X_{R_f}

A based quartic ring R (with a cubic resolvent) is described by a pair of ternary quadratic forms vanishing on X_R. A based quintic ring R (with a sextic resolvent) is described by an element $A \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$, and the five sub-pfaffians of A are quadrics vanishing on X_R. In both these cases, these quadrics in fact form a basis for the space of quadrics vanishing on X_R.

Now that we know what X_{R_f} looks like, we can explicitly find such quadrics in these cases and use these to lead us to the element in the relevant parameter space which describes R_f.

Lemma 3.3.1. *A basis for the space of quadrics vanishing on $V_r \subseteq \mathbb{P}^r$ is given by the following quadrics:*

$$Q_{ijkl} = t_i t_l - t_j t_k \tag{3.40}$$

with $i < j \leq k < l, i + l = j + k$, $i = 0$ if $s \leq r$ and $l = r$ if $s > r$.

Proof. V_r is the collection of elements of the form $q_r(x, y) = (x^r, x^{r-1}y, \ldots, y^r)$. Let Q be a quadric vanishing on all such elements. Evaluating Q at this generic element, we obtain a degree $2r$ polynomial in x, y. We can partition Q into sums of terms $t_i t_j$ with $i + j$ fixed, which correspond to the monomial $x^{2r-i-j}y^{i+j}$. For a fixed value $s = i + j$, let $Q(s)$ be the sum of terms in Q with $i + j = s$. We need the sum of the coefficients in each $Q(s)$ to equal 0.

If $s \in \{0, 1, 2r - 1, 2r\}$, there is only one monomial $t_i t_j$ in $Q(s)$ (respectively, $t_0^2, t_0 t_1, t_{r-1} t_r, t_r^2$), so the coefficients of these terms are all 0. If $s \leq r$, the vanishing property of $Q(s)$ means it has to be in the span of Q_{0ijs} with $0 < i \leq j < s$ and $i + j = s$, and these quadrics are seen to be linearly independent. If $s > r$, $Q(s)$ is in the span of $Q_{(s-r)ijr}$ with $s - r < i \leq j < r$ and $i + j = s$. Gathering these various quadrics, we retain linear independence and obtain the given basis. □

Lemma 3.3.2. *A basis for the space of quadrics vanishing on $X_{R_f} \subseteq \mathbb{P}^{n-2}$ is given by the quadrics of Lemma 3.3.1 together with the following quadrics:*

$$Q_i = f_0 t_0 t_i + f_1 t_0 t_{i+1} + \ldots + f_{n-2-i} t_0 t_{n-2} + f_{n-1-i} t_1 t_{n-2} + \ldots + f_n t_{i+2} t_{n-2} \tag{3.41}$$

for $0 \leq i \leq n - 4$.

Proof. Recall from Theorem 17 that $X_{R_f} = \{q_{n-2}(\lambda, \mu) : f(\lambda, \mu) = 0\}$. In particular, it is contained in V_{n-2} so the quadrics in Lemma 3.3.1 certainly vanish on X_{R_f}.

To see that all other quadrics vanishing on X_{R_f} are captured by the new quadrics Q_i, we first check that the Q_i do indeed vanish on X_{R_f}:

$$Q_i(q_{n-2}(x, y)) = f_0 x^{2n-4-i} y^i + \ldots + f_n x^{n-4-i} y^{n+i} \tag{3.42}$$

$$= x^{n-4-i} y^i \cdot f(x, y) \tag{3.43}$$

Hence, the Q_i vanish on X_{R_f}. From the set $\{Q_i(q_{n-2}(x, y)) : 0 \leq i \leq n - 4\}$ and the basis of Lemma 3.3.1 both being linearly independent, we see that the proposed basis $\{Q_{ijkl}\} \cup \{Q_i\}$ is linearly independent.

It remains to check that any quadric vanishing on X_{R_f} is in their span. Let Q be such a quadric. Then $Q(q_{n-2}(x,y))$ is a polynomial in x, y vanishing at the roots of $f(x,y)$. Since f has non-zero discriminant, f is square free and so $Q(q_{n-2}(x,y))$ is a multiple of $f(x,y)$. Thus, $Q(q_{n-2}(x,y)) = \sum_i a_i Q_i(q_{n-2}(x,y))$ for some a_i, and $Q - \sum_i a_i Q_i$ is a quadric vanishing on V_{n-2}, so it is in the span of $\{Q_{ijkl}\}$. □

Applying this result in the case of binary quartic forms, we are led to a pair of forms which are essentially those derived by Wood:

Corollary 3.3.3. *Let $f = f_0x^4 + f_1x^3y + \ldots + f_4y^4$ of non-zero discriminant, and let R_f be given by a pair of ternary quadratic forms (A, B). Then A, B lie in the span of the forms $\{A', B'\}$ below:*

$$A' = t_0t_2 - t_1^2 \tag{3.44}$$

$$B' = f_0t_0^2 + f_1t_0t_1 + f_2t_0t_2 + f_3t_1t_2 + f_4t_2^2 \tag{3.45}$$

These can be written as the following two matrices:

$$\begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix}, \begin{pmatrix} f_0 & \frac{f_1}{2} & \frac{f_2}{2} \\ \frac{f_1}{2} & 0 & \frac{f_3}{2} \\ \frac{f_2}{2} & \frac{f_3}{2} & f_4 \end{pmatrix} \tag{3.46}$$

Proof. By Lemma 2.5.2, the forms A, B span the quadrics vanishing on X_{R_f}, and so this follows from the previous result. □

Note: It is not immediate that this pair of forms indeed give rise to the ring R_f. A priori, they could give rise to some other ring in the same etale algebra. However, the result is still useful in that it leads us in the right direction.

Similarly, we can say the following in the quintic case:

Corollary 3.3.4. *Let $f = f_0x^5 + f_1x^4y + \ldots + f_5y^5$ of non-zero discriminant, and let R_f be given by $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. With the coordinates of $\mathbb{P}^3$ being t_1, t_2, t_3, t_4, the sub-pfaffians of A lie in the span of the forms below:*

$$P_1 = t_1t_3 - t_2^2 \tag{3.47}$$

$$P_2 = t_1t_4 - t_2t_3 \tag{3.48}$$

$$P_3 = t_2t_4 - t_3^2 \tag{3.49}$$

$$P_4 = f_0t_1t_2 + f_1t_2^2 + f_2t_2t_3 + f_3t_3^2 + f_4t_3t_4 + f_5t_4^2 \tag{3.50}$$

$$P_5 = f_0t_1^2 + f_1t_1t_2 + f_2t_2^2 + f_3t_2t_3 + f_4t_3^2 + f_5t_3t_4 \tag{3.51}$$

Proof. By Proposition 2.7.5, the sub-pfaffians of A span the space of quadrics vanishing on $X_{R(A)} = X_{R_f}$. This result then follows from Lemma 3.3.2 with some slight changes to the precise basis chosen. □

This result will be key in the next chapter, where we closely analyse the quintic rings given by binary quintic forms.

Chapter 4

Maps from $(Sym^5\mathbb{Z}^2)^* \to \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$

The maps below mimic closely the maps from binary quartics to $\mathbb{Z}^2 \otimes Sym^2\mathbb{Z}^3$ defined by Wood.

Denote a generic element $f \in (Sym^5\mathbb{Z}^2)^*$ by $f = f_0x^5 + f_1x^4y + f_2x^3y^2 + f_3x^2y^3 + f_4xy^4 + f_5y^5$.

Theorem 19. *The following map $\Phi : (Sym^5\mathbb{Z}^2)^* \to \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ respects the two constructions of based quintic rings:*

$$\Phi(f) = \begin{pmatrix} 0 & t_3 & -t_2 & t_1 & 0 \\ -t_3 & 0 & -f_0t_1 - f_1t_2 & -f_2t_2 - f_3t_3 & -t_4 \\ t_2 & f_0t_1 + f_1t_2 & 0 & -f_4t_3 - f_5t_4 & t_3 \\ -t_1 & f_2t_2 + f_3t_3 & f_4t_3 + f_5t_4 & 0 & -t_2 \\ 0 & t_4 & -t_3 & t_2 & 0 \end{pmatrix}$$

Proof. Computation of the SL_5-invariants leads to the multiplicative structure of $R(\Phi(f))$, which is seen to match that of the ring R_f defined by Birch and Merriman. □

However, the derivation of this map was not entirely guesswork. It relies on noticing that the sub-pfaffians can be taken to be quite simple quadrics as explained by our earlier result, Corollary 3.3.4, which we restate below.

Corollary 4.0.1. *Let $f = f_0x^5 + f_1x^4y + \ldots + f_5y^5$ of non-zero discriminant, and let R_f be given by $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. With the coordinates of $\mathbb{P}^3$ being*

t_1, t_2, t_3, t_4, the sub-pfaffians of A lie in the span of the forms below:

$$P_1 = t_1t_3 - t_2^2 \tag{4.1}$$
$$P_2 = t_1t_4 - t_2t_3 \tag{4.2}$$
$$P_3 = t_2t_4 - t_3^2 \tag{4.3}$$
$$P_4 = f_0t_1t_2 + f_1t_2^2 + f_2t_2t_3 + f_3t_3^2 + f_4t_3t_4 + f_5t_4^2 \tag{4.4}$$
$$P_5 = f_0t_1^2 + f_1t_1t_2 + f_2t_2^2 + f_3t_2t_3 + f_4t_3^2 + f_5t_3t_4 \tag{4.5}$$

This knowledge of the sub-pfaffians simplifies and guides the brute-force search for Φ. The signed sub-pfaffians of $\Phi(f)$ turn out to be $[P_4, P_1, P_2, P_3, -P_5]$.

We begin investigating the map Φ and list key properties below.

Corollary 4.0.2. *The map Φ is discriminant-preserving.*

Proof. For $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$, the discriminant of $R(A)$ was shown by Bhargava to be $Disc(A)$. Similarly, Birch and Merriman showed that the discriminant of R_f is $\Delta(f)$. The result then follows from Theorem 19. □

Theorem 20. *If $\gamma \in GL_2(\mathbb{Z})$, then $\Phi(\gamma \cdot f)$ and $\Phi(f)$ are $GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$-equivalent.*

Explicitly, define $\sigma : GL_2(\mathbb{Z}) \to SL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ as follows:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{4.6}$$
$$\sigma(\gamma) = (\psi(\gamma), \rho(\gamma)) \tag{4.7}$$
$$\psi(\gamma) = (ad - bc)\begin{pmatrix} a^3 & a^2b & ab^2 & b^3 \\ 3a^2c & 2abc + a^2d & 2abd + b^2c & 3b^2d \\ 3ac^2 & 2acd + bc^2 & 2bcd + ad^2 & 3bd^2 \\ c^3 & c^2d & cd^2 & d^3 \end{pmatrix} \tag{4.8}$$
$$\rho(\gamma) = \begin{pmatrix} d & 0 & 0 & 0 & -c \\ 0 & a^2 & 2ab & b^2 & 0 \\ 0 & ac & bc + ad & bd & 0 \\ 0 & c^2 & 2cd & d^2 & 0 \\ -b & 0 & 0 & 0 & a \end{pmatrix} \tag{4.9}$$

Recall that $H \leqslant SL_5(\mathbb{Z})$ is the group of all matrices of the form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ * & 1 & 0 & 0 & * \\ * & 0 & 1 & 0 & * \\ * & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.10}$$

Then, there exists $h \in H$ such that $\Phi(\gamma \cdot f) = (1, h) \cdot \sigma(\gamma) \cdot \Phi(f)$.

Proof. This can be checked by explicit computation, but the derivation of the result in the first place is illuminating.

Let $g = \gamma \cdot f$. Nakagawa proved that $R_f = R_g$, with their bases related (mod $\mathbb{Z}$) by $\psi(\gamma)$. Hence, if $\Phi(g) = (\alpha, \beta) \cdot \Phi(f)$ for some $(\alpha, \beta) \in \Gamma$, then $\alpha = \psi(\gamma)$.

To find a candidate for β, we consider the action on sub-pfaffians. Denote the five 4×4 signed sub-pfaffians of $\Phi(f)$ by $P_{1,f}, \ldots, P_{5,f}$, and do the same for g. If $\Phi(g) = (\alpha, \beta) \cdot \Phi(f)$ then Higher Composition Laws IV tells us that:

$$\begin{pmatrix} P_{1,g} \\ P_{2,g} \\ P_{3,g} \\ P_{4,g} \\ P_{5,g} \end{pmatrix} = (\det \beta)(\beta^{-1})^t \begin{pmatrix} \alpha P_{1,f} \alpha^t \\ \alpha P_{2,f} \alpha^t \\ \alpha P_{3,f} \alpha^t \\ \alpha P_{4,f} \alpha^t \\ \alpha P_{5,f} \alpha^t \end{pmatrix} \tag{4.11}$$

Using $\alpha = \psi(\gamma)$, we compute this all and see that β would have to be of the form $h \cdot \rho(\gamma)$ for a unique h.

Then, we check with this β that indeed $\Phi(g) = (\alpha, \beta) \cdot \Phi(f)$. □

There is a relative Φ' of Φ, which is $GL_2(\mathbb{Z})$-equivariant on the nose (i.e. not up to some $h \in H$), but is only defined for integer-matrix quintic forms. They are related in the sense that $\Phi(f)$ and $\Phi'(f)$ are $SL_5(\mathbb{Z})$-translates:

Proposition 4.0.3. *There exists $\Phi' : Sym^5\mathbb{Z}^2 \to \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ and $\sigma : GL_2(\mathbb{Z}) \to SL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ as above, such that $\Phi'(\gamma \cdot f) = \sigma(\gamma) \cdot \Phi'(f)$. We also have that $R(\Phi'(f)) = R_f$ as based rings.*

In full detail, $\Phi(f) = t_1 A_1 + t_2 A_2 + t_3 A_3 + t_4 A_4$ for:

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ & 0 & -f_0 & -\frac{2f_1}{5} & 0 \\ & & 0 & -\frac{f_2}{10} & 0 \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix} \tag{4.12}$$

$$A_2 = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 \\ & 0 & -\frac{3f_1}{5} & -\frac{3f_2}{5} & 0 \\ & & 0 & -\frac{3f_3}{10} & 0 \\ & & & 0 & -1 \\ & & & & 0 \end{pmatrix} \tag{4.13}$$

$$A_3 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ & 0 & -\frac{3f_2}{10} & -\frac{3f_3}{5} & 0 \\ & & 0 & -\frac{3f_4}{5} & 1 \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix} \tag{4.14}$$

$$A_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ & 0 & -\frac{f_3}{10} & -\frac{2f_4}{5} & -1 \\ & & 0 & -f_5 & 0 \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix} \tag{4.15}$$

Proof. We aim to find a $SL_5(\mathbb{Z})$-translate of $\Phi(f)$, which respects the $GL_2(\mathbb{Z})$ action on the nose and does not need slight adjustment by $h \in H$. Thus, we look for a polynomial map $P(f) \in H$ such that $\Phi'(f) = P(f) \cdot \Phi(f)$ is $GL_2(\mathbb{Z})$-equivariant, i.e. we want $\Phi'(\gamma \cdot f) = \sigma(\gamma) \cdot \Phi'(f)$.

Our work from Theorem 20 in fact tells us that $\Phi(\gamma \cdot f) = (1, h(\gamma, f)) \cdot \sigma(\gamma) \cdot \Phi(f)$, for $h(\gamma, f)$ polynomial in γ and f. We calculate:

$$\begin{aligned} \Phi'(\gamma \cdot f) &= P(\gamma \cdot f) \cdot \Phi(\gamma \cdot f) && (4.16) \\ &= P(\gamma \cdot f) \cdot (1, h(\gamma, f)) \cdot \sigma(\gamma) \cdot \Phi(f) && (4.17) \\ &= P(\gamma \cdot f) \cdot (1, h(\gamma, f)) \cdot \sigma(\gamma) \cdot P(f)^{-1}\Phi'(f) && (4.18) \\ &= (\psi(\gamma), P(\gamma \cdot f)h(\gamma, f)\rho(\gamma)P(f)^{-1}) \cdot \Phi'(f) && (4.19) \end{aligned}$$

Thus, we see that we need P such that $P(\gamma \cdot f)h(\gamma, f)\rho(\gamma)P(f)^{-1} = \rho(\gamma)$. From explicit calculation, the following P arises and indeed does the job, leading to $\Phi'(f)$:

$$P(f) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -\frac{2}{5}f_1 & 1 & 0 & 0 & \frac{2}{5}f_2 \\ -\frac{1}{10}f_2 & 0 & 1 & 0 & \frac{1}{10}f_3 \\ -\frac{2}{5}f_3 & 0 & 0 & 1 & \frac{2}{5}f_4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.20}$$

□

This map is only defined for integer-matrix forms, but there is a third, related map which respects the action of $GL_2(\mathbb{Z})$ and is defined for all binary quintic forms. Inspired by the analogous map in the case of binary quartics, we can map to a quotient of $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$:

Corollary 4.0.4. *Define* $\bar{\Phi} : Sym^5\mathbb{Z}^2 \to H\backslash(\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5)$ *by* $\bar{\Phi}(f) = H\Phi(f)$. *Then* $\bar{\Phi}(\gamma \cdot f) = \sigma(\gamma) \cdot \bar{\Phi}(f)$.

Proof. Follows from Theorem 20. [Note that this claim is well-defined: $\sigma(\gamma) \cdot \bar{\Phi}(f)$ is a left H-coset because $\sigma(\gamma)H\sigma(\gamma)^{-1} = H$.] □

Corollary 4.0.5. *The maps* Φ' *and* $\bar{\Phi}$ *are both discriminant-preserving.*

Proof. The based quintic ring in question is unchanged, so the same proof as that of Corollary 4.0.2 applies. □

Chapter 5

The sextic resolvent ring S_f

Binary quartic forms have the special property that they describe quartic rings whose cubic resolvent is monogenic. Given a binary quintic form, with associated quintic ring and sextic resolvent, what special properties does the resolvent ring have?

For binary quartic forms, the basis of the cubic resolvent ring depends only on the $GL_2(\mathbb{Z})$-orbit of the binary quartic in question. This is because the relevant map $GL_2(\mathbb{Z}) \to GL_2(\mathbb{Z}) \times GL_3(\mathbb{Z})$ has trivial $GL_2(\mathbb{Z})$ component. This means that the structure of the cubic resolvent can be understood in terms of the GL_2 invariants of the binary quartic form.

For binary quintic forms, since the map σ lands non-trivially in $SL_5(\mathbb{Z})$, this is not the case; just as the structure coefficients of the based ring R_f depend on f and not just its equivalence class, so the same will be true for the sextic resolvent $S_f = S(\Phi(f))$.

Yet, the block matrix form of $\rho(\gamma)$ is intriguing, and suggests there may be special structure in the resolvent ring; indeed, this has to do with the relation between $\{\beta_1^*, \beta_5^*\}$ and $\{\beta_2, \beta_3, \beta_4\}$.

5.1 The structure of the sextic resolvent ring

Recall the definition of dual-digenicity:

Definition 5.1.1. *Let (R, S) be a quintic ring / sextic resolvent pair, with both rings of non-zero discriminant. Consider S as a based ring, with basis denoted by $\{1, \beta_1, \ldots, \beta_5\}$. Denote the dual basis with respect to the trace pairing by $\{\beta_0^*, \beta_1^*, \ldots, \beta_5^*\}$, i.e. $\beta_i^* \in S \otimes \mathbb{Q}$ such that $Tr(\beta_i^* \beta_j) = \delta_{ij}$.*

Then, we say that the based ring S is dual-digenic *if it has the following property:*

$$(\beta_2, \beta_3, \beta_4) \equiv 8\, Disc(R) \cdot ((\beta_1^*)^2, 2\beta_1^*\beta_5^*, (\beta_5^*)^2)\, mod \mathbb{Q} \tag{5.1}$$

This can also be rephrased in terms of $Disc(S)$ using $Disc(S) = (16 \cdot Disc(R))^3$.

We also define a (non-based) ring S to be dual-digenic if it has a basis in which it is dual-digenic.

A few notes on this definition:

- That S is based means that the β_i are only determined mod $\mathbb{Z}$. However, the β_i^* will then be completely determined. Thus, the notion of dual-digenicity is well-defined.
- Since the basis of S is determined only mod $\mathbb{Z}$, it wouldn't make sense for this definition to be stated on the nose with an equality.
- But, then why is it stated mod $\mathbb{Q}$ and not mod $\mathbb{Z}$? We will see that, for $S = S_f$, the three expressions $8\Delta(f) \cdot ((\beta_1^*)^2, 2\beta_1^*\beta_5^*, (\beta_5^*)^2)$ may not lie in S, but some $\mathbb{Q}$-translate of each of them does. These will in turn be congruent to $\beta_2, \beta_3, \beta_4$ mod $\mathbb{Z}$.

Theorem 21. *Let f be a binary quintic form of non-zero discriminant $\Delta(f)$. Then, the based ring S_f is dual-digenic.*

Proof. Proof is by computation of the SL_4-invariants of $\Phi(f)$, from which the multiplicative structure of S_f can be computed as explained in Higher Composition Laws IV. [See Appendix for multiplication table.] □

[Note: If we had a different way to prove the Segre cubic = trace cubed property of Theorem 23, that would result in an alternative proof of the above result. Currently, the proof of Theorem 23 also relies on the multiplication table of S_f, though it is true for all $S(A)$.]

In a based sextic ring S_f, we shall use the shorthand $x = \beta_1^*, y = \beta_5^*$. Dual-digenicity of S_f tells us the following about x, y:

Lemma 5.1.2. $Tr(x^3) = Tr(x^2y) = Tr(xy^2) = Tr(y^3) = 0$

Proof. Since $Tr(\beta_i\beta_j^*) = 0$ for $i \neq j$ and $Tr(\beta_j^*) = 0$ for $j \neq 0$, choosing $i \in \{2, 3, 4\}$, $j \in \{1, 5\}$ and applying Theorem 21 does the job. □

Lemma 5.1.3. $(8\Delta(f))^2 \cdot Tr(x^iy^j) \in \mathbb{Z}$ *for* $i, j \geq 0, i + j = 5$.

Proof. For $i, j \in \{2, 3, 4\}$, $k \in \{1, 5\}$, $\mathbb{Z} \ni d_{ij}^k = Tr(\beta_i\beta_j\beta_k^*)$ and this expression is invariant under translating β_i, β_j by elements of $\mathbb{Q}$. Hence:

$$d^1_{22} = (8\Delta(f))^2 \quad \cdot Tr(x^5) \tag{5.2}$$
$$d^5_{22} = (8\Delta(f))^2 \quad \cdot Tr(x^4 y) \tag{5.3}$$
$$d^1_{23} = 2(8\Delta(f))^2 \cdot Tr(x^4 y) \tag{5.4}$$
$$d^5_{23} = 2(8\Delta(f))^2 \cdot Tr(x^3 y^2) \tag{5.5}$$
$$d^1_{24} = (8\Delta(f))^2 \quad \cdot Tr(x^3 y^2) \tag{5.6}$$
$$d^5_{24} = (8\Delta(f))^2 \quad \cdot Tr(x^2 y^3) \tag{5.7}$$
$$d^1_{33} = 4(8\Delta(f))^2 \cdot Tr(x^3 y^2) \tag{5.8}$$
$$d^5_{33} = 4(8\Delta(f))^2 \cdot Tr(x^2 y^3) \tag{5.9}$$
$$d^1_{34} = 2(8\Delta(f))^2 \cdot Tr(x^2 y^3) \tag{5.10}$$
$$d^5_{34} = 2(8\Delta(f))^2 \cdot Tr(x y^4) \tag{5.11}$$
$$d^1_{44} = (8\Delta(f))^2 \quad \cdot Tr(x y^4) \tag{5.12}$$
$$d^5_{44} = (8\Delta(f))^2 \quad \cdot Tr(y^5) \tag{5.13}$$

□

Lemma 5.1.4. $(8\,\Delta(f))^2 \cdot Tr((u\beta_5^* - v\beta_1^*)^5) = -10f(u,v)$

Proof. Finding the structure coefficients d^k_{ij} in the Appendix, we see that for $i,j \in \{2,3,4\}, k \in \{1,5\}$, they are all integer multiples of some f_i:

$$d^1_{22} = 10f_5 \;||\, d^5_{22} = -2f_4 \tag{5.14}$$
$$d^1_{23} = -4f_4 \,||\, d^5_{23} = 2f_3 \tag{5.15}$$
$$d^1_{24} = f_3 \quad ||\, d^5_{24} = -f_2 \tag{5.16}$$
$$d^1_{33} = 4f_3 \quad ||\, d^5_{33} = -4f_2 \tag{5.17}$$
$$d^1_{34} = -2f_2 \,||\, d^5_{34} = 4f_1 \tag{5.18}$$
$$d^1_{44} = 2f_1 \quad ||\, d^5_{44} = -10f_0 \tag{5.19}$$

Lemma 5.1.3 then completes the proof. □

Corollary 5.1.5. *A based sextic ring S can arise from at most one binary quintic form as $S_f = S(\Phi(f))$.*

Proof. If $S = S_f$ for some f, then f is encoded in β_1^*, β_5^* as in Lemma 5.1.4. □

5.2 An associated Segre cubic threefold

There is a variety called a Segre cubic 3-fold attached to an element $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$. This is work of Seok Hyeong (Sean) Lee [All original work? If not, which parts are due to Seok Hyeong?]. The construction is as follows:

Given a quadruple $A = (A_1, A_2, A_3, A_4)$ of skew-symmetric 5×5 matrices, for each point $x = (x_1 : x_2 : x_3 : x_4)$ in $\mathbb{P}^3$, the 5×5 skew-symmetric matrix

$x_1A_1 + x_2A_2 + x_3A_3 + x_4A_4$ has even rank. We denote this matrix by $A(x)$. For generic $x \in \mathbb{P}^3$, it has rank 4, but for bad x - which turn out to be the five points of $X_{R(A)}$ - its rank will be 2. Consider the following subvariety of $\mathbb{P}^3 \times \mathbb{P}^4$: $V = \{(x, y) : y \in ker(A(x))\}$. When we consider the map $V \to \mathbb{P}^3$, away from the five bad points identified, there is a unique point above each point $x \in \mathbb{P}^3$, since $dim(ker(A(x))) = 1$ generically. At the five bad points, by virtue of $dim(ker(A(x))) = 3$, there is a plane above each such point. So, V is $\mathbb{P}^3$ blown up at five points. If we now consider the image of V in $\mathbb{P}^4$, it turns out that this is a Segre cubic 3-fold, which is a dimension 3 cubic variety with ten singularities, which are all nodal.

Theorem 22 (S. H. Lee?). *Let $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$, $y, z \in \mathbb{C}^5$ with $y = (y_1, y_2, y_3, y_4, y_5)^t$ and $z = (z_1, z_2, z_3, z_4, z_5)^t$. The determinant $A_1y \wedge A_2y \wedge A_3y \wedge A_4y \wedge z$ factors as $\langle y, z\rangle \cdot F_A(y)$, where $\langle y, z\rangle = \sum y_iz_i$ is the usual bilinear dot product and $F_A(y)$ is a cubic form in y. Then, F_A cuts out the Segre cubic threefold associated to A.*

Lemma 5.2.1. *Let $(g, h) \in GL_4(\mathbb{C}) \times SL_5(\mathbb{C})$, and let $A' = (g, h) \cdot A$. Then:*

$$F_{A'}(y) = \det(g)\, F_A(h^ty) \tag{5.20}$$

Proof.

$$\begin{aligned}
\langle y, z\rangle \cdot F_{A'}(y) &= A'_1y \wedge A'_2y \wedge A'_3y \wedge A'_4y \wedge z && (5.21)\\
&= \det(g)\cdot \\
&\quad (hAh^t)_1y \wedge (hAh^t)_2y \wedge (hAh^t)_3y \wedge (hAh^t)_4y \wedge z && (5.22)\\
&= \det(g)\det(h)\cdot \\
&\quad (Ah^t)_1y \wedge (Ah^t)_2y \wedge (Ah^t)_3y \wedge (Ah^t)_4y \wedge h^{-1}z && (5.23)\\
&= \det(g)\langle h^ty, h^{-1}z\rangle \cdot F_A(h^ty) && (5.24)\\
&= \det(g)\langle y, z\rangle \cdot F_A(h^ty) && (5.25)
\end{aligned}$$

□

Before we state how the form F_A is related to the arithmetic of the sextic resolvent ring, we take a moment to note that the formulae of Higher Composition Laws IV define a commutative, associative sextic $\mathbb{C}$-algebra $S(A)$ when we extend them to $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$. Furthermore, $SL_4(\mathbb{C}) \times SL_5(\mathbb{C})$ acts on the basis of $S(A)/\mathbb{C}$ in the same way that $SL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ acts on the basis of $S(A)/\mathbb{Z}$ for integral A.

Now we can state the meaning of F_A in the sextic algebra $S(A)$:

Theorem 23. *Let A, F_A, y be as in Theorem 22, but with $Disc(A) \neq 0$. The sextic resolvent algebra $S = S(A)$ comes equipped with a basis of $S/\mathbb{C}$, and a corresponding dual basis of $\tilde{S}$ which we denote by $\{\beta_1^*, \ldots, \beta_5^*\}$. Then:*

$$8\, Disc(A) \cdot Tr((y_1\beta_1^* + \ldots + y_5\beta_5^*)^3) = -3\, F_A(y) \tag{5.26}$$

Proof. The $G = GL_4(\mathbb{C}) \times SL_5(\mathbb{C})$ representation $\mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ is a prehomogeneous vector space, meaning that is has a dense open orbit. This orbit is comprised of the elements of non-zero discriminant. So, if we can prove that the equation is G-invariant and that it holds for some A of non-zero discriminant, then it will hold for all A of non-zero discriminant, as desired.

Taking $A = \Phi(f)$ for any binary quintic of non-zero discriminant, our knowledge of the structure coefficients of $S(A)$ enables us to prove explicitly that this formula holds.

Now to prove G-invariance. Let $(g, h) \in G$ and $A' = (g, h) \cdot A$. We know from Lemma 5.2.1 that $F_{A'}(y) = \det(g)\, F_A(h^t y)$. We will prove that the left hand side of the equation transforms in the same way, by looking at the actions of $SL_4(\mathbb{C}) \times SL_5(\mathbb{C})$ and the scalar matrices $(\lambda I_4, I_5)$ separately.

Let $(g, h) \in SL_4(\mathbb{C}) \times SL_5(\mathbb{C})$. From our note above on the action of $SL_4(\mathbb{C}) \times SL_5(\mathbb{C})$ on the basis of $S(A)/\mathbb{C}$, we know that the action of (g, h) on the basis $\{\beta_1^*, \ldots, \beta_5^*\}$ of $\tilde{S(A)}$ is just by h. Transferring this change of basis to a transformation on y amounts to replacing y by $h^t y$. The polynomial $Disc(A)$ is invariant under $SL_4(\mathbb{C}) \times SL_5(\mathbb{C})$. Thus, both sides of the equation transform in the same way: by applying h^t to y.

Consider the action of $(\lambda I_4, I_5)$ on the equation. The structure coefficients of the sextic resolvent algebra are degree 12 polynomials in the entries of A. This means that λI_4 acts on them by λ^{12}. Hence, $(\lambda I_4, I_5)$ acts on the basis of the sextic resolvent algebra by λ^{12}, and the action on the dual basis is by λ^{-12}. The polynomial $Disc(A)$ is degree 40 and so $(\lambda I_4, I_5)$ acts by λ^{40}. Thus $(\lambda I_4, I_5)$ acts on the left hand side of the equation by λ^4. The action on the right hand side results in $\det(\lambda I_4) F_A(y) = \lambda^4 F_A(y)$, so we have equality. □

Let's compute the equation of the Segre cubic associated to $\Phi(f)$, which we denote by F_f:

$$\begin{aligned} F_f(y) = {} & -f_0f_2y_2^3 - f_0f_3y_2^2y_3 - f_0f_4y_2y_3^2 + f_0f_5y_2y_3y_4 \\ & -f_0f_5y_3^3 + f_0y_2^2y_5 - f_1f_3y_2^2y_4 - f_1f_4y_2y_3y_4 \\ & -f_1f_5y_3^2y_4 - f_1y_1y_2^2 - f_2f_4y_2y_4^2 - f_2f_5y_3y_4^2 \\ & +f_2y_2y_4y_5 - f_3f_5y_4^3 - f_3y_1y_2y_4 + f_4y_4^2y_5 \\ & -f_5y_1y_4^2 - y_1^2y_2 - y_1y_3y_5 - y_4y_5^2 \end{aligned} \tag{5.27}$$

Corollary 5.2.2. *Let $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. Then $S(A)$ is dual-digenic if and only if F_A takes the following form:*

$$F_A(y) = -y_1^2y_2 - y_1y_3y_5 - y_4y_5^2 + \textit{(lower order terms in } y_1, y_5\textit{)} \tag{5.28}$$

Proof. The product $\beta_i^*\beta_j^* \in S \otimes \mathbb{Q}$ has an expansion in terms of the basis $\{1, \beta_1, \ldots, \beta_5\}$ of $S \otimes \mathbb{Q}$. The β_k coefficient is given by $Tr(\beta_i^*\beta_j^*\beta_k^*)$. From Theorem 23, we know that these expressions are encoded in F_A, and the expansions of $(\beta_1^*)^2, 2\beta_1^*\beta_5^*, (\beta_5^*)^2$ will be given by the terms of F_A which are quadratic or cubic in y_1, y_5. □

Lemma 5.2.3. *Suppose $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ vanishes on a 2-dimensional subspace $V \subseteq \mathbb{C}^5$. Then $F_A(y) = 0$ for all $y \in V$.*

Proof. Fix non-zero $y \in V$. Consider the following 5×5 matrix:

$$\begin{pmatrix} | & | & | & | & | \\ A_1\, y & A_2\, y & A_3\, y & A_4\, y & \bar{y} \\ | & | & | & | & | \end{pmatrix}^t \tag{5.29}$$

where $\bar{y}$ denotes complex conjugation.

Its kernel contains $V \cap \{\bar{y}\}^\perp$, hence is non-trivial. So the determinant $F_A(y)\langle y, \bar{y}\rangle$ is zero, so $F_A(y) = 0$. □

We can now say exactly which quintic ring / sextic resolvent pairs are described by binary quintic forms.

Theorem 24. *Let (R, S) be a quintic ring / sextic resolvent pair, basis-free, of non-zero discriminant, with fundamental alternating map $\phi : \wedge^2\tilde{S} \to \tilde{R}$. Then, (R, S) arise from some binary quintic form if and only if the following two conditions hold:*

- *S has a basis $\{1, \beta_1, \dots, \beta_5\}$ in which it is dual-digenic*
- *The associated dual basis has the property $\phi(\beta_1^*, \beta_5^*) = 0$*

Proof. The forward implication is true by Theorem 21 and because $\Phi(f)$ has top-right entry equal to 0.

The reverse implication, however, needs proof: Let $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ giving rise to (R, S) with S in the given special basis.

The condition $\phi(\beta_1^*, \beta_5^*) = 0$ translates to $A(e_1, e_5) = 0$, from which we see that A is of the form:

$$\begin{pmatrix} 0 & a & b & c & 0 \\ -a & 0 & * & * & -d \\ -b & * & 0 & * & -e \\ -c & * & * & 0 & -f \\ 0 & d & e & f & 0 \end{pmatrix} \tag{5.30}$$

for some $a, b, c, d, e, f \in \mathbb{Z}[t_1, t_2, t_3, t_4]$. The entries marked $*$ will be unimportant.

By Corollary 5.2.2, we know that the terms of F_A cubic in y_1, y_5 all vanish and that the partial derivatives of F_A evaluated at $y_1 e_1 + y_5 e_5$ take the form:

$$\nabla F_A(y_1 e_1 + y_5 e_5) = (0, -y_1^2, -y_1 y_5, -y_5^2, 0) \tag{5.31}$$

These properties will impose conditions on a, b, c, d, e, f which will lead us to see that we are $SL_4(\mathbb{Z})$ equivalent to some $\Phi(f)$.

First, note that by Lemma 5.2.3, the vanishing of terms of F_A which are cubic in y_1, y_5 is already apparent. So, the only interesting conditions are on ∇F_A.

Recall the formula $F_A(y)\langle y, z\rangle = A_1y \wedge A_2y \wedge A_3y \wedge A_4y \wedge z$. Differentiating with respect to y_i, we get:

$$\begin{aligned}\frac{\partial F_A}{\partial y_i}(y)\langle y, z\rangle + F_A(y)z_i &= A_1e_i \wedge A_2y \wedge A_3y \wedge A_4y \wedge z + \dots \\ &\quad + A_1y \wedge A_2y \wedge A_3y \wedge A_4e_i \wedge z \qquad (5.32)\end{aligned}$$

Taking $y = y_1e_1 + y_5e_5$, this simplifies to:

$$\begin{aligned}\frac{\partial F_A}{\partial y_i}(y)\langle y, z\rangle &= A_1e_i \wedge A_2y \wedge A_3y \wedge A_4y \wedge z + \dots \\ &\quad + A_1y \wedge A_2y \wedge A_3y \wedge A_4e_i \wedge z \qquad (5.33)\end{aligned}$$

We can explicitly compute the determinants on the right hand side here, and thus the partial derivatives. The partial derivatives with respect to y_1 and y_5 come out as identically 0, as we expect from Lemma 5.2.3. The other partial derivatives are more interesting and are listed below. We use the notation $\Delta(pqrs)$ to mean the determinant of the 4×4 matrix whose rows are given by $p, q, r, s \in \mathbb{Z}^4 \simeq \mathbb{Z}[t_1, t_2, t_3, t_4]$.

$$\frac{\partial F_A}{\partial y_2}(y) = -y_1^2\,\Delta(abcd) + y_1y_5\,[\Delta(abdf) - \Delta(acde)] - y_5^2\,\Delta(adef) \quad (5.34)$$

$$\frac{\partial F_A}{\partial y_3}(y) = -y_1^2\,\Delta(abce) + y_1y_5\,[\Delta(abef) - \Delta(bcde)] - y_5^2\,\Delta(bdef) \quad (5.35)$$

$$\frac{\partial F_A}{\partial y_4}(y) = -y_1^2\,\Delta(abcf) + y_1y_5\,[\Delta(acef) - \Delta(bcdf)] - y_5^2\,\Delta(cdef) \quad (5.36)$$

Hence, we need the following equations to be satisfied by a, b, c, d:

$$\begin{aligned}\Delta(abcd) &= 1 &(5.37)\\ \Delta(abdf) - \Delta(acde) &= 0 &(5.38)\\ \Delta(adef) &= 0 &(5.39)\\ \Delta(abce) &= 0 &(5.40)\\ \Delta(abef) - \Delta(bcde) &= -1 &(5.41)\\ \Delta(bdef) &= 0 &(5.42)\\ \Delta(abcf) &= 0 &(5.43)\\ \Delta(acef) - \Delta(bcdf) &= 0 &(5.44)\\ \Delta(cdef) &= 1 &(5.45)\end{aligned}$$

It is not too hard to solve these by hand, but running them through any computer algebra package will effortlessly inform you that they amount to $e = -a, f = -b, \Delta(abcd) = 1$. This is true over any field, not just over the ring $\mathbb{Z}$.

Thus, the matrix with rows a, b, c, d lies in $SL_4(\mathbb{Z})$, and furthermore the transformation τ taking (a, b, c, d) to $(t_3, -t_2, t_1, t_4)$ also lies in $SL_4(\mathbb{Z})$. Thus, we can write:

$$A' = \tau \cdot A = \begin{pmatrix} 0 & t_3 & -t_2 & t_1 & 0 \\ -t_3 & 0 & * & * & -t_4 \\ t_2 & * & 0 & * & t_3 \\ -t_1 & * & * & 0 & -t_2 \\ 0 & t_4 & -t_3 & t_2 & 0 \end{pmatrix} \tag{5.46}$$

This matrix is almost of the form $\Phi(f)$. We will be able to show that we can transform it into the required form by applying an element $h \in H \leq SL_5(\mathbb{Z})$, where H is the subgroup of matrices of the form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ * & 1 & 0 & 0 & * \\ * & 0 & 1 & 0 & * \\ * & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{5.47}$$

Note: Any $h \in H$ gives rise to a change of basis of S; this change of basis will fix β_1^*, β_5^* and $\beta_2, \beta_3, \beta_4$ mod $\mathbb{Z}$, so it will preserve the dual-digenization of S.

So, we are looking for $h \in H$ which will transform A' into a matrix of the form $\Phi(f)$. We just have to find h which kills certain t_i coefficients in the central 3×3 block of A'. For example, in order to kill the t_4 term in $A'(e_2, e_3)$, we translate e_3 by a choice multiple n of e_5, as $A'(e_2, e_3 + ne_5) = A'(e_2, e_3) - nt_4$. These conditions amount to six linear equations in the entries of h, easily seen to have a unique solution; if we didn't have $A'(e_1, e_5) = 0$, these equations would be quadratic and their solubility would be unclear. □

5.3 The action of $GL_2(\mathbb{Z})$ on the sextic resolvent ring

Recall Theorem 20:

Theorem 25. *Let $f \in (Sym^5\mathbb{Z}^2)^*$ and $\gamma \in GL_2(\mathbb{Z})$. Then there exists $h \in H$ such that $\Phi(\gamma \cdot f) = (1, h) \cdot \sigma(\gamma) \cdot \Phi(f)$*

This results in the following action on the basis of the sextic resolvent ring:

Corollary 5.3.1. *Let $f \in (Sym^5\mathbb{Z}^2)^*$, $\gamma \in GL_2(\mathbb{Z})$ and $g = \gamma \cdot f$.*

Denote the basis of S_f by $\{1, \beta_{1,f}, \ldots, \beta_{5,f}\}$, with the usual notation $\beta_{i,f}^*$ for the dual basis of $\tilde{S_f}$. Denote the basis elements of S_g and $\tilde{S_g}$ analogously.

Then:

$$\begin{pmatrix} \beta_{1,g}^* \\ \beta_{5,g}^* \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \begin{pmatrix} \beta_{1,f}^* \\ \beta_{5,f}^* \end{pmatrix} \tag{5.48}$$

$$\begin{pmatrix} \beta_{2,g} \\ \beta_{3,g} \\ \beta_{4,g} \end{pmatrix} \equiv \begin{pmatrix} d^2 & -cd & c^2 \\ -2bd & bc + ad & -2ac \\ b^2 & -ab & a^2 \end{pmatrix} \begin{pmatrix} \beta_{2,f} \\ \beta_{3,f} \\ \beta_{4,f} \end{pmatrix} \quad mod \quad \mathbb{Z} \tag{5.49}$$

Proof. The SL_5 component of $(1,h)\cdot\sigma(\gamma)$ is of the form:

$$\begin{pmatrix} d & 0 & 0 & 0 & -c \\ * & a^2 & 2ab & b^2 & * \\ * & ac & bc+ad & bd & * \\ * & c^2 & 2cd & d^2 & * \\ -b & 0 & 0 & 0 & a \end{pmatrix} \tag{5.50}$$

An element $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ represents a map $\wedge^2\tilde{S} \to \tilde{R}$, and the action of $SL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ on this space gives rise to a change of basis of $\tilde{S}$, given by the SL_5 component. Since $(1,h)\cdot\sigma(\gamma) \in SL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$, the matrix above tells us the relation between the bases of $\tilde{S_f}$ and $\tilde{S}_g$, while the transpose inverse tells us how the bases of $S_f/\mathbb{Z}$ and $S_g/\mathbb{Z}$ are related. The result follows. □

Note that this respects the dual-digenicity relation between $\{\beta_1^*, \beta_5^*\}$ and $\{\beta_2, \beta_3, \beta_4\}$.

There is also a subtle point to be made here: We can view $S_f^* \otimes \mathbb{Q}$ as a 6-dimensional representation of $GL_2(\mathbb{Z})$, and likewise for $S_f \otimes \mathbb{Q}$. From the block matrix form of $\rho(\gamma) \in GL_5(\mathbb{Z})$, we see that both these representations break into irreducible components of dimensions 1, 2 and 3. We have an equality $S_f^* \otimes \mathbb{Q} = S_f \otimes \mathbb{Q}$ given by the trace pairing, and we might then think that the subrepresentations occuring in each representation are equal. However, this is not the case; the key point to be noted is that, on this shared space, the two $GL_2(\mathbb{Z})$-actions are in general different, as explained by the following lemma:

Lemma 5.3.2. *Let K be a field. Suppose that V is a K-vector space with basis $\{v_0, v_1, \ldots, v_{n-1}\}$, and with a non-degenerate pairing $\langle -,- \rangle : V \otimes_K V \to K$. Using $\langle -,- \rangle$, we can identify V^* and V; denote the dual basis by $\{v_0^*, v_1^*, \ldots, v_{n-1}^*\} \subset V$. Let $\sigma \in GL(V)$ such that $\sigma(v_i) = w_i$ and $\sigma(v_i^*) = w_i^*$, where $\{w_0^*, w_1^*, \ldots, w_{n-1}^*\}$ is the dual basis of $\{w_0, w_1, \ldots, w_{n-1}\}$. Then σ stabilises $\langle -,- \rangle$.*

Proof. The dual basis is obtained as follows:

$$\begin{pmatrix} v_0^* \\ v_1^* \\ \cdots \\ v_{n-1}^* \end{pmatrix} = \big(\langle v_i, v_j \rangle\big)_{i,j}^{-1} \begin{pmatrix} v_0 \\ v_1 \\ \cdots \\ v_{n-1} \end{pmatrix} \tag{5.51}$$

Since σ is K-linear, we have:

$$\begin{pmatrix} \sigma(v_0^*) \\ \sigma(v_1^*) \\ \cdots \\ \sigma(v_{n-1}^*) \end{pmatrix} = \big(\langle v_i, v_j \rangle\big)_{i,j}^{-1} \begin{pmatrix} \sigma(v_0) \\ \sigma(v_1) \\ \cdots \\ \sigma(v_{n-1}) \end{pmatrix} \tag{5.52}$$

But if $\sigma(v_i) = w_i$ and $\sigma(v_i^*) = w_i^*$ then this simplifies:

$$\begin{pmatrix} w_0^* \\ w_1^* \\ \cdots \\ w_{n-1}^* \end{pmatrix} = \big(\langle v_i, v_j \rangle\big)_{i,j}^{-1} \begin{pmatrix} w_0 \\ w_1 \\ \cdots \\ w_{n-1} \end{pmatrix} \tag{5.53}$$

However, we also know to obtain w_i^* in the following way:

$$\begin{pmatrix} w_0^* \\ w_1^* \\ \dots \\ w_{n-1}^* \end{pmatrix} = \big(\langle w_i, w_j\rangle\big)_{i,j}^{-1} \begin{pmatrix} w_0 \\ w_1 \\ \dots \\ w_{n-1} \end{pmatrix} \tag{5.54}$$

Hence, $\langle w_i, w_j\rangle = \langle v_i, v_j\rangle$ for all i, j, and so σ stabilises the pairing. □

This means that we should be careful when using this representation-theoretic perspective to draw links between S_f and S_f^*.

5.4 Classes of binary quintic forms and sextic resolvent rings

Now that we understand how $GL_2(\mathbb{Z})$ acts on the bases of the quintic ring and sextic resolvent, we will be able to fully understand classes of binary quintics through the lens of these rings.

First, we introduce two definitions which recognise the isomorphisms between rings coming from the $GL_2(\mathbb{Z})$ action:

Definition 5.4.1. *Let (R, S) be a quintic ring / sextic resolvent pair, with both rings of non-zero discriminant.*

Consider the map which sends a dual-digenic basis $\mathfrak{B}$ of S to the submodule $\mathbb{Z}\{1, \beta_2, \beta_3, \beta_4\} \subseteq S$. A dual-digenization *of S is a non-empty preimage under this map, i.e. a class of dual-digenic bases of S, all producing the same submodule via the construction $\mathbb{Z}\{1, \beta_2, \beta_3, \beta_4\}$.*

Equivalently, each class is determined by $\mathbb{Z}\{\beta_1^*, \beta_5^*\}$, as this is the submodule of S^* which is orthogonal to $\mathbb{Z}\{1, \beta_2, \beta_3, \beta_4\}$.

The key structure of a dual-digenic based ring comes from the relation between $\{\beta_1^*, \beta_5^*\}$ and $\{\beta_2, \beta_3, \beta_4\}$. However, applying an element of $GL_2(\mathbb{Z})$ to $\{\beta_1^*, \beta_5^*\}$ gives rise to a new dual-digenic basis, so the key object is really $\mathbb{Z}\{\beta_1^*, \beta_5^*\}$. The definition of dual-digenization is cooked up to recognise this.

Definition 5.4.2. *Let S and S' be based sextic rings of non-zero discriminant, with dual-digenic bases. A* dual-digenic isomorphism *between S and S' is an isomorphism which respects the dual-digenizations of the two rings.*

Corollary 5.4.3. *Let f be a binary quintic form of non-zero discriminant, let $\gamma \in GL_2(\mathbb{Z})$ and $g = \gamma \cdot f$. Then there is a dual-digenic isomorphism from S_f to S_g.*

Proof. Theorem 20 implies that S_f and S_g are isomorphic. Corollary 5.3.1 details this isomorphism and makes clear that it preserves the dual-digenizations of S_f and S_g. □

Note: It is possible to have two distinct dual-digenizations of a sextic ring S which are isomorphic via a dual-digenic isomorphism. A useful analogy to consider is the monogenizations of the quadratic ring $R = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$. This has distinct monogenizers ω and ω^2, but these are isomorphic monogenizations in the sense that there is an automorphism of R taking ω to ω^2.

We can now state our main theorem relating classes of binary quintic forms to quintic rings and sextic resolvent rings:

Theorem 26. *There is a bijection between the following two sets:*

$$GL_2(\mathbb{Z})\backslash(Sym^5\mathbb{Z}^2)^* \leftrightarrow \left\{ \begin{array}{l} (R,S), R \textit{ basis-free,} \\ S \textit{ dual-digenic with a} \\ \textit{fixed dual-digenization} \\ \textit{and } \phi(\beta_1^*, \beta_5^*) = 0 \end{array} \right\} / \sim \tag{5.55}$$

given by $f \mapsto$ the class of (R_f, S_f), where the $\sim$ denotes isomorphism of R and dual-digenic isomorphism of S, and where ϕ is the fundamental alternating map $\wedge^2\tilde{S} \to \tilde{R}$.

Proof. From Theorem 24, we know that every binary quintic form gives rise to a sextic resolvent ring S_f with a dual-digenic basis, with $\phi(\beta_1^*, \beta_5^*) = 0$, and furthermore by Corollary 5.4.3 the map above descends to classes of forms.

Conversely, let (R, S) be a quintic ring / sextic resolvent pair, with a fixed dual-digenization of S and $\phi(\beta_1^*, \beta_5^*) = 0$. Theorem 24 also tells us that there are bases of R and S such that (R, S) is given by $\Phi(f)$ for some f. The change of basis of S comes from $h \in H$, so it preserves the choice of dual-digenization. Hence, the map in the statement of this theorem is surjective.

For injectivity, suppose (R_f, S_f) and (R_g, S_g) are isomorphic, with a dual-digenic isomorphism of S_f and S_g. Because $\mathbb{Z}\{\beta_1^*, \beta_5^*\}$ is fixed, one component of the change of basis from $\tilde{S_f}$ to $\tilde{S_g}$ looks like:

$$\begin{pmatrix} \beta_{1,g}^* \\ \beta_{5,g}^* \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \begin{pmatrix} \beta_{1,f}^* \\ \beta_{5,f}^* \end{pmatrix} \tag{5.56}$$

for some matrix $\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in GL_2(\mathbb{Z})$.

Recall from Lemma 5.1.4 that $Tr((u\beta_{5,f}^* - v\beta_{1,f}^*)^5) = -10f(u, v)$, and similarly for g. It follows that f and g are $GL_2(\mathbb{Z})$-equivalent, as desired. □

5.5 The Cayley-Klein resolvent map

Recall from Higher Composition Laws IV the Cayley-Klein resolvent map $\psi : R \to \tilde{S}$, defined as

$$\begin{aligned} \alpha \mapsto \frac{1}{\sqrt{Disc(R)}} (&\alpha^{(1)}\alpha^{(2)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(3)}\alpha^{(4)} + \alpha^{(4)}\alpha^{(5)} + \alpha^{(5)}\alpha^{(1)} \\ &-\alpha^{(1)}\alpha^{(3)} - \alpha^{(3)}\alpha^{(5)} - \alpha^{(5)}\alpha^{(2)} - \alpha^{(2)}\alpha^{(4)} - \alpha^{(4)}\alpha^{(1)}) \end{aligned} \tag{5.57}$$

Lemma 5.5.1. *The Cayley-Klein map $\psi : R_f \to \tilde{S_f}$ has the following property:*

$$\psi(x^3\alpha_1 + x^2y\alpha_2 + xy^2\alpha_3 + y^3\alpha_4) = 4f(x,y)(y\beta_1^* - x\beta_5^*) \tag{5.58}$$

Proof. Bhargava shows that, for $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ and the associated based quintic ring $R = R(A)$, this map is given by the 4×4 signed sub-Pfaffians $(P_1, \ldots, P_5)$ of A as follows:

$$\psi(t_1\alpha_1 + \ldots + t_4\alpha_4) = 4P_1(t)\beta_1^* + \ldots + 4P_5(t)\beta_5^* \tag{5.59}$$

Recall that when $A = \Phi(f)$, the sub-pfaffians are in the span of the following five quadrics:

$$Q_1 = t_1t_3 - t_2^2 \tag{5.60}$$

$$Q_2 = t_1t_4 - t_2t_3 \tag{5.61}$$

$$Q_3 = t_2t_4 - t_3^2 \tag{5.62}$$

$$Q_4 = f_0t_1t_2 + f_1t_2^2 + f_2t_2t_3 + f_3t_3^2 + f_4t_3t_4 + f_5t_4^2 \tag{5.63}$$

$$Q_5 = f_0t_1^2 + f_1t_1t_2 + f_2t_2^2 + f_3t_2t_3 + f_4t_3^2 + f_5t_3t_4 \tag{5.64}$$

In fact, the five 4×4 signed sub-pfaffians are easily seen to be:

$$Q(A) = [Q_4, Q_1, Q_2, Q_3, -Q_5] \tag{5.65}$$

When $A = \Phi(f)$ and $(t_1, \ldots, t_4) = (x^3, x^2y, xy^2, y^3)$, because of the special form of the sub-Pfaffians, they simplify to give the stated result. □

This mimics the behaviour of the resolvent maps for binary cubics and quartics:

- For a binary cubic, the resolvent map has the property:

$$x\alpha_1 + y\alpha_2 \mapsto f(x,y)\omega \tag{5.66}$$

  where ω generates the quadratic resolvent ring.

- For a binary quartic, the resolvent map has the property:

$$x^2\alpha_1 + xy\alpha_2 + y^2\alpha_3 \mapsto f(x,y)\omega \tag{5.67}$$

  where ω generates the cubic resolvent ring.

So, it seems that the resolvent map picks out some of the key structure of the resolvent ring, when evaluated on a certain family of elements corresponding to the relevant rational normal curve.

Chapter 6

Counting binary quintics of bounded discriminant

From Theorem 26, we understand how classes of binary quintic forms map into the space $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$. Results counting Γ-classes of bounded discriminant in $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ exist [source?], and we would like to port these over to give counting results on binary quintics. The one missing ingredient is our understanding of how many $GL_2(\mathbb{Z})$-classes of binary quintics can map into one Γ-orbit, which is the principal problem we aim to tackle here. We will explain geometric and algebraic approaches to this problem.

6.1 A geometrical viewpoint

6.1.1 Lines on the Segre cubic

Let $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ and $S = S(A)$. Recall from Corollary 5.2.2 that dual-digenicity of S is reflected in the equation F_A of the associated Segre cubic. Specifically, the based ring S is dual-digenic if and only if F_A takes the form $F_A(y) = -y_1^2y_2 - y_1y_3y_5 - y_4y_5^2 +$ (lower order terms in y_1, y_5). In particular, there is a distinguished projective line $L = \mathbb{C}\{e_1, e_5\}$ on the Segre cubic.

We will see that all dual-digenizations of the ring S have associated lines on the Segre cubic and that the ones arising from binary quintics, meaning that also $\phi(\beta_1^*, \beta_5^*) = 0$, actually come from a special component of the Fano variety of lines on the Segre cubic.

Lemma 6.1.1. *Let $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ of non-zero discriminant, and let $S = S(A)$. Consider S as a basis-free ring. Then, each dual-digenization of S (if any exist) gives rise to a distinct line on the Segre cubic associated to A, which we denote by V_A.*

Proof. We know that A gives rise to a dual-digenic basis of S if and only if $F_A(y) = -y_1^2y_2 - y_1y_3y_5 - y_4y_5^2 +$ (lower order terms in y_1, y_5). In this situation, we also then have the weaker statement that F_A vanishes on $sp\{e_1, e_5\}$.

Now, let's consider different bases of S. Lemma 5.2.1 tells us that if $(\tau, \gamma) \in GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ and $A' = (\tau, \gamma) \cdot A$ then:

$$F_{A'}(y) = \det(\tau)\, F_A(\gamma^t y) \tag{6.1}$$

Denote the i-th row of γ by γ_i. If A' gives rise to a dual-digenic basis of S, $F_{A'}$ vanishes on $\mathbb{C}\{e_1, e_5\}$, and F_A vanishes on $\mathbb{C}\{\gamma_1, \gamma_5\}$.

We need to see that this construction gives the same line for two bases precisely when they are in the same dual-digenization. Recall that two dual-digenic bases are in the same dual-digenization if $\mathbb{Z}\{\beta_1^*, \beta_5^*\}$ is the same for both of them. The rows of γ give the change of dual basis (up to the factor $\det(\tau) \in \{\pm 1\}$), so taking a different basis in the same dual-digenization means acting on (γ_1, γ_5) by some element of $GL_2(\mathbb{Z})$. Such a transformations keeps the line constructed above fixed. Conversely, if γ, γ' give rise to the same line L, then (γ_1, γ_5) and (γ'_1, γ'_5) are related by an element of $GL_2(\mathbb{Z})$, as they are $\mathbb{Z}$-bases of the integral lattice contained in L. If they both give rise to dual-digenic bases, they are therefore in the same dual-digenization. □

This means that each dual-digenization of S gives rise to a unique point in the Fano variety of lines on V_A. Dolgachev proves that this variety is a 2-dimensional variety given by 15 planes and 6 degree five del Pezzo surfaces, and gives a description of the lines represented by each component. In particular, each of its irreducible components has infinitely many rational points. We know there are finitely many classes of forms of the same discriminant, so only finitely many of these lines can be of note to us. There must be other equations to cut down the search, and at some point we need to work over $\mathbb{Z}$.

The next step is to show that the lines arising from binary quintics all come from a distinguished one of these del Pezzo surfaces, which Dolgachev calls D_6.

6.1.2 The del Pezzo surface D_6

There is a quadratic map $\psi_A : \mathbb{P}^3 \to V(A)$ given by the sub-pfaffians of A. Its indeterminacy locus is 5 points $\{p_1, \ldots, p_5\}$, which is actually the set $X_{R(A)}$. Given a twisted cubic C in $\mathbb{P}^3$ passing through these 5 points, the image of C under this map will be a line on the Segre cubic. The component D_6 of the Fano variety is precisely all such lines.

For $\Phi(f)$, denote the quadratic map $\psi_{\Phi(f)}$ by ψ_f. This map is given by the following forms:

$$Q_1 = f_0 t_1 t_2 + f_1 t_2^2 + f_2 t_2 t_3 + f_3 t_3^2 + f_4 t_3 t_4 + f_5 t_4^2 \tag{6.2}$$

$$Q_2 = t_1 t_3 - t_2^2 \tag{6.3}$$

$$Q_3 = t_1 t_4 - t_2 t_3 \tag{6.4}$$

$$Q_4 = t_2 t_4 - t_3^2 \tag{6.5}$$

$$Q_5 = -(f_0 t_1^2 + f_1 t_1 t_2 + f_2 t_2^2 + f_3 t_2 t_3 + f_4 t_3^2 + f_5 t_3 t_4) \tag{6.6}$$

Note that the rational normal curve in $\mathbb{P}^3$, cut out by the vanishing of $\{Q_2, Q_3, Q_4\}$, has image $\mathbb{C}\{e_1, e_5\}$, and that the indeterminacy locus of this map lies on the rational normal curve. So this line is represented by a point of D_6. In fact, all the dual-digenizations coming from binary quintic forms will give rise to points of D_6; however, this is not the case for any dual-digenization, as we will see later.

Lemma 6.1.2. *Let f be a binary quintic form of non-zero discriminant, $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ and $(\tau, \gamma) \in GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ such that $\Phi(f) = (\tau, \gamma) \cdot A$. Then, the line on V_A coming from the dual-digenic basis given by (τ, γ) is represented by a point of D_6.*

Proof. We have seen that we have a line on the Segre cubic $V_{\Phi(f)}$ which is the image of a twisted cubic; namely, the line $\mathbb{C}\{e_1, e_5\}$ which is the image of the rational normal curve.

The maps $\psi_f : \mathbb{P}^3 \to V_{\Phi(f)}$ and $\psi_A : \mathbb{P}^3 \to V_A$ are related by (τ, γ) via an action on the sub-pfaffians, described in Lemma **??** (action on sub-pfaffians) which was proved in Higher Composition Laws IV. The following commutative diagram summarises the relation:

$$\begin{tikzcd}
\mathbb{P}^3 \arrow[r, "\psi_A"] & V_A \\
\mathbb{P}^3 \arrow[r, "\psi_f"] \arrow[u, "\tau^t"] & V_{\Phi(f)} \arrow[u, "\gamma^t"']
\end{tikzcd} \tag{6.7}$$

To use this diagram to our benefit, we trace the image of the rational normal curve in the bottom $\mathbb{P}^3$ through the various maps. Its image in the top $\mathbb{P}^3$ is a twisted cubic. Furthermore, this curve goes through the five points of $X_{R(A)}$; this is because the rational normal curve goes through X_{R_f} and $X_{R(A)} = \tau^t X_{R_f}$. Meanwhile, the image of the rational normal curve under ψ_f is the line $\mathbb{C}\{e_1, e_5\} \subseteq V_{\Phi(f)}$, whose image in V_A under γ^t is the line $\mathbb{C}\{\gamma_1, \gamma_5\}$. So, the line on V_A coming from γ is represented by a point of D_6, according to Dolgachev's description. □

The component D_6 of the Fano variety of V_A has a very neat description in terms of A. We state this result here, but postpone its proof to later, as Corollary 6.2.2:

Proposition 6.1.3. *Let $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$. Then the component D_6 of the Fano variety of V_A is the set of all lines L for which $A|_L = 0$.*

We have narrowed the problem down to searching for rational points on this component D_6. However, a degree five del Pezzo surface is birational to $\mathbb{P}^2$ over $\mathbb{Q}$, so this component still has infinitely many rational points!

Furthermore, our problem concerns integral binary quintics, not rational binary quintics, so we need to move our problem over to $\mathbb{Z}$ by dehomogenising D_6, and then find a subvariety of this that captures only the finitely many points represented by classes of integral binary quintic forms. As we move to $\mathbb{Z}$, the problem will take on a more algebraic flavour.

But, before we move on to these problems, let us understand the other components of the Fano variety a little better.

6.1.3 The other components of the Fano variety

First of all, the 15 planes of the Fano variety are the lines contained in the 15 planes of the Segre cubic.

Lemma 6.1.4. *Let $A \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ of non-zero discriminant, and let $S = S(A)$. A line arising from a dual-digenization of S does not lie on a plane of the Segre cubic.*

Proof. Let L be a line on the Segre cubic V_A arising from a dual-digenization of S. We can find $(\tau, \gamma) \in GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ such that the basis of S arising from $A' = (\tau, \gamma) \cdot A$ is in this dual-digenization. Thus, $L = \mathbb{C}\{\gamma_1, \gamma_5\}$. Recall from Lemma 5.2.2 that:

$$F_{A'}(y) = -y_1^2 y_2 - y_1 y_3 y_5 - y_4 y_5^2 + (\text{lower order terms in } y_1, y_5) \tag{6.8}$$

This can be rephrased as:

$$\nabla F_{A'}(y_1 e_1 + y_5 e_5) = (0, -y_1^2, -y_1 y_5, -y_5^2, 0) \tag{6.9}$$

Also, recall from Lemma 5.2.1 that:

$$F_{A'}(y) = \det(\tau) F_A(\gamma^t y) \tag{6.10}$$

Differentiating this equation gives:

$$\nabla F_{A'}(y) = \det(\tau) \nabla F_A(\gamma^t y) \cdot \gamma^t \tag{6.11}$$

When we evaluate this last equation at $y = y_1 e_1 + y_5 e_5$ and apply $(\gamma^t)^{-1}$, we see that:

$$\dim(\mathrm{sp}\{\nabla F_A(l) : l \in L\}) = 3 \tag{6.12}$$

However, if L were contained in some plane P then $\{\nabla F_A(l) : l \in L\}) \subseteq P^{\perp}$, hence its dimension would be bounded by 2. $\square$

The other five del Pezzos, $D_1, \ldots, D_5$, are given as follows: take p_i in the indeterminacy locus of the map $\psi_f : \mathbb{P}^3 \to V(\Phi(f))$. The image under this map of a line passing through p_i is a line on the Segre cubic. The component D_i is the union of such lines.

Lemma 6.1.5. *Let f be binary quintic forms of non-zero discriminant, $A \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ and $(\tau, \gamma) \in GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ such that $\Phi(f) = (\tau, \gamma) \cdot A$. Then, the line on V_A coming from the dual-digenic basis arising from (τ, γ) is not represented by a point of $D_1, \ldots, D_5$.*

Proof. Start with the simplest case: the line $L = \mathbb{C}\{e_1, e_5\}$ on $V_{\Phi(f)}$. By looking at the five sub-pfaffians giving ψ_f, it is easy to see that the preimage of L under this map is the rational normal curve. This curve contains no lines and so L does not lie in any of the del Pezzos $D_1, \ldots, D_5$.

Consider the following diagram:

$$\begin{tikzcd}
\mathbb{P}^3 \arrow[r, "\psi_A"] & V_A \\
\mathbb{P}^3 \arrow[u, "\tau^t"] \arrow[r, "\psi_f"] & V_{\Phi(f)} \arrow[u, "\gamma^t"']
\end{tikzcd} \tag{6.13}$$

Now let L be the line on V_A coming from γ, i.e. $L = \mathbb{C}\{\gamma_1, \gamma_5\}$. This diagram shows us that:

$$\psi_A^{-1}(L) = \tau^t \psi_f^{-1}(\mathbb{C}\{e_1, e_5\}) \tag{6.14}$$

$$= \tau^t V_3 \tag{6.15}$$

where V_3 is the rational normal curve in $\mathbb{P}^3$. Hence, L is not the image under ψ_A of any line in $\mathbb{P}^3$, and so it is not represented by a point of $D_1, \ldots, D_5$. □

This means that all the lines in V_A of interest to us (i.e. those coming from binary quintic forms) lie in only the del Pezzo component D_6 of the Fano variety.

6.2 An algebraic viewpoint

Now that we understand the geometry of the situation, we would like to find equations pinning down precisely those points of D_6 corresponding to classes of binary quintic forms. First of all, we'll find equations cutting out D_6, and then we'll dehomogenise our equations so we can truly work over $\mathbb{Z}$ and introduce further equations satisfied by dual-digenic bases.

Before we prove these results, we note that the Fano variety lives inside $Gr(2, 5)$, which is the space of lines in $\mathbb{P}^4$. Let $L = \mathbb{C}\{x, y\}$ be a line in $\mathbb{P}^4$. We attach to L its Pluecker coordinates $p_{ij} = x_i y_j - x_j y_i$ for $i < j$. This gives a well-defined map $Gr(2, 5) \to \mathbb{P}^9$, which is known as the Pluecker embedding. The image is a dimension 6 subvariety of $\mathbb{P}^9$ cut out by the 5 equations of the form $p_{ij}p_{kl} + p_{jk}p_{il} + p_{ki}p_{jl} = 0$, called the Pluecker relations. Using algebraic geometry, it is possible to calculate that this is a dimension 6, degree 5 variety in $\mathbb{P}^9$.

Proposition 6.2.1. *Let f be a binary quintic form of non-zero discriminant. Let L be a line in $\mathbb{P}^3$ on which $\Phi(f)$ vanishes identically. Then L is a line on the Segre cubic $V_{\Phi(f)}$, and the points of D_6 correspond precisely to all such lines.*

Hence, D_6 is cut out by the following equations inside $Gr(2, 5)$, which come *from the equation $\Phi(f)(x,y) = 0$:*

$$p_{14} - f_0 p_{23} = 0 \tag{6.16}$$

$$-p_{45} - p_{13} - f_1 p_{23} - f_2 p_{24} = 0 \tag{6.17}$$

$$p_{12} + p_{35} - f_3 p_{24} - f_4 p_{34} = 0 \tag{6.18}$$

$$-p_{25} - f_5 p_{34} = 0 \tag{6.19}$$

Proof. Let $L = \mathbb{C}\{x, y\}$, with $\Phi(f)(x,y) = 0$. The line L lies on the Segre cubic by Lemma 5.2.3. Furthermore, the property of $\Phi(f)$ vanishing on L is independent of the basis of L, so it should be given by equations in the Pluecker coordinates p_{ij}. This is seen to be the case by looking at each t_i component of $\Phi(f)(x,y) = 0$, and this is how the four equations above enter the picture.

The Pluecker relations and these linear equations combined cut out a subvariety of $\mathbb{P}^9$, which we denote by W. Since the image of the Pluecker embedding has dimension 6, intersecting it with four hyperplanes results in a (possibly reducible) variety with irreducible components of dimension at least 2. However, we know that W is a subvariety of the 2-dimensional Fano variety of the Segre cubic, so the dimension of each irreducible component is precisely 2. Intersecting an irreducible variety with a hyperplane preserves degree, so every irreducible component of W has dimension 2 and W has degree 5 (with multiplicity). Since its degree is 5, it is either one of the del Pezzo surfaces, or a union of at most five planes.

Up until now, everything was true for a generic $A \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$. At this point, we use something about the shape of $\Phi(f)$. Namely, $\Phi(f)$ always has top-right entry 0, so the line $L = \mathbb{C}\{e_1, e_5\}$ - given by $p_{15} = 1, p_{ij} = 0$ for all other (i,j) - is in W. However, we saw that it is not contained in any of the planes or any of the del Pezzo surfaces $D_1, \ldots, D_5$. Hence, $W = D_6$. □

Corollary 6.2.2. *Let $A \in \mathbb{C}^4 \otimes \wedge^2 \mathbb{C}^5$. Then the component D_6 of the Fano variety of V_A is the set of all lines L for which $A|_L = 0$.*

Proof. Consider the open set of nondegenerate $A \in \mathbb{C}^4 \otimes \wedge^2 \mathbb{C}^5$. The $GL_4(\mathbb{C}) \times SL_5(\mathbb{C})$-action on this set induces an action on the associated Segre cubics, summarised by the following equation and diagram, where $A' = (\tau, \gamma) \cdot A$:

$$F_{A'}(y) = \det(\tau)\, F_A(\gamma^t y) \tag{6.20}$$

$$\begin{tikzcd}
\mathbb{P}^3 \arrow[r, "\psi_A"] & V_A \\
\mathbb{P}^3 \arrow[u, "\tau^t"] \arrow[r, "\psi_{A'}"] & V_{A'} \arrow[u, "\gamma^t"']
\end{tikzcd} \tag{6.21}$$

This action preserves lines on the Segre cubic, so it induces an action on the associated Fano varieties. In fact, because lines, planes and twisted cubics are preserved under the action of GL_n, and because $X_{R(A)} = \tau^t \cdot X_{R(A')}$, the diagram above shows that the following sets of components of the Fano variety are invariant under this action:

- The 15 components coming from lines through the planes of the Segre cubic
- $D_1, \ldots, D_5$, as these come from lines in $\mathbb{P}^3$ passing through at least one point of $X_{R(A)}$
- D_6, as this component comes from twisted cubics in $\mathbb{P}^3$ through all of $X_{R(A)}$

The nondegenerate elements of $\mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ form an open orbit under the action of $GL_4(\mathbb{C}) \times SL_5(\mathbb{C})$, so given A we can find (τ, γ) such that $A = (\tau, \gamma) \cdot \Phi(f)$. Denote the D_6 component of the Fano variety of V_A by $D_6(A)$, and use analogous notation for $\Phi(f)$. Let L be a line in $\mathbb{P}^5$, which we view as living in $Gr(2, 5)$. Then, invoking Lemma 6.2.1:

$$\begin{aligned} L \in D_6(A) &\iff \gamma^t L \in D_6(\Phi(f)) && (6.22)\\ &\iff \Phi(f)|_{\gamma^t L} = 0 && (6.23)\\ &\iff \gamma\Phi(f)\gamma^t|_L = 0 && (6.24)\\ &\iff A|_L = 0 && (6.25) \end{aligned}$$

□

Our next step is to introduce stricter equations for dual-digenicity of a basis. Previously, we only used that the Segre cubic has no terms cubic in y_1, y_5 in this case, but we did not use the full property of Lemma 5.2.2. This is genuinely an integral property, so it has the added bonus of finally moving our equations over $\mathbb{Z}$.

Let $A' = (\tau, \gamma) \cdot A$, with $S(A')$ having a dual-digenic basis. Dual-digenicity is a strong property, and it will place rigid equations on γ. Intuitively, we should be able to find equations for dual-digenicity in terms of γ_1, γ_5, because these represent β_1^*, β_5^* respectively (up to sign), and in a dual-digenic basis these determine almost the entire structure of the ring. The equations that follow can be interpreted as conditions on the bases of $\tilde{S}$ and $S/\mathbb{Z}$, tied together by the map $\tilde{S} \to S/\mathbb{Z} : \beta \mapsto 8\,Disc(R) \cdot \beta^2$ which is represented by ∇F_A, as implied by Theorem 23.

We know from Lemma 5.2.2 and from the proof of Lemma 6.1.4 that:

$$\nabla F_{A'}(y_1e_1 + y_5e_5) = (0, -y_1^2, -y_1y_5, -y_5^2, 0) \tag{6.26}$$

$$\nabla F_{A'}(y) = u \cdot \nabla F_A(\gamma^t y) \cdot \gamma^t \tag{6.27}$$

where $u = \det(\tau) \in \{\pm 1\}$ for shorthand.

Thus, the top equation, which encodes dual-digenicity, is true if and only if:

$$(0, -y_1^2, -y_1y_5, -y_5^2, 0) = u \cdot \nabla F_A(y_1\gamma_1 + y_5\gamma_5) \cdot \gamma^t \tag{6.28}$$

Below, we abuse notation and view the quadratic form ∇F_A as a bilinear map, i.e. $\nabla F_A(x, y) = \frac{1}{2}(\nabla F_A(x + y) - \nabla F_A(x) - \nabla F_A(y))$.

$$\iff \begin{cases} -\gamma^{-1} \cdot e_2 &= u\nabla F_A(\gamma_1)^t \\ -\gamma^{-1} \cdot (e_2 + e_3 + e_4) &= u\nabla F_A(\gamma_1 + \gamma_5)^t \\ -\gamma^{-1} \cdot e_4 &= u\nabla F_A(\gamma_5)^t \end{cases} \tag{6.29}$$

$$\iff \gamma^{-1} = \quad u \begin{pmatrix} - & a & - \\ - & -\nabla F_A(\gamma_1, \gamma_1) & - \\ - & -2\nabla F_A(\gamma_1, \gamma_5) & - \\ - & -\nabla F_A(\gamma_5, \gamma_5) & - \\ - & b & - \end{pmatrix}^t \tag{6.30}$$

for some $a, b \in \mathbb{Z}^5$, or equivalently:

$$\iff u \begin{pmatrix} - & a & - \\ - & -\nabla F_A(\gamma_1, \gamma_1) & - \\ - & -2\nabla F_A(\gamma_1, \gamma_5) & - \\ - & -\nabla F_A(\gamma_5, \gamma_5) & - \\ - & b & - \end{pmatrix} \gamma^t = I_5 \tag{6.31}$$

Let $M_{ij}(x,y) = \begin{pmatrix} - & e_i & - \\ - & -\nabla F_A(x,x) & - \\ - & -2\nabla F_A(x,y) & - \\ - & -\nabla F_A(y,y) & - \\ - & e_j & - \end{pmatrix}$ and let $Q_{ij} = \det M_{ij}$, so that Q_{ij} is a function of x, y. In fact, because $F_A \in \mathbb{Z}[x,y]$, M_{ij} has entries in $\mathbb{Z}[x,y]$ and $Q_{ij} \in \mathbb{Z}[x,y]$ too. These functions will be important in making dual-digenicity explicit. Furthermore, note that Q_{ij} is $GL_2(\mathbb{Z})$-invariant up to sign; this reflects the dual-digenization-preserving action of $GL_2(\mathbb{Z})$, and means that it is a function of $L = \mathbb{Z}\{x, y\}$ (up to sign).

Proposition 6.2.3. *Let $A \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ of non-zero discriminant. Let $x, y \in \mathbb{Z}^5$ be linearly independent, and suppose $L = \mathbb{Z}\{x, y\}$ lies on V_A. Then, L arises from a dual-digenic change of basis if and only if there exists $u = \pm 1$ such that*

$$Q_{ij} = u\, p_{ij} \text{ for all } i, j \tag{6.32}$$

where p_{ij} are the Pluecker coordinates defined in terms of x, y.

Proof. Suppose L arises from a dual-digenic basis. There exists $(\tau, \gamma) \in \Gamma$ such that this basis arises from $(\tau, \gamma) \cdot A$. Let $x = \gamma_1, y = \gamma_5$ and $u = \det(\tau) \in \{\pm 1\}$. From our work above, there exist $a, b \in \mathbb{Z}^5$ such that:

$$u \begin{pmatrix} - & a & - \\ - & -\nabla F_A(x,x) & - \\ - & -2\nabla F_A(x,y) & - \\ - & -\nabla F_A(y,y) & - \\ - & b & - \end{pmatrix} \gamma^t = I_5 \tag{6.33}$$

Since L lies on V_A, $0 = 3\,F_A(sx+ty) = \nabla F_A(sx+ty)\cdot(sx+ty)$ for all $s,t \in \mathbb{C}$, and so the following equations hold for all i,j:

$$M_{ij}(x,y)\,\gamma^t = \begin{pmatrix} x_i & * & * & * & y_i \\ 0 & u & 0 & 0 & 0 \\ 0 & 0 & u & 0 & 0 \\ 0 & 0 & 0 & u & 0 \\ x_j & * & * & * & y_j \end{pmatrix} \tag{6.34}$$

Taking determinants, we get $Q_{ij} = u\,p_{ij}$, which is of the required form.

Proving the converse is more involved. First, we prove that if x,y solve $Q_{ij} = u\,p_{ij}$ for some u, then the vector (p_{ij}) of Pluecker coordinates is primitive. Suppose this is not the case, and take any prime p such that $min\{ord_p(p_{ij})\} = r > 0$. There exists a basis $\{x',y'\}$ of L such that $x' = p^m x'', y' = p^n y''$ with $x'',y'' \in \mathbb{Z}^5, m+n=r$; this is proved inductively based off the simpler claim of Lemma 6.2.4 below. Now, choose i,j such that $ord_p(p_{ij}) = r$. Meanwhile, Q_{ij} is $GL_2(\mathbb{Z})$-invariant (up to sign), so $ord_p(Q_{ij}(x,y)) = ord_p(Q_{ij}(p^m x'', p^n y'')) \geq p^{3(m+n)} = p^{3r}$. But this contradicts $Q_{ij} = u\,p_{ij}$, so (p_{ij}) has to be primitive.

Primitivity of the p_{ij} implies that $\{x,y\}$ extends to a basis of $\mathbb{Z}^5$, or equivalently extends to an element of $GL_5(\mathbb{Z})$, and looking at the inverse of such a matrix, we see there exist $a,b \in \mathbb{Z}^5$ such that:

$$\begin{pmatrix} a\cdot x & a\cdot y \\ b\cdot x & b\cdot y \end{pmatrix} = u\,I_2 \tag{6.35}$$

Similarly, since $Q_{ij} = u\,p_{ij}$, the Q_{ij} are also primitive and the set $\{-\nabla F_A(x,x), -2\nabla F_A(x,y), -\nabla F_A(y,y)\}$ extends to a basis $\{a', -\nabla F_A(x,x), -2\nabla F_A(x,y), -\nabla F_A(y,y), b'\}$ of $\mathbb{Z}^5$.

We can write:

$$a = n_{11}a' + n_{12}b' + \ldots \tag{6.36}$$

$$b = n_{21}a' + n_{22}b' + \ldots \tag{6.37}$$

for some $n_{kl} \in \mathbb{Z}$. Let N be the 2×2 matrix with $N_{ij} = n_{ij}$.

We noted that x,y are orthogonal to the vectors $\{-\nabla F_A(x,x), -2\nabla F_A(x,y), -\nabla F_A(y,y)\}$, from which we see:

$$u\,I_2 = \begin{pmatrix} a\cdot x & a\cdot y \\ b\cdot x & b\cdot y \end{pmatrix} \tag{6.38}$$

$$= N\cdot\begin{pmatrix} a'\cdot x & a'\cdot y \\ b'\cdot x & b'\cdot y \end{pmatrix} \tag{6.39}$$

Hence, $N \in GL_2(\mathbb{Z})$ and so $\{a, -\nabla F_A(x,x), -2\nabla F_A(x,y), -\nabla F_A(y,y), b\}$ is a basis of $\mathbb{Z}^5$. Let $\gamma \in GL_5(\mathbb{Z})$ be given by the following equation:

$$u\begin{pmatrix} - & a & - \\ - & -\nabla F_A(x,x) & - \\ - & -2\nabla F_A(x,y) & - \\ - & -\nabla F_A(y,y) & - \\ - & b & - \end{pmatrix}\gamma^t = I_5 \tag{6.40}$$

Then, the conditions on a, b mean that the first and last rows of γ are necessarily x and y respectively.

Replacing a, b by e_i, e_j and taking determinants, we can see that $u\, Q_{ij}(x, y) \det(\gamma) = p_{ij}(x, y)$. We assumed $Q_{ij}(x, y) = u\, p_{ij}(x, y)$, and not all p_{ij} are zero because $\{x, y\}$ is linearly independent, so $\gamma \in SL_5(\mathbb{Z})$.

From our work before the statement of this proposition, for any $\tau \in GL_4(\mathbb{Z})$ with $\det(\tau) = u$, (τ, γ) gives rise to a dual-digenic change of basis corresponding to $L = \mathbb{Z}\{x, y\}$. □

Lemma 6.2.4. *Let $x, y \in \mathbb{Z}^5$, let $L = \mathbb{Z}\{x, y\}$ with Pluecker coordinates $p_{ij} = p_{ij}(x, y)$. Let p be a prime dividing all the p_{ij}. Then, there exists a basis $\{x', py'\}$ of L, with $x', y' \in \mathbb{Z}^5$.*

Proof. If x or y are already divisible by p, we are done. If not, then let the first entry of x coprime to p be x_i. Choose $t \in \mathbb{Z}$ such that the i-th entry of $z = y + tx$ is divisible by p. For $j \neq i$, $p_{ij}(x, z) = p_{ij}(x, y) \equiv 0 \bmod p$, but also $p_{ij}(x, z) = x_i z_j - x_j z_i \equiv x_i z_j \bmod p$ because $p \mid z_i$ by construction. We chose i so that $p \nmid x_i$, hence $p \mid z_j$, and we are done. □

Let $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$. For $u \in \mathbb{C}$, we define a variety $W_{A,u} = V(I_{A,u}) \subseteq \mathbb{A}^{10}$, where the coordinates of $\mathbb{A}^{10}$ are the Pluecker coordinates p_{ij} and $I_{A,u}$ is the following set of equations:

- The five Pluecker relations: $p_{ij}p_{kl} + p_{jk}p_{il} + p_{ki}p_{jl} = 0$
- The four linear equations from the vanishing of A on a line: $A_i(x, y) = 0$ for all i
- The ten equations from dual-digenicity: $Q_{ij} = u\, p_{ij}$ for $i < j$

These equations are all $SL_2(\mathbb{C})$-invariant, so they are well-defined in terms of affine Pluecker coordinates, and $W_{A,u}$ is well-defined. Also, note that each $W_{A,u}$ is a subvariety of D_6.

Because $\mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ with the action of $GL_4(\mathbb{C}) \times SL_5(\mathbb{C})$ is a prehomogeneous vector space, the varieties $W_{A,u}$ are all closely related:

Proposition 6.2.5. *Let $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$ be non-degenerate, and $(\tau, \gamma) \in GL_4(\mathbb{C}) \times SL_5(\mathbb{C})$. Let $A' = (\tau, \gamma) \cdot A$. The action of $SL_5(\mathbb{C})$ on $\mathbb{A}^5$ induces an action on Pluecker coordinates, which we view as an action on $\mathbb{A}^{10}$. Then, with this action:*

$$W_{A,u} = \gamma^t \cdot W_{A',(\det \tau)^3 u} \tag{6.41}$$

Furthermore, for $\lambda \in \mathbb{C}$, $\lambda \cdot W_{A,u} = W_{A,\lambda^2 u}$. Hence, the $W_{A,u}$ are all isomorphic.

Proof. The image of the Pluecker embedding in $\mathbb{A}^{10}$ is invariant under the action of $SL_5(\mathbb{C})$, because this group takes lines to lines. We also argued in Lemma 6.2.2 that $\gamma^t \cdot D_6(A') = D_6(A)$. All that remains is to study the equations of the form $Q_{ij} = u\, p_{ij}$.

Because Q_{ij} depends on the alternating matrix in question, we shall write these functions as $Q_{ij,A}$ and $Q_{ij,A'}$.

Let $(p_{ij}) \in W_{A',(\det\tau)^3u}$, represented by $x, y \in \mathbb{C}^5$. We note the following:

$$Q_{ij,A'}(x,y) = \det\begin{pmatrix} - & e_i & - \\ - & -\nabla F_{A'}(x,x) & - \\ - & -2\nabla F_{A'}(x,y) & - \\ - & -\nabla F_{A'}(y,y) & - \\ - & e_j & - \end{pmatrix} \tag{6.42}$$

$$= \det\begin{pmatrix} - & e_i & - \\ - & -\det(\tau)\nabla F_A(\gamma^t x, \gamma^t x)\gamma^t & - \\ - & -2\det(\tau)\nabla F_A(\gamma^t x, \gamma^t y)\gamma^t & - \\ - & -\det(\tau)\nabla F_A(\gamma^t y, \gamma^t y)\gamma^t & - \\ - & e_j & - \end{pmatrix} \tag{6.43}$$

$$= \det(\tau)^3 \det\begin{pmatrix} - & e_i(\gamma^t)^{-1} & - \\ - & -\nabla F_A(\gamma^t x, \gamma^t x) & - \\ - & -2\nabla F_A(\gamma^t x, \gamma^t y) & - \\ - & -\nabla F_A(\gamma^t y, \gamma^t y) & - \\ - & e_j(\gamma^t)^{-1} & - \end{pmatrix} \tag{6.44}$$

$$= \det(\tau)^3 \sum_{k,l} m_{ki} m_{lj} Q_{kl,A}(\gamma^t x, \gamma^t y) \tag{6.45}$$

where $\gamma^{-1} = (m_{ij})_{ij}$. Hence:

$$\det(\tau)^3(\gamma^{-1})^t(Q_{kl,A}(\gamma^t x, \gamma^t y))_{kl}\gamma^{-1} = (Q_{ij,A'}(x,y))_{ij} \tag{6.46}$$

$$= \det(\tau)^3 u \cdot (p_{ij}(x,y))_{ij} \tag{6.47}$$

where we use that $(p_{ij}) \in W_{A',(\det\tau)^3u}$.

If $\gamma^t(p_{ij}(x,y))_{ij}\gamma = (p_{ij}(\gamma^t x, \gamma^t y))_{ij}$, then we'll be done.

$$p_{ij}(\gamma^t x, \gamma^t y) = \sum_{k,l}(\gamma_{ki}x_k \cdot \gamma_{lj}y_l - \gamma_{lj}x_l \cdot \gamma_{ki}y_k) \tag{6.48}$$

$$= \sum_{k,l} \gamma_{ki}\gamma_{lj} p_{kl}(x,y) \tag{6.49}$$

This is precisely the equality that we need.

The assertion $\lambda \cdot W_{A,u} = W_{A,\lambda^2 u}$ is true because $Q_{ij,A}(\lambda x, y) = \lambda^3 Q_{ij,A}(x,y)$ and $p_{ij}(\lambda x, y) = \lambda\, p_{ij}(x,y)$.

To see that all the $W_{A,u}$ are isomorphic, we can use the prehomogeneity of the space and the first relation to see that $W_{A,u} \simeq W_{A',t}$ for any nondegenerate A' for some t, and then use the second property to see that $W_{A',t} \simeq W_{A',s}$ for any $s \in \mathbb{C}$. □

We can say the following about the variety $W_{A,u}$, though we postpone the proof until later in Proposition 6.3.1.

Proposition 6.2.6. *Let $f(x,y) = x^5 + y^5$. Then $W_{\Phi(f),u} \backslash \{0\}$ is a 2-dimensional variety, cut out by the following equations:*

- *The five Pluecker relations:* $p_{ij}p_{kl} + p_{jk}p_{il} + p_{ki}p_{jl} = 0$
- *The four linear equations from the vanishing of* $\Phi(f)$ *on a line:* $\Phi(f)_i(x, y) = 0$ *for all* i

$$\begin{aligned} p_{14} - p_{23} &= 0 && \textit{(6.50)} \\ -p_{45} - p_{13} &= 0 && \textit{(6.51)} \\ p_{12} + p_{35} &= 0 && \textit{(6.52)} \\ -p_{25} - p_{34} &= 0 && \textit{(6.53)} \end{aligned}$$

- *The ten equations from dual-digenicity reduce to one equation:*

$$p_{15}^2 - 11p_{15}p_{24} - p_{24}^2 = u \tag{6.54}$$

Corollary 6.2.7. *For any nondegenerate* $A \in \mathbb{C}^4 \otimes \wedge^2\mathbb{C}^5$*,* $W_{A,u}\backslash\{0\} \subseteq \mathbb{A}^{10}$ *is a 2-dimensional variety, cut out by the following equations:*

- *The five Pluecker relations:* $p_{ij}p_{kl} + p_{jk}p_{il} + p_{ki}p_{jl} = 0$
- *The four linear equations from the vanishing of* A *on a line:* $A_i(x, y) = 0$ *for all* i
- *The ten equations from dual-digenicity reduce to one equation:*

$$q_A((p_{ij})_{ij}) = u \tag{6.55}$$

, where q_A *is quadratic.*

Proof. Follows from Proposition 6.2.5 and the above proposition. □

In the meantime, we prove how $W_{A,u}$ relates to counts of classes of binary quintics.

Corollary 6.2.8. *Let* $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ *of non-zero discriminant, with associated map* $\phi : \wedge^2\widetilde{S(A)} \to \widetilde{R(A)}$*. Then:*

$$\left\{ \begin{array}{l} \textit{Dual-digenizations of } S(A) \\ \textit{with } \phi(\beta_1^*, \beta_5^*) = 0 \end{array} \right\} \leftrightarrow^{\textit{1-1}} \left\{ \begin{array}{l} \textit{Non-zero points of} \\ W_{A,1}(\mathbb{Z}) \cup W_{A,-1}(\mathbb{Z}) \end{array} \right\} / \{\pm 1\} \tag{6.56}$$

where ± 1 *act as scalars on* $W_{A,u} \subseteq \mathbb{A}^{10}$*.*

Proof. By Proposition 6.2.3, a dual-digenization with $\phi(\beta_1^*, \beta_5^*) = 0$ gives rise to a point of $W_{A,1}(\mathbb{Z}) \cup W_{A,-1}(\mathbb{Z})$. This corresponds to a genuine projective line, so the resulting point (p_{ij}) is non-zero. However, this point is only well-defined up to sign, because changing basis of $\mathbb{Z}\{x, y\}$ by $\gamma \in GL_2(\mathbb{Z})$ multiplies the Pluecker coordinates by $\det(\gamma)$.

Projective Pluecker coordinates $(p_{ij}) \in \mathbb{P}^9$ determine a unique projective line, provided the Pluecker relations are satisfied. Hence, affine Pluecker coordinates determine a line up to multiplication by scalars. Thus, by Lemma 6.1.1, distinct dual-digenizations give rise to distinct points of $W_{A,1}(\mathbb{Z}) \cup W_{A,-1}(\mathbb{Z})$, even up to sign.

Conversely, let $(p_{ij}) \in W_{A,1}(\mathbb{Z}) \cup W_{A,-1}(\mathbb{Z})$, not all p_{ij} zero. By Lemma 6.2.9 below, there exist $x, y \in \mathbb{Z}^5$ such that $p_{ij} = p_{ij}(x, y)$. By definition of $W_{A,u}$, we know that A vanishes on $L = \mathbb{Z}\{x, y\}$, so by Lemma 5.2.3 we know L lies on V_A. Hence, by Proposition 6.2.3, the point (p_{ij}) comes from a dual-digenization of $S(A)$, and the condition $\phi(\beta_1^*, \beta_5^*) = 0$ is already baked into the definition of $W_{A,u}$. □

Lemma 6.2.9. *Let $p_{ij} \in \mathbb{Z}$ for $i < j$, not all zero, satisfying the Pluecker relations. Then there exist $x, y \in \mathbb{Z}^5$ such that $p_{ij} = p_{ij}(x, y)$.*

Proof. We shall start with a rational basis $\{w, z\}$ of the line with Pluecker coordinates (p_{ij}) and refine it into an integral basis. Suppose $p_{kl} \neq 0$. Let $w_k = 1, w_l = 0, z_k = 0, z_l = p_{kl}$. This forces the following choices upon us: $z_j = p_{kj}, w_i = p_{il}/p_{kl}$ for $j \neq k, i \neq l$. (Here, we use the notation $p_{ij} = -p_{ji}$ if $i > j$.)

We need to check that $\{w, z\}$ give the right values for the other p_{ij}. Take p_{ij} with $i \neq k, j \neq l$. We expand this as:

$$\begin{aligned} p_{ij}(w, z) &= w_i z_j - w_j z_i && (6.57) \\ &= \frac{1}{p_{kl}}(p_{il}p_{kj} - p_{jl}p_{ki}) && (6.58) \\ &= p_{ij} && (6.59) \end{aligned}$$

by one of the Pluecker relations. So, $\{w, z\}$ do the job rationally.

Suppose $\{w, z\}$ are not integral at p. We will act by an element of $SL_2(\mathbb{Z}[\frac{1}{p}])$ to make them integral at p. Performing this procedure in turn for each bad prime will do the job. First, take $r > 0$ such that $w' = p^r w, z' = p^r z \in \mathbb{Z}^5$. Then, $p_{ij}(w', z') = p^{2r} p_{ij}$ for all i, j. By repeatedly applying the proof of Lemma 6.2.4, we can find an element of $SL_2(\mathbb{Z})$ transforming (w', z') to (x', y'), such that $x' = p^m x, y' = p^n y$ with $x, y \in \mathbb{Z}^5$ and $m + n = 2r$. Then, $p_{ij}(x, y) = p^{-2r} p_{ij}(x', y') = p^{-2r} p_{ij}(w', z') = p_{ij}$, as required. □

Corollary 6.2.10. *Let $A \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ of non-zero discriminant. The number of $GL_2(\mathbb{Z})$-classes of binary quintic forms f for which $\Phi(f)$ and A are Γ-equivalent is bounded by $\frac{1}{2}(\#W_{A,1}(\mathbb{Z}) + \#W_{A,-1}(\mathbb{Z}) - 2)$.*

Furthermore:

$$\frac{1}{2}(\#W_{A,1}(\mathbb{Z}) + \#W_{A,-1}(\mathbb{Z}) - 2) = \sum_{\{f \, mod \, GL_2(\mathbb{Z}) : \Phi(f) \in \Gamma \cdot A\}} \frac{\#Aut(A)}{\#Aut(f)} \qquad (6.60)$$

In particular, $\#W_{A,u}(\mathbb{Z})$ is finite for $u = \pm 1$.

Proof. Recall the statement of Theorem 26:

There is a bijection between the following two sets:

$$GL_2(\mathbb{Z})\backslash(Sym^5\mathbb{Z}^2)^* \leftrightarrow \left\{ \begin{array}{l} (R,S), \text{R basis-free} \\ \text{S dual-digenic with a} \\ \text{fixed dual-digenization} \\ \text{and } \phi(\beta_1^*, \beta_5^*) = 0 \end{array} \right\} / \sim \tag{6.61}$$

given by $f \mapsto$ the class of (R_f, S_f), where the $\sim$ denotes isomorphism of R and dual-digenic isomorphism of S, and where ϕ is the fundamental alternating map $\wedge^2\tilde{S} \to \tilde{R}$.

For a moment, we ignore the quotient by dual-digenic isomorphism and focus on the subset of objects on the right for which $(R,S) = (R(A), S(A))$. By Corollary 6.2.8, this set maps bijectively to the non-zero points of $W_{A,1}(\mathbb{Z}) \cup W_{A,-1}(\mathbb{Z})$, quotiented by the action of $\{\pm 1\}$. This set is of size $\frac{1}{2}(\#W_{A,1}(\mathbb{Z}) + \#W_{A,-1}(\mathbb{Z}) - 2)$.

When we reintroduce the quotient by dual-digenic isomorphism, it can happen that two distinct dual-digenizations are actually isomorphic, so we overcount slightly, leading to the desired upper bound.

To figure out how severe this overcount is, and to obtain the formula in the statement of the result, we need to count how many dual-digenizations of S correspond to a given class of forms. It is enough to focus on a single representative form f, because if a dual-digenization corresponds to the class of f then there is a dual-digenic basis in this dual-digenization coming from f.

Suppose $\Phi(f)$ gives rise to (R,S) in two pairs of bases; in other words, the fundamental map $\phi : \wedge^2\tilde{S} \to \tilde{R}$ is given by $\Phi(f)$ in two pairs of bases of (R,S). Changing between these two pairs of bases is represented by the action of some $(\tau, \gamma) \in \Gamma$, so $\Phi(f) = (\tau,\gamma)\cdot\Phi(f)$ and $(\tau,\gamma) \in Aut(\Phi(f))$. Since $\Phi(f) \in \Gamma \cdot A$, $\#Aut(\Phi(f)) = \#Aut(A)$. Conversely, any automorphism of $\Phi(f)$ will take one pair of bases of (R,S) corresponding to f to another. These two operations are clearly inverse to one another.

However, how many of these automorphisms are giving genuinely new dual-digenizations?

Suppose that $(\tau_1,\gamma_1), (\tau_2,\gamma_2) \in Aut(\Phi(f))$ give rise to the same dual-digenization. There is precisely a $GL_2(\mathbb{Z})$-worth of dual-digenic bases within a fixed dual-digenization, so there exists $\gamma' \in GL_2(\mathbb{Z})$ relating the respective (β_1^*, β_5^*) of the two dual-digenic bases. Recall from Lemma 5.1.4 that $(8\,Disc(R))^2 \cdot Tr((u\beta_5^* - v\beta_1^*)^5) = -10f(u,v)$. But if the two pairs of (β_1^*, β_5^*) are both associated to f, this tells us that γ' corresponds to an element $\gamma \in Aut(f)$, where:

$$\gamma = M\gamma' M^{-1} \tag{6.62}$$

$$M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{6.63}$$

In fact, the (τ_i, γ_i) are related by $(1,h)\cdot\sigma(\gamma)$ for a unique $h \in H$: dual-digenicity of the bases and the relation between (β_1^*, β_5^*) being by γ', implies that the GL_5 component of $(\tau_1\tau_2^{-1}, \gamma_1\gamma_2^{-1})$ is $h' \cdot \rho(\gamma)$ for some $h' \in H$.

$(\tau_1\tau_2^{-1}, \gamma_1\gamma_2^{-1}) \in Aut(\Phi(f))$ and also $(1,h)\cdot\sigma(\gamma) \in Aut(\Phi(f))$ for some well-chosen h, by Theorem 20. Furthermore, h is easily seen to be unique. Taking their quotient, we get an element of the form $(g, h'') \in Aut(\Phi(f))$. The element $h'' \in H$ does not affect the outside rows and columns, so g has to fix these, hence it is trivial. Then, h'' is also seen to be trivial, else it ruins the middle 3×3 block of $\Phi(f)$. Hence, the (τ_i, γ_i) differ by $(1,h)\cdot\sigma(\gamma)$ for a unique $h \in H$.

On the other hand, if $\gamma \in Aut(f)$ and $(\tau_1, \gamma_1) \in Aut(\Phi(f))$, then there exists $h \in H$ such that $(1,h)\cdot\sigma(\gamma)\cdot(\tau_1,\gamma_1) \in Aut(\Phi(f))$, and this will give rise to a dual-digenic basis corresponding to f in the same dual-digenization as the basis coming from (τ_1, γ_1). Hence, the two operations concerning dual-digenic bases coming from f in the same dual-digenization are inverse to each other.

In summary, there are $\#Aut(\Phi(f)) = \#Aut(A)$ dual-digenic bases which arise from f, and within each dual-digenization that appears here there are $\#Aut(f)$ of these bases. The formula in the statement of the result follows.

Finiteness of $\#W_{A,u}(\mathbb{Z})$ follows from the finiteness of $Aut(A)$, and the fact that there are finitely many classes of binary quintic forms of bounded discriminant, as proved by Birch & Merriman. □

In fact, $\#W_{A,u}(\mathbb{Z})$ is uniformly bounded across all $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5, u \in \{\pm 1\}$. The proof of this relies on the following result of Evertse-Gyory:

Theorem 27 (Evertse-Gyory)**.** *Let K be a finite etale $\mathbb{Q}$-algebra with $[K:\mathbb{Q}] =: n \geq 3$, and R an order of K. Then there are at most 2^{5n^2} $GL_2(\mathbb{Z})$-classes of binary n-ic forms $f \in (Sym^n\mathbb{Z}^2)^*$ such that $R \simeq R_f$.*

Corollary 6.2.11. *$\#W_{A,u}(\mathbb{Z})$ is uniformly bounded across all $A \in \mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5, u \in \{\pm 1\}$.*

Proof. For each class of binary n-ic forms, choose a representative f and denote the class by $\bar{f}$. By Corollary 6.2.10, Theorem 27 and because $Aut(A) \leqslant Aut_{\mathbb{C}}(A) = S_5$:

$$\begin{aligned}
\#W_{A,u}(\mathbb{Z}) - 1 &\leq 2\cdot\#Aut(A)\cdot\#\{\bar{f} : \Phi(f) \in \Gamma\cdot A\} && (6.64)\\
&\leq 2\cdot\#S_5\cdot\#\{\bar{f} : (R_f, S_f) \simeq (R(A), S(A))\} && (6.65)\\
&\leq 240\cdot\#\{\bar{f} : R_f \simeq R(A)\} && (6.66)\\
&\leq 240\cdot 2^{125} && (6.67)
\end{aligned}$$

□

Conversely, a tighter bound on $\#W_{A,u}(\mathbb{Z})$, together with information on how many sextic resolvents a given quintic ring can have, would give an improvement of Evertse & Gyory's result in the case $n = 5$.

6.3 Examples

Proposition 6.3.1. *Let $f(x,y) = ax^5 + by^5$ with $ab \neq 0$. Then $W_{\Phi(f),u}\backslash\{0\} \subseteq \mathbb{A}^{10}$ is itself a variety and is cut out by the following equations:*

- *The five Pluecker relations:* $p_{ij}p_{kl} + p_{jk}p_{il} + p_{ki}p_{jl} = 0$
- *The four linear equations from the vanishing of* $\Phi(f)$ *on a line:* $\Phi(f)_i(x, y) = 0$ *for all* i

$$p_{14} - a\,p_{23} = 0 \tag{6.68}$$

$$-p_{45} - p_{13} = 0 \tag{6.69}$$

$$p_{12} + p_{35} = 0 \tag{6.70}$$

$$-p_{25} - b\,p_{34} = 0 \tag{6.71}$$

- *The ten equations from dual-digenicity reduce to one equation:*

$$p_{15}^2 - 11ab\,p_{15}p_{24} - a^2b^2\,p_{24}^2 = u \tag{6.72}$$

Furthermore, $W_{\Phi(f),u}\backslash\{0\}$ *is a 2-dimensional variety.*

Proof. Modulo the four linear equations above, $Q_{ij} \equiv p_{ij}(p_{15}^2 - 11ab\,p_{15}p_{24} - a^2b^2\,p_{24}^2)$. This can be seen using MAGMA, or your favourite computer algebra package. Thus, upon recalling that some $p_{kl} \neq 0$, the ten equations $Q_{ij} = u\,p_{ij}$ reduce to the single equation above.

From Dolgachev's work, $D_6 \subseteq \mathbb{P}^9$ is an irreducible 2-dimensional projective variety. To obtain $W_{\Phi(f),u}\backslash\{0\}$, we take the cone over D_6 in $\mathbb{A}^{10}$ and intersect with an additional inhomogeneous equation. Thus, the intersection is an affine variety of dimension at most 2. In fact, MAGMA tells us that this variety is of dimension precisely 2. □

Carrying out a brute force search for integral points (p_{ij}) on the varieties $W_{\Phi(f),1}$ and $W_{\Phi(f),-1}$ for $f = x^5 + y^5$, with $|p_{ij}| \leq 10$, leads to only the points $\pm P_1 \in W_{\Phi(f),1}$ and $\pm P_2 \in W_{\Phi(f),-1}$, where:

- P_1 has $p_{15} = 1$ and $p_{ij} = 0$ for all other i, j
- P_2 has $p_{24} = 1$ and $p_{ij} = 0$ for all other i, j

The point P_1 corresponds to the standard dual-digenization of S_f, and P_2 corresponds to a new dual-digenization, which in fact also comes from f; i.e. there is a dual-digenic isomorphism taking one of these dual-digenizations to the other. The proof of Corollary 6.2.10 says that $\pm P_1$ and $\pm P_2$ give rise to different cosets of $Aut(\Phi(f))/Aut(f)$, where we have abused notation and consider $Aut(f) \subseteq Aut(\Phi(f))$ via σ. Indeed, P_1 gives rise to the trivial coset and P_2 gives rise to the following $(\tau, \gamma) \in Aut(\Phi(f))$, which does not arise from

$Aut(f)$ via σ:

$$\tau = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \end{pmatrix} \tag{6.73}$$

$$\gamma = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{6.74}$$

Recall from Corollary 6.2.7 that the ten equations from dual-digenicity always reduce to a single inhomogeneous quadratic equation $q_A((p_{ij})_{ij}) = u$. To understand the general behaviour of $W_{A,u}$, it is instructive to compute q_A in more cases.

Lemma 6.3.2. *Let $f(x,y) = x^5 - xy^4$. Then $W_{\Phi(f),u} \backslash \{0\} \subseteq \mathbb{A}^{10}$ is cut out by the following equations:*

- *The five Pluecker relations: $p_{ij}p_{kl} + p_{jk}p_{il} + p_{ki}p_{jl} = 0$*
- *The four linear equations from the vanishing of $\Phi(f)$ on a line: $\Phi(f)_i(x,y) = 0$ for all i*

$$p_{14} - p_{23} = 0 \tag{6.75}$$
$$-p_{45} - p_{13} = 0 \tag{6.76}$$
$$p_{12} + p_{35} + p_{34} = 0 \tag{6.77}$$
$$-p_{25} = 0 \tag{6.78}$$

- *The inhomogeneous equation $q_{\Phi(f)}((p_{ij})_{ij}) = u$, where*

$$q_{\Phi(f)} = p_{15}^2 + 4p_{12}^2 - p_{35}^2 - 4p_{23}^2 \tag{6.79}$$

Lemma 6.3.3. *Let $f(x,y) = x^5 + 3xy^4 - xy^4 - 4y^5$. Then $W_{\Phi(f),u} \backslash \{0\} \subseteq \mathbb{A}^{10}$ is cut out by the following equations:*

- *The five Pluecker relations: $p_{ij}p_{kl} + p_{jk}p_{il} + p_{ki}p_{jl} = 0$*
- *The four linear equations from the vanishing of $\Phi(f)$ on a line: $\Phi(f)_i(x,y) = 0$ for all i*

$$p_{14} - p_{23} = 0 \tag{6.80}$$
$$-p_{45} - p_{13} - 3p_{23} = 0 \tag{6.81}$$
$$p_{12} + p_{35} + p_{34} = 0 \tag{6.82}$$
$$-p_{25} + 4p_{34} = 0 \tag{6.83}$$

- *The inhomogeneous equation* $q_{\Phi(f)}((p_{ij})_{ij}) = u$*, where*

$$\begin{aligned} q_{\Phi(f)} = {} & p_{15}^2 + 44p_{15}p_{24} + 3p_{15}p_{23} + 36p_{15}p_{34} - p_{24}^2 - 4p_{24}p_{13} \\ & +4p_{24}p_{23} + 48p_{24}p_{34} - 144p_{24}p_{35} + 36p_{13}p_{23} \qquad \textit{(6.84)} \\ & +3p_{13}p_{35} + 3p_{23}p_{34} + p_{34}p_{35} \qquad \textit{(6.85)} \end{aligned}$$

In a different direction, we give an example below which shows that dual-digenicity of a basis is not sufficient for it to come from a binary quintic form; we also need the condition $\phi(\beta_1^*, \beta_5^*) = 0$:

Lemma 6.3.4. *There exists nondegenerate* (R, S) *with* S *having a dual-digenic basis but without* $\phi(\beta_1^*, \beta_5^*) = 0$*.*

Proof. The necessary equations for a dual-digenic basis are those of the form $Q_{ij} = u\,p_{ij}$ for $u \in \{\pm 1\}$, plus the equations for $L = \mathbb{C}\{x, y\}$ being a line on the Segre cubic V_A; this is the assertion of Proposition 6.2.3. This latter condition is normally implied by $\phi(\beta_1^*, \beta_5^*) = 0$, or equivalently $L \in D_6$, but we are excluding this condition here.

Taking $f(x, y) = x^4y + x^3y^2 + xy^4, \gamma_1 = (0, 1, 0, 1, 1), \gamma_5 = (0, 1, 0, 0, 0)$ leads to a dual-digenic basis, as can be shown by checking by computer that the necessary equations are all satisfied, with $u = 1$.

Indeed, such a γ with these γ_1, γ_5 is given by:

$$(\gamma^{-1})^t = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 1 & -1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \end{pmatrix} \tag{6.86}$$

However, $\Phi(f)(\gamma_1, \gamma_5) \neq 0$. □