2-2020

Arithmetic of Binary Cubic Forms

Gennady Yassiyevich
The Graduate Center, City University of New York

Arithmetic of Binary Cubic Forms

by

Gennady Yassiyevich

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2020

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

Professor Gautam Chinta

Date

Chair of Examining Committee

Professor Ara Basmajian

Date

Executive Officer

Professor Kenneth Kramer
Professor Cormac O'Sullivan
Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Arithmetic of Binary Cubic Forms

by

Gennady Yassiyevich

Advisor: Professor Gautam Chinta

The goal of the thesis is to establish composition laws for binary cubic forms. We will describe both the rational law and the integral law. The rational law of composition is easier to describe. Under certain conditions, which will be stated in the thesis, the integral law of composition will follow from the rational law. The end result is a new way of looking at the law of composition for integral binary cubic forms.

Acknowledgments

This thesis is dedicated to my grandfather.

Contents

Introduction **1**

1 Composition of Binary Quadratic Forms **3**

1.1 The Gauss Composition Law 3

1.2 Rational Quadratic Forms 7

1.3 Relationship Between Integral and Rational Quadratic Forms 12

1.4 Composition of Integral Forms Revisited 15

1.5 Integral Bhargava Cubes 16

1.6 Rational Bhargava Cubes 18

1.7 Composition Laws for Bhargava Cubes 20

2 Binary Cubic Forms **22**

2.1 Integral Binary Cubic Forms 22

2.2 Composition Law for Integral Cubic Forms 25

2.3 Rational Cubic Forms 26

2.4 Proof of Injectivity 27

2.5 Composition of Rational Cubic Forms 32

3 Composition of Rational Binary Cubic Forms **33**

3.1 Introduction 33
3.2 Fundamental Cubic Decomposition 34
3.3 Determination of the Decomposition 35
3.4 Orientation 39
3.5 The Elliptic Map 41
3.6 The Hyperbolic Map 49
3.7 Relationship between Integral and Rational Cubic Forms 50
3.8 Law of Composition for Integral Cubic Forms 54
3.9 The View from High Above 57

4 Binary Cubic Forms of a Squared Discriminant 58

4.1 Introduction 58
4.2 Fundamental Cubic Decomposition Revisited 58
4.3 Law of Composition for Projective Cubic Forms 63
4.4 Further Questions and Generalizations 66

Bibliography 67

Introduction

The first chapter of the thesis is an overview of binary quadratic forms, both with integral and rational coefficients. This chapter is not critical to the thesis but it is will help motivate some of the ideas that are to follow in the thesis. In this chapter we will review the classical Gauss composition law for integral binary quadratic forms. We will then follow up this concept by a composition law for rational binary quadratic forms. The ideas that will be presented in this chapter will parallel what follows ahead. The main result of this chapter is that the natural map $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ is a homomorphism of commutative groups.

The second chapter is devoted to binary cubic forms. In this chapter we will lay the definitions that will be used for the thesis. Since much of this thesis is based on the works of Bhargava [**Bhargava**] it will be necessary for us to review his ideas before we can present any new insights. We develop also some new concepts that will emerge again later in the thesis. The main result of this chapter is that the natural map $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ is an injective map on "*sets*" when D is square-free. The set $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$ has a structure of a group, however it will not be in any way obvious whether $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ has a natural group structure.

The third chapter is the main part of the thesis. The primary concern of this chapter is the study of rational binary cubic forms. The work behind this chapter is inspired

from Slupinksi and Stanton [**Slupinski-Stanton**]. It will be necessary to present their work and their results. Our development is self contained and does not require knowledge of the mathematics that is used by Slupinski and Stanton. It is in this chapter that we show how the Slupinski-Stanton composition law for rational binary cubic forms carries over to the Bhargava composition law for integral binary cubic forms. In this chapter we will equip $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ with a structure of a group. It will be seen that the natural map $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ from Chapter 2 is an embedding of commutative groups. In the end we show how this embedding allows us to reformulate Bhargava's composition law in a new light.

The fourth and final chapter is extra material. It is not required for the main idea of the thesis. From the work that we develop in the third chapter we are able to get some nice consequences to integral binary cubic forms which have a squared discriminant. This is seen as the antipodal case from chapter 3, where the discriminant is square free. In this chapter we classify all such cubic forms whose discriminant is a perfect square and also describe the composition law.

Finally, we will conclude with some potential future questions which can be part of future research and new generalizations. These are natural questions that are not resolved in the thesis and are interesting to pursue in further research.

Chapter 1

Composition of Binary Quadratic Forms

1.1 The Gauss Composition Law

We begin with a brief summary of the classical Gauss composition law and then present Bhargava's modern description of it. This will be helpful in motivating the cubic composition law in the later chapters of this paper.

An "*integral binary quadratic form*" is quite simply a quadratic homogenous polynomial in two indeterminates with integral coefficients, i.e. $f(X,Y) = aX^2 + bXY + cY^2$ where $a, b, c \in \mathbb{Z}$. The space of all such polynomials will be denoted as $\text{sym}^2\mathbb{Z}^2$. This notation suggests that $\text{sym}^2\mathbb{Z}^2$ should rather be the space of polynomials of the form $aX^2 + 2bXY + cY^2$, however it will be our convention in this paper, for the sake of notational simplicity, that $\text{sym}^2\mathbb{Z}^2$ will refer to quadratic forms where the central coefficient can be even or odd.

The "*discriminant*" of $f(X,Y)$ is defined to be the quantity $D = b^2 - 4ac$. Clearly, the only possible values of the discriminant are integers $D \equiv 0, 1 (\text{mod } 4)$. In the later chapters of this paper we will work with discriminants that are square free, and so $D \equiv 1 (\text{mod } 4)$. Therefore, we adopt the convention in this paper that D will be square free unless otherwise stated.

We denote by $\mathrm{SL}(2,\mathbb{Z})$ the group of all 2×2 integer matrices with determinant $= 1$. If,

$$g = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

then we can act by g on the form $P(X,Y)$ by defining

$$(P^g)(X,Y) = P(rX + sY, tX + uY)$$

This defines a right action of the group $\mathrm{SL}(2,\mathbb{Z})$ on the space $\mathrm{sym}^2\mathbb{Z}^2$. Furthermore, if P has discriminant D then a straightforward calculation will show that P^g also has discriminant D.

We say a quadratic form $f(X,Y) = aX^2 + bXY + cY^2$ is "*primitive*" if the gcd of its coefficients is the unit, i.e. $\gcd(a,b,c) = 1$. It is an easy exercise to show that if $P \in \mathrm{sym}^2\mathbb{Z}^2$ is primitive and $g \in \mathrm{SL}(2,\mathbb{Z})$ then P^g is also primitive.

From now on fix a discriminant D. Consider all primitive quadratic forms which have D as their discriminant. The action of the group on $\mathrm{sym}^2\mathbb{Z}^2$ partitions all primitive forms of discriminant D into equivalence classes under the action of $\mathrm{SL}(2,\mathbb{Z})$. We denote the set of all of these equivalence classes by $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$. We will use the notation $[P]$ to denote the equivalence class of P. It turns out that there are only finitely many such classes and furthermore Gauss defined a group law on these equivalence classes now referred to as "*Gauss composition*" [**Cox**, **§3.A**], see also [**Bouyer**, **Def. 2.8.**].

Definition 1.1.1. Let $P(X,Y)$ and $Q(X,Y)$ be two primitive forms of discriminant D (the D does not need to be square free). Their "*composition*" is defined to be a third quadratic form $R(X,Y)$ such that:

$$P(X_1,Y_1)Q(X_2,Y_2) = R(X_3,Y_3)$$

with

$$X_3 = a_1X_1X_2 + b_1X_1Y_2 + c_1X_2Y_1 + d_1X_2Y_2$$
$$Y_3 = a_2X_1X_2 + b_2X_1Y_2 + c_2X_2Y_1 + d_2X_2Y_2$$

where $a_i, b_i, c_i, d_i \in \mathbb{Z}$ and the initial conditions:

$$\begin{cases} a_1b_2 - a_2b_1 &= P(1,0) \\ a_1c_2 - a_2c_1 &= Q(1,0) \end{cases}$$

are satisfied.

In order to make this definition plausible the following Proposition is necessary.

Proposition 1.1.2. *The above definition is well-defined on equivalence classes of* $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$. *That is to say, if P and Q are representatives for classes then the R, as in the definition, is unique up to* $\mathrm{SL}(2,\mathbb{Z})$*-equivalence. Furthermore, the "composition" of P and Q is well-defined regardless of what representatives are chosen. Thus, we have a well-defined binary operation, called* $+$,

$$+ : \mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \times \mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$$

Proof. This is a classical result of arithmetic [**Cox**, **Prop. 3.8.**]. ■

The law of composition described in **Def. 1.1.1.** and **Prop. 1.1.2.** will be referred to as "*Gauss composition*".

What is remarkable is that Gauss composition is a group composition law.

Theorem 1.1.3. With $+$ defined as in **Def. 1.1.1.** and **Prop. 1.1.2.** the set $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ acquires a structure of a commutative group.

Proof. Again, this is a classic result of arithmetic [**Cox**, **Thm. 3.9.**]. ■

One of the disadvantages of this law of composition is that it is extremely difficult to compute the composition. The resulting new form in **Def. 1.1.1.** is not given explicitly.

Subsequently, it has been recognized that the group law for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ is related to the multiplication of fractional ideals of the ring of integers in the number field $\mathbb{Q}(\sqrt{D})$. Let us first define the ring and ideals we will be working with.

Definition 1.1.4. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field (we are assuming D is square free) and denote by $\mathbb{Z}_K$ the ring of integers of K. If I and J are non-zero fractional ideals, i.e. rank two $\mathbb{Z}$-submodules of K, then we say $I \sim J$ if and only if there exists a non-zero $\alpha \in K$ such that $I = \alpha J$. The set of equivalence classes of these fractional ideals is denoted by $\mathrm{Cl}(\mathbb{Z}_K)$ and referred to as the "*class group*".

We will have to modify the above definition slightly. Essentially we are trying to construct a group arising from the non-zero ideals of $\mathbb{Z}_K$ which will be isomorphic to the group $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$. Here is the modified definition.

Definition 1.1.5. If I and J are non-zero fractional ideals, then we say $I \approx J$ if and only if there exists a non-zero $\alpha \in K$ such that $I = \alpha J$ and $N_{K/\mathbb{Q}}(\alpha) > 0$. The set of equivalence classes of these fractional ideals is denoted by $\mathrm{Cl}^+(\mathbb{Z}_K)$ and referred to as the "*narrow class group*".

In the case when $D < 0$ one has $\mathrm{Cl}(\mathbb{Z}_K) = \mathrm{Cl}^+(\mathbb{Z}_K)$ since the norm of any non-zero element of K will be automatically positive. It is precisely in the real case, $D > 0$, where we have to modify the class group.

We now present the isomorphism between $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ and $\mathrm{Cl}^+(\mathbb{Z}_K)$.

Theorem. 1.1.6. *There is an isomorphism*,

$$\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \to \mathrm{Cl}^+(\mathbb{Z}_K)$$

given by,

$$[aX^2 + bXY + cY^2] \mapsto \alpha \left\langle a, \frac{-b + \sqrt{D}}{2} \right\rangle$$

where $\langle u, v\rangle$ denotes the ideal generated by u and v,

and $\alpha \in K$ is chosen so that $N_{K/\mathbb{Q}}(\alpha)a > 0$.

Proof. This is a well-known isomorphism in algebraic number theory [**Cohen**, **§5.2**].

■

This concludes the brief overview of Gauss composition law. In the next section we introduce rational binary quadratic forms. We will give the law of composition for rational binary quadratic forms and show how it relates to the law of composition given in **Thm. 1.3.3.**.

1.2 Rational Quadratic Forms

One can also consider binary rational quadratic forms $P(X, Y) = aX^2 + bXY + cY^2$ where $a, b, c \in \mathbb{Q}$. The space of all such rational quadratic forms will be denoted by $\mathrm{sym}^2\mathbb{Q}^2$. Unlike integral quadratic forms, all of these rational quadratic forms are automatically primitive (unless all coefficients are zero) since the gcd of any two non-zero rational numbers is a unit. We can act on this space by the group $\mathrm{SL}(2, \mathbb{Q})$. Just as with integral forms we can fix a discriminant D and partition all forms into $\mathrm{SL}(2, \mathbb{Q})$ equivalence classes of this fixed discriminant D. The set of all such equivalence classes will be denoted by $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$.

Unlike the integral case where $D \equiv 0, 1 (\bmod 4)$, in the rational case D can be any rational number. Indeed, $X^2 - \frac{1}{4}DY^2$ is a rational form with discriminant equal to D. However, for the purposes of this paper we will assume in this section that D is an integer which is not a perfect rational square.

Proposition 1.2.1. *Let $f(X, Y)$ be a rational quadratic form of discriminant D. There exists a quadratic form, of the type $aX^2 + bY^2$, such that $f(X, Y)$ is $\mathrm{SL}(2, \mathbb{Q})$-equivalent to*

aX^2+bY^2. Furthermore, $-4ab = D$. We call the quadratic form aX^2+bY^2 a "sum-of-squares representative".

Proof. If we write $f(X,Y) = pX^2 + qXY + rY^2$ then we can act on $f(X,Y)$ by the matrix,

$$g = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Q})$$

where u is an arbitrary rational number. It is then clear that if we compute $(f^g)(X,Y)$ then we can configure u so that the central coefficient of XY becomes zero. This new resulting quadratic form will be of the "*sum-of-squares*" type $aX^2 + bY^2$. Furthermore, from the fact that the discriminant is invariant it is clear that $D = -4ab$. ■

In §1 we gave $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ a law of composition which defined a commutative group structure. In this section we give the analogue for the law of composition for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ which will give a new group structure.

To motivate the group structure for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ let $P(X_1,Y_1) = a_1X_1^2 + b_1Y_1^2$ and $Q(X_2,Y_2) = a_2X_2^2 + b_2Y_2^2$ be two rational sum-of-squares forms of the same discriminant D. Thus, $-4a_1b_1 = D$ and $-4a_2b_2 = D$. Their product will be,

$$P(X_1,Y_1)Q(X_2,Y_2) = (a_1a_2)(X_1X_2)^2 + (b_1b_2)(Y_1Y_2)^2 + (a_1b_2)(X_1Y_2)^2 + (a_2b_1)(X_2Y_1)^2$$

Take the first two terms, and complete the square,

$$(a_1a_2)(X_1X_2)^2 + (b_1b_2)(Y_1Y_2)^2 = (a_1a_2)(X_1X_2 + \tfrac{D}{4a_1a_2}Y_1Y_2)^2 - \tfrac{D}{2}X_1X_2Y_1Y_2$$

Thus, we obtain from here that,

$$P(X_1,Y_1)Q(X_2,Y_2) = (a_1a_2)(X_1X_2 + \tfrac{D}{4a_1a_2}Y_1Y_2)^2 - \tfrac{D}{4a_1a_2}(a_1X_1Y_2 + a_2X_2Y_1)^2$$

We see that, $P(X_1,Y_1)Q(X_2,Y_2) = R(X_3,Y_3)$ where $R(X,Y) = a_1a_2X^2 - \frac{D}{4a_1a_2}Y^2$ and where,

$$\begin{cases} X_3 &= X_1X_2 + \frac{D}{4a_1a_2}Y_1Y_2 \\ Y_3 &= a_1X_1Y_2 + a_2X_2Y_1 \end{cases}$$

The form $R(X,Y)$ now satisfies the conditions of **Def. 1.1.1.**. Of course in **Def. 1.1.1.** the law of composition was defined over integral forms, here we are working with rational forms. Nonetheless we can proceed by analogy and use this observation to define the composition of rational quadratic forms in this manner.

Theorem 1.2.2. *The set of classes* $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ *is a group with composition given by,*

$$[a_1X^2 + b_1Y^2] + [a_2X^2 + b_2Y^2] = [a_3X^2 + b_3Y^2]$$

where $a_3 = a_1a_2$ *and* $-4a_3b_3 = D$.

Proof. According to **Prop. 1.2.1.** if $[P]$ is an equivalence class in $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ then it can be represented as a sum-of-squares representative. Thus, it is sufficient to define the law of composition on the sum-of-squares representatives. It is also easy to see that the identity form is $X^2 - \frac{1}{4}DY^2$ and that every rational form has an inverse. Thus, this law of composition does define a group structure for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$. The one issue which is not clear is whether this map is well-defined. To see this, one has that $[a_1X^2 + b_1Y^2] = [a_1'X^2 + b_1'Y^2]$ if and only if $a_1' = a_1(u^2 - Dv^2)$ for some $u, v \in \mathbb{Q}$ (see **Prop. 1.2.3.** and its proof for the details). With this result the verification that the map is well-defined is now a straightforward computation.

■

Observe that $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ has the same identity element as does $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ when $D \equiv 0(\mathrm{mod}4)$. This is not surprising since the law of composition for rational forms was defined in a similar manner as integral forms.

As we remarked before $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ has finitely many classes, whereas $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ has infinitely many classes (as seen in **Prop. 1.2.3.**). Thus, the group $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ is much larger than $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$. However, the group $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ has a much simpler

description of the composition law in comparison with $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$.

Every form of the sum-of-squares type $aX^2 + bY^2$ is essentially determined by a since b is related by $-4ab = D$. However, since $aX^2 + bY^2$ is equivalent under $\mathrm{SL}(2, \mathbb{Q})$ to possibly another sum-of-squares form $cX^2 + dY^2$, we see that a and c, even though different numbers, need to be identified as equivalent in some way. Below is the correct equivalence condition that needs to be placed on the non-zero rational numbers [**Slupinksi-Stanton**, **Prop. 2.8**]. We refine the authors original statement of the proposition to be more suitable for our purposes in this paper.

Proposition 1.2.3. *Denote by $\mathbb{Q}^\times$ the multiplicative group of rational numbers. We also denote by $\mathbb{Q}_D^\times$ the subgroup,*

$$\mathbb{Q}_D^\times = \{q \in \mathbb{Q}^\times \mid q = x^2 - Dy^2 \text{ for } x, y \in \mathbb{Q}\}$$

Construct the map

$$\varphi : \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D) \to \mathbb{Q}^\times/\mathbb{Q}_D^\times$$

defined by the rule

$$\varphi([aX^2 + bY^2]) = \overline{a}$$

This map is well-defined on the sum-of-squares representatives for P and is an isomorphism of groups.

Proof. The fact that $\mathbb{Q}_D^\times$ is a subgroup is an easy argument. One needs to observe the identity

$$(x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2.$$

Let $aX^2 + bY^2$ be a representative for P with $-4ab = D$. And pick some

$$g = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Q})$$

If we act by g on P such that P^g is a sum-of-squares, say $P^g = cX^2 + dY^2$ then,

$$P^g = (as^2 + bu^2)X^2 + (at^2 + bv^2)Y^2$$

Thus, $c = as^2 + bu^2$ and $d = at^2 + bv^2$.

We need to show that $\overline{a} = \overline{c}$. It is clear that,

$$c = a\left(s^2 + \tfrac{b}{a}u^2\right) = a\left(s^2 - \tfrac{D}{4a^2}u^2\right) = a\left(x^2 - Dy^2\right)$$

where $x = s$ and $y = \frac{u}{2a}$, so a and c differ by a multiple of $\mathbb{Q}_D^\times$. Hence, we have shown that, $\overline{a}$ and $\overline{c}$ are the same. This shows that φ is well-defined.

The fact that φ is an homomorphism follows immediately from **Thm. 1.2.2.**

The surjectivity part is obvious. The last remaining part of the proof is to verify that φ is injective.

Let $P = aX^2 + bY^2$ be such that $\varphi([P]) = \overline{a} = \overline{1}$. We want to find a

$$g = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Q})$$

such that $P^g = X^2 - \frac{1}{4}DY^2$, the identity form for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$.

If we act on P by g then we obtain,

$$P^g = (as^2 + bu^2)X^2 + (2st + 2uv)XY + (at^2 + bv^2)Y^2$$

Since we want P^g to be the identity we need to pick rational numbers s, u so that,

$$as^2 + bu^2 = 1$$

Since $a \in \mathbb{Q}_D^\times$, and $\mathbb{Q}_D^\times$ is a group, $\frac{1}{a} \in \mathbb{Q}_D^\times$, we can thus write $\frac{1}{a} = x^2 - Dy^2$ for some rational numbers x, y. Thus,

$$s^2 + \tfrac{b}{a}u^2 = x^2 - Dy^2 \implies s^2 - \tfrac{D}{4a^2}u^2 = x^2 - Dy^2$$

Pick $s = x$ and $u = 2ay$. Since s, u are determined it remains to determine t, v. The conditions on t, v are determined by the requirement that $st+uv = 0$ and that the $\det(g) = 1$ i.e. $-ut + sv = 1$. This is a system of linear equations in terms of t, v which is solvable since the determinant of this system, $s^2 + u^2$, is non-zero. By picking s, t, u, v in this way we construct g which will transform $aX^2 + bY^2$ into $X^2 - \frac{1}{4}Y^2$, hence $[P]$ is the identity class, which proves that φ is injective. This completes the proof. ■

1.3 Relationship Between Integral and Rational Quadratic Forms

In §1 we defined the group $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ and in §2 we defined the group $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$. Since both groups were defined in a very similar manner it is reasonable to ask what kind of relationship exists between these two groups?

Before we say anything we need to introduce some notation. If $P(X, Y)$ is a quadratic form with integral coefficients then it is also a quadratic form with rational coefficients. We need to introduce some notation to distinguish whether we think of $[P]$ as a class in $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ or as a class in $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$.

Definition 1.3.1. Let $P(X, Y) = aX^2 + bXY + cY^2$ be a quadratic form with discriminant D and $a, b, c \in \mathbb{Z}$. We use the notation $[P]_{\mathbb{Z}}$ to denote the class of P in $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$. We use the notation $[P]_{\mathbb{Q}}$ to denote the class of P in $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$.

Here is our first simple relationship between between these two groups.

Proposition 1.3.2. *We have a natural map,* $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ *given by,*

$$[P]_{\mathbb{Z}} \mapsto [P]_{\mathbb{Q}}$$

Proof. We need to show this map is well-defined. Suppose that $[P]_{\mathbb{Z}} = [Q]_{\mathbb{Z}}$, then it means,

by definition of equivalence, there is a $g \in \mathrm{SL}(2,\mathbb{Z})$ such that $P^g = Q$. However, $g \in \mathrm{SL}(2,\mathbb{Q})$ also, which implies that $[P]_{\mathbb{Q}} = [Q]_{\mathbb{Q}}$. ■

By **Thm. 1.1.6.** we have the isomorphism $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \simeq \mathrm{Cl}^+(\mathbb{Z}_K)$ and by **Prop. 1.2.3.** we have the isomorphism $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D) \simeq \mathbb{Q}^\times/\mathbb{Q}_D^\times$. Thus, it is natural to consider what is the analogous map in **Prop. 1.3.2.** in terms of these isomorphic groups? The answer in provided in the following Theorem.

Theorem 1.3.3. *We have the following commutative diagram of commutative groups,*

$$\begin{array}{ccc} \mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) & \longrightarrow & \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D) \\ \simeq\downarrow & & \downarrow\simeq \\ \mathrm{Cl}^+(\mathbb{Z}_K) & \longrightarrow & \mathbb{Q}^\times/\mathbb{Q}_D^\times \end{array}$$

where the upper horizontal map is from ***Prop. 1.3.2.****, the left isomorphism is from* ***Thm. 1.1.6.****, the right isomorphism is from* ***Prop. 1.2.3.****, and the lower horizontal map is defined as follows: given a class* $[I] \in \mathrm{Cl}^+(\mathbb{Z}_K)$*, we map* $[I] \mapsto \overline{N(I)} \in \mathbb{Q}^\times/\mathbb{Q}_D^\times$ *(where* $N(\cdot)$ *indicates the ideal-norm). In particular, the map in* **Prop. 1.3.2.** *can be seen as an ideal-norm map.*

Proof. We first show that the map $[I] \mapsto \overline{N(I)}$ is well-defined. If I, J are two fractional ideals in the same narrow class then $I = \alpha J$ for some $\alpha \in K = \mathbb{Q}(\sqrt{D})$ with $N_{K/\mathbb{Q}}(\alpha) > 0$. We have that $N(I) = N(\alpha)N(J)$. Observe that if $\alpha = x + y\sqrt{D} \in D$ then $N(\alpha) = x^2 - Dy^2$, which by definition belongs to the subgroup $\mathbb{Q}_D^\times$. Thus, we see that $N(I)$ and $N(J)$ differ up to a multiple factor in $\mathbb{Q}_D^\times$. Thus, the lower horizontal map is well-defined.

Let $P = aX^2 + bXY + cY^2$. To establish the commutativity of the diagram we need to verify that,

$$\overline{N\left(\alpha\left\langle a, \tfrac{-b+\sqrt{D}}{2}\right\rangle\right)} = \overline{a}$$

where $\alpha \in K$ is chosen so that $aN(\alpha) > 0$.

For definiteness, say $D \equiv 1(\mathrm{mod}4)$. If $I = \langle\alpha, \beta\rangle$ is an ideal of $\mathbb{Z}_K$ then the norm of I

can be computed as follows,

$$N(I) = \frac{1}{\sqrt{D}} \left| \overline{\alpha}\beta - \alpha\overline{\beta} \right|$$

where $\overline{\alpha}$ and $\overline{\beta}$ denote the conjugates of α and β under the non-trivial automorphism of $\mathrm{Gal}(K/\mathbb{Q})$. If we apply this computation to our case we find that,

$$N\left(\alpha \left\langle a, \tfrac{-b+\sqrt{D}}{2} \right\rangle\right) = |N(\alpha)a| = N(\alpha)a$$

But we observed above that $N(\alpha) \in \mathbb{Q}_D^{\times}$, thus this establishes the claim. ■

We can now answer the question we raised earlier whether the natural map in **Prop. 1.3.2.** is a homomorphism of commutative groups.

Corollary 1.3.4. *The natural map in* ***Prop. 1.3.2.*** *is a homomorphism.*

Proof. This natural map factors as a product of the three maps by the maps provided in the commutative diagram of **Thm. 1.3.3.**, furthermore each of the three maps is a homomorphism. Clearly, the two vertical maps are homomorphisms as they are isomorphisms, and the lower horizontal map is a homomorphism as it is the ideal-norm map. ■

The last natural question to ask is whether the homomorphism of **Prop. 1.3.2.** is injective? Thus, does $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ embed as a subgroup of $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$? The answer is in general no.

Remark 1.3.5. The natural map,

$$\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$$

is in general non-injective. Indeed, $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ is a group of exponent at most 2, while $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ in general is not. Note, it appears that this map is injective on genus classes, however this observation will not be used anywhere in this paper.

1.4 Composition of Integral Forms Revisited

We have two composition laws, one for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ which is "*hard*", and one for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ which is "*easy*". We also have the natural homomorphism between them given by $[P]_{\mathbb{Z}} \mapsto [P]_{\mathbb{Q}}$ as mentioned in §3. Unfortunately, this homomorphism is not necessarily injective (cf. **Remark 1.3.5.**), but if it is then we have an "*easier*" way of describing the composition in **Thm. 1.1.3.**, which is the content of the following Proposition.

Proposition. 1.4.1. *Suppose D is a discriminant such that $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \hookrightarrow \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$. Let $P_1, P_2, ..., P_n$ be a set of representatives for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$. Given $i, j \in \{1, 2, ..., n\}$ there exists a unique $1 \leq \ell \leq n$ such that,*

$$[P_i]_{\mathbb{Q}} + [P_j]_{\mathbb{Q}} = [P_\ell]_{\mathbb{Q}}.$$

We then have that $[P_i]_{\mathbb{Z}} + [P_j]_{\mathbb{Z}} = [P_\ell]_{\mathbb{Z}}$.

Proof. There exists a $1 \leq k \leq n$ so that,

$$[P_i]_{\mathbb{Z}} + [P_j]_{\mathbb{Z}} = [P_k]_{\mathbb{Z}}$$

Since the natural map $[P]_{\mathbb{Z}} \to [P]_{\mathbb{Q}}$ is a homomorphism by **Cor. 1.3.4.** we obtain,

$$[P_i]_{\mathbb{Q}} + [P_j]_{\mathbb{Q}} = [P_k]_{\mathbb{Q}}$$

Hence, such an ℓ certainly exists as claimed in the Proposition. It must be unique because we have,

$$[P_k]_{\mathbb{Q}} = [P_\ell]_{\mathbb{Q}} \implies [P_k]_{\mathbb{Z}} = [P_\ell]_{\mathbb{Z}} \implies P_k = P_\ell$$

by the injective hypothesis. ■

Thus, the composition law for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ can be "*explained*" by looking at the two classes of integral forms instead as rational forms, then computing composition of those two

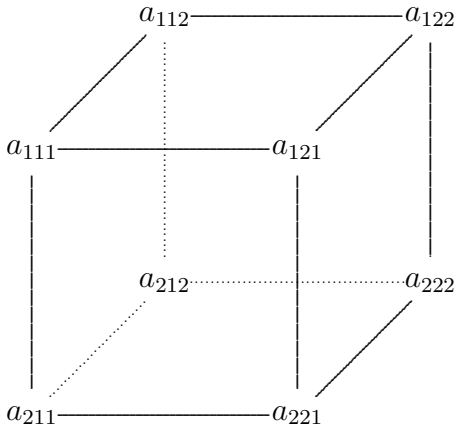
forms in the "*easier*" rational way. The problem is, as we alluded to already, the condition on D in **Prop. 1.4.1.** is too strong, and so this result is not much applicable in most desirable computations.

Later in this paper we will discuss cubic forms, both integral and rational, and we will see that the analogue of this Proposition does carry through quite nicely. We mention this Proposition here only as a means to motivate the idea that are to follow in this paper.

1.5 Integral Bhargava Cubes

To begin with consider a "*Bhargava cube*". Our approach is informed by the works of Bhargava [**Bhargava,** §2.1] and Kable [**Kable**] who introduced the prespective we adopt at roughly the same time.

A "*Bhargava cube*" is, by definition, an element of the space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, a free $\mathbb{Z}$-module of rank 8 with basis $e_i \otimes e_j \otimes e_k$ where $i, j, k \in \{0, 1\}$ and $e_1 = (1, 0)$ and $e_2 = (0, 1)$ is the standard basis for $\mathbb{Z}^2$. As such any element of $\sum_{i,j,k} a_{ijk}\ e_i \otimes e_j \otimes e_k \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ can therefore by represented by a cube with integer corners.



Let $\Gamma_{\mathbb{Z}} = \mathrm{SL}(2, \mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z})$. The group $\Gamma_{\mathbb{Z}}$ acts on $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ "*coordinate-by-coordinate*" in the same way as $\mathrm{SL}(2, \mathbb{Z})$ acts on $\mathbb{Z}^2$. More explicitly, if $\gamma \in \Gamma_{\mathbb{Z}}$, write

$\gamma = (g_1, g_2, g_3)$ where $g_i \in \mathrm{SL}(2, \mathbb{Z})$ and if $C = \sum_{i,j,k} a_{ijk} e_i \otimes e_j \otimes e_k$ then $\gamma \cdot C = \sum_{i,j,k} a_{i,j,k} (g_1 \cdot e_1) \otimes (g_2 \cdot e_2) \otimes (g_3 \cdot e_3)$.

A more geometric way to see the action $\gamma \cdot C$ is as follows. Cut the cube C into two squares by using front/back squares, left/right squares, and top/bottom squares. That is, cut the cube into the following pairs of matrices:

$$\begin{cases} M_1 = (a_{i,j,1}) & \text{and} & N_1 = (a_{i,j,2}) & \text{front and back} \\ M_2 = (a_{j,1,i}) & \text{and} & N_2 = (a_{j,2,i}) & \text{left and right} \\ M_3 = (a_{1,i,j}) & \text{and} & N_3 = (a_{1,i,j}) & \text{top and bottom} \end{cases}$$

where $(i, j) \in \{(1, 1), (1, 2), (2, 1), (2, 2)\}$. These matrix pairs (M_i, N_i) will be referred to as the "*cuttings*" of the cube.

If $\gamma = (g_1, g_2, g_3)$ and $g_i = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ then g_i transforms C by taking the pair of matrices (M_i, N_i) and replacing them by $(rM_i + sN_i, tM_i + uN_i)$. The order of how each g_1, g_2, g_3 acts on the cube is irrelevant and the final resulting cube is $\gamma \cdot C$. In other words, we can transform C by acting by g_1 then g_2 then g_3, or we can transform C by acting in the order g_3 then g_2 then g_1, or any other permutation.

Given such a cube C, we can obtain from it three pairs of quadratic forms corresponding to each type of cutting, namely, the three quadratic forms,

$$P_i^C(X, Y) = -\det(M_i X - N_i Y)$$

for each $i = 1, 2, 3$. These three quadratic forms, arising from the cube C, can all be shown to have the same discriminant. This common discriminant value will be denoted by $\mathrm{disc}(C)$ and will be referred to as the "*discriminant*" of the Bhargava cube C.

Just as with quadratic forms we have a notion of primitiveness, so too we have a similar notion for cubes. We say a cube C is "*projective*" if the three associated quadratic forms P_i^C are primitive for $i = 1, 2, 3$.

If C is a Bhargava cube and $\gamma \in \Gamma_{\mathbb{Z}}$ then the following two facts are analogous as with quadratic forms. First, if C is primitive then $\gamma \cdot C$ is primitive. Second, $\mathrm{disc}(C) = \mathrm{disc}(\gamma \cdot C)$. Thus, just as with quadratic forms, we consider the equivalence classes of projective cubes with a fixed discriminant D. We denote the set of these equivalence classes by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$. We also use the notation $[C]$ to denote the equivalence class of C.

If $[C] = [C']$ in $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$ then $[P_i^C] = [P_i^{C'}]$ in $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$.

Here is the remarkable connection to Gauss composition.

Theorem 1.5.1. *If* $[C] \in \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$ *then,*

$$[P_1^C] + [P_2^C] + [P_3^C] = 0$$

where the "+" denotes Gauss composition in $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$.

Furthermore, if $[P_1], [P_2], [P_3] \in \mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ *are such that,*

$$[P_1] + [P_2] + [P_3] = 0$$

then there exists a unique $[C] \in \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$ *such that,* $[P_i^C] = [P_i]$.

Proof. This is a known result [**Bhargava**, **Thm. 1**]. ■

1.6 Rational Bhargava Cubes

In §5 we introduced integral Bhargava cubes. In this section we introduce rational Bhargava cubes, i.e. cubes with rational cubical corners. More precisely, a rational Bhargava cube C is an element of the space $C \in \mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2$ (where the tensor product is taken over the ring $\mathbb{Q}$).

When dealing with integral Bhargava cubes we put the requirement that they should be *projective*. In the rational case we do not impose this restriction as the gcd of any set of

non-zero rational numbers is automatically a unit. This is similar to the situation in §2 with rational quadratic forms.

If we define the group $\Gamma_{\mathbb{Q}} = \mathrm{SL}(2,\mathbb{Q}) \times \mathrm{SL}(2,\mathbb{Q}) \times \mathrm{SL}(2,\mathbb{Q})$ then $\Gamma_{\mathbb{Q}}$ acts on $\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2$ in the similar manner as $\Gamma_{\mathbb{Z}}$ acts on $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Given a rational cube C we can likewise define $\mathrm{disc}(C)$. If C and C' are equivalent under $\Gamma_{\mathbb{Q}}$ then they have the same discriminant, this can be verified by applying the formulas and performing a direct computation.

In a similar way we introduce the equivalence classes of $\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2$ mod $\Gamma_{\mathbb{Q}}$ of a fixed discriminant D (just like in the previous section let us assume that D is an integer which is not a perfect square). We denote these classes by $\mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$.

Without any surprise we have the analog of **Thm 1.5.1.**, with one big change. In **Thm. 1.5.1.** we have uniqueness. In the rational analog of this theorem everything carries over except for uniqueness. This non-uniqueness issue will be become annoying in **Chapter 2** but we will have a way to deal around it.

Theorem 1.6.1. *If* $[C] \in \mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$ *then,*

$$[P_1^C] + [P_2^C] + [P_3^C] = 0$$

where the "+" *denotes Gauss composition in* $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$.

Furthermore, if $[P_1], [P_2], [P_3] \in \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ *such that,*

$$[P_1] + [P_2] + [P_3] = 0$$

then there exists a $[C] \in \mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$ *such that,* $[P_i^C] = [P_i]$.

Proof. The proof of this result is identical to the proof of **Thm. 1.5.1.**, the only distinction is that by using rational coefficients we cannot force uniqueness. ■

1.7 Composition Laws for Bhargava Cubes

In the previous sections we put a composition law for $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ and $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ in such a way that the natural map $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ is a morphism. In this section we will put a law of composition on $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$. [**Bhargava**, **§2.3**]

Let C_1 and C_2 be two cubes in $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$. As we have seen in **Thm 1.5.1.** that we have,

$$[P_1^{C_i}] + [P_2^{C_i}] + [P_3^{C_i}] = 0$$

for $i = 1, 2$. Thus, by adding these classes we obtain,

$$\left([P_1^{C_1}] + [P_1^{C_2}]\right) + \left([P_2^{C_1}] + [P_2^{C_2}]\right) + \left([P_3^{C_1}] + [P_3^{C_2}]\right) = 0$$

Thus, we have three quadratic forms which add up to the identity form, so by **Thm. 1.5.1.** again, we can find a unique cube C_3, up to $\Gamma_{\mathbb{Z}}$-equivalence, such that $[P_j^{C_3}] = [P_1^{C_1}] + [P_1^{C_2}]$ for all $j = 1, 2, 3$. We can then go ahead and define $[C_3] = [C_1] + [C_2]$.

The above construction defines a law of composition for $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$. It is natural to replace $\mathbb{Z}$ by $\mathbb{Q}$ and hope that the same process used above can be carried through to put a law of composition on $\mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$. Unfortunately, the analog of **Thm. 1.6.1.** does not satisfy the uniqueness property as **Thm. 1.5.1.**.

We can still be optimistic that a law of composition for $\mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$ still exists and is compatible with $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$. We formulate the following conjecture.

Conjecture 1.7.1. *There is a law of composition for* $\mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$ *such that the natural map* $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D) \to \mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$, *given by* $[C]_{\mathbb{Z}} \mapsto [C]_{\mathbb{Q}}$, *from integral cubes to rational cubes, is a homomorphism of groups.*

This conjecture will not be settled in this paper because it will not be necessary for us.

We simply introduce this conjecture for the purposes of interest and as a possible means of generalizing some of the ideas in this paper.

Chapter 2

Binary Cubic Forms

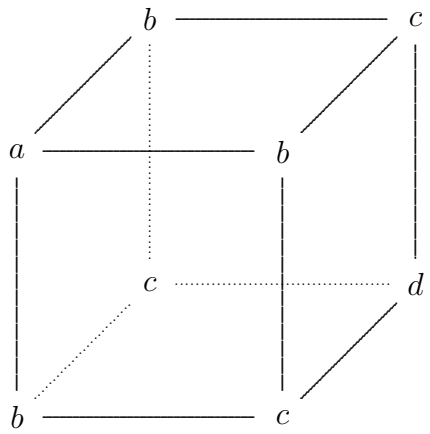
2.1 Integral Binary Cubic Forms

In **Chapter 1**, we discussed quadratic forms $aX^2 + bXY + cY^2$ where the coefficients were integral. In this chapter we will introduce "*binary cubic forms*". These can be thought of as polynomials in two indeterminates of the form,

$$aX^3 + 3bX^2Y + 3cXY^2 + dY^3$$

We denote the space of all integral binary cubic forms by $\text{sym}^3\mathbb{Z}^2$. This notation is bit inconsistent with $\text{sym}^2\mathbb{Z}^2$, as with binary quadratic forms we allowed the central term XY to have odd coefficients, in this paper $\text{sym}^3\mathbb{Z}^2$ will refer to those binary cubic forms were the X^2Y and XY^2 coefficients are multiples of three. This is a bit unfortunate but we hope the reader will not be confused by our notation.

Such a cubic form can be represented by a Bhargava cube,



If $f(X,Y)$ is our cubic form we can associate to it a cube C of the type above. We have seen that for each cube C there corresponds three quadratic forms $P_1^C(X,Y)$, $P_2^C(X,Y)$, and $P_3^C(X,Y)$ (**cf.** §1.5). Because of the symmetry of the cube all of these three quadratic forms $P_i^C(X,Y)$ are the same, namely,

$$P_i^C(X,Y) = -\det\left(\begin{bmatrix} aX & bX \\ bX & cX \end{bmatrix} - \begin{bmatrix} bY & cY \\ cY & dY \end{bmatrix}\right) = -\det\left(\begin{bmatrix} aX - bY & bX - cY \\ bX - cY & cX - dY \end{bmatrix}\right)$$

This computes to be equal to,

$$P_i^C(X,Y) = (b^2 - ac)X^2 + (ad - bc)XY + (c^2 - bd)Y^2$$

For simplicity we will denote the above quadratic form by $H(f)$.

The careful reader will observe that $H(f)$ is not quite the Hessian, the classical Hessian has $-(ad - bc)$ term, whereas $H(f)$ has a positive term. We keep the notation $H(f)$ to be consistent with Bhargava's notation.

Definition 2.1.1. Let $f(X,Y) = aX^2 + 3bX^2Y + 3cXY^2 + dY^3$ be a cubic form. We denote by $H(f)$ to be the quadratic form,

$$H(f) = (b^2 - ac)X^2 + (ad - bc)XY + (c^2 - bd)Y^2$$

In **Chapter 1**, we defined primitive quadratic forms and the discriminant of quadratic forms. When dealing with cubic forms we will have similar notions as well. This is the content of the next two definitions.

Definition 2.1.2. Let $f(X,Y)$ be an integral cubic form. We say $f(X,Y)$ is a "*projective*" if $H(f)$ is primitive quadratic form (**cf.** §1.1).

Thus, $f(X,Y)$ is projective if and only if,

$$\gcd(b^2 - ac, ad - bc, c^2 - bd) = 1$$

Definition 2.1.3. The "*discriminant*" of $f(X,Y)$ is defined to be the discriminant of its corresponding cube C as in **Chapter 1**. In other words, the discriminant of f is the discriminant of $H(f)$, thus,

$$\text{disc}(f) = a^2d^2 - 3b^2c^2 - 6abcd + 4b^3d + 4ac^3$$

The following simple result ensures that we have projective forms automatically.

Proposition 2.1.4. *If $f(X,Y)$ is an integral cubic form whose discriminant is square-free then $f(X,Y)$ is projective.*

Proof. If $f(X,Y)$ is not projective then there exists a positive integer $\ell > 1$ which divides every coefficient of $H(f)$. But then ℓ^2 will divide the discriminant of $H(f)$. However, the discriminant of $H(f)$ is the discriminant of f. Thus, ℓ^2 divides $\text{disc}(f)$, which is a contradiction. ■

Assumption 2.1.5. For the rest of this paper we will assume that the discriminant D is square-free. This assumption, by **Prop. 2.1.4.**, will imply that our cubic forms are automatically projective.

Just as with quadratic forms we have the right action of $\text{SL}(2,\mathbb{Z})$ on the space $\text{sym}^3\mathbb{Z}^2$.

More explicitly, if $g = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ then $(f^g)(X,Y) = f(rX+sY, tX+uY)$. The following proposition parallels the action with quadratic forms.

Proposition 2.1.6. *Let $f(X,Y)$ be an integral cubic form and $g \in \mathrm{SL}(2,\mathbb{Z})$.*

(i) *If f is projective then f^g is projective.*

(ii) *The discriminant is preserved under the action, i.e.* $\mathrm{disc}(f) = \mathrm{disc}(f^g)$

Proof. This is immediate from the fact that $H(f)^g = H(f^g)$, which is a straightforward computation in writing out each of the formulas. To prove **(i)** note that $H(f)$ is primitive, since $H(f)^g$ is also primitive it follows that $H(f^g) = H(f)^g$ is primitive. Likewise, disc $(f^g) =$ disc $H(f^g) =$ disc $H(f)^g =$ disc $H(f)$. ■

We next identify certain cubic forms as the same and consider equivalence classes.

Definition 2.1.7. Fix D to be a square-free discriminant (in this definition it does not need to be square-free, but our assumption is to assume that D will always be square-free in this paper). Two projective cubic forms, f_1 and f_2, of the same discriminant D, are said to be "*equivalent*", if there exists $g \in \mathrm{SL}(2,\mathbb{Z})$ such that $f_1^g = f_2$. We denote the equivalence classes of all projective cubic forms of a fixed discriminant D by $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$.

2.2 Composition Law for Integral Cubic Forms

We can equip $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$ with a structure of a group. The main idea comes from the composition law on Bhargava cubes described in §1.7. Let $P(X,Y)$ and $Q(X,Y)$ be two representatives in $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$. We can think of P and Q as triply-symmetric Bhargava cubes in $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$. If we compose $[P], [Q]$, thinking of them in the space $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$, then we will get another triply-symmetric cube $[R] \in \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$, we can go back and think of R as a cubic form again. With this procedure we define $[P] + [Q] = [R]$

where $[P], [Q], [R] \in \mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$.

We state this as a Theorem below.

Theorem. 2.2.1. *There is a law of composition on* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$ *such that the map* $H : \mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ *is a group homomorphism.*

Proof. The above paragraph is a summary of how the law of composition is defined for $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$, but it is by no means a proof. The full proof of this Theorem is a known result [**Bhargava**, **Cor. 15**]. ■

2.3 Rational Cubic Forms

We denote by $\mathrm{sym}^2\mathbb{Q}^2$ to be the space of all cubic forms $P(X, Y) = aX^3 + b(3X^2Y) + c(3XY^2) + dY^3$ where $a, b, c, d \in \mathbb{Q}$. In a similar manner as we did in §1 we have the quadratic form $H(P)$ and as well as the discriminant $\mathrm{disc}(P)$, all defined in a similar manner.

The group $\mathrm{SL}(2, \mathbb{Q})$ acts in a similar way on this space. The one contrast between integral vs rational cubic forms is that we do not have any notion of projectivity. All rational cubic forms, as long as they are non-zero, will be considered and we will not limit them to being projective.

Definition. 2.3.1. We denote by $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$ to be the equivalence classes of all rational cubic forms under the group action $\mathrm{SL}(2, \mathbb{Q})$.

If $P(X, Y)$ is a projective integral cubic form of discriminant D then it is automatically a rational cubic form of the same discriminant D.

Proposition 2.3.2. *Let* $P(X, Y)$ *be an integral projective cubic form of discriminant* D. *We let* $[P]_{\mathbb{Z}}$ *denote its class in* $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Z}^2, D)$ *and* $[P]_{\mathbb{Q}}$ *denote its class in* $\mathrm{Cl}(\mathrm{sym}^2\mathbb{Q}^2, D)$.

There is a natural map,

$$\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$$

given by $[P]_{\mathbb{Z}} \mapsto [P]_{\mathbb{Q}}$.

Proof. This is clear. ■

The map in **Prop. 1.3.2.** parallels the analogous map for binary quadratic forms given in **Prop. 2.3.2.**. What is remarkable is that while the map in **Prop. 1.3.2.** is, in general, not injective, the map in **Prop. 2.3.2.** is injective!

Theorem 2.3.3. *The natural map in* **Prop. 2.3.2.** *is injective.*

Proof. We delay the proof into the next section. The Theorem will be stated more generally in **Thm. 2.4.1.** and the more general result will be proven. From here the proof will follow. ■

2.4 Proof of Injectivity

Let $P \in \mathrm{sym}^3\mathbb{Z}^2$ be the cubic form given by,

$$P(X, Y) = aX^3 + b(3X^2Y) + c(3XY^2) + dY^3.$$

We define the "*projection*" of $P(X, Y)$ to be the following quantity,

$$\mathrm{proj}(P) = \gcd(b^2 - ac, ad - bc, c^2 - bd) = \text{content of } H(P)$$

We say a cubic form P is "*projective*" if $\mathrm{proj}(P) = 1$.

Fix a prime number p. We define,

$$\mathrm{proj}_p(P) = \gcd(b^2 - ac, ad - bc, c^2 - bd) \in \mathbb{Z}_{(p)}$$

where by $\mathbb{Z}_{(p)}$ we mean the localization of $\mathbb{Z}$ at the prime ideal (p). Since $\mathbb{Z}_{(p)}$ is a discrete valuation ring the gcd exists and is unique up to a unit factor.

Our goal is to prove the following theorem.

Theorem 2.4.1. *Let $P, Q \in \mathrm{sym}^3\mathbb{Z}^2$ be two cubic forms and $g \in \mathrm{SL}(2,\mathbb{Q})$ such that $P^g = Q$. If $\mathrm{disc}(P) = \mathrm{disc}(Q)$ is not divisible by p^2 then $g \in \mathrm{SL}(2,\mathbb{Z}_{(p)})$.*

A consequence of this theorem is,

Corollary. 2.4.2. *Let $P, Q \in \mathrm{sym}^3\mathbb{Z}^2$ be two projective cubic forms of the same discriminant such that $\mathrm{disc}(P) = \mathrm{disc}(Q)$ is square-free and $g \in \mathrm{SL}(2,\mathbb{Q})$ so that $P^g = Q$ then $g \in \mathrm{SL}(2,\mathbb{Z})$. In particular the natural map in* **Thm. 2.3.3.** *is an injective map.*

Proof. Let p be a prime. Since the quantity $\mathrm{disc}(P)$ is square-free it is not divisible by p^2. Thus, by the Theorem, $g \in \mathrm{SL}(2,\mathbb{Z}_{(p)})$. This is true for each prime. Thus,

$$g \in \bigcap_p \mathrm{SL}(2,\mathbb{Z}_{(p)}) = \mathrm{SL}\left(2, \bigcap_p \mathbb{Z}_{(p)}\right) = \mathrm{SL}(2,\mathbb{Z})$$

■

Now we give a proof of **Theorem 2.4.1.**.

We start by writing,

$$g = \begin{bmatrix} i/D & j/D \\ k/D & \ell/D \end{bmatrix}$$

where $i, j, k, \ell, D \in \mathbb{Z}$ and $\gcd(i, j, k, \ell) = 1$ with $i\ell - jk = D^2$ and $D > 0$. (Here D refers to the common denominator of the fractions which make up the numbers in the matrix g, it is not in any way related to the discriminant D.)

Thus, if $P^g = Q$ then we can write,

$$P\begin{bmatrix} i & j \\ k & \ell \end{bmatrix} = Q\begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix}$$

It follows from here that,

$$\mathrm{proj}\left(P\begin{bmatrix} i & j \\ k & \ell \end{bmatrix}\right) = \mathrm{proj}\left(Q\begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix}\right)$$

It is clear that, if $\mathrm{proj}(Q) = 1$, then,

$$\mathrm{proj}\Big(Q\begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix}\Big) = D^6$$

We can now state an easy observation.

Observation 2.4.3. If $P \in \mathrm{sym}^3\mathbb{Z}^2$ and

$$g = \begin{bmatrix} i/D & j/D \\ k/D & \ell/D \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Q})$$

is such that $(P^g) \in \mathrm{sym}^3\mathbb{Z}^2$, then

$$\mathrm{proj}\left(P\begin{bmatrix} i & j \\ k & \ell \end{bmatrix}\right) = D^6$$

Hence, the only possible counter-examples to the **Theorem** (which do not exist!), must necessarily be of the type provided in **Obv. 2.4.3.** Furthermore, in searching for counter-examples, we can assume without lose of generality that $k = 0$, since, after a suitable action of $\mathrm{SL}(2,\mathbb{Z})$ we can transform that integer-matrix into one where the lower-left coefficient is zero.

Suppose, for the sake of contradiction, there is a prime number p which divides D. Write $D = p^e D_0$ where D_0 is not divisible by p. Therefore, the image of D in $\mathbb{Z}_{(p)}$ will be εp^e where ε is a unit in $\mathbb{Z}_{(p)}$.

Suppose, for sake of contradiction, that the theorem is false, then

$$\mathrm{proj}_p\left(P\begin{bmatrix} i & j \\ 0 & \ell \end{bmatrix}\right) = (\varepsilon p^e)^6$$

for some integers i, j, ℓ which are relatively prime and $i\ell = (\varepsilon p^e)^2$ in $\mathbb{Z}_{(p)}$.

Therefore, the matrix when viewed as living in the ring $\mathbb{Z}_{(p)}$ will be of the form,

$$\begin{bmatrix} \alpha p^u & j \\ 0 & \beta p^v \end{bmatrix}$$

where α, β are units and $u + v = 2e$. Thus, the g which produces the counter-example, will be,

$$g = \begin{bmatrix} \alpha p^{u-e} & jp^{-e} \\ 0 & \beta p^{v-e} \end{bmatrix}$$

If $\frac{3}{2}e < u \leq 2e$ then P^g will produce a cubic form where the X^3 coefficient is equal to $a\alpha p^{3u-3e}$. Since $u > e$ it means the exponent $3u - 3e$ is at least 2 and so this coefficient is divisible by p^2. Furthermore, the $3X^2Y$ coefficient is equal to $\alpha^2 p^{2u-3e}(aj + b\beta p^v)$. Since $u > \frac{3}{2}e$ we have that $2u - 3e > 0$ and so this coefficient is divisible by p. By looking at the definition of the discriminant, if the X^3 coefficient is divisible by p^2 and the $3X^2Y$ coefficient is divisible by p, it follows that p^2 will divide $\mathrm{disc}(P)$. This is a contradiction.

If $0 \leq u < \frac{1}{2}e$ then we will show this case also leads to a contradiction. We can replace g by g^{-1}, since if $P^g = Q$ then $Q^{g^{-1}} = P$. Therefore, if g is a counter-example to the Theorem then so is g^{-1}. We calculate that,

$$g^{-1} = \begin{bmatrix} \alpha p^{e-u} & -\frac{j}{\alpha\beta} p^{e-u-v} \\ 0 & \beta p^{e-v} \end{bmatrix}$$

by using the equation $u + v = 2e$, and denoting $j' = -\frac{j}{\alpha\beta}$, we simplify this to,

$$g^{-1} = \begin{bmatrix} \alpha p^{e-u} & j'p^{-e} \\ 0 & \beta p^{e-v} \end{bmatrix}$$

Ignoring the irrelevant term j' this is the same matrix except instead of $u - e$ we have $e - u$. In other words, u gets substituted by $2e - u$. If $0 \leq u < \frac{1}{2}e$ then $\frac{3}{2}e < 2e - u \leq 2e$. We are back again in the first case that we considered. The first case leads to a contradiction, hence this second case also leads to a contradiction.

Thus, the last remaining possibility for u is that $\frac{1}{2}e \leq u \leq \frac{3}{2}e$. We split this last case into two cases. One where $e \leq u \leq \frac{3}{2}e$ and the other where $\frac{1}{2}e \leq u \leq e$. Again by replacing g by

g^{-1} we can rule out either case immediately once we rule out one of these. Let us assume then that $\frac{1}{2}e \leq u \leq e$.

For the moment ignore the special case when $u = e$. We have that $u < e$. Since the X^3 coefficient of P^g is equal to $a\alpha p^{3u-3e}$ we find that the power of p is negative. However, the coefficient of X^3 is in the ring $\mathbb{Z}_{(p)}$, so it must appear to a non-negative p power. We conclude from this that p divides a. If however $u = e$ then $v = e$ also, and in this special case, the $3X^2Y$ coefficient computes to $\alpha^2 p^{2u-3e}(aj + b\beta p^v) = \alpha^2 p^{-e} aj + b\beta$. Again this coefficient belongs to $\mathbb{Z}_{(p)}$, therefore, $\alpha^2 aj$ is divisible by p^e. Since α is a unit, and j is a unit (it is relatively prime to p), we conclude that a is divisible by p^e, and so by p. Therefore, in the case when $\frac{1}{2}e \leq u \leq e$ we are led to the consequence that p divides a.

Since we have that, for some unit $\theta \in \mathbb{Z}_{(p)}$,

$$\mathrm{proj}_p \left(P \begin{bmatrix} i & j \\ 0 & \ell \end{bmatrix} \right) = \mathrm{proj}_p \left(P \begin{bmatrix} \alpha p^u & j \\ 0 & \beta p^v \end{bmatrix} \right) = \theta p^{6e}$$

Now expand out proj_p to obtain, inside the ring $\mathbb{Z}_{(p)}$,

$$\begin{aligned} p^{4e} \gcd \Big(& \alpha^4 \beta^2 p^{2u}(b^2 - ac), \\ & \alpha^3 \beta^3 p^e (ad - bc) - 2j\alpha^3 \beta^2 p^u (b^2 - ac), \\ & \alpha^2 \beta^2 j^2 (b^2 - ac) + \alpha^2 \beta^4 p^{2v} (c^2 - bd) - \alpha^2 \beta^3 j p^v (ad - bc) \Big) = \theta p^{6e} \end{aligned}$$

Therefore, the last component of the gcd is divisible by p^2, and so divisible by p. Since the second and third term are divisible by p, it follows that p must divide the first term. However, α, β, j are units in $\mathbb{Z}_{(p)}$. We obtain that p divides $b^2 - ac$. Since, as we argued above, p divides a, the conclusion is that p divides b^2, therefore p divides b. Now, the last component on the gcd is divisible by p^2. Since $p|a$ and $p|b$, we can see that p^2 must therefore divide the middle and last term. The conclusion is that p^2 divides $b^2 - ac$, but $p|b$, and so p^2 divides ac. Because a is divisible by p and $p^2|(ac)$ we either have that $p^2|a$ or else $p|c$.

To summarize, we have shown, that in the case when $\frac{1}{2}e \leq u \leq \frac{3}{2}e$, that one of the two occur: **(i)** $p|a$, $p|b$, $p|c$. **(ii)** $p^2|a$, $p|b$. If **(i)** is true then p^2 will divide disc(P). If **(ii)** is true then p^2 will divide disc(P). Regardless we arrive at the contradiction that the discriminant is divisible by p^2.

The contradiction came from the supposition that D was divisible by a prime p. To avoid this contradiction we must take D to be a unit in $\mathbb{Z}_{(p)}$. Therefore, the matrix g has coefficients in $\mathbb{Z}_{(p)}$. This completes the proof of the theorem. ■

2.5 Composition of Rational Cubic Forms

We can equip $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ with the structure of a group. The idea here is to follow the construction in §2. Namely, if P and Q are rational cubic forms then we can regard them as triply-symmetric Bhargava cubes and execute their composition in $\mathrm{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$. Unfortunately, because of **Conjecture 1.7.1.**, it is not clear to us if this construction actually works. Fortunately, however, we are able to circumvent the need for this conjecture to state our result.

Theorem. 2.5.1. *There exists a law of composition for* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ *such that the natural map* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ *is a homomorphism.*

Proof. We will prove this result in the next chapter. Our approach instead will equip $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ with the structure of a group, in a totally new manner not based on Bhargava composition, rather based on the works of Slupinski and Stanton [**Slupinski-Stanton, Thm. 3.46**], and then show that this way of defining composition will satisfy the theorem. ■

Chapter 3

Composition of Rational Binary Cubic Forms

3.1 Introduction

In the previous chapter we introduced classes of integral cubic forms of a fixed discriminant and put on them a group law. This was all inspired by the works of Bhargava. As we alluded, there is also a group law on classes of rational cubic forms for a fixed discriminant. However, we will not describe this using Bhargava's approach. It is the goal of this chapter to study rational cubic forms themselves in more detail. In the end we will have a way to describe the rational group law, as stated in **Thm. 2.5.1.**.

From our understanding of rational cubic forms we will gain insight about integral forms. In the end we will conclude with the law of composition for classes of integral cubic forms of a fixed discriminant, and describe in a new way of looking at Bhargava's original composition law.

Much of this chapter is inspired by the works of Slupinksi and Stanton [**Slupinski-Stanton, Chapter 3.**]. As stated in the previous chapter our convention will be that $D \neq 1$ is an integer which is square free.

3.2 Fundamental Cubic Decomposition

We say a rational cubic form $P(X,Y)$ is a "*triple root*" if $P(X,Y) = a(L(X,Y))^3$ where $L(X,Y)$ is a linear form, i.e. $P(X,Y) = a(bX+cY)^3$ where $a,b,c \in \mathbb{Q}$.

Let D be a fixed discriminant and denote by $K = \mathbb{Q}(\sqrt{D})$ and $G = \mathrm{Gal}(K,\mathbb{Q})$ be the Galois group.

Theorem 3.2.1. *Let $P(X,Y)$ be a rational cubic form of discriminant D. Then we can write,*

$$P(X,Y) = T_1 + T_2$$

where T_j are triple roots with coefficients in K, and $\sigma T_1 = T_2$ where σ is the non-trivial automorphism in G. Furthermore, this decomposition is unique up to the order of the summands. We refer to this decomposition as the "fundamental cubic decomposition".

The proof of this theorem is presented in the paper by Slupinksi and Stanton [**Slupinski-Stanton Thm. 3.27.**]. However, their version is stated a little bit differently from our version.

We define a map $\Psi : \mathrm{sym}^3\mathbb{Q}^2 \to \mathrm{sym}^3\mathbb{Q}^2$ as follows,

given $P = aX^3 + bX^2Y + cXY^2 + dY^3$, we set,

$$\begin{aligned}\Psi(P) = 3\Big[&- a(ad-bc) - 2b(b^2-ac)\Big]X^3 \\ 3\Big[&- 2a(bd-c^2) - b(ad-bc) - 4c(b^2-ac)\Big]X^2Y \\ 3\Big[&- 4b(bd-c^2) + c(ad-bc) - 2d(b^2-ac)\Big]XY^2 \\ 3\Big[&- 2c(bd-c^2) + d(ad-bc)\Big]Y^3\end{aligned}$$

(this map Ψ is essentially the classical cubic covariant)

Then we can construct,

$$T_1 = \frac{1}{2}\left(P + \frac{1}{3\sqrt{D}}\Psi(P)\right) \text{ and } T_2 = \frac{1}{2}\left(P - \frac{1}{3\sqrt{D}}\Psi(P)\right)$$

From here it is immediate that $T_1 + T_2 = P$ and that $\sigma T_1 = T_2$ since $\sigma(\sqrt{D}) = -\sqrt{D}$. The only part which takes work to show is that T_1 and T_2 are indeed triple roots. We do not present the proof here and simply reference the result. The reader who is bothered by this unsupported claim can wait until the end of this section to see a different justification for the fundamental cubic decomposition.

If T is a triple root, then we can write,

$$T(X,Y) = a(bX + cY)^3 = ab^3\left(X + \tfrac{c}{b}Y\right)^3 = \alpha(X + \beta Y)^3$$

where $\alpha = ab^3$ and $\beta = \frac{c}{b}$. With this notation, we can restate **Thm. 3.2.1.** a little bit differently which will be more convenient for us.

Theorem 3.2.2. *Let $P(X,Y)$ be a rational cubic form of discriminant D. Then we can write,*

$$P(X,Y) = \alpha(X + \beta Y)^3 + \overline{\alpha}(X + \overline{\beta}Y)^3$$

where $\alpha, \beta \in K = \mathbb{Q}(\sqrt{D})$ and $\overline{\alpha}, \overline{\beta}$ are the Galois conjugates of α, β under the non-trivial automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Furthermore, this decomposition is unique other than the order of the sum.

We give explicit formulas for the coefficients α and β in **Prop. 3.3.3.** of the following section. Then it is simply a computation to verify that such a decomposition exists!

3.3 Determination of the Decomposition

In the previous section we said that each rational cubic form $P(X,Y)$ has a so-called "*fundamental decomposition*". The previous theorem, **Thm. 3.2.2.**, is existential, it asserts

the existence of such a decomposition, but does not provide much insight on how to find it. In this section we will describe a method for computing the α and β constants in a rather simple way.

As introduced in **Chapter 2**, if P is a rational cubic form we can construct a corresponding quadratic form $H(P)$, which is related to the Hessian of P. The classical Hessian is defined by,

$$\text{classical Hessian of } P(X,Y) = -\frac{1}{36}\begin{vmatrix} P_{XX} & P_{XY} \\ P_{YX} & P_{YY} \end{vmatrix}$$

The quadratic form $H(P)$ which we use is changed where the XY coefficient is replaced by a negative sign, i.e. replace (X,Y) by $(X,-Y)$.

Our first determination is on the constant β.

Proposition. 3.3.1. *Let $P(X,Y)$ be a rational cubic form and $H(X,Y) = H(P)$. Write $P(X,Y)$ in the fundamental cubic decomposition,*

$$P(X,Y) = \alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3.$$

Then, $\beta, \overline{\beta}$ are roots of $H(X,1)$.

Proof. This is one of those results in mathematics where the hard part is to see the statement, but proving it is quite straightforward. Indeed, if we write,

$$P(X,Y) = \alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3$$

then we can compute,

$$P_X = 3\alpha(X+\beta Y)^2 + 3\overline{\alpha}(X+\overline{\beta}Y)^3$$

likewise,

$$P_Y = 3\alpha\beta(X+\beta Y)^2 + 3\overline{\alpha\beta}(X+\overline{\beta}Y)^2$$

continuing in this way we can find P_{XX}, P_{XY}, and P_{YY}. In the end we will obtain,

$$P_{XX}P_{YY} - P_{XY}^2 = -36\alpha^2\beta^2(X + \beta Y)^2$$

Thus, we see that if $X = \beta$ and $Y = -1$, then we see the quantity $= 0$.

This completes the proof. ■

Corollary. 3.3.2. *If* $P(X, Y) = aX^3 + b(3X^2Y) + c(3XY^2) + dY^3$ *then,*

$$\beta = \frac{(ad - bc) \pm \sqrt{D}}{b^2 - ac}$$

where D *is the discriminant of* $P(X, Y)$.

Proof. This follows from observing that,

$$H(P) = (b^2 - ac)X^2 - (ad - bc)XY + (c^2 - bd)Y^2$$

and then the rest follows from observing that if $Y = 1$ then the roots of this polynomial are $\beta, \overline{\beta}$. ■

The next question that remains is how do we determine α?

The α can be determined by equating the coefficients of,

$$P(X, Y) = \alpha(X + \beta Y)^3 + \overline{\alpha}(X + \overline{\beta}Y)^3$$

By equating coefficients in front of X^3 and $3X^2Y$ we find that,

$$\alpha + \overline{\alpha} = a \text{ and } \alpha\beta + \overline{\alpha}\overline{\beta} = b$$

We get that,

$$\alpha\beta + (a - \alpha)\overline{\beta} = b$$

Therefore,

$$\alpha = \frac{1}{2}a + \frac{2b(b^2 - ac) + a(ad - bc)}{2\sqrt{D}}$$

We summarize these observations in a Proposition.

Proposition. 3.3.3. *If* $P = aX^3 + b(3X^2Y) + c(3XY^2) + dY^3$ *then the fundamental cubic decomposition*,

$$P = \alpha(X + \beta Y)^3 + \overline{\alpha}(X + \overline{\beta}Y)^3$$

is given by,

$$\begin{cases} \alpha &= \frac{1}{2}a \pm \frac{2b(b^2-ac)+a(ad-bc)}{2\sqrt{D}} \\ \beta &= \frac{-(ad-bc)\pm\sqrt{D}}{2(b^2-ac)} \end{cases}$$

Where the $\pm$ *sign is a choice arising from the permutation of the order of the summands in the fundamental cubic decomposition.*

For example, if $P(X,Y) = X^3 + 3(3X^2Y) - 6(3X^2Y) - 7Y^3$. The we immediately find that,

$$P(X,Y) = \alpha(X + \beta Y)^3 + \overline{\alpha}(X + \overline{\beta}Y)^3$$

where $\alpha = \frac{1}{2}\boxed{+}\frac{101}{2\sqrt{D}}$ and $\beta = \frac{-11\boxed{+}\sqrt{D}}{30}$ and $D = -3299$. Here we decided to use the $+$ sign in the formula given in **Prop. 3.3.3.**, if we instead used $-$ sign then we will get the same decomposition with the factors reversed.

The above formulas for α and β are quite hideous. A more satisfactory way of looking at those two constants is by rather determining their minimial polynomials. In the case of β the minimal polynomial for β was related to the Hessian. This is a deeper way of seeing β. We can ask what is the minimal polynomial for α? Fortunately, since we have given the explicit formulas above we can apply Viete's formulas for roots to reconstruct the minimal polynomials. We state this next result in the Proposition below.

Proposition. 3.3.4. *Let* $P = aX^3 + b(3X^2Y) + c(3XY^2) + dY^3$ *be a rational cubic form. Then the fundamental decomposition constants* α *and* β *have the following minimal*

polynomials over $\mathbb{Z}$,

$$\begin{cases} \min_\alpha(X) &= DX^2 - aDX - (b^2-ac)^3 \\ \min_\beta(X) &= (b^2-ac)X^2 + (ad-bc)X + (c^2-bd) \end{cases}$$

We can now give a proof, at least for the existence part, of **Thm. 3.2.2.**, if we use the formulas for α and β in **Prop. 3.3.3.**, then when we expand $P(X,Y) = \alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3$ we find that,

$$P(X,Y) = \mathrm{Tr}(\alpha)X^3 + \mathrm{Tr}(\alpha\beta)(3X^2Y) + \mathrm{Tr}(\alpha\beta^2)(3XY^2) + \mathrm{Tr}(\alpha\beta^3)Y^3$$

where $\mathrm{Tr}(\cdot)$ is the trace map for the Galois extension $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$, i.e. more explicitly, the trace map is given by $\mathrm{Tr}(x+y\sqrt{-D}) = 2x$ whenever $x, y \in \mathbb{Q}$.

The reader can now compute the products $\alpha\beta^\ell$ for $\ell = 0, 1, 2, 3$ and then extract the trace map. It will then be evident after a very straightforward (but very tedious computation!), that,

$$\mathrm{Tr}(\alpha) = a,\ \mathrm{Tr}(\alpha\beta) = b,\ \mathrm{Tr}(\alpha\beta^2) = c,\ \mathrm{Tr}(\alpha\beta^3) = d$$

This proves the existence part of **Thm. 3.2.2.**

3.4 Orientation

If we were to use the fundamental cubic decomposition on the cubic form $P(X,Y)$ then we can express $P(X,Y)$ in one of two ways,

$$\alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3 \quad \text{or} \quad \overline{\alpha}(X+\overline{\beta}Y)^3 + \alpha(X+\beta Y)^3$$

It will be important for us to distinguish these two decompositions as different. We will need a way to decide which decomposition to use, i.e. we give each decomposition an "*orientation*".

Definition. 3.4.1. Let $P(X,Y)$ be a cubic form, we say the decomposition,

$$P(X,Y) = \alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3$$

is "*positively oriented*" if $\beta = x + y\sqrt{D}$ with $y > 0$.

Lemma. 3.4.2. *Let $K = \mathbb{Q}(\sqrt{D})$ and $\mathbb{P}^1_K$ the projective line of the field K. Let $\mu : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a Mobius transformation defined by,*

$$\mu(z) = \frac{az+b}{cz+d}$$

where $a,b,c,d \in \mathbb{Z}$ with $ad - bc = 1$. If $\beta = x + y\sqrt{D}$ with $y > 0$ then $\mu(\beta) = x' + y'\sqrt{D}$ with $y' > 0$ also. In other words, integral Mobius transformations map points in the "upper half-plane" to themselves.

Proof. If $D < 0$ then this is a well-known result from complex analysis and conformal mappings. More generally, this is just a matter of computation and verifying that the image point has a positive $\sqrt{D}$ component. ■

One nice property about orientations is that they are preserved under the action of $\mathrm{SL}(2,\mathbb{Q})$, i.e. $\mathrm{SL}(2,\mathbb{Q})$ is an orientation preserving action on the fundamental decomposition of binary cubic forms. More precisely, we have the following result.

Proposition. 3.4.3. *Let $P(X,Y) = \alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3$ be positively oriented and $g = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Q})$. Then,*

$$(P^g)(X,Y) = \alpha(r+t\beta)^3\left(X + \left(\tfrac{s+u\beta}{r+t\beta}\right)Y\right)^3 + \overline{\alpha}(r+t\overline{\beta})^3\left(X + \left(\tfrac{s+u\overline{\beta}}{r+t\overline{\beta}}\right)Y\right)^3$$

is positively oriented.

Proof. If $g = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ then g acts on $P(X,Y)$ by replacing,

X by $rX + sY$ and Y by $tX + uY$.

We obtain that,

$$\begin{aligned}(P^g)(X,Y) &= \alpha\Big(rX+sY+\beta(tX+uY)\Big)^3 + \overline{\alpha}\Big(rX+sY+\overline{\beta}(tX+uY)\Big)^3 \\ &= \alpha(r+t\beta)^3\left(X+\left(\tfrac{s+u\beta}{r+t\beta}\right)Y\right)^3 + \overline{\alpha}(r+t\overline{\beta})^3\left(X+\left(\tfrac{s+u\overline{\beta}}{r+t\overline{\beta}}\right)Y\right)^3 \\ &= \alpha_0(X+\beta_0 Y)^3 + \overline{\alpha_0}(X+\overline{\beta_0}Y)^3\end{aligned}$$

It remains to show that this particular ordering of the decomposition is positively oriented.

To that end consider the Mobius transformation $f(z) = \frac{uz+s}{tz+r}$. This is a Mobius transform since $ur - st = 1$. Furthermore, β is in the upper half-plane, since, in the hypothesis of the Proposition, $P(X,Y)$ was written with a positive orientation. Since $\beta_0 = f(\beta)$, and β is in the upper half-plane, it means, by **Lem. 3.4.2.**, β_0 is also in the upper half-plane. Thus, β_0 is also in the upper half-plane, hence the fundamental cubic decomposition for $(P^g)(X,Y)$ is positively oriented in the way it is currently written. ■

3.5 The Elliptic Map

In this section the discriminant $D < 0$ is fixed. We define the following set,

$$G_D = \{(x,y) \in \mathbb{Q}\times\mathbb{Q} \mid x^2 - Dy^2 = 1\}$$

Geometrically G_D is the ellipse in the plane consisting of rational points.

There is a group structure on G_D. Namely,

$$(x_1,y_1)\cdot(x_2,y_2) = (x_1x_2 + Dy_1y_2\ ,\ x_1y_2 + x_2y_1)$$

This group structure on G_D is not anything new. This is essentially the group structure defined in §1.1.2 on $\mathbb{Q}_D^\times$.

If $P(X,Y)$ is a rational cubic form with discriminant D we define $I_D(P)$ to be,

$$I_D(P) = \frac{\alpha}{\overline{\alpha}}$$

where α is the constant determined from §3. This map $I_D(\cdot)$ was first introduced by Slupinski and Stanton [**Slupinski-Stanton, Chapter 3**], we slightly modify it in our paper for our purposes. There is a little bit of ambiguity in how $I_D(P)$ is defined. Since, as we seen in §3, the constant α is unique up to a complex conjugate. If we use $\overline{\alpha}$ instead then we will get the reciprocal of $I_D(P)$. This ambiguity will be dealt by using the *positive orientation* of the fundamental cubic decomposition. This choice eliminates the ambiguity in how $I_D(P)$ is defined.

The quantity $I_D(P)$ essentially assigns to a cubic form of discriminant D a point on the ellipse G_D. More precisely we have the following statement.

Proposition 3.5.1. *Let $P(X,Y)$ be a rational binary cubic form of discriminant D.*

If $I_D(P) = x + y\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ then $(x,y) \in G_D$.

Proof. We have,

$$I_D(P) = \frac{\alpha}{\overline{\alpha}}$$

by definition of $I_D(\cdot)$. Since $\alpha \in \mathbb{Q}(\sqrt{D})$ and $D < 0$, α is a complex number. Thus, α divided by its conjugate will lie on the unit circle and have absolute value equal to 1. Thus, if we write $I_D(P) = x + y\sqrt{D}$, then the absolute value of this quantity is equal to $x^2 - Dy^2$, which we said is equal to 1. This shows that $(x,y) \in G_D$ and completes the proof. ■

We also have an explicit formula for $I_D(P)$.

Proposition 3.5.2. *If $P = aX^3 + b(3X^2Y) + c(3XY^2) + dY^3$ then $I_D(P)$ satisfies the*

polynomial equation,

$$X^2 - \left(2 - \frac{(a^2d - 3abc + 2b^3)^2}{(b^2 - ac)^3}\right) X + 1 = 0$$

and its sign, from the quadratic formula, is determined by the sign of $b^2 - ac$.

Proof. This is an immediate computation which follows from formulas in §3. ■

Since we will be dealing with classes of cubic forms it is reasonable to ask how I_D acts on a different form which is equivalent to P. This is the motivation for the next proposition. The following proposition appears in Slupinski's and Stanton's paper [**Slupinski-Stanton, Thm. 3.33**] in a more general context over an arbitrary field of characteristic not 2 nor 3. The version in this paper is more specific to our needs.

Proposition 3.5.3. *If* $I_D(P) = \varepsilon \in \mathbb{Q}(\sqrt{D})$ *and* $g \in \mathrm{SL}(2, \mathbb{Q})$ *then*,

$$I_D(P^g) = \varepsilon \cdot \gamma^3 \quad \text{for some} \quad \gamma \in \mathbb{Q}(\sqrt{D})$$

Proof. We can write, using the fundamental decomposition theorem,

$$P(X, Y) = \alpha(X + \beta Y)^3 + \overline{\alpha}(X + \overline{\beta} Y)^3$$

Say that g is given by the matrix,

$$g = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

By acting g on the cubic form $P(X, Y)$ we get a new form,

$$(P^g)(X, Y) = \alpha\Big(rX + sY + \beta(tX + uY)\Big)^3 + \overline{\alpha}\Big(rX + sY + \overline{\beta}(tX + uY)\Big)^3$$

$$= \alpha(r + t\beta)^3 \left(X + \left(\tfrac{s+u\beta}{r+t\beta}\right)\right)^3 + \overline{\alpha}(r + t\overline{\beta})^3 \left(X + \left(\tfrac{s+u\overline{\beta}}{r+t\overline{\beta}}\right)\right)^3$$

By **Prop. 3.4.3.**, this cubic decomposition of P^g is *positively oriented*.

Set $\gamma = \frac{r+t\beta}{r+t\overline{\beta}}$. We therefore see that,

$$I_D(P^g) = \frac{\alpha(r+t\beta)^3}{\alpha(r+t\overline{\beta})^3} = \frac{\alpha}{\overline{\alpha}} \cdot \gamma^3 = \varepsilon\gamma^3$$

This completes the proof. ■

In what follows next we will show that the converse of **Prop. 3.5.3.** is also true! Generally showing that two cubic forms are equivalent is not easy. The invariant $I_D(\cdot)$ is able to completely detect the cubic class. Before we are able to prove this result, however, we need an extremely convenient formula which *links* the two constants α and β, as well as the discriminant, into a single equation. We will refer to this equation as the "*link equation*" and will reference it a few times in this paper. The inspiration of this equation is derived from Slupinski and Stanton's work, [**Slupinski-Stanton, Thm. 3.27**]. The version of the "*link equation*" in their paper is very different from ours. We present a different approach which can be proven from the formulas that we developed in the earlier sections.

Proposition 3.5.4. *If $P(X,Y)$ is a positively oriented cubic form then,*

$$\alpha\overline{\alpha}(\beta - \overline{\beta})^3 = -\sqrt{D}$$

Proof. This is again one of those situations where finding the formula is the hard part but proving it is straightforward. Indeed, by using the formulas from §3 for α and β this identity is immediate. ■

We also need to get a silly Lemma out of a way which is true for any field K. In our application, of course, K will be chosen to be $K = \mathbb{Q}(\sqrt{D})$.

Lemma 3.5.5 *If K is a field and $x, y \in K$ are such that $x^2 = y^3$ then,*

x is a cube (in K) and y is a square (in K).

Proof. Without lose of generality we can assume x and y are non-zero.

We can write, $x^3 = xy^3$ from which it follows that $x = \left(\frac{x}{y}\right)^3$.

Likewise, $x^2 = yy^2$ from which it follows that $y = \left(\frac{x}{y}\right)^2$. ■

We can now prove the converse of **Prop. 3.5.3.**.

Proposition 3.5.6. *Let $P(X,Y)$ and $P_0(X,Y)$ be two cubic forms such that $I_D(P) = I_D(P_0)\cdot\gamma^3$ for some $\gamma \in \mathbb{Q}(\sqrt{D})$ then P and P_0 are equivalent cubic forms, i.e. there exists $g \in \mathrm{SL}(2,\mathbb{Q})$ such that $P^g = P_0$.*

Proof. Let α, β be the two constants associated to $P(X,Y)$ as in §2, and likewise use the same notation for α_0, β_0. We can assume, without lose of generality, that $\beta = \beta_0$, since we can always find a $g = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Q})$ such that $\frac{s+u\beta}{r+t\beta} = \beta_0$. Then P^g will be a new form which will have its β constant equal to β_0, just like P_0. We will, from now on, assume this simplifying assumption.

Since $I_D(P) = I_D(P_0)\cdot\gamma^3$ it means that,

$$\frac{\alpha}{\overline{\alpha}} = \frac{\alpha_0}{\overline{\alpha_0}}\cdot\gamma^3$$

Now, by using the Link Equation in **Prop. 3.5.4.**, we can say that,

$$\alpha\overline{\alpha}(\beta-\overline{\beta})^3 = -\sqrt{D} = \alpha_0\overline{\alpha_0}(\beta_0-\overline{\beta_0})^3$$

However, $\beta = \beta_0$ and so we conclude that $\alpha\overline{\alpha} = \alpha_0\overline{\alpha_0}$.

Thus, we obtain,

$$\frac{\alpha}{\overline{\alpha}}\cdot\frac{\alpha}{\alpha} = \frac{\alpha_0}{\overline{\alpha_0}}\cdot\frac{\alpha_0}{\alpha_0}\cdot\gamma^3$$

Thus, by using the previous equation, $\alpha\overline{\alpha} = \alpha_0\overline{\alpha_0}$, this simplifies to,

$$\alpha^2 = \alpha_0^2\gamma^3 \implies \left(\frac{\alpha}{\alpha_0}\right)^2 = \gamma^3$$

From **Lem. 3.5.5.**, we obtain that $\alpha_0 = \alpha\delta^3$ for some $\delta \in \mathbb{Q}(\sqrt{D})$.

Now choose rational numbers r, s, t, u such that,

$$\frac{s+u\beta}{r+t\beta} = \beta \quad r + t\beta = \delta \quad ru - st = 1$$

This is possible since there are 3 equations and 4 degrees of freedom.

Then, if we set,

$$g = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

then $g \in \mathrm{SL}(2, \mathbb{Q})$ and it will satisfy the requirement that $P^g = P_0$.

This completes the proof of this Proposition. ■

Given a cubic form P we saw, from **Prop. 3.5.1.**, that $I_D(P) = x + y\sqrt{D}$ and the pair (x, y) lies on the ellipse G_D. A reasonable question to ask if every point of the ellipse G_D can be obtained as the image of $I_D(\cdot)$ in such a manner? The answer is yes (also see, [**Slupinski-Stanton Theorem 3.33**]). This is the next Proposition. However, we do have to be careful, since by the orientation convention the way we pick α will force $I_D(P)$ to always be in the upper half of the ellipse G_D.

Proposition 3.5.7. *Let $(x, y) \in G_D$ with $y > 0$. There exists a cubic form $P(X, Y)$ such that $I_D(P) = x + y\sqrt{D}$.*

Proof. If α, β are the two constants which come from the fundamental cubic decomposition of $P(X, Y)$ then we have that,

$$\frac{\alpha}{\overline{\alpha}} = x + y\sqrt{D}$$

If $\alpha = a + b\sqrt{D}$ then by solving the above equation we find that,

$$\alpha = -tyD + t(1 - x)\sqrt{D}$$

where t is an arbitrary positive rational number t.

A simple computation will show now that,

$$\alpha\overline{\alpha} = 2t^2D(x-1)$$

From the Link Equation, $\alpha\overline{\alpha}(\beta-\overline{\beta})^3 = -\sqrt{D}$, we obtain,

$$2t^2D(x-1)(\beta-\overline{\beta})^3 = -\sqrt{D}$$

If we denote $\beta = c + d\sqrt{D}$ then $\beta - \overline{\beta} = 2d\sqrt{D}$, thus,

$$16t^2D^2(1-x)d^3 = 1 \implies d^3 = \frac{1}{(4tD)^2(1-x)}$$

Now $1-x$ is a rational number between -1 and 1. Regardless of what rational number we pick we can always find a rational number t such that $(4tD)^2(1-x)$ is a perfect rational cube. This is easy to see by a prime factorization argument. Thus, if we pick t in such a way, then d can be solved for by taking the cube root. Thus, d and t exist which make the above equation solvable in terms of rational numbers. Then we simply set $\alpha = -tyD + t(1-x)\sqrt{D}$ and $\beta = c + d\sqrt{D}$ where c is completely arbitrary. With such choices we will then have that

$$P(X,Y) = \alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3$$

will be a cubic form of discriminant D such that $I_D(P) = x + y\sqrt{D}$. ■

It is helpful to summarize what we have said so far up to this point. We observed that if P and P_0 are equivalent cubic forms then $I_D(P)$ and $I_D(P_0)$ are the same up to a cube factor of $\mathbb{Q}(\sqrt{D})$. Conversely, if P and P_0 are cubic forms such that $I_D(P)$ and $I_D(P_0)$ are the same up to a cube factor then P and P_0 are equivalent. Since we wish to be working with classes of rational cubic forms of discriminant D we will identify them as being equivalent on the ellipse G_D. The following map, which we call the *elliptic map*, is now defined.

Definition 3.5.8. Define a map $\varphi_D : \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D) \to G_D/G_D^3$ by the rule,

$$\varphi_D([P]_{\mathbb{Q}}) = [I_D(P)]_D$$

where $[P]_{\mathbb{Q}}$ denotes the class of P in $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ and $[*]_D$ denotes the class of $*$ in the quotient group G_D/G_D^3 (here G_D^3 denotes the sub-group of all cubes in G_D).

Proposition 3.5.9. *The elliptic map φ_D satisfies the following properties*:

(i) *φ_D is well-defined.*

(ii) *φ_D is injective.*

(iii) *φ_D is surjective.*

Proof. We have proven all of these facts already. For **(i)** we did so in **Prop. 3.5.3.**, for **(ii)** we did so in **Prop. 3.5.6.**, and for **(iii)** we almost did so in **Prop. 3.5.7.**. For **(iii)** what we shown is that if $(x, y) \in G_D$ and $y > 0$ then we can find P such that $I_D(P) = x + y\sqrt{D}$. However, if $y < 0$ then we simply take advantage of the fact that $x + y\sqrt{D}$ is equivalent to $-x - y\sqrt{D}$ since $(-1) = (-1)^3 \in G_D^3$, so $x + y\sqrt{D}$ is equivalent to its negative mod the subgroup G_D^3 (also see [**Slupinski-Stanton Thm. 3.33**]).■

Since we have a bijective correspondence between $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ and G_D/G_D^3 we can transport the group structure by the elliptic map to equip $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ with a group structure.

Definition 3.5.10. We define the law of composition on $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ by transport of structure via the elliptic map φ_D with the group G_D/G_D^3. This defines a group law for equivalence classes of rational cubic forms of discriminant D.

We can now restate **Thm. 2.5.1.**.

Theorem 3.5.10. *The composition law provided in* **Def. 3.5.10.** *for* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ *defines a composition such that the natural map,* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$, *given*

by **Prop. 2.4.2.**, *is a homomorphism of commutative groups.*

We will prove this Theorem and its consequences later in this paper, see **Cor. 3.7.4.**.

3.6 The Hyperbolic Map

In §5 we assumed that $D < 0$, the resulting group

$$G_D = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x^2 - Dy^2 = 1\}$$

was geometrically an ellipse. However, we only assumed that $D < 0$ to make the proofs "simpler", i.e. since we can reference properties of complex numbers. Fortunately, the same conclusions hold forth for $D > 0$, instead we need to supply a more algebraic proof as opposed to complex analytic.

If $D > 0$ we likewise define G_D in the same manner, except, geometrically G_D looks like a hyperbola. Just as before we have the map $I_D(\cdot)$ from cubic forms of discriminant D to points on the hyperbola G_D. Word-for-word we get the following analogue of **Prop. 3.5.9.**, which we state below.

Proposition 3.6.1. *Define the following map,* $\varphi_D : \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D) \to G_D/G_D^3$ by the rule,

$$\varphi_D([P]_{\mathbb{Q}}) = [I_D(P)]_D$$

where $[P]_{\mathbb{Q}}$ *denotes the class of* P *in* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ *and* $[*]_D$ *denotes the class of* $*$ *in the quotient group* G_D/G_D^3 (*here* G_D^3 *denotes the sub-group of all cubes in* G_D). *We call this map the "hyperbolic map", and it satisfies the properties*:

(i) φ_D *is well-defined.*

(ii) φ_D *is injective.*

(iii) φ_D *is surjective.*

As before in §5, by transport of structure, we get a group structure on $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$. The same analogue of **Thm. 3.5.10.** will be true in this case as well when $D > 0$.

Thus, algebraically speaking, whether $D > 0$ or $D < 0$, it does not matter, the computations and the propositions are all the same. The same map φ_D is used to establish an isomorphism between cubic classes of forms and points of the group G_D/G_D^3. The only thing that changes is how we visualize the groups G_D. From now on we will not care whether D is a positive or negative integer and just work more generally.

3.7 Relationship between Integral and Rational Cubic Forms

Let us start by giving a different description for the group $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$. Recall our notation that $K = \mathbb{Q}(\sqrt{D})$ and $\mathbb{Z}_K$ denotes the ring of integers of K. We denote by $\mathrm{Cl}^+(\mathbb{Z}_K)$ the narrow class group. We saw, in §1.1, there is an isomorphism between $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$ and $\mathrm{Cl}^+(\mathbb{Z}_K)$. In this section we will establish a similar isomorphism for $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$ instead.

Definition 3.7.1. We denote by $\mathrm{Cl}_3^+(\mathbb{Z}_K)$ to be the group of all equivalence classes of (I, δ) where $I \in \mathrm{ideal}(\mathbb{Z}_K)$ is a fractional ideal, $\delta \in K$, with the condition that $I^3 \subseteq \delta\mathbb{Z}_K$ and $N(I)^3 = N(\delta)$ where $N(\cdot)$ denotes the ideal-norm map. Two pairs (I, δ) and (J, η) are equivalent if one is a non-zero scalar multiple of another.

Here is the analogue of **Thm. 1.1.6.** for cubic forms instead.

Theorem. 3.7.2. *There is an isomorphism between* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$ *and* $\mathrm{Cl}_3^+(\mathbb{Z}_K)$.

Proof. Let us introduce the map $\pi : K \to \mathbb{Q}$ given by,

$$\pi(z) = \frac{z - \overline{z}}{\sqrt{D}}$$

this map is simply the projection onto the radical component.

Given an ideal-pair (I, δ) we explain how to correspond a cubic form. This will, in turn, descend to a map between equivalence classes and define a mapping correspondence between $\mathrm{Cl}_3^+(\mathbb{Z}_K)$ and $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$. To that end, write $I = \langle \alpha, \beta \rangle$, as an ideal generated by non-zero $\alpha, \beta \in K$. Construct the following cubic form,

$$P(X, Y) = \pi \left(\frac{(\alpha X + \beta Y)^3}{\delta} \right)$$

This correspondence will establish an isomorphism from $\mathrm{Cl}_3^+(\mathbb{Z}_K)$ onto $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$. The verification that this correspondence is a well-defined isomorphism is an known result [**Bhargava**, **Thm. 13**]. We refer the reader to the complicated details of the proof. ■

In §5 and §6 we established an isomorphism between $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ and G_D/G_D^3. We also have the natural map $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$. It is reasonable to ask what is the corresponding map between $\mathrm{Cl}_3^+(\mathbb{Z}_K)$ and G_D/G_D^3. The answer is settled in the following theorem.

Theorem. 3.7.3. *The following diagram is a commutative of commutative groups,*

$$\begin{array}{ccc} \mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) & \longrightarrow & \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D) \\ \simeq\downarrow & & \downarrow\simeq \\ \mathrm{Cl}_3^+(\mathbb{Z}_K) & \longrightarrow & G_D/G_D^3 \end{array}$$

where the upper-horizontal map is the natural map given in ***Prop. 2.3.2.****, the left-vertical map is the isomorphism of* ***Thm. 3.7.2.****, the right-vertical map is the isomorphism of* ***Prop. 3.6.1.****, and the lower-horizontal map is defined by,*

$$[(I, \delta)] \mapsto \left[\frac{\delta}{\overline{\delta}} \right]$$

(strictly speaking, the quantity $\frac{\delta}{\overline{\delta}}$ is in the field K and of norm 1, not on the conic G_D. However, if we separate the two components (x, y) of this quantity then it will lie on the conic $x^2 - Dy^2 = 1$. We are using this abuse of notation for simplicity.)

Proof. Let us start with the observation that the lower-horizontal map is well-defined. If (I, δ) and (J, η) are equivalent then there exists an $\varepsilon \in K^\times$ such that $\delta = \varepsilon^3 \eta$. Thus, (I, δ) will get mapped to $\frac{\eta}{\overline{\eta}} \cdot \left(\frac{\varepsilon}{\overline{\varepsilon}}\right)^3$, which is equivalent to $\frac{\eta}{\overline{\eta}}$ in the group G_D/G_D^3.

We next check that this diagram is commutative. Let $P(X, Y)$ be a representative class in $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$. The difficulty in determining the image of $P(X, Y)$ by the left-vertical map lies in the fact that this is the inverse map of the one given in proof of **Thm. 3.7.2.**. Fortunately, for us we can easily find it by using the fundamental cubic decomposition,

$$P(X, Y) = \alpha(X + \beta Y)^3 + \overline{\alpha}(X + \overline{\beta} Y)^3$$

We claim that the a representative for the corresponding ideal-pair in $\mathrm{Cl}_3^+(\mathbb{Z}_K)$ is given by,

$$\left(\langle 1, \beta \rangle, \frac{1}{\alpha\sqrt{D}}\right)$$

if we are willing to accept this claim for the time being the remainder of the proof is soon over. Indeed, cascading this ideal-pair by the lower-horizontal map we get the point,

$$\frac{\alpha\sqrt{D}}{\overline{\alpha\sqrt{D}}} = -\frac{\alpha}{\overline{\alpha}} \in G_D/G_D^3$$

Let us check that the same result occurs when we apply the composing maps along the other side of the diagram. If we start with $P(X, Y)$ then a representative image in $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$ is quite simply itself. Cascading with the left-vertical map we obtain the representative conic point $\frac{\alpha}{\overline{\alpha}}$. At first it seems that something is wrong as we get a negative answer but this is settled by recalling that conic points in G_D/G_D^3 are equivalent up to a cubic factor, in our case $(-1)^3 = (-1)$. This establishes that the diagram is indeed commutative.

The only remaining part is to justify that the appropriate ideal-pair corresponding to $P(X, Y)$ is given by what we wrote above. To that end, we need to verify the conditions

that,

$$\pi\left(\frac{(X+\beta Y)^3}{\left(\frac{1}{\alpha\sqrt{D}}\right)}\right) = P(X,Y)$$

the condition that,

$$\langle 1,\beta\rangle^3 \subseteq \left(\frac{1}{\alpha\sqrt{D}}\right)\mathbb{Z}_K$$

and finally the condition that,

$$N\Big(\langle 1,\beta\rangle\Big)^3 = N\left(\frac{1}{\alpha\sqrt{D}}\right)$$

To verify the first condition we expand,

$$\pi(\alpha\sqrt{D}(X+\beta Y)^3) = \frac{\alpha\sqrt{D}(X+\beta Y)^3 - \overline{\alpha}\overline{\sqrt{D}}(X+\overline{\beta}Y)^3}{\sqrt{D}} = \alpha(X+\beta Y)^3 + \overline{\alpha}(X+\overline{\beta}Y)^3$$

This polynomial is $P(X,Y)$ from the fundamental cubic decomposition!

The second condition is simply equivalent to,

$$\alpha\sqrt{D}\left\langle 1,\beta,\beta^2,\beta^3\right\rangle \subseteq \mathbb{Z}_K$$

It is sufficient then to show that $\alpha\beta^\ell\sqrt{D} \in \mathbb{Z}_K$ for $\ell = 0,1,2,3$. This is a straightforward computation by using the explicit formulas in **Prop. 3.3.3.** and the well-known fact [**Cohen**] that $\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ (recall our convention that D is square-free).

The second condition computation will require us to compute the norm of the ideal $\langle 1,\beta\rangle$. By using the formula as we did in the proof of **Thm. 1.3.3.** we find that,

$$N\Big(\langle 1,\beta\rangle\Big) = \frac{1}{\sqrt{D}}|\beta - \overline{\beta}|$$

By convention the fundamental cubic decomposition is oriented according to **Def. 3.3.1.** we can omit the absolute value and conclude that,

$$N\Big(\langle 1,\beta\rangle\Big)^3 = \frac{1}{D\sqrt{D}}(\beta - \overline{\beta})^3$$

Therefore, the second verification comes down to the equation,

$$\frac{1}{D\sqrt{D}}(\beta-\overline{\beta})^3=\frac{1}{-\alpha\overline{\alpha}D}\iff \alpha\overline{\alpha}(\beta-\overline{\beta})^3=-\sqrt{D}$$

But this is the *link equation* of **Prop. 3.5.4.**! With these two computations verified the argument is complete. ■

We have some immediate corollaries from this theorem. The first is **Theorem. 3.5.10.** and much more than that.

Corollary 3.7.4. *The natural map* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2,D)\to\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2,D)$ *is a homorphism of groups. Furthermore, this is an injective map so it embeds* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2,D)$ *as a subgroup of* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2,D)$.

Proof. The fact that this map is homomorphism follows from the commutative diagram. The upper-horizontal natural map can be factored as a product of three group homomorphisms, as such, it is a homomorphism. The fact that the natural map is injective was proven in **Cor. 2.4.2.** ■

3.8 Law of Composition for Integral Cubic Forms

We are now in position to finally state the law of composition for integral cubic forms as in **Thm. 2.2.1.** by giving a more explicit manner in how this composition law actually works for explicitly given cubic forms.

Theorem 3.8.1. *Let* $\mathcal{S}=\{P_1,P_2,...,P_n\}$ *be an set of representatives for* $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2,D)$. *Each cubic* P_i *corresponds to a point* p_i *on the conic* G_D *via the map* $I_D(P_i)$. *For every* i,j *with* $1\le i,j\le n$ *there exists a unique* $1\le k\le n$ *such that* $p_ip_j=p_k\omega^3$ *for some* $\omega\in\mathbb{Q}(\sqrt{D})$. *We then have that* $[P_i]_{\mathbb{Z}}+[P_j]_{\mathbb{Z}}=[P_k]_{\mathbb{Z}}$.

Proof. If we apply the map $I_D(\cdot)$, from §4, on each of these cubic forms P_i we will get

a number $I_D(P_i) = x_i + y_i\sqrt{D} \in \mathbb{Q}(\sqrt{D})$. The coordinate $p_i = (x_i, y_i)$ will be a point on the rational conic G_D (recall, that G_D is a an ellipse when $D < 0$ and a hyperbola when $D > 0$, but we will simply just refer to it as a conic). Every cubic form in our set $\mathcal{S}$ will correspond to a point p_i on the conic G_D.

Pick two classes of cubic forms $[P_i]_{\mathbb{Z}}$ and $[P_j]_{\mathbb{Z}}$. The composition of these two classes will be another class $[P_k]_{\mathbb{Z}}$. If we replace $\mathbb{Z}$ by $\mathbb{Q}$, i.e. think of these forms are rational forms, then $[P_i]_{\mathbb{Q}} + [P_j]_{\mathbb{Q}} = [P_k]_{\mathbb{Q}}$ by **Cor. 3.7.4.**. It now follows by the Slupinkski-Stanton composition law that we have $[p_i] \cdot [p_j] = [p_k]$ within the quotient group G_D/G_D^3.

Thus, given i and j, there exists a k, such that $[p_i p_j] = [p_k]$. But the crucial observation is that this integer k must be unique! For if ℓ was another integer and $[p_i p_j] = [p_\ell]$ then it will mean that $[p_k] = [p_\ell]$, in particular, we will have $[P_k]_{\mathbb{Q}} = [P_\ell]_{\mathbb{Q}}$. By the injectivity of the homomorphism $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D) \to \mathrm{Cl}(\mathrm{sym}^3\mathbb{Q}^2, D)$, by **Cor. 3.7.4.** again, we conclude that $[P_k]_{\mathbb{Z}} = [P_\ell]_{\mathbb{Z}}$, and so $P_k = P_\ell$. Hence such a k is unique.

To summarize, given P_i and P_j, these correspond to points p_i and p_j on the conic G_D. There exists a unique k such that $p_i p_j$ is equivalent to p_k mod G_D^3, i.e. $p_i p_j = p_k \omega^3$ for some $\omega \in G_D$. This p_k is precisely the point which corresponds to the cubic form P_k. Thus, the composition $[P_i]_{\mathbb{Z}} + [P_j]_{\mathbb{Z}}$ is determined to be $[P_k]_{\mathbb{Z}}$. ■

It may be helpful to illustrate this Theorem with a specific example. The author expresses much gratitude to Prof. Takashi Taniguchi [**Taniguchi**] who provided a large table of classes of integral cubic forms which allowed the author to perform computations to aid in this research.

For example, let $D = 257$, this is a square-free integer, in fact it happens to be a prime, but this is all irrelevant. From the known reduction theory of cubic forms there are 9 classes.

We will use the compact notation (a, b, c, d) to represent the cubic form,

$$aX^3 + b(3X^2Y) + c(3XY^2) + dY^3$$

Here is a representative set for these nine classes for $D = 257$,

Name	Form	Conic Point
E	$(0, 1, 1, 65)$	$(-1, 0)$
P_1	$(1, -2, 2, -13)$	$\left(-\frac{273}{16}, \frac{17}{16}\right)$
P_2	$(1, 0, 4, 1)$	$\left(\frac{129}{128}, -\frac{1}{128}\right)$
P_3	$(2, 1, 1, 9)$	$(513, -32)$
P_4	$(1, 1, 3, 22)$	$\left(\frac{241}{16}, -\frac{15}{16}\right)$
Q_1	$(1, 2, 2, 13)$	$\left(-\frac{273}{16}, -\frac{17}{16}\right)$
Q_2	$(1, 0, 4, -1)$	$\left(\frac{129}{128}, \frac{1}{128}\right)$
Q_3	$(2, -1, 1, -9)$	$(513, 32)$
Q_4	$(1, -1, 3, -22)$	$\left(\frac{241}{16}, \frac{15}{16}\right)$

Each rational conic point will lie on the hyperbola $x^2 - 257y^2 = 1$. Observe that the form P_3 corresponds to the point $(513, 32)$, an integral point of the hyperbola, i.e. it solves Pell's equation. However, the other integral cubic forms do not correspond to integral points. Thus, integral cubic forms do not necessarily correspond to solutions of Pell's equation, in fact they usually do not.

Since the cubic form E corresponds to the point $(-1, 0)$ it means that E is a representative for the identity class, indeed -1 is a perfect cube in $\mathbb{Q}(\sqrt{257})$ since $-1 = (-1)^3$. Let us now look at a few computations.

If we take the forms P_1 and P_2 and denote by p_1 and p_2 their corresponding points on the conic G_{257} then p_1p_2 will be equal to $\left(-\frac{241}{16}, \frac{15}{16}\right)$. This point is the negative of the point corresponding to Q_4. Thus, $p_1p_2 = -q_4$. However, as we said above, (-1) is a perfect cube in our field, and so p_1p_2 is equivalent to q_4 modulo the cubes. Therefore, we have determined that $[P_1]_{\mathbb{Z}} + [P_2]_{\mathbb{Z}} = [Q_4]_{\mathbb{Z}}$.

As another example, we can see that $p_1p_3 = -p_4$. Therefore, for the reasons as we said above, this implies that $[P_1]_{\mathbb{Z}} + [P_3]_{\mathbb{Z}} = [P_4]_{\mathbb{Z}}$.

We also see that $p_k q_k = (1, 0)$ for every $1 \leq k \leq 4$. Since $(1, 0)$ represents the identity class in the quotient group we conclude that $[P_k]_{\mathbb{Z}}$ and $[Q_k]_{\mathbb{Z}}$ are inverses, i.e. $[P_k]_{\mathbb{Z}} + [Q_k]_{\mathbb{Z}} = [E]_{\mathbb{Z}}$.

Finally, consider P_2 and P_3. We see that $p_2 \cdot p_3 = \left(\frac{74401}{128}, \frac{4641}{128}\right)$. This is not on the list of points in our table above. However, this is not a problem. Since this new point is equivalent to one of the points on our list. Indeed, a computation will show that $p_2 p_3 = p_1 \omega^3$ where $\omega = \left(-\frac{273}{16}, -\frac{17}{16}\right)$. Thus, we have determined that $[P_2]_{\mathbb{Z}} + [P_3]_{\mathbb{Z}} = [P_1]_{\mathbb{Z}}$.

We can now carry out this procedure between any two pairs of forms and determine what their composition is. These examples illustrate what **Thm. 3.8.1.** is saying about the law of composition.

3.9 The View from High Above

In this final section of Chapter 3 we will summarize the main idea of everything that we said. There are many formulas in this Chapter and it is easy to get lost of what is really going on on a deeper level.

One should compare **Prop. 1.4.1.** with **Thm. 3.8.1.**. The earlier proposition from Chapter 1 is the analogue of **Thm 3.8.1.**, with one big difference, there is an assumption being made on the natural map being injective. This is not usually true, even if D is square-free. With the case of cubic forms the situation is much better behaved.

Thus, quite simply, working over $\mathbb{Q}$ is easier than working over $\mathbb{Z}$, however, in the case of quadratic forms we lose information (from the non-injectivity of the natural homomorphism). In contrast with cubic forms were there is no lose of information. Thus, we can "*understand*" integral cubic forms by thinking of them rationally instead.

Chapter 4

Binary Cubic Forms of a Squared Discriminant

4.1 Introduction

We have assumed that the discriminant D is square-free. In this chapter we consider the extreme case when D is a perfect square. We will write $D = \Delta^2$. For simplicity our assumption will be that Δ is a positive odd number not divisible by three.

The main goal of this chapter is to study the group $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, \Delta^2)$.

4.2 Fundamental Cubic Decomposition Revisited

In **Chapter 3** we saw that if $P(X, Y)$ is a cubic form of discriminant D then we can write,

$$P(X, Y) = \alpha_1\lambda_1^3 + \alpha_2\lambda_2^3$$

where $\alpha_j \in K = \mathbb{Q}(\sqrt{D})$ and $\lambda_j \in \mathrm{sym}^1 K^2$ are linear forms over K. The "*link equation*" said that if the cubic decomposition is chosen such that $\lambda_j = X + \beta_j Y$ then,

$$\alpha_1\alpha_2(\beta_1 - \beta_2)^3 = \pm\sqrt{D}$$

where the $\pm$ sign is determined by the orientation of the cubic decomposition.

In this section we will generalize the link equation which will be more convenient for us. First we will need to introduce some notation.

Definition 4.2.1. Let $\lambda_1, \lambda_2 \in \mathrm{sym}^1 K^2$ be a pair of linear forms over $K = \mathbb{Q}(\sqrt{D})$. Write $\lambda_j = \varepsilon_j X + \theta_j Y$. We denote by $\omega(\lambda_1, \lambda_2)$ to be the quantity,

$$\omega(\lambda_1, \lambda_2) = \det \begin{bmatrix} \varepsilon_1 & \theta_1 \\ \varepsilon_2 & \theta_2 \end{bmatrix} = \varepsilon_1\theta_2 - \theta_1\varepsilon_2$$

Using this notation we can generalize the link equation.

Proposition 4.2.2. *Let $P(X, Y)$ be a cubic form of discriminant D. Write,*

$$P = \alpha_1\lambda_1^3 + \alpha_2\lambda_2^3$$

such that $\alpha_j \in K$ and $\lambda_j \in \mathrm{sym}^1 K^2$. We have the following link equation,

$$\alpha_1\alpha_2\ \omega(\lambda_1, \lambda_2)^3 = \pm\sqrt{D}$$

Proof. If λ_j both have the special form $\lambda_j = X + \beta_j Y$ then $\omega(\lambda_1, \lambda_2) = (\beta_2 - \beta_1)$, so this equation simply follows from the original link equation. More generally say $\lambda_j = \varepsilon_j X + \eta_j Y$. We need to show that,

$$\alpha_1\alpha_2(\varepsilon_1\eta_2 - \varepsilon_2\eta_1)^3 = \pm\sqrt{D}$$

To that end, write,

$$P = \alpha_1\varepsilon_1^3\hat{\lambda}_1^3 + \alpha_2\varepsilon_2^3\hat{\lambda}_2^3$$

where $\hat{\lambda}_j = X + \frac{\eta_j}{\varepsilon_j}Y$. From the special case we get,

$$\alpha_1\varepsilon_1^3\alpha_2\varepsilon_2^3\left(\tfrac{\eta_1}{\varepsilon_1} - \tfrac{\eta_2}{\varepsilon_2}\right)^3 = \pm\sqrt{D} \implies \alpha_1\alpha_2(\varepsilon_1\eta_2 - \varepsilon_2\eta_1)^3 = \pm\sqrt{D}$$

This completes the proof. ■

In this entire chapter we will be assuming that $D = \Delta^2$ where Δ is as mentioned at the start of the chapter. The fundamental cubic decomposition will be stated different from how

it was in **Chapter 3**. This new way of decomposing a cubic form will be more convenient in this chapter.

Proposition 4.2.3. *If $P(X,Y)$ is a cubic form of discriminant $D = \Delta^2$ then we can write, in a unique way,*

$$P = \frac{s_1}{2\Delta}\lambda_1^3 + \frac{s_2}{2\Delta}\lambda_2^3$$

such that,

(i) *s_1, s_2 are positive integers*

(ii) *$\lambda_j \in \mathrm{sym}^1\mathbb{Z}^2$, i.e. $\lambda_j = n_jX + m_jY$ with $n_j, m_j \in \mathbb{Z}$*

(iii) *each λ_j is a "primitive" linear form, i.e. $\gcd(n_j, m_j) = 1$*

(iv) *$\omega(\lambda_1, \lambda_2) > 0$*

Proof. According to the fundamental cubic decomposition, we can write, in a unique way up to the order of the summands, $P = T_1 + T_2$ where T_j are "*triple-roots*", i.e. $T_j = \alpha_j\lambda_1^3$ where λ_j is a linear form. The crucial observation about the T_j's is that they have rational coefficients which are, "*at worst*", containing of a denominator of $2\sqrt{D} = 2\Delta$. Thus, by clearing denominators, and factoring out common factors, we get a cubic decomposition which satisfies the first three properties. This decomposition is almost unique except for the order of the summands, but we can force an ordering by observing that $\omega(\lambda_2, \lambda_1) = -\omega(\lambda_1, \lambda_2)$. Thus, we can force an ordering which will also satisfy the fourth condition. With this ordering condition the cubic decomposition is unique. ■

In **Chapter 2** the law of composition for $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, D)$ was for classes of *projective* cubic forms. If D is square-free then all cubic forms are automatically projective and so this restriction is not necessary. In general, however, and in our case when $D = \Delta^2$, we will need to restrict ourselves to projective classes of cubic forms. Fortunately, there is a very simple

fundamental cubic decomposition description for projective cubic forms.

Theorem 4.2.4. *If $P(X,Y)$ is a projective cubic form of discriminant $D=\Delta^2$ then we can write, in a unique way,*

$$P=\frac{1}{\Delta}\lambda_1^3+\frac{1}{\Delta}\lambda_2^3$$

such that,

(i) $\lambda_j\in \mathrm{sym}^1\mathbb{Z}^2$, *i.e.* $\lambda_j=n_jX+m_jY$ *with* $n_j,m_j\in\mathbb{Z}$

(ii) *each* λ_j *is a "primitive" linear form, i.e.* $\gcd(n_j,m_j)=1$

(iii) $\omega(\lambda_1,\lambda_2)=\Delta$

Proof. If P is a cubic form with $\mathrm{disc}(P)=\Delta^2$ then we can write, by **Prop. 4.2.3.**,

$$P=\frac{s_1}{2\Delta}\ell_1^3+\frac{s_2}{2\Delta}\ell_2^3$$

where (ℓ_1,ℓ_2) is a primitive linear form pair. If $\omega=\omega(\ell_1,\ell_2)$ then, by the generalized link equation of **Prop 4.2.2.**,

$$s_1s_2\omega^3=4\Delta^3$$

By a suitable action of $\mathrm{SL}(2,\mathbb{Z})$ we can transform,

$$(\ell_1,\ell_2)\mapsto(X,jX+\omega Y)$$

where $j\in(\mathbb{Z}/\omega\mathbb{Z})^\times$. Thus, we can assume that P can be written as,

$$P=\frac{s_1}{2\Delta}X^3+\frac{s_2}{2\Delta}(jX+\omega Y)^3$$

Now the cubic form P has integral coefficients, thus,

(i) $s_1+s_2j^3\equiv 0(\mathrm{mod}2\Delta)$

(ii) $3s_2j^2\omega\equiv 0(\mathrm{mod}2\Delta)$

(iii) $3s_2j\omega^2\equiv 0(\mathrm{mod}2\Delta)$

(iv) $s_2\omega^3 \equiv 0(\mathrm{mod}2\Delta)$

The equation $s_1 s_2 \omega^3 = 4\Delta^3$ implies that ω is an odd positive integer. Therefore, from **(iv)**, $s_2\omega^2$ is divisible by 2Δ, which implies that s_2 is even. From **(i)** we obtain $s_1 + s_2 j^3 \equiv 0(\mathrm{mod}2)$, and since s_2 is even, it follows s_1 is even as well.

We can then write $s_1 = 2t_1$ and $s_2 = 2t_2$, where t_i are positive integers, and they satisfy,

$$t_1 t_2 \omega^3 = \Delta^3$$

Furthermore, the cubic form P will decompose more simply as,

$$P = \frac{t_1}{\Delta} X^3 + \frac{t_2}{\Delta}(jX + \omega Y)^3$$

If we expand this out we will obtain,

$$P = \left(\frac{t_1 + t_2 j^3}{\Delta}\right) X^3 + 3\left(\frac{t_2 j^2 \omega}{\Delta}\right) X^2 Y + 3\left(\frac{t_2 j \omega^2}{\Delta}\right) X Y^2 + \left(\frac{t_2 \omega^3}{\Delta}\right) Y^3$$

This cubic form is projective, if and only if,

$$\left(-\frac{t_1 t_2 j \omega^2}{\Delta^2}, \frac{t_1 t_2 \omega^3}{\Delta^2}, 0\right)$$

is a primitive triplet.

If we substitute $t_1 t_2 = \frac{\Delta^3}{\omega^3}$ then we will obtain,

$$\gcd\left(\frac{t_1 t_2 j \omega^2}{\Delta^2}, \frac{t_1 t_2 \omega^3}{\Delta^2}\right) = \gcd\left(\frac{\Delta j}{\omega}, \Delta\right)$$

Since ω divides Δ, it means $\frac{\Delta}{\omega}$ divides both $\frac{\Delta j}{\omega}$ and Δ.

Therefore, in order for P to be projective, it must be the case that $\frac{\Delta}{\omega} = 1$. Furthermore, if $\omega = \Delta$ the cubic form will be projective because $\gcd\left(\frac{\Delta j}{\omega}, \Delta\right) = \gcd(j, \Delta) = 1$ since $j \in (\mathbb{Z}/\Delta\mathbb{Z})^{\times}$. We have therefore proved the theorem. ■

4.3 Law of Composition for Projective Cubic Forms

In this section we will completely describe the law of composition for $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, \Delta^2)$. First we describe all equivalence classes in a convenient way.

Proposition 4.3.1. *If $P(X,Y)$ is a cubic form of discriminant Δ^2 then for some $g \in \mathrm{SL}(2,\mathbb{Z})$ we can write,*

$$P^g = \frac{1}{\Delta}X^3 + \frac{1}{\Delta}(jX + \Delta Y)^3$$

where j is an integer determined by the mod class $\mathbb{Z}/\Delta\mathbb{Z}$ and is relatively prime to Δ. We refer to the above representative for P as the "basic representative".

Proof. This idea was already used in proof of **Thm. 4.2.4.**, namely write,

$$P = \frac{1}{\Delta}\lambda_1^3 + \frac{1}{\Delta}\lambda_2^3$$

where (λ_1, λ_2) is a primitive linear form pair with $\omega(\lambda_1, \lambda_2) = \Delta$.

Now by taking a suitable matrix $g \in \mathrm{SL}(2,\mathbb{Z})$ we can transform (λ_1, λ_2) into a primitive form pair which looks like,

$$(\lambda_1, \lambda_2) \mapsto (1X + 0Y, jX + \Delta Y)$$

and j must be relatively prime to Δ as this is a primitive linear form pair. From here the theorem follows. ■

We can now state the law of composition for projective cubic forms in terms of this so-called "*basic representative*".

Theorem 4.3.2. *The group $\mathrm{Cl}(\mathrm{sym}^3\mathbb{Z}^2, \Delta^2)$ is isomorphic to the 3-part of the multiplicative group $(\mathbb{Z}/\Delta\mathbb{Z})^\times$. Where the identity for $(\mathbb{Z}/\Delta\mathbb{Z})^\times$ is $(-1 \mod \Delta)$ and multiplication is defined by,*

$$(n \bmod \Delta)(m \bmod \Delta) = (-nm \bmod \Delta)$$

The isomorphism is given explicitly as follows. If $P(X,Y)$ is a basic representative, write,

$$P(X,Y) = \frac{1}{\Delta}X^3 + \frac{1}{\Delta}(jX + \Delta Y)^3$$

according to ***Prop. 4.3.1.****, then $P(X,Y)$ corresponds to the mod class*

$$(j \bmod \Delta) \in (\mathbb{Z}/\Delta\mathbb{Z})^\times$$

Proof.

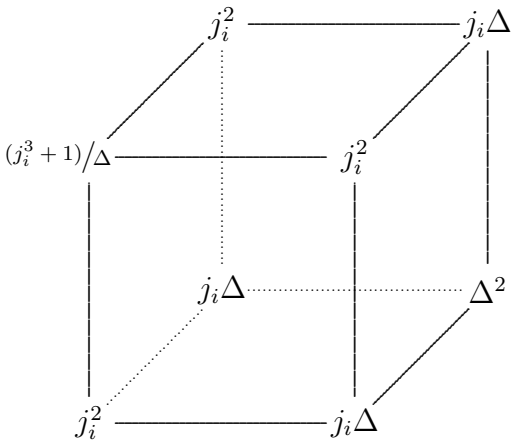
What needs to be confirmed is that the composition provided in **Thm. 4.2.2.** is the "*correct*" one. In other words, the same composition law as given by Bhargava in **Chapter 2**. Let $P_1(X,Y)$ and $P_2(X,Y)$ be the following two cubic forms,

$$P_1(X,Y) = \frac{1}{\Delta}X^3 + \frac{1}{\Delta}(j_1X + \Delta Y)^3 \text{ and } P_2(X,Y) = \frac{1}{\Delta}X^3 + \frac{1}{\Delta}(j_2X + \Delta Y)^3$$

We claim that,

$$P_1 \circ P_2 = P_3 \text{ where } P_3(X,Y) = \frac{1}{\Delta}X^3 + \frac{1}{\Delta}(-j_1j_2X + \Delta Y)^3$$

To that end, we associate to P_i its corresponding "*Bhargava cube*",



Denote by M to be the front face of this cube and N the back face,

$$M = \begin{bmatrix} (j_i^3+1)/\Delta & j_i^2 \\ j_i^2 & j_i\Delta \end{bmatrix} \text{ and } N = \begin{bmatrix} j_i^2 & j_i\Delta \\ j_i\Delta & \Delta^2 \end{bmatrix}$$

The other two pairs, of "*fundamental slicings*", of this cube, arising from the top/bottom face, and the left/right face, will be given by the same matrices. Thus, the three quadratic binary forms associated to this cube will all be the same, and be given by,

$$Q_i(X,Y) = -\det(MX - NY) = -j_i X^2 + \Delta XY$$

In order to check that,

$$P_1 \circ P_2 = P_3$$

it is enough to check that,

$$\mathscr{C}_{j_1} \circ \mathscr{C}_{j_2} = \mathscr{C}_{-j_1 j_2}$$

where $\mathscr{C}_*$ denotes the above Bhargava cube.

In order to check the cube composition law in $\mathrm{Cl}(\mathbb{Z}_2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, \Delta^2)$ it is enough to show that ,

$$Q_1 \circ Q_2 = -(j_1 j_2)X^2 + \Delta XY$$

where the above composition law is ordinary Gaussian composition.

If we denote $Q(X,Y) = -(j_1 j_2)X^2 + \Delta XY$, the reader can verify,

$$Q_1(X_1, Y_1)Q_2(X_2, Y_2) = Q(X_3, Y_3)$$

where

$$X_3 = X_1 Y_1 \text{ and } Y_3 = -j_1 X_1 Y_2 - j_2 X_2 Y_1 + \Delta Y_1 Y_2$$

and so, by the classic definition of Gauss composition (**Def. 1.1.1.**), $Q = Q_1 \circ Q_2$.

This concludes the proof that the composition law is the correct one. ■

4.4 Further Questions and Generalizations

We conclude this paper with some remaining questions and possible generalizations that came follow from the work that we presented. The most natural question to ask is how do we describe the most general composition law for binary integral cubic forms when D is an integer $\equiv 0, 1 (\text{mod} 4)$? In Chapter 3 we explained the composition law when D is square-free. In this chapter we explained the composition law when $D = \Delta^2$ was a perfect square. In general, we can write $D = D_0 D_1^2$ where D_0 is square-free and D_1^2 is the perfect square factor. It is therefore reasonable to suggest that the general composition law should involve the two special cases from Chapter 3 and Chapter 4. However, this is an issue that has not been resolved in this paper and is subject to further research.

Another question that came up in this paper that we did not resolve is **Conjecture 1.7.1**. In fact, there could be an entire collection of rational composition laws where we essentially replace $\mathbb{Z}$ with $\mathbb{Q}$. The first place to start would be with $\text{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$. We aim to construct a composition law so that the natural map $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D) \rightarrow \text{Cl}(\mathbb{Q}^2 \otimes \mathbb{Q}^2 \otimes \mathbb{Q}^2, D)$ is a homomorphism. The author of this paper does wish to continue thinking about this problem and will try to settle it in the near future.

Bibliography

[**Bhargava**] Bhargava, M., 2004. Higher composition laws I: A new view on Gauss composition, and quadratic generalizations. Annals of Mathematics, pp.217-250.

[**Bouyer**] Bouyer, F., 2005. Composition and Bhargava's Cubes. `https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/gauss_composition.pdf`

[**Cohen**] Cohen, H., 2013. A course in computational algebraic number theory (Vol. 138). Springer Science Business Media.

[**Cox**] Cox, D., 1989. Primes of the form $x^2 + ny^2$. Wiley.

[**Kable**] Kable, A.C., 2000. Classes of integral 3-tensors on 2-space. Mathematika, 47(1-2), pp.205-217.

[**Slupinski-Stanton**] Slupinski, M.J. and Stanton, R.J., 2012. The special symplectic structure of binary cubics. In Representation theory, complex analysis, and integral geometry (pp. 185-230). Birkhäuser Boston.

[**Takashi Taniguchi**] Table of Binary Cubic Forms. Private Correspondence.