Space-time Codes, Non-associative Division Algebras, and Elliptic Curves

Steve Limburg
University of Colorado at Boulder, steve.limburg@gmail.com

Follow this and additional works at: https://scholar.colorado.edu/math_gradetds
Part of the Algebra Commons, and the Systems and Communications Commons

Recommended Citation
https://scholar.colorado.edu/math_gradetds/11

This Dissertation is brought to you for free and open access by Mathematics at CU Scholar. It has been accepted for inclusion in Mathematics Graduate Theses & Dissertations by an authorized administrator of CU Scholar. For more information, please contact cuscholaradmin@colorado.edu.
Space-time Codes, Non-associative Division Algebras, and Elliptic Curves

by

Steve Limburg

B.A., Colorado College, 2004
M.S., Oregon State University, 2006

A thesis submitted to the
Faculty of the Graduate School of the
University of Colorado in partial fulfillment
of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

2012
This thesis entitled:
Space-time Codes, Non-associative Division Algebras, and Elliptic Curves
written by Steve Limburg
has been approved for the Department of Mathematics

________________________
David Grant

________________________
Sebastian Casalaina-Martin

Date ____________________

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.
Space-time codes are used to reliably send data from multiple transmit antennas and are directly related to non-associative division algebras. While interested in classifying and building space-time codes, using this relationship this thesis considers the corresponding problem of classifying and building non-associative division algebras. The first four chapters develop the problem and give a classification of 4-dimensional non-associative division algebras. Using the classification in chapter 4, I identify a class with no previously known examples. The rest of the thesis develops the background material necessary to understand two methods to build new non-associative division algebras in the aforementioned class. The thesis ends with the methods to build new non-associative division algebras and two examples using the methods. The intermediary steps used in the construction of the examples use tools from the arithmetic of elliptic curves over number fields, commutative algebra, and algebraic number theory.
## Contents

### Chapter

1. **Introduction**  
   1

2. **Communications Motivation**  
   4
   
   2.1 Codes  
   4
   
   2.2 Non-associative Division Algebras  
   8
   
   2.3 Associative Division Algebras  
   15

3. **Background Mathematics**  
   17
   
   3.1 Some Notions from Algebraic Geometry  
   17
   
   3.2 Hilbert Polynomials  
   19
   
   3.3 Quadric Surfaces  
   20
   
   3.4 Group Cohomology  
   24
   
   3.5 Cyclic Quartic Extensions  
   26
   
   3.6 Determinantal Ideals  
   26

4. **Possible Factorizations of an Anisotropic Quartic Form**  
   31
   
   4.1 Arithmetic of \( f \)  
   32
   
   4.2 Geometry of \( X \)  
   35
   
   4.3 Putting the Arithmetic and Geometry Together  
   36
   
   4.4 Known Examples of 4-dimensional NADAs  
   39
## Elliptic Curves

5.1 Properties of Elliptic Curves .................................................. 45
5.2 Homogeneous Spaces .............................................................. 48
5.3 The Selmer and Tate-Shafarevich Groups ................................... 52
5.4 Rational $4$-torsion and homogeneous spaces ............................ 58
5.5 Explicit Equations for a Family of Elliptic Curves and Their Twists . . . 62

## $f$ Factors into Two Quadrics over a Quadratic Extension

6.1 Building a $4 \times 4$ Matrix ......................................................... 69
6.2 Main Theorem ........................................................................... 72
6.3 Rational $2$-torsion and $4$-torsion Corollaries ............................ 78

## Methods to Build New NADAs

7.1 Examples using Methods 1 and 2 .............................................. 84

## Bibliography

92
Chapter 1

Introduction

Non-associative algebras, which we will abbreviate as NAAs, have a rich history. Some of the notable mathematicians who have considered their study include Dickson, Albert, Menichetti, Bhargava, and many others. While much is known about NAAs, there are still many open questions — even for NAAs of relatively low dimension. This thesis focuses on non-associative division algebras (NADAs) of dimension 4 over a number field $K$. Our motivation for studying NADAs over $K$ is that NADAs can be used to construct “space-time codes” which are used to increase reliability of communication in systems with more than one transmit antenna. We will detail this engineering application in Chapter 2. As with associative algebras, given a choice of basis for a NAA, there is a left-regular representation of the algebra. For a 4-dimensional NAA over $K$, this representation will be a $4 \times 4$ matrix with entries that are $K$-linear forms in 4 variables. We give a classification of 4-dimensional NADAs over $K$ depending on how the determinant of the left-regular representation factors over $\bar{K}$, an algebraic closure of $K$. Under this classification there are known examples of NADAs over $K$ that populate most of the classes, but there are several classes with no known examples. We study one of these classes — which heretofore was unknown to contain any NADAs — and produce methods to build examples in this class using elliptic curves.

More specifically, attached to an elliptic curve $E$ defined over $K$, are other genus 1 curves defined over $K$ called homogeneous spaces. Geometrically, homogeneous spaces and
the elliptic curve are the same, but arithmetically they can be different, i.e. \( E \cong C \) over \( \bar{K} \) but \( C \) is only isomorphic to \( E \) over \( K \) when \( C \) has a \( K \)-rational point. It is precisely this ability of certain \( C \) to have no \( K \)-rational points which we exploit to build NADAs over \( K \). By forcing some arithmetic conditions on \( E \) (or equivalently by forcing arithmetic conditions on a homogeneous space \( C \)) one of the main results of this thesis is that there is a correspondence between these elliptic curves with arithmetic conditions and 4-dimensional NADAs over \( K \) that populate one of the classes with no previously known examples.

In more detail, let \( A \) be a 4-dimensional NADA over \( K \), and let \( f_A \) be the determinant of its left-regular representation. Then \( f_A \) is a quartic form in 4 variables. Suppose \( f_A \) is irreducible over \( K \) but factors into absolutely irreducible quadratics over a quadratic extension, \( K' \) of \( K \), with \( \text{Gal}(K'/K) = <\sigma> \). That is, \( f_A \) factors as \( qq^\sigma \) over \( K' \), and if \( \mathcal{H} \), the zero locus of \( q \) and \( q^\sigma \) in \( \mathbb{P}^3 \), happens to be an irreducible curve, then we show that \( \mathcal{H} \) is a homogeneous space (with no \( K \)-rational points) for an elliptic curve \( E/K \) which has a divisor of a certain type. So the correspondence of most interest (which will be studied more closely in Chapter 6) is

\[
\begin{align*}
\{ \text{Elliptic curves over } K \\
\text{with certain arithmetic conditions} \} & \leftrightarrow \{ \text{4-dimensional NADAs over } K \\
\text{such that the determinant} \} \\
\text{of the left-regular representation} & \leftrightarrow \{ \text{factors in a certain way} \}.
\end{align*}
\]

To get to this correspondence, we need to solve a more fundamental problem along the way. The function \( \mu(A) = f_A \) is a map from NADAs over \( K \) to the set \( T \) of quaternary quartics over \( K \) with no non-trivial \( K \)-rational solutions. There is a subset \( T^Q \) of \( T \) of those quartics which factor as \( qq^\sigma \) over some quadratic extension \( K' \) of \( K \) with \( \text{Gal}(K'/K) = <\sigma> \), such that \( q, q^\sigma \) are absolutely irreducible, and \( V(q, q^\sigma) \) is irreducible. The class of NADAs over \( K \) we will be studying is \( N^Q = \mu^{-1}(T^Q) \). Key to our investigation is studying the image,
\( \mu(N^Q) \subset T^Q \). We prove that the image consists precisely of those quartics which factor as \( qq^0 \) over \( K' \) and such that the quadric surface \( V(q) \subset \mathbb{P}^3 \) contains a \( K' \)-rational line. We also study under what conditions \( \mu(A) = \mu(A') \), for NADAs \( A \) and \( A' \).

This thesis is laid out as follows. Chapter 2 shows the connections between space-time codes over \( K \), 4-dimensional NADAs over \( K \), and homogeneous quartic polynomials in \( K[x, y, z, w] \) with no non-trivial solutions over \( K \). Chapter 3 gives all of the necessary mathematical background to understand the constructions that are given in the latter chapters. Chapter 4 gives the classification of quartic forms in 4 variables with no \( K \)-rational points depending on how they factor over \( \overline{K} \), and will identify the class of NADAs for which we produce new examples. The rest of the thesis lays the groundwork to build these new examples. Chapter 5 contains all of the necessary background material on the theory of elliptic curves. Chapter 6 gives the main theorems outlined above, and Chapter 7 gives two methods of constructing NADAs from elliptic curves and gives several examples of new NADAs using these methods.
Chapter 2

Communications Motivation

2.1 Codes

The goal of this section is to start with an introduction to classical coding theory and to end with a discussion of the theory of space-time codes, part of which is the motivation for this dissertation. Throughout this thesis \( k \) will denote a perfect field and \( \bar{k} \) will denote an algebraic closure of \( k \). For any commutative ring \( R \) we let \( \mathcal{M}_n(R) \) denote the ring of \( n \times n \) matrices with entries in \( R \). For any \( M \in \mathcal{M}_n(R) \) we will write \( \det M \) for the determinant of \( M \), and we will write \( \text{adj} M \) for the (classical) adjoint of \( M \).

Much of the material on codes in this section can be found in [30]. Codes are used to add redundancy to messages so we can more reliably transmit data either through the air (radio waves) or wires (telephone, cable, fiber optic, etc.). This redundancy is added so that if the received signal is slightly different from the transmitted coded message, we are still able to recover the information in the (coded) message.

**Definition 2.1.1.** Given an alphabet \( S \) (a finite set), a code of length \( m \) is a subset \( C \subset S^m \). We call elements of \( C \) codewords. If \( S \) is a field \( k \), we say \( C \) is a \( k \)-linear code of length \( m \) if it is a \( k \)-vector subspace of \( k^m \). Let \( C \) be a \( k \)-linear code of length \( m \). Then we define the dimension of \( C \) to be the dimension of \( C \) as a \( k \)-vector space. If \( \dim_k C = n \), then we define the rate of \( C \) to be \( n/m \).

If \( C \) is a \( k \)-linear code of length \( m \) and dimension \( n \), then there exists \( n \) linearly independent vectors of length \( m \) in \( C \). Let \( G \) be the \( m \times n \) matrix with columns consisting
of these vectors: we call $G$ a generating matrix of $C$. We then have $C = \{Gv|v \in k^n\}$.

We would like to have a metric to judge how “good” a code is. That is, a measure of how much it increases our ability to decode information. Often the appropriate metric is the Hamming distance.

**Definition 2.1.2.** For two codewords $x,y \in C$, the Hamming distance between them is $d(x,y) = \#\{i|x_i \neq y_i\}$. The minimal distance of the code $C$ is

$$d_C = \min_{x \neq y \in C} d(x,y).$$

Why is this metric of interest? Classically, information (in the form of codewords) was sent via one transmit and one receive antenna. If the transmission is via a radio wave, then what is transmitted is a complex number $x$: its modulus is the amplitude of the wave and its argument is the phase. The mathematical model for this channel is

$$y = hx + \eta,$$

where $\eta \in \mathbb{C}$ is the “noise” (which is a continuous random variable whose distribution is a property of the channel), $h \in \mathbb{C}$ is the channel gain (one can think of power, and it is a random variable whose distribution is a property of the channel) and $y \in \mathbb{C}$ is the received signal. The above model is applied to $T$ uses, or time slots, of the channel. So then we have

$$y_i = h_ix_i + \eta_i,$$

$1 \leq i \leq T$. If $h_i$ is constant over the $T$ time slots, then we say that the channel is slow fading. The model for this channel is then

$$\vec{y} = h\vec{x} + \vec{\eta},$$

where $\vec{x},\vec{y} \in \mathbb{C}^T$, and we assume $\vec{\eta}$ is a vector of identically distributed independent random variables.
Where the coding theory comes into play is that we pick a bijection $\iota$ from our alphabet $S$ to a finite set $U \subset \mathbb{C}$ (there is an art to picking $U$ called modulation). This induces a bijection $\iota : S^T \to U^T \subset \mathbb{C}^T$ and for a code $C \subset S^T$ we let $\mathcal{C} = \iota(C) \subset \mathbb{C}^T$. The way we send a message $v \in k^n$ is to encode it as $Gv \in C$ and then modulate it as $x = \iota(Gv) \in \mathcal{C}$. We then transmit the vector $x$ over our channel. Having received $y \in \mathbb{C}^T$, we need a way to decode $y$, i.e. choose an $\tilde{x} \in \mathcal{C}$ given $y$. The point of code and modulation design, i.e. picking $C \subset k^T$, $\iota : C \to U \subset \mathbb{C}^T$ is to guarantee both low probability of pair error, $P_e = P(\tilde{x} \neq x)$, as well as computational ease of decoding. Instituting structure (algebraic or otherwise) on $\mathcal{C}$ helps with both of these tasks. If we pick $C$ and $\iota : C \to U$ such that they have enough structure, a lattice in $\mathbb{C}^T$ for instance, then decoding is computationally feasible. For codes $C$ with certain structure, decoding via the Hamming distance is known to minimize the pair error probability.

The above has a very natural generalization, which has been a major area of communications research in recent years. Suppose there are $n_t$ transmit and $n_r$ receive antennas, and that a message is sent over $T$ time slots. Then we can extend our mathematical model for this channel to

$$y_s = Hx_s + \eta_s,$$

where $1 \leq s \leq T$ is a time index, $x_s \in \mathbb{C}^{n_t}$ is the transmitted vector at time $s$, $\eta_s \in \mathbb{C}^{n_r}$ is the noise, the entries for all $\eta_s$ are random variables which are independent and identically gaussian distributed, $H \in \mathcal{M}_{n_r \times n_t}(\mathbb{C})$ is the matrix of channel gains (the $ij^{th}$ entry is a random variable whose distribution depends on the channel and measures the relative strength between transmit antenna $i$ and receive antenna $j$), and $y_s \in \mathbb{C}^{n_r}$ is the received vector. Note that everything in the above model depends on the time $s$ except $H$ because we will assume the channel to be slow fading.

With this model messages are sent across both spatial and temporal variables. Codes of this type are called space-time codes, and a codeword is a matrix $x = (x_1, \ldots, x_T) \in \mathcal{M}_{n_t \times T}$,
and the received signal is a matrix $y = (y_1, ..., y_T) \in \mathcal{M}_{n_r \times T}$. In this more general setting $H$ is assumed to be of full rank. This is a reasonable assumption because if $H$ were not of full rank then one would use fewer transmit antennas to save power and yet have the same effect. Thus we can talk about $H^{-1}y \in \mathcal{M}_{n_t \times T}$. Here the space-time code $\mathcal{C}$ lies in $\mathcal{M}_{n_t \times T}(\mathbb{C})$, but in [12] they show that without loss of generality one can assume that a code $\mathcal{C}$ is contained in $\mathcal{M}_{n_t \times T}(K)$, where $K$ is a number field. Depending on how the entries of $H$ are modeled as random variables, the Hamming distance is not the appropriate metric to use to decode space-time codes.

**Definition 2.1.3.** The rank metric for two matrices $A, B$, of the same size is denoted by $d_{rk}(A, B) = \text{rank}(A - B)$. The rank distance for a space-time code $\mathcal{C} \subset \mathcal{M}_{n_t \times T}(\mathbb{C})$ is defined as

$$d_{rk}(\mathcal{C}) = \min\left\{ d_{rk}(A, B) | A, B \in \mathcal{C} \text{ with } A \neq B \right\}.$$  

In [29] they show that if the entries of $H$ are independent identically Rayleigh distributed random variables, then maximizing the rank metric of $H^{-1}y$ to an $\tilde{x} \in \mathcal{C}$ minimizes the probability of pair error, $P(\tilde{x} \neq x)$, for space-time codes. Although in practice $C$ is a finite set, mathematically we prefer to allow it to be infinite (and we just transmit from a finite subset). To allow $\iota(C)$ to lie in a lattice in $\mathbb{C}^n$, let $\mathcal{O}_K$ denote the ring of integers of the number field $K$. We will consider the case where $C$ is a rank $n$ $\mathcal{O}_K$-submodule of $\mathcal{M}_{n_t \times T}(K)$. Then $C \otimes K$ is an $n$-dimensional $K$-vector space, and we will set $\dim_K C = \dim_K C \otimes K$.

For space-time codes we need to generalize the idea of a generating matrix given above. Let $C$ be a rank $n$ $\mathcal{O}_K$-submodule of $\mathcal{M}_{n_t \times T}(K)$. Then there exists $n$ elements $c_i \in C$ that form a basis for $C$ over $\mathcal{O}_K$. Let $\{x_i\}_{i=1}^n$ be independent indeterminates and define

$$G_C = \sum_{i=1}^n x_i c_i.$$  

We call $G_C$ the generating matrix for $C$. Note the entries of $G_C$ are linear forms over $K$ in $n$ variables.
Throughout the rest of the paper we will use the word “code” to mean a space-time code. Suppose that a code $C$ is an $\mathcal{O}_K$-submodule of $\mathcal{M}_{n_t \times T}(K)$. Then it is clear that the maximal (rank) distance the code can have is $\min(n_t, T)$. But, a “good” code should also have maximum rate, i.e. the rate should be as large as possible. So our goal is to maximize $d_{rk}(C)$ and then, for the maximum $d_{rk}(C)$, to maximize $\dim_K C$. For $C \subset \mathcal{M}_{n_t \times T}(K)$ we trivially have $d_{rk}(C) \leq \min(n_t, T)$, but equality is possible. When we achieve equality, we say that $C \otimes K$ is a maximal non-singular space, and it happens precisely when each non-zero $c \in C$ has maximal rank. Let $n = \max(n_t, T)$. If $C \otimes K$ is a maximal non-singular space in $\mathcal{M}_n(K)$, then chopping off rows or columns gives a maximal non-singular space in $\mathcal{M}_{n_t \times T}(K)$. So we will concentrate on building maximal non-singular spaces in $\mathcal{M}_n(K)$. If $C$ is an $\mathcal{O}_K$-submodule of $\mathcal{M}_n(K)$ and $d_{rk}(C) = n$, considering the top rows of elements in $C$ shows $\dim_K C \leq n$. The codes we want to construct are maximal non-singular spaces in $\mathcal{M}_n(K)$ which meet this bound, i.e. $C$ will be a code in $\mathcal{M}_n(K)$ such that $d_{rk}(C) = n$ and $\dim_K C = n$.

The space-time codes $C$ that this thesis will consider have $C \otimes K$ being a maximal non-singular space of dimension 4 over a number field $K$, i.e. $C$ is an $\mathcal{O}_K$-submodule of $\mathcal{M}_4(K)$, $d_{rk}(C) = 4$, and $\dim_K C = 4$. In the next section, we show that codes of this type correspond to 4-dimensional non-associative division algebras over $K$.

### 2.2 Non-associative Division Algebras

Let $k$ be a perfect field with $\text{char } k \neq 2$, and $K$ a number field. Non-associative algebras over $k$, which we abbreviate as NAAs — have long been studied (see [25]) and here we present the concept in full generality. Note that most of the concepts below are exactly analogous to the corresponding concepts for associative algebras.

**Definition 2.2.1.** A $k$-algebra $A$ is a pair $(V, \ast)$, where $V$ is a $k$-vector space and $\ast : V \times V \to$
$V$ is a $k$-bilinear map, that is,

$$r(a \ast b) = a \ast rb = ra \ast b,$$

$$(a + b) \ast c = (a \ast c) + (b \ast c), \ a \ast (b + c) = (a \ast b) + (a \ast c),$$

for $r \in k$, $a, b, c \in V$.

Furthermore, if an algebra $A$ satisfies $a \ast b = b \ast a$ for all $a, b \in A$, we call it commutative, and if it satisfies $(a \ast b) \ast c = a \ast (b \ast c)$ for all $a, b, c \in A$, then we call it associative. If these conditions are not assumed to hold we say $A$ is non-commutative or non-associative. We emphasize that we will use the term non-associative to describe algebras which may or may not be associative. Unless otherwise specified, by “algebra” we will mean a non-associative algebra.

**Definition 2.2.2.** An algebra $A$ is called a *division algebra* if the equations

$$a \ast x = b \text{ and } y \ast a = b$$

have unique solutions $x, y \in A$ for fixed $a, b \in A$ and $a \neq 0$. This is equivalent to the condition that the maps $L_a, R_a : V \to V$ defined by $L_a(x) = a \ast x, \ R_a(y) = y \ast a$, are invertible for all $a \in A - \{0\}$.

We will use the acronym NADA to stand for “non-associative division algebra”.

**Definition 2.2.3.** We say the *dimension* of a $k$-algebra $A$, denoted $\dim_k A$, is the dimension of $V$ as a $k$-vector space (if $k$ is apparent from context, we will omit it from the notation). If $\dim_k V$ is finite, we say $A$ is a *finite dimensional* $k$-algebra; otherwise it is *infinite dimensional*.

**Definition 2.2.4.** We say an element $a \in A - \{0\}$ is a *left zero divisor* of $A$ if there exists $b \in A - \{0\}$ such that $a \ast b = 0$. Analogously, we define right zero divisors. An element $a \in A$ is a *zero divisor* if is a left or right zero divisor.
**Proposition 2.2.5.** A finite dimensional algebra $A$ is a division algebra if and only if $A$ has no zero-divisors.

*Proof.* Suppose $A$ is a division algebra. Then $L_a$ and $R_a$ are invertible for all $a \neq 0$. But since $V$ is finite dimensional, this implies that $L_a$ and $R_a$ are isomorphisms for all $a \in A$. Thus $a$ is not a zero divisor for all non-zero $a \in A$. For the converse, suppose $A$ has no zero-divisors. This implies that $L_a$ and $R_a$ are injective. But since $A$ is finite dimensional this means that $L_a$ and $R_a$ are invertible. \qed

**Definition 2.2.6.** Two $k$-algebras $A, B$ are *isomorphic* if there is an isomorphism of the underlying vector spaces which respects the multiplication. So if $A = (V, \ast)$ and $B = (W, \cdot)$, then $A \cong B$ if there exists a $k$-vector space isomorphism $\phi : V \to W$ such that $\phi(a \ast b) = \phi(a) \cdot \phi(b)$.

In an attempt to classify all non-associative $k$-algebras (of a given dimension) Albert found there were too many isomorphism classes so in [1] he introduced the following more general equivalence of algebras.

**Definition 2.2.7.** Two $k$-algebras, $A = (V, \ast)$, $B = (W, \cdot)$ are said to be $k$-*isotopic* if there exists a $k$-vector space isomorphism $V \xrightarrow{\iota} W$ and automorphisms, $\phi, \rho, \sigma$ of $V$ such that $\iota((\phi(a) \ast \rho(b))^{\sigma}) = \iota(a) \cdot \iota(b)$ for all $a, b \in V$.

Note isotopy is more general then isomorphism because if $\iota : A \to B$ is an isomorphism of algebras $A = (V, \ast), B = (W, \cdot)$, then letting $\phi, \rho, \sigma$ be the identity gives $\iota(a \ast b) = \iota(a) \cdot \iota(b)$ for all $a, b \in A$. We will only be interested in building or classifying non-associative division algebras up to isotopy.

We would like to point out one major difference between NADAs and associative division algebras. Unlike for associative division algebras, Albert in [1] showed that if $A$ is a NADA, then $A$ does not in general have a multiplicative identity. However, if $A = (V, \ast)$...
is a NADA without identity, then there is a NADA $B$ such that $A$ and $B$ are isotopic and $B$ has a multiplicative identity. To see this, let $x, y \in A - \{0\}$. Since $A$ is a NADA, the maps $L_x, R_y$ are isomorphisms of $A$, which we can view as automorphisms of $V$. Now let $B = (V, \cdot)$ where multiplication in $B$ is defined by $r \cdot s = (R_y^{-1}r \ast L_x^{-1}s)$ for all $r, s \in B$. It is easily checked that $B$ is a NADA which is $k$-isotopic to $A$. Now the element $x \ast y$ is a multiplicative identity of $B$. As with associative algebras, the multiplicative identity is 2-sided and unique.

Now we would like to understand the correspondence between NAAs and forms of given degree.

**Definition 2.2.8.** Suppose we have a non-associative algebra $A$ over $k$, such that $\dim_k A = n < \infty$. Let $B_1, B_2, B_3$ be three $k$-bases of $A$. For any $a, b, c \in A$ such that $a = b \ast c$, we write their coordinates with respect to the different bases as the column vectors $[a]_{B_1}, [b]_{B_2}, [c]_{B_3}$. Then by the bilinearity of $\ast$ there exists $M_i \in M_n(k)$ such that

$$[a]_{B_1} = (\sum_{i=1}^{n} b_i M_i)[c]_{B_3},$$

where $b_i$ is the $i^{th}$ entry of $[b]_{B_2}$. Let $\{x_1, \ldots, x_n\}$ be independent indeterminates and consider $M_A = \sum_{i=1}^{n} x_i M_i$. We call $M_A$ the **left-regular representation** of $A$. We will let $F_A = \det M_A$.

Similarly there exits $N_i \in M_n(k)$ such that

$$[a]_{B_1}^t = [b]_{B_2}^t (\sum_{i=1}^{n} c_i N_i),$$

where $c_i$ is the $i^{th}$ entry of $[c]_{B_3}$. We define the **right-regular representation** of $A$ to be $N_A = \sum_{i=1}^{n} x_i N_i$.

**Lemma 2.2.9.** Let $A$ be a finite dimensional $k$-algebra. Then $A$ has zero-divisors if and only if the form $F_A$ has non-trivial solutions over $k$. The analogous assertion holds for the determinant of the right representation, $\det N_A$. 
Proof. By definition 2.2.8,
\[ \sum_{i=1}^{n} b_i M_i \]
has a trivial null space for all \((b_1, \ldots, b_n)^t \in k^n - \{0\}\) if and only if \(F_A\) has no non-trivial solutions over \(k\).

We say that a homogeneous polynomial \(F\) in \(m\) variables and of degree \(n\) is an \(m\)-ary \(n\)-form. A \(k\)-anisotropic form is a form with coefficients in \(k\) which has no non-trivial solutions in \(k\). So Definition 2.2.8 says an \(n\)-dimensional non-associative algebra \(A\) over \(k\) gives rise to a corresponding \(n\)-ary \(n\)-form, \(F_A = \det M_A\), defined over \(k\), and Lemma 2.2.9 says that \(A\) is a NADA if and only if \(F_A\) is a \(k\)-anisotropic form. But now we consider the converse construction. Given an \(n\)-ary \(n\)-form \(F\) over \(k\), what are the necessary conditions for it to be the determinant of a left-regular representation of a \(n\)-dimensional NAA over \(k\)?

**Definition 2.2.10.** We say an \(n\)-form \(F \in k[x_1, \ldots, x_n]\) is determinantal over \(k\) if there exists linear forms \(l_{ij} \in k[x_1, \ldots, x_n]\) such that if \(L = [l_{ij}]_{1 \leq i, j \leq n}\), then \(\det L = F\).

**Proposition 2.2.11.** Let \(F\) be an \(n\)-ary \(n\)-form determinantal over \(k\). Then there is a NAA \(A_L\) over \(k\) such that \(F\) is the determinant of the left-regular representation of \(A_L\).

Proof. Suppose \(F\) is determinantal and let \(L\) be a \(n \times n\) matrix of linear forms in \(k[x_1, \ldots, x_n]\) such that \(\det L = F\). Now consider the decomposition \(L = \sum_{i=1}^{n} x_i L_i\) with \(L_i \in \mathcal{M}_n(k)\), and let \(V = k^n\). We have the canonical basis, \(\{e_i\}\) of \(V\) and we define \(L_{e_i} : V \to V\) by \(e_i * v = L_i v\). We then extend the left multiplication of \(V\) to make it \(k\)-linear. Then \(A_L = (V, *)\) is an \(n\)-dimensional non-associative algebra over \(k\), whose left-regular representation is \(L\).

Lemma 2.2.9 implies that \(A_L\) has zero-divisors if and only if \(F\) has non-trivial \(k\)-rational solutions. Thus if we start with an \(k\)-anisotropic determinantal form \(F\), then \(A_L\) is a NADA.

The above leads to the following diagram:
where the map \( \rho \) is defined by \( A \mapsto M_A \) and the map \( \mu \) is defined by \( M \mapsto \det M \). The proof of Proposition 2.2.11 shows \( \rho \) is a bijection.

**Remark 2.2.12.** There may be multiple \( L \) such that \( \det L = F \) and in fact, the “twisted fields” of Section 4.4 will provide examples where \( \{ A_L | \det L = F \} \) contains non-isotopic algebras.

Proposition 2.2.11 shows that \( \mu \) is surjective but Remark 2.2.12 illustrates that \( \mu \) is not injective.

The following lemma will tie in space-time code design with NADAs. Part (1) follows from the fact that a matrix is non-singular if and only if its determinant does not vanish, and part (2) follows from the proof of Lemma 2.2.9.

**Lemma 2.2.13.** Let \( K \) be a number field and \( x_1, \ldots, x_n \) be indeterminants.

1. If \( V \) is an \( n \)-dimensional subspace of \( \mathcal{M}_n(K) \) with basis \( P_i, 1 \leq i \leq n \), then \( V \) is a maximal nonsingular space if and only if the determinant of the linear matrix \( P_V = \sum_{i=1}^n x_i P_i \) is \( K \)-anisotropic.

2. Let \( P_i \in \mathcal{M}_n(K), 1 \leq i \leq n, \) be such that the determinant of the linear matrix \( P = \sum_{i=1}^n x_i P_i \) is \( K \)-anisotropic. Then \( P \) is the left-representation of an \( n \)-dimensional non-associative division algebra over \( K \).
The above lemma shows that we get the following restriction (and expansion) of Equation 2.1.

\[ \begin{align*}
\text{NADAs } A \text{ over } K \\
\text{with } \dim A = n \\
\text{up to isotopy}
\end{align*} \xrightarrow{\rho} \begin{align*}
\text{Linear matrices } M &= \sum_{i=1}^{n} x_i M_i \\
\text{where } M_i &\in M_n(K) \\
\text{is a basis of a maximal} \\
\text{non-singular space up to} \\
\text{multiplying } M \text{ on the left or} \\
\text{right by an invertible matrix or} \\
\text{replacing } \vec{x} \text{ by a } K\text{-linear} \\
\text{change of variables}
\end{align*} \xrightarrow{\mu} \begin{align*}
\text{n-ary degree } n \\
\text{K-anisotropic} \\
\text{determinantal forms}
\end{align*} \tag{2.2}

\[ \tau \]

\[ \begin{align*}
\text{Generating matrices } G \\
\text{of space-time codes} \\
\text{over } K \text{ with } \dim_K C = \\
d_{rk}(C) = n \text{ up to multiplying } G \\
on the left and/or right \\
by invertible matrices or a \\
K\text{-linear change of variables in } G
\end{align*} \]

We would like to consider the map \( \tau \) further. A code \( C \) with a chosen basis \( \{P_i\} \) is only defined up to the span of \( P_i \). So letting \( Q_i = \sum a_{ij} P_j \) for any matrix \( A = (a_{ij}) \in M_n(K) \) such that \( \det A \neq 0 \) will satisfy \( C \otimes K = \text{span}_K\{Q_i\} = \text{span}_K\{P_i\} \). So Lemma 2.2.13 implies that the map \( \tau \) is a bijection.

Although our motivation is to classify and build space-time codes over number fields
$K$ of dimension 4, we will use Equation 2.2 to solve the equivalent problem of building/classifying 4-dimensional NADAs over $K$.

### 2.3 Associative Division Algebras

As above, $k$ will be a perfect field with $\text{char } k \neq 2$. The goals of this thesis are to classify and build new 4-dimensional non-associative division algebras. Towards this end we would like to recall the well understood theory of associative division algebras over fields. This will be useful for verifying that the algebras we will build are not associative algebras. The material for this section can all be found in [23].

For any degree four field extension $[L : k] = 4$, $L$ can be regarded as a degree 4 associative division algebra over $k$. The algebra multiplication is just the field multiplication. The rest of this section covers more general associative $k$-algebras $(A, \ast)$. We will use the standard notation $Z(A)$ to stand for the center of $A$. Recall $x \in Z(A)$ means that $x \ast y = y \ast x$ for all $y \in A$. Recall $M_r(k)$ is the $k$-algebra whose elements are matrices of size $r \times r$ with entries in $k$.

**Definition 2.3.1.** An algebra $A$ is *simple* if it contains no non-trivial two-sided ideals. A $k$-algebra is a *central simple $k$-algebra* if it is simple and $Z(A) = k$.

Since associative division algebras have identities, they have no non-trivial ideals and so are simple. We will let $\mathcal{S}(k) = \{\text{central simple algebras } A|Z(A) = k \text{ and } k \text{ is a field}\}$.

**Lemma 2.3.2 ([23], p.236).** If $A \in \mathcal{S}(k)$ then $\dim_k A = m^2$ for some $m \in \mathbb{N}$.

**Definition 2.3.3.** We will define the *degree* of $A$, written $\text{Deg } A$, to be $(\dim_k A)^{1/2}$ for $A \in \mathcal{S}(k)$.

For any $a, b \in k$ we define a *quaternion algebra* to be a degree 2 central simple algebra over $k$ with basis $\{1, i, j, ij\}$ and multiplication given by $i^2 = a$, $j^2 = b$, $ij = -ji$ and then extended by $k$-linearity and associativity.
Theorem 2.3.4 ([23], p.236). If \( \text{char } k \neq 2 \), \( A \in \mathfrak{S}(k) \) and \( \text{Deg } A = 2 \), then \( A \) is isomorphic to a quaternion algebra.

Recall that a quaternion algebra is either split (isomorphic to \( \mathcal{M}_2(k) \)) or non-split (a division algebra). We are interested in the case where \( A \) is a division algebra with the property that it is associative and \( \dim_k A = 4 \). Any associative division algebra \( A \) is simple, so it is central simple over its center. So if \( A \) is an associative division algebra and \( \dim_k A = 4 \) it is either a field extension of degree 4 (central simple of degree 1), or if \( \text{char } k \neq 2 \), a quaternion algebra (central simple of degree 2). Thus if \( \text{char } k \neq 2 \), any associative 4-dimensional division algebra over \( k \) is either a field extension of degree 4 or a non-split quaternion algebra.
Chapter  3

Background Mathematics

3.1  Some Notions from Algebraic Geometry

We assume the reader is familiar with a basic knowledge of algebraic geometry, e.g. definitions of projective varieties, dimension, and divisors. This section serves to establish notation. Let \( k \) be a perfect field and \( \overline{k} \) be an algebraic closure of \( k \). Let \( F \) be a Galois field extension of \( k \) with \( G = \text{Gal}(F/k) \). Let \( H \) be a subgroup of \( G \). Then we will use the notation \( \text{Fix}(F,H) \) to mean the subfield of \( F \) containing \( k \) fixed by \( H \).

Let \( \mathbb{P}^n \) denote projective \( n \)-space. Let \( f_1, \ldots, f_m \in \overline{k}[x_0, \ldots, x_n] \) be \( m \) homogeneous polynomials. Let \( V(f_1, \ldots, f_m) \) be the algebraic set of points \( x \in \mathbb{P}^n(\overline{k}) \) that satisfy \( f_1(x) = \ldots = f_m(x) = 0 \). Given a set of points \( X \subset \mathbb{P}^n(\overline{k}) \), let \( I(X) \) be the homogeneous ideal in \( \overline{k}[x_0, \ldots, x_n] \) consisting of those \( f \in I(X) \) such that \( f(x) = 0 \) for all \( x \in X \). We will say \( X \) is defined over \( k \) if \( I(X) \) has generators that lie in \( k[x_0, \ldots, x_n] \). A variety over \( \overline{k} \) (respectively \( k \)) is an absolutely irreducible algebraic set defined over \( \overline{k} \) (respectively \( k \)). We reserve the word morphism to be a morphism of the underlying varieties in \( \mathbb{P}^n(\overline{k}) \). All divisors that we use are Weil divisors.

**Definition 3.1.1.** Let \( \mathcal{X} \) be a non-singular variety defined over \( \overline{k} \) and \( D_1 = \sum n_1(P)P \) and \( D_2 = \sum n_2(P)P \) be two divisors of \( \mathcal{X} \), the sums being over irreducible codimension 1 subvarieties of \( \mathcal{X} \). We say \( D_1 \geq D_2 \iff n_1(P) \geq n_2(P) \) for all \( P \). Let \( \deg D_1 = \sum n_1(P) \).

We will denote the group of divisors on \( \mathcal{X} \) by \( \text{Div}(\mathcal{X}) \) and the set of divisors of degree \( n \) by
Div\textsuperscript{n}(\mathcal{X}).

If \mathcal{X} is defined over \mathbb{k}, and \textit{G} = \text{Gal}(\bar{\mathbb{k}}/\mathbb{k})\text{, we let } \text{Div}_{k}(\mathcal{X}) \text{ and } \text{Div}_{k}^{n}(\mathcal{X})\text{ respectively denote the elements of } \text{Div}(\mathcal{X}) \text{ and } \text{Div}\textsuperscript{n}(\mathcal{X}) \text{ fixed by } \textit{G}.

We let \bar{k}(\mathcal{X})\text{ denote the function field of } \mathcal{X}, \text{ and if } \mathcal{X} \text{ is defined over } \mathbb{k}, \mathbb{k}(\mathcal{X})\text{ denote the function field of } \mathcal{X} \text{ over } \mathbb{k}, \text{ which is } \text{Fix}(\bar{k}(\mathcal{X}), \textit{G}).

For a divisor \textit{D} on a variety \mathcal{X} there is an associated \bar{k}\text{-vector space } \mathcal{L}(D) = \{ f \in \bar{k}(\mathcal{X})^{*}| \text{div}(f) \geq -D \} \cup \{0\}.

If \mathcal{X} \text{ and } \textit{D} \text{ are defined over } \mathbb{k} \text{ then a basis for } \mathcal{L}(D) \text{ can be found which is defined over } \mathbb{k}.

We will say two divisors \textit{D}_{1}, \textit{D}_{2} \text{ are linearly equivalent, and write } \textit{D}_{1} \sim \textit{D}_{2}, \text{ if } \textit{D}_{1} - \textit{D}_{2} = \text{div}(f) \text{ for some } f \text{ in } \bar{k}(\mathcal{X}). \text{ We will denote the dimension of the finite dimensional } \mathcal{L}(D) \text{ by } l(D) = \dim_{\bar{k}} \mathcal{L}(D).

For a more in-depth treatment of the above see [17] or [28].

For an irreducible non-singular curve \textit{C} there is a divisor \textit{\kappa} called the canonical divisor, which is well-defined up to linear equivalence, for details see [28]. If \textit{C} \text{ is defined over } \mathbb{k}, \text{ then so is } \kappa.

**Theorem 3.1.2.** (Riemann-Roch for Non-Singular Curves) Given a curve \textit{C} over \mathbb{k}, let \kappa be a canonical divisor of \textit{C}. Then there is a number \textit{g} called the genus of \textit{C} such that for all \textit{D} \in \text{Div}(\textit{C}),

\[ l(D) - l(\kappa - D) = \deg(D) - g + 1. \]

For details see [27] or [28]. Note that setting \textit{D} = 0 gives \textit{l}(\kappa) = g. Similarly, setting \textit{D} = \kappa gives that \deg \kappa = 2g - 2.
Let $\varphi : C_1 \to C_2$ be a surjective morphism of non-singular irreducible curves. Then we define a map $\varphi^* : \bar{k}(C_2) \to \bar{k}(C_1)$ by $\phi^*(f) = f \circ \varphi$ and we call $\varphi^*(f)$ the pullback of $f$.

We also define a map $\varphi^* : \text{Div}(C_2) \to \text{Div}(C_1)$ defined for $P$ on $C_2$ by $\varphi^*(P) = \sum_{\phi(Q) = P} Q$ and then extended by $\mathbb{Z}$-linearity to any $D \in \text{Div}(C_2)$. We call $\varphi^*(D)$ the pullback of $D$.

Lastly, we define a map $\varphi_* : \text{Div}(C_1) \to \text{Div}(C_2)$ defined by $\varphi_*(D) = \varphi_*(\sum n_P P) = \sum n_P \varphi(P)$ and we call $\varphi_*$ the pushforward of $D$.

### 3.2 Hilbert Polynomials

This section does not attempt to address most of the material known about Hilbert polynomials but merely gives the basics that we will use. Most of this material can be found in [9] and [10]. Throughout this section let $R = k[x_0, \ldots, x_m]$, which is a graded ring $\bigoplus_{i \geq 0} R_i$, where $R_i$ is the vector space spanned by the monomials in $x_0, \ldots, x_m$ of degree $i$.

**Definition 3.2.1.** Let $R$ be as above. Then a graded $R$-module $M$ is an $R$-module with a decomposition

$$M = \bigoplus_{i=-\infty}^{\infty} M_i$$

as abelian groups, such that $R_i M_j \subset M_{i+j}$ for all $i \geq 0, j \in \mathbb{Z}$, so each $M_i$ is a $k$-vector space. Furthermore, we define

$$h_M(n) = \dim_k M_n,$$

if defined, and call $h_M(n)$ the Hilbert function of $M$.

**Theorem 3.2.2.** (Theorem 1.11 of [9]) If $M$ is a finitely generated graded module over $R$, then $h_M(n)$ agrees, for large $n$, with a unique polynomial $p_M(n) \in \mathbb{Q}[n]$ of degree at most $m$. We call $p_M(n)$ the Hilbert polynomial of $M$.

Given a graded $R$-module $M$, we let $M(d)$ be the graded $R$-module such that $M(d)_n = M_{n+d}$. We will call $M(d)$ the module $M$ twisted by $d$. It follows that $p_{M(d)}(n) = p_M(n + d)$.

An exact sequence of graded $R$-modules is an exact sequence of $R$-modules with maps which take degree 0 elements to degree 0 elements.
Lemma 3.2.3. Given a short exact sequence of graded $R$-modules,

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0,$$

the Hilbert polynomial and function are additive, i.e.

$$h_B(n) = h_A(n) + h_C(n), \quad p_B(n) = p_A(n) + p_C(n).$$

The above lemma often gives a way to calculate Hilbert polynomials. If two of the modules have known Hilbert polynomials, then the third can be computed.

Suppose $k = \bar{k}$. For a homogeneous ideal $I \subset R$, various geometric aspects of the algebraic set $X = V(I)$ can be defined in terms of the Hilbert polynomial of $R/I$. The degree of $p_{R/I}(n)$ is the dimension $d$ of $X$, the degree of $X$ is $\frac{1}{d!}$ times the leading coefficient of $p_{R/I}(n)$, and the arithmetic genus of $X$, written $p_a(X)$, is $(-1)^d(p_{R/I}(0) - 1)$. For $X$ an algebraic set we also write $p_X(n)$ for $p_{R/I(X)}(n)$.

Example 3.2.4. The Hilbert polynomial for projective $m$-space is

$$p_{\mathbb{P}^m}(n) = \binom{m + n}{m}.$$  

For details see [16].

Now we specialize to $m = 3$.

Lemma 3.2.5. Let $C \subset \mathbb{P}^3$ be a curve inside of $\mathbb{P}^3$. Then its Hilbert polynomial is linear and of the form $p_C(n) = an + b$, where the degree of $C$ is $a$, and the arithmetic genus of $C$, denoted $p_a(C)$, is $1 - b$.

3.3 Quadric Surfaces

Much of this material can be found in [15] and [16].
Let \( q \in k[x, y, z, w] \) be a quadratic form, char \( k \neq 2 \). It is well known that \( q \) can be diagonalized over \( k \), i.e. there is a \( k \)-linear change of variables such that \( q = ax^2 + by^2 + cz^2 + dw^2 \). The number of non-zero coefficients in a diagonalized form is called the rank of \( q \) and is independent of the diagonalization chosen. We note that \( q \) is absolutely irreducible if rank \( q \) = 3 or 4 (as is the variety \( V(q) \)) and that by the Jacobian criterion, \( V(q) \) is non-singular if rank \( q \) = 4. In this case we also say that \( q \) is non-singular. If \( q \) is irreducible and singular, i.e. rank \( q \) = 3, then \( q \) is a cone and \( V(q) \) has a unique singular point. Throughout this section let \( Q \) be a non-singular quadric surfaces in \( \mathbb{P}^3(\bar{k}) \), by which we mean \( Q = V(q) \) for a quadratic form \( q \) with rank \( q \) = 4.

The Segre embedding

\[
\begin{align*}
s : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3
\end{align*}
\]

is given by \([x_0, x_1], [y_0, y_1] \mapsto ([x_0y_0, x_1y_0, x_0, y_1, x_1y_1]) \) and the image \( s(\mathbb{P}^1 \times \mathbb{P}^1) \) is the variety defined by the non-singular quadric surface \( V(z_0z_3 - z_1z_2) \) in \( \mathbb{P}^3 \).

The remarkable fact is that every non-singular quadric surface \( Q \subset \mathbb{P}^3 \) is isomorphic to \( V(z_0z_3 - z_1z_2) \) over \( \bar{k} \). So there is an isomorphism \( r : Q \to \mathbb{P}^1 \times \mathbb{P}^1 \). We say the morphism \( r \) is a ruling on \( Q \). Let \( \pi_i \) denote the projection from \( \mathbb{P}^1 \times \mathbb{P}^1 \) onto the first \((i = 1)\) or second \((i = 2)\) coordinate. From the ruling \( r \) and for every divisor \( D \) on \( Q \), \((r^{-1})^*(D)\) is a divisor on \( \mathbb{P}^1 \times \mathbb{P}^1 \) which via \( \pi_1 \) and \( \pi_2 \) gives divisors of degrees \( a \) and \( b \) on the copies of \( \mathbb{P}^1 \). We say that \((r^{-1})^*(D)\) has bidegree \((a, b)\) and we will say that \( D \) is of type \((a, b)\) on \( Q \). Note that up to switching the order of \( a \) and \( b \), the bidegree is well-defined regardless of the choice of ruling. A hyperplane section always has bidegree \((1, 1)\). For more details see [16].

Let (.) denote the intersection pairing of divisors on non-singular quadric surfaces. If \( D_1 \) and \( D_2 \) are two divisors on \( Q \) of type \((a_1, b_1)\) and \((a_2, b_2)\) respectively, then \((D_1.D_2) = a_1b_2 + a_2b_1\), for details see [16]. If \( D_1 \) and \( D_2 \) are effective divisors not sharing any components then \((D_1.D_2)\) is the number of points in the intersection of \( D_1 \) and \( D_2 \) counted with multiplicity.
For more details see Chapter V in [16].

**Lemma 3.3.1.** Let $C$ be a divisor of type $(a,b)$ on $Q$. Then $\deg C = a + b$ and $p_a(C) = (a - 1)(b - 1)$.

**Proof.** See [16].

Thus for a curve $C$ of type $(a,b)$ on a non-singular quadric, we see that $p_C(n) = (a+b)n - (ab - a - b)$.

We only need a specific adaptation of the Riemann-Roch Theorem for surfaces, which we give here, but a more general theorem can be found in [16].

**Theorem 3.3.2.** (Adapted Riemann-Roch Theorem for non-singular quadric surfaces) If $C$ is a divisor of type $(a,b)$ with $a, b \geq 0$ on $Q$ then

$$l(C) = ab + (a + b) + 1 = p_a(C) + 2 \deg C.$$ 

**Proof.** See [16].

**Lemma 3.3.3.** Let $C$ be an effective divisor of type $(1,0)$ on $Q$. Then $C$ is a line.

**Proof.** Let $P_1$ and $P_2$ be two distinct points on $C$ and $L$ be the unique line passing through $P_1$ and $P_2$. Let $H$ be any hyperplane containing $L$ (there is a $\mathbb{P}^1$ of hyperplanes containing $L$) and let $D_H$ be the divisor of $H \cap Q$, so $D_H$ is of type $(1,1)$. From the intersection pairing we see that $C.D_H = 1$. Since $C$ and $D_H$ are effective divisors on $Q$ and $P_1, P_2 \subset C \cap D_H$ it follows that $C \subset H$. Let $H_1, H_2$ be any two distinct hyperplanes containing $L$ (which exists since there is a $\mathbb{P}^1$ of hyperplanes containing $L$) then from construction $H_1 \cap H_2 = L$. But $C \subset H_1 \cap H_2$ which implies that $C \subset H_1 \cap H_2 = L$. From degree considerations it follows that $C = L$ and so $C$ is a line.

Note, if $C$ is not an effective divisor then the above Lemma can be generalized by saying there is a line in the linear system $|C|$.
The following is the key computation needed to derive some calculations that will follow. It is due to Hironaka, see [18].

**Lemma 3.3.4.** Let \( C \) be a possibly reducible curve contained in a smooth surface. Then

\[
p_a(C) = \pi(C) + \sum_{P \in C} \delta(P : C) - (r - 1),
\]

where \( r \) is the number of irreducible components of \( C \), \( \pi(C) \) is the sum of the geometric genera of the irreducible components of \( C \), and \( \delta(P : C) \) is the order of singularity at \( P \) on \( C \).

To explain the above notation further, if \( P \) is a non-singular point of \( C \) then \( \delta(P : C) = 0 \). If \( P \) is a double point then \( \delta(P : C) = 1 \). Moreover, if \( P \) is a singular point then \( \delta(P : C) \geq 1 \).

**Lemma 3.3.5.** Suppose that \( C \) is an effective divisor of type \((n, 0)\) for \( n \geq 2 \) on \( Q \) such that each component has multiplicity 1. Then \( C \) is the disjoint union of \( n \) lines.

*Proof.* From Lemma 3.3.1 it follows that \( p_a(C) < 0 \). But from Lemma 3.3.4 we see that irreducible curves have non-negative genus. Thus, \( C \) is not irreducible, so is the union of at least 2 components of the form \((a, 0)\) with \( 1 \leq a < n \). By induction on \( n \) it follows that an effective divisor \( C \) of type \((n, 0)\) is actually the union of \( n \) distinct effective divisors of type \((1, 0)\). By Lemma 3.3.1 any two distinct effective curves of type \((1, 0)\) are disjoint. So \( C \) is the union of \( n \) distinct disjoint divisors of type \((1, 0)\). By Lemma 3.3.3 curves of this type are lines. So an effective divisor of type \((n, 0)\) on \( Q \) such that each component has multiplicity 1 is a disjoint union of \( n \) lines. \(\square\)

**Lemma 3.3.6.** With notation as above, let \( Q_1 \) be a quadratic surface in \( \mathbb{P}^3 \). Then \( Q_1 \cap Q \) is a curve of type \((2, 2)\) on \( Q \). By Lemma 3.3.1 it follows that \( \mathcal{H} = Q_1 \cap Q \) is a curve with \( p_H(n) = 4n \), and so \( \deg \mathcal{H} = 4 \) and \( p_a(\mathcal{H}) = 1 \).

*Proof.* See [15], [16], or [27]. \(\square\)
Lemma 3.3.7. With notation as above, if a line $L$ intersects $Q$ in 3 or more points then $L \subset Q$.

Proof. Suppose that a line $L$ is not contained in $Q$. Since $\deg L = 1$, $\deg Q = 2$, and $\dim L = \text{codim} Q$, Bezout’s Theorem implies that $\#(L \cap Q) = 2$ when counting multiplicity correctly. The result follows.

Let $Q_1 = V(q_1)$ and $Q_2 = V(q_2)$ be two irreducible quadrics surfaces in $\mathbb{P}^3$ defined over $k$, and let $\mathcal{H} = V(q_1, q_2)$. So $q_1, q_2$ are quadratic forms in 4 variables of rank 3 or 4. Let $A, B \in \mathcal{M}_4(k)$ be symmetric matrices, $X = (x, y, z, w)$, such that $X^tAX = q_1$ and $X^tBX = q_2$. Let $P$ be a point on $\mathcal{H}$, i.e. $P^tAP = P^tBP = 0$, then we define the tangent line of $\mathcal{H}$ at $P$ to be the intersection of the two tangent planes $T_{A,P}, T_{B,P}$ defined by $T_{A,P} = V(P^tAX)$ and $T_{B,P} = V(P^tBX)$. By construction, the tangent line of $P$ is defined over the field $k(P)$.

Although the original statement of the following Lemma is more general, we adapt it to our needs.

Lemma 3.3.8. Let $Q_1$ be a non-singular quadric surface, $Q_2$ be another irreducible quadric surface in $\mathbb{P}^3$, and $\mathcal{H} = Q_1 \cap Q_2$. If $\mathcal{H}$ is irreducible then it is non-singular.

Proof. This follows from section 3 in [14].

3.4 Group Cohomology

This section will introduce the basic structures of group cohomology that we will need to use in our construction of non-associative division algebras. It is not intended as a comprehensive introduction to cohomology but merely covers the basics we will be using. Much of this section can be found in [4], [19], and [28].
Definition 3.4.1. Let $A$ be an abelian group and $G$ a group. $A$ is a $G$-module if $A$ is a $\mathbb{Z}[G]$-module. For ease of notation we shall write $a^g$ to mean the action of $g$ on $a$ for all $a \in A$, $g \in G$.

Let $A, B$ be two $G$-modules. A group homomorphism $\phi : A \to B$ is a $G$-homomorphism if the action of $G$ commutes with $\phi$, i.e. $\phi(a^g) = \phi(a)^g$.

We now introduce some definitions that can be found in [17].

Definition 3.4.2. Let $A^G = \{ a \in A | a^g = a \text{ for all } g \in G \}$. This group (it is easy to check that $A^G$ is a subgroup of $A$) is also written $H^0(G, A)$ and is called the 0th cohomology group of the $G$-module $A$.

Let $A = (A, +)$ be a $G$-module. Then a map $\phi : G \to A$ satisfying $\phi(gh) = \phi(g)^h\phi(h)$ for all $g, h \in G$ is called a 1-cocycle. We will let $Z(G, A)$ denote the group (under $+$) of all cocycles from $G$ to $A$. Two cocycles $\phi_1, \phi_2$ are called cohomologous if there exists an $a \in A$ such that $\phi_2(g) - \phi_1(g) = a^g - a$ for all $g \in G$, and being cohomologous is an equivalence relation $\sim$. We define the first cohomology group to be

$$H^1(G, A) = Z(G, A)/\sim.$$ 

An important corollary to the definition is that if $A$ is a trivial $G$-module then $H^1(G, A) = \text{Hom}(G, A)$. Now for the main theorem that shows up in cohomology.

Theorem 3.4.3. Let $A, B, C$ be $G$-modules and suppose there is a short exact sequence

$$0 \to A \to B \to C \to 0$$

of $G$-modules. Then there is an induced long exact sequence of cohomology groups

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to \ldots.$$ 

Proof. For a proof see [4].
3.5 Cyclic Quartic Extensions

A Galois field extension $K/k$ is a cyclic quartic extension if $\text{Gal}(K/k) = < \sigma >$ for some $\sigma$ and $[K : k] = 4$. Let $H$ be the subfield of $K$ fixed by $\sigma^2$. Since $\text{char } k \neq 2$ we have $H = k(\sqrt{d})$ for some $d \in k$. We call $H$ the (unique) quadratic subfield of $K$. Since $K/k(\sqrt{d})$ is a quadratic extension, there exist $a, b \in k$ such that $\tau = \sqrt{a + b\sqrt{d}}$ is a generator for $K$ over $k$. Note that $N_{K/k}(\tau) = a^2 - db^2$. In [26] it is shown that $a^2 - db^2 = dc^2$ for some $a, b, c \in k^*$. Let $\tau' = \sqrt{\frac{a}{c} + \frac{b}{c}\epsilon}$, then $k(\tau') = K = k(\tau)$ and $\tau'(\tau')^\sigma = \sqrt{d}$. So without loss of generality we can assume $K = k(\tau)$ with $\tau\tau^\sigma = \sqrt{d}$.

3.6 Determinantal Ideals

Most of this material comes from [9], [10] and [22]. Let $k$ be a perfect field, $R = k[x, y, z, w]$. For a matrix $M \in M_{r \times s}(R)$ we will denote the ideal generated by the $t \times t$ minors of $M$ by $I_t(M)$, for $t \leq \min(r, s)$. For a prime ideal $p$ in any commutative Noetherian ring $A$ we define the codimension of $p$, written $\text{codim } p$, to be the dimension of the local ring $A_p$. For any ideal $I \subset A$ we define the codimension of $I$, written $\text{codim } I$, to be the minimum of the codimensions of the primes containing $I$. For an ideal $J \in R \otimes \bar{k}$, this definition of codimension agrees with the geometric definition, i.e. $\text{codim } J = \text{codim } V(J)$.

There are a couple of theorem from [10] that we will use in this section so we restate them here. The first involves the notion of the depth of an ideal $I$ in a Noetherian ring, but we will only apply the theorem over Cohen-Macaulay rings, where the depth of an ideal coincides with its codimension (Theorem A2.38 in [10]).

Theorem 3.6.1. (Hilbert-Burch, Theorem 3.2 in [10])

Suppose that an ideal $I$ in a Noetherian ring $R$ admits a free resolution of length 1:

$$0 \to F^\beta \to G \to I \to 0.$$
(That is we have a short exact sequence of $R$-modules where $F$ and $G$ are free $R$-modules.) If the rank of $F$ is $t$, then the rank of $G$ is $t+1$, so given bases of $F$ and $G$, we can represent $\beta$ as a matrix multiplication by some $\tilde{M} \in \mathcal{M}_{t \times (t+1)}(R)$. Then there exists a non-zero divisor $a \in R$ such that $I = aI_t(\tilde{M})$, and the generator of $I$ that is the image of the $i$-th basis vector of $G$ is $\pm a$ times the determinant of the submatrix of $\tilde{M}$ formed from all except the $i$-th column. Moreover, the depth of $I_t(\tilde{M})$ is 2.

Conversely, given a non-zero divisor $a \in R$ and given a $t \times (t+1)$ matrix $\tilde{M}$ with entries in $R$ such that the depth of $I_t(\tilde{M}) \leq 2$, the ideal $I = aI_t(\tilde{M})$ admits a free resolution of length one as above. The ideal $I$ has depth 2 if and only if the element $a$ is a unit.

The other theorem we need is:

**Theorem 3.6.2.** (Theorem A2.54 in [10]) If $A$ is a $p \times q$ matrix with entries in a Noetherian ring $R$, $t \leq \min(p, q)$, and $I_t(A) \neq R$, then

$$\text{codim } I_t(A) \leq (p - t + 1)(q - t + 1).$$

Let $M$ be a $4 \times 4$ matrix of linear forms in $R$ such that $\det M = f$, $f$ is irreducible over $k$, and $f$ factors as $qq^\sigma$ over a quadratic extension $k(\sqrt{d})$ of $k$, with $\text{Gal}(k(\sqrt{d})/k) = \langle \sigma \rangle$. Let $\tilde{M}$ be the $3 \times 4$ matrix gotten by deleting the last row of $M$, and let $N = (n_{11}, ..., n_{14})$ be the row vector of maximal minors of $\tilde{M}$. So $N$ is a $1 \times 4$ vector of cubic forms in $R$ and is also a column of $\text{adj}(M)$. Let $I$ be the ideal in $R$ generated by $N$, $Y = V(I)$, so $Y \subset \mathbb{P}^3$. Our goal for the remainder of the section is to apply these theorems to study $Y$, and in particular to compute its Hilbert polynomial.

Being a field, $k$ is Cohen-Macaulay, so Theorem A2.33 in [10] implies that $R$ is Cohen-Macaulay. Hence for any ideal $J$ of $R$ the depth of $J$ is the same as codim $J$. We will apply this to $J = I$. 

From degree considerations $I \neq R$, so Theorem 3.6.2 says $\text{codim } I \leq 2$. Let $a = 1$, the converse direction of Theorem 3.6.1 says that

$$0 \rightarrow R^{3} \xrightarrow{\tilde{M}} R^{4} \xrightarrow{N} I \rightarrow 0.$$ 

is an exact sequence. Notice that the entries of $N$ are cubic forms and the entries of $\tilde{M}$ are linear forms. To calculate the Hilbert polynomial from an exact sequence, it must be an exact sequence of graded $R$-modules, so we consider the twist of the above sequence:

$$0 \rightarrow R^{3}(-4) \xrightarrow{\tilde{M}} R^{4}(-3) \xrightarrow{N} I \rightarrow 0,$$  \hspace{1cm} (3.1)

in which degree 0 elements are taken to degree 0 elements. From the free resolution in Equation 3.1 it follows that the

$$p_I(n) = 4p_R(n - 3) - 3p_R(n - 4) = 4 \binom{n}{3} - 3 \binom{n - 1}{3} = \frac{(n + 9)(n - 1)(n - 2)}{6}.$$ 

But we also have the sequence:

$$0 \rightarrow R/I \rightarrow R \rightarrow I \rightarrow 0.$$ 

So

$$p_Y(n) = p_{R/I}(n) = p_R(n) - p_I(n) = \binom{n + 3}{3} - \frac{(n + 9)(n - 1)(n - 2)}{6} = 6n - 2.$$ 

Thus the dimension 1 components of $Y$ form a degree 6 (possibly reducible) curve in $X = V(f)$.

We would like to consider the decomposition of $Y$ into irreducible components further. Recall that $I$ has a minimal primary decomposition

$$I = \bigcap_{j=1}^{n} q_j,$$
where each $q_j$ is a $p_j$-primary ideal of $R$ for some unique primes $p_j$ with $p_j = \sqrt{q_j}$, and $p_j \neq p_i$ for $i \neq j$. Renumbering the $q_i$ if necessary, let $Q^{reg} = \{q_m\}_{m=1}^{k}$ be the set of $p_m$ such that $p_m \not\subseteq p_i$ for any $p_i$, $1 \leq i \leq n$ and $i \neq m$, and

$$q^{\text{reg}} = \bigcap_{q \in Q^{\text{reg}}} q.$$ 

Let $Q^{\text{emb}} = \{q_i\}_{i=1}^{n} - Q^{\text{reg}}$ and

$$q^{\text{emb}} = \bigcap_{q \in Q^{\text{emb}}} q.$$ 

The superscripts are meant to be suggestive, for each $q \in Q^{\text{emb}}$, $V(q)$ is an embedded component of $Y$ whereas the components of $Y$ coming from $V(q^{\text{reg}})$ are not embedded components. From [3] the $q_i \in Q^{\text{reg}}$ are uniquely determined, i.e. independent of our choice of minimal primary decomposition of $I$.

Let $Y^{\text{reg}} = V(q^{\text{reg}})$. Then $Y^{\text{reg}}$ can further be stratified into two sets of components, depending on their dimension. From the Hilbert polynomial we saw that $\dim Y = 1$, and so each component of $Y$ will have dimension 0 or 1. Let $q^{\text{reg}}_1$ be the intersection of ideals of codimension 2 in $Q^{\text{reg}}$ and $q^{\text{reg}}_0$ be the intersection of ideals of codimension 3 in $Q^{\text{reg}}$. So $q^{\text{reg}} = q^{\text{reg}}_1 \cap q^{\text{reg}}_0$. On the geometric side, let $C = V(q^{\text{reg}}_1)$ and $P^{\text{iso}} = V(q^{\text{reg}}_0)$. We will think of the $C$ as the union of the components of $Y^{\text{reg}}$ of dimension 1 (curves) and $P^{\text{iso}}$ as the union of the dimension 0 components (points) of $Y^{\text{reg}}$. Furthermore, we will think of $P^{\text{iso}}$ as the set of isolated points of $Y$.

For any $s \in Q^{\text{emb}}$ let $S = V(s)$. Then there exists a $t \in Q^{\text{reg}}$ with $T = V(t)$ and $S \subset T$. So any component $S$ of $Y - Y^{\text{reg}}$ must have dimension 0 and be contained in a dimension 1 component $T$. We will let $P^{\text{emb}} = V(q^{\text{emb}})$, which we will think of as the set of embedded points of $Y$ (these are not uniquely determined from the choice of minimal primary decomposition of $I$).
Let $I_C = q_1^{reg}$, $I_P = (q_0^{reg} \cap q^{emb})$, and $P = V(I_P)$. So $P = P^{iso} \cup P^{emb}$. From construction

$$I = I_C \cap I_P.$$ 

Furthermore, this means that both of the hilbert polynomials $p_{I_C+I_P}(n), p_{I_P}(n)$ are constants since their zero sets are dimension 0, i.e. points.

We have the following exact sequences of graded $R$-modules

$$0 \rightarrow I \xrightarrow{\Delta} I_C \oplus I_P \xrightarrow{s} I_C + I_P \rightarrow 0,$$

where $\Delta$ is the diagonal map and $s(a, b) = a - b$, and hence the exact sequence of graded $R$-modules

$$0 \rightarrow R/I \rightarrow R/I_C \oplus R/I_P \rightarrow R/(I_C + I_P) \rightarrow 0.$$

Hilbert polynomials are additive along exact sequences of graded $R$-modules, which implies that

$$6n + m + h_{R/I_P}(n) = 6n - 2 + h_{R/(I_C+I_P)}(n),$$

for an appropriate $m$ depending on $C$. But from containment of ideals, $0 \leq h_{R/(I_C+I_P)}(n) \leq h_{R/I_P}(n) \leq \delta$ for some $\delta \in \mathbb{Z}_{\geq 0}$ and so

$$m + 2 = h_{R/(I_C+I_P)}(n) - h_{R/I_P}(n) \leq 0. \quad (3.2)$$

We will return to the equality in (3.2) in a proof in Chapter 6.

**Remark 3.6.3.** Let $G = \text{Gal}(\bar{k}/k)$. Then $G$ acts on the components of $Y$ (or equivalently the ideals $q$ in the minimal primary decomposition of $I$) and must send components of a given dimension to components of the same dimension. Thus the curve $C$, defined above, is actually defined over $k$. So the dimension 1 components of $Y$ not only form a degree 6 curve, they form a degree 6 curve defined over $k$. 
Chapter 4

Possible Factorizations of an Anisotropic Quartic Form

Let $K$ be a number field. Throughout this chapter let $f$ be a quaternary quartic form over $K$. In this chapter we consider two aspects of $f$, its arithmetic and geometry. What arithmetic conditions are needed such that $f$ is $K$-anisotropic? What geometric conditions are needed to guarantee that $f$ is determinantal? We first consider these two conditions separately and then put the results together.

In this section we will use lower case letters to denote homogeneous polynomials and the corresponding capital letter to denote the corresponding algebraic set. For instance, $V(q_1) = Q_1$ and $q_1 \in I(Q_1)$, the one exception being we write $X = V(f)$. A polynomial $g$ over $K$ is said to be absolutely irreducible if it is irreducible over every finite extension of $K$.

Let $f$ be a quaternary quartic form over $K$. Then over $\bar{K}$, $f$ must factor in one of the following ways:

1. $f$ doesn’t factor,
2. $f$ factors into two irreducible quadratics forms,
3. $f$ factors into an irreducible quadratic and two linear forms,
4. $f$ factors into an irreducible cubic and a linear form,
(5) $f$ factors into four linear forms.

Let $G = \text{Gal}(K/K)$. With notation as above, by applying Galois theory to the 5 possible factorizations of $f$ over $K$, $f$ must fall into one of the following 7 classes as a polynomial over $K$;

(1) $f$ can be absolutely irreducible,

(2) $f$ can factor into two absolutely irreducible quadratic forms $q_1, q_2$ over $K$,

(3) $f$ is irreducible over $K$ but can factor into two absolutely irreducible quadratic forms $q_1, q_2$ over a quadratic extension $K(\sqrt{d})$,

(4) $f$ can factor into 4 linear forms over a quartic extension $L$, $[L : K] = 4$,
   
   i) at least one of the linear factors can be defined over $K$
   
   ii) none of the linear factors can be defined over $K$

(5) $f$ can factor into an absolutely irreducible cubic form $c$ and a linear form $l_1$ over $K$,

(6) $f$ can factor into an absolutely irreducible quadratic form $q$ over $K$ and an irreducible quadratic form $q'$ over $K$ which factors into two linear forms $l_1, l_2$ over $K(\sqrt{d})$,

(7) $f$ can factor over $K$ into an absolutely irreducible quadratic form $q$ and two linear forms $l_1, l_2$.

Throughout this chapter we will refer to the above 7 classes of $f$ via their number, i.e. $f$ absolutely irreducible is class 1. Note in class 3, after multiplying $f$ by an element of $K^*$, we can assume $f = qq^\sigma$ where $<\sigma> = \text{Gal}(K(\sqrt{d})/K)$. Likewise, in class 6 we can assume $l_1$ and $l_2$ are conjugate linear forms over $K(\sqrt{d})$.

4.1 Arithmetic of $f$

The following describes in each class what arithmetic conditions are necessary to guarantee that $f$ is $K$-anisotropic.
Classes 4i, 5, 6, and 7

In classes 4i, 5 and 7 \( f \) is divisible by a \( K \)-rational linear form \( l_1 \). But any \( K \)-rational linear form has solutions over \( K \). Thus \( f \) is not \( K \)-anisotropic.

In class 6 \( f \) has two linear factors \( l_1, l_2 \) which after multiplying by a constant, we can assume are conjugate and not associates over a quadratic extension \( K(\sqrt{d}) \) of \( K \). Then \( V(l_1, l_2) = V(l_1 + l_2, \frac{l_1 - l_2}{\sqrt{d}}) \) is a line in \( \mathbb{P}^3 \) defined over \( K \). So \( l_1 \) and \( l_2 \) have a simultaneous solution which is a \( K \)-rational point, and \( f \) is not \( K \)-anisotropic. Thus for \( f \) to be \( K \)-anisotropic only classes 1, 2, 3, 4ii can occur.

Class 1

For \( f \) in class 1, if \( X \) is non-singular, then \( X \) is a \( K3 \) surface. Much is known about the arithmetic of \( X \) for specific cases, e.g. when \( f \) is a diagonal quartic form ([6]). But in general, understanding the arithmetic of \( K3 \) surfaces is quite hard. In particular we do not know much about anisotropic absolutely irreducible quaternary quartic forms. So we will not consider \( f \) of class 1 in this thesis.

Class 2

In class 2, \( f = q_1q_2 \) where each \( q_i \) is a quadratic form over \( K \). The Hasse-Minkowski Theorem says each \( q_i \) has a non-trivial solution over \( K \) if and only if it has a non-trivial solution over all completions of \( K \), which can be determined with a finite amount of computation. Furthermore each \( q_i \) must be a rank 3 or 4 quadratic form since it is irreducible. Let \( Q_i = V(q_i) \). If \( Q_i \) is singular it is a cone but this forces the vertex of the cone (the unique singular point) to be \( K \)-rational. So for \( f \) in class 2 each \( Q_i \) is non-singular, i.e. \( \text{rank } q_i = 4 \), and each \( q_i \) has no non-trivial solutions over some completion of \( K \).
Class 3

In class 3, \( f \) is an element of \( K^* \) times a product of conjugate quadratics \( q_1, q_2 \) over \( K(\sqrt{d}) \) with \( q_1 = r_1 + \sqrt{d}r_2, q_2 = r_1 - \sqrt{d}r_2 \), and \( r_1 \) is a quadratic over \( K \). Hence \( f \) will have a solution over \( K \) if and only if there is a simultaneous solution to \( r_1 \) and \( r_2 \) over \( K \). Letting \( \mathcal{H} = V(q_1, q_2) = V(r_1, r_2) \), then \( \mathcal{H} \) is an algebraic set defined over \( K \) and \( f \) is \( K \)-anisotropic if and only if \( \mathcal{H}(K) = \emptyset \). If \( \mathcal{H} \) is irreducible and non-singular, then \( \mathcal{H} \) is an elliptic curve over \( \bar{K} \) and as we will see in Chapter 5, \( \mathcal{H} \) is a non-trivial homogeneous space for an elliptic curve \( E \) over \( K \) precisely when \( f \) is \( K \)-anisotropic. This will be the case under study in this thesis and the topic of chapters 5, 6 and 7.

If \( \mathcal{H} \) is not irreducible, then the Galois action on the components of \( \mathcal{H} \) shows that \( \mathcal{H} \) is either a union of two degree 2 curves or is the union of four degree 1 curves.

Class 4ii

In class 4ii, \( f \) factors into 4 linear forms, none of which can be defined over \( K \). One possibility is that \( f \) is an element in \( K^* \) times four linear forms which are conjugate over a quartic extension \( L \) of \( K \). In this case, \( f = al_1l_2l_3l_4 \) for some \( a \in K \). There is a solution to \( f \) over \( K \) if and only if there is a solution of \( l_i \) over \( K \) for some \( i = 1, \ldots, 4 \). But then by Galois theory it is a solution to all \( l_i \), which implies that \( \bigcap V(l_i) \neq \emptyset \). But \( \bigcap V(l_i) \) is a linear variety over \( K \), so, if it is non-empty, it has a \( K \)-rational point. So \( f \) is \( K \)-anisotropic if and only if \( V(l_1, \ldots, l_4) = \emptyset \).

The only other possibility is that \( f \) factors into \( al_1l_2l_3l_4 \) over \( K(\sqrt{d}) \) for some quadratic extension of \( K \) where \( a \in K \) and the linear forms are conjugate in pairs. Let \( \sigma \) be the non-trivial element of \( \text{Gal}(K(\sqrt{d})/K) \). Then, without loss of generality, \( l_2 = l_1^\sigma \) and \( l_4 = l_3^\sigma \). From linear algebra, there is a simultaneous solution to \( l_1 = l_2 = 0 \) over \( K \) since \( \{ l_1 + l_2, \frac{d_1 - d_2}{\sqrt{d}} \} \) is a set of linear equations defined over \( K \).

Thus for \( f \) to factor into linear forms over \( \bar{K} \) and be \( K \)-anisotropic, \( f \) must factor as
an element of $K^*$ times a product of four conjugate linear forms over a quartic extension of $K$.

4.2 Geometry of $X$

We will say that $X$ is determinantal if and only if $f$ is. This section covers the necessary geometric constraints on $X$ to guarantee that $X$ is determinantal over $\bar{K}$. As will be seen below, for all classes of $f$, $X$ is determinantal over $\bar{K}$ except perhaps for $X$ in class 1. Keep in mind that this section only deals with the geometry of $X$, the following two sections deal with whether $f$ is determinantal over $K$. Having eliminated $f$ of classes 5, 6, 7 from being $K$-anisotropic, we only henceforth consider $f$ of classes 1, 2, 3, and 4.

Class 1

In class 1, $X$ is a (potentially singular) $K3$ surface. If $X$ is non-singular then [5] and [8] give the necessary conditions for $X$ to be determinantal. The classical results can be found in [24] which state that $X$ is determinantal if and only if $X$ contains a degree 6 genus 3 curve (under certain assumptions on $X$).

Classes 2 and 3

In class 2 the quartic surface $X$ is either a non-reduced surface (when $f = aq^2$ for some $a \in K$) or $X = Q_1 \cup Q_2$ the union of two irreducible quadric surfaces over $K$. From the arithmetic to force $f$ to be $K$-anisotropic, in class 2 both $Q_i$ are non-singular surfaces and $X = Q_1 \cup Q_2$ is always determinantal over $\bar{K}$. Indeed, there exists linear changes of variables over $\bar{K}$ such that $Q_1 = V(xz - yw)$ and $Q_2 = V(l_1l_2 - l_3l_4)$ for some linear forms
$l_i \in \bar{K}[x, y, z, w]$ and

$$V \left( \begin{vmatrix} x & y & 0 & 0 \\ w & z & 0 & 0 \\ 0 & 0 & l_1 & l_3 \\ 0 & 0 & l_4 & l_2 \end{vmatrix} \right) = X.$$ 

In the case when $X$ is not reduced we can take $l_1 = x$, $l_2 = y$, $l_3 = z$, $l_4 = w$.

In class 3, $X$ is a reducible surface with two conjugate irreducible quadric surfaces $Q_1$ and $Q_2$ as components over some $K(\sqrt{d})$. If $Q_1$ and $Q_2$ are non-singular then the above argument still holds to show that $X$ is determinantal. If $Q_1$ is a cone, then up to a linear change of variables over $K(\sqrt{d})$, $Q_1 = V(x^2 - yz)$. So,

$$X = V \left( \begin{vmatrix} x & y & 0 & 0 \\ z & x & 0 & 0 \\ 0 & 0 & x^\sigma & y^\sigma \\ 0 & 0 & z^\sigma & x^\sigma \end{vmatrix} \right)$$

where $<\sigma> = \text{Gal}(K(\sqrt{d})/K)$.

**Class 4**

In class 4, $X$ is a union of 4 hyperplanes and $X$ is always determinantal, potentially over a finite extension of $K$. Indeed if $f = l_1l_2l_3l_4$, a product of 4 linear forms, then

$$X = V \left( \begin{vmatrix} l_1 & 0 & 0 & 0 \\ 0 & l_2 & 0 & 0 \\ 0 & 0 & l_3 & 0 \\ 0 & 0 & 0 & l_4 \end{vmatrix} \right).$$

**4.3 Putting the Arithmetic and Geometry Together**

We’ve investigated the necessary arithmetic conditions to guarantee that $f$ is $K$-anisotropic and what geometric conditions are necessary to ensure that $f$ is determinantal
over $\bar{K}$. In this section we consider what conditions are necessary to make $X$ determinantal over $K$.

**Class 1**

We do not attempt to determine which conditions make $X$ determinantal over $K$. As in the last section, if $X$ is non-singular and contains an irreducible curve $C$ of degree 6 and genus 3 defined over $K$, then by [5] $X$ is determinantal over $K$.

**Class 2**

We do not attempt to determine which conditions ensure that $X$ is determinantal over $K$.

**Class 3**

Suppose we are in class 3 with $f$ factoring over some $K(\sqrt{d})$ as $qq^\sigma$ where $< \sigma > = \text{Gal}(K(\sqrt{d})/K)$. Then $Q = V(q) \subset \mathbb{P}^3$ can be a non-singular quadric surface or a cone. First we need a lemma.

**Lemma 4.3.1.** Let $q$ be a quadratic form in 4 variables of rank 4 defined over a field $k$ (char $k \neq 2$) and let $Q = V(q) \subset \mathbb{P}^3$. Then $Q$ contains a line defined over $k$ if and only if $Q$ is determinantal over $k$.

**Proof.** For the forward direction, suppose that $Q$ contains a line $L$ defined over $k$ so up to a $k$-linear change of variables $L = V(x, y)$. Then $q = xl_1 - yl_2$ for some linear forms $l_i \in k[x, y, z, w]$. Thus

$$q = \det \begin{pmatrix} x & l_2 \\ y & l_1 \end{pmatrix}.$$
For the reverse direction, suppose that $Q$ is determinantal over $k$. So $Q = V(q)$ where

$$q = \det \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix},$$

for some linear forms $l_i \in k[x, y, z, w]$. Then the line $L = V(l_1, l_2)$ is contained in $Q$ and defined over $k$. (Note that $V(l_1) \neq V(l_2)$ since $Q$ is irreducible, so $L$ is indeed a line.)

With notation as above let $f = qq^\sigma$, $Q = V(q)$, and suppose that $Q$ is non-singular. Then Lemma 4.3.1 says there is a line $L$ contained in $Q$ with $L$ defined over $K(\sqrt{d})$ if and only if $Q$ is determinantal over $K(\sqrt{d})$. If there is such a line, then from Lemma 4.3.1, it follows that $Q = V(\det M)$ for some $2 \times 2$ matrix $M$ of linear forms in $K(\sqrt{d})[x, y, z, w]$ and we can write $M = S + \sqrt{d}T$ for some $2 \times 2$ matrices $S, T$ of linear forms in $K[x, y, z, w]$. Now consider the $4 \times 4$ matrix

$$N = \begin{pmatrix} S & T \\ dT & S \end{pmatrix}$$

Then by direct computation we see that

$$\det N = \det (S^2 - dT^2) = \det ((S + \sqrt{d}T)(S - \sqrt{d}T)) = \det M \det M^\sigma = qq^\sigma = f. \quad (4.1)$$

So an irreducible quartic form $f$ defined over $K$ which factors into two absolutely irreducible quadrics of rank 4, $q, q^\sigma$, defined and conjugate over $K(\sqrt{d})$ is determinantal over $K$ if $Q = V(q)$ contains a line defined over $K(\sqrt{d})$. (When the converse of this holds is a main result of Chapter 6.)

If $f = qq^\sigma$ and rank $q = 3$, then we do not know what conditions are necessary and sufficient to guarantee that $f$ is determinantal over $K$. Ternary quadratic forms have a rich history and this problem might already be solved, but we will not consider this case further.

**Class 4**

We will only consider the case where $f$ is $K$-anisotropic. Suppose $f$ factors into four linear forms over $L$ where $[L : K] = 4$. Let $L_g$ be the Galois closure of $L/K$ and $G = \text{Gal}(L_g/K)$. 
Since the \( K \)-anisotropic quartic form \( f \) factors into 4 linear forms over an extension field \( L \), there are distinct \( \sigma, \tau, \gamma \in G \) such that \( l_2 = l_1^\sigma, \ l_3 = l_1^\tau, \ l_4 = l_1^\gamma \) and \( f = \alpha l_1^\sigma l_1^\tau l_1^\gamma \) with \( \alpha \in K \).

Let \( l_1 = ax + by + cz + dw \). Since, \( l_1 \) has no solutions over \( K \) it follows that \( \{a, b, c, d\} \) is a vector space basis for \( L \) over \( K \). Thus multiplication by \( a \) can be represented by a matrix \( M_a \) with respect to the above basis. Similarly let \( M_b, M_c, M_d \) represent multiplication by \( b, c, d \) with respect to this basis. By \( K \)-linearity we have \( \rho : L^* \to GL_4(K) \) a representation of a commutative group. All irreducible such representations are 1-dimensional, and standardly since \( \rho \) is 4-dimensional and defined over \( K \), \( \rho \) is the sum of \( \epsilon \in \{id, \sigma, \gamma, \tau\} \).

So if \( M = xM_a + yM_b + zM_c + wM_d \), then

\[
\det(M) = \prod_{\epsilon \in \{id, \sigma, \gamma, \tau\}} (\epsilon(x)M_a + \epsilon(y)M_b + \epsilon(z)M_c + \epsilon(w)M_d) = N_K^L(l_1) = f/\alpha.
\]

Thus in class 4 it follows that \( f \) is always determinantal over \( K \) if it is \( K \)-anisotropic.

### 4.4 Known Examples of 4-dimensional NADAs

In chapter 2 we gave a map \( \mu \circ \rho \) from 4-dimensional NADAs over \( K \) (up to isotopy) to \( K \)-anisotropic quaternary quartic forms (up to \( K \)-linear change of variables). The earlier sections of this chapter stratified such quartics into 7 classes: we extend this stratification to 4-dimensional NADAs \( A \) (up to isotopy) by saying that \( A \) is in a certain class if and only if \( \mu \circ \rho(A) \) is in that class. Now we recall all of the constructions of 4-dimensional NADAs that we know of, and give their class.

**Example 4.4.1.** Let \( a, b \in K^* \) and \( Q \) be the quaternion algebra over \( K \) with basis \( (1, i, j, ij) \) and relations \( i^2 = a, \ j^2 = b, \ ij = -ji \). We compute that the left-regular representation of
\( \mathcal{Q} \) (with all bases of \( \mathcal{Q} \) over \( K \) taken to be \((1, i, j, ij)\)) is:

\[
M_\mathcal{Q} = \begin{pmatrix}
x & ay & bz & -abw \\
y & x & bw & -bz \\
z & -aw & x & ay \\
w & -z & y & x
\end{pmatrix}.
\]

Then \( \det M_\mathcal{Q} = (x^2 - ay^2 - bz^2 + abw^2)^2 \). When \( a, b \) are chosen such that \( \mathcal{Q} \) is non-split, then \( \mathcal{Q} \) is a NADA of class 2.

**Example 4.4.2.** Consider a 4-dimensional non-associative algebra \( A \) with multiplication table given by

<table>
<thead>
<tr>
<th></th>
<th>x</th>
<th>y</th>
<th>z</th>
<th>w</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>x</td>
<td>y</td>
<td>z</td>
<td>w</td>
</tr>
<tr>
<td>y</td>
<td>y</td>
<td>-x</td>
<td>\gamma w</td>
<td>-\beta'z</td>
</tr>
<tr>
<td>z</td>
<td>z</td>
<td>-\gamma'w</td>
<td>-x</td>
<td>\alpha y</td>
</tr>
<tr>
<td>w</td>
<td>w</td>
<td>\beta z</td>
<td>-\alpha' y</td>
<td>-x</td>
</tr>
</tbody>
</table>

Let \( M \) be the left-regular representation of \( A \) with respect to the chosen basis. Then in [7] it is shown that the form \( f = \det M \) factors as

\[
f = (x^2 + y^2 + z^2 + w^2)(x^2 + \beta \gamma y^2 + \gamma \alpha z^2 + \alpha \beta w^2)
\]

if and only if \( \alpha, \beta, \gamma, \alpha', \beta', \gamma' \) satisfy either

\[
(\alpha - \beta')(\beta - \alpha') = (\beta - \gamma')(\gamma - \beta') = (\gamma - \alpha')(\alpha - \gamma') = 0
\]

or one of the three sets of equations coming from the permutations of \( \alpha, \beta, \gamma \) (which induce a similar permutation of \( \alpha', \beta', \gamma' \)) of

\[
(\alpha - \beta')(\beta - \alpha')(\beta \gamma - 1)(\beta' \gamma' - 1) = (\gamma \alpha - 1)(\gamma' \alpha' - 1) = 0.
\]

We will call quaternary quartic forms which factor into two quadrics over \( K \) as above \textit{Bruck quartics}, and if they are \( K \)-anisotropic then \( A \) is a NADA in class 2.
Example 4.4.3. (Example of a Bruck quartic which corresponds to a NADA in class 2) Let $A$ be a 4-dimensional NAA over $\mathbb{Q}$ with multiplication given by

$$
\begin{array}{cccc}
x & y & z & w \\
x & x & y & z & w \\
y & y & -x & 3w & 3z \\
z & z & -w & -x & y \\
w & w & 2z & -2y & -x \\
\end{array}
$$

Then

$$M = \begin{pmatrix}
x & y & z & w \\
y & -x & 3w & -3z \\
z & -w & -x & y \\
w & 2z & -2y & -x \\
\end{pmatrix}
$$

and $f = \det M = (x^2 + y^2 + z^2 + w^3)(x^2 + 6y^2 + 3z^2 + 2w^2)$. Since all of the coefficient are positive $f$ is a $\mathbb{Q}$-anisotropic Bruck quartic.

Example 4.4.4. This example introduces an important class of non-associative division algebras, known as *twisted fields*, first introduced by A.A. Albert in [2]. Suppose there are fields $k, F$ with $[F : k] = n < \infty$ and $F$ is a cyclic Galois extension of $k$ with $\text{Gal}(F/k) = \langle \alpha \rangle$. Fix a $\gamma \in F$ with $N_F^k(\gamma) \neq 1$. Let $A$ be the $k$-algebra whose underlying $k$-vector space is $F$ and whose multiplication is defined by

$$x * y - \frac{1}{1 - \gamma} (xy^\alpha - \gamma x^\alpha y).$$

Then $A$ is a division algebra, called a twisted field.

In 1996 Menichetti generalized the above construction in [20] as follows:

Definition 4.4.5. With notation as above, let $A(F, s, t, c)$, with $s, t \in \mathbb{Z}$, and $c \in F$ such that $N_F^k(c) \neq 1$, denote the $n$-dimensional $k$-algebra whose underlying $k$-vector space is $F$ and whose multiplication is defined by

$$x * y = xy - cx^\alpha y^\alpha$$

for all $x, y \in F$. 
An algebra constructed in this way is called a twisted field, and is a division algebra.

Following Menichetti’s notation, we define the following quantities. Let \( n = \dim_k(F) \), 
\( d = \gcd(n, s) \), 
\( d' = \gcd(n, t) \), 
\( n = ld \), 
\( n = l'd' \).

**Definition 4.4.6.** Let \( L, R \) be the left- (respectively right-)regular representations of a twisted field \( A(F, s, t, c) \). Let \( \Lambda, P \) be defined by 
\( \Lambda = V(\det L) \), 
\( P = V(\det R) \), which (following Menichetti) we will call the hypersurfaces of left (respectively right) zero-divisors of \( A(F, s, t, c) \).

Note when \( n = 4 \) both \( \Lambda \) and \( P \) are the algebraic sets of \( k \)-anisotropic quaternary quartic forms and \( \Lambda = V(\mu \circ \rho(A(F, s, t, c))) \). Hence the next theorem is an important tool for characterizing non-associative division algebras as twisted fields or not.

**Theorem 4.4.7.** (Prop. 28 in [20]) If \( d \nmid t \), then \( \Lambda \) is the union of \( d \) hypersurfaces of degree \( l \), absolutely irreducible and conjugate over \( F' \), where \( F \supseteq F' \supseteq k \) and \([F' : k] = d\). If \( d\mid t \) then \( \Lambda \) is the union of \( n \) hyperplanes conjugate over \( F \). By replacing \( d, t, l \) with \( d', s, l' \), the analogous result holds for \( P \).

**Proof.** For details see [20].

Let’s consider the theorem further when \( n = 4 \). Then there are several cases of what \((s, t) \in (\mathbb{Z}/4\mathbb{Z})^2\) can be. Note if \( s \) (respectively \( t \)) is relatively prime to 4, then the above theorem tells us that \( \Lambda \) (respectively \( P \)) is the union of 4 conjugate hyperplanes over \( F \). Suppose that \( s = 2 \) and \( t = 1 \) or 3, then \( d = 2, d' = 1 \), and thus \( \Lambda \) is the union of two conjugate quadric surfaces over \( F' \) with \([F' : k] = 2\). By reversing the roles of \( s, t \) the analogous result will hold for \( P \). The only other case to consider is when \( s = t = 2 \), in which case \( \Lambda, P \) will both be the union of 4 conjugate hyperplanes over \( F \).

In the case where \( \Lambda \) or \( P \) is the union of two absolutely irreducible conjugate quadric surfaces, we can analyze the intersection of these 2 quadrics.
**Lemma 4.4.8.** Let $F$ be a cyclic quartic extension of $k$ and $c \in F$ such that $N_k^F(c) \neq 1$. Let $\Lambda$, $P$ be the hypersurfaces of left and right zero divisors for $A(F, s, t, c)$, where $s = 2$, $t \in \{1, 3\}$. Then the curve $C$ which is the intersection of the two absolutely irreducible quadric surfaces whose union is $\Lambda$ is a reducible curve of degree 4 and arithmetic genus 1 in $\mathbb{P}^3$. Moreover, $C$ is the union of 4 lines. Reversing the roles of $s$ and $t$, we have the analogous result for $P$.

**Proof.** Lemma 20 in [20] shows that the defining equation for $\Lambda$ can be factored in $F[z_0, z_1, z_2, z_3]$ and in fact, $\Lambda = V((z_0z_2 - cc^α^2z_1z_3)(z_1z_3 - c^αc^α^3z_0z_2))$. Let $Q_1 = V(z_0z_2 - cc^α^2z_1z_3)$, $Q_2 = V(z_1z_3 - c^αc^α^3z_0z_2)$, and so $C = Q_1 \cap Q_2$. Note $C$ is only defined by the pencil generated by $Q_1, Q_2$. Consider the two quadric surfaces in the pencil: $c^αc^α^3Q_1 + Q_2 = (1 - N_k^F(c))z_1z_3$, and $Q_1 + cc^α^2Q_2 = (1 - N_k^F(c))z_0z_2$. Hence $C = V(z_0z_2, z_1z_3) = V(z_0, z_1) \cup V(z_0, z_3) \cup V(z_2, z_1) \cup V(z_2, z_3)$, so $C$ is reducible and the union of 4 lines. It follows that $\deg C = 4$ and Lemma 3.3.4 shows $p_a(C) = 1$. \qed

To summarize, among our 7 classes of quaternary quartics over $k$ the only classes which can be $k$-anisotropic are cases (1), (2), (3) and (4ii). Hence via $\mu \circ \rho$, these are the only 4 classes which potentially contain 4-dimensional NADAs over $k$.

The associative algebras are either fields which are in class 4ii, or non-split quaternion algebras, which are in class 2. The non-associative algebras we know of come from Bruck quartics, so are of class 2, or twisted fields, which are either of class 4ii (when $(s, t) \in \{1, 3\} \times \{1, 3\} \cup \{2, 2\}$) or class 3 (when $(s, t) \in \{(2, 1), (2, 3), (1, 2), (3, 2)\}$).

NADAs of class 1 are beyond the scope of this thesis but we will study class 3 NADAs, i.e. $A$ such that $\mu \circ \rho(A) = f$, where $f$ factors as $qq^σ$ over a quadratic extension $K(\sqrt{d})$ of $K$, where $\langle \sigma \rangle = \text{Gal}(K(\sqrt{d})/K)$. We let $\mathcal{H} = V(q, q^σ)$. Lemma 4.4.8 suggests our study of NADAs of class 3 should be more focused. There are 2 subcases of class 3:

- $(3)^{\text{red}}$— when $\mathcal{H}$ is reducible over $\bar{k}$,
• $\text{(3)}^{\text{irred}}$—when $\mathcal{H}$ is irreducible over $\bar{k}$,

and Lemma 4.4.8 says twisted fields of dimension 4 can be of class $\text{(3)}^{\text{red}}$ but never $\text{(3)}^{\text{irred}}$. We do not know any previously described examples in the class $\text{(3)}^{\text{irred}}$ and in the coming chapters we will study and construct new NADAs of class $\text{(3)}^{\text{irred}}$. 
Chapter 5

Elliptic Curves

5.1 Properties of Elliptic Curves

Definition 5.1.1. An elliptic curve $E$ over $k$ is an irreducible non-singular projective curve of genus 1 defined over $k$, with a specified basepoint $O \in E(k)$. We will call $O$ the origin of $E$.

Consider the $k$-vector spaces $\mathcal{L}(nO)$ for $n = 1, 2, \ldots, 6$. From Theorem 3.1.2 we see that $l(nO) = n$. Let $x$ be an element in $\mathcal{L}(2O) - \mathcal{L}(O)$ and $y$ be an element in $\mathcal{L}(3O) - \mathcal{L}(2O)$. These are functions on $E$ which have poles of order 2 and 3 at the origin of $E$. Furthermore, $y^2, x^3, xy, x^2, y, x, 1$ all lie in $\mathcal{L}(6O)$. But $l(6O) = 6$. Thus, there must be a $k$-linear relation amongst the 7 elements. It follows that any elliptic curve can be represented via a homogenized Weierstrass equation (See Proposition III.3.1 in [28])

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

for $a_i \in k$, where $O = [0 : 1 : 0]$ and the equation is non-singular.

Conversely, for a Weierstrass equation to define a curve of genus 1, we must have that the equation is non-singular. Let

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3).$$

Non-singularity means that $\partial F/\partial X, \partial F/\partial Y, \partial F/\partial Z$ do not simultaneously vanish. If all of the partials vanish at a point $P$, then $F(P) = 0$, since by Euler’s formula, $F = 1/3(X\partial F/\partial X + Y\partial F/\partial Y + Z\partial F/\partial Z)$. 
If all of the the \( a_i \) are in a field \( k \) then \( F \) defines an elliptic curve over \( k \) with \( \mathcal{O} = (0, 1, 0) \).

Let \( E \) be an elliptic curve over \( k \). We can then consider \( E(k) \), which are points of \( E \) defined over \( k \). Note that we always have \( \mathcal{O} \in E(k) \). Since \( E \subset \mathbb{P}^2 \), a point \( P \in E \) is defined over \( k \) if there exists a representation of \( P \) such that its coordinates are all in \( k \). We will most often be working in affine space with the affine slice defined by \( Z = 1 \), so we can dehomogenize and get the affine curve defined by

\[
E_{\text{aff}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,
\]

where \( y = Y/Z \) and \( x = X/Z \). Note that \( E(k) = E_{\text{aff}}(k) \cup \{0 : 1 : 0\} \).

We now restrict our attention to elliptic curves defined over a number field \( K \). Then up to a change of variables defined over \( K \), we can always put the defining equation for \( E_{\text{aff}} \) in the form \( E_{\text{aff}} : y^2 = x^3 + ax + b \), where \( a, b \in \mathcal{O}_K \), the ring of integers of \( K \). For a prime ideal \( p \subseteq \mathcal{O}_K \), \( p \neq 0 \), we will write \( K_p \) for the completion of \( K \) with respect to the non-archimedean place \( p \), and \( k_p \) for the residue field \( \mathcal{O}_K/p \). Furthermore, we will let \( M_K \) denote a complete set of places for \( K \) (including the archimedean places) and \( K_v \) will denote the completion of \( K \) with respect to \( v \in M_K \). Furthermore, we will let \( M_K^\infty \) denote the complete set of archimedean places. Note for each \( v \in M_K \) there is also an injection \( K \hookrightarrow K_v \). So if we can show an equation (or geometric object) does not have solutions in \( K_v \) (respectively points defined over \( K_v \)) then there are no solutions (respectively points) defined over \( K \).

**Definition 5.1.2.** Let \( E_{\text{aff}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \). The discriminant of \( E \), written \( \Delta(E) \), is a numerical value attached to the Weierstrass equation (for the formula \( f(a_1, a_2, a_3, a_4, a_6) = \Delta(E) \) see [28]). A model of \( E_{\text{aff}} \) is minimal at \( v \) (for all \( v \in M_K \)) if after all possible change of variables, \( y \mapsto y + \alpha x + \beta, \ x \mapsto x + \gamma \) with \( \alpha, \beta, \gamma \in \mathcal{O}_{K_v} \), it is chosen such that \( a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_{K_v} \) and \( v(\Delta(E)) \) is minimized. For a minimal model of \( E_{\text{aff}} \), if \( v(\Delta(E)) = 0 \) we say \( v \) is a prime of good reduction. If \( v(\Delta(E)) > 0 \) then we say \( v \) is
a prime of *bad reduction*.

**Lemma 5.1.3.** Let *E* be an elliptic curve over *K* and *v* be a prime of good reduction. Then *E*(*K*<sub>*v*<sub>) ≠ ∅.

**Proof.** The result follows from Hensel’s Lemma (recalled in Chapter 7). See [28] for details.

It is well known that there is an addition map (morphism), +<sub>*E* : *E* × *E* → *E* defined over *K*, that turns *E*(<overline>*K*) and *E*(*K*) into abelian groups.

**Lemma 5.1.4.** Let *D*<sub>1</sub> = ∑<sub>*P*</sub> (*n*<sub>*P*</sub> *P*) and *D*<sub>2</sub> = ∑<sub>*P*</sub> (*n*<sub>*P*</sub> *P*) be two divisors on an elliptic curve *E*. Then *D*<sub>1</sub> ∼ *D*<sub>2</sub> if and only if deg *D*<sub>1</sub> = deg *D*<sub>2</sub> and ∑<sub>*E*</sub> (*n*<sub>*E*</sub>*P*) = ∑<sub>*E*</sub> (*n*<sub>*E*</sub>*P*) as sums of points on *E*.

**Proof.** See [28].

The famous Mordell-Weil Theorem says that

\[ E(\mathbb{K}) = E(\mathbb{K})_{\text{tors}} \times \mathbb{Z}^r, \]

for some finite number *r* called the (Mordell-Weil) rank of *E/\mathbb{K}* and that *E*(\mathbb{K})<sub>\text{tors}</sub> is finite.

Let us consider *E*(\mathbb{K})<sub>\text{tors}</sub> further. Let *m* ∈ \mathbb{Z}_{>0} and let [\text{\textit{m}}] : *E* → *E* denote the multiplication map on *E*, i.e. [\text{\textit{m}}]*P* = P +<sub>*E*</sub> P +<sub>*E*</sub> P, *m* times, if *m* > 0. If *E* is defined over *K* then [\text{\textit{m}}] is defined over *K*. Thus,

\[ E(\mathbb{K})_{\text{tors}} = \bigcup_{m \in \mathbb{Z}_{\geq 1}} \ker[\text{\textit{m}}](\mathbb{K}). \]

**Definition 5.1.5.** Let (*E*<sub>1</sub>, *O*<sub>1</sub>), (*E*<sub>2</sub>, *O*<sub>2</sub>) be elliptic curves. An *isogeny* *φ* : *E*<sub>1</sub> → *E*<sub>2</sub> is a surjective morphism of curves such that \(\phi(O_1) = O_2\). An isogeny is necessarily a group homomorphism and we will denote \(\ker \phi\) by *E*[\text{\textit{φ}}] and *E*[\text{\textit{φ}}](\mathbb{K}) = *E*(\mathbb{K}) ∩ *E*[\text{\textit{φ}}].
Suppose that $\phi$ is an isogeny of elliptic curves and $\#(\ker \phi) = m$. Then we will say that $\phi$ is an $m$-isogeny.

**Lemma 5.1.6.** Let $\phi : E_1 \to E_2$ be an $m$-isogeny. Then there exists an isogeny $\hat{\phi} : E_2 \to E_1$ called the dual isogeny such that $\phi \circ \hat{\phi} = [m]$ on $E_2$ and $\hat{\phi} \circ \phi = [m]$ on $E_1$.

*Proof.* See [28].

A central result is,

**Lemma 5.1.7.** With notation as above, $\ker[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

The above lemma only holds when considering $\ker[m]$ as a subset of $E(\bar{K})$. We will specifically be interested in two subgroups of $E(K)_{\text{tors}}$, namely $E[2](K)$ and $E[4](K)$. Suppose $E[2](K)$ is nontrivial, i.e $E[2](K) \neq \mathcal{O}$. Then by a $K$-linear change of variables we can move the 2−torsion point to $(0, 0)$ and can represent $E$ by

$$E : y^2 = x^3 + ax^2 + bx,$$

where $\text{div}(x) = 2(0, 0) - 2\mathcal{O}$.

Let $t \in K$ and $E$ be an elliptic curve given by the equation

$$E : v^2 = u^3 + (t^2 + 2)u^2 + u,$$

then $(-1, t) \in E[4](K) - E[2](K)$. Since $(v-tu)(v+tu) = u(u+1)^2$ it follows that $\text{div}(v+tu) = 2(-1, t) + (0, 0) - 3\mathcal{O}$.

### 5.2 Homogeneous Spaces

Let $E/K$ be an elliptic curve defined over $K$. Much of the following can be found in [21] and [28].
**Definition 5.2.1.** We will say that a pair $(C, \mu)$ is a *principal homogeneous space* for $E$ if $C/K$ is a non-singular curve defined over $K$ and the following holds:

(i) $\mu : C \times E \to C$ is a morphism defined over $K$ such that,

(ii) $\mu(P, O) = P$.

(iii) $\mu(\mu(P, Q), R) = \mu(P, Q + E R)$.

(iv) For all $P, Q \in C$ there exists a unique $R \in E$ such that $\mu(P, R) = Q$.

**Remark 5.2.2.** There is also a “subtraction” map on $C$, namely a morphism $\nu : C \times C \to E$ given by $\nu(P, Q) = R$ where $R$ is the unique point from part (iv) above such that $\mu(P, R) = Q$.

**Definition 5.2.3.** A curve $C/K$ is a *twist* of $E/K$ if both curves are defined over $K$ and $C \cong E$ over $\bar{K}$.

The following lemma shows that principal homogeneous spaces of $E/K$ give rise to twists of $E/K$.

**Lemma 5.2.4.** Let $E/K$ be an elliptic curve. Let $C/K$ be a principal homogeneous space for $E/K$. Fix a point $P \in C(\bar{K})$. Define $\phi_P : E \to C$ by $\phi_P(Q) = \mu(P, Q)$. Then $\phi_P$ is an isomorphism of $E$ and $C$ defined over $K(P)$.

*Proof.* See [28] chapter X.

We will say that two homogeneous spaces, $(C, \mu) \sim (C', \mu')$ are $K$-equivalent if there exists an isomorphism $\phi : C \to C'$ defined over $K$ such that $\mu'(\phi(Q), P) = \phi(\mu(Q, P))$ for all $Q \in C, P \in E$.

**Definition 5.2.5.** We define the *Weil-Chatelet* group of $E/K$ to be

$$WC(E/K) = \{C | C \text{ is a principle homogenous space over } K \}/ \sim .$$

We will denote the equivalence class in $WC(E/K)$ of a curve $C$ by $\{C/K\}$. 
Theorem 5.2.6. Let $E/K$ be an elliptic curve. There is a bijection

$$
\beta : WC(E/K) \to H^1(\text{Gal}(\bar{K}/K), E), \quad \text{defined as follows.}
$$

Let $\{C/K\} \in WC(E/K)$ and fix a point $P \in C(\bar{K})$. Then $\beta(\{C/K\}) = \{\sigma \to \nu(P^\sigma, P)\}$

and the bijection is independent of the choice of $P$.

Proof. See [28] chapter X.

In Theorem 5.2.6, $\nu$ is the subtraction map from Remark 5.2.2. The bijection $\beta$ in
Theorem 5.2.6 induces a group structure on $WC(E/K)$. Furthermore, one can check that
$C(K) \neq \emptyset$ if and only if $\{C/K\}$ is trivial in $WC(E/K)$.

Definition 5.2.7. We define the period of $\{C/K\} \in WC(E/K)$ to be the order of $\{C/K\}$
in $WC(E/K)$. We define the index of $\{C/K\}$ to be the degree of the smallest field extension
$L$ of $K$ such that $\{C/L\}$ is trivial in $WC(E/L)$, i.e. $C(L) \neq \emptyset$.

It is well known that the period divides the index and that if $C \in \text{III}(E/K)$, then the
period equals the index ($\text{III}(E/K)$ will be defined in the next section).

Theorem 5.2.8. Given a non-singular projective curve $C/K$ of genus 1, there is an elliptic
curve $E/K$ such that $C \in WC(E/K)$. Furthermore, $E/K$ is unique up to $K$-isomorphism
and $E/K$ is called the Jacobian of $C/K$. We’ll write $E = \text{Jac}(C)$.


Let $E$ be an elliptic curve and $\text{Isom}(E)$ be the group of isomorphisms from $E$ to $E$.
Note that $\text{Isom}(E)$ has two important subgroups, namely $\text{Aut}(E)$, which is the set of all
isomorphisms which are isogenies from $E$ to $E$, and the translation subgroup $\{\tau_P : P \in E\}$,
where $\tau_P(Q) = Q +_E P$.

Remark 5.2.9. We now describe more fully how Theorem 5.2.6 builds a homogeneous space
$C/K$ from a cocycle $\xi : \text{Gal}(\bar{K}/K) \to E$. A more detailed discussion can be found in [28].
First we consider $E$ embedded into $Isom(E)$ by sending $P$ to the translation-by-$P$ map, $\tau_P$. Consider $\xi \in H^1(\Gal(\overline{K}/K), Isom(E))$. There is a curve $C/K$ and a $\overline{K}$-isomorphism $\theta : C \to E$ such that

$$\theta^\sigma \circ \theta^{-1} = \xi(\sigma)$$

for all $\sigma \in \Gal(\overline{K}/K)$. In [28] it is shown that $(C/K, \theta)$ is a homogeneous space for $E$ and from Theorem 5.2.6 it follows that $\xi$ corresponds to $\{C/K\}$.

**Remark 5.2.10.** Let $G = \Gal(\overline{K}/K)$. We would like to describe in more detail how $\xi \in H^1(G, E[\phi])$ can be used to build a homogeneous space when $\phi$ is an isogeny over $K$, and $E[\phi]$ is $G$-invariant. Namely, let $E_1 : y^2 = x^3 + ax + b$ be defined over $K$, $\phi : E_1 \to E_2$ be an isogeny over $K$ with $E[\phi] \subset E(K)$, and $\rho : G \to E[\phi]$ be a surjective group homomorphism. Here we are thinking of $E[\phi] \hookrightarrow Isom(E)$ via $P \in E[\phi] \mapsto \tau_P$, the translation-by-$P$ map on $E$. Since $E[\phi]$ is a trivial $G$-module it follows that $H^1(G, E[\phi]) = \Hom(G, E[\phi])$, and so $\rho \in H^1(G, E)$. There are two different actions of $G$ on $\overline{K}(E_1)$. Let $g \in G$ and $f \in \overline{K}(E_1)$. Then we can let $g$ act on the coefficients of $f$, and let $\rho(g)$ act on $f$ via $\tau_{\rho(g)}^*$. Specifically, let $\overline{K}(E_1) = \overline{K}(x, y)/(y^2 - x^3 - ax - b)$, and $H$ be the image of $G$ under the composite map $G \overset{\Delta}{\to} G \times G \overset{1 \times \rho}{\to} G \times \rho(G)$, where $\Delta$ is the diagonal map. We define the action of $G \times \rho(G)$ on $\overline{K}(E_1)$ by letting $(g, 0)$ act only on the coefficients of $f \in \overline{K}(E_1)$, and having $(0, \rho(g))$ leave the coefficients unchanged, but send $f$ to $\tau_{\rho(g)}^*f$ (i.e. sends a function $f(x, y)$, where $(x, y)$ is a generic point on $E$, to $f((x, y) + E \rho(g)))$. This induces an action of $H$ on $\overline{K}(E_1)$.

Let $F = \Fix(\overline{K}(E_1), H)$. In [28] it is shown that $F = K(C)$ for some curve $C/K$ which is a homogeneous space for $E/K$ corresponding to $\rho$ as in Theorem 5.2.6. The defining equations for $C$ can be found by finding all of the relations amongst the functions in $K(C)$ using the defining equation for $E$. Moreover, let $L = \Fix(\overline{K}, \ker \rho)$. Then $[L : K] = \deg \phi$, $\Gal(L/K) \cong E_1[\phi]$, and $C \cong E$ over $L$. We will say that the curve $C$ is a **twist by the isogeny $\phi$ over $L$**.
We can summarize Remark 5.2.10 by giving a lattice of subgroups of $G \times \rho(G)$ and the corresponding lattice of subfields of $\bar{K}(E_1)$ under the Galois correspondence:

5.3 The Selmer and Tate-Shafarevich Groups

Let $\phi : E \to E'$ be an isogeny, where both curves and $\phi$ are defined over $K$. Then there is an exact sequence

$$0 \to E[\phi] \to E(\bar{K}) \xrightarrow{\phi} E'(\bar{K}) \to 0.$$ 

Let $G = \text{Gal}(\bar{K}/K)$. All of the groups in the above exact sequence are $G$-modules, and from Definition 3.4.2 it follows that $H^0(G, E(\bar{K})) = E(\bar{K})^G = E(K)$ (and similarly for $E'$). Thus there is the long exact sequence of $G$-modules

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{} H^1(G, E[\phi]) \xrightarrow{} H^1(G, E(\bar{K})) \xrightarrow{} H^1(G, E'(\bar{K})) \to \ldots$$

By a standard abuse in notation, we call both labeled maps above $\phi$. This long exact sequence induces the short exact sequence

$$0 \to E'(K)/\phi(E(K)) \to H^1(G, E[\phi]) \to H^1(G, E(\bar{K}))[\phi] \to 0.$$ 

From Theorem 5.2.6 we see that $H^1(G, E(\bar{K}))$ is in bijection with the Weil–Chatelet group $WC(E_1/K)$. 
For a number field $K$, let $M_K$ be a complete set of places for $K$. Let $M'_K$ be the subset of $M_K$ consisting of the archimedean places of $K$. Let $K_v$ denote the completion of $K$ with respect to $v \in M_K$ along with an inclusion $K \hookrightarrow K_v$. Let $V$ be a variety over $K$ in $\mathbb{P}^n$. If $V$ has a point in $\mathbb{P}^n(K_v)$ for all $v \in M_K$, then we say that $V$ is locally soluble.

Let $G = \text{Gal}(\bar{K}/K)$ and $G_v = \text{Gal}(\bar{K}_v/K_v)$, along with an inclusion $G_v \hookrightarrow G$. Consider the following commutative diagram, where the downward arrows are restriction maps:

$$
\begin{array}{ccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \longrightarrow & H^1(G, E(\bar{K})[\phi]) & \longrightarrow & H^1(G, E(\bar{K}))[\phi] & \longrightarrow & 0 \\
0 & \longrightarrow & \prod_{v \in M_K} E'(K)/\phi E(K_v) & \longrightarrow & \prod_{v \in M_K} H^1(G_v, E(\bar{K}_v)[\phi]) & \longrightarrow & \prod_{v \in M_K} H^1(G_v, E(\bar{K}_v))[\phi] & \longrightarrow & 0
\end{array}
$$

(5.1)

**Definition 5.3.1.** For elliptic curves $E/K, E'/K$ and an isogeny $\phi$ defined over $K$, $\phi : E/K \rightarrow E'/K$, we define the $\phi$-Selmer group to be

$$
S^{(\phi)}(E/K) = \ker\{H^1(G, E[\phi]) \rightarrow \prod_{v \in M_K} H^1(G_v, E(\bar{K}_v))[\phi]\}.
$$

We define the Tate-Shafarevich group to be

$$
\Sha(E/K) = \ker\{H^1(G, E(\bar{K})) \rightarrow \prod_{v \in M_K} H^1(G_v, E(\bar{K}_v))\}.
$$

So from commutative diagram 5.1 it follows that $S^{(\phi)} = \ker f$ and $\Sha(E/K)[\phi] = \ker h$.

We should think of the non-trivial elements of $\Sha(E/K)$ as representatives of equivalence classes of homogeneous spaces which have points in $K_v$ for all $v \in M_K$ (so are locally soluble) but fail to have $K$-rational points. Thus $\Sha(E/K)$ measures the failure of the Hasse “local-global” principle for $E$.

Thus from commutative diagram 5.1, we see that an isogeny of curves defined over $K$, ...
\( \phi : E \to E' \), induces the short exact sequence

\[
0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to \III(E/K)[\phi] \to 0. \tag{5.2}
\]

Equation 5.2 shows that if the \( \phi \)-Selmer group can be computed, then the size of \( \III(E/K)[\phi] \) can be bounded. The problem with computing \( \III(E/K) \) directly is that for \( C \in S^{(\phi)} \) there is no "good" way to compute if \( C(K) = \emptyset \) or not.

**Remark 5.3.2.** In our discussion in Chapter 7 we will refer to the Birch and Swinnerton-Dyer Conjecture (BSD). Without going through all of the background, we would like to just mention its basic statement. There is an \( L \)-function attached to an elliptic curve \( E \) defined over \( K \), called \( L(E, s) \). The BSD conjecture states that the rank \( E \) (the number \( r \) from the Mordell-Weil Theorem) is the order of zero of \( L(E, s) \) at \( s = 1 \), and that the coefficient of \( (s - 1)^r \) in the taylor expansion of \( L(E, s) \) at \( s = 1 \) involves various computable constants attached to \( E \), and the potentially uncomputable constant \( |\III(E/K)| \). So assuming BSD, one can often numerically calculate \( |\III(E/K)| \). This conjecture has been proved in many special cases, and although widely believed to be true, it is unproved in general.

The following definition and lemma give a way to effectively compute \( S^{(\phi)} \).

**Definition 5.3.3.** Let \( G = \text{Gal}(\bar{K}/K) \), \( v \in M_K \), and \( I_v \subset G_v \subset G \) be the inertia group of \( v \). For \( A \) a \( G \)-module, we say that \( \xi \in H^1(G, A) \) is unramified at \( v \) if the restriction of \( \xi \) is trivial in \( H^1(I_v, A) \).

Let \( T \subset M_K \) and let \( \varpi_T = \{ \xi \in H^1(G, E(\bar{K})[\phi]) : \text{\( \xi \) is unramified outside \( T \)} \}. \)

**Lemma 5.3.4.** Let \( T \subset M_K \) be a finite set of places containing \( M^K \cup \{ \mathfrak{p} \text{ a prime of bad reduction of } E \text{ in } \mathcal{O}_K \} \cup \{ \mathfrak{p} : \text{char}(k_p) | \deg \phi \} \). Then \( S^{(\phi)} \subset \varpi_T \).

The above lemma allows one to effectively compute elements of \( S^{(\phi)} \). Take \( \xi \in \varpi_T \) and let \( \{ C/K \} \) be the corresponding element in \( WC(E/K) \) from Theorem 5.2.6 and the map
\(H^1(G, E[\phi]) \to H^1(G, E)\) induced by the inclusion \(E[\phi] \hookrightarrow E\). Then \(C \in S^{(\phi)}(E/K)\) if and only in \(C(K_v) \neq \emptyset\) for all \(v \in T\).

Since \(T\) is finite, and Hensel’s lemma (see Chapter 7) can be used to check whether \(C(K_v) \neq \emptyset\) at \(v\) a finite place, whether or not \(\xi \in S^{(\phi)}(E/K)\) reduces to a finite amount of computation.

If \(\xi \in S^{(\phi)}(E/K)\), then \(g(\xi) \in \text{III}(E/K)\), but as we said, there is no known effective way to determine whether \(g(\xi)\) is trivial in \(\text{III}(E/K)\) or not. (We will often automatically refer to an element of \(S^{(\phi)}(E/K)\) as being in \(\text{III}(E/K)\) without explicit reference to the map \(g\).)

Usually, the idea of a “\(\phi\)-descent” is to hope that \(\text{III}(E/K)[\phi] = 0\), and that every homogeneous space in \(S^{(\phi)}(E/K)\) has a \(K\)-rational point. (Ironically, in our case, we want to find non-trivial elements in \(\text{III}(E/K)[\phi]\).) If a \(\phi\)-descent doesn’t determine \(E'(K)/\phi(E(K))\), one resorts to “higher descents” (which we’ll write out when \(\phi\) is the multiplication-by-\(m\) map \([m]\)).

If one is lucky, higher descent theory can be used to compute the Mordell-Weil rank of \(E\), and hence that certain elements of \(\text{III}(E/K)[m]\) are non-trivial. The following commutative diagram is at the heart of understanding the “higher descents” that we will use to produce examples of non-trivial elements in \(\text{III}(E/K)[m]\). Let \(m, j \in \mathbb{Z}_{>1}\), then we have:

\[
\begin{array}{cccccc}
E(K) & \longrightarrow & S^{(m^j)}(E/K) & \longrightarrow & \text{III}(E/K)[m^j] & \longrightarrow & 0 \\
\downarrow \text{id} & & \downarrow & & \downarrow \text{mult. by } m^{j-1} & & \\
E(K) & \longrightarrow & S^{(m)} & \longrightarrow & \text{III}(E/K)[m] & \longrightarrow & 0 \\
\end{array}
\tag{5.3}
\]

If we are lucky enough that \([m^{j-1}]\text{III}(E/K)[m^j] = 0\), then it follows that the image of some \(D \in S^{(m^j)}(E/K)\) is some \(C \in S^{(m)}(E/K)\) which maps to 0 in \(\text{III}(E/K)\). If \(C\) is the image of some \(D\) then we say that \(D\) is an \(m^j\)-descendent of \(C\). So given a \(C\) in \(S^{(m)}(E/K)\) not in the image of \(S^{(m^j)}\), \(C\) maps to a non-trivial element of \(\text{III}(E/K)\), and we will say that
Remark 5.3.5. In other words, while it is always the case that if \( C \in S^{(m)}(E/K) \) has no \( m^j \)-descendents for any \( j \in \mathbb{Z}_{\geq 1} \), then it projects to a non-trivial element of \( \text{III}(E/K)[m] \), if we are so lucky that \( [m^{j-1}] \text{III}(E/K)[m^j] = 0 \), then \( C \) projects to a non-trivial element of \( \text{III}(E/K) \) if and only if \( C \) has no \( m^j \)-descendents (i.e. every element of \( H^1(G,E)[m^j] \) which maps to \( C \) is not everywhere locally soluble). Hence, if \( [m^{j-1}] \text{III}(E/K)[m^j] = 0 \), whether \( C(K) \neq 0 \) or not becomes effectively computable.

So if one were trying to find a \( C \) which projects onto non-trivial elements of \( \text{III}(E/K)[m] \), one would want to search for \( E/K \) using computational data assuming BSD to bound \( \text{III}(E/K)[m^\infty] \), and pick a \( j \) so that one would expect that \( [m^{j-1}] \text{III}(E/K)[m^j] = 0 \). This gives one the courage to try to show that \( C \) has no \( m^j \)-descendents. We will apply this in Chapter 7 in the case where \( m = 2 \) and \( j = 2 \) or 3.

We work out the requisite twists of \( E \) now.

Example 5.3.6. (Quadratic Twist of \( E \)) Suppose \( E : y^2 = x^3 + ax^2 + bx \) is an elliptic curve defined over \( K \), and let \( K(\sqrt{d}) \) be a quadratic extension. The point \( P = (0,0) \) is a point of order 2 on \( E \), so consider the isogeny \( E \xrightarrow{\phi} E'' = E/\langle P \rangle \), which is the natural projection.

Consider the homomorphism \( \rho : G \to E[\phi] \cong \mathbb{Z}/2\mathbb{Z} \). So \( \rho \in \text{Hom}(G,E[\phi]) = H^1(G,E[\phi]) \subset H^1(G,E) \) given by

\[
\sigma \mapsto \begin{cases} 
\mathcal{O}_E & \text{if } \sqrt{d'} = \sqrt{d}, \\
\mathcal{O}_E & \text{if } \sqrt{d'} = -\sqrt{d}.
\end{cases}
\]

With this definition of \( \phi \) and \( \rho \), \( \rho \) is a map of the type in Remark 5.2.10 and so builds a corresponding homogeneous space \( C_d \) that is a twist of \( E \) by \( \phi \) over \( K(\sqrt{d}) \). Indeed, the function field of \( C_d \) over \( K \) is the fixed field of the automorphism \( \delta \) of \( K(\sqrt{d})(E) \) that acts on the coefficients of a function in \( K(\sqrt{d})(E) \) by sending \( \sqrt{d} \mapsto -\sqrt{d} \) and acts on the argument of a function \( f(Q) \) (for a generic point \( Q \) on \( E \)) by sending \( Q \) to \( Q +_E P \). Since the fixed field
of $K(\sqrt{d})$ under $\delta$ is $K$, $C_d$ is defined over $K$ and $K(C_d)$ is a quadratic extension of $K(E'')$, and we get an induced morphism of degree 2

$$\gamma : C_d \rightarrow E''$$

over $K$.

In the literature, and below, these curves (one for each choice of quadratic extension of $K$) are called \textit{quadratic twists} of $E$. Moreover, there is an isomorphism $\theta : C_d \rightarrow E$ defined over $K(\sqrt{d})$ which gives us a commutative diagram of morphisms.

$$
\begin{array}{ccc}
C_d & \xrightarrow{\theta} & E \\
\downarrow{\gamma} & & \phi \\
E & \xrightarrow{\phi} & E''
\end{array}
$$

The defining equations for the above diagram are:

$$
\begin{align*}
E : y^2 &= x^3 + ax^2 + bx \\
E'' : y^2 &= q^3 - 2aq^2 + (a^2 - 4b)q \\
C_d : dw^2 &= d^2 - 2adz^2 + (a^2 - 4b)z^4, \\
\phi(x,y) &= \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right), \\
\gamma(z,w) &= \left( \frac{d}{z^2}, \frac{-dw}{z^3} \right), \\
\theta(z,w) &= \left( \frac{\sqrt{d}w - az^2 + d}{2z^2}, \frac{dw = \sqrt{d}az^2 + d\sqrt{d}}{2z^3} \right).
\end{align*}
$$

(5.4)

Since $C_d$ is a quadratic in $w$, it is a homogeneous space of index 1 or 2. Hence if it is everywhere locally soluble, it projects onto an element of order 1 or 2 in $\text{III}(E/K)$.

Now $C_d$ has two points $\infty_+, \infty_-$ at infinity, so by the Riemann-Roch theorem, the divisor $2(\infty_+ + \infty_-)$ is very ample and $l(2(\infty_+ + \infty_-)) = 4$. One can check that $\mathcal{L}(2(\infty_+ + \infty_-))$ is spanned by $z, w, 1, z^2$, so $C_d$ can be embedded into $\mathbb{P}^3$ via $\iota((z,w)) = (z, w, 1, z^2)$, and we will call $\iota(C_d) = \mathcal{C}$. So $\mathcal{C}$ is the intersection of two quadrics in $\mathbb{P}^3$. Indeed, the defining
equations for $C$ are:

$$C : z_0^2 - z_2 z_3 = -dz_1^2 + d^2 z_2^2 - 2adz_0^2 + (a^2 - 4b)z_3^2 = 0.$$  

**Remark 5.3.7.** We want $C_d$ to be $K$-anisotropic and locally soluble, so an element of order 2 in $\text{III}(E/K)$. We will try to show $C_d(K) = \emptyset$ by using a higher descent.

Suppose we find an $E/K$ such that BSD and analytic computations tell us that $[2] \text{III}(E/K)[2^\infty] = 0$. Then since $E[\phi] \subset E[2]$, we have $S(\phi)(E/K) \subset S^{(2)}(E/K)$, and $\text{III}(E/K)[\phi] \subset \text{III}(E/K)[2]$, so to show a space $C$ in $S(\phi)(E/K)$ is non-trivial in $\text{III}(E/K)[\phi]$, we can consider $C \in S^{(2)}(E/K)$ and show it is non-trivial in $\text{III}(E/K)[2]$. Presuming that $[2] \text{III}(E/K)[4] = 0$, we should have that $C$ is non-trivial in $\text{III}(E/K)[2]$ precisely when $C$ has no 4-descendents. So we will perform a 4-descent on $E$ and hope to show that $C$ has no 4-descendents.

In [28] it is shown that for $T$ as in Lemma 5.3.4 and $\phi$ the 2-isogeny as in Example 5.3.6, then $S(\phi)(E/K) \subset \{C_d | d \in K(T, 2)\}$, where

$$K(T, 2) = \{b \in K^*/(K^*)^2 | \text{ord}_v(b) = 0 \text{ for all } v \notin T\}.$$  

### 5.4 Rational 4-torsion and homogeneous spaces

While the theory of quadratic twists of elliptic curves with a rational 2-torsion point is well-known, in this section we will develop (perhaps for the first time) the corresponding theory for twists of elliptic curves with a rational 4-torsion point.

Let $E$ be an elliptic curve with a non-trivial $K$-rational 4-torsion point, i.e. there is a $P \in E[4](K) - E[2](K)$. As above, let $G = \text{Gal}(\bar{K}/K)$. Then $H^1(G, < P >) = H^1(G, \mathbb{Z}/4\mathbb{Z}) = \text{Hom}(G, \mathbb{Z}/4\mathbb{Z})$ and any surjective homomorphism from $G$ to $\mathbb{Z}/4\mathbb{Z}$ factors through the Galois group of a cyclic quartic extension of $K$. So let $K(\tau)$ be a cyclic quartic extension of $K$ with $\text{Gal}(K(\tau)/K) = < \sigma >$, and consider the homomorphism
ξ : Gal(\overline{K}/K) \to E defined by

\[ \alpha \mapsto \begin{cases} O_E & \text{if } \tau^\alpha = \tau, \\ P & \text{if } \tau^\alpha = \tau^\sigma, \\ 2P & \text{if } \tau^\alpha = \tau^{\sigma^2}, \\ 3P & \text{if } \tau^\alpha = \tau^{\sigma^3}. \end{cases} \] (5.5)

Since \( P \) is a \( K \)-rational 4-torsion point there are elliptic curves \( E'' \), \( E' \) and 2-isogenies \( \phi, \psi \) (natural projections) all defined over \( K \) such that

\[ E \xrightarrow{\phi} E'' = E/\langle 2P \rangle \xrightarrow{\psi} E' = E/\langle P \rangle. \]

Note that \( \psi \circ \phi \) is a 4-isogeny from \( E \) to \( E' \) whose kernel is \( \langle P \rangle \). From Remarks 5.2.9 and 5.2.10 we can use \( \xi \) to build a homogeneous space for \( E \). Let \( K(\sqrt{d}) \) denote the unique quadratic extension of \( K \) in \( K(\tau) \).

Consider the diagram

\[ E \xrightarrow{\phi} E'' \xrightarrow{\psi} E' \]

with \( E'', E' \) as above. We will now expand upon Remark 5.2.10 to explain how to build two elements of \( WC(E/K) \) (named \( C_d \) and \( H_\tau \) respectively), corresponding to twists by the 2-isogeny \( \phi \) over \( K(\sqrt{d}) \) and the 4-isogeny \( \psi \circ \phi \) over \( K(\tau) \) respectively. We will define both curves in terms of their function fields \( K(C_d), K(H_\tau) \), which are subfields of the function field \( L = K(\tau)(E) \).

Let \( G_\tau = \text{Gal}(K(\tau)/K) = \langle \sigma \rangle \) and \( H = \langle \nu \rangle \) where \( G_\tau \) acts on \( L \) by acting on the coefficient of function on \( E \), and \( \nu \) acts on \( L \) by leaving the coefficients alone but sending a function \( f \) to \( \tau^\sigma f \), i.e. if \( Q \) is a generic point on \( E \) then \( \nu \) takes \( f \) evaluated at \( Q \) to \( f \) evaluated at \( Q + E P \). Note that \( G_\tau \cong H \cong \mathbb{Z}/4\mathbb{Z} \) since \( P \in E[4](K) - E[2](K) \) and \( K(\tau) \) is a cyclic quartic extension. Consider the induced action of \( G_\tau \times H \) on \( L \). Then \( K(E) = \text{Fix}(L, \langle (1,0) \rangle) \). Note that \( E' \) is fixed under \( \nu \) by definition, so \( H \) fixes \( E' \). It follows that \( K(E') = \text{Fix}(L, \langle (1,0),(0,1) \rangle) \).
Let $C_d$ be the curve defined by the function field,

$$K(C_d) = \text{Fix}(L, < (1, 2 >)).$$

(Note that the field of constants in $\text{Fix}(L, < 1, 2 >)$ is $\text{Fix}(K(\tau), < \sigma >) = K$, so $C_d$ is
defined over $K$.)

The curve $C_d$ is a quadratic twist of $E$ which was discussed in Example 5.3.6. Indeed
$C_d$ is the twist of $E$ by $\phi$ over $K(\sqrt{d})$. As in the last section, we get a commutative diagram of morphisms:

$$\begin{array}{ccc}
C_d & \xrightarrow{\gamma} & C_d, \\
\downarrow{\theta} & & \downarrow{\gamma} \\
E & \xrightarrow{\phi} & E'',
\end{array} \hspace{1cm} (5.6)$$

where the vertical arrow $\theta$ is an isomorphism over $K(\sqrt{d})$, and $\gamma$ and $\phi$ are $K$-rational 2-
\textit{covers}, i.e. degree 2 surjective morphisms defined over $K$.

Now let $\mathcal{H}_\tau$ be the curve defined by the function field,

$$K(\mathcal{H}_\tau) = \text{Fix}(L, < (1, 1 >)).$$

(Note that $\mathcal{H}_\tau$ is defined over $K$ since $(1, 1)$ restricted to $K(\tau)$ is $\sigma$.) We also let $C_{d,\tau}$ be the
curve defined by the function field,

$$K(C_{d,\tau}) = \text{Fix}(L, < (1, 1), (0, 2) >).$$

(Note that $C_{d,\tau}$ is defined over $K$ since $\mathcal{H}_\tau$ is.)

So $\mathcal{H}_\tau$ is the twist of $E$ corresponding to $\xi \in H^1(\text{Gal}(\overline{K}/K), E)$, that is a twist of $E$
by $\psi \circ \phi$ over $K(\tau)$. We now have a commutative diagram of morphisms:

$$\begin{array}{ccc}
\mathcal{H}_\tau & \xrightarrow{\gamma} & C_{d,\tau} \\
\downarrow{\epsilon} & & \downarrow{\gamma} \\
E & \xrightarrow{\phi} & E'',
\end{array} \hspace{1cm} (5.7)$$

Again, the vertical arrows $\epsilon$ and $\theta$ are isomorphisms over $K(\tau)$ and $K(\sqrt{d})$ respectively, and
Γ, γ, φ, ψ are K-rational 2-covers. Note the triangle on the right side of the commutative diagram above is analogous to (5.6) except that \( C_{d,\tau} \in WC(E''/K) \) not \( WC(E/K) \). (Indeed, \( C_{d,\tau} \) is the quadratic twist of \( E'' \) by \( \psi \) over \( K(\sqrt{d}) \).)

The full lattice of subgroups of \( \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) and the corresponding fixed fields of \( K(\tau)(E) \) via Galois theory are

\[
\begin{array}{c}
\text{G} = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \\
< (1, 0), (0, 2) > \\
< (1, 0) > \\
< (1, 2) > \\
< (1, 1) > \\
< (2, 0), (0, 2) > \\
< (3, 1) > \\
< (2, 1) > \\
< (0, 1) > \\
< (2, 2) > \\
< (0, 2) > \\
< (0, 0) >
\end{array}
\]

It should be noted that the second diagram is upside down, i.e. the biggest field is on the bottom and the smallest function subfield is on the top. To determine explicit equations for \( C_d, C_{d,\tau}, \mathcal{H}_\tau \) one needs to find relations amongst the functions in \( K(C_d), K(C_{d,\tau}), K(\mathcal{H}_\tau) \) using the defining equation for \( E \) (and \( E'' \)). In the next section we give explicit equations for \( C_d, C_{d,\tau}, \mathcal{H}_\tau \) for a specific family of elliptic curves with a K-rational 4-torsion point.
Remark 5.4.1. Suppose that \( C_d \) represents a non-trivial element in \( \III(E/K) \), hence by Example 5.3.6, \( C_d \) has order 2. Then we will show that if \( \mathcal{H}_r \) is locally soluble then it is of order 4 in \( \III(E/K) \). Recall that \( \mathcal{H}_r \) is the homogeneous space corresponding to the surjective homomorphism \( \rho : G \rightarrow \langle P \rangle \). If \( \mathcal{H}_r \) is locally soluble, then \( \mathcal{H}_r \in \III(E/K) \). Using that \( \III(E/K) \) is a group, let \( C = [2] \mathcal{H}_r \). From Theorem 5.2.6 the cocycle corresponding to \( C \) is \([2] \rho = \rho + \rho \) defined pointwise. So \([2] \rho \) is a surjective homomorphism from \( G \) to \( < 2P > = \ker \phi \), and we see that \( C \) is the quadratic twist of \( E \) by \( \phi \) over \( K(\sqrt{d}) \), the unique quadratic subfield of \( K(\tau) \), and so \( C = C_d \). Therefore, since \( C_d \) is non-trivial in \( \III(E/K) \), \( \mathcal{H}_r \) is of order 4 in \( \III(E/K) \).

5.5 Explicit Equations for a Family of Elliptic Curves and Their Twists

Recall that our overarching goal is to build new 4-dimensional NADAs over \( K \), specifically those of class \((3)_{irred}\). For NADAs of class 3, we need to build \( K \)-anisotropic determinantal quaternary quartic forms \( f \) that factor as \( f = qq^\sigma \) over some \( K(\sqrt{d}) \). Recall that \( f \) being \( K \)-anisotropic means that if \( \mathcal{H} = V(q, q^\sigma) \) then \( \mathcal{H}(K) = \emptyset \), and \( f \) being of class \((3)_{irred}\) means that \( \mathcal{H} \) is irreducible. We have seen that this means that if \( V(q) \) is non-singular, then

1. \( \mathcal{H} \) is non-singular if \( \mathcal{H} \) is irreducible,

2. \( \mathcal{H} \) has genus 1,

3. So \( \mathcal{H} \) is a homogeneous space of its jacobian \( E \), of index 2 or 4 since it is the intersection of 2 quadrics in \( \mathbb{P}^3 \).

So we want to use what we have developed about the theory of elliptic curves to build such \( \mathcal{H} \). For \( \mathcal{H}(K) = \emptyset \), either \( \mathcal{H} \) does not have points over some completion \( K_v \) of \( K \), or \( \mathcal{H} \in \III(E/K) - \{0\} \). The case where \( \mathcal{H}(K_v) = \emptyset \) is properly a study of NADAs over local fields, so for us the most interesting case is when \( \mathcal{H} \in \III(E/K) - \{0\} \). Since \( \mathcal{H} \in \III(E/K) \) means its period is the same as its index, we concentrate on \( \mathcal{H} \in \III(E/K) \) of order 2 or 4.
If $E$ has a rational 4-torsion point $P$, we will use the isogenies $\phi$ and $\psi$ of the last section to build homogeneous spaces $\mathcal{C}_d \in \text{III}(E/K)[\phi] \subseteq \text{III}(E/K)[2]$ and $\mathcal{H}_\tau \in \text{III}(E/K)[\psi \circ \phi] \subseteq \text{III}(E/K)[4]$ which are twists of $E$ over $K(\sqrt{d})$ and $K(\tau)$ respectively, where $K(\sqrt{d})$ is the unique quadratic subfield of the cyclic quartic extension $K(\tau)$ of $K$. We explicitly want to write down $\mathcal{C}_d$ and $\mathcal{H}_\tau$ as the intersection of 2 quadrics in $\mathbb{P}^3$.

Let $\text{Gal}(K(\tau)/K) \cong \mathbb{Z}/4\mathbb{Z}$ be generated by $\sigma$, so $K(\sqrt{d}) = \text{Fix}(K(\tau), \langle \sigma^2 \rangle)$. We saw in Section 3.5 that without loss of generality we can assume $\tau \sigma = \sqrt{d}$.

Recall that for the family of elliptic curves

$$E : v^2 = u^3 + (t^2 + 2)u^2 + u, \quad \triangle(E) \neq 0,$$

for $t \in K$, the point $P = (-1, t)$ is of order 4, and,

$$<P > = \{(-1, t), (0, 0), (-1, -t), \mathcal{O}\}.$$

Thus with $\phi$ and $\psi$ as in the last section we have the following diagram of isogenies

$$E \xrightarrow{\phi} E'' \xrightarrow{\psi} E',$$

and Example 5.3.6 (and more specifically equation (5.4) when $a = t^2 + 2$ and $b = 1$) gives a defining equation for $E''$ and $\phi$:

$$E'' : y^2 = m^3 - 2(t^2 + 2)m^2 + t^2(t^2 + 4)m$$

$$(m, y) = \phi(u, v) = \left(\frac{v^2}{u^2}, \frac{v(1 - u^2)}{u^2}\right)$$

Under $\phi$ we have $\phi((-1, t)) = (t^2, 0)$ in $(m, y)$ coordinates, so we compose $\phi$ with the $K$-linear change of variables $m \mapsto m - t^2 = x$ and $y \mapsto y$. This composition then gives us the defining equations for $E''$ and $\phi$:

$$E'' : y^2 = x^3 + (t^2 - 4)x^2 - 4t^2x,$$

$$(x, y) = \phi(u, v) = \left(\frac{v^2}{u^2 - t^2}, \frac{v(1 - u^2)}{u^2}\right).$$
We do the above $K$-linear change of variables so we can directly apply equation (5.4) to $E''$ (now with $a = t^2 - 4$ and $b = -4t^2$), to get defining equations for $E'$ and $\psi$:

\[
E' : V^2 = U^3 - 2(t^2 - 4)U^2 + (t^2 + 4)^2U,
\]

\[
(U, V) = \psi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(-4t^2 - x^2)}{x^2}\right).
\]

By construction $\phi(-1, t^2) = (0, 0)$, and so $\ker(\psi \circ \phi) = \langle P \rangle$. Consider the following diagram giving $C_d$ as a 2-cover of $E''$.

\[
P^3 \supset C \xleftarrow{\phi} C_d \xrightarrow{\gamma} \xrightarrow{\theta} \xrightarrow{\gamma} E \xrightarrow{\phi} E'' \xrightarrow{\psi} E'.
\]

As in the last section, we can write $C_d$ as the intersection of two quadrics (which we call $C \subseteq P^3$) and it is visibly of index 2 if it has no $K$-rational points. Indeed,

\[
C_d : dw^2 = d^2 - 2(t^2 + 2)dz^2 + ((t^2 + 2)^2 - 4)z^4,
\]

\[
(x, y) = \gamma(z, w) = \left(\frac{d}{z^2} - t^2, \frac{-dw}{z^3}\right), \quad \text{and}
\]

\[
C : z_0^2 - z_2z_3 = -dz_1^2 + d^2z_2^2 - 2(t^2 + 2)dz_0^2 + ((t^2 + 2)^2 - 4)z_3^2 = 0.
\]

Similarly, as in the last section, consider the diagram giving $C_{d, \tau}$ as a 2-cover and $\mathcal{H}_\tau$ as a 4-cover of $E'$.

\[
\mathcal{H}_\tau \xrightarrow{\gamma} C_{d, \tau} \xrightarrow{\theta} \xrightarrow{\gamma} \xrightarrow{\gamma} E \xrightarrow{\phi} E'' \xrightarrow{\psi} E'.
\]

The equations for $C_{d, \tau}$ and $\gamma$ are given analogously to the construction of $C_d$. But writing
down $\mathcal{H}_\tau$, $\Gamma$, and $\epsilon$ requires more work. For aesthetic reasons we do the change of variables $z \mapsto 1/z$ and $w \mapsto -w/z^2$ on the model of $C_{d,\tau}$, and so now we have:

$$C_{d,\tau} : dw^2 = d^2 z^4 - 2d(t^2 - 4)z^2 + (t^2 + 4)^2,$$

$$\gamma(z, w) = (dz^2, dw).$$

The right hand side of the equation for $C_{d,\tau}$ factors as

$$d^2 z^4 - 2d(t^2 - 4)z^2 + (t^2 + 4)^2 = (dz^2 - 2\sqrt{dt}z + (t^2 + 4))(dz^2 + 2\sqrt{dt}z + (t^2 + 4)).$$

We set

$$\tau^2(\alpha_1 + \sqrt{d}\alpha_2)^2 = dz^2 + 2\sqrt{dt}z + (t^2 + 4)$$

$$(\tau^\sigma)^2(\alpha_1 - \sqrt{d}\alpha_2)^2 = dz^2 - 2\sqrt{dt}z + (t^2 + 4)$$

(5.8)

for variables $\alpha_1, \alpha_2$. These equations give an unramified double cover $\mathcal{H}_\tau$ of $C_{d,\tau}$ over $K$. Indeed, if $\infty_+, \infty_-$ are the two points at infinity of $C_{d,\tau}$, $z$ has a pole of order 1 at each and no other poles, so the divisor of poles of $g = dz^2 - 2\sqrt{dt}z + t^2 + 4$ is $2(\infty_+ + \infty_-)$. Since $g$ and its conjugate under $\sqrt{d} \mapsto -\sqrt{d}$ are relatively prime, the divisor of zeroes of $g$ is of the form $2S_1 + 2S_2$ for some $S_1, S_2 \in C_{d,\tau}(\bar{K})$. To get a corresponding morphism $\Gamma : \mathcal{H} \to C_{d,\tau}$, from this 2-cover, we set

$$w = \alpha_1^2 - d\alpha_2^2 \quad \text{so,}$$

$$dw^2 = (\tau)^2(\tau^\sigma)^2(\alpha_1^2 - d\alpha_2^2)^2.$$

By adding and subtracting (and then rescaling) the equations in (5.8), we get a pair of defining equations for $\mathcal{H}_\tau$:

$$2dz^2 + 2(t^2 + 4) = (\tau^2 + (\tau^\sigma)^2)(\alpha_1^2 + d\alpha_2^2) + \frac{(\tau^2 - (\tau^\sigma)^2)}{\sqrt{d}}(2d\alpha_1\alpha_2)$$

(5.9)

$$4tz = \frac{(\tau^2 - (\tau^\sigma)^2)}{\sqrt{d}}(\alpha_1^2 + d\alpha_2^2) + (\tau^2 + (\tau^\sigma)^2)(2\alpha_1\alpha_2).$$

And our morphism $\Gamma : \mathcal{H}_\tau \to C_{d,\tau}$ is given by

$$(z, w) = \Gamma(z, \alpha_1, \alpha_2) = (z, \alpha_1^2 - d\alpha_2^2).$$
Recall that $\text{Gal}(K(\tau)/K) = \langle \sigma \rangle$, and that $K(\sqrt{d})$ is the unique quadratic subfield of $K(\sqrt{d})$, and since $\sqrt{d} = \tau \tau^\sigma$, and $(\sqrt{d})^\sigma = -\sqrt{d}$, we have $\tau^\sigma \tau^{\sigma^2} = -\sqrt{d} = -\tau \tau^\sigma$ so $\tau^{\sigma^2} = -\tau$. Using this it can checked without too much difficulty that $\tau^2 + (\tau^\sigma)^2$ and $\tau^2 - (\tau^\sigma)^2$ are in $K$, and so the equations in (5.9) have coefficients in $K$, and $\mathcal{H}_\tau$ is defined over $K$.

Furthermore, the maps are given by

\[
\Gamma(z, \alpha_1, \alpha_2) = (z, \alpha_1^2 - d\alpha_2^2),
\]

\[
\epsilon(z, \alpha_1, \alpha_2) = \left( \frac{x_0 - 2\tau \tau^\sigma z}{x_0 + 2\tau \tau^\sigma z}, \frac{x_0 - 2\tau \tau^\sigma z}{2x_0 + 2\tau \tau^\sigma z} \right),
\]

\[
\epsilon^{-1}(u, v) = \left( \frac{-v(1-u)}{\sqrt{d}u(1+u)}, \frac{4t}{u(1+u)} \right).
\]

where $x_0 = (\tau - \tau^\sigma)\alpha_1 + \tau \tau^\sigma(\tau + \tau^\sigma)\alpha_2$. Since $\epsilon$ is an isomorphism, $\mathcal{H}_\tau$ is some twist of $E$ coming from the isogeny $\phi \circ \psi$. We also have that $\mathcal{H}_\tau$ is a 2-cover of $C_{d, \tau}$ over $K$.

So $\mathcal{H}_\tau$ is a twist of $E$ by $\psi \circ \phi$ over $F$, some cyclic quartic extension of $K$. To determine which quartic extension of $K$, $F$ is, we will compute the cocycle corresponding to $\mathcal{H}_\tau$ as in Theorem 5.2.6.

Let $P' = (0,0)_{E'}$. From the above it follows that

\[
(U, V) = \gamma \circ \Gamma(z, \alpha_1, \alpha_2)
\]

\[
= (dz^2, dz(\alpha_1^2 - d\alpha_2^2)).
\]

So when we pullback $P'$ to $\mathcal{H}_\tau$ we get the following points (call them $Q_1, Q_2, Q_3, Q_4$) in $(z, \alpha_1, \alpha_2)$ coordinates;

\[
(\gamma \circ \Gamma)^{-1}(P') = \{(0, \frac{\sqrt{t^2+4(\tau+\tau^\sigma)}}{2\tau \tau^\sigma}, \frac{-\sqrt{t^2+4(\tau-\tau^\sigma)}}{2(\tau \tau^\sigma)^2}), (0, -\frac{\sqrt{t^2+4(\tau-\tau^\sigma)}}{2\tau \tau^\sigma}, \frac{\sqrt{t^2+4(\tau+\tau^\sigma)}}{2(\tau \tau^\sigma)^2})\}
\]

\[
(0, \frac{\sqrt{t^2+4(\tau-\tau^\sigma)}}{2\tau \tau^\sigma}, \frac{-\sqrt{t^2+4(\tau+\tau^\sigma)}}{2(\tau \tau^\sigma)^2}), (0, -\frac{\sqrt{t^2+4(\tau+\tau^\sigma)}}{2\tau \tau^\sigma}, -\frac{\sqrt{t^2+4(\tau-\tau^\sigma)}}{2(\tau \tau^\sigma)^2})\}
\]

which are defined over $M = K(\tau, \sqrt{t^2+4})$ but not necessarily over $K(\tau)$. So before we compute the cocycle corresponding to $\mathcal{H}_\tau$ we need a short digression.
Let \( K(\tau) \) be as above, \( L = K(\sqrt{t^2 + 4}) \), so \( M \) is the compositum of \( K(\tau) \) and \( L \). If \( \sqrt{t^2 + 4} \in K(\tau) \) then \( M = K(\tau) \). If not, then we have the following diagram of lattices of subfields of \( M \) containing \( K \), and the corresponding subgroups of \( \text{Gal}(M/K) \) under the Galois correspondence:

\[
\begin{array}{ccc}
K(\tau, \sqrt{t^2 + 4}) & \xrightarrow{2} & L \\
F & \xleftarrow{2} & \{0\} \times \{0\}
\end{array}
\]

\[
\begin{array}{ccc}
K & \xleftarrow{4} & \{0\} \times \{0\}
\end{array}
\]

\[
\begin{array}{ccc}
Z/4Z \times \{0\} & \xleftarrow{Z/4Z \cong <1, 1>} & \{0\} \times Z/2Z
\end{array}
\]

\[
\begin{array}{ccc}
Z/4Z \times Z/2Z & \xleftarrow{Z/4Z \times Z/2Z}
\end{array}
\]

Let \( \nu \) be the non-trivial element of \( \text{Gal}(L/K) \). Hence \((1, 0)\) restricts to \( \sigma \) on \( K(\tau) \) and the identity on \( L \), and \((0, 1)\) restricts to the identity on \( K(\tau) \) and \( \nu \) on \( L \). So \( F \) is a cyclic quartic extension of \( K \) related to \( K(\tau) \), which is the fixed field of \((1, 1)\), that is, the element of \( \text{Gal}(M/K) \) which restricts to \( \sigma \) on \( K(\tau) \) and \( \nu \) on \( L \). We see now that each of the \( Q_i \) is fixed by \((1, 1)\), so are points in \( \mathcal{H}_\tau(F) \). Let \( \alpha \) be the generator of \( \text{Gal}(F/K) \) which is \((1, 0)\) \((\text{mod} \ <(1, 1)>\)\). Then since \((1, 0)\) acts as \( \sigma \) on \( \tau \) and \( \nu \) on \( \sqrt{t^2 + 4} \), we see that \( Q_1^\alpha = Q_3 \).

Following Theorem 5.2.6 we compute that:

\[
\nu(Q_1, Q_1^\alpha) = \epsilon(Q_1) - \epsilon(Q_1^\alpha) = \epsilon(Q_1) - \epsilon(Q_3) = \frac{t - \sqrt{t^2 + 4}}{t + \sqrt{t^2 + 4}}, 0 - \epsilon(1, -\sqrt{t^2 + 4}) = (-1, t) = P.
\]

It follows that \( \mathcal{H}_\tau \) corresponds to a \( \xi' \in H^1(\text{Gal}(\bar{K}/K), \langle P \rangle) = \text{Hom}(\text{Gal}(\bar{K}/K), \langle P \rangle) \) that factors through \( \text{Gal}(F/K) \), so is of the form given in (5.5), except that it is a quartic twist of \( E \) by \( \psi \circ \phi \) over \( F \) instead of over \( K(\tau) \). (If we took a quadratic twist of \( \mathcal{H}_\tau \) by replacing \( \alpha_1, \alpha_2 \) by \( \frac{\alpha_1}{\sqrt{t^2 + 4}}, \frac{\alpha_2}{\sqrt{t^2 + 4}} \), we would have the twist corresponding to the original \( \xi \) in...
equation (5.5).

Let’s recap what we have built. Starting with an elliptic curve with either a rational 2-torsion point or a rational 4-torsion point and a quadratic extension $K(\sqrt{d})$ of $K$ or a cyclic quartic extension $K(\tau)$ over $K$, we have constructed homogeneous spaces $C_d, \mathcal{H}_\tau$ which are intersections of quadrics in $\mathbb{P}^3$. These genus one curves will fall into one of three categories. They might have points over $K$, they might not have points over $K_v$ for some $v \in M_K$, or they might be non-trivial elements of $\III(E/K)$. But since we are interested in building NADAs, as opposed to NAAs, we are only interested in the latter two cases. Furthermore, we are most interested in the last case, so our goal is to find $E$ and $d$ or $\tau$ so we can build $C_d, \mathcal{H}_\tau \in \III(E/K)$ with $C_d$ of order 2 or $\mathcal{H}_\tau$ of order 4.
Chapter 6

f Factors into Two Quadrics over a Quadratic Extension

The goal of this chapter is to show that if $K$ is a number field, and if we have a $K$-anisotropic quaternary quartic form $f \in K[x, y, z, w]$ such that $f$ is irreducible over $K$, but factors as $qq^\sigma$ over some quadratic extension $K(\sqrt{d})$ of $K$, where $\text{Gal}(K(\sqrt{d})/K) = \langle \sigma \rangle$, $Q = V(q)$ is non-singular, and $H = V(q, q^\sigma)$ is irreducible, then $X = V(f)$ is determinantal over $K$ if and only if we have divisors satisfying certain arithmetic conditions. Thus, this chapter addresses $K$-anisotropic quaternary quartics of subclass (3)irred in Chapter 4. Recall from Chapter 4 that there are no previously known examples of NADAs that generate quaternary quartic forms of this type — using the results of this chapter we will build such example in Chapter 7.

6.1 Building a $4 \times 4$ Matrix

With notation as above, suppose that $Q = V(q)$ contains a line $L$ defined over $K(\sqrt{d})$ and let $C = H \cup L \cup L^\sigma$.

Then we can write $L = V(l, n)$ and $q = lp - nm$ for $l, n, p, m$ linear forms over $K(\sqrt{d})$. Consider the four cubic forms defined over $K(\sqrt{d})$

$$k_1 = l^\sigma q, \quad k_2 = lq^\sigma, \quad k_3 = n^\sigma q, \quad k_4 = nq^\sigma.$$

Then $k_i \in I(C)$ for all $i$. Now we show that $\{k_i\}_{i=1}^4$ is a linearly independent set over $\bar{K}$. 
Suppose that
\[ a_1k_1 + \ldots + a_4k_4 = 0 \]
for some \( a_i \in \bar{K}. \) Then
\[ (a_1l^\sigma + a_3n^\sigma)q = -(a_2l + a_4n)q^\sigma. \]

But from degree considerations and since \( q, q^\sigma \) are absolutely irreducible and not associates (since \( f \) is irreducible over \( K \)) it follows that
\[ (a_1l^\sigma + a_3n^\sigma) = (a_2l + a_4n) = 0. \]

But again, \( l, n \) define distinct hyperplanes and so it follows that \( a_i = 0 \) for all \( i. \) Therefore, \( \{k_i\}_{i=1}^4 \) is a linearly independent set over \( \bar{K}. \)

There are the following relations amongst the \( \{k_i\}: \)
\begin{align*}
n^\sigma k_1 &= l^\sigma k_3, \quad nk_2 = lk_4, \quad pk_2 - mk_4 = p^\sigma k_1 - m^\sigma k_3 = f; \\
and we can represent these equations via
\begin{pmatrix}
n^\sigma & 0 & -l^\sigma & 0 \\
0 & n & 0 & -l \\
-p^\sigma & p & m^\sigma & -m \\
\end{pmatrix}
\begin{pmatrix}
k_1 \\
k_2 \\
k_3 \\
k_4 \\
\end{pmatrix}
= 
\begin{pmatrix}
0 \\
0 \\
0 \\
\end{pmatrix}. \\
\text{(6.2)}
\end{align*}

Let \( r_i \) be the \( i^{th} \) row of the left most matrix. Clearly \( r_1 \) and \( r_2 \) are linearly independent since \( n \) and \( l \) are non-associate linear forms. So if the left most matrix is not full rank then there exists non-zero \( a, b \in K(\sqrt{d})(x, y, z, w) \) such that \( ar_1 + br_2 = r_3. \) But then, \( bn = p, \) and \( bl = m \) which implies \( pl - mn = 0, \) which is a contradiction since \( pl - mn = q \neq 0. \) So the three relations in equation (6.1) are linearly independent.

Since \( k_2 = k_1^\sigma, \ k_4 = k_3^\sigma, \) consider the change of basis
\[ c_1 = k_1 + k_2, \ c_2 = \frac{k_1 - k_2}{\sqrt{d}}, \ c_3 = k_3 + k_4, \ c_4 = \frac{k_3 - k_4}{\sqrt{d}}. \]
Then \( c_i \in I(C) \) and all \( c_i \) are defined over \( K \). Also since the \( \{k_i\} \) were linearly independent over \( \overline{K} \), the \( \{c_i\} \) will be linearly independent over \( K \). Since the \( \{c_i\} \) are a change of basis from \( \{k_i\} \), there must be 3 linearly independent relations with coefficients as linear forms in \( K[\sqrt{d}][x, y, z, w] \) amongst the \( \{c_i\} \), but since each \( c_i \) is defined over \( K \), we can take these relations to have coefficients which are linear forms in \( K[\sqrt{d}][x, y, z, w] \). For \( l, p, n, m \) as above, let

\[
l = l_1 + \sqrt{d}l_2, \quad p = p_1 + \sqrt{d}p_2, \quad n = n_1 + \sqrt{d}n_2, \quad m = m_1 + \sqrt{d}m_2,
\]

where each \( l_i, p_i, n_i, m_i \) is a linear form in \( K[x, y, z, w] \), for \( i = 1, 2 \).

From equation (6.2) and the change of basis we see that:

\[
\begin{pmatrix}
  n_1 & -dn_2 & -l_1 & dl_2 \\
  -n_2 & n_1 & l_2 & -l_1 \\
  -p_2 & p_1 & m_2 & -m_1 \\
  p_1 & -dp_2 & m_1 & -dm_2
\end{pmatrix}
\begin{pmatrix}
  c_1 \\
  c_2 \\
  c_3 \\
  c_4
\end{pmatrix}
= 
\begin{pmatrix}
  0 \\
  0 \\
  0 \\
  4f
\end{pmatrix}.
\]  

(6.3)

Now let

\[
M = 
\begin{pmatrix}
  n_1 & dn_2 & -l_1 & -dl_2 \\
  n_2 & n_1 & -l_2 & -l_1 \\
  -p_2 & -p_1 & m_2 & m_1 \\
  p_1 & dp_2 & -m_1 & -dm_2
\end{pmatrix}.
\]  

(6.4)

The matrix \( M \) comes from the left most matrix in 6.3 by changing the signs of \( p, m, \) and \( \sqrt{d} \), which just maps \( q \to -q^\sigma \) and \( q^\sigma \to -q \), so leaves \( f = qq^\sigma \) invariant. The matrix \( M \) is of tantamount importance to us because via \( M \) we show (by construction) that \( f = qq^\sigma \) is a determinantal form over \( K \), i.e.

\[
\det M = qq^\sigma = f.
\]
6.2 Main Theorem

Let $f, q,$ and $\mathcal{H}$ be as above. Recall that Lemma 4.3.1 says that if $Q = V(q)$ contains a line over $K(\sqrt{d})$ then $X$ is determinantal, and equation 6.4 gives another matrix $M$ such that $\det M = f = qq^\sigma$. We would first like to understand some of the arithmetic which follows from the geometric construction in equation 4.1 or equation 6.4.

Let $D \in \text{Div}^2(\mathcal{H})$, so $D = P_1 + P_2$, $P_i \in \mathcal{H}$. If $P_1 \neq P_2$ then we will say the line defined by $D$ is the unique line passing through the two distinct points $P_1$ and $P_2$. If $P_1 = P_2$ then we will say the line defined by $D$ is the unique line tangent to $\mathcal{H}$ through $P_1$.

We first need a lemma. Let $q_1, q_2 \in K[x, y, z, w]$ be two homogeneous irreducible quadratic forms.

**Lemma 6.2.1.** Let $\mathcal{H} = V(q_1, q_2)$, $Q_1 = V(q_1)$, and $Q_2 = V(q_1)$, with $Q_1$ or $Q_2$ non-singular. Furthermore, suppose that $\mathcal{H}$ is irreducible, hence non-singular of genus one. Given a divisor $D \in \text{Div}^2(\mathcal{H})$ there exists a unique point $[a : b] \in \mathbb{P}^1$ such that the line defined by $D$, call it $L_D$, satisfies $L_D \subset V(q_{ab})$ where $q_{ab} = aq_1 + bq_2$. Moreover, suppose we are given two divisors $D_1, D_2 \in \text{Div}^2(\mathcal{H})$ with corresponding points $[a_1 : b_1], [a_2 : b_2]$ in $\mathbb{P}^1$. Then $[a_1 : b_1] = [a_2 : b_2]$ if and only if $D_1 \sim D_2$ or $D_1 + D_2$ is a hyperplane section of $\mathcal{H}$.

*Proof.* See [31].

**Theorem 6.2.2.** Let $f \in K[x, y, z, w]$ be a $K$-irreducible $K$-anisotropic quartic form and suppose that $f$ factors as $qq^\sigma$ over $K(\sqrt{d})$ for some $d \in K^* - (K^*)^2$, $\text{Gal}(K(\sqrt{d})/K) = \langle \sigma \rangle$ and that $q, q^\sigma$ are absolutely irreducible and non-singular. Furthermore let $X = V(f)$, and $\mathcal{H} = V(q, q^\sigma)$ be such that $\mathcal{H}$ is irreducible.

If the surface $X$ is determinantal then,
(1) there is a divisor $D_1 \in \text{Div}_{K(\sqrt{d})}^1(\mathcal{H})$, $D_1 = P$, with $2P \not\sim 2P_\sigma$ and $2P + 2P_\sigma$ is not a hyperplane section of $\mathcal{H}$,

(2) or more generally, there is a divisor $D_1 \in \text{Div}_{K(\sqrt{d})}^2(\mathcal{H})$ with $D_1 \not\sim D_1^\sigma$ and $D_1 + D_1^\sigma$ is not a hyperplane section of $\mathcal{H}$.

Conversely, if $\mathcal{H} = V(q_1, q_2)$ is irreducible, $Q_1 = V(q_1)$, $Q_2 = V(q_2)$ non-singular, and there exists a $K(\sqrt{d})$ with $D_1$ as in (1) or (2), then there is a quadric $q$ in the pencil generated by $q_1$ and $q_2$ such that $\mathcal{H} = V(q, q^\sigma)$ and $f = qq^\sigma$ is determinantal.

Proof. First we'll prove the forward direction of 6.2.2. With notation as above, suppose that $X$ is determinantal. Then $f = \det M$ for some matrix $M$ of $K$-rational linear forms, $f$ factors as $qq^\sigma$ over $K(\sqrt{d})$, and we set $N = \text{adj } M$. Let $\mathcal{H} = V(q, q^\sigma)$ and $Q = V(q)$. From Lemma 3.3.6 we see that $\deg \mathcal{H} = 4$, $\mathcal{H}$ is non-singular, and the genus of $\mathcal{H} = 1$. Section 3.6, and more specifically Remark 3.6.3, shows that the first row of $N$, call it $(c_{11}, c_{12}, c_{13}, c_{14})$, is an ideal in $K[x, y, z, w]$ which cuts out a degree 6 curve $C$ defined over $K$ on $X$. But since $f$ factors as $qq^\sigma$ over $K(\sqrt{d})$, the degrees of $C \cap Q$ and $C \cap Q^\sigma$ are the same, so $C$ must be as in one of two cases. Either:

(1) $C = C^3 \cup (C^3)^\sigma$ for some degree 3 curve $C^3 \subset Q$, defined over $K(\sqrt{d})$, where $< \sigma >= \text{Gal}(K(\sqrt{d})/K)$, so for some ruling on $Q$ over $\bar{K}$,

(a) $C^3$ is of type $(2, 1)$ on $Q$, or

(b) $C^3$ is of type $(3, 0)$ on $Q$,

(2) or $C = \mathcal{H} \cup L \cup L^\sigma$, where $\mathcal{H}$ is the degree 4 curve $V(q, q^\sigma)$ and $L$ is a degree 1 curve on $Q$ defined over $K(\sqrt{d})$.

Suppose we are in case 1a so $C^3$ is of type $(2, 1)$. The intersection of $Q$ with a hyperplane defined over $K$ (which cannot contain $Q$ since $Q$ is a non-singular quadric) is a curve of type $(1, 1)$ on $Q$ defined over $K(\sqrt{d})$. So there is a divisor $D$ of type $(2, 1) - (1, 1) = (1, 0)$ on $Q$
defined over $K(\sqrt{d})$. As in the proof of Lemma 3.3.3 there is a line $L$ in the linear system $|D|$ on $Q$ defined over $K(\sqrt{d})$.

Now consider case 1b so $C^3$ is of type $(3,0)$ on $Q$. From Section 3.3 we saw that divisors of this type on $Q$ either have components with multiplicity greater than 1 (i.e. $C^3$ is non-reduced) or are unions of disjoint lines, so $C^3$ is either

i ) a union of 3 disjoint lines,

ii ) the union of a double line and a disjoint line,

iii ) or a triple line.

In both cases 1bii and 1biii, the Galois action on $C^3$ shows there is a line on $Q$ defined over $K(\sqrt{d})$.

Let $S = \bar{K}[x,y,z,w]$. Consider $C^3$ as in case 1bi so $C^3 = L_1 \cup L_2 \cup L_3$ and $(C^3)^\sigma = L_4 \cup L_5 \cup L_6$, where the $L_i$ are lines over $\bar{K}$, and $L_4, L_5, L_6 \subset Q^\sigma$. Now we consider the possible arithmetic genus of $C$. Note that there cannot be singularities on $C^3$ as it is a union of disjoint lines and lines cannot have singular points. If, without loss of generality, $L_1 \cap (C^3)^\sigma \geq 3$, then $L_1 \subset Q^\sigma$ from Lemma 3.3.7. But this is a contradiction since $L_1 \subset Q$ and $L_1 \not\subset H$ as $H$ is irreducible. So there can be at most 6 points of intersection amongst the $\{L_i\}_{i=1}^6$. Hence Lemma 3.3.4 implies that $p_a(C) \leq 1$ and Lemma 3.2.5 then implies that the Hilbert polynomial of $C$ is $p_C(n) = 6n + m$ with some $m \geq 0$. This contradicts equation (3.2) so $C$ cannot be as in case 1bi.

In case 2, the curve $L \subset Q \subset \mathbb{P}^3$ has degree 1 so by Lemma 3.3.3 it is a line on $Q$ defined over $K(\sqrt{d})$. Thus in the forward direction, there is always a line $L$ on $Q$ defined over $K(\sqrt{d})$. From the intersection pairing on non-singular quadratic surfaces, and since $H$ is curve of type $(2,2)$ of $Q$, we see that $L.H = 2$. Since $L$ and $H$ have no components in common ($L \not\subset H$) the intersection pairing gives that $\#L \cap H$ consists of 2 points, counted with multiplicity. Let these two points of intersection be called $P_1$ and $P_2$. If $L$ is a tangent
line to $\mathcal{H}$, then $P_1 = P_2$ and $P_1 \in \text{Div}^1_{K(\sqrt{d})}(\mathcal{H})$, and so $P_1 + P_1^* \in \text{Div}^2_K(\mathcal{H})$. If $L$ is a secant line, then $P_1 \neq P_2$ and $D_1 = P_1 + P_2 \in \text{Div}^2_{K(\sqrt{d})}(\mathcal{H})$. Recall, $L \subset Q \neq Q^\sigma \supset L^\sigma$ and so by Lemma 6.2.1 $P_1 + P_2 \not\sim (P_1 + P_2)^\sigma$ and $(P_1 + P_2) + (P_1 + P_2)^\sigma$ is not a hyperplane section of $\mathcal{H}$. So the forward direction of the theorem is proved.

Now we will show the reverse direction. Suppose we have a genus one degree 4 irreducible curve $\mathcal{H} = V(q_1, q_2)$ where $Q_1 = V(q_1)$, $Q_2 = V(q_2)$ are non-singular quadric surfaces defined over $K$ in $\mathbb{P}^3$. Note that $\mathcal{H}$ is only defined by the pencil of quadratics generated by $q_1$ and $q_2$ not by the choice of $q_1$ and $q_2$. We need to consider two cases. Either;

1. there is a divisor $D_1 \in \text{Div}^1_{K(\sqrt{d})}(\mathcal{H})$, $D = P$, with $2P \not\sim 2P^\sigma$ and $2P + 2P^\sigma$ is not a hyperplane section of $\mathcal{H}$, for some $d \in K^* - (K^*)^2$, where $\text{Gal}(K(\sqrt{d})/K) =< \sigma >$,

2. or there is a divisor $D_1 \in \text{Div}^2_{K(\sqrt{d})}(\mathcal{H})$ with $D_1 \not\sim D_1^\sigma$ and $D_1 + D_1^\sigma$ is not a hyperplane section of $\mathcal{H}$, for some $d \in K^* - (K^*)^2$, where $\text{Gal}(K(\sqrt{d})/K) =< \sigma >$.

First, suppose there is a divisor $D \in \text{Div}^1_{K(\sqrt{d})}(\mathcal{H})$, $D = P$, with $2P \not\sim 2P^\sigma$ and $2P + 2P^\sigma$ is not a hyperplane section of $\mathcal{H}$, for some $d \in K^* - (K^*)^2$, where $\text{Gal}(K(\sqrt{d})/K) =< \sigma >$. Let $L$ be the tangent line to $\mathcal{H}$ through $P$. So $L$ is defined over $K(\sqrt{d})$. By Lemma 6.2.1 there is a unique quadric $q_{ab} = aq_1 + bq_2$ with $[a, b] \in \mathbb{P}^1$, in the pencil generated by $q_1$ and $q_2$, such that $L \subset Q_{ab} = V(q_{ab})$. By the uniqueness and Hilbert’s Theorem 90, we can take $a, b \in K(\sqrt{d})$. Moreover from Lemma 6.2.1, $Q_{ab} \neq Q_{ab}^\sigma$. So we have a line $L$ contained in a quadric surface $Q_{ab}$ both defined over $K(\sqrt{d})$ and not over $K$ and so by Section 6.1, and more specifically by equation (6.4) it follows that $V(q_{ab}, q_{ab}^\sigma)$ is determinantal over $K$.

Lastly, suppose for some $d \in K^* - (K^*)^2$, and $\text{Gal}(K(\sqrt{d})/K) =< \sigma >$ there is a divisor $D_1 \in \text{Div}^2_{K(\sqrt{d})}(\mathcal{H})$ with $D_1 \not\sim D_1^\sigma$ and $D_1 + D_1^\sigma$ is not a hyperplane section of $\mathcal{H}$, where $D_1 = P_1 + P_2$ with $P_1 \neq P_2$. Let $L$ be the line through the two distinct points $P_1$ and $P_2$. As above there is a unique quadratic surface $Q_{ab}$ containing $L$. Since $D_1 \not\sim D_1^\sigma$ and
\[ D_1 + D'_1 \text{ is not a hyperplane section, it follows from Lemma 6.2.1 that } Q_{ab} \neq Q'_{ab}. \] So we have a line \( L \) contained in a quadric surface \( Q_{ab} \) both defined over \( K(\sqrt{d}) \) and not over \( K \) and so by Section 6.1, and more specifically by equation (6.4) it follows that \( V(q_{ab}, q'_{ab}) \) is determinantal over \( K \) and the reverse direction is proved.

\[ \square \]

**Remark 6.2.3.** From the proof of Theorem 6.2.2, and equation (6.4), we have the more succinct but less precise result that \( X \) is determinantal if and only if \( V(q) \) is defined over \( K(\sqrt{d}) \) but not \( K \) and contains a line defined over \( K(\sqrt{d}) \).

**Remark 6.2.4.** In the converse direction of Theorem 6.2.2, if \( \mathcal{H}(K) \neq \emptyset \), then there is a matrix \( M \) of linear forms over \( K \) with \( \det M = f = q_{ab}q'_{ab} \) but \( f \) is not \( K \)-anisotropic. So \( M \) is the left representation of a NAA but not a NADA. As we want to construct new NADAs we will want to apply Theorem 6.2.2 in the case that \( \mathcal{H}(K) = \emptyset \). There are two ways this can happen. Either;

\[ 1) \text{ there is a } v \in M_K \text{ such that } \mathcal{H}(K_v) = \emptyset, \]

\[ 2) \text{ or } \mathcal{H} \text{ is non-trivial in } III(\text{Jac}(\mathcal{H})/K). \]

In either case Theorem 6.2.2 will not only build a determinantal surface \( X = V(\det M) \) over \( K \), but \( M \) will be the representation of a NADA that arises in class \((3)^{irred}\) from Chapter 4. We are most interested when (2) holds, and the examples that we give in the next chapter come from non-trivial elements in \( III(E/K) \) for some elliptic curve \( E \) over \( K \).

Moreover, suppose that \( \mathcal{H} \) is non-trivial in \( III(\text{Jac}(\mathcal{H})/K) \), so its order equals its index. Then the requirements on the existence of certain divisors from Theorem 6.2.2 implies that the index (hence the order of \( \mathcal{H} \) in \( III \)) will be 2 or 4. Furthermore, if \( \mathcal{H} \) has a divisor as in (1) of Theorem 6.2.2, then the order of \( \mathcal{H} \) will be 2.

With the above as a guide, the methods in Chapter 7 start with an elliptic curve \( E \) and the construction of elements of \( III(E/K) \) of order 2 or 4.
Suppose $M$ and $N$ are two linear matrices over $K$ such that $\det M = \det N = f$. The proof of Theorem 6.2.2 produces divisors $D_1^M$ attached to $M$ and $D_1^N$ attached to $N$.

**Corollary 6.2.5.** With notation as above, $D_1^M \sim D_1^N$ or $D_1^M + D_1^N$ is a hyperplane section.

**Proof.** Construct $D_1^M$ and $D_1^N$ as in the proof of Theorem 6.2.2. Then $D_1^M$ and $D_1^N$ each define points $[a_M, b_M]$ and $[a_N, b_N] \in \mathbb{P}^1$ such that the lines defined by $D_1^M$ and $D_1^N$, $L_{D_1^M}$ and $L_{D_1^N}$ lie in $Q_{a_M b_M}$ and $Q_{a_N b_N}$ respectively. Since $L_{D_1^M}$, $L_{D_1^N} \subset Q$, then $[a_M, b_M] = [a_N, b_N]$ by Lemma 6.2.1. The result follows. 

So if there are two different linear matrices $M, N$ such that $\det M = \det N = f = qq^\sigma$, then they correspond to linearly equivalent divisors on $H$ or they correspond to a hyperplane section of $H$.

**Remark 6.2.6.** The proof of Theorem 6.2.2 shows that if $M$ is the representation of a NADA $A$ of class $(3)^{irred}$, so $\det M$ factors as $qq^\sigma$ over some quadratic extension $K(\sqrt{d})$ of $K$ with $\text{Gal}(K(\sqrt{d})/K) \approx \langle \sigma \rangle$, and $Q = V(q)$ is nonsingular and $H = V(q, q^\sigma)$ is absolutely irreducible, then a row of $N = \text{adj}(M)$ defines an ideal that cuts out a curve $C^3 \subset Q$. If $C^3$ is of type $(2, 1)$ in some ruling on $Q$ (so is a (possibly degenerate) twisted cubic) then we say that $A$ is of type $(3)^{irred}_{twisted}$. If $C^3$ is of type $(3, 0)$ on $Q$ then we will say $A$ is of type $(3)^{irred}_{nonred}$ (to suggest non-reduced). If on the other hand $H \subset C^3$, we say that $A$ is of type $(3)^{irred}_{elliptic}$. We claim it is “not hard” to show that this designation is independent of the choice of row (or column) of $N$. The theorem and its corollaries give us ways to build NADAs of type $(3)^{irred}_{elliptic}$ — we do not know if there are any NADAs of type $(3)^{irred}_{twisted}$ or for that matter of type $(3)^{irred}_{nonred}$. If $A \in (3)^{irred}_{elliptic}$ and $H$ is (everywhere) locally soluble, so of order 2 or 4 in $\text{III}(\text{Jac}(H)/K)$, we say that $A$ is of type $(3)^{irred}_{elliptic,2}$ or $(3)^{irred}_{elliptic,4}$. We will produce examples of NADAs of both of these types in the next chapter.
### 6.3 Rational 2-torsion and 4-torsion Corollaries

The following corollaries supplement the analysis of Theorem 6.2.2.

Suppose we have an elliptic curve $E/K$ with a $K$-rational 2-torsion point $P$ as in Example 5.3.6. Let $E'' = E/ < P >$ and $\phi : E \to E''$ be the corresponding 2-isogeny. Let $K(\sqrt{e})$ be a non-trivial quadratic extension of $K$ and let $C_e$ be the quadratic twist of $E$ by $\phi$ over $K(\sqrt{e})$. Then recall we have the following commutative diagram of morphisms,

\[
\begin{array}{ccc}
C_e & \xrightarrow{\theta} & E' \\
\downarrow{\gamma} & & \downarrow{\phi} \\
E & \xrightarrow{\phi} & E''
\end{array}
\]

where $\gamma$ is a 2-cover defined over $K$, $\hat{\phi}$ is the dual isogeny of $\phi$, and the defining equation for $E$ is:

\[y^2 = x^3 + ax^2 + bx.\]

Moreover we have the embedding of $C_e$ into $\mathbb{P}^3$ called $\iota : C_e \hookrightarrow \mathbb{P}^3$ via $(z, w) \mapsto (z, w, 1, z^2)$, we call $\iota(C_e) = C$. Recall from Section 5.5 that the defining equations for $C$ are:

\[z_3z_2 - z_0^2 = e z_1^2 - e^2 z_2^2 + 2ae z_0^2 - (a^2 - 4b)z_3^2 = 0.\]

The divisor on $C$ defined by the hyperplane section $z_0 = 0$ is

\[H = (0, \sqrt{e}, 1, 0) + (0, -\sqrt{e}, 1, 0) + (0, \sqrt{\frac{a^2 - 4b}{e}}, 0, 1) + (0, -\sqrt{\frac{a^2 - 4b}{e}}, 0, 1).\]

We now want to derive the divisor $H$ in a different way. Indeed, we want to show that $H$ is the divisor $\iota \circ \gamma^* \circ (\hat{\phi})^*(\mathcal{O}_E)$. First note that $(\hat{\phi})^*(\mathcal{O}_E) = \mathcal{O}_{E''} + (0, 0)_{E''}$, i.e. $\ker \hat{\phi} = \{\mathcal{O}_{E''}, (0, 0)_{E''}\}$. Now we consider points on $C$ which map onto $\mathcal{O}_{E''}$ and $(0, 0)_{E''}$. From the isomorphism $\iota : C_d \to C$ we also have

\[\iota^{-1}((0, \pm \sqrt{e}, 1, 0)) = (0, \pm \sqrt{e}),\]
Thus we have
\[ \gamma(\infty_\pm) = (0, 0)_{E''} \text{ and } \gamma((0, \pm \sqrt{e})) = O_{E''}. \]

But, \( \gamma \) is a degree 2 map and so \( \gamma^*((0, 0)_{E''}) = \infty_+ + \infty_- \) and \( \gamma^*(O_{E''}) = (0, \sqrt{e}) + (0, -\sqrt{e}) \).

Thus we have
\[ \iota \circ \gamma^* \circ (\hat{o})^*(O_E) = \iota \circ \gamma^*(O_{E''} + (0, 0)_{E''}) = \iota(\infty_+ + \infty_- + (0, \sqrt{e})_{C_{d}} + (0, -\sqrt{e})_{C_{d}}) = H. \]

Therefore, the hyperplane section \( H \) is the pullback of \( O_E \) via \( \gamma^* \circ (\hat{o})^* \).

**Corollary 6.3.1.** With notation as above, let \( C_e \) be the quadratic twist of \( E \) by \( \phi \) over \( K(\sqrt{d}) \). Let \( K(\sqrt{d}) \) be a non-trivial quadratic extension of \( K \) with \(< \sigma > = \text{Gal}(K(\sqrt{d})/K) \) and such that there is a \( Q \in E''(K(\sqrt{d})) \) with \( Q + E^o, Q - E^o \not\in \ker \hat{o} \). Then the divisor \( D = \gamma^*(Q) + \gamma^*(Q^o) \) is a divisor on \( C_e \) as specified in (1) or (2) in Theorem 6.2.2.

**Proof.** Suppose there is a \( Q \in E''(K(\sqrt{d})) \) such that \( Q + E^o, Q - E^o \not\in \ker \hat{o} \). Let \( D_1 = \gamma^*(Q) \). Then if \( D_1 \sim D_1^o \), we have \( \gamma^*(Q) \sim \gamma^*(Q^o) \) which implies \( \phi^*(Q) \sim \phi^*(Q^o) \). Since \( \phi^*(Q) = R_1 + (R_1 + E^o P) \), and \( \phi^*(Q^o) = R_2 + (R_2 + E^o P) \), for some \( R_1, R_2 \in E \), then from Lemma 5.1.4 we have \( 2R_1 \sim 2R_2 \). This implies \( R_1 - E^o R_2 \in E[2] \). But \( \phi(R_1 - E^o R_2) = Q - E^o Q^o \) and so \( O_E = [2](R_1 - E^o R_2) = \hat{o}(Q - E^o Q^o) \) a contradiction.

Suppose that \( \iota(D_1 + D_1^o) \) is a hyperplane section. Any two hyperplane sections are linearly equivalent and so \( \theta_*(D_1 + D_1^o) \sim \theta_*(\iota^{-1}(H)) = \theta_* \theta^* \circ \phi^* \circ \hat{o}^*(O_E) = [2]^*(O_E) \sim 4O_E \) by Lemma 5.1.4. So Lemma 5.1.4 implies \( 2R_1 + E^o 2R_2 = O_E \) which implies \( R_1 + E^o R_2 \in E[2] \). But \( [2](R_1 + E^o R_2) = \hat{o}(Q + E^o Q^o) \) which implies \( Q + E^o Q^o \in \ker \hat{o} \), a contradiction. Therefore \( D_1 \) is a divisor satisfying the requirements of Theorem 6.2.2 and the corollary is proved by contradiction. \( \square \)
Suppose we have an elliptic curve $E$ with a $K$-rational 4-torsion point $P$ as in Section 5.5. Let $K(\tau)$ be a cyclic quartic extension of $K$ whose unique quadratic subfield is $K(\sqrt{\epsilon})$. Let $C_{e,\tau}$, $\mathcal{H}_\tau$, $E''$, and $E'$ be as in Section 5.5 and recall the commutative diagram of morphisms:

\[
\begin{array}{ccc}
\mathcal{H}_\tau & \xrightarrow{\Gamma} & C_{e,\tau} \\
\downarrow^\epsilon & & \downarrow^\gamma \\
E & \xrightarrow{\phi} & E'' \\
& \searrow^\psi & \searrow \\
& & E'
\end{array}
\]  

(6.6)

Recall that the homogenized defining equations for $E'$ is:

\[ V^2W = U^3 - 2(t^2 - 4)U^2W + (t^2 + 4)^2UW^2, \]

and the defining equations for $\mathcal{H}_\tau$ are:

\[
2dz^2 + 2(t^2 + 4)\mu^2 = (\tau^2 + (\tau^\sigma)^2)(\alpha_1^2 + d\alpha_2^2) + \frac{(\tau^2 - (\tau^\sigma)^2)(2d\alpha_1\alpha_2)}{\sqrt{d}} \\
4tz\mu = \frac{(\tau^2 - (\tau^\sigma)^2)}{\sqrt{d}}(\alpha_1^2 + d\alpha_2^2) + (\tau^2 + (\tau^\sigma)^2)(2d\alpha_1\alpha_2).
\]

The homogenized defining equation for $\gamma \circ \Gamma$ is:

\[
(U, V, W) = \gamma \circ \Gamma(z, \alpha_1, \alpha_2) = (dz^2\mu, dz(\alpha_1^2 - d\alpha_2^2), \mu^3)
\]

Consider the divisor $H = \Gamma^* \circ \gamma^*(\mathcal{O}_{E'}) = \Gamma^* \circ \gamma^*((0, 1, 0))_{E'}$ on $\mathcal{H}_\tau$. It follows from the equations above that $H$ is also the hyperplane section of $\mathcal{H}_\tau$ defined by $\mu = 0$ and so the pullback of the identity on $E'$ is a hyperplane section on $\mathcal{H}_\tau$. (From the cocycle calculation in Section 5.5 we also see that the pullback of $(0, 0)_{E'}$ is a hyperplane section on $\mathcal{H}_\tau$.) Furthermore, then we have that $\epsilon_*(H) = \phi^* \circ \psi^*(\mathcal{O}_{E'}) = \mathcal{O}_E + P + [2]P + [3]P$.

**Corollary 6.3.2.** With notation as above, let $\mathcal{H}_r$ be the twist of $E$ by $\phi \circ \psi$ over a cyclic quartic extension $K(\tau)$ of $K$, as in the diagram (6.6) above. Suppose $C_{e,\tau}$ is of index 2 over $K$. Let $R \in E'(K)$ be such that $R \notin \ker \widehat{\phi} \circ \psi$. Then $D = \Gamma^* \circ \gamma^*(R)$ will be a divisor on $\mathcal{H}_r$ as specified in (2) of Theorem 6.2.2, for some quadratic extension $K(\sqrt{d})$ of $K$. 

Remark 6.3.3. Since $\Gamma$ is a 2-cover over $K$, if $H_\tau$ is index 4 over $K$ then $C_{e,\tau}$ is index 2 over $K$. 

Proof. Let $R \in E'(K)$ and $D' = \gamma^*(R)$. Since $C_{e,\tau}$ is index 2 we have $D' = Q + Q''$, $Q \in C_{e,\tau}(K(\sqrt{d})) - C_{e,\tau}(K)$ for some $d \in K^* - (K^*)^2$ with $< \sigma > = Gal(K(\sqrt{d})/K)$. Let $D_1 = \Gamma^*(Q)$, then $D''_1 = \Gamma^*(Q'')$ since $\Gamma$ is defined over $K$.

By way of contradiction, suppose that $D_1 \sim D''_1$. Then via the isomorphism $\epsilon$, we get that $\epsilon_*(D_1) = \phi^*(\theta(Q)) \sim \epsilon_*(D''_1) = \phi^*(\theta(Q''))$. But $\mathcal{O}_{E''} \neq \theta(Q) - E'' \theta(Q'') \in ker \psi$ so $\theta(Q) = \theta(Q'') + E'' \phi(P)$. Thus $\phi^*(\theta(Q)) = \tau_p \circ \phi^*(\theta(Q''))$. Let $S \in \phi^{-1}(\theta(Q))$ so then $\phi^*(\theta(Q)) = S + (S + E[2]P)$ and $\phi^*(\theta(Q'')) = (S + E P) + (S + E[3]P)$. Hence by Lemma 5.1.4 $S + (S + E[2]P) \sim (S + E P) + (S + E[3]P)$ if and only if $S + E(S + E[2]P) = (S + E P) + E(S + E[3]P)$. But $P$ is 4-torsion and so the above equality reduces to

$$[2]P = 0, \quad (6.7)$$

which is a contradiction. So, $D_1 \not\sim (D_1)'$ on $H_\tau$.

Now suppose that $D_1 + D''_1$ is a hyperplane section. As above, we consider the corresponding divisor on $E$ and we have $\epsilon_*(D_1 + D''_1) = \phi^* \circ \psi^*(R) = S + (S + E P) + (S + E [2]P) + (S + E [3]P)$, for some $S \in E$. Let $H$ be the divisor in the discussion preceding the corollary, which is a hyperplane section of $H_\tau$ and maps to the divisor $\mathcal{O}_E + P + [2]P + [3]P$ via $\epsilon$. But any two hyperplane sections are linearly equivalent and $P$ is 4-torsion. Hence by Lemma 5.1.4 we have,


But $[4]S = \mathcal{O}_E$ implies that $\phi \circ \psi(R) = \mathcal{O}_E$, so $R \in ker \phi \circ \psi$ which is a contradiction. Thus, $D_1$ is a divisor satisfying the requirements of Theorem 6.2.2 and the corollary is shown by contradiction.

$\square$
Chapter 7

Methods to Build New NADAs

Recall that 4-dimensional NADAs can be classified depending on how the determinant of their left representations factor. This chapter provides methods for building examples of NADAs of class \((3)_{\text{irred}}^{\text{elliptic},2}\) and \((3)_{\text{irred}}^{\text{elliptic},4}\), which are the subclasses of class 3 in Chapter 4 and are described in Remark 6.2.6. Recall that there are no previously known NADAs that fall into these classes. The two methods to build new NADAs in these classes requires building a non-trivial element of order 2 or 4 in \(\text{III}(E/K)\) for some elliptic curve \(E\) over \(K\). The methods are quite similar.

Method 1

1. Let \(E : y^2 = x^3 + ax^2 + bx\) be an elliptic curve over \(K\) with the rational 2-torsion point \(P = (0, 0)\). We seek such an \(E\) with \(#\text{III}(E/K)[2^\infty] = 4\). Then by the Cassels pairing, \(\text{III}(E/K)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) and \(2\text{III}(E/K)[2^\infty] = 0\). (For more details on the Cassels pairing see Chapter \(X\) in [28]. The only way we know to find such \(E\) is through a computer search that assumes BSD to numerically calculate \(|\text{III}(E/K)|\).)

2. Let \(\phi : E \rightarrow E'' = E/\langle P \rangle\) be the natural projection, and perform a \(\phi\)-descent on \(E/K\). This involves building \(C_d\) for \(d \in K(T, 2)\) (as in Example 5.3.6), where \(C_d\) is a twist of \(E\) by \(\phi\) over \(K(\sqrt{d})\), a quadratic extension of \(K\). This produces the \(\phi\)-Selmer group, \(S^{(\phi)}(E/K)\).

3. Since we believe \([2]\text{III}(E/K)[2^\infty] = 0\) this gives us confidence that we can pick a
$d$ such that $C_d \in S^{(\phi)}(E/K)$ and such that there are no 4-descendents above $C_d$, as in Remark 5.3.5. We perform a 4-descent on $E$ and if there is a $C_d$ with no 4-descendents then $C_d$ is order 2 in $\text{III}(E/K)$. (To check existence of 4-descendents one can use the command $\text{FourDescent}$ in Magma.) Although it requires faith to believe such a $C_d$ exists, the 4-descent can actually verify that it does.

(4) We need to build a $D_1 \in \text{Div}^2_{K(\sqrt{d})}(C_d)$ with the properties specified in Theorem 6.2.2. Let $< \sigma > = \text{Gal}(K(\sqrt{d})/K)$. We can use Corollary 6.3.1 to find such a $D_1$, although this is not the only way to do so. Once a $D_1$ is chosen, $L, L^\sigma, Q = V(q), Q^\sigma = V(q^\sigma)$ are uniquely determined.

(5) We now have a line $L$ and a non-singular quadric surface $Q$ containing $L$, both defined over $K(\sqrt{d})$ but not over $K$ with $H = V(q, q^\sigma)$ irreducible. So by Section 6.1 we can build a matrix $M$ such that $\det M = qq^\sigma$ as in equation (6.4).

**Method 2**

(1) Let $E : v^2 = u^3 + (t^2 + 2)u^2 + u$ be an elliptic curve over $K$ with a $K$-rational 4-torsion point $P = (-1, t)$. We seek $E$ such that $\#\text{III}(E/K)[2^\infty] = 16$. We hope in fact $\text{III}(E/K)[2^\infty] = (\mathbb{Z}/4\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})^4$ so all elements of $\text{III}$ are of order less then 8. (The only way we know to find such $E$ is through a computer search that assumes BSD to numerically calculate $|\text{III}(E/K)|$.)

(2) Let $E \xrightarrow{\phi} E'' = E/ < 2P > \xrightarrow{\psi} E' = E/ < P >$ be the natural projections, and perform a $\phi \circ \psi$-descent on $E/K$. Build $\mathcal{H}_\tau$ as in Section 5.5 (recall that this produces $\mathcal{H}_\tau$, the twist of $E$ by $\phi \circ \psi$ over a cyclic quartic extension $K(\tau)$ of $K$).

(3) As in method 1, the existence of $\tau$ such that $\mathcal{H}_\tau$ is non-trivial in $\text{III}(E/K)$ is not guaranteed. But if we pick a $\tau$ such that $C_d = [2]\mathcal{H}_\tau$ is of index 2 in $\text{III}(E/K)$ and such that $\mathcal{H}_\tau$ is locally soluble, then by Remark 5.4.1, $\mathcal{H}_\tau$ is of order 4 in $\text{III}(E/K)$. (The index of $C_d$ can be verified using the techniques mentioned in method
1, although a higher descent may be necessary, such as an 8-descent, which can be performed in Magma with the command EightDescent. This is not the only technique to verify that the order of $\mathcal{H}_r$ is 4, but merely the technique we use in our examples below.)

(4) Build $D_1 \in \text{Div}^2_{K(\sqrt{d})}(\mathcal{H}_r)$ with the properties specified in (2) of Theorem 6.2.2. One such divisor $D_1$ is given in Corollary 6.3.2. By fixing $D_1$, if $<\sigma> = \text{Gal}(K(\sqrt{d})/K)$, then $L, L^\sigma, Q = V(q), Q^\sigma = V(q^\sigma)$ are uniquely determined.

(5) We now have a line $L$ and a non-singular quadric surface $Q = V(q)$ containing $L$, both defined over $K(\sqrt{d})$ but not over $K$ with $\mathcal{H} = V(q, q^\sigma)$ irreducible. So by Section 6.1 we can build a matrix $M$ such that $\det M = qq^\sigma$ as in equation (6.4).

Both Methods build the left-representation of a NAA $A$. But since $C_d$ and $\mathcal{H}_r$ were chosen to be non-trivial in $\Pi(E/K)$, $A$ will actually be a NADA in the classes $(3)_{\text{irred elliptic, 2}}$ or $(3)_{\text{irred elliptic, 4}}$ of Remark 6.2.6, both of which had no previously known examples.

### 7.1 Examples using Methods 1 and 2

Notation in this section is taken from Section 5.5. Recall the following commutative diagram of curves and morphisms:

$$
\begin{align*}
\mathbb{P}^3 \ni C & \xrightarrow{\zeta} C_d & \xrightarrow{\phi} E & \xrightarrow{\psi} E' \\
\phi & \downarrow \gamma \\
E & \xrightarrow{\zeta} & E'' & \xrightarrow{\psi} E'
\end{align*}
$$
where \( t \in \mathbb{Q} \) and

\[
E : \quad v^2 = u^3 + (t^2 + 2)u^2 + u
\]
\[
E'' : \quad Y^2 = X^3 + (t^2 - 4)X^2 - 4t^2X
\]
\[
E' : \quad V^2 = U^3 - 2(t^2 - 4)U^2 + (t^2 + 4)^2U
\]
\[
C_d : \quad dw^2 = d^2 - 2(t^2 + 2)dz^2 + t^2(t^2 + 4)z^4
\]
\[
C : \quad x^2 - zw = dy^2 - d^2z^2 + 2(t^2 + 2)dx^2 - t^2(t^2 + 4)w^2 = 0
\]

Let \( t = 10 \) and so,

\[
E : v^2 = u^3 + (102)u^2 + u.
\]

We pick this \( E \) because SAGE computes (via the command \( E.sha().an() \)) that \(|\text{III}(E/\mathbb{Q})| = 4\). This calculation assumes BSD but gives us the confidence to search for non-trivial elements in \( \text{III}(E/\mathbb{Q})[2] \). SAGE can also effectively compute the \( \phi \)-Selmer group, and using the command \( E.simon\_two\_descent() \) it tells us that \(|S^{(\phi)}(E/\mathbb{Q})| = 8\). SAGE also computes the primes of bad reduction of \( E \) which are 2, 5, 13. But given this, we can write down \( S^{(\phi)}(E/\mathbb{Q}) \) by hand. Using the notation of Section 5.3 we have

\[
\mathbb{Q}(T, 2) = \{ \pm 1, \pm 2, \pm 5, \pm 10, \pm 13, \pm 26, \pm 65, \pm 130 \}.
\]

The defining equation of \( C_d \) is:

\[
C_d : dw^2 = d^2 - 204dz^2 + 10400z^4.
\]

If \( d < 0 \), the left hand side is non-positive whereas the right hand side is always positive, so there cannot be a solution over \( \mathbb{R} \), i.e. \( C_d(\mathbb{R}) = \emptyset \) when \( d < 0 \).
So \( S^{(\phi)}(E/\mathbb{Q}) = \{C_1, C_2, C_5, C_{10}, C_{13}, C_{26}, C_{65}, C_{130}\} \).

Furthermore, SAGE calculates via a descent with the dual \( \hat{\phi} : E'' \rightarrow E \) that \( |S^{(\hat{\phi})}(E''/\mathbb{Q})| = 2 \) and \( \text{III}(E''/\mathbb{Q})[\hat{\phi}] = 0 \). So SAGE provably gives (not using BSD) that \( \text{rk } E'' = 0 \). Hence \( \text{rk } E = 0 \), too. Torsion is effectively computable and SAGE computes that \( |E(\mathbb{Q})_{\text{tors}}| = 4 \) and \( |E''(\mathbb{Q})_{\text{tors}}| = 4 \). But from construction of \( E \) and \( E'' \) we have \( |E''[2](\mathbb{Q})| = 4 \) and \( |E[4](\mathbb{Q})| = 4 \), so \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \) and \( E''(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2 \). It follows that \( E''(\mathbb{Q}) = \{O_{E''}, (-t^2, 0), (0, 0), (4, 0)\} \) and via the definition of \( \phi \) we conclude that \( E''(\mathbb{Q})/\phi(E(\mathbb{Q})) = 2 \).

Recall equation (4.4), which we state again with regards to the 2-isogeny \( \phi \),

\[
0 \rightarrow E''(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} S^{(\phi)}(E/\mathbb{Q}) \rightarrow \text{III}(E/\mathbb{Q})[\phi] \rightarrow 0.
\]

The above exact sequence will allow us to calculate elements of \( \text{III}(E/\mathbb{Q}) \) (since \( \text{III}(E/\mathbb{Q})[\phi] \) injects into \( \text{III}(E/\mathbb{Q}) \)).

First we need to calculate \( \delta(E''(\mathbb{Q})/\phi(E(\mathbb{Q}))) \). The definition of \( \delta \) when \( \ker \phi =< (0, 0)_E > \) is given in [28] in terms of \((m, y)\)-coordinates (from Section 5.5) as

\[
\delta(O_{E''}) = 1, \quad \delta((0, 0)_{E''}) = (102)^2 - 4 = 26, \quad (\text{mod } (\mathbb{Q}^*)^2)
\]

and for \((m, y) \neq (0, 0), O_{E''} \), \( \delta((m, y)) = m \quad (\text{mod } (\mathbb{Q}^*)^2) \).

So writing \( E'' \) in terms of \((x, y)\)-coordinates (as in Section 5.5), since \( x = m - 100, y = y, \delta \) takes the form,

\[
\begin{align*}
\delta(O_{E''}) &= 1 \quad (\text{mod } (\mathbb{Q}^*)^2), \\
\delta((-t^2, 0)) &= 26 \quad (\text{mod } (\mathbb{Q}^*)^2), \\
\delta((0, 0)) &= 1 \quad (\text{mod } (\mathbb{Q}^*)^2), \\
\delta((4, 0)) &= 26 \quad (\text{mod } (\mathbb{Q}^*)^2).
\end{align*}
\]

Thus any \( C_d \in S^{(\phi)}(E/\mathbb{Q}) \) other than \( C_1 \) or \( C_{26} \) will project onto a non-trivial element of \( \text{III}(E/\mathbb{Q}) \). For instance, \( C_2 \) is defined by

\[
C_2 : 2w^2 = 4 - 408z^2 + 10400z^4 \implies C_2 : w^2 = 2 - 204z^2 + 5200z^4.
\]
Since $C_2 \in \text{III}(E/\mathbb{Q}) - \{0\}$ we have $C_2$ is of order 2 in $\text{III}(E/\mathbb{Q})$, because it has index dividing 2 and its order is not 1.

Consider the divisor $D_{E'} = (1, 25\sqrt{17}) + (1, -25\sqrt{17})$ on $E'$. Now it pulls back to a degree 8 divisor $D'$ on $C_2$. We observed that 2 of the points in the support of $D'$ form the divisor $D_1 = \left( \frac{-2}{\sqrt{5(21 + 5\sqrt{17})}}, \frac{2(19 - 5\sqrt{17})}{\sqrt{5(21 + 5\sqrt{17})(21 + 5\sqrt{17})}} \right) + \left( \frac{2}{\sqrt{5(21 + 5\sqrt{17})}}, \frac{-2(19 - 5\sqrt{17})}{\sqrt{5(21 + 5\sqrt{17})(21 + 5\sqrt{17})}} \right).

Although the points in the support of $D_1$ are defined over a quartic extension (a quadratic extension of $\mathbb{Q}(\sqrt{17})$) the divisor $D_1$ is defined over $\mathbb{Q}(\sqrt{17})$.

Let $\langle \sigma \rangle = \text{Gal}(\mathbb{Q}(\sqrt{17})/\mathbb{Q})$. Let $D = D_1 + D'_1$, so $D = \left( \frac{-2}{\sqrt{5(21 + 5\sqrt{17})}}, \frac{2(19 - 5\sqrt{17})}{\sqrt{5(21 + 5\sqrt{17})(21 + 5\sqrt{17})}} \right) + \left( \frac{2}{\sqrt{5(21 + 5\sqrt{17})}}, \frac{-2(19 - 5\sqrt{17})}{\sqrt{5(21 + 5\sqrt{17})(21 + 5\sqrt{17})}} \right) + \left( \frac{-2}{\sqrt{5(21 - 5\sqrt{17})}}, \frac{2(19 + 5\sqrt{17})}{\sqrt{5(21 - 5\sqrt{17})(21 - 5\sqrt{17})}} \right) + \left( \frac{2}{\sqrt{5(21 - 5\sqrt{17})}}, \frac{-2(19 + 5\sqrt{17})}{\sqrt{5(21 - 5\sqrt{17})(21 - 5\sqrt{17})}} \right)$.

Now $C_2$ and $D$ can be embedded into $\mathbb{P}^3$ via $(z, w) \rightarrow (z, w, 1, z^2) = (x_0, x_1, x_2, x_3)$. Let $q_1 = x_0^2 - x_2x_3$ and $q_2 = 2x_1^2 - 4x_2^2 + 408x_0^2 - 10400x_3^2$. Then $\mathcal{C} = V(q_1, q_2)$ is a model of $C_2$ inside of $\mathbb{P}^3$. Let $L$ be the line determined by $D_1$. So, $L \subset Q_{ab} = V(q_{ab})$ with $q_{ab} = aq_1 + bq_2$, $a = 1$, $b = \frac{21 - 5\sqrt{17}}{50(-253 + 21\sqrt{17})}$.

Using equation (6.4) we get the following matrix $M =$
\[
\left(\begin{array}{cccc}
\frac{65}{2}x_3 + 19x_2 & 17(\frac{25}{2}x_3 - 5x_2) & 26x_0 - 866x_1 & -17(-10x_0 + 210x_1) \\
\frac{25}{2}x_3 - 5x_2 & \frac{65}{2}x_3 + 19x_2 & 10x_0 - 210x_1 & 26x_0 - 866x_1 \\
30x_0 - 170x_1 & -178x_0 - 698x_1 & -707200x_3 + 14120x_2 & -2903680x_3 + 58216x_2 \\
178x_0 + 698x_1 & 17(-30x_0 + 170x_1) & 2903680x_3 - 58216x_2 & -17(-707200x_3 + 14120x_2)
\end{array}\right).
\]

So we have built an $M$ such that $\det M = q_{ab}q_{\sigma}^{ab}$ and $V(q_{ab}, q_{\sigma}^{ab}) = C$. Moreover, since $C_2(\mathbb{Q}) = \emptyset$, $M$ represents a NADA $A$ over $\mathbb{Q}$. Furthermore, $C_2$ has order 2 in $\text{III}(E/\mathbb{Q})$, so $A$ is in class $(3)_{\text{irred}}^{\text{elliptic},2}$. 

The next example will build a homogeneous space of order 4 in a Tate-Shafarevich group. First we need a lemma that will be used to check for local solubility.

**Lemma 7.1.1.** (Hensel’s Lemma) For $0 \leq r < n$ let $f = (f_{r+1}, \ldots, f_n)$ be $n - r$ polynomials in $n$ variables over a discrete valuation ring $R$. Let $\pi$ be a uniformizing parameter for $R$. Assume there exists an $a \in R^n$ and an integer $k > 0$ such that

\[ f(a) \equiv 0 \pmod{\pi^{2k+1}}, \]

and such that the Jacobian matrix $M_f(a) = (\partial f_i/\partial x_j(a))$ reduced mod $\pi^{k+1}$ has maximal rank $n - r$. Then there exists some $b \in R^n$ which is a zero of all elements of $f$ such that

\[ b \equiv a \pmod{\pi^{k+1}}. \]

**Proof.** See [13].

Consider the following commutative diagram, with maps and curves as given in Section 5.5.
Now let $t = 41$ so the curve $E$ is defined by $E : y^2 = x^3 + (41^2 + 2)x^2 + x$. Such a $t$ was chosen because SAGE tells us (assuming BSD) that $|\text{III}(E/\mathbb{Q})| = 16$, so $\text{III}(E/\mathbb{Q})$ may have elements of order 4. Let $P = (-1, 41)$ and recall that $P \in E[4](\mathbb{Q}) - E[2](\mathbb{Q})$.

SAGE calculates that the primes of bad reduction for $E$ are $2, 5, 41, 337$. We choose $\tau = \sqrt{5 + 2\sqrt{5}}$ and so $\mathbb{Q}(\tau)$ is a cyclic quartic extension of $\mathbb{Q}$ with unique quadratic subfield $\mathbb{Q}(\sqrt{5})$. From Section 5.5 we have

$$q_1 = z^2 + 337\mu^2 - \alpha_1^2 - 5\alpha_2^2 - 4\alpha_1\alpha_2, \quad q_2 = 41z\mu - \alpha_1^2 - 5\alpha_2^2 - 5\alpha_1\alpha_2,$$

and $\mathcal{H}_\tau = V(q_1, q_2)$.

We want to show that $\mathcal{H}_\tau$ is of order 4 in $\text{III}(E/\mathbb{Q})$.

In Remark 5.4.1, we saw that if $\mathcal{H}_\tau$ is locally soluble, then $C_5$, the non-trivial quadratic twist of $E$ by $\phi$ over $\mathbb{Q}(\sqrt{5})$, satisfies $C_5 = [2]\mathcal{H}_\tau$ in $\text{III}(E/\mathbb{Q})$. If $C_5$ is of index 2 in $\text{III}(E/\mathbb{Q})$, then $\mathcal{H}_\tau$ will be order 4 in $\text{III}(E/\mathbb{Q})$.

Using Magma (or SAGE), we can show that $C_5 \in S^{(\phi)}(E/\mathbb{Q})$ (i.e. $C_5$ is locally soluble). Furthermore, running the command $\text{FourDescent}$ in Magma shows that there are four 4-descendents of $C_5$, running an $\text{EightDescent}$ on each 4-descendent, we see that there are no 8-descendents of $C_5$. So from Remark 5.3.5 we see that $C_5$ is a non-trivial element in $\text{III}(E/K)$, i.e. it has index 2.

Thus $C_5$ has no $\mathbb{Q}$-rational points, which implies that $\mathcal{H}_\tau(\mathbb{Q}) = \emptyset$. If we can show that $\mathcal{H}_\tau$ is (everywhere) locally soluble, then it is order 4 in $\text{III}(E/K)$.

The curve $\mathcal{H}_\tau$ will always have points locally at the primes of good reduction other than 2, so we need to only check $\mathcal{H}_\tau(K_v) \neq \emptyset$ for primes of bad reduction, the prime 2, and
the infinite primes. Recall that the primes of bad reduction for $E$ are $\{2, 5, 41, 337\}$.

Using Hensel’s lemma we can produce the following points in $\mathcal{H}_r(\mathbb{Q}_p)$ for $p = 2, 5, 41, 337, \infty$. We will give the value of $k$ and the point on $\mathcal{H}_r(\mathbb{Z}/p^{2k+1}\mathbb{Z})$ in $(\alpha_1, \alpha_2, z, \mu)$ coordinates, for each $p$. For $p = 2$, let $k = 1$ and then $(7, 1, 7, 3)$ is the requisite point on $E \pmod{8}$. For $p = 5$, let $k = 0$ and then $(4, 1, 3, 2)$ is the requisite point on $E \pmod{5}$. For $p = 41$, let $k = 0$ and then $(33, 8, 33, 39)$ is the requisite point on $E \pmod{41}$. For $p = 337$, let $k = 0$ and then $(254, 260, 235, 20)$ is the requisite point on $E \pmod{337}$. By simple substitution it is not hard to see that $E/(\mathbb{Q})$ has points at the (real) infinite prime as well. Thus $\mathcal{H}_r$ has points everywhere locally (i.e. is locally soluble) and so $\mathcal{H}_r$ is of order 4 in $\text{III}(E/\mathbb{Q})$.

Now we need to find a divisor on $\mathcal{H}_r$ satisfying the hypotheses of Theorem 6.2.2. Note that $R = (t^2 + 4, \pm 4(t^2 + 4))|_{t=41} \in E'(\mathbb{Q})$. But in [11] it is shown that $\ker \hat{\psi} \circ \phi(\mathbb{Q}) = \{O_{E'}, (0, 0)_{E'}\}$. Thus $R \in E'(\mathbb{Q}) - \ker \hat{\psi} \circ \phi$. So let $R = (1685, 6740)$. Its pullback onto $\mathcal{H}_r$ in $(\alpha_1, \alpha_2, z, \mu)$-coordinates is

$$(\Gamma \circ \gamma)^{-1}(R) = \left\{ \left(-\sqrt{1685 + 80\sqrt{337}}, \frac{674 + 41\sqrt{337}}{\sqrt{1685 + 80\sqrt{337}}}, -\sqrt{337}, 1\right), \right.$$

$$\left(\sqrt{1685 + 80\sqrt{337}}, -\frac{674 + 41\sqrt{337}}{\sqrt{1685 + 80\sqrt{337}}}, -\sqrt{337}, 1\right),$$

$$\left(-\sqrt{1685 - 80\sqrt{337}}, \frac{674 - 41\sqrt{337}}{\sqrt{1685 - 80\sqrt{337}}}, \sqrt{337}, 1\right),$$

$$\left(\sqrt{1685 - 80\sqrt{337}}, -\frac{674 - 41\sqrt{337}}{\sqrt{1685 - 80\sqrt{337}}}, \sqrt{337}, 1\right) \right\}.$$ 

Now call these 4 points $R_1, R_2, R_3, R_4$ respectively. Note that the divisor $D_1 = R_1 + R_2$ is defined over $\mathbb{Q}(\sqrt{337})$ and since $\Gamma^* \circ \gamma^*(R)$ is defined over $\mathbb{Q}$ we have $D_1^* = R_3 + R_4$, where $< \sigma > = \text{Gal}(\mathbb{Q}(\sqrt{337})/\mathbb{Q})$. Let $L$ be the line through the points $R_1, R_2$ and so a computation shows,

$$L : z + \sqrt{337} \mu = (674 + 41\sqrt{337})\alpha_1 + (1685 + 80\sqrt{337})\alpha_2 = 0.$$ 

This also uniquely defines the quadric $q_{ab}$ in the pencil generate by $q_1$ and $q_2$ such that $L \subset Q_{ab} = V(q_{ab})$, by Lemma 6.2.1. But now from Section 6.1 and equation (6.4) we get
\[
M =
\begin{pmatrix}
z & 337\mu & -674\alpha_1 - 1685\alpha_2 & -337(41\alpha_1 + 80\alpha_2) \\
\mu & z & -41\alpha_1 - 80\alpha_2 & -674\alpha_1 - 1685\alpha_2 \\
164\alpha_1 + 373\alpha_2 & 3029\alpha_1 + 6814\alpha_2 & 124189z + 2265988\mu & 2265988z + 41851693\mu \\
-3029\alpha_1 - 6814\alpha_2 & 337(-164\alpha_1 - 373\alpha_2) & -2265988z - 41851693\mu & -337(124189z + 2265988\mu)
\end{pmatrix}.
\]

Therefore, \( \det M = f = q_{ab}q_{ab}^\sigma \) with \( \mathcal{H}_r = V(q_{ab}, q_{ab}^\sigma) \), where \( <\sigma> = \text{Gal}(\mathbb{Q}(\sqrt{337})/\mathbb{Q}) \).

Now from construction, the determinants of the two matrices given in this chapter fall into class \((3)^{\text{irred}}\) from Chapter 4, and more specifically classes \((3)^{\text{irred}}_{\text{elliptic},2}\) and \((3)^{\text{irred}}_{\text{elliptic},4}\) respectively. So we know that the algebras they represent do not come from twisted fields. Furthermore, they do not represent quaternion algebras which are in class 2, and they do not represent field extensions of degree 4 which are in class 4. Thus, not only do the methods produce examples of algebras in a class with no previous known examples, the algebras they produce are not just NADAs, but specifically they are NOT associative algebras!
Bibliography


