Platonic Solids and Solutions to $\mathbf{X^2 + Y^3 = dZ^r}$

Platonische Lichamen
en Oplossingen voor
$X^2 + Y^3 = dZ^r$

(met een samenvatting in het Nederlands)

Proefschrift

ter verkrijging van de graad van doctor aan de Universiteit Utrecht op gezag van de Rector Magnificus, Prof. dr. W.H. Gispen, ingevolge het besluit van het College voor Promoties in het openbaar te verdedigen op vrijdag 4 februari 2005 des ochtends te 10:30 uur

door

Edward Jonathan Edwards

geboren op 16 mei 1961, te Urmston in Engeland

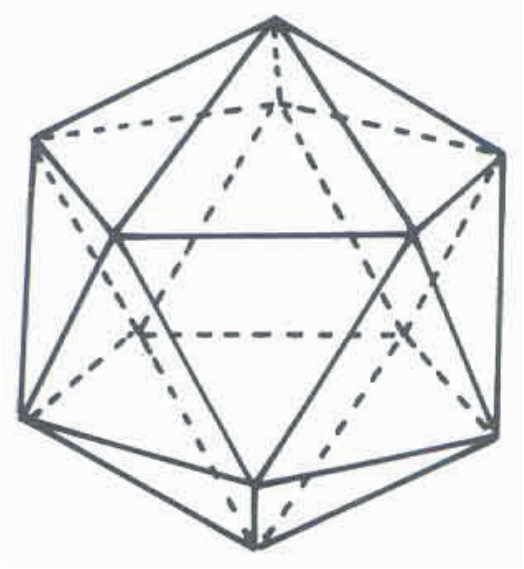
Promotor: Prof. dr. Frits Beukers
Faculteit Wiskunde en Informatica
Universiteit Utrecht

Mathematics Subject Classification: 11D41

Edwards, Johnny
Platonic Solids and solutions to $X^2 + Y^3 = Z^r$
Proefschrift Universiteit Utrecht — Met samenvatting in het Nederlands.

ISBN 90-393-3921-X

Printed by All Print, Utrecht.



Icosahedron

To my parents

Contents

Summary

This manuscript investigates the properties of the diophantine equation $X^2+Y^3 = dZ^r$. Here d is a given integer, r is one of 3,4, or 5 and the unknowns X,Y,Z are required to be integers with no common factor other than ± 1.

These equations have many properties in common with the better known (and in fact studied by the Babylonians since at least 1600 BC) Pythagoras equation $X^2 + Y^2 = Z^2$.

There is an infinite number of solutions to the Pythagoras equation. Many will remember the triples $(3, 4, 5)$ and $(5, 12, 13)$ from their high school days. An infinite set of solutions can be obtained by assigning integer values to (s, t) in the formula $X = s^2-t^2$, $Y = 2st$, $Z = s^2+t^2$. In fact, all solutions to the Pythagoras equation can be obtained if we also allow X to be swapped with Y, and Z to be replaced by $-Z$.

A similar thing happens with $X^2+Y^3 = dZ^r$. There is an infinite number of solutions and these solutions can all be obtained by assigning integer values to (s, t) in a finite set of formulae for (X, Y, Z). This thesis describes this phenomenon as well as an algorithm to generate these formulae.

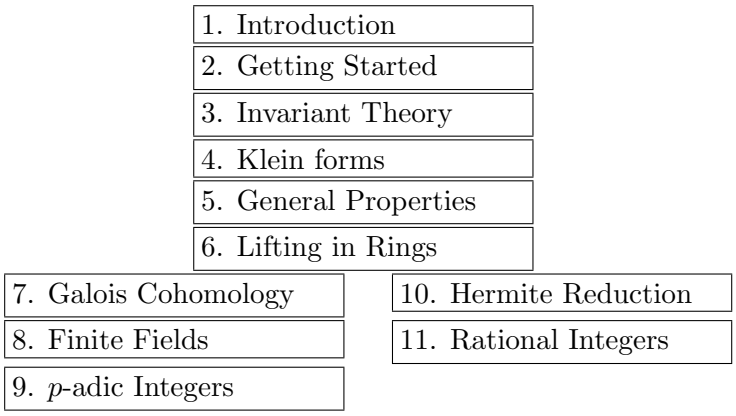
The methods and results in this thesis are an important addition to the theory of diophantine equations. The method lends on several mathematical techniques from Invariant Theory—an important branch of mathematics at the end of 19th century. The title of the thesis is explained by the fact that the 60 symmetries of the 20-sided platonic solid called the icosahedron play a key role in producing solutions to the equation $X^2 + Y^3 = dZ^5$.

Reader's Guide

Theorems, lemmas, propositions, and corollaries are numbered consecutively in the form **c.s.n** where **c** is the chapter and **s** is the section. Displayed equations are numbered consecutively within each chapter in the form **(c.n)**. References [n] are to books and papers listed beginning on page 101. The end (or absence) of a proof is signalled by the symbol '□'.

Structure of the Thesis

The layout of the thesis is illustrated by the following reading scheme.



Chapter 1 is an introduction.

Chapters 2–6 develop the theory of parameterizations in a general setting. This requires Classical Invariant Theory and a knowledge of Klein forms. A characterization of these forms is given that allows us to consider *parameterizations* as an algebraic set of dimension 3 inside the space of all binary forms of the correct degree.

The thesis then forks. Readers who are only interested in parameterizations for the rational integers, may skip chapters 7–9 and only need to read chapters 10 and 11. Finite Field people and p-adic people, on the other hand, can concentrate on chapters 7–9.

There are four appendices. Appendix A contains the explicit equations that define the space of parameterizations $\mathcal{C}(r, d)$. Appendix B contains the

proofs of various propositions that require special arguments when the field has low non-zero characteristic. Appendix C describes the theory of Twisted Conjugacy Classes. Appendix D lists full sets of parameterizations to the equations $X^2 + Y^3 = \pm Z^r$, $r \in \{3, 4, 5\}$, that specialize to all co-prime rational integer solutions.

Chapter 1

Introduction

Numbers have fascinated mankind for thousands of years. The Babylonian tablet in the G. A. Plimpton collection at Columbia University, known as Plimpton 322, is an example of a mathematical tablet constructed by the Babylonians. From the style of the script the era of construction of the tablet is given as the Old Babylonian Period (ca. 1900 to 1600 B.C.). It contains lists of integer solutions to the equation

$$X^2 + Y^2 = Z^2.$$

This thesis continues in this great tradition by showing how to generate integer solutions to the equations

$$X^2 + Y^3 = Z^3,$$
$$X^2 + Y^3 = Z^4,$$
$$X^2 + Y^3 = Z^5.$$

In this chapter we review (some of) what is known about so called *generalized Fermat equations*. This will enable the reader to place the subject matter of this thesis within the context of higher order diophantine equations.

The last section summarizes the new results in this thesis.

Generalized Fermat Equations

Generalized Fermat equations are equations of the form

$$AX^p + BY^q = CZ^r, \quad \gcd(X, Y, Z) = 1, \tag{1.1}$$

where A, B, C are non-zero integers, and the exponents p, q, r are positive integers greater than 1. The unknowns X, Y, Z are in $\mathbb{Z}$.

The requirement that the unknowns be co-prime excludes the trivial solution $(0, 0, 0)$. Triples (X, Y, Z) that satisfy $AX^p + BY^q = CZ^r$ but are

not necessarily co-prime are easy to construct. For instance, from $a+b=c$ it would follow after multiplication by $a^{33}b^{44}c^{54}$ that

$$(a^{17}b^{22}c^{27})^2 + (a^{11}b^{15}c^{18})^3 = (a^3b^4c^5)^{11},$$

providing us with infinitely many non co-prime solutions to $X^2+Y^3=Z^{11}$. It is conjectured that there are no co-prime solutions with $XYZ \neq 0$.

It is instructive to begin by examining what is known about the solutions to these equations. The main characteristics of equation (1.1) can be shown to be governed by the value of

$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}.$$

The behavior of the equations varies most strikingly depending on whether this values is less than, equal to, or greater than one. The equation is then called *hyperbolic*, *euclidean*, or *spherical* respectively.

Hyperbolic Case: $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$.

We are not able to solve these diophantine equations for general values of p,q,r. However, we can get a feel for how these equations (probably) behave via the ABC-Conjecture. (The name ABC has nothing to do with the A,B,C of equation (1.1)).

Noting that $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ implies that

$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r} \leq \frac{1}{2}+\frac{1}{3}+\frac{1}{7}=\frac{41}{42},$$

and applying the ABC-Conjecture produces the following.

Conjecture 1.0.1. *Fix non-zero integers A,B,C. Then there is a constant N_0 depending only on ABC with the following property.*

If X,Y,Z are co-prime integers and $p,q,r>1$ are integers satisfying equation (1.1) and $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ then $|XYZ| \leq N_0$.

The case $A=B=C=1$ is sufficiently difficult testing ground for this conjecture. All known solutions of $X^p+Y^q=Z^r$, with X,Y,Z co-prime positive integers and $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ are

$$
\begin{aligned}
1^n + 2^3 &= 3^2 \quad (n > 6),\\
13^2 + 7^3 &= 2^9,\\
2^7 + 17^3 &= 71^2,\\
2^5 + 7^2 &= 3^4,\\
3^5 + 11^4 &= 122^2,\\
17^7 + 76271^3 &= 21063928^2,\\
1414^3 + 2213459^2 &= 65^7,\\
9262^3 + 15312283^2 &= 113^7,\\
33^8 + 1549034^2 &= 15613^3,\\
43^8 + 96222^3 &= 30042907^2.
\end{aligned}
$$

Is this all? Tijdeman and Zagier noticed that the exponent 2 always occurs in the list.

Question 1.0.2. *If $p, q, r \geq 3$ are there any co-prime solutions to $X^p + Y^q = Z^r$ with $XYZ \neq 0$?*

Unbeknown to Tijdeman and Zagier, in Texas, the bank owner and amateur mathematician Andy Beal had asked the very same question. He originally offered $\$5,000$ for anyone who could come up with an answer. See [17]. The pot would increase by $\$5,000$ every year up to a maximum of $\$50,000$. The question is now known as the Beal Prize Conjecture. Since the AMS article the prize money has been further increased and at time of writing stands at $\$100,000$.

The prize problem seems far from being answered. However, in 1995, Darmon and Granville were able to use the recently proven Faltings' Theorem to prove the following folklore conjecture in [4].

Theorem 1.0.3 (Darmon and Granville (1995)). *For given non-zero A, B, C, and $p, q, r \geq 2$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ the number of co-prime integer solutions to equation (1.1) is finite.*

Sketch of Proof. I shall sketch the ideas behind the proof. By the Riemann Existence Theorem (see [21], Theorem 6.3.1) there is curve $\mathfrak{X}/\overline{\mathbb{Q}}$ and a branched Galois covering map

$$\pi : \mathfrak{X} \to \mathbb{P}^1,$$

unramified over $\mathbb{P}^1 - \{0, 1, \infty\}$, and with ramification indices over $0, 1$ and ∞ of p, q and r respectively. Let g be the genus of $\mathfrak{X}$ and n the degree of π.

The Riemann-Hurwitz formula gives

$$\begin{aligned} 2-2g &= n(2-2.0) - \left(n - \frac{n}{p}\right) - \left(n - \frac{n}{q}\right) - \left(n - \frac{n}{r}\right) \\ &= n\left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1\right). \end{aligned}$$

Since $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, the curve $\mathfrak{X}$ has genus $g > 1$. We can find a number field K so that $\mathfrak{X}$, π, and $\mathrm{Gal}(\mathfrak{X}/\mathbb{P}^1)$ are all defined over K. Let V denote a finite set of primes of K, including all primes dividing ABC and all primes for which the covering map $\pi : \mathfrak{X} \to \mathbb{P}^1$ has bad reduction. For $t \in \mathbb{P}^1(K)$, let L_t denote the extension of K obtained by adjoining the points $\pi^{-1}(t)$. If $t \neq 0, 1, \infty$ this is a Galois extension of K of degree at most n.

For a place v of K and $t \in \mathbb{P}^1(K) - \{0, 1, \infty\}$, we define the arithmetic intersection numbers by

$$\begin{aligned} (t \cdot 0)_v &:= \max(\mathrm{ord}_v(t), 0), \\ (t \cdot 1)_v &:= \max(\mathrm{ord}_v(t-1), 0), \\ (t \cdot \infty)_v &:= \max(\mathrm{ord}_v(1/t), 0). \end{aligned}$$

Proposition 1.0.4 (Beckmann). *Suppose $t \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ and v is a place of K not in the set V. If*

$$(t \cdot 0)_v \equiv 0 \pmod{p}, \quad (t \cdot 1)_v \equiv 0 \pmod{q}, \quad (t \cdot \infty)_v \equiv 0 \pmod{r},$$

then L_t is unramified above v.

Suppose that (X, Y, Z) is a solution to equation (1.1) with $XYZ \neq 0$. Let $t := AX^p/CZ^r$. Beckmann's Proposition applies and we deduce that L_t is unramified outside of V. By Hermite's Theorem there are only a finite number of possibilities for L_t, so they are all contained in a single larger number field extension L.

An infinite number of co-prime solutions to equation (1.1) would imply an infinite number of L-rational points on $\mathfrak{X}$. This is impossible by Faltings' Theorem.

□

Euclidean Case: $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$.

The only possibilities for (p, q, r) up to permutation are $(2, 3, 6), (3, 3, 3)$ and $(2, 4, 4)$. The curve $\mathfrak{X}$ has genus 1, and the covering $\pi : \mathfrak{X} \to \mathbb{P}^1$ relates co-prime solutions to rational points on an elliptic curve.

For instance, co-prime solutions to

$$X^2 - Y^3 = Z^6$$

are related to $\mathbb{Q}$-rational points on the elliptic curve

$$E : u^2 = w^3 + 1$$

by setting $u = X/Z^3, w = Y/Z$.

Spherical Case: $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$.

We are in the class of equations that I will be examining in this thesis. Up to permutation the possibilities for (p, q, r) are: $\{p, q, r\} = \{2, 2, n\}$, $\{2, 3, 3\}$, $\{2, 3, 4\}$ and $\{2, 3, 5\}$.

The genus of $\mathfrak{X}$ is 0, so $\mathfrak{X} \cong \mathbb{P}^1$. There is the possibility of an infinite number of co-prime solutions to our headline equation (1.1). This was studied by Beukers in [1].

It is useful to consider binary forms $\hat{X}, \hat{Y}, \hat{Z} \in \mathbb{Q}[s, t]$ which satisfy

$$A\hat{X}^p + B\hat{Y}^q = C\hat{Z}^r.$$

We call $(\hat{X}, \hat{Y}, \hat{Z})$ a parameterized solution if $\hat{X}, \hat{Y}, \hat{Z}$ are in the ring $\mathbb{Q}[s, t]$ but do not lie in the subring $\mathbb{Q}$. It is called a co-prime parameterization if $\hat{X}, \hat{Y}, \hat{Z}$ are co-prime in the ring $\mathbb{Q}[s, t]$. By Mason's Theorem ([16], page 194), co-prime parameterized solutions are only possible in the spherical case. By specializing (s, t) to integer values we can hope to obtain solutions to equation (1.1).

Theorem 1.0.5 (Beukers (1998)). *There is a finite set of co-prime parameterized solutions $(\hat{X}, \hat{Y}, \hat{Z}) \in \mathbb{Q}[s, t]^3$ to equation (1.1) such that their integer specializations include all co-prime integer solutions to equation (1.1).*

One way to appreciate these results is to realize that the well-known Pythagoras equation

$$X^2 + Y^2 = Z^2$$

has certain easily verifiable properties that are typical of *spherical Fermat equations*. There are an infinite number of co-prime solutions, and any co-prime solution is the integer specialization of one of the following 4 parameterized solutions

$$(s^2 - t^2)^2 + (2st)^2 = (\pm(s^2 + t^2))^2,$$
$$(2st)^2 + (s^2 - t^2)^2 = (\pm(s^2 + t^2))^2.$$

The theory developed by Beukers does not give a feasible method for actually calculating parameterizations. Other methods are needed. Again, using $X^p + Y^q = \pm Z^r$ as a test case, we find the following lists of parameterized solutions in the literature.

$X^2 + Y^3 = Z^3$, $\gcd(X, Y, Z) = 1$.

This was solved by Mordell in his 1969 book Diophantine Equations [18]. Mordell achieved his result by specializing the parameters in a syzygy from the Invariant Theory of binary quartic forms.

$X^2 + Y^3 = \pm Z^4$, $\gcd(X, Y, Z) = 1$.

This was solved by Zagier and the results are quoted in Beukers' paper [1]. The approach here was to take the parameterized solutions of the $\{2, 3, 2\}$ case and try to find specializations in which the value of Z is a square.

New Results in this Thesis

The theory contained in this thesis is a new approach to solving the equations of the type $X^2 + Y^3 = dZ^r$ where r is one of 3,4 or 5. It has its roots in a quest to generalize Mordell's method of solving the $\{2, 3, 3\}$-equation.

This is a unified approach to solving these equations. For the $\{2, 3, 3\}$-equation it is simply another way of looking at Mordell's Method. For the $\{2, 3, 4\}$-equation it is an alternate method to that of Zagier for generating complete sets of parameterizations. In the $\{2, 3, 5\}$-case my theory solves the hitherto inaccessible equation $X^2 + Y^3 = Z^5$.

We have seen that solutions to generalized Fermat equations are intimately linked to branched coverings of $\mathbb{P}^1$. For the exponent triples $\{2, 3, r\}$ these are given by

$$\mathbb{P}^1 \to \mathbb{P}^1/\Gamma,$$

where $\Gamma \in \mathrm{SL}_2(\mathbb{C})$ is the Binary Tetrahedral, Octahedral or Icosahedral Group depending on which of r in $\{3, 4, 5\}$ is currently under consideration.

The resulting solutions to our generalized Fermat equation take the form

$$(\boldsymbol{t}(f)/2)^2 + \boldsymbol{H}(f)^3 = df^r, \tag{1.2}$$

where f is a binary form with roots corresponding to the vertices of a tetrahedron, octahedron or icosahedron. The binary forms $\boldsymbol{t}(f)$ and $\boldsymbol{H}(f)$ are up to a constant the Hessian and the Jacobian covariant of f. Up to scaling factors these are the famous relations used by Klein to find the roots of polynomials of degree r.

In fact, any parameterization is only a slight variation on that given in equation (1.2). We show that we can assume that any parameterization is obtainable by replacing f by an $\mathrm{SL}_2(\mathbb{C})$ twist f' of f, and replacing $\boldsymbol{t}(f), \boldsymbol{H}(f)$ by $\boldsymbol{t}(f')$ and $\boldsymbol{H}(f')$ in (1.2).

We then use a gem of Paul Gordan from 1875 who characterized $\mathrm{GL}_2(\mathbb{C})$ twists of the 'Klein form' f as a 4-dimensional quasi-affine subspace of the space of all binary form of the same degree. We prove a slight variation—the

$\mathrm{SL}_2(\mathbb{C})$ twists are a 3-dimensional *affine* subspace defined over $\mathbb{Q}(d)$ which we call $\mathcal{C}(r,d)$.

We now have an explicit variety on which we can perform arithmetic. The parameterizations correspond to points on $\mathcal{C}(r,d)$. There is an action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathcal{C}(r,d)$. A set of $\mathrm{SL}_2(\mathbb{Z})$ equivalent parameterizations is an $\mathrm{SL}_2(\mathbb{Z})$ orbit of $\mathcal{C}(r,d)$. We find that co-prime integer solutions to $X^2+Y^3=dZ^r$ are the $\mathbb{Z}$-specializations of forms $f\in\mathcal{C}(r,d)$ with integral coefficients. An application of Hermite reduction theory to the *integral* binary forms lying on this variety is our algorithm for solving $X^2+Y^3=dZ^r$.

This result has also been published in [5].

There are a number of interesting open questions about the local/global behavior of the spherical Fermat equations. For this it is important to know how parameterizations behave in other rings than just the rational integers—in particular in finite fields and the p-adic integers. Here we see another attraction of the new method. Much of the theory consists of arithmetic on the explicit affine variety $\mathcal{C}(r,d)$, and this can be performed for any ring R.

We therefore develop a general theory valid for any entire ring R. Much of the theory carries through provided the characteristic of the quotient field does not belong to a set of bad primes. This allows us to give results about the parameterizations in finite fields and p-adic integers. In the algorithm to produce parameterizations in these rings the use of Hermite reduction is replaced by Galois cohomology.

Chapter 2

Getting Started

The aim of this chapter is to introduce the mathematical objects we are going to study in this thesis. These are defined here, and various notation and conventions that I follow are explained.

2.1 Definitions

The first step is to introduce the diophantine equations we are going to study and give the definition of a parameterization.

Definition 2.1.1 ($\mathcal{D}(r,d)$). *Let R be a ring. For any $r \in \{3,4,5\}$ and any $d \in R$ we define $\mathcal{D}(r,d)(R)$ to be the set of triples $(X,Y,Z) \in R^3$ that satisfy*

$$X^2 + Y^3 = dZ^r. \tag{2.1}$$

Definition 2.1.2 (Parameterization). *Suppose R is an entire ring and $r \in \{3,4,5\}$. Let K be the quotient field of R and $\bar{K}$ an algebraic closure of K. We assume that x, y are algebraically independent and transcendental over $\bar{K}$.*

A parameterization of $\mathcal{D}(r,d)(R)$ is a triple $\chi := (\hat{X}, \hat{Y}, \hat{Z})$ in $\mathcal{D}(r,d)(K[x,y])$ such that the equation

$$\hat{X}^2 + \hat{Y}^3 = d\hat{Z}^r$$

is homogeneous in the x, y of some degree $n > 0$. The integer n is called the order of the parameterization. If $\hat{X}, \hat{Y}, \hat{Z}$ are co-prime in $\bar{K}[x,y]$ we say that the parameterization is co-prime.

Definition 2.1.3 (Specialization). *Suppose that χ is a parameterization of $\mathcal{D}(r,d)(R)$. We say that $(X,Y,Z) \in \mathcal{D}(r,d)(R)$ is obtained by an R-specialization of χ if it can be obtained from χ by specializing the variables x, y to values in R.*

2.2 G-spaces

Much of this thesis will involve analyzing the action of a group G on a space X. We say that $x, x' \in X$ are G-equivalent if there is a $g \in G$ so that $x' = gx$. We call the classes of G-equivalent elements of X the G-orbits. If the whole space consists of a single G-orbit we say that X is a *homogeneous G-space*.

For any $x \in X$, the set $\mathrm{Stab}_G(x)$ is defined to be those $g \in G$ such that $gx = x$. Maps between G-spaces that commute with the action of G are called G-equivariant maps.

In most cases G will be a subgroup of $\mathrm{GL}_2(K)$, where K is a field. The group $\mathrm{GL}_2(K)$ acts on elements of K^2 and $K[x, y]$ as follows.

Definition 2.2.1 (Actions of $\mathbf{GL}_2(K)$). *Suppose that*

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K).$$

We let $GL_2(K)$ act on K^2 by

$$(x, y) \mapsto (ax + by, cx + dy).$$

We extend this to an action on $K[x, y]$ by

$$f(x, y) \mapsto g \cdot f := f(g^{-1}(x, y)).$$

This induces an action of $GL_2(K)$ on parameterizations by

$$\chi := (\hat{X}, \hat{Y}, \hat{Z}) \mapsto g \cdot \chi := (g \cdot \hat{X}, g \cdot \hat{Y}, g \cdot \hat{Z}).$$

2.3 A First Lemma

Lemma 2.3.1. *Fix a ring R. Then any $\lambda \in R^*$ induces a bijection:*

$$\begin{aligned} \mathcal{D}(r, d)(R) &\to \mathcal{D}(r, \lambda^{r-6} d)(R), \\ (X, Y, Z) &\mapsto (\lambda^3 X, \lambda^2 Y, \lambda Z). \end{aligned}$$

We will be interested in looking at how many parameterizations are needed to specialize to all co-prime $(X, Y, Z) \in \mathcal{D}(r, d)(R)$. If R is a domain, the map can also be applied to the ring $Q(R)[x, y]$, where $Q(R)$ is the quotient field of R. As this map commutes with R-specialization, the 'theory of parameterizations' depends only on d modulo $R^{*(6-r)}$.

2.4 Reserved Symbols

Throughout this thesis the symbols r, k, N will have a special meaning. The symbol r will always represent a number in the set $\{3, 4, 5\}$. This will be the exponent of Z in the equation $X^2 + Y^3 = dZ^r$. We associate $k \in \{4, 6, 12\}$ and $N \in \{12, 24, 60\}$ to these equations depending on which of the $r \in \{3, 4, 5\}$ is currently under consideration.

We will be associating a platonic solid to each of the $r \in \{3, 4, 5\}$. The solid is the tetrahedron, the octahedron, and the icosahedron respectively. To motivate these numbers I include the following table.

Symbol	Values	Interpretation
r	$\{3, 4, 5\}$	The exponent of Z in $X^2 + Y^3 = dZ^r$.
k	$\{4, 6, 12\}$	The number of vertices of the associated platonic solid.
N	$\{12, 24, 60\}$	The order of the group of rotational symmetries of the Solid.

Chapter 3

Invariant Theory

This chapter introduces the notation and results from Invariant Theory that will be used in this thesis. This will be Invariant Theory as known at the end of the 19th century and my main reference will be the notes from a series of lectures given by David Hilbert in 1897 in Göttingen [12] on the subject.

3.1 Definitions

In those days everything was done relative to the field $\mathbb{C}$ of complex numbers. We do not want to be so restrictive and would like to consider more general fields K inside a fixed algebraic closure $\bar{K}$.

For historical reasons the order of a binary form is defined to be its degree in the variables x, y. We start with a binary f form of order k. We would like to follow Hilbert and write the generic form of order k (also called the *base form*) as

$$f = a_0 x^k + \begin{pmatrix} k \\ 1 \end{pmatrix} a_1 x^{k-1} y + \begin{pmatrix} k \\ 2 \end{pmatrix} a_2 x^{k-2} y^2 + \cdots + a_k y^k.$$

This forces us to restrict the characteristic of the base field. To avoid having to deviate too far from the Invariant Theory of Hilbert's day, I assume that

$$\boxed{\text{char}(K) = 0 \ \text{ or } \ \text{char}(K) > \text{ the order of the base form } f.}$$

(In section 3.4, I show how this assumption can be dropped).

If we consider a vector formed from the coefficients of f as a vector space of dimension $k+1$, we see that the action of $\mathrm{GL}_2(K)$ on the generic form f is a $k+1$ dimensional representation $\mathrm{GL}_2(K) \to K^{k+1}$. One of the major objects of study in the 19th century was:

Definition 3.1.1 (Covariant). *A binary form $\boldsymbol{C}(f) \in K[a_0, \ldots, a_k][x, y]$ is called a covariant if it is homogeneous in the variables x, y and there is a $p \in \mathbb{Z}_{\geq 0}$ such that for all $g \in GL_2(\bar{K})$*

$$g \cdot \boldsymbol{C}(f) = \det(g)^p \boldsymbol{C}(g \cdot f),$$

where $\boldsymbol{C}(g \cdot f)$ denotes the form obtained by replacing all occurrences of a_i with the i-th coefficient of $g \cdot f$. The integer p is called the weight of the covariant.

3.2 Examples and Basic Properties

Although the covariance properties place severe restrictions on $\boldsymbol{C}$, there are several well-known algebraic constructions that are covariants:

$$\boldsymbol{H}(f) := \left(\frac{1}{k(k-1)}\right)^2 \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix}, \qquad \boldsymbol{t}(f) := \frac{1}{k(k-2)} \begin{vmatrix} f_x & f_y \\ \boldsymbol{H}_x & \boldsymbol{H}_y \end{vmatrix}.$$

These can be shown to be covariants of weight 2 and 3 respectively.

Many of the elementary properties of covariants can be established by noting that

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

generate $\mathrm{GL}_2(K)$ and seeing what conditions this forces onto the covariants.

Definition 3.2.1 (Differential Operators for Invariant Theory). *Let x', y' be variables. We define*

$$\begin{aligned} D &:= a_0 \frac{\partial}{\partial a_1} + 2a_1 \frac{\partial}{\partial a_2} + \cdots + k a_{k-1} \frac{\partial}{\partial a_k}, \\ \Delta &:= k a_1 \frac{\partial}{\partial a_0} + (k-1) a_2 \frac{\partial}{\partial a_1} + \cdots + a_k \frac{\partial}{\partial a_{k-1}}, \\ \Omega &:= \frac{\partial^2}{\partial x \partial y'} - \frac{\partial^2}{\partial x' \partial y}. \end{aligned}$$

The first two operators are known as the Cayley Aronhold operators. The last is simply referred to as the Omega *operator.*

Theorem 3.2.2. *The expression*

$$\boldsymbol{C} = \sum_{i=0}^{m} C_i x_i^{m-i} y^i, \quad \text{with } C_i \in K[a_0, \ldots, a_k]$$

is a covariant of the base form f if and only if C_0 is a homogeneous isobaric function of the a_i of degree n and weight p such that $m = kn - 2p$, which satisfies the differential equations

$$DC_0 = 0, \quad C_i = \frac{1}{i!}\Delta^i C_0 \quad \textit{for all } i > 0.$$

In particular, a covariant is determined by its leading coefficient C_0.

Proof. See [12], lecture XIII. □

There are various operations on covariants. We will need the transvectant process which creates a form $(\boldsymbol{C}_1, \boldsymbol{C}_2)_i$ called the i-th transvectant from 2 forms $\boldsymbol{C}_1, \boldsymbol{C}_2$ (see [9], page 46) by the following formula:

$$(\boldsymbol{C}_1, \boldsymbol{C}_2)_i := \left(\frac{(k-i)!}{k!}\right)^2 \Omega^i \boldsymbol{C}_1(x,y)\boldsymbol{C}_2(x',y')\Big|_{\substack{x,x'=x\\ y,y'=y}}.$$

If $\boldsymbol{C}_1, \boldsymbol{C}_2$ are covariants of a base form then $(\boldsymbol{C}_1, \boldsymbol{C}_2)_i$ is a also a covariant. Transvectants (also referred to as transvections in the literature) were very important in 19-th century Invariant Theory. The $\boldsymbol{H}, \boldsymbol{t}$ above are $\boldsymbol{\tau}_2(f), \boldsymbol{\tau}_3(f)$ in the series

$$\boldsymbol{\tau}_{2m}(f) := \frac{1}{2}(f,f)_{2m}, \quad \boldsymbol{\tau}_{2m+1}(f) := (f, \boldsymbol{\tau}_{2m}(f))_1.$$

Finally, the Catalecticant is the covariant $\boldsymbol{j}(f)$, whose leading term is given by

$$\begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix}.$$

This is covariant of weight 6 ([18], Chapter 25, page 233).

Identifying these covariants by their leading term (which is reasonable by Theorem 3.2.2), we have:

$$\begin{aligned}
f &= a_0x^k + \dots, \\
\boldsymbol{H}(f) &= (a_0a_2 - a_1^2)x^{2k-4} + \dots, \\
\boldsymbol{t}(f) &= (a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3)x^{3k-6} + \dots, \\
\boldsymbol{\tau}_4(f) &= (a_0a_4 - 4a_1a_3 + 3a_2^2)x^{2k-8} + \dots, \\
\boldsymbol{\tau}_6(f) &= (a_0a_6 - 6a_1a_5 + 15a_2a_4 - 10a_3^2)x^{2k-12} + \dots, \\
\boldsymbol{j}(f) &= (a_0a_2a_4 + 2a_1a_2a_3 - a_2^3 - a_0a_3^2 - a_1^2a_4)x^{3k-12} + \dots \quad .
\end{aligned}$$

3.3 Other Properties of Covariants

This section collects together some less mainstream properties of binary forms and covariants that will be used in this thesis.

Definition 3.3.1 (Rationality). *For $r \in \{3, 4, 5\}$ we define the following sets:*

$$\begin{aligned}\Omega_3 &:= \{a_0, \ldots, a_4\},\\ \Omega_4 &:= \{a_0, \ldots, a_6\},\\ \Omega_5 &:= \{a_0, \ldots a_5, 7a_6, a_7 \ldots a_{12}\}.\end{aligned}$$

If $k \in \{4, 6, 12\}$ and f is a binary form of order k we denote the specialization of the set Ω_r to the coefficients of f by $\Omega_r(f)$.

Proposition 3.3.2. *Fix a ring R, an integer $k \in \{4, 6, 12\}$, a form f of order k and a matrix $g \in M_2(R)$. Then*

$$\Omega_r(f) \subseteq R \quad \Longrightarrow \quad \Omega_r(f \circ g) \subseteq R.$$

Proof. Let

$$g := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \mho = \left(b\frac{\partial}{\partial x} + d\frac{\partial}{\partial y} \right).$$

Then $f' = f \circ g$ has coefficients given by

$$a'_m = \frac{(k-m)!}{k!} \mho^m f \Big|_{x=a, y=c}.$$

Taking a hint from symbolic notation [9], this implies that

$$a'_m = \sum_{j=0}^{k} D_{m,j} a_j,$$

where $D_{m,j}$ is a form given by the coefficient of x^j in

$$(ax + c)^m (bx + d)^{k-m}.$$

The result follows if we can show that for $k = 12, m \neq 6$; $D_{m,6} \in 7\mathbb{Z}[a, b, c, d]$. By symmetry we can suppose that $m < 6$. We then get:

$$D_{m,6} = \sum_{s=0}^{m} \begin{pmatrix} m \\ s \end{pmatrix} \begin{pmatrix} k-m \\ 6-s \end{pmatrix} a^s c^{m-s} b^{6-s} d^{6-m+s}.$$

The claim is true since 7 divides $\begin{pmatrix} k-m \\ 6-s \end{pmatrix}$ for every $s = 0 \ldots m$ in the above equation for $D_{m,6}$. □

Proposition 3.3.3. *Let R be a ring. Fix $r \in \{3,4,5\}$ and $k \in \{4,6,12\}$ for the order of the base form. Let $\boldsymbol{C} = \sum_{i=0}^{m} C_i x^{m-i} y^i$ be a covariant. Suppose $C_0 \in R[a_0 ... a_k]$ and if $r = 5$ that the covariant has weight ≤ 5. Then $\boldsymbol{C}(f) \in R[\Omega_r; x, y]$. In particular*

$$\Omega_r(f) \subseteq R \implies \boldsymbol{C}(f) \in R[x, y].$$

Proof. By [12], section I.12, page 103, $\boldsymbol{C}(f)$ can be obtained by replacing the a_i in C_0 by

$$\begin{aligned} f_i &:= \frac{(k-i)!}{k!} f^{(i)} \\ &= \sum_r \begin{pmatrix} k-i \\ r \end{pmatrix} a_r x^{k-r-i} y^r, \end{aligned}$$

where $f^{(i)}$ denotes the i-th derivative of f with respect to x. This implies the result for $r = 3, 4$. For $r = 5$ the extra assumption means that C_0 is isobaric of weight ≤ 5 in the a_i. But $f_0, f_1 \ldots f_5 \in \mathbb{Z}[\Omega_5; x, y]$ and the result for $r = 5$ follows too. □

Lemma 3.3.4. *Let C be a covariant of weight p, homogeneous of degree n in the a_i. If $p > n$ then $\boldsymbol{C}(x^k) = 0$ and $\boldsymbol{C}(x^{k-1}y) = 0$.*

Proof. By Theorem 3.2.2, we see that each coefficient of $\boldsymbol{C}(f)$ is isobaric of weight at least p in the a_i (in fact, the i-th coefficient has weight $p + i$). For $f = x^k, x^{k-1}y$ the only non-zero a_i have $i = 0$ or 1. Therefore $\boldsymbol{C}(f) = 0$. □

3.4 Covariants in Arbitrary Characteristic

In this section I give another way to interpret the covariance property that can be used to define covariants in fields of arbitrary characteristic. The covariants defined earlier in terms of generic binary forms will continue to be formulae for covariants of arbitrary characteristic.

Lemma 3.4.1. *Let K be any field. Then $GL_2(K)$ is generated by the set of all matrices of the form*

$$\begin{pmatrix} \kappa & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} 1 & -\nu \\ 0 & 1 \end{pmatrix}, w := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

with $\kappa, \lambda \in K^*$ and $\nu \in K$. The group $SL_2(K)$ is generated by the same set, but with the additional restriction that $\kappa\lambda = 1$.

We find that the action of $\mathrm{GL}_2(K)$ on the coefficients a_i of a binary form of order k agrees with the following action at the generators of $\mathrm{GL}_2(K)$.

Definition 3.4.2. *Define an action of $GL_2(K)$ on $[a_0, \ldots, a_k] \in \mathbb{A}^{k+1}(K)$ by*

$$\begin{pmatrix} 1 & -\nu \\ 0 & 1 \end{pmatrix} : \; a_i \mapsto \sum_{j=0}^{i} \binom{i}{j} a_j \nu^{i-j},$$

$$\begin{pmatrix} \kappa & 0 \\ 0 & \lambda \end{pmatrix} : \; a_i \mapsto \kappa^{i-k} \lambda^{-i} a_i,$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : \; a_i \mapsto (-1)^i a_{k-i}.$$

This extends to an action of $\mathrm{GL}_2(K)$ on $K[a_0, \ldots, a_k]$ that does not place any requirement on the characteristic of K. In fact as 7 divides $\binom{i}{6}$ whenever $6 < i \leq 12$ this also extends to an action on $K[\Omega_r]$ in all characteristics.

Definition 3.4.3 (Covariant, Arbitrary Characteristic). *A binary form $\boldsymbol{C}(\Omega_r) \in \bar{K}[\Omega_r][x, y]$ is a covariant if it is homogeneous in the variables x, y and there is a $p \in \mathbb{Z}_{\geq 0}$ such that for all $g \in GL_2(\bar{K})$*

$$g \cdot \boldsymbol{C}(\Omega_r) = \det(g)^p \boldsymbol{C}(g \cdot \Omega_r),$$

where the action of g on $K[x, y]$ is that of Definition 2.2.1 and the action of g on Ω_r is given by Definition 3.4.2. The integer p is called the weight of the covariant.

'Old-Style' covariants were defined in terms of the coefficients a_i, so they are certainly candidates to be covariants in this more general setting. In fact, any covariant $\boldsymbol{C}(f) \in \mathbb{Z}[\Omega_r][x, y]$ constructed via 'generic forms' is a covariant in arbitrary characteristic. Indeed, the equation witnessing the covariance property must vanish identically and so be valid for all K.

Chapter 4

Klein forms

In this chapter we introduce the Klein forms. These were well studied in the 19th century, not least by Felix Klein who wrote a famous treatise [14] on their connection with solutions to the quintic equation.

4.1 Definitions and Properties

In [14] Felix Klein inscribes the tetrahedron, octahedron, icosahedron in the 2-sphere which he then projects onto the extended complex plane. After a suitable rotation of the sphere, forms whose roots correspond to the vertices of the solid are given by the $\bar{f}_r$ in the following table.

Definition 4.1.1.

r	Solid	The vertices
3	Tetrahedron	$\bar{f}_3 = 81\sqrt{3}\ (y^4 + 2\sqrt{3}x^2y^2 - x^4)$
4	Octahedron	$\bar{f}_4 = 2^8 3^6 \quad xy(x^4 + y^4)$
5	Icosahedron	$\bar{f}_5 = 1728 \quad xy(y^{10} + 11x^5y^5 - x^{10})$

The constant factors in these forms have been chosen so that we get Klein's relations in the form

$$(\frac{1}{2}\boldsymbol{t}(\bar{f}_r))^2 + \boldsymbol{H}(\bar{f}_r)^3 = \bar{f}_r^r.$$

This confirms that k agrees with the number of vertices of the solid and N with the order of the group of rotational symmetries of the solid.

Klein was interested in the complex numbers. However the forms make sense in any algebraically closed field $\bar{K}$. By calculating the discriminants and resultants, we see that the forms $(\frac{1}{2}\boldsymbol{t}(\bar{f}_r), \boldsymbol{H}(\bar{f}_r), \bar{f}_r)$ stay co-prime and have no multiple roots if $\mathrm{char}(\bar{K})$ is zero or co-prime to N.

Proposition 4.1.2. *Suppose that f_1 satisfies*

$$(\frac{1}{2}\boldsymbol{t}(f_1))^2 + \boldsymbol{H}(f_1)^3 = df_1^r \tag{4.1}$$

for some $d \in K^*$. Let $f_2 := \lambda g \cdot f_1$ where $\lambda \in K^*$ and $g \in GL_2(K)$. Then

$$(\frac{1}{2}\boldsymbol{t}(f_2))^2 + \boldsymbol{H}(f_2)^3 = d' \ f_2^r,$$

where $d' = \lambda^{6-r} \det(g)^{-6} d$.

Proof. In equation (4.1) we have that the LHS/RHS is a covariant of weight 6 and homogeneous of degree $6 - r$ in the a_i. The result follows. □

Definition 4.1.3 (Twists). *Define $\mathcal{C}_0(r)$ to be the set of all forms $f = g \cdot \bar{f}_r$ with $g \in GL_2(\bar{K})$ and $\bar{f}_r$ the Klein form given in Definition 4.1.1. For $d \in \bar{K}^*$ we define $\mathcal{C}_0(r, d)$ to be those twists with $\det(g)^{-6} = d$.*

The constraint on $\det(g)$ is equivalent to requiring that

$$(\frac{1}{2}\boldsymbol{t}(f))^2 + \boldsymbol{H}(f)^3 = df^r.$$

Definition 4.1.4 (Rational Twists). *If R is a ring inside $\bar{K}$ we define $\mathcal{C}_0(r, d)(R)$ to be those $f \in \mathcal{C}_0(r, d)$ for which $\Omega_r(f) \subseteq R$, where Ω_r is given in Definition 3.3.1.*

Notation 4.1.5 (Klein forms). *We call $\mathcal{C}_0(3) \cup \mathcal{C}_0(4) \cup \mathcal{C}_0(5)$ the Klein forms, $\mathcal{C}_0(3)$ the tetrahedral Klein forms, $\mathcal{C}_0(4)$ the octahedral Klein forms, and $\mathcal{C}_0(5)$ the icosahedral Klein forms.*

Definition 4.1.6 (The Parameterization $\chi(f)$). *Given $f \in \mathcal{C}_0(r, d)(K)$, we define*

$$\chi(f) := (\frac{1}{2}\boldsymbol{t}(f), \boldsymbol{H}(f), f).$$

This is a parameterization of $\mathcal{D}(r, d)(K)$.

Proposition 4.1.7. *Let R be an integral domain with $N \neq 0$ in R. Then $f \in \mathcal{C}_0(r, d)(R)$ implies that $\boldsymbol{H}(f), \boldsymbol{t}(f) \in R[x, y]$. If furthermore R is integrally closed in its quotient ring then $\boldsymbol{t}(f)/2 \in R[x, y]$.*

Proof. By definition $\Omega_r(f) \subset R$. Hence by Proposition 3.3.3, $\boldsymbol{H}(f), \boldsymbol{t}(f) \in R[x, y]$. Since R has no zero divisors, R being integrally closed implies that $R[x, y]$ is integrally closed. The second claim now follows since

$$\left(\frac{1}{2}\boldsymbol{t}(f)\right)^2 + \boldsymbol{H}(f)^3 = df^r.$$

□

Lemma 4.1.8. *Suppose $f \in \mathcal{C}_0(r,d)(\bar{K})$. Then there is a $g \in GL_2(\bar{K})$ of determinant a primitive 6-th root of unity such that $g \cdot f = f$.*

Proof. If $g \in \mathrm{GL}_2(\bar{K})$ fixes f and $f' = h \cdot f$ for some $h \in \mathrm{GL}_2(\bar{K})$ then $g' = hgh^{-1}$ fixes f', so we only have to demonstrate the claim for a specific form in each of the three classes $\mathcal{C}_0(3)$, $\mathcal{C}_0(4)$ and $\mathcal{C}_0(5)$. The following table (in which ξ_{12} is a primitive 12th root of unity) does this .

r	Solid	Form	g
3	Tetrahedron	$x(x^3+y^3)$	$\begin{pmatrix} \xi_{12}^3 & 0 \\ 0 & \xi_{12}^7 \end{pmatrix}$
4	Octahedron	$xy(x^4+y^4)$	$\begin{pmatrix} 0 & \xi_{12}^{-2} \\ \xi_{12}^{-2} & 0 \end{pmatrix}$
5	Icosahedron	Any	$\begin{pmatrix} \xi_{12} & 0 \\ 0 & \xi_{12} \end{pmatrix}$

□

Corollary 4.1.9. *If $f_1, f_2 \in \mathcal{C}_0(r,d)(\bar{K})$ then f_1, f_2 are $SL_2(\bar{K})$-equivalent.*

Proof. From Definition 4.1.3 we see that there is a $g \in \mathrm{GL}_2(\bar{K})$ with $\det(g)^6 = 1$ such that $g \cdot f_1 = f_2$. By Lemma 4.1.8 we can assume $\det(g) = 1$. □

4.2 Classification of Klein forms

By their nature, the set of forms defined by the vanishing of a covariant is a union of $\mathrm{GL}_2(\bar{K})$-equivalence classes of forms. Thus the set of forms defined by the vanishing of a covariant can often be assigned a geometric meaning. Clebsch wondered what the vanishing of the 4-th tranvectant of the base form over itself implied about the base form. This was answered by Gordan [8], page 204. The answer will turn out to have a great impact on our equations.

Theorem 4.2.1 (Gordan 1887). *Let K be a field and k an integer greater than 3. Suppose that one of the following is true.*

- *$char(K) = 0$.*
- *$k = 4, 6$ or 12; and $char(K) > k - 4$.*
- *$char(K) \geq k^2$.*

Then the 4th covariant $\boldsymbol{\tau}_4(f)$ of a form f of order k is identically zero iff one of the following is true.

- $f \sim x^k$ *or* $f \sim x^{k-1}y$ *(degenerate cases),*
- $k = 4$ *and* $f \sim y(x^3 + y^3)$ *(Tetrahedron),*
- $k = 6$ *and* $f \sim xy(x^4 + y^4)$ *(Octahedron),*
- $k = 12$ *and* $f \sim xy(x^{10} - 11x^5y^5 - y^{10})$ *(Icosahedron),*

where $\sim$ *denotes equivalence modulo* $GL_2(\bar{K})$*.*

Proof. (Sufficiency) We verify that $\boldsymbol{\tau}_4$ vanishes on the Klein forms by direct calculation. The covariant $\boldsymbol{\tau}_4$ vanishes on the degenerate forms by Lemma 3.3.4.

(Necessity) For the necessity we assume that $\boldsymbol{\tau}_4(f) = 0$ and f is not in one of the degenerate cases. From this we will deduce that f is one of the Klein forms. We know that $\boldsymbol{\tau}_4(f)$ has order $2k-8$ and so can be written as

$$\boldsymbol{\tau}_4(f) = \sum_{j=0}^{2k-8} D_j x^{2k-j} y^j,$$

where the D_j are isobaric of degree 2 and weight $4+j$ in the a_i. A calculation gives:

$$D_j = \sum_{i+l=j} \binom{k-4}{i} \binom{k-4}{l} \left[a_i a_{l+4} - 4a_{i+1}a_{l+3} + 3a_{i+2}a_{l+2}\right].$$

We will make heavy use of these explicit equations to deduce the result. These coefficients (up to a constant multiple) for the cases $k = 4, 6, 12$ are given in the Appendix A.

Step I - Show that f has a root of multiplicity 1.

Suppose not. Since f is not degenerate, at least one of its roots has multiplicity $\leq \frac{k}{2}$. Send such a root to infinity so that if a_s is the first non-zero coefficient of f we have $1 < s \leq k/2$.

We have for $2 \leq t \leq k-2$ that:

$$D_{2t-4} = 3\binom{k-4}{t-2}^2 a_t^2 + \ldots$$

where the omitted terms are all isobaric of weight $2t$ but contain an a_i with $i < t$. We have that $a_0, a_1 = 0$. Induction shows that $a_2 \ldots a_{k-2}$ are also zero. As $k - 2 \geq k/2$ we get $a_s = 0$. This contradiction shows that f has a root of multiplicity one.

Step II - Finish off.

We send this simple root to infinity and assume that $[a_0, a_1, a_2 \dots] = [0, 1, 0 \dots]$. From the explicit expansion of $\boldsymbol{\tau}_4$

$$D_0 = a_0 a_4 - 4a_1 a_3 + a_2^2,$$
$$D_j = \cdots + \frac{k}{j} \begin{pmatrix} k-4 \\ j-1 \end{pmatrix} \left[j - 4 + \frac{12}{k} \right] a_1 a_{j+3} + \dots \quad \text{when } j \geq 1, \quad (4.2)$$

where the omitted terms all contain a_0 or an a_i out of the set $\{a_2, \dots, a_{j+2}\}$. I claim that $k = 4, 6$ or 12. Indeed, if not an induction shows that f is equivalent to the degenerate $x^{k-1}y$. By scaling using a diagonal matrix we can assume that we are in one of the following cases:

- $k = 4$ and $f = y(x^3 + y^3)$, or
- $k = 6$ and $f = x^5 y + xy^5 + \dots$, or
- $k = 12$ and $f = x^{11}y - 11x^6y^6 + \dots$,

where the omitted coefficients contain higher powers of y. Furthermore, equation (4.2) shows that the omitted coefficients of f are uniquely determined. This means that f is one of the Klein forms given in the announcement of the theorem. □

We are in a position to give a complete classification of the sets $\mathcal{C}_0(r, d)$.

Theorem 4.2.2 (Classification of Klein forms). *Suppose $N, d \in \bar{K}^*$. If char$(K) = 0$ or char$(K) > k$, then*

$$\begin{aligned}
\mathcal{C}_0(3,d) &= \{f \in \bar{K}[x,y]_4 \;\mid\; \boldsymbol{\tau}_4(f) = 0, \boldsymbol{j}(f) = -4d\},\\
\mathcal{C}_0(4,d) &= \{f \in \bar{K}[x,y]_6 \;\mid\; \boldsymbol{\tau}_4(f) = 0, \boldsymbol{\tau}_6(f) = -72d\},\\
\mathcal{C}_0(5,d) &= \{f \in \bar{K}[x,y]_{12} \;\mid\; \boldsymbol{\tau}_4(f) = 0,\\
&\qquad\qquad 7\boldsymbol{\tau}_6(f) = -360df,\ 7\boldsymbol{\tau}_{12}(f) = 3110400d^2\}.
\end{aligned}$$

Proof. Fix $r \in \{3, 4, 5\}$. Call the right hand sides of the claimed equalities $V(3, d)$, $V(4, d)$, $V(5, d)$.

The last relation in each $V(r, d)$ prevents zero being in $V(r, d)$. The covariants $\boldsymbol{j}, \boldsymbol{\tau}_6, \boldsymbol{\tau}_{12}$ all have weights that are higher than their degree in the a_i. By Lemma 3.3.4, this means that x^k, $x^{k-1}y \notin V(r, d)$. By Theorem 4.2.1, we can restrict attention to f which are $\mathrm{GL}_2(\bar{K})$-equivalent to a Klein form. Using Lemma 3.1.1 and the fact that $\boldsymbol{\tau}_6, \boldsymbol{j}$ have weight 6 and $\boldsymbol{\tau}_{12}$ has weight 12 we get that

$$f \in V(r, d) \iff g \cdot f \in V(r, \det(g)^{-6} d).$$

By Proposition 4.1.2 we only have to show that $\bar{f}_r \in V(r, 1)$. This is verified by direct calculation.

□

Remark 4.2.3. *If you are of the opinion that a binary form of degree* 12 *is by definition non-zero, you can omit the last relation* $\boldsymbol{\tau}_{12}(f) = \ldots$ *from the characterization of* $\mathcal{C}_0(5, d)$.

4.3 Their Symmetry Groups

In this chapter we introduce the symmetry groups of the Klein forms. These are established as abstract groups. For future use, we work out the actual representations of these groups for certain Klein forms.

4.3.1 Definitions

Definition 4.3.1. *Let* $f \in K[x, y]$ *and* $\alpha \in K^*$. *Define*

$$\Gamma_\alpha(f)(K) := \{g \in SL_2(K) \mid g \cdot f = \alpha f\},$$
$$\Gamma(f)(K) := \bigcup_{\alpha \in K^*} \Gamma_\alpha(f)(K).$$

We denote the projective versions of these sets by $\widetilde{\Gamma}_\alpha(f)(K)$ *and* $\widetilde{\Gamma}(f)(K)$. *These are the subsets of* $PSL_2(K)$ *obtained by dividing out by* $\pm I$.

For any $f \in K[x, y]$, the sets $\Gamma(f)(K)$ and $\Gamma_1(f)(K)$ are clearly groups, as are their quotients in $\mathrm{PSL}_2(K)$. The groups $\{\Gamma(\bar{f}_3)(\bar{K}), \Gamma(\bar{f}_4)(\bar{K}), \Gamma(\bar{f}_5)(\bar{K})\}$ are known as the *Binary Tetrahedral*, *Binary Octahedral*, and *Binary Icosahedral Group* respectively. They have order $2N$.

The projective versions $\{\widetilde{\Gamma}(\bar{f}_3), \widetilde{\Gamma}(\bar{f}_4), \widetilde{\Gamma}(\bar{f}_4)\} \subset \mathrm{PSL}_2(\bar{K})$ are isomorphic to the rotational symmetry group of the tetrahedron, octahedron, icosahedron respectively. These groups have order N. The isomorphism arises from our identification of the roots of the Klein form with the vertices of the platonic solid. The projective group is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/r\mathbb{Z})$ which in turn is isomorphic to $\{A_4, S_4, A_5\}$.

In the next sections we will give explicit representations for these groups. If $g \in \Gamma(f)(K)$, then $g \in \Gamma_\alpha(f)(K)$ for some $\alpha = \alpha(g) \in \bar{K}^*$. The map $g \mapsto \alpha(g)$ is a group character. The explicit representations will show that we have the following exact sequence.

$$1 \longrightarrow \Gamma_1(\bar{f}_r) \longrightarrow \Gamma(\bar{f}_r) \xrightarrow{\alpha} \mu_{6-r} \longrightarrow 1.$$

4.3.2 Tetrahedron

Consider the tetrahedral Klein form

$$f = -4y(x^3 - dy^3) \in \mathcal{C}_0(3, d).$$

The form f has zeros at $\infty, \gamma_1, \gamma_1, \gamma_1$, where γ_i are the 3 solutions to $\gamma^3 = d$. We have that

$$\Gamma_1(f) = \langle g_1, g_2, g_3 \mid g_i^2 = g_1 g_2 g_3 = -1 \rangle$$

is the Quaternion Group of order 8, with g_i given by

$$g_i = \frac{1}{\sqrt{-3}} \begin{pmatrix} 1 & 2\gamma_i \\ \gamma_i^{-1} & -1 \end{pmatrix}.$$

The full group $\Gamma(f)$ has order 24 and is given by

$$\Gamma(f) = \left\langle \Gamma_1(f), \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \right\rangle,$$

where ω is a primitive 3rd root of unity.

Permutations of the Vertices

If we look at the projective group we have that $\widetilde{\Gamma}(f) \simeq A_4$ via the permutation that rotations induce on the vertices. We have $\widetilde{\Gamma}_1(f) = V_4$ (the Klein 4 Group). The permutations in $\widetilde{\Gamma}_1(f)$ are the identity and the 180 degree rotations around the axes connecting opposite edges.

4.3.3 Octahedron

Consider the octahedral Klein form

$$f = 36xy(x^4 - dy^4) \in \mathcal{C}_0(4, -3d).$$

It has roots $0, \infty, \beta_i$ where $i = 0, \ldots, 3$ and the β_i are the 4 solutions of $\beta^4 = d$. If we call $f' := 6xy(x^4 - y^4)$, we see that up to a constant f is just $\begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}.f'$ for some β satisfying $\beta^4 = d$. This gives a bijection

$$\Gamma(f') \xrightarrow{\sim} \Gamma(f), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a, & \beta^{-2}b \\ \beta^2 c, & d \end{pmatrix}.$$

We have that

$$\widetilde{\Gamma}_1(f') = \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1+i & -1+i \\ 1+i & 1-i \end{pmatrix} \right\rangle,$$

where i is a primitive 4-th root of unity. The full group $\widetilde{\Gamma}(f')$ is given by

$$\widetilde{\Gamma}(f') = \left\langle \widetilde{\Gamma}_1(f'), \begin{pmatrix} \zeta_8 & 0 \\ 0 & \zeta_8^{-1} \end{pmatrix} \right\rangle,$$

where ζ_8 is a primitive 8-th root of unity.

Permutations of Pairs of Opposite Faces

There is another way of looking at the projective group. We have that $\widetilde{\Gamma}(f) = S_4$ by the permutation that $\Gamma(f)$ induces on the axes joining opposite faces of the octahedron.

The mid-points of the faces are given by the covariant $\boldsymbol{H}(f)$. A calculation shows that these pairs of faces are given by:

$$h_\nu(f) = x^2 + i^\nu(1+i)\beta xy - (-1)^\nu i\beta^2 y^2,$$

where i is a primitive 4-th root of unity, β is a fixed solution to $\beta^4 = d$ and $\nu = 0, 1, 2, 3$.

There are 2 embedded tetrahedrons whose vertices together correspond to the faces of the octahedron. Rotations of the octahedron either preserve the tetrahedra or swap them. We have $\widetilde{\Gamma}_1(f) = A_4$. These are the rotations that preserve the embedded tetrahedrons.

4.3.4 Icosahedron

Consider the icosahedral Klein form

$$f = 1728d\ xy(x^{10} + 11x^5y^5 - y^{10}) \in \mathcal{C}_0(5, d).$$

The zeros of f are $0, \infty,\ \zeta^i(\zeta + \zeta^4),\ \zeta^i(\zeta^2 + \zeta^3)$, where $i = 0, \ldots, 4$ and ζ is a primitive 5th root of unity. $\Gamma(f)$ equals $\Gamma_1(f)$ and is the group of order 120 given by

$$\begin{aligned}\Gamma_1(f) &= \left\langle -I,\ \begin{pmatrix} \zeta^3 & 0 \\ 0 & \zeta^2 \end{pmatrix},\ \frac{1}{\sqrt{5}}\begin{pmatrix} \zeta - \zeta^4, & -\zeta^2 + \zeta^3 \\ -\zeta^2 + \zeta^3, & -\zeta + \zeta^4 \end{pmatrix} \right\rangle \\ &=: \langle -I, S, T \rangle .\end{aligned}$$

Define $U := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then

$$\begin{aligned} S^i &= \begin{pmatrix} \zeta^{3i} & 0 \\ 0 & \zeta^{2i} \end{pmatrix}, \quad US^i = \begin{pmatrix} 0 & -\zeta^{2i} \\ \zeta^{3i} & 0 \end{pmatrix}, \\ S^iTS^j &= \frac{1}{\sqrt{5}}\begin{pmatrix} \zeta^{3i+3j}(\zeta - \zeta^4), & -\zeta^{3i+2j}(\zeta^2 - \zeta^3) \\ -\zeta^{2i+3j}(\zeta^2 - \zeta^3), & -\zeta^{2i+2j}(\zeta - \zeta^4) \end{pmatrix}, \\ US^iTS^j &= \frac{1}{\sqrt{5}}\begin{pmatrix} \zeta^{2i+3j}(\zeta^2 - \zeta^3), & \zeta^{2i+2j}(\zeta - \zeta^4) \\ \zeta^{3i+3j}(\zeta - \zeta^4), & -\zeta^{3i+2j}(\zeta^2 - \zeta^3) \end{pmatrix}, \end{aligned}$$

where $i = 0, \ldots, 4$ and $j = 0, \ldots, 4$ is an enumeration of the $N = 60$ elements of the projective group $\widetilde{\Gamma}(f)$.

Permutations of Embedded Octahedra

There is another way to consider the projective group $\widetilde{\Gamma}(f)$. The 30 edges of the icosahedron define the vertices of 5 embedded octahedra. The group $\widetilde{\Gamma}(f)$ is isomorphic to A_5 by the permutation action it induces on these 5 embedded octahedra. The edges of the icosahedron are given by the covariant $\boldsymbol{t}(f)$. The vertices of the octahedra can be calculated (see [7], page 62). They are given by

$$t_\nu = (\zeta^{3\nu}x^6 + \zeta^{2\nu}y^6) + 2xy(\zeta^{2\nu}x^4 + \zeta^{3\nu}y^4) - 5x^2y^2(\zeta^{\nu}x^2 + \zeta^{4\nu}y^2),$$

where $\nu = 0, \ldots, 4$.

Chapter 5

General Properties of Parameterizations

The previous chapter has provided us with a set of binary forms $\mathcal{C}_0(r,d)$. Any $f \in \mathcal{C}_0(r,d)$ gives a parameterization $\chi(f)$ and we have the following situation.

$$\begin{array}{ccc} \mathcal{C}_0(r,d) & & f \\ {\scriptstyle\pi}\big\downarrow & & \big\downarrow \\ \mathcal{D}(r,d) & & \pi(f) := \chi(f)(1,0). \end{array}$$

Our route via 19th century Invariant Theory forced us to assume that our fields have $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > k$. We will start by showing how such parameterizations can be defined in fields of arbitrary characteristic. This is then taken as our definition of parameterizations for the rest of the thesis.

We call this larger class of parameterizations $\mathcal{C}(r,d)$ and show that it is indeed a generalization of the set $\mathcal{C}_0(r,d)$. Various basic properties of parameterizations are then proven. We show that parameterizations continue to behave well, provided that $N \in K^*$.

In this chapter R is a ring inside a field K whose characteristic is arbitrary unless otherwise specified. The algebraic closure of K is denoted by $\bar{K}$.

5.1 Definitions in Arbitrary Characteristic

We want to define parameterizations for more general fields as the set of $(k+1)$-tuples of values that can be assigned to the set Ω_r so that relations given in characterization of $\mathcal{C}_0(r,d)$ in Theorem 4.2.2 are satisfied. Once explicit equations with this property have been chosen, these cut out an algebraic subset of $\mathbb{A}^{k+1}$ that will become our definition of $\mathcal{C}(r,d)$.

5.1.1 (The Defining Equations). *Consider the coefficients of $\boldsymbol{\tau}_4(f)$. These are elements D_i of $\mathbb{Z}[\Omega_r]$. Divide out by any integer content to produce elements $D_i' \in \mathbb{Z}[\Omega_r]$. We require that the polynomials D_i' vanish. Next we take the auxiliary relations mentioned in Theorem 4.2.2. These are elements of $\mathbb{Z}[\Omega_r, d][x, y]$. I consider these as binary forms in the variables x and y. The coefficients are elements of $\mathbb{Z}[\Omega_r, d]$ that we require to vanish.* [1] *Finally, when $r = 5$, an equation labelled D_4^* in Appendix A is required to vanish (If $char(K) \neq 5$ the vanishing of D_4^* is implied by the vanishing of the D_i'). The resulting collections of polynomials defining $\mathcal{C}(r, d)$ are given in Appendix A.*

Definition 5.1.2 ($\mathcal{C}(r, d)$). *We define $\mathcal{C}(r, d) \subset \mathbb{A}^{k+1}$ to be the algebraic set defined by the polynomials given in Appendix A.*

I have chosen not to introduce a new symbol for $(7a_6)$. Instead I try to always bracket this expression and leave it to the reader to note that when $\mathrm{char}(K) = 7$ and the icosahedral equations are being considered, care should be taken. $(7a_6)$ is not zero but, as an element of Ω_5, is transcendental over $\bar{K}$.

The class $\mathcal{C}(r, d)$ has been constructed to be a generalization of $\mathcal{C}_0(r, d)$. We make this explicit in the following proposition.

Proposition 5.1.3. *Suppose K is a field with $char(K) = 0$ or $char(K) > k$. We identify $f \in K[x, y]$ of order k with $\Omega_r(f) \in \mathbb{A}^{k+1}(K)$. Then*

$$f \in \mathcal{C}_0(r, d) \;\Leftrightarrow\; \Omega_r(f) \in \mathcal{C}(r, d).$$

Proof. This follows from the classification of $\mathcal{C}_0(r, d)$ given in Theorem 4.2.2. □

To emphasize the difference between $\mathcal{C}(r, d)$ and $\mathcal{C}_0(r, d)$ I will initially use the symbol φ when referring to an element in $\mathcal{C}(r, d)$.

Definition 5.1.4 ($f(\varphi)$). *We associate a binary form $\boldsymbol{f}(\varphi)$ with an element $\varphi \in \mathbb{A}^{k+1}$ by*

$$\boldsymbol{f}(\varphi) := \sum_{i=0}^{k} a_i \begin{pmatrix} k \\ i \end{pmatrix} x^{k-i} y^i. \tag{5.1}$$

This is a K-linear and $\mathrm{GL}_2(\bar{K})$-equivariant map. However, the map is not injective if $\mathrm{char}(K) \leq k$.

[1] We explicitly **do not** divide out any integer content in the auxiliary equations.

Definition 5.1.5 (χ, π). *If char$(K) \neq 2$ we define $\chi(\varphi)$ and $\pi(\varphi)$ for any $\varphi := [a_0, \ldots, a_k] \in \mathcal{C}(r, d)$ by*

$$\begin{aligned}\chi(\varphi) &:= \left(\frac{1}{2}\boldsymbol{t}(\varphi), \boldsymbol{H}(\varphi), \boldsymbol{f}(\varphi)\right), \\ \pi(\varphi) &:= \chi(\varphi)(1,0) \\ &= \left(\frac{1}{2}(a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3),\ a_0 a_2 - a_1^2,\ a_0\right).\end{aligned}$$

5.2 Properties of $\mathcal{C}(r, d)$

Some properties of $\mathcal{C}(r, d)$ continue to hold in all characteristics. Other properties only hold with some restriction the characteristic of K. In this section we (re)establish various properties of $\mathcal{C}(r, d)(K)$. We will see that $\mathcal{C}(r, d)$ is well behaved if $N \in K^*$. The proofs, which are often technical, are given in Appendix B.

Definition 5.2.1 (Parabolic Subgroup). *For a ring R, define the parabolic subgroup of $SL_2(R)$ as*

$$\{\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in R\}.$$

Elements of this group are called the parabolic elements.

Note that the parabolic elements can also be characterized as the elements of the stabilizer of the point $(1, 0)$.

5.2.1 Properties for all K

Lemma 5.2.2. *If K is a field and $d \in K^*$ then $\mathcal{C}(r, d)(K) \neq \emptyset$.*

Proof. See Appendix B, Lemma B.0.1. □

Proposition 5.2.3. *Suppose K a field and $d \in K^*$. If $g \in GL_2(K)$ and $\lambda \in K^*$ then*

$$\varphi \in \mathcal{C}(r, d) \Rightarrow \lambda g \cdot \varphi \in \mathcal{C}(r, d'),$$

where $d' = \lambda^{6-r} \det(g)^{-6} d$.

Proof. See Appendix B, Proposition B.0.3. □

5.2.2 Properties whenever $2 \in K^*$

Proposition 5.2.4. *Suppose that $2, d \in K^*$. If $(X, Y, Z) \in \mathcal{D}(r, d) - (0, 0, 0)$, then there is a $\varphi \in \mathcal{C}(r, d)(K)$ with $\pi(\varphi) = (X, Y, Z)$.*

Proof. See Appendix B, Proposition B.0.2. □

5.2.3 Properties whenever $N \in K^*$

Proposition 5.2.5 (Canonical Lift). *Suppose $N, d \in K^*$. If $(X, Y, Z) \in \mathcal{D}(r, d) - (0, 0, 0)$, then there is a canonical $\varphi \in \mathcal{C}(r, d)(K)$ with $\pi(\varphi) = (X, Y, Z)$. It is given by*

$$\varphi := \begin{cases} [Z, 0, \frac{Y}{Z}, \frac{2X}{Z}, \dots] & \text{if } Z \neq 0, \\ [0, \frac{-X}{Y}, 0, \dots] & \text{if } Z = 0, \end{cases} \tag{5.2}$$

where the omitted terms are uniquely determined by the defining equations of $\mathcal{C}(r, d)$.

If $\varphi' \in \mathcal{C}(r, d)(K)$ also satisfies $\pi(\varphi') = (X, Y, Z)$, then there is a unique parabolic element $g \in SL_2(K)$ such that $\varphi' = g \cdot \varphi$.

Proof. See Appendix B, Proposition B.0.7. □

Lemma 5.2.6. *Suppose $N, d \in \bar{K}^*$. Then $\mathcal{C}(r, d)(\bar{K})$ is a homogeneous $SL_2(\bar{K})$-space and $\mathcal{C}(r) := \bigcup_{d \in \bar{K}^*} \mathcal{C}(r, d)$ is a homogeneous $GL_2(\bar{K})$-space.*

Proof. See Appendix B, Lemma B.0.5. □

Definition 5.2.7. *Let $\varphi \in \mathbb{A}^{k+1}$ and $\alpha \in K^*$. Define*

$$\Gamma_\alpha(\varphi)(K) := \{g \in SL_2(K) \mid g \cdot \varphi = \alpha\varphi\},$$
$$\Gamma(\varphi)(K) := \bigcup_{\alpha \in K^*} \Gamma_\alpha(\varphi)(K).$$

Lemma 5.2.8. *If $N, d \in K^*$ and $\varphi \in \mathcal{C}(r, d)$ then $\#\Gamma(\varphi)(\bar{K}) = 2N$. Furthermore, if φ corresponds to the coefficients of one of the forms chosen in § 4.3, then the explicit description of the group called $\Gamma(f)$ in § 4.3 is the group $\Gamma(\varphi)(\bar{K})$.*

Proof. See Appendix B, Lemma B.0.8. □

5.3 Properties of the map χ

The set of K-specializations of the parameterizations associated to $\varphi, \varphi' \in \mathcal{C}(r, d)(K)$ will be equal if φ, φ' lie in the same $\mathrm{SL}_2(K)$-orbit. In this section we give a partial converse. If $N \in K^*$ and φ, φ' lie in different $\mathrm{SL}_2(K)$-orbits, we show that $(0, 0, 0)$ is the only common K-specialization.

Proposition 5.3.1. *Suppose $N \in K^*$. If $\varphi \in \mathcal{C}(r, d)(\bar{K})$ and $(X, Y, Z) \in \mathcal{D}(r, d)(\bar{K})$, then there is an $s \in \bar{K}^2$ such that $\chi(\varphi)(s) = (X, Y, Z)$.*

Proof. Let φ' be the canonical lift of (X, Y, Z) given by Proposition 5.2.5. By Lemma 5.2.6, $\mathcal{C}(r, d)(\bar{K})$ is a homogeneous $\mathrm{SL}_2(\bar{K})$-space. Therefore, there is a $g \in \mathrm{SL}_2(\bar{K})$ so that $\varphi = g \cdot \varphi'$. Then $s = g(1, 0)$ works. □

Lemma 5.3.2. *Suppose $\Gamma \subset SL_2(K)$ is a finite group and the characteristic of K is either zero or co-prime to the order of Γ. Then for any $s \in K^2$*

$$s \neq (0,0) \;\Rightarrow\; Stab_\Gamma(s) = 1.$$

Proof. Suppose $s \neq (0,0)$. By replacing Γ by a conjugate group we can assume that $s = (1,0)$. Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} =: g$ is in the stabilizer. Therefore

$$g = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}.$$

Since $\det(g) = 1$ we have $d = 1$. As the order of g divides the order of the Γ, the conditions on the characteristic of K imply that $b = 0$. □

Lemma 5.3.3. *Suppose $N, d \in K^*$. Suppose that $\varphi \in \mathcal{C}(r,d)(K)$. Then*

$$\chi(\varphi)(s) = (0,0,0) \Leftrightarrow s = (0,0).$$

Proof. This follows since the resultant of $\boldsymbol{f}(\varphi)$ and $\boldsymbol{H}(\varphi)$ is divisible only by primes dividing Nd. □

Proposition 5.3.4. *Suppose $N, d \in K^*$ and $(X,Y,Z) \in \mathcal{D}(r,d)(K)$ is non-zero. Suppose that $\varphi_1, \varphi_2 \in \mathcal{C}(r,d)(K)$ and $s_1, s_2 \in K^2$ satisfy*

$$\chi(\varphi_1)(s_1) = \chi(\varphi_2)(s_2) = (X,Y,Z).$$

Then there is a unique $g \in SL_2(K)$ such that

$$s_1 = gs_2, \quad \varphi_1 = g \cdot \varphi_2.$$

Proof. (1) Existence. Choose $g_i \in \mathrm{SL}_2(K)$ so that $g_i s_i = (1,0)$. Then $\pi(g_i \cdot \varphi_i) = (X,Y,Z)$. By Proposition 5.2.5, there is a parabolic $h \in \mathrm{SL}_2(K)$ so that $g_1.\varphi_1 = hg_2.\varphi_2$. Set $g := g_1^{-1} h g_2$. The element g satisfies $\varphi_1 = g \cdot \varphi_2$. Since h is parabolic $s_1 = gs_2$. (2) Uniqueness. If not, we could find a non-trivial $g \in \Gamma_1(\varphi_1)(K)$ such that $gs_2 = s_2$. This contradicts Lemma 5.3.2 with $\Gamma = \Gamma_1(\varphi_1)(K)$. □

Theorem 5.3.5. *Suppose $N, d \in K^*$. Then*

$$\mathcal{D}(r,d)(K) - (0,0,0) = \bigcup_{\varphi \in \mathcal{C}(r,d)(K)} \pi(\varphi).$$

Furthermore, for $\varphi_1, \varphi_2 \in \mathcal{C}(r,d)(K)$

- *$\chi(\varphi_1)(K^2) = \chi(\varphi_2)(K^2)$ if φ_1, φ_2 are $SL_2(K)$-equivalent,*
- *$\chi(\varphi_1)(K^2) \wedge \chi(\varphi_2)(K^2) = \{(0,0,0)\}$ otherwise.*

Proof. The first claim is just Proposition 5.2.5. The other claims are from Lemma 5.3.3 and Proposition 5.3.4. □

5.4 All parameterizations are twists of each other

We have defined a family of parameterizations of $\mathcal{D}(r,d)(K)$ by taking $\chi(f)$ and letting f range over $\mathcal{C}(r,d)$. One might worry that we are missing out on many useful parameterizations by restricting ourselves in this way.

In this section I show that this is not so. Assuming that $N \in K^*$, we show that any parameterization is derived from a Klein form. In this section we follow Hartshorne, Algebraic Geometry [10], Chapter IV. In particular a *curve* means a complete, non-singular curve over an algebraically closed field.

Theorem 5.4.1 (Hurwitz). *Let $\phi : C_1 \to C_2$ be a non-constant separable map of curves. Then:*

$$2g_1 - 2 \geq (\deg\ \phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1),$$

where g_i is the genus of C_i and $e_\phi(P)$ are the ramification indices. Further, equality holds iff either:

- *$char(\bar{K}) = 0$; or*
- *$char(\bar{K}) = p > 0$ and p does not divide $e_\phi(P)$ for all $P \in C_1$.*

Proof. See [10], Chapter IV, Proposition 2.2 and Corollary 2.4. □

Lemma 5.4.2. *Suppose $\psi : C_1 \to C_2$ is a non-constant map of curves of degree n over a field $\bar{K}$. If $n \in \bar{K}^*$, then the map is separable.*

Proof. Let $\bar{K}(C_i)$ be the function fields. If the map is not separable, then $\mathrm{char}(\bar{K}) = p > 0$ and there is an intermediate field $\bar{K}'$ so that $\bar{K}(C_2) \subset \bar{K}' \subset \bar{K}(C_1)$, and $[\bar{K}' : \bar{K}(C_2)] = p^u$ for some $u > 0$. This means that n is zero as an element of $\bar{K}$. □

Theorem 5.4.3. *Suppose $N, d \in K^*$ and $f \in \mathcal{C}(r,d)(K)$. Suppose $(\hat{X}, \hat{Y}, \hat{Z})$ is a co-prime parameterization of $\mathcal{D}(r,d)(K)$ of order $n > 0$. Then N divides n and there are co-prime binary forms $u, v \in \bar{K}[x,y]$ of order n/N so that*

$$(\hat{X}, \hat{Y}, \hat{Z}) = \chi(f)(u, v).$$

Proof. (Step I - Reduce to a claim about a map between curves).

Dehomogenize and rename the variables so that $\chi(f) \in \bar{K}[t]^3$ and $(\hat{X}, \hat{Y}, \hat{Z}) \in \bar{K}[x]^3$.

Consider the map of curves $\psi : \mathfrak{X} \to \mathbb{P}^1$ corresponding to the finite field extension of $\bar{K}(x)$ obtained by appending a root of the polynomial

$$p(t) := p(t,x) := \boldsymbol{t}(f)^2 - 4\frac{\hat{X}^2}{\hat{Y}^3}\boldsymbol{H}(f)^3$$

to $\bar{K}(x)$. Call this field extension $\bar{K}(t,x)$.

We will show that

the map ψ is a non-constant separable, unramified map of curves.

Assuming this, we apply Hurwitz' Theorem, and deduce that ψ is an isomorphism $\mathfrak{X} \simeq \mathbb{P}^1$. Therefore $K(t,x) = K(x)$ and t is in $K(x)$. Going back to homogeneous notation we can find co-prime binary forms u, v and $\gamma \in \bar{K}^*$ so that

$$\chi(f)(u,v) = \gamma(\hat{X}, \hat{Y}, \hat{Z}).$$

By scaling u, v, we can assume that $\gamma = 1$. The theorem is proven.

The map ψ is clearly non-constant. We are left to show that ψ is separable and unramified.

(Step II - The map ψ is separable).

The group $\Gamma(f) \subset \mathrm{GL}_2(\bar{K})$ acts transitively on the roots of $p(t)$. Therefore, the extension $\bar{K}(t,x) : \bar{K}(x)$ is Galois of degree dividing N. In particular, it is separable by Lemma 5.4.2.

(Step III - The map ψ is unramified).

For any $x_0 \in \bar{K}$, the group $\Gamma(f)$ acts freely on the roots of $p(t, x_0)$ unless one of $\hat{X}(x_0)$,$\hat{Y}(x_0)$,$\hat{Z}(x_0)$ is zero. Ramification is only possible above points x_0 where $p(t, x_0)$ has multiple roots. This means that ramification is only possible above primes corresponding to $x_0 \in \bar{K}$ for which $\hat{X}(x_0)\hat{Y}(x_0)\hat{Z}(x_0) = 0$.

Suppose that the prime ideal Q corresponds to a point $x_0 \in \bar{K}$ with $\hat{X}(x_0) = 0$, and P is a prime ideal with $\psi(P) = Q$. Then P must correspond to a point (x_0, t_0) with $\boldsymbol{t}(t_0) = 0$. Let $\hat{\vartheta}_P$ and $\hat{\vartheta}_Q$ be the completions of the local rings at P and Q. We apply a change of co-ordinates $x \mapsto x + x_0$ and $t \mapsto t + t_0$ so that the ideals can be written $P = (t, x)$, $Q = (x)$.

Since $\boldsymbol{t}$ has distinct roots, the inclusion $\hat{\vartheta}_Q \subset \hat{\vartheta}_P$ can be written

$$\bar{K}[[x]] \subset \bar{K}[[x,t]]$$

for some t satisfying $\alpha(t)t^2 - \beta(x)x^{2s} = 0$ with s a positive integer, $\alpha(t) \in \bar{K}[[t]]^*$ and $\beta(x) \in \bar{K}[[x]]^*$.

As $\bar{K}$ is algebraically closed, we can can take n-th roots of α and β and assume that $\alpha = \beta = 1$. This shows that $\hat{\vartheta}_P = \hat{\vartheta}_Q$. Therefore, there is no ramification above x_0 satisfying $\hat{X}(x_0) = 0$. Similarly, there is no ramification above x_0 satisfying $\hat{Y}(x_0) = 0$ or $\hat{Z}(x_0) = 0$.

Conclusion: ψ is unramified.

□

Corollary 5.4.4. *Suppose $N, d \in \bar{K}^*$ and χ is a co-prime parameterization of $\mathcal{D}(r,d)(K)$ of order N. Then there is a $\lambda \in K^*$ and $f \in \mathcal{C}(r, \lambda^{-6}d)(K)$ so that*

$$\chi = (\frac{1}{2}\lambda^3 \boldsymbol{t}(f), \lambda^2 \boldsymbol{H}(f), f).$$

Proof. Let $(\hat{X}, \hat{Y}, \hat{Z}) := \chi$. Choose $f \in \mathcal{C}(r,d)(K)$. By Theorem 5.4.3 , there is a $g \in \mathrm{GL}_2(\bar{K})$ so that $g \cdot \chi(f) = (\hat{X}, \hat{Y}, \hat{Z})$. Letting $\lambda = \det(g)$, this expands to

$$\begin{aligned}
\hat{Z} &= g \cdot f, \\
\hat{Y} &= g \cdot \boldsymbol{H}(f) = \lambda^2 \boldsymbol{H}(g \cdot f), \\
\hat{X} &= \frac{1}{2} g \cdot \boldsymbol{t}(f) = \frac{1}{2}\lambda^3 \boldsymbol{t}(g \cdot f).
\end{aligned}$$

We have $g \cdot f \in \mathcal{C}(r, \lambda^{-6}d)$ by Proposition 5.2.3. Since all the binary forms above are in $K[x,y]$, we have $\lambda \in K^*$. □

Chapter 6

Lifting from Rings R

In this chapter R is any ring (with 1) without zero divisors and K is its quotient field, which we assume has $\mathrm{char}(K) \neq 2$. The algebraic closure of K is denoted by $\bar{K}$.

We will show in this chapter that if $(X, Y, Z) \in \mathcal{D}(r, d)(R)$ is co-prime in R, then there is a $\varphi \in \mathcal{C}(r, d)(R)$ with $\pi(\varphi) = (X, Y, Z)$. Under mild extra conditions on R we prove that any other $\varphi' \in \mathcal{C}(r, d)(R)$ with $\pi(\varphi') = (X, Y, Z)$ is $\mathrm{SL}_2(R)$-equivalent to φ.

6.1 Existence of Lifts

Theorem 6.1.1 (Lifting Theorem). *Suppose R is a ring inside a field K with char$(K) \neq 2$ and $d \in R$ is non-zero. If $(X, Y, Z) \in \mathcal{D}(r, d)(R)$ is co-prime, then there exists a $\varphi \in \mathcal{C}(r, d)(R)$ with*

$$\pi(\varphi) = (X, Y, Z).$$

Proof. **Step I - Deal with the case $Z = 0$.**

If $Z = 0$, set $a := -X/Y$ and consider the following binary form φ.

Case	φ
Tetrahedron	$[0, a, 0, 0, 4a^{-2}d]$
Octahedron	$[0, a, 0, 0, 0, 12a^{-1}d, 0]$
Icosahedron	$[0, a, 0, 0, 0, 0, \frac{144d}{7}, 0, 0, 0, 0, -a^{-1}(144d)^2, 0]$

A calculation shows that $\varphi \in \mathcal{C}(r, d)(K)$ and $\pi(\varphi) = (X, Y, Z)$. Since $\gcd(X, Y) = 1$ we have $X, Y \in R^*$, so that $a \in R^*$. In particular $\varphi \in \mathcal{C}(r, d)(R)$.

Step II - $Z \neq 0$.

Since $\mathrm{char}(K) \neq 2$, Proposition 5.2.5 gives us a $\varphi \in \mathcal{C}(r, d)(K)$ with $\pi(\varphi) = (X, Y, Z)$. We will show that this initial φ can be twisted so that it has the properties in the announcement of the Theorem.

Since $\pi(\varphi) = (X, Y, Z)$ we have

$$a_0 = Z, \quad (a_0 a_2 - a_1^2) = Y, \quad (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) = 2X.$$

We let a matrix $g := \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix}$ act on φ for an appropriate $\alpha \in \bar{K}$. The matrix g is a parabolic element of $\mathrm{SL}_2(\bar{K})$, so $\pi(g \cdot \varphi) = \pi(\varphi)$. By varying α we can ensure that a_1 takes on any chosen value. Since Y, Z are co-prime, Y is invertible modulo Z^r and we choose α so that $a_1 \in R$ and $a_1 \equiv -XY^{-1}$ modulo Z^r. Replace φ by $g \cdot \varphi$. I claim that $\varphi \in \mathcal{C}(r, d)(R)$.

Let S be the multiplicative set generated by Z, and R_S the localization of R by S. By the defining equations of $\mathcal{C}(r, d)$ we see that $\Omega_r(\varphi) \subset R_S$. Our task will be to show that $\Omega_r(\varphi) \subset R$. This is clearly true if $Z \in R^*$, so we assume it is not.

Let $\nu : R_S \mapsto \mathbb{Z} \cup \infty$ be the valuation coming from Z. I.e. $\nu(\alpha) := \max\{n \mid Z^{-n}\alpha \in R\}$. From the formulae $\boldsymbol{H}(1, 0) = Y$ and $\boldsymbol{t}(1, 0) = 2X$ we get

$$\begin{aligned} a_0 a_2 &\equiv Y + (\frac{X}{Y})^2 = -\frac{dZ^r}{Y^2}, \\ a_0^2 a_3 &\equiv -X\frac{X^2 + Y^3}{Y^3} = \frac{-dXZ^r}{Y^3}, \end{aligned}$$

where $\equiv$ means equivalence modulo Z^r.

This shows that $a_0, a_1, a_2, a_3 \in R$ and that

$$\nu(a_0) = 1, \ \nu(a_1) = 0, \ \nu(a_2) \geq r - 1, \ \nu(a_3) \geq r - 2.$$

Step III - Finishing Off.

The remaining calculations used to show that $\Omega_r(f) \subset R$ depend on the $r \in \{3, 4, 5\}$ under consideration.

Step IIIa - Tetrahedron, $Z \neq 0$.

We already have that $a_0, a_1, a_2, a_3 \in R$ and that

$$\nu(a_0) = 1, \quad \nu(a_1) = 0, \quad \nu(a_2) \geq 2, \quad \nu(a_3) \geq 1.$$

The equation $\boldsymbol{\tau}_4(\varphi) = 0$ expands to

$$0 = a_0 a_4 - 4a_1 a_3 + 3a_2^2,$$

which implies that $a_4 \in R$. We conclude that $\Omega_3(\varphi) \subset R$, as required.

Step IIIb - Octahedron, $Z \neq 0$.

We already have that $a_0, a_1, a_2, a_3 \in R$ and that

$$\nu(a_0) = 1, \quad \nu(a_1) = 0, \quad \nu(a_2) \geq 3, \quad \nu(a_3) \geq 2.$$

The defining equations of $\mathcal{C}(4,d)$ derived from the initial coefficients of $\boldsymbol{\tau}_4(\varphi)=\sum_{i=0}^4 D_i x^{4-i}y^i$ are

$$\begin{aligned} D_0/1 : 0 &= a_4a_0 - 4a_3a_1 + 3a_2^2,\\ D_1/2 : 0 &= a_5a_0 - 3a_4a_1 + 2a_3a_2,\\ D_2/1 : 0 &= a_6a_0 - 9a_4a_2 + 8a_3^2. \end{aligned}$$

Here the labelling $D_1/2$ means that the equation was obtained by dividing the coefficient D_1 of $\boldsymbol{\tau}_4(\varphi)$ by 2 and equating the resulting polynomial to zero. Going through these equations we deduce

$$\begin{aligned} D_0 = 0 &\implies \nu(a_4)\geq 1,\\ D_1 = 0 &\implies \nu(a_5)\geq 0,\\ D_2 = 0 &\implies \nu(a_6)\geq 3. \end{aligned}$$

We conclude that $\Omega_4(\varphi)\subset R$, as required.

Step IIIc - Icosahedron, $Z\neq 0$.

We already have that $a_0,a_1,a_2,a_3\in R$ and that

$$\nu(a_0)=1,\ \nu(a_1)=0,\ \nu(a_2)\geq 4,\ \nu(a_3)\geq 3.$$

The defining equations of $\mathcal{C}(5,d)$ derived from the initial coefficients of $\boldsymbol{\tau}_4(\varphi)=\sum_{i=0}^4 D_i x^{4-i}y^i$ are

$$\begin{aligned} D_0/1 :\ & 0 = a_0a_4 - 4a_1a_3 + 3a_2^2,\\ D_1/8 :\ & 0 = a_0a_5 - 3a_1a_4 + 2a_2a_3,\\ D_2/4 :\ & 0 = a_0(7a_6) - 12a_1a_5 - 15a_2a_4 + 20a_3^2,\\ D_3/56 :\ & 0 = a_0a_7 - 6a_2a_5 + 5a_3a_4,\\ D_4/14 :\ & 0 = 5a_0a_8 + 12a_1a_7 - 6a_2(7a_6) - 20a_3a_5 + 45a_4^2,\\ D_5/56 :\ & 0 = a_0a_9 + 6a_1a_8 - 6a_2a_7 - 4a_3(7a_6) + 27a_4a_5,\\ D_6/28 :\ & 0 = a_0a_{10} + 12a_1a_9 + 12a_2a_8 - 76a_3a_7 - 3a_4(7a_6) + 72a_5^2,\\ D_7/8 :\ & 0 = a_0a_{11} + 24a_1a_{10} + 90a_2a_9 - 130a_3a_8 - 405a_4a_7 + 60a_5(7a_6),\\ D_8/1 :\ & 0 = a_0a_{12} + 60a_1a_{11} + 534a_2a_{10} + 380a_3a_9 - 3195a_4a_8\\ &\qquad\qquad - 720a_5a_7 + 60(7a_6)^2,\\ D_9/8 :\ & 0 = a_1a_{12} + 24a_2a_{11} + 90a_3a_{10} - 130a_4a_9 - 405a_5a_8 + 60(7a_6)a_7. \end{aligned}$$

We also have the equation labelled D_4^*.

$$D_4^* :\ a_0^3a_8 = 12a_0a_1a_2a_3 + 18a_0a_2^2a_4 - 24a_0a_2a_3^2 + 4a_0^2a_3a_5 - 9a_0^2a_4^2.$$

Going through the equations in the order D_0,D_1,D_2,D_3,D_4^*,D_5,D_6,D_7 shows that:

$$\nu(a_4) \geq 2, \quad \nu(a_5) \geq 1, \quad \nu(7a_6) \geq 0, \quad \nu(a_7) \geq 4, \quad \nu(a_8) \geq 3,$$
$$\nu(a_9) \geq 2, \quad \nu(a_{10}) \geq 1, \quad \nu(a_{11}) \geq 0.$$

We are assuming that $Z \notin R^*$. This means that a_0, a_1 are non-zero and co-prime. Therefore from equation D_9 we deduce that $\nu(a_{12}) \geq 4$.

We have shown that the a_i (respectively $7a_6$) are in R. I.e. we have proven that $\Omega_5(\varphi) \subset R$, as required.

□

6.2 Uniqueness of Lifts

Definition 6.2.1. *We say that a ring R is* '2Nice' *if R is a domain, integrally closed in its quotient field, and either $2 \in R^*$ or (2) is a prime ideal.*

Theorem 6.2.2 (Uniqueness Theorem). *Suppose R is a '2Nice' ring inside a field K with $N \in K^*$ and $d \in R$ is non-zero.*

Suppose $(X, Y, Z) \in \mathcal{D}(r, d)(R)$ is co-prime and $f, f' \in \mathcal{C}(r, d)(R)$ satisfy

$$\pi(f) = \pi(f') = (X, Y, Z).$$

Then there is an $\alpha \in R$ so that

$$f' = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} \cdot f \quad .$$

Proof. We let $[a_0, \ldots, a_k]$ denote the coefficients of f and *dashed* versions denote the coefficients of f'. We will show that we can apply a map of the form $x \mapsto x + \alpha y$ for some $\alpha \in R$ to f and a map of the form $x \mapsto x + \alpha' y$ for some $\alpha' \in R$ to f' so that the two forms become equal.

(Case I : $Z = 0$). We have that $a_0 = 0$ and $a_1 = -Y/X \in R^*$.

Since the leading term of $\boldsymbol{\tau}_4(f)$ is $a_0 a_4 - 4a_1 a_3 + 3a_2^2$, we have that $\frac{a_2}{2}^2 \in R$. Since R is '2Nice' this implies $a_2 \in 2R$. We replace x by $x - \frac{a_2}{2a_1} y$, so that $a_2 = 0$. The remaining a_i are completely determined by the equations defining $\mathcal{C}(r, d)$.

(Case II : $Z \neq 0$). We have $a_0 = a_0' = Z$. Combining the formulae $2X = \boldsymbol{t}(f)(1, 0)$ and $Y = \boldsymbol{H}(f)(1, 0)$ gives

$$2(a_1 - a_1')Y = Z^2(a_3 - a_3') - Z(a_1 a_2 - a_1' a_2'). \tag{6.1}$$

As R is '2Nice' there are 3 possibilities (not mutually exclusive):

- $2 \in R^*$,
- 2 is prime and divides $Z(a_3 - a_3') - (a_1 a_2 - a_1' a_2')$,
- 2 is prime and divides $Z = a_0 = a_0'$.

If the last holds, then as the leading term of $\boldsymbol{\tau}_4(f)$ is $a_0a_4 - 4a_1a_3 + 3a_2^2$, its vanishing implies that 2 divides a_2. Similarly 2 divides a_2' . This shows that one of first two possibilities always holds.

Using the fact that Y, Z are co-prime, we find an $\alpha' \in R$ so that $a_1 - a_1' = \alpha Z$. Replacing x by $x + \alpha' y$ in f' makes $a_1' = a_1$. Furthermore, a_2 is determined from $\boldsymbol{H}(f)(1,0) = Y$, and a_3 from $\boldsymbol{t}(f)(1,0) = 2X$. This means that $a_2 = a_2'$ and $a_3 = a_3'$. The remaining a_i are completely determined by the equations defining $\mathcal{C}(r,d)$. Conclusion: $f = f'$. □

Corollary 6.2.3. *Suppose R is a '2Nice' ring inside a field K with $N \in K^*$ and $d \in R$ is non-zero.*

Suppose $(X,Y,Z) \in \mathcal{D}(r,d)(R)$ is co-prime, ζ is an element of R satisfying $\zeta^6 = 1$, and that $f, f' \in \mathcal{C}(r,d)(R)$ satisfy

$$\pi(f) = (X,Y,Z), \quad \pi(f') = (\zeta^3 X, \zeta^2 Y, Z).$$

Then there is an $\alpha \in R$ so that

$$f' = \begin{pmatrix} 1 & -\alpha \\ 0 & \zeta^{-1} \end{pmatrix} \cdot f \quad .$$

Proof. Replacing y by ζy in f produces a new form f'' with the coefficients a_i replaced by $\zeta^i a_i$. Since $\boldsymbol{t}(f)(1,0)$,$\boldsymbol{H}(f)(1,0)$ and $f(1,0)$ are isobaric in the a_i of weight $3, 2, 0$ respectively, we have

$$\pi(\begin{pmatrix} 1 & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \cdot f) = (\zeta^3 X, \zeta^2 Y, Z).$$

This means that we can assume that $\zeta = 1$. The result, therefore, follows from Theorem 6.2.2. □

Theorem 6.2.4 (Uniqueness Theorem, Version 2). *Suppose R is a '2Nice' ring inside a field K with $N \in K^*$ and $d \in R$ is non-zero.*

Suppose $(X,Y,Z) \in \mathcal{D}(r,d)(R)$ is co-prime, ζ is an element of R satisfying $\zeta^6 = 1$, and that $f, f' \in \mathcal{C}(r,d)(R)$ and $s, s' \in R^2$ satisfy

$$\chi(f)(s) = (X,Y,Z), \quad \chi(f')(s') = (\zeta^3 X, \zeta^2 Y, Z).$$

Then there is a $g \in GL_2(R)$ with $\det(g) = \zeta^{-1}$ so that

$$f' = g \cdot f \ .$$

Proof. As $f, \boldsymbol{H}(f) \in R[x,y]$ and $\chi(f)(s)$ is co-prime in R, we have that the entries of s are co-prime in R. Therefore, there is a $g \in \mathrm{SL}_2(R)$ so that $g(1,0) = s$. We replace f by $g \cdot f$ and assume that $s = (1,0)$. Similarly we can assume that $s' = (1,0)$. The result follows from Corollary 6.2.3. □

6.3 The Twisting Matrices

We know that if $N \in K^*$ and $d \in R$ is non-zero, then $\mathcal{C}(r,d)(\bar{K})$ consists of a single $\mathrm{SL}_2(\bar{K})$ orbit. Assume that R is a domain and $(X,Y,Z) \in \mathcal{D}(r,d)(R)$ is co-prime. In this section we take $f \in \mathcal{C}(r,d)(R)$ and investigate what can be said about the entries of a matrix $g \in \mathrm{SL}_2(\bar{K})$ such that $\pi(g \cdot f) = (X,Y,Z)$. We establish conditions in which g can be assumed to be in $\mathrm{SL}_2(\bar{R})$, where $\bar{R}$ is the integral closure of R in $\bar{K}$.

Lemma 6.3.1 (General Integrality Criterion). *Let R be an entire ring. Let $z_1, \ldots, z_m$ be elements of some extension field of its quotient field K. Assume that each z_s $(s = 1, \ldots, m)$ satisfies a polynomial relation*

$$z_s^{d_s} + g_s(z_1, \ldots, z_m) = 0$$

where $g_s(Z_1, \ldots, Z_m) \in R[Z_1, \ldots, Z_m]$ is a polynomial of total degree $< d_s$. Then $z_1, \ldots, z_m$ are integral over R.

Proof. See Theorem 3.7 of chapter VII in Lang's Algebra [16]. □

Corollary 6.3.2. *Let R be a domain with quotient field K, and let $\bar{K}$ be an algebraic closure of K. Let $\bar{R}$ be the integral closure of R in $\bar{K}$. Suppose $f_1, f_2 \in R[x,y]$ are forms with $Res(f_1, f_2) \in R^*$. Then for any $u, v \in \bar{K}$*

$$f_1(u,v), f_2(u,v) \in R \quad \Longrightarrow \quad u, v \in \bar{R}.$$

Proof. By the properties of resultants, there are forms $h_1, h_2 \in R[x,y]$ such that

$$h_1 f_1 + h_2 f_2 = \mathrm{Res}(f_1, f_2) x^n.$$

Therefore u, v satisfy the relation

$$\mathrm{Res}(f_1, f_2) x^n - f_1(u,v) h_1(x,y) - f_2(u,v) h_2(x,y) = 0,$$

where the h_i have degree less than n. Similarly, there are $h_1', h_2' \in R[x,y]$ of degree less than n so that u, v satisfy the relation

$$\mathrm{Res}(f_1, f_2) y^n - f_1(u,v) h_1'(x,y) - f_2(u,v) h_2'(x,y) = 0.$$

By Lemma 6.3.1, $u, v \in \bar{R}$. □

Proposition 6.3.3. *Let R be a domain, integrally closed in its quotient field K, and $\bar{K}$ be an algebraic closure of K. Let $\bar{R}$ be the integral closure of R in $\bar{K}$.*

Suppose $N, d \in R^*$. Suppose $f \in \mathcal{C}(r,d)(R)$ and $(X,Y,Z) \in \mathcal{D}(r,d)(R)$ are co-prime in R. Then there is a $g \in SL_2(\bar{R})$ such that $g \cdot f \in \mathcal{C}(r,d)(R)$ and

$$\pi(g \cdot f) = (X,Y,Z).$$

Proof. Let $H := \boldsymbol{H}(f)$. By Proposition 5.3.1 there are $u, v \in \bar{K}$ such that $\chi(f)(u,v) = (X,Y,Z)$. Since $f \in \mathcal{C}(r,d)$ and $N, d \in R^*$, we have that $\mathrm{Res}(f, \boldsymbol{H}(f)) \in R^*$. Hence, by Corollary 6.3.2, $u, v \in \bar{R}$.

As Y, Z are co-prime in R and $k, 2k-4 \in R^*$, we can find $\alpha, \beta \in R$ so that

$$\alpha k Z + (2k-4)\beta Y = 1. \tag{6.2}$$

We substitute

$$Z = f(u,v) = \frac{1}{k}\left(u\frac{\partial f}{\partial x}(u,v) + v\frac{\partial f}{\partial y}(u,v)\right),$$
$$Y = \boldsymbol{H}(u,v) = \frac{1}{2k-4}\left(u\frac{\partial H}{\partial x}(u,v) + v\frac{\partial H}{\partial y}(u,v)\right)$$

into equation (6.2). Rearranging gives $uv' - vu' = 1$ where

$$v' = \alpha\frac{\partial f}{\partial x}(u,v) + \beta\frac{\partial H}{\partial x}(u,v), \quad -u' = \alpha\frac{\partial f}{\partial y}(u,v) + \beta\frac{\partial H}{\partial y}(u,v).$$

Let $g^{-1} := \begin{pmatrix} u & u' \\ v & v' \end{pmatrix}$. We claim that $g \in \mathrm{SL}_2(\bar{R})$ is the matrix we are looking for.

Certainly $g \in \mathrm{SL}_2(\bar{R})$ and $f' := g \cdot f \in \mathcal{C}(r,d)(\bar{R})$. It remains to show that $f' \in \mathcal{C}(r,d)(R)$. As R is integrally closed in its quotient field K, we only need to show that the coefficients $a'_0, \ldots, a'_k$ of f' are in K.

We have $a'_0 = f(u,v) = Z$, so that $a'_0 \in R$. Furthermore

$$\begin{aligned} k a'_1 &= \frac{\partial}{\partial y} f(ux + u'y, vx + v'y)\Big|_{x=1,y=0} \\ &= u'\frac{\partial f}{\partial x}(u,v) + v'\frac{\partial f}{\partial y}(u,v)\Big|_{x=1,y=0} \\ &= -\beta \begin{pmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial H}{\partial x} & \frac{\partial H}{\partial y} \end{pmatrix}(u,v) \\ &= -\beta k^2 (k-1)^2 \boldsymbol{t}(f)(u,v), \end{aligned}$$

so that $a'_1 = -2Bk(k-1)^2 X$. Hence $a'_1 \in R$. If $Z \neq 0$, the remaining a'_i are forced to be in $Q(R)$ by the defining equations of $\mathcal{C}(r,d)$ and the fact that $X, Y, Z \in R$.

If $Z = 0$, they are forced to be in $Q(R)$ once we can show that $a'_2 \in Q(R)$. We have $X, Y \in R^*$, so that $a'_1 \in R^*, a'_2 \in \bar{R}$. We also have $2 \in R^*$. We further twist f by the matrix

$$\begin{pmatrix} 1 & -\frac{a'_2}{2a'_1} \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\bar{R}).$$

This leaves a'_0, a'_1 unchanged, but makes $a'_2 = 0$. The result follows.

□

Chapter 7

Galois Cohomology

In this chapter we will use Galois Cohomology to categorize the set $\mathcal{C}(r,d)(K)$ modulo $\mathrm{SL}_2(K)$-equivalence. The main reference to Galois Cohomology is Jean-Pierre Serre [22], especially Chapter X, §5. However, much can be gained from Silverman's 1st book on Elliptic curves [23], Chapter X, §2, where similar methods are use to categorize twists of elliptic curves.

7.1 Definitions

Let K be any field and $\bar{K}$ the algebraic closure. We know that $G_{\bar{K}/K} := \mathrm{Gal}(\bar{K}/K)$ acts on the left on $\mathrm{GL}_2(\bar{K})$ by

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto {}^{\sigma}A := \begin{pmatrix} \sigma(a) & \sigma(b) \\ \sigma(c) & \sigma(d) \end{pmatrix}.$$

We also denote ${}^{\sigma}A$ by $\sigma(A)$.

We give $\mathrm{GL}_2(\bar{K})$ the discrete topology, in which all sets are open, and $G_{\bar{K}/K}$ the profinite topology, in which a fundamental set of neighborhoods of the identity is given by the subgroups of the form $\mathrm{Gal}(\bar{K}/L)$ with L/K a finite Galois field extension of K.

We assume that we have groups $\Gamma_1 \leq \Gamma \leq \mathrm{GL}_2(\bar{K})$ closed under this action.

Definition 7.1.1 (1-cocycles). *The set of 1-cocycles of $G_{\bar{K}/K}$ into Γ is the set of* continuous *maps*

$$\xi : G_{\bar{K}/K} \to \Gamma, \quad \sigma \mapsto \xi_\sigma,$$

that also satisfy

$$\xi_{\sigma\tau} = \xi_\sigma {}^{\sigma}\xi_\tau \quad \textit{for all} \quad \sigma, \tau \in G_{\bar{K}/K}.$$

We denote the set of 1-cocycles by $Z^1(K,\Gamma)$.

Definition 7.1.2 (Equivalence via a coboundary from Γ_1). *We say that two 1-cocycles ξ, ζ are equivalent via a coboundary from Γ_1 if there is an $h \in \Gamma_1$ such that*

$$\zeta_\sigma = h^{-1}\xi_\sigma {}^\sigma h \quad \textit{for all} \quad \sigma \in G_{\bar{K}/K}.$$

Definition 7.1.3 (1st Cohomology Set).

$$H^1(G_{\bar{K}/K}, \Gamma : \Gamma_1) := \frac{\textit{1-cocycles from } G_{\bar{K}/K} \textit{ into } \Gamma}{\textit{equivalence via a coboundary from } \Gamma_1}.$$

As a notational convenience, we usually just write this as $H^1(K, \Gamma : \Gamma_1)$. Furthermore, if $\Gamma_1 = \Gamma$ we just write $H^1(K, \Gamma)$.

7.2 $\mathcal{C}(r,d)$ modulo $\mathrm{SL}_2(K)$-equivalence

This section contains our main application of Galois Cohomology. We assume that K is a field with $N \in K^*$.

For each $r \in \{3,4,5\}$ we choose a $d_0 \in K^*$ and $\bar{f} \in \mathcal{C}(r,d_0)(K)$. These will be fixed for the rest of this section. Let $\Gamma := \Gamma(\bar{f})$ and $\Gamma_1 := \Gamma_1(\bar{f})$.

For each $d \in K^*$ choose a $\lambda \in \bar{K}^*$ so that $\lambda^{6-r} = d/d_0$. By Corollary 4.1.9, $\mathcal{C}(r,d)(\bar{K})$ can be categorized as

$$\mathcal{C}(r,d)(\bar{K}) = \{\lambda g \cdot \bar{f} \mid \ g \in \mathrm{SL}_2(\bar{K})\}. \tag{7.1}$$

Theorem 7.2.1. *Suppose $N, d \in K^*$ and we categorize $\mathcal{C}(r,d)(\bar{K})$ via (7.1). Then the map*

$$\frac{\mathcal{C}(r,d)(K)}{SL_2(K) \textit{ equivalence}} \hookrightarrow H^1(K, \Gamma(\bar{f}) : \Gamma_1(\bar{f})),$$
$$\lambda g \cdot \bar{f} \mapsto \left(\ \sigma \mapsto g^{-1}\sigma(g) \ \right),$$

is well-defined and injective.
The image consists of exactly those $\xi \in H^1(K, \Gamma(\bar{f}) : \Gamma_1(\bar{f}))$ such that

$$\xi_\sigma \in \Gamma_{\lambda/\sigma(\lambda)} \quad \textit{for all} \quad \sigma \in G_{\bar{K}/K}. \tag{7.2}$$

Proof. (Step I - The map is well defined). The map $\sigma \mapsto g^{-1}\sigma(g)$ is a cocycle. A priori it has values in $\mathrm{SL}_2(\bar{K})$. However, since $\lambda g \cdot \bar{f} = \sigma(\lambda g \cdot \bar{f}) = \sigma(\lambda)\sigma(g)\bar{f}$, it takes values in $\Gamma(\bar{f})$.

If $f_1 = \lambda g_1 \bar{f}$ is $\mathrm{SL}_2(K)$-equivalent to $f_2 = \lambda g_2 \bar{f}$, then

$$g_2 = h g_1 \delta \ \text{ for some } \ h \in \mathrm{SL}_2(K) \text{ and } \delta \in \Gamma_1(\bar{f}).$$

This means that

$$g_2^{-1}\sigma(g_2) = \delta^{-1} g_1^{-1}\sigma(g_1)\sigma(\delta) \ \text{ for all } \ \sigma \in \mathrm{Gal}(\bar{K}/K).$$

Hence f_1, f_2 map to cocycles that differ by a coboundary from Γ_1. Therefore the map is well-defined.

(Step II - the map is injective). Suppose, conversely, that two maps differ only by a coboundary from Γ_1. This means that there is a $\delta \in \Gamma_1$ with

$$g_2^{-1}\sigma(g_2) = \delta^{-1}g_1^{-1}\sigma(g_1)\sigma(\delta) \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}/K),$$

so that

$$h := g_2\delta^{-1}g_1^{-1} \in \mathrm{SL}_2(K).$$

Therefore $g_2 = hg_1\delta$. This means that $\lambda g_1 \bar{f}$ is $\mathrm{SL}_2(K)$-equivalent to $\lambda g_2 \bar{f}$. Therefore the map is injective.

(Step III - the image is as claimed).
Suppose that $\lambda g \cdot \bar{f} \in K[x, y]$. Then

$$\lambda g \bar{f} = \sigma(\lambda g \cdot \bar{f}) = \sigma(\lambda)\sigma(g).\bar{f}$$

for all $\sigma \in G_{\bar{K}/K}$, so that cocycles in the image satisfy (7.2). Conversely, suppose that ξ is a cocycle in the image. Then it is certainly a cocycle in the more standard $H^1(K, \mathrm{SL}_2(\bar{K}))$. By "Hilbert 90 for $\mathrm{SL}_2(\bar{K})$" (see [20] Chapter X), this cohomology set is trivial. Therefore, there is a $g \in \mathrm{SL}_2(\bar{K})$ so that

$$\xi_\sigma = g^{-1}\sigma(g) \quad \text{for all} \quad \sigma \in G_{\bar{K}/K}.$$

Since ξ satisfies (7.2), $f' := \lambda g \cdot \bar{f} \in K[x, y]$. By construction f' maps to ξ. □

7.3 Other Cohomology Sets

In section 7.2 we were able to classify $\mathcal{C}(r, d)$ modulo $\mathrm{SL}_2(K)$-equivalence using the 1st Cohomology Set $H^1(K, \Gamma : \Gamma_1)$. In this section we will categorize $\mathcal{C}(r, d)(K)$ modulo $\mathrm{GL}_2(K)$ matrices with determinant a sixth root of unity. The reason for wanting to categorize such sets, is that we can then apply Corollary 6.2.3 to shorten lists of parameterizations by

- Identifying $\pm X$, and
- Identifying $\zeta_3 Y$ with Y if ζ_3 is in the ground field.

We will continue to assume, as in section 7.2, that K is a field with $N \in K^*$, and we have chosen $d_0 \in K^*$ and a $\bar{f} \in \mathcal{C}(r, d_0)(K)$. We give a classification of $\mathcal{C}(r, d_0)$ modulo $g \in \mathrm{GL}_2(K)$ with $\det(g)^6 = 1$. We do not

generalize to $d \neq d_0$. This seems to make the theorems more complicated, but not more illuminating.

In this section we identify K^* with the diagonal matrices of $\mathrm{GL}_2(K)$. I.e. $u \in \bar{K}^*$ is identified with $\begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \in \mathrm{GL}_2(K)$.

For any positive integer m let $\mu_m \subset \bar{K}$ be the m-th roots of unity. Clearly $\mu_{2m}\Gamma$ is the group of matrices g with $\det(g)^m = 1$ that permute the roots of $\bar{f}$. We define

$$(\mu_{2m}\Gamma)_1 := \{g \in \mu_{2m}\Gamma(\bar{f}) \mid g \cdot \bar{f} = \bar{f}\}.$$

Lemma 7.3.1. *Let $m \in \{1, 2, 3, 6\}$. Then the sequence*

$$1 \longrightarrow \Gamma_1 \longrightarrow (\mu_{2m}\Gamma)_1 \xrightarrow{\det} \mu_m \longrightarrow 1$$

is exact.

Proof. Clearly Γ_1 is the kernel of the det arrow, so we only have to prove that det is onto. Suppose that $\zeta^2 \in \mu_m$. Then $\zeta \cdot f = \alpha f$ for some α satisfying $\alpha^{6-r} = 1$. Choose $g \in \Gamma$ with $g \cdot f = \alpha^{-1} f$. Then ζg is a member of $(\mu_{2m}\Gamma)_1$ of determinant ζ^2. Hence the det arrow is onto. □

This means that we can pass in cohomology to the exact sequence

$$H^1(K, \Gamma_1) \longrightarrow H^1(K, (\mu_{2m}\Gamma)_1) \longrightarrow H^1(K, \mu_m). \tag{7.3}$$

By Lemma 4.1.8 and Corollary 4.1.9, for any given $m \in \{1, 2, 3, 6\}$, $\mathcal{C}(r, d_0)(\bar{K})$ can be categorized as

$$\mathcal{C}(r, d)(\bar{K}) = \{g \cdot \bar{f} \mid \ g \in \mathrm{GL}_2(K), \det(g)^m = 1\}. \tag{7.4}$$

Theorem 7.3.2. *Let $m \in \{1, 2, 3, 6\}$. We categorize $\mathcal{C}(r, d_0)(\bar{K})$ via (7.4). Then the map*

$$\frac{\mathcal{C}(r, d_0)(K)}{GL_2(K) \text{ with } \det(g)^m = 1} \to Im\left(H^1(K, \Gamma_1) \to H^1(K, (\mu_{2m}\Gamma)_1)\right),$$
$$\lambda g \cdot \bar{f} \mapsto \left(\ \sigma \mapsto g^{-1}\sigma(g) \ \right),$$

is well-defined and bijective.

Proof. (Sketch) (Step I - the map is well defined and injective).

The map $\xi_\sigma := g^{-1}\sigma(g)$ is a cocycle taking values in $\mu_{2m}\Gamma$. This means that we can write $g = \epsilon h$ for $h \in \Gamma$, $\epsilon \in \mu_{2m}$. Therefore ξ_σ becomes trivial in $H^1(K, \mu_m)$. By (7.3) the cocycle is the image of some $\xi' \in H^1(K, \Gamma_1)$. The rest of the proof that the map is well-defined and injective is similar to the proof of Theorem 7.2.1.

(Step II - the map is onto). Conversely, if ξ is in the claimed image it becomes trivial in $H^1(K, \mu_m)$. Therefore, it can be written

$$\xi_\sigma = \frac{\sigma(\epsilon)}{\epsilon}\xi'_\sigma \quad \text{for some} \quad \epsilon \in \mu_{2m},\ \xi' \in Z^1(K, \Gamma).$$

By Hilbert 90 for $\mathrm{SL}_2(\bar{K})$ we can find $h \in \mathrm{SL}_2(\bar{K})$ so that

$$\xi'_\sigma = h^{-1}\sigma(h) \quad \text{for all} \quad \sigma \in G_{\bar{K}/K}.$$

One checks that $f' := (\epsilon h) \cdot \bar{f} \in \mathcal{C}(r, d_0)(K)$ and that f' maps to ξ. □

An obvious next step in the quest to shorten the lists of parameterizations would be to identify Z with $\zeta_r Z$, where ζ_r is a primitive r-th root of unity whenever ζ_r is in the field K. The following proposition shows that this is not usually necessary.

Proposition 7.3.3. *Suppose $\chi(f)(s_1, s_2) = (X, Y, Z)$. Let ζ_3, i, ζ_5 be primitive 3-rd, 4-th, and 5-th roots of unity. Then*

Case	ζ	$\chi(f)(\zeta s_1, \zeta s_2) =$
Tetrahedron	ζ_3	$(X, \zeta_3 Y, \zeta_3 Z)$
Octahedron	$\sqrt{-i}$	$(-X, Y, iZ)$
Icosahedron	ζ_5^3	$(X, Y, \zeta_5 Z)$

7.4 The Splitting of the Forms

We can also use Cohomology Sets to deduce how a $\sigma \in \mathrm{Gal}(\bar{K}/K)$ permutes the roots of any covariant of f. For finite fields we can apply this to the Frobenius element to deduce how such a form splits.

Proposition 7.4.1. *Identify the $SL_2(K)$-orbit of $f = \lambda g \cdot \bar{f} \in \mathcal{C}(r, d)(K)$, using Theorem 7.2.1, with an image point in $H^1(K, \Gamma(\bar{f}) : \Gamma_1(\bar{f}))$. Let ξ be a cocycle representing this image point.*

Let $\boldsymbol{C}$ be a covariant and label the roots of $\boldsymbol{C}(\bar{f})$ as $\beta_1, \ldots \beta_m$. Then for any $\sigma \in Gal(\bar{K}/K)$ the natural action of σ on the roots of $\boldsymbol{C}(f)$ is the same as the following action on the roots of $\boldsymbol{C}(\bar{f})$

$$\beta \mapsto \xi_\sigma\ \sigma(\beta).$$

Proof. As $\boldsymbol{C}(\bar{f})$ has roots $\beta_1, \ldots \beta_m$; $\boldsymbol{C}(f)$ has roots $g(\beta_1), \ldots g(\beta_m)$. Furthermore, the following diagram commutes.

$$\begin{array}{ccc} z & \xrightarrow{g} & g(z) \\ \downarrow & & \sigma\downarrow \\ g^{-1}\sigma(g)(\sigma(z)) & \xrightarrow{g} & \sigma(g)(\sigma(z)) \end{array} .$$

This shows that the permutation on the roots agrees when we choose the cocycle to be

$$\xi_\sigma := g^{-1}\sigma(g).$$

We are left to show that the permutation is independent of the representative cocycle. If we adjust ξ by a coboundary from Γ_1, we replace ξ by

$$\xi'_\sigma := (gh)^{-1}\sigma(gh), \quad \text{for some } h \in \Gamma_1(\bar{f}).$$

However, $f = \lambda g \cdot \bar{f} = \lambda(gh)\cdot\bar{f}$. As $\boldsymbol{C}$ is a covariant, $h\beta_1, \ldots, h\beta_m$ is another enumeration of the roots of $\boldsymbol{C}(\bar{f})$. The result follows as before.

□

7.5 Special Consideration for Finite Fields

In this section we assume that $K = \mathbb{F}_q$ is a finite field with q elements and F is a Frobenius element of $\mathrm{Gal}(\bar{K}/K)$. We give an alternative description of the 1st Cohomology Set. This alternate description is considerably simpler to apply in both theoretical and practical situations.

Definition 7.5.1. *Let $K = \mathbb{F}_q$ be a finite field and F a Frobenius element of $Gal(\bar{K}/K)$. Assume that $\Gamma_1 \leq \Gamma$ are subgroups of $SL_2(K)$ that are closed under the action of F. We define (F, Γ_1)-conjugacy as the equivalence relation on Γ given by*

$$\gamma \sim \gamma' \Leftrightarrow \textit{there exists } \delta \in \Gamma_1 \textit{ with } \gamma' = \delta^{-1}\gamma(F(\delta)).$$

Theorem 7.5.2 (Lang's Theorem). *Let $K = \mathbb{F}_q$ be a finite field and F the Frobenius. Then the map $SL_2(\bar{K}) \to SL_2(\bar{K})$:*

$$g \mapsto g^{-1}F(g)$$

is surjective.

Proof. See [15]. □

We also need the following lemma, which makes use of the fact that F generates $\mathrm{Gal}(\bar{K}/K)$ topologically.

Lemma 7.5.3. *Suppose $\xi', \xi \in Z^1(K, GL_2(\bar{K}))$ are 1-cocycles. Then*

$$\xi_F = \xi'_F \quad \Rightarrow \quad \xi = \xi'.$$

Proof. Suppose that $\xi_F = \xi'_F$. Let $G := \mathrm{Gal}(\bar{K}/K)$ and define

$$\Theta := \{\sigma \in G \mid \xi_\sigma = \xi'_\sigma\}.$$

It is an easy exercise to show that Θ is a group. As 1-cocycles are continuous, the group is closed in the pro-finite topology of G. As Θ contains the Frobenius F and the cyclic group generated by F is dense in G, the group Θ is dense in G. Since Θ is closed and dense in G, it equals G. □

Proposition 7.5.4. *Let $K = \mathbb{F}_q$ be a finite field and F a Frobenius element of $Gal(\bar{K}/K)$. Assume that $\Gamma_1 \leq \Gamma$ are subgroups of $SL_2(K)$ that are closed under the action of $Gal(\bar{K}/K)$. Then the map*

$$\begin{aligned} H^1(K, \Gamma : \Gamma_1) &\to \frac{\Gamma}{(F, \Gamma_1) - \textit{conjugacy}}, \\ \xi &\mapsto \xi_F \end{aligned}$$

is well defined and bijective.

Proof. (Step I - The map is well defined).

Suppose that $\xi, \xi' \in Z^1(K, \Gamma)$ are equivalent via a coboundary from Γ_1. This means that there is an $h \in \Gamma_1$ such that

$$\xi'_\sigma = h^{-1}\xi_\sigma\sigma(h) \quad \text{for all} \quad \sigma \in G_{\bar{K}/K}.$$

In particular $\xi'_F = h^{-1}\xi_F F(h)$, so that ξ_F and ξ'_F are (F, Γ_1)-conjugate. This shows that the map is well-defined.

(Step II - It is injective).

Conversely, if ξ_F and ξ'_F are (F, Γ_1)-conjugate then there is an $h \in \Gamma_1$ so that

$$\xi'_F = h^{-1}\xi_F F(h).$$

By Lemma 7.5.3, the cocycles ξ'_σ and $h^{-1}\xi_\sigma\sigma(h)$ agree everywhere. Hence ξ, ξ' are then equivalent via the coboundary $h \in \Gamma_1$. This means that the map is injective.

(Step III - It is surjective).

Finally if $\delta \in \Gamma$, we can apply Lang's Theorem and find a $g \in \mathrm{SL}_2(K)$ so that $\delta = g^{-1}F(g)$. We define

$$\xi_\sigma := g^{-1}\sigma(g).$$

This is a cocycle. Since $\xi_F \in \Gamma$, we have that $\xi_\sigma \in \Gamma$ for all σ in the cyclic group generated by F. As cocycles are continuous (by definition), Γ is closed, and F generates $\mathrm{Gal}(\bar{K}/K)$ topologically, we have that $\xi_\sigma \in \Gamma$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$.

Hence we have an $\xi \in Z^1(K, \Gamma)$ that maps to δ. Hence the map is surjective.

□

Theorem 7.5.5. *Let $K = \mathbb{F}_q$ be a finite field and F the Frobenius. Let $\bar{f} \in \mathcal{C}(r, d_0)$ be the Klein form chosen in section 7.2 and $\Gamma := \Gamma(\bar{f})$. Any $f \in \mathcal{C}(r,d)(\bar{K})$ can be written $f = \lambda g \cdot \bar{f}$ with $g \in SL_2(\bar{K})$. The map*

$$\frac{\mathcal{C}(r,d)(K)}{SL_2(K)\text{-}equivalence} \hookrightarrow \frac{\Gamma_{\lambda/F(\lambda)}}{(F,\Gamma_1)\text{-}conjugacy},$$
$$\lambda g \cdot \bar{f} \mapsto g^{-1}F(g)$$

is well-defined and bijective.

Proof. The map is a combination of the maps given in Theorem 7.2.1 and Proposition 7.5.4. It follows that the map is well-defined and injective.

To show that the map is surjective, pick any element of $\Gamma_{\lambda/F(\lambda)}$. By Lang's Theorem (Theorem 7.5.2) this can be written $g^{-1}F(g)$ for some $g \in \mathrm{SL}_2(\bar{K})$. Since

$$F(\lambda g.\bar{f}) = \lambda g \cdot \bar{f} \;\Leftrightarrow\; g^{-1}F(g) \in \Gamma_{\lambda/F(\lambda)},$$

we have that $f' := \lambda g.\bar{f} \in \mathcal{C}(r,d)(K)$. The binary form f' maps to $g^{-1}F(g)$, so the map is surjective. □

Chapter 8

Parameterizations in Finite Fields

In this chapter we examine parameterizations of $\mathcal{D}(r,d)(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field with q elements and $N, d \in \mathbb{F}_q^*$. By Theorem 5.3.5, we can assume that parameterizations are of the form $\chi(f)$ with $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$. Furthermore, giving a set of parameterizations specializing to all of $\mathcal{D}(r,d)(\mathbb{F}_q)$ is equivalent to giving a representative f from every $\mathrm{SL}_2(\mathbb{F}_q)$-orbit of $\mathcal{C}(r,d)(\mathbb{F}_q)$.

In sections 8.1–8.3 we state and prove formulae for the number of $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$, along with the values of various attributes that can be assigned to these orbits.

In sections 8.4–8.5 we analyze these results in terms of the automorphism that the Frobenius F induces on the group $\Gamma_1(\bar{f})$, where $\bar{f}$ is a chosen element of $\mathcal{C}(r,d)(\mathbb{F}_q)$. The Frobenius F determines an element in the group

$$\frac{\text{Automorphisms of } \Gamma_1}{\text{Inner Automorphisms}}.$$

We show that the number of $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$ depends only on the value of F in this group.

In the last section we show how the number of $\mathrm{SL}_2(\mathbb{F}_q)$-orbits can be deduced from the action that F induces on the projective groups — i.e. the automorphism induced on the Platonic Solid. This method is less computational than the method presented in section 8.3.

8.1 Results

We will prove the following theorems in this chapter.

Theorem 8.1.1 (Weak Version). *Suppose $\mathbb{F}_q$ is a finite field with q elements and $N, d \in \mathbb{F}_q^*$. Then the number of $SL_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$ is given in the following table.*

r	*Condition*	*# Orbits*
3	$q \equiv 1(3), d \in \mathbb{F}_q^{*3}$	5
	$q \equiv 1(3), d \notin \mathbb{F}_q^{*3}$	2
	$q \equiv 2(3)$	3
4	$-3d \in \mathbb{F}_q^{*2}$	7
	$-3d \notin \mathbb{F}_q^{*2}$	3
5	$q \equiv \pm 1(5)$	9
	$q \equiv \pm 2(5)$	5

Definition 8.1.2. *For a given $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$ we call the number $\#\Gamma_1(f)(\mathbb{F}_q)$ the $\mathbb{F}_q$-multiplicity of f, or just the multiplicity if this is clear from the context.*

The choice of name can be explained by the following proposition.

Proposition 8.1.3. *Suppose K is a field and $N, d \in K^*$. Suppose that $f \in \mathcal{C}(r,d)(K)$, $s \in \mathbb{F}_q^2 - (0,0)$ and that $\chi(f)(s) = (X,Y,Z)$. Then $\chi(f)^{-1}(X,Y,Z)$ is the $\Gamma_1(f)(K)$-orbit of s.*

Proof. This follows from Lemma 5.3.3 and Proposition 5.3.4. □

Corollary 8.1.4. *Suppose $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$ and $N, d \in \mathbb{F}_q^*$. Then $\chi(f)$ has exactly $\frac{q^2-1}{\#\Gamma_1(f)(\mathbb{F}_q)}$ non-zero $\mathbb{F}_q$-specializations.*

The multiplicity of f and how f splits in $\mathbb{F}_q[x,y]$ is the same for all forms in an $\mathrm{SL}_2(\mathbb{F}_q)$-orbit of $\mathcal{C}(r,d)(\mathbb{F}_q)$.

Theorem 8.1.5 (Strong Version). *The $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$ have multiplicities and split into irreducible factors as given in tables 8.1, 8.2 and 8.3.*

In the tables (e.g.) Splitting= $f_1^4 f_2 + 4f_6 + 2f_2^3$ means that Klein forms in the 1st $SL_2(\mathbb{F}_q)$-orbit split into 4 linear factors and a quadratic factor, the forms in the next 4 orbits are irreducible, and the last 2 orbits contain Klein forms that are the product of 3 irreducible quadratic factors.

	$d \in \mathbb{F}_q^{*3}$	$d \notin \mathbb{F}_q^{*3}$
$q \equiv 1(3)$	5 Orbits Multiplicities=$[4,4,4,8,8]$	2 Orbits Multiplicities=$[2,2]$
$q \equiv 2(3)$	3 Orbits Multiplicities=$[2,4,4]$	
$q \equiv 1(3)$	Splitting= $3f_2^2 + 2f_1^4$	Splitting=$2f_1 f_3$
$q \equiv 2(3)$	Splitting= $f_1^2 f_2 + 2f_4$	

Table 8.1: The Tetrahedron

	$-3d \in \mathbb{F}_q^{*2}$	$-3d \notin \mathbb{F}_q^{*2}$
	7 Orbits Multiplicities=$[4,6,6,6,6,24,24]$	3 Orbits Multiplicities=$[2,4,4]$
$q \equiv 1(4)$	Splitting=$f_1^2 f_2^2 + 4f_3^2 + 2f_1^6$	Splitting= $f_2^3 + 2f_1^2 f_4$
$q \equiv 3(4)$	Splitting=$f_1^4 f_2 + 4f_6 + 2f_2^3$	Splitting= $f_1^2 f_2^2 + 2f_2 f_4$

Table 8.2: The Octahedron

	$q \equiv \pm 1(5)$	$q \equiv \pm 2(5)$
	9 Orbits Multiplicities=$[4,6,6,$ $10,10,10,10,120,120]$	5 Orbits Multiplicities=$[4,4,6,6,6]$
$q \equiv 1(5)$	Splitting= $f_2^6 + 2f_3^4 + 4f_1^2 f_5^2 + 2f_1^{12}$	
$q \equiv \pm 2(5)$		$2f_1^2 f_2 f_4^2 + f_4^3 + 2f_{12}$
$q \equiv 4(5)$	$f_1^4 f_2^4 + 2f_6^2 + 4f_2 f_{10} + 2f_2^6$	

Table 8.3: The Icosahedron

8.2 Checking Particular Cases

It is possible to calculate the number of $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$, along with the multiplicities and splitting behavior of the forms they contain, for particular values of (r,q,d).

ALGORITHM(Gathering Information on $\mathcal{C}(r,d)(\mathbb{F}_q)$)
INPUT (r,q,d)
SET bag= All triples $(X,Y,Z) \in \mathbb{F}_q^3 - (0,0,0)$
WHILE bag not empty DO
Get next triple (X,Y,Z)
IF $X^2 + Y^3 \neq dZ^r$ THEN
Throw way triple
ELSE
Lift to an $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$ with $\pi(f) = (X,Y,Z)$
REMARK We have found a new specialization.
OUTPUT Its multiplicity := $\frac{q^2-1}{\#\text{specializations}}$
OUTPUT Its splitting := the splitting of f
Throw all specializations of $\chi(f)$ out of the bag
END-IF
END-WHILE
STOP

Proposition 8.2.1. *The algorithm above identifies exactly one f in every $SL_2(K)$-orbit of $\mathcal{C}(r,d)(\mathbb{F}_q)$. For each f the algorithm outputs the multiplicity of f and splitting behavior of f.*

Proof. The proposition is proven by the following 3 observations:

1. The program stops. Indeed, the bag is filled with a finite set of triples. In each loop at least one triple is removed and the program stops when the bag is empty.

2. Given any $f \in \mathrm{SL}_2(\mathbb{F}_q)$, an f' will be output whose $\chi(f')$ specializes to $\chi(f)(1,0)$. By Theorem 5.3.5, f' will be $\mathrm{SL}_2(\mathbb{F}_q)$-equivalent to f. Therefore at least one f in each $\mathrm{SL}_2(\mathbb{F}_q)$-orbit gets output.

3. The algorithm prevents f, f' with a common non-zero specialization being output. Therefore, by Theorem 5.3.5, at most one f from any $\mathrm{SL}_2(\mathbb{F}_q)$-orbit is output.

□

8.3 The Finiteness Argument

In this section we prove Theorem 8.1.5.

Proposition 8.3.1 (Tetrahedron). *Suppose $N, d \in \mathbb{F}_q^*$. The splitting of $\mathcal{C}(3,d)(\mathbb{F}_q)$ into $SL_2(\mathbb{F}_q)$-orbits and the multiplicities and the splitting behavior of the f in these orbits depends only on:*

1. *Whether $\omega \in \mathbb{F}_q$,*
2. *Whether $\sqrt[3]{d} \in \mathbb{F}_q$,*

where ω is a primitive 3rd root of unity. In particular the truth of Theorem 8.1.5 for tetrahedral equations can be verified by checking it for some $\mathcal{C}(3,d)(\mathbb{F}_q)$ satisfying each possible combination of conditions.

Proof. By Theorem 7.5.5, the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(3,d)(\mathbb{F}_q)$ correspond to the (F,Γ_1)-conjugacy classes of Γ_α, where

- F is a Frobenius element generating $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$,
- $\Gamma = \Gamma(\bar{f})$, for $\bar{f} = 4x(y^3 - x^3) \in \mathcal{C}(3,1)(\mathbb{F}_q)$,
- $\alpha = \lambda/F(\lambda)$ for some λ satisfying $\lambda^3 = d$.

In particular, choosing λ to be rational if possible, the coset Γ_α depends only on whether or not $\sqrt[3]{d} \in \mathbb{F}_q$ (up to an isomorphism of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$). Deciding whether 2 elements $g_1, g_1 \in \Gamma$ are (F,Γ_1)-conjugate involves taking every $h \in \Gamma_1$ and checking whether

$$g_1 = h^{-1} g_2 F(h)?$$

The elements of Γ are given in subsection 4.3.2. Since all the entries of elements of Γ lie in the field $\mathbb{F}_q(\omega)$, we have that the automorphism of Γ induced by F depends only on whether $\omega \in \mathbb{F}_q$. This means that the number and multiplicity of the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(3,d)(\mathbb{F}_q)$ depend only on the variables in the statement of the proposition.

To deduce how the $f \in \mathcal{C}(3,d)(\mathbb{F}_q)$ split, we apply Proposition 7.4.1 to see what permutation the Frobenius induces on the roots of f. Since the roots of $\bar{f}$ also lie in $\mathbb{F}_q(\omega)$ the splitting behavior also depends only on the variables in the statement of the proposition.

□

Proposition 8.3.2 (Octahedron). *Suppose $N, d \in \mathbb{F}_q^*$. The splitting of $\mathcal{C}(4,d)(\mathbb{F}_q)$ into $SL_2(\mathbb{F}_q)$-orbits and the multiplicities and the splitting behavior of the f in these orbits depends only on:*

1. *Whether $i \in \mathbb{F}_q$,*
2. *Whether $\sqrt{2} \in \mathbb{F}_q$,*
3. *Whether $\sqrt{-3d} \in \mathbb{F}_q$,*

where i is a primitive 4th root of unity. In particular the truth of Theorem 8.1.5 for octahedral equations can be verified by checking it for some $\mathcal{C}(4,d)(\mathbb{F}_q)$ satisfying each possible combination of conditions.

Proof. By Theorem 7.5.5, the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(4,d)(\mathbb{F}_q)$ correspond to the (F,Γ_1)-conjugacy classes of Γ_α, where

- F is a Frobenius element generating $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$,
- $\Gamma = \Gamma(\bar{f})$, for $\bar{f} = 36xy(x^4 - y^4) \in \mathcal{C}(4,-3)(\mathbb{F}_q)$,
- $\alpha = \lambda/F(\lambda)$ for some λ satisfying $-3\lambda^2 = d$.

In particular, the coset Γ_α depends only whether or not $\sqrt{-3d} \in \mathbb{F}_q$. Deciding whether 2 elements $g_1, g_1 \in \Gamma$ are (F,Γ_1)-conjugate involves taking every $h \in \Gamma_1$ and checking whether

$$g_1 = h^{-1} g_2 F(h)?$$

The elements of Γ were calculated in subsection 4.3.3. Since all the entries of elements of Γ lie in the field $\mathbb{F}_q(i,\sqrt{2})$, we have that the automorphism of Γ induced by F only depends on which of i and $\sqrt{2}$ are contained in $\mathbb{F}_q$. This means that the number and multiplicity of the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(4,d)(\mathbb{F}_q)$ depends only on the variables in the statement of the proposition.

To deduce how the $f \in \mathcal{C}(4,d)(\mathbb{F}_q)$ split, we apply Proposition 7.4.1 to see what permutation the Frobenius induces on the roots of f. Since the roots of $\bar{f}$ lie in $\mathbb{F}_q(i)$ the splitting behavior also depends only on the variables in the statement of the proposition.

□

Proposition 8.3.3 (Icosahedron). *Suppose $N, d \in \mathbb{F}_q^*$. The splitting of $\mathcal{C}(5,d)(\mathbb{F}_q)$ into $SL_2(\mathbb{F}_q)$-orbits and the multiplicities and the splitting behavior of the f in these orbits depends only on:*

1. *The degree of the field extension $\mathbb{F}_q(\zeta_5) : \mathbb{F}_q$.*

In particular the truth of the Theorem 8.1.5 for icosahedral equations can be verified by checking it for $\mathcal{C}(5,1)(\mathbb{F}_q)$ for an $\mathbb{F}_q$ with an extension of each possible degree.

Proof. By Theorem 7.5.5, the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(5,d)(\mathbb{F}_q)$ correspond to the (F,Γ_1)-conjugacy classes of Γ_1 where

- F is a Frobenius element generating $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$
- $\Gamma = \Gamma(\bar{f})$, for $\bar{f} = 1728\ xy(x^{10} + 11x^5y^5 - y^{10}) \in \mathcal{C}(5,1)(\mathbb{F}_q)$.

Deciding whether 2 elements $g_1, g_1 \in \Gamma$ are (F, Γ_1)-conjugate involves taking every $h \in \Gamma_1$ and checking whether

$$g_1 = h^{-1} g_2 F(h)?$$

The elements of Γ were calculated in subsection 4.3.4. Since all the entries of elements of Γ lie in the field extension $\mathbb{F}_q(\zeta_5)$, we have that the permutation of Γ induced by F only depends how F acts on ζ_5 — i.e. on the degree of the extension $\mathbb{F}_q(\zeta_5) : \mathbb{F}_q$.

Since the roots of $\bar{f}$ also lie in $\mathbb{F}_q(\zeta_5)$, Proposition 7.4.1 shows that the permutation the Frobenius induces on the roots of f is also determined by the degree of this field extension. □

Proof of Theorem 8.1.5. Using the computer program listed in § 8.2, we verify that the claims of Theorem 8.1.5 are true in the examples listed in Table 8.4.

r	Condition	Action of Frobenius on certain elements of $\bar{\mathbb{F}}_q$	Example
3	$q \equiv 1(3), d \in \mathbb{F}_q^3$	$(\omega, \sqrt[3]{d}) \mapsto (\omega, \sqrt[3]{d})$	$\mathcal{C}(3,1)(\mathbb{F}_{13})$
	$q \equiv 1(3), d \notin \mathbb{F}_q^3$	$(\omega, \sqrt[3]{d}) \mapsto (\omega, \omega\sqrt[3]{d})$	$\mathcal{C}(3,2)(\mathbb{F}_{13})$
	$q \equiv 2(3)$	$(\omega, \sqrt[3]{d}) \mapsto (\omega^2, \sqrt[3]{d})$	$\mathcal{C}(3,1)(\mathbb{F}_{17})$
4		$(\sqrt{-3d}, \sqrt{2}, i) \mapsto$	
	$q \equiv 1(8),\ -3d \in \mathbb{F}_q^2$	$(\sqrt{-3d}, \sqrt{2}, i)$	$\mathcal{C}(4,1)(\mathbb{F}_{17})$
	$q \equiv 3(8),\ -3d \in \mathbb{F}_q^2$	$(\sqrt{-3d}, -\sqrt{2}, -i)$	$\mathcal{C}(4,1)(\mathbb{F}_{19})$
	$q \equiv 5(8),\ -3d \in \mathbb{F}_q^2$	$(\sqrt{-3d}, -\sqrt{2}, i)$	$\mathcal{C}(4,1)(\mathbb{F}_{13})$
	$q \equiv 7(8),\ -3d \in \mathbb{F}_q^2$	$(\sqrt{-3d}, \sqrt{2}, -i)$	$\mathcal{C}(4,1)(\mathbb{F}_{23})$
	$q \equiv 1(8),\ -3d \notin \mathbb{F}_q^2$	$(-\sqrt{-3d}, \sqrt{2}, i)$	$\mathcal{C}(4,3)(\mathbb{F}_{17})$
	$q \equiv 3(8),\ -3d \notin \mathbb{F}_q^2$	$(-\sqrt{-3d}, -\sqrt{2}, -i)$	$\mathcal{C}(4,2)(\mathbb{F}_{19})$
	$q \equiv 5(8),\ -3d \notin \mathbb{F}_q^2$	$(-\sqrt{-3d}, -\sqrt{2}, i)$	$\mathcal{C}(4,11)(\mathbb{F}_{13})$
	$q \equiv 7(8),\ -3d \notin \mathbb{F}_q^2$	$(-\sqrt{-3d}, \sqrt{2}, -i)$	$\mathcal{C}(4,5)(\mathbb{F}_{23})$
5	$q \equiv 1(5)$	$\zeta_5 \mapsto \zeta_5$	$\mathcal{C}(5,1)(\mathbb{F}_{31})$
	$q \equiv 4(5)$	$\zeta_5 \mapsto \zeta_5^{-1}$	$\mathcal{C}(5,1)(\mathbb{F}_{19})$
	$q \equiv \pm 2(5)$	$\zeta_5 \mapsto \zeta_5^{\pm 2}$	$\mathcal{C}(5,1)(\mathbb{F}_{17})$

Table 8.4: Table of Examples

In the table, ω, ζ_5 are primitive 3rd and 5th roots of unity. These examples allow us to imply Theorem 8.1.5 from Propositions 8.3.1, 8.3.2 and 8.3.3.

□

8.4 Twisted Conjugacy Classes

In this section we develop the theory of twisted conjugacy classes. The (F, Γ_1)-conjugacy classes are examples of twisted conjugacy classes. Many of the proofs are routine, but not very instructive. These have been placed in Appendix C.

In this section we assume that $H \leq G$ are arbitrary finite groups. We assume that ψ is an automorphism of G that induces an automorphism of H.

Definition 8.4.1. *(ψ, H)-conjugacy is the equivalence relation on G given by*

$$g \sim g' \Leftrightarrow \text{there exists } h \in H \text{ with } g' = h^{-1} g \psi(h).$$

If ψ is the identity we simply refer to H-conjugacy. If ψ is the identity and $G = H$ we simply refer to conjugacy.

Definition 8.4.2. *For any $g \in G$ we define the following objects:*

$$[g]_{(\psi,H)} := \{g' \in G \mid g' \text{ is } (\psi, H)\text{-conjugate to } g\},$$
$$C_{(\psi,H)}(g) := \{h \in H \mid g = h^{-1} g \psi(h)\}.$$

If ψ is the identity we will also refer to these objects as $[g]_H$ and C_H.

Lemma 8.4.3. *Take any $g \in G$. Then $C_{(\psi,H)}(g)$ is a subgroup of H. We have*

$$\#[g]_{(\psi,H)} \ \ \#C_{(\psi,H)}(g) \ = \ \#H.$$

Proof. See Lemma C.0.1. □

Proposition 8.4.4. *Suppose that $[G : H] = 2$ and ψ is given by conjugation by an element $s \in G - H$. Then there is a $1-1$ correspondence between H and $G - H$ that takes (ψ, H)-conjugacy classes of H to G-conjugacy classes of $G - H$. Furthermore, if $\gamma \mapsto \gamma'$, then*

$$\#C_{(\psi,H)}(\gamma) = \frac{1}{2} \#C_G(\gamma').$$

Proof. See Proposition C.0.2. □

If H, G are subgroups of $\mathrm{SL}_2(K)$ we further assume that $-I \in H$ and that $\psi(-I) = -I$. This means that ψ commutes with negation and so acts as an automorphism of the projective versions of these groups. We denote the projective versions of all objects with tildes. We have a quotient map

$$G/\text{ conjugation } \to \widetilde{G}/\text{ conjugation }, \quad [\gamma]_{(\psi,H)} \mapsto [\gamma]_{(\psi,\widetilde{H})}.$$

Lemma 8.4.5. *Suppose that H is a subgroup of $SL_2(K)$ and $\psi \in Aut(H)$. Suppose that $-I \in H$ and $\psi(-I) = -I$. Suppose that $\widetilde{H}$ has no subgroup of index 2.*

Then ψ is an inner automorphism of H if and only if its image $\widetilde{\psi}$ in $Aut(\widetilde{H})$ is an inner automorphism.

Proof. This follows from Proposition C.0.3. □

Lemma 8.4.6. *Suppose $H \leq G$ are subgroups of $SL_2(K)$. Assume that $-I \in H$ and that $\psi(-I) = -I$. Then*

- $C_{(\psi,H)}(1) = \{h \in H \mid h = \psi(h)\}$,
- *If H has a unique H-conjugacy class of trace zero, then there is an $h \in H$ with $[h]_{(\psi,H)} = [-h]_{(\psi,H)}$.*

If $g \in G$ then the following hold.

- $\#C_{(\psi,H)}(g)$ *is even,*
- *If $[g]_{(\psi,H)} = [-g]_{(\psi,H)}$ then $\#C_{(\psi,H)}(g) = \#C_{(\psi,\widetilde{H})}(g)$,*
- *If $[g]_{(\psi,H)} \neq [-g]_{(\psi,H)}$ then $\#C_{(\psi,H)}(g) = 2\#C_{(\psi,\widetilde{H})}(g)$.*

Proof. See Lemma C.0.4. □

Proposition 8.4.7. *Suppose H is a group and $\psi_i \in Aut(H)$ for $i = 1, 2$. Suppose there is an $s \in H$ so that $\psi_1 = s^{-1}\psi_2 s$. Then*

$$H \to H, \quad g \mapsto gs^{-1}$$

is a bijection that maps (ψ_1, H)-conjugacy classes to (ψ_2, H)-conjugacy classes.

Proof. See Proposition C.0.6. □

8.5 Geometric Approach

In this section we will use the machinery of twisted conjugacy classes to interpret the results on the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$ in a more geometric fashion.

By Theorem 7.5.5, the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$ correspond to (F,Γ_1)-conjugacy classes of Γ_1. We show first that the multiplicities of the orbits correspond to the orders of the groups $C_{(\Gamma_1,F)}(g)$.

Proposition 8.5.1. *Suppose $\bar{f} \in \mathcal{C}(r,d_0)(\mathbb{F}_q)$. Write $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$ as in Theorem 7.5.5 as $f = \lambda g \cdot \bar{f}$. Let $H := \Gamma_1(\bar{f})$ and $\delta := g^{-1}F(g)$. Then*

$$\Gamma_1(f)(\mathbb{F}_q) = gC_{(H,F)}(\delta)g^{-1}.$$

Proof.

$$\begin{aligned}\Gamma_1(f)(\mathbb{F}_q) &= \{m \in \Gamma_1(f) \mid F(m) = m\} \\ &= \{ghg^{-1} \mid h \in \Gamma_1(\bar{f}),\ F(ghg^{-1}) = ghg^{-1}\} \\ &= \{ghg^{-1} \mid h \in \Gamma_1(\bar{f}),\ h^{-1}\delta F(h) = \delta\}\end{aligned}$$

□

Corollary 8.5.2. *Suppose $N, d \in \mathbb{F}_q^*$, then $\#\mathcal{D}(r,d)(\mathbb{F}_q) = q^2$.*

Proof. This follows from Proposition 8.5.1 and Corollary 8.1.4. □

Theorem 8.5.3. *Suppose $N, d \in \mathbb{F}_q^*$. Choose $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$ and set $\Gamma_1 := \Gamma_1(f)$.*

Then the number of $SL_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$ as well as the multiplicity of the forms in these orbits depends only on the Frobenius F as an element in the group

$$\frac{\textit{Automorphisms of } \Gamma_1}{\textit{Inner Automorphisms}}.$$

Proof. By Theorem 7.5.5, the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_q)$ correspond to (F, Γ_1)-conjugacy classes of Γ_1. By Proposition 8.4.7, the conjugacy classes have the same size if the automorphisms that F induce differ only by an inner automorphism. □

8.6 Automorphisms of the Platonic Solids

In chapter 4.3 we indicated how the projective groups $\widetilde{\Gamma}, \widetilde{\Gamma}_1$ are related to the rotational symmetries of the platonic solids. Each group is isomorphic with the induced permutations on a certain orbit space. To wit:

r	Solid	Orbit Space Σ	$\widetilde{\Gamma}_1$	$\widetilde{\Gamma}$
3	Tetrahedron	The 4 Vertices	V_4	Even Permutations
4	Octahedron	4 Pairs of Opposite Faces	Even Permutations	All Permutations
5	Icosahedron	5 Embedded Octahedra	Even Permutations	Even Permutations

The Frobenius F acts on the binary groups Γ and Γ_1. Since F commutes with $\pm I$, it also acts on the projective groups and hence on these orbit spaces.

If we number the elements of the orbit space $x, \ldots, x_n$; where $n = |\Sigma|$, then F permutes the x_i. Therefore F can be seen as an element $s \in S_n$: $x_i \mapsto x_{s(i)}$. Similarly we can define $g(i)$ for $g \in \widetilde{\Gamma}_1$ by $g : x_i \mapsto x_{g(i)}$. Then

$$F(g) \cdot x_{s(i)} = F(g \cdot x_i) = F(x_{g(i)}) = x_{sg(i)},$$

so that $F(g) = sgs^{-1}$. This means that when we identify $\widetilde{\Gamma}_1$ with a subgroup of S_n, the action of F on $\widetilde{\Gamma}_1$ corresponds to conjugation using the element s.

The permutation that F induces on the orbit space Σ can be calculated for a particular $f \in \mathcal{C}(r,d)(\mathbb{F}_q)$. This allows us to calculate the $(F, \widetilde{\Gamma}_1)$-conjugacy classes of $\widetilde{\Gamma}_1(f)$. These can then be lifted to (F, Γ_1)-conjugacy classes of $\Gamma_1(f)$. This gives an alternative (computer free) proof of some of the results proven in section 8.3 using a finiteness argument.

8.6.1 Icosahedron

Let $f = 1728d\ xy(x^{10} + 11x^5y^5 - y^{10}) \in \mathcal{C}(5,d)(\mathbb{F}_q)$. This is the Klein form that was analyzed in subsection 4.3.4 of this thesis. The group $\Gamma_1(f)$ is the Binary Icosahedral Group. If we divide out by $\pm I$ we get the Icosahedral Rotation Group of order 60. The embedded octahedra are given by t_ν and the Frobenius F permutes the t_ν via

$$\text{Permutation } s = \begin{cases} s_1 := (1), & \text{if } \xi \in \mathbb{F}_q; \\ s_2 := (14)(23), & \text{if } [\mathbb{F}_q(\xi) : \mathbb{F}_q] = 2; \\ s_4 := (1243), & \text{if } [\mathbb{F}_q(\xi) : \mathbb{F}_q] = 4. \end{cases}$$

Case I - $p \equiv \pm 1(5)$

We have that $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = 1$ or 2, and F induces an inner automorphism of $\widetilde{\Gamma}_1$. The group $\widetilde{\Gamma}_1 = A_5$ has no subgroups of index 2, so by Lemma 8.4.5, F induces an inner automorphism of Γ_1. By Proposition 8.4.7, the number and multiplicities of the parameterizations is the same as in the $\xi \in \mathbb{F}_q$ case when everything is rational. We 'only' have to count the usual conjugacy classes in the Binary Icosahedral Group. This can be read from the character table of Γ_1.

Case II - $p \equiv \pm 2(5)$

The Frobenius F induces an automorphism of $\widetilde{\Gamma}_1$ that corresponds to conjugation by the odd permutation $s_4 \in S_5$. I.e. F induces an outer automorphism of $\widetilde{\Gamma}_1$. As $\widetilde{\Gamma}_1 \cong A_5$, the $(F, \widetilde{\Gamma}_1)$-conjugacy classes of $\widetilde{\Gamma}_1$ can be deduced from the S_5-conjugacy classes of S_5 using Proposition 8.4.4. The conjugacy classes of S_5 are well-known in terms of cycle shapes. We get

$(F, \widetilde{\Gamma}_1)$-conjugacy class	$\#C_{(F,\widetilde{\Gamma}_1)}$
A	6
B	2
C	3

Each $(F, \widetilde{\Gamma}_1)$-conjugacy class of $\widetilde{\Gamma}_1$ lifts to either 1 or 2 (F, Γ_1) conjugacy classes of Γ_1. We say that the class is *inert*, respectively *splits*.

Using Lemma 8.4.6, we deduce the following

- C splits into 2 classes of multiplicity 6. (Multiplicities are always even).
- B splits into 2 classes of multiplicity 4. ($\#\Gamma_1(\mathbb{F}_q) = 4$, so some multiplicity is 4).
- A remains 1 class with multiplicity 6. (Γ_1 has a unique Γ_1-conjugacy class of trace zero. Therefore at least one class is inert).

Therefore the following table is an enumeration of the (F, Γ_1)-conjugacy classes of Γ_1 along with the sizes of the groups $C_{(F,\Gamma_1)}$.

(F, Γ_1)-conjugacy class	$\#C_{(F,\Gamma_1)}$
A	6
$B, -B$	4, 4
$C, -C$	6, 6

Conclusion

By Theorem 7.5.5, the (F, Γ_1)-conjugacy classes of Γ_1 can be identified with $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(5, d)(\mathbb{F}_q)$.

We have, therefore, given an alternative proof of the number and multiplicities of the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(5, d)(\mathbb{F}_q)$, proven by a finiteness argument in section 8.3.

8.6.2 Octahedron

Let $f = 36xy(x^4 - dy^4) \in \mathcal{C}(4, -3d)$. This is the octahedral Klein form that was analyzed in subsection 4.3.3. It has roots $0, \infty, \beta_i$ where $i = 0, \ldots, 3$ and the β_i are the 4 solutions of $\beta^4 = d$.

The group $\Gamma(f)$ is the Binary Octahedral Group. If we divide out by $\pm I$ we get the Octahedral Rotation Group $\widetilde{\Gamma}$ of order 24. This is isomorphic to S_4 by the permutations it induces on pairs of opposite faces. $\widetilde{\Gamma}_1$ is isomorphic to A_4 and corresponds to even permutations. The faces are given by

$$h_\nu(f) = x^2 + i^\nu(1 + i)\beta xy - (-1)^\nu i\beta^2 y^2,$$

where i is a primitive 4-th root of unity, β is a fixed solution to $\beta^4 = d$ and $\nu = 0, 1, 2, 3$.

The Frobenius acts on i, β by

$$F : i \mapsto \pm i, \quad \beta \mapsto \begin{cases} \pm\beta & \text{if } d \in \mathbb{F}_q^{*2}, \\ \pm i\beta & \text{otherwise.} \end{cases}$$

From this we deduce that F corresponds to an even permutation of the faces if $d \in \mathbb{F}_q^{*2}$ and an odd permutation otherwise.

Case I - $d \in \mathbb{F}_q^{*2}$

We see that when $d \in \mathbb{F}_q^{*2}$, the Frobenius F induces an inner automorphism of $\widetilde{\Gamma}_1$. The group $\widetilde{\Gamma}_1 = A_4$ has no subgroups of index 2, so by Lemma 8.4.5, F induces an inner automorphism of Γ_1. Hence, by Proposition 8.4.7, the number and multiplicity of the parameterizations is the same as the number and multiplicity of the 'usual' conjugacy classes of Γ_1. We 'only' have to count the usual conjugacy classes in the Binary Octahedral Group. This can be read from the character table of Γ_1.

Case II - $d \notin \mathbb{F}_q^{*2}$

We see that when $d \notin \mathbb{F}_q^{*2}$, the Frobenius F induces an outer automorphism of $\widetilde{\Gamma}_1$. As $\widetilde{\Gamma}_1 \cong A_4$, the $(F, \widetilde{\Gamma}_1)$-conjugacy classes of $\widetilde{\Gamma}_1$ can be deduced from the S_4-conjugacy classes of S_5 using Proposition 8.4.4. The conjugacy classes of S_4 are well-known in terms of cycle shapes. We get

$(F, \widetilde{\Gamma}_1)$-conjugacy class	$\#C_{(F,\widetilde{\Gamma}_1)}$
A	2
B	2

Each $(F, \widetilde{\Gamma}_1)$-conjugacy class of $\widetilde{\Gamma}_1$ lifts to either 1 or 2 (F, Γ_1)-conjugacy classes of Γ_1. We say that the class is *inert*, respectively *splits*.

Using Lemma 8.4.6, we deduce the following

- One of the classes A (say) splits into 2 classes of multiplicity 4. ($\#\Gamma_1(\mathbb{F}_q) \geq 4$, so some multiplicity is at least 4).
- B remains 1 class with multiplicity 2. (Γ_1 has a unique Γ_1-conjugacy class of trace zero. Therefore at least one class is inert).

Therefore the following table is an enumeration of the (F, Γ_1)-conjugacy classes of Γ_1 along with the sizes of the groups $C_{(F,\Gamma_1)}$.

(F, Γ_1)-conjugacy class	$\#C_{(F,\Gamma_1)}$
$A, -A$	$4, 4$
B	2

Conclusion

By Theorem 7.5.5, the (F, Γ_1)-conjugacy classes of Γ_1 can be identified with $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(4, -3d)(\mathbb{F}_q)$.

We have, therefore, given an alternative proof of the number and multiplicities of the $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(4, -3d)(\mathbb{F}_q)$, proven by a finiteness argument in section 8.3.

8.6.3 Tetrahedron

Let $f = -4y(x^3 - dy^3) \in \mathcal{C}(3, d)$. This is the tetrahedral Klein form analyzed in subsection 4.3.2. The group $\widetilde{\Gamma}(f)$ is isomorphic to A_4 via the set of even permutations of the roots of f. The roots of f are $\infty, \gamma_1, \gamma_2, \gamma_3$ with γ_i the roots of $\gamma^3 = d$. This means that the Frobenius F permutes the roots via

$$\text{Permutation } s = \begin{cases} s_3 := (\infty)(\gamma_1, \gamma_2, \gamma_3), & \text{if } [\mathbb{F}_q(\omega, \sqrt[3]{d}) : \mathbb{F}_q] = 3; \\ s_2 := (\infty)(\gamma_1)(\gamma_2, \gamma_3), & \text{if } [\mathbb{F}_q(\omega, \sqrt[3]{d}) : \mathbb{F}_q] = 2; \\ s_1 := \text{ identity }, & \text{if } [\mathbb{F}_q(\omega, \sqrt[3]{d}) : \mathbb{F}_q] = 1; \end{cases}$$

where ω is a primitive cube root of unity. We further identified $\widetilde{\Gamma}_1$ as the subgroup V_4 of S_4. We have $V_4 \subset A_4 \subset S_4$. We see that the number of $\mathrm{SL}_2(\mathbb{F}_q)$-orbits of $\mathcal{C}(3, d)(\mathbb{F}_q)$ corresponds to whether F induces an automorphism of V_4 that is conjugation by an element of V_4, A_4 or S_4.

Conclusion

We have shown how the different sizes of the $\mathrm{SL}_2(\mathbb{F}_q)$-orbit spaces of $\mathcal{C}(3, d)(\mathbb{F}_q)$ correspond to different values that F takes in the Outer Automorphism Group of $\widetilde{\Gamma}_1$.

Chapter 9

Parameterizations in $\mathbb{Z}_p$

This chapter describes the parameterizations of $\mathcal{D}(r,d)(\mathbb{Z}_p)$. The most simple case is when parameterizations can be lifted from parameterizations of $\mathcal{D}(r,d)(\mathbb{F}_p)$ using Hensel's Lemma. This is described in sections 9.1 and 9.3.

In particular if $N, d \in \mathbb{Z}_p^*$, then parameterizations can be assumed to be of the form $\chi(f)$ with $f \in \mathcal{C}(r,d)(\mathbb{Z}_p)$. Reduction modulo p then gives a bijection between the $\mathrm{SL}_2(\mathbb{Z}_p)$-orbits of $\mathcal{C}(r,d)(\mathbb{Z}_p)$ and the $\mathrm{SL}_2(\mathbb{F}_p)$-orbits of $\mathcal{C}(r,d)(\mathbb{F}_p)$.

The last section (§ 9.4) describes what can be said about parameterizations if a direct lift of a parameterization of $\mathcal{D}(r,d)(\mathbb{F}_p)$ is not possible.

9.1 Hensel's Lemma

This section contains a many dimensional version of Hensel's Lemma. This can be used to deduce the existence of actual solutions to a system of equations in a complete local ring from the existence of an approximate solution.

Lemma 9.1.1 (Hensel's Lemma). *Suppose R is a ring, complete relative to an ideal $\mathbf{m}$. Fix $f_1, \ldots, f_n \in R[[x, \ldots, x_n]]$. Define the jacobian matrix by*

$$J(\bar{x}) := (\partial f_i / \partial x_j)\,.$$

Let $\Delta := \det(J(\bar{a})) \in R$. Suppose that $(a_1, \ldots, a_n) \in R^n$, that l is a positive integer and that

$$f_i(\bar{a}) \in \mathbf{m}^l \Delta^2 \qquad \text{for each } i.$$

Then there is a $(b_1, \ldots, b_n) \in R^n$ such that

$$f_i(\bar{b}) = 0, \quad a_i - b_i \ \in \mathbf{m}^l \Delta$$

for all i. The solution is unique if Δ is not a zero divisor in the ring R.

Proof. See [6], Exercise 7.26, or [19], page 177. Or for a full proof [3], section 4.6, Theorem 2. □

9.2 Some Jacobians

We want to lift the results proven about finite fields to $\mathbb{Z}_p$. This is done using the many dimensional form of Hensel's Lemma given in the last section. To apply this lemma we need to calculate the jacobians of systems of equations.

Let f be a form of order k written generically as

$$f = \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a_i \, x^{k-i} y^i.$$

Let $g = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$ where, $m_1, \ldots, m_4$ are variables. Let $f' = f \circ g$ have coefficients $[a'_0 \ldots a'_k]$.

Lemma 9.2.1. *The first order changes in* $\det(g)$ *and the coefficients* a'_i *at the identity are summarized in the following* $(k+2) \times 4$ *matrix*

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ ka_0 & 0 & ka_1 & 0 \\ (k-1)a_1 & a_0 & (k-1)a_2 & a_1 \\ (k-2)a_2 & 2a_1 & (k-2)a_3 & 2a_2 \\ & \vdots & \vdots & \\ a_{k-1} & (k-1)a_{k-2} & a_k & (k-1)a_{k-1} \\ 0 & ka_{k-1} & 0 & ka_k \end{pmatrix},$$

where for $0 \le i \le k$ *and* $1 \le j \le 4$ *we have*

$$M_{1,j} = \frac{\partial}{\partial m_j} \det|_{g=I}, \quad M_{2+i,j} = \frac{\partial}{\partial m_j} a'_i|_{g=I}.$$

Proposition 9.2.2 (Covariant Minors). *Specialize to* $k \in \{4, 6, 12\}$. *The determinants of the* 4×4 *minors of the above matrix are isobaric forms in the* a_i. *They are the leading terms of a covariant iff we choose either*

- *Rows 1 thru 4, or*
- *Rows 2 thru 5.*

We call these determinants J_1, J_2 *respectively.*

Proof. By Theorem 3.2.2, such a $C_0 \in R[a_0, \ldots, a_k]$ is the leading term of a covariant if and only if it is isobaric in the a_i and satisfies $D(C_0) = 0$, where D is the Cayley Aronhold Operator

$$D = a_0 \frac{\partial}{\partial a_1} + 2a_1 \frac{\partial}{\partial a_2} + \cdots + ka_{k-1} \frac{\partial}{\partial a_k}.$$

The proposition is therefore reduced to calculation for all 4×4 minors of the matrix M. □

Proposition 9.2.3. *Suppose $f \in \mathcal{C}(r,d)(\mathbb{Z}_p)$ and $\pi(f) = (X,Y,Z)$. Then*

$$J_1 = -2k(k-2)Y,$$
$$J_2 = 12k(k-2)dZ^{r-2},$$

where J_i are the determinants referred to in Proposition 9.2.2.

Proof. We can calculate the covariants $\boldsymbol{C}_i$ whose leading term is J_i using the algorithm of [12], page 64. This algorithm takes the leading term of a covariant and outputs the covariant as a polynomial in the transvectants $f, \boldsymbol{\tau}_2, \boldsymbol{\tau}_3, \ldots \boldsymbol{\tau}_k$ divided by a power of f. This produces the following.

$$\boldsymbol{C}_1 = -k(k-2)\boldsymbol{t}(f),$$
$$\boldsymbol{C}_2 = 3k(k-2)\frac{\boldsymbol{t}(f)^2 + 4\boldsymbol{H}(f)^3}{f^2} - 2k(k-3)\boldsymbol{H}(f)\boldsymbol{\tau}_4(f).$$

As $f \in \mathcal{C}(r,d)$, we have $\tau_4(f) = 0$ and $\boldsymbol{t}(f)^2 + 4\boldsymbol{H}(f)^3 = 4df^r$. Evaluating these expressions at $(1,0)$ gives the result. □

9.3 Lifting from $\mathbb{F}_p$ to $\mathbb{Z}_p$

Proposition 9.3.1. *Suppose $N, d \in \mathbb{Z}_p$ are non-zero and $f_1, f_2 \in \mathcal{C}(r,d)(\mathbb{Z}_p)$. Suppose $s \in \mathbb{Z}_p^2$ is co-prime. Let $(X,Y,Z) := \chi(f_2)(s)$ and define $\Delta := 2k(k-2)X$. Then for any integer $l > 0$, if*

$$\Omega_r(f_1) \equiv \Omega_r(f_2) \mod p^l\Delta^2,$$

then there is a unique $g \in SL_2(\mathbb{Z}_p)$ with

$$f_1 = g \cdot f_2, \quad g \equiv I \mod p^l\Delta.$$

Proof. (Step I - Simplification).

As s is co-prime, there is a $g \in \mathrm{SL}_2(\mathbb{Z}_p)$ with $gs = (1,0)$. Replacing f_1 by $g \cdot f_1$ and f_2 by $g \cdot f_2$ allows us to assume that $s = (1,0)$.

(Step II - Hensel's Lemma).

Let $f := f_2 = [a_0 \ldots a_k]$ and $f' := f_1 \circ g = [a'_0 \ldots a'_k]$. We are looking for a g which makes these 2 sequences of coefficients equal.

We use Hensel's Lemma 9.1.1 to solve the following simultaneous system of equations in the entries g:

$$a'_0 = a_0, \quad a'_1 = a_1, \quad a'_2 = a_2, \quad \det(g) = 1,$$

where a solution mod $p^l\Delta^2$ is given by $g = I$.

By Proposition 9.2.3, the jacobian at the identity has determinant $-2k(k-2)X$. Hensel's Lemma implies a unique lift of the identity matrix to $g \in \mathrm{SL}_2(\mathbb{Z}_p)$ such that

$$[a_0', a_1', a_2'] = [a_0, a_1, a_2], \quad g \equiv I \mod p^l\Delta.$$

Let

$$(X, Y, Z) := \pi(f), \text{ and } \quad (X', Y', Z') := \pi(f').$$

By the definition of π and since $(X, Y, Z) \in \mathcal{D}(r, d)$ we have

$$\begin{aligned} Z &= a_0, \\ Y &= a_0a_2 - a_1^2, \\ 2X &= a_0^2a_3 - 3a_0a_1a_2 + 2a_1^2, \\ X^2 &= dZ^r - Y^3, \end{aligned}$$

and a similar set of *dashed* equations. Therefore $Z = Z'$, $Y = Y'$, $X = \pm X'$. If $X = X'$ then $[a_0, a_1, a_2, a_3, \dots]$ equals $[a_0', a_1', a_2', a_3', \dots]$ and the defining equations of $\mathcal{C}(r, d)$ show that $f = f'$.

To finish we will assume that $X' = -X \neq 0$ and derive a contradiction. Since $\Omega_r(f_1) \equiv \Omega_r(f_2)$ and $g \equiv I$ modulo $p^l\Delta$ we have

$$\boldsymbol{t}(f_1 \circ g) \equiv \boldsymbol{t}(f_2) \mod p^l\Delta,$$

so that after specialization at $(1, 0)$

$$4X \equiv 0 \mod p^l\Delta.$$

As $4X$ divides Δ and $l > 0$, this implies that $X = 0$. Contradiction. □

Proposition 9.3.2. *Suppose $N, d \in \mathbb{Z}_p$ are non-zero and $f_1, f_2 \in \mathcal{C}(r, d)(\mathbb{Z}_p)$. Suppose $s \in \mathbb{Z}_p^2$ is co-prime. Let $(X, Y, Z) := \chi(f_2)(s)$ and define $\Delta := 12k(k-2)Z^{r-2}$. Then for any integer $l > 0$, if*

$$\Omega_r(f_1) \equiv \Omega_r(f_2) \mod p^l\Delta^2,$$

then there is a unique $g \in SL_2(\mathbb{Z}_p)$ with

$$f_1 \circ g = f_2, \quad g \equiv I \mod p^l\Delta.$$

Proof. This is similar to the previous proposition, but we now use the jacobian matrix from rows 2 through 5. Let $f := f_2 = [a_0 \dots a_k]$ and $f' := f_1 \circ g = [a_0' \dots a_k']$. The identity matrix then lifts to a $g \in \mathrm{GL}_2(\mathbb{Z}_p)$ with

$$[a_0', a_1', a_2', a_3'] = [a_0, a_1, a_2, a_3], \quad g \equiv I \mod p^l\Delta$$

By Proposition 5.2.5, this forces $f_1 \circ g = f_2$. We only need to show that $\det(g) = 1$. Certainly $\det(g) \equiv 1$ modulo $p^l\Delta$, and the twist can only be in $\mathcal{C}(r,d)$ again if $\det(g)^6 = 1$.

We find that $\det(g) \in \mathbb{Z}_p$ satisfies the following equations in the variable t

$$t^6 = 1, \quad t \equiv 1 \mod 6p^l.$$

A solution modulo $36p^l$ is given by $t = 1$. Therefore, by the uniqueness statement of Hensel's Lemma we have $\det(g) = 1$.

□

Theorem 9.3.3. *Suppose $N, d \in \mathbb{Z}_p$ are non-zero and $d \not\equiv 0 \mod p^2$. Suppose $f_1, f_2 \in \mathcal{C}(r,d)(\mathbb{Z}_p)$ and there is an $s \in \mathbb{Z}_p^2$ so that $\chi(f_1)(s) = (X,Y,Z)$ is co-prime. Then for any integer $l > 0$, if*

$$\Omega_r(f_1) \equiv \Omega_r(f_2) \mod p^l,$$

then there is a $g \in SL_2(\mathbb{Z}_p)$ with

$$f_1 = g \cdot f_2, \quad g \equiv I \mod p^l.$$

Proof. (X,Y,Z) being co-prime forces s to be co-prime. If $\nu_p(d) = 1$, this forces the relatively prime specialization (X,Y,Z) to have $X \in \mathbb{Z}_p^*$ and the result follows from Proposition 9.3.1. Otherwise $d \in \mathbb{Z}_p^*$ so either $X \in \mathbb{Z}_p^*$ and we can apply Proposition 9.3.1, or $Z \in \mathbb{Z}_p^*$ and we can apply Proposition 9.3.2. □

Theorem 9.3.4. *Suppose $N \in \mathbb{Z}_p$ is non-zero and $d \in \mathbb{Z}_p^*$. Suppose that $f_1, f_2 \in \mathcal{C}(r,d)(\mathbb{Z}_p)$ both have co-prime $\mathbb{Z}_p$-specializations.*

Then f_1, f_2 are $SL_2(\mathbb{Z}_p)$-equivalent iff their restrictions f_1', f_2' to $\mathcal{C}(r,d)(\mathbb{F}_p)$ are $SL_2(\mathbb{F}_p)$-equivalent.

Proof. Clearly $\mathrm{SL}_2(\mathbb{Z}_p)$-equivalent implies $\mathrm{SL}_2(\mathbb{F}_p)$-equivalent. We only have to prove the converse. Assume $g'.f_1' = f_2'$ for some $g' \in \mathrm{SL}_2(\mathbb{F}_q)$. Using Hensel's Lemma we can lift g' to some $g \in \mathrm{SL}_2(\mathbb{Z}_p)$ so that $g \cdot f_1 \equiv f_2$ modulo p. The result follows from Theorem 9.3.3. □

Corollary 9.3.5. *Suppose $N, d \in \mathbb{Z}_p^*$. Then the results of Theorem 8.1.1 hold with $\mathbb{F}_p$ replaced everywhere by $\mathbb{Z}_p$.*

Proof. This follows by using Theorem 9.3.4 to lift the results about the finite field $\mathbb{F}_p$ given in Theorem 8.1.1. □

9.4 Solutions in $\mathbb{Z}_p$ - Part II

In this section we cover some cases that cannot be deduced by simply lifting parameterizations over finite fields.

Proposition 9.4.1. *[Allows $d \notin \mathbb{Z}_p^*$] Suppose $N, d \in \mathbb{Z}_p$ are non-zero. Then there is a finite number of $f \in \mathcal{C}(r,d)(\mathbb{Z}_p)$ such that the $\mathbb{Z}_p$ specializations of $\chi(f)$ include all co-prime $(X,Y,Z) \in \mathcal{D}(r,d)(\mathbb{Z}_p)$.*

Proof. By Theorem 6.1.1 we can assume we are looking for parameterizations $\chi(f)$ derived from $f \in \mathcal{C}(r,d)(\mathbb{Z}_p)$. Take any such f and suppose $\pi(f) = (X,Y,Z)$. Let $t := \boldsymbol{t}(f)$. By the properties of resultants, there are $A, B \in \mathbb{Z}_p[x,y]$ so that

$$Af + Bt = \ \mathrm{Res}(f, \boldsymbol{t})x^n$$

for some $n > 0$. Specializing at $(1,0)$ gives

$$aZ + bX = 2\mathrm{Res}(f, \boldsymbol{t}), \quad \text{with} \ \ a, b \in \mathbb{Z}_p.$$

However, since $\mathcal{C}(r,d)(\overline{\mathbb{Q}}_p)$ is a homogeneous $\mathrm{SL}_2(\overline{\mathbb{Q}}_p)$-space, $\mathrm{Res}(f, \boldsymbol{t})$ is independent of the f chosen. Therefore $\max(\nu(X), \nu(Z))$ has an upper bound that depends only on r and d. The result follows by applying Proposition 9.3.1 and Proposition 9.3.2. □

Proposition 9.4.2. *[Allows $\gcd(X,Y,Z) \notin \mathbb{Z}_p^*$] Suppose $N \in \mathbb{Z}_p^*$. Fix non-zero $d \in \mathbb{Z}_p$. There are a finite number of $f \in \mathcal{C}(r,d)(\mathbb{Q}_p)$ such that the $\mathbb{Z}_p$ specializations of $\chi(f)$ include all $(X,Y,Z) \in \mathcal{D}(r,d)(\mathbb{Z}_p)$ with $\gcd(X,Y,Z) = 1$.*

Proof. (Sketch) Using the techniques of section 11.7, we can reduce the problem to a finite set of associated problems of the following type.

Problem 9.4.3. *Fix a non-zero $d' \in \mathbb{Z}_p$. Find a finite set of $f_\alpha \in \mathcal{C}(r,d')(\mathbb{Q}_p)$ so that their $\mathbb{Z}_p$-specializations include all co-prime $(X,Y,Z) \in \mathcal{D}(r,d')(\mathbb{Z}_p)$ as well as all $(X,Y,Z) \in \mathcal{D}(r,d')(\mathbb{Z}_p)$ with $\nu_p(Z) = 1$.*

Finding a finite set of f that specialize to the co-prime $(X,Y,Z) \in \mathcal{D}(r,d')(\mathbb{Z}_p)$ follows from Proposition 9.4.1. If $\nu_p(Z) = 1$, consider the canonical form $f = [Z, 0, -\frac{Y}{Z}, \frac{2X}{Z^2}, \dots]$. Define $f' := p^k f \in \mathcal{C}(r, d'p^{k(6-r)})(\mathbb{Z}_p)$ and $(X', Y', Z') := \pi(f')$. By Proposition 9.3.2, there are only a finite number of such f', modulo $\mathrm{SL}_2(\mathbb{F}_q)$equivalence.

□

Chapter 10

Hermite Reduction Theory

Hermite reduction theory is a generalization of the reduction theory of positive definite real binary quadratic forms. In the latter theory, we say that a form is reduced if the unique root z_0 in $\mathbb{H}$ is in the usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\mathcal{D} := \{z = x + iy \ \mid \ |z| \geq 1, \ -\frac{1}{2} \leq x \leq \frac{1}{2}\}.$$

Every form is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to some reduced form and there is a bound on the coefficients of reduced forms in terms of the discriminant.

Hermite reduction theory applies to higher order forms. The Hermite determinant takes the place of the discriminant. There is an associated representative point $z_0 \in \mathbb{H}$ — usually unique. A form is reduced if z_0 in $\mathbb{H}$ is in the usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$. Every form is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to some reduced form and there is a bound on the coefficients of reduced forms in terms of the Hermite determinant.

10.1 Definition of the Hermite Determinant

Take a form $f \in \mathbb{R}[x_1, x_2]$ of order k with roots $(\mu_i : \nu_i) \in \mathbb{P}_1(\mathbb{C})$. Then

$$f = A \prod_i (\nu_i x_1 - \mu_i x_2)$$

for some $A \in \mathbb{C}^*$. For $t_i \in \mathbb{R}^*$, define $\varphi = \varphi(\overrightarrow{t})$ by

$$\varphi = \sum_{i=1}^{k} t_i^2 (\nu_i x_1 - \mu_i x_2)(\bar{\nu}_i x_1 - \bar{\mu}_i x_2).$$

This is a real quadratic form. Real values of x_1, x_2 with $(x_1, x_2) \neq (0, 0)$ give positive values of φ, so φ is a positive definite quadratic form for all t_i. Let δ be its determinant — i.e. if $\varphi = Px_1^2 - 2Qx_1x_2 + Rx_2^2$ then $\delta = PR - Q^2$.

For a fixed set of representatives μ_i, ν_i for the roots of f define

$$\Phi(\overrightarrow{t}) := \frac{|A|^2\delta^{k/2}}{(\prod t_i)^2}.$$

Definition 10.1.1 (Hermite covariant). *For a form $f \in \mathbb{R}[x_1, x_2]$ and $z \in \mathbb{C}$ define*

$$\Theta(f, z) := \begin{cases} \min \Phi(\overrightarrow{t}) & \text{over all } \overrightarrow{t} \text{ such that } \varphi(z, 1) = 0, \\ \infty & \text{if } \varphi(z, 1) = 0 \text{ for all } \overrightarrow{t}. \end{cases}$$

The use of the minimum ensures that $\Theta(f, z)$ is independent of the representatives for the roots and so is a well defined function of f and z. Since the quadratic form φ is real and positive definite it is convenient to assume $z \in \mathbb{H}$.

Definition 10.1.2 (Hermite determinant). *For any form $f \in \mathbb{R}[x_1, x_2]$ define*

$$\Theta(f) := \min_{z \in \mathbb{H}} \Theta(f, z).$$

Definition 10.1.3 (Representative point). *For any form $f \in \mathbb{R}[x_1, x_2]$, a representative point is any $z \in \mathbb{H}$ such that $\Theta(f, z) = \Theta(f)$.*

Definition 10.1.4 (Hermite-reduced). *A form $f \in \mathbb{R}[x_1, x_2]$ is called* Hermite-reduced *if it has a representative point in the usual fundamental domain for $SL_2(\mathbb{Z})$.*

10.2 Basic Properties

Theorem 10.2.1 (Covariance). *Let $f \in \mathbb{R}[x_1, x_2]$ be homogeneous of order k. Let $g \in GL_2(\mathbb{R})$. Then*

$$\Theta(f \circ g, z) = |\det(g)|^k \Theta(f, gz).$$

In particular, $\Theta(f \circ g) = |\det(g)|^k \Theta(f)$.

For this chapter only, we attach another meaning to the letter r. Following tradition, we say that a real form f has signature (r, s) if it has r real roots and s pairs of complex conjugates (counting multiplicities).

Proposition 10.2.2. *Suppose f is a real form of order k and signature (r, s) with distinct roots. If $k > 2$ or $s > 0$ then f has a unique representative point in $\mathbb{H}$.*

Proof. By Theorem 10.2.1 we can assume the roots are finite. If the signature is $(0, 1)$ we have a definite quadratic form and the representative point is its root in $\mathbb{H}$. Otherwise $k > 2$ and this is [24], Proposition 5.1. □

Proposition 10.2.3. *Suppose $f = A\prod_i(\nu_i x_1 - \mu_i x_2)$ is a real form of order $k \geq 3$ with k distinct roots. If $\Theta(f)$ is the Hermite Determinant and $z = x + iy \in \mathbb{H}$ is the representative point then*

$$\Theta(f) = \left(\frac{k}{2y}\right)^k |A|^2 \quad \prod_{j=1}^{k} \left(|\nu_j x - \mu_j y|^2 + |\nu_j y|^2\right).$$

Proof. If the roots are all finite this is contained in [24], Proposition 5.1. (Warning: the definition of the Hermite determinant in [24] differs from our definition by a constant factor $\left(\frac{2}{k}\right)^k$). When there is a root at ∞, use Theorem 10.2.1 to move the zeroes away from infinity. □

If the signature of a real form is (r, s) then it will have real roots $\alpha_1, \ldots \alpha_r$ and pairs of complex conjugate roots $\beta_1, \bar{\beta}_1, \ldots \beta_s, \bar{\beta}_s$. Using the AM/GM inequality you can show that the weight factors (t_i^2) at complex conjugate roots causing the Hermite determinant to be attained can be assumed to be equal. We therefore use the naming convention that the weights assigned to the real roots are $t_1^2, \ldots t_r^2$, and those assigned to the complex roots are $u_1^2, u_1^2, \ldots u_s^2, u_s^2$.

Proposition 10.2.4. *Suppose $f \in \mathbb{R}[x_1, x_2]_4$, and that all its roots are finite. Then weights which cause the Hermite determinant to be attained are given by:*

Signature	*Roots*	*Weights*
$(4, 0)$	$\alpha_1, \ldots \alpha_4$	$t_i^2 = \frac{1}{\lvert f'(\alpha_i, 1)\rvert}$
$(2, 1)$	α_1, α_2	$t_1^2 = \lvert\beta - \bar{\beta}\rvert\lvert\alpha_2 - \beta\rvert^2$, $t_2^2 = \lvert\beta - \bar{\beta}\rvert\lvert\alpha_1 - \beta\rvert^2$
	$\beta, \bar{\beta}$	$u_1^2 = \lvert\alpha_1 - \alpha_2\rvert\lvert\alpha_1 - \beta\rvert\lvert\alpha_2 - \beta\rvert$
$(0, 2)$	$\beta_1, \bar{\beta}_1$	$u_1^2 = \lvert\beta_2 - \bar{\beta}_2\rvert$
	$\beta_2, \bar{\beta}_2$	$u_2^2 = \lvert\beta_1 - \bar{\beta}_1\rvert$

where in the totally real case, f' denotes the derivative of f with respect to x_1.

Proof. See [13], pages 48, 57 and 59. □

Theorem 10.2.5. *Suppose*

$$f = \sum_{i=1}^{k} \binom{k}{i} a_i x_1^{k-i} x_2^i$$

is a real form of order k. If f is Hermite-reduced, then

$$|a_i a_j| \leq \left(\frac{4}{3k^2}\right)^{\frac{k}{2}} \Theta(f) \qquad \text{whenever } i+j \leq k.$$

Proof. The special case $i+j=k$ was proven by Hermite in [11]. The general case is proven in section 10.3. □

Lemma 10.2.6. *Take $f \in \mathbb{R}[x_1, x_2]$ a form of order $k > 2$ and signature (r, s). Suppose f has distinct roots and satisfies*

$$f(x_2, -x_1) = \pm f(x_1, x_2),$$

then the representative point of f is i.

Furthermore, if we factor f as $f_1 f_2$, where f_1, f_2 are real forms of signature $(r, 0)$ and $(0, s)$ respectively, then:

- *If $r > 2$, then i is also the representative point of f_1.*
- *If $s > 0$, then i is also the representative point of f_2. In particular, if $s = 1$, then i is the unique root of f_2 in $\mathbb{H}$.*

Proof. $z \mapsto -1/z$ is an $\mathrm{SL}_2(\mathbb{R})$ map which permutes the roots of f_1, f_2 and f. The only fixed points of this map are $\pm i$. As the map takes $\mathbb{H}$ into itself, i will be the representative point of any of these forms provided the representative point is unique. The result follows from Proposition 10.2.2. □

10.3 Proving the Hermite Inequalities

This section is devoted to proving Theorem 10.2.5. I do this by proving Theorem 10.3.1. Since $y \geq \frac{\sqrt{3}}{2}\max\{1, |z|\}$ whenever $z = x + iy$ is in the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$, Theorem 10.2.5 follows.

In this section we will be using S as a variable denoting a subset of the integers $\{0, 1, 2, \ldots, k\}$. Its compliment $\{0, 1, 2, \ldots, k\} \setminus S$ will be denoted S'. For any $b \in \mathbb{C}^{k+1}$ we define $b_S := \prod_{i \in S} b_i$.

Theorem 10.3.1. *Suppose*

$$f = \sum_{i=0}^{k} \binom{k}{i} a_i x_1^{k-i} x_2^i$$

is a real form of order k. Let $z \in \mathbb{H}$ and write $z = x + iy$. Then

$$|a_l|^2 \leq \frac{|z|^{2l}}{(ky)^k} \Theta(f, z) \qquad \text{for all } l.$$

Proof. Set $\Theta = \Theta(f, z)$. Choose (μ_i, ν_i) to represent the roots of f in such a way that $f = \prod(\nu_i x_1 - \mu_i x_2)$. By the definition of Θ there is a $\delta > 0$ and $t_i > 0$ such that

$$f = \frac{\sqrt{\Theta}}{\delta^{\frac{k}{4}}} \prod (t_i \nu_i x_1 - t_i \mu_i x_2),$$

and a positive definite quadratic form $\varphi := Px_1^2 - 2Qx_1x_2 + Rx_2^2$ of determinant $\delta = PR - Q^2$ which has $(z : 1)$ as a root, and whose coefficients are given by:

$$P = \sum t_i^2 |\nu_i|^2, \quad 2Q = \sum t_i^2 (\mu_i \bar{\nu}_i + \bar{\mu}_i \nu_i), \quad R = \sum t_i^2 |\mu_i|^2.$$

Writing $z = x + iy$ this means:

$$Q = xP, \quad R = P|z|^2, \quad \delta = P^2 y^2.$$

Choose $b_i, c_i \in \mathbb{C}$ so that: $\sqrt{P} b_i = \nu_i t_i$, $\sqrt{R} c_i = -\mu_i t_i$. Then $\sum |b_i|^2 = \sum |c_i|^2 = 1$ and

$$a_l = \sqrt{\Theta} \left(\frac{|z|^l}{y^{k/2}} \right) \begin{pmatrix} k \\ l \end{pmatrix}^{-1} \left(\sum_{\#S=l} b_{S'} c_S \right).$$

The theorem follows from Lemma 10.3.2. □

Lemma 10.3.2. *Suppose $b_i, c_i \in \mathbb{C}$ and $\sum_1^k |b_i|^2 = \sum_1^k |c_i|^2 = 1$. Then*

$$\left| \sum_{\#S=l} b_{S'} c_S \right| \leq \begin{pmatrix} k \\ l \end{pmatrix} \left(\frac{1}{k} \right)^{\frac{k}{2}}.$$

Proof. Clearly, the lemma holds if it holds for real non-negative b_i, c_i. By the Cauchy Schwartz inequality [2], page 9,

$$\left(\sum_{\#S=l} b_{S'} c_S \right)^2 \leq \left(\sum_{\#S=l} b_{S'}^2 \right) \left(\sum_{\#S=l} c_S^2 \right).$$

By the generalized AM/GM Inequality [2], page 15, exercise 22,

$$\sum_{\#S=l} b_{S'}^2 \leq \begin{pmatrix} k \\ l \end{pmatrix} \left(\frac{\sum_i b_i^2}{k} \right)^{k-l}, \quad \sum_{\#S=l} c_S^2 \leq \begin{pmatrix} k \\ l \end{pmatrix} \left(\frac{\sum_i c_i^2}{k} \right)^{l}.$$

Combining these inequalities gives the result. □

Chapter 11

Parameterizations in $\mathbb{Z}$

This chapter describes an algorithm to construct a finite set of parameterizations of $\mathcal{D}(r,d)(\mathbb{Z})$ for any non-zero integer d, with the property that their $\mathbb{Z}$-specializations include all co-prime $(X,Y,Z) \in \mathcal{D}(r,d)(\mathbb{Z})$.

By Theorem 6.1.1 we can assume that the parameterizations are of the form $\chi(f)$ with $f \in \mathcal{C}(r,d)(\mathbb{Z})$. By Theorem 6.2.4 constructing a complete set of parameterizations is now equivalent to giving a representative f_α for every $\mathrm{SL}_2(\mathbb{Z})$-orbit of $\mathcal{C}(r,d)(\mathbb{Z})$ that contains a binary form f whose parameterization $\chi(f)$ has a co-prime $\mathbb{Z}$-specialization.

A main ingredient to this algorithm is the fact that $\mathcal{C}(r,d)(\mathbb{R})$ is a homogeneous $\mathrm{SL}_2(\mathbb{R})$ space. This means that we can calculate the Hermite Determinant and list all of the Hermite-reduced $f \in \mathcal{C}(r,d)(\mathbb{Z})$ via a finite computer search.

The algorithm then takes this list and reduces it further so that to all f in the list are $\mathrm{SL}_2(\mathbb{Z})$-distinct and have a co-prime specialization. This is the output of the algorithm.

A variant on the algorithm reduces the list further to a list of $\mathrm{GL}_2(\mathbb{Z})$ distinct forms. By Theorem 6.2.4, reducing to a set of representatives of the $\mathrm{GL}_2(\mathbb{Z})$-orbits is equivalent to identifying $(\pm X, Y, Z) \in \mathcal{D}(r,d)(\mathbb{Z})$.

A final section 11.7 shows how the algorithm can be generalized to produce complete sets of parameterizations to diophantine equations of the type

$$AX^2 + BY^3 = CZ^r, \qquad \gcd(X,Y,Z) = 1,$$

where $A, B, C \in \mathbb{Z}$ and the unknowns X, Y, Z are required to be in $\mathbb{Z}$.

11.1 Hermite Reduction Attributes

This section shows that $\mathcal{C}(r,d)(\mathbb{R})$ is a homogeneous $\mathrm{SL}_2(\mathbb{R})$-space. We can, therefore, associate a Hermite Determinant Θ to $\mathcal{C}(r,d)(\mathbb{Z})$. Its value is

calculated along with the associated bounds on the coefficients of Hermite-reduced $f \in \mathcal{C}(r,d)(\mathbb{R})$. A method of calculating the Representative Point of $f \in \mathcal{C}(r,d)(\mathbb{R})$ is presented.

Lemma 11.1.1. *If $f \in \mathcal{C}(r,d)(\mathbb{R})$, then f has a real root.*

Proof. The Klein forms $\bar{f_r}$ were produced by taking the roots to be the image of the vertices of the platonic solids under the 1-1 correspondence between the Riemann Sphere $\mathrm{S}_2(\mathbb{R})$ and the extended complex plane $\mathbb{P}(\mathbb{C})$, given by stereographic projection.

As such the roots of $\bar{f_r}$ inherit the following properties from the platonic solid:

(Special Properties)
No circles on $\mathbb{P}(\mathbb{C})$ going through an even number of roots of $\bar{f_r}$ can go through more than 4 roots.
If a circle goes through 4 roots, the circle will split $\mathbb{P}(\mathbb{C})$ into 2 distinct regions. There will be roots in the interior of both regions.

Since the action of $\mathrm{GL}_2(\mathbb{C})$ is continuous on $\mathbb{P}(\mathbb{C})$ and $\mathrm{GL}_2(\mathbb{C})$ is connected, topological properties are $\mathrm{GL}_2(\mathbb{C})$ invariant. The action also sends circles to circles.[1] This means that these special properties of $\bar{f_r}$ will be true of all $\mathrm{GL}_2(\mathbb{C})$ twists as well.

Suppose that $f \in \mathcal{C}(r,d)(\mathbb{R})$ has only complex roots. By shrinking a large circle enclosing all its roots we can produce a circle witnessing the fact that f cannot possibly have these special properties.

Therefore f has a real root. □

Theorem 11.1.2. *Let $f \in \mathcal{C}(r,d)(\mathbb{R})$ and $f' \in \mathcal{C}(r,d')(\mathbb{R})$ be real Klein forms.*

- *If $dd' > 0$ then f, f' are $GL_2(\mathbb{R})^+$-equivalent*
- *If $dd' < 0$ and r is odd, then f is $GL_2(\mathbb{R})^+$-equivalent to $-f'$.*

(Here $GL_2(\mathbb{R})^+$ is the set of $GL_2(\mathbb{R})$ matrices of positive determinant).

Proof. By Proposition 4.1.2, $-f \in \mathcal{C}(r,(-1)^r d)$, so the second claim follows from the first. We therefore assume that $dd' > 0$. Another call to Proposition 4.1.2 shows that we can apply a $\mathrm{GL}_2(\mathbb{R})^+$ transformation and assume $d = d' = \pm 1$.

By Lemma 11.1.1, f has a real root. Therefore we can apply an $\mathrm{SL}_2(\mathbb{R})$ transformation and assume that the root is ∞ and the initial coefficients $[a_0, a_1, a_2 \dots]$ of f are $[0, 1, 0 \dots]$. The defining equations for $\mathcal{C}(r,d)$ determine f completely.

We can do the same to f'. This means that f, f' are $\mathrm{GL}_2(\mathbb{R})^+$-equivalent. □

[1] where as usual we count straight lines through ∞ as circles in $\mathbb{P}(\mathbb{C})$

Corollary 11.1.3. *If $d \in \mathbb{R}^*$, then $\mathcal{C}(r,d)(\mathbb{R})$ is a homogeneous $SL_2(\mathbb{R})$-space.*

Theorem 11.1.4. *Suppose $f \in \mathcal{C}(r,d)(\mathbb{R})$. Write $f = f_1 f_2$, where f_1, f_2 are real forms, and all roots of f_1 are real and all roots of f_2 are complex. Then:*

Class	*Signature*	$\Theta(f)$	*A fast way to find the Representative Point*
$\mathcal{C}(3,d)$	$(2,1)$	$2^6 3^3 \lvert d\rvert^{2/3}$	
$\mathcal{C}(4,d), d>0$	$(4,1)$	$2^8 3^9 \lvert d\rvert$	*The unique root of f_2 in $\mathbb{H}$*
$\mathcal{C}(4,d), d<0$	$(2,2)$	$2^8 3^9 \lvert d\rvert$	*The representative point of f_2*
$\mathcal{C}(5,d)$	$(4,4)$	$2^{24} 3^{18} 5^5 \lvert d\rvert^2$	*The representative point of f_1*

In particular, the representative point of f can be found using at most an application of Proposition 10.2.4 to find the representative point of a biquadratic form.

Proof. We start by verifying the table for the special representatives of the 4 rows: $\bar{f} = \bar{f}_3, \bar{f}_4, \bar{f}_4^*, \bar{f}_5$. Certainly the signature is correct.

Using Proposition 10.2.4, we find that i is the representative point of $\bar{f}_3$. By Lemma 10.2.6, i is also the representative point of the other $\bar{f}$ and the suggested method in the last column is a way of finding the representative point of these $\bar{f}$. Knowing that i is the representative point, we can use Proposition 10.2.3 and verify that the table produces the correct value for $\Theta(\bar{f})$. So the table is correct for $\bar{f}$.

By Theorem 11.1.2, a general $f \in \mathcal{C}(r,d)$ satisfies $\pm f = \bar{f} \circ g$ for some $g \in \mathrm{GL}_2(\mathbb{R})^+$. Furthermore, by Proposition 4.1.2 and Theorem 10.2.1

$$\det(g)^6 = d, \quad \Theta(f) = |\det(g)|^k \Theta(\bar{f}).$$

This and the covariance of the representative point under $\mathrm{GL}_2(\mathbb{R})^+$ transformations show that the table is correct for all $f \in \mathcal{C}(r,d)$. □

Theorem 11.1.5. *Suppose $f \in \mathcal{C}(r,d)(\mathbb{R})$ is* Hermite-reduced. *Then the $|a_i a_j|$ satisfy*

$$\max\{|a_i a_j| \mid i+j \le k\} \le B^2,$$

where the bound B is given by

Class	B
$\mathcal{C}(3,d)$	$2\sqrt{3}\lvert d\rvert^{1/3}$
$\mathcal{C}(4,d)$	$16\sqrt{\lvert d\rvert}$
$\mathcal{C}(5,d)$	$1600\sqrt{5}\lvert d\rvert \sim 3578\lvert d\rvert$

.

In particular $|a_i| \le B$ for all $i \le \frac{1}{2}k$.

Proof. The bounds are obtained applying Theorem 10.2.5 to the Hermite determinant as listed in the table in Theorem 11.1.4 □

11.2 Listing Hermite-reduced $f \in \mathcal{C}(r,d)(\mathbb{Z})$

By Theorem 11.1.5, Hermite-reduced $f \in \mathcal{C}(r,d)(\mathbb{Z})$ have coefficients that are bounded in terms of r and d. Furthermore, examining the defining equations of $\mathcal{C}(r,d)$ shows that the form is known once a_0, a_1, a_2, a_3 is given.

The following pseudo-code shows how to produce a list of $f \in \mathcal{C}(r,d)(\mathbb{Z})$ including all forms which are Hermite-reduced and have $a_0 \neq 0$.

ALGORITHM(Hermite-reduced Forms; $a_0 \neq 0$)
    INPUT (r,d)
    Calculate B from the table in Theorem 11.1.5
    FOR $a_0, a_1, a_2 \in \mathbb{Z}$ with $|a_i| \leq B, a_0 \neq 0$ DO
        $Z := a_0$, $Y := a_0 a_2 - a_1^2$
        FOR the at most 2 integers $X := \pm\sqrt{-Y^3 - dZ^r}$ DO
            Determine a_3 from $a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3 = 2X$
            The remaining $a_4, \ldots, a_k$ are determined from
                the equations defining $\mathcal{C}(r,d)$

            IF all of Ω_r are integers
            AND the a_i satisfy the bounds of Theorem 11.1.5
                OUTPUT the form $f = [a_0, a_1 \ldots a_k]$
            END-IF
        END-FOR
    END-FOR
    STOP

A slight variant on this pseudo-code allows us to list the Hermite-reduced forms with $a_0 = 0$. We use Theorem 11.1.4 to find the representative points of the forms. We reduce our list to a set of Hermite-reduced $f \in \mathcal{C}(r,d)(\mathbb{Z})$ by discarding any forms for which the representative point is not in the fundamental domain.

Remark 11.2.1. *This is the computationally expensive part of the algorithm. My C program running in a* 350 *Mhz Pentium II took* 6 *hours to produce the list associated with the icosahedral equation* $X^2 + Y^3 = -Z^5$.

11.3 Listing $\mathrm{GL}_2(\mathbb{Z})$-orbits of $\mathcal{C}(r,d)(\mathbb{Z})$

In this section, we show how to take the list of Hermite-reduced forms, and reduce the list to a set of $\mathrm{GL}_2(\mathbb{Z})$ inequivalent forms.

The group $\mathrm{GL}_2(\mathbb{Z})$ acts on $\mathbb{C} - \mathbb{R}$. Conjugation acts freely on $\mathbb{C} - \mathbb{R}$ and commutes with the $\mathrm{GL}_2(\mathbb{Z})$ action. Since $\mathbb{H} = (\mathbb{C} - \mathbb{R})/ <$ conjugation $>$ it follows that $\mathrm{GL}_2(\mathbb{Z})$ acts on $\mathbb{H}$. The $\mathrm{GL}_2(\mathbb{Z})$ map $z \mapsto -z$ becomes $x + iy \mapsto -x + iy$ on $\mathbb{H}$.

A fundamental domain for $\mathrm{GL}_2(\mathbb{Z})$ is given by

$$\mathcal{D}^- := \{z = x + iy \mid |z| \geq 1, -\frac{1}{2} \leq x \leq 0\}.$$

Every $z \in \mathbb{H}$ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a unique $z \in \mathcal{D}^-$. We say that a form f is $\mathrm{GL}_2(\mathbb{Z})$ reduced if $z(f) \in \mathcal{D}^-$. We throw away all but the $\mathrm{GL}_2(\mathbb{Z})$ reduced forms.

Furthermore 2 reduced forms f_1, f_2 are $\mathrm{GL}_2(\mathbb{Z})$-equivalent if and only if $z(f_1) = z(f_2) =: z$ and $f_1 = f_2 \circ g$ for some $g \in \mathrm{Stab}(z) := \mathrm{Stab}(z, \mathrm{GL}_2(\mathbb{Z}))/\pm I$. The following lemma gives us a definite test of which forms are equivalent.

Lemma 11.3.1. *Let $i = \sqrt{-1}$ and $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Define*

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Suppose $z = x + iy \in \mathcal{D}^-$. The group Stab$(z)$ is trivial on the interior of $\mathcal{D}^-$. On the boundary of $\mathcal{D}^-$ it is the finite group given in the following table.

z	*Stab*(z)	$\#$*Stab*(z)	$z \neq i, w$	*Stab*(z)	$\#$*Stab*(z)
w	$< ST, US >$	6	$x = 0$	$< U >$	2
i	$< S, U >$	4	$\lvert z\rvert = 1$	$< US >$	2
			$x = -\frac{1}{2}$	$< U >$	2

11.4 Listing $\mathrm{SL}_2(\mathbb{Z})$-orbits of $\mathcal{C}(r,d)(\mathbb{Z})$

Only listing representatives of $\mathrm{GL}_2(\mathbb{Z})$-orbits keeps our lists as short as possible. However by Theorem 6.2.2, every f gives us potentially two parameterizations $(\pm\frac{1}{2}\boldsymbol{t}(f), \boldsymbol{H}(f), f)$. These correspond to one or two distinct parameterizations depending on whether the $\mathrm{GL}_2(\mathbb{Z})$-orbit of f splits into one or two $\mathrm{SL}_2(\mathbb{Z})$-orbits. This section shows how to recognize when a $\mathrm{GL}_2(\mathbb{Z})$-orbit splits using the representative point.

Proposition 11.4.1. *Let a $GL_2(\mathbb{Z})$-orbit be represented by f with representative point in $\mathcal{D}^-$. Let $z = x + iy$ be that point. The binary form $f \in \mathbb{R}[s,t]$ remains the representative of a single $SL_2(\mathbb{Z})$-orbit if and only if z is on the boundary of $\mathcal{D}^-$ and:*

$(z = \omega)$ *$f(s+t, -t) = f(s,t)$,$f(-t, s+t)$ or $f(s+t, -s)$.*

$(z = i)$ *$f(s,t) = f(t,s)$ or the odd index coefficients of f are zero.*

$(z \neq i, \omega)$

- *$x = 0$ and the odd index coefficients of f are zero.*

- *Or* $|z| = 1$ *and* $f(s,t) = f(t,s)$.
- *Or* $x = -\frac{1}{2}$ *and* $f(s+t,-t) = f(s,t)$.

Proof. If it is also an $\mathrm{SL}_2(\mathbb{Z})$ class, there is a $g \in \mathrm{SL}_2(\mathbb{Z})$ so that $f \circ g = f(s,-t)$. This must map $z = x+iy \mapsto -x+iy$. The proposition enumerates the possibilities. □

11.5 Ensuring Co-prime Specializations

This section shows how we can establish whether an $f \in \mathcal{C}(r,d)(\mathbb{Z})$ has any co-prime $\mathbb{Z}$-specializations.

Proposition 11.5.1. *Fix* $f \in \mathcal{C}(r,d)(\mathbb{Z})$ *with* $d \in \mathbb{Z}_{\neq 0}$. *Either*

- $\chi(f)$ *has no co-prime integer specializations; or*
- *there are* $(s_1,s_2) \in \mathbb{Z}^2$ *with* $|s_i| \leq N_0$ *such that* $\chi(f)(s_1,s_2)$ *are co-prime;*

where N_0 *is the product of all odd primes dividing* Nd.

Proof. (sketch) This is a standard application of resultant theory (e.g. [16], Chapter IX) to the forms $f, \boldsymbol{H}(f)$. These forms have integer coefficients, and the primes that divide their resultant can be shown to be exactly the primes dividing Nd. □

11.6 The Algorithm for $X^2 + Y^3 = dZ^r$

This section presents the explicit algorithm to construct a complete set of parameterizations of $\mathcal{D}(r,d)(\mathbb{Z})$ whose $\mathbb{Z}$-specializations include all co-prime $(X,Y,Z) \in \mathcal{D}(r,d)(\mathbb{Z})$.

ALGORITHM ($X^2 + Y^3 = dZ^r$)
INPUT (r,d)
Produce a complete list of Hermite-reduced $f \in \mathcal{C}(r,d)(\mathbb{Z})$ (section 11.2)
Reduce the list down to a set of $\mathrm{GL}_2(\mathbb{Z})$ inequivalent forms (section 11.3)
Remove forms not specializing to co-prime integers (section 11.5)
OUTPUT($f_1, f_2, \ldots, f_n$)
STOP

For every co-prime integer solution (X,Y,Z), at least one of $(\pm X, Y, Z)$ is an integer specialization of one of the parameterizations $\chi(f_1), \ldots \chi(f_n)$. By Theorem 6.2.2, this list is minimal.

If you do not like the $\pm$ you should add $f_i(x_1,s_2)^* := f_i(x_1,-x_2)$ to the list for every f_i whose $\mathrm{GL}_2(\mathbb{Z})$-equivalence class splits into two $\mathrm{SL}_2(\mathbb{Z})$ classes. Section 11.4 shows how to identify such forms. The integer specializations of this larger list $\chi(f_1), \ldots \chi(f_m)$ includes all co-prime integer solutions. By Theorem 6.2.2, this list is also minimal.

11.7 Generalizing to $AX^2 + BY^3 = CZ^r$

In this section we show how the algorithm can be generalized to some other diophantine problems associated to the indices $\{2, 3, r\}$.

Proposition 11.7.1. *Fix a non zero integer d and a finite set of primes S. There is a finite set of solutions in $\mathbb{Z}_S[x_1, x_2]$ to*

$$X^2 + Y^3 = dZ^r$$

such that

- *their integer specializations include all integer solutions with* $\gcd(X, Y, Z) \in \mathbb{Z}_S^*$,
- *their $\mathbb{Z}_S$ specializations include all $\mathbb{Z}_S$ solutions with* $\gcd(X, Y, Z) \in \mathbb{Z}_S^*$.

Proof. Suppose $f \in \mathcal{C}(r, d)(\mathbb{C})$, $\lambda \in \mathbb{C}^*$ and $s_1, s_2 \in \mathbb{C}$. If $\chi(f)(s_1, s_2) = (X, Y, Z)$ then

$$\chi(f)(\lambda s_1, \lambda s_2) = (\lambda^{N/2} X, \lambda^{N/3} Y, \lambda^{N/r}). \tag{11.1}$$

The claim about $\mathbb{Z}_S$ solutions follows from the claim about $\mathbb{Z}$ solutions. We assume X, Y, Z are $\mathbb{Z}$-integers. By (11.1) we can assume that the valuation of $\gcd(X^2, Y^3, Z^r)$ at any prime p is less than N.

Take a prime p that divides $\gcd(X, Y)$. If $p^5 | dZ^r$ then :

$$X = p^3 X', \quad Y = p^2 Y', \quad dZ = d'(p^s Z')$$

for some $s \geq 0$ and some integers X', Y', Z', d' satisfying

$$X'^2 + Y'^3 = d' Z'^r.$$

In this way we can reduce to a finite set of equations in which we can assume that if p divides $\gcd(X, Y)$ then $\nu_p(Z^r)$ is less than 5. For $r = 5$ this is equivalent to assuming $\gcd(X, Y, Z) = 1$. For $r = 3, 4$ it is that $p | \gcd(X, Y)$ implies that $\nu_p(Z) = 0$ or 1.

The proofs go through producing $f \in \mathbb{Z}_S[x_1, x_2]$ with coefficients of both bounded absolute value and bounded denominator. Hermite reduction can therefore still be used to produce the parameterizations. □

Theorem 11.7.2. *Fix $r \in \{3, 4, 5\}$. Fix a finite set of primes S. Fix $A, B \in Z_S^*$ and non zero $C \in Z_S$. Then there is a finite set of solutions in $\mathbb{Z}_S[x_1, x_2]$ to*

$$AX^2 + BY^3 = CZ^r$$

such that

- *their integer specializations include all integer solutions with* $\gcd(X, Y, Z) \in \mathbb{Z}_S^*$,
- *their* $\mathbb{Z}_S$ *specializations include all* $\mathbb{Z}_S$ *solutions with* $\gcd(X, Y, Z) \in \mathbb{Z}_S^*$.

Proof. Without loss of generality $A, B, C \in \mathbb{Z}$. Multiply the diophantine equation by A^3B^2 to give:

$$(A^2BX)^2 + (ABY)^3 = (A^3B^2C)Z^r.$$

Since $A^2B, AB \in \mathbb{Z}_S^*$ the theorem follows from Proposition 11.7.1. □

Appendix A

Defining Equations of $\mathcal{C}(r, d)$

This appendix contains a definition of the map $\pi : \mathcal{C}(r, d) \to \mathbb{A}^3$, along with the explicit set of equations used to define the algebraic set $\mathcal{C}(r, d) \subset \mathbb{A}^{k+1}$.

For any $f \in \mathcal{C}(r, d)$, we have the map $f \mapsto 2 * \pi(f) := (2X, 2Y, 2Z)$. This is defined by

$$\begin{aligned} Z &= a_0, \\ Y &= a_0 a_2 - a_1^2, \\ 2X &= a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3. \end{aligned}$$

A.1 $\mathcal{C}(3, d)$ - The Tetrahedron

If $d \in \bar{K}^*$ then $\mathcal{C}(3, d) \subseteq \mathbb{A}^5$ is defined by

$$\begin{aligned} 0 &= a_0 a_4 - 4a_1 a_3 + 3a_2^2, \\ -4d &= a_0 a_2 a_4 + 2a_1 a_2 a_3 - a_2^3 - a_0 a_3^2 - a_1^2 a_4. \end{aligned}$$

A.2 $\mathcal{C}(4, d)$ - The Octahedron

If $d \in \bar{K}^*$ then $\mathcal{C}(4, d) \subseteq \mathbb{A}^7$ is defined by

$$\begin{aligned} D_0/1 : 0 &= a_0 a_4 - 4a_1 a_3 + 3a_2^2, \\ D_1/2 : 0 &= a_0 a_5 - 3a_1 a_4 + 2a_2 a_3, \\ D_2/1 : 0 &= a_0 a_6 - 9a_2 a_4 + 8a_3^2, \\ D_3/2 : 0 &= a_1 a_6 - 3a_2 a_5 + 2a_3 a_4, \\ D_4/1 : 0 &= a_2 a_6 - 4a_3 a_5 + 3a_4^2, \\ A : -72d &= a_0 a_6 - 6a_1 a_5 + 15a_2 a_4 - 10a_3^2. \end{aligned}$$

A.3 $\mathcal{C}(5, d)$ - The Icosahedron

If $d \in \bar{K}^*$ then $\mathcal{C}(5, d) \subseteq \mathbb{A}^{13}$ is defined by

$$
\begin{aligned}
D_0/1 :&\ 0 = a_0a_4 - 4a_1a_3 + 3a_2^2,\\
D_1/8 :&\ 0 = a_0a_5 - 3a_1a_4 + 2a_2a_3,\\
D_2/4 :&\ 0 = a_0(7a_6) - 12a_1a_5 - 15a_2a_4 + 20a_3^2,\\
D_3/56 :&\ 0 = a_0a_7 - 6a_2a_5 + 5a_3a_4,\\
D_4/14 :&\ 0 = 5a_0a_8 + 12a_1a_7 - 6a_2(7a_6) - 20a_3a_5 + 45a_4^2,\\
D_5/56 :&\ 0 = a_0a_9 + 6a_1a_8 - 6a_2a_7 - 4a_3(7a_6) + 27a_4a_5,\\
D_6/28 :&\ 0 = a_0a_{10} + 12a_1a_9 + 12a_2a_8 - 76a_3a_7 - 3a_4(7a_6) + 72a_5^2,\\
D_7/8 :&\ 0 = a_0a_{11} + 24a_1a_{10} + 90a_2a_9 - 130a_3a_8 - 405a_4a_7 + 60a_5(7a_6),\\
D_8/1 :&\ 0 = a_0a_{12} + 60a_1a_{11} + 534a_2a_{10} + 380a_3a_9 - 3195a_4a_8\\
&\qquad\qquad - 720a_5a_7 + 60(7a_6)^2,\\
D_9/8 :&\ 0 = a_1a_{12} + 24a_2a_{11} + 90a_3a_{10} - 130a_4a_9 - 405a_5a_8 + 60(7a_6)a_7,\\
A_0 :&\ 0 = 360a_0d + a_0(7a_6) - 42a_1a_5 + 105a_2a_4 - 70a_3^2,\\
A_1 :&\ 0 = 6(720a_1d + 7a_0a_7 - 5a_1(7a_6) + 63a_2a_5 - 35a_3a_4),
\end{aligned}
$$

along with equations labelled $D_{10}, \ldots, D_{16}$ and $A_2, \ldots, A_{12}$ that have been omitted. These omitted equations are not required in practical calculations. If necessary, they may be obtained as follows.

$$
\begin{aligned}
D_{16-i}(a_0, \ldots, a_{12}) &= D_i(a_{12}, \ldots, a_0),\\
A_i(a_0 \ldots a_{12}) &= \frac{1}{i!}\Delta^i A_0
\end{aligned}
$$

(where Δ is the Cayley Aronhold Operator of Definition 3.2.1).

Finally, we require that the following equations be satisfied.

$$
\begin{aligned}
D_4^* :&\ 0 = -a_0^3a_8 + 12a_0a_1a_2a_3 + 18a_0a_2^2a_4 - 24a_0a_2a_3^2 + 4a_0^2a_3a_5 - 9a_0^2a_4^2,\\
A' :&\ 0 = -2^9 3^5 5^2 d^2 + 7a_0a_{12} - 84a_1a_{11} + 462a_2a_{10} - 1540a_3a_9\\
&\qquad + 3465a_4a_8 - 5544a_5a_7 + 66(7a_6)^2.
\end{aligned}
$$

(If $\mathrm{char}(K) \neq 5$, the equation labelled D_4^* is implied by $D_2 = D_3 = D_4 = 0$).

Appendix B

Fields of Low Characteristic

Certain propositions about $\mathcal{C}(r,d)$ that are trivial when $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > k$ become false or, if true, need extra arguments in low non-zero characteristics. This Appendix contains proofs of these properties.

Lemma B.0.1. *Suppose $d \in K^*$ and $a \in K^*$. Then*

$$\hat{\varphi}(a) := \begin{cases} [0,a,0,0,4a^{-2}d] & \textit{Tetrahedron}, \\ [0,a,0,0,0,12a^{-1}d,0] & \textit{Octahedron}, \\ [0,a,0,0,0,0,\frac{144d}{7},0,0,0,0,-a^{-1}(144d)^2,0] & \textit{Icosahedron} \end{cases}$$

is an element of $\mathcal{C}(r,d)(K)$. In particular $\mathcal{C}(r,d)(K) \neq \emptyset$.

Proof. This is verified by calculation. □

Proposition B.0.2. *Suppose K is a field and $2, d \in K^*$. If $(X,Y,Z) \in \mathcal{D}(r,d) - (0,0,0)$, there is a $\varphi \in \mathcal{C}(r,d)(K)$ so that $\pi(\varphi) = (X,Y,Z)$.*

Proof. If $Z = 0$, we let $\varphi := \hat{\varphi}(-X/Y)$, where $\hat{\varphi}$ is the function defined in Lemma B.0.1. One checks that $\pi(\varphi) = (X,Y,Z)$.

If $Z \neq 0$, define

$$\varphi := [Z, 0, \frac{Y}{Z}, \frac{2X}{Z}, \dots],$$

where the omitted terms are uniquely determined by the first $k-3$ defining equations of $\mathcal{C}(r,d)$. The coefficients of φ can be expressed as elements in the ring $\mathbb{Z}[X,Y,Z,Z^{-1}]$. With the help of PARI we get the algebraic identities

$$\boldsymbol{\tau}_4(\varphi) = 0, \quad 7\boldsymbol{\tau}_6(\varphi) = -360\left(\frac{X^2+Y^3}{Z^5}\right),$$
$$7\boldsymbol{\tau}_{12}(\varphi) = 3110400\left(\frac{X^2+Y^3}{Z^5}\right)^2,$$

when $r = 5$, and similar identities when $r = 3, 4$. This shows that φ is a 'generic' lift of the element (X,Y,Z). The result follows. □

Proposition B.0.3. *Suppose K a field and $d \in K^*$. If $g \in GL_2(K)$ and $\lambda \in K^*$ then*

$$\varphi \in \mathcal{C}(r,d) \Rightarrow \lambda g \cdot \varphi \in \mathcal{C}(r,d'),$$

where $d' = \lambda^{6-r} \det(g)^{-6} d$.

Proof. The claim about multiplication by $\lambda \in K^*$ is clear by examining the defining equations of $\mathcal{C}(r,d)(K)$. Furthermore, any $g \cdot f$ can be written as $g \cdot f = \lambda g'.f$ with $g' \in \mathrm{SL}_2(K)$ and $\lambda \in K^*$ satisfying $\lambda^{6-r} = \det(g)^6$. Therefore we can assume $g \in \mathrm{SL}_2(K)$.

We are left to show that if $g \in \mathrm{SL}_2(K)$ and $\varphi \in \mathcal{C}(r,d)(K)$ then $g \cdot \varphi \in \mathcal{C}(r,d)$. The subsets of the equations defining $\mathcal{C}(r,d)$ that are equivalent to the vanishing of a polynomial combination of covariants of φ, necessarily remain valid by the definition of a covariant. This is true for all equations, except the equations derived from the coefficients of the 4th covariant $\boldsymbol{\tau}_4(\varphi)$, and the icosahedral equation labelled D_4^*.

The equations obtained by requiring that $\boldsymbol{\tau}_4$ vanish remain valid after an $\mathrm{SL}_2(K)$ substitution because of the covariance of $\boldsymbol{\tau}_4$. However, there is an added complication since the equations for $\mathcal{C}(r,d)$ are obtained from the coefficients of $\boldsymbol{\tau}_4(f)$ after dividing out by their content. Let V be the algebraic set defined by these equations.

Note that

$$\begin{pmatrix} \kappa & 0 \\ 0 & \kappa^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix}, \tag{B.1}$$

where $\kappa \in K^*$ and $\nu \in K$, generate $\mathrm{SL}_2(K)$. By inspection V is closed under the action of the first two generators. A calculation (e.g. with the help of a computer package) shows that it is also closed under the action of the last generator.

Finally, we must check the equations remain closed under $\mathrm{SL}_2(K)$-substitutions if we also require that D_4^* is satisfied in the icosahedral case. This is also done by checking the claim on the generators (B.1) of $\mathrm{SL}_2(K)$.

□

Lemma B.0.4. *Suppose $d \in K^*$ and $\varphi \in \mathcal{C}(r,d)(\bar{K})$. Then there is a $g \in SL_2(\bar{K})$ so that $a_0(g \cdot \varphi) = 0$. If $N \in K^*$, there is a $g \in SL_2(K)$ so that $g \cdot \varphi = [0,1,0,\dots]$.*

Proof. Let $f := f(\varphi)$. We can find $g \in \mathrm{SL}_2(\bar{K})$ so that the binary form $g \cdot f$ has a zero at ∞. Since $\varphi \mapsto f(\varphi)$ is $\mathrm{SL}_2(\bar{K})$-equivariant we have $a_0(g \cdot \varphi) = 0$.

If $N \in K^*$, f has no multiple roots, as the discriminant of f is non-zero. Therefore, by equivariance, $a_1(g \cdot \varphi) \neq 0$. Twisting with an $\mathrm{SL}_2(K)$ matrix of the shape $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ allows us to suppose $g \cdot \varphi = [0,1,0,\dots]$.

□

Lemma B.0.5. *Suppose $N, d \in K^*$. Then $\mathcal{C}(r,d)(\bar{K})$ is a homogeneous $SL_2(\bar{K})$-space and $\mathcal{C}(r)(\bar{K})$ is a homogeneous $GL_2(\bar{K})$-space.*

Proof. Suppose $\varphi \in \mathcal{C}(r,d)(\bar{K})$. By Lemma B.0.4, we can assume that $\varphi = [0,1,0,\dots]$. However, as $N \in K^*$, the missing coefficients are determined by the defining equations of $\mathcal{C}(r,d)$. We have shown that there is a single element of $\mathcal{C}(r,d)$ to which every $\varphi \in \mathcal{C}(r,d)$ is $\mathrm{SL}_2(\bar{K})$-equivalent. This means that $\mathcal{C}(r,d)(\bar{K})$ is a homogeneous $\mathrm{SL}_2(\bar{K})$-space. As a corollary $\mathcal{C}(r)(\bar{K})$ is a homogeneous $\mathrm{GL}_2(\bar{K})$-space. □

Remark B.0.6. *Lemma B.0.5 is not true without some restrictions on the characteristic of K. For instance, if K has char$(K) = 2$ then $[0,1,0,0,1]$ and $[0,1,0,1,0]$ are elements of $\mathcal{C}(3,1)(K)$. These lie in distinct $SL_2(\bar{K})$-orbits, since being of the shape $[0,*,0,*,0]$ is an $SL_2(\bar{K})$-invariant property.*

Proposition B.0.7. *Suppose K is a field and $N \in K^*$. Suppose $(X,Y,Z) \in \mathcal{D}(r,d) - (0,0,0)$. If $\varphi \in \mathcal{C}(r,d)(K)$ and $\pi(\varphi) = (X,Y,Z)$ then there is a unique parabolic $g \in SL_2(K)$ so that*

$$g \cdot \varphi := \begin{cases} [Z, 0, \frac{Y}{Z}, \frac{2X}{Z}, \dots] & \text{if } Z \neq 0, \\ [0, -X/Y, 0, \dots] & \text{if } Z = 0, \end{cases}$$

where the omitted terms are uniquely determined by the defining equations of $\mathcal{C}(r,d)$.

Proof. (Existence) Since $N \in K^*$, there is a parabolic $g \in \mathrm{SL}_2(K)$ so that the φ has the shape $[*,0,\dots]$ if $Z \neq 0$, and $[0,*,0,\dots]$ if $Z = 0$. Since $\pi(\varphi) = \pi(g \cdot \varphi) = (X,Y,Z)$, the initial coefficients of φ agree with the coefficients in the announcement of the proposition. The defining equations of $\mathcal{C}(r,d)$ determine the rest of Ω_r.

(Uniqueness) Suppose φ has the canonical form given. Since $N \in K^*$, there is no non-zero parabolic $g \in \mathrm{SL}_2(K)$ that fixes φ.

□

Lemma B.0.8. *If $N, d \in K^*$ and $\varphi \in \mathcal{C}(r,d)$ then $\#\Gamma(\varphi) = 2N$. Furthermore, if φ corresponds to the coefficients of one of the forms chosen in § 4.3, then the explicit description of the group given in § 4.3 is the group $\Gamma(\varphi)(\bar{K})$.*

Proof. Since $N \in K^*$, the space $\mathcal{C}(r)(K)$ is a homogeneous $\mathrm{GL}_2(K)$-space by Lemma B.0.5. This means that we can assume that φ corresponds to one of the Klein forms mentioned in § 4.3. Let Γ' denote the group of symmetries mentioned in § 4.3, and $\Gamma := \Gamma(\varphi)$ the full group of symmetries. Clearly $\Gamma' \subset \Gamma(\varphi)$. Indeed, the set of equations witnessing the truth of the statement $\Gamma' \subset \Gamma(\varphi)$ in $\overline{\mathbb{Q}}$ can be written as a set of polynomial equations in the ring generated by $\mathbb{Z}$ and the entries of elements of Γ'. These identities remain valid in the field K.

Suppose that $g \in \Gamma(\varphi)$. We will show that $g \in \Gamma'$. Let $f := f(\varphi)$. Calculating the discriminant we see that the roots of f are distinct if $N, d \in K^*$. Since Γ' is transitive on the roots of f, we can multiply g by an element of Γ' and assume that g fixes the root at ∞. Therefore, $g = \begin{pmatrix} \kappa & \nu \\ 0 & \kappa^{-1} \end{pmatrix}$ for some $\kappa \in K^*$, $\nu \in K$. Since $\varphi = [0, *, 0, \dots]$ and $N \in K^*$ we calculate that $\nu = 0$. The matrix g is diagonal and we deduce that $g \in G'$. Conclusion: $\Gamma(\varphi) = \Gamma'$.

Finally, we must show that $\#\Gamma' = 2N$. I.e. that Γ' has no kernel when we reduce from $\mathrm{SL}_2(\overline{\mathbb{Q}})$ to $\mathrm{SL}_2(\bar{K})$. Let $f := \boldsymbol{f}(\varphi)$. Suppose $g \in \Gamma'(\overline{\mathbb{Q}})$ is not $\pm I$. Then g induces a non-trivial permutation of the roots of $f \in \overline{\mathbb{Q}}[x, y]$. As $N, d \in \bar{K}^*$, we have $\mathrm{disc}(f) \neq 0$, so the roots of f remain distinct in $\bar{K}$. Therefore the kernel is contained in $\{\pm I\}$. As $2 \in \bar{K}^*$, the matrix $-I$ is not in the kernel. Conclusion: $\#\Gamma(\varphi)(K) = \#\Gamma(\varphi)(\overline{\mathbb{Q}}) = 2N$.

□

Remark B.0.9. *Consider* $\varphi = [0, 144, 0, 0, 0, 0, \frac{144}{7}, 0, 0, 0, 0, -144, 0]$. *We have* $f := f(\varphi) = 1728d\ xy(x^{10} + 11x^5y^5 - y^{10})$

Suppose K *is a field with* $char(K) = 11$. *Then* f *has distinct roots, as the discriminant is non-zero. However,* $\Gamma(f)$ *contains the cyclic group of order* 11 *generated by* $g := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. *This means that* $\Gamma(f) \neq \Gamma(\varphi)$. *Set* $\varphi' := g \cdot \varphi$. *Then* φ, φ' *are distinct elements of* $\mathcal{C}(5, d)$ *with* $f(\varphi) = f(\varphi')$.

Appendix C

Twisted Conjugacy Classes

This Appendix contains proofs of various claims about twisted conjugacy classes. These objects act in many ways like the usual conjugacy classes of Group Theory. The proofs have been placed in this appendix for completeness.

In this appendix we assume that $H \leq G$ are arbitrary finite groups. We assume that ψ is an automorphism of G that induces an automorphism of H. See § 8.4 for the definitions of (ψ, H)-conjugacy, $[g]_{(\psi,H)}$ and $C_{(\psi,H)}(g)$.

Lemma C.0.1. *Take any $g \in G$. Then $C_{(\psi,H)}(g)$ is a subgroup of H. We have*

$$\#[g]_{(\psi,H)} \ \ \#C_{(\psi,H)}(g) \ = \ \#H.$$

Proof. $C_{(\psi,H)}(g)$ is clearly a subgroup of H. For $h_1, h_2 \in H$ we have

$$\begin{aligned} h_1^{-1} g\psi(h_1) = h_2^{-1} g\psi(h_2) \Leftrightarrow & \quad g = (h_1 h_2^{-1})^{-1} g\psi(h_2 h_1^{-1}) \\ \Leftrightarrow & \quad h_1 h_2^{-1} \in C_{(\psi,H)}(g), \end{aligned}$$

so that the distinct elements of $[g]_{(\psi,H)}$ are in $1-1$ correspondence with the right cosets of $C_{(\psi,H)}$. The result follows. □

Proposition C.0.2. *Suppose $H \lhd G$ are groups and G/H is a cyclic group of order n. Suppose ψ is the automorphism of H given by conjugation $a \mapsto sas^{-1}$ for some $s \in G$ whose image in G/H generates this cyclic group. Then*

$$H \to Hs, \quad g \mapsto gs$$

is a bijection that maps (ψ, H)-conjugacy classes of H to G-conjugacy classes of the coset Hs of G. Furthermore

$$\#C_{(\psi,H)}(g) = \frac{1}{n} \ \#C_G(gs).$$

Proof. Suppose $g, g' \in H$. If $h \in H$ then

$$g = h^{-1}g'\psi(h) \Leftrightarrow gs = h^{-1}g'sh.$$

Therefore $[g]_{(\psi,H)} = [gs]_H \subset [gs]_G$. The proof will be complete if we can show that $\#C_G(gs) = n\#C_H(gs)$, since Lemma C.0.1 then implies that $\#[gs]_H = \#[gs]_G$. The element $h \in C_H(gs)$ if and only if $(gs)h \in C_G(gs)$. Since gs generates G/H we have $\#C_G(gs) = n\#C_H(gs)$. □

Proposition C.0.3. *Suppose $-I \in H$, that $H \leq G \leq SL_2(K)$ and that $\psi_1, \psi_2 \in Aut(G)$ satisfy $\psi_i(-I) = -I$. Denote projective versions of objects by tilde and suppose that $\widetilde{\psi_1} = \widetilde{\psi_2} \in Aut(\widetilde{G})$. Then either $\psi_1 = \psi_2$ or there is a subgroup $G' \leq G$ such that*

$$[G : G'] = [\widetilde{G} : \widetilde{G}'] = 2 \quad \text{and } \psi_1 = \epsilon\psi_2,$$

where ϵ is the unique non-trivial character $G/G' \to \{\pm 1\}$.

Proof. Consider the map

$$\rho : G \to \pm 1, \quad g \mapsto \psi_1(g)\psi_2(g)^{-1}.$$

This is a group character. Let $G' := \ker(\rho)$. The two cases correspond to whether ρ is trivial or not. Since $\psi_i(-I) = -I$, the mapping ρ takes the same value on $\pm g$. Therefore $[G : G'] = 2$ implies that $[\widetilde{G} : \widetilde{G}'] = 2$. □

Lemma C.0.4. *Suppose $-I \in H$, that $H \leq G \leq SL_2(K)$ and that $\psi \in Aut(G)$ satisfies $\psi(-I) = -I$. Then the following holds.*

- *For any $g \in G$, $\#C_{(\psi,H)}(g)$ is even.*
- *$C_{(\psi,H)}(1) = \{h \in H \mid h = \psi(h)\}$.*
- *Suppose that H has unique H-conjugacy class of trace 0 and that ψ restricts to an automorphism of H. Then there is a $g \in H$ such that $[-g]_{(\psi,H)} = [g]_{(\psi,H)}$.*

Proof. For the first claim, note that if $h \in C_G(g)$ then so is $-h$. The second is clear. For the third, take any h in the unique H-conjugacy class of trace 0. Then $-\psi(h)$ also has trace 0, so $-\psi(h)$ is H-conjugate to h. This means that there is a $g \in H$ with $h = -g\psi(h)g^{-1}$. The result follows. □

Lemma C.0.5. *Suppose G is a subgroup of $SL_2(K)$, that $-I \in H$ and that $\psi \in Aut(G)$ satisfies $\psi(-I) = -I$. Denote projective versions of objects by tilde. Fix $g \in G$. Then exactly one of the following two situations holds.*

	Situation 1	*Situation* 2
$\exists h \in H$ *such that* $-g = h^{-1}g\psi(h)$*?*	*YES*	*NO*
$[g]_{(\psi,H)} = [-g]_{(\psi,H)}$*?*	*YES*	*NO*
$\#C_{(\psi,H)}(g)$ *equals ...*	$\#C_{(\psi,\widetilde{H})}(g)$	$2\#C_{(\psi,\widetilde{H})}(g)$

Proof. An element h such that $-g = h^{-1}g\psi(h)$ is exactly the witness needed to show that $[g]_{\psi,H} = [-g]_{\psi,H}$. Since $\#H = 2\#\widetilde{H}$, Lemma C.0.1 implies that

$$\#C_{\psi,H}(g) = 2\frac{\#[g]_{\psi,\widetilde{H}}}{\#[g]_{\psi,H}}\#C_{\psi,\widetilde{H}}(g).$$

Since

$$\#[g]_{\psi,H} = \begin{cases} 2\#[g]_{\psi,\widetilde{H}} & \text{if } [g]_{\psi,H} = [-g]_{\psi,H}, \\ \#[g]_{\psi,\widetilde{H}} & \text{otherwise,} \end{cases}$$

the result follows. □

Proposition C.0.6. *Suppose H is a group and $\psi_i \in Aut(H)$ for $i = 1, 2$. If there is an $s \in H$ so that $\psi_1 = s^{-1}\psi_2 s$, then*

$$H \to H, \quad g \mapsto gs^{-1}$$

is a bijection that maps (ψ_1, H)-conjugacy classes to (ψ_2, H)-conjugacy classes.

Proof. Suppose $x, y, h \in H$. Then

$$\begin{aligned} x = h^{-1}y\psi_1(h) &\Leftrightarrow x = h^{-1}ys^{-1}\psi_2(h)s \\ &\Leftrightarrow xs^{-1} = h^{-1}ys^{-1}\psi_2(h). \end{aligned}$$

□

Appendix D

Parameterizing $X^2 + Y^3 = \pm Z^r$

This appendix gives complete parameterizations to $\mathcal{D}(r, \pm 1)(\mathbb{Z})$ whose $\mathbb{Z}$-specializations include all co-prime $(X, Y, Z) \in \mathcal{D}(r, \pm 1)(\mathbb{Z})$.

To keep the lists as short as possible, we identify the parameterizations by identifying $\pm X$. If the corresponding $\mathrm{GL}_2(\mathbb{Z})$ class of f breaks into two $\mathrm{SL}_2(\mathbb{Z})$ classes these are really 2 distinct parameterizations.

The case $r = 3$ was already done by Mordell in [18], Chapter 25 using a syzygy from invariant theory. The cases $r = 4$ were done by Zagier and quoted in [1], appendix A. The $r = 5$ case is new.

D.1 Complete Parameterization of $X^2 + Y^3 = -Z^3$

Using the algorithm, we get a complete list of parameterizations:

	f	$RepresentativePoint$
$A1$	$[0, 1, 0, 0, -4]$	$\sqrt{2}i$
$A2$	$[-1, 0, 0, 2, 0]$	$\sqrt{2}i$
$B1$	$[-2, -1, 0, -1, -2]$	$-0.268 + 0.963i$
$B2$	$[-1, 1, 1, 1, -1]$	$-0.268 + 0.963i$
$C1$	$[-1, 0, -1, 0, 3]$	$\sqrt[4]{3}i$
$C2$	$[1, 0, -1, 0, -3]$	$\sqrt[4]{3}i$

In Mordell's book [18] he further shortens the list by assuming that Z is odd. This means that $A1, B1$ can be omitted. However, Mordell gives 5 parameterizations: $A2, B2, C1, C2$ and $f = [-1, -2, -4, -6, 0]$ According to my theory the 5th should be superfluous. It is. I calculate its representative point to be $-2 + \sqrt{2}i$. This means that $f(x - 2y, y)$ must be $A1$ or $A2$. It is $A2$!

Beukers [1], on page 78 omits parameterizations obtained by interchanging Y and Z. For $f \in \mathcal{C}(3, 1)$ we have $H^2(f) = f$, so that interchanging

$Y \leftrightarrow Z$ is the same as swapping between $f \leftrightarrow \boldsymbol{H}(f)$. The naming has been chosen so that $A2 = \boldsymbol{H}(A1)$ etc. Therefore a full set of parameterizations in this sense is given by $A1, B1, C1$—the same number as given in that paper.

D.2 Complete Parameterization of $X^2 + Y^3 = \pm Z^4$

These two equations were solved by Zagier and quoted in Beukers. To keep the lists short we identify $\pm X$ and $\pm Z$. This means every parameterization in the list is shorthand for $\pm f(x, \pm y)$. The first $\pm$ is the $\pm Z$.

$X^2 + Y^3 = -Z^4$.

Applying the algorithm gives 4 parameterizations:

	f	Representative Point
f_1	$[0, 1, 0, 0, 0, -12, 0]$	$1.86i$
f_2	$[0, 3, 0, 0, 0, -4, 0]$	$1.07i$
f_3	$[-1, 0, 1, 0, 3, 0, -27]$	$\sqrt{3}i$
f_4	$[-3, -4, -1, 0, 1, 4, 3]$	$-0.268 + 0.964i$

In Beukers, we also have 4 parameterizations: f_1, f_2, f_3 and a 4th one involving denominators.

$X^2 + Y^3 = Z^4$.

Applying the algorithm gives 7 parameterizations:

	f	Representative Point
f_1	$[0, 1, 0, 0, 0, 12, 0]$	$1.86i$
f_2	$[0, 3, 0, 0, 0, 4, 0]$	$1.07i$
f_3	$[-1, 0, 0, 2, 0, 0, 32]$	$1.78i$
f_4	$[-1, 0, -1, 0, 3, 0, 27]$	$\sqrt{3}i$
f_5	$[-1, 1, 1, 1, -1, 5, 17]$	$-0.158 + 1.50i$
f_6	$[-5, -1, 1, 3, 3, 3, 9]$	$-0.436 + 1.01i$
f_7	$[-7, -1, 2, 4, 4, 4, 8]$	ω

Zagier gives 6 parameterizations: $f_1, \ldots, f_6$. This means that the list there is incomplete in our sense, since the minimality property proven in section 11.6 shows that f_7 cannot be dropped.

A possible explanation was given to me by Nils Bruin. He noticed that

$$f_7(x, y) = \frac{1}{6^3} f_4(3x, x + 2y).$$

If $\chi(f_7)(s_1, s_2) = (X, Y, Z)$ then

$$\chi(f_4)(3s_1, s_1 + 2s_2) = (6^6 X, 6^4 Y, 6^3 Z).$$

In the language of Beukers [1], page 63: every f_7 specialization is equivalent to an f_4 specialization. If Zagier was identifying equivalent integer solutions he was justified in omitting the 7th parameterization!

D.3 Complete Parameterization of $X^2 + Y^3 = -Z^5$

The $\{2, 3, 5\}$ case is new. Beukers was able to produce parameterizations, though his method was unable to produce a complete set. If we identify $\pm X$, the algorithm produces the following complete set:

$$
\begin{aligned}
f_1 &= [0, 1, 0, 0, 0, 0, -144/7, 0, 0, 0, 0, -20736, 0],\\
f_2 &= [-1, 0, 0, -2, 0, 0, 80/7, 0, 0, 640, 0, 0, -102400],\\
f_3 &= [-1, 0, -1, 0, 3, 0, 45/7, 0, 135, 0, -2025, 0, -91125],\\
f_4 &= [1, 0, -1, 0, -3, 0, 45/7, 0, -135, 0, -2025, 0, 91125],\\
f_5 &= [-1, 1, 1, 1, -1, 5, -25/7, -35, -65, -215, 1025, -7975, -57025],\\
f_6 &= [3, 1, -2, 0, -4, -4, 24/7, 16, -80, -48, -928, -2176, 27072],\\
f_7 &= [-10, 1, 4, 7, 2, 5, 80/7, -5, -50, -215, -100, -625, -10150],\\
f_8 &= [-19, -5, -8, -2, 8, 8, 80/7, 16, 64, 64, -256, -640, -5632],\\
f_9 &= [-7, -22, -13, -6, -3, -6, -207/7, -54, -63, -54, 27, 1242, 4293],\\
f_{10} &= [-25, 0, 0, -10, 0, 0, 80/7, 0, 0, 128, 0, 0, -4096],\\
f_{11} &= [6, -31, -32, -24, -16, -8, -144/7, -64, -128, -192, -256, 256, 3072],\\
f_{12} &= [-64, -32, -32, -32, -16, 8, 248/7, 64, 124, 262, 374, 122, -2353],\\
f_{13} &= [-64, -64, -32, -16, -16, -32, -424/7, -76, -68, -28, 134, 859, 2207],\\
f_{14} &= [-25, -50, -25, -10, -5, -10, -235/7, -50, -49, -34, 31, 614, 1763],\\
f_{15} &= [55, 29, -7, -3, -9, -15, -81/7, 9, -9, -27, -135, -459, 567],\\
f_{16} &= [-81, -27, -27, -27, -9, 9, 171/7, 33, 63, 141, 149, -67, -1657],\\
f_{17} &= [-125, 0, -25, 0, 15, 0, 45/7, 0, 27, 0, -81, 0, -729],\\
f_{18} &= [125, 0, -25, 0, -15, 0, 45/7, 0, -27, 0, -81, 0, 729],\\
f_{19} &= [-162, -27, 0, 27, 18, 9, 108/7, 15, 6, -51, -88, -93, -710],\\
f_{20} &= [0, 81, 0, 0, 0, 0, -144/7, 0, 0, 0, 0, -256, 0],\\
f_{21} &= [-185, -12, 31, 44, 27, 20, 157/7, 12, -17, -76, -105, -148, -701],\\
f_{22} &= [100, 125, 50, 15, 0, -15, -270/7, -45, -36, -27, -54, -297, -648],\\
f_{23} &= [192, 32, -32, 0, -16, -8, 24/7, 8, -20, -6, -58, -68, 423],\\
f_{24} &= [-395, -153, -92, -26, 24, 40, 304/7, 48, 64, 64, 0, -128, -512],\\
f_{25} &= [-537, -205, -133, -123, -89, -41, 45/7, 41, 71, 123, 187, 205, -57],\\
f_{26} &= [359, 141, -1, -21, -33, -39, -207/7, -9, -9, -27, -81, -189, -81],\\
f_{27} &= [295, -17, -55, -25, -25, -5, 31/7, -5, -25, -25, -55, -17, 295].
\end{aligned}
$$

Just in case anyone was wondering, the associated representative points $z(f)$ are:

	$z(f)$		$z(f)$		$z(f)$
f_1	$2.701i$	f_2	$2.615i$	f_3	$2.590i$
f_4	$2.590i$	f_5	$-0.06962 + 2.463i$	f_6	$-0.03610 + 2.141i$
f_7	$-0.2189 + 1.752i$	f_8	$-0.2272 + 1.586i$	f_9	$-0.3756 + 1.483i$
f_{10}	$1.529i$	f_{11}	$-0.4664 + 1.334i$	f_{12}	$-0.5000 + 1.295i$
f_{13}	$-0.4652 + 1.231i$	f_{14}	$-0.3451 + 1.266i$	f_{15}	$-0.1409 + 1.291i$
f_{16}	$-0.3560 + 1.245i$	f_{17}	$1.158i$	f_{18}	$1.158i$
f_{19}	$-0.1915 + 1.119i$	f_{20}	$1.121i$	f_{21}	$-0.2856 + 1.073i$
f_{22}	$-0.3119 + 1.061i$	f_{23}	$-0.01805 + 1.070i$	f_{24}	$-0.3479 + 0.9612i$
f_{25}	$-0.4131 + 0.9106i$	f_{26}	$-0.2619 + 0.9650i$	f_{27}	$-0.1459 + 0.9893i$

The $\mathrm{GL}_2(\mathbb{Z})$ classes of the 27 forms split into 2 distinct $\mathrm{SL}_2(\mathbb{Z})$ classes, unless $f = f_3, f_4, f_{17}, f_{18}, f_{27}$. This means that the above list becomes 49 parameterizations if we do not identify $\pm X$.

Bibliography

[1] Frits Beukers, *The diophantine equation* $ax^p + by^q = cz^r$, Duke Math. J. **91** (1998), 68–88.

[2] Béla Bollobás, *Linear analysis*, Cambridge University Press, 1990.

[3] N. Bourbaki, *Algèbre*, Masson, Paris, France, 1981 (french), English Translation: Springer Verlag, 1990.

[4] Henri Darmon and Andrew Granville, *On the equations* $z^m = f(x, y)$ *and* $ax^p + by^q = cz^r$, Bull. London Math. Soc. **27** (1995), 513–543.

[5] Johnny Edwards, *A complete solution to* $x^2 + y^3 + z^5 = 0$, J. reine angew. Math. **571** (2004), 213–236.

[6] David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, 1995.

[7] Robert Fricke, *Lehrbuch der Algebra II*, Braunschweig, 1926.

[8] Paul Gordan, *Paul Gordan's Vorlesungen über Invariantentheorie*, Teubner, Leipzig, 1887.

[9] J.H. Grace and A. Young, *The algebra of invariants*, Chelsea, New York, 1965 (first published in 1903).

[10] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, 1977.

[11] Charles Hermite, *Sur l'introduction des variables continues dans la théorie des nombres*, J. reine aangew. Math. **41** (1850), Also in Œuvres de Charles Hermite, publiés par Émile Picard, Tome I, Gauthiers-Villars, Paris(1905), 164–192, Sections V and VI.

[12] David Hilbert, *Theory of algebraic invariants*, Cambridge University Press, 1993 (translation of lecture notes from 1897).

[13] Gaston Julia, *Étude sur les formes binaires non quadratiques*, Mém. Acad. Sci. Inst. France, vol. 55, Acad. Sci. l'Inst. France, 1917, Also in Julia's Œuvres, vol. 5.

[14] Felix Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, Dover publications, New York, 1956 (translation of original 1884 edition).

[15] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **75** (1956), 555–563.

[16] ———, *Algebra*, third ed., Addison-Wesley, Reading MA, 1995.

[17] Daniel Maudlin, *A generalization of Fermat's last theorem: The Beal conjecture and prize problem*, Notices of the AMS **44** (1997), no. 11, 1436–1437.

[18] Louis Mordell, *Diophantine equations*, Academic Press, London, 1969.

[19] David Mumford, *The red book of varieties and schemes*, Lecture Notes in Math, Springer-Verlag, 1999.

[20] Jean-Pierre Serre, *Corps locaux*, Publications de l'institut de mathématique de l'université de Nancago VIII, Hermann, Paris, 1962.

[21] ———, *Topics in Galois theory*, Research Notes in Maths, vol. 1, Jones and Bartlett, Boston, 1992.

[22] ———, *Galois cohomology*, Springer Monographs in Mathematics, Springer Verlag, 1996.

[23] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[24] Michael Stoll and John Cremona, *On the reduction theory of binary forms*, J. reine angew. Math. **565** (2003), 79–99.

[25] Steve Thiboutot, *Courbes elliptiques, représentations galoisiennes, et l'équation* $x^2 + y^3 = z^5$, Master's thesis, McGill Univ., Montreal, 1996.

Index

Samenvatting

In dit proefschrift worden de eigenschappen onderzocht van de diophantische vergelijking $X^2 + Y^3 = dZ^r$. Hier is d een gegeven geheel getal, r is 3,4 of 5 en X, Y, Z zijn de onbekende gehele getallen waarvan de grootste gemeenschappelijke deler 1 moet zijn.

Deze vergelijkingen hebben veel gemeen met de welbekende vergelijking van Pythagoras $X^2 + Y^2 = Z^2$ (reeds in 1600 v.Chr. door de Babyloniërs bestudeerd).

Er zijn oneindig veel oplossingen voor de vergelijking van Pythagoras. Twee daarvan, $(3, 4, 5)$ en $(5, 12, 13)$ zijn voor velen nog bekend uit de middelbare schooltijd. Een oneindige verzameling oplossingen kan verkregen worden door waarden van (s, t) in te vullen in $X = s^2 - t^2$, $Y = 2st$, $Z = s^2 + t^2$. Door eventuele verwisseling van X,Y en $-Z$ in plaats van Z te nemen, krijgt men zelfs de volledige oplossingsverzameling.

Soortgelijke verschijnselen vinden plaats bij $X^2 + Y^3 = dZ^r$. Er zijn oneindig veel oplossingen en ze kunnen allemaal verkregen worden door waarden van (s, t) in een eindig stel formules voor X, Y, Z in te vullen. In dit proefschrift geven we hier een beschrijving van en een methode om de formules te vinden.

De methoden en resultaten in dit proefschrift vormen een belangrijke bijdrage tot de theorie van de diophantische vergelijkingen. De gebruikte methode vindt zijn oorsprong in de invariantentheorie, een belangrijke tak van de wiskunde uit de 19e eeuw. De titel van dit proefschrift wordt verklaard door het feit dat de 60 symmetrieën van het regelmatig 20-vlak (icosaeder) een sleutelrol spelen in de oplossing van de vergelijking $X^2 + Y^3 = dZ^5$.

Acknowledgements

First of all I would like to express my gratitude to Frits Beukers for agreeing to be my Ph.D. supervisor. I am much indebted to him for introducing me to the topic of spherical diophantine equations, as well as his continued help and encouragement while I was writing this thesis. Most of the work described in this manuscript stemmed from his idea to try to generalize Mordell's method for the $\{2, 3, 3\}$-equation.

The reading committee is thanked for the time and expertise they have invested in reading the manuscript. These are the professors Henri Cohen, Hendrik Lenstra jr., Frans Oort, and Michael Stoll.

I am also grateful to Utrecht University and the people at the Mathematics Institute for providing me with a conducive environment in which to study and conduct research. I have enjoyed being part of a very active mathematical community.

I was particularly lucky to be able to consult with Tonny Springer—an expert in (among other things) Invariant Theory. This theory plays a prominent role in this thesis. His input in a number of aspects of this thesis is much appreciated.

Credits to the various people I have shared a room with over the years. Having a break and a chat is not only good against RSI—it makes the day much more pleasant.

I thank friends and family for being friends and family. Finally I would like to thank my partner Marjon Pluimers for her love and support through all the years.

Curriculum Vitae

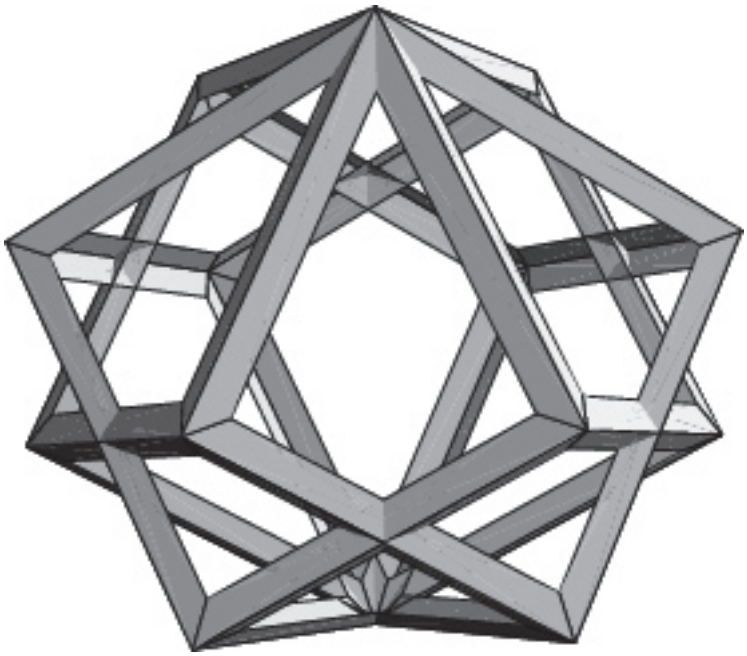
Johnny Edwards was born in Urmston near Manchester, England on the 16th of May 1961. After 8 years in the next avenue up from 60's Brit-Pop band "Herman's Hermits" (No Milk Today) the family moved to Holywood, Northern Ireland in 1969. Johnny attended Sullivan Upper School from 1972 to 1979.

Johnny was a reserve on the British Maths Olympiad Team of 1979. Later that year he moved to England to Trinity College Cambridge to study mathematics. He was made a senior scholar at Trinity after winning 2 tripos prizes. Johnny received an honors B.A. in mathematics in 1982.

Johnny left the maths world in 1983 to begin a career in computing. His work has included projects in air traffic control, industry, telecommunications and banking. This brought him to the Netherlands. In 1994 he got the opportunity to continue his career part-time. Since then he has worked in the ICT sector 3 days a week, spending the other 2 days studying mathematics.

From 1994 to 1997, Johnny followed maths doctoral courses and master class courses at Utrecht University. In 1997 he obtained his Netherlands *doctoral diploma*, cum laude, with an average mark of 9.2. His final year master's thesis entitled *Logic and Computational Complexity* was written under the guidance of Ieke Moerdijk.

The years 1998 to 2004 have seen Johnny studying number theory as a Ph.D. student under Frits Beukers at Utrecht. His main topic of interest has been diophantine equations. Johnny has attended seminars and given lectures on the subject. The present manuscript describes a theory of *spherical* Fermat equations that he has developed and includes his results on diophantine equations of the form $X^2 + Y^3 = dZ^r$.



Intersecting cubes from Escher's "Stars"
— a wood engraving from 1948.