Declaration

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Preface and specified in the text. It is not substantially the same as any that I have submitted, or, is being concurrently submitted for a degree or diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text. I further state that no substantial part of my dissertation has already been submitted, or, is being concurrently submitted for any such degree, diploma or other qualification at the University of Cambridge.
Acknowledgements

I am deeply indebted to my mentor Tom Fisher for his guidance, patience, encouragement, and sharing of ideas. I am also grateful to Trinity College for their financial support during the past eight years.

I would also like to thank my friend Stevan Gajovic and my office mates Jiali Yan and Yanning Xu for many mathematical and non-mathematical conversations. Finally, I would like to thank my parents and my brothers for their continuous support and love.
Capitulation Discriminants of Genus One Curves

Lazar Radicevic

Summary

In this thesis we study genus one curves of degree \( n \) embedded in projective space \( \mathbb{P}^{n-1} \). We are specifically interested in the curves defined over \( \mathbb{Q} \) that are counterexamples to the Hasse principle, that is the curves that have points everywhere locally but no \( \mathbb{Q} \)-points. These curves correspond to non-trivial elements of the Tate-Shafarevich group of the Jacobian curve \( E \) of \( C \). Such a curve \( C \) will always admit a point over a degree \( n \) field extension \( F \) of \( \mathbb{Q} \), and we say \( C \) capitulates over \( F \), and that the discriminant of \( F \) is a capitulation discriminant for \( C \). Our aim will be to obtain a bound for the capitulation discriminant in terms of the invariants of the minimal model of the elliptic curve \( E \).

To do so, we study the minimal free resolution of the ideal defining curve \( C \), and extend the classical theory of genus one models of degree \( n \), where \( n = 1, 2, 3, 4 \) or \( 5 \), to all odd values of \( n \). In particular we prove a formula giving a equation for the Jacobian curve \( E \) in terms of the invariants of a genus model associated to \( C \), and we prove a minimization result, stating that if \( C \) is everywhere locally soluble, then it can be defined by an integral genus one model with invariants as small as possible.

In parallel, we obtain a formula for the discriminant of a rank \( n \) ring, realized as a ring of functions of \( n \) points in the projective space \( \mathbb{P}^{n-2} \), for all \( n \). Our methods extend the classical results that give parametrizations of rank \( n \) rings for \( n \leq 5 \). We then study rings obtained by intersecting the curve \( C \) with a hyperplane, and use geometry of numbers together with a compactness argument to prove a bound for the capitulation discriminant. For small values of \( n \) we then explain how to make this bound effective.

In the second part of the thesis we study Kolyvagin classes in the \( p \)-Selmer group of an elliptic curve \( E \), for \( p \) an odd prime. Our aim will be to obtain explicit geometric representation of these classes, which frequently correspond to non-trivial elements of the Tate-Shafarevich group of \( E \), as degree \( p \) curves embedded in the projective space \( \mathbb{P}^{p-1} \). These classes are defined using Heegner points, which are points of \( E \) defined over a degree \( 2p \) dihedral extension \( L \) of \( \mathbb{Q} \). We explain how to compute Heegner points explicitly, and then give a method, based on Galois descent, to obtain a geometric representation of the Kolyvagin class as an element of \( H^1(\mathbb{Q}, E[p]) \), from its definition in terms of the Heegner point as an element of \( H^1(L, E[p]) \).
We remark that our method will naturally result in nice integral models for these curves, i.e. minimal in the sense of the first part of the thesis. At the end we give examples, including an example of a genus one curve in $\mathbb{P}^6$ that represents a non-trivial element of the 7-torsion part of the Tate-Shafarevich group of the Jacobian $E$. 
Contents

1 Introduction

2 Preliminaries
   2.1 Torsors, n-diagrams and Galois cohomology
   2.2 Free resolutions and the Gorenstein condition
      2.2.1 Basic properties
      2.2.2 Algebra structures on resolutions

3 Resolutions, curves and algebras
   3.1 Resolution models
   3.2 Ω-quadrics and the invariant theory of resolution models
   3.3 Ω-matrices and genus one normal curves
   3.4 Ω-quadrics and changes of coordinates
      3.4.1 The proof of Proposition 3.2.3
      3.4.2 The invariant differential under changes of coordinates
   3.5 Ω-quadrics and structure constants of algebras
   3.6 Proof of Lemma 3.5.8
   3.7 The discriminant form
   3.8 A refinement of the construction of structure constants

4 The unprojection construction
   4.1 Overview
   4.2 Motivation - plane cubics
   4.3 The mapping cone construction
   4.4 Construction of the unprojection data
   4.5 Unprojection and sets of n points in \( \mathbb{P}^{n-2} \)
   4.6 Unprojection of genus one normal curves of degree n
   4.7 The local minimization theorem
   4.8 Proof of the global minimization theorem

5 Analytic theory of elliptic normal curves
   5.1 Heisenberg invariant diagrams
   5.2 Analytic description of the Ω-matrix
   5.3 Analytic theory over the real numbers
6 Bounding the capitulation discriminant 103
  6.1 Proof of the main theorem 103
  6.2 Bounding monomial sums 106
  6.3 Bounding the coefficients 108
  6.4 Examples 112

7 Kolyvagin classes 117
  7.1 Introduction 117
  7.2 Background on Heegner points and Kolyvagin classes 118
  7.3 Geometric realization of the Kolyvagin class 122
    7.3.1 The \( n \)-diagram associated to the Kolyvagin class 122
    7.3.2 Computing the matrices \( M_g \) 124
  7.4 Minimization and reduction 128
    7.4.1 Minimal genus one models 131
    7.4.2 Practical computation of a minimal model 132
    7.4.3 Reducing the model 136
  7.5 Computing the Heegner point 138
  7.6 Examples 142
Chapter 1

Introduction

Let $E$ be an elliptic curve defined over $\mathbb{Q}$. The main subject of this thesis is the study of geometric representations of the elements of the Tate-Shafarevic group $\text{III}(E/\mathbb{Q})$. More precisely, we study the problem of capitulation for these elements.

As an example, consider the following well known counterexample to the Hasse principle for genus one curves, due to Selmer. Let $C$ be a plane curve defined by the cubic

$$3x^3 + 4y^3 + 5z^3 = 0$$

The curve $C$ is smooth and of genus one, admits points over every completion of $\mathbb{Q}$, but no $\mathbb{Q}$-points. However it clearly admits a point over a small cubic extension of $\mathbb{Q}$. For example, we see that it has a point over $\mathbb{Q}(\sqrt[3]{6})$ by setting $z = 0$, $y = 1$, and solving for $x$ by extracting a cube root. The curve $C$ represents a 3-torsion element of the Tate-Shafarevic group of an elliptic curve defined over $\mathbb{Q}$, and we say this element capitulates over the extension $\mathbb{Q}(\sqrt[3]{6})$.

In general, elements of $n$-torsion parts the Tate-Shafarevic group capitulate over a degree $n$ number field. In this thesis we prove that, under mild assumptions, this number field can be chosen to be "small" in a suitable sense.

Recall that, as a set, $\text{III}(E/\mathbb{Q})$ is defined to be the set of (isomorphism classes of) locally trivial torsors under $E$. An important method for computing the Mordell-Weil group $E(\mathbb{Q})$ is given by the theory of $n$-descent, for $n \geq 2$ an integer. An $n$-descent on $E$ will compute the $n$-Selmer group $\text{Sel}^{(n)}(E/\mathbb{Q})$ of $E$. We can obtain information about the Mordell-Weil group $E(\mathbb{Q})$, and the Tate-Shafarevic group $\text{III}(E/\mathbb{Q})$, from the following short exact sequence:

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \text{Sel}^{(n)}(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[n] \to 0$$

There is a geometric interpretation of the $n$-Selmer group, due to Cassels [Cas62], as the set of isomorphism classes of everywhere locally soluble $n$-diagrams. An $n$-diagram $[C \to \mathbb{P}^{n-1}]$ is an morphism of a torsor $C$ under $E$ into $\mathbb{P}^{n-1}$, induced by a complete linear system of dimension $n$. When $n \geq 3$, this morphism is a closed embedding, and if $n = 2$, it is a double cover of $\mathbb{P}^1$. It is said to be everywhere locally soluble if the torsor $C$ is everywhere locally trivial, i.e. the curve $C$ admits a point over every completion of $\mathbb{Q}$.

Hence a class $c$ in $\text{III}(E/\mathbb{Q})[n]$ can be represented by a genus one curve $C$ embedded in $\mathbb{P}^{n-1}$. 

1
The class \( c \) is non-trivial if and only if \( C(\mathbb{Q}) = \emptyset \). In other words, non-zero elements of \( \text{III}(E/\mathbb{Q}) \) correspond to counter-examples to the Hasse principle.

A basic observation is that \( C \) is a curve of degree \( n \), and hence that the intersection of \( C \) and a generic hyperplane in \( \mathbb{P}^{n-1} \) is a set of \( n \) points in general position. Thus the curve \( C \), even if it does not have a \( \mathbb{Q} \)-point, has a \( K \)-point for some degree \( n \) field extension \( K \) of \( \mathbb{Q} \). When this happens, we say that the class \( C \) capitulates over \( K \). To measure the arithmetic complexity of the class \( c \), we define the capitulation discriminant of \( c \) to be the smallest absolute value of the discriminant of a number field over which \( c \) capitulates.

Our aim is to give a bound on the capitulation discriminant in terms of the invariants of \( E \). Let \( c_4(E) \) and \( c_6(E) \) be the invariants of a minimal Weierstrass equation of \( E \), and define the naive height of \( E \) to be \( H_E = \max(|c_4(E)|^{1/4}, |c_6(E)|^{1/6}) \). We prove the following.

**Theorem 1.0.1.** Let \( n \geq 3 \) be an odd integer, and let \([C \to \mathbb{P}^{n-1}]\) be an everywhere locally soluble \( n \)-diagram representing an element of the \( n \)-Selmer group of the elliptic curve \( E \). There exists a constant \( c(n) \), depending only on the integer \( n \), and an order \( O \) in an \( n \)-dimensional commutative \( \mathbb{Q} \)-algebra \( K \), such that the set of \( K \)-points \( C(K) \) is non-empty, and we have \(|\text{disc}(O)| < c(n)H_E^{2n-2} \).

The index of a smooth curve \( C \), defined over a perfect field \( k \), is the smallest degree a positive \( k \)-rational divisor \( D \) on \( C \) can take. Note that we do not require that the points of \( D \) are rational, only the divisor \( D \) itself. The next theorem is a corollary of the previous one.

**Theorem 1.0.2.** Let \( n \geq 3 \) be an odd integer, and let \( C \) be a torsor under \( E \) that represents an element of \( \text{III}(E/\mathbb{Q})[n] \). Suppose that the index of \( C \) is equal to \( n \). There exists a constant \( c(n) \), depending only on \( n \), and a degree \( n \) number field \( K \) of discriminant at most \( c(n)H_E^{2n-2} \), such that \( C \) admits a \( K \)-rational point.

In other words, the capitulation discriminant of \( C \) is bounded above by \( c(n)H_E^{2n-2} \). The condition on the index of \( C \) is needed to ensure that the algebra \( K \) of Theorem 1.0.1 is in fact a field. This is a mild restriction. For example, it is satisfied when \( n \) is prime and the class \( c \in \text{III}(E/\mathbb{Q}) \) is non-zero - this follows from the well known fact the period and the index of an element of \( \text{III}(E/\mathbb{Q})[p] \) are equal. We expect that the theorem is true for \( n \) even as well, but the proof will require more work. However, the assumption that \( C \) corresponds to an element of \( \text{III}(E/\mathbb{Q}) \), i.e. admits a point over every completion of \( \mathbb{Q} \), is essential, and we do not expect the theorem to hold if it is removed.

We furthermore compute explicit values for the constant \( c(n) \) for \( n = 3 \) and \( n = 5 \). There is interest in trying to compute sharp values for the constants \( c(n) \). For example, they can be used to obtain results on concrete Diophantine equations. We will find that we can take \( c(3) = 0.63548 \) and \( c(5) = 1.94641 \). For the elliptic curve labeled 11a3 in Cremona’s tables, the bounds of Theorem 1.0.2 evaluate to 18.094 in the case \( n = 3 \), and 1578.583 in the case \( n = 5 \). But the smallest value the absolute discriminant of a cubic field can take is 23, and the discriminant of a quintic field is at least 1609, as one can find by consulting the LMFDB database. We can thus conclude, without the need to do a 3-descent and a 5-descent on \( E \), that the groups \( \text{III}(E/\mathbb{Q})[3] \) and \( \text{III}(E/\mathbb{Q})[5] \) are trivial. There are a few more curves for which one can prove results like this - though it should be noted that for any given \( n \), there are only
finitely many curves for which this method can prove vanishing of $\text{III}(E/\mathbb{Q})[n]$. Geometry of numbers methods for proving the vanishing of $\text{III}(E/\mathbb{Q})[3]$, similar in spirit to this one, were studied before in [Fis12].

**Remark 1.0.3.** We have chosen the word capitulation to highlight an analogy with the classical problem of capitulation of ideal classes in class groups of number field. Suppose $K$ is a number field. We say an ideal class $[a] \in \text{Cl}(K)$ capitulates in a field extension $L/K$, if the ideal $a$ becomes principal in $L$. An elementary argument shows that if $[a] \in \text{Cl}(K)[n]$, then there exists a degree $n$ number field $L$ in which $[a]$ capitulates.

There is a strong analogy between Tate-Shafarevich groups of elliptic curves and class groups of number fields. A nice exposition can be found in Section 1 of [SW10]. If we view an element of $\text{III}(E/\mathbb{Q})$ as a cohomology class $c$ in $H^1(\mathbb{Q}, E)$, we see that $c$ capitulates in $L$, if and only if it is in the kernel of the restriction map $H^1(\mathbb{Q}, E) \to H^1(L, E)$. There is a similar interpretation of the class group $\text{Cl}(K)$ as a subgroup of the Galois cohomology group $H^1(K, U)$, where $U$ is the group of units in $\mathcal{O}_{\overline{Q}}$, and $\mathcal{O}_{\overline{Q}}$ is the integral closure of $\mathbb{Z}$ in an algebraic closure $\overline{Q}$. An ideal class $c \in \text{Cl}(K)$ capitulates in $L$, if and only if it is in the kernel of the restriction map $H^1(K, U) \to H^1(L, U)$.

**Genus one models.** For small values of $n$, it is well known how to represent $n$-diagrams $[C \to \mathbb{P}^{n-1}]$ by the equations that define them. One defines a genus one model of degree $n$ to be a

(i) if $n = 2$, an equation of the form $y^2 = f(x_1, x_2)$, where $f$ is a binary quartic.

(ii) if $n = 3$, a ternary cubic $F(x_1, x_2, x_3)$,

(iii) if $n = 4$, a pair of quadrics $P$ and $Q$, in the four variables $x_1, x_2, x_3$ and $x_4$.

For example, a 3-diagram $[C \to \mathbb{P}^2]$ is a closed embedding, and the image $C$ is a plane curve of degree 3, and so can be defined by a ternary cubic $F(x, y, z)$. Conversely, a generic cubic $F$ defines a plane degree 3 curve $C$. If $C$ is non-singular, it will be a smooth curve of genus one, and will admit a structure of a torsor under its Jacobian curve $E \cong \text{Pic}^0(C)$. We say that the cubic $F$ is a model of the 3-diagram $[C \subset \mathbb{P}^2]$.

There is a similar notion of a model of an $n$-diagram for $n = 2, 4$ and 5, and genus one models have been studied extensively in the context of descent theory. A model of an $n$-diagram is not unique - for example, by considering the action of $GL_3(\mathbb{Q})$ on $\mathbb{P}^2$, we see that we only care about the cubic $F$ up to linear substitutions.

We can recover a Weierstrass equation for the Jacobian $E$ from the cubic $F$. There exist polynomials $c_4, c_6$ and $\Delta$ in the coefficients of the cubic $F$, invariant under the action of $\text{SL}_3(\mathbb{Q})$ by linear substitution, such that if $\Delta(F) \neq 0$,

$$y^2 = x^3 - 27c_4(F) - 54c_6(F)$$

is a Weierstrass equation defining $E$. The polynomials $c_4$ and $c_6$ are known as the invariants of $F$, and date back to the nineteenth century invariant theorists. The observation that they can
be used to write down an equation for the Jacobian is due to Weil ([Wei83],[Wei54]). There are similar results for $n = 2$ and $4$ - for a survey see Section 2 of [CFS10], and [AKM+01].

The 3-diagrams $[C \to \mathbb{P}^2]$ that correspond to the elements of the 3-Selmer group of $E$, i.e. diagrams for which the set $C(\mathbb{Q}_p)$ is non-empty for every prime $p$, can be represented by particularly nice cubics $F$, with small integral coefficients. More precisely, Theorem 1.1 of [CFS10] asserts that $[C \to \mathbb{P}^2]$ admits a minimal model - a cubic $F \in \mathbb{Z}[x_0, x_1, x_2]$, with $\Delta(F) = \Delta_E$, where $\Delta_E$ is the discriminant of a minimal Weierstrass model of $E$. This fact, known as the minimization theorem, plays an important role in, for example, algorithms for explicit $n$-descent on elliptic curves and in Bhargava and Shankar’s work on the average sizes of $n$-Selmer groups.

Formulating and proving analogues of these results that hold for all odd $n \geq 3$ is the key step for the proof of Theorem 1.0.2. When $n \geq 5$, $n$-diagrams $[C \subset \mathbb{P}^{n-1}]$ are no longer complete intersections. It turns out that the equations defining $C$ no longer suffice when $n \geq 5$ - one should instead consider the entire minimal graded free resolution of the homogeneous ideal that defines the curve in $\mathbb{P}^{n-1}$.

Suppose $C \subset \mathbb{P}^{n-1}$ is a smooth curve projectively normal curve, of degree $n$, defined over a field $k$. Consider the minimal graded free resolution of the homogeneous coordinate ring of $C$. This is a chain complex of graded $R$-modules, where $R = k[x_1, \ldots, x_n]$, of the form

$$R(-n) \xrightarrow{\phi_{n-2}} R(-n + 2)^{\phi_{n-3}} \xrightarrow{\phi_{n-3}} \ldots \xrightarrow{\phi_3} R(-3)^{\phi_2} \xrightarrow{\phi_2} R(-2)^{\phi_1} \xrightarrow{\phi_1} R,$$

where $R(k)$ is the module $R$ with the grading shifted by $k$ - i.e. the element $1 \in R(k)$ has degree $k$. From the resolution, we can recover the equations for the defining ideal $I$ of $C$, as the ideal generated by the entries of the row vector $(f_1, \ldots, f_k)$ that represents the differential $\phi_1$.

One can recover this free resolution from the definition of a genus one model for small $n$ given above - for example, if $F$ is a ternary cubic, then the corresponding resolution is

$$R(-3) \xrightarrow{F} R,$$

and if $(P, Q)$ are a pair of quadrics, then the resolution is

$$0 \to R(-4) \xrightarrow{(Q \quad -P)} R(-2)^2 \xrightarrow{(P \quad Q)} R \to 0.$$

For $n = 5$ and onwards, it is not sufficient to just use equations in the definition of a genus one model. To give an indication of why this is the case, observe that a genus one curve of degree 5 is defined by five quadrics in $\mathbb{P}^4$. These quadrics are very special - five generic quadrics do not even define a curve in $\mathbb{P}^4$. For example, when $n = 5$, a genus one model of degree 5 is a $5 \times 5$ alternating matrix of linear forms $A$, in five variables $x_0, \ldots, x_4$, that serves as the first syzygy matrix for the five quadrics that define $C$. One can recover these quadrics as the $4 \times 4$ sub-Pfaffians of $A$. The corresponding free resolution is

$$0 \to R(-5) \xrightarrow{PT} R(-3)^5 \xrightarrow{A} R(-2)^5 \xrightarrow{P} R.$$
where $P$ is the vector of signed Pfaffians of $A$.

**Rings of small rank.** The theory of parametrizations of rings of small rank is remarkably parallel to the theory of genus one models. The simplest example are quadratic fields, which are all of the form $\mathbb{Q}(\sqrt{D})$ for some integer $D$, and there is no difficulty in describing orders in quadratic fields explicitly as well.

Next, we have the Delone-Faddeev correspondence [DF], which associates to any binary cubic form a cubic ring. This correspondence defines a bijection between the $GL_3(\mathbb{Z})$-orbits of the space of binary cubic forms, and the set of isomorphism classes of cubic rings, i.e. rings that are free of rank 3 as $\mathbb{Z}$-modules.

Bhargava ([Bha04],[Bha08]) has extended these parametrizations to rings of rank 4 and 5. In particular, to a pair of quadratic forms $P_1$ and $P_2$, in variables $x_0, x_1$ and $x_2$, he associates a ring $Q$ that is free of rank 4 as a $\mathbb{Z}$-module, and to an alternating matrix of linear forms $A$, in four variables $x_0, x_1, x_2$ and $x_3$, he associates a ring $R$ that is a free $\mathbb{Z}$-module of rank 5.

The invariant theory of binary cubics, pairs of ternary quadratic forms, and quinary alternating matrices of linear forms, can be used to describe the structure constants that determine the multiplication in the associated ring, and in particular to give a formula for its discriminant. It is this aspect of the theory that we generalize to rings of arbitrary rank $n$.

The basic idea is, roughly, that when $n \geq 3$, given an $n$-dimensional non-degenerate $\mathbb{Q}$-algebra $A$, there is a natural way to associate to $A$ a set $X$ of $n$ points in $\mathbb{P}^{n-2}$, and to identify $A$ with the ring of global functions $\Gamma(X, \mathcal{O}_X)$. When $n = 3$, a set of 3 points in $\mathbb{P}^2$ is cut out by a binary cubic form. When $n = 4$, $X$ is a set of four points in $\mathbb{P}^2$, cut out by a pair of quadrics.

For $n \geq 5$, as in the case of curves, the natural object to consider is the minimal graded free resolution $F_*$ of the homogeneous ideal defining the set $X$. Our main result on rank $n$ rings is Theorem 3.5.7, a conjecture of Tom Fisher, giving explicit formulas for the structure constants and the discriminant of $A$ in terms of the resolution $F_*$. For $n$ odd, we give a further refinement of these formulas, which when specialised to $n = 3$ recovers the Delone-Faddeev correspondence, and when specialised to $n = 5$ recovers Bhargava’s construction of quintic rings.

**Strategy for the proof of Theorem 1.0.1.** Given an $n$-diagram $[C \rightarrow \mathbb{P}^{n-1}]$, intersecting $C$ with a generic hyperplane $U$ in $\mathbb{P}^{n-1}$ yields a set $X_U$ of $n$ points in $\mathbb{P}^{n-2}$. Let $A_U$ denote the algebra of global functions on $U$. If $U$ is sufficiently generic, the algebra $A_U$ will be étale, and hence can be expressed as a product of number fields $L_1 \times \ldots \times L_k$, where the degrees of the fields $L_i$ add up to $n$. The curve $C$ capitulates over each of these number fields, and if $C$ corresponds to an element of $\text{III}(E/\mathbb{Q})$ of index $n$, an easy argument shows that in fact $A = L$ is a field. In any case, the discriminant of the algebra $A_U$ is an upper bound for the discriminant of each field $L_i$.

Our results on rank $n$ rings will allow us to define a discriminant form $D(U)$, which will be the determinant of the trace pairing on $A_U$, with respect to a certain basis of $A_U$. If we write out the equation for the hyperplane $U = u_0x_0 + \ldots + u_{n-1}x_{n-1}$, then $D(U)$ will be a homogeneous polynomial of degree $2n$ in the variables $u_0, u_1, \ldots, u_{n-1}$.

The discriminant form $D$ is defined in terms of the minimal free resolution of the ideal defining $C$, i.e. the "model" of $C$. The vanishing locus of $D$ can be interpreted as the set of
hyperplanes that are tangent to some point of $C$, i.e. it can be identified with the projective dual of $C$. The key property of $D$ is that if the model of $C$ is integral in a suitable sense, then $D(U)$ will be a polynomial with integer coefficients, and if the hyperplane $U = u_0x_0 + \ldots + u_{n-1}x_{n-1}$ is integral, i.e. we have $u_i \in \mathbb{Z}$, then $D(u_0, u_1, \ldots, u_{n-1})$ will be the discriminant of an order in $A_U$.

If $[C \to \mathbb{P}^{n-1}]$ corresponds to an element of the $n$-Selmer group, we will prove in Theorem 4.1.1 that it admits a minimal model, i.e. an integral model with invariants equal to the invariants of a minimal Weierstrass equation of $E$. For this model, we seek to prove that there exists a hyperplane $U$ with integral coefficients for which the value $D(U)$ satisfies the desired bound. This is accomplished by developing a reduction theory for these discriminant forms, allowing us to bound their coefficients, together with input from the geometry of numbers provided by Minkowski's theorem.

Example 1.0.4. We have excluded even $n$ in the statement of Theorem 1.0.1 because we have not managed to fully develop the theory of genus one models of even degree so far. The theorem is true for $n = 2$ and $n = 4$, and the method of proof is similar to the proof for odd $n$. We sketch the argument for the simple case $n = 2$, since it will illustrate all of the key ingredients of the proof of Theorem 1.0.1. Fix a minimal Weierstrass equation for $E$,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$ 

The invariants $c_4, c_6$ and $\Delta$ are certain polynomials in the coefficients $a_i$, see Chapter III of [Sil09]. Let $[C \to \mathbb{P}^1]$ be a 2-diagram that represents an element of $\text{Sel}^2(E/\mathbb{Q})$, defined by a binary quartic $F$:

$$y^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

The binary quartic $F$ has invariants $c_4(F) = 2^4I$ and $c_6(F) = 2^3J$, where

$$I = 12ae - 3bd + c^2$$
$$J = 72ace - 27ad^2 - 27b^2e + 9bcd - 2e^3.$$ 

Since the curve $C$ is everywhere locally soluble, by Theorem 1.1 of [CFS10], we can assume that the quartic $F$ is minimal, i.e. it has integer coefficients, and $c_k(F) \leq 2^k c_k$. Furthermore, by Proposition 2.8 of [Fis12] and Minkowski’s theorem on lattice points, there exists a constant $M$, independent of the curve $E$, such that the coefficients of $F$ are bounded in absolute value by $MH_E^2$. Hence there exists a constant $M'$, independent of $E$, with $|F(1,0)| \leq M'H_E^2$. The curve $C$ admits a point over the field $\mathbb{Q}(\sqrt{F(1,0)})$, and the result follows.

Note that here the input from geometry of numbers is Proposition 2.8 of [Fis12], together with Minkowski's theorem. For larger values of $n$, and to obtain effective bounds, it is more convenient to use Minkowski’s theorem in a different way, as we will see in the next example.

Example 1.0.5. Let us look at the case $n = 3$, where the formulas are still reasonably simple. Let $[C \subset \mathbb{P}^2]$ be a 3-diagram, defined over a field $K$, and let $F(x, y, z) \in K[x, y, z]$ be a ternary cubic that defines $C$. The discriminant form $D$ can be computed by the following recipe. Consider a hyperplane $H$ in $\mathbb{P}^2$, defined by $ux + vy + wz = 0$ for some $u, v, w \in K$. At least one
of \(u, v, w\) is non-zero - assume it is \(w\). We then have the parametrization \(\phi : \mathbb{P}^1 \to H:\)

\[
(x : y) \mapsto (wx : wy : -ux - vy).
\]

Composing \(F\) and \(\phi\), we obtain a binary cubic form \(f(x, y) = F(wx, wy, -ux - vy)\). The three zeros of \(f\) correspond to the three points of the intersection of \(C\) and \(H\). Now recall that the discriminant of a binary cubic form

\[
a x^3 + b x^2 y + c x y^2 + d y^3,
\]

is given by

\[
b^2 c^2 - 4ac^3 - 4b^3 d - 27a^2 d^2 + 18abcd.
\]

The discriminant of the form \(f\) is a homogeneous polynomial in \(u, v\) and \(w\), of degree 12, that is divisible by \(w^6\). The discriminant form \(D\) turns out to be equal to \(\text{disc}(f)/w^6\). If \(F \in \mathbb{Z}[x, y, z]\) and the cubic \(f\) is irreducible, \(D(u, v, w)\) is the discriminant of an order in the number field defined by \(f\).

A general cubic form \(F\) depends on 10 coefficients, and the formula for the form \(D\) is fairly intimidating. However, by the means of a \(\text{SL}_3(\mathbb{R})\)-transformation, we may assume that \(F\) is in the following simple form, called the Hesse normal form:

\[
F = a(x^3 + y^3 + z^3) - 3bxyz.
\]

For such forms, the discriminant form is equal to

\[
D(u, v, w) = -27a^4(u^6 + v^6 + w^6) + 162a^2 b^2(u^4 vw + uv^4 w + uvw^4)
+ (54a^4 - 108ab^3)(u^3 v^3 + v^3 w^3 + w^3 u^3) + (-324a^3 b + 81b^4)u^2 v^2 w^2.
\]

This reduces the problem of proving that the original form \(D\) takes a small value at some point in \((u, v, w)\) for some \((u, v, w) \in \mathbb{Z}^3\), to the problem of proving that the Hesse normal form of \(D\) takes a small value at some point \((u, v, w) \in \Lambda\), where \(\Lambda\) is a lattice in \(\mathbb{R}^3\) of covolume one. This problem can now be tackled using methods from the geometry of numbers.

**Kolyvagin classes.** The final subject we treat is construction of explicit counterexamples to Hasse principle. We give a brief overview here. Let \(E/\mathbb{Q}\) be an elliptic curve of conductor \(N\), with a fixed modular parametrization \(\pi : X_0(N) \to E\). Let \(K\) be an imaginary quadratic field satisfying the Heegner hypothesis, that is, all prime factors of \(N\) split in \(K\). Let \(L\) be the Hilbert class field of \(K\). Using the theory of complex multiplication and the modular parametrization \(\pi\), one can define the points \(x_K \in E(L)\) and \(y_D = \text{Tr}_{L/K}(x_D) \in E(K)\), known as the Heegner point and the basic Heegner point.

Fix now an odd prime \(p\), and assume that the degree of \(L/K\) is \(p\). Kolyvagin ([Gro91]) has constructed certain cohomology classes from these points that serve as candidates for non-trivial elements of \(\text{III}(E/K)[p]\). Our aim is to give explicit descriptions of these classes, as \(p\)-diagrams \([C \to \mathbb{P}^{p-1}]\), and thus obtain counterexamples to the Hasse principle.
This is especially interesting if \( p > 5 \), and \( E \) does not admit a \( p \)-isogeny, since then the classical method of \( p \)-descent for computing such examples is not feasible. In particular we give the first explicit realization of a non-trivial element of \( \text{III}(E/Q)[7] \) for an elliptic curve \( E \) that does not have a 7-isogeny.

For elliptic curves for which it is feasible to carry out our calculations, Kolyvagin classes give a different perspective on bounding capitulation discriminants, as by construction they will capitulate over a degree \( p \) subfield of the Hilbert class field.

These classes have already been studied from a computational point of view by Jetchev, Leuter and Stein in [JLS09]. However they stop at their representation as elements of \( E(L)/pE(L) \), which suffices if one wants to check that a class is non-zero, whereas we will use them to give explicit counterexamples to the Hasse principle for genus one curves.

**Organization of the thesis.** In Chapter 2 we cover preliminary material, concerning standard interpretations of Galois cohomology groups \( H^1(Q,E) \) and \( H^1(Q,E[n]) \) as groups of torsors and \( n \)-diagrams. We then explain some classical results of commutative algebra, on graded free resolutions and differential algebra structures on them, that might be less familiar to number theorists.

In Chapter 3 we state our results on minimal free resolutions, notably Theorem 3.3.5 and Theorem 3.5.7. In Section 3.1 we give our definition of a resolution model of degree \( n \). A resolution model is intended to be a simultaneous generalization of the notion of a model of a genus one normal curve of degree \( n \), and the notion of a model of a rank \( n \) ring. In Section 3.2 we then introduce certain invariants of resolution models called \( \Omega \)-quadrics. For a genus one curve, these invariants take the shape of an alternating matrix of quadratic forms, called the \( \Omega \)-matrix. We then state a formula for the Jacobian of a genus one curve, Theorem 3.3.5, which is intended to generalize a well known result from the theory of genus one models of degree \( n \leq 5 \).

Afterwards, we turn to resolution models of sets of \( n \) points in projective space. For these sets, we prove Theorem 3.5.7, which essentially says that \( \Omega \)-quadrics of a set of \( n \) points can be interpreted as structure constants of an associated ring of rank \( n \). The theorem is proven in Section 3.6, using an explicit description of the minimal free resolution. In Section 3.7 we explain the connection between resolution models of curves and resolution models of a set of \( n \) points, and define the key object for our proof of Theorem 1.0.1, the discriminant form. In Section 3.8 we give a strengthening of Theorem 3.5.7 which relates our work to the constructions of Delone-Faddeev and Bhargava for \( n = 3 \) and \( n = 5 \).

The proof of Theorem 3.3.5 is divided over Chapter 4 and Chapter 5. In Chapter 4 we explain the method of unprojection, which allows us to construct free resolutions inductively, and is the key technical tool in our proofs. The main result of Chapter 4 is Theorem 4.1.1, generalizing the minimization theorem of [CFS10] to resolution models. The theorem is deduced from the local minimization result, Theorem 4.7.1, and the Jacobian formula, Theorem 3.3.5, using strong approximation. Theorem 4.7.1 is proven by an induction, using unprojection.

The method of unprojection was developed by Kustin and Miller in [KM83], and used by Fisher in [Fis06] to compute minimal free resolutions of genus one normal curves. We refine and develop this method further in Section 4.3 and Section 4.4. Two key points for the proof of
Theorem 4.1.1 is that our method works over base rings more general than fields, most notably \( \mathbb{Z} \), and that it is possible to compute \( \Omega \)-quadrics using unprojection, as seen in Lemma 4.3.10. In Section 4.5, we give a second method to compute the minimal free resolution of a set of points in general position, based on unprojection.

In Chapter 5 we recall the classical theory of embedding elliptic curves into projective space by means of theta functions. These embeddings give rise to particularly symmetric \( n \)-diagrams, invariant under the action of the standard Heisenberg group, which we hence call the Heisenberg invariant diagrams. The key point is that we are able to obtain a \( q \)-expansion for the associated \( \Omega \)-matrix. This reduces the proof of the formula for Jacobian to a calculation already done in [Fis18].

In Chapter 6 we finally prove Theorem 1.0.1. The first step is to prove an inequality for discriminant forms over \( \mathbb{R} \), Theorem 6.1.1. This is done using a compactness argument. We then use Theorem 4.1.1, together with an argument from the geometry of numbers, to prove Theorem 1.0.1. We then compute explicit values for the constants \( c(3) \) and \( c(5) \). In Section 6.2 we use \( q \)-series derived in Chapter 5 to bound the coefficients of the discriminant form, and in Section 6.2 we estimate the monomials. We combine these bounds in Section 6.4 to prove Theorem 6.4.1 and obtain explicit values for \( c(3) \) and \( c(5) \) mentioned before.

Chapter 7 is then dedicated to algorithms for constructing Kolyvagin classes. The problem naturally breaks into two parts: first we have to compute a Heegner point, and then construct a minimized and reduced model of the associated Kolyvagin class. At the end we give examples, which were obtained by computer calculations using MAGMA ([BCP97]). A more detailed introduction is given at the beginning of Chapter 7.
Chapter 2

Preliminaries

2.1 Torsors, $n$-diagrams and Galois cohomology

In this section we recall certain standard interpretations of the cohomology groups $H^1(K, E)$ and $H^1(K, E[n])$. Proofs of the assertions in this section can be found in [CFO+08]. In what follows, let $K$ be a number field, $E/K$ an elliptic curve and $n$ an integer.

**Definition 2.1.1.** A torsor under $E$ is a pair $(C, \mu)$, where $C$ is a smooth projective curve of genus one (defined over $K$), and $\mu : E \times C \to C$ is a morphism that induces a simple transitive action $E \times T \to T$.

The trivial torsor under $E$ is the curve $E$ itself, with the action defined by the group law $E \times E \to E$. An isomorphism of torsors $T_1$ and $T_2$ is defined to be an isomorphism of curves $T_1$ and $T_2$, that respects the action by $E$. A torsor $T$ is isomorphic to the trivial torsor if and only if the set $T(K)$ is non-empty.

It is easy to verify that the automorphisms of the trivial torsors are precisely the translations by the points of $E$. Every torsor under $E$ is a twist of the trivial torsor, i.e. it is isomorphic to the trivial torsor over the algebraic closure $\bar{K}$. Thus, according to the general principle that the twists of an object $X$ are parametrised by the Galois cohomology group $H^1(K, \text{Aut}(X))$, we have the following well known fact.

**Proposition 2.1.2.** The $K$-isomorphism classes of torsors under $E$ are parametrised by the Galois cohomology group $H^1(K, E)$.

Under this parametrisation, the Tate-Shafarevich group $\text{III}(E/K)$ corresponds to the kernel of the map $H^1(K, E) \to \prod H^1(K_v, E)$, where $v$ runs over all of the finite places of $K$, and the map is the product of the restriction maps $H^1(K, E) \to H^1(E, K_v)$.

Instead of torsors, one can also consider pairs $(C, \omega)$, where $C$ is a smooth genus one curve with Jacobian $E$, and $\omega$ is a regular differential on $C$. Given a Weierstrass equation $W$ for $E$,

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

we define the trivial pair to be $(E, \omega_E)$, where $\omega_E = \frac{dx}{2y + a_1 x + a_3}$ is the invariant differential on $E$ associated to the equation $W$. The automorphisms of $E$ that preserve the differential $\omega_E$ are exactly the translation maps.
Proposition 2.1.3. There is a natural bijection between the set of $K$-isomorphism classes of twists $(C, \omega)$ of the trivial pair $(E, \omega_E)$ and the group $H^1(K, E)$.

We now recall two interpretations of the group $H^1(K, E[n])$, for $n \geq 2$ an integer.

\begin{definition}
(i) A torsor divisor class pair $(C, [D])$ is a torsor $C$ under $E$ together with a $K$-rational divisor class $[D]$ on $C$ of degree $n$.

(ii) An isomorphism of torsor divisor class pairs $(C_1, [D_1]) \cong (C_2, [D_2])$ is an isomorphism of torsors $\phi : C_1 \cong C_2$ with $\phi^* D_2 \sim D_1$.
\end{definition}

The trivial torsor divisor class pair for $E$ is $(E, [n \cdot 0_E])$. Note that in the definition of $(C, [D])$ only the class $[D]$ has to be $K$-rational, not the divisor $D$ itself. Every torsor divisor class pair is a twist of the trivial one, and we have

Proposition 2.1.5. The torsor divisor class pairs, regarded as twists of $(E, [n \cdot 0_E])$, are parametrised up to isomorphism by $H^1(K, E[n])$.

The group law on $E$ induces a map $\text{sum} : \text{Div} E \to E$, defined by

$$\sum \text{formal sum} n_p \cdot (P) \mapsto \sum \text{addition on } E n_p P.$$ 

The (isomorphism classes of) torsor divisor class pairs $(E, [D])$, where the torsor is trivial, can be identified with the group $E(K)/pE(K)$, via the map $(E, [D]) \mapsto \text{sum}(D)$. It is simple to check that this is well-defined and injective, as well as surjective - given $[P] \in E(K)/pE(K)$, we see that $(E, [(n-1)0_E + P]) \mapsto [P]$. The inverse of this map can be interpreted as the Kummer map $\delta : E(K)/pE(K) \to H^1(K, E[n])$.

\begin{definition}
(i) A diagram $[C \to S]$ is a morphism from a torsor $C$ under $E$ to a variety $S$.

(ii) An isomorphism of diagrams $[C_1 \to S_1] \sim [C_2 \to S_2]$ is an isomorphism of torsors $\phi : C_1 \cong C_2$ together with an isomorphism of varieties $\psi : S_1 \cong S_2$ making the diagram

$$
\begin{CD}
C_1 @>>> S_1 \\
\phi \downarrow @. \downarrow \psi \\
C_2 @>>> S_2
\end{CD}
$$

commute.
\end{definition}

The trivial diagram is $[E \to \mathbb{P}^{n-1}]$ with the map determined by any choice of basis for the Riemann-Roch space $\mathcal{L}(n \cdot 0_E)$. We define an $n$-diagram, in the literature also known as a Brauer-Severi diagram, to be a twist $[C \to S]$ of the trivial diagram. In particular, the variety $S$ is a twist of the projective space, and hence a Brauer-Severi variety.

Proposition 2.1.6. The group $H^1(K, E[n])$ parameterises the $K$-isomorphism classes of $n$-diagrams $[C \to S]$. 


2.2. FREE RESOLUTIONS AND THE GORENSTEIN CONDITION

If the diagram \([C \to S]\) represents an element of the \(n\)-Selmer group of \(E\), then \(C\) has points everywhere locally, and hence \(S\) has points everywhere locally. By the local-global principle for the Brauer group we see that \(S \cong \mathbb{P}^{n-1}\), and so elements of the \(n\)-Selmer group are represented by the diagrams of the form \(C \to \mathbb{P}^{n-1}\).

Given a diagram \([C \to S]\), we have \(S \cong \mathbb{P}^{n-1}\) over \(\bar{K}\). Pullback of the hyperplane divisor then defines a \(\bar{K}\)-rational divisor \(D\) on \(C\), and one can check that \([D]\) is a well-defined \(K\)-rational divisor class on \(C\), i.e. independent of the choice of \(\bar{K}\)-isomorphism \(S \cong \mathbb{P}^{n-1}\), and invariant under the action of \(\text{Gal}(\bar{K}/K)\).

Given a torsor divisor class pair \((C, [D])\), where the divisor \(D\) itself is defined over \(K\) (not just the divisor class \([D]\)), the complete linear system \(|D|\) defines a \(n\)-diagram \([C \to \mathbb{P}^{n-1}]\). Conversely, to an \(n\)-diagram \([C \to \mathbb{P}^{n-1}]\) we associate the pair \((C, [H])\), where \(H\) is any hyperplane section of \(C\). These classes correspond to elements of \(H^1(K, E[n])\) with trivial obstruction - see Section 2 of [CFO+08] for more details.

2.2 Free resolutions and the Gorenstein condition

We recall here some basic results from commutative algebra. The main references for this section will be [Eis13], [BH98] and [KM83].

2.2.1 Basic properties

We work throughout over the graded polynomial ring \(R = k[x_0, \ldots, x_m]\), where \(k\) is a field. For \(M = \oplus M_d\) a graded \(R\)-module, let \(M(c) = \oplus M_{c+d}\) be the graded \(R\)-module with grading shifted by \(c\). We say that the direct sums of the modules \(R(c)\) are the free graded \(R\)-modules.

**Definition 2.2.1.** A graded free resolution of a graded \(R\)-module \(M\) is a chain complex \(F_\bullet\) of graded free \(R\)-modules

\[
F_r \xrightarrow{\phi_r} F_{r-1} \xrightarrow{\phi_{r-1}} \cdots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0,
\]

that is exact in degree \(> 0\), and has \(H_0(F_\bullet) = F_0/\phi_0(F_1) \cong M\).

Let \(m = (x_1, \ldots, x_m)\) be the maximal homogeneous ideal of \(R\). We say a resolution \(F_\bullet\) is minimal if we have \(\phi_k(F_k) \subset mF_{k-1}\) for every \(k \geq 1\).

**Remark 2.2.2.** If we represent the maps \(\phi_k\) concretely as matrices of homogeneous polynomials, a resolution is minimal if and only if every non-zero entry of every matrix is of positive degree. Moreover, by Nakayama's lemma, this is equivalent to requiring that \(\phi_1\) takes the basis of \(F_1\) to a minimal set of generators for \(\ker(\phi_1)\), see Corollary 1.5 of [Eis05]. This characterization makes it clear that every finitely generated graded module admits a minimal free resolution.

Minimal free resolutions have a strong uniqueness property. First let us recall the standard comparison theorem, true for arbitrary rings \(R\).

**Lemma 2.2.3 (Comparison lemma).** Let \(R\) be a commutative ring. Let \(F_\bullet\) be a chain complex of \(R\)-modules

\[
\cdots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \cdots \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0
\]
with each $F_i$ projective, and let $G_•$.

\[ \ldots \xrightarrow{\delta_{n+1}} G_n \xrightarrow{\delta_n} \ldots \xrightarrow{\delta_1} G_0 \xrightarrow{\delta_0} N \rightarrow 0 \]

be a chain complex of $R$-modules with no homology, i.e. an exact complex. For any map $\phi : M \rightarrow N$, there exists a lift of $\phi$ to a map of complexes $\tilde{\phi} : F_• \rightarrow G_•$, represented by the commutative diagram:

\[ \ldots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \ldots \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \]

\[ \ldots \xrightarrow{\delta_{n+1}} G_n \xrightarrow{\delta_n} \ldots \xrightarrow{\delta_1} G_0 \xrightarrow{\delta_0} N \]

If $\tilde{\phi}$ is another such lift, then $\bar{\phi}$ and $\tilde{\phi}$ are chain homotopic, meaning that there exists a collection of maps $h : F_i \rightarrow G_{i+1}$ with

\[ \bar{\phi} - \tilde{\phi} = \delta_{i+1} h_i + h_{i-1} d_i : F_i \rightarrow G_i. \]

For a proof, see Lemma 20.3 of [Eis13]. Taking $\phi$ to be the identity map, we see that any two projective resolutions of a module $M$ are chain homotopy equivalent. For minimal free resolutions of graded modules, we have the following stronger result.

**Proposition 2.2.4.** Let $M$ be a finitely generated graded $R$-module. Up to isomorphism of chain complexes, there is only one minimal free resolution of $M$.

More precisely, we have the following. Suppose $F_•$ and $G_•$ are minimal graded free resolutions of $M$. Then every lift of the identity map $M \rightarrow M$ to a map of complexes $F_• \rightarrow G_•$ is an isomorphism.

**Proof.** This statement follows from Theorem 20.2 of [Eis13]. The proof is an application of (graded) Nakayama’s lemma. Note however, that the statement there is given for the case when $R$ is a local ring, but the same proof applies to the case when $R$ is a positively graded algebra over a field.

A fundamental result of Hilbert states that minimal free resolutions have finite length.

**Proposition 2.2.5 (Hilbert syzygy theorem).** Let $M$ be a finitely generated graded $k[x_1, \ldots, x_n]$-module. Then the minimal free resolution of $M$ is finite, of length at most $n$.

The modules we consider will be homogeneous coordinate rings of projective varieties. We will be particularly interested in Gorenstein rings, which we define below. We need a preliminary technical definition.

The length of a minimal free resolution is called the projective dimension of $M$ and is denoted by $\text{proj dim } M$. We write $\text{codim } I$ for the codimension of a homogeneous ideal $I \subset R$. By the Auslander-Buchsbaum formula, we have the inequality $\text{codim } I \leq \text{proj dim } I$. We say a homogeneous ideal $I$ is perfect if $\text{codim } I = \text{proj dim } R/I$. 
Sign conventions for the dual complex. For a graded module \( M \), we will denote by \( M^* \) the dual module \( \text{Hom}(M,R) \). Note that \( R(n)^* \cong R(-n) \) as a graded module. The dual of a finite chain complex \( (F_\bullet, \phi_\bullet) \), of length \( n \), of graded \( R \)-modules \( M \) will for us be a chain complex (as opposed to a cochain complex) of graded free \( R \)-modules, denoted by \( F_\bullet^* \), with \( F_i^* = \text{Hom}(F_{n-i}, R) \). We adopt the sign convention that the differential \( F_i^* \to F_{i+1}^* \) is given by \((-1)^i \phi_{n-i}^* \).

**Definition 2.2.6.** Let \( I \subset R \) be a perfect ideal, and let \( F_\bullet \) be the minimal graded free resolution of \( I \). We say that \( I \) is a Gorenstein ideal if \( F_\bullet \) is isomorphic to its dual, up to a shift in the degree, i.e. if \( F_\bullet \cong F^*(c) \), for some integer \( c \).

There are many equivalent definitions of the Gorenstein property, see Chapter 21 of [Eis13] and Chapter 3 of [BH98].

Koszul resolutions. The basic example of a minimal free resolution is the Koszul complex. We briefly recall its definition and basic properties, following [Eis13] and [Mat89]. Let \( R \) be a commutative ring and let \( E \) be a free \( R \)-module of finite rank \( r \). Given an \( R \)-linear map \( f: E \to R \), the Koszul complex associated to \( f \) is the chain complex of \( R \)-modules

\[
K_\bullet(f): 0 \to \Lambda^r E \xrightarrow{d_r} \Lambda^{r-1} E \to \ldots \to \Lambda^1 E \xrightarrow{d_1} R
\]

where the differential \( d_k \) is given by, for any \( e_1, e_2, \ldots, e_k \in E \)

\[
d_k(e_1 \wedge \ldots \wedge e_k) = \sum_{i=1}^{k} (-1)^{i+1} f(e_i) e_1 \wedge \ldots \wedge \hat{e_i} \wedge \ldots \wedge e_k.
\]

Now let \( e_i \) be a basis of \( E \) and let \( x_i = f(e_i) \).

**Theorem 2.2.7.** If \( x_1, \ldots, x_r \) is a regular sequence in \( R \), meaning that \( x_i \) is not a zero-divisor on \( R/(x_1, \ldots, x_{i-1}) \) for all \( i \), then \( K_\bullet(f) \) is a free resolution of \( R/(x_1, \ldots, x_r) \).

**Proof.** This is Theorem 16.5(i) of [Mat89].

The case of the theorem we will be using is when \( R = S[x_1, \ldots, x_m] \), for an arbitrary base ring \( S \) and \( m \geq r \). In this case \( K_\bullet(f) \) is a graded free resolution of the ideal \( (x_1, \ldots, x_r) \), with the grading given by \( K_\bullet(f)_k = (\Lambda^k E)(-k) \).

It is easy to verify that the pairings \( \Lambda^i E \times \Lambda^j E \to \Lambda^{i+j} E \) satisfy the Leibniz rule: for \( f_i \in \Lambda^i E \) and \( f_j \in \Lambda^j E \) we have

\[
d_{i+j}(f_i \wedge f_j) = d_i(f_i) \wedge f_j + (-1)^i f_i \wedge d_j(f_j).
\]

Furthermore \( f_i \wedge f_j = (-1)^{ij} f_j \wedge f_i \). Thus the wedge product makes the Koszul complex the simplest example of differential graded commutative algebra, which we will define in Section 2.2.2.
The Koszul complex is self-dual: we can identify $\Lambda^* E = R$, using, for example, the generator $e_1 \wedge \ldots \wedge e_r$. Then the pairings $\Lambda^* E \times \Lambda^{r-i} E \to \Lambda^* E = R$ induces a map $\eta : K_\bullet \to K_\bullet^*$, which is a map of chain complexes by the Leibniz rule, and an isomorphism as the pairings are perfect.

2.2.2 Algebra structures on resolutions

In this section we will consider graded modules over the ring $R = S[ x_0, \ldots, x_m ]$. In our applications, the ring of scalars $S$ will either be a field, or a ring of $p$-adic integers $\mathbb{Z}_p$, for some prime $p$.

Let $(C_\bullet, d)$ be a chain complex of $R$-modules with $C_0 = R$. A differential graded algebra structure on $C_\bullet$ is a collection of maps $C_i \otimes C_j \to C_{i+j}$ that satisfies the Leibniz rule. In other words, a multiplication rule on $C_\bullet$ such that, if $z_i \in C_i$ and $z_j \in C_j$, then $z_i \cdot z_j \in C_{i+j}$, and

$$d_{i+j}(z_i \cdot z_j) = d_i(z_i) \cdot z_j + (-1)^i z_i \cdot d_j(z_j).$$

We will also require that the map $C_0 \otimes C_i \to C_i$ is just the usual multiplication $R \otimes C_i \to C_i$, when we identify $C_0 = R$. In other words, 1 $\in C_0$ is the identity element.

We omit the subscripts on the differential maps when there is no danger of confusion. We say the algebra is commutative if we have $z_i \cdot z_j = (-1)^{ij} z_j \cdot z_i$ for $i$ and $j$, and $z_i \cdot z_i = 0$ for all $i$ odd. In this case, we say $C_\bullet$ has a DGCA (differential graded commutative algebra) structure.

Buchsbaum-Eisenbud construction. Now let $F_\bullet$ be a finite graded free resolution of an ideal $I \subset R$, so that $F_0 = R$, and $H_i(F_\bullet) = 0$ for $i > 0$. There is a natural way to define a DGCA structure on $F_\bullet$, due to Buchsbaum and Eisenbud [BE82]. We describe their construction. Define the symmetric square $S^2(F_\bullet)$ to be

$$S^2(F_\bullet) = (F_\bullet \otimes F_\bullet)/M$$

where $M$ is the submodule of $F_\bullet \otimes F_\bullet$ generated by

$$\{ z_i \otimes z_j - (-1)^{ij} z_j \otimes z_i \mid z_k \in F_k \} \cup \{ z_i \otimes z_i \mid z_i \in F_i, i \text{ odd} \}$$

Then $S^2(F_\bullet)$ is a chain complex, with the differential induced from the differential on $F_\bullet \otimes F_\bullet$,

$$d(z_i \otimes z_j) = dz_i \otimes z_j + (-1)^i z_i \otimes dz_j.$$
2.2. FREE RESOLUTIONS AND THE GORENSTEIN CONDITION

In particular, note that $S^2(F_\bullet)$ is a complex of free modules. We have $S^2(F)_0 = F_0 \otimes F_0$ and $S^2(F)_1 = F_0 \otimes F_1$. Identifying the left $F_0$ with $R$, we obtain maps $S^2(F)_0 = R \otimes F_0 \to F_0$ and $S^2(F)_1 = R \otimes F_1 \to F_1$. These maps commute with differentials on $S^2(F)$ and $F$. As $H_i(F_\bullet) = 0$ for $i \geq 1$, by Lemma 2.2.3 they can be extended to a map of chain complexes $\alpha : S^2(F_\bullet) \to F_\bullet$. For homogeneous elements $z_i$ and $z_j$, we put $z_i \cdot z_j = \alpha(z_i \otimes z_j)$. It is clear that this defines a DGCA structure on $F_\bullet$.

Construction of a null homotopy. Suppose that $F_\bullet$ and $G_\bullet$ are DGCA algebras, and that $\beta : F_\bullet \to G_\bullet$ is a map of chain complexes. The map $\beta$ does not need to respect the DGCA structure on the nose, but it does so up to homotopy. The following result, Lemma 1.2 of [KM83], makes this precise.

**Lemma 2.2.8.** Let $\beta : F_\bullet \to G_\bullet$ be a map of complexes of free $R$-modules.

\[
\begin{array}{cccccccc}
\cdots & \phi_{n+1} & F_n & \phi_n & \cdots & \phi_2 & F_1 & \phi_1 & F_0 \\
\downarrow{\beta_n} & & \downarrow{\beta_n} & & \downarrow{\beta_1} & & \downarrow{\beta_0} \\
\cdots & \psi_{n+1} & G_n & \psi_n & \cdots & \psi_2 & G_1 & \psi_1 & G_0 \\
\end{array}
\]

Suppose that $F_\bullet$ and $G_\bullet$ are both DGCA. If $H_i(G_\bullet) = 0$ for $i \geq 1$, then there exists a collection of maps $\xi : F_i \otimes F_j \to G_{i+j+1}$, defined for $i, j \geq 0$, such that:

(i) $\xi(z_i \otimes z_j) = (-1)^{ij}\xi(z_j \otimes z_i),$

(ii) $\xi(z_i \otimes z_i) = 0$ if $i$ is odd,

(iii) $\xi(z_0 \otimes z_i) = 0,$

(iv) $\beta_{i+j}(z_i \cdot z_j) - \beta_i(z_i) \cdot \beta_j(z_j) = \xi(\phi_i(z_i) \otimes z_j) + (-1)^i \xi(\phi_j(z_j) \otimes z_i) + \psi_{i+j+1}(\xi(z_i \otimes z_j))$ for $z_i \in F_i$.

**Proof.** Consider the maps $F_i \otimes F_j \to G_{i+j+1}$ defined by $z_i \otimes z_j \mapsto \beta_{i+j}(z_i \cdot z_j) - \beta_i(z_i) \cdot \beta_j(z_j)$. It is easy to check, using the Leibniz rule, that these maps induce a map of chain complexes $S_2(F_\bullet) \to G_\bullet$, that is zero in degrees zero and one. Hence, by Lemma 2.2.3, there is a null homotopy $\xi : F_i \otimes F_j \to G_{i+j+1}$, and it is clear that $\xi$ satisfies properties (i)-(iv).

DGCA structures on self-dual resolutions. Now suppose that $F_\bullet$ is of length $n - 1$, so that the last non-zero module in $F$ is $F_{n-2}$, and suppose that the resolution $F_\bullet$ is self-dual, so that $F_\bullet \cong F^*_\bullet$, up to a shift in grading. We identify $R = F_0 = F^*_n$. For each $i$, algebra multiplication $F_i \otimes F_{n-2-i} \to R$ induces a map $s_i : F_i \to F^*_n$.

We then have the following statement, based on Proposition 3.4.4 of [BH98], with a slight difference given by our sign convention for the dual complex.

**Proposition 2.2.9.** The maps $s_i : F_i \to F^*_n$ define a homomorphism of chain complexes $s : F_\bullet \to F^*_\bullet$, lifting the isomorphism $F_0 \to F^*_n$. This map is symmetric, meaning that for any $f_i \in F_i$ and $f_{n-2-i} \in F_{n-2-i}$ we have

\[s_i(f_i)(f_{n-2-i}) = (-1)^{(n-2-i)} s_{n-2-i}(f_{n-2-i})(f_i).\]
If $R = k[x_1, \ldots, x_m]$ is the graded polynomial ring over a field $k$, and $F_\bullet$ is a minimal free resolution, then this homomorphism is an isomorphism.

**Proof.** The symmetry property follows from the commutativity of the algebra. We check that the $s_i$ define a chain map. Let $a \in F_i$ and $b \in F_{n-1-i}$. Then $a \cdot b \in F_{n-1}$, and hence $a \cdot b = 0$. Therefore $0 = \phi(a \cdot b) = \phi(a) \cdot b + (-1)^i a \cdot \phi(b)$, and so $\phi(a) \cdot b = (-1)^{i+1} a \cdot \phi(b)$. We then compute

$$s_{i-1}(\phi(a))(b) = \phi(a) \cdot b = (-1)^{i+1} a \cdot \phi(b) = (-1)^{i+1} s_i(a)(\phi(b)),$$

$$= (-1)^{i+1} \phi^*(s_i(a))(b).$$

Hence $s_{i-1} \circ \phi = (-1)^{i+1} \phi^* \circ s_i$, and it follows that the maps $s_i$ define a homomorphism of chain complexes. As $1 \in F_0 = R$ is the identity element for the DGCA structure, the map $s_0$ is an isomorphism. When $R = k[x_1, \ldots, x_m]$ and $F_\bullet$ is a minimal free resolution, the map $s : F_\bullet \rightarrow F_\bullet^*$ is an isomorphism by Proposition 2.2.4. \qed
Chapter 3

Minimal free resolutions, genus one curves and algebras

In this chapter we study the invariant theory of minimal free resolutions of the homogeneous coordinate rings of two kinds of projective varieties, namely genus one normal curves of degree \( n \) in \( \mathbb{P}^{n-1} \), and sets of \( n \) points in general position in \( \mathbb{P}^{n-2} \).

We start by explaining how the data of a minimal free resolution can be viewed as a generalization of the notion of a genus one model of degree \( n \), introduced in [CFS10]. Proposition 3.3.5 gives an equation of the Jacobian \( E \) of a genus one normal curve \( C \), in terms of the data of the minimal free resolution of \( C \). Theorem 3.5.7 gives a formula for the structure constants associated to the algebra of global functions on a set \( X \) of \( n \) points in \( \mathbb{P}^{n-2} \), again in terms of a minimal free resolution of \( X \). In Section 3.7 we then relate these two constructions to define the discriminant form, a key object in our proof of Theorem 1.0.1.

3.1 Resolution models

We will be concerned with minimal graded free resolutions of the following two types of varieties. Throughout this section, let \( k \) be a field.

Definition 3.1.1. A genus one normal curve of degree \( n \) is a smooth curve of genus one and degree \( n \) that spans \( \mathbb{P}^{n-1} \).

In the literature, these curves are also known as elliptic normal curves.

Definition 3.1.2. We say a zero dimensional variety \( X \subset \mathbb{P}^{n-2} \), defined over \( k \), is a set of \( n \) points in general position in \( \mathbb{P}^{n-2} \), if \( X \) is of degree \( n \) and the set of geometric points \( X(\bar{k}) \) consists of \( n \) points in general position, meaning that no subset of \( X \) of size \( n-1 \) is contained in a hyperplane.

Notably, such sets arise as hyperplane sections of genus one normal curves of degree \( n \).

Theorem 3.1.3. Let \( n \geq 4 \), and let \( R = A[x_1, \ldots, x_m] \) be a polynomial ring over a base ring
A. We consider chain complexes of length \( n - 1 \) and of the form
\[
0 \to R(-n) \xrightarrow{\phi_{n-2}} R(-n+2) b_{n-3} \xrightarrow{\phi_{n-3}} R(-n+3) b_{n-4} \xrightarrow{\phi_{n-4}} \ldots \xrightarrow{\phi_3} R(-3) b_2 \xrightarrow{\phi_2} R(-2) b_1 \xrightarrow{\phi_1} R \to 0,
\] (⋆)
where the Betti numbers are given by \( b_i = n \binom{n-2}{i} - \binom{n}{i+1} \).

(i) Let \( C \subset \mathbb{P}^{n-1} \) be a genus one normal curve of degree \( n \), defined over \( k \), and let \( I := I(C) \) be the homogeneous ideal defining \( C \). Then \( I \) is Gorenstein, and the minimal free resolution \( F_\bullet \) of \( A/I \) is of the form (⋆), with \( R = k[x_1, \ldots, x_n] \).

(ii) Let \( X \subset \mathbb{P}^{n-2} \) be a set of \( n \) points in general position. Let \( I := I(X) \) be the homogeneous ideal of \( k[x_1, \ldots, x_{n-1}] \) defining \( X \). Then \( I \) is Gorenstein, and the minimal free resolution \( F_\bullet \) of \( A/I \) is of the form (⋆), with \( R = k[x_1, \ldots, x_{n-1}] \).

Proof. Both of these results are well known, and in fact (ii) follows from (i). For a proof of (i) see [BH03], or Theorem 1.1 of [Fis06], and for (ii), see the discussion of Theorem 138 in [Wil13]. As a byproduct of our work in Chapter 4, we will reprove the theorem along the lines of the method used in [Fis06].

Throughout this section, we consider only rings \( R = A[x_1, \ldots, x_m] \) with \( m \) equal to either \( n \), the case of curves, or \( n - 1 \), the case of points.

Example 3.1.4. Let \( C_n \) and \( X_n \) denote a genus one normal curve of degree \( n \), and a set of \( n \) points in general position in \( \mathbb{P}^{n-2} \) respectively.

(i) The case \( n = 3 \) does not quite fit in the setting of the theorem, but is easy to describe.

The curve \( C_3 \) is a degree 3 plane curve, and so is defined by a ternary cubic form. The set \( X_3 \) consists of 3 distinct points of \( \mathbb{P}^1 \), and so is defined by a binary cubic form. The minimal free resolution is in both cases of the form \( 0 \to R(-3) \xrightarrow{E} R \to 0 \).

(ii) \( n = 4 \). In this case, both \( C_4 \) and \( X_4 \) are codimension 2 subsets, defined by a pair of quadratic forms. Thus they are complete intersections, and their free resolution is given by a Koszul complex,
\[
0 \to R(-4) \xrightarrow{\phi_2} R(-2)^2 \xrightarrow{\phi_1} R \to 0
\]
where \( \phi_2 = (F_2, -F_1)^T \) and \( \phi_1 = (F_1, F_2) \), and \( F_1, F_2 \) are pairs of quaternary or ternary quadratic forms respectively.

(iii) \( n = 5 \). The resolution (⋆) is then
\[
0 \to R(-5) \xrightarrow{\phi^T} R(-3)^5 \xrightarrow{A} R(-2)^5 \xrightarrow{\phi} R \to 0
\]
\( C_5 \) and \( X_5 \) are Gorenstein varieties of codimension 3. Thus their minimal free resolutions are self-dual, and one can choose the bases of the modules in the resolutions so that the differentials of (⋆) take on a symmetric form, as observed by Buchsbaum and Eisenbud in [BE82]. The map \( R(-3)^5 \to R(-2)^5 \) is represented by an alternating matrix of linear forms \( A \), and the entries of \( \phi \) and its transpose \( \phi^T \) are the signed \( 4 \times 4 \) sub-Pfaffians of \( A \).
A generic ternary cubic defines a plane curve $C$, and if $C$ is non-singular, it will be a genus one normal curve of degree 3. Similarly, a generic pair of quadrics will define a smooth genus one curve of degree 4. When $n = 5$ however, $C$ is not a complete intersection, and the quadrics that cut out $C$ are very special. Indeed, a randomly chosen set of five quadrics will not, most of the time, even define a curve in $\mathbb{P}^4$.

However, for a generic $5 \times 5$ alternating matrix of linear forms in four variables, the $4 \times 4$ sub-Pfaffians will define a genus one normal curve of degree 5, and all such curves are obtained in this way. This observation, together with algebra structures on resolutions we discussed in Section 2.2.2, motivates our next definition.

**Definition 3.1.5.** Let $S$ be an arbitrary commutative ring, $n \geq 3$ and $m \geq 2$ integers, and let $R = S[x_1, \ldots, x_m]$. A resolution model of degree $n$, defined over $S$, is a collection of maps $(\phi_i)_{i=1}^{n-2}$ of graded $R$-modules, that fit together into a chain complex $F_\bullet$ of the form (*)

$$
0 \to R(-n) \xrightarrow{\phi_{n-2}} R(-n+2)b_{n-3} \xrightarrow{\phi_{n-3}} R(-n+3)b_{n-4} \to \ldots \xrightarrow{\phi_3} R(-3)b_2 \xrightarrow{\phi_2} R(-2)\to R \to 0,
$$

for which there exists an isomorphism $\eta : F_\bullet \to \text{Hom}(F_\bullet, R(-n))$ of graded chain complexes, that is symmetric, in the following sense. We have, for all $f_i \in F_i$ and $f_{n-2-i} \in F_{n-2-i}$

$$
\eta_i(f_i)(f_{n-2-i}) = (-1)^{(n-2-i)}\eta_{n-2-i}(f_{n-2-i})(f_i).
$$

We will also refer to the complex $F_\bullet$ as a resolution model, with the understanding that we have chosen a basis for each module $F_i$. When $m = n - 1$, we will also say $F_\bullet$ is a genus one model of degree $n$.

**Example 3.1.6.** Suppose $n = 5$ and $F_3 \xrightarrow{\phi_3} F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0$ is a resolution model. If the bases of $F_2$ and $F_3$ are chosen to be dual to each other with respect to the pairing induced by $\eta$, then the condition that $\eta$ is symmetric implies that $\phi_2$ is represented by an alternating matrix of linear forms.

**Definition 3.1.7.** We say that a resolution model $F_\bullet$ is non-degenerate when the homology modules $H_i(F_\bullet)$ vanish for $i > 0$, i.e. when $F_\bullet$ is a free resolution of an ideal $I$.

**Example 3.1.8.** Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve, defined over a field $k$. By Proposition 2.2.9, a minimal free resolution $F_\bullet$ of the coordinate ring of $C$, with a choice of basis of each module $F_i$, is a resolution model of degree $n$. We say that $F_\bullet$ represents the $n$-diagram $[C \to \mathbb{P}^{n-1}]$.

**Lemma 3.1.9.** Let $F_\bullet$ be a chain complex of the form (*), that is a resolution of an ideal $I \subset S[x_1, \ldots, x_m]$. Suppose that there exists an isomorphism $\eta : F_\bullet \to \text{Hom}(F_\bullet, R(-n))$. Then $\eta$ is unique up to scaling by the invertible elements of $S$, and $\eta$ is symmetric.

**Proof.** As $F_0 \cong F_0^* = R$, and $\eta_0$ is an isomorphism of graded modules, we see that $\eta_0$ is multiplication by an element of $S^\times$. By Lemma 2.2.3, the map $\eta_0$ determines the map $\eta$ up to a chain homotopy $\gamma$. But looking at the grading of the modules $F_i$, we see that such a $\gamma$ is necessarily zero.
Now note that the map $s$ constructed in Proposition 2.2.9 is symmetric, and also a chain map lifting an isomorphism $R \to \Hom(R(-n), R(-n))$. Thus the map $\eta$ is chain homotopic to an $S^g$-multiple of $s$. Arguing as before, the homotopy must be zero, and $\eta$ is equal to an $S^g$-multiple of $s$, and is thus symmetric.

Denote the set of all resolution models defined over a ring $S$ by $X_n(S)$. A ring homomorphism $S \to S'$ induces a natural map $X_n(S) \to X_n(S')$.

**Definition 3.1.10.** Let $k$ be the field of fractions of an integral domain $S$, and let $C$ be a genus one normal curve of degree $n$, defined over $k$. An $S$-integral model of $C$ is a non-degenerate resolution model $F_\bullet \in X_n(S)$ that maps into a genus one model of $C$ under the map $X_n(S) \to X_n(k)$.

**Equivalence of resolution models.** A resolution model includes a choice of basis for each module in the resolution, and so the group $G^{\text{res}}_n = \text{GL}_{b_{n-2}} \times \cdots \times \text{GL}_{b_0}$ acts on the space $X_n$ of genus one models. We give an explicit description of this action. Let $F_\bullet$ be a resolution model defined over $S$, with the differentials represented by matrices $\phi_1, \ldots, \phi_{n-2}$. For $0 \leq i \leq n-2$, an element $g_i \in \text{GL}_{b_i}(S)$ acts on $F_\bullet$ by replacing $\phi_i$ and $\phi_{i+1}$ with $g_i \phi_i$ and $\phi_{i+1} g_i^{-1}$ respectively, with $\phi_0$ and $\phi_{n-1}$ understood to be zero.

The action of the group $\text{GL}_{m'}$ on $\mathbb{P}^{m-1}$ also lifts to an action on the space $X_n$. Let $g = (g_{ij}) \in \text{GL}_{m+1}$, and put $x'_j = \sum_{i=1}^{m} g_{ij} x_i$. Regard matrices $\phi_r = \phi_r(x_1, \ldots, x_m)$ as functions of the variables $x_1, \ldots, x_m$, and put, for $1 \leq r \leq n-2$

$$\phi'_r(x_1, \ldots, x_m) = \phi_r(x'_1, \ldots, x'_m)$$

We define $g \cdot F_\bullet$ to be the resolution model specified by the differentials $\phi'_1, \ldots, \phi'_{n-2}$. We define $G_n = G^{\text{res}}_n \times \text{GL}_m$, and say two models $F_\bullet, F'_\bullet \in X_n(S)$ are equivalent over $S$ if there exists a $g \in G_n(S)$ with $g \cdot F_\bullet = F'_\bullet$.

**Proposition 3.1.11.** Let $F_\bullet$ and $F'_\bullet$ be resolution models that represent genus one normal curves $C \subset \mathbb{P}^{m-1}$ and $C' \to \mathbb{P}^{m-1}$, defined over a field $K$. The models $F_\bullet$ and $F'_\bullet$ are equivalent over $K$ if and only if there exists an element of $\text{PGL}_n(K)$ that takes $C$ to $C'$.

**Proof.** This follows from Proposition 2.2.4 and the definition of isomorphism of $n$-diagrams.

**Remark 3.1.12.** For $n \leq 5$ the definition of a genus one model agrees with the existing definitions of a genus one model in the literature. In this thesis we will be concerned only with non-degenerate genus one models, and among those mainly with the genus one models that correspond to genus one curves defined over a field. For such models, we were able to prove many analogues of the properties that holds for $n \leq 5$, so we hope that our definition is the morally correct one.

However, the space of degenerate genus one models is mysterious when $n > 5$. For example, if we are given a non-degenerate genus one model with $\mathbb{Z}$-coefficients, that corresponds to a smooth genus one curve over $\mathbb{Q}$, a natural operation in number theory would be to reduce the model modulo a prime $p$, and the reduced model need not be non-degenerate anymore.
3.2 Ω-QUADRICS AND THE INVARIANT THEORY OF RESOLUTION MODELS

Thus we would like the space of genus one models to contain the closure of the space of non-degenerate genus one models, which our definition accomplishes. However, it might be too relaxed - the space might not be irreducible, which is not the case for \( n \leq 5 \), where the space of genus one models is in fact an affine space.

For example, Miles Reid has studied the structure theory of codimension 4 Gorenstein ideals in [R\(^{+}15\)], which corresponds to our case \( n = 6 \), and there he has singled out an irreducible component of the space of the self-dual chain complexes as the right space to study.

### 3.2 Ω-quadrics and the invariant theory of resolution models

Let \( F_\bullet \) be a resolution model of degree \( n \), for \( R = S[x_1, \ldots, x_m] \), where \( n \geq 3, m \geq 1 \) are integers. We represent the differentials \( \phi_r \) of \( F_\bullet \) by matrices of homogeneous forms. Note that \( \phi_{n-2} \) and \( \phi_{i} \) are represented by matrices consisting of quadratic forms, while the maps \( \phi_i \) for \( 1 < i < n - 2 \), are represented by matrices of linear forms. For \( 1 \leq a_1, a_2, \ldots, a_{n-2} \leq m \) we define the quadrics:

\[
[a_1, a_2, \ldots, a_{n-2}]_{F_\bullet} = \frac{\partial \phi_1}{\partial x_{a_1}} \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \frac{\partial \phi_{n-2}}{\partial x_{a_{n-2}}},
\]

where a partial derivative of a matrix is the matrix of the partial derivatives of the entries, and the product is matrix multiplication. Let \( \sigma \) be the \((n-2)\)-cycle \((12 \ldots n-2)\) in \( S_{n-2} \), and then define

\[
[[a_1, a_2, \ldots, a_{n-2}]_{F_\bullet}] = \sum_{k=1}^{n-2} [a_{\sigma^{2k}(1)}, a_{\sigma^{2k}(2)}, \ldots, a_{\sigma^{2k}(n-2)}].
\]

Most of the time, unless there is danger of confusion, we omit the subscript \( F_\bullet \). For each tuple \((b_1, b_2, \ldots, b_{m-n+2})\), where \( 1 \leq b_i \leq m \) are distinct integers, let \( a_1, a_2, \ldots, a_{n-2} \) be the complement of \( \{b_1, \ldots, b_{m-n+2}\} \) in \( \{1, 2, \ldots, m\} \), ordered so that

\[
(b_1, \ldots, b_{m-n+2}, a_1, \ldots, a_{n-2})
\]

is an even permutation of \( \{1, \ldots, m\} \).

**Definition 3.2.1.** With notation as above, for each tuple \( b_1, \ldots, b_{m-n+2} \) as above, we define a quadric form \( \Omega_{b_1, \ldots, b_{m-n+2}} = [[a_1, \ldots, a_{n-2}]_{F_\bullet}] \).

Let \( V = \langle x_1, \ldots, x_m \rangle \) be the space of linear forms on \( \mathbb{P}^{m-1} \), and denote the dual basis of \( V^* \) by \( x_1^*, \ldots, x_m^* \). To the collection of Ω-quadrics we associate an element \( \Omega \) of \( \wedge^{m-n+2} V^* \otimes_k S^2 V \) via the formula

\[
\Omega := \sum x_{b_1}^* \wedge x_{b_2}^* \wedge \cdots \wedge x_{b_{m-n+2}}^* \otimes \Omega_{b_1, \ldots, b_{m-n+2}}.
\]

where the sum is over all tuples \( (b_1, \ldots, b_m) \) as above. The proposition below shows that this construction is well-defined, i.e. invariant under change of basis of \( V \).

We are mainly interested in the cases \( m = n \) and \( m = n - 1 \), corresponding to resolution models of genus one curves and resolution models of sets of points respectively. In the first case, \( \Omega \in \wedge^2 V^* \otimes_k S^2 V \) can be represented by an alternating \( n \times n \)-matrix of quadratic forms in
CHAPTER 3. RESOLUTIONS, CURVES AND ALGEBRAS

In the second case \( \Omega \in V^* \otimes_k S^2V \) is represented by \( n \) quadratic forms in \( x_1, \ldots, x_{n-1} \). Thus according to which case we are in, \( \Omega \) has either one or two subscripts.

**Remark 3.2.2.** The construction of \( \Omega \)-quadrics is independent of the choice of basis of the free \( R \)-modules in the resolution, except for the leftmost module \( R(\mathbf{-}n) \), where change of basis has the effect of multiplying all the \( \Omega \)-quadrics by the same constant.

To see this, observe that changing the basis of \( F_i \) would mean replacing \( \phi_i \) by \( \phi_i A \) and \( \phi_{i+1} \) by \( A^{-1} \phi_{i+1} \), where \( A \) is a matrix with entries in \( S \). Applying the product rule, one immediately sees that this does not change the expression \[ \left[ a_1, a_2, \ldots, a_{n-2} \right] . \]

**Proposition 3.2.3.** Let \( F \bullet \) be a degree \( n \) resolution model. Let \( x'_j = \sum_{i=1}^m g_{ij} x_i \) for some \( g = (g_{ij}) \in \text{GL}_m \). With respect to the new coordinates given by \( x'_j \), \( R/I \) has a free resolution \( F' \bullet \), again of the form \((\ast)\), with the maps given by matrices \( \phi'_1, \ldots, \phi'_{n-2} \) where

\[
\phi'_r(x_1, \ldots, x_m) = \phi_r(x'_1, \ldots, x'_m).
\]

Let \( \Omega, \Omega' \) be the elements of \( \wedge^{n-m+2}V^* \otimes S^2V \) associated to resolutions \( \phi, \phi' \) respectively. Then we have

\[
\Omega' = \det(g) g \cdot \Omega,
\]

where the action of \( g \) on \( \Omega \) is the standard action of \( \text{GL}_m \) on \( \wedge^{m-n+2}V^* \otimes S^2V \).

**Remark 3.2.4.** The action of \( \text{GL}_m = \text{GL}(V) \) may be written in a simpler form if we instead define to be \( \Omega \) and \( \Omega' \) as elements of the \( \text{GL}(V) \)-representation \( \text{det}(V) \otimes \wedge^{m-n+2}V^* \otimes S^2V \), by using the formula

\[
\Omega := (x_1 \wedge \ldots \wedge x_m) \otimes \sum x_{b_1}^* \wedge x_{b_2}^* \wedge \ldots \wedge x_{b_{m-n+2}}^* \otimes \Omega_{b_1, \ldots, b_{m-n+2}}.
\]

With respect to this action, Proposition 3.2.3 states that \( \Omega' = g \cdot \Omega \).

We prove Proposition 3.2.3 in Section 3.4. Before that, we give some applications and examples.

### 3.3 \( \Omega \)-matrices and genus one normal curves

We now focus on the \( \Omega \)-quadrics associated to resolution models of genus one normal curves. In this section, we will restrict to the case when the field \( k \) is of characteristic 0.

**Example 3.3.1.** Let \( F \bullet \) be a genus one model of a genus one normal curve \( C_n \subset \mathbb{P}^{n-1} \). Taking \( m = n \), the above construction yields an element of \( \wedge^2V^* \otimes S^2V \), which can be represented by an alternating matrix of quadratic forms, called the \( \Omega \)-matrix.

(i) \( n = 3 \). Suppose \( C_3 \) is defined by a ternary cubic \( F \). The \( \Omega \)-matrix attached to the resolution \( 0 \to R(\mathbf{-}3) \xrightarrow{F} R \to 0 \) is

\[
\Omega_3 = \begin{pmatrix}
0 & \frac{\partial F}{\partial x_2} & -\frac{\partial F}{\partial x_1} \\
-\frac{\partial F}{\partial x_3} & 0 & \frac{\partial F}{\partial x_1} \\
\frac{\partial F}{\partial x_3} & -\frac{\partial F}{\partial x_2} & 0
\end{pmatrix}
\]
(ii) $n = 4$. Suppose $C_4$ is defined by a pair of quadratic forms $F_1$ and $F_2$, and consider the free resolution of Example 3.1(ii). Then $\Omega_4$ is given by

$$(\Omega_4)_{i,j} = \frac{\partial F_1}{\partial x_k} \frac{\partial F_2}{\partial x_l} - \frac{\partial F_1}{\partial x_l} \frac{\partial F_2}{\partial x_k}$$

where $(i, j, k, l)$ is an even permutation of $(1, 2, 3, 4)$.

We will denote the action of $\text{GL}_n$ on the space $\wedge^2 V^* \otimes S^2 V$ by the symbol $\star$. Explicitly, it is given by

$$g \star \Omega(x_1, \ldots, x_n) = g^{-T} \left( \sum_{i=1}^n g_i x_i, \ldots, \sum_{i=1}^n g_n x_i \right) g^{-1}$$

where $g^{-T}$ is the inverse of the transpose of $g$. Note that this action differs from the action of Proposition 3.2.3 by a factor of $\det(g)$. Under the $\star$-action, scalar matrices act trivially, so we have an induced action of $\text{PGL}_n$.

**Invariant differentials.** Let $F_\bullet$ be a resolution model of a genus one normal curve $C \subset \mathbb{P}^{n-1}$, and let $\Omega$ be the associated $\Omega$-matrix. We define the invariant differential associated to the matrix $\Omega$ to be a rational differential form on $C$, given by the expression

$$\omega_{ij} = (n-2) \frac{x_i^2 d(x_i/x_j)}{\Omega_{ij}(x_1, \ldots, x_n)},$$

for any distinct $i, j$. In fact, we will prove the following in Chapter 4.

**Proposition 3.3.2.** Let $\Omega$ be an $\Omega$-matrix associated to a resolution model $F_\bullet$ of a curve $C \subset \mathbb{P}^{n-1}$.

(i) The differential $\omega_{ij}$ is independent of the choice of indices $i$ and $j$, and we denote it just by $\omega$.

(ii) The differential $\omega$ is in fact a regular differential form on $C$.

We say that the model $F_\bullet$ represents the pair $(C, \omega)$.

The differential $\omega$ transforms in a natural way under the action of $\text{GL}_n$, as we will see in Lemma 3.4.8. Now, following [Fis18], we define certain polynomials in the coefficients of the $\Omega$-matrix that are invariant under the action of $\text{GL}_n$.

We start by defining

$$M_{ij} = \sum_{r,s=1}^n \frac{\partial \Omega_{ir}}{\partial x_r} \frac{\partial \Omega_{js}}{\partial x_s},$$

$$N_{ijk} = \sum_{r=1}^n \frac{\partial M_{ij}}{\partial x_r} \Omega_{rk}.$$ 

We then define the polynomials $c_4(\Omega)$ and $c_6(\Omega)$ as

$$c_4(\Omega) = \frac{3(n-2)^2}{2^4 n(n+3)} \sum_{i,j,r,s=1}^n \frac{\partial^2 M_{ij}}{\partial x_r \partial x_s} \frac{\partial^2 M_{rs}}{\partial x_i \partial x_j},$$

$$c_6(\Omega) = \frac{5(n-2)^2}{2^6 n(n+3)(n+5)} \sum_{i,j,r,s=1}^n \frac{\partial^2 M_{ij}}{\partial x_r \partial x_s} \frac{\partial^2 M_{rs}}{\partial x_i \partial x_j}.$$
and
\[ c_6(\Omega) = \frac{(n-2)^3}{2^{n(n+3)}} \sum_{i,j,k,r,s,t=1}^{n} \frac{\partial^3 N_{ijk}}{\partial x_r \partial x_s \partial x_t} \frac{\partial^3 N_{rst}}{\partial x_i \partial x_j \partial x_k}. \]

One can show that these polynomials are invariants of \( \Omega \), in the following sense:

**Proposition 3.3.3.** For \( g \in \text{GL}_n(k) \) and \( \Omega \in \Lambda^2 V \otimes S^2 V \), we have \( c_k(g \ast \Omega) = c_k(\Omega) \) for \( k = 4, 6 \).

**Proof.** The proof is a direct calculation, and given as Lemma 2.2 of [Fis18]. \( \square \)

**Remark 3.3.4.** The denominators appearing in the formulas for \( c_4(\Omega) \) and \( c_6(\Omega) \) are the reason we restrict to characteristic 0. For small values of \( n \), the invariant theory of genus one models, as described in [Fis08], makes no assumption on the characteristic of \( k \). It would be interesting to see if it is possible to replace the formulas given above with expressions that make sense in every characteristic.

The reason we are interested in \( \Omega \)-matrices is that they can be used to give a formula for the Jacobian of the curve \( C \). More precisely, we have the following.

**Theorem 3.3.5 (The formula for the Jacobian).** Let \( C/k \) be a genus one normal curve of degree \( n \), where \( n \geq 3 \) is an odd integer, and let \( \omega \) be an invariant differential of \( C \). Let \( F_\bullet \) be a genus one model of \( I(C) \), and let \( \Omega \) be the \( \Omega \)-matrix associated to \( F_\bullet \). Then the Jacobian \( E \) of \( C \) is defined by the Weierstrass equation \( W \)

\[ y^2 = x^3 - 27c_4(\Omega)x + 54c_6(\Omega), \]

where \( c_4(\Omega) \) and \( c_6(\Omega) \) are defined as above. Moreover, there is a \( \bar{k} \)-isomorphism \( \gamma : C \to E \) such that, for each \( i \neq j \),

\[ \gamma^*(3dx/y) = \frac{x^2 d(x_i/x_j)}{\Omega_{ij}}. \]

The proof of this result will require complex analytic methods, and will be given in Chapter 5.

**Remark 3.3.6.** In [Fis18], a different definition of the \( \Omega \)-matrix associated to a genus one curve is given, and the analogue of Theorem 3.3.5 is shown to hold for all values of \( n \), without the restriction that \( n \) is odd. We expect that the two definitions are equivalent. It is possible to check this is true for small values of \( n \) by a generic calculation, but we still haven’t found a proof that works for all \( n \). We also expect that, with more work, one should be able to extend our proof of Theorem 3.3.5 to even values of \( n \).

**Remark 3.3.7.** The invariants \( c_4 \) and \( c_6 \) of a Weierstrass equation of \( E \) can also be viewed as functions on pairs \((E, \omega)\), where \( \omega \) is a regular differential on \( E \) - this follows from the change-of-variable formulas for the Weierstrass equations, given in Chapter III of [Sil09]. We can extend \( c_4 \) and \( c_6 \) to functions on pairs \((C, \omega)\), where \( C \) is a genus one curve and \( \omega \) is a regular differential on \( C \) - choose a \( \bar{k} \)-isomorphism \( \gamma : E \to C \), and define \( c_k(C, \omega) = c_k(E, \gamma^*\omega) \). One then checks that this is well-defined i.e. independent of the choice of \( \gamma \).
We want to check that for any $g \in \text{GL}_m$ the following equation holds.

$$
\sum x_{b_1}^* \wedge x_{b_2}^* \wedge \ldots \wedge x_{b_{m-n+2}}^* \otimes \Omega'_{a_1,\ldots,a_{n-2}}(x_1,\ldots,x_m)
= \det(g) \sum g \cdot (x_{b_1}^* \wedge x_{b_2}^* \wedge \ldots \wedge x_{b_{m-n+2}}^* \otimes \Omega_{a_1,\ldots,a_{n-2}}(x_1,\ldots,x_m))
$$

where the matrix $\Omega'$ is associated to the resolution model $F'_\bullet$, with the differentials specified by

$$
\phi'(x_1,\ldots,x_m) = \phi_r(x'_1,\ldots,x'_m),
$$

where $x'_j = \sum_{i=1}^m g_{ij} x_i$.

First, note that the group $\text{GL}_m$ is generated by permutation matrices, diagonal matrices and matrices of the form $I + tE_{21}$. Thus it suffices to prove our result for $g$ of this form.

Let us first consider the case where $g$ is diagonal, with $g_{ii} = \lambda_i$. By the chain rule, we have

$$
[a_1, a_2, \ldots, a_{n-2}]F'_\bullet = \lambda_1 \cdots \lambda_{a_{n-2}}[a_1, a_2, \ldots, a_{n-2}]F'_\bullet.
$$

The action of $g$ on the $\Lambda^{m-n+2}V$ component is given by

$$
g \cdot (x_{b_1}^* \wedge x_{b_2}^* \wedge \ldots \wedge x_{b_{m-n+2}}^*) = (\lambda_{b_1} \cdots \lambda_{b_{m-n+2}})^{-1} x_{b_1}^* \wedge x_{b_2}^* \wedge \ldots \wedge x_{b_{m-n+2}}^*,
$$

while $g \cdot \Omega_{a_1,\ldots,a_{n-2}}(x_1,\ldots,x_m) = \Omega_{a_1,\ldots,a_{n-2}}(x'_1,\ldots,x'_m)$. Observing that

$$
\det(g) = (\lambda_1 \cdots \lambda_{a_{n-2}})(\lambda_{b_1} \cdots \lambda_{b_{m-n+2}}),
$$

the claim follows by the definition of $\Omega'$. We next consider the case in which $g$ is a permutation matrix. We need a few preliminary lemmas.

**Lemma 3.4.1.** If $2 \leq r \leq n - 3$ then

$$
[a_1, \ldots, a_r, a_{r+1}, \ldots, a_{n-2}] = -[a_1, \ldots, a_{r+1}, a_r, \ldots, a_{n-2}].
$$

**Proof.** For this range of $r$, both $\phi_r$ and $\phi_{r+1}$ are matrices of linear forms. We differentiate the relation $\phi_r \phi_{r+1} = 0$. By the Leibniz rule,

$$
0 = \frac{\partial^2(\phi_r \phi_{r+1})}{\partial x_{a_r} \partial x_{a_{r+1}}} = \frac{\partial \phi_r}{\partial x_{a_r}} \frac{\partial \phi_{r+1}}{\partial x_{a_{r+1}}} + \frac{\partial \phi_r}{\partial x_{a_{r+1}}} \frac{\partial \phi_{r+1}}{\partial x_{a_r}}.
$$

3.4 $\Omega$-quadrics and changes of coordinates

3.4.1 The proof of Proposition 3.2.3

We now prove Proposition 3.2.3. We’ve learned of this argument from an unpublished note of Tom Fisher. Let $F'_\bullet$ be a resolution model. Recall that the symbols $[a_1, \ldots, a_{n-2}]$ are defined by

$$
[a_1, a_2, \ldots, a_{n-2}] = \frac{\partial \phi_1}{\partial x_{a_1}} \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \frac{\partial \phi_{n-2}}{\partial x_{a_{n-2}}}.
$$

With this in mind, we can also view $c_k(F'_\bullet)$, as defined in terms of $\Omega$-matrices, as functions on pairs $(C, \omega)$, and Theorem 3.3.5 can be interpreted as saying they agree with $c_k$ defined in terms of the Weierstrass equation.
hence the desired relation.

**Remark 3.4.2.** The lemma holds only for $2 \leq r \leq n - 3$, i.e. it is not in general true that $[a_1, a_2, \ldots, a_{n-2}] = -[a_2, a_1, \ldots, a_{n-2}]$. This is the reason we introduce symbols $[[a_1, a_2, \ldots, a_{n-2}]]$, and in Lemma 3.4.5 we show that they do have this property for all $r$.

**Lemma 3.4.3.** We have $[a_1, a_2, \ldots, a_{n-2}] = \pm [a_{n-2}, a_{n-3}, \ldots, a_1]$, where the sign is $+1$ if $n \equiv 2, 3 \pmod{4}$ and $-1$ if $n \equiv 0, 1 \pmod{4}$.

**Proof.** This follows from the self-duality of the resolution, by Lemma 2.2.9, and our sign convention for the dual complex.

**Lemma 3.4.4.** If the terms indicated by $\ldots$ are the same in each case then

(i) $[a, \ldots, b] + [b, \ldots, a] = 0$, and

(ii) $[a, b, \ldots, c, d] + [b, a, \ldots, c, d] + [a, b, \ldots, d, c] + [b, a, \ldots, d, c] = 0$.

**Proof.** Part (i) follows from Lemma 3.4.1 and 3.4.3. For the second part, as $\phi_1 \phi_2 = 0$ and $\phi_{n-3} \phi_{n-2} = 0$, we have

$$0 = \frac{\partial^2 (\phi_1 \phi_2)}{\partial x_a \partial x_b} = \frac{\partial \phi_1}{\partial x_a} \frac{\partial \phi_2}{\partial x_b} + \frac{\partial \phi_1}{\partial x_b} \frac{\partial \phi_2}{\partial x_a} + \frac{\partial^2 \phi_1}{\partial x_a \partial x_b} \phi_2,$$

and similarly,

$$0 = \frac{\partial^2 (\phi_{n-3} \phi_{n-2})}{\partial x_c \partial x_d} = \frac{\partial \phi_{n-3}}{\partial x_c} \frac{\partial \phi_{n-2}}{\partial x_d} + \frac{\partial \phi_{n-3}}{\partial x_d} \frac{\partial \phi_{n-2}}{\partial x_c} + \phi_{n-3} \frac{\partial^2 \phi_{n-2}}{\partial x_c \partial x_d}.$$
and \([a_3, a_4, \ldots, a_{n-2}, a_1, a_2]\). We treat them together. By repeatedly using Lemma 3.4.1 to move \(a_3\) to the right, we have

\[
[a_2, a_1, a_3, \ldots, a_{n-2}] = (-1)^n[a_2, a_1, a_4, \ldots, a_3, a_{n-2}],
\]

and similarly

\[
[a_3, a_4, \ldots, a_{n-2}, a_2, a_1] = -[a_1, a_4, \ldots, a_{n-2}, a_2, a_3] = (-1)^n[a_1, a_2, a_4, \ldots, a_{n-2}, a_3]
\]

where the first equality is a consequence of Lemma 3.4.1(i) and the second is a repeated application of Lemma 3.4.1. By Lemma 3.4.4(ii), we find that

\[
(-1)^n(\{a_2, a_1, a_4, \ldots, a_3, a_{n-2}\} + \{a_1, a_2, a_4, \ldots, a_{n-2}, a_3\})
\]

\[
= (-1)^{n-1}(\{a_1, a_2, a_4, \ldots, a_{n-3}, a_3, a_{n-2}\} + \{a_2, a_1, a_4, \ldots, a_{n-2}, a_3\})
\]

and this is equal, by Lemma 2.5.1 and repeated application of Lemma 2.3, to

\[
-[a_1, a_2, \ldots, a_{n-2}] - [a_3, a_4, \ldots, a_m, a_1, a_2].
\]

Thus we are done in the case \(\tau = (12)\). Also note that the lemma holds for \(\sigma^2\), for \(\sigma = (12\ldots n - 2)\). If \(n\) is odd, \(\sigma^2\) and \(\tau\) generate \(S_{n-2}\) and we are done. For even \(n\), \(S_{n-2}\) is generated by \(\sigma^2\), \(\tau\) and (23), and a similar argument as for \(\tau\) shows that the lemma is true for (23).

We remark here that if \(n\) is odd, using \(\sigma\) instead of \(\sigma^2\) would make no difference in the definition of \([[\ldots]]\), but for even \(n\) would result in an expression that is identically zero.

We now proceed to prove Proposition 3.2.3 for permutation matrices. It suffices to prove the claim for \(\tau = (ab)\) a transposition, with \(a < b\). Write \(\Omega \in \Lambda^{m-n+2}V \otimes S^2V\) as

\[
\sum x_{b_1}^* \wedge x_{b_2}^* \wedge \ldots \wedge x_{b_{m-n+2}}^* \otimes \Omega_{a_1, \ldots, a_{n-2}}.
\]

Then \(\Omega'\) is given by

\[
\sum x_{\tau(b_1)}^* \wedge x_{\tau(b_2)}^* \wedge \ldots \wedge x_{\tau(b_{m-n+2})}^* \otimes \Omega_{\tau(a_1), \ldots, \tau(a_{n-2})}.
\]

We look at the terms of this sum individually. If either both \(a, b \in \{a_1, a_2, \ldots, a_{n-2}\}\) or both \(a, b \notin \{a_1, a_2, \ldots, a_{n-2}\}\), then

\[
x_{\tau(b_1)}^* \wedge x_{\tau(b_2)}^* \wedge \ldots \wedge x_{\tau(b_{m-n+2})}^* \otimes \Omega_{\tau(a_1), \ldots, \tau(a_{n-2})} = -x_{b_1}^* \wedge x_{b_2}^* \wedge \ldots \wedge x_{b_{m-n+2}}^* \otimes \Omega_{a_1, \ldots, a_{n-2}},
\]

by Lemma 3.4.5. The terms with \(a \in \{b_1, \ldots, b_{m-n+2}\}\) and \(b \in \{a_1, \ldots, a_{n-2}\}\) are mapped by \(\tau\) to terms with \(a \in \{a_1, \ldots, a_{n-2}\}\) and \(b \in \{b_1, \ldots, b_{m-n+2}\}\), and vice versa, with a minus sign in front as the permutation \((\tau(b_1), \ldots, \tau(b_{m-n+2}), \tau(a_1), \ldots, \tau(a_{n-2}))\) is now odd. Therefore the conclusion of the theorem holds for permutation matrices.

We are left with the case \(g = I + tE_{21}\). As before, we set \(x_i' = g \cdot x_i\). Note that \(g^{-T} = I - tE_{12}\),
and hence \( g \cdot x_i^* = x_2 - tx_1 \) and \( g \cdot x_i^* = x_i^* \) for \( i \neq 2 \). We need to check that the following equation holds:

\[
\sum g \cdot \left( x_{i_1}^* \land x_{i_2}^* \land \ldots \land x_{i_{m-2}}^* \land \Omega_{\alpha_1,\ldots,\alpha_{n-2}}(x_1,\ldots,x_m) \right) = \sum x_{i_1}^* \land x_{i_2}^* \land \ldots \land x_{i_{m-2}}^* \land \Omega'_{\alpha_1,\ldots,\alpha_{n-2}}(x_1,\ldots,x_m).
\]

(\ast)

We have two possibilities for the action of \( g \) on each term of the sum. If either \( 2 \not\in \{b_1,\ldots,b_{m-2}\} \), or \( \{2,1\} \subset \{b_1,\ldots,b_{m-2}\} \), then

\[
g \cdot (x_{i_1}^* \land x_{i_2}^* \land \ldots \land x_{i_{m-2}}^*) = x_{i_1}^* \land x_{i_2}^* \land \ldots \land x_{i_{m-2}}^*.
\]

otherwise, we have

\[
g \cdot (x_{i_1}^* \land x_{i_2}^* \land \ldots \land x_{i_{m-2}}^*) = x_{i_1}^* \land \ldots \land (x_2^* - tx_1^*) \land \ldots \land x_{i_{m-2}}^*.
\]

Equating the coefficients in (\ast), it suffices to prove that

(i) If either one of \( 2 \not\in \{a_1,\ldots,a_{n-2}\} \) or \( \{2,1\} \subset \{a_1,\ldots,a_{n-2}\} \) holds, then

\[
\Omega'_{\alpha_1,\ldots,\alpha_{n-2}}(x_1,\ldots,x_m) = \Omega_{\alpha_1,\ldots,\alpha_{n-2}}(x_1',\ldots,x_m').
\]

(ii) Otherwise, if \( a_k = 2 \) and \( 1 \not\in \{a_1,\ldots,a_{n-2}\} \), then we have

\[
\begin{align*}
\Omega'_{\alpha_1,\ldots,a_{k-1},2,a_{k+1},\ldots,a_{n-2}}(x_1,\ldots,x_m) &= \\
\Omega_{\alpha_1,\ldots,a_{k-1},2,a_{k+1},\ldots,a_{n-2}}(x_1',\ldots,x_m') + t \cdot \Omega_{\alpha_1,\ldots,a_{k-1},1,a_{k+1},\ldots,a_{n-2}}(x_1',\ldots,x_m').
\end{align*}
\]

Here we used the fact that switching the places of 1 and 2 changes the sign of the permutation \( (b_1,\ldots,b_{m-2},a_1,\ldots,a_{n-2}) \), since it is the same as multiplying with the transposition \( (1,2) \).

The maps \( \phi' \) are given by

\[
\phi'_r(x_1,\ldots,x_m) = \phi_r(x_1 + tx_2,x_2,\ldots,x_m).
\]

So by the chain rule

\[
\frac{\partial \phi'_r}{\partial x_2}(x_1,\ldots,x_m) = \left( \frac{\partial \phi_r}{\partial x_2} + t \frac{\partial \phi_r}{\partial x_1} \right)(x_1 + tx_2,x_2,\ldots,x_m),
\]

and for \( j \neq 2 \)

\[
\frac{\partial \phi'_r}{\partial x_j}(x_1,\ldots,x_m) = \frac{\partial \phi'_r}{\partial x_j}(x_1',\ldots,x_m').
\]

Therefore, if \( 2 \not\in \{a_1,\ldots,a_{n-2}\} \),

\[
[[a_1,\ldots,a_{n-2}]](x_1,\ldots,x_m) = [[a_1,\ldots,a_{n-2}]](x_1',\ldots,x_m').
\]
3.4. $\Omega$-QUADRICS AND CHANGES OF COORDINATES

and this is exactly (i). If on the other hand $a_k = 2$, then

$$[[a_1, \ldots, a_{k-1}, 2, a_{k+1}, \ldots, a_{n-2}]](x_1, \ldots, x_m) = [[a_1, \ldots, a_{k-1}, 2, a_{k+1}, \ldots, a_{n-2}]](x'_1, \ldots, x'_m) + t[[a_1, \ldots, a_{k-1}, 1, a_{k+1}, \ldots, a_{n-2}]](x'_1, \ldots, x'_m).$$

Note that if we have $1 \in \{a_1, \ldots, a_{n-2}\}$, then the term $[[a_1, \ldots, a_k, 1, a_{k+2}, \ldots, a_{n-2}]]$ vanishes, as 1 appears twice, by Lemma 3.4.5. This completes the proof of (ii), and hence the proof of Proposition 3.2.3.

3.4.2 The invariant differential under changes of coordinates

In this section we study how the differential $\omega$ associated to an $\Omega$-matrix behaves under changes of coordinates. The following lemma is a generalization of Proposition 5.19 of [Fis08], and immediately implies part (i) of Lemma 3.3.2.

**Lemma 3.4.6.** Let $C$ be a genus one normal curve of degree $n$, let $F_\ast$ be a free resolution of $R/I(C)$, and consider the associated quadrics $[a_1, \ldots, a_{n-2}]$. Then, for $i, j, a_1, \ldots, a_{n-2}$ an even permutation of $1, 2, \ldots, n$ and $\tau \in S_n$, we have the following equality of rational differential forms on $C$

$$\frac{x^2 d(x_j/x_i)}{[a_1, \ldots, a_{n-2}]} = \text{sgn}(\tau) \frac{x^2_{\tau(j)} d(x_\tau(i)/x_\tau(j))}{[\tau(a_1), \ldots, \tau(a_{n-2})]}.$$

**Proof.** To make notation clearer, we can assume $i = 1$, $j = 2$ and $a_k = k + 2$ for each $k$. It suffices to prove the lemma for the transpositions $(k, k+1)$, for $1 \leq k \leq n-1$, as they generate $S_n$. By Lemma 3.4.1, when $\tau = (k, k+1)$ and $4 \leq k \leq n-2$, we have

$$[3, \ldots, k, (k+1), \ldots, n] = -[3, \ldots, (k+1), k, \ldots, n],$$

so it is clear the conclusion holds for these transpositions. We thus only have to check the symmetries $(1, 2)$, $(2, 3)$ and $(n-1, n)$. The symmetry $(12)$ follows from the identity

$$x^2 d(x_2/x_1) = -x^2 d(x_1/x_2).$$

For the transposition $(n-1, n)$, observe that by differentiating the relation $\phi_{n-3}\phi_{n-2} = 0$ with respect to $x_{n-1}$ and $x_n$, we obtain

$$\frac{\partial \phi_1 }{\partial x_3} \frac{\partial \phi_2 }{\partial x_4} \cdots \frac{\partial \phi_{n-4} }{\partial x_{n-2}} \frac{\partial \phi_{n-3} }{\partial x_{n-1}} \frac{\partial \phi_{n-2} }{\partial x_n} + \frac{\partial \phi_{n-3} }{\partial x_n} \frac{\partial \phi_{n-2} }{\partial x_{n-1}} = \frac{\partial \phi_1 }{\partial x_3} \frac{\partial \phi_2 }{\partial x_4} \cdots \frac{\partial \phi_{n-4} }{\partial x_{n-2}} \frac{\partial \phi_{n-3} }{\partial x_{n-1}} \frac{\partial \phi_{n-2} }{\partial x_n}.$$

Using the relation $\phi_r \frac{\partial \phi_{r+1} }{\partial x_p} = -\frac{\partial \phi_r }{\partial x_p} \phi_{r+1}$, this is equal to

$$\pm \phi_1 \frac{\partial \phi_2 }{\partial x_3} \cdots \frac{\partial \phi_{n-4} }{\partial x_{n-2}} \frac{\partial \phi_{n-3} }{\partial x_{n-1}} \frac{\partial \phi_{n-2} }{\partial x_n}.$$

As entries of $\phi_1$ are in $I(C)$, the above expression is also in $I(C)$ and hence vanishes on $C$. The case $\tau = (34)$ follows from this case and the Lemma 3.4.3. We are left with the case $\tau = (2, 3)$.
Using Euler’s identity, we compute
\[
\sum_{i=1}^{n} d(x_i/x_1) \frac{\partial \phi_1}{\partial x_i} = \sum_{i=1}^{n} \frac{dx_i x_1 - x_i dx_1}{x_1^2} \frac{\partial \phi_1}{\partial x_i} = \frac{d\phi_1}{x_1} - \frac{\phi_1 dx_1}{x_1^2} = 0 \mod I(C),
\]
and hence
\[
0 = \left( d(x_i/x_1) \sum_{i=1}^{n} \frac{\partial \phi_1}{\partial x_i} \right) \frac{\partial \phi_2 \partial \phi_3 \cdots \partial \phi_{n-2}}{\partial x_4 \partial x_5 \cdots \partial x_n} \mod I(C)
\]
\[
= \sum_{i=2}^{n} d(x_i/x_1)[i, 4, 5, \ldots, n] \mod I(C).
\]
From Lemma 3.4.1 we deduce \([i, 4, 5, \ldots, n] = 0\) for \(4 < i < n\). By Lemma 3.4.4(i), we have \([n, 4, 5, \ldots, n] = 0\). Furthermore, the term with \(i = 4\) is zero \(\mod I(C)\). This is because we have, reasoning in the same way as in the case \((n - 1, n)\),
\[
2 \frac{\partial \phi_1 \partial \phi_2}{\partial x_2 \partial x_4} \cdots \frac{\partial \phi_{n-2}}{\partial x_n} d(x_2/x_1) + \frac{\partial \phi_1 \partial \phi_2}{\partial x_3 \partial x_4} \cdots \frac{\partial \phi_{n-2}}{\partial x_n} d(x_3/x_1) = 0,
\]
and we are done. \(\square\)

**Lemma 3.4.7.** With notation as in previous lemma, we have the equality of differential forms on \(C\),
\[
x_i^2 d(x_i/x_j) = (n - 2) \frac{x_i^2 d(x_i/x_j)}{[a_1, \ldots, a_{n-2}]/[[a_1, \ldots, a_{n-2}]]}.
\]

**Proof.** This follows from the definition of the symbol \([[]]\)
\[
[[a_1, a_2, \ldots, a_{n-2}]] = \sum_{k=1}^{n-2} [a_{\sigma^{2k}(1)}, a_{\sigma^{2k}(2)}, \ldots, a_{\sigma^{2k}(n-2)}],
\]
where \(\sigma\) is the \((n - 2)\)-cycle \((1, 2, \ldots, n - 1)\), and the previous lemma. \(\square\)

**Lemma 3.4.8.** Let \(C\) and \(C'\) be genus one normal curves in \(\mathbb{P}^{n-1}\). Suppose \(g \in \text{GL}_n\) takes \(C'\) to \(C\), and let \(x'_j = \sum_{i=1}^{n} g_{ij} x_i\). Fix a minimal free resolution \(F\) of \(I(C)\) and let \(F'\) be the resolution of \(I(C')\), such that the boundary maps \(\phi'\) and \(\phi'_r\) satisfy
\[
\phi'_r(x_1, \ldots, x_n) = \phi_r(x'_1, \ldots, x'_n).
\]
Then, for \(i \neq j\) we have the equality of rational differential forms on \(C'\)
\[
g^*(\frac{x_i^2 d(x_i/x_j)}{\Omega_{C,ij}}) = \det(g) \frac{x_i^2 d(x_i/x_j)}{\Omega_{C',ij}}.
\]
3.5. Ω-QUADRICS AND STRUCTURE CONSTANTS OF ALGEBRAS

Proof. We wish to prove the equality

\[(x'_jdx'_i - x'_i dx'_j)(\Omega_C)_{ij}(x_1, \ldots, x_n) \equiv \text{det}(g)(x_jdx_i - x_idx_j)(\Omega_C)_{ij}(x'_1, \ldots, x'_n)\]

It suffices to check the lemma for a set of generators of $\text{GL}_n$. When $g$ is a diagonal matrix or $g = I + tE_{21}$, the claim follows from Proposition 3.2.3. When $g$ is a permutation matrix, the claim follows from Lemma 3.4.6.

3.5 Ω-quadrics and structure constants of algebras

Let $n \geq 3$ be an integers, and let $X \subset \mathbb{P}^{n-2}$ be a set of $n$ points in general position, defined over a field $k$. Note that $X$ is an affine variety, and so we can associate to $X$ an $n$-dimensional $k$-algebra $A$ in a natural way, by taking the ring $\Gamma(X, \mathcal{O}_X)$ of regular functions defined on all of $X$.

In this section we study the connection between the invariant theory of a resolution model of $X$ and the algebra $A$. Our main result is Theorem 3.5.7. We show that a resolution model of $X$ determines in a natural way a basis $\alpha_1, \ldots, \alpha_n$ of $A$. The structure constants of this basis are elements $c^k_{ij} \in k$ that determine the multiplication on $A$ via $\alpha_i \alpha_j = \sum_{k=1}^n c^k_{ij} \alpha_k$. We further prove, as Corollary 3.5.10, an (unpublished) conjecture of Tom Fisher, and express the structure constants in terms of the $\Omega$-quadrics of the resolution model.

A key feature of our construction is that when $k = \mathbb{Q}$ and the resolution model has integral coefficients, the associated structure constants will be integral, and hence actually determine an order $B$ in the algebra $A$. We thus obtain a formula for the discriminant of this order in terms of $\Omega$-quadrics, and this fact plays an important role in the proof of Theorem 1.0.1.

Theorem 3.5.7 is closely related to parametrizations of rings of rank $n$, when $n \leq 5$. Indeed, a resolution model of degree 3 is just a binary cubic, and similarly resolution models of degree 4 and 5 can be represented by a pair of ternary quadrics and an alternating matrix of quaternary linear forms respectively.

It is well known how to associate a ring of rank $n$ to this data - for $n = 3$ this is a classical result, due to Delone and Faddeev [DF], and for $n = 4$ and $n = 5$, due to Bhargava [Bha04], [Bha08]. Our construction can be viewed as a generalization of these parametrizations to all values of $n$. Note that the order $B$ we construct is slightly different from the one obtained in these parametrizations - this is due to a difference in the way we normalize the basis of the order. As a consequence, $B$ is never a maximal order - see Remark 3.5.13.

It is of interest to us to obtain the largest order possible, as this will allow us to obtain sharper bounds in Theorem 1.0.1. In Section 3.8 we give a modification of our construction for all odd $n \geq 3$, that when specialized to $n = 3$ and $n = 5$ recovers the results of Delone-Faddeev and Bhargava.

Equivalence between non-degenerate algebras and sets of $n$ points in $\mathbb{P}^{n-2}$. We give here a slightly different perspective on the classical fact that there is an equivalence of categories between the category of finite sets of points with a continuous action of the absolute Galois group, and the category of finite dimensional étale algebras. These ideas feature prominently in the
aforementioned papers of Bhargava, as well as the work of his students Wood [Woo] and Wilson [Wil13], and also appear in the work of Casnati and Edelhoch [CE96].

Let $\mathcal{X} = \{ X \subset \mathbb{P}^{n-2} : X \text{ is a set of } n \text{ points in general position} \}$. There is a natural action of the group $\text{PGL}_{n-1}(k)$ on the set $\mathcal{X}$.

We say an $n$-dimensional commutative $k$-algebra $A$ is non-degenerate if the trace form associated to $A$ is non-degenerate. This is equivalent to requiring that $A$ is étale over $k$, or that there exists an isomorphism $A \otimes_k \bar{k} \cong \bar{k}^n$. Let $\mathcal{A}$ be the set of isomorphism classes of $n$-dimensional, non-degenerate $k$-algebras.

The ring $A = \Gamma(X, \mathcal{O}_X)$ of global functions on a set of $n$ points $X \in \mathcal{X}$ is a non-degenerate $k$-algebra, of dimension $n$ as $X$ has degree $n$, and so we obtain a map $\mathcal{X} \to \mathcal{A}$. Any two elements of $\mathcal{X}$ that lie in the same $\text{PGL}_{n-1}(k)$-orbit of $\mathcal{X}$ have isomorphic rings of global functions, and so map to the same element of $\mathcal{A}$.

The following fact seems to be well-known, but we could not find an adequate reference.

**Proposition 3.5.1.** Let $\mathcal{A}$ be the set of isomorphism classes of non-degenerate $n$-dimensional $k$-algebras. The map $X \mapsto \Gamma(X, \mathcal{O}_X)$ induces a bijection between the set of $\text{PGL}_{n-1}$-orbits of $\mathcal{X}$ and the set $\mathcal{A}$.

We will prove this by constructing an inverse map, see discussion after the proof of Lemma 3.5.6. We need a few preliminary results.

**Lemma 3.5.2.** Let $A$ be a non-degenerate $n$-dimensional $k$-algebra. Let $M$ be a locally free $A$-module of rank 1, i.e. an invertible module. Then $M$ is free, i.e. it is isomorphic to $A$ as an $A$-module.

*Proof.* As $A$ is non-degenerate, as an algebra it is isomorphic to a direct product of fields, and we have $A \cong A_1 \times \cdots \times A_k$. For each $1 \leq i \leq k$, let $e_i$ be the idempotent corresponding to the factor $A_i$, so that $\sum_{i=1}^k e_i = 1$, $A e_i \cong A_i$ as an $A$-module, $e_i^2 = e_i$ and $e_i e_j = 0$ for any distinct $i$ and $j$.

Then we have the decomposition $M = e_1 M \oplus e_2 M \oplus \cdots \oplus e_k M$, where each module $e_i M$ is an $A_i$-vector space. Since $M$ is locally free of rank 1, each $e_i M$ is 1-dimensional, and we choose a basis vector $f_i$. It follows that we have $M = Af \cong A$, where $f = \sum_{i=1}^k f_i$. \qed

Following [Bha08] and [CE96], we give a canonical way to define an inverse to the map $X \mapsto A$. We assume $n \geq 3$. Given an $n$-dimensional $k$-algebra $A$, consider the $A$-module $\text{Hom}_k(A, k)$. When $A$ is non-degenerate, $\text{Hom}_k(A, k)$ is isomorphic to $A$ as an $A$-module, with the isomorphism given by the map $x \mapsto (y \mapsto \text{Tr}_k^A(xy))$.

Fix a basis $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ of $A$, with $1 = \alpha_0$ and $\text{Tr}_k^A(\alpha_i) = 0$, and let $\alpha_0^*, \alpha_1^*, \ldots, \alpha_{n-1}^*$ be the basis of $K$ dual to $\alpha_0, \ldots, \alpha_{n-1}$ with respect to the trace pairing, i.e. we have $\text{Tr}_k^A(\alpha_i \alpha_j^*) = \delta_{ij}$ for all $0 \leq i, j \leq n-1$.

**Definition 3.5.3.** We define $\phi_A : \text{Spec } A \to \mathbb{P}^{n-2}$ to be the embedding induced by $\alpha_1^*, \ldots, \alpha_{n-1}^*$, viewed as a basis of the $(n-1)$-dimensional $k$-subspace $V := \{ f \in \text{Hom}_k(A, k) : f(1) = 0 \}$ of the $A$-module $\text{Hom}_k(A, k)$, via the isomorphism provided by the trace pairing.

Note that this definition requires a choice of basis of $V$. 


Example 3.5.4. Suppose $A = K$ is a number field of degree $n$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of $K$ into $\mathbb{C}$, and let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be a basis of $K$ as above. The set $X$ of $\mathbb{C}$-points of the image of $\phi_A$ is the set

$$X = \{ (\sigma_i(\alpha_j^*) : \sigma_i(\alpha_2^*) : \ldots : \sigma_i(\alpha_{n-1}^*)) \in \mathbb{P}^{n-2}(\mathbb{C}) : 1 \leq i \leq n-1 \}.$$

Remark 3.5.5. We can interpret $\phi_A$ as the map into projective space arising from a certain line bundle on $\text{Spec } A$. In our setting, by Lemma 3.5.2, every line bundle on $\text{Spec } A$ is trivial. However one can generalize the definition of $\phi_A$ to more general rings. For example, if $A = O_K$ is the maximal order of a number field, then $\alpha_1^*, \ldots, \alpha_{n-1}^*$ are elements of the inverse different ideal of $O_K$, and can be viewed as sections of the corresponding line bundle on $\text{Spec } O_K$, and this line bundle is not necessarily trivial.

Lemma 3.5.6. Let $X \subset \mathbb{P}^{n-2}$ be a set of $n$ points, defined over $k$, that is not contained in any hyperplane. Then $X$ is in general position if and only if it arises as the image of the map $\phi_A$, where $A = \Gamma(X, O_X)$ is the ring of global functions on $X$.

Proof. Since $X$ is an affine scheme, the embedding $X \subset \mathbb{P}^{n-2}$ is determined by an $A$-module $M$ that is locally free of rank 1, together with a set of elements $l_1, \ldots, l_{n-1} \in M$. Since $X$ is not contained in any hyperplane, $l_1, \ldots, l_{n-1}$ are linearly independent over $k$. By Lemma 3.5.2, we may assume $M = A$. To prove the claim, we need to show that there exists an element $\lambda \in A^*$ such that $\lambda_1, \ldots, \lambda_{n-1}$ is a basis for the set of trace zero elements of $A$, if and only if $X$ is in general position.

Observe that $\text{Tr}_k^A(\lambda \cdot l_i) = 0$ for $i = 1, \ldots, n-1$ is a set of $n-1$ linear conditions on $\lambda$. As $A$ is $n$-dimensional, there exists a non-zero $\lambda \in A$ that satisfies them. It suffices to show that $\lambda \in A^*$ if and only if $X$ is in general position.

To check this, we may extend scalars and replace $A$ by $A \otimes \bar{k}$ so that $A \cong \bar{k}^n$. Suppose $l_i = (a_{i1}, \ldots, a_{in})$ for $1 \leq i \leq n-1$, and $\lambda = (\lambda_1, \ldots, \lambda_n)$. The coordinates of the points $P_1, \ldots, P_n$ are the columns of the following $(n-1) \times n$-matrix:

$$P = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \ldots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \ldots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \ldots & a_{n-1,n-1} & a_{n-1,n} \end{pmatrix}$$

Since $l_i$ are $k$-linearly independent, $P$ has rank $n-1$. The set $X$ is not in general position if and only if some $(n-1) \times (n-1)$-minor of the above matrix $P$ vanishes, and $\lambda \notin A^*$ if and only if $\lambda_i \neq 0$ for some $i$. Since we have $0 = \text{Tr}(\lambda l_i) = \sum_{j=1}^n \lambda_j a_{ij}$ for all $i$, we see that $P \cdot (\lambda_1, \ldots, \lambda_n)^T = 0$. Thus $(\lambda_1, \ldots, \lambda_n)$ is a non-zero scalar multiple of the row vector of minors, and the lemma follows.

We can now finish the proof of Proposition 3.5.1. First, note that the map $\mathcal{X} \to A$ is surjective, since for any algebra $A \in \mathcal{A}$, the image of $\phi_A$ is a set $X \in \mathcal{X}$, with ring of functions isomorphic to $A$. Furthermore, if $X_1$ and $X_2$ both map to $A$, by the above lemma both $X_1$ and
$X_2$ are embedded in $\mathbb{P}^{n-2}$ via $\phi_A$, with (possibly) different choices of bases for the trace zero subspace $V$ in Definition 3.5.3. Hence there exists an element of $\text{PGL}_n(k)$ taking $X_1$ to $X_2$.

The main result of this section is the following theorem giving an expression for the structure constants of the algebra $A$ in terms of the $\Omega$-quadrics of the set $X$.

**Theorem 3.5.7.** Let $A$ be an $n$-dimensional non-degenerate $k$-algebra. Fix a basis $\alpha_1, \ldots, \alpha_{n-1}$ of the trace zero subspace of $A$, and let $X \subset \mathbb{P}^{n-2}$ be the image of $\text{Spec} \ A$ under the map $\phi_A$. Then, if $\Omega_1, \ldots, \Omega_{n-1}$ are the $\Omega$-quadrics associated to a resolution model of $X$, there exists a non-zero scalar $\lambda$ such that we have

$$\alpha_i \alpha_j = c^0_{ij} + \sum_{k=1}^{n-1} \lambda \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \alpha_k,$$

for some $c^0_{ij} \in k$, for all $1 \leq i, j, k \leq n-1$.

The proof will require the following lemma, the proof of which is postponed to the next section.

**Lemma 3.5.8.** Let $X \subset \mathbb{P}^{n-2}$ be set of $n$ points in general position. Suppose that the set $X(\bar{k})$ consists of points $P_1 = (1 : 0 : \ldots : 0), P_2 = (0 : 1 : 0 : \ldots : 0), \ldots, P_{n-1} = (0 : 0 : \ldots : 0 : 1)$ and $P_n = (1 : 1 : \ldots : 1)$. There exists a $\lambda \in k$, for which the following holds. For every permutation $\tau = (a_1, \ldots, a_{n-1})$ of $(1, 2, \ldots, n-1)$, we have the identity

$$[a_1, \ldots, a_{n-2}] = \lambda \cdot \text{sgn}(\tau)(x_{a_{n-1}} - x_{a_1} - x_{a_{n-2}})x_{a_{n-1}},$$

where the symbols $[\ldots]$ are as defined in Section 3.2.

This lemma allows us to compute the $\Omega$-quadrics associated to $X$.

**Lemma 3.5.9.** Let $X \subset \mathbb{P}^{n-2}$ be a set of $n$ points as in the previous lemma. The quadrics $\Omega_i$ are given, up to an overall scalar, by $\Omega_i = n x_i^2 - 2x_i \sum_{j=1}^{n-1} x_j$, for all $1 \leq i \leq n-1$.

**Proof.** By definition, $\Omega_i = (-1)^i[[1, \ldots, \hat{i}, \ldots, n-1]]$, with the double square bracket symbol given by

$$[[a_1, a_2, \ldots, a_{n-2}]] = \sum_{k=1}^{n-2} [a_{\sigma^2k(1)}, a_{\sigma^2k(2)}, \ldots, a_{\sigma^2k(n-2)}].$$

Recall that $\sigma$ is the $(n-2)$-cycle $(1, 2, \ldots, n-2)$ in $S_{n-2}$. Note that this is in cycle notation - i.e. we mean that $\sigma(i) = i + 1 \mod n - 2$. Let us suppose that $(a_1, \ldots, a_{n-1}) = (1, 2, \ldots, \hat{i}, \ldots, n -
1, i). We first consider the case when \( n \) is odd. Using Lemma 3.5.8, we compute

\[
\sum_{k=1}^{n-2} [a_{\sigma^k(1)}, a_{\sigma^k(2)}, \ldots, a_{\sigma^k(n-2)}] = \sum_{k=1}^{n-2} [a_{\sigma^k(1)}, a_{\sigma^k(2)}, \ldots, a_{\sigma^k(n-2)}] = \lambda \sum_{k=1}^{n-2} (-1)^i (x_{a_{\sigma^k(1)}} + x_{a_{\sigma^k(n-2)}} - x_i) x_i
\]

\[
= \lambda(-1)^i (2 \sum_{j=1}^{n-1} x_{a_j} - (n-2)x_i) x_i
\]

\[
= -\lambda(-1)^i (nx_i^2 - 2x_i \sum_{j=1}^{n-1} x_j).
\]

Since we are only computing \( \Omega_i \) up to an overall scalar, the factor \(-\lambda\) is not important, and we are done in this case. Now suppose \( n \) is even. Then we have \( \sigma^2 = (13 \ldots n - 1)(24 \ldots n - 4) \) - again in cycle notation. Accordingly, we compute

\[
\sum_{k=1}^{n-2} [a_{\sigma^{2k}(1)}, a_{\sigma^{2k}(2)}, \ldots, a_{\sigma^{2k}(n-2)}] = \lambda \sum_{k=1}^{n-2} (-1)^i (x_{a_{\sigma^{2k}(1)}} + x_{a_{\sigma^{2k}(n-2)}} - x_i) x_i
\]

\[
= \lambda(-1)^i (2 \sum_{j=1, j \text{ odd}}^{n-2} x_{a_j} + 2 \sum_{j=1, j \text{ even}}^{n-2} x_{a_j} - (n-2)x_i) x_i
\]

\[
= \lambda(-1)^i (2 \sum_{j=1}^{n-1} x_{a_j} - (n-2)x_i) x_i
\]

\[
= -\lambda(-1)^i (nx_i^2 - 2x_i \sum_{j=1}^{n-1} x_j)
\]

concluding the proof. \( \square \)

**Proof of Theorem 3.5.7.** We are free to extend the base field \( k \), and we assume \( k = \overline{k} \) is algebraically closed. For any basis \( \alpha_0, \ldots, \alpha_{n-1} \) of \( A \), the structure constants of \( A \) associated to this basis are defined to be \( c_{ij}^k \in k \), for \( 0 \leq i, j, k \leq n - 1 \), with \( \alpha_i \alpha_j = \sum_{k=0}^{n-1} c_{ij}^k \alpha_k \). We claim that under linear changes of coordinates, coefficients of \( \Omega \)-quadrics transform in the same way as the structure constants of an algebra, up to an overall scalar. Let \( V \) be the space of linear forms on \( \mathbb{P}^{n-2} \). Identifying \( \text{Spec} \ A \) with \( X \) by the embedding \( \phi_A \), we obtain a natural decomposition \( A = (k \cdot 1) \oplus V^* \).

By Proposition 3.2.3, the map \( X \mapsto \Omega = \sum_{k=1}^{n-1} x_k \otimes \Omega_k \in V^* \otimes S^2 V \), well defined up to a scalar multiple of \( \Omega \), respects the action of \( \text{GL}_{n-1} \). On the other hand, by definition, the structure constants \( c_{ij}^k \), with \( 1 \leq i, j, k \leq n - 1 \), form the matrix representing the linear map \( V^* \otimes_k V^* \rightarrow V^* \) induced by multiplication in \( A \), composed with the projection \( A \rightarrow V \). This map corresponds to the element \( \sum_{i=1}^{n-1} x_i \otimes \sum_{1 \leq i, j \leq n-2} c_{ij}^k x_i x_j \in V^* \otimes S^2 V \), and now the claim is clear.

Thus to prove the theorem, it is enough to do so for a single choice of the basis \( \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \).
As \( A \) is non-degenerate, we can identify \( A \cong \tilde{k}^n = k^n \). We take our basis to be

\[
\alpha_0 = (1,1,\ldots,1), \\
\alpha_1 = (2n-2,-2,\ldots,-2), \\
\alpha_2 = (-2,2n-2,-2,\ldots,-2), \\
\vdots \\
\alpha_{n-1} = (-2,-2,\ldots,2n-2,-2).
\]

The multiplication on \( k^n \) is given by multiplication in each component separately, and the trace pairing on \( k^n \) is given by the standard dot product. We compute the dual basis:

\[
\alpha^*_0 = \frac{1}{n}(1,1,\ldots,1), \\
\alpha^*_1 = \frac{1}{2n}(1,0,\ldots,0,-1), \\
\alpha^*_2 = \frac{1}{2n}(0,1,0,\ldots,0,-1), \\
\vdots \\
\alpha^*_{n-1} = \frac{1}{2n}(0,0,\ldots,1,0,-1).
\]

The elements of \( X(k) \) correspond to algebra homomorphisms \( k^n \to k \), which are just projections to individual components. The points of the set \( X(k) \) are given by the same formula as in Example 3.5.4, and we compute them to be

\[
P_1 = (1:0:\ldots:0), \\
P_2 = (0:1:\ldots:0), \\
\vdots \\
P_{n-1} = (0,0,\ldots,0,1), \\
P_n = (1:1:\ldots:1).
\]

Thus, by Lemma 3.5.9, we have \( \Omega_i = nx_i^2 - 2x_i \sum_{j=1}^{n-1} x_j \) for \( 1 \leq i \leq n-1 \). We compute the structure constants \( c_{ij}^k \) associated to the basis \( \alpha_0, \ldots, \alpha_{n-1} \). If \( i \) and \( j \) are distinct, we have

\[
\alpha_i \alpha_j = (4,\ldots,4,4(1-n),4,\ldots,4,4(1-n),4,\ldots,4) \\
= 4\alpha_0 - 2\alpha_i - 2\alpha_j.
\]

If \( i = j \),

\[
\alpha_i^2 = (4,\ldots,4,4n^2 - 8n + 4,4,\ldots,4) \\
= (4n-4)\alpha_0 + 2(n-2)\alpha_i,
\]

and hence we do have \( c_{ij}^k = \frac{\partial^2 \Omega_i}{\partial x_i \partial x_j} \), as required.

As a corollary to the theorem and Lemma 3.5.6, we obtain a proof of the following conjecture.
of Fisher.

**Corollary 3.5.10.** Let $X$ be a set of $n$ points in general position in $\mathbb{P}^{n-1}$, and let $\Omega_1, \ldots, \Omega_{n-1}$ be the quadrics associated to a minimal free resolution of $X$. Then there exists a commutative and associative $k$-algebra $A$, of dimension $n$, with a basis $1, \alpha_1, \ldots, \alpha_{n-1}$, such that for all $1 \leq i, j \leq n-1$ we have

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^{n-1} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \alpha_k,$$

for some $c_{ij}^0 \in k$. Moreover $A$ is isomorphic to the ring of global functions on $X$, and $\alpha_i$ span the trace zero subspace.

Similarly to the situation in page 68 of [Bha08], we can use the associative law in $A$ to obtain expressions for the coefficients $c_{ij}^0$, and consequently for the matrix representing the trace pairing on $A$.

**Lemma 3.5.11.** For $1 \leq i, j \leq n-1$, we have

$$c_{ij}^0 = \sum_{r=1}^{n-1} \left( \frac{\partial^2 \Omega_r}{\partial x_i \partial x_j} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_r}{\partial x_i \partial x_j} \frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} \right).$$

We have $\text{Tr}(\alpha_i \alpha_j) = nc_{ij}^0$, $\text{Tr}(\alpha_i) = 0$ and $\text{Tr}(\alpha_0) = n$, for $1 \leq i \leq n-1$. Thus the determinant of the matrix representing the trace form then follows, using the fact that $\text{Tr}(\alpha_0) = \text{Tr}(1) = n$, while $\text{Tr}(\alpha_i) = 0$ for $i > 0$.

**Proof.** The above identity follows by equating the coefficients of $\alpha_k$ in $\alpha_i (\alpha_j \alpha_k)$ and $(\alpha_i \alpha_j) \alpha_k$. The assertion on the matrix representing the trace form then follows, using the fact that $\text{Tr}(\alpha_0) = \text{Tr}(1) = n$, while $\text{Tr}(\alpha_i) = 0$ for $i > 0$.

**Remark 3.5.12.** Now assume $k = \mathbb{Q}$, and suppose that $F_\bullet$ is an integral model, in the sense of Definition 3.1.10. Concretely, this just means that if $F_\bullet$ is given by

$$0 \rightarrow R(-n) \xrightarrow{\phi_{n-2}} R(-n+2) \xrightarrow{\phi_{n-3}} \ldots \xrightarrow{\phi_2} R(-2) \xrightarrow{\phi_1} R \rightarrow 0$$

then the maps $\phi_k$, for $1 \leq k \leq n-2$ are represented by matrices of homogeneous polynomials with integral coefficients.

From the definition of the $\Omega$-quadrics, it is clear that if $F_\bullet$ is integral, then $\Omega_1, \ldots, \Omega_{n-1}$ are quadrics in with integer coefficients. Hence the structure constants of the algebra $A$ constructed in Corollary 3.5.10 are integers, and the lattice $B = \mathbb{Z} \alpha_0 + \mathbb{Z} \alpha_1 + \ldots + \mathbb{Z} \alpha_{n-1}$ is naturally an order in $A$.

**Remark 3.5.13** (Maximal orders). The order $B$ we constructed cannot be the maximal order in $A$. As an example, if $X$ is the set of $n$ points as in Lemma 3.5.9, we have $A = \mathbb{Q}^n$, the maximal order in $A$ is $\mathbb{Z}^n$ and $B$ is the order $\mathbb{Z} \cdot 1 + 2n \cdot \mathbb{Z}$.

The issue is that the order $B$ we construct decomposes, as a $\mathbb{Z}$-module, as $B = \mathbb{Z} \cdot 1 \oplus V_\mathbb{Z}$, where $V_\mathbb{Z}$ is the trace zero subspace. As $\text{Tr}(1) = n$, this implies that $\text{Tr}(B) = n\mathbb{Z}$. Hence if $B$ is
a maximal order, then primes dividing \( n \) are necessarily ramified in \( A \), and so not all maximal orders can arise.

In Section 3.8 we give, under the assumption that \( n \) is odd, a modification of our construction that has a better chance to produce a maximal order. For \( n = 3 \) and \( n = 5 \), this construction will agree with the Delone-Faddeev parametrization of cubic rings and Bhargava’s parametrization of quintic rings.

### 3.6 Proof of Lemma 3.5.8

Our approach is inspired by an the explicit description of a resolution model of the set \( X \), due to Wilson, see Chapter 5 of [Wil13]. Note that in Section 4.5 we will give a different proof of Lemma 3.5.8, based on the method of unprojection.

**Lemma 3.6.1.** If \( n \geq 4 \), the ideal \( I := I(X) \subset k[x_1, \ldots, x_{n-1}] = R \) is generated by the quadrics \( x_i(x_j - x_k) \) for \( 1 \leq i, j, k \leq n-1 \). If \( n = 3 \), \( I_3 \) is generated by \( x_1x_2(x_1 - x_2) \).

**Proof.** The case \( n = 3 \) is obvious. The case \( n \geq 4 \) is Lemma 146. on page 152 of [Wil13]. The proof is a simple computation, since by Theorem 3.1.3(ii) we know that \( I \) is generated by quadrics.

The case \( n = 3 \) of Lemma 3.5.9 follows immediately, and from now on we assume \( n \geq 4 \). Let us fix a minimal graded free resolution of \((F_\bullet, \phi)\) of \( I \).

The idea is to describe \( F_\bullet \) by splicing together Koszul complexes. For each pair \( J = (j, k) \), with \( 1 \leq j, k \leq n-1 \), consider the ideal \( I^J \subset I \) generated by the set of quadrics

\[
\{x_i(x_j - x_k) : 1 \leq i \leq n-1, i \neq j, i \neq k\}.
\]

As a graded \( k[x_1, \ldots, x_{n-1}] \)-module, \( I^J \) is isomorphic to the ideal \( I'^J \) generated by linear forms spanned \( \{x_i : 1 \leq i \leq n-1, i \neq j, i \neq k\} \). Let \( E_j \) be the \((n-3)\)-dimensional vector space spanned by these forms. By Theorem 2.2.7, the ideal \( I'^J \) is resolved by the Koszul complex associated to the sequence \( f = (x_1, \ldots, \hat{x}_j, \ldots, \hat{x}_k, \ldots, x_{n-1}) \). Thus \( I^{(jk)} \) is resolved by a complex \( K^J_\bullet \),

\[
K^J_\bullet : 0 \rightarrow \Lambda^{n-3} E_j \xrightarrow{d_{n-3}} \Lambda^{n-4} E_j \xrightarrow{d_{n-4}} \cdots \xrightarrow{d_3} E_j \xrightarrow{d_1} R.
\]

Let \( e_1, \ldots, e_{n-3} \) be a basis of \( E^J \). For \( m > 1 \), the differential \( d_m \) is given by

\[
d_m(e_{b_1} \wedge \ldots \wedge e_{b_m}) = \sum_{l=1}^{m} (-1)^l x_{b_l} e_{b_1} \wedge \ldots \wedge \hat{e}_{b_l} \wedge \ldots \wedge e_{b_m},
\]

and if \( m = 1 \), we have \( d_1(e_i) = x_i(x_j - x_k) \).

There exists a unique map of chain complexes \( K^J_\bullet \rightarrow F_\bullet \) lifting the map \( R/I^J \subset R/I \). Let us denote the image of \( e_{b_1} \wedge \ldots \wedge e_{b_m} \) in \( F_\bullet \) by the symbol \( b_1 \wedge \ldots \wedge b_m \otimes (j, k) \). From the above
equation, we deduce that

$$\phi_m(b_1 \wedge \ldots \wedge b_m \otimes (j, k)) = \sum_{l=1}^{m} (-1)^l x_b b_1 \wedge \ldots \wedge \hat{b}_l \wedge \ldots \wedge b_m \otimes (j, k). \quad (*)$$

Note that as a graded module, $F_m \cong R(-m-1)^{b_m}$ and $\deg(b_1 \wedge \ldots \wedge b_m \otimes (j, k)) = m + 1$. For each $1 \leq m \leq n - 3$, the degree $m + 1$ subspace of $F_m$ is the space of constant forms $k^{b_m}$. Note also that $\ker\phi_m = \ker\phi_{m+1}$ is generated by tuples of linear forms if $m \leq n - 4$, and by tuples of quadratic forms if $m = n - 3$. Thus $\phi_m$ is injective on the degree $m + 1$ subspace of $F_m$.

**Remark 3.6.2.** The above formula can be viewed as a description of the maps $\phi_m$ for $m \leq n - 3$ on the submodule of $F_m$ spanned by the elements $b_1 \wedge \ldots \wedge b_m \otimes (j, k)$. These elements were also considered in Chapter 5 of [Wil13] - note that the notation used for them there is $s_{I,J}$. Wilson introduces an action of the group $S_n = \text{Aut}(X)$ on the degree zero part of each module $F_m$. He proves that this representation is irreducible, in Theorem 150, and that the span of $b_1 \wedge \ldots \wedge b_m \otimes (j, k)$ is a subrepresentation, in Lemma 152. It follows then that this span is equal to the whole space. We won’t need this fact for the proof of Lemma 3.5.8, and so we do not give more details.

From now on we assume that $n \geq 4$, since the somewhat degenerate case $n = 3$ is easy to handle by a direct computation. We now give a formula for the differential $\phi_{n-2} : F_{n-2} \rightarrow F_{n-3}$.

**Lemma 3.6.3.** The map $\phi_{n-2}$, up to scaling by an element of $k^*$, is determined by $1 \mapsto t$, where

$$t = \sum_{J = (j,k)} \text{sgn}(\tau_J) x_j x_k \cdot b_1 \wedge \ldots \wedge b_{n-3} \otimes (j, k), \quad (**)$$

where for each pair $J = (j, k)$ we fix a permutation $\tau_J \in S_{n-1}$ with $\tau_J = (b_1, \ldots, b_{n-3}, j, k)$.

**Proof.** As $F_{n-2} \cong R(-n)$, the map $\phi_{n-2}$ is determined by the $\phi_{n-2}(1)$. As $1 \in F_{n-2}$ has degree $n$, and $t \in F_{n-3} = R(-n-2)^{b_{n-3}}$ has degree $n - 2$, both $\phi_{n-2}(1)$ and $t$ have degree $n$. Since $\phi_1$ is exact, $\phi_1(1)$ spans the degree $n$ component of $\text{im}(\phi_{n-2}) = \ker(\phi_{n-3})$. Hence it suffices to show $t \in \ker(\phi_{n-3})$, and that $t$ is non-zero.

We do the case $n = 4$ separately, since the formula for $\phi_{n-3} = \phi_1$ is slightly different in this case. We have

$$t = x_1 x_2 \cdot 3 \otimes (1, 2) + x_2 x_3 \cdot 1 \otimes (2, 3) + x_3 x_1 \cdot 2 \otimes (1, 3),$$

and we compute

$$\phi_1(t) = x_1 x_2 \cdot x_3(x_1 - x_2) + x_2 x_3 \cdot x_1(x_2 - x_3) + x_3 x_1 \cdot x_2(x_1 - x_3) = 0.$$

Now assume $n \geq 5$, and compute

$$\phi_{n-3}(t) = \sum_{j<k} \text{sgn}(\tau_{(j,k)}) x_j x_k \cdot \phi_{n-3}(b_1 \wedge \ldots \wedge b_{n-3} \otimes (j, k))$$

$$= \sum_{j<k} \sum_{l \neq j,l \neq k} \text{sgn}(\tau_{(j,k)}) x_j x_k x_l \cdot b_1 \wedge \ldots \wedge \hat{l} \wedge \ldots \wedge b_{n-3} \otimes (j, k).$$
To make notation simpler, we prove that the coefficient $c$ of $x_1x_2x_3$ in the above expression vanishes - the same argument will apply to all the other coefficients, and we can then conclude $\phi_{n-3}(t) = 0$. We compute

$$c = 4 \wedge \ldots \wedge (n-1) \otimes (1, 2) + 4 \wedge \ldots \wedge (n-1) \otimes (2, 3) + 4 \wedge \ldots \wedge (n-1) \otimes (3, 1) \in F_{n-4}.$$ 

We have $\deg(c) = n - 2$, and as we have seen above, $\phi_{n-3}$ is injective in this degree. Thus it suffices to prove $\phi_{n-3}(c) = 0$. For any $k \in \{3, 4, \ldots, n-2\}$, we see that the $x_k$ coefficient of $\phi_{n-3}(c)$ is

$$c_k = (-1)^k (4 \wedge \ldots \wedge \hat{k} \wedge \ldots \wedge (n-1) \otimes (1, 2) + 4 \wedge \ldots \wedge \hat{k} \wedge \ldots \wedge (n-1) \otimes (2, 3) + 4 \wedge \ldots \wedge \hat{k} \wedge \ldots \wedge (n-1) \otimes (3, 1)).$$

So up to a sign, an expression of the same form as the previous one, with the symbol $k$ deleted everywhere. To check this is zero, it is again sufficient to check if it maps to zero under $\phi_{n-4}$. Continuing in this way, iteratively applying $\phi$, each time deleting an entry of $I$, we are left with checking that for every $i \in \{3, 4, \ldots, n-2\}$, we have

$$0 = \phi_1(i \otimes (1, 2) + i \otimes (2, 3) + i \otimes (3, 1)),$$

and this is equivalent to

$$0 = x_i(x_1 - x_2) + x_i(x_2 - x_3) + x_i(x_3 - x_1),$$

which is clearly true. Finally, if $t$ was zero, then the coefficient of $x_jx_k$ in $t$ is zero for all $j, k$, i.e. $b_1 \wedge \ldots \wedge b_{n-3} \otimes (j, k) = 0$. Using the description $(\ast)$ of the differential $\phi$ on these elements, this would imply that $i \otimes (j, k) = 0$ for all $i, j, k$ distinct, but this is impossible.

We now prove Lemma 3.5.8. As $\phi_1(i \otimes (j, k)) = x_i(x_j - x_k)$, we see that

$$\frac{\partial \phi_1}{\partial x_i}(i \otimes (j, k)) = x_j - x_k,$$

and therefore

$$\frac{\partial \phi_1}{\partial x_j}(i \otimes (j, k)) = x_i, \quad \frac{\partial \phi_1}{\partial x_k}(i \otimes (j, k)) = -x_i.$$ 

For $2 \leq m \leq n-3$, we have $\phi_m = \sum_{i=1}^{n-1} x_i \frac{\partial \phi_m}{\partial x_i}$. Using the equation $(\ast)$ we find, for $2 \leq m \leq n-3$,

$$\frac{\partial \phi_m}{\partial x_b}(b_1 \wedge \ldots \wedge b_m \otimes (j, k)) = (-1)^k b_1 \wedge \ldots \wedge \hat{b}_k \wedge \ldots \wedge b_m \otimes (j, k).$$

If $k \not\in i$, then $\frac{\partial \phi_m}{\partial x_b}(b_1 \wedge \ldots \wedge b_m \otimes (j, k)) = 0$. Similarly, we use the formula $(\ast \ast)$ giving $t$ to compute

$$\frac{\partial \phi_{n-2}}{\partial x_k}(1) = \sum_{1 \leq j \leq n-1, j \neq k} \text{sgn}(\tau_{(j,k)}) x_j \cdot b_1 \wedge \ldots \wedge b_{n-3} \otimes (j, k)$$

Now let $(a_1, \ldots, a_{n-1})$ be a permutation in $S_{n-1}$. Regarding $\phi_i$ as maps, rather than matrices, we seek to compute
3.7. THE DISCRIMINANT FORM

\[ [a_1, a_2, \ldots, a_{n-2}] = \left( \frac{\partial \phi_1}{\partial x_{a_1}} \circ \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \frac{\partial \phi_{n-2}}{\partial x_{a_{n-2}}} \right) (1) \]
\[ = \left( \frac{\partial \phi_1}{\partial x_{a_1}} \circ \frac{\partial \phi_2}{\partial x_{a_2}} \cdots \frac{\partial \phi_{n-3}}{\partial x_{a_{n-3}}} \right) \left( \sum_{1 \leq j \leq n-1, j \neq a_{n-2}} \text{sgn}(\tau_{(j,a_{n-1})}) x_j \cdot b_1 \wedge \cdots \wedge b_{n-3} \otimes (j,a_{n-2}) \right). \]

Now the action of the map \( \frac{\partial \phi_{an-m}}{\partial x_{an-m}} \), for \( 2 \leq m \leq n - 3 \) kills all \( b_1 \wedge \cdots \wedge b_m \otimes (j,k) \) with \( a_m \notin \{b_1, \ldots, b_n\} \). Thus the only terms that contribute to the above sum correspond to tuples \((b_1, \ldots, b_{n-3})\) that contain \( a_2, a_3, \ldots, a_{n-3} \), and do not contain \( a_{n-2} \). We see that the only possibilities correspond to terms \((a_2, a_3, \ldots, a_{n-3}, a_{n-1})\) or \((a_1, a_2, \ldots, a_{n-3})\). Hence

\[ [a_1, a_2, \ldots, a_{n-2}] = \text{sgn}(a_1, \ldots, a_{n-1}) \frac{\partial \phi_1}{\partial x_{a_1}} (x_{a_{n-1}} a_1 \otimes (a_{n-1}, a_{n-2}) - x_{a_1} a_{n-1} \otimes (a_1, a_{n-2})) \]
\[ = \text{sgn}(a_1, \ldots, a_{n-1}) (x_{a_{n-1}} - x_{a_{n-2}}) x_{a_{n-1}} - \text{sgn}(a_1, \ldots, a_{n-1}) x_{a_1} x_{a_{n-1}} \]
\[ = \text{sgn}(a_1, \ldots, a_{n-1}) (x_{a_{n-1}} - x_{a_{n-2}} - x_{a_1}) x_{a_{n-1}} \]

concluding the proof of Lemma 3.5.8. Note that the constant \( \lambda \) in Lemma 3.5.8 arises because the map \( \phi_{n-2} \) is only unique up to a scalar, and in the above calculation we have taken \( \phi_{n-2} \) to be the map determined by \( 1 \mapsto t \).

3.7 The discriminant form

We now study the connection between genus one normal curves of degree \( n \), and sets of \( n \) points in general position. For a genus one curve \( C \subset \mathbb{P}^{n-1} \), we associate a discriminant to every hyperplane \( H \subset \mathbb{P}^{n-1} \). We first do this for the hyperplane \( \{x_1 = 0\} \), and then use the action of \( \text{SL}_n \) on \( \mathbb{P}^{n-1} \) to reduce the general case to this situation.

Let \( [C \to \mathbb{P}^{n-1}] \) be an \( n \)-diagram, defined over a field \( K \) of characteristic 0. Fix a resolution model \( F_* \) of \( [C \to \mathbb{P}^{n-1}] \). The intersection of \( C \) and the hyperplane \( x_1 = 0 \) is a set \( X \) of \( n \) points in \( \mathbb{P}^{n-2} \). A resolution model of \( X \) can be obtained by setting \( x_1 = 0 \) in the differentials of \( F_* \), as we will now see.

Let \( A = R/\phi_1(F_1) \) be the homogenous coordinate ring of \( C \). We can identify the homogenous coordinate ring of \( X \) with \( A/(x_1 A) \). The key observation is the following lemma, whose proof will make use of basic properties of the functor Tor, an exposition of which can be found in Chapter 6 of [Eis13].

Lemma 3.7.1. (i) The chain complex \( F_*^{(0)} = F_* \otimes_R (R/x_1 R) \) is a minimal free resolution of \( A/(x_1 A) \), viewed as a graded \( R \)-module, where \( R^{(0)} = R/x_1 R \cong K[X_1, \ldots, X_{n-1}] \).

Concretely, if \( \phi_1 : F_i \to F_{i-1} \) are the differentials of \( F_* \), viewed as matrices of homogenous forms in \( x_1, \ldots, x_{n-1} \), the differentials \( \phi_1^{(0)} : F_i^{(0)} \to F_{i-1}^{(0)} \) are obtained by setting \( \phi_1^{(0)}(x_1, \ldots, x_{n-1}) = \phi_1(0, x_1, \ldots, x_{n-1}) \).

(ii) Let \( \Omega_{F_*} \) be the \( \Omega \)-matrix associated to the resolution model \( F_* \). The \( \Omega \)-quadrics associated
to the model \(F^0\) are given by
\[
\Omega_k(X_1, X_2, \ldots, X_{n-1}) = \Omega_{1k}(0, X_1, X_2, \ldots, X_{n-1})
\]
for \(1 \leq k \leq n-1\).

\begin{proof}
As \(F\) is a free resolution of \(A\), in the category of \(R\)-modules, by definition of the functor Tor, the homology groups of the chain complex \(F^0\) are \(\text{Tor}_i^R(A, R/x_1 R)\). The short exact sequence
\[
0 \to R \xrightarrow{x_1} R \to R/x_1 R \to 0
\]
induces a long exact sequence
\[
\cdots \to \text{Tor}_i^R(A, R) \xrightarrow{x_1} \text{Tor}_i^R(A, R) \to \text{Tor}_i^R(A, R/x_1 R) \to \text{Tor}_{i-1}^R(A, R) \to \cdots
\]
Computing Tor with respect to the second variable, we find for \(i \geq 1\), \(\text{Tor}_i^R(A, R) = 0\), and for \(i = 0\), \(\text{Tor}_0^R(A, R) = A\). The long exact sequence then implies that \(\text{Tor}_i^R(A, R/x_1 R)\) is zero for \(i \geq 2\).

Next, note that \(x_1\) is not a zero-divisor on \(A\), as \(C\) is a genus one normal curve, so in particular irreducible, and so if \(x_1\) was a zero divisor then \(C\) would be contained in the hyperplane \(x_1 = 0\), which is impossible. Thus \(\text{Tor}_0^R(A, R) \xrightarrow{x_1} \text{Tor}_0^R(A, R)\) is injective, with cokernel isomorphic to \(A/x_1 A\), and hence \(\text{Tor}_1^R(A, R/x_1 R) = 0\) and \(\text{Tor}_0^R(A, R/x_1 R) = A/x_1 A\), concluding the proof of (i).

Part (ii) follows from the explicit description of the differentials \(\phi^0\), and the definition of the \(\Omega\)-quadrics.
\end{proof}

We regard the curve \(C\) as a subvariety of the projective space \(\mathbb{P}^{n-1}\), with coordinates \(x_1, \ldots, x_n\), corresponding to a basis of the space of linear forms on \(\mathbb{P}^{n-1} = \mathbb{P}(V)\). Consider the dual projective space \(\mathbb{P}(V^*)\), with coordinates \(u_1, \ldots, u_n\). To a point \((u_1 : \ldots : u_n) \in \mathbb{P}(V^*)\), we associate a hyperplane \(\{u_1x_1 + \ldots + u_nx_n = 0\} \subset \mathbb{P}(V)\).

We now define the discriminant form associated to a resolution model \(F^\bullet\) of \(C\), first as a function \(D_{F^\bullet} : K^n \to K\). Given \((u_1, u_2, \ldots, u_n) \in K^n \setminus \{0\}\), choose a \(\gamma \in \text{SL}_n(K)\) with \(\gamma_{1i} = u_i\) for \(i = 1, \ldots, n\). Note that \(\gamma\) maps the hyperplane \(\{u_1x_1 + \ldots + u_nx_n = 0\}\) to the hyperplane \(\{x_1 = 0\}\). Let \(G^\bullet = \gamma^{-1} \cdot F^\bullet\), and let \(G^0\) be the resolution obtained by setting \(x_1 = 0\) in \(G^\bullet\), as in Lemma 3.7.1. Then \(G^0\) is a resolution model of a set of \(n\) points in the hyperplane \(\{x_1 = 0\} \cong \mathbb{P}^{n-2}\). Let \(A\) be the \(n\)-dimensional \(K\)-algebra associated to \(G^0\) by Theorem 3.5.7, together with the basis \(\alpha_0, \ldots, \alpha_{n-1}\). We define \(D_{F^\bullet}(u_1, \ldots, u_n)\) to be the determinant of the matrix representing the trace pairing on \(A\) with respect to the basis \(\alpha_0, \ldots, \alpha_{n-1}\).

\begin{lemma}
The function \(D_{F^\bullet} : K^n \to K\) is well-defined, i.e. independent of the choice of \(\gamma \in \text{SL}_n(K)\). It depends only on the \(\Omega\)-matrix associated to \(F^\bullet\), and for all \(\lambda \in K\) we have \(D_{F^\bullet}(\lambda u_1, \ldots, \lambda u_n) = \lambda^{2n}D_{F^\bullet}(u_1, \ldots, u_n)\). We say that \(D_{F^\bullet}\) is the discriminant form associated to the model \(F^\bullet\).
\end{lemma}

\begin{proof}
Suppose we are given \(\gamma, \gamma' \in \text{SL}_n(K)\) with \(\gamma_{0i} = \gamma'_{0i} = u_i\) for \(0 \leq i \leq n-1\). Let \(X = \gamma(C) \cap \{x_1 = 0\}\) and \(X' = \gamma'(C) \cap \{x_1 = 0\}\). Then \(\beta = \gamma' \gamma^{-1}\) takes the set \(X\) to \(X'\), and

Lemma 3.7.3. \( \lambda \) contributes the remaining factor bases is rescaled by \( \lambda \). This rescaling contributes the factor \( \lambda^2 \), and the determinant of \( \beta^0 \) contributes the remaining factor \( \lambda^2 \).

In fact, we have a more precise statement.

**Lemma 3.7.3.** \( D_{F_*} \) is a homogeneous polynomial of degree \( 2n \) in the variables \( u_1, u_2, \ldots, u_n \), and its coefficients are homogeneous polynomials of degree \( 2n - 2 \) in the coefficients of the \( \Omega \)-matrix of \( C \).

**Proof.** Observe that if \( u_1 \) is non-zero, we can take \( \gamma \) to be the matrix

\[
\begin{pmatrix}
    u_1 & 0 & 0 & 0 & \ldots & 0 & 0 \\
    u_2 & 1/u_1 & 0 & 0 & \ldots & 0 & 0 \\
    u_3 & 0 & 1 & 0 & \ldots & 0 & 0 \\
    \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    u_n & 0 & 0 & 0 & \ldots & 0 & 1
\end{pmatrix}
\]

Thus \( D_{F_*}(u_1, \ldots, u_n) \) is a rational function in \( u_1, \ldots, u_n \), with denominator a power of \( u_1 \). But the choice of the hyperplane \( x_1 = 0 \) was arbitrary, and by an argument similar to the one we used to show that \( D \) is well-defined, we can show that \( D_{F_*} \) takes on the same value if we instead require that the \( i \)-th column of \( \gamma \) is (the transpose of) \( (u_1, \ldots, u_n) \). Thus, arguing by symmetry, we conclude that \( D \) is a polynomial, and by Lemma 3.7.2, it must be a homogeneous polynomial of degree \( 2n \). Going through the description of the various group actions involved, we see that its coefficients are homogeneous forms of degree \( 2n - 2 \) in the coefficients of the entries of \( \Omega_{F_*} \). \( \square \)
Lemma 3.7.4. Suppose we are given two resolution models $F_*$ and $F'_*$, of curves $C \subset \mathbb{P}^{n-1}$ and $C' \subset \mathbb{P}^{n-1}$ respectively, with $g \cdot F_* = F'_*$ for some $g \in \text{SL}_n(K)$. Let $x'_j = \sum_{i=1}^{n} g_{ij} x_i$, and let $u'_j = \sum_{i=1}^{n} g'^{ij} u_i$. We then have

$$D_{F_*}(u'_1, \ldots, u'_n) = D_{F'_*}(u_1, \ldots, u_n).$$

Proof. It follows from Proposition 3.2.3. Note that the definition of $u'_j$ comes from identifying $u_1, \ldots, u_n$ with the dual basis to $x_1, \ldots, x_n$, and considering the action of the group $\text{SL}_n$ on the dual of the standard representation.

Lemma 3.7.5. Suppose $K = \mathbb{Q}$ and the model $F_*$ is $\mathbb{Z}$-integral. Then $D_{F_*} \in \mathbb{Z}[u_1, \ldots, u_n]$, and for any $(u_1, \ldots, u_n) \in \mathbb{Z}^n$, where the $u_i$ are not all zero, $D_{F_*}(u_1, \ldots, u_n)$ is the discriminant of an order in the algebra $A$.

Proof. We may assume that the integers $u_1, \ldots, u_n$ are coprime. Then, in the definition of the discriminant $D_{F_*}(u_1, \ldots, u_n)$ we may take $\gamma$ to be an element of $\text{SL}_n(\mathbb{Z})$ - this follows from the standard fact that $\text{SL}_n(\mathbb{Z})$ acts transitively on $\mathbb{F}^{n-1}(\mathbb{Q})$, see for example Lemma 3.13 of [CFS10]. Then $G_0$ is an integral resolution model, and so, as explained in Remark 3.5.12, the structure constants that define the algebra $A$ also define an order $B$ in $A$, of discriminant $D_{F_*}(u_1, \ldots, u_n)$.

Example 3.7.6. Let us take $n = 3$. We look at the example mentioned in Chapter 1 in more detail. In this case $C \subset \mathbb{P}^2$ is a plane cubic curve, and a resolution model of $C$ is a ternary cubic $F(x_0, x_1, x_2)$. Let $\gamma$ be as defined in Lemma 3.7.3. We have

$$\gamma^{-1} = \begin{pmatrix} 1/u_1 & 0 & 0 \\ -u_2 & u_1 & 0 \\ -u_3/u_1 & 0 & 1 \end{pmatrix}$$

Set $G(x_0, x_1, x_2) = \gamma^{-1} \cdot F = F(x_1/u_1 - u_2 x_2 - u_3/u_1 x_3, u_1 x_2, x_3)$. Next, we set $x_1 = 0$ in $G$, and obtain $G^0(x_2, x_3) = G(0, x_2, x_3) = F(-u_2 x_2 - u_3/u_1 x_3, x_3)$, a binary cubic form in $x_2$ and $x_3$, with coefficients rational functions of $u_1, u_2$ and $u_3$. Then we see that $D_{F_*}(u_1, u_2, u_3)$ is the discriminant of $G^0$. Recall, as mentioned in the Chapter 1, that the discriminant of a form

$$ax^3 + bx^2y + cxy^2 + dy^3$$

is given by

$$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

By Lemma 3.7.3 we see that $D_{F_*}(u_1, u_2, u_3)$ is a degree 6 polynomial in $u_1, u_2$ and $u_3$, even though the coefficients of $G^0$ are rational functions, with denominators powers of $u_1$. There is no difficulty in using computer algebra software to compute formulas for the coefficients of $D_{F_*}$. These expressions are fairly involved however, and so we omit them here. In Chapter 1 we gave a formula for $D_{F_*}$ in the special case when $C$ is in Hesse normal form.

Remark 3.7.7. In the next section, in Theorem 3.8.1, we give a different order associated to a resolution model of a set of $n$ points than the one constructed in Theorem 3.5.7. The
discriminant of this order is smaller by a factor of $(2n)^{2n-2}$, and if we define the discriminant form using this order, all of the properties we proved remain true, and the discriminant form is smaller by a factor $(2n)^{2n-2}$.

3.8 A refinement of the construction of structure constants

As explained in Remark 3.5.13, the order $B$ we constructed in Section 3.5 has no chance of being maximal. In this section, for $n$ odd, we modify our construction to produce a larger order. The reader interested only in the proof of Theorem 1.0.1 can skip this section on the first reading - the result is obtained by a lengthy computation, and the relation to Theorem 1.0.1 is that it allows us to obtain sharper explicit values for the constants $c(n)$. Note that we only compute explicit values for $c(3)$ and $c(5)$, and in these cases Theorem 3.8.1 essentially follows from the work of Delone-Faddeev and Bhargava. Thus we are mainly interested in Theorem 3.8.1 as a result in the theory of ring parametrizations.

The goal of this section is to prove the following result.

**Theorem 3.8.1.** Let $X$ be a set of $n$ points in $\mathbb{P}^{n-2}$, defined over $\mathbb{Q}$, and let $F_*$ be a resolution model of $X$ defined over $\mathbb{Z}$, with the associated algebra $A$. Let $B = \langle 1, \alpha_1, \ldots, \alpha_{n-1} \rangle$ be the order of $A$ associated to $F_*$ in Remark 3.5.12. There exists a basis $1 = \beta_0, \beta_1, \ldots, \beta_{n-1}$ of $B$, for which the structure constants are given by

$$\beta_i \cdot \beta_j = d_{ij}^0 + \sum_{k=1}^{n-1} d_{ij}^k \beta_k,$$

where we have $d_{ij}^k = 2n \cdot e_{ij}^k$ for $k > 0$, and $d_{ij}^0 = (2n)^2 \cdot e_{ij}^0$, for some integers $e_{ij}^k$. Hence $B' = \langle 1, \frac{\beta_1}{2n}, \ldots, \frac{\beta_{n-1}}{2n} \rangle$ is an order of $A$, with $\text{disc}(A) = (2n)^{2n-2} \text{disc}(B)$, with multiplication given by

$$\frac{\beta_i}{2n} \cdot \frac{\beta_j}{2n} = e_{ij}^0 + \sum_{k=1}^{n-1} e_{ij}^k \beta_k\frac{2n}{2n},$$

The idea of the proof is to take $\beta_i$ to be a normal basis, generalizing the definition given on page 67 of [Bha08]. Let $S$ be a ring and let $R$ be a free $S$-algebra of rank $n$, for $n \geq 3$ an odd integer. We say a basis $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ of $R$ is normal, if $\alpha_0 = 1$, and for $1 \leq k \leq (n-1)/2$, the coefficients of $\alpha_{2k-1}$ and $\alpha_{2k}$ in $\alpha_{2k-1}\alpha_{2k}$ are zero.

Every basis can be modified to a normal basis via a unimodular transformation.

**Lemma 3.8.2.** Let $1 = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be a basis of $S$, with $\alpha_i \alpha_j = \sum_{k=0}^{n-1} e_{ij}^k \alpha_k$. Set $\beta_0 = \alpha_0 = 1$ and $\beta_{2k-1} = \alpha_{2k-1} - c_{2k-1, 2k}^k$, $\beta_{2k} = \alpha_{2k} - c_{2k-1, 2k}^{2k}$, for $1 \leq k \leq (n-1)/2$. Then $\beta_0, \ldots, \beta_{n-1}$ is a normal basis of $S$.

Furthermore, write $\beta_i = \alpha_i - b_i$, $1 \leq i \leq n - 1$. Then the structure constants for the basis
Lemma 3.8.4. (i) $d_{ij}^k = c_{ij}^k$

(ii) $d_{ii}^i = c_{ii}^i$

(iii) $d_{ij}^i = c_{ij}^i - b_j$

(iv) $d_{ii}^i = c_{ii}^i - 2b_i$

Proof. A simple calculation. \hfill \Box

Our strategy for the proof of Theorem 3.8.1 is to prove, in Lemma 3.8.4, that for the normal basis $\beta_0, \ldots, \beta_n$ obtained from the $\alpha_0, \ldots, \alpha_n$ via the above lemma, the structure constants $d_{ij}^k$ are given by integer polynomials in the coefficients of $F_\star$ divisible by $2n$, from which the theorem follows immediately.

Example 3.8.3. Suppose $X = \{P_1, \ldots, P_n\}$ is the set of points as in Lemma 3.5.9. The algebra $A$ associated to this set is isomorphic to $\mathbb{Q}^n$. In the proof of Theorem 3.5 we have computed the associated basis $\alpha_i$. The normal basis $\beta_0, \ldots, \beta_{n-1}$ obtained from $\alpha_0, \ldots, \alpha_{n-1}$ is given by $\beta_0 = (1, 1, \ldots, 1), \beta_1 = (2n, 0, 0, \ldots, 0), \beta_2(0, 2n, 0, \ldots, 0), \ldots, \beta_{n-1} = (0, 0, \ldots, 2n).

We start by describing the building blocks of our expression for the constants $d_{ij}^k$. Let $F_\star$ be a resolution model of degree $n$. For integers $0 \leq a_1, \ldots, a_n \leq n - 2$ we define the symbols $\{a_1 \ldots a_n\}$, taking values in the base field $k$, by

$$\{a_1a_2 \ldots a_n\} := \frac{\partial^2 \phi_1}{\partial x_{a_1} \partial x_{a_2}} \frac{\partial \phi_2}{\partial x_{a_3}} \ldots \frac{\partial \phi_{n-3}}{\partial x_{a_{n-2}}} \frac{\partial^2 \phi_{n-2}}{\partial x_{a_{n-2}} \partial x_{a_n}}.$$

We remark that the symbols $\{a_1, \ldots, a_n\}$, regarded as polynomials in the coefficients $F_\star$, have integer coefficients, divisible by 2 if $a_1 = a_2$ or $a_{n-1} = a_n$, and divisible by 4 if both $a_1 = a_2$ and $a_{n-1} = a_n$.

These symbols satisfy the following properties.

Lemma 3.8.4. (i)\ $\frac{\partial^2 \phi}{\partial x_i \partial x_j} [a_1 \ldots a_{n-2}] = \{ia_1 \ldots a_{n-2}j\} + \{ja_1 \ldots a_{n-2}i\}.$

(ii) \ $\{a_1 \ldots a_{n-2}ab\} = \{a_1 \ldots a_{n-2}ba\}.$

(iii) For $2 < i < n - 2$, we have

$$\{a_1, \ldots, a_{i-1}, a_i, a_{i+1}, a_{i+2}, \ldots, a_n\} = -\{a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_n\},$$

and hence, for $\tau \in S_{n-4}$

$$\{a, b, a_1, \ldots a_{n-4}, c, d\} = \text{sgn}(\tau) \{a, b, a_{\tau(1)} \ldots a_{\tau(n-4)}, c, d\}.$$

(iv) \ $\{a_1, \ldots, a_n\} = (-1)^{1+\left\lfloor \frac{n}{2} \right\rfloor} \{a_n, \ldots, a_1\},$ and as a consequence

$$\{a_1, a_2, a_3, \ldots, a_{n-2}, a_{n-1}, a_n\} = -\{a_n, a_{n-1}, a_3, \ldots, a_{n-2}, a_2, a_1\}.$$
(v) \(\{a_1, \ldots, a_{n-3}abc\} + \{a_1, \ldots, a_{n-3}, b, c, a\} + \{a_1, \ldots, a_{n-3}, c, b, a\} = 0\), and as a special case with \(b = c\), \(\{a_1 \ldots a_{n-3}baa\} = -2\{a_1 \ldots a_{n-3}aba\}\).

(vi) \(\{a, b, c, a_1, \ldots, a_{n-3}\} + \{b, c, a, a_1, \ldots, a_{n-3}\} + \{c, b, a, a_1, \ldots, a_{n-3}\} = 0\).

(vii) If \(a_1 = a_k\) for some \(3 < k < n - 1\) then
\[
\{a_1, a_2, a_3, a_4, \ldots, a_n\} = -\{a_1, a_3, a_2, a_4, \ldots, a_n\}.
\]

(viii) If \(a_n = a_k\) for some \(3 < k < n - 2\) then
\[
\{a_1, \ldots, a_{n-3}, a_{n-2}, a_{n-1}, a_n\} = -\{a_1, \ldots, a_{n-3}, a_{n-1}, a_{n-2}, a_n\}.
\]

**Proof.** For (i), we are done by applying Leibniz rule, as \(\phi_i\) are matrices of linear forms for \(2 \leq i \leq n - 3\), and matrices of quadratic forms for \(i = 1\) and \(i = n - 2\). Property (ii) follows immediately from the definition, while (iii) follows from Lemma 3.4.1. Property (iv) is proved using self-duality of the resolution, in the same way as Lemma 3.4.3, and the second part follows from Lemma 3.4.1. Using Leibniz rule we find
\[
0 = \frac{\partial^3}{\partial x_d \partial x_b \partial x_c} (\phi_{n-3} \phi_{n-2}) = \frac{\partial^2 \phi_{n-2} \partial \phi_{n-3}}{\partial x_d \partial x_b} + \frac{\partial^2 \phi_{n-2} \partial \phi_{n-3}}{\partial x_b \partial x_c} + \frac{\partial^2 \phi_{n-2} \partial \phi_{n-3}}{\partial x_d \partial x_c}
\]
and (v) follows. Part (vi) follows from (v) and (iv). For (vii), let \(a = a_1 = a_k\), and observe that we have
\[
\{a, a_2, a_3, \ldots, a_{k-1}, a, a_{k+1}, \ldots, a_n\} = (-1)^{k-2} \{a, a_2, a_3, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n\} \quad \text{(iii)}
\]
\[
= (-1)^{k-2} \left(\frac{-1}{2}\right) \{a, a, a_2, a_3, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n\} \quad \text{(vi)}
\]
\[
= (-1)^{k-2} \left(\frac{1}{2}\right) \{a, a, a_2, a_3, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n\} \quad \text{(ii)}
\]
\[
= (-1)^{k-2+1} \{a, a, a_2, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n\} \quad \text{(vii)}
\]
\[
= \{a, a_3, a_2, \ldots, a_{k-1}, a, a_{k+1}, \ldots, a_n\}, \quad \text{(iii)}
\]
as required. Property (viii) then follows by combining (vii) and (iv). \(\square\)

We warn the reader that the proof of the next lemma, consisting of manipulations of symbols using rules established above, is long and tedious, and advise them to substitute \(n = 5\) on the first reading, since most features of the general case will show up. The lemma implies that \(d_{ij}^k = 2n \cdot e_{ij}^k\), for \(1 \leq i, j \leq n - 1\) and \(k > 0\), where \(e_{ij}^k \in \mathbb{Z}\). We then obtain \(d_{ij}^0 = (2n)^2 \cdot e_{ij}^0\), \(e_{ij}^0 \in \mathbb{Z}\) using the formulae of Lemma 3.5.11, proving Theorem 3.8.1.

**Lemma 3.8.5.** Assume \(n \geq 3\) is an odd integer. For pairwise distinct integers \(1 \leq i, j, k \leq n - 1\), we have the identities:
Proof. Part (i): We may assume \( i < j \). We have \( \Omega_k = (-1)^k[[1, 2, \ldots, \hat{k}, \ldots, n - 1]], \) as defined in Section 3.2, so by 3.8.2(i), we have

\[
\frac{\partial^2 \Omega_k}{\partial x_i \partial x_j} = (-1)^k \sum_{l=1}^{n-2} \{i, l, l + 1, \ldots, \hat{k}, \ldots, n - 1, 1, 2, \ldots, l - 1, j\}
\]

\[+ (-1)^k \sum_{l=1}^{n-2} \{j, l, l + 1, \ldots, \hat{k}, \ldots, n - 1, 1, 2, \ldots, l - 1, i\}
\]

In the proof, we will assign a type to each term arising in the two sums above, and then prove that all terms of the same type are equal to a fixed multiple (depending only on the type) of the symbol \( \{i, i, 1, \ldots, n - 1, j, j\} \).

A remark on notation - to make the proof more legible, we will frequently omit symbols \( \hat{k} \) that indicate that a letter in a sequence is skipped.

We look first at the terms in the first sum. Assume first \( \{i, j\} \cap \{l - 1, l\} = \emptyset \), so that \( i \) and \( j \) are in the inner \( n - 4 \) elements. We will say such a term is of type \( \{iabj\} \). We have:

\[
\{i, l, l + 1, \ldots, \hat{k}, \ldots, n - 1, 1, 2, \ldots, l - 2, l - 1, j\} = (-1)^{i-j} \{i, i, l, l + 1, \ldots, -j, j, l - 1, j\} \quad \text{by } 3.8.2(ii)
\]

\[
= (-1)^{i-j} \left(\frac{-1}{2}\right) \{i, i, l, \ldots, n - 1, 1, \ldots, j, l - 1, j\} \quad \text{(v)}
\]

\[
= (-1)^{i-j} \left(\frac{1}{3}\right) \{i, i, l, \ldots, n - 1, 1, \ldots, l - 1, j, j\} \quad \text{(vi)}
\]

\[
= (-1)^{i-j} \left(\frac{1}{4}\right) \{i, i, 1, 2, \ldots, \hat{k}, \ldots, n - 1, j, j\}. \quad \text{(ii)}
\]

In the first equality we move \( i \) and \( j \) by successive swaps to the left and right as far as Lemma 3.8.2(ii) applies. This always takes \( n + i - j \) swaps modulo 2, independent of \( l \). In the 3rd and 4th equality we use the special case, with two letters equal, of 3.8.2(v) and 3.8.2(vi). In the final equality, we observe that the inner \( (n - 4)\) word \((l, l + 1, \ldots, l - 1)\) is odd cyclic permutation of \((1, 2, \ldots, \hat{k}, \ldots, n - 1)\), and apply 3.8.2(iii).

Now assume \( i = l \) and \( j \neq l - 1 \). This is a term of type \( \{iibj\} \).

\[
\{i, i, i + 1, \ldots, i - 2, i - 1, j\} = (-1)^{n-i-j} \{i, i, i + 1, \ldots, i - 2, j, i - 1, j\} \quad \text{by } 3.8.2(ii)
\]

\[
= (-1)^{n-i-j} \left(\frac{-1}{2}\right) \{i, i, i + 1, \ldots, i - 1, j, j\} \quad \text{(v)}
\]

\[
= (-1)^{i-j} \left(\frac{1}{2}\right) \{i, i, 1, 2, \ldots, n - 1, j, j\}. \quad \text{(iii)}
\]
3.8. A REFINEMENT OF THE CONSTRUCTION OF STRUCTURE CONSTANTS

Similarly, if \( i \neq l \) and \( j = l - 1 \), the term of type \( \{iajj\} \) is

\[
\{i, j + 1, j + 2, \ldots, j - 1, j, j\} = (-1)^{(n-4)-(j-i)} \{i, j + 1, i, \ldots, j - 1, j, j\} \\
= (-1)^{n-i-j+1} \left(-\frac{1}{2}\right) \{i, i, j + 1, \ldots, j - 1, j, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i, 1, 2, \ldots, n-1, j, j\}.
\]

(iii)

\[
\{i, i + 1, \ldots, i - 1, i, j\} = (-1)^{n-4-(j-i-1)} \{i, i + 1, \ldots, i - 1, j, i, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i + 1, \ldots, i - 1, i, j, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i + 1, \ldots, i - 1, j, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i, 1, 2, \ldots, n-1, j, j\}.
\]

(iii)

Now suppose \( i = l - 1 \) and \( j \neq l \). This is a term of type \( \{i'aij\} \).

\[
\{i, i + 1, \ldots, i - 1, i, j\} = (-1)^{n-4-(j-i-1)} \{i, i + 1, \ldots, i - 1, j, i, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i + 1, \ldots, i - 1, j, i, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i + 1, \ldots, i - 1, j, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i, 1, 2, \ldots, n-1, j, j\}.
\]

(iii)

A similar argument, with the roles of \( i \) and \( j \) reversed, shows that if \( i \neq l - 1 \) and \( j = l \), denoted as type \( \{ijbj\} \), we have:

\[
\{i, j, j + 1, \ldots, j - 1, j\} = (-1)^{n-4-(j-i-1)} \{i, j, i, \ldots, j - 1, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i, j + 1, \ldots, j - 1, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i, j + 1, \ldots, j - 2, j, j - 1, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i, j + 1, \ldots, j - 2, j - 1, j, j\} \\
= (-1)^{i-j} \left(-\frac{1}{2}\right) \{i, i, 1, 2, \ldots, n-1, j, j\}.
\]

(iii)

If \( i = l - 1 \) and \( j = l \), then the two terms discussed above do not occur, and instead we have the term of type \( \{ijij\} \):

\[
\{i, i + 1, \ldots, i, i + 1\} = -\{i, i + 1, \ldots, i, i + 1\} = 0,
\]

(iv) by 3.8.2(iv). Finally, we have type \( \{iijj\} \):

\[
\{i, i, l + 1, \ldots, l - 1, j, j\} = \{i, i, 1, \ldots, n - 1\}.
\]

(iii)

Thus we have dealt with all of the terms that can appear in the first sum.

We now consider the terms in the second sum. Again first consider the terms where \( i \) and \( j \)
appear in the inner $n - 4$ elements, denoted as type $\{jabi\}$. We have

\[
\{j, l, l + 1, \ldots, l - 2, l - 1, i\} = (-1)^{j-i+1} \{j, l, j + 1, \ldots, l - 2, l - 1, i\} \quad \text{(iii)}
\]

\[
= (-1)^{i-j+1} \left(\frac{1}{4}\right) \{j, j, l + 1, \ldots, l - 1, i, i\} \quad \text{(v), (vi)}
\]

\[
= (-1)^{i-j+1} \left(\frac{-1}{4}\right) \{i, i, l + 1, \ldots, l - 1, l, j\} \quad \text{(iv)}
\]

\[
= (-1)^{i-j} \left(\frac{1}{4}\right) \{i, i, 1, 2, \ldots, n - 1, j, j\}. \quad \text{(iii)}
\]

In determining the sign after applying (ii), note that swapping $i$ and $j$ counts as both moving $i$ to the right and $j$ to the left. Now suppose $l = i$ and $l - 1 \neq j$, denoted as type $\{jibi\}$.

\[
\{j, i, i + 1, \ldots, i - 2, i - 1, i\} = (-1)^{j-i-1} \{j, i, j, i + 1, \ldots, i - 1, i\} \quad \text{(iii)}
\]

\[
= (-1)^{j-i} \left(\frac{1}{2}\right) \{j, j, i + 1, \ldots, i - 1, i\} \quad \text{(vi)}
\]

\[
= (-1)^{j-i+n-5} \left(\frac{1}{2}\right) \{j, j, i + 1, \ldots, i - 1, i, i\} \quad \text{(iii)}
\]

\[
= (-1)^{n+j-i} \left(\frac{1}{4}\right) \{j, j, i + 1, \ldots, i - 1, i, i\} \quad \text{(v)}
\]

\[
= (-1)^{n+j-i} \left(\frac{-1}{4}\right) \{i, i, i + 1, \ldots, i - 1, j, j\} \quad \text{(iv)}
\]

\[
= (-1)^{i-j} \left(\frac{1}{4}\right) \{i, i, 1, 2, \ldots, n - 1, j, j\}. \quad \text{(iii)}
\]

If $j = l - 1, i \neq l$, type $\{jaji\}$,

\[
\{j, j + 1, \ldots, j - 1, j, i\} = (-1)^{j-1-i} \{j, j + 1, \ldots, j - 1, j, i, i\} \quad \text{(iii)}
\]

\[
= (-1)^{j-i} \left(\frac{-1}{2}\right) \{j, j + 1, \ldots, j - 1, j, i, i\} \quad \text{(v)}
\]

\[
= (-1)^{n-5+j-1-i} \left(\frac{-1}{2}\right) \{j, j + 1, \ldots, j - 1, i, i\} \quad \text{(iii)}
\]

\[
= (-1)^{n+i-j} \left(\frac{1}{4}\right) \{j, j, j + 1, \ldots, j - 1, i, i\} \quad \text{(vi)}
\]

\[
= (-1)^{n+i-j} \left(\frac{-1}{4}\right) \{i, i, j + 1, \ldots, j - 1, j, j\} \quad \text{(iv)}
\]

\[
= (-1)^{i-j} \left(\frac{1}{4}\right) \{i, i, 1, 2, \ldots, n - 1, j, j\}. \quad \text{(iii)}
\]
If $j = l$, $i \neq l - 1$, type $\{jjbi\}$,

$$\{j, j, j + 1, \ldots, j - 1, i\} = (-1)^{j-i}\{j, j, i, j + 1, \ldots, j - 2, i, j - 1, i\}$$  (iii)

$$= (-1)^{j-i}\left(-\frac{1}{2}\right)\{j, j, j + 1, \ldots, j - 1, i, i\}$$  (v)

$$= (-1)^{j-i-j}\left(\frac{1}{2}\right)\{i, i, j + 1, \ldots, j - 1, j, j\}$$  (iv)

$$= (-1)^{j-i-j}\left(\frac{1}{2}\right)\{i, i, 1, \ldots, n - 1, j, j\}.$$  (iii)

If $i = l - 1, j \neq l$, type $\{jaii\}$, then

$$\{j, i + 1, \ldots, i - 1, i, i\} = (-1)^{j-i-2}\{j, i + 1, j, \ldots, i - 1, i, i\}$$  (iii)

$$= (-1)^{j-i-2}\left(-\frac{1}{2}\right)\{j, j, i + 1, \ldots, i - 1, i, i\}$$  (v)

$$= (-1)^{j-i-j}\left(\frac{1}{2}\right)\{i, i, i + 1, \ldots, i - 1, j, j\}$$  (iv)

$$= (-1)^{j-i-j}\left(\frac{1}{2}\right)\{i, i, 1, \ldots, n - 1, j, j\}.$$  (iii)

If $j = l, i = l - 1$, type $\{jjii\}$,

$$\{j, j, j + 1, \ldots, i - 1, i, i\} = \{j, j, 1, 2, \ldots, n - 1, i, i\}$$  (iii)

$$= (-1)^{i-j}\{i, i, 1, 2, \ldots, n - 1, j, j\}.$$  (iv)

Finally, if $j = l - 1, i = l$, type $\{jiji\}$, then

$$\{j, i, \ldots, j, i\} = -\{j, i, \ldots, j, i\} = 0,$$  (iv)

and we have computed all of the terms that can occur in the second sum.

We now put everything together. We may assume, without loss of generality, that $i < j$. The term $\{ii, \ldots, j,j\}$ can appear if and only if $i = 1$ and $j = n - 1$, if $k \neq n - 1$, and if $k = n - 1$, then if and only if $i = 1$ and $j = n - 2$. We deal with this case first.

The first sum then consists of a single term of type $\{iijj\}$, a term of type $\{iaij\}$, a term of type $\{ijbj\}$, and $n - 5$ terms of type $\{iabj\}$. As an example, if $n = 5, i - 1, j = 3, k = 4$, then it is given by:

$$\{11233\} + \{12313\} + \{13123\}$$

We conclude that the first sum is equal to $(-1)^{j-i-1}(1 + \frac{1}{4} + \frac{1}{4} + \frac{n-5}{4})\{i, i, 1, \ldots, n - 1, j, j\}$. The second sum consists of a term of type $\{jiji\}$, a term of type $\{jaii\}$, a term of type $\{jjbi\}$, and $n - 3$ terms of type $\{jabi\}$. In our example, it is given by:

$$\{31231\} + \{32313\} + \{33121\}$$

We conclude that it is equal to $(-1)^{j-i-1}(0 + \frac{1}{2} + \frac{1}{2} + \frac{n-5}{4})\{i, i, 1, \ldots, n - 1, j, j\}$, concluding the proof in this case.
We next deal with the case \( j = i + 1 \), for \( i < n - 1 \). The first sum consists of a term of type \( \{(iibj) \} \), a term of type \( \{ijij\} \), a term of type \( \{iajj\} \), and \( n - 5 \) terms of type \( \{iabj\} \). It is equal to \((-1)^{i-j}(\frac{1}{2} + \frac{1}{2} + \frac{n-5}{4})\{i, i, 1, \ldots, n-1, j, j\}\).

The second sum consists of a term of type \( \{(jibi)\} \), a term of type \( \{jjii\} \), a term of type \( \{jaji\} \), and \( n - 5 \) terms of type \( \{jabi\} \). It is equal to \((-1)^{i-j}(\frac{1}{4} + \frac{1}{4} + \frac{n-5}{4})\{i, i, 1, \ldots, n-1, j, j\}\), and so we are done in this case.

Finally assume that \( j > i + 1 \) and that we are not in the first case. This can only happen if \( n > 5 \). In this case the first sum consists of a term of type \( \{(iibj)\} \), a term of type \( \{ijbj\} \), a term of type \( \{iaij\} \), a term of type \( \{iajj\} \), and \( n - 6 \) terms of type \( \{iabj\} \). Thus the first sum is equal to \((-1)^{i-j}(\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{n-6}{4})\{i, i, 1, \ldots, n-1, j, j\}\).

The second sum consists of a term of type \( \{(jibi)\} \), a term of type \( \{jjbi\} \), a term of type \( \{jaii\} \), and \( n - 6 \) terms of type \( \{jabi\} \), summing to \((-1)^{i-j}(\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{n-6}{4})\{i, i, 1, \ldots, n-1, j, j\}\), thus completing the proof of part (i).

**Proof of (ii)** By 3.8.2(i), we have

\[
\frac{\partial^2 \Omega_k}{\partial x_i^2} = 2(-1)^k \sum_{l=1}^{n-2} \{i, l, l+1, \ldots, \hat{k}, \ldots, n-1, l, 1, \ldots, 1, l-1, i\}
\]

We follow the same strategy as before. If \( l \neq i \) and \( i \neq l - 1 \), so the term is of type \( \{iabi\} \), we can cycle the inner \( n - 2 \) letters,

\[
\{i, l, l+1, \ldots, l-2, l-1, i\} = \{i, l-1, l, \ldots, l-3, l-2, i\}
\]

(iii),(vii),(viii)

If \( l = i \), type \( \{iibi\} \), then

\[
\{i, i, i+1, \ldots, i-2, i-1, i\} = 2\{i, i-1, i, \ldots, i-3, i-2, i\}
\]

(iii),(v),(viii)

and if \( l - 1 = i \), type \( \{iaii\} \), then

\[
\{i, i+1, i+2, \ldots, i-1, i, i\} = 2\{i, i+2, i+3, \ldots, i, i+1, i\}
\]

(iii),(vi),(vii)

Combining these rules, we see that there are \( n - 2 \) terms of type \( \{iabi\} \), and they all are equal to \( \frac{1}{2}\{i, i, \ldots, i-1, i\} \), while there are two terms of type \( \{iaii\} \) and \( \{iibi\} \), both equal to \( \{i, i, \ldots, i-1, i\} \), and part (ii) now follows immediately.

**Proof of (iii)** Let \( a_1, \ldots, a_{n-2} \) be the sequence \( 1, 2, \ldots, i-1, i+1, \ldots, n-1 \). We treat first the case \( k = a_s \) and \( j = a_{s+1} \) for \( t \neq i - 1 \), where we read the indices modulo \( n - 2 \).

Note that, when \( s < n - 1 \), this means that \( j = k + 1 \). To make the proof easier to read, we have assumed \( s < n - 1 \), but the argument applies without change to the case \( s = n - 1 \).
We have

\[
\frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_{j+1}}{\partial x_i \partial x_{j+1}} = (-1)^j \sum_{l=1}^{n-2} \{i, l, l+1, \ldots, j, \ldots, n-1, 1, 2, \ldots, l-1, j\} \\
+ (-1)^j \sum_{l=1}^{n-2} \{j, l, l+1, \ldots, j, \ldots, n-1, 1, 2, \ldots, l-1, i\} \\
+ (-1)^j \sum_{l=1}^{n-2} \{i, l, l+1, \ldots, j+1, \ldots, n-1, 1, 2, \ldots, l-1, j+1\} \\
+ (-1)^j \sum_{l=1}^{n-2} \{k, l, l+1, \ldots, j+1, \ldots, n-1, 1, 2, \ldots, l-1, i\}.
\]

We group up the terms in the first and the third sum. Suppose \( l \not\in \{j, j+1\} \).

\[
(-1)^j \left( \{i, l, l+1, \ldots, \hat{j}, \ldots, n-2, l-1, j\} + \{i, l, l+1, \ldots, \hat{j+1}, \ldots, n-2, l-1, j+1\} \right)
\]

\[
= (-1)^{j+l-2-i-1} \{i, l, \ldots, \hat{j}, j+1, \ldots, n-2, j+1, l-1, j\} \\
+ (-1)^{j+l-2-i-1} \{i, l, \ldots, \hat{j}, j+1, \ldots, n-2, j, l-1, j+1\} \quad (iii)
\]

\[
= (-1)^{j,i} \{i, l, \ldots, \hat{j}, j+1, \ldots, n-2, l-1, j, j+1\} \quad (v)
\]

If \( l = j \), the corresponding terms are:

\[
(-1)^j \left( \{i, j+1, j+2, \ldots, j-2, j-1, j\} + \{i, j+2, \ldots, j-2, j-1, j+1\} \right).
\]

If \( i = j-1 \) the above sum is zero by (iv). Otherwise, the conditions for applying rule (vii) are met, so we may cycle entries labeled 2 through \( n-2 \).

\[
= (-1)^{j+1} \{i, j+2, \ldots, j-2, j+1, j-1, j\} + \{i, j+2, \ldots, j-2, j, j-1, j+1\} \quad (iii),(vii)
\]

\[
= (-1)^{j+2} \{i, j+2, \ldots, j-1, j, j+1\}. \quad (v)
\]

If \( l = j+1 \), the corresponding terms are:

\[
(-1)^j \left( \{i, j+2, j+3, \ldots, j-2, j-1, j+1\} + \{i, j+2, \ldots, j-2, j-1, j, j+1\} \right)
\]

\[
= 2(-1)^{j+2} \{i, j+2, j+3, \ldots, j-2, j-1, j+1\}.
\]

The analysis of the terms in the second and fourth sum mirrors the above argument. For terms with \( l \not\in \{j, j+1\} \)

\[
(-1)^j \left( \{j, l, l+1, \ldots, \hat{j}, j+1, \ldots, n-2, l-1, i\} + \{j+1, l, l+1, \ldots, j, j+1, \ldots, n-2, l-1, i\} \right)
\]

\[
= (-1)^{j+l+1-i-1} \{j, l, j+1, l+1, \ldots, \hat{j}, j+1, \ldots, n-2, l-1, i\} \\
+ (-1)^{j+l+1-i-1} \{j+1, l, j+1, l+1, \ldots, \hat{j}, j+1, \ldots, n-2, l-1, i\} \quad (iii)
\]

\[
= (-1)^i \{j, j+1, l, l+1, \ldots, j, j+1, \ldots, n-2, l-1, i\} \quad (vi)
\]

\[
= (-1)^{i-1} \{i, l-1, l+1, \ldots, \hat{j}, j+1, \ldots, n-2, j, j+1\} \quad (iv)
\]
Suppose now \( l = j \), and compute
\[
(-1)^j \left( \{j, j + 1, j + 2, \ldots, j - 2, j - 1, i\} + \{j + 1, j + 2, \ldots, j - 2, j - 1, i\} \right)
\]
\[
= 2(-1)^j \{j, j + 1, j + 2, \ldots, j - 2, j - 1, i\} - \{j + 1, j + 2, \ldots, j - 2, j, j + 1\}. \quad (iv)
\]

If \( l = j + 1 \), then the corresponding terms are:
\[
(-1)^j \left( \{j, j + 2, j + 3, \ldots, j - 1, j + 1, i\} + \{j + 1, j + 2, j + 3, \ldots, j - 1, j, i\} \right).
\]

If \( i = j + 2 \), then the sum vanishes by (iv). Otherwise, we can apply rule (viii), and cycle symbols labeled 3 through \( n - 1 \).
\[
= (-1)^{j+1} \{j, j + 2, j + 1, j + 3, \ldots, j - 1, i\} + \{j + 1, j + 2, j, j + 3, \ldots, j - 1, i\} \quad (iii), (vii)
\]
\[
= (-1)^{j-1} \{i, j - 1, j + 2, \ldots, j - 2, j, j + 1\}. \quad (iv)
\]

Now observe that, as long \( l - 1 \neq i \) and \( l \neq i \), by cycling symbols 2 through \( n - 3 \), we have
\[
(-1)^{j} \{i, l, \ldots, j, j + 1, \ldots, l - 1, j, j + 1\} = \frac{(-1)^i}{2} \{i, i, i + 1, \ldots, j, j + 1, \ldots, i - 1, j, j + 1\}.
\]

We now put everything together. We examine first the case \( i = j - 1 \). In this case, by the above observation, we see that the first and the third sum add up to
\[
\left(\frac{n - 5}{2} + 2 + 1\right)(-1)^{j-1} \{i, i, \ldots, j, j + 1\},
\]
while the second and the fourth sum add up to
\[
\left(\frac{n - 4}{2} + 1 + 1\right)(-1)^{j-1} \{i, i, \ldots, j, j + 1\}
\]
and hence the total is equal to \( n \cdot (-1)^{j-1} \{i, i, \ldots, j, j + 1\} \), as desired. The case \( i = j + 2 \) is similar, with the sums swapping values. For \( i \not\in \{j - 1, j + 2\} \), both pairs of sums add up to
\[
\left(\frac{n - 4}{2} + 1 + 1\right)(-1)^{j-1} \{i, i, \ldots, j, j + 1\},
\]
and so we are done.

Now suppose that \( i = a_l, j = a_s \) and \( k = a_{s+r} \). The base case \( r = 1 \) was proven above. Assume that we do not have \( s < l < s + r \). Write \( k = j + t \). Then, we have
\[
\frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_{j+t}}{\partial x_i \partial x_{j+t}} = \frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_{j+1}}{\partial x_i \partial x_{j+1}} + \frac{\partial^2 \Omega_{j+1}}{\partial x_i \partial x_{j+1}} - \frac{\partial^2 \Omega_{j+1+t}}{\partial x_i \partial x_{j+1+t}}.
\]
By the induction hypothesis,

\[
\begin{align*}
& n \cdot (-1)^{i+j+k-1} \{i, i, i+1, \ldots, j, j+1, \ldots, i-1, j, j+1\} \\
& + n \cdot (-1)^{i+j+k+1} \{i, i, i+1, \ldots, j, j+1, \ldots, i-1, j+1, j+t\} \\
& = n \cdot (-1)^{j+t} \{i, i, i+1, \ldots, i-1, j, j+1\} + \{i, i, i+1, \ldots, i-1, j, j+1, t\} \\
& = n \cdot (-1)^{j+t-1} \{i, i, i+1, \ldots, i-1, j+1, j+t\} \\
& = n \cdot (-1)^{i+j+j+t-1} \{i, i, i+1, \ldots, j, j+1, \ldots, i-1, j, j+t\} \\
& \tag{iii}
\end{align*}
\]

as required. If we have \( s < l < s + r, \) the above argument does not apply, as it might happen that \( j + 1 = i, \) so that the first use of (iii) above is not valid. In that case, we use the fact that we read indices \( a_1, \ldots, a_{n-2} \) modulo \( n - 2, \) and run the induction step in the other direction, proving that if result is true for \( j = a_s \) and \( k, \) then it is true for \( j = a_{s-1} \) and \( k. \)

**Proof of (iv)** It suffices to prove the result for a single value of \( j. \) Indeed, suppose \( i, k \) and \( j_1 < j_2 \) are pairwise distinct. Subtracting the right hand sides of the identities we seek to prove, and dividing them by \( n, \) we compute

\[
\begin{align*}
& (-1)^{i+j+k} \{i, j_1, i+1, \ldots, i-1, k, i\} - (-1)^{i+j_2+k} \{i, j_2, i+1, \ldots, i-1, k, i\} \\
& = (-1)^{i+j_2+k} \{i, j_1, j_2, i+1, \ldots, i-1, k\} - \{i, j_2, j_1, i+1, \ldots, i-1, k\} \\
& = (-1)^{i+j_2+k-1} \{j_1, j_2, i, i+1, \ldots, i-1, k, i\} \\
& = (-1)^{i+j_2+k} \{j_1, j_2, i, i+1, \ldots, i-1, k, i\} \\
& = (-1)^{i+j+k-1} \{i, i, i+1, \ldots, i-1, j_1, j_2\} \\
& \tag{vii}
\end{align*}
\]

This agrees with the difference of the left hand sides, proving the claim. Note that a similar argument applies to \( k \) as well. We assume \( j = i - 1. \) Now observe that

\[
\begin{align*}
& \left( \frac{\partial^2 \Omega_i}{\partial x_i \partial x_i} - \frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_k}{\partial x_i \partial x_k} \right) - \left( \frac{\partial^2 \Omega_j}{\partial x_i \partial x_j} - \frac{\partial^2 \Omega_k}{\partial x_i \partial x_k} \right) \\
& = \frac{\partial^2 \Omega_i}{\partial x_i \partial x_i} - 2 \frac{\partial^2 \Omega_j}{\partial x_i \partial x_j}.
\end{align*}
\]

Thus, by the property (iii) we have proven above, it suffices to prove that this is equal to

\[
\begin{align*}
& n(-1)^{i+i-1+k-1} \left( 2\{i, i-1, i+1, \ldots, k, \ldots, i-1, k, i\} + \{i, i, i+1, \ldots, k, \ldots, i-2, i-1, k\} \right).
\end{align*}
\]
We group terms in the first and the third sum. Assuming that 

$$\frac{\partial^2 \Omega_i}{\partial x_l \partial x_i} - 2 \frac{\partial^2 \Omega_j}{\partial x_l \partial x_j} = (-1)^i \cdot 2 \sum_{l=1}^{n-2} \{i, l, l + 1, \ldots, \hat{i}, \ldots, l - 2, l - 1, i\}$$

$$+ (-1)^i \cdot 2 \sum_{l=1}^{n-2} \{i, l, l + 1, \ldots, \hat{j}, \ldots, l - 2, l - 1, i - 1\}$$

$$+ (-1) \cdot 2 \sum_{l=1}^{n-2} \{i - 1, l, l + 1, \ldots, \hat{j}, \ldots, l - 2, l - 1, i\}$$

We group terms in the first and the third sum. Assuming that \(l \not\in \{i - 1, i\}\), we have

\[
(-1)^i \{i, l, l + 1, \ldots, l - 1, l - 1, \} + (-1)^{i-1+1} \{i, l, l + 1, \ldots, l - 1, i\}
\]

\[
= (-1)^{i-1-1-l-1} \{i, l, i - 1, \ldots, l - 1, i\}\]

\[
= (-1)^{i-1-1-l} \{i, i - 1, l + 1, \ldots, l - 2, l - 1, i\}\]

\[
= (-1)^{i-1-l} \{i, i - 1, l + 1, \ldots, l - 1, \ldots, i - 2, l - 1, i\}\]

For terms in the second sum, with \(l \not\in \{i - 1, i\}\), we have

\[
(-1)^i \{i, l, l + 1, \ldots, l - 2, l - 1, i - 1\}\]

\[
= (-1)^i \left(\frac{1}{2}\right) \{i, i, i + 1, \ldots, i - 2, l - 1, i - 1\}\]

Now observe that we have the following identities, valid for any \(l_1 < l_2\).

\[
(-1)^{l_1} \{i, i - 1, i + 1, \ldots, \hat{j}, \ldots, i_1, \ldots, i - 2, l_1, i\} -
\]

\[
(-1)^{l_2} \{i, i - 1, i + 1, \ldots, \hat{j}, \ldots, i_2, \ldots, i - 2, l_2, i\}
\]

\[
= (-1)^{l_1-l_2-(i-2)} \{i, i - 1, i + 1, \ldots, i - 2, l_1, i_1, \} + \{i, i - 1, i + 1, \ldots, i - 2, l_1, l_2, i\}\]

\[
= (-1)^{l_1+l_2-i+1} \{i, i - 1, i + 1, \ldots, l - 2, i, l_1, l_2\}\]

\[
(\text{iii}), (\text{vii})
\]

and

\[
(-1)^{l_1} \{i, i, i + 1, \ldots, i - 2, l_1, i - 1\} - (-1)^{l_2} \{i, i, i + 1, \ldots, i - 2, l_2, i - 1\}
\]

\[
= (-1)^{l_1+l_2-i+2} \{i, i, i + 1, \ldots, i - 2, l_2, l_1, i - 1\} + \{i, i, i + 1, \ldots, i - 2, l_1, l_2, i - 1\}\]

\[
= (-1)^{l_2+l_1+i+1} \{i, i, i + 1, \ldots, i - 2, l_1, l_2\}\]

\[
= 2 \cdot (-1)^{l_1+l_2+i} \{i, i - 1, i + 1, \ldots, i - 2, i, l_1, l_2\}\]

\[
(\text{iii}), (\text{vii})
\]

From these identities, taking \(l_i\) to be \(l\) and \(k\), we conclude that the sum of all terms with \(l \not\in \{i - 1, i\}\), is equal to

\[
(n - 4) \cdot (-1)^i \left(2 \{i, i - 1, i + 1, \ldots, i - 2, k, i\} + \{i, i, i + 1, \ldots, i - 2, i - 1, k\}\right).
\]
Now recall our observation that it suffices to prove the identity for any particular value of \( k \), and choose \( k = i - 2 \), so the above is equal to
\[
(n - 4) \cdot (-1)^k (2\{i, i - 1, i + 1, \ldots, i - 3, i - 2, i\} + \{i, i, i + 1, \ldots, i - 3, i - 1, i - 2\})
\]
The terms with \( l \in \{i - 1, i\} \) contribute
\[
+ 2 \cdot (-1)^l (\{i, i - 1, i + 1, \ldots, i - 3, i - 2, i\} + \{i, i + 1, i + 2, \ldots, i - 2, i - 1\})
\]
\[
+ 2 \cdot (-1)^l (\{i, i, i + 1, \ldots, i - 3, i - 2, i - 1\} + \{i, i, i + 1, i + 2, \ldots, i - 2, i, i - 1\})
\]
This sum simplifies to
\[
+ 4 \cdot (-1)^l (\{i, i - 1, i + 1, \ldots, i - 3, i - 2, i\} + \{i, i + 1, i + 2, \ldots, i - 2, i - 1\})
\]
\[
+ 2 \cdot (-1)^l (\{i, i, i + 1, \ldots, i - 3, i - 2, i - 1\} + \{i - 1, i + 1, i + 2, \ldots, i - 2, i, i - 1\})
\]
We have
\[
4 \cdot (-1)^l \{i, i + 1, i + 2, \ldots, i - 2, i - 1, i\}
\]
\[
= 4 \cdot (-1)^{l+1} (\{i, i + 1, i + 2, \ldots, i - 3, i, i - 1, i - 2\} + \{i, i + 1, i + 2, \ldots, i - 3, i - 1, i - 2\})
\]
\[
= 4 \cdot (-1)^l \left( \frac{1}{2} (i, i, i + 1, \ldots, i - 3, i - 1, i - 2) - \{i, i + 1, i + 2, \ldots, i - 3, i - 1, i - 2\} \right)
\]
\[
= 4 \cdot (-1)^l \left( \frac{1}{2} (i, i, i + 1, \ldots, i - 3, i - 1, i - 2) - \{i, i + 1, i - 1, \ldots, i - 3, i - 2, i\} \right).
\]

Focusing on the final term, we compute
\[
4 \cdot (-1)^{l+1} \{i, i + 1, i - 1, \ldots, i - 3, i - 2, i\}
\]
\[
= 4 \cdot (-1)^l (\{i, i - 1, i + 1, \ldots, i - 3, i - 2, i\} + \{i - 1, i + 1, i, \ldots, i - 3, i - 2, i\})
\]
\[
= 4 \cdot (-1)^l \left( \{i, i - 1, i + 1, \ldots, i - 3, i - 2, i\} - \frac{1}{2} (i - 1, i + 1, i + 2, \ldots, i - 2, i, i) \right)
\]
\[
= 4 \cdot (-1)^l \left( \{i, i - 1, i + 1, \ldots, i - 3, i - 2, i\} + \{i, i, i + 1, \ldots, i - 3, i - 1, i - 2\} \right).
\]
We deduce that the sum of the remaining terms is equal to
\[
4 \cdot (-1)^l (2\{i, i - 1, i + 1, \ldots, i - 3, i - 2, i\} + \{i, i, i + 1, \ldots, i - 3, i - 1, i - 2\})
\]
concluding the proof.
Chapter 4

The unprojection construction

4.1 Overview

In this chapter we prove the following theorem.

**Theorem 4.1.1** (Minimization theorem). Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n$, defined over the field $\mathbb{Q}$. Suppose that the set $C(\mathbb{Q}_p)$ is non-empty for every prime $p$. Let $E$ be the Jacobian of $C$, defined by a minimal Weierstrass equation $W$,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$ 

Then one can choose coordinates on $\mathbb{P}^{n-1}$, and then a $\mathbb{Z}$-integral genus one model $F_\bullet$ of $C$ with the associated invariant differential $\omega$, such that, for every prime $p$, there exists an isomorphism $\gamma : E \to C$, defined over $\mathbb{Q}_p$, with

$$\omega = \gamma^* \left( \frac{dx}{2y + a_1x + a_3} \right).$$

We say such a genus one model is a *minimal* model of $C$. Furthermore, the invariants $c_4(F_\bullet)$ and $c_6(F_\bullet)$, as defined in Chapter 2, are equal to $(n-2)^4c_4(W)$ and $(n-2)^6c_6(W)$, where $c_4(W)$ and $c_6(W)$ are invariants of the equation $W$, as defined in Chapter III of [Sil09].

**Remark 4.1.2.** The powers of $(n-2)$ appearing in $c_k(F_\bullet)$ are a matter of convention - they appear because we have normalized the invariants of the $\Omega$-matrix to agree with the invariants of the alternative definition of $\Omega$-matrix given in [Fis18]. In [FS14], in the case $n = 5$, the invariants of $\Omega$ are normalized so that the factors of $(n-2)^k$ do not appear. Essentially, as we will see from the proof of Theorem 4.1.1, the difference between these normalizations is accounted for by Lemma 3.4.7.

The theorem is proved by an induction on $n$. The base case of the induction, $n = 3$, is Theorem 1.1 of [CFS10]. Our induction step can be viewed as a generalization of the method used to deduce cases $n = 4$ and $n = 5$ from the case $n = 3$ in [CFS10] and [? ].

Our main tool will be the technique of *unprojection*, introduced in [KM83]. Unprojection was used to obtain minimal free resolutions of genus one normal curves by Fisher in [Fis06], and our
results can be viewed as refinements of his. Reid and Papadakis have also studied unprojection extensively, and they give a more intrinsic point of view in [PR00].

The first section consists of an informal discussion motivating and explaining our results. We then prove a technical result in homological algebra that will serve as the induction step in our proofs. We then prove Lemma 3.3.2, i.e. that the differential form on a genus one normal curve $C$ constructed from its $\Omega$-matrix is regular. We then prove, assuming Theorem 3.3.5, the local version of the minimization theorem and from it deduce the global version.

**Remark 4.1.3.** Note that the proof of the formula for the Jacobian, i.e. Theorem 3.3.5, which we give in Chapter 5 uses Lemma 3.3.2. Thus, to clarify, formally the proof of Theorem 4.1.1 proceeds as follows: in this chapter we prove, using unprojection, Lemma 3.3.2. In Chapter 5 we deduce Theorem 3.3.5 from Lemma 3.3.2 and Lemma 4.5.3, via a complex analytic calculation. Note that Lemma 4.5.3 does not really depend on the methods of unprojection, and is proved just using the results of Chapter 3. Then using Theorem 3.3.5 and unprojection we deduce Theorem 4.7.1, and from this theorem we deduce Theorem 4.1.1.

### 4.2 Motivation - plane cubics

As a motivation for what follows, we now describe the unprojection construction in the classical setting of genus one normal curves of degree 3, i.e. smooth plane cubics. Our exposition is closely related to the argument used in Section 3 of [CFS10].

Suppose we are given a genus one normal curve $C_4 \subset \mathbb{P}^3$ of degree 4, defined over a field $k$, and suppose that $C$ has a $k$-rational point $P \in C(k)$. As the curve $C_4$ has a $k$-rational point, we can identify it with its Jacobian $E$. Let $D$ be a degree 4 divisor on $C_4$ that corresponds to a hyperplane section of $C_4$ passing through the point $P$, and note that $C_4$ is the embedding of $E$ into $\mathbb{P}^3$ induced by the complete linear system $|D|$.

Consider the linear projection map $\pi : \mathbb{P}^3 \to \mathbb{P}^2$ from $P$. As $C_4$ is a smooth curve, $\pi$ extends to a regular map from $C_4$ onto its image, which we will denote by $C_3$. The curve $C_3 \subset \mathbb{P}^2$ is the image of $E$ under the embedding induced by the complete linear system $|D - P|$, and hence a genus one normal curve of degree 3.

It is a simple matter to obtain an equation defining $C_3$ from the equations defining the curve $C_4$. By making a linear change of coordinates if necessary, we assume that $P = (0 : 0 : 0 : 1)$. Then the projection $\pi$ is given by $(x_1 : x_2 : x_3 : x_4) \mapsto (x_1 : x_2 : x_3)$. The curve $C_4$ is defined by two quadratic forms $p_1$ and $p_2$, in the variables $x_1, x_2, x_3$ and $x_4$. As $Q_1$ and $Q_2$ vanish at the point $P$, we have

\begin{align*}
  p_1 &= x_4 l_1 + q_1, \\
  p_2 &= x_4 l_2 + q_2,
\end{align*}

for some $l_1, l_2, q_1, q_2 \in k[x_1, x_2, x_3]$, with the forms $l_i$ and $q_i$ being of degree 1 and 2 respectively. We obtain a ternary cubic form $f$ vanishing on $C_3$ by eliminating the variable $x_4$,

\begin{align*}
  f &= l_1 p_2 - l_2 p_1 \\
  &= l_1 q_2 - l_2 q_1 \in k[x_1, x_2, x_3].
\end{align*}
4.2. MOTIVATION - PLANE CUBICS

The projection $\pi$ induces an isomorphism from $C_4$ onto $C_3$, with the inverse given by

$$\phi : (x_1 : x_2 : x_3) \mapsto (x_1 l_1 : x_2 l_1 : x_3 l_1 : -q_1) = (x_1 l_2 : x_2 l_2 : x_3 l_2 : -q_2),$$

and the point $\pi(P) \in C_3$ is defined by $l_1 = l_2 = 0$.

The opposite direction, going from equations for a plane cubic $C_3 \subset \mathbb{P}^2$ and a point $Q \in C_3(k)$ to equations for a quadric intersection $C_4 \subset \mathbb{P}^3$ that projects onto $C_3$, is the simplest example of an unprojection.

Suppose that $C_3$ is defined by a ternary cubic $f \in k[x_1, x_2, x_3]$, and that $Q$ is defined by a pair of linear forms $l_1, l_2 \in k[x_1, x_2, x_3]$. As $f(Q) = 0$, the cubic $f$ is in the ideal of $k[x_1, x_2, x_3]$ generated by $l_1$ and $l_2$, and hence there exist quadratic forms $q_1, q_2 \in k[x_1, x_2, x_3]$ with $f = l_1 q_2 - l_2 q_1$.

We set $p_1 = x_1 l_1 + q_1$ and $p_2 = x_2 l_2 + q_2$, and let $C_4 \subset \mathbb{P}^2$ be the curve defined by $p_1$ and $p_2$. The map $\phi$ defined above is an isomorphism from $C_3$ onto $C_4$, and takes the point $Q$ to the point $P = (0 : 0 : 0 : 1)$. Thus $C_4$ is a genus one normal of degree 4, and projection from $P$ maps $C_4$ onto the curve $C_3$.

**Remark 4.2.1.** The key observation for the proof of the minimization theorem, is that the $\omega$-invariants of the ternary cubic $f$ and quaternary quadrics $p_1$ and $p_2$, constructed as above, are the same.

This fact can be proved by a brute force calculation, or one can check that the invariant differentials associated to the two genus one models are identified under the isomorphism $\phi$. The second method is better suited to generalization, as we shall see later in the chapter.

**Remark 4.2.2.** Suppose that we have $k = \mathbb{Q}$ or $\mathbb{Q}_p$ for a prime $p$. If the coefficients of quadrics $p_1$ and $p_2$ are integral, then so are the coefficients of the cubic $f$.

Conversely, if the cubic $f$ has integral coefficients, and we take $l_1$ and $l_2$ to be the basis for the space of linear forms with integer coefficients that vanish on the point $Q$, then we can choose quadrics $q_1$ and $q_2$ so that they have integral coefficients, and hence so do the quadrics $p_1$ and $p_2$.

Thus, combining this observation with the previous remark, if the minimization theorem holds for the curve $C_3$, it holds for the curve $C_4$, and conversely. This is the key step in the proof given in Section 3 of [CFS10].

**Reformulation in terms of minimal free resolutions.** We now give a different point of view on the construction of $p_1$ and $p_2$, that will be better suited to generalization. Let $R = k[x_1, x_2, x_3]$, and consider the homogeneous ideals $J = (l_1, l_2) \subset R$ and $I = (f) \subset R$. The minimal free resolution of the ideal $J$ is given by the Koszul complex associated to the regular sequence $l_1, l_2$:

$$0 \rightarrow R(-2) \xrightarrow{(l_1)} R(-1)^2 \xrightarrow{(l_2 - l_1)} R \rightarrow 0,$$
while the minimal free resolution of the ideal \( I \) is simply
\[
0 \to R(-3) \xrightarrow{(F)} R \to 0.
\]
The inclusion \( I \subset J \) induces a map of free resolutions of \( I \) and \( J \), represented by the commutative diagram
\[
\begin{array}{ccccccccc}
0 & \to & 0 & \to & R(-3) & \xrightarrow{(F)} & R & \to & 0 \\
\downarrow & & \downarrow & & \downarrow \beta & \downarrow & \downarrow \text{id} & & \\
0 & \to & R(-2) & \xrightarrow{\beta \left( l_2 - l_1 \right)} & R & \to & 0
\end{array}
\]
From the diagram we deduce that the map \( \beta \) is represented by the column vector \( \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \), where \( q_1 \) and \( q_2 \) are quadratic forms that satisfy \( f = l_2 q_1 - l_1 q_2 \). Thus the map \( \beta \) encodes the equations of the curve \( C_4 \).

**General picture for \( n \geq 4 \).** Let \( C_n \subset \mathbb{P}^{n-1} \) be a genus one normal curve of degree \( n \), and let \( Q \in C_n(k) \) be a \( k \)-rational point. Let \( R = k[x_1, \ldots, x_n] \), and let \( I_n \) and \( J \) be the homogeneous ideals of \( R \) defining \( C_n \) and \( Q \) respectively. Let \((F, \phi) \) and \((G, \psi) \) be their respective minimal free resolutions. The inclusion \( I_n \subset J \) induces a map of the free resolutions, represented by the commutative diagram:
\[
\begin{array}{ccccccccccc}
0 & \to & F_{n-2} & \xrightarrow{\phi_{n-2}} & F_{n-3} & \xrightarrow{\phi_{n-3}} & \ldots & \xrightarrow{\phi_1} & F_1 & \xrightarrow{\phi_0} & F_0 \\
\downarrow & & \downarrow \beta_{n-2} & & \downarrow \beta_{n-3} & & \ldots & & \downarrow \beta_2 & & \downarrow \beta_1 \\
G_{n-1} & \xrightarrow{\psi_{n-2}} & G_{n-2} & \xrightarrow{\psi_{n-3}} & \ldots & \xrightarrow{\psi_2} & G_2 & \xrightarrow{\psi_1} & G_1 & \xrightarrow{\psi_0} & G_0
\end{array}
\]
The top row is a resolution model of \( C_n \), as described in Chapter 3. Let \( l_1, l_2, \ldots, l_{n-1} \) be a basis for the space of linear forms vanishing at \( Q \). The bottom row can then be described explicitly as the Koszul complex associated to the sequence \( l_1, l_2, \ldots, l_{n-1} \). The maps \( \psi_i \) are represented by matrices of linear forms, and each \( G_i \) is a direct sum of copies of \( R(-i) \).

Now fix a basis for each module \( F_i \) in \( F \) and \( G_i \in G \), with the following requirement. The ideals \( I \) and \( J \) are Gorenstein, and so as explained in Chapter 2, \( F \) and \( G \) are self-dual, and there exist perfect pairings \( F_i \otimes F_{n-2-i} \to k \) and \( G_i \otimes G_{n-1-i} \to k \). We require that the basis of \( F_i \) is dual to the basis of \( F_{n-2-i} \), and similarly that the basis of \( G_i \) is dual to the basis of \( G_{n-1-i} \), for each \( i \leq (n-1)/2 \).

In particular, we have \( F_{n-2} \cong R(-n) \) and \( G_{n-2} \cong R(-n+2)^{n-1} \), and so the map \( \beta_{n-2} \) is represented by a column vector whose entries are quadratic forms \( h_1, h_2, \ldots, h_{n-1} \). Let \( f_1, \ldots, f_m \) be a set of generators of \( I \). Introduce a new variable \( x_n \), and let \( I_{n+1} \) be the homogeneous ideal of the ring \( k[x_1, \ldots, x_{n+1}] \) generated by \( f_1, f_2, \ldots, f_m, x_{n+1}l_1 + h_1, x_{n+1}l_2 + h_2, \ldots, x_{n+1}l_{n-1} + h_{n-1} \).

Let \( C_{n+1} \subset \mathbb{P}^n \) be the variety defined by the ideal \( I_{n+1} \). In the next section, we show that \( C_{n+1} \) is a genus one normal curve of degree \( n + 1 \), containing the point \( P = (0 : 0 : \ldots : 0 : 1) \). Linear projection from \( P \) defines an isomorphism from \( C_{n+1} \) onto \( C_n \), that takes the point \( P \) to the point \( Q \). We also prove analogues of other properties we discussed in the case \( n = 3 \).

We will in fact construct a minimal free resolution of the ideal \( I_{n+1} \), from the data of the
resolutions $F$, $G$ and the comparison map $\beta$.

### 4.3 The mapping cone construction

In this section we give an algebraic construction that will provide the induction step for our later arguments. Our work is a refinement of the results of Section 9 of [Fis06], and our notation and exposition will follow [Fis06] and [KM83] closely.

The arguments in this and the next section are made in the abstract language of commutative algebra. In Section 4.5, we give an explicit description of our construction in a simple case.

We begin with the following general construction. Let $R = S[x_1, \ldots, x_{m-1}]$ be a graded ring. Throughout we consider graded $R$-modules.

**Mapping cones.** We recall some basic facts about mapping cones. For a reference see Section 1.5 of [Wei95].

**Definition 4.3.1.** Let $\alpha : A_* \to B_*$ be a map of chain complexes $(A_*, d_A)$ and $(B_*, d_B)$. The mapping cone $M(\alpha)$ of $\alpha$ is the chain complex with $M(\alpha)_n = B_n \oplus A_{n-1}$ and the differential $d^n$ represented by the matrix

$$d^n = \begin{pmatrix} d^n_B & -\alpha_{n-1} \\ 0 & -d^n_{A-1} \end{pmatrix},$$

i.e. $d^n(a_{n-1}, b_n) = (-d^n_{A-1}(a_{n-1}), -\alpha_{n-1}(a_{n-1}) + d^n_B(b_n))$.

**Lemma 4.3.2.** Suppose that $\alpha, \beta : A_* \to B_*$ are chain homotopic morphisms of chain complexes. The mapping cones $M(\alpha)$ and $M(\beta)$ are isomorphic, with an isomorphism determined by a choice of homotopy between $\alpha$ and $\beta$.

**Proof.** Let $h : A_i \to B_{i+1}$ be a chain homotopy, with $\beta_n - \alpha_n = h_{n-1}d^n_A + d^{n+1}_Bh_n$. We define maps $u_n : M(\alpha)_n \to M(\beta)_n$ by

$$u_n = \begin{pmatrix} id_{B_n} & h_{n-1} \\ 0 & id_{A_{n-1}} \end{pmatrix}.$$

We verify that the $u_n$ define a chain map

$$d^n_{M(\beta)}u_n = \begin{pmatrix} d^n_B & -\beta_{n-1} \\ 0 & -d^n_{A-1} \end{pmatrix} \begin{pmatrix} id_{B_n} & h_{n-1} \\ 0 & id_{A_{n-1}} \end{pmatrix} = \begin{pmatrix} d^n_B & d^n_Bh_{n-1} - \beta_{n-1} \\ 0 & -d^n_{A-1} \end{pmatrix},$$

which is equal to

$$u_{n-1}d^n_{M(\alpha)} = \begin{pmatrix} id_{B_{n-1}} & h_{n-2} \\ 0 & id_{A_{n-2}} \end{pmatrix} \begin{pmatrix} d^n_B & -\alpha_{n-1} \\ 0 & -d^n_{A-1} \end{pmatrix} = \begin{pmatrix} d^n_B & -\alpha_{n-1} - h_{n-2}d^n_{A-1} \\ 0 & -d^n_{A-1} \end{pmatrix}.$$

An inverse is provided by the maps $v_n : M(\beta)_n \to M(\alpha)_n$

$$v_n = \begin{pmatrix} id_{B_n} & -h_{n-1} \\ 0 & id_{A_{n-1}} \end{pmatrix}.$$
Proposition 4.3.3. The short exact sequence $B_* \to M(\alpha) \to A_*[1]$ induced by the natural maps gives rise to a long exact sequence of homology modules:

$$\ldots \xrightarrow{\alpha_*} H_{i+1}(B) \to H_{i+1}(M(\alpha)) \to H_i(A) \xrightarrow{\alpha_*} H_i(B) \to H_i(M(\alpha)) \to \ldots$$

Now suppose we are given the following data.

**Definition 4.3.4 (Unprojection data).**

(i) $(F_*, \phi)$ and $(G_*, \psi)$ be chain complexes of graded $R$-modules, of length $n-2$ and $n-1$ respectively, with $F_0 = G_0 = R$.

(ii) Chain maps $\alpha : G_*(-1) \to F_*[-1]$ and $\beta : F_*(-1) \to G_*(-1)$, with $\beta_0 : F_0 \to G_0$ equal to the identity map.

(iii) A null homotopy $\gamma$ for the map $\alpha \circ \beta$. In other words, maps $\gamma_{i+1} : F_i \to F_i$ that satisfy the identity

$$\alpha_i \beta_i = \phi_i \gamma_{i+1} + \gamma_i \phi_i,$$

for all $i$. We furthermore require that $\gamma_1 = 0$.

We summarise this information in the following commutative diagram.

\[ 
\begin{array}{cccccccc}
0 & \rightarrow & F_{n-2}(-1) & \xrightarrow{\phi_{n-2}} & \ldots & \xrightarrow{\phi_3} & F_2(-1) & \xrightarrow{\phi_2} & F_1(-1) & \xrightarrow{\phi_1} & F_0(-1) \\
\downarrow & & \downarrow & & \ldots & & \downarrow & & \downarrow & & \downarrow \\
G_{n-1}(-1) & \xrightarrow{\psi_{n-2}} & G_{n-2}(-1) & \xrightarrow{\psi_{n-2}} & \ldots & \xrightarrow{\psi_3} & G_2(-1) & \xrightarrow{\psi_2} & G_1(-1) & \xrightarrow{\psi_1} & G_0(-1) \\
F_{n-2} & \xrightarrow{\phi_{n-2}} & F_{n-3} & \xrightarrow{\phi_{n-3}} & \ldots & \xrightarrow{\phi_2} & F_1 & \xrightarrow{\phi_1} & F_0 & \xrightarrow{\phi_0} & 0 \\
\end{array} \]

(\*)

Lemma 4.3.5. (i) The maps $h_i : M(\beta)_i := G_i(-1) \oplus F_{i-1} \to F_{i-1}$ given by $h(g, f) = -\alpha_i(g) + \gamma_i(f)$ define a map of chain complexes $h : M(\beta)[1] \to F_*$.

(ii) If we replace the null homotopy $\gamma$ by a different null homotopy $\gamma'$, the resulting map $h' : M(\beta)[1] \to F_*$ is chain homotopic to $h$. The same conclusion holds if we replace $\alpha$ by a chain homotopic map $\alpha'$.

**Proof.** (i) We need to check that $h_{i-1}d_i^M = \phi_i h_i$ for all $i$. We have

$$h_{i-1}d_i^M = \left( -\alpha_{i-1}, \gamma_{i-1} \right) \left( \psi_i, -\beta_i, 0, -\phi_i \right) = \left( -\alpha_{i-1} \psi_i, \alpha_{i-1} \beta_i - \gamma_{i-1} \phi_i \right),$$

and

$$\phi_i h_i = \phi_i \left( -\alpha_i, \gamma_i \right) = \left( -\phi_i \alpha_i, \phi_i \gamma_i \right).$$

As $\alpha$ is a map of chain complexes, we have $-\alpha_{i-1} \psi_i = -\phi_{i+1} \alpha_i$, and by assumption we have $\alpha_{i-1} \beta_i - \gamma_{i-1} \phi_i = \phi_{i+1} \gamma_i$. Therefore the two expressions displayed above are equal, and $h$ is a chain map.
(ii) Let $\gamma'' = \gamma - \gamma'$, then $(h_i - h'_i)(f, g) = \gamma''_{i-1}(f)$, and $\phi_i\gamma''_{i+1} + \gamma''\phi_i = 0$ for all $i$. From this, we deduce that the maps $(-1)^i\gamma''_i$ define a chain map $F_i(-1) \to F_i$. As $\gamma''_i = 0$, by the comparison lemma this chain map is null homotopic, and hence there exist maps $\rho_i : F_i(-1) \to F_{i+1}$ with $\gamma''_i = -\rho_{i-1}\phi_i + \phi_i\rho_{i+1}$. Then $\rho$ defines a null homotopy for $h - h'$, as seen from the following identity

$$
\begin{pmatrix}
0 & \gamma''_{i-1}
\end{pmatrix} = \begin{pmatrix}
0 & \rho_{i-2} & -\beta_{i-1} & 0 \\
0 & -\phi_{i-1} & 0 & \phi_i
\end{pmatrix}.
$$

Now suppose $\alpha$ and $\alpha'$ are chain homotopic. Put $\alpha'' = \alpha - \alpha'$, and let $h$ be a null homotopy for $\alpha$. Then $h$ defines a null homotopy for $h - h'$:

$$
\begin{pmatrix}
\alpha''_{i-1} & 0
\end{pmatrix} = \begin{pmatrix}
h_i & 0
\end{pmatrix} \begin{pmatrix}
\psi_i & -\beta_{i-1} \\
0 & -\phi_{i-1}
\end{pmatrix} + \phi_i \begin{pmatrix}
h_{i-1} & 0
\end{pmatrix}.
$$

Definition 4.3.6. For any triple of maps $\alpha, \beta, \gamma$ as above, we define $\mathcal{H}(\alpha, \beta, \gamma)$ to be the mapping cone of the map $h : M(\beta)[1] \to F$.

Lemma 4.3.7. The complex $\mathcal{H}(\alpha, \beta, \gamma)$ is independent of the chain homotopy classes of $\alpha$ and $\beta$, and independent of the choice of the homotopy $\gamma$. When there is no danger of confusion, we will denote $\mathcal{H}(\alpha, \beta, \gamma)$ simply as $\mathcal{H}$.

Proof. This follows from Lemma 4.3.2 and Lemma 4.3.5.

Lemma 4.3.8. Suppose that we have $H_i(F_\bullet) = 0$ for $i \geq 1$ and $H_i(G_\bullet) = 0$ for $i \geq 2$. Then the homology groups $H_i(\mathcal{H})$ vanish for $i \geq 2$.

Proof. We have the mapping cone long exact sequences:

$$
\ldots \to H_{i+1}(M(\beta)) \to H_i(F) \xrightarrow{\beta} H_i(G) \to H_i(M(\beta)) \to \ldots
$$

and

$$
\ldots \to H_{i+1}(\mathcal{H}) \to H_{i+1}(M(\beta)) \xrightarrow{h} H_i(F) \to H_i(\mathcal{H}) \to \ldots
$$

As $H_i(F) = H_i(G) = 0$ for $i \geq 1$, from the first sequence we deduce that $H_i(M(\beta)) = 0$ for $i \geq 2$, and then from the second one that $H_i(\mathcal{H}) = 0$ for $i \geq 2$.

Let us now adjoin an indeterminate $x_m$ to $R$, and put $\mathcal{R} = R[x_m] = S[x_1, \ldots, x_m]$. We extend scalars, and work in the category of graded $\mathcal{R}$-modules, putting $\mathcal{F} = F \otimes \mathcal{R}$, $\mathcal{G} = G \otimes \mathcal{R}$. Let

$$
\delta_i = \gamma_i + (-1)^i x_m : \mathcal{F}_{i-1}(-1) \to \mathcal{F}_i
$$

It is simple to verify that this map satisfies

$$
\alpha_i\beta_i = \phi_i\delta_{i+1} + \delta_i\phi_i.
$$
Thus $\alpha, \beta$ and $\delta$ also satisfy the conditions of Definition 4.3.4, and we may form the chain complex of graded $\mathcal{R}$-modules $\mathcal{H}$. Unwrapping the definitions, we have the following explicit description of $\mathcal{H}$:

\[
\begin{align*}
\mathcal{G}_{n-1}(-1) & \oplus \mathcal{F}_{n-2}(-1) \xrightarrow{d_{n-1}} \ldots \\
\mathcal{G}_1(-1) & \oplus \mathcal{F}_1(-1) \xrightarrow{d_1} \mathcal{G}_0(-1) \oplus \mathcal{F}_0(-1) \xrightarrow{d_0} \mathcal{G}_{-1}(-1) \oplus \mathcal{F}_{-1}(-1) \xrightarrow{d_{-1}} \ldots \\
\mathcal{F}_2 & \oplus \mathcal{G}_2(-1) \oplus \mathcal{F}_1(-1) \xrightarrow{d_2} \mathcal{F}_1 \oplus \mathcal{G}_1(-1) \oplus \mathcal{F}_0(-1) \xrightarrow{d_1} \mathcal{F}_0 \oplus \mathcal{G}_0(-1)
\end{align*}
\]  

with the differential given by the matrix

\[
d_i = \begin{pmatrix} \phi_i & \alpha_i & -\delta_i \\ 0 & -\psi_i & \beta_i^{-1} \\ 0 & 0 & \phi_{i-1} \end{pmatrix}
\]

where we regard the maps and modules labelled with negative indices as zero objects. When there is no danger of confusion, we refer to $\mathcal{H}(\alpha, \beta, \gamma)$ as $\mathcal{H}(\alpha, \beta)$ or simply as $\mathcal{H}$. One can visualise this chain complex by taking direct sums of the modules on each (right-to-left) diagonal of the big diagram (1) as modules in the complex, with the maps as specified by the diagram.

Let $I = \phi_1(F_1) \subset F_0$ and $J = \psi_1(G_1) \subset G_0$. As $F_0 = G_0 = \mathcal{R}$, we can identify $I$ and $J$ with homogeneous ideals of $\mathcal{R}$, and complexes $F_\bullet$ and $G_\bullet$ with their graded free resolutions. Fix a basis $a_1, \ldots, a_t$ of $F_1$ and a basis $b_1, \ldots, b_s$ of $G_1$. Then $I$ and $J$ are generated by the elements $\phi_1(a_i) = f_i$, $i = 1, \ldots, t$ and $\psi_1(b_i) = g_i$, $i = 1, \ldots, s$, respectively. Furthermore, let $h_i = \alpha_1(b_i) \in \mathcal{R}$. Now define $\mathcal{I} \subset \mathcal{R}$ to be the ideal generated by $f_1, \ldots, f_t, x_mg_1 + h_1, \ldots, x_mg_s + h_s$.

Note that $\mathcal{I}$ is a homogeneous ideal, since the degrees of the elements $g_i$ are one less than the degrees of $h_i$, by the grading of the maps $\alpha$ and $\beta$.

**Proposition 4.3.9.** With assumptions as in Lemma 4.3.8, we have $H_1(\mathcal{H}) = 0$, and $H_0(\mathcal{H}) = \mathcal{R}/\mathcal{I}$. Hence $\mathcal{H}$ is a graded free resolution of $\mathcal{R}/\mathcal{I}$.

**Proof.** After Lemma 4.3.8, we only have to prove that the cokernel of $d_1$ is isomorphic to $\mathcal{R}/\mathcal{I}$, and that $H_1(\mathcal{H}) = \frac{\ker(d_1)}{\text{im}(d_2)} = 0$. Consider

\[
\begin{align*}
\mathcal{F}_2 \oplus \mathcal{G}_2(-1) \oplus \mathcal{F}_1(-1) \xrightarrow{d_2} & \mathcal{F}_1 \oplus \mathcal{G}_1(-1) \oplus \mathcal{F}_0(-1) \xrightarrow{d_1} \mathcal{F}_0 \oplus \mathcal{G}_0.
\end{align*}
\]

The map $d_1$ is given by $d_1(u, v, w) = (\phi_1(u) + \alpha_1(v) + x_nw, -\psi_1(v) + w)$. We identify $\mathcal{F}_0 \oplus \mathcal{G}_0$ with $\mathcal{R} \oplus \mathcal{R}(-1)$. The image of $d_1$ is generated by $(f_i, 0)(h_i, -g_i)$ and $(x_m, 1)$. Consider the map $\mathcal{R} \oplus \mathcal{R}(-1) \to \mathcal{R}$ defined by $(a, b) \mapsto x_m b - a$. This map takes the pairs $(f_i, 0)$ to $f_i$, $(h_i, -g_i)$ to $x_mg_i + h_i$ and $(x_m, 1)$ to 0. Thus it maps the image of $d_1$ onto $\mathcal{I}$, and hence induces an isomorphism

\[
\text{coker } d_1 = \frac{\mathcal{R} \oplus \mathcal{R}(-1)}{\text{im}(d_1)} \cong \mathcal{R}/\mathcal{I}.
\]

The map $d_2$ is given by $d_2(u, v, w) = (\phi_2(u) + \alpha_2(v) - x_nw - \gamma_2(w), -\psi_2(v) + \beta_2(w), \phi_1(u))$. Suppose $(u, v, w) \in \ker(d_1)$. Then

\[
\phi_1(u) + \alpha_1(v) + x_mw = 0,
\]

and...
Let $u = u_p x_n^p + \ldots + u_1 x_1 + u_0$ and $v = v_q x_n^q + \ldots + v_1 x_1 + v_0$, where $u_i \in F_1$ and $v_i \in G_1$. We prove $(u, v, w) \in \text{im}(d_2)$ by induction on $\Delta(u,v) := \max(2p, 2q+1)$. The base case is $p = q = 0$, when the leading coefficient of $(1)$ is equal to $w$. Hence $w = 0$, and so $\psi_1(v) = 0$. As $G$ is exact in degrees at least 1, we see that $v = \psi_2(v')$, so $\alpha_1(v) = \alpha_1(\psi_2(v')) = \phi_1(\alpha_2(v'))$, and hence by $(1)$, $\phi_1(u + \alpha_2(v')) = 0$. Therefore $u + \alpha_2(v') = \phi_2(u')$, and we conclude that $d_2(u', v', 0) = (u, v, 0)$ as desired.

Now suppose $\Delta(u,v) > 0$. If $p > q$, let $(u', v', w') = (u, v, w) + d_2(0, 0, u_p x_m^{p-1})$ - then $\Delta(u', v') < \Delta(u,v)$ as

$$d_2(0, 0, u_p x_m^{p-1}) = (-\gamma_2(u_p)x_m^{p-1} - u_p x_m^p, \beta_2(u_p)x_m^{p-1}, \phi_1(u_p)x_m^{p-1}),$$

so the $x_m^p$ coefficient in the first factor vanishes, and by the induction hypothesis $(u,v,w) \in \text{im}(d_2)$. If $q > p$, then by looking at the leading coefficient of $(1)$ we see that $\psi_1(v_q) = 0$, so that $v_q = \psi_2(v)$ for some $e \in G_2$. Let $(u', v', w') = (u, v, w) + d_2(0, v_q x_m^q, 0)$. Then $\Delta(u', v') < \Delta(u,v)$ as

$$d_2(0, v_q x_m^q, 0) = (\alpha_2(e)x_m^q, -v_q x_m^q, 0),$$

so the $x_m^q$ coefficient in the second factor vanishes, and the highest power of $x_m$ in the first factor is $x_m^q$, concluding the proof of the induction step.

We will compute the $\Omega$-quadrics attached to $H$ using the following result.

**Proposition 4.3.10.** Let $1 \leq a_1, a_2, \ldots, a_{n-2} \leq m$ be integers, and suppose that $a_k = m$ for $2 \leq k \leq n - 3$. Then

$$[a_1, a_2, \ldots, a_{n-2}]_{H_{\alpha, \beta, \delta}} = (-1)^{k+1} [a_1, a_2, \ldots, a_{k-1}, a_{k+1}, \ldots, a_{n-2}]_F,$$

where the square bracket symbols are as defined in Chapter 3.

**Proof.** Consider the formula $\hat{\delta}$ describing the differential of the complex $H(\alpha, \beta, \delta)$. Notice that, as $\delta$ is the only map whose definition directly involves the monomial $x_m$, we have:

$$\frac{\partial d_k}{\partial x_m} = \begin{pmatrix} 0 & 0 & (-1)^{k+1} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

But for any upper-triangular matrix, we have

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$
Thus \([a_1, a_2, \ldots, a_{n-2}] = \frac{\partial d_{i-1}}{\partial x_{a_1}} \frac{\partial d_{i+1}}{\partial x_{a_2}} \cdots \frac{\partial d_{n-2}}{\partial x_{a_{n-2}}}\) will be the product of top-leftmost entries of \(\frac{\partial d_i}{\partial x_{a_i}}\) for \(i < k\), multiplied by the product of the bottom-rightmost entries of \(\frac{\partial d_i}{\partial x_{a_i}}\) for \(i > k\), with the sign \((-1)^{k+1}\) in front. Examining what these entries are, we find that

\[ [a_1, a_2, \ldots, a_{n-2}] = (-1)^{k+1} [a_1, a_2, \ldots, \hat{a}_k, \ldots, a_{n-2}] \].

\(\square\)

**Self-duality.** Now suppose that \(F_*\) and \(G_*\) are self-dual. Fix isomorphisms \(\eta : F_*^{\circ} \to F_*\) and \(\theta : G_* \to G_*^{\circ}\), and define maps \(\beta^T : G_*(-1) \to F_*[-1]\) and \(\delta^T : F_* \to F_*[-1]\) by setting

\[ \beta^T = \eta \circ \beta^{\circ} \circ \theta, \]

and

\[ \delta^T = \eta \circ \delta^{\circ} \circ \theta. \]

**Lemma 4.3.11.** Suppose that we have \(\alpha = \beta^T\). Then there exists a null homotopy \(\delta\) for the map \(\alpha \circ \beta\), with \(\delta = \delta^T\).

**Proof.** Identify \(F \cong F^{\circ}\) and \(G \cong G^{\circ}\), using the homomorphism defined above. We have \(\phi_{n-2-i} = \phi_i^{\circ}\), and \(\beta_i^{\circ} = \beta_{n-2-i}^T\). Let \(\delta\) be any null homotopy for \(\beta^T \circ \beta\). Dualizing the identity

\[ \beta^T_i \beta_i = \phi_i \delta_{i+1} + \delta_i \phi_i, \]

we find that

\[ \beta^T_{n-2-i} \beta_{n-2-i} = \phi_{n-2-i} \delta_i^{\circ} + \delta_{i+1}^{\circ} \phi_{n-2-i}. \]

Thus, for \(2i < n-2\), we replace \(\delta_i\) with \(\delta_{n-2-i}^{\circ}\). The resulting \(\delta\) is still a null-homotopy for \(\beta^T \circ \beta\) and satisfies \(\delta = \delta^T\). \(\square\)

**Lemma 4.3.12.** Assume that we have \(\alpha = \beta^T\) and \(\delta = \delta^T\). Then the chain complex \(\mathcal{H}(\alpha, \beta, \delta)\) is self-dual.

**Proof.** The dual complex \(\mathcal{H}(\alpha, \beta, \delta)^{\circ}\) is given by

\[ G_{n-1}^*(-1) \oplus F_{n-2}^*(-1) \xleftarrow{d^T_{i-1}} \cdots \xleftarrow{d^T_{i+1}} F_i^* \oplus G_i^*(-1) \oplus F_{i-1}^*(-1) \xleftarrow{d^T_{i}} \cdots \\
\xleftarrow{d^T_{i}} F_2^* \oplus G_2^*(-1) \oplus F_1^*(-1) \xleftarrow{d^T_{1}} F_1^* \oplus G_1^*(-1) \xleftarrow{d^T_{1}} F_0^* \oplus G_0^*(-1) \]

with \(d^T_i\) given by

\[ d^T_i = \begin{pmatrix}
\phi_i^* & 0 & 0 \\
\alpha_i^* & -\psi_i^* & 0 \\
-\delta_i^* & \beta_i^* & \phi_{i-1}^*
\end{pmatrix} \]
4.4. CONSTRUCTION OF THE UNPROJECTION DATA

Switching the places of the two $F^*$ terms, the matrix representing $d^*_i$ will be

$$\begin{pmatrix}
\phi^*_{i-1} & \beta^*_{i} & -\delta^*_{i} \\
0 & -\psi^*_{i} & \alpha^*_{i} \\
0 & 0 & \phi^*_{i}
\end{pmatrix}$$

Now identify $F_\bullet$ and $F^*_\bullet$ with $\eta$, and identify $G_\bullet$ and $G^*_\bullet$ with $\theta$. The matrix representing $d^*_i$ is the same as the matrix representing $d_{n-1-i}$. In other words, we have proven that the map

$$\mathcal{H} \to \mathcal{H}^* : (f_1, g, f_2) \mapsto (\eta(f_2), \theta^{-1}(g), \eta(f_1))$$

is an isomorphism of chain complexes.

**Construction of a minimal free resolution.** The free resolution $\mathcal{H}(\alpha, \beta, \delta)$ is not a minimal free resolution. When $\alpha_{n-2}$ is an isomorphism, we can modify $\mathcal{H}$ to obtain a minimal resolution. We eliminate $\alpha_{n-2}$ and $\beta_1$ from $\mathcal{H}$ to produce a chain complex $\mathcal{H}_{min}$ as follows. Set

$$\mathcal{H}_{min}(\alpha, \beta, \delta)_{n-1} = F_{n-2}(-1), \quad \mathcal{H}_{min}(\alpha, \beta, \delta)_{n-2} = F_{n-3}(-1) \oplus G_{n-2}(-1),$$

$$\mathcal{H}_{min}(\alpha, \beta, \delta)_1 = F_1 \oplus G_1(-1), \quad \mathcal{H}_{min}(\alpha, \beta, \delta)_0 = F_0.$$

When $n > 4$, for the differentials, we set

$$d'_{n-1} = \left(\begin{array}{c}
\beta_{n-2} - \psi_{n-1}\alpha_{n-2}^{-1}\delta_{n-1} \\
\phi_{n-2}
\end{array}\right), \quad d'_{n-2} = \left(\begin{array}{cc}
\alpha_{n-2} & -\delta_{n-2} \\
-\psi_{n-2} & \beta_{n-3} \\
0 & \phi_{n-3}
\end{array}\right),$$

$$d'_2 = \left(\begin{array}{cc}
\phi_2 & \alpha_2 & -\delta_2 \\
0 & -\psi_2 & \beta_1
\end{array}\right), \quad d'_1 = \left(\begin{array}{c}
\phi_1 & \alpha_1 - \delta_1\beta_1^{-1}\psi_1
\end{array}\right)$$

In all other cases, we take $\mathcal{H}_{min}(\alpha, \beta, \delta)_i = \mathcal{H}(\alpha, \beta, \delta)_i$ and $d'_i = d_i$.

When $n = 4$, we need to slightly modify the formulae for $d'_2 = d'_{n-2} : G_2(-1) \oplus F_1(-1) \to F_1 \oplus G_1(-1)$, and instead take

$$d'_2 = \left(\begin{array}{cc}
\alpha_2 & -\delta_2 \\
-\psi_2 & \beta_1
\end{array}\right)$$

The complex $\mathcal{H}_{min}$ is also a self-dual free resolution of the ideal $I_n$, and the final term of the complex is $\mathcal{R}(-n)$. When $S = k$ is a field, then $\mathcal{H}_{min}$ is a minimal free resolution of $I_n$. Furthermore, this modification does not affect the forms $[a_1, \ldots, a_{n-2}]$. In other words, we have

$$[a_1, a_2, \ldots, a_{n-2}]\mathcal{H}_{a,\beta,\delta} = [a_1, a_2, \ldots, a_{n-2}]\mathcal{H}'_{a,\beta,\delta}.$$

4.4 Construction of the unprojection data

In this section we describe various ways to get ahold of maps $\beta : F_\bullet(-1) \to G_\bullet(-1)$ and $\alpha : G_\bullet(-1) \to F_\bullet[-1]$ that satisfy the conditions of Definition 4.3.4. Recall that in Section 2.2.2 we have put a differential graded algebra structure on both $F_\bullet$ and $G_\bullet$. 
Proposition 4.4.1. Let $I$ and $J$ be homogeneous ideals of $R = S[x_1, \ldots, x_{m-1}]$, with $I \subset J$. Assume that $I$ is generated by forms of degree $r + 1$, while $J$ is generated by forms of degree $r$, for some positive integer $r$.

Let $F_\bullet$ and $G_\bullet$ be graded free resolutions of $I$ and $J$, of length $n - 2$ and $n - 1$ respectively. Assume that the maps $F_\bullet \to F_\bullet$ and $G_\bullet \to G_\bullet$ induced by choices of a DGCA structure on $F_\bullet$ and $G_\bullet$ are isomorphisms. Then there are maps $\alpha, \beta$ and $\delta$ that satisfy the conditions of Definition 4.3.4, and the chain complex $\mathcal{H}_{\text{min}}$ is a self-dual free resolution.

The map $\beta$. The inclusion $I \subset J$ induces the comparison map of resolutions $\beta : F_\bullet(-1) \to G_\bullet(-1)$, by Lemma 2.2.3

\[ 0 \to F_{n-2}(-1) \xrightarrow{\phi_{n-2}} \cdots \xrightarrow{\phi_3} F_2(-1) \xrightarrow{\phi_2} F_1(-1) \xrightarrow{\phi_1} F_0(-1) \to 0 \]

\[ G_{n-1} \xrightarrow{\psi_{n-1}} G_{n-2} \xrightarrow{\psi_{n-2}} \cdots \xrightarrow{\psi_3} G_2 \xrightarrow{\psi_2} G_1 \xrightarrow{\psi_1} G_0 \to 0 \]

The map $\alpha$ as a dual. By assumption, the induced pairings $F_i \otimes F_{n-2-i} \to R$ and $G_i \otimes G_{n-1-i} \to R$ are perfect. Following the proof of Theorem 1.4 of [KM83], we define the map $\alpha$. Define $\alpha_i : G_i(-1) \to F_{i-1}$ by taking $\alpha(z_i)$ to be the unique element of $F_{i-1}$ such that

\[ \alpha_i(z_i) \cdot z_{n-1-i} = (-1)^{i+1} z_i \cdot \beta_{n-1-i}(z_{n-1-i}) \]

The map $\alpha$ is the same as the map $\beta^T$ defined in the previous section, with isomorphisms $F_\bullet \cong F_\bullet$ and $G_\bullet \cong G_\bullet$ induced by the DGCA structures, as explained in Section 2.2.2. Note that the map $\alpha_{n-2}$ corresponds to multiplication by the unit $(-1)^n$. Thus $\alpha$ is a homomorphism of chain complexes, represented by the following diagram.

\[ 0 \to G_{n-1}(-1) \xrightarrow{\psi_{n-1}} \cdots \xrightarrow{\psi_3} G_2(-1) \xrightarrow{\psi_2} G_1(-1) \xrightarrow{\psi_1} G_0(-1) \]

\[ 0 \to F_{n-2} \xrightarrow{\phi_{n-2}} \cdots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \to 0 \]

The following lemma shows that $\alpha$ and $\beta$ correspond to unprojection data.

Lemma 4.4.2. The map $\alpha \circ \beta : F_\bullet(-1) \to F_\bullet[-1]$ is null homotopic.

Proof. Let $\xi : F_i(-1) \otimes F_j(-1) \to F_{i+j}$ be the chain homotopy defined in Lemma 2.2.8. We define a null homotopy $h : F_i(-1) \to F_i$ by taking $h_i(z_i)$ to be the unique element such that

\[ h_i(z_i) \cdot z_{n-2-i} = (-1)^{i+1} \xi(z_i \otimes z_{n-2-i}) \text{ for all } z_{n-2-i} \in F_{n-2-i}(-1). \]

By (iii) of Lemma 2.2.8,
h_0 = h_{n-2} = 0. By part (iv), we compute

\[(h_{i-1}\phi_i + \phi_i h_i)(z_i) \cdot z_{n-1-i} = h_{i-1}(\phi_i(z_i)) \cdot z_{n-2-i} + \phi_i(h_i(z_i)) \cdot z_{n-1-i} \]

\[= (-1)^i \xi(\phi_i(z_i) \otimes z_{n-1-i}) + (-1)^{i+1} h_i(z_i) \cdot (\phi_{n-1-i}(z_{n-1-i})) \]

\[= (-1)^i \xi(\phi_i(z_i) \otimes z_{n-1-i}) + (-1)^i (z_i \otimes \phi_{n-1-i}(z_{n-1-i})) \]

\[= (-1)^{i+1} \beta_i(z_i) \cdot \beta_{n-1-i}(z_{n-1-i}) \]

\[= \alpha_i(\beta_i(z_i)) \cdot z_{n-1-i}. \]

Note that in the second and the third equality we used the Leibniz rule. Hence \(\alpha_i\beta_i = h_{i-1}\phi_i + \phi_i h_i\), concluding the proof of the lemma, and Proposition 4.4.1.

We are interested in constructing resolutions for ideals that arise from genus one normal curves of degree \(n\), or sets of \(n\) points in general position. The ideals \(I\) and \(J\) will be generated by quadrics, and define varieties \(C \subset \mathbb{P}^{m-1}\) and \(C \subset \mathbb{P}^m\). The variety \(C\) contains the point \(P = (0 : 0 : \ldots : 0 : 1)\), and linear projection from \(P\) defines a birational map \(C \to C\). The ideal \(J\) will be generated by linear forms. If this map extends to a map defined at \(P\), as will be the case when \(C\) is a smooth curve, \(J\) will be the ideal defining the image of the point \(P\) in \(\mathbb{P}^{n-1}\). If \(C\) is a set of \(n\) points, then \(J\) will be the irrelevant ideal of \(R\). We formalize these properties as follows.

**Definition 4.4.3.** We say a graded free resolution \(F_*\) of a homogeneous ideal \(I \subset R\) is an **admissible** resolution if it is self-dual, and of the following form:

\[0 \to R(-n) \xrightarrow{\phi_{n-2}} R(-n + 2)^{b_{n-3}} \xrightarrow{\phi_{n-3}} R(-n + 3)^{b_{n-4}} \xrightarrow{\phi_{n-4}} \ldots \]

\[\ldots \xrightarrow{\phi_3} R(-3)^{b_1} \xrightarrow{\phi_2} R(-2)^{b_1} \xrightarrow{\phi_1} R \to 0, \]

with the Betti numbers given by \(b_i = n\binom{n-2}{i} - \binom{n}{i+1}\).

**Definition 4.4.4.** Let \(S = k\) be a field, so that \(R = k[x_1, \ldots, x_{m-1}]\). Let \(I\) and \(J\) be Gorenstein ideals of \(R\), and let \(\mathcal{I}\) be an ideal of \(R\). We say \(I, J\) and \(\mathcal{I}\) form an unprojection triple if they satisfy the following conditions:

(i) \(I, J\) and \(\mathcal{I}\) are generated by forms of degrees 2, 1 and 2 respectively.

(ii) \(\mathcal{I} \cap R = I\) and \(I \subset J\).

(iii) \(J\) is the set of leading coefficients of \(\mathcal{I}\), viewed as an ideal of \(R = R[x_m]\).

(iv) \(I\) admits a minimal admissible resolution \((F_*, \phi)\) of length \(n - 2\), while the minimal graded free resolution \((G_*, \psi)\) of \(J\) is of length \(n - 1\), given by a Koszul complex

\[R(-n + 1) \xrightarrow{\psi_{n-1}} R(-n + 2)^{c_{n-2}} \xrightarrow{\psi_{n-3}} \ldots \xrightarrow{\psi_2} R(-1) \xrightarrow{\psi_1} R. \]

We extend this definition to \(n = 3\) by modifying the condition (i) to require that \(I\) be generated by a form of degree 3.
A remark on grading. For this section we adopt the convention that the dual of the graded module $M$ is the module $M^* = \text{Hom}(M, R(-n+1))$. Then the fact that $I$ and $J$ are Gorenstein implies that $G_\bullet \cong G_\bullet^*$ and $F_\bullet \cong F_\bullet^*(1)$.

The map $\alpha$ for an unprojection triple. The inclusion $I \subset J$ induces the map $\beta : F_\bullet(-1) \to G_\bullet^*(-1)$ in the same way as before. We now give an alternative way to describe the map $\alpha$. Fix a basis $a_1, \ldots, a_t$ of $F_1$ and a basis $b_1, \ldots, b_s$ of $G_1$. Then $I$ is generated by $\phi_1(a_i) = f_i$, $i = 1, \ldots, t$ and $J$ is generated by $\psi_1(b_i) = g_i$, $i = 1, \ldots, s$. By conditions (i), (ii) and (iii), there exist quadrics $h_i \in R$ such that

$$I = (f_1, \ldots, f_t, x_m g_1 + h_1, \ldots, x_m g_s + h_s).$$

Define $\alpha_1 : G_1(-1) \to F_0$ by $\alpha(b_i) = h_i$. We will extend $\alpha$ to a map of chain complexes $G(-1) \to F[-1]$, represented by the following diagram.

$$
\begin{array}{cccccccc}
0 & \longrightarrow & G_{n-1}(-1) & \overset{\psi_{n-1}}{\longrightarrow} & G_2(-1) & \overset{\phi_2}{\longrightarrow} & G_1(-1) & \overset{\psi_1}{\longrightarrow} & G_0(-1) \\
\downarrow & & \downarrow \alpha_{n-1} & & \downarrow & & \downarrow \alpha_2 & & \downarrow \alpha_1 \\
0 & \longrightarrow & F_{n-2} & \overset{\phi_{n-2}}{\longrightarrow} & F_1 & \overset{\phi_1}{\longrightarrow} & 0 & & 0
\end{array}
$$

To do this, we check that the image of the map $\alpha_1 \psi_2$ is contained in $\phi_1(F_1) = I$. This implies that there exists a map $\alpha_2 : G_2(-1) \to F_1$ with $\phi_1 \alpha_2 = \alpha_1 \psi_2$. As the complex $F[-1]$ is acyclic in degrees greater than 2, and $G(-1)$ is a complex of projective modules, by Lemma 2.2.3, we can extend $\alpha_1$ to a chain map.

Let $e_1, e_2, \ldots, e_p$ be a basis of $G_2$. Then $\psi_2(e_j) = \sum \xi_{ij} b_i$ for some $\xi_{ij} \in R$. Since $\psi_1 \psi_2 = 0$ we have $\sum \xi_{ij} g_i = 0$. Then

$$\alpha_1 \psi_2(e_j) = \sum \xi_{ij} h_i = \sum \xi_{ij} (x_m g_i + h_i) \in I \cap R = I$$

as desired. We now check that this agrees with our previous definition of $\alpha$.

**Lemma 4.4.5.** Suppose that the ideal $I$ has the property that for every linear form $l \in R$, there exists a linear form $g \in J$ with $(l + x_m)g \notin I$.

Then the map $\alpha : G_\bullet(-1) \to F_\bullet[-1]$, defined above, is chain homotopic to a non-zero scalar multiple of the map $\beta^T : G_\bullet(-1) \to F_\bullet[-1]$, obtained by dualizing the map $\beta$.

**Proof.** Consider the diagram obtained by dualizing the diagram defining the map $\alpha$.

$$
\begin{array}{cccccccc}
0 & \longrightarrow & F_0 & \overset{\phi_1}{\longrightarrow} & \cdots & \overset{\phi_2}{\longrightarrow} & F_{n-4} & \overset{\phi_{n-3}}{\longrightarrow} & F_{n-3} & \overset{\phi_{n-2}}{\longrightarrow} & F_{n-2} \\
\downarrow & & \downarrow \alpha_1 & & \downarrow \alpha_{n-3} & & \downarrow \alpha_{n-2} & & \downarrow \alpha_{n-1} \\
G_0^*(1) & \overset{\psi_1^*}{\longrightarrow} & G_1^* & \cdots & \overset{\psi_{n-3}^*}{\longrightarrow} & G_{n-3}^* & \overset{\psi_{n-2}^*}{\longrightarrow} & G_{n-2}^* & \overset{\psi_{n-1}^*}{\longrightarrow} & G_{n-1}^*(1)
\end{array}
$$

By the comparison lemma, it suffices to show that $\alpha_{n-1}^* : F_{n-2}^*(-1) \to G_{n-1}^*(1)$ is an isomorphism of graded modules, since the above diagram is isomorphic to the one defining the map $\beta$. 

As \( \alpha^*_i \) respects the grading, it must be multiplication by a scalar element of \( k \). To show it is an isomorphism, it suffices to show that it is non-zero.

Suppose otherwise. By the comparison lemma, \( \alpha^* \), is homotopic to the zero map, and so there exist maps \( \rho_i : F_i^* \to G_i^* \), with \( \rho_{n-3} = 0 \), and

\[
\alpha^*_i = \rho_i \phi^*_i + \psi^*_i \rho_{i-1}
\]

for all \( i \leq n - 3 \). In particular \( \alpha^*_i = \rho_i \phi^*_i + \psi^*_i \rho_0 \), and dualizing again, we see \( \alpha_1 = \rho^*_1 \phi_1 + \psi_1 \rho^*_0 \).

As \( \rho^* \) is a degree zero map from \( G_0(-1) \cong R(-1) \) to \( F_0 \cong R \), it must be multiplication by some linear form \( l \in R \). For \( 1 \leq i \leq s \), we find

\[
l g_i - h_i = \rho_0^* \psi_1(b_i) - \alpha_1(b_i) = \phi_1(\rho_1^*(b_i)) \in I \subset J.
\]

As \( x_m g_i + h_i \in J \), we have \( (l + x_m) g_i \in I \) for all \( i \), and hence \( (l + x_m) g = 0 \) for every linear form \( g \in J \), contradicting our assumption. \( \square \)

**Remark 4.4.6.** Notably, the hypothesis of the lemma is satisfied when \( J \) is a prime ideal, as \( (x_m + l) g \in J \) implies that either \( x_m + l \in J \) or \( g \in J \), and \( J \) contains no non-zero linear forms.

**Remark 4.4.7.** The upshot of all this is, that by Lemma 4.3.9, the complex \( \mathcal{H} \) is the minimal free resolution of the ideal \( I \), constructed entirely from the data of resolutions \( F_\bullet, G_\bullet \) and the comparison map \( \beta \). In other words, if \( I, J \) and \( \mathcal{I} \) form an unprojection triple, we can recover \( \mathcal{I} \) from \( I \) and \( J \).

### 4.5 Unprojection and sets of \( n \) points in \( \mathbb{P}^{n-2} \)

In this section we explain how unprojection allows us to compute a resolution model of a set of \( n \) points in general position, and give an explicit example illustrating the construction of Section 4.4. We then use unprojection to give a short proof of Lemma 3.5.8. Finally, we prove a lemma we will need later, in Chapter 5.

We recall the setup of Lemma 3.5.8. Let \( k \) be a field, and \( n \geq 3 \) an integer. We consider \( X_n = \{P_1, \ldots, P_n\} \subset \mathbb{P}^{n-2} \), a set of \( n \) points in general position, viewed as a variety defined over \( k \), where the points \( P_i \) are given by \( P_1 = (1 : 0 : \ldots : 0), P_2 = (0 : 1 : 0 : \ldots : 0), \ldots, P_{n-1} = (0 : \ldots : 0 : 1) \) and \( P_n = (1 : 1 : \ldots : 1) \). Let \( I_n = I(X_n) \) be the homogeneous ideal of \( R = k[x_1, \ldots, x_{n-1}] \) defining \( X_n \). Recall that by Lemma 3.6.1, if \( n \geq 4 \), \( I_n \) is generated by quadrics \( x_i(x_j - x_k) \), and if \( n = 3 \), \( I_3 \) is generated by \( x_1 x_2(x_1 - x_2) \).

**Lemma 4.5.1.** Let \( J = (x_1, \ldots, x_{n-1}) \) be the maximal homogeneous ideal of \( R \). The ideals \( I_n, J \) and \( I_{n+1} \) form an unprojection triple. Furthermore, the ideal \( I_n \) satisfies the conditions of Lemma 4.4.5.

**Proof.** Conditions (i) and (iv) of Definition 4.4.4 are satisfied, by Theorem 3.1.3(ii) for the resolution of \( I_n \), and by Theorem 2.2.7 for the resolution of \( J \). For condition (ii), Lemma 3.6.1 implies that \( I_n \subset J \) and \( I_n \subset I_{n+1} \cap R \). For the other inclusion, let \( f \in I_{n+1} \cap R \). It is easy to verify that the vanishing of \( f \) at the points of \( X_{n+1} \) implies vanishing of \( f \) at the points of \( X_n \).
CHAPTER 4. THE UNPROJECTION CONSTRUCTION

Condition (iii) also follows immediately from Lemma 3.6.1. The final claim follows from Lemma 3.6.1. □

Thus we may construct a resolution model of $X_n$ inductively, via unprojection. Note that in the construction of the preceding two sections, we take $m = n - 1$.

**Example 4.5.2.** Let us take $n = 4$. In this case, $I_4$ is generated by $p_1 = x_1(x_2 - x_3)$ and $p_2 = x_2(x_1 - x_3)$. A resolution model of $X_4$ is given by the Koszul complex $F_*$,

$$F_*: 0 \to R(-2) \xrightarrow{(x_1(x_2 - x_3))} R(-1)^2 \xrightarrow{(x_2(x_1 - x_3) - x_1(x_2 - x_3))} R \to 0.$$ 

The ideal $J$ is generated by $x_0, x_1$ and $x_2$, and is resolved by the Koszul complex $G_*$,

$$G_*: 0 \to R(-3) \xrightarrow{(x_1, x_2, x_3)} R(-2)^3 \xrightarrow{(0, x_3, -x_2, -x_3, 0, x_1)} R(-1)^3 \xrightarrow{(x_1, x_2, x_3)} R \to 0.$$ 

We start by computing a map $\beta : F_* \to G_*$ lifting the inclusion $I \subset J$,

$$
\begin{array}{cccccc}
0 & \xrightarrow{\psi_3} & R(-3) & \xrightarrow{\psi_2} & R(-2)^3 & \xrightarrow{\beta_1} & R(-1)^3 & \xrightarrow{\psi_1} & R \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
R(-4) & \xrightarrow{\phi_2} & R(-2)^2 & \xrightarrow{\phi_1} & R & & & \\
\end{array}
$$

The map $\beta_0 : R \to R$ is the identity. We can write $p_2 = x_2 \cdot x_2 - x_2 \cdot x_3$ and $-p_1 = -x_1 \cdot x_2 + x_1 \cdot x_3$, and thus a lift $\beta_1 : R(-2)^2 \to R(-1)^3$ is represented by the matrix

$$\begin{pmatrix}
x_2 & 0 \\
0 & -x_1 \\
-x_2 & x_1
\end{pmatrix}.$$ 

The map $\phi_2 \circ \beta_1$ is represented by

$$\begin{pmatrix}
x_2 & 0 \\
0 & -x_1 \\
-x_2 & x_1
\end{pmatrix} \cdot \begin{pmatrix}
x_1(x_2 - x_3) \\
x_2(x_1 - x_3)
\end{pmatrix} = \begin{pmatrix}
x_1x_2(x_2 - x_3) \\
x_1x_2(x_3 - x_1) \\
x_1x_2(x_1 - x_2)
\end{pmatrix}.$$ 

We take $\beta_2 : R(-4) \to R(-2)^3$ to be the map represented by

$$\begin{pmatrix}
-x_1x_2 \\
x_1x_2 \\
-x_1x_2
\end{pmatrix}.$$
Then the matrix representing $\psi_2 \circ \beta_2$ is

$$
\begin{pmatrix}
0 & x_3 & -x_2 \\
-x_3 & 0 & x_1 \\
x_2 & -x_1 & 0
\end{pmatrix}
\cdot
\begin{pmatrix}
-x_1x_2 \\
-x_1x_2 \\
-x_1x_2
\end{pmatrix}
= 
\begin{pmatrix}
x_1x_2(x_2 - x_3) \\
x_1x_2(x_3 - x_1) \\
x_1x_2(x_1 - x_2)
\end{pmatrix}.
$$

And so indeed $\phi_2 \circ \beta_2 = \psi_2 \circ \beta_3$, and the diagram defining $\beta$ commutes. Note that $\beta$ is unique only up to chain homotopy, and so this is only one possible solution. The ideal constructed in Proposition 4.4.1 from the data of the map $\beta$ is generated by $p_1, p_2$ and $x_4x_3 - x_1x_2$, $x_4x_2 - x_1x_2$ and $x_4x_3 - x_1x_2$. As $x_4x_3 - x_1x_2 - (x_4x_2 - x_1x_2) = x_4x_3 - x_4x_2$, we see that this ideal is, as expected, the defining ideal of the set $X_5 \subset \mathbb{P}^3$.

We now compute the map $\alpha : G_{\ast}(-1) \to F_{\ast}$.

\[
\begin{array}{cccc}
& R(-3) & \xrightarrow{\psi_3} & R(-2)^3 & \xrightarrow{\psi_2} & R(-1)^3 & \xrightarrow{\psi_1} & R \\
\downarrow & \alpha_3 & & \downarrow & \alpha_2 & & \downarrow & \alpha_1 \\
0 & \downarrow & \rightarrow & R(-4) & \xrightarrow{\phi_2} & R(-2)^2 & \xrightarrow{\phi_1} & R
\end{array}
\]

We take $\alpha$ to be the dual of the map $\beta$, with the respect to the natural self-duality of the Koszul complex - see discussion after Theorem 2.2.7. The matrix representing $\alpha_i$ is the transpose of the matrix representing $(-1)^i \beta_{n-2-i}$.

To compute a null homotopy $\gamma$, we observe that since

$$
\begin{pmatrix}
-x_1x_2 & -x_1x_2 & -x_1x_2 \\
0 & 0 & -x_1 \\
-x_2 & x_1
\end{pmatrix}
\cdot
\begin{pmatrix}
x_2 & 0 \\
0 & -x_1 \\
-x_2 & x_1
\end{pmatrix}
= 
\begin{pmatrix}
0 & 0 & 0
\end{pmatrix}.
$$

we have $\alpha_2 \circ \beta_1 = 0$ and $\alpha_3 \circ \beta_2 = 0$, and hence we can take $\gamma = 0$.

The complex $H_{\text{min}}(\alpha, \beta)$ is given by

$$
0 \to R(-5) \xrightarrow{d_3} R(-3)^5 \xrightarrow{d_2} R(-2)^5 \xrightarrow{d_1} R \to 0
$$

where the matrix $d_2$ is

$$
\begin{pmatrix}
x_2 & 0 & -x_2 & -x_4 & 0 \\
0 & x_1 & -x_1 & 0 & -x_4 \\
0 & -x_3 & x_2 & 0 & -x_2 \\
x_3 & 0 & -x_1 & x_1 & 0 \\
-x_2 & x_1 & 0 & -x_1 & x_2
\end{pmatrix}
$$

and

$$
d_1 = \begin{pmatrix}
-x_1x_2 + x_1x_3 & -x_1x_2 + x_2x_3 & -x_1x_2 + x_1x_4 & -x_1x_2 + x_2x_4 & -x_1x_2 + x_3x_4
\end{pmatrix},
$$

$$
d_3^T = \begin{pmatrix}
-x_1x_2 + x_1x_4 & -x_1x_2 + x_2x_4 & -x_1x_2 + x_3x_4 & x_1x_2 - x_2x_3 & -x_1x_2 + x_1x_3
\end{pmatrix}
$$
using the formulae given at the end of Section 4.4. To represent this resolution model by a matrix of alternating forms, and hence make the self-duality of \( H_{\min}(\alpha, \beta) \) explicit, we need to choose bases so that the matrix representing \( d_2 : R(-3)^5 \rightarrow R(-2)^5 \) is alternating. One way to do this corresponds to replacing \( d_2 \) by \( A = d_2 \cdot T \):

\[
T = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & -1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0
\end{pmatrix}
\]

\[
A = \begin{pmatrix}
0 & -x_4 & -x_2 & 0 & x_2 \\
x_1 & 0 & 0 & x_1 & -x_1 \\
x_2 & 0 & 0 & x_3 & -x_2 \\
0 & -x_1 & -x_3 & 0 & x_1 \\
-x_2 & x_1 & x_2 & -x_1 & 0
\end{pmatrix}
\]

This corresponds to the chain complex

\[
0 \rightarrow R(-5) \xrightarrow{P^T} R(-3)^5 \xrightarrow{A} R(-2)^5 \xrightarrow{P} R
\]

where \( P \) the row vector of signed \( 4 \times 4 \) sub-Pfaffians of \( A \),

\[
\left(-x_1x_2 + x_1x_3 \quad -x_1x_2 + x_2x_3 \quad -x_1x_2 + x_1x_4 \quad -x_1x_2 + x_2x_4 \quad -x_1x_2 + x_3x_4\right)
\]

In an analogous way, one can compute explicitly the unprojection of a genus one normal curve \( C \subset \mathbb{P}^3 \) of degree 4, defined by two quadrics that pass through the point \((0 : 0 : 0 : 1)\). The reader seeking explicit formulae will have no trouble translating Lemma 2.3 of [Fis13b] into our language.

There is no difficulty in computing the quadrics \([ijk]\) of the complex \( H(\alpha, \beta, \delta) \), and verifying that they are as predicted by Lemma 3.5.8 and Lemma 4.3.10. In fact, Lemma 4.3.10 allows us to give a short proof of Lemma 3.5.8, which we now give.

*A second proof of Lemma 3.5.8.* We seek to show, for \( X \) as above, with a fixed resolution model \( F_* \), that up to a constant \( \lambda \in k \), for any permutation \( \tau = (a_1, \ldots, a_{n-1}) \) of \((1, \ldots, n-1)\), we have

\[
[a_1, \ldots, a_{n-2}] = \lambda \cdot \text{sgn}(\tau)(x_{a_{n-1}} - x_{a_1} - x_{a_{n-2}})x_{a_{n-1}}.
\]

We treat the case \( n = 3 \) separately. A resolution model \( F_*^3 \) of \( X_3 \) is specified by the binary cubic \( f = x_1x_2(x_1 - x_2) \). We compute

\[
[1] = \frac{\partial f}{\partial x_1} = 2x_1x_2 - x_2^2,
\]

\[
[2] = \frac{\partial f}{\partial x_2} = x_1^2 - 2x_2x_1,
\]

and we see that the lemma is true for \( n = 3 \). We now construct a resolution model \( F_* \) of \( X_n \),
by repeated unprojection.

By Lemma 4.5.1, $I_k, J_k = (x_1, \ldots, x_{k-1})$ and $I_{k+1}$ form an unprojection triple for $3 \leq k \leq n$, and so we can use the construction of Section 4.3 to obtain a sequence of resolution models $F^3_\bullet, F^4_\bullet, \ldots, F^n_\bullet = F_\bullet$ of $X_3, X_4, \ldots, X_n$.

For example, the model $F^3_\bullet$ is given by the binary cubic $x_1x_2(x_1 - x_2)$. The model $F^4_\bullet$ corresponds to the pair of quadrics $x_3x_1 - x_2x_1$ and $x_1x_2 - x_3x_2$, and in the previous example we explained how to compute the model $F^5_\bullet$. Note that in the construction of $F^{k+1}_\bullet$ from $F^k_\bullet$ we need to make a choice of maps $\beta$ and $\alpha$, which are unique only up to chain homotopy.

Our induction starts at $n = 4$. For the model $F^4_\bullet$ given by $x_3x_1 - x_2x_1$ and $x_1x_2 - x_3x_2$, we compute

$$[1, 2]_{F^4_\bullet} = \frac{\partial \phi_1 \partial \phi_2}{\partial x_1 \partial x_2} = (x_1 - x_3 - x_1) \cdot (x_2 - x_3 - x_2) = (x_3 - x_1 - x_2)x_3$$

Recall that by Lemma 4.3.10, we have

$$[a_1, \ldots, a_{k-2}, a_{k-1}, a_k]_{F^k_\bullet} = (-1)^k[a_1, \ldots, a_{k-2}, a_k]_{F^{k-1}_\bullet}$$

and so we compute

$$[1, 3, 4, \ldots, n - 2, 2]_{F^k_\bullet} = \pm[1, 3, 4, \ldots, n - 3, 2]_{F^{k-1}_\bullet} = \ldots = \pm[1, 2]_{F^4_\bullet} = \pm(x_3 - x_1 - x_2)x_3,$$

where the final sign is seen to be the sign of the permutation $(1, 3, 4, \ldots, n - 2, 2) \in S_{n-1}$.

To compute the rest of the quadrics $[\ldots]$, we make use of the observation that the set $X_n$ is invariant under any relabeling of the coordinates $x_1, \ldots, x_{n-1}$, and that hence $S_{n-1}$ acts on resolution models of $X_n$. Let $\phi_r : F_r \to F_{r-1}$ denote the $r$-th differential of $F_\bullet$, and for a permutation $\sigma \in S_{n-1}$, observe that the maps $\phi^\sigma_r : F_r \to F_{r-1}$ defined by $\phi^\sigma_r(x_1, \ldots, x_{n-1}) = \phi_r(x_\sigma(1), \ldots, x_\sigma(n-1))$. The maps $(\phi^\sigma_r)_{r=1}^{n-2}$ are the differentials of a resolution model $F^\sigma_\bullet$ of $X_n$. It follows from the definition of the symbols $[\ldots]$ and the chain rule that we have

$$[a_1, \ldots, a_{n-2}]_{F^\sigma_\bullet}(x_1, \ldots, x_{n-1}) = [\sigma(a_1), \ldots, \sigma(a_{n-2})]_{F^\sigma_\bullet}(x_\sigma(1), \ldots, x_\sigma(n-1)).$$

Since both $F_\bullet$ and $F^\sigma_\bullet$ are resolution models of $X_n$, we deduce that there exists $\lambda_\sigma \in k$ such that $[\ldots]_{F^\sigma_\bullet} = \lambda_\sigma[\ldots]_{F_\bullet}$ holds for all quadrics $[\ldots]$. Thus $\sigma \mapsto \lambda_\sigma$ is a group homomorphism $S_{n-1} \to k^\times$, and is hence either trivial or the sign homomorphism. To see it is not trivial, consider the transposition $\sigma = (12)$. We see that the model $F^\sigma_\bullet$ is obtained in the same way as $F_\bullet$, by repeated unprojection, but with the difference that we start from the binary cubic $-x_1x_2(x_1 - x_2)$, and thus $\lambda_\sigma = -1$. Hence $\sigma \mapsto \lambda_\sigma$ is the sign character, and the lemma follows from the above equation and the computation we did for $[1, 2, \ldots, n - 2]$.

We now prove a lemma we will need in Chapter 5.

**Lemma 4.5.3.** Let $n \geq 4$ be an integer. Let $a_1, a_2, \ldots, a_{n-1} \in \mathbb{C}^\times$ be non-zero complex numbers, and let $\zeta \in \mathbb{C}$ be a primitive $n$th root of unity. Let $X' = \{P'_1, \ldots, P'_n\} \subset \mathbb{P}^{n-2}$ be a set of $n$ points in general position, with coordinates given by $P'_i = (\zeta^ia_1 : \zeta^{2i}a_2 : \ldots : \zeta^{(n-1)i}a_{n-1})$. Then...
the quadrics $\Omega_k$ associated to a resolution model of $X'$ are given, up to a scalar, by

$$
\sum_{i=1, i \neq k}^{n-1} a_k a_{n+k-i} x_i x_{n+k-i},
$$

where the subscripts are read modulo $n$.

**Proof.** Define $g \in \text{GL}_{n-1}(\mathbb{C})$ by $g_{ij} = a_j \zeta_{ij}$. Then $g$ takes the set $X$ to $X'$. Let $x_j' = \sum_{i=1}^{n-1} g_{ij} x_i$. By Theorem 3.2.3, it suffices to check that

$$
\Omega_{X', k}(x_1', x_2', ..., x_{n-1}') = \sum_{r=1}^{n-1} g_{rk} \Omega_{X, r}(x_1, x_2, ..., x_{n-1}),
$$

holds for all $k$. We first compute the right hand side:

$$
\sum_{r=1}^{n-1} g_{rk} \Omega_{X, r} = \sum_{r=1}^{n-1} a_k \zeta^r (nx_r^2 - 2x_r \sum_{p=1}^{n-1} x_p)
$$

$$
= \sum_{r=1}^{n-1} (n-2) a_k \zeta^r x_r^2 - \sum_{1 \leq p < r \leq n-1} 2(\zeta^r + \zeta^p) a_k x_r x_p.
$$

The left hand side is given by

$$
\sum_{i=1, i \neq k}^{n-1} a_k a_{n+k-i} x_i x_{n+k-i} = \sum_{i=1, i \neq k}^{n-1} a_k a_{n+k-i} \left( \sum_{p=1}^{n-1} a_p \zeta^{pi} x_p x_{n+k-i} \right) \left( \sum_{r=1}^{n-1} a_r \zeta^{r(n+k-i)} x_r \right)
$$

The coefficient of $x_r^2$ is $(n-2) a_k \zeta^r$ and the coefficient of $x_r x_p$, for $r$ and $p$ distinct, is given by

$$
a_k \left( \sum_{i=1, i \neq k}^{n-1} \zeta^{pi+r(n+k-i)} + \zeta^{ri+p(n+k-i)} \right) = a_k \left( (-1 - \zeta^{k(p-r)}) \zeta^r k + (-1 - \zeta^k(r-p)) \zeta^p k \right)
$$

$$
= 2(\zeta^r + \zeta^p) a_k,
$$

as desired. \hfill \Box

### 4.6 Unprojection of genus one normal curves of degree $n$

We now apply the machinery developed in the previous section to genus one curves. Throughout, $k$ will be a field, $n \geq 3$ an integer, and $R = k[x_1, \ldots, x_n]$ and $\mathcal{R} = k[x_1, \ldots, x_{n+1}]$.

We need some preliminary lemmas. The following argument is a special case of the well known fact that genus one normal curves embedded in projective space are projectively normal.

**Lemma 4.6.1.** Let $E$ be an elliptic curve over a field $k$ of characteristic 0, $D$ a divisor of $E$ of degree $n \geq 3$, and let $x_1, x_2, \ldots, x_n$ be a basis of the $n$-dimensional Riemann-Roch space $\mathcal{L}(D)$. Then the monomials $x_i x_j$, $1 \leq i, j \leq n$ span the $2n$-dimensional space $\mathcal{L}(2D)$.

**Proof.** For the proof we are free to extend our base field and assume $k = \bar{k}$ is algebraically closed. Observe that we are free to replace $D$ by any linearly equivalent divisor. For a point
4.6. UNPROJECTION OF GENUS ONE NORMAL CURVES OF DEGREE $N$

$Q \in E(k)$, let $\tau_Q$ denote the translation by $Q$ map. We may also replace $D$ by $\tau_Q^*(D)$ for any $Q \in E(k)$. Now recall that for an elliptic curve, two divisors are linearly equivalent if and only if they have the same degree and the same sum.

As $k$ is algebraically closed, there exists a $Q \in E(k)$ with $n \cdot Q = \sum(D)$, so that $\sum(\tau_Q^*(D)) = \sum(D) - nQ = 0$. Hence $\sum(\tau_Q^*(D))$ has sum $0$ and degree $n$, and so is linearly equivalent to $n \cdot 0$. Thus we may replace $D$ with $n \cdot 0$. Note that it suffices to prove the claim for a single choice of the basis $x_1, x_2, \ldots, x_n$, i.e. we are really asserting that the natural map $S^2(L(D)) \to L(2D)$ is surjective. As $1, x, y, x^2, xy, \ldots, x^{\frac{m}{2}}$ form a basis of $L(m \cdot 0)$ for $m$ even, and $1, x, y, x^2, xy, \ldots, x^\frac{m-1}{2}$ form a basis for $m$ odd, this statement is clear.

In what follows, let $C \subset \mathbb{P}^n$ be a genus one normal curve of degree $n + 1$ defined over a field $k$, where $n \geq 3$. We assume that $C$ contains the point $P = (0 : 0 : \ldots : 0 : 1)$.

**Lemma 4.6.2.** The projection map $\pi$ from the point $P$,

$$\pi : \mathbb{P}^n \to \mathbb{P}^{n-1} : (x_1 : \ldots : x_{n+1}) \to (x_1 : \ldots : x_n),$$

restricts to a regular map $C \to \mathbb{P}^{n-1}$, also denoted $\pi$. The image of $\pi$ is a genus one normal curve of degree $n$, denoted $C$.

**Proof.** We identify $C$ with its Jacobian $E = \text{Pic}^0(C)$ via the map $Q \mapsto (Q) - (P)$. Let $H$ be a hyperplane in $\mathbb{P}^{n-1}$ passing through $P$, and regard $D = C \cap H$ as a divisor of $E$. Then the embedding $C \subset \mathbb{P}^n$ is identified with the embedding of $E$ into $\mathbb{P}^n$ associated to the complete linear system $|D|$, and the forms $x_i$ for $i \leq n$, are identified with elements of $L(D - P)$. As $C$ is a genus one normal curve, $x_1, \ldots, x_n$ is basis of of $L(D - P)$. Thus $C \subset \mathbb{P}^{n-1}$ is the embedding associated to the complete linear system $|D - P|$, and hence is a genus one normal curve of degree $n$.

**Lemma 4.6.3.** Let $J$ be the ideal generated by the linear forms in $R$ that vanish on the tangent space $T_P C$ at $P$. Let $I$ and $I$ be the homogeneous ideals of $R$ and $R$ that define the curves $C$ and $C$ respectively. Then the ideals $I, J = J \cap R$ and $I$ form an unprojection triple.

**Proof.** We check condition (i) of Definition 4.3.4. By Theorem 3.1.3, ideals $I$ and $I$ are generated by quadrics. By definition, $J$ is generated by linear forms.

For condition (ii), as $C = \pi(C)$, we have $I = I \cap R$. We may identify the space of linear forms vanishing at $T_P C$ with the Riemann-Roch space $L(D - 2P)$. As $D - 2P = (D - P) - P$, we can identify $L(D - 2P)$ with the space of linear forms on $\mathbb{P}^{n-1}$ that vanish at $\pi(P)$, and the ideal $J = \mathcal{I} \cap R$ with the ideal generated by these forms. As $\pi(P) \in C(k)$, we have $I \subset J$.

Let us verify condition (iii). Identify $x_0, x_1, \ldots, x_n$ with a basis of $L(D)$, with $x_0, \ldots, x_{n-1}$ also serving as a basis of $L(D - P)$. As $I$ is generated by forms of degree 2, its leading coefficient ideal, denoted $J'$, must be generated by linear forms. We claim that $J = J'$. Let us first show that $J' \subset J$.

Let $f \in I$ be a quadric, and write $f = x_{n+1} l + h$, where $l$ is a linear form and $h \in R$, so that $l$ is the leading coefficient of $f$. The form $h$ is a quadric in $x_1, \ldots, x_n$, so vanishes at $P$.
with multiplicity at least 2. As $x_{n+1}$ does not vanish at $P$, $l$ must vanish at $P$ with multiplicity at least 2, and hence $l \in \mathcal{J}$. As $l$ is a linear form, it can be written as a linear combination of $x_1, \ldots, x_{n+1}$. Since $l(P) = 0$, the coefficient of $x_{n+1}$ must be 0, and thus $l \in R$, and hence $l \in J = \mathcal{J} \cap R$.

By Lemma 4.6.1, the forms $x_i x_j$ for $1 \leq i, j \leq n$ span the space $\mathcal{L}(2D - 2P)$. For any $l \in \mathcal{L}(D - 2P)$, we have $x_{n+1} l \in \mathcal{L}(2D - 2P)$. Thus by Lemma 4.6.1, we have $x_{n+1} l = \sum_{i,j} c_{i,j} x_i x_j$ for some constants $c_{i,j}$, and $x_{n+1} l - \sum_{i,j} c_{i,j} x_i x_j$ is a quadric in $\mathcal{I}$ with leading coefficient $l$. Thus $J' \subset J$, and hence $J = J'$.

The condition (iv) of Definition 4.3.4 follows from general results on the structure of minimal free resolutions of genus one normal curves, e.g. Theorem 3.1.3. \hspace{1cm} \square

We now give our first application, finishing the proof of Lemma 3.3.2(ii).

**Lemma 4.6.4.** Let $C_n \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n$, defined over a field $k$ of characteristic 0, let $I$ be the defining ideal of $C$, let $F_n^\bullet$ be a resolution model of $C$ and let $\Omega$ be the $\Omega$-matrix associated to this data, as explained in Chapter 3.

Then the rational differential form $\omega$, associated to $\Omega$, is regular on $C_n$. More precisely, for $1 \leq i < j \leq n$, the differential

$$\omega = \frac{x_j^2 d(x_i/x_j)}{\Omega_{ij}(x_1, \ldots, x_n)}$$

is regular on $C_n$.

**Proof.** The proof is by induction on $n$. The base case $n = 3$, is just the statement that if $F$ is the ternary cubic that defines $C$, the differential $\frac{x_2^2 d(x_2/x_1)}{\partial F/\partial x_2}$ is regular on $C$, and this is an elementary fact from the theory of plane curves. Let us suppose that lemma is true for $n - 1$.

For the proof of the statement we are free to enlarge the base field, and assume that $k = \tilde{k}$ is algebraically closed, and thus that there exists a $k$-rational point $P \in C_n(k)$. By Lemma 3.4.8, we are also free to make a change of coordinates on $\mathbb{P}^{n-1}$, and thus assume that $P = (0 : 0 : \ldots : 0 : 1)$. Let $i, j, a_1, \ldots, a_{n-2}$ be a permutation of the set $\{1, 2, \ldots, n\}$. By Lemma 3.4.7, it suffices to prove that

$$\frac{x_j^2 d(x_i/x_j)}{a_1, \ldots, a_{n-2}} = (n - 2)\omega$$

is regular. Note that we use the hypothesis that $k$ is of characteristic 0 here, so that $n - 2$ is non-zero. By Lemma 3.4.6, it suffices to prove the lemma for any permutation of $i, j, a_1, \ldots, a_{n-2}$. Thus we may assume that $n - 2 \notin \{i, j\}$.

Now let $\pi$ be the projection from point $P$, and let $C_{n-1} = \pi(C_n)$. Let $I_{n-1}$ and $I_n$ be the ideals defining $C_{n-1}$ and $C_n$, and let $J$ be the ideal defining $\pi(P)$. By Lemma 4.6.3, $I_{n-1}, J$ and $I_n$ form an unprojection triple. Let $F^{n-1}_\bullet$ and $G_\bullet$ be minimal graded free resolutions of $I_{n-1}$ and $J$.

Note that the matrix $\Omega$ depends on the choice of the resolution $F_n^\bullet$ only up to a non-zero scalar multiple. Thus, we may assume $F_n^\bullet$ is the chain complex $\mathcal{H}(\alpha, \beta, \delta)$ constructed from $F_{n-1}^\bullet$ and $G_\bullet$. By Proposition 4.3.10,

$$[a_1, a_2, \ldots, a_{n-2}] = \pm [a_1, a_2, \ldots, \hat{n}, \ldots, a_{n-2}],$$
Suppose we are also given a point \( P \) defined over the field of \( C \). Let \( \pi \) be the projection \( \pi \) is given by \( (x_1 : \ldots : x_n) \mapsto (x_0 : \ldots : x_{n-1}) \), we have

\[
\frac{x_j^3 d(x_i/x_j)}{[a_1, \ldots, a_{n-2}]} = \pi^* \left( \pm \frac{x_j^3 d(x_i/x_j)}{[a_1, a_2, \ldots, \widehat{n}, \ldots, a_{n-2}]} \right)
\]

and we are done by the induction hypothesis, as \( \pi : C_n \to C_{n-1} \) is an isomorphism. \( \square \)

### 4.7 The local minimization theorem

We now give our first arithmetic application, the local version of the minimization theorem. Throughout, we fix a prime \( p \). Let \( \mathbb{Q}_p \) be the field of \( p \)-adic numbers and let \( \mathbb{Z}_p \) be the ring of \( p \)-adic integers. The following theorem is a generalization of Theorem 3.4 of [CFS10].

**Theorem 4.7.1.** Let \( p \) be a prime, and let \( C \subset \mathbb{P}^{n-1} \) be a genus one normal curve of degree \( n \), defined over the field of \( p \)-adic numbers \( \mathbb{Q}_p \). Suppose that the set \( C(\mathbb{Q}_p) \) is non-empty. Let \( E \) be the Jacobian of \( E \), defined by a minimal Weierstrass equation \( W \)

\[
y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.
\]

Then one can choose coordinates on \( \mathbb{P}^{n-1} \), and then a \( \mathbb{Z}_p \)-integral genus one model \( F_\bullet \) of \( C \) with the associated invariant differential \( \omega \), such that there exists an isomorphism \( \gamma : E \to C \) with

\[
\omega = \gamma^* \left( \frac{dx}{2y + a_1 x + a_3} \right)
\]

We say such a genus one model is a **minimal** model of \( C \).

Once we prove Theorem 3.3.5, this theorem will immediately imply the following corollary.

**Corollary 4.7.2.** Let \( n \) be an odd integer. If \( \Omega \) is the \( \Omega \)-matrix of a minimal model of a genus one curve \( C \) as above, we have \( c_k(\Omega) = (n - 2)^k c_k(W) \), for \( k = 4, 6 \), where \( c_k(W) \) are the \( \epsilon \)-invariants of a minimal Weierstrass equation \( W \) of \( E \), as defined in Chapter III of [Sil09].

The induction step in the proof of the theorem is provided by the following lemma, which may be viewed as a generalization of Lemma 3.14 of [CFS10].

**Lemma 4.7.3.** Let \( E/\mathbb{Q}_p \) be an elliptic curve and let \( D \) be a degree \( n \) divisor on \( E \), for \( n \geq 3 \). Let \( i : E \to \mathbb{P}^{n-1} \) be an embedding induced by a choice of basis of \( \mathcal{L}(D) \), and let \( C_n = i(E) \subset \mathbb{P}^{n-1} \). Suppose we are also given a point \( P \in E(\mathbb{Q}_p) \).

Let \( F_\bullet \) be a \( \mathbb{Z}_p \)-integral genus one model of \( C_n \), with \( l_n = \phi_1(F_1) \subset \mathbb{Z}_p[x_1, \ldots, x_n] \). Further, let \( l_1, \ldots, l_{n-1} \) be a \( \mathbb{Z}_p \)-basis for the space of linear forms with integral coefficients that vanish at \( i(P) \in \mathbb{P}^{n-1} \), and denote by \( G_\bullet \) the Koszul complex associated to \( J = (l_1, l_2, \ldots, l_{n-1}) \). Then:

(i) The complexes \( F_\bullet \) and \( G_\bullet \) satisfy the hypothesis of Proposition 4.4.1, and the associated complex \( H_{\text{min}} \) is a \( \mathbb{Z}_p \)-integral genus one model of \( C_{n+1} \subset \mathbb{P}^n \), where \( C_{n+1} \) is the image of \( E \) under an embedding induced by a choice of basis of \( \mathcal{L}(D + P) \).
(ii) The point $P$ maps to the point $(0 : 0 : \ldots : 0 : 1) \in C_{n+1}(\mathbb{Q}_p)$, and projection from $P$ defines an isomorphism $\pi : C_{n+1} \rightarrow C_n$. Moreover, if $\omega_n$ and $\omega_{n+1}$ are differentials associated to models $F_*$ and $\mathcal{H}_{min}$, we have $\pi^*(\omega_n) = \pm \omega_{n+1}$.

**Proof.** We first prove that $l_1, \ldots, l_{n-1}$ is a regular sequence on $\mathbb{Z}_p[x_1, \ldots, x_n]$. By the definition of the forms $l_i$ and the theory of elementary divisors, we can find a linear form $l_n \in \mathbb{Z}_p[x_0, \ldots, x_{n-1}]$ so that $l_1, \ldots, l_n$ is a basis for the $\mathbb{Z}_p$-module of integral linear forms.

Then we can identify rings $\mathbb{Z}_p[x_1, \ldots, x_n] = \mathbb{Z}_p[l_1, \ldots, l_n]$, and hence $l_1, \ldots, l_{n-1}$ is a regular sequence. By Theorem 2.2.7, the Koszul complex $G_\bullet$ is a free resolution of the ideal $J = (l_1, l_2, \ldots, l_{n-1})$, and as explained in Section 2.2, the DGC structure on $G_\bullet$ induces an isomorphism $G_\bullet \rightarrow G_\bullet^\ast$. By the definition of a genus one model, this is true for $F_*$ as well.

To see that $I_n \subset J$, again identify $\mathbb{Z}_p[x_1, \ldots, x_n] = \mathbb{Z}_p[l_1, \ldots, l_n]$. Then every quadric $f \in I_n$ can be expressed as $\sum_{i,j} c_{ij} l_i l_j$, and if $f(P) = 0$, the coefficient of $l_n^2$ is zero, and $f \in J$. Thus the conditions of Proposition 4.4.1 are satisfied.

To verify (ii), we are free to extend scalars from $\mathbb{Z}_p$ to $\mathbb{Q}_p$, and identify $I_n$ and $J$ with ideals of $\mathbb{Q}_p[x_1, \ldots, x_n]$. Let $I_{n+1}$ be the ideal of $\mathbb{Q}_p[x_1, \ldots, x_{n+1}]$ resolved by $\mathcal{H}^{min}(\alpha, \beta, \delta)$. There exists a choice of basis of $\mathcal{L}(D + P)$ so that the corresponding embedding $j : E \rightarrow \mathbb{P}^n$ we have $j(P) = (0 : \ldots : 0 : 1)$, and projection $\pi$ from $P$ defines an isomorphism $C_{n+1} \rightarrow C_n$.

Let $I_{n+1}'$ be the ideal defining $C_{n+1}$. By Lemma 4.6.3, $I_n, J$ and $I_{n+1}$ are an unprojection triple, and so $I_{n+1}'$ is resolved by the complex $\mathcal{H}^{min}(\alpha', \beta', \delta')$. By Lemma 4.3.7, $\mathcal{H}^{min}(\alpha', \beta', \delta')$ is isomorphic to $\mathcal{H}^{min}(\alpha, \beta, \delta)$, and hence we have $I_{n+1}' = I_{n+1}$.

Finally, recall that invariant differential associated to a genus one model $F_*$ is given by

$$\omega_n = \frac{(n-2)x_j^2d(x_i/x_j)}{\Omega_{ij}(x_1, \ldots, x_n)} = \frac{x_j^2d(x_i/x_j)}{[a_1, \ldots, a_{n-2}]}.$$  

Hence the assertion that $\pi^*(\omega_n) = \pm \omega_{n+1}$ follows from Lemma 4.3.10, in the same way as in the proof of Lemma 4.6.4.  

**Proof of Theorem 4.7.1.** The proof is by induction. Choose a point $P \in C_n(\mathbb{Q}_p)$. Note that as $\mathbb{Z}_p$ is a principal ideal domain, by elementary divisor theory, the group $\text{SL}_n(\mathbb{Z}_p)$ acts transitively on $\mathbb{P}^{n-1}(\mathbb{Q}_p)$. We may assume, making a $\text{SL}_n(\mathbb{Z}_p)$-change of coordinates if necessary, that $P = (0 : 0 : \ldots : 0 : 1)$. Let $C_{n-1} = \pi(C_n) \subset \mathbb{P}^{n-2}$ be the projection of $C_n$ from $P$. By Lemma 4.7.3, the assertion of the theorem is true for the curve $C_{n-1}$ if and only if it is true for the curve $C_n$.

Thus we are reduced to the case $n = 3$. Now let $D$ be a hyperplane section of $C_3$, identified with a degree 3 divisor on $E$. The description of the group law on $E$ implies that $D$ is linearly equivalent to a divisor $4 \cdot 0_E - Q$, for some $Q \in E(\mathbb{Q}_p)$. By Lemma 4.7.3, it suffices to prove the theorem for the curve $C_4$, the image of $E$ embedded via the linear system $|4 \cdot 0_E|$. Applying Lemma 4.7.3 for the final time, we are reduced to the case of $E$ embedded in $\mathbb{P}^2$ by $|3 \cdot 0_E|$. Choose the basis $1, x, y$ of $\mathcal{L}(3 \cdot 0_E)$. Then the image of $E$ in $\mathbb{P}^2$ is defined by the cubic

$$F = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$$

and we easily compute that the differential $\omega$ associated to $F$ agrees with the Neron differential
4.8. **Proof of the Global Minimization Theorem**

We now deduce Theorem 4.1.1 from the local result, Theorem 4.7.1, using (basic) results on strong approximation. The idea is to begin by choosing arbitrarily a resolution model $F_*$ of $C \subset \mathbb{P}^{n-1}$ defined over $\mathbb{Q}$. Clearing denominators, we may assume $F_*$ is defined over $\mathbb{Z}$. It follows from Theorem 3.3.5 that $F_*$ is potentially not minimal for a finite set $S$ of primes, namely those that divide both $c_4(F_*)$ and $c_6(F_*)$. For every $p \in S$, we construct a minimal model using Theorem 4.7.1. We then use strong approximation to modify $F_*$, so that it is $\mathbb{Z}_p$-equivalent to this minimal model for every $p \in S$, while preserving minimality for $p \not\in S$, concluding the proof. This is essentially the approach taken in [Fis07] to prove a minimization theorem for binary quartics and ternary cubics.

For a prime $p$, let $||·||_p$ be the $p$-adic absolute value. For any $A = (a_{ij}) \in \text{Mat}_n(\mathbb{Q}_p)$, let $||A||_p = \max_{1 \leq i,j \leq n} ||a_{ij}||$.

**Lemma 4.8.1.** Let $S$ be a finite set of primes of $\mathbb{Q}$. Suppose we are given, for each $p \in S$, an element $A_p \in \text{SL}_n(\mathbb{Z}_p)$. Let $\epsilon > 0$. Then there exists $A \in \text{SL}_n(\mathbb{Z})$ with $||A - A_p||_p < \epsilon$ for all $p \in S$.

**Proof.** This is Lemma 3.2 of [Fis07]. Alternatively, this follows from the well known fact that for any integer $N$, the map $\text{SL}_n(\mathbb{Z}) \to \text{SL}_n(\mathbb{Z}/N\mathbb{Z})$ is surjective - see Lemma 6.3.10 in [Coh08].

Note that the result is false if we replace $\text{SL}_n$ with $\text{GL}_n$, as can already be seen in the case $n = 1$. We do however have the following result.
Lemma 4.8.2. Let $S$ be a finite set of primes of $\mathbb{Q}$ and let $\delta \in \mathbb{Z}$ be an integer. Suppose we are given, for each $p \in S$, $A_p \in \text{Mat}_n(\mathbb{Z})$ with $\det(A_p) = \delta$. Let $\epsilon > 0$. There exists $A \in \text{Mat}_n(\mathbb{Z})$ such that $\det(A) = \delta$, and $\|A - A_p\|_p < \epsilon$ for each $p \in S$.

Proof. Follows from the previous lemma, together with a Smith normal form argument - see Lemma 3.3 of [Fis07].

Lemma 4.8.3. Let $A \in \text{GL}_n(\mathbb{Q}_p)$. There exists an $\epsilon > 0$, such that for every $B \in \text{GL}_n(\mathbb{Q}_p)$ with $\|A - B\|_p < \epsilon$, we have $A = UB$, for some $U \in \text{GL}_n(\mathbb{Z}_p)$.

Proof. We have $AB^{-1} = I_n + (A - B)B^{-1} = I_n + \det(B)^{-1}(A - B)\text{adj}(B)$, where $\text{adj}(B)$ denotes the adjugate matrix of $B$. Since $\det(B)$ and $\text{adj}(B)$ depend continuously on $B$, it is clear there exists an $\epsilon > 0$ such that $\|A - B\|_p < \epsilon$ implies that $AB^{-1} \in \text{Mat}_n(\mathbb{Z}_p)$ and $\|\det(B)\|_p = \|\det(A)\|_p$, and hence $AB^{-1} \in \text{GL}_n(\mathbb{Z}_p)$.

Proof of Theorem 4.1.1. To begin, choose any resolution model $F_\bullet$, defined over $\mathbb{Q}$, that represents the n-diagram $[C \subset \mathbb{P}^{n-1}]$. Clearing denominators if needed, we may assume $F_\bullet$ is defined over $\mathbb{Z}$. By Theorem 3.3.5, $c_k(F_\bullet)$ are the $c$-invariants of a Weierstrass equation for $E$. Hence there exists $\lambda \in \mathbb{Q}$ with $c_k(F_\bullet) = \lambda^k(n - 2)^k c_k(W)$. Let $S$ be the set of primes that contains all of the primes that appear in the numerator and denominator of $\lambda$ as well as the primes for which $F_\bullet$ is not $\mathbb{Z}_p$-integral. The idea is to use Lemma 4.8.2 to construct an integral model $F_\bullet'$, that is $\mathbb{Q}$-equivalent to $F_\bullet$, and $\mathbb{Z}_p$-equivalent to a minimal model for each $p \in S$.

As $C(\mathbb{Q}_p)$ is non-empty for every $p \in S$, we may apply Theorem 4.7.1. Thus $F_\bullet$ is $\mathbb{Q}_p$-equivalent to a $\mathbb{Z}_p$-integral model $F'_\bullet$, with $c_k(F'_\bullet) = (n - 2)^k c_k(W)$. Recall that $\mathcal{G}_n = \mathcal{G}_n^{\text{res}} \times \text{GL}_n$, where $\mathcal{G}_n^{\text{res}} = \text{GL}_{b_{n-1}} \times \ldots \times \text{GL}_{b_0}$ acts on the modules in $F_\bullet$, while $\text{GL}_n$ acts by linear substitution in the variables $x_0, x_1, \ldots, x_{n-1}$. Let $g^p = (g^p_{n-2}, \ldots, g^p_1, g^p_0) \times (\gamma^p) \in \mathcal{G}_n(\mathbb{Q}_p)$ be such that we have $g^p \cdot F_\bullet = F'_\bullet$.

We now modify the transformations $g^p$ so that we can apply Lemma 4.8.2. We first show that we can assume that for every $p \in S$, we have $g^p_i \in \text{Mat}_{b_i}(\mathbb{Z}_p)$ for all $i$, as well as $\gamma^p \in \text{Mat}_n(\mathbb{Z}_p)$. To see this, observe that replacing $x_i$ by $tx_i$, for some non-zero $t \in \mathbb{Q}$ and all $i$, has the same effect as replacing $\phi_i$ by $t^{\deg(\phi_i)} \phi_i$, for $1 \leq i \leq n - 2$, as $\phi_i$ is a matrix of homogeneous forms in $x_1, \ldots, x_n$, of degree $\deg(\phi_i)$. But this is the same as rescaling the basis of each module $F_i$ by $t^{\sum_{j < i} \deg(\phi_j)}$. In other words, we can replace $g^p$ with $(t^{-n} \cdot g^p_{n-2}, \ldots, t^{-2} \cdot g^p_1, g^p_0) \times (t \cdot \gamma^p)$. We choose $t$ so that $t \cdot \gamma^p \in \text{Mat}_n(\mathbb{Z}_p)$ for all $p \in S$, and then modify the transformations $g^p$ as described. Furthermore, for any $t' \in \mathbb{Q}_p$, we can rescale the basis of each $F_i$ by $t'$ - this does not change the matrices $\phi_i$, and hence does not change $\lambda$. In doing this, we replace $g^p$ with $(t' \cdot g^p_{n-2}, \ldots, t' \cdot g^p_1, t' \cdot g^p_0) \times (\gamma^p)$. We choose $t' \in \mathbb{Q}$ to ensure that $g^p_i \in \text{Mat}_{b_i}(\mathbb{Z}_p)$ for all $i$.

Finally, we modify the local minimal models $F^p_i$, so that we have, for each $i$ $\det(g^p_i) = \delta_i$ for some $\delta_i \in \mathbb{Z}$, as well as $\det(\gamma^p) = \delta$, for some $\delta \in \mathbb{Z}$. We do this as follows. Let $\det(g^p_i) = \delta_i^p$. As the set $S$ is finite, and $\mathbb{Z}$ is a principal ideal domain, there exists a $\delta_i \in \mathbb{Z}$ with $||\delta_i||_p = ||\delta_i^p||_p$ for every $p \in S$, and $||\delta_i||_p = 0$ for $p \notin S$. Now multiply a basis vector of $F^p_i$ by $\delta_i/\delta_i^p$ - this has the effect of rescaling a column of $g^p_i$ by $\delta_i/\delta_i^p$, and corresponds to a $\mathcal{G}_n(\mathbb{Z}_p)$-transformation, hence the modified model is still minimal. The same procedure can be used for matrices $\gamma^p$ as well.

By Lemma 4.8.3 and Lemma 4.8.2, there exist $g^p_i \in \text{Mat}_{b_i}(\mathbb{Z})$ and $\gamma^p \in \text{Mat}_n(\mathbb{Z})$, with the property that for all $p \in S$, we have $g^p_i = U^p_i g^p_i$ and $\gamma^p = U^p \gamma^p$, for some $U^p_i \in \text{GL}_{b_i}(\mathbb{Z}_p), U^p \in \text{GL}_n(\mathbb{Z}_p)$.
4.8. PROOF OF THE GLOBAL MINIMIZATION THEOREM

GL_n(Z_p). Put $F'_\bullet = g' \cdot F_\bullet$. Then $F'_\bullet$ is $\mathbb{Z}_p$-equivalent to a minimal model for every $p \in S$ via the transformation $(U_{n-2}^p, \ldots, U_0^p) \times (U^p)$.

The model $F'_\bullet$ is defined over $\mathbb{Z}$. Indeed, it suffices to check it is $\mathbb{Z}_p$-integral for every prime $p$. For primes $p \in S$, this is by construction. For primes $p \notin S$, by construction we have $g' \in G_n(\mathbb{Z}_p)$, and as $F_\bullet$ is integral, then so is $F'_\bullet$.

We now claim that for every prime $p$, we have $||c_k(F'_\bullet)||_p = ||(n-2)^k c_k(W)||_p$. For primes $p \in S$, this is by construction. For $p \notin S$, observe that our modification of $F_\bullet$ does not change $||c_k(F_\bullet)||_p$ for $p \notin S$, and since we assumed $||\lambda||_p = 1$ for $p \notin S$, we have $||c_k(F'_\bullet)||_p = ||c_k(F_\bullet)||_p = ||(n-2)^k F_\bullet||_p$. Hence, for every prime $p$ we have $||c_k(F'_\bullet)||_p = ||(n-2)^k c_k(W)||_p$. Thus $c_k(F'_\bullet) = \pm (n-2)^k c_k(W)$, and it follows from Theorem 3.3.5 that $c_k(F'_\bullet) = (n-2)^k c_k(W)$, and hence that the model $F'_\bullet$ is a global minimal model. \qed
Chapter 5

Analytic theory of elliptic normal curves

5.1 Heisenberg invariant diagrams

Let \([C \to \mathbb{P}^{n-1}]\) be an \(n\)-diagram, defined over \(\mathbb{C}\), and let \(E\) be the Jacobian of \(C\). The \(n\)-torsion subgroup \(E[n]\) acts on \(\mathbb{P}^{n-1}\) by projective linear transformations in a natural way, and this action is compatible with the embedding \(C \to \mathbb{P}^{n-1}\). In this section we will use the theory of elliptic functions to choose coordinates on \(\mathbb{P}^{n-1}\) so that this action of \(E[n]\) and the embedding \(C \subset \mathbb{P}^{n-1}\) take a particularly simple form. This construction is classical, and dates back to Klein. In Section 5.2, we use it to prove Theorem 3.3.5. The results of this chapter will also play an important role later on in Chapter 6, in obtaining effective bounds for constants in Theorem 1.0.1.

Our main reference will be the first chapter of [Hul86], as well as Chapter 4 of [Fis00]. Throughout we fix an odd integer \(n \geq 3\). A remark on the notation - in this chapter, we will label the coordinates on \(\mathbb{P}^{n-1}\) starting from 0, as \(X_0, \ldots, X_{n-1}\), since this will simplify the notation slightly.

We first recall some basic properties of the Weierstrass \(\sigma\)-function, the proofs of which can be found in [Sil94]. Fix \(n \geq 3\) odd. Let \(\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}\) be a lattice, with \(\text{Im}(\omega_2/\omega_1) > 0\).

The quasi-period map \(\eta : \Lambda \to \mathbb{C}\) is defined by

\[
\eta(\omega) := -\int_0^\infty \wp(z, \Lambda)dz
\]

where \(\wp(z, \Lambda)\) is the Weierstrass p-function. Let \(\eta_1 = \eta(\omega_1)\) and \(\eta_2 = \eta(\omega_2)\) be the period constants of \(\Lambda\). We then have:

**Proposition 5.1.1.**

(i) The quasi-period map \(\eta\) is a homomorphism of \(\Lambda\) into \(\mathbb{C}\), and we have the Legendre relation: \(\omega_2 \eta_1 - \omega_1 \eta_2 = 2\pi i\).

(ii) The infinite product

\[
\sigma(z, \Lambda) := z \prod_{\omega \in \Lambda, \omega \neq 0} (1 - z/\omega)e^{z/\omega + (1/2)(z/\omega)^2}
\]
defines a holomorphic function on $\mathbb{C}$ with simple zeros on $\Lambda$ and no other zeros, called the Weierstrass $\sigma$–function, (associated to the lattice $\Lambda$).

(iii) For all $z \in \mathbb{C}$, we have the following formulas describing translation by $\omega_1$ and $\omega_2$:

$$
\sigma(z + \omega_1, \Lambda) = -e^{\eta_1(z + \frac{\omega_1}{2})} \sigma(z, \Lambda)
$$

$$
\sigma(z + \omega_2, \Lambda) = -e^{\eta_2(z + \frac{\omega_2}{2})} \sigma(z, \Lambda)
$$

Now let $\sigma_{pq}(z, \Lambda) := \sigma(z - \frac{p\omega_1 + q\omega_2}{n}, \Lambda)$, and define constants

$$
\omega := e^{-\frac{n-1}{2} \eta_2}, \theta := e^{-\frac{\omega_1}{2n}}
$$

and for all $m \in \mathbb{Z}$, define functions $x_m(z, \Lambda)$ by

$$
x_m(z, \Lambda) := \omega^m \theta^m e^{m \eta_1} \prod_{i=0}^{n-1} \sigma_{m,i}(z, \Lambda).
$$

These functions have the following properties (Theorem I.2.3 of [Hul86]):

**Proposition 5.1.2.** (i) For all $m \in \mathbb{Z}$ we have $x_{n+m} = x_m$.

(ii) Let $\zeta := e^{-\frac{2\pi i}{n}}$. There exist holomorphic nowhere vanishing functions $j, j_1$ and $j_2$, such that, for all $m \in \mathbb{Z}$, we have the following formulas:

(a) $x_m(-z, \Lambda) = j(z) x_{-m}(z, \Lambda),$

(b) $x_m(z - \frac{\omega_1}{n}, \Lambda) = j_1(z) \cdot x_{m+1}(z, \Lambda),$

(c) $x_m(z + \frac{\omega_2}{n}, \Lambda) = j_2(z) \cdot \zeta^m x_m(z, \Lambda)$

(d) $x_m(0, \Lambda) = -x_{n-m}(0, \Lambda)$

Proof is a straightforward calculation - see [Hul86].

**Proposition 5.1.3.** The functions $x_0, \ldots, x_{n-1}$ can be viewed as a basis of the space of global sections of the line bundle $\mathcal{O}_{\mathbb{C}/\Lambda}(n \cdot 0)$, and hence the map

$$
\mathbb{C}/\Lambda \rightarrow \mathbb{P}^{n-1} : z \mapsto (x_0(z, \Lambda) : \ldots : x_{n-1}(z, \Lambda))
$$

defines an $n$-diagram, which we denote by $B_{\Lambda}$. Furthermore, identifying $\mathbb{C}/\Lambda$ with its image, which we will denote by $C_{\tau}$, translation by $\frac{\omega_1}{n}$ extends to the automorphism of $\mathbb{P}^{n-1}$ defined by

$$(x_0 : x_1 : \ldots : x_{n-1}) \mapsto (x_{n-1} : x_0 : \ldots : x_{n-2}),$$

translation by $\frac{\omega_2}{n}$ is defined by

$$(x_0 : x_1 : \ldots : x_{n-1}) \mapsto (x_0 : \zeta x_1 : \ldots : \zeta^{n-1} x_{n-1}),$$

and the inversion map $z \mapsto -z$ corresponds to

$$(x_0 : x_1 : x_2 : \ldots : x_{n-2} : x_{n-1}) \mapsto (x_0 : x_{n-1} : x_{n-2} : \ldots : x_2 : x_1).$$
This proposition follows immediately from the previous one, except for the statement on the linear independence of the functions $x_0, \ldots, x_{n-1}$, the proof of which can be found in [Hul86].

**Proof.** It follows from Lemma 5.1.2(ii) that the functions $x_r(z, \Lambda)$ are global sections of a line bundle on $\mathbb{C}/\Lambda$. The function $\sigma(z, \Lambda)$, as explained in Chapter I of [Sil94], has a simple zero at every $\omega \in \Lambda$, and no other zeros. We then see that the divisor of zeros of $x_r$, viewed as a section of this line bundle, consists of points

$$\frac{r\omega_1}{n}, \frac{r\omega_1 + \omega_2}{n}, \ldots, \frac{r\omega_1 + (n-1)\omega_2}{n}.$$  

The sum of this divisor is $r\omega_1 + \frac{n-1}{2}\omega_2$, and hence, as $n$ is odd, we deduce that the line bundle is isomorphic to $\mathcal{O}_{\mathbb{C}/\Lambda}(n \cdot 0)$. Thus we indeed have an induced map $\mathbb{C}/\Lambda \to \mathbb{P}^{n-1}$. For it to define an $n$-diagram, we only need to prove that the functions $x_r(z)$ span the space of global sections, which by the Riemann-Roch theorem is equivalent to proving that they are linearly independent. This follows from the representation theory of Heisenberg group, which we will now introduce. More details can be found in [Hul86].

**Remark 5.1.4.** The projective representation of $E[n]$ on $\mathbb{P}^{n-1}$ lifts to a linear representation of the Heisenberg group $H_n$ on an $n$-dimensional vector space $V$. $H_n$ can be defined as the subgroup of $\text{GL}_n(\mathbb{C})$ generated by the lifts $\sigma_{\omega_1/n}$ and $\sigma_{\omega_2/n}$ of the translation maps by $\frac{\omega_1}{n}, \frac{\omega_2}{n}$:

$$\sigma_{\omega_1/n} := \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}, \quad \sigma_{\omega_2/n} := \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \zeta & 0 & \ldots & 0 & 0 \\ 0 & 0 & \zeta^2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & \zeta^{n-1} \end{pmatrix}.$$  

$H_n$ is a non-abelian group of order $n^3$, with the centre $Z(H_n) = \{ \zeta^r \mid n \cdot r \in \mathbb{Z} \}$. For this reason we will refer to diagrams $[\mathbb{C}/\Lambda \to \mathbb{P}^{n-1}]$ constructed in this way as the Heisenberg invariant diagrams.

The representation $V$ is the known as the Schrodinger representation of $H_n$. It is an irreducible representation, and this fact implies that $x_0, \ldots, x_r$ are linearly independent, finishing the proof of Lemma 5.1.3. Again, for more details, see [Hul86].

We now recall the product expansion of the Weierstrass $\sigma$-function. Let $\mathcal{H}$ denote the upper halfplane. For $\tau \in \mathcal{H}$, let $\Lambda_\tau := \mathbb{Z} \oplus \mathbb{Z}\tau$ be a lattice. For legibility we will denote the diagram $B_{\Lambda_\tau}$ by $B_{\tau}$. Set $q := e^{2\pi i \tau}$ and $u := e^{2\pi i z}$. We then have [Sil94]:

$$\sigma(z, \Lambda_\tau) = -\frac{1}{2\pi i} e^{(1)z^2} e^{-\pi i z (1 - u)} \prod_{n \geq 1} \frac{(1 - q^n u)(1 - q^n u^{-1})}{(1 - q^n)^2}.$$  

**Proposition 5.1.5.** The functions $x_r(z, \Lambda_\tau)$ admit the product expansion:

$$x_r(z, \Lambda_\tau) = C \cdot (-1)^r q^{\frac{(2\tau - n)z^2}{sn}} u^{-r} \prod_{m \geq 1} (1 - q^{nm-r} u^n) \prod_{m \geq 0} (1 - q^{nm+r} u^{-n}) \prod_{m \geq 1} (1 - q^m)^{-2n}$$
where the factor \( C := e^{\frac{n(1)}{2}(n^2 - (n-1)^2)}q^\frac{n}{2}u^{n/2} \) is independent of \( r \).

**Proof.** A simple computation, using the definition of the \( x_r \) and the Legendre relation. \( \square \)

Rescaling the functions \( x_0, \ldots, x_{n-1} \) by a nowhere vanishing holomorphic function of \( q \) does not change the corresponding embedding \( \mathbb{C}/\Lambda_r \to \mathbb{P}^{n-1} \). Thus for each \( r \) we multiply the above expression for \( x_r \) by \( \frac{1}{\tau} \prod_{m \geq 1} (1 - q^{nm})^2 \prod_{m \geq 1} (1 - q^{nm}) \), and define

\[
x_r(z, \tau) := (-1)^r q^{\frac{(2r-n)^2}{8n}} u^{-r} \prod_{m \geq 1} (1 - q^{nm-r} u^n) \prod_{m \geq 0} (1 - q^{nm+r} u^{-n}) \prod_{m \geq 1} (1 - q^{nm}).
\]

We furthermore define the functions \( \alpha_0(\tau), \ldots, \alpha_{n-1}(\tau) \) by

\[
\alpha_r(\tau) := x_r(0, \tau) = (-1)^r q^{\frac{(2r-n)^2}{8n}} \prod_{m \geq 1} (1 - q^{nm-r}) \prod_{m \geq 0} (1 - q^{nm+r}) \prod_{m \geq 1} (1 - q^{nm}).
\]

By Proposition 5.1.2, \( \alpha_0(\tau) = 0 \), and \( \alpha_r(\tau) = -\alpha_{n-r}(\tau) \). For \( k > 0 \), using the fact that \( \sigma(z, \tau) \) vanishes only at the points \( z \in \Lambda_r \), it is easy to see that \( \alpha_k(\tau) \) is a nowhere vanishing function of \( \tau \).

Functions \( \alpha_0, \ldots, \alpha_{n-1} \) satisfy a functional equation. This result is probably classical, but we could not find a reference in the literature. We have learned about this proof from Tom Fisher.

**Proposition 5.1.6.** For \( 0 \leq r \leq n - 1 \) we have:

\[
\alpha_r(\tau + 1) = \zeta^{\frac{(2r-n)^2}{8n}} \alpha_r(\tau),
\]

where we take \( \zeta = e^{2iz/8} \), and

\[
\alpha_r(-1/\tau) = (-1)^{(n-1)/2} \sqrt{\frac{i\tau}{n}} \sum_{s=0}^{n-1} \zeta^{rs} \alpha_s(\tau).
\]

**Proof.** The first equation is an immediate consequence of the product expansion of \( \alpha_r \). To prove the second equation, we make use of the theta function \( \Theta_1 \):

\[
\Theta_1(z, \tau) = -i \sum_{m \in \mathbb{Z}} e^{(2m+1)iz} q^{(2m+1)/2} / 8 = 2q^{1/8} \sin z \prod_{m \geq 1} (1 - q^m)(1 - e^{2iz} q^m)(1 - e^{-2iz} q^m),
\]

where the equality of two expressions follows from the Jacobi triple product identity. Comparing the infinite products for \( x_r \) and \( \Theta_1 \), we rewrite \( \alpha_r \) in terms of \( \Theta_1 \):

\[
\alpha_r(\tau) = iq^{r^2/2n} \Theta_1(\pi r \tau, n \tau)
\]

The theta function satisfies the functional equation (page 476, [WW20]):

\[
\sqrt{\frac{\tau}{i}} \Theta_1(z, \tau) = -e^{\frac{-z^2}{4}} \Theta_1(-\frac{z^2}{r^2}, \frac{1}{\tau}).
\]
Substituting \( z = \pi r \tau \) and \( \tau := n \tau \), we obtain

\[
\sqrt{\frac{n \tau}{i}} \Theta_1(\pi r \tau, \tau) = i q^{-r^2/(2n)} \Theta_1(\pi r/n, -1/(n \tau)).
\]

Thus we have

\[
\alpha_r(\tau) = (-1)^r \sqrt{\frac{i}{n \tau}} \Theta_1(\pi r/n, -1/(n \tau)).
\]

Replacing \( \tau \) by \(-1/\tau\) we find

\[
\alpha_r(-1/\tau) = -(-1)^r \sqrt{\frac{\tau}{in}} \Theta_1(\pi r/n, -\tau/n)
= (-1)^r \sqrt{\frac{\tau}{in}} \Theta_1(\pi r/n, \tau/n).
\]

We then find, using the power series for \( \Theta_1 \),

\[
\Theta_1(\pi r/n, \tau/n) = -i \sum_{m \in \mathbb{Z}} (-1)^m e^{(2m+1)i\pi r/n} q^{(2m+1)^2/8n}
= (-1)^{(n-1)/2} i \sum_{m \in \mathbb{Z}} (-1)^m e^{(2m-n)i\pi r/n} q^{(2m-n)^2/8n}
= (-1)^{(n-1)/2} \sum_{m \in \mathbb{Z}} (-1)^m \zeta^m q^{(2m-n)^2/8n}
= (-1)^{(n-1)/2} (-1)^r \sum_{s=1}^{n} \zeta^{rs} \alpha_s(\tau).
\]

and the functional equation now follows immediately. Note that the second equality was obtained by replacing \( m \) with \( m - (n-1)/2 \).

If \( n \geq 3 \), the point \( 0 : \alpha_1 : \ldots : \alpha_{n-1} \), the image of \( 0 \in \mathbb{C}/\Lambda_{\tau} \), determines the diagram \( B_\tau \) uniquely, in the following sense.

**Lemma 5.1.7.** (i) Let \( H_1 = [C_1 \subset \mathbb{P}^{n-1}] \) and \( H_2 = [C_2 \subset \mathbb{P}^{n-1}] \) be \( n \)-diagrams. Suppose \( n > 3 \). If \( |C_1 \cap C_2| > 2n \), then \( C_1 = C_2 \). The same conclusion holds if \( n = 3 \) and \( |C_1 \cap C_2| > 9 \).

(ii) Consider the matrices \( S = ((-1)^{(n-1)/2} \sqrt{\frac{1}{n}} \zeta^{ij} )_{i,j=0}^{n-1} \) and \( T = (\delta_{ij} \zeta^{(2i-n)^2/8})_{i,j=0}^{n-1} \). We have \( S \cdot B_\tau = B_{-1/\tau} \) and \( T \cdot B_\tau = B_{r+1} \).

**Proof.** (i) For \( n > 3 \), both \( C_1 \) and \( C_2 \) are defined by quadrics. Let \( f \) be a quadric vanishing on \( C_1 \), then \( f \) vanishes on \( C_1 \cap C_2 \), and hence the zero set of \( f \) meets \( C_2 \) in more than \( 2n \) points. By Bezout’s theorem, it follows that \( f \) vanishes on \( C_2 \), and hence \( C_2 \subset C_1 \). By the same argument, \( C_1 \subset C_2 \), and hence \( C_1 = C_2 \). A similar argument applies in the case \( n = 3 \).

(ii) By Proposition 5.1.6, if we regard \( S \) and \( T \) as elements of \( \text{PGL}_n \),

\[
S \cdot (0 : \alpha_1(\tau) : \ldots : \alpha_{n-1}(\tau)) = (0 : \alpha_1(-1/\tau) : \ldots : \alpha_{n-1}(-1/\tau)),
\]

then by (i) the point \( 0 : \alpha_1(\tau) : \ldots : \alpha_{n-1}(\tau) \) lies on \( C_1 \). Similarly \( C_2 \) meets \( \text{PGL}_n \) on the same \( \alpha_i(\tau) \).

Furthermore, we have

\[
S \cdot (0 : \alpha_1(-1/\tau) : \ldots : \alpha_{n-1}(-1/\tau)) = (0 : \alpha_1(\tau) : \ldots : \alpha_{n-1}(\tau)),
\]

so \( C_2 \) meets \( \text{PGL}_n \) on the same \( \alpha_i(\tau) \).
\[
T \cdot (0 : \alpha_1(\tau) : \ldots : \alpha_{n-1}(\tau)) = (0 : \alpha_1(\tau + 1) : \ldots : \alpha_{n-1}(\tau + 1))
\]

Let \( F_{\tau} \subseteq \mathbb{P}^{n-1} \) be the image of the set of \( n \)-torsion points of \( \mathbb{C}/\Lambda_{\tau} \). We first show that \( B_{-1/\tau} = \{ S \cdot f \mid f \in F_{\tau} \} \) and \( B_{\tau+1} = \{ T \cdot f \mid f \in F_{\tau} \} \). By Remark 5.1.4, we see that \( F_{\tau} = \{ h \cdot (0 : \alpha_1(\tau) : \ldots : \alpha_{n-1}(\tau)) \mid h \in H_n \} \), and thus
\[
\{ S \cdot f \mid f \in F_{\tau} \} = \{ S \cdot h \cdot (0 : \alpha_1(\tau) : \ldots : \alpha_{n-1}(\tau)) \}
\]
\[
= \{ ShS^{-1} \cdot (0 : \alpha_1(-1/\tau) : \ldots : \alpha_{n-1}(-1/\tau)) \}
\]
It is simple to check, using the description of \( H_n \) in terms of generators \( \sigma_{\omega_1/n} \) and \( \sigma_{\omega_2/n} \), that \( S \cdot H_n \cdot S^{-1} = H_n \), and hence the above set is equal to \( F_{-1/\tau} \). The same argument applies for \( T \) as well. Now note that \( |B_{\tau}| = n^2 \), and that \( F_{-1/\tau} \subseteq S \cdot C_{\tau} \cap C_{-1/\tau} \), \( F_{\tau+1} \subseteq T \cdot C_{\tau} \cap C_{\tau+1} \). For \( n > 3 \), we are done by (i).

For the case \( n = 3 \), the image of 0 is the point \((0 : 1 : -1)\), independent of \( \tau \), so we have to use a different method. One can generalize the functional equation proved in Proposition 5.1.6 to a functional equation for the functions \( x_{\tau}(z, \tau) \), of the form
\[
x_{\tau}(z, \tau + 1) = k_S(z, \tau) \cdot \zeta^{(2r-n)^2} x_{\tau}(z, \tau),
\]
\[
x_{\tau}(z, -1/\tau) = k_T(z, \tau)(-1)^{(n-1)/2} \sqrt{\frac{2\tau}{n}} \sum_{s=0}^{n-1} \zeta^{rs} x_s(z\tau, \tau).
\]
where \( k_S \) and \( k_T \) are nowhere vanishing functions of \( z \), independent of \( r \), with \( k_S(0, \tau) = 1 \). The proof is the same as before, with some added bookkeeping. These equations then imply (ii) directly, for all \( n \).

\[\square\]

### 5.2 Analytic description of the \( \Omega \)-matrix, and proof of the formula for the Jacobian

In this section we prove Theorem 3.3.5. The first step is to prove an analytic version of the theorem. Recall that, by Lemma 4.6.4 the differential on a genus one curve \( C \) associated to an \( \Omega \)-matrix is regular, and that regular differentials on a complex torus \( \mathbb{C}/\Lambda \) are scalar multiples of \( dz \).

**Theorem 5.2.1.** For any \( \tau \in \mathcal{H} \), let \( B_{\tau} = [\mathbb{C}/\Lambda_{\tau} \xrightarrow{\phi} \mathbb{P}^{n-1}] \) denote the \( n \)-diagram constructed in the previous section. Let \( \Omega_{\tau} \) be the \( \Omega \)-matrix associated to this diagram, scaled so that if \( \omega \) is the differential determined by \( \Omega_{\tau} \), we have \( \phi^*\omega = dz \). Let \( c_4(\Omega_{\tau}), c_6(\Omega_{\tau}) \) be the invariants of \( \Omega_{\tau} \) defined in Section 3.3 and let \( E_4(\tau) \) and \( E_6(\tau) \) be the Eisenstein series. We then have
\[
c_4(\Omega_{\tau}) = (2\pi)^4 E_4(\tau),
\]
and
\[
c_6(\Omega_{\tau}) = (2\pi)^6 E_6(\tau).
\]
We start by proving that \( c_k(\Omega_\tau) \) satisfy the functional equation.

**Lemma 5.2.2.** The functions \( c_4(\Omega_\tau) \) and \( c_6(\Omega_\tau) \) are weakly modular of weight 4 and 6, i.e. for \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \), we have

\[
c_k(\Omega_{g\tau + \tau'}) = (ct + d)^k c_k(\Omega_\tau).
\]

**Proof.** Write \( \tau' = \frac{\sigma\tau + \tau}{ct + d} \). Over an algebraically closed field, any two \( n \)-diagrams with the same Jacobian curve are isomorphic, and hence there exists a commutative diagram

\[
\begin{array}{ccc}
\mathbb{C}/\Lambda_\tau & \xrightarrow{\phi_\tau} & \mathbb{P}^{n-1} \\
\psi \downarrow & & \downarrow \rho \\
\mathbb{C}/\Lambda_{\tau'} & \xrightarrow{\phi_{\tau'}} & \mathbb{P}^{n-1}
\end{array}
\]

The left vertical arrow is \( \psi : z \mapsto \frac{z}{c\tau + d} \), and the right vertical arrow is an automorphism \( \rho \) of \( \mathbb{P}^{n-1} \). Let \( \Omega' \) be an \( \Omega \)-matrix for \( \phi_{\tau'} \), scaled so that for the associated differential \( \omega' \) we have \( \phi_{\tau'}^*\omega' = (ct + d)dz \). We claim that \( \rho^*(\omega') = \omega \).

Indeed, note that as \( \psi^*((ct + d)dz) = dz \), we have \( (\phi_{\tau'} \circ \psi)^*(\omega') = dz \). As the above diagram commutes, \( dz = (\phi_{\tau'} \circ \psi)^*(\omega') = (\phi_{\tau} \circ \rho)^*(\omega') \), i.e. \( \rho^*(\omega') = \omega \).

We may assume that \( \rho \) is represented by a matrix \( N \in \text{GL}_n(\mathbb{C}) \). Now it follows, from our scaling of \( \Omega' \), Proposition 3.2.3 and Lemma 3.4.8, that we have \( \Omega_\tau = N \star \Omega' \). Hence, by Lemma 3.3.3, we have \( c_k(\Omega_\tau) = c_k(\Omega') \).

By the definition of \( \Omega' \), we have \( (ct + d)\Omega' = \Omega_{\tau'} \). As \( c_4(\Omega) \) and \( c_6(\Omega) \) are homogeneous polynomials of degree 4 and 6 in the coefficients of \( \Omega \), we find that \( c_k(\Omega_{\tau + \tau'}) = (ct + d)^k c_k(\Omega_\tau) \), as desired. \( \square \)

Now it remains to prove that \( c_k(\Omega_\tau) \) is holomorphic at the cusp, which forces it to be a scalar multiple of \( E_k \), and then to check that this scalar is 1. To do this we will need an explicit description of \( \Omega_\tau \). Recall that \( \Omega_\tau \) is an alternating matrix of homogeneous quadric forms.

Throughout the chapter, to avoid confusion with the functions \( x_i(z, \tau) \), we label the standard coordinates on \( \mathbb{P}^{n-1} \) by \( X_0, \ldots, X_{n-1} \).

**Proposition 5.2.3.** There exist functions \( u_i : \mathcal{H} \to \mathbb{C} \), for \( 0 \leq i \leq n - 1 \), such that for \( 0 \leq k, l \leq n - 1 \), we have

\[
(\Omega_\tau)_{k,l} = u_{l-k}(\tau)X_kX_{l-k} - \frac{\partial^2}{\partial \tau^2}(0, \tau) \sum_{1 \leq i \leq n-1, i \neq k-l} \frac{\alpha_{l-k}(\tau)}{\alpha_i(\tau)\alpha_i+l-k(\tau)}X_{i+k}X_{i+l-k},
\]

where the subscripts are read mod \( n \).

We divide the proof into a sequence of lemmas.

**Lemma 5.2.4.** For \( 0 \leq k, l \leq n - 1 \), we have

(i) \( (\Omega_\tau)_{k,l}(X_0, \zeta X_1, \ldots, \zeta^{n-1}X_{n-1}) = \zeta^{k+l}(\Omega_\tau)_{k,l}(X_0, X_1, \ldots, X_{n-1}) \)
(ii) \((\Omega_\tau)_{k,l}(X_1, X_2, \ldots, X_{n-1}, X_0) = (\Omega_\tau)_{k+1,l+1}(X_0, X_1, \ldots, X_{n-1})\)

Proof. The automorphisms of \(\mathbb{P}^{n-1}\) defined in Remark 5.1.4, \(\sigma_{1/n}\) and \(\sigma_{\tau/n}\), take the curve \(C_\tau\) to itself. Since \(\det(\sigma_{1/n}) = \det(\sigma_{\tau/n}) = 1\), by Lemma 3.4.8, \(\sigma_{1/n} \ast \Omega_\tau\) and \(\sigma_{\tau/n} \ast \Omega_\tau\) all have the same associated differential on \(C_\tau\). Thus we must have \(\Omega_\tau = \sigma_{1/n} \ast \Omega_\tau\) and \(\Omega_\tau = \sigma_{\tau/n} \ast \Omega_\tau\), and the lemma follows. \(\square\)

To compute \(g\)-expansions of the coefficients of \(\Omega_\tau\), we intersect the curve \(C_\tau\) with the hyperplane \(X_0 = 0\). The computation we did in Section 4.5 allows us to compute the \(\Omega\)-quadrics of the resulting set of \(n\) points.

**Lemma 5.2.5.** The intersection of the curve \(C_\tau\) and the hyperplane \(X_0 = 0\) is the set
\[
Z_\tau := \{(0 : \zeta^i\alpha_1(\tau) : \cdots : \zeta^{i(n-1)}\alpha_{n-1}) : i \in \{0, 1, \ldots, n-1\}\}
\]

Proof. First note that, for \(0 \leq i \leq n-1\),
\[
x_\tau(i/n, \tau) = (-1)^r q^\left(2r-n-2\right) \zeta^{-i} \prod_{m \geq 1} (1 - q^{nm-r}\zeta^n) \prod_{m \geq 0} (1 - q^{nm+r}\zeta^{-n}) \prod_{m \geq 1} (1 - q^{nm}) = \zeta^{-i}\alpha_r(\tau)
\]
and hence \(\phi_\tau(i/n) = (0 : \zeta^{-i}\alpha_1(\tau) : \cdots : \zeta^{-(i-1)}\alpha_{n-1}) \in C_\tau \cap \{X_0 = 0\}\). As \(C_\tau\) is a curve of degree \(n\), \(C_\tau \cap \{X_0 = 0\}\) consists of \(n\) points, hence the conclusion. \(\square\)

**Lemma 5.2.6.** Let \(F^0_\ast\) be a resolution model of the set \(Z_\tau \subset \mathbb{P}^{n-2}\), and let \(\{\Omega_1, \ldots, \Omega_{n-1}\}\) be the set of \(\Omega\)-quadrics associated to \(F^0_\ast\). For \(1 \leq k \leq n-1\), we have
\[
\Omega(X_1, X_2, \ldots, X_{n-1}) = (\Omega_\tau)_{0,k}(0, X_1, X_2, \ldots, X_{n-1})
\]
and furthermore, we have
\[
(\Omega_\tau)_{0,k}(0, X_1, \ldots, X_{n-1}) = \lambda \cdot \sum_{1 \leq i \leq n-1, i \neq n-k} \frac{\alpha_k(\tau)}{\alpha_i(\tau)\alpha_{k-i}(\tau)} X_i X_{k-i}
\]
where \(\lambda = -\frac{\partial x_0(0, \tau)}{n-2}\).

Proof. The first part of the lemma follows from Lemma 3.7.1(ii). The existence of the constant \(\lambda\) follows from Lemma 4.5.3, where we computed the \(\Omega\)-quadrics for the set \(Z_\tau\). To compute \(\lambda\) exactly, we need to take the scaling of the matrix \(\Omega_\tau\) into account.

Recall that the differential \(\omega\) associated to \(\Omega_\tau\) satisfies, for \(1 \leq k \leq n-1\),
\[
\omega = \frac{X_0^2 d(X_k/X_0)}{(\Omega_\tau)_{0,k}}
\]
and thus
\[
dz = \phi^* \omega = \frac{x_0(z, \tau) \frac{\partial x_k}{\partial z}(z, \tau) - x_k(z, \tau) \frac{\partial x_0}{\partial z}(z, \tau)}{(\Omega_\tau)_{0,k}(x_0(z, \tau), \ldots, x_{n-1}(z, \tau))} \cdot dz.
\]
We thus conclude that the expression in front of $dz$ is identically equal to 1. Setting $z = 0$, and noting that $x_i(0, \tau) = \alpha_i(\tau)$, as well as $x_0(0, \tau) = 0$, we find

$$x_0(0, \tau) \frac{\partial x_k}{\partial z}(z, \tau) - x_k(z, \tau) \frac{\partial x_0}{\partial z}(0, \tau) = -\alpha_k(\tau) \frac{\partial x_0}{\partial z}(0, \tau),$$

and

$$(\Omega)_{0,k}(x_0(0, \tau), \ldots, x_{n-1}(0, \tau)) = (\Omega)_{0,k}(0, \alpha_1(\tau) \ldots, \alpha_{n-1}(\tau))$$

$$= \lambda \cdot \sum_{1 \leq i \leq n-1, i \neq k} \frac{\alpha_k(\tau)}{\alpha_i(\tau)} \alpha_k(\tau)\alpha_{k-i}(\tau)
= \lambda(n - 2)\alpha_k(\tau).$$

From the definition of $\alpha_k(\tau)$, we see that for $k > 0$ it is nowhere vanishing, so we can cancel it and find $\lambda = -\frac{\partial x_0(0, \tau)}{n-2}$.

We can now finish the proof of Proposition 5.2.3. By Lemma 5.2.4(ii), it suffices to prove the identity for the entries $(\Omega)_{0,k}$ and by Lemma 5.2.4(i), the monomials occurring in $(\Omega)_{0,k}$ are $X_iX_{k-i}$, as $i$ ranges over $\mathbb{Z}/N\mathbb{Z}$. Lemma 5.2.6 determines the coefficients of all of these monomials, except for the coefficient in front of $X_0X_k$, which we define to be $u_k(\tau)$, concluding the proof.

To prove Theorem 2.1, we will need to compute the beginning of the $q$-expansion of the coefficients of $(\Omega)_{k,l}$.

**Lemma 5.2.7.** Coefficients of $(\Omega)_{0,k}$ are holomorphic functions of $q^{1/(8n)}$. In other words, they can be expressed as power series in the variable $q^{1/(8n)}$. Furthermore the only coefficient of $(\Omega)_{0,k}$ with a non-zero constant term is $u_k$, with the constant term equal to $-2\pi i^{n-2}k$.

**Proof.** By Proposition 5.2.3, for $1 \leq i \leq n - 1$, $i \neq k$, the coefficient of $X_iX_{k-i}$ is

$$-\frac{\partial x_0(0, \tau)}{n-2} \frac{\alpha_k(\tau)}{\alpha_i(\tau)\alpha_{k-i}(\tau)}.$$

Differentiating and applying the product rule to the infinite product

$$x_r(z, \tau) = (-1)^r q^{(2r-n)^2} u^{-r} \prod_{m \geq 1} (1 - q^{nm-r}u^n) \prod_{m \geq 0} (1 - q^{nm+r}u^{-n}) \prod_{m \geq 1} (1 - q^{nm}),$$

we obtain

$$\frac{\partial x_r}{\partial z}(z, \tau) = 2\pi i x_r \left( -r + n \sum_{m \geq 0} q^{nm+r}u^{-n} - n \sum_{m \geq 1} \frac{q^{nm-r}u^n}{1 - q^{nm-r}u^n} \right),$$

and so in particular

$$\frac{\partial x_0}{\partial z}(u, \tau) = 2\pi i x_0 \left( -n \sum_{m \geq 1} \frac{q^{nm}u^{-n}}{1 - q^{nm}u^{-n}} - n \sum_{m \geq 1} \frac{q^{nm}u^n}{1 - q^{nm}u^n} \right) + \frac{2\pi nx_0}{1 - u^{-n}}.$$
Since \(x_0(0, \tau) = 0\), the first summand vanishes at \(u = 0\). For the second one, we have
\[
\frac{2\pi n x_0}{1 - u^{-\alpha}} = 2\pi n \cdot q^{\frac{x_0}{n}} \prod_{m \geq 1} (1 - q^{2m} u^n)(1 - q^{2m} u^{-\alpha})(1 - q^{2m}),
\]
and hence we find
\[
\frac{\partial x_0}{\partial z}(0, \tau) = 2\pi n \cdot q^{\frac{x_0}{n}} \prod_{m \geq 1} (1 - q^{2m})^3.
\]
From these formulas it is clear that the coefficient of \(X_kX_{k-i}\) is a meromorphic function of \(q^{1/(8n)}\). We compute, reminding the reader that subscripts are read mod \(n\), that the valuation of the coefficient is equal to
\[
\frac{(2k - n)^2 + n^2 - (2i - n)^2 - (n - 2i + 2k)^2}{8n} = \frac{(2i - 2k)(4n - 4i)}{8n} > 0,
\]
in the case that \(i > k\), and equal to
\[
\frac{(2k - n)^2 + n^2 - (2i - n)^2 - (2k - 2i - n))^2}{8n} = \frac{(2k - 2i)4i}{8n} > 0
\]
otherwise. Hence these coefficients are holomorphic functions of \(q^{1/(8n)}\), with zero constant term.

We now deal with the coefficient \(u_k\). The equation (5.1) can be restated as
\[
x_0 \frac{\partial x_k}{\partial z} - x_k \frac{\partial x_0}{\partial z} = u_k(\tau)x_0x_k - \frac{\partial x_0}{\partial z}(0, \tau) \sum_{1 \leq i \leq n-1, i \neq n-k} \frac{\alpha_k(\tau)}{\alpha_i(\tau)\alpha_{k-i}(\tau)} x_ix_{k-i},
\]
or
\[
u_k(\tau)x_0x_k = x_0 \frac{\partial x_k}{\partial z} - x_k \frac{\partial x_0}{\partial z} + \frac{\partial x_0}{\partial z}(0, \tau) \sum_{1 \leq i \leq n-1, i \neq n-k} \frac{\alpha_k(\tau)}{\alpha_i(\tau)\alpha_{k-i}(\tau)} x_ix_{k-i}
\]
Using this formula, it is easy to see that \(u_k(\tau+n) = u_k(\tau)\), and that hence \(u_k\) can be expressed as a Laurent series in \(q^{1/n}\). Regard both sides of the above equation as power series in \(q^{1/(8n)}\) with coefficients power series in \(u\). The smallest power of \(q\) appearing in \(x_0x_k\) is \(q^{(2k-n)^2+n^2)/(8n)}\), with the coefficient equal to
\[
(-1)^k(1 - u^{-\alpha})u^{-k}.
\]
On the other hand, using the formula (5.2), we can compute that the smallest power of \(q\) appearing on the right is \(q^{(2k-n)^2+n^2)/(8n)}\), with the coefficient equal to
\[
(-1)^{k+1}2\pi i(nu^{-k} - n)(1 - u^{-\alpha})u^{-k} - \frac{n}{n - 2}((k - 1)u^{-k} + (n - 1 - k)u^{-k-n})).
\]
\[
= (-1)^{k+1}2\pi i\frac{n - 2k}{n - 2}(1 - u^{-\alpha})u^{-k}
\]
We conclude that there are no negative powers of \(q\) appearing in the \(q\)-expansion of \(u_k\), and comparing the above expressions we find that the constant coefficient is equal to \(-2\pi i\frac{n - 2k}{n - 2}\), concluding the proof of the lemma.

**Remark 5.2.8.** In fact, it will follow from our proof of Lemma 5.3.3 that the coefficients of \(\Omega_\tau\) are actually power series in \(q^{1/n}\), but we won’t need this for now.
To finish the proof of Theorem 5.2.1 we need Lemma 8.4 of [Fis18]:

**Lemma 5.2.9.** The alternating matrix of quadratic forms

\[
\Omega^{\text{const}} = \begin{pmatrix}
0 & (n-2)X_0X_1 & (n-4)X_0X_2 & (n-6)X_0X_3 & \ldots & (2-n)X_0X_{n-1} \\
0 & (n-2)X_1X_2 & (n-4)X_1X_3 & \ldots & (4-n)X_1X_{n-1} \\
& \vdots & \ddots \ & \vdots \ & \vdots \ & \vdots \\
0 & (n-2)X_{n-2}X_{n-1} & \ldots & (n-2)X_{n-2}X_{n-1} & \ldots & (n-2)X_{n-2}X_{n-1} \\
& & & & & 0
\end{pmatrix}
\]

has invariants \( c_4(\Omega^{\text{const}}) = (n-2)^4 \) and \( c_6(\Omega^{\text{const}}) = -(n-2)^6 \).

The proof is a computation, and can be found on pages 20 and 21 of [Fis18].

**Proof of Theorem 5.2.1.** By Lemma 5.2.2, \( c_n(\Omega_\tau) \) are invariant under \( \tau \mapsto \tau + 1 \), and so are holomorphic functions of \( q \). By Lemma 5.2.2 again, they are modular forms of weight \( k \). The space of modular forms of weight \( k \) for \( \text{SL}_2(\mathbb{Z}) \) is 1-dimensional, and spanned by the Eisenstein series \( E_k \) for \( k = 4 \) and \( k = 6 \).

Write \( \Omega_\tau = \frac{-2\pi i}{n-2} \Omega^{\text{const}} + \Omega' \), where the coefficients of the entries of \( \Omega' \) have no constant term, viewed as power series of \( q^{1/(8n)} \). As \( c_k(\Omega) \) are homogenous of degree \( k \), we have

\[ c_k(\Omega_\tau) = (2\pi)^k (1 + o(q)) \]

and therefore we conclude \( c_k(\Omega_\tau) = (2\pi)^k E_k(\tau) \). \( \square \)

Theorem 5.2.1 is related to the formula for the Jacobian given in Theorem 3.3.5 via the following standard result on uniformization of elliptic curves. As stated, this is Lemma 3.5 of [Fis12].

**Lemma 5.2.10.** Let \( E \) be an elliptic curve over \( \mathbb{C} \) with Weierstrass equation \( W \)

\[ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \]

Let \( \Lambda \) be the period lattice obtained by integrating the differential \( dx/(2y + a_1x + a_3) \). Then the map

\[ \rho : E(\mathbb{C}) \to \mathbb{C}/\Lambda : (x, y) \mapsto \int_{\gamma} \frac{dx}{2y + a_1x + a_3} \]

where \( \gamma \) is an arbitrary path from \( 0 \in E \) to \( (x, y) \), is a \( \mathbb{C} \)-analytic isomorphism, with \( \rho^*(dz) = \frac{dx}{2y + a_1x + a_3} \). Furthermore, choose a basis \( \omega_1, \omega_2 \) for \( \Lambda \) so that \( \tau = \omega_2/\omega_1 \in \mathcal{H} \). Then the invariants \( c_4 \) and \( c_6 \) of the Weierstrass equation \( W \) are given by \( c_k = (2\pi \omega_1)^k E_k(\tau) \).

**Proof of Theorem 3.3.5.** Note that it suffices to prove the theorem with the ground field replaced by \( \mathbb{C} \). Thus let \( [C \to \mathbb{P}^{n-1}] \) be an \( n \)-diagram defined over \( \mathbb{C} \), let \( \Omega \) be an \( \Omega \)-matrix for \( [C \to \mathbb{P}^{n-1}] \), with the associated invariant differential \( \omega \). We identify \( C \) with its Jacobian \( E \). Fix a Weierstrass equation for \( E \) such that \( \omega \) is identified with \( dx/(2y + a_1x + a_3) \).
Let $\Lambda = \mathbb{Z} \omega_1 \oplus \mathbb{Z} \omega_2$ be as in the above lemma, and let $\Lambda_\tau = \frac{1}{\omega_1} \Lambda$. Let $\psi : \mathbb{C}/\Lambda_\tau \rightarrow \mathbb{C}/\Lambda$ be the isomorphism $z \mapsto \omega_1 z$. By composing with $\rho^{-1} \circ \psi$, we obtain an $n$-diagram $[C/\Lambda_\tau \rightarrow \mathbb{P}^{n-1}]$, with $\phi^* \omega = \omega_1 dz$. As $\mathbb{C}$ is algebraically closed, this diagram is isomorphic to the Heisenberg invariant diagram, and thus by Theorem 5.2.1 and the above lemma, we conclude $c_k(\Omega) = (\frac{2\pi}{\omega_1})^k E_k(\tau) = c_k$, as required.

5.3 Analytic theory over the real numbers

We now collect some standard results about elliptic curves over $\mathbb{R}$ that we will need in Chapter 6.

**Proposition 5.3.1.** Let $E/\mathbb{R}$ be an elliptic curve, defined by a Weierstrass equation $W$. Let $\Lambda$ be the period lattice obtained by integrating $\omega = dx/(2y + a_1 x + a_3)$. Then

(i) There exists a basis $\omega_1, \omega_2$ of $\Lambda$ with $\tau = \omega_2/\omega_1 \in H$ and $\text{Re}(\tau) \in \{0, 1/2\}$. If the discriminant of $E$ is positive, then $\text{Re}(\tau) = 0$, otherwise $\text{Re}(\tau) = 1/2$.

(ii) For such a $\tau$, we have $q = e^{2i\pi \tau} \in \mathbb{R}$, with $|q| < 1$. Furthermore, the uniformization $\mathbb{C}$-analytic isomorphism $\mathbb{C}/\Lambda_\tau \cong \mathbb{C}^*/q^2 \rightarrow E(\mathbb{C})$ commutes with complex conjugation, and hence restricts to an $\mathbb{R}$-analytic isomorphism $\mathbb{R}^*/q^2 \rightarrow E(\mathbb{R})$.

This is a standard fact, e.g. see Proposition VI.2.3 of [Sil94]. As a consequence, note that as $q \in \mathbb{R}$, and the functions $x_i(z, q)$ were given in terms of $q$-expansions, it is easy to show that the Heisenberg invariant embedding $\mathbb{C}/\Lambda_\tau \rightarrow \mathbb{P}^{n-1}$ is commutes with complex conjugation and is hence defined over $\mathbb{R}$.

**Lemma 5.3.2.** Let $E/\mathbb{R}$ be an elliptic curve, and let $n$ be an odd integer. Then the Galois cohomology group $H^1(\mathbb{R}, E[n])$ is trivial.

**Proof.** As $|\text{Gal}(\mathbb{C}/\mathbb{R})| = 2$ is coprime to $|E[n]| = n^2$, this is standard, a consequence of the fact that for any finite group $G$ and a $G$-module $A$, the group $H^1(G, A)$ is annihilated by multiplication by $|G|$, see Chapter VII, Proposition 6 of [Ser13].

By the lemma, any two $n$-diagrams defined over $\mathbb{R}$ with the same Jacobian curve are isomorphic.

**Lemma 5.3.3.** Every $n$-diagram $[C \rightarrow \mathbb{P}^{n-1}]$, defined over $\mathbb{R}$, is $\text{PGL}_n(\mathbb{R})$-equivalent to a Heisenberg invariant diagram $B_\tau$, for some $\tau \in H$ with $\text{Re}(\tau) \in \{0, n/2\}$. Let $E$ be the Jacobian of $C$. If the discriminant of $E$ is positive, then we have $\text{Re}(\tau) = 0$, and if it is negative, $\text{Re}(\tau) = n/2$.

**Proof.** By Lemma 5.3.1, we can identify $E$ with a torus $\mathbb{C}^*/q^2$, where $q = e^{2i\pi \tau}$ and $\text{Re}(\tau) \in \{0, 1/2\}$. We are free to translate $\tau$ by any integer in $\mathbb{Z}$, and so as $n$ is odd, if $\text{Re}(\tau) = 1/2$, we replace $\tau$ by $\tau + (n - 1)/2$. Hence we may assume that $\text{Re}(\tau) \in \{0, n/2\}$. By Lemma 5.3.2, it suffices to show that the diagram $B_\tau$ is defined over $\mathbb{R}$.
Recall the series that for the functions \( x_r(z, q) \) that define the embedding \( B_\tau \)

\[
x_r(z, q) = (-1)^r q^{\frac{(2r-n)^2}{8n}} u^{-r} \prod_{m \geq 1} (1 - q^{nm-r} u^n) \prod_{m \geq 0} (1 - q^{nm+r} u^{-n}) \prod_{m \geq 1} (1 - q^m)^{-2n}.
\]

Note that \( q^{1/n} = e^{2\pi \tau/n} \in \mathbb{R} \) precisely when \( \text{Re}(\tau) \in \{0, n/2\} \). For such \( \tau \), all powers of \( q \) in the above expression are real, except for the factor \( q^{(2r-n)^2/8n} = q^{n/8} \cdot q^{(r^2-2rn)/(2n)} \). As \( n \) is odd, \( 2|r^2 - rn \) for all \( r \), and hence \( q^{(r^2-2rn)/(2n)} \in \mathbb{R} \) for all \( r \). The non-real factor \( q^{n/8} \) is independent of \( r \). Thus the map \( u \mapsto (x_0(u, q) : \ldots : x_{n-1}(u, q)) \) is compatible with complex conjugation, and hence the diagram \( B_\tau = [\mathbb{C}^*/q^\mathbb{Z} \to \mathbb{P}^{n-1}] \) is defined over \( \mathbb{R} \).
Chapter 6

Bounding the capitulation discriminant

We have now developed the necessary tools to prove Theorem 1.0.1 and Theorem 1.0.2, and we give the proofs in Section 6.1. Rest of the chapter is devoted to making the inequalities of these theorems effective, with our main result in this direction being Theorem 6.4.1.

6.1 Proof of the main theorem

Let \( n \geq 3 \) be an odd integer and let \( E/\mathbb{R} \) an elliptic curve, with a Weierstrass equation \( W 

\begin{align*}
y^2 + a_1 xy + a_3 y &= x^3 + a_2 x^2 + a_4 x + a_6.
\end{align*}

Let \( \omega = dx/(2y + a_1 x + a_3) \) be the invariant differential associated to the equation \( W \). Let \( \Lambda \subset \mathbb{C} \) be the period lattice obtained by integrating \( \omega \), and let \( \phi : \mathbb{C}/\Lambda \to E \) be the corresponding complex uniformization. Consider the \( n \)-diagram \( B_{\Lambda} = [E \cong \mathbb{C}/\Lambda \to \mathbb{P}^{n-1}] \) defined in Proposition 5.1.3. Let \( \Omega_{\Lambda} \) be the \( \Omega \)-matrix for \( B_{\Lambda} \) scaled so that for the corresponding differential \( \omega_{\Lambda} \) we have \( \phi^* \omega_{\Lambda} = \omega \), and let \( D_{\Lambda} \) be the discriminant form for the diagram \( B_{\Lambda} \) associated to this scaling, as explained in Section 3.7.

The following theorem, together with the minimization theorem and Minkowski’s theorem, will imply Theorem 1.0.1. Set \( H_W = \max(\frac{|c_4|}{4}, \frac{|c_6|}{6}) \).

**Theorem 6.1.1.** Let \( K \) be a compact subset of \( \mathbb{R}^n \). There exists a constant \( c(n, K) \), depending only on \( n \) and \( K \), such that, for all elliptic curves \( E/\mathbb{R} \), with a Weierstrass equation \( W \), we have

\[
\max_{(u_0, \ldots, u_{n-1}) \in K} |D_{\Lambda}(u_0, \ldots, u_{n-1})| \leq c(n, K) H_W^{2n-2}
\]

**Proof.** By the Proposition 5.3.1, we may write \( \Lambda = \omega_1 \cdot (\mathbb{Z} \oplus \mathbb{Z} \tau) \), where Re(\( \tau \)) \( \in \{0, 1/2\} \). By the Lemma 5.2.10, we have \( c_k(W) = (\frac{2\pi}{\omega_1})^k E_k(\tau) \), and hence

\[
H_W^{2n-2} = (\frac{\omega_1}{2\pi})^{2n-2} \max(|E_4(\tau)^{1/4}|, |E_6(\tau)^{1/6}|)^{2n-2} = (\frac{\omega_1}{2\pi})^{2n-2} H(\tau)^{2n-2},
\]

where \( H(\tau) = \max(|E_4(\tau)|^{1/4}, |E_6(\tau)|^{1/6}) \). By comparing the differentials attached to \( \Omega_{\Lambda} \) and \( \Omega_\tau \), we see that \( \Omega_{\Lambda} = \omega_1 \Omega_\tau \). As the coefficients of \( D_{\Lambda} \) are homogenous polynomials of degree \( 2n - 2 \) in the entries of \( \Omega_{\Lambda} \) we see that \( D_{\Lambda}(u_0, \ldots, u_{n-1}) = \omega_1^{2n-2} D_\tau(u_0, \ldots, u_{n-1}) \), where the
coefficients of $D_\tau$ are power series in the variable $q^{1/n}$. Note also that, if we let $B_\tau$ denote the Heisenberg invariant diagram $B_{(1,\tau)}$, the form $D_\tau$ is then the discriminant form associated to $B_\tau$.

We introduce the normalization $D_\tau = \frac{D_\tau(u_0,\ldots,u_{n-1})}{H(\tau)^{2n-2}}$. We seek to prove that the expression

$$\max_{(u_0,\ldots,u_{n-1}) \in K} D_\tau(u_0,\ldots,u_{n-1})$$

is bounded as a function of $\tau$. As $D_\tau$ is a polynomial of degree $2n$ and $K$ is compact, we can find a constant $M$ that is an upper bound on $K$ for each of the finitely many monomials that appear in $D_\tau$.

By Lemma 5.3.3, as $E$ is an elliptic curve defined over $\mathbb{R}$, we may restrict to $\tau$ with $\text{Re}(\tau) \in \{0,n/2\}$. In other words, it suffices to show that the coefficients of $D_\tau$ are bounded, as functions of $\tau$ on the set $A := \{\tau \in \mathcal{H} : \text{Re}(\tau) \in \{0,n/2\}\}$. Let us choose two arbitrary constants $C_1 > C_2 > 0$. Our strategy will be to write $A = A_1 \cup A_2 \cup A_3$, where $A_1 = \{\tau \in A : \text{Im}(\tau) > C_1\}, A_2 = \{\tau \in A : C_2 < \text{Im}(\tau) \leq C_1\}$ and $A_3 = \{\tau \in A : \text{Im}(\tau) \leq C_2\}$, and prove that they are bounded on each set separately.

As $B_\tau$ does not vanish anywhere, since $E_4$ and $E_6$ have no common zeroes, these coefficients are continuous functions of $\tau$, and in fact, examining the $q$-expansions of the coefficients of $\Omega_\tau$ obtained in Lemma 5.2.7 holomorphic functions on the unit disc, in the variable $q^{1/(8n)}$. Thus they must be bounded in any neighbourhood of 0. In term of the variable $\tau$, this means there exists a constant $M_1$ that is an upper bound for the absolute values of these coefficients on the set $A_1 := \{\tau \in A : \text{Im}(\tau) \geq C_1\}$.

Now observe that for any $g \in \text{SL}_2(\mathbb{Z})$, there is an isomorphism of complex tori $\mathbb{C}/\langle 1, \tau \rangle \rightarrow \mathbb{C}/\langle 1, g \cdot \tau \rangle$. Hence the Heisenberg invariant diagrams $B_\tau$ and $B_{g \cdot \tau}$ are isomorphic over $\mathbb{C}$, and in particular, there exists $M_g \in \text{PGL}_n(\mathbb{C})$ such that $[C_{g \cdot \tau} \rightarrow \mathbb{P}^{n-1}] = M_g \cdot [C_\tau \rightarrow \mathbb{P}^{n-1}]$. By Lemma 3.7.4, we have $D_\tau(u_0,\ldots,u_{n-1}) = D_{g \cdot \tau}((u_0,\ldots,u_{n-1}) \cdot M_g^T)$.

Thus, if the coefficients of $D_\tau$ are bounded on some subset of $\mathcal{H}$, they will be bounded, possibly by a different constant, on any $\text{SL}_2(\mathbb{Z})$-translate of that subset. By choosing $g_1, g_2 \in \text{SL}_2(\mathbb{Z})$ that map the cusp at $\infty$ to cusps at 0 and $n/2$ respectively, and noting that $\text{Re}(\tau) \in \{0,n/2\}$, we deduce that the coefficients are bounded on the set $A_3 := \{\tau \in A : \text{Im}(\tau) \leq C_2\}$.

As the set $A_2 := \{\tau \in \mathcal{H} : C_2 \leq \text{Im}(\tau) \leq C_1, \text{Re}(\tau) \in \{0,n/2\}\}$ consists of two closed and bounded intervals, it is compact, and hence there exists a uniform bound for the coefficients on $A_3$, concluding the proof.

As this proof relies on a compactness argument, it does not furnish explicit constants $c(n,K)$. However, it does provide the blueprint for the method we will use to compute them for small values of $n$ and $K$ the unit $n$-ball in $\mathbb{R}^n$.

Recall now the setting of the Theorem 1.0.1. Let $E/Q$ be an elliptic curve, with a minimal Weierstrass equation $W$, and corresponding invariant differential $\omega$. The naive height $H_E$ is defined to be equal to $H_W$. Let $[C \rightarrow \mathbb{P}^{n-1}]$ be an $n$-diagram that represents an element of the $n$-Selmer group $\text{Sel}^{(n)}(E/Q)$. We wish to prove the existence of a constant $c(n)$, that depends only on $n$, such that $C$ admits a point defined over a $\mathbb{Q}$-algebra $A$, of degree $n$, and of
discriminant at most \(c(n)H^2_{E}^{2n-2}\).

**Proof of Theorem 1.0.1.** By Theorem 4.1.1, we may assume that \([C \to \mathbb{P}^{n-1}]\) admits a minimal integral model, i.e., a resolution model \(F_\bullet\) defined over \(\mathbb{Z}\), with the \(c\)-invariants of the corresponding \(\Omega\)-matrix given by \(c_k(\Omega) = c_k(W)\).

Let \(D_C\) be the discriminant form associated to the model \(F_\bullet\). By Lemma 3.7.5, for any \(n\) integers \(u_0, \ldots, u_{n-1}\), not all zero, \(D_C(u_0, \ldots, u_{n-1})\) is the discriminant of an order in the \(n\)-dimensional \(\mathbb{Q}\)-algebra \(\Gamma(C \cap \{u_0x_0 + \ldots + u_{n-1}x_{n-1}\})\).

As explained in Section 5.3, the diagram \([C \to \mathbb{P}^{n-1}]\) and the diagram \(B_\Lambda = [\mathbb{C}/\Lambda \to \mathbb{P}^{n-1}]\) are isomorphic over \(\mathbb{R}\). Hence there exists a \(g \in \text{SL}_n(\mathbb{R})\) with \(g \cdot B_\Lambda = [C \to \mathbb{P}^{n-1}]\). By Theorem 5.2.1, the matrices \(\Omega_\Lambda\) and \(\Omega_C\) have the same invariants, so we must have \(\Omega_C = g \cdot \Omega_\Lambda\). As the discriminant form is contravariant, we have \(D_\Lambda = D_C \circ g^T\), i.e., \(D_C = D_\Lambda \circ g^{-T}\).

Now let \(K\) be the \(n\)-ball centered at \(0 \in \mathbb{R}^n\) of volume \(2^n\). The lattice \(L = g^{-T}(\mathbb{Z}^n)\) has co-volume one, so by Minkowski’s theorem, \(K\) contains a non-zero element \(a\) of \(L\). By Theorem 6.1.1, we have \(|D_C(g^T \cdot a)| = |D_\Lambda(a)| \leq c(n,K)H^{2n-2}_{E}\). As \(g^T \cdot a \in \mathbb{Z}^n\), the value \(D_C(g^T \cdot a)\) is the discriminant of an order in an \(n\)-dimensional \(\mathbb{Q}\)-algebra \(A\), and is hence an upper bound for every field occurring in the decomposition of \(A = K_1 \times K_2 \ldots \times K_p\) as a product of fields, proving the theorem.

As a corollary, we obtain Theorem 1.0.2. Assume that the curve \(C\) has index \(n\), i.e., has no positive divisors of degree less than \(n\), that are defined over \(\mathbb{Q}\). The algebra \(A\) in the above proof is the ring of functions on a hyperplane section \(C \cap H\). This section must consist of \(n\) distinct points, as otherwise, \(C\) would admit a \(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\)-invariant divisor of degree less than \(n\). Hence \(A\) must be étale, and can be decomposed as a product of number fields \(A = K_1 \times K_2 \ldots \times K_p\). Using the assumption on the index again, we conclude that \(A = K\) is a number field, and the theorem follows.

The aim of the next two sections will be to give a method to compute explicit values for the constants \(c(n,B^{n-1})\), where \(B^{n-1}\) is the \(n\)-ball of volume \(2^n\), for small values of \(n\). It seems to be difficult to compute the optimal value for this constant. Our aim was to compute constants at least good enough to imply vanishing of \(\text{III}[n]\) for concrete elliptic curves, as mentioned in the introduction.

As an illustration, consider the case \(n = 3\). We compute the first few terms of \(q\)-expansions of coefficients of \(D_\tau\):

\[
\begin{align*}
D_\tau &= q^{1/3}(-27q - 108q^2 - 378q^3 - 756q^4 + O(q^5))(u_0^6 + u_1^6 + u_2^6) \\
&+ q^{2/3}(18 + 252q + 1170q^2 + 2664q^3 + 6192q^4 + O(q^5))(u_0^3u_1^3u_2 + u_0u_1^4u_2 + u_0u_1u_2^4) \\
&+ q^{1/3}(-4 - 22q - 296q^2 - 756q^3 - 1232q^4 + O(q^5))(u_0^3u_1^3 + u_1^3u_2^3 + u_2^3u_0^3) \\
&+ (1 - 84q - 756q^2 - 2082q^3 - 6132q^4 + O(q^5))u_0^2u_1u_2^2.
\end{align*}
\]

We have \(H(\tau)^4 = \max(|E_4(\tau)|, |E_6(\tau)|)^{2/3}\), and our aim is to produce an explicit constant \(c(n,K)\) with \(\max_{u \in \mathbb{P}^1} |D_\tau(u)/H(\tau)^4| \leq c(n,S^2)\). We do this by bounding the monomial sums, appearing in brackets, and bounding the coefficients of these sums.
6.2 Bounding monomial sums

A first approach to bounding the monomial sums is via calculus, by directly solving for the stationary points.

**Lemma 6.2.1.** Let $F : \mathbb{R}^n \rightarrow \mathbb{R}$ be a non-constant homogeneous polynomial function. Let $F_{ij} = u_i \frac{\partial F}{\partial u_j} - u_j \frac{\partial F}{\partial u_i}$. If $p := (a_0, a_1, \ldots, a_{n-1})$ is a stationary point of $F$ on the ball $B^n$, then $(a_0, a_1, \ldots, a_{n-1})$ is on the boundary $\partial B^n = S^{n-1}$, and $F_{ij}(a_0, a_1, \ldots, a_{n-1}) = 0$ for all $i, j$.

**Proof.** As $F$ is homogeneous, the first claim follows immediately. For the second claim, the tangent space to $p \in S^n$ is the subspace of $\mathbb{R}^n$ orthogonal to the vector $(a_0, a_1, \ldots, a_{n-1})$, and so $p$ is a stationary point of $F$ if and only if $\nabla F = (\frac{\partial F}{\partial a_0}, \ldots, \frac{\partial F}{\partial a_{n-1}})(p)$ is a scalar multiple of $(a_0, a_1, \ldots, a_{n-1})$, hence the claim. \qed

Thus to compute the global maximum of $F$, we can try to solve the system of equations $F_{ij} = 0$ on $S^n$. The variety defined by these equations often has positive dimension, and hence infinitely many points. This issue can in practice often be solved by adding the condition that $F \neq 0$ at a stationary point.

Thus let $I \subset \mathbb{Q}[u_0, \ldots, u_{n-1}]$ be the ideal generated by $F_{ij}$, for $0 \leq i, j \leq n-1$, and consider the colon ideal $J := ((F) : I) = \{ f \in \mathbb{Q}[u_0, \ldots, u_{n-1}] : f \cdot I \subset (F) \}$. The variety $V$ defined by $J$ is the set theoretic difference of the variety defined by $I$ and the variety defined by $(F)$, and the global maximum of $F$ corresponds to an $\mathbb{R}$-point of $V$. If $V$ is a 0-dimensional variety, which will be the case in practice, there exist standard algorithms to compute the finite set $V(\mathbb{R})$, and hence find the global maximum.

As an example, take $F = u_0^6 + u_1^6 + u_2^6$. Then $V$ is a dimension 0 variety defined over $\mathbb{Q}$. We list the defining equations of irreducible components of $V$ that have real points:

(i) $u_0 \pm 1, u_1, u_2$

(ii) $u_0 \pm u_1, u_1^2 - 1/2, u_2$

(iii) $u_0 \pm u_1, u_1 \pm u_2, u_2^2 - 1/3$

together with the sets equations obtained by permuting the coordinates. Now it is easy to see that the maximum of $F$ on $S^2$ is 1, and is attained at $(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)$.

This method works very well when $n = 3$ or if $F$ is a monomial function. For more complicated examples however, solving for stationary points exactly becomes computationally difficult, and we resort to the following brute force method to estimate the maximum.

Taking into account symmetries of $D_2$, we only need to consider $F$ obtained via the following averaging procedure. Let $F_1$ be a monomial of degree $2n$. Set $F_2 = \sum_{i \in \mathbb{Z}/n} F_1(u_{0+i}, \ldots, u_{n-2+i})$, where the subscripts are read mod $n$, and then set

$$F = F_2(u_0, u_1, u_2, \ldots, u_{n-2}, u_{n-1}) + F_2(u_0, u_{n-1}, u_{n-2}, \ldots, u_2, u_1).$$

It is easy to check that $F(u_0, u_1, u_2, \ldots, u_{n-2}, u_{n-1}) = F(u_1, u_2, \ldots, u_{n-1}, u_0)$, and that replacing $u_i$ by $-u_i$ does not change $|F(u_0, \ldots, u_{n-1})|$. The following procedure returns an upper bound for $|F|$ on the sphere $S^{n-1} \subset \mathbb{R}^n$. 

Subdividing into boxes. It suffices to bound $F$ on the subset
\[ S^+ = \{(u_0, \ldots, u_{n-1}) \in S^{n-1} | u_0 \geq 0, u_1 \geq u_0, \ldots, u_{n-1} \geq u_0, \\
\quad u_1 + \ldots + u_{(n-1)/2} \leq u_{(n-1)/2+1} + \ldots + u_{n-1} \}. \]
Let $B^+$ be the projection of $S^+$ on the hyperplane $u_0 = 0$. If $B^n$ denotes the $n$-dimensional unit ball, then
\[ B^+ = \{(u_1, \ldots, u_{n-1}) \in B^n | \min(u_1, \ldots, u_{n-1}) \geq 1 - u_1^2 - \ldots - u_{n-1}^2, \\
\quad u_1 + \ldots + u_{(n-1)/2} \leq u_{(n-1)/2+1} + \ldots + u_{n-1} \}. \]
We have the parametrization $p : B^+ \to S^+$
\[ p(u_1, \ldots, u_{n-1}) = (\sqrt{1 - u_1^2 - \ldots - u_{n-1}^2}, u_1, \ldots, u_{n-1}) \]
Let $N$ be a large integer, and consider the set $I_N = \{(a_1, \ldots, a_{n-1}) \in B^n | Na_i \in \mathbb{Z}\}$. For any $\epsilon > 0$ and $a \in S^+$, let $B_{a, \epsilon} = \{(v_0, \ldots, v_{n-1}) \in S^+ | \max(|v_k - a_k|) < \epsilon\}$. It is easy to compute, for any given $\epsilon$, an integer $N_\epsilon$ such that for any $a \in S^+$ we have $a \in B_{a, \epsilon}$ for some $i \in I_{N_\epsilon}$, and hence $\{B_{i, \epsilon}|i \in I_{N_\epsilon}\}$ is an open cover of $S^+$.

Bounding $F$ on $B_{i, \epsilon}$. We consider Taylor expansion of $F$ at points $a \in I_{N_\epsilon}$. Define
\[ G(a_0, \ldots, a_{n-1}, v_0, \ldots, v_{n-1}) = F(a_0 + v_0, \ldots, a_{n-1} + v_{n-1}), \]
and express $G$ as
\[ G = F(a_0, \ldots, a_{n-1}) + \sum_{i=0}^{n-1} c_i v_i + H(a_0, \ldots, a_{n-1}, v_0, \ldots, v_{n-1}) \]
where $H$ has only terms of degree at least 2 in the variables $v_0, \ldots, v_{n-1}$. We then bound $H$ uniformly on all the boxes $B_{a, \epsilon}$ for $a \in S^+$, by using the estimates $|a_i| < 1$, $|v_i| < \epsilon$ and the triangle inequality. It is straightforward to compute the maximum of the linear part $\sum_{i=0}^{n-1} c_i v_i$ for each box $B_{a, \epsilon}$ separately, and thus obtain an upper bound for $F$.

Refining the bound. To obtain a sharp bound for the monomial sum $F$, we can iterate the process described above. We start by guessing what the bound should be, by evaluating $F$ on all vertices of the grid $I_N$ for some large integer $N$. This can be done very quickly and in practice appears to be a very accurate heuristic to determine what the maximum of $|F|$ should be. To obtain a rigorous bound, we take a real number $C$ slightly larger than our heuristic bound, and try to prove that $\max_{S^+} |F| < C$. We start by (arbitrarily) choosing an integer $N > 0$, enumerating all elements of $I_N$, and then bounding $F$ on all the boxes $B_{i, \epsilon}$. We discard all of the boxes for which the bound is less than $C$. For the remaining boxes, we replace $N$ by $2N$, subdivide these boxes further, and then compute bounds on this refined cover, again discarding all of the boxes for which we can prove that $|F| < C$. We iterate this procedure until there are
no boxes left. At that point, we have proven that $|F|<C$ on the entire sphere $S$.

### 6.3 Bounding the coefficients

By Lemma 5.3.3, to obtain effective constants in Theorem 6.1.1, we need to bound the coefficients of the normalized discriminant form $D_\tau = D_\tau/H_{2n-2}^2$ on the set $A = \{\tau \in \mathcal{H} : \text{Re}(\tau) \in \{0,n/2\}\}$. The coefficients of the form $D_\tau$ are homogeneous polynomials of degree $2n-2$ in the coefficients of the matrix $\Omega_\tau$, and hence are power series in $q^{1/n}$. The height function $H_\tau = \max(|E_4(\tau)|^{1/4}, |E_6(\tau)|^{1/6})$ is also defined in terms of $q$-series. These power series converge quickly, and roughly speaking, our strategy will be to prove a bound on their tails, and then bound the polynomials obtained by truncating the series.

**Power series expressions.** We start by explaining how to compute power series expansions of the coefficients of $\Omega_\tau$ to arbitrary precision, as well as how to bound their coefficients. We recall the $q$-series expansions for the functions $x_\tau, 0 \leq q \leq n-1$. Recall the Jacobi triple product identity:

$$\prod_{m \geq 1} (1 - x^{2m})(1 - x^{2m-1}z)(1 - x^{2m-1}z^{-1}) = \sum_{m \in \mathbb{Z}} (-1)^m x^{m^2} z^m$$

We will use this identity to turn the infinite product expression of $x_\tau(u,q)$

$$x_\tau(z) = (-1)^r q^{\frac{(2r-n)^2}{8n}}(1 - q^r u^{-n})u^{-r} \prod_{m \geq 1} (1 - q^{nm-r}u^m)(1 - q^{nm+r}u^{-n})(1 - q^{nm})$$

into an infinite sum. Substitute $x := q^{n/2}$ and $z := q^{-n/2+r}u^{-n}$ in the Jacobi triple product identity. We find that $u^r x_\tau(u,q)$ is equal to

$$(-1)^r q^{\frac{(2r-n)^2}{8n}} \prod_{m \geq 1} \left(1 - (q^{n/2})^{2m}\right) \left(1 - (q^{n/2})^{2m-1}q^{-\frac{n}{2}+r}u^{-n}\right) \left(1 - (q^{n/2})^{2m-1}(q^{-n/2+r}u^{-n})^{-1}\right)$$

$$= (-1)^r q^{\frac{(2r-n)^2}{8n}} \sum_{m \in \mathbb{Z}} (-1)^m (q^{n/2})^{m^2} \cdot (q^{-n/2+r}u^{-n})^m$$

$$= (-1)^r \sum_{m \in \mathbb{Z}} (-1)^m q^{\frac{(2r-n)^2}{8n}+nm^2/2+(-n/2+r)m} u^{-nm}$$

$$= \sum_{m \in \mathbb{Z}} (-1)^{m+r} q^{\frac{(2r-n+2mn)^2}{8n}} u^{-nm}$$

Set $u = 1$ to obtain power series for functions $\alpha_\tau(\tau)$,

$$\alpha_\tau(\tau) \equiv (-1)^r q^{\frac{(2r-n)^2}{8n}} \prod_{m \geq 1} (1 - q^{nm-r})(1 - q^{nm+r})(1 - q^{nm})$$

$$= \sum_{m \in \mathbb{Z}} (-1)^{m+r} q^{\frac{(2r-n+2mn)^2}{8n}}.$$

**Bounding tails of power series.** We will bound tails of power series by comparison with a geometric series. This estimate will, in our case, be rather crude, but sufficient as the relevant
power series converge rapidly.

**Lemma 6.3.1.** Let \( f = \sum_{m=0}^{\infty} a_m q^m \) be a power series, with \( a_m \in \mathbb{R} \), and \( |a_m| < Cm(m-1)\cdots(m-k+1) \) for some fixed integer \( k \geq 0 \) and a fixed constant \( C > 0 \). Then, for every integer \( M \geq 0 \) and every real number \( q \in (-1, 1) \), we have \( \sum_{m=\max(M+M)}^{\infty} a_m q^m \leq C^{M(M-1)} \cdots (M+M-k) \).

**Proof.** We compute, using the Taylor expansion of \( \Omega \):

\[
|\sum_{m=\max(M+M)}^{\infty} a_m q^m| \leq |q|^{M} \sum_{m=0}^{\infty} a_{m+M} q^m \leq C|q|^M \sum_{m=0}^{\infty} (m+k)\cdots(m+1)|q|^m = \frac{C|q|^M}{(1-|q|)^k}.
\]

\( \square \)

**Lemma 6.3.2.** Let \( f = \sum_{m=0}^{\infty} a_m q^m \) and \( g = \sum_{m=0}^{\infty} b_m q^m \) be power series, and suppose that there exists constants \( C, C' > 0 \) and integers \( k, l \geq 0 \) with \( |a_m| \leq C n^k \), \( |b_m| \leq C' n^l \). Then, if \( f + g = \sum_{m=0}^{\infty} c_m q^m \) and \( f g = \sum_{m=0}^{\infty} d_m q^m \), we have \( |c_m| \leq \max(C, C') m^{\max(k,l)} \) and \( |d_m| \leq |CC'| m^{k+l+1} \).

**Proof.** Follows immediately from the triangle inequality. \( \square \)

**Coefficients of \( \Omega_r \).** Now recall the formula for the coefficients of \( \Omega_r \), proved in Lemma 5.2.3.

\[
(\Omega_r)_{k,l} = u_{l-k}(\tau) X_k X_{l-k} - \frac{\partial x_0}{\partial z}(0, \tau) \frac{\partial x_k}{\partial z} = \sum_{1 \leq i \leq n-1, i \neq k} \alpha_{l-k}(\tau) - i, l-k X_{i+k} X_{i+l-k},
\]

Differentiating the power series for \( x_0 \), we obtain a power series for \( \frac{\partial x_0}{\partial z} \). We can thus compute power series for all coefficients of \( \Omega_{hl} \), except \( u_{l-k} \). To compute \( u_k \), recall the equation

\[
u_k(\tau)x_0 x_k = x_0 \frac{\partial x_k}{\partial z} - x_k \frac{\partial x_0}{\partial z} + \frac{\partial x_0}{\partial z}(0, \tau) \sum_{1 \leq i \leq n-1, i \neq k} \frac{\alpha_k(\tau)}{\alpha_i(\tau) \alpha_{k-i}(\tau)} x_i x_{k-i} \]

Let \( d_k \) and \( n_k \) be the coefficients of \( u^{-k} \) in \( x_0(z) x_k(z) \) and the right hand side of the above equation respectively. Then we have \( u_k = \frac{d_k}{n_k} \). We can use the expressions for the functions \( x_\tau(u, q) \) to compute \( q \)-series for \( d_k \) and \( n_k \), and hence \( u_k \), to arbitrary precision.

To estimate tails of these series, we want to use Lemma 6.3.1. To be able to apply Lemma 6.3.2, we need to clear the denominators in the entries \( \Omega_r \). Thus, put \( \Omega_r' = \alpha_1 \cdots \alpha_{n-1} \Omega_r \). Then, let \( d'_k = \alpha_1 \cdots \alpha_{n-1} d_k \) and \( n'_k = \alpha_1 \cdots \alpha_{n-1} n_k \), and put \( \Omega_r'' = d_1 \cdots d_{n-1} \Omega_r' \).

The coefficients of \( \Omega_r'' \) are polynomials in \( \alpha_1, \ldots, \alpha_{n-1}, x_0'(0) \) and \( n'_1, \ldots, n'_{n-1} \). The coefficients of \( \alpha_i \) are \( O(1) \) - in fact, they are all 0, 1 or -1. The coefficients of \( x_0'(0) \) are \( O(\sqrt{m}) \).

It remains to bound the coefficients \( n'_k \) and \( d'_k \). We have

\[
x_r x_{k-r} = \left( \sum_{m=\mathbb{Z}} (-1)^{m+r} q^{(2r-n+2mn)/8n} u^{-nm-r} \right) \left( \sum_{m=\mathbb{Z}} (-1)^{m+k-r} q^{(2r-n+2mn)/8n} u^{-nm-r-k} \right)
\]

\[
= \sum_{m=\mathbb{Z}} u^{-nm-k} \sum_{p=\mathbb{Z}} (-1)^{m+k} q^{(2r-n+2mn)/8n} (2r-n+2mn)/(8n).
\]
Hence the coefficient of $u^{-k}$ is given by
\[ \sum_{p \in \mathbb{Z}} (-1)^k q^\left(\frac{(2r-n+2pm)^2+(2r-n-2pm)^2}{8n}\right) = \sum_{p \in \mathbb{Z}} (-1)^k q^\left(\frac{(2r-n)^2+4p^2n^2}{8n}\right). \]

The coefficients of this series are thus $O(1)$. Similarly, one sees that the coefficients of $u^{-k}$ in $\frac{\partial x_0}{\partial x}$ and $\frac{\partial x}{\partial x_0} x_0$ are $q$-series, with $m$-th coefficient bounded by $O(m)$. Now, the entries of $\Omega''$ are given by
\[ \Omega''_{kl} = (\alpha_1 \cdots \alpha_{n-1})(d_1 \cdots \widehat{d_{i-k}} \cdots d_{n-1}) \cdot n_{l-k} x_k x_{l-k} \]
\[ + \sum_{1 \leq i \leq n-1, i \neq k} \frac{x_0(0)}{n-2} (\alpha_1 \cdots \alpha_{i+k} \cdots \alpha_{l-i} \cdots \alpha_{n-1})(d_1 \cdots d_{n-1}) \alpha_{l-k} x_{i+k} x_{l-i}. \]

Coefficients of $\alpha_i$ are $O(1)$ and coefficients of $d_i$ are $O(1)$. Lemma 6.3.2 implies that the coefficients of series in the above expression are $O(m^{n-1}) = O(m^{2n-1})$, and there is no difficulty into making this estimate effective. Lemma 6.3.1 also implies an effective estimate for the tail of the denominator $d = \alpha_1 \cdots \alpha_{n-1} d_1 \cdots d_{n-1}$.

**Coefficients of $D_\tau$.** Recall the definition of the discriminant form $D$ associated to an $\Omega$-matrix of a genus one curve, from Section 3.7. For variables $u_0, \ldots, u_{n-1}$, we put
\[ g = \begin{pmatrix} u_0 & 0 & 0 & 0 & \ldots & 0 & 0 \\ u_1 & 1/u_0 & 0 & 0 & \ldots & 0 & 0 \\ u_2 & 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ u_{n-1} & 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}, \]
and set $\Omega'(x_0, x_1, \ldots, x_{n-1}) = g \ast \Omega = g^{-T} \cdot \Omega(x_0', x_1', \ldots, x_{n-1}') \cdot g^T$, where $x_j' = \sum_{i=0}^{n-1} g_{ij} x_i$. The entries of $\Omega'$ are homogeneous quadrics in $x_0, \ldots, x_{n-1}$, with coefficients rational functions of $u_0, u_1, \ldots, u_{n-1}$. The form $D$ is the determinant of the $(n-1) \times (n-1)$-matrix $n \cdot e^0$, where we have
\[ d_{ij}^0 = \sum_{r=1}^{n-1} \frac{\partial^2 \Omega'}{\partial x_j \partial x_k} \cdot \frac{\partial^2 \Omega'}{\partial x_r \partial x_l} - \frac{\partial^2 \Omega'_r}{\partial x_r \partial x_j} \cdot \frac{\partial^2 \Omega'_l}{\partial x_r \partial x_k}. \]

The first step is to compute this determinant for a generic matrix $\Omega$, and hence express coefficients of $D$ as homogeneous polynomials of degree $2n-2$ in the coefficients of $\Omega$. The form $D_\tau$ is the discriminant form attached to $\Omega_\tau$. Let $D''_\tau = d^{n-2} D_\tau$ be the discriminant form associated to $\Omega''_\tau = d\Omega_\tau$. We use the tail estimates we have obtained for the coefficients of $\Omega''_\tau$ and Lemma 6.3.2 to bound the tails of coefficients of $D''_\tau$.

Our aim is to bound the coefficients of the normalized discriminant form
\[ D_\tau(u_0, \ldots, u_{n-1}) = \frac{D''_\tau(u_0, \ldots, u_{n-1})}{d^{2n-2} H(\tau)^{2n-2}}. \]

Recall that the function $H(\tau) = \max(|E_4(\tau)|^{1/4}, |E_6(\tau)|^{1/6})$ is defined in terms of Eisenstein
series, and we can use Lemma 6.3.1 to estimate them as well. At this point, for a given \( \tau \) in the upper half-plane, the tail bounds we have proven allow us to compute the coefficients of the form \( D_\tau \) to whatever precision we like.

**Functional equation.** On the set \( A = \{ \tau \in \Re(\tau) \in \{0, n/2\} \} \), the function \( q^{1/n} \) takes on values in the interval \((-1, 1)\). To ensure that our \( q \)-series converge rapidly, we need to bound \( \tau \) away from the real axis in \( \mathcal{H} \). To do this, we exploit the fact that the coefficients of \( D_\tau \) are modular forms.

The involutions \( S \cdot \tau = -1/\tau \) and \( R \cdot \tau = \frac{n\tau - (n^2 + 1)/2}{2\tau - n} \) induce bijections

\[
S : A_u^1 := \{it \mid t > 1\} \rightarrow A_1^1 := \{it \mid t < 1\},
\]

\[
R : A_u^2 := \{n/2 + it \mid t > 1/2\} \rightarrow A_1^2 := \{n/2 + it \mid t < 1/2\}.
\]

By Lemma 5.1.7, we have \( B_{-1/\tau} = S_n \cdot B_\tau \) and \( B_{1/\tau} = T_n \cdot B_\tau \), where \( S_n, T_n \) are matrices representing elements of \( \mathrm{PGL}_n(\mathbb{C}) \). We may rescale \( S_n \) and \( T_n \) to ensure that \( \det(S_n) = \det(T_n) = 1 \).

Let \( T \) be the transformation \( \tau \mapsto \tau + 1 \). We can express the transformation \( R \) in terms of \( S \) and \( T \) as \( R = T^{(n-1)/2} \cdot ST^{-2}ST^{-1} \cdot T^{-(n-1)/2} \). It follows that \( D_\tau = R_n \cdot D_{R_\tau} \), where \( R_n = T_n^{(n-1)/2} \cdot S_n T_n^{-2} S_n T_n^{-1} \cdot T_n^{-(n-1)/2} \).

Arguing as in the proof of Lemma 5.2.2, for the action of \( \mathrm{SL}_n(\mathbb{C}) \) on the space of discriminant forms, described in Lemma 3.7.4, we have

\[
D_{-1/\tau}(u_0, \ldots, u_{n-1}) = \tau^{2n-2}D_{-1/\tau}((u_0, \ldots, u_{n-1}) \cdot S_n)
\]

and

\[
D_{1/\tau} = D_\tau((u_0, \ldots, u_{n-1}) \cdot T_n).
\]

Since \( H(\tau + 1) = H(\tau) \) and \( H(-1/\tau) = |\tau| \cdot H(\tau) \), for \( \tau \in A \) we find

\[
D_\tau(u_0, \ldots, u_{n-1}) = \pm D_{S_\tau}((u_0, \ldots, u_{n-1}) \cdot S_n),
\]

\[
D_\tau(u_0, \ldots, u_{n-1}) = \pm D_{R_\tau}((u_0, \ldots, u_{n-1}) \cdot R_n),
\]

the sign arises from the absolute value in the functional equation for \( H(\tau) \). For any monomial \( m \) of degree \( 2n \), let \( c(\tau) \) be the coefficient of \( m \) in \( D_\tau \). From the above equation we obtain power series \( c_1(q^{1/n}) \), \( c_2(q_S^{1/n}) \) and \( c_3(q_R^{1/n}) \) that converge to \( c_m(\tau) \), in variables \( q = e^{2i\pi \tau}, q_S = e^{2i\pi S\tau} \) and \( q_R = e^{2i\pi R\tau} \) respectively. As described before, we compute effective bounds for the tails of these series, and then truncate the tail, putting \( c_i = c_i^{\text{pol}} + c_i^{\text{tail}} \).

On sets \( A_u^1 \) and \( A_u^2 \), the variable \( q = e^{2i\pi \tau/n} \) takes on values in \((-e^{-\pi/n}, e^{-2\pi/n})\). On the set \( A_1^1, q_S^{1/n} = e^{2i\pi S\tau/n} \) takes on values in \((0, e^{-2\pi/n})\), while on the set \( A_1^2, q_R = e^{2i\pi R\tau/n} \) takes on values in \((-e^{-\pi/n}, 0)\). We thus bound \( c(\tau) \) by bounding \( c_1 \) on \( A_u^1 \) and \( A_u^2 \), and bounding \( c_2 \) and \( c_3 \) on \( A_1^1 \) and \( A_1^2 \). We bound polynomials \( c_i^{\text{pol}} \) using a similar method to the method we used to bound monomial sums - we subdivide the interval \((-\pi/n, e^{-2\pi/n})\) into many smaller intervals, and use Taylor expansion on the vertices of the subdivision, together with triangle inequality.
6.4 Examples

We now put together the results of the previous two sections to compute values for \( c(3, B) \) and \( c(5, B) \), where \( B \) is the \( n \)-ball in \( \mathbb{R}^n \), centered at the origin, of volume \( 2^n \). Since it is understood that we are restricting \( K \) to be this ball, we write just \( c(n) \) for \( c(n, K) \) throughout.

We write \( D_c = \sum c_m(q) \cdot m(u_0, \ldots, u_{n-1}) \), where the sum is over all invariant monomial sums \( m \), as described in Section 6.2. We then compute an upper bound for each \( c_m(q) \) on \( A \), and an upper bound for each \( m \) on \( B^{n-1} \), and obtain a value for \( c(n) \) by the triangle inequality. Our main result is the following theorem.

**Theorem 6.4.1.** In Theorem 6.1.1, and hence in Theorem 1.0.1, we can take \( c(3) = 0.63548 \) and \( c(5) = 1.94641 \).

**The case \( n = 3 \).** As an illustration, we give the first few terms of the \( q \)-expansion of \( \Omega_3 \),

\[
\begin{align*}
\Omega_{01} &= (-1 - 3q + 19q - 7q^3 - 32q^4 + O(q^5))x_0x_1 + q^{1/3}(3 - 6q - 6q^2 + 27q^4 + O(q^5))x_2^3 \\
\Omega_{02} &= (1 + 3q - 19q + 7q^3 + 32q^4 + O(q^5))x_0x_2 + q^{1/3}(-3 + 6q + 6q^2 - 27q^4 + O(q^5))x_1^2 \\
\Omega_{12} &= (-1 - 3q + 19q - 7q^3 - 32q^4 + O(q^5))x_1x_2 + q^{1/3}(3 - 6q - 6q^2 + 27q^4 + O(q^5))x_0^2
\end{align*}
\]

We can also compute the corresponding ternary cubic:

\[
F = (-1 - 3q + 19q - 7q^3 - 32q^4 + O(q^5))x_0x_1x_2 + q^{1/3}(3 - 6q - 6q^2 + 27q^4 + O(q^5))(x_0^3 + x_1^3 + x_2^3)
\]

The \( q \)-expansion of the (non-normalized) discriminant form \( D_c \) is

\[
D_c = q^{1/3}(-27q - 108q^2 - 378q^3 - 756q^4 + O(q^5))(u_0^6 + u_1^6 + u_2^6) \\
+ q^{2/3}(18 + 252q + 1170q^2 + 2664q^3 + 6192q^4 + O(q^5))(u_0^4u_1u_2 + u_0u_1^4u_2 + u_0u_1u_2^4)
+ q^{1/3}(-4 + 3q - 296q^2 - 756q^3 - 1232q^4 + O(q^5))(u_0u_1^3 + u_1^3u_2 + u_2^3u_0) \\
+ (1 + 8q - 756q^2 - 2028q^3 + 6132q^4 + O(q^5))u_0^2u_2^2u_2.
\]

It is not difficult to check, via a generic calculation of a discriminant form for a Heisenberg invariant plane cubic, that the coefficients of monomials not listed in the above expression are identically zero. Thus we only need to bound the monomial sums and the coefficients listed above.

We list the results below. The monomial bounds on the unit sphere were computed exactly, using the calculus method given at the beginning of Section 6.2.

(i) \( \max_{u \in S^2} u_0^6 + u_1^6 + u_2^6 = 1 \), achieved at \( (0, 0, 1) \in S^+ \),
(ii) \( \max_{u \in S^2} u_0^4u_1u_2 + u_0u_1^4u_2 + u_0 + u_1u_2^4 = 1/9 \), achieved at \( (1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3}) \in S^+ \),
(iii) \( \max_{u \in S^2} u_0^3u_1^3 + u_0^3u_2^3 + u_2^3u_3^3 = 1/8 \), achieved at \( (0, 1/\sqrt{2}, 1/\sqrt{2}) \in S^+ \),
(iv) \( \max_{u \in S^2} u_0^2u_1^2u_2^2 = 1/27 \), achieved at \( (1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3}) \in S^+ \).
6.4. EXAMPLES

For our compact set $K$, we take the ball centered at the origin, of volume $2^3$, which satisfies the conditions of Minkowski’s theorem. Note that $D_{\tau}$ is a homogeneous polynomial of degree 6, and the monomial bounds listed above are computed for the unit ball. Thus we need to multiply them by $r^6$, where $r = (6/\pi)^{1/3}$ is the radius of $K$. Note that to 5 digits of precision, $r^6 = 3.6475$.

In the next table we list bounds for the coefficients we have computed using the method of Section 6.3, rounded to 5 or 6 digits of precision.

<table>
<thead>
<tr>
<th>Monomial sum</th>
<th>Bound on $A^1_u$</th>
<th>Bound on $A^1_l$</th>
<th>Bound on $A^2_u$</th>
<th>Bound on $A^2_l$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u^6_0 + u^6_1 + u^6_2$</td>
<td>0.0042973</td>
<td>0.037037</td>
<td>0.059853</td>
<td>0.097034</td>
</tr>
<tr>
<td>$u^4_0u_1u_2 + u_0u^3_1u_2 + u_0 + u_1u^2_2$</td>
<td>0.19245</td>
<td>0.26456</td>
<td>0.32619</td>
<td>0.22222</td>
</tr>
<tr>
<td>$u^3_0u^3_1 + u^3_1u^3_2 + u^3_2u^3_3$</td>
<td>0.34193</td>
<td>0.34244</td>
<td>0.32871</td>
<td>0.22564</td>
</tr>
<tr>
<td>$u^2_0u^2_1u^2_2$</td>
<td>1.0000</td>
<td>0.57735</td>
<td>1.0000</td>
<td>0.57735</td>
</tr>
</tbody>
</table>

Putting everything together, we find that the constant $c(3)$ can be taken to be 0.63548.

We can also obtained more refined results for certain families of elliptic curves. Indeed, the method we have used to bound coefficients of $D_{\tau}$ on the set $A$ also implies (sharper) coefficient bounds for any subset of $A$. For example, the subset $A^1_u \cup A^1_l$ corresponds to elliptic curves of positive discriminant. From the above table, we see that for curves with $\tau \in A^1_u$ the upper bound evaluates 0.38467, and for curves in $A^1_l$ it evaluates to 0.47645. Thus, if we restrict Theorem 1.0.1 to elliptic curves with positive discriminant, we can improve the constant $c(3)$ to 0.47645.

We can also restrict to a single value of $q$, or equivalently $\tau \in A$, and obtain even sharper results. This corresponds to restricting Theorem 1.0.1 to a family of real quadratic twists of a given elliptic curve. For a given $\tau \in A$, let us denote the corresponding constant in Theorem 1.0.1, restricted to curves uniformized by the torus $\mathbb{C}/(1, \tau)$, by $c(3, \tau)$.

As an illustration, we give some values for the constant $c(3, \tau)$ that we have computed. Recall that $q = e^{2\pi\tau}$, $q_S = e^{2\pi S\tau}$ and $q_T = e^{2\pi T\tau}$, where $S \cdot \tau = -1/\tau$ and $R \cdot \tau = \frac{-\tau-\tau^2+1/2}{2\tau-n}$ were defined in the last section. The value of $c(3, \tau)$ given in the table below only depends on the value of the relevant parameter $q, q_S$ or $q_R$.

<table>
<thead>
<tr>
<th>$q^{1/3}(\tau)$</th>
<th>$c(3, \tau)$</th>
<th>$q_S^{1/3}(\tau)$</th>
<th>$c(3, \tau)$</th>
<th>$q_T^{1/3}(\tau)$</th>
<th>$c(3, \tau)$</th>
<th>$q_R^{1/3}(\tau)$</th>
<th>$c(3, \tau)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.00000</td>
<td>0.13510</td>
<td>0.00000</td>
<td>0.30396</td>
<td>0.00000</td>
<td>0.13510</td>
<td>0.00000</td>
<td>0.30396</td>
</tr>
<tr>
<td>0.02462</td>
<td>0.18055</td>
<td>0.02462</td>
<td>0.29661</td>
<td>-0.07018</td>
<td>0.27426</td>
<td>-0.07018</td>
<td>0.40265</td>
</tr>
<tr>
<td>0.04925</td>
<td>0.23519</td>
<td>0.04925</td>
<td>0.28689</td>
<td>-0.14037</td>
<td>0.34399</td>
<td>-0.14037</td>
<td>0.39502</td>
</tr>
<tr>
<td>0.07388</td>
<td>0.28122</td>
<td>0.07388</td>
<td>0.30634</td>
<td>-0.21055</td>
<td>0.40089</td>
<td>-0.21055</td>
<td>0.42072</td>
</tr>
<tr>
<td>0.09851</td>
<td>0.31332</td>
<td>0.09851</td>
<td>0.32516</td>
<td>-0.28074</td>
<td>0.53653</td>
<td>-0.28074</td>
<td>0.55019</td>
</tr>
<tr>
<td>0.12314</td>
<td>0.32757</td>
<td>0.12314</td>
<td>0.32757</td>
<td>-0.35092</td>
<td>0.47171</td>
<td>-0.35092</td>
<td>0.47171</td>
</tr>
</tbody>
</table>

The two tables on the left side give bounds for $c(3, \tau)$ for a few values of $\tau$ in $A^1_u$ and $A^1_l$, while the tables on the right side give bounds for $\tau \in A^2_u$ and $\tau \in A^2_l$. In the first and the third table, the entry with $q^{1/3} = 0$ corresponds to the degenerate case where we take $\tau$ to be the cusp $\infty$. In the second and the fourth table, entries with $q_S^{1/3} = 0$ and $q_R^{1/3} = 0$ correspond to $\tau$ being the cusp at 0 and $n/2$ respectively.
We next look at applications to concrete elliptic curves. The following theorem is a consequence of the well known fact that the cubic field with the smallest (absolute) discriminant is $\mathbb{Q}[X]/(X^3 - X^2 + 1)$, of discriminant is -23.

**Theorem 6.4.2.** If $E/\mathbb{Q}$ is an elliptic curve with $c(3)H_E^3 < 23$, then $\text{III}(E/\mathbb{Q})[3]$ is trivial.

Among the curves of conductor less than 1000, the theorem applies to curves labeled 11a3, 15a8, 17a4, 19a3, 26a3 and 27a3 in Cremona’s tables. If we instead use the refined constant $c(3, \tau)$, we can in addition prove that $\text{III}(E/\mathbb{Q})[3]$ vanishes for curves 14a4, 20a2, 21a4, 24a4, 32a2, 37a1, 39a4, 43a1, 48a4, 53a1, 55a4, 57b2, 64a4, 65a1, 73a2, 80a2, 80b2, 89b2, 101a1, 141d1 and 142b1. We note that this is not a new result, since for any of these curves we can compute the 3-Selmer group by 3-descent.

**The case $n = 5$.** In this case the expression $D_\tau = \sum_m c(m) \cdot m$ consists of 31 monomial sums. To bound them on the sphere $S^4$, we use the second method we developed. For a monomial sum $m$, let $c_0^1(m), c_1^1(m), c_0^2(m), c_1^2(m)$ be bounds for the absolute value of $c(m)$ on $A_0^1, A_1^1, A_0^2, A_1^2$. We summarise bounds we have computed in the following table.
### 6.4. EXAMPLES

<table>
<thead>
<tr>
<th>Monomial sum $m$</th>
<th>Bound on $m$</th>
<th>$c_1^*(m)$</th>
<th>$c_1^1(m)$</th>
<th>$c_1^2(m)$</th>
<th>$c_1^3(m)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1^{10} + \ldots$</td>
<td>1.2000</td>
<td>$1.8066 \times 10^{-8}$</td>
<td>0.00032000</td>
<td>0.00027331</td>
<td>0.0057956</td>
</tr>
<tr>
<td>$u_1^{7}u_2u_3 + \ldots$</td>
<td>0.048829</td>
<td>$2.2562 \times 10^{-6}$</td>
<td>0.00320000</td>
<td>0.0011756</td>
<td>0.029918</td>
</tr>
<tr>
<td>$u_1^{6}u_3u_4 + \ldots$</td>
<td>0.048829</td>
<td>$4.0792 \times 10^{-5}$</td>
<td>0.0034291</td>
<td>0.014470</td>
<td>0.056744</td>
</tr>
<tr>
<td>$u_1^{5}u_2^2u_4 + \ldots$</td>
<td>0.022877</td>
<td>$7.6605 \times 10^{-5}$</td>
<td>0.00363633</td>
<td>0.014000</td>
<td>0.052352</td>
</tr>
<tr>
<td>$u_1^{7}u_2u_5^3 + \ldots$</td>
<td>0.022877</td>
<td>$0.00030253$</td>
<td>0.00584300</td>
<td>0.029088</td>
<td>0.069920</td>
</tr>
<tr>
<td>$u_1^{6}u_3u_5^3 + \ldots$</td>
<td>0.014605</td>
<td>$0.00075644$</td>
<td>0.0079122</td>
<td>0.038177</td>
<td>0.080796</td>
</tr>
<tr>
<td>$u_1^{5}u_2^2u_5^2 + \ldots$</td>
<td>0.0098583</td>
<td>$1.6181 \times 10^{-6}$</td>
<td>0.011200</td>
<td>0.0090680</td>
<td>0.045459</td>
</tr>
<tr>
<td>$u_1^{5}u_2u_3u_4u_5 + \ldots$</td>
<td>0.0026236</td>
<td>$0.0033224$</td>
<td>0.015373</td>
<td>0.14519</td>
<td>0.36536</td>
</tr>
<tr>
<td>$u_1^{4}u_2^3 + \ldots$</td>
<td>0.014605</td>
<td>$0.0052573$</td>
<td>0.019636</td>
<td>0.078319</td>
<td>0.12375</td>
</tr>
<tr>
<td>$u_1^{4}u_2u_4^3 + \ldots$</td>
<td>0.0098583</td>
<td>$0.016888$</td>
<td>0.041713</td>
<td>0.16412</td>
<td>0.26279</td>
</tr>
<tr>
<td>$u_1^{3}u_2^4 + \ldots$</td>
<td>0.037463</td>
<td>$0.0042541$</td>
<td>0.0025592</td>
<td>0.011384</td>
<td>0.021497</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3u_4u_5 + \ldots$</td>
<td>0.0049798</td>
<td>$0.0076926$</td>
<td>0.019200</td>
<td>0.065775</td>
<td>0.19603</td>
</tr>
<tr>
<td>$u_1^{5}u_2^2u_4u_5 + \ldots$</td>
<td>0.0039359</td>
<td>$0.020350$</td>
<td>0.044403</td>
<td>0.26507</td>
<td>0.52994</td>
</tr>
<tr>
<td>$u_1^{4}u_2u_3u_4u_5 + \ldots$</td>
<td>0.0039359</td>
<td>$0.040525$</td>
<td>0.073184</td>
<td>0.21290</td>
<td>0.24233</td>
</tr>
<tr>
<td>$u_1^{3}u_2^2u_4^2 + \ldots$</td>
<td>0.0049798</td>
<td>$0.15926$</td>
<td>0.22019</td>
<td>0.58937</td>
<td>0.47901</td>
</tr>
<tr>
<td>$u_1^{2}u_2^3 + \ldots$</td>
<td>0.037463</td>
<td>$0.095884$</td>
<td>0.11034</td>
<td>0.21878</td>
<td>0.12677</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3u_4u_5 + \ldots$</td>
<td>0.0030394</td>
<td>$0.012425$</td>
<td>0.020665</td>
<td>0.19181</td>
<td>0.40177</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_4^3 + \ldots$</td>
<td>0.0059137</td>
<td>$0.032426$</td>
<td>0.044865</td>
<td>0.10849</td>
<td>0.11555</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_4u_5 + \ldots$</td>
<td>0.0037261</td>
<td>$0.12681$</td>
<td>0.14492</td>
<td>0.34381</td>
<td>0.40120</td>
</tr>
<tr>
<td>$u_1^{2}u_3^2u_4 + \ldots$</td>
<td>0.0049281</td>
<td>$0.0072955$</td>
<td>0.016000</td>
<td>0.023227</td>
<td>0.083938</td>
</tr>
<tr>
<td>$u_1^{2}u_3^2u_4^2 + \ldots$</td>
<td>0.0059137</td>
<td>$0.083300$</td>
<td>0.085675</td>
<td>0.13457</td>
<td>0.12046</td>
</tr>
<tr>
<td>$u_1^{2}u_2^2u_3u_4u_5 + \ldots$</td>
<td>0.0018034</td>
<td>$0.18279$</td>
<td>0.23860</td>
<td>0.92330</td>
<td>1.2166</td>
</tr>
<tr>
<td>$u_1^{2}u_2^2u_5^2 + \ldots$</td>
<td>0.0037261</td>
<td>$0.029039$</td>
<td>0.066442</td>
<td>0.16803</td>
<td>0.28580</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3u_4^2u_5 + \ldots$</td>
<td>0.0018034</td>
<td>$1.0770$</td>
<td>1.0084</td>
<td>2.1090</td>
<td>1.6399</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3^2u_4 + \ldots$</td>
<td>0.0030394</td>
<td>$0.78656$</td>
<td>0.78553</td>
<td>0.71090</td>
<td>0.24902</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3^2u_4^2 + \ldots$</td>
<td>0.0049281</td>
<td>$0.65671$</td>
<td>0.61520</td>
<td>0.59272</td>
<td>0.21025</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3u_5^2 + \ldots$</td>
<td>0.0017934</td>
<td>$0.052514$</td>
<td>0.13046</td>
<td>0.52645</td>
<td>0.97984</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3u_4u_5 + \ldots$</td>
<td>0.0017236</td>
<td>$0.93247$</td>
<td>0.93369</td>
<td>0.74326</td>
<td>0.48774</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3^2u_4u_5 + \ldots$</td>
<td>0.0017236</td>
<td>$0.94989$</td>
<td>0.94989</td>
<td>1.2449</td>
<td>1.6848</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3^2u_4^2 + \ldots$</td>
<td>0.0017934</td>
<td>$0.70737$</td>
<td>0.56767</td>
<td>0.65029</td>
<td>0.32846</td>
</tr>
<tr>
<td>$u_1^{2}u_2u_3u_4^2u_5^2 + \ldots$</td>
<td>0.00033177</td>
<td>$1.0325$</td>
<td>1.4325</td>
<td>4.5368</td>
<td>3.3664</td>
</tr>
</tbody>
</table>

From these bounds one obtains the constant $c(5) = 1.94641$. As in the case $n = 3$, we can obtain various refinements of this result. If we restrict to curves of positive discriminant, we can replace $c(5)$ with 0.823139. We can also compute $c(5, \tau)$ for a given $\tau \in \mathbb{A}$. We give some examples in the table below, using the same notation as in the case $n = 3$. 
Consulting the LMFDB database of number fields of small degree, we find that the quintic field of smallest (absolute) discriminant is $\mathbb{Q}[X]/(X^5 - X^3 - X^2 + X + 1)$, of discriminant 1609. Theorem 6.4.1 then implies the following.

**Theorem 6.4.3.** If $E/\mathbb{Q}$ is an elliptic curve with $c(5)H^5_E < 1609$, then $\text{III}(E/\mathbb{Q})[5]$ is trivial.

With the value 1.94641 for $c(5)$, the theorem as stated applies only to the curve 11a3, of height 2.31. Using instead the sharper constant $c(5,\tau)$, the theorem applies to curves 11a3, 15a8, 17a4, 19a3, 26a3, 27a3, 32a2, 37a1, 39a4, 48a4 and 57b2.
Chapter 7

Kolyvagin classes

7.1 Introduction

Let $E/Q$ be a modular elliptic curve of conductor $N$, with a fixed modular parametrization $\phi : X_0(N) \to E$. Let $K$ be an imaginary quadratic field satisfying the Heegner hypothesis, that is, all prime factors of $N$ split in $K$. Let $H$ be the Hilbert class field of $K$. Using the theory of complex multiplication and the modular parametrization $\phi$, one defines certain points in $E(H)$, known as the Heegner points.

Let us now fix an odd prime $p$. Kolyvagin ([Gro91]) has used Heegner points to construct certain cohomology classes in the $p$-Selmer group $\text{Sel}^p(E/Q)$. The images of these classes under the natural map $\text{Sel}^p(E/Q) \to \text{III}(E/Q)[p]$ are known as the Kolyvagin classes. Our aim in this chapter is to describe a method to explicitly compute representations of these classes as $p$-diagrams $[C \to \mathbb{P}^{p-1}]$.

More precisely, we give a method to compute equations defining the homogeneous space $C$ as a subvariety of $\mathbb{P}^{p-1}$. The genus one curve $C$ represents an element of Tate-Shafarevich group $\text{III}(E/Q)[p]$, and if this element is non-trivial, $C$ represents a counter-example to the Hasse principle. In other words, it admits points over every completion of $Q$, but not $Q$ itself.

These calculations are especially interesting if $p > 5$, and the curve $E$ does not admit a $p$-isogeny. For such $p$, the method of $p$-descent, which is the standard way to obtain such counterexamples, is not feasible in practice, as one runs into difficulties with computing class groups of very large number fields. Our method does not run into this problem, and in particular, in Section 7.6, we compute the first known explicit realization of a non-trivial element of $\text{III}(E/Q)[7]$ for an elliptic curve $E$ that does not have a 7-isogeny.

These classes have already been studied from a computational point of view by Jetchev, Leuter and Stein in [JLS09]. They are able to compute representations of these classes as elements of $E(L)/pE(L)$, where $L$ is a certain abelian extension of $K$. Their aim is only to test whether these classes are non-zero, for which this representation is sufficient, whereas we compute explicit equations defining the corresponding homogeneous space.

The problem of computing these equations breaks up into two problems. First, given a suitable elliptic curve $E$, a discriminant $D$ and a prime $p$, we compute a Heegner point $x_D$, defined over a certain dihedral extension of $Q$. Our method for doing this is Algorithm 7.5.3. To this point we associate a Kolyvagin class $c \in \text{Sel}^p(E/Q)$. Algorithm 7.4.12 then represents
this class by a genus one curve $C \subset \mathbb{P}^p - 1$. The main difficulty in our computations is caused by the fact that typically the Heegner points $x_D$ have very large height, making them hard to compute and work with. We note that despite this, the output of Algorithm 7.4.12 is a model for the curve $C$ with small integral coefficients, i.e. a minimized and reduced model, in the sense of [CFS10].

7.2 Background on Heegner points and Kolyvagin classes

In this section we review basic material from the theory of Heegner points. The main references are the articles of Gross, [Gro91] and [Gro84], as well as [Wes15], [Wat05] and Chapter 8 of [Coh08]. We will also need some foundational material from the theory of modular curves, see [DS05], and from the theory of complex multiplication, see Chapter II of [Sil94].

The modular curve $Y_0(N)$. For $N \geq 1$ an integer, let $Y_0(N)$ be the open modular curve, defined over $\mathbb{Q}$. The $\mathbb{C}$-points of $Y_0(N)$ classify isomorphism classes of cyclic $N$-isogenies $E \to E'$, defined over $\mathbb{C}$. If $K$ is a number field, then the situation is a bit subtler: $K$-points of $Y_0(N)$ classify $K$-isomorphism classes of cyclic $N$-isogenies $E \to E'$, where $E$, $E'$ and the isogeny are defined over $K$. In any case, to a cyclic $N$-isogeny $E \to E'$ defined over $K$ we can associate a point of $Y_0(N)(K)$, and so this subtlety will not be important to us.

The set of complex points $Y_0(N)(\mathbb{C})$ can be identified with the quotient $\mathcal{H}/\Gamma_0(N)$ of the upper half-plane. We describe the map $Y_0(N)(\mathbb{C}) \to \mathcal{H}/\Gamma_0(N)$. Suppose $E \to E'$ corresponds to a point of $Y_0(N)(\mathbb{C})$. We can identify $E \to E'$ with an isogeny of complex tori $\mathbb{C}/M \to \mathbb{C}/M'$. Rescaling the lattice $M'$ if necessary, we may assume that the $M \subset M'$, and that the isogeny is induced by the identity map $\mathbb{C} \to \mathbb{C}$. Then $M'/M \cong \mathbb{Z}/N\mathbb{Z}$, and so by elementary divisor theory, there exists a basis $\omega_1, \omega_2$ of $M$, such that $M' = \mathbb{Z} \cdot \omega_1 \oplus \mathbb{Z} \cdot \omega_2/N$, and moreover we have $\text{Re}(\omega_1/\omega_2) > 0$, so that $\tau = \omega_1/\omega_2 \in \mathcal{H}$. The $\Gamma_0(N)$-orbit of $\tau$ is the point of $\mathcal{H}/\Gamma_0(N)$ associated to the isogeny $E \to E'$.

Conversely, to a point $\tau \in \mathcal{H}$, we associate the isogeny $\mathbb{C}/(\tau, 1) \to \mathbb{C}/(\tau, 1/N)$. This induces the inverse map $\mathcal{H}/\Gamma_0(N) \to Y_0(N)(\mathbb{C})$.

Heegner points on the modular curve $Y_0(N)$. Let $K$ be an imaginary quadratic field and let $\mathcal{O}$ be an order in $\mathcal{O}_K$, the ring of integers of $K$. We assume $\mathcal{O}$ has discriminant $D$, where $D \neq -3, 4$. A (complex) Heegner point, of discriminant $D$ and level $N$, is a point on $Y_0(N)(\mathbb{C})$ that corresponds to a cyclic $N$-isogeny $[E \to E']$, where $E$ and $E'$ have complex multiplication by $\mathcal{O}$.

We restrict here to the case where $N$ and $D$ are coprime. We write $D = d_Kc^2$, where $d_K$ is the discriminant of $\mathcal{O}_K$, and the integer $c$ is the conductor of $\mathcal{O}$. In most of our applications, the order $\mathcal{O}$ will be the maximal order.

For the set of Heegner points to be non-empty, the field $K$ needs to satisfy the Heegner hypothesis: every prime dividing $N$ splits completely in $K$. Indeed, suppose $\mathbb{C}/M \to \mathbb{C}/M'$ corresponds to a Heegner point. We may, modifying by a homothety if necessary, assume that $a = M$ and $b = M'$ are projective $\mathcal{O}$-submodules of $K$. As the kernel $M'/M$ is cyclic of order
7.2. BACKGROUND ON HEEGNER POINTS AND KOLYVAGIN CLASSES

N, we see that \( N = ab^{-1} \) is an invertible ideal with \( \mathcal{O}/N = \mathbb{Z}/N\mathbb{Z} \), and it is easy to see that such an ideal exists if and only if the Heegner condition is met.

Given such an ideal \( N \), an ideal class \([a] \in \text{Cl}(\mathcal{O})\) determines an isogeny \( \mathbb{C}/a \to \mathbb{C}/aN^{-1} \) with kernel \( aN^{-1}/a \cong \mathbb{Z}/N\mathbb{Z} \), and hence a Heegner point in \( Y_0(N)(\mathbb{C}) \). We denote this point by the triple \((\mathcal{O}, [a], N)\). Conversely, it is clear that all Heegner points arise in this way.

Note that the ideal \( N \) is not unique - it corresponds to a factorization \( NO = N\bar{N} \). For example, if the conductor \( N \) is square-free with \( s \) prime factors, there are \( 2^s \) choices for the ideal \( N \). The choices for the ideal \( N \) are accounted for by the action of Atkin-Lehner involutions on \( Y_0(N) \), see Section 5 of [Gro84].

We can characterise the images of the Heegner points in the upper half plane \( \mathcal{H} \) as follows. We say \( \tau \in \mathcal{H} \) is a CM point if it is a root of a quadratic equation \( A\tau^2 + B\tau + C = 0 \), where \( A, B \) and \( C \) are integers. We assume \((A, B, C) = 1 \) and \( A > 0 \), which makes \( A, B \) and \( C \) unique, and define \( f_s(x, y) = Ax^2 + Bxy + Cy^2 \). We say \( \Delta(\tau) = B^2 - 4AC \) is the discriminant of \( \tau \).

**Definition 7.2.1.** We say a CM point \( \tau \in \mathcal{H} \) is a Heegner point of level \( N \) and discriminant \( D \), if it satisfies \( \Delta(\tau) = \Delta(N\tau) \)

It is straightforward to verify that the set of Heegner points is stable under the action of \( \Gamma_0(N) \) on \( \mathcal{H} \). The set of \( \Gamma_0(N) \)-orbits of Heegner points is in bijection with the Heegner points on \( Y_0(N) \) we defined earlier. This essentially follows from the classical bijection between equivalence classes of primitive binary quadratic forms of discriminant \( D \), and the ideal class group \( \text{Cl}(\mathcal{O}) \), see Theorem 7.7 of [Cox11]. Briefly, to a form \( Ax^2 + Bxy + Cy^2 \) we associate the ideal \([A, (-B + \sqrt{D})]/2\). Conversely, to an ideal \([\omega_1, \omega_2]\), where \( \omega_1 \) and \( \omega_2 \) are an oriented basis, so that \( \tau = \omega_1/\omega_2 \in \mathcal{H} \), we associate the form \( N_{K/Q}(x\omega_1 - y\omega_2)/N_{K/Q}(a) \), where \( N_{K/Q} \) is the norm from \( K \) to \( \mathbb{Q} \). Given a Heegner point \((\mathcal{O}, a, N)\), choose an oriented basis \( a = [\omega_1, \omega_2] \) so that \( aN^{-1} = [\omega_1, \omega_2/N] \) and \( \tau = \omega_1/\omega_2 \in \mathcal{H} \). Then the quadratic forms associated to these ideals have \( \tau \) and \( N\tau \) as roots, are integral, primitive, and of discriminant \( D \), and hence \( \tau \) is a Heegner point.

**Rationality of Heegner points.** A key property of Heegner points, implied by the theory of complex multiplication, is that they are defined over certain (relatively) small abelian extensions of the field \( K \). More precisely, let \((\mathcal{O}, [a], N)\) be a Heegner point. This point is defined over the ring class field \( H \) associated to the order \( \mathcal{O} \). The key point is that both \( \mathbb{C}/a \) and \( \mathbb{C}/aN^{-1} \) have complex multiplication by \( \mathcal{O} \). See §5 of [Gro84]. This is a consequence of the Shimura reciprocity law, as explained in Chapter 6.8 of [Shi71], or, for the case \( \mathcal{O} = \mathcal{O}_K \), Chapter II of [Sil94].

The ring class field \( H \) is an abelian extension of \( K \), unramified outside the set of primes that divide the conductor \( c \), and the Artin map provides a canonical \( F : \text{Cl}(\mathcal{O}) \to \text{Gal}(H/K) \). Explicitly, by Shimura reciprocity, for an ideal class \([b]\) we have \( j([a])^{F([b])} = j([ab^{-1}]) \), and hence

\[
(\mathcal{O}, [a], N)^{F([b])} = (\mathcal{O}, [ab^{-1}], N).
\]

Suppose that \( \tau \in \text{Gal}(H/\mathbb{Q}) \) is a lift of complex conjugation. The action of \( \tau \) is given by

\[
(\mathcal{O}, [a], N)^\tau = (\mathcal{O}, [\tau(a)], \tau(N)).
\]
We remark that if $O = O_K$ is maximal, $H$ is the Hilbert class field of $K$.

**Heegner points on elliptic curves and Kolyvagin classes.** Now let $E$ be an elliptic curve defined over $\mathbb{Q}$, of conductor $N$. Let $X_0(N)$ be the compactified modular curve of level $N$. By the modularity theorem (see [BCDT01]), there exists a modular parametrization map $\phi : X_0(N) \rightarrow E$. For every discriminant $D$ that satisfies the Heegner condition, we fix an ideal $\mathcal{N}$ with $N\mathcal{O} = \mathcal{N}\mathcal{N}$, and define the Heegner point $x_D \in E(H)$ by setting $x_D = \phi(O, [n], \mathcal{N})$. We also define the basic Heegner point $y_D \in E(K)$ by setting $y_D = \text{Tr}_{H/K} x_D$.

Let $p > 2$ be a prime such that $E(H)[p]$ is trivial, $y_D \in pE(K)$ and $p$ divides $|\text{Cl}(\mathcal{O})| = |H : K|$ exactly once. These assumptions are fairly mild, as we will see later. Then there exists a unique degree $p$ subfield $H$, which we denote by $L$. Let $z_D = \text{Tr}_{H/L} x_D$, and let $\sigma$ be a generator of $G = \text{Gal}(L/K)$. Now define the operators $D_\sigma$ and $\text{Tr}$ in $\mathbb{Z}[G]$ by

$$D_\sigma = \sum_{i=0}^{p-1} \sigma^i, \quad \text{Tr} = \sum_{i=1}^{p-1} i\sigma^i.$$  

The operator $D_\sigma$ is known as the *Kolyvagin derivative* and $\text{Tr}$ is just the trace operator. They satisfy the identity

$$(\sigma - 1)D_\sigma = p - \text{Tr},$$

We now define the *derived* Heegner point $P$ as $P = D_\sigma \cdot z_D$. The class $[P] \in E(L)/pE(L)$ is invariant under the action of $G$, since we have

$$(\sigma - 1)(D_\sigma \cdot z_D) = pz_D - \text{Tr}(z_D) = pz_D - \text{Tr}_{H/K}(x_K) = pz_D - y_D,$$

and by assumption $y_D \in pE(K)$. The Kummer map $\delta : E(L)/p(L) \rightarrow H^1(L, E[p])$ is Galois equivariant, and so we can define a cohomology class $c_L \in H^1(L, E[p])^\text{Gal}(L/K)$ by $c_L = \delta([P])$.

We have the inflation-restriction exact sequence

$$H^1(L/K, E[p](L)) \xrightarrow{\text{inf}} H^1(K, E[p]) \xrightarrow{\text{res}} H^1(L, E[p])^\text{Gal}(L/K) \rightarrow H^2(L/K, E[p](L)).$$

As $E[p](L)$ is trivial, the two outermost groups are trivial, and the restriction map defines an isomorphism $\text{res} : H^1(K, E[p]) \rightarrow H^1(L, E[p])^\text{Gal}(L/K)$. We define $c \in H^1(K, E[p])$ to be the preimage of $c_L$ under the restriction map. The class $c$ is in fact an element of the $p$-Selmer group $\text{Sel}^{(p)}(E/K)$, see Prop. 6.2 of [Gro91]. At the primes of good reduction, this follows immediately from the fact that $L/K$ is unramified, at the primes of bad reduction the argument is a bit more involved. For the classes we compute in Section 7.6, we will be able to check local solubility directly. Finally, let $d$ be the image of $c$ in $H^1(K, E)$. Then $d$ is an element of $\text{III}(E/K)[p]$.

**Motivation - Kolyvagin’s theorem.** Our starting data is an elliptic curve $E/\mathbb{Q}$, for which the BSD conjecture predicts that $\text{III}(E/\mathbb{Q})[p]$ is non-trivial. For the above construction to apply, we need to find a discriminant $D$ so that: $E(H)[p]$ is trivial, $p$ divides $|\text{Cl}(\mathcal{O})| = |H : K|$ exactly once, the rank of $E/\mathbb{Q}$ is 0, and the basic Heegner point $y_D$ is divisible by $p$ in $E(K)$. This is not difficult to do, as we now explain.
7.2. BACKGROUND ON HEEGNER POINTS AND KOLYVAGIN CLASSES

By an easy argument, see Lemma 4.3 of [Gro91], the first assumption holds if the Galois group \( \text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/p\mathbb{Z}) \), which we know is the case for all but finitely many \( p \), by a well known result of Serre. In practice, this condition will be met for most of the elliptic curves that are of interest to us i.e. those that do not admit a \( p \)-isogeny over \( \mathbb{Q} \).

The second condition is also easy to satisfy. For example, if we assume that \( \mathcal{O} = \mathcal{O}_K \), usually a naive search quickly finds a field \( K \) satisfying the Heegner condition, where \( p \) divides \( |\text{Cl}(K)| \) exactly once. The third condition is then often automatically satisfied, by the following famous result of Kolyvagin.

**Theorem 7.2.2** (Kolyvagin). Assume that the point \( y_D \) has infinite order in \( E(K) \). Then

1. The group \( E(K) \) has rank 1, so the index \( I_K = [E(K) : \mathbb{Z}y_D] \) is finite.

2. The group \( \text{III}(E/K) \) is finite, of order dividing \( t_{E/K}t_K^2 \). The number \( t_{E/K} \) is a positive integer whose prime factors depend only on the curve \( E \): they consist of 2 and the odd primes \( p \) where the Galois group of the extension of \( \mathbb{Q}(E[p])/\mathbb{Q} \) is smaller than expected.

For a proof, see Theorem 1.3 of [Gro91]. One can often use the above theorem to prove that \( p|I_K \), i.e. the point \( y_D \) is divisible by \( p \) in \( E(K) \).

**Remark 7.2.3.** The Kolyvagin classes we construct are slightly different from the ones used by Kolyvagin for the proof of his theorem, as explained in [Gro91], since we consider classes constructed using the Kolyvagin derivative \( D_\sigma \) for arbitrary \( \sigma \in \text{Gal}(H/K)[p] \). Essentially, we are able to do this because of the assumption that \( p|y_D \) in \( E(K) \). Our classes are closely related to those mentioned in §11 of [Gro91]. There Gross poses the question - what subgroup of \( \text{III}(E/Q) \) can be constructed from Kolyvagin classes? In this chapter we try to shed some light on this question by computing explicit examples.

**Descent to \( \mathbb{Q} \) and description of results.** Let \( \epsilon \) be the sign of the functional equation of \( E/Q \). The proof of Proposition 5.4 in [Gro91] shows that the class \( c \) lies in the \( \epsilon \)-eigenspace for the action of complex conjugation on \( H^1(K, E[p]) \). Thus, if \( E \) is a curve of rank 0, \( c \) is fixed by complex conjugation, and by the same inflation-restriction argument we naturally obtain an element of \( H^1(\mathbb{Q}, E[p]) \), which we will also call \( c \).

As \( E \) has no non-trivial \( p \)-torsion and rank 0, the group \( E(\mathbb{Q})/pE(\mathbb{Q}) \) is trivial, and hence if \( c \) is non-zero, its image \( d \) in \( H^1(K, E[p]) \) will be a non-trivial element of \( \text{III}(E/Q)[p] \). Tracing through the isomorphisms used to define \( c \), we see that the class \( c \) is non-zero if and only if the point \( P \) is not divisible by \( p \) in \( E(L) \).

As explained in Chapter 2, the class \( c \) can be represented by a \( p \)-diagram \([C \to \mathbb{P}^{p-1}]\). The main aim of this chapter is to describe a method to compute this diagram explicitly. We have succeeded in applying this method to concrete examples for \( p \leq 7 \) - see Section 7.6.

If the curve \( E \) has rank 1, then the class \( d \) is in the \((-1)\)-eigenspace of complex conjugation, and hence is obtained as the restriction of an element of \( \text{III}(E_D/Q)[p] \), where \( E_D \) is the quadratic twist of \( E \) by \( D \). If this quadratic twist has rank 0, then by the same argument, the class \( d \) is non-zero if and only if the class \( c \) is.

Our method applies in this case as well, and in fact we are able to compute an example with \( p = 11 \), i.e. a genus one normal curve \( C \subset \mathbb{P}^{10} \) that is a counter-example to the Hasse principle.
We suspect that $p$ could be increased even further - in this case, computing the Heegner point appears to be much easier. Note that in this case, as the Kolyvagin class is naturally an element of $\mathcal{I}_I$ for the quadratic twist of the curve we begin with, it seems difficult to use our method as a tool to compute the $\mathcal{I}_I(E/Q)[p]$ of a given curve $E$. See Section 7.6 for more details.

7.3 Geometric realization of the Kolyvagin class

7.3.1 The $n$-diagram associated to the Kolyvagin class

In this section we explain how to compute, given a Heegner point, equations for the $p$-diagram representing the Kolyvagin class. We first formalize the input we need from Heegner points.

Throughout this section, we fix the following data. Let $E/Q$ be an elliptic curve of rank 0, let $p$ be an odd prime and $K/Q$ be a quadratic field. In addition, let $L/Q$ be a dihedral extension, of degree $2p$, that contains $K$, such that $E(L)[p]$ is trivial.

**Proposition 7.3.1.** Let $P \in E(L)$ be a point such that the class $[P] \in E(L)/pE(L)$ is invariant under the action of $G = \text{Gal}(L/Q)$. Let $\delta : E(L)/pE(L) \to H^1(L, E[p])$ be the Kummer map, and let $\text{res} : H^1(Q, E[p]) \to H^1(L, E[p])$ be the restriction map.

Then there exists a unique class $c \in H^1(Q, E[p])$ such that $\text{res}(c) = \delta([P])$.

**Proof.** This is the inflation-restriction argument from the previous section.

The aim of this section is to give method to compute equations for the $p$-diagram representing the class $c$. This is accomplished by Galois descent, and involves explicit cocycle calculations. Let $\sigma \in G$ be an element of order $p$, and let $\tau \in G$ be an involution that fixes $K$.

**Lemma 7.3.2.** Suppose we are given $[P] \in (E(L)/pE(L))^G$ as in the previous proposition, and suppose that we also have $\tau(P) = P$. We then have the following.

(i) For each $g \in G$, there exists a unique $R_g \in E(L)$ with $pR_g = g(P) - P$. The map $g \mapsto R_g$ defines a cocycle in $H^1(G, E(L))$, meaning that for any $g, h \in G$ we have

$$R_{gh} = g(R_h) + R_g,$$

and for $k \in \mathbb{Z}$ we have the following identities:

$$\sum_{i=1}^{p} \sigma^i(R_\sigma) = 0_E,$$

$$R_{\sigma^k} = \sigma(R_{\sigma^{k-1}}) + R_\sigma = \sum_{i=1}^{k} \sigma^{i-1}(R_\sigma),$$

$$R_{\sigma^k\tau} = R_{\sigma^k},$$

and

$$\tau(R_{\sigma^k}) = R_{\sigma^{p-k}}.$$  

(ii) We have $[P] = [D_\sigma R_\sigma] = \sum_{i=1}^{p-1} i\sigma^i(R_\sigma) = [\sum_{i=1}^{p-1} R_{\sigma^i}] \in E(L)/pE(L).$
7.3. GEOMETRIC REALIZATION OF THE KOLYVAGIN CLASS

Proof. The fact that \([P]\) is invariant under \(G\) implies the existence of \(R_g\) with \(pR_g = g(P) - P\), and the uniqueness follows from the assumption that \(E(L)[p]\) is trivial. The cocycle condition (7.1) then follows from

\[ pR_{gh} = gh(P) - P = g(h(P) - P) + g(P) - P = pg(R_h) + pR_g = p(g(R_h) + R_g), \]

and (7.2) and (7.3) follow readily from (7.1). To prove identity (7.4), observe that as \(\tau(P) = P\) we have \(\sigma^k\tau(P) - P = \sigma^k(P) - P\). For (7.5), note that we have \(\sigma^{p^{-k}}\tau = \tau\sigma^k\), and compute:

\[ p \cdot \tau(R_{\sigma^k}) = \tau(\sigma^k(P) - P) = \sigma^{p^{-k}}\tau(P) - \tau(P) = \sigma^{p^{-k}}(P) - P = pR_{\sigma^{p^{-k}}}, \]

whence \(\tau(R_{\sigma^k}) = R_{\sigma^{p^{-k}}},\) as \(E(L)[p]\) is trivial.

We now turn to part (ii). Using (7.3), we compute

\[ \sum_{i=1}^{p-1} R_{\sigma^i} = \sum_{i=1}^{p-1} \sum_{j=1}^{i} \sigma^{j-1}(R_{\sigma^i}) = \sum_{i=1}^{p-1} i\sigma^i(R_{\sigma^i}). \]

Next, we prove \([P] = [D_\sigma R_g],\) i.e. that \(Q = P - D_\sigma R_{\sigma^i} \in pE(L)\). The identity \((\sigma - 1) \cdot D_\sigma = p - \sum_{i=1}^{p-1} \sigma^i\), together with (7.2), implies that \(\sigma(D_\sigma R_g) - D_\sigma R_{\sigma^i} = pR_g - \sum_{i=1}^{p-1} \sigma^i(R_{\sigma^i}) = pR_g\).

Applying (7.5), we compute \(\tau(D_\sigma R_g) = \tau(\sum_{i=1}^{p-1} R_{\sigma^i}) = \sum_{i=1}^{p-1} R_{\sigma^{p^{-1}}} = D_\sigma R_g\). Thus \(\sigma(Q) = \tau(Q) = Q\), and hence \(Q \in E(Q)\). But we have assumed that \(E(Q)\) is finite, so \(Q\) is a torsion point. As \(E(L)[p]\) is trivial, \(Q\) is not a nonzero \(p\)-torsion point, so the image of \(Q\) in \(E(L)/pE(L)\) is zero, and hence \([P] = [D_\sigma R_g]\), as desired. \(\Box\)

We now describe the \(p\)-diagram corresponding to \(c_L\) and the action of the Galois group on this diagram.

Proposition 7.3.3. (i) Consider the degree \(p\) divisor \(D\) on \(E\), defined by \(D = \sum_{i=1}^{p-1} R_{\sigma^i}\). The class \(c_L\) is represented by the torsor divisor class pair \((E, [D])\). Let \(l_1, ..., l_p\) be a basis of the space \(\mathcal{L}(D)\) and let \(E \xrightarrow{l} \mathbb{P}^{p-1}\) be the induced map. Then \([E \xrightarrow{l} \mathbb{P}^{p-1}]\) is the \(p\)-diagram representing \(c_L\).

(ii) The action of the Galois group \(G\) on the divisor \(D\) is given by

\[ g(\sum_{i=0}^{p-1} R_{\sigma^i}) = \tau_{R_g}(\sum_{i=0}^{p-1} R_{\sigma^i}), \]

(iii) For each \(g \in G\), the translation map \(\tau_{R_g}\) induces an isomorphism of torsor divisor class pairs \([E, D]\) and \([E, g(D)]\). In terms of diagrams, we have an isomorphism of diagrams \([E \xrightarrow{g\cdot l} \mathbb{P}^{p-1}]\) and \([E \xrightarrow{\tau_{R_g} \cdot l} \mathbb{P}^{p-1}]\), represented by a commutative diagram

\[ \begin{array}{ccc}
E & \xrightarrow{g\cdot l} & \mathbb{P}^{p-1} \\
\tau_{R_g} \downarrow & & \downarrow M_g \\
E & \xrightarrow{\tau_{R_g} \cdot l} & \mathbb{P}^{p-1}
\end{array} \]

with \(M_g \in \PGL_p(L)\). The map \(g \mapsto M_g\) determines a cocycle in \(H^1(G, \PGL_p(L))\).
Proof. By Lemma \ref{lem:brauer}(ii), we have \([\text{sum}(D)] = [D_\sigma \cdot R_\sigma] = [P] \in E(L)/pE(L).\) Then part (i) follows from the discussion at the end of Section 2.1. For part (ii), by equations (7.3) and (7.5) we have

\[
\sigma\left(\sum_{i=0}^{p-1} R_{\sigma^i}\right) = \tau_{R_g}^{-1} \left(\sum_{i=0}^{p-1} R_{\sigma^i}\right),
\]

and

\[
\tau\left(\sum_{i=0}^{p-1} R_{\sigma^i}\right) = \left(\sum_{i=0}^{p-1} R_{\sigma^i}\right).
\]

The cocycle condition for \(g \mapsto R_g\) implies the result for all \(g \in G\). The isomorphism of torsor divisor class pairs in (iii) then follows from (ii).

To see the isomorphism of \(p\)-diagrams in (iii), note that by (ii) we have \(\tau_{R_g}^{-1}(D) = g(D)\), and that \(g(l_1), \ldots, g(l_p)\) and \(\tau_{R_g}(l_1), \ldots, \tau_{R_g}(l_p)\) are two bases of \(\mathcal{L}(g(D))\). We can then take \(M_g\) to be the matrix taking one base to the other. Finally, to see that \(g \mapsto M_g\) is a cocycle, let \(C_L\) be the image of \(E\) in \(\mathbb{P}^{p-1}\). \(C_L\) is a genus one normal curve of degree \(p\), so in particular it spans \(\mathbb{P}^{p-1}\), and \(M_g\) restricted to \(C_L\) is equal to \(\tau_{R_g}\). As \(g \mapsto \tau_{R_g}\) is a cocycle, we deduce that \(M_{gh} = g(M_h)M_g\) holds on \(C_L\), and as \(C_L\) spans \(\mathbb{P}^{p-1}\) and \(M_g\) is an automorphism of \(\mathbb{P}^{p-1}\), it must hold on the entire \(\mathbb{P}^{p-1}\).

\(\square\)

Remark 7.3.4. In fact, we will later see that if we choose matrices \(M_g\) as in the proof, then \(g \mapsto M_g\) determines a cocycle in \(H^1(G, GL_p(L))\), not just in \(H^1(G, \text{PGL}_p(L))\). This choice of scaling can be interpreted as explicitly showing that the obstruction of the class \(c \in H^1(Q, E[p])\) in the Brauer group \(\text{Br}(Q)\) is zero, and that hence \(c\) may be represented by a \(p\)-diagram \([C \to \mathbb{P}^{p-1}]\).

Let \(C_L\) be the image of \(E\) under \(l\). From the above diagram, we see that that \(g(C_L) = M_g(C_L)\). Assuming that we have lifted \(g \mapsto M_g\) to a cocycle valued in \(GL_p(L)\), by Hilbert’s Theorem 90 \(H^1(G, GL_p(L))\) is trivial, and so \(g \mapsto M_g\) is a coboundary. Thus there exists \(B \in \text{PGL}_p(L)\) with \(M_g = Bg(B^{-1})\). If we set \(C = B^{-1}(C_L)\), the curve \(C\) will be stable under the action of \(\text{Gal}(L/Q)\), hence defined over \(Q\), and the diagram \([C \to \mathbb{P}^{n-1}]\) represents the Kolyvagin class \(c \in H^1(Q, E[p])\).

We wish to find explicit equations defining \(C\). To do this, we need to find the matrices \(M_g\) explicitly, and then solve for the matrix \(B\).

7.3.2 Computing the matrices \(M_g\)

In this section, we assume that we have explicitly computed the points \(R_{g}\), and explain how to compute the matrices \(M_g\) from them. Throughout this section we assume that the points \(R_{\sigma}\), are pairwise distinct - it is easy to see that this assumption holds if the class \([P] \in E(L)/pE(L)\) is non-trivial.

We begin by fixing an explicit basis of \(\mathcal{L}(D)\). From now on, to make the formulas simpler, we will assume \(E\) is in short Weierstrass form, defined by \(y^2 = x^3 + Ax + B\). Let \(R_g = (x_g, y_g)\) for each \(g \in G\). Define \(l_k = \frac{y_{g_{k+1}} - y_{g_k}}{x_{g_{k+1}} - x_{g_k}}\) for \(1 \leq k \leq p - 1\), and set \(l_p = 1\).

For \(k < p\), it is clear that \(l_k\) has a simple pole at \(0_E\). We note that it has a simple pole at \(R_{\sigma}\), and no other poles. Indeed, \(x - x_{g_{k+1}}\) is of degree two and vanishes at \(R_{g_k}\) and \(-R_{g_k}\), and \(y + y_{R_{\sigma}}\)
vanishes at \(-R_\alpha\). Now it follows easily that \(l_k \in \mathcal{L}(D)\), and furthermore that \(l_1, l_2, \ldots, l_{p-1}, l_p\) are linearly independent, and so they span the \(p\)-dimensional space \(\mathcal{L}(D)\).

The diagram (7.6) determines the matrices \(M_g\), up to a scalar in \(L^*\), as follows:

\[
M_g \begin{pmatrix} g(l_1) \\ g(l_2) \\ \vdots \\ g(l_p) \end{pmatrix} = f_g \begin{pmatrix} \tau^*_{R_g}(l_1) \\ \tau^*_{R_g}(l_2) \\ \vdots \\ \tau^*_{R_g}(l_p) \end{pmatrix},
\]

where \(f_g\) is a rational function with \(\text{div}(f_g) = g(D) - \tau^*_{-R_g}(D)\). By Proposition 7.3.3(ii), we in fact have \(g(D) - \tau^*_{-R_g}(D) = 0\), and hence the function \(f_g\) is constant. We fix the scaling of the matrix \(M_g\) by requiring that

\[
M_g \begin{pmatrix} g(l_1) \\ g(l_2) \\ \vdots \\ g(l_p) \end{pmatrix} = \begin{pmatrix} \tau^*_{R_g}(l_1) \\ \tau^*_{R_g}(l_2) \\ \vdots \\ \tau^*_{R_g}(l_p) \end{pmatrix},
\]

(7.7)

For any two elements \(g, h \in G\), we have

\[
M^{-1}_g \cdot \tau^*_{gh} = M^{-1}_g \cdot \tau^*_{g(R_h)} = M^{-1}_g \cdot \tau^*_{g(R_h) + R_g} = g(M^{-1}_h) \cdot \tau^*_{(R_h) + R_g} = g(M^{-1}_h) \cdot \tau^*_{g(R_h) + R_g} = g(M^{-1}_h) \cdot \tau^*_{g(R_h)} = g(M^{-1}_h) \cdot \tau^*_{g(R_h)} = g(M^{-1}_h) \cdot \tau^*_{g(R_h) + R_g}.
\]

As \(g \rightarrow R_g\) is a cocycle, we have \(g(R_h) + R_g = R_{gh}\). Since \(l_1, l_2, \ldots, l_p\) is a basis of \(\mathcal{L}(D)\), we deduce \(g(M^{-1}_h) M^{-1}_g = M^{-1}_{gh}\), i.e. \(M_{gh} = M_g \cdot g(M_h)\). Hence \(g \rightarrow M_g\) is a cocycle valued in \(\text{GL}_p(L)\), not just \(\text{PGL}_p(L)\), as promised before.

We next turn to giving explicit expressions for the matrices \(M_g\), in terms of the coordinates of the points \(R_g\). It suffices to compute \(M_\sigma\) and \(M_\tau\), as \(\sigma\) and \(\tau\) generate \(G\).

**Proposition 7.3.5.** The matrix \(M_\sigma\) is given by

\[
M_\sigma = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -1 & 0 \\ 1 & 0 & 0 & \ldots & 0 & -1 & c_2 \\ 0 & 1 & 0 & \ldots & 0 & -1 & c_3 \\ 0 & 0 & 1 & \ldots & 0 & -1 & c_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -1 & c_{p-1} \\ 0 & 0 & 0 & \ldots & 0 & 0 & 1 \end{pmatrix},
\]
where \( c_k = \frac{y_{\sigma}^k + y_{\sigma}k}{x_{\sigma} - x_{\sigma}^k} \) for \( 2 \leq k \leq p - 1 \). The matrix \( M_\sigma \) is given by

\[
M_\sigma = \begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & 1 & 0 \\
0 & 0 & 0 & \ldots & 1 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 1 & 0 & \ldots & 0 & 0 & 0 \\
1 & 0 & 0 & \ldots & 0 & 0 & 0 \\
0 & 0 & 0 & \ldots & 0 & 0 & 1 \\
\end{pmatrix}.
\]

To prove this assertion, we will make use of the following general lemma.

**Lemma 7.3.6.** Let \( E \) be an elliptic curve over a field \( k \). For any \( P \in E(k) \), let \( l_P = \frac{y_P + y_{\sigma}}{x_P - x_{\sigma}} \in k(E) \). Let \( P_1, P_2 \in E(k) \) be points such that \( P_1 \neq -P_2 \) and consider the rational function defined by \( f_{P_1, P_2} = \frac{\tau_{P_2}(l_{P_1 + P_2})}{l_{P_1}} \in k(E) \). Then \( f_{P_1, P_2} \) is regular at \( P_1 \) and we have \( f_{P_1, P_2}(P_1) = 1 \).

In addition, for any \( R \in E(k) \), we have \( \tau_{R}(l_{R}) = -1 \).

**Proof.** It is clear that \( f \) is regular at \( P_1 \). We can thus define a rational function \( g \in k(E) \) by the rule \( P \to f_{P, P}(P_1) \). As \( \frac{y_P + y_{\sigma}}{x_P - x_{\sigma}} \) has a simple pole at \( P_1 + P_2 \), \( \tau_{P_2}(\frac{y_P + y_{\sigma}}{x_P - x_{\sigma}}) \) has a simple pole at \( P_1 \), and therefore \( g \) is regular with no zeros on the open set \( E \setminus \{ P_1 \} \). But the only such rational function is the constant one, and as it is clear that \( g(0_E) = 1 \), we deduce \( g = 1 \), and \( f_{P_1, P_2}(P_1) = 1 \) as desired.

To prove the second assertion, note that both \( \tau_{R}(l_{R}) + l_{-R} \) have simple poles at \(-R\) and \(0_E\). The Riemann-Roch space \( \mathcal{L}((0_E) + (-R)) \) is 2-dimensional, and therefore there exists a \( c_R \in k \) such that \( \tau_{R}(l_{R}) + c_R l_{-R} \) is a constant function, i.e. the function on \( E \times E \)

\[
y_P + y_R + c_R \frac{y_P - y_R}{x_P - x_R},
\]

depends only on \( R \), and so can be viewed as a rational function on \( E \). It is clearly regular on \( E \setminus \{0_E\} \), and therefore it must be constant. Letting \( R \) tend to \( 0_E \), the terms \( y_R \) and \( x_R \) tend to infinity, while the other remain bounded, so we deduce that \( c = 1 \), as otherwise there would be a pole at \( 0_E \). \( \square \)

We first compute the matrix \( M_\sigma \). Observe that \( R_{\sigma^{p-2}} = \sum_{i=0}^{p-2} \sigma^i(R_\sigma) = -\sigma^{p-1}(R_\sigma) \) and that \( \sigma(R_{\sigma^k}) = R_{\sigma^{k+1}} - R_\sigma \). Also note that as \( l_p = 1 \), we have \( \sigma(l_p) = \tau_{R_\sigma}^*(l_p) = 1 \), giving the last row of \( M_\sigma \). The proposition amounts to proving that for \( 1 \leq k \leq p - 2 \) we have

\[
\tau_{R_\sigma}^*(l_{k+1}) = \sigma(l_k) - \sigma(l_{p-1}) + c_k l_p,
\]
as well as

\[
\tau_{R_\sigma}^*(l_1) = -\sigma(l_{p-1}).
\]

Suppose first that \( k < p - 1 \). Note that \( \tau_{R_\sigma}^*(l_{k+1}) \) has simple poles at \( R_{\sigma^{k+1}} - R_\sigma = \sigma(R_{\sigma^k}) \) and \(-R_\sigma \), \( \sigma(l_k) \) has simple poles at \( \sigma(R_{\sigma^k}) \) and \( 0_E \), and \( \sigma(l_{p-1}) \) has simple poles at \( \sigma(R_{\sigma^{p-1}}) = -R_\sigma \) and \( 0_E \).
7.3. GEOMETRIC REALIZATION OF THE KOLYVAGIN CLASS

Hence the function \( \frac{\tau_{R_\sigma}(l_{k+1})}{\sigma(l_k)} \) is regular at the point \( \sigma(R_{\sigma^k}) \). By Lemma 7.3.6, taking \( P_1 = \sigma(R_{\sigma^k}) = R_{\sigma^{k+1}} - R_\sigma \) and \( P_2 = -R_\sigma \), we see that \( \frac{\tau_{R_\sigma}(l_{k+1})}{\sigma(l_k)}(\sigma(R_{\sigma^k})) = 1 \). As a consequence we see that the function \( \tau_{R_\sigma}(l_{k+1}) - \sigma(l_k) \) is regular at \( \sigma(R_{\sigma^k}) \). We next observe that \( \sigma(l_k) - \sigma(l_{p-1}) \) is regular at \( 0_E \), and in fact \( \sigma(l_k - l_{p-1})(0_E) = 0 \), as

\[
l_k - l_{p-1} = \frac{y + y_{\sigma^k}}{x - x_{\sigma^k}} - \frac{y + y_{\sigma^{p-1}}}{x - x_{\sigma^{p-1}}} = \frac{(y_{\sigma^k} + y_{\sigma^{p-1}})x - (x_{\sigma^k} + x_{\sigma^{p-1}})y - (y_{\sigma^k} x_{\sigma^{p-1}} + x_{\sigma^k} y_{\sigma^{p-1}})}{(x - x_{\sigma^k})(x - x_{\sigma^{p-1}})}.
\]

(7.8)

The numerator has a pole of order 3 at \( 0_E \), the denominator has pole of order 4, so \( l_k - l_{p-1} \) vanishes at \( 0_E \), and hence so does \( \sigma(l_k - l_{p-1}) \).

We thus see that the rational function \( \tau_{R_\sigma}^*(l_{k+1}) - \sigma(l_k) + \sigma(l_{p-1}) \) has no poles except perhaps a simple one at \( -R_\sigma \), and therefore must be the constant \(-c_k\). By evaluating at \( 0_E \), we find that

\[
c_k = -(\tau_{R_\sigma}^*(l_{k+1}) - \sigma(l_k) + \sigma(l_{p-1})) = -(\tau_{R_\sigma}^*(l_{k+1}))(0_E) = -l_{k+1}(R_\sigma) = -\frac{y_{\sigma^k+1} + y_\sigma}{x_\sigma - x_{\sigma^k+1}}.
\]

as desired. To prove that \( \sigma(l_{p-1}) = -\tau_{R_\sigma}^*(l_1) \), note that in the notation of Lemma 7.3.6, \( \sigma(l_{p-1}) = l_{-R_\sigma} \), and \( l_1 = l_{R_\sigma} \), and so we are done by the final assertion of Lemma 7.3.6.

The computation of \( M_\tau \) is simpler. Note that \( R_\tau = 0_E \), and so the last row of \( M_\tau \) is the assertion that \( \tau(l_p) = l_p = 1 \). For the other rows, we need to show that \( \tau(l_k) = l_{p-k} \). This follows from the identity \( \tau(R_{\sigma^p}) = R_{\sigma^{p-k}} \), which is the content of (7.5).

The cocycle condition determines the other \( M_g \) as follows: \( M_{g^k} = M_g \sigma(M_g) \cdots \sigma^{k-1}(M_g) \), and \( M_{g^{k+1}} = M_{g^k} M_{\tau} \). We now explain how to solve for a choice of coordinates that yields a curve defined over \( \mathbb{Q} \).

**Proposition 7.3.7.** (i) Consider the \( L \)-vector space \( L(D) \). The cocycle \( M_g \) determines a semilinear action of \( G = \text{Gal}(L/\mathbb{Q}) \) on \( L(D) \), with \( g \in G \) acting via the matrix \( M_g^{-1} \), with respect to the basis \( l_1, l_2, ..., l_p \).

(ii) Now consider the induced action of \( G \) on \( \mathbb{P}^{p-1} = \mathbb{P}(L(D)) \). Denote the image of \( E \) in \( \mathbb{P}^{p-1} \) under the map \( \mathbb{P} \to [l_1(P) : l_2(P) : ... : l_p(P)] \) by \( C_L \). For all \( g \in G \), \( g(C_L) \) is the image of \( E \) under the map \( \mathbb{P} \to [g(l_1)(P) : g(l_2)(X) : ... : g(l_p)(P)] \).

(iii) The set of invariant elements \( L(D)^G \) is a \( p \)-dimensional \( \mathbb{Q} \)-vector subspace of \( L(D) \). We have \( L(D) \cong L(D)^G \otimes_{\mathbb{Q}} L \), i.e. \( L(D) \) has a basis of \( G \)-invariant vectors. Furthermore, let \( \alpha_1, \alpha_2, ..., \alpha_{2p} \) be a basis of \( L \) over \( \mathbb{Q} \). Then \( L(D)^G \) is spanned by the elements \( \sum_{g \in G} g(\alpha_i l_j) \) for \( 1 \leq i \leq 2p, 1 \leq j \leq p \).

(iv) Let \( i_1^Q, i_2^Q, ..., i_p^Q \) be a \( G \)-invariant basis of \( L(D) \). Then the image \( C_Q \) of \( E \) under the embedding \( X \to [i_1^Q(X) : i_2^Q(X) : ... : i_p^Q(X)] \) can be defined over \( \mathbb{Q} \), i.e. the ideal defining \( C_Q \) as a projective curve has a basis consisting of polynomials with rational coefficients.

The Brauer-Severi diagram \( C_Q \to \mathbb{P}^{p-1} \) represents the Kolyvagin class \( c \).

**Proof.** (i) and (ii): Recall that a semilinear action of \( \text{Gal}(L/\mathbb{Q}) \) on an \( L \)-vector space \( V \) is a
the height of the curve $E$ small in a certain sense, e.g. it is possible to bound the coefficients of the equations in terms of $C$. The last section will result in equations for that have very large coefficients. We know from the general theory of genus one models of elliptic curves that there exists a model of $C_Q$ which is small in a certain sense, e.g. it is possible to bound the coefficients of the equations in terms of the height of the curve $E$, and the model will have good reduction at all the places where $E$ has good reduction.

There is a heuristic explanation why this will not be the case for the model of $C_L$ obtained from the basis $l_1, l_2, \ldots, l_p$. Let $p$ be a prime of $L$ for which $E$ has good reduction, and the reductions of two points in the support of $D$ are the same, say $\text{red}_p(R_\sigma) = \text{red}_p(R_{\sigma^2})$. Let $C_L$ denote the images of the embedding $i : E \to \mathbb{P}^{p-1}$ given by $Q \mapsto [l_1(Q) : l_2(Q) : \ldots : l_p(Q)]$.

If $C_L$ admits a nice model, defined over the ring of integers $\mathcal{O}_L$, with good reduction properties, it is reasonable to expect that the map $i$ also behaves nicely, and reduces to an embedding $\widetilde{E} \to \mathbb{P}^{p-1}$ of the reduction of $E$ mod $p$. Then, the images of $R_\sigma$ and $R_{\sigma^2}$ would reduce to the same point. However, one can quickly compute that $R_\sigma$ and $R_{\sigma^2}$ map to the points
(1 : 0 : 0... : 0) and (0 : 1 : 0 : ... : 0), and so their reductions mod \( p \) are also given by (1 : 0 : 0... : 0) and (0 : 1 : 0 : ... : 0). Thus we expect \( C_L \) to be singular at any such \( p \), and as Heegner points in our examples tend to have large height, the resulting equations will be very complicated, i.e. they could take many pages to write down.

To deal with this issue we need to make a careful choice of the basis \( \tilde{f}_1^0, \tilde{f}_2^0, \ldots, \tilde{f}_p^0 \) of \( \mathcal{L}(D) \). Essentially, the idea is to do the linear algebra of Proposition 7.3.7 over \( \mathbb{Z} \). Proposition 7.4.6 explains how to do this and gives a sense in which the resulting model will be nice. In Section 7.4.1 we give an account of the general theory of minimal genus one models and explain the sense in which the model constructed in Proposition 7.4.6 is minimal.

Let us explain what we mean by an integral model. Let \( R \) be an integral domain and let \( K \) be the field of fractions of \( R \).

**Definition 7.4.1.** An integral model \( C_R \) of a genus one normal curve \( C_K \) of degree \( n \geq 4 \) is a set of quadrics \( f_1, \ldots, f_{n(n-3)/2} \in R[x_1, \ldots, x_n] \), that generate the ideal \( I \) that defines \( C_K \) in \( \mathbb{P}^{n-1} \).

If \( n = 3 \), then an integral model is a ternary cubic \( F \in R[x_1, x_2, x_3] \) that generates \( I \).

**Definition 7.4.2.** Let \( C \) be an integral model as above. For a prime \( p \) of \( R \), with the residue field \( k_p \), we define the reduction of \( C \) modulo \( p \) to be the curve \( C_p \subset \mathbb{P}^{n-1}_{k_p} \) defined by the reductions \( \tilde{f}_1, \ldots, \tilde{f}_{n(n-3)/2} \). We say \( C \) has good reduction at \( p \) if \( C_p \) is a genus one normal curve of degree \( n \) over \( k_p \).

**Remark 7.4.3.** These definitions can also be formulated in the language of resolution models developed in Chapter 3.

Assume now, for simplicity, that \( L \) is a number field of class number one. This assumption holds in most examples we were able to compute.

**Lemma 7.4.4.** Let \( V \) be an \( n \)-dimensional \( L \)-vector space and let \( W \leq V \) be a subspace of dimension \( m \). Let \( e_1, \ldots, e_n \) be a basis of \( V \), and let \( S \) be a free \( \mathcal{O}_L \)-module with the basis \( e_1, \ldots, e_n \). Let \( T = W \cap S \). Then \( T \) is a free \( \mathcal{O}_L \)-module of rank \( m \), and there exists a basis \( g_1, \ldots, g_m \) of \( S \) such that \( g_1, \ldots, g_m \) is a basis of \( T \).

**Proof.** \( T \) is a submodule of a free \( \mathcal{O}_L \)-module, and \( \mathcal{O}_L \) is a PID, so \( T \) is a free \( \mathcal{O}_L \)-module. As \( T \otimes_{\mathcal{O}_K} L \cong W \), \( T \) has rank \( m \). By the theorem on Smith Normal Form, there exists a basis \( g_1, \ldots, g_n \) of \( S \) and \( s_1, \ldots, s_m \in \mathcal{O}_L \) such that \( s_1g_1, \ldots, s_m g_m \) is a basis of \( T \). But we have defined \( T \) as \( S \cap W \), thus \( s_i \in \mathcal{O}'_L \), and we may assume \( s_i = 1 \) for every \( i \), proving the claim.

Let us now go back to the setup of Section 7.3.1. We have an elliptic curve \( E \), a dihedral extension \( L/\mathbb{Q} \) of degree \( 2p \), and a point \( P \) satisfying the conditions of Lemma 7.3.2. Fix an integral Weierstrass equation \( W \) of \( E \),

\[
y^2 + a_1 xy + a_3y = x^3 + a_2 x^2 + a_4 x + a_6.
\]

and let \( \mathcal{E} \) be the scheme over \( \mathbb{Z} \) defined by the equation \( W \).

Let \( D' \) be the divisor \((2p-1) \cdot 0_E - (-R_\sigma) - \ldots - (-R_{p-1}) \). As \( \text{sum}(D') = \text{sum}(D) \) and both \( D' \) and \( D \) have degree \( p \), we have \([D] = [D'] \) in \( \text{Pic}(E) \), and the Kolyvagin class \( c_L \in H^1(L, E[p]) \).
is represented by the torsor divisor class pair \((E, [D'])\). A choice of a rational function \(f\) with \(\text{div}(f) = D - D'\) determines an isomorphism between the vector spaces \(\mathcal{L}(D)\) and \(\mathcal{L}(D')\), and we transport the action of \(G\) to \(\mathcal{O}_E(D')\) via such an isomorphism. We can naturally view \(\mathcal{L}(D')\) as a subspace of \(\mathcal{O}_E((2p-1) \cdot 0_E)\) that consists of functions that vanish at \(R_{\sigma}, R_{\sigma^2}, ..., R_{\sigma^{p-1}}\).

Note that \(1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y\) is a basis of \(\mathcal{L}((2p-1) \cdot 0_E)\). Let \(S \subset \mathcal{L}((2p-1) \cdot 0_E)\) be the free \(\mathcal{O}_L\)-module spanned by \(1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y\) and let \(T = S \cap \mathcal{L}(D')\). As \(\mathcal{O}_L\) is a principal ideal domain, \(T\) is a free \(\mathcal{O}_L\)-module of rank \(p\).

**Lemma 7.4.5.** Let \(g_1, ..., g_p\) be a basis of \(T\), and let \(C\) be the image of \(E\) under the associated embedding \(E \xrightarrow{\varphi} \mathbb{P}^{p-1}\). Then there exists an integral model \(\mathcal{C}\) of \(C\), with good reduction at all primes that do not divide the discriminant of the Weierstrass equation \(W\).

**Proof.** If \(p > 3\), let \(V\) be the \(p(p-3)/2\)-dimensional \(K\)-vector space of quadrics that vanish on \(C\), and choose a basis \(g_1, ..., g_{p(p-3)/2}\) of the free \(\mathcal{O}_L\)-submodule of integral elements of \(V\). We take \(\mathcal{C}\) to be the integral model of \(C\) defined by this basis. If \(p = 3\), we define \(\mathcal{C}\) in a similar way, taking \(V\) to be the 1-dimensional space of cubics that vanish on \(C\).

Let \(\mathcal{E}\) be scheme over \(\mathcal{O}_L\) defined by the Weierstrass equation. The isomorphism \(E \to C\) extends to a morphism \(\mathcal{E} \to C_{\mathcal{O}_L}\), as \(g_i\) can be expressed as integral linear combinations of \(1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y\).

Let \(\mathfrak{p}\) be a prime of \(\mathcal{O}_L\) that does not divide the discriminant of \(W\), and let \(k\) be the residue field \(\mathcal{O}_L/\mathfrak{p}\). Let \(\tilde{E}\) and \(\tilde{C}\) be the reductions of \(E_{\mathcal{O}_L}\) and \(C_{\mathcal{O}_L}\) mod \(\mathfrak{p}\). We claim that the morphism \(\mathcal{E}_{\mathcal{O}_L} \to C_{\mathcal{O}_L}\) reduces to an isomorphism \(\tilde{E} \to \tilde{C}\).

The morphism \(\tilde{E} \to \tilde{C}\) is induced by the reductions \(\tilde{g}_1, \tilde{g}_2, ..., \tilde{g}_p \in \mathcal{O}_{\tilde{E}}(\tilde{D'})\). By Lemma 3.3, the basis \(g_1, ..., g_p\) of \(S'\) can be extended to a basis \(g_1, g_2, ..., g_{2p-1}\) of \(S\), and there exists a matrix \(A \in \text{GL}_{2p-1}(\mathcal{O}_L)\) taking \(1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y\) to \(g_1, g_2, ..., g_p\). The reductions of \(1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y\) form a basis of \(\mathcal{O}_{\tilde{E}}((2p-1) \cdot 0_{\tilde{E}})\), and the matrix \(\tilde{A} \in \text{GL}(k)\) takes \(1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y\) to \(\tilde{g}_1, \tilde{g}_2, ..., \tilde{g}_{2p-1}\). We deduce that \(\tilde{g}_1, \tilde{g}_2, ..., \tilde{g}_p\) are linearly independent, proving the claim.

We claim that \(\tilde{C}\) is the special fiber of \(C\) at \(\mathfrak{p}\). Indeed, by the above, \(\tilde{C}\) is a genus one normal curve, and is therefore defined by \(p(p-3)/2\) quadrics if \(p > 3\). The special fiber \(\tilde{C}\) is defined by \(p(p-3)/2\) quadrics if \(p > 3\), and therefore must be the same as \(\tilde{C}\). A similar argument applies if \(p = 3\), finishing the proof.

By Proposition 7.3.3, the action of \(G\) on \(\mathcal{L}(D')\) restricts to an action on the \(\mathcal{O}_L\)-submodule \(T\), and the set of invariant elements \(T^G\) is a free \(\mathbb{Z}\)-module of rank \(p\).

**Proposition 7.4.6.** Let \(f_1, f_2, ..., f_p\) be a basis of \(T^G\). Let \(C\) be the image of \(E\) under the embedding determined by the functions \(f_1, ..., f_p\). Then

(i) \(C\) is a genus one normal curve defined over \(\mathbb{Q}\), and the diagram \(C \to \mathbb{P}^{p-1}\) represents the Kolyvagin class \(c\).

(ii) Let \(C_q\) be the integral model of \(C\). Then the reduction \(C_q\) of \(C\) modulo any prime \(q\) that does not divide the discriminant of the Weierstrass equation \(W\) of \(E\) and the discriminant of \(L\), is a genus one normal curve of degree \(p\) over \(\mathbb{F}_q\). In particular \(C_{\mathfrak{p}}\) is nonsingular.
Proof. (i) is a restatement of Proposition 7.3.3.

For (ii), consider the embedding $E \to \mathbb{P}^{p-1}$ defined by an $\mathcal{O}_L$-basis $g_1, \ldots, g_p$ of $T$, as in Lemma 3.4. Let the image of $E$ be a genus one normal curve $C_L$. Let $\mathcal{E}_{\mathcal{O}_L}$ be the $\mathcal{O}_L$-scheme defined by the Weierstrass equation $W$ and let $\mathcal{C}_{\mathcal{O}_L}$ be the integral model of $C_L$.

Next, let $q \in \mathbb{Z}$ be a prime that satisfies the conditions of (ii), and let $q$ be a prime of $\mathcal{O}_L$ above $q$. Let $L_q$ be the completion of $L$ at $q$ and $\mathcal{O}_q$ be the ring of integers of $L$. Let $\mathcal{C}_q$ and $\mathcal{C}_{q,L}$ be the schemes over $\mathcal{O}_q$ obtained from base change of $\mathcal{C}_\mathbb{Z}$ and $\mathcal{C}_{\mathcal{O}_L}$. We claim that $\mathcal{O}_q \cdot T^G = \mathcal{O}_q \cdot T$.

This implies that there exists a $B \in \text{GL}(\mathcal{O}_p)$ taking $g_1, \ldots, g_p$ to $f_1, \ldots, f_p$, and hence that there is an isomorphism of $\mathbb{P} \mathcal{O}_q$ taking $\mathcal{C}_{q,L}$ to $\mathcal{C}_q$. By Lemma 3.4, $\mathcal{C}_{q,L}$ has good reduction at $q$, and therefore so does $\mathcal{C}_q$. It is then clear that $\mathcal{C}_\mathbb{Z}$ has good reduction at $q$, as desired.

As $T^G \subset T$, we have $\mathcal{O}_q \cdot T^G \subset \mathcal{O}_q \cdot T$. Let $1 = \alpha_1, \ldots, \alpha_{2p}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_L$, and let $t \in T$. For $1 \leq i \leq 2p$, consider the $G$-invariant elements
\[
t^G_i = \sum_{g \in G} g(\alpha_i t) = \sum_{g \in G} g(\alpha_i) g(t).
\]

Let $G = \{\text{id} = g_1, g_2, \ldots, g_{2p}\}$, and consider the matrix $M = (g_i(\alpha_j))_{1 \leq i, j \leq 2p}$. As $\det(A)^2 = \text{Disc}(L)$ and $q$ does not divide $\text{Disc}(L)$, we have $M \in \text{GL}(\mathcal{O}_q)$. From the identity
\[
M \cdot \begin{pmatrix}
g_1(t) \\
g_2(t) \\
\vdots \\
g_{2p}(t)
\end{pmatrix} = \begin{pmatrix}
t^G_1 \\
t^G_2 \\
\vdots \\
t^G_{2p}
\end{pmatrix},
\]
we conclude that $t \in \mathcal{O}_q \cdot T^G$, proving the claim. 

Remark 7.4.7. One can generalize Proposition 7.4.6 to the case where the class group of $L$ is not necessarily trivial. The same argument will show that the integral model defined by a basis of $S^G$ has good reduction away from the primes dividing the discriminant of $E$, the discriminant of $L$, and the finite set of primes we need to invert to make the class group trivial.

Furthermore, we expect that the resulting model actually has good reduction at all primes except those that divide the discriminant of $E$, and is in fact a globally minimal model, in the sense of Theorem 4.1.1. This occurs in all of the examples we computed in Section 7.6. We hope to investigate this question further in future work.

7.4.1 Minimal genus one models

In this section we explain the connection between the $p$-diagram constructed in the previous section and the theory of resolution models studied in Chapter 3 and Chapter 4.

Suppose that $\mathcal{O}_K$ is a principal ideal domain, with field of fractions $K$. Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n$, defined over $K$, for some odd integer $n$. The following proposition gives an algorithm to compute the change of coordinates taking $C$ to a curve admitting a minimal resolution model, in the case when $C$ admits a $K$-rational point.
Proposition 7.4.8. (i) Let $E/K$ be an elliptic curve with an integral Weierstrass equation $W$

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$ 

Then the embedding $i : E \to \mathbb{P}^{n-1}$ determined by the basis $1, x, y, x^2, xy, \ldots, x^{n-1}, x^{n-3} y$ of $L(n \cdot 0_E)$ defines a genus one normal curve $C$ that admits a minimal genus one model of degree $n$ with respect to $W$. The embedding $E \to \mathbb{P}^{n-1}$ corresponds to the torsor divisor class pair $(E, [n \cdot 0_E])$. We define the space of integral linear forms to be the free $\mathcal{O}_K$-module with the basis $1, x, y, x^2, xy, \ldots, x^{n-1}, x^{n-3} y$.

(ii) Let $P_1, P_2, \ldots, P_k \in E(K)$ be distinct rational points, with $k < n$, and let $V$ be the $\mathcal{O}_K$-module of integral linear forms that vanish at $i(P_1), \ldots, i(P_k)$. Then, as the class group of $K$ is trivial, $V$ is a free $\mathcal{O}_K$-module of rank $n-k$, and the image $C$ of $E$ under the embedding determined by a basis $l_0, \ldots, l_{n-1}$ of $V_P$ is a genus one normal curve of degree $n-k$ that admits a minimal genus one model of degree $n-k$ with respect to $W$. The embedding $E \to \mathbb{P}^{n-k}$ corresponds to the torsor divisor class pair $(E, [n \cdot 0_E - P_1 - P_2 - \ldots - P_k])$.

Proof. This is a restatement of the local minimization result, Theorem 4.7.1. Note that we have proven local minimization theorem over the ring of $p$-adic integers, but it is clear that the same proof applies to any principal ideal domain.

Definition 7.4.9. Let $C$ be an integral genus one model of a curve $C$, with the Jacobian of $C$ given by an integral Weierstrass model $W$. We say $C$ is minimal at a prime $p$ if we have $v_p(c_k(C)) = v_p((n-2)^k c_k(W))$, where $v_p$ is the valuation of $K$ associated to $p$. If this holds for every prime $p$ of $\mathcal{O}_K$, we say $C$ is globally minimal.

The argument used in the proof of Proposition 7.4.6, together with Proposition 7.4.8, proves the following statement.

Proposition 7.4.10. Let $C$ be the genus one model of the $p$-diagram $[C \subset \mathbb{P}^{n-1}]$ that represents the Kolyvagin class $c$, constructed in Proposition 7.4.6. $C$ is minimal at all primes that do not divide discriminant of $L$.

Remark 7.4.11. As in Proposition 7.4.6, we suspect that the model constructed will also be minimal at the primes dividing the discriminant of $L$, and hence globally minimal. This has been the case in the examples we were able to compute, and can be proved for $p = 5$ and $p = 3$ using the results of [Sad10] and [FS14]. We hope to extend these arguments to all $p$ in future work.

7.4.2 Practical computation of a minimal model

In this section we explain how to compute a minimal model for a Kolyvagin class $c_Q$, assuming that we have are given a Heegner point representing the class $c_Q$. The proofs of results in the Section 7.3.1 and the beginning of Section 7.4 give a procedure that one can use the compute this model in principle. Our concern in this section will be to give a description of a practical way to go about doing this.
7.4. MINIMIZATION AND REDUCTION

We assume that we have the data specified in Lemma 7.3.2: an elliptic curve $E/\mathbb{Q}$, an odd prime $p$, an imaginary quadratic field $K/\mathbb{Q}$, a cyclic extension $L/K$ of degree $p$, and a point $P \in E(L)$ such that $[P] \in (E(L)/pE(L))^G$, where $G = \text{Gal}(L/\mathbb{Q})$. We also assume $L$ has class number one. From this data one can compute the points $R_g \in E(L)$ giving rise to the cocycle $g \mapsto R_g$ defined in Lemma 7.3.2.

Fix a short Weierstrass equation $W$ of $E$, and let $R_g = (x_g, y_g)$ for $g \in G$. Recall that we have defined two divisors on $E$

$$D = 0_E + (R_0) + \ldots + (R_{p-1}),$$

$$D' = (2p - 1) \cdot 0_E - (-R_0) - \ldots - (-R_{p-1}).$$

**Matrix representation of a basis of $L(D')$.** We have an inclusion $L(D') \subset L((2p - 1) \cdot 0_E)$. Let $e_1 = 1, e_2 = x, e_3 = y, \ldots, e_{2p-2} = x^{p-1}, e_{2p-1} = x^{p-3}y$ be the usual basis of $L(D')$. For a basis $f_1, \ldots, f_p$ of $L(D')$, we can then write $f_i = \sum_{j=1}^{2p-1} A_{ij} e_j$ for some $A_{ij} \in L$, and from now on we identify the vector space $L(D')$ with the span of rows of $A$.

Recall that we have defined a free $\mathcal{O}_L$-module $T$ as the subset of elements of $L(D')$ that can be expressed as $\mathcal{O}_L$-integral linear combinations of $e_1, \ldots, e_{2p-1}$. Under the above identification, elements of $T$ correspond to linear combination of rows with integral entries.

**Making the action of $\text{Gal}(L/\mathbb{Q})$ explicit.** In Section 2 we have defined a basis of $L(D)$ by setting $I_1 = \frac{y + y_p}{x - x_p}, \ldots, I_{p-1} = \frac{y + y_{p-1}}{x - x_{p-1}}, I_p = 1$. Set $l_i' = \prod_{j=1}^{p-1} (x - x_j) \cdot l_i$, so that $l_i'$ are a basis of $L(D')$. Let $\alpha_1, \ldots, \alpha_{2p}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_L$, and consider $L(D')$ as a $\mathbb{Q}$-vector space with the basis $\alpha_i f_j$, $1 \leq i \leq 2p$, $1 \leq j \leq p$. Recall the matrices $M_g$ defined in 7.6. Let $N_g = M_g^{-1}$. By Proposition 7.3.3, we have

$$\begin{pmatrix} g(l_1') \\ g(l_2') \\ \vdots \\ g(l_p') \end{pmatrix} = N_g \cdot \begin{pmatrix} l_1' \\ l_2' \\ \vdots \\ l_p' \end{pmatrix}.$$ 

As the action of $G$ is semilinear, by multiplying the left and right sides by $g(\alpha_i)$ we obtain

$$\begin{pmatrix} g(\alpha_i l_1') \\ g(\alpha_i l_2') \\ \vdots \\ g(\alpha_i l_p') \end{pmatrix} = g(\alpha_i) N_g \cdot \begin{pmatrix} \alpha_1 l_1' \\ \alpha_1 l_2' \\ \vdots \\ \alpha_1 l_p' \end{pmatrix}.$$ 

For a general basis $f_1, \ldots, f_p$ of $L(D)$ we have a similar formula, with $N_g$ represented by $g(T)N_gT^{-1}$, where $T \in \text{GL}_{2p}(L)$ is the matrix relating the bases $l_i'$ and $f_i$.

**Computing an integral basis of $T^G$.** Using the above formulas we can compute the row vector representation of $g(\alpha_i f_j)$ for each $i$ and $j$. Let $A_1 \in \text{Mat}_{2p^2, 2p-1}(L)$ be the matrix formed
Algorithm 7.4.12. 

1. Compute the points \( R_g \), and then the matrices \( M_g \) using the Proposition 7.3.5.

2. Choose a basis \( f_1, ..., f_p \) of \( \mathcal{L}(D') \), and represent it by a matrix \( A \in \text{Mat}_{p,2p-1}(L) \). Use the formulas defining the Galois action to compute the matrix \( A_1 \in \text{Mat}_{2p^2,2p-1}(L) \) representing a set of generators of \( \mathcal{L}(D')^G \), and its restriction-of-scalars representation \( A_2 \in \text{Mat}_{2p^2,2p(2p-1)}(\mathbb{Q}) \), as described above. Let \( V \) be the \( \mathbb{Q} \)-span of rows of \( A_2 \), and set \( T' = \mathbb{Z}^{2p(2p-1)} \cap V \).

3. Compute a basis of \( T' \) as a matrix \( B' \in \text{Mat}_{p,2p(2p-1)}(\mathbb{Z}) \), and then compute the matrix \( B \in \text{Mat}_{p,2p-1}(\mathcal{O}_L) \) such that \( B' \) is the restriction of scalars of \( B \). We recover a basis of \( T \) by setting \( f_i^G = \sum_{j=1}^{2p} B_{ij} e_j \) for \( 1 \leq i \leq p \).

4. Compute a basis \( q_1, ..., q_{p(p-3)/2} \) for the \( \mathbb{Z} \)-module of quadrics with \( \mathbb{Z} \)-coefficients vanishing on the image of \( E \) in \( \mathbb{P}^{p-1} \) under the map \( e \) induced by \( f_1^G, ..., f_p^G \), and return as the model \( \mathcal{C} \) the subscheme of \( \mathbb{P}^{n-1}_\mathbb{Z} \) defined by the \( q_i \).

Two steps of the algorithm need further explanation. We need to explain how to compute the quadrics in Step 4, which is straightforward and we will do now, and we need explain how to choose the basis in Step 2, which is a subtler problem.

**Step 4 of the algorithm.** Let \( C_Q \) be the image of \( E \), under \( e \) and let \( C_L \) be the base change of \( C_Q \) to \( L \). As \( C_L \) is a genus one normal curve, so in particular projectively normal, the monomials \( f_i^G f_j^G, 1 \leq i, j \leq p \), span the \( 2p \)-dimensional \( L \)-vector space \( \mathcal{L}(2D') \).
Let $x_1, ..., x_p$ be the coordinates on $\mathbb{P}^{p-1}$, and let $V_Q$ be the $\mathbb{Q}$-space of all rational quadratic forms, spanned by the monomials $x_i x_j$, $1 \leq i, j \leq p$. We then define a $\mathbb{Q}$-linear map $j : V \to \mathcal{L}(2D')$ by the rule $x_i x_j \mapsto f_i^G f_j^G$.

The kernel of this map consists of all of the quadrics that vanish on $C_Q$. We compute a matrix representing the map $j$, and then use linear algebra over $\mathbb{Z}$ to compute a set of generating quadrics $q_1, ..., q_{p(p-3)/2}$ of $I(C_Q)$, with the property that they generate the $\mathbb{Z}$-submodule of integral quadrics that vanish at $C_Q$.

When $p = 3$, $C_Q$ is defined by a single ternary cubic, and it is simple to adapt the above method to work in this case as well.

**Picking a basis in Step 2.** A natural choice of basis of $\mathcal{L}(D')$, given the computation of Proposition 7.3.5, would be $l'_1, ..., l'_p$. This, however, does not lead to a practical algorithm.

With this choice, computing the basis of $T'$ in Step 3 can be very time consuming, as the dimension of matrix $A_2$ grows quickly with $p$ and the entries of $A_2$ tend to be rational numbers of large height, as they were obtained from the coordinates of the Heegner point. We now describe a more careful way to choose a basis.

We start by rescaling the basis $l'_i$. For legibility write $x_i = x_{\sigma^i}$ and $y_{\sigma^i} = y_i$. As $O_L$ is a PID, it is a standard fact that we can write $x_i = \frac{t_i}{r_i}$ and $y_i = \frac{s_i}{r_i}$ for some $r_i, s_i, t_i$, with $r_i, t_i$ and $s_i, t_i$ being pairs of coprime algebraic integers. For $1 \leq i \leq p - 1$, we put

$$f'_i = t_i \cdot t_2^2 \cdots t_{p-1}^2 \cdot l'_i = (t_1^2 x - r_1) \cdots (t_{i-1}^2 + r_{i-1}) / (t_i^2 y + s_i) (t_{i+1}^2 + r_{i+1}) \cdots (t_{p-1}^2 x - r_{p-1})$$

Having chosen this scaling, we see that $f'_i \in T$, i.e. the matrix $A'$ whose rows represent $f'_i$ have integral entries, and so do the corresponding matrices $A'_1$ and $A'_2$.

We now make a heuristic observation to motivate our next step. Note that, for $l < k < p$, we have $R_{\sigma^k} - R_{\sigma^l} = \sum_{i=l}^{k-1} \sigma^i - \sum_{i=l}^{k-1} \sigma^i = \sigma^j(R_{\sigma^k})$. If for a prime $p$ of $O_L$ the point $\sigma^j(R_{\sigma^k})$ reduces to $0 \in \mathbb{F}_p$, then $\overline{R_{\sigma^k}} = \overline{R_{\sigma^l}}$, and hence $\overline{f_k} = \overline{f_l}$. Hence $p$ will divide all entries of the difference $r_{k,l}$ of rows of $A'$ corresponding to $f_k$ and $f_l$. As the primes for which $\sigma^j(R_{\sigma^k})$ reduces to zero are exactly those that divide $\sigma^j(k_{l-1})$, we expect that the entries of $r_{k,l}$ and $\sigma^{k-l}(t_l)$ will have a large common divisor.

To cancel out these divisors for all pairs of rows we use the following procedure, reminiscent of Gaussian elimination. Let $r_1, ..., r_p$ be the rows of $A'$. For $1 \leq k \leq p - 1$, consider the $2 \times (2p - 1)$ submatrix $A_k$ of $A'$ formed by $r_k$ and $r_{p-1}$, and let $d_k$ be the generator of the ideal of $O_L$ generated by the $2 \times 2$ minors of $A_k$. We then compute $c_k \in O_L$ such that the entries of $r_{p-1} - c_k r_k$ are divisible by $d_k$ - this amounts to putting $A_k$ in Hermite normal form (over $O_L$), which is possible since we assumed $O_L$ is a PID, and can be done efficiently.

Next compute a generator $D_k$ of the ideal $(d_k, d_1 \cdot d_k, d_2 \cdot d_{k+1}, ..., d_{p-2})$, and find $i_k \in O_L \frac{d_k}{D_k}$ and $j_k \in O_L \frac{d_k}{D_k}$, with $i_k + j_k = 1$ - this is also a standard problem, see [Coh3]. We then replace $r_{p-1}$ with $r'_{p-1} = r_{p-1} - j_k c_1 \cdot r_1 - ... - j_{p-2} c_{p-2} \cdot r_{p-2}$, and then divide $r'_{p-1}$ by the GCD of its entries. In practice $D_k$ will often be a unit or at worst divisible by a few small primes, and so this GCD will be the product $d_{1,p-1} \cdots d_{p-2,p-1}$, up to a small factor. We then repeat this process for rows $r_1, ..., r_{p-2}$, with $r_{p-2}$ taking the role of $r_{p-1}$, and so on.
At the end of this process we obtain a new matrix $A'' \in \text{Mat}_{p,2p-1}(O_L)$ and $U \in \text{GL}_p(L)$ with $A'' = UA'$. We then take $f_1, ..., f_p$ to be the basis of $L(D')$ that corresponds to the rows of $A''$. To account for the change of basis, we replace $M_g$ by $UM_gg(U^{-1})$ for each $g \in G$, and then compute a basis $f_1^G, ..., f_p^G$ of $T^G$ using the approach described for $A$.

## 7.4.3 Reducing the model

In the previous section we have described how to compute a minimal model $\mathcal{C}$ of $c_Q$, with the property that the invariants $c_4(\mathcal{C})$ and $c_6(\mathcal{C})$ are as small as possible. However, small invariants do not guarantee that the equations defining $C$ will be simple. Note that making a $\text{GL}_p(\mathbb{Z})$-change of coordinates preserves the integrality and the invariants of $\mathcal{C}$. Thus we will seek to find a unimodular change of coordinates that makes the equations of $C$ as simple as possible. This is accomplished via reduction. The theory of reduction has been developed for genus one models of degree $n \leq 5$, and extends directly to the case of general $n$. Our exposition follows Section 6 of [CFS10].

Let $n \geq 3$ be an integer and let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n$, defined over $\mathbb{C}$. Let $E$ be the Jacobian of $C$, and note that $C$ is a torsor of $E$. The action of $E[n]$ on $C$ extends to an action of $E[n]$ on $\mathbb{P}^{n-1}$, and moreover if $E$ is defined over $\mathbb{Q}$ then so is this action, see Section 1 of [CFO+08]. Thus we obtain a homomorphism $\chi : E[n] \to \text{PGL}_n(\mathbb{C})$. Let $H_n$ be the preimage of $\chi(E[n])$ under the projection $\text{SL}_n(\mathbb{C}) \to \text{PGL}_n(\mathbb{C})$. We then have the following diagram:

$$
\begin{array}{ccc}
\mu_n & \longrightarrow & H_n \\
\downarrow & & \downarrow \\
\mu_n & \longrightarrow & \text{SL}_n(\mathbb{C}) \\
& & \downarrow_{\chi} \\
& & \text{PGL}_n(\mathbb{C})
\end{array}
$$

(7.9)

The group $H_n$ is also known as the Heisenberg group and is non-abelian of order $n^3$. It can be shown that the $n$-dimensional representation $V$ of $H_n$ induced by the middle vertical arrow is irreducible. By Weyl’s unitary trick, there is a unique, up to scaling by $\mathbb{R}_{>0}$, $H_n$-invariant inner product on $V$.

From the above discussion we obtain the following analogue of Theorem 6.1 of [CFS10]. Let $\mathcal{H}_n(\mathbb{C})^+$ be the space of positive definite Hermitian matrices, and $\mathcal{H}_n(\mathbb{R})^+$ the space of positive definite symmetric matrix. For a field $k$, let $X_n(k)$ be the set of genus one normal curves of degree $n$ defined over $k$. There is a natural action of $\text{SL}_n(\mathbb{C})$ on both $X_n(\mathbb{C})$ and $\mathcal{H}_n(\mathbb{C})^+$.

**Theorem 7.4.13.** Let $\phi_C : X_n(\mathbb{C}) \to \mathcal{H}_n^+(\mathbb{C})/\mathbb{R}_{>0}$ be the map defined by mapping $C$ to a matrix representing the $H_n$-invariant inner product. Then $\phi_C$ is the unique such map that is compatible with the action of $\text{SL}_n(\mathbb{C})$ in the following sense. For $g \in \text{SL}_n(\mathbb{C})$ and $C \in X_n(\mathbb{C})$, we have

$$
\phi_C(g+C) = g^{-1} \phi_C(C) g^{-1}
$$

Furthermore, $\phi_C$ restricts to a map

$$
\phi_R : X_n(\mathbb{R}) \to \mathcal{H}_n^+(\mathbb{R})/\mathbb{R}_{>0}.
$$
Proof. Let \( H_n \) and \( H'_n \) denote the Heisenberg groups of \( C \) and \( g \cdot C \) respectively. It is clear that we have \( H'_n = gH_ng^{-1} \), from which the covariance property follows. The second statement follows from the fact that the action of \( H_n \) is Galois equivariant and hence compatible with complex conjugation.

In practice we compute \( \phi_C(C) \) by averaging an arbitrary inner product over \( E[n] \).

**Proposition 7.4.14.** Let \( M_T \) describe the action of \( T \in E(\mathbb{C})[n] \) on \( C \subset \mathbb{P}^{n-1} \). Then the reduction covariant \( \phi_C(C) \) is

\[
\sum_{T \in E(\mathbb{C})[n]} \frac{1}{|\det M_T|^{2/n}} M_T^t M_T.
\]

**Proof.** By Weyl’s unitary trick, to obtain an \( H_n \)-invariant inner product we can take any inner product \( \langle , \rangle \) and average over \( H_n \), setting

\[
\langle v, w \rangle_{H_n} = \sum_{h \in H_n} \langle h \cdot v, h \cdot w \rangle.
\]

If we take \( \langle , \rangle \) to be the standard inner product on \( \mathbb{C}^n \), represented by the identity matrix \( I_n \), we find that

\[
\phi_C(C) = \sum_{h \in H_n} \bar{h}^{-t} h^{-1} = \sum_{h \in H_n} \bar{h}^t h
\]

Now note that the preimages of \( M_T \) in \( H_n \) are given by \( h = \alpha^{-1} M_T \), where \( \alpha^n = \det M_T \). We have

\[
\bar{h}^t h = \alpha^{-1} \bar{M}_T^t M_T = \frac{1}{|\det M_T|^{2/n}} M_T^t M_T
\]

Noting that this expression takes the same value for every preimage \( h \) of \( M_T \) and fibering the sum over \( E[n] \), we obtain the proposition.

**Definition 7.4.15.** We say a genus one normal curve \( C \subset \mathbb{P}^{n-1} \) defined over \( \mathbb{R} \) is LLL reduced if \( \phi_\mathbb{R}(C) \) is the Gram matrix of an LLL reduced lattice basis.

Thus to compute a reduced model from a minimal model it suffices to compute the reduction covariant \( \phi_\mathbb{R}(C) \), as we can then use the LLL algorithm to find a \( U \in \text{SL}_n(\mathbb{Z}) \) such that the Gram matrix \( M = U^t \phi_\mathbb{R}(C) U \) is LLL reduced. Thus \( \phi_\mathbb{R}(U^{-1} \cdot C) \) = \( M \) is LLL reduced, and hence \( U^{-1} \cdot C \) is a minimized and reduced model.

**Proposition 7.4.16.** Let \( E/\mathbb{C} \) be an elliptic curve, \( n \geq 3 \) an integer, and \( D \) a divisor of degree \( n \). Let \( l_1, \ldots, l_n \) be a basis of \( \mathcal{L}(D) \), and let \( i : E \to \mathbb{P}^{n-1} \) be the corresponding embedding of \( E \). Write \( C = i(E) \), and let \( F \) be the set of flex points of \( C \), i.e. the set of points \( P \in C \) with the property that the intersection of the tangent plane \( T_P C \) and \( C \) consists only of point \( P \) (with multiplicity \( n \)). Then

(i) The automorphisms \( M_T \) preserve the set \( F \), and hence induce an action of \( E[n] \) on \( F \).
(ii) Let $Q \in E(\mathbb{C})$ be a point with $nQ = \text{sum}(D)$. The embedding $i$ induces a bijection between the set $\{Q + T : T \in E[n]\}$ and $F$, and this bijection is $E[n]$-invariant.

Proof. Part (i) is clear, as $M_T$ define automorphisms of $C$ that extend to automorphisms of the ambient $\mathbb{P}^{n-1}$. For (ii), note that for a point $P \in C$, we have $P \in F$ if and only if the divisor class $[D - nP]$ in $\text{Pic}^0(C)$ is trivial, i.e. if and only if $n \cdot i^{-1}(P) = \text{sum}(D)$. \qed

The proposition determines the action of $M_T$ on the set $F$. One can show that the points of $F$ span $\mathbb{P}^{n-1}$, and hence the action of $M_T$ on $F$ determines $M_T$ uniquely, up to a scalar.

In the setting of Section 7.4.2, one may compute a reduced model as follows. Assume that we have carried out Step 3 of Algorithm 7.4.12, and so have a basis $f^\mathcal{G} = \sum_{j=1}^{2p-1} B_{ij} e_j$ of $\mathcal{L}(D)^\mathcal{G}$. Choose an embedding $j$ of $L$ into $\mathbb{C}$, and a small $\epsilon > 0$. Then carry out the following calculations to precision $\epsilon$:

1. Compute $j(\text{sum}(D)) \in E(\mathbb{C})$, and $j(B_{ij}) \in \mathbb{C}$.
2. Use the complex uniformisation of $E$ to find points of $E[n](\mathbb{C})$, and then a $Q \in E(\mathbb{C})$ with $pQ = j(\text{sum}(D))$. Hence obtain the points of $\{Q + T : T \in E[n]\}$.
3. Under the embedding of $E/\mathbb{C} \to \mathbb{P}^{n-1}$ determined by matrix $j(B)$, compute the set of flex points $F$ as the image of the set $\{Q + T : T \in E[n]\}$.
4. Find a subset $S$ of $F$ that spans $\mathbb{P}^{n-1}$. For each $T \in E[n]$, use the bijection of Proposition 7.4.16 to compute the action of $M_T$ on $S$, and then use linear algebra to compute $M_T$.
5. Use the formula of Proposition 7.4.14 to compute the reduction covariant $\phi_{\mathbb{R}}(C)$, and then use the LLL algorithm to compute $U \in \text{SL}_p(\mathbb{Z})$ so that $U^t \phi_{\mathbb{R}}(C) U$ is LLL reduced. Replace $B$ by $U^{-1}B$, and go to the Step 4 of of Algorithm 7.4.12.

In practice we choose the precision by trial and error, i.e. we try smaller and smaller $\epsilon$ until we obtain equations with small coefficients.

### 7.5 Computing the Heegner point

In this section we describe the algorithm we will use to compute a point satisfying the conclusions of Lemma 7.3.2.

Let us recall the definition of Heegner points from Section 7.2. Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$, $p$ an odd prime, and let $K$ be an imaginary quadratic field. We assume that $K$ contains an order $\mathcal{O}$, of discriminant $-D \neq 3, 4$, that satisfies the Heegner hypothesis: all prime factors of $N$ split in $K$. We fix an ideal $\mathcal{N}$ with $N\mathcal{O}_K = N\mathcal{N}$. Let $H$ be the Hilbert class field of $K$, and fix a modular parametrisation $\phi : X_0(N) \to E$ that maps the cusp $\infty$ to the origin of $E$. The Heegner point $x_D$ is defined to be the image $x_D = \phi(\mathcal{O}_K, [\mathcal{O}, \mathcal{N}]) \in E(H)$.

Now, assume that $H$ has a unique subfield $L$ of degree $p$ over $K$. Then the extension $L/\mathbb{Q}$ will be dihedral of order $2p$, with Galois group $G = \text{Gal}(L/\mathbb{Q})$. Let $z_D = \text{Tr}_{H/L}(x_D) \in E(L)$ and $y_D = \text{Tr}_{H/K}(x_D) \in E(K)$.
7.5. Computing the Heegner Point

As usual, let \( \sigma \) be a generator of \( \text{Gal}(L/K) \), let \( \tau \in G \) be a lift of complex conjugation, and let \( D_\sigma = \sum_{i=0}^{p-1} i\sigma^i \). We define the derived Heegner point as \( P = D_\sigma \cdot z_D \). As in the introduction, we have

\[
(\sigma - 1)(D_\sigma \cdot z_D) = pz_D - \text{Tr}(z_D) = pz_D - y_D \in pE(L),
\]

Hence the class \( [P] \in E(L)/pE(L) \) is invariant under the action of \( \text{Gal}(L/K) \), and so the class \( [P + \tau(P)] \) is invariant under the full action of \( G \). Thus \( P + \tau(P) \) satisfies the conditions of Lemma 7.3.2, and we can attach a Kolyvagin class \( c_Q \in H^1(Q, E[p]) \) to it.

Our goal in this section will be to explain how to compute the point \( x_D \) and hence \( P + \tau(P) \). The problem of computing Heegner points has been studied extensively before - but usually the application in mind is computing a generator of \( E(Q) \), in the case when \( E \) has analytic rank one, and so one only needs to compute the trace \( \text{Tr}_{L/Q}(z_D) \). The problem of computing the point \( z_D \) has been considered in \([JLS09]\), and an algorithm similar to the one they propose has been implemented in MAGMA by Steve Donnelly. For our purposes however, this method is too slow to handle the case when \( p \geq 5 \), so in this section we propose a variant to this method that seems to work quite well.

Remark 7.5.1. In defining the point \( P \) we have made a choice of factorization \( NO_K = NN \) and we have chosen a generator of \( \text{Gal}(L/K) \). One can prove that, up to a non-zero scalar multiple, the class \( [P] \) is independent of these choices.

Following \([JLS09]\), we give an explicit description of the map \( \phi \). Let \( \Lambda \) be the period lattice associated to \( E \), and let \( f \in S_2(\Gamma_0(N)) \) be the newform associated to \( E \). Let \( H^* = H \cup \bar{Q} \cup \{\infty\} \) be the extended upper half plane, and identify the modular curve \( X_0(N) \) with the quotient \( H^*/\Gamma_0(N) \). The modular parametrization map \( \phi : X_0(N) \to \mathbb{C}/\Lambda \) is given by integrating the holomorphic differential \( f(z)dz \) on \( X_0(N) \). We can compute it using the power series

\[
\phi(\tau) = \int_\tau^\infty f(z)dz = \sum_{n \geq 1} \frac{a_n}{n} e^{2\pi in\tau}, \tag{7.10}
\]

where \( f = \sum_{n \geq 1} a_n q^n \) is the Fourier expansion of \( f \). To obtain a parametrization \( X_0(N) \to E \), we compose with the uniformization \( \psi = \mathbb{C}/\Lambda \to E(\mathbb{C}) \). The map \( \psi \) is defined using the Weierstrass \( \wp \)-function, and is easy to compute numerically to high precision.

The Artin map provides us with an isomorphism between the class group \( \text{Cl}(\mathcal{O}) \) and the Galois group \( \text{Gal}(L/K) \). We first compute a set of representatives \( a_1, \ldots, a_p \) for \( \text{Cl}_K \). Let \( \sigma_i \) be the image of \( a_i \) under the Artin map. As explained in Section 7.2, the Galois conjugates of the point \( x \) corresponding to the isogeny \( [\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/N^{-1}] \) are given by

\[
\sigma_i(x) = [\mathbb{C}/a_i^{-1} \to \mathbb{C}/a_i^{-1} N^{-1}]. \tag{7.11}
\]

For every conjugate we then compute a corresponding point \( \tau \) in the upper half plane. Now fix an embedding \( i \) of \( L \) into \( \mathbb{C} \). As the morphism \( \phi \) is defined over \( \mathbb{Q} \), we can use the above description of the Galois action to compute the coordinates of the Galois conjugates \( \sigma_i(x_D) \), viewed as elements of \( \mathbb{C} \) via the embedding \( L \hookrightarrow \mathbb{C} \), to whatever precision we like. Next, we
again use the description of the Galois action to compute approximations of coordinates of the point \( z_D = \text{Tr}_{H/L} x_D \).

Let us write \( z_D = (x,y) \in E(L) \). The standard method to recognize \( x \) as an algebraic number from the data of a set of complex numbers \( x_g \), serving as approximations to \( i(g(x)) \in \mathbb{C} \) as \( g \) ranges over \( \text{Gal}(L/Q) \), is to approximate the minimal polynomial \( f \) of \( x \) by \( \prod_{g \in \text{Gal}(L/Q)} (x - x_g) \), and try to recognize the coefficients of \( f \) as rationals, using continued fractions, or better yet the LLL algorithm.

However, for us this method is not efficient enough, since \( x \in L \) typically has large height in examples we want to consider, and the coefficients of polynomial \( f \) are symmetric polynomials in \( g(x) \), and hence of even larger height. We instead take advantage of the fact that we know that \( x \) is defined over a ring class field, and try to recognize \( x \) directly as an element of \( L \).

We first find a defining equation of \( L \) and compute an integral basis \( \alpha_1, \ldots, \alpha_{2p} \) of the ring integers \( \mathcal{O}_L \) - this can be done quickly using standard algorithms of computational class field theory. We then use lattice reduction to guess an expression for \( x \) as a fraction \( \sum u_i \alpha_i / \sum v_i \alpha_i \). In what follows, we have fixed an embedding of \( L \) into \( \mathbb{C} \).

**Definition 7.5.2.** Let \( \epsilon > 0 \), \( C = 10^B \) for an integer \( B > 0 \), \( z \in L \) and \( z_1, \ldots, z_{2p} \in \mathbb{C} \) be such that \( |\sigma_i(z) - z_i| < \epsilon \). Let \( \alpha_{ij} \in \mathbb{C} \) be such that \( |\sigma_j(\alpha_i) - \alpha_{ij}| < \epsilon \). To this data we associate the \( 4p \times 6p \) integer matrix \( A_{z,\epsilon,C} \):

\[
\begin{pmatrix}
1 & 0 & \ldots & 0 & 0 & |C\alpha_{1,1}| & |C\alpha_{1,2}| & \ldots & |C\alpha_{1,2p-1}| & |C\alpha_{1,2p}| \\
0 & 1 & \ldots & 0 & 0 & |C\alpha_{2,1}| & |C\alpha_{2,2}| & \ldots & |C\alpha_{2,2p-1}| & |C\alpha_{2,2p}| \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & |C\alpha_{2p-1,1}| & |C\alpha_{2p-1,2}| & \ldots & |C\alpha_{2p-1,2p-1}| & |C\alpha_{2p-1,2p}| \\
\vdots & \vdots & \vdots & \vdots & \vdots & |C\alpha_{2p,1}| & |C\alpha_{2p,2}| & \ldots & |C\alpha_{2p,2p-1}| & |C\alpha_{2p,2p}| \\
0 & 0 & \ldots & 1 & 0 & |C\alpha_{2p-1,1}| & |C\alpha_{2p-1,2}| & \ldots & |C\alpha_{2p-1,2p-1}| & |C\alpha_{2p-1,2p}| \\
0 & 0 & \ldots & 0 & 1 & |C\alpha_{2p,1}| & |C\alpha_{2p,2}| & \ldots & |C\alpha_{2p,2p-1}| & |C\alpha_{2p,2p}| \\
\end{pmatrix}
\]

i.e. the left \( 4p \times 4p \)-block is the \( 4p \times 4p \) identity matrix, and the right \( 4p \times 2p \)-second block splits into the upper \( 2p \times 2p \) block \( (|C\alpha_{ij}|)_{ij} \) and the lower \( 2p \times 2p \) block \( (|C\alpha_{ij}z_j|)_{ij} \). We define \( L_{z,\epsilon,C} \) to be the lattice in \( \mathbb{R}^{6p} \) spanned by the rows of \( A_{z,\epsilon,C} \).

To recover \( z \) from \( A_{z,\epsilon,C} \), our strategy will be to use the LLL lattice reduction algorithm to find short vectors in the lattice \( L_{z,\epsilon,C} \). We will take \( C = 10^B \) to be a large constant and \( \epsilon \) as small as possible. Let the rows of \( A_{z,\epsilon,C} \) be \( r_1, r_2, \ldots, r_{4p} \). The lattice reduction algorithm gives us integers \( u_1, u_2, \ldots, u_{4p} \) such that the row vector \( \sum_{i=1}^{4p} u_i r_i \) is "small", and if \( \epsilon \) is small enough, we hope that we will have

\[
0 = u_1 \alpha_1 + u_2 \alpha_2 + \ldots + u_p \alpha_{2p} + u_{2p+1} \alpha_{2p+1} + u_{2p+2} \alpha_{2p+2} + \ldots + u_{4p} \alpha_{4p},
\]
7.5. COMPUTING THE HEEGNER POINT

\[ z = -\frac{\sum_{i=1}^{2p} u_i \alpha_i}{\sum_{i=1}^{2p} u_{2i+1} \alpha_i} \]

and hence recover \( z \) from the matrix \( A_{z,\epsilon,C} \). We summarise the discussion of this section in the following algorithm.

**Algorithm 7.5.3.**

- **INPUT:** An elliptic curve \( E \), a Heegner discriminant \( D \), and a prime \( p \) that divides \( |\Cl(O)| \) exactly once.

- **OUTPUT:** Coordinates \((x, y)\) of a point \( P \in E(L) \) that is (conjecturally) the point \( z_D = \text{Tr}_{H/L} x_D \).

1. Find a set of representatives \( a_1, a_2, ..., a_n \) for the class group \( \Cl(K) \), and for each point \([C/a_i^{-1} \to C/a_i^{-1}.N^{-1}]\), compute a corresponding \( \tau_i \) in the upper half plane.

2. Compute an integral basis of the maximal order \( \mathcal{O}_L \).

3. Pick an \( \epsilon > 0 \), and compute \( \phi(\tau_i) \in \mathbb{C} \) to precision \( \epsilon/2 \), using the formula (7.10), by computing enough of the Fourier coefficients \( a_n \).

4. Compute the period lattice \( \Lambda \) and hence the uniformisation map \( \psi : \mathbb{C}/\Lambda \to E \) to the required precision, and hence find \( \psi(\phi(\tau_i)) \). Then use the description of the Galois action on Heegner points 7.11, to take the trace from \( H \) to \( L \), and hence obtain \( z_1, ..., z_{2p} \) with \( |\sigma_i(x) - z_i| < \epsilon \).

5. Using \( z_1, z_2, ..., z_{2p} \) and choosing a large \( C \), form the matrix \( A_{z,\epsilon,C} \) as in Definition 7.5.2. Use the LLL algorithm to find \( U \in \text{SL}_{4p}(\mathbb{Z}) \) so that the rows of \( UA_{z,\epsilon,C} \) form an LLL-reduced basis of \( L_{z,\epsilon,C} \). Then let \( x = -\frac{\sum_{i=1}^{2p} u_{1i} \alpha_i}{\sum_{i=1}^{2p} u_{2i+1} \alpha_i} \) and test if \( x \) is the \( x \)-coordinate of a point in \( E(L) \). If it is, solve for the \( y \)-coordinate and return \((x, y)\). Otherwise, replace \( \epsilon \) by \( \epsilon/2 \), and return to Step 3.

Steps 1, 2 and 3 of the algorithm have been studied extensively in the literature, see for example Section 8.6 of [Coh08] or [Wat05], so we do not provide details on how to implement them. We have used existing MAGMA implementations of these steps in our calculations. The algorithm has not proven that the point \((x, y)\) is indeed the point \( x_D \), although we believe it is highly improbable that it isn’t, nor have we proven that it always terminates. However, in practice we have been able to use it to compute points for \( p \leq 11 \).

The main bottleneck is Step 3. If the height of the Heegner point is very large, then we may need to take \( \epsilon \) very small for the algorithm to return a point in \( E(L) \), and this might require computing a very large number of the Fourier coefficients \( a_n \).

**Remark 7.5.4.** The output of our algorithm, if it terminates, will be a point \( y \in E(H) \), and as noted in [JLS09], verifying that this point coincides with the point \( x_D \) is a nontrivial matter. It is very unlikely that the point \( y \) is not the point \( z_D \). However, for the purpose of constructing examples of non-trivial elements of the Tate-Shafarevich group of \( E \), it will suffice...
to just compute the point $y$ and verify that the corresponding point $P$ satisfies conditions of Lemma 7.3.2.

**Remark 7.5.5.** A further improvement one can make is to use the fact that we can also compute numerically the $y$-coordinate, and look for linear relations of the form $A + Bx + Cy = 0$. Recall that we have assumed that $L$ is of class number 1, so that $x = r/t^2$ and $y = s/t^3$, for some $r, s, t \in \mathcal{O}_L$. Thus if $A + Bx + Cy = 0$, we see that $t|A$, and that hence $A^2 x \in \mathcal{O}_L$. It is then simple to recover $A^2 x$ from its numerical approximation, and hence compute the point $(x, y)$.

In practice this is a useful improvement - heuristically the minimal $A, B, C$ should be smaller than the minimal $u, v$ appearing in a relation $u + vx = 0$, and so should be easier to guess from numerical approximation.

### 7.6 Examples

In this section we apply the theory we developed to concrete examples, and construct elements of $p$-torsion subgroups of Tate-Shafarevich groups, for $p \leq 11$ an odd prime. We first focus on the case when the curve $E$ is of rank 0. To illustrate our method, in the first two examples, we compute equations representing a non-trivial element of $\text{III}(E_1/\mathbb{Q})[3]$ and a non-trivial element $\text{III}(E_2/\mathbb{Q})[5]$, where $E_1$ and $E_2$ are the curves 681b3 and 1058d1. These two examples can also be computed using complete $p$-descent, as described in [CFO +08] and [Fis13a], and can be found in Fisher’s tables. We then follow with our main result, explicit equations representing an element of $\text{III}(E/\mathbb{Q})[p]$ for $p = 7$, where $E$ is the curve 3364c1.

In the rank 0 case, we were unable to compute an example of a non-trivial 11-torsion element of $\text{III}(E/\mathbb{Q})$. The curve of smallest conductor with non-trivial $X(E/\mathbb{Q})[11]$ and no 11-isogeny is 8350c1, for which we were unable to recognize a Heegner point that defines a Kolyvagin class - it appears that they have enormous height. We were however able to compute an example in the rank 1 case. In particular, for the curve $E = 37a1$ and the discriminant $D = -2731$ we have computed equations for a non-trivial element of $\text{III}(E_D/\mathbb{Q})[11]$, where $E_D$ is the quadratic twist of $E$ by $D$.

**Example 7.6.1.** Consider the elliptic curve $E$ labeled 681b3 in Cremona’s tables. $E$ has no rational 3-isogeny and $\text{III}(E)[3] = (\mathbb{Z}/3\mathbb{Z})^2$, and furthermore there are no elliptic curves of smaller conductor with this property, so $E$ is a natural first candidate. $E$ is defined by the minimal Weierstrass equation

$$y^2 + xy = x^3 + x^2 - 1154x - 15345$$

For our Heegner discriminant, we choose $D = -107$. The conductor of $E$ is $N = 3 \cdot 227$, and one verifies that 3 and 227 split completely in $K = \mathbb{Q}(\sqrt{-107})$, so $D$ satisfies the Heegner hypothesis.

For our field $L$, we take the Hilbert class field of $K$. As $K$ has class number 3, by class field theory $L/\mathbb{Q}$ is a dihedral extension of degree 6. We use the machinery implemented in MAGMA to find that $L = \mathbb{Q}[\alpha]$, where the minimal polynomial of $\alpha$ is $x^6 - 2x^5 - 2x^3 + 30x^2 - 52x + 29$, etc.
and that $L$ has class number 1. The Galois group $G$ is generated by an element $\sigma$, of order 3, determined by

$$\sigma(\alpha) = \frac{1}{94}(24\alpha^5 - 8\alpha^4 - 29\alpha^3 - 112\alpha^2 + 502\alpha - 239)$$

and by the lift $\tau$ of complex conjugation, determined by

$$\tau(\alpha) = \frac{1}{94}(-7\alpha^5 + 18\alpha^4 + 30\alpha^3 + 17\alpha^2 - 260\alpha + 338)$$

We fix an ideal $N$ with $N/N = \mathcal{O}_K = 681\mathcal{O}_K$. Let $z_D \in E(H)$ be the Heegner point that is the image of the point $(O, [O], N)$. There are 4 possible choices for $N$, corresponding to the factorization $N = 3 \cdot 227$. Which one we choose is not important for the purpose of constructing non-trivial Kolyvagin classes, since changing the choice of $N$ replaces $z_D$ by $\pm z_D + T$, where $T \in E_{\text{tors}}(\mathbb{Q})$. See Proposition 5.3 of [Gro91].

**Remark 7.6.2.** However, for the purpose of making the computations more efficient, a clever choice of $N$ could help to compute the modular parametrization $\phi : \mathcal{H}/\Gamma_0(N) \to \mathbb{C}/\Lambda$. The idea is that the $q$-series we use to compute $\phi$ will converge faster if the imaginary part of the Heegner point $\tau \in \mathcal{H}$ is large, and so we could try to use Atkin-Lehner operators to increase the imaginary parts of the Heegner conjugates $\tau_1, \ldots, \tau_2p \in \mathcal{H}$. This is explained in Section 8.6.5 of [Coh08], and also mentioned in §8.2 of [EJL]. Thus far we have not implemented this trick - it would be interesting to see if it could help us compute more examples.

We use Algorithm 7.5.3 to compute the point $z_D$. The denominator of the $x$-coordinate is

$$3504270831713779744633042806412917667418070133773414493608013900835961250175$$

while the numerator is given by

$$-1085550829179464325401557750389867359355783146309141591754344691521088631486 \cdot \alpha^5 + 110940816304672404324989494231306705758806796781642621701269045587691351016 \cdot \alpha^4 - 5208256682384098419737490165336960436611863084231447639629677751394231026630966 \cdot \alpha^3 + 12976602732945282246653692905257941699857931285487886545715881513817523902062 \cdot \alpha^2 - 116190478368051571534835458588889561171836130133844072263056787033445394766272 \cdot \alpha + 602533470305397687827644570535196979877285515761653797296338950445773259752$$

This computation took less than a second of computer time, and required computing the modular parametrization to 200 digits of precision. The trace of the point $z_D$ down to $K$ is the point $y_D = z_D + \sigma(z_D) + \sigma^2(z_D)$, which is divisible by 3 in $E(K)$, and can be written as $y_D = 3Q$, where

$$Q = \left(\frac{-551080\sqrt{-107} - 883774}{184041} : \frac{1504723940\sqrt{-107} + 22208410826}{78953589} : 1\right)$$

The Kolyvagin class $c_Q \in H^1(\mathbb{Q}, E[p])$ associated to $z_D$ corresponds to the class $[D_\sigma z_D] \in E(L)/pE(L)$. As the point $D_\sigma z_D \in E(L)$ is not necessarily fixed by the complex conjugation $\tau$, to apply the theory developed in Section 7.3, we instead compute an $n$-diagram representing the class $[D_\sigma z_D + \tau(D_\sigma z_D)] \in E(L)/pE(L)$. By general theory, $c_Q$ is fixed by complex conjugation,
and this class is just $2c_Q$. Hence it will also be non-zero if $c_Q$ is, and so is just as good for the purposes of exhibiting non-trivial elements of $III$.

In notation of Lemma 7.3.2, we put $P = D_\sigma z_D + \tau(D_\sigma z_D)$. Note that the Algorithm 7.4.12, which we use to compute the corresponding 3-diagram, only requires the coordinates of the points $R_\sigma$, $1 \leq i \leq p - 1$ as the input, not the point $P$ itself. Indeed, by Lemma 7.3.2, $[P] = [D_\sigma R_\sigma] \in E(L)/pE(L)$.

To summarise, we compute the 3-diagram associated to $[D_\sigma R_\sigma] \in E(L)/3E(L)$. We obtain the point $R_\sigma$ from the relation $pR_\sigma = \sigma(P) - P$. The $x$-coordinate of the point $R_\sigma$ is

$$1/1741682413263770958143450(483403026915311979182787081\alpha^3 + 35453825605498566073743810\alpha^4 - 137498458568104949011766487\alpha^3 - 2452468960182058461987679215\alpha^2 + 9038525365115044024894770546\alpha - 3473956084362757366189406163)$$

**Remark 7.6.3.** In this example, we were able to compute the point $z_D$ directly, but for $p \geq 5$, the large height of this point makes this difficult. We describe now an optimization to our algorithm, based on the observation that we only need the coordinates of the point $R_\sigma$.

In practice, of all the points on $E$ that occur in our computations, the points $R_\sigma$ have the smallest height, and are hence easiest to recognise from numerical approximations. Thus the optimal approach is to use Algorithm 7.5.3 to compute the point $R_\sigma$ directly, and obtain the rest of $R_\sigma$ using Lemma 7.3.2.

We assume that the point $y_D = \text{Tr}_{L/K} z_D \in E(K)$ is divisible by $p$ in $E(K)$, and write $y_D = pQ$. In practice, this often follows from Theorem 7.2.2. Then, as $\sigma(Q) = Q$, we have $D_\sigma \cdot Q = \frac{p(p-1)}{2}Q \in pE(L)$. We compute

$$D_\sigma(z_D - Q) + \tau(D_\sigma(z_D - Q)) = D_\sigma z_D + \tau(D_\sigma z_D) + \frac{p(p-1)}{2}(Q + \tau(Q))$$

Thus $[P] = [D_\sigma(z_D - Q) + \tau(D_\sigma(z_D - Q))] \in (E(L)/pE(L))^\text{Gal}(L/Q)$, and we see that it suffices to compute the point $z_D - Q$.

We cannot use Algorithm 7.5.3 to compute the point $z_D - Q$ directly. The issue is that we do not know the point $Q$, and so cannot yet compute numerical approximations for the $x$-coordinate of $z_D - Q$. Note that as $E(L)[p]$ is trivial, $Q$ is unique. It is often feasible to recognise the point $Q$ directly, since its coordinates are defined over $K$. Alternatively, there are $p^2$ candidates for $Q$ as an element of $E(C)$, and we can recognise $y_D - Q$ by looping over all of them. This improvement is particularly important if the height of $Q$ is large, since the height of $z_D - Q$ can be much smaller than the height of $Q$ and $z_D$.

We return to our example. We run the Algorithm 7.4.12 up to Step 3, computing the rational
functions \( l_1, l_2 \) and \( l_3 \) that form an invariant basis of \( \mathcal{L}(5 \cdot 0_E - R_\sigma - R_{\sigma^2}) \).

\[
l_1 = \frac{1}{47}(176855470404\alpha^5 - 20242622720490\alpha^4 - 63177952499457\alpha^3 - 68185112511530\alpha^2 + 343696620903934\alpha - 745048783796769)x^2 + \\
1/47(8466648389785^5 + 4288692455140\alpha^4 - 395648289364\alpha^3 - 8522016650030\alpha^2 + 680560058228\alpha + 47744730691732)xy + \\
1/47(1753838747086818\alpha^5 - 408615009576136\alpha^4 - 730459128913922\alpha^3 - 468304363966954\alpha^2 + 4031987024066296\alpha + 1045449296914556)x + \\
1/47(173338598423528\alpha^5 - 106194481998772\alpha^4 - 573113036269970\alpha^3 - 76049851011868\alpha^2 + 3092001020772764\alpha - 750482884455365)y + \\
1/47(-1122219198324102\alpha^5 + 7008908878507566\alpha^4 + 6871112034226089\alpha^3 - 139781288687056\alpha^2 - 38982233808708330\alpha + 567554038170381623),
\]

\[
l_2 = \frac{1}{47}(302018626712\alpha^5 - 4110376939908\alpha^4 - 11115748350090\alpha^3 - 10990556193652\alpha^2 + 60654116847116\alpha - 95447012403290)x^2 + \\
1/47(-549968573644\alpha^5 + 66244890120\alpha^4 + 1683028165992\alpha^3 + 2683597978100\alpha^2 - 8998231848664\alpha - 10209123391776)xy + \\
1/47(-672970851698766\alpha^5 + 762342835784084\alpha^4 + 2400083972961340\alpha^3 + 2602511422664746\alpha^2 - 13054562134388508\alpha + 2872023735389225)x + \\
1/47(-76036744440886\alpha^5 + 83497715283216\alpha^4 + 26985909064266\alpha^3 + 29668606921214\alpha^2 - 1467081056903824\alpha + 3133571884295572)y + \\
1/47(-12421184633305258\alpha^5 + 21669530734146544\alpha^4 + 48098319266989046\alpha^3 + 40436392432379746\alpha^2 - 263747546335323760\alpha + 142716928850047322),
\]

\[
l_3 = \frac{1}{47}(-3704068125012\alpha^5 + 6788687657626\alpha^4 + 145065482038493\alpha^3 + 11731652967434\alpha^2 - 79631152973070\alpha + 22789388608393)x^2 + \\
1/47(-463605563330\alpha^5 - 656683599780\alpha^4 + 1062474890100\alpha^3 + 2974711416430\alpha^2 - 5447638213940\alpha - 13803514435140)xy + \\
1/47(-803487132697280\alpha^5 - 301754845848628\alpha^4 + 2259583975167526\alpha^3 + 431919059335028\alpha^2 - 11950529585610596\alpha - 9653767876150098)x + \\
1/47(-73229973735836\alpha^5 + 66759104880000\alpha^4 + 253069473647958\alpha^3 + 299390763798280\alpha^2 - 1371956894416076\alpha + 1980431040593561)y + \\
1/47(26128032498281696\alpha^5 + 3027262603073772\alpha^4 - 7687046619330820\alpha^3 - 133667425094482252\alpha^2 + 408966732163285820\alpha + 10791464166237161),
\]

Let \( C \) be the image of \( E \) in \( \mathbb{P}^2 \) under the map \((x, y) \mapsto (l_1(x, y) : l_2(x, y) : l_3(x, y)) \). Step 4 of Algorithm 7.4.12 does not apply in this case, since \( C \) is defined by a ternary cubic rather than by quadrics. However it is easy to compute a cubic \( F \) defining \( C \), using the standard algorithms
We compute the \( c \)-invariants of \( G \), using the already existing MAGMA routines. We find that \( c_4(G) = c_6(G) = 113737 \), and \( c_6(G) = c_6(E) = 12842515 \). In other words, \( G \) is already minimal, as conjectured in Remark 7.4.7. To reduce \( G \), we use the already existing MAGMA routine for reducing ternary cubics, and find that making a change of variables associated to the matrix

\[
\begin{pmatrix}
-1 & -5 & -9 \\
0 & 3 & 4 \\
0 & 1 & 1
\end{pmatrix}
\]

takes \( G \) to the cubic

\[
F = x^3 + 2x^2y - 3x^2z - xy^2 + 9xyz - 8xz^2 + y^3 - 11y^2z - 5yz^2 + 6z^3
\]

and this is essentially as nice as an equation as we can hope for. Let \( C \subset \mathbb{P}^2 \) be the curve defined by \( F \). The diagram \([C \to \mathbb{P}^2]\) is the representation of the class \( c_Q \in H^1(Q, E[3]) \) that we set out to obtain.

We check that \( c_Q \) is in the 3-Selmer group \( \text{Sel}^{(3)}(E/\mathbb{Q}) \), i.e. that \( C \) is everywhere locally soluble. Since we have represented \( c \) by the ternary cubic \( F \), a standard way to do so would be to compute and factor the discriminant of \( G \), and test solubility for the primes that divide the discriminant, using standard algorithms for genus one models implemented in MAGMA. We give now an alternative way to do this, based on the theory we developed in Section 7.4, that has the advantage of generalizing nicely to \( p > 5 \).

By Proposition 7.4.6, \( C \) has good reduction at primes \( p \) different from 3, 227 and 107. By Lang’s theorem, the reduction \( \tilde{C} \) of \( C \) admits an \( \mathbb{F}_p \)-point, which lifts to a \( \mathbb{Q}_p \)-point by Hensel’s lemma. It is easy to find a smooth \( \mathbb{F}_q \)-point on \( \tilde{C} \) for \( q \in \{3, 227, 107\} \), and such a point again lifts to a \( \mathbb{Q}_p \)-point by Hensel’s lemma. Thus \( C \) is everywhere locally soluble, and \( c_Q \) maps to \( \text{III}(E/\mathbb{Q})[3] \).

**Remark 7.6.4.** Note that we are using the geometric form of Hensel’s lemma, i.e. a smooth point on the reduction lifts to a \( \mathbb{Q}_p \)-point. See Proposition 5, Section 2.3 of [BLR12] for a reference.

Finally, to check that the image of \( c_Q \) is a non-trivial element of \( \text{III}(E/\mathbb{Q}) \), note that \( E \) has rank 0 and \( E(\mathbb{Q})[3] \) is trivial. Hence \( E(\mathbb{Q})/3E(\mathbb{Q}) \) is trivial, and we only need to show that \( c_Q \) is non-zero. Thus it suffices to check that the class \([D_\sigma R]\) is non-zero in \( E(L)/3E(L) \), i.e. that \( D_\sigma \cdot R_\sigma \) is not divisible by 3, and it is easy to check that this is indeed the case. Hence \( C(\mathbb{Q}) \) is empty, and \( C \) is a counterexample to the Hasse principle.

**Remark 7.6.5.** One can easily find an equation for \( c_Q \) using the method of 3 descent. However, we note that our method gives us an additional piece of information - we know that the class
c_Q capitulates over the field L. By construction of our model for \([C \to \mathbb{P}^{n-1}]\), we know that the images of the points \(R_\sigma\), where \(0 \leq i \leq p - 1\), under the embedding \(E \overset{\psi}{\to} \mathbb{P}^{p-1}\), lie on the intersection of the curve \(C\) and a hyperplane \(H\) defined over \(\mathbb{Q}\). We can compute an equation for \(H\) using linear algebra, since \(p\) points uniquely determine a hyperplane in \(\mathbb{P}^{p-1}\). In our case, we find

\[
H = 771x - 2818y + 4751z.
\]

Hence, the binary cubic obtained by substituting \(z = -771/4751x + 2818/4751y\) in \(F\) splits as a product of three distinct linear forms over \(L\).

We can also compare our result with Theorem 6.4.1. The curve \(C\) capitulates over the totally real subfield of \(L\), which is a cubic extension of \(\mathbb{Q}\), of discriminant \(-107\). Theorem 6.4.1 predicts that \(C\) capitulates over a number field of (absolute) discriminant at most \(0.63548 \cdot H_E^4 = 72277.58876\).

As to what the actual smallest number field is, the smallest discriminant we were able to find via a naive search corresponds to the hyperplane \(z = 0\). The resulting binary cubic is \(x^3 - 2x^2y - xy^2 - y^3\), of discriminant \(-87\). To prove that this is the smallest number field over which \(C\) capitulates, one would have to show that \(C\) does not capitulate over any of the 7 cubic fields of absolute discriminant less than 87. It seems to be challenging to either prove or disprove this assertion.

We now give an example with \(p = 5\). Background on the theory of genus one models of degree 5 can be found in [Fis13a].

**Example 7.6.6.** We now look at the curve \(E\) labelled 1058d1 in Cremona’s tables, and given by a minimal Weierstrass equation \(y^2 + xy = x^3 - x^2 - 332311x - 7373731\). \(E\) is the smallest example of a curve with non-trivial \(\text{III}(E/\mathbb{Q})[5]\) and no rational 5-isogeny. For the Heegner discriminant, we take \(D = -79\). The field \(K = \mathbb{Q}(\sqrt{-79})\), has class number 5, and so \(L\), the Hilbert class field of \(K\), is a degree 10 dihedral extension of \(\mathbb{Q}\), defined by the equation

\[
x^{10} - 3x^8 + 3x^7 + 22x^6 + 33x^5 + 22x^4 + 3x^3 - 3x^2 + 1
\]

As explained in the Remark 7.6.3, we compute the point \(R = z_D - y_D/5\) directly. This requires, in Step 3 of Algorithm 7.5.3, computing the images of Heegner points under the modular parametrization to precision 250, and takes a few seconds of computer time. The point \(R\) is of height 294.12, so we do not give its coordinates, as they would fill up several pages. We then use Algorithm 7.4.12 to compute equations for the corresponding curve \(C \subset \mathbb{P}^4\), and obtain the
five quadrics

\[ q_1 = 446x_1^2 - 589x_1x_2 - 153x_1x_3 + 255x_1x_4 + 177x_1x_5 - 194x_2^2 + 140x_2x_3 - 190x_2x_4 - 240x_2x_5 + 14x_3^2 - 64x_3x_4 + 42x_3x_5 + 73x_4^2 + 85x_4x_5 + 8x_5^2, \]

\[ q_2 = 24x_1^2 + 76x_1x_2 + 316x_1x_3 - 157x_1x_4 + 659x_1x_5 - 37x_2^2 + 78x_2x_3 + 217x_2x_4 + 495x_2x_5 - 63x_3^2 + 127x_3x_4 - 4x_3x_5 - 300x_4^2 - 454x_4x_5 - 87x_5^2, \]

\[ q_3 = 964x_1^2 + 574x_1x_2 - 123x_1x_3 - 186x_1x_4 + 467x_1x_5 + 168x_2^2 + 17x_2x_3 - 322x_2x_4 - 19x_2x_5 - 7x_3^2 + 13x_3x_4 - 74x_3x_5 + 111x_4^2 + 154x_4x_5 + 105x_5^2, \]

\[ q_4 = 3x_1^2 + 361x_1x_2 - 40x_1x_3 + 506x_1x_4 + 666x_1x_5 + 202x_2^2 - 38x_2x_3 - 110x_2x_4 + 34x_2x_5 + 14x_3^2 - 197x_3x_4 - 212x_3x_5 + 442x_4^2 + 821x_4x_5 + 406x_5^2, \]

\[ q_5 = 357x_1^2 + 350x_1x_2 - 390x_1x_3 + 862x_1x_4 + 475x_1x_5 - 32x_2^2 - 206x_2x_3 + 637x_2x_4 + 411x_2x_5 + 56x_3^2 - 129x_3x_4 - 96x_3x_5 - 98x_4^2 - 41x_4x_5 + 6x_5^2. \]

We then make a $\operatorname{SL}_5(\mathbb{Z})$-change of coordinates to reduce the curve $C$. We represent the reduced model by a $5 \times 5$ alternating matrix of linear forms $A$.

\[
A = \begin{pmatrix}
0 & x_1 - x_3 - x_5 & x_1 - x_2 + x_3 + 2x_4 & -2x_1 - 2x_3 + x_5 & x_2 + x_3 + x_4 + x_5 \\
0 & -2x_1 + 2x_3 + x_4 + x_5 & -x_1 + 2x_2 - x_4 - x_5 & x_1 + x_4 + x_5 \\
-x_1 - x_3 - x_5 & 0 & -x_1 - x_3 - x_5 & -x_3 + x_4 + x_5 \\
0 & 0 & 0 & -x_1 \\
0 & 0 & 0 & 0
\end{pmatrix}
\]

We compute the invariants of the model $A$ and find that they are the same as the invariants of the curve $E$, i.e. the model is minimal. The curve is defined by the $4 \times 4$ Pfaffians of $A$, the five quadrics:

\[ q_1 = -x_1^2 + 3x_1x_3 + x_1x_4 + 2x_1x_5 - 2x_2x_3 + 2x_2x_4 + 2x_2x_5 + x_3x_4 + x_3x_5 - x_4^2 - x_4x_5, \]

\[ q_2 = -x_1^2 - 4x_1x_3 + 3x_1x_4 + x_1x_5 - x_2x_3 - 2x_3^2 + 2x_3x_4 + 2x_3x_5 - 2x_4x_5 - 2x_5^2, \]

\[ q_3 = -x_1^2 + x_1x_2 - 2x_1x_3 - x_1x_4 - x_1x_5 - 2x_2^2 - 2x_2x_3 - x_2x_4 - x_2x_5 - x_3x_4 - x_3x_5 + x_4^2 + 3x_4x_5 + 2x_5^2, \]

\[ q_4 = -x_1^2 - x_1x_2 - 4x_1x_3 - 2x_1x_5 + 2x_2x_3 + 2x_2x_4 + 2x_2x_5 + 3x_3^2 + x_3x_4 + 2x_3x_5 + 3x_4^2 + 3x_4x_5, \]

\[ q_5 = -4x_1^2 + 3x_1x_2 - 2x_1x_3 + 3x_1x_4 + 3x_1x_5 - 2x_2^2 + 2x_2x_3 - x_2x_4 + x_2x_5 + 4x_3^2 + x_3x_4 - 2x_3x_5 + 2x_4^2 + x_4x_5 - 2x_5^2. \]

We check that $C$ is everywhere locally soluble. The curve $C$ has good reduction for primes different from 2 and 23, so as in the previous example $C$ is automatically locally soluble at those primes. For $q = 2$ and $q = 23$, a computer search quickly finds a smooth point in $C(\mathbb{F}_q)$, which lifts to a point in $C(\mathbb{Q}_q)$ by Hensel's lemma.

As in the previous example, $E$ has rank 0 and $E(\mathbb{Q})[5]$ is trivial, so to prove that the image
of \( c_Q \) in \( \text{III}(E/\mathbb{Q}) \) is non-zero, we show that \( D_\sigma R_\sigma \) is not divisible by 5 in \( E(L) \). It suffices to show that the reduction of \( D_\sigma R_\sigma \) modulo some prime \( p \) of \( \mathcal{O}_L \) is not divisible by 5. Such a prime can be found very quickly by a naive search. In our case, we find that we can take \( p \) to be one of the primes lying above 37. Thus we have shown that \( C \) represents a non-trivial element of \( \text{III}(E/\mathbb{Q}) \).

We also note that by varying the Heegner discriminant \( D \), we can obtain different elements of \( \text{III}(E/\mathbb{Q})[5] \). Indeed, if we instead take the Heegner discriminant to be equal to \( D = -103 \), we obtain the element

\[
B = \begin{pmatrix}
0 & x_2 + x_3 - 2x_4 & x_1 - x_5 & -x_2 + x_3 - 2x_5 & -x_3 - x_5 \\
0 & -x_1 + x_2 - 2x_3 - x_4 - x_5 & x_1 + x_2 + x_4 & -x_2 - x_4 + 2x_5 & -x_4 - x_5 \\
0 & 0 & -x_3 - x_4 & 2x_4 - 2x_5 & 0
\end{pmatrix}
\]

We check, using algorithms for genus one models of degree 5 implemented in MAGMA, that \( B \) is not in the span of \( A \) in \( \text{III}(E/\mathbb{Q})[5] \). Since we know that \( |\text{III}(E/\mathbb{Q})[5]| \cong (\mathbb{Z}/5\mathbb{Z})^2 \), for example by 5-descent, we see that \( A \) and \( B \) are generators for \( \text{III}(E/\mathbb{Q})[5] \).

As explained in Remark 7.6.5, \( C \) capitulates over the field \( L \). As before, there is a hyperplane \( H \) with integer coefficients passing through the points \( R_\sigma, R_{\sigma^2}, R_{\sigma^3} \) and \( R_{\sigma^4} \) on \( C \). We have computed these coefficients, but we do not print them here as they are enormous - the largest one has 201 digits. Note that, as in the case \( p = 3 \), there is no difficulty in computing equations for \( C \) using 5-descent. The extra information from Heegner points tells us that \( C \) capitulates over a rather special number field - in particular over a dihedral extension of \( \mathbb{Q} \). Intersecting \( C \) with a generic hyperplane should give a generic quintic extension, with Galois group \( S_5 \), so we expect that such number fields are rare.

We now give two examples with \( p > 5 \). These are the first such examples we know of - at the moment, the method of complete \( p \)-descent is not feasible for elliptic curves when \( p > 5 \).

**Example 7.6.7.** Let \( E \) be the curve labeled 3364c1 in Cremona’s tables, defined by a minimal Weierstrass equation \( y^2 = x^3 - 4062871x - 3152083138 \). Similarly to the previous examples, we chose \( E \) because it is the smallest rank 0 curve with no rational 7-isogeny and \( \text{III}(E/\mathbb{Q})[7] \cong (\mathbb{Z}/7\mathbb{Z})^2 \).

For the Heegner discriminant, we take \( D = -71 \), which has class number 7. The Hilbert class field \( L \) of \( K = \mathbb{Q}(\sqrt{-71}) \) is a degree 14 dihedral extension of \( \mathbb{Q} \), defined by

\[
f = x^{14} + 7x^{13} + 25x^{12} + 59x^{11} + 103x^{10} + 141x^9 + 159x^8 + 153x^7 + \\
129x^6 + 95x^5 + 58x^4 + 27x^3 + 10x^2 + 3x + 1.
\]

The class group of the Hilbert class field \( L \) of \( K \) is trivial, so \( \mathcal{O}_L \) is a PID. We compute \( R = z_P - Q \) directly, using 250 digits of precision in the computation of modular parametrization, and finding a point of height 194.99. This calculation took less than a minute with our MAGMA implementation.
As before, we use the algorithm of Section 7.4.2 to compute the rational functions \( l_1, l_2, \ldots, l_7 \) that define an embedding \( E \to \mathbb{P}^6 \) over \( L \). The image of the embedding is a curve \( C \), that admits a minimal model defined over \( \mathbb{Q} \). We then reduce this curve, using the algorithm of Section 7.4.3, and then finally compute a basis for the 14-dimensional space of quadrics that cut out the curve \( C \). In our implementation, this takes about a minute. As in the previous example, we check that the curve \( C \) constructed in this way is locally soluble at every prime \( p \). To check that it corresponds to a non-zero element of the Tate-Shafarevich group, and hence has no \( \mathbb{Q} \)-points, we verify that the reduction of \( D_\sigma R_\sigma \) modulo a prime lying above 47 is non-zero.

On the next two pages we give 14 quadrics that define the curve \( C \) after minimization and reduction. Strikingly, the coefficients of all of the equations are remarkably small. We also give the equation of a hyperplane \( H \) passing through the (images of) points \( R_\sigma \), on \( C \) - the coefficients are large, but still much smaller than the coordinates of \( R_\sigma \).
7.6. EXAMPLES

\[ f_1 = 2x_1x_2 - 2x_1x_3 + 2x_1x_5 - x_1x_6 + x_2^2 - x_2x_3 - x_2x_4 + 2x_2x_5 - 4x_2x_6 + 2x_2x_7 - 3x_3^2 - 3x_3x_5 \]
\[ - x_3x_6 + 4x_4^2 - 2x_4x_5 + 3x_4x_6 - x_4x_7 - 3x_5^2 - 4x_5x_6 - x_5x_7 + 2x_6^2 - x_6x_7 - 2x_7^2 \]
\[ f_2 = x_1x_3 + x_1x_4 + x_1x_5 + 2x_1x_6 - x_1x_7 + 4x_2x_4 - x_2x_5 + 2x_2x_6 - 2x_2x_7 - x_3^2 + 4x_3x_4 \]
\[ - 2x_3x_5 + 5x_3x_6 - 3x_3x_7 + x_4^2 + 2x_4x_5 - x_4x_6 - 4x_4x_7 + 3x_5x_6 - 2x_5x_7 + 2x_6^2, \]
\[ f_3 = x_1^2 + 4x_1x_3 + x_1x_5 + x_1x_6 - 4x_1x_7 - x_2x_3 + 3x_2x_4 - 2x_2x_5 + x_2x_6 - x_2x_7 + x_3^2 - 2x_3x_4 + x_3x_5 + x_3x_6 - x_3x_7 - x_4^2 + x_4x_5 + x_4x_6 + 3x_4x_7 + x_5^2 + 2x_5x_6 - 2x_5x_7 + 5x_5^2 \]
\[ - 5x_6^2 - 5x_7^2, \]
\[ f_4 = x_1^2 + 4x_1x_3 + x_1x_5 + x_1x_6 - 6x_1x_7 + x_2^2 + x_2x_3 + 2x_2x_4 + x_2x_5 + x_2x_6 + 2x_2^2 + x_3x_4 + 3x_3x_6 - 3x_3x_7 - x_4^2 - 2x_4x_5 + 2x_4x_6 - 3x_4x_7 + 2x_5^2 + 2x_5x_6 + 3x_7^2 - 4x_6^2 - 4x_6x_7 - x_7^2, \]
\[ f_5 = x_1x_2 - 3x_1x_3 - x_1x_4 - x_1x_5 - 2x_1x_6 + 5x_1x_7 - x_2^2 - x_2x_3 - x_2x_4 - x_2x_5 - 2x_2x_6 + 3x_2x_7 - 3x_3^2 - 3x_3x_5 - 3x_3x_6 - 3x_3x_7 - x_4^2 - 4x_4x_5 + 2x_4x_6 - 2x_4x_7 - 3x_5^2 - 6x_5x_6 - 2x_6x_7 - 3x_7^2, \]
\[ f_6 = 2x_1^2 + x_1x_3 + x_1x_5 + 2x_1x_6 - x_1x_7 + 5x_1x_7 - x_2^2 - 3x_2x_3 - x_2x_4 - x_2x_5 - 2x_2x_6 + 2x_2x_7 - x_3^2 + x_3x_4 + 3x_3x_6 - x_3x_7 - x_4^2 + x_4x_5 + x_4x_6 + 3x_4x_7 + x_5^2 + 2x_5x_6 - 2x_5x_7 + 5x_6^2 \]
\[ - 5x_7^2, \]
\[ f_7 = x_1^2 + x_1x_2 + x_1x_3 + 2x_1x_4 + x_1x_5 + x_1x_6 - 3x_1x_7 - x_2^2 - 2x_2x_3 - 4x_2x_5 + x_2x_6 - 2x_2x_7 + 2x_3^2 - x_3x_4 - 3x_3x_6 - x_3x_7 - x_4^2 - x_4x_5 - x_4x_6 - x_4x_7 - x_5^2 - 3x_5x_6 + 5x_5x_7 - 2x_6^2 - 3x_6x_7 + 5x_7^2, \]
\[ f_8 = x_1^2 + 3x_1x_2 + x_1x_3 + 4x_1x_5 + x_1x_7 - 2x_2^2 + 2x_2x_3 + x_2x_4 - x_2x_5 + 3x_2x_6 + 4x_2x_7 + x_3^2 + x_3x_4 + 4x_3x_5 + x_3x_6 - x_3x_7 - 3x_4^2 + 3x_4x_5 - x_4x_7 - 3x_5^2 + 2x_5x_6 - 4x_5x_7 + x_6^2 - x_6x_7 - 4x_7^2, \]
\[ f_9 = x_1^2 + x_1x_2 + x_1x_3 - 2x_1x_4 + 3x_1x_5 - 2x_1x_6 + x_2^2 - x_2x_3 - x_2x_4 + 2x_2x_5 - x_2x_6 + 4x_2x_7 - x_3^2 - 2x_3x_4 + 3x_3x_5 + 2x_3x_6 + 4x_3x_7 + x_4^2 - 5x_4x_6 - x_5^2 + 5x_5x_6 + 2x_5x_7 - 3x_6^2 + 3x_6x_7 - 2x_7^2, \]
\[ f_{10} = 2x_1x_2 - 3x_1x_3 - 2x_1x_4 + x_1x_5 - x_1x_6 + 2x_1x_7 - 3x_2^2 + x_2x_3 - 4x_2x_4 + 4x_2x_5 + 4x_2x_6 + 2x_2x_7 + x_3^2 + 2x_3x_4 - x_3x_6 - 7x_3x_7 - 4x_4^2 + x_4x_5 + x_4x_6 - 2x_4x_7 - x_5^2 - 2x_5x_6 + 2x_5x_7 - 3x_6^2 + x_6x_7, \]
\[ f_{11} = x_1^2 + x_1x_2 + 3x_1x_3 + x_1x_4 + 2x_1x_5 - 2x_1x_6 - 5x_1x_7 + x_2^2 + x_2x_4 + x_2x_5 - x_2x_6 - 6x_2x_7 - 4x_3^2 + 3x_3x_4 + 3x_3x_5 - 3x_3x_6 - x_3x_7 - 2x_4x_5 - 2x_4x_6 - x_4x_7 - 2x_5x_6 - 2x_5x_7, \]
\[ - 2x_7x_5 - x_7x_6 - 2x_7^2, \]
\[ f_{12} = x_1^2 - 2x_1x_2 + 4x_1x_3 - x_1x_4 - 2x_1x_5 + x_1x_6 + x_1x_7 - x_2^2 + 2x_2x_3 - 4x_2x_4 + 2x_2x_5 - x_2x_6 + 4x_2x_7 + x_3^2 + 3x_3x_6 - 2x_4^2 - 4x_4x_5 - 4x_4x_6 - 2x_4x_7 + 2x_5^2 + 5x_5x_6 + 4x_5x_7 - x_6^2 + 3x_6x_7 + 4x_7^2, \]
\[ f_{13} = 3x_1x_2 - x_1x_3 + 2x_1x_4 + 3x_1x_5 + x_1x_6 + x_2^2 + 2x_2x_4 + x_2x_5 - 2x_2x_7 + x_3^2 - x_3x_4 + 4x_3x_5 - 5x_3x_6 + 3x_3x_7 + 4x_4^2 - 5x_4x_5 + 2x_4x_6 - x_5^2 - 6x_5x_6 - x_5x_7 - 2x_6^2 - x_7^2, \]
\[ f_{14} = x_1^2 + 3x_1x_2 - x_1x_3 - 3x_1x_7 - 2x_2^2 - 2x_2x_3 - x_2x_4 + 2x_2x_5 + 3x_2x_6 - 2x_3^2 + 4x_3x_4 - 4x_3x_5 + 2x_4x_6 + 3x_4x_7 - 2x_5^2 + 4x_5x_6 + 3x_6x_7 - 7x_6^2 + 6x_7x_7. \]
CHAPTER 7. KOLYVAGIN CLASSES

We now give an equation for the hyperplane $H$.

$$
34542637458019442954867343968102379363426084241489245079286056887071608690314
+ 53554287440068976413401551053164653308904117607174511644544936990215764209995
+ 651774347616753864738710459725378644855569214046584583 \cdot x_1 +
+ 2092915203967799872780809646744924654280489101587933007640774369056954565115190
+ 7436332585941992930087790138162002216621575735923527441790771591222579611733444
+ 7274091248479933001765988330764754337199803562383775390 \cdot x_2 +
+ 517547639104289201804588550570690443203708608997738887930798907500354005184580
+ 61106278431748866183423309818997221869992582587663874171180689479277669782667685
+ 6629617788797792928083962230041524425267341494598798880 \cdot x_3 +
+ 2011842252145162883350129266569787983237955935392410745169437216006623096369713
+ 30285238636750313987747561485211218236711597332973351030312109371293384547802363
+ 7667531064129400964504392001887962976833218190805801358 \cdot x_4 -
+ 76080675492236193831943793715931779027781404588679071365000433744603381890315
+ 62840763662672494870982627152151671716522482527302647771192212919773798156053975
+ 17712988154345603985160766897808951863948789617756230 \cdot x_5 -
+ 220078304672845549650456209252468095888038487006238224179670973441735581699
+ 009500137840089191451443316248408608798136656001739475231776593332665493728748
+ 5652512335242962634003669965048105325039228022715250769 \cdot x_6 -
+ 819216261971126237070615128113732233335042241976785243371686035160160006110528
+ 3961832173055262010679525564303833138780832894717765351276174018877211088037781
+ 180819368567876444445469903977673188810299530887001489 \cdot x_7.
$$

Example 7.6.8. To conclude we give an example with $p = 11$. We consider the elliptic curve $E$ labeled 37a1 in Cremona’s tables. This is the rank 1 curve of smallest conductor. As explained in Section 7.2, for curves of rank 1, the Kolyvagin class $c$ is naturally an element of the $p$-Selmer group $\text{Sel}^p(E_D/\mathbb{Q})$, where $E_D$ is the quadratic twist of $E$ by $D$. We take $D = -2731$. This is the smallest value of $D$ for which the BSD conjecture predicts that $\text{III}(E_D/\mathbb{Q})[11] \cong (\mathbb{Z}/11\mathbb{Z})^2$, the Heegner condition is satisfied, the curve $E_D$ is of rank 0, and the class number of $\mathbb{Q}(\sqrt{D})$ is equal to 11.

The curve $E$ is defined by the equation $y^2 + y = x^3 - x$. The field $L$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-2731})$. It is a degree 22 dihedral extension of $\mathbb{Q}$, defined by the equation

$$
x^{22} - 28x^{21} + 396x^{20} - 3674x^{19} + 24812x^{18} - 129080x^{17} + 539180x^{16} -
+ 1876792x^{15} + 5664352x^{14} - 15391790x^{13} + 38390124x^{12} - 87423872x^{11} +
+ 179145147x^{10} - 330090500x^9 + 550943004x^8 - 820329360x^7 +
+ 1045507664x^6 - 1085086912x^5 + 879577280x^4 - 527946240x^3 +
+ 225328896x^2 - 60217344x + 10036224.
$$

Let $\alpha \in L$ be a root of this equation. As before, we compute the point $R = z_D - y_D/11$. The
7.6. EXAMPLES

quadratic twist $E_D$ has a minimal Weierstrass equation $y^2 + y = x^3 - 7458361x - 5092195973$. With respect to this model, the numerator of the $x$-coordinate of $R$ is given in the table below, while the denominator is equal to

$$54008514922943163123827641268100658423160721232625664.$$  

While these numbers seem rather imposing, the point $R$ is significantly simpler than in the examples with $p = 5$ and $p = 7$. The height of $R$ is approximately 3.812, much smaller than before. In this example, the computation of the point $R$ took several minutes of computer time, but in contrast with the earlier examples, most of this time was spent in computing a nice model for the field $L$, and in running the LLL algorithm to recognize the point. Comparatively little time was spent on computing the modular parametrization to high precision. This phenomenon appears to be related with the small conductor of the curve $E$.

<table>
<thead>
<tr>
<th>Monomial</th>
<th>Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha^{21}$</td>
<td>361692949335627821435016397647126108048540509970321</td>
</tr>
<tr>
<td>$\alpha^{20}$</td>
<td>10726571866008126582598012262862110639811735407430406</td>
</tr>
<tr>
<td>$\alpha^{19}$</td>
<td>158929054662600789068116165750940206782898114483404716</td>
</tr>
<tr>
<td>$\alpha^{18}$</td>
<td>15362211154623802431168489641223060223053109237407220058</td>
</tr>
<tr>
<td>$\alpha^{17}$</td>
<td>107577231947126884070272783121236770228466471389073285</td>
</tr>
<tr>
<td>$\alpha^{16}$</td>
<td>57734821708581218872158844883332302964833021907940277536</td>
</tr>
<tr>
<td>$\alpha^{15}$</td>
<td>24705004200578013711440080663907290804051531133577292</td>
</tr>
<tr>
<td>$\alpha^{14}$</td>
<td>8733312274889562767023759433903790663389239126793095021232</td>
</tr>
<tr>
<td>$\alpha^{13}$</td>
<td>26512947684101691977059182598092417308600887884511675476720</td>
</tr>
<tr>
<td>$\alpha^{12}$</td>
<td>720047199730389327110366802737413480330296279062726726009198</td>
</tr>
<tr>
<td>$\alpha^{11}$</td>
<td>1796691009625158323119761308274767685654853708397870035512</td>
</tr>
<tr>
<td>$\alpha^{10}$</td>
<td>40992172977289340751118506752608381967474880160166302605909</td>
</tr>
<tr>
<td>$\alpha^{9}$</td>
<td>8395273493705318234487063965289650961350597558030491249195</td>
</tr>
<tr>
<td>$\alpha^{8}$</td>
<td>15390065782010509729575590242065306019280009769854305048754</td>
</tr>
<tr>
<td>$\alpha^{7}$</td>
<td>25171375962518375280582233213478619764246470363509436338908</td>
</tr>
<tr>
<td>$\alpha^{6}$</td>
<td>370577951732804536004419987556390225625975158120906375926752</td>
</tr>
<tr>
<td>$\alpha^{5}$</td>
<td>46066325458603631000500032163084675471833130541072876196248</td>
</tr>
<tr>
<td>$\alpha^{4}$</td>
<td>4423534309536186007243754138587782493135512736820156167700288</td>
</tr>
<tr>
<td>$\alpha^{3}$</td>
<td>3028792043045820067731101949052771276608177714730295154880</td>
</tr>
<tr>
<td>$\alpha^{2}$</td>
<td>1388806961285597679085104857921474477704315006130684686464</td>
</tr>
<tr>
<td>$\alpha^{1}$</td>
<td>372912565130001260916750068357633984905927000213674055017216</td>
</tr>
<tr>
<td>1</td>
<td>642165069450711858972370751607663542560287937842770013184</td>
</tr>
</tbody>
</table>

As before, we compute a minimal model of a diagram $[C \subset \mathbb{P}^{10}]$ representing the Kolyvagin
class. The curve \( C \) is defined by 44 quadrics in 10 variables. These quadrics have small integer coefficients, in the range \((-12, 10)\), but the sheer number of coefficients makes them impractical to print here. As before, we are also able to compute a hyperplane \( H \) passing through the points \( R_{\sigma_i}, 1 \leq i \leq 11 \). The coefficients are, in contrast with the previous examples, very small:

\[
H = 1593x_1 + 1774x_2 + 849x_3 - 1801x_4 - 324x_5 + 37x_6 - 2178x_7 - 1319x_8 - 805x_9 - 1266x_{10} + 1820x_{11}
\]
Bibliography


