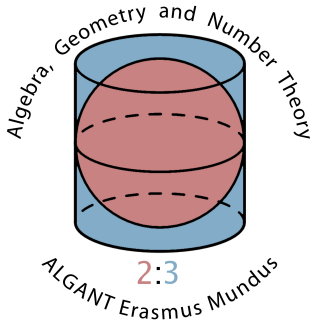


Universiteit Leiden
Mathematisch Instituut

Master Thesis

Density of Rational Points on a Family of Diagonal Quartic Surfaces

Thesis Advisor
Prof. Ronald M. van Luijk

Candidate
Dino Festi

Academic Year 2011–2012

Contents

To Antonella

Introduction

Finding integer solutions of a system of equations with integer coefficients only is one of the most ancient mathematical problems: the first attempt to solve such a problem can be found in India, around 800 b.C. In the third century we can find the first large study about this problem, by Diophantus of Alexandria: this is why now we call this kind of problems *diophantine problems*.
In his studies, Diophantus treated only some particular equations, and did not develop a general theory about these equations.
Even though mathematicians reached many new results about diophantine problems throughout history, a formulation of a general theory about the problem is still an unfulfilled aim.
In the last centuries a geometric approach to the problems turned out to be advantagious: in this approach, the so called K3 surfaces play an important role.
The K3 surfaces are the 2-dimensional analogues of elliptic curves in the sense that their canonical sheaf is trivial (see [19, 20] for more details).The K3 surfaces are just in between surfaces that are geometrically relatively easy in some technical sense and surfaces that are geometrically complicated. Smooth quartic surfaces in $\mathbb{P}^3$ are examples of K3 surfaces. Little is known about the arithmetic of these surfaces. It is for instance not known whether there exists a K3 surface over the rational numbers (or any number field) on which the set of rational points is neither empty nor dense.

In 2010, Logan, McKinnon and van Luijk gave in [9] an interesting result about density of rational points on a large family of projective diagonal quartic surfaces, namely:

Theorem (Theorem 3.4)**.** *Let $a, b, c, d \in \mathbb{Q}^\times$ be nonzero rational numbers with abcd square. Let $P = (x_0 : y_0 : z_0 : w_0)$ be a rational point on the surface*

$$V\colon ax^4 + by^4 + cz^4 + dw^4 = 0,$$

and suppose that all the coordinates of P are nonzero and that P does not lie on

any of the 48 lines of the surface. Then the set of rational points of the surface is dense in both the Zariski and the real analitic topology.

To prove this result, the authors consider two elliptic fibrations of the surface, and they show that any smooth fiber with at least one rational point, viewed as elliptic curve has four rational 2-torsion points. Using the hypotheses concerning P they show that then P does not lie on an intersection of two singular fibers and it has infinite order on at least one of the smooth fibers passing through it. Then they use this point and the group structure of the fiber to get infinitely many other rational points on the fiber. For each of these points they apply the same argument, but with respect to the other fibration, deducing the Zariski density of the set of rational points on V.

In this thesis we will use a similar argument, but for a more specific case, not covered by the previous theorem. The case is less general, since the family we consider is given by two parameters instead of the four (in fact three) of the family considered in [9], but we get a similar result assuming weaker hypotheses. Recall that we will always assume the existence of at least one rational point on the surface. We can state our result as follows:

Theorem. *Let c_1, c_2 be two nonzero rationals and W be the surface defined as*

$$W\colon\ x^4 - 4c_1^2y^4 - c_2z^4 - 4c_2w^4 = 0.$$

Let $P = (x_0 : y_0 : z_0 : w_0)$ be a rational point on W with x_0 and y_0 both nonzero. If $|2c_1|$ is a square in $\mathbb{Q}^\times$, then also assume that z_0, w_0 are not both zero. Then the set of rational points on the surface is Zariski dense.

To prove this result we consider two elliptic fibration of W defined over the rationals and we show that any smooth fiber with at least one rational point, viewed as an elliptic curve, has at most one nontrivial rational 2-torsion point and no other rational torsion points. Using the hypotheses concerning P we show that then P does not lie on an intersection of two singular fibers and it has infinite order on at least one of the smooth fibers passing through it. Then, using the same argument as in [9] we deduce the Zariski density of the set of rational points on W.
Another similar result can be found in [7]: in this paper Elkies shows that on the surface $x^4+y^4+z^4-w^4 = 0$ the set of rational points is dense in both the Zariski and real topology. This surface is neither in our family nor in the family considered in [18].

In [18], van Luijk focuses on the set of rational points on a surface which do not ensure the Zariski density of the set of rational points. He obtained the following result:

Theorem (Theorem 2.2)**.** *Let k be a number field and let $\overline{k}$ be an algebraic closure of k. Let V be a projective smooth surface over k. For each integer d there exists an explicitly computable closed subset $Z \subseteq V$ such that for each field extension K of k of degree at most d over $\mathbb{Q}$ and for each twist W of V, with corresponding isomorphism $\phi\colon W_{\overline{k}} \mapsto V_{\overline{k}}$, the set $W(K)$ is Zariski dense in W as soon as it contains any point outside $\phi^{-1}(Z)$.*

In our work, in 4.2, we give an explicit (although very simple) example of such a subset for our case.

We start our work introducing the family of diagonal quartic surfaces together with two rational fibrations. We also study the lines on the surface and give some results about the image of the lines on the surface under the fibrations.
For a good comprehension of the fibration it is crucial to study their fibers. This is what we do in the second chapter. First we consider only a special case, for $c_1 = \frac{1}{2}$ and $c_2 = 1$; then we study the general case, showing that our fibrations are actually elliptic fibrations. We compute the j-invariant and discriminant of the smooth fibers, and give an explicit list of the singular fibers.
Proposition 2.2.4 is crucial in providing the explicit example for Theorem 2.2 in [18].
In the next chapter we study the torsion subgroup of the fibers with a rational point, viewed as elliptic curves. At the end of the chapter we can finally state theorem 3.5.2, which gives an explicit description of the torsion subgroup. This is the most important part of our work.
Thanks to the result given in chapter 3, in chapter 4 we state and prove Theorem 4.1.1, which represents our main result, together with a straightforward Corollary. In the proof we apply the same argument used in the proof of Theorem 3.4 in [9] even if our result does not represent a special case of that theorem.
In the fifth and last chapter we introduce another family of projective diagonal quartic surfaces in order to apply our results to this family as well. This chapter is uncomplete and it will represent a stimulus for our further works.

Chapter 1

A family of projective diagonal quartic surfaces

Consider the following family of diagonal quartic surfaces in $\mathbb{P}^3(\overline{\mathbb{Q}})$, named $A148$ in [4, A1, pag. 135]:

$$W_{c_1,c_2}\colon x^4 - 4c_1^2y^4 - c_2z^4 - 4c_2w^4 = 0 \tag{1.1}$$

where $c_1, c_2 \in \mathbb{Q}^\times$. When c_1 and c_2 are clear from the context, we will denote W_{c_1,c_2} by simply W.

1.1 Fibrations defined over $\mathbb{Q}$

The equation defining the surface gives raise to a natural fibration defined over $\mathbb{Q}$: indeed we have that

$$x^4 - 4c_1^2y^4 = c_2(z^4 + 4w^4)$$

and hence

$$(x^2 - 2c_1y^2)(x^2 + 2c_1y^2) = c_2(z^2 + 2zw + 2w^2)(z^2 - 2zw + 2w^2)$$

so that we can consider the following fibrations from W to $\mathbb{P}^1$:

$$\psi_1 \colon (x : y : z : w) \mapsto (x^2 - 2c_1y^2 : z^2 + 2zw + 2w^2) = (c_2(z^2 - 2zw + 2w^2) : x^2 + 2c_1y^2), \tag{1.2}$$

$$\psi_2 \colon (x : y : z : w) \mapsto (x^2 - 2c_1y^2 : z^2 - 2zw + 2w^2) = (c_2(z^2 + 2zw + 2w^2) : x^2 + 2c_1y^2) \tag{1.3}$$

Proposition 1.1.1. *The fibrations defined in* (1.2) *and* (1.3) *are well defined on* W.

Proof. Start considering ψ_1. We can use the same arguments to prove the proposition in the case of ψ_2.
We have to show that the quantities $x^2 - 2c_1y^2, z^2 + 2zw + 2w^2, z^2 - 2zw + 2w^2$ and $x^2 + 2c_1y^2$ are not all zero for any $(x : y : z : w)$ on W. Consider $P = (x_0 : y_0 : z_0 : w_0)$ on W and assume that

$$x_0^2 - 2c_1y_0^2 = 0 = z_0^2 + 2z_0w_0 + 2w_0^2.$$

Recall that since P is an element of the projective space, its coordinates cannot be all zero. Now notice that $x^2 - 2c_1y^2$ and $x^2 + 2c_1y^2$ have no common factors in $\overline{\mathbb{Q}}[x, y]$; the same holds for $z^2 + 2zw + 2w^2$ and $z^2 - 2zw + 2w^2$ in $\overline{\mathbb{Q}}[z, w]$. From

$$z_0^2 + 2z_0w_0 + 2w_0^2 = 0$$

it follows then that either $z_0 = 0 = w_0$ or $z_0^2 - 2z_0w_0 + 2w_0^2 \neq 0$.
If $z_0^2 - 2z_0w_0 + 2w_0^2 \neq 0$ then we are done.
So assume $z_0 = w_0$: then

$$z_0^2 - 2z_0w_0 + 2w_0^2 = 0$$

and at least one of x_0 and y_0 is nonzero. But from $x_0^2 - 2c_1y_0^2 = 0$ we have that then both are nonzero. It follows that $x_0^2 + 2c_1y_0^2$ is nonzero, since $x^2 - 2c_1y^2$ and $x^2 + 2c_1y^2$ have no common factors in $\overline{\mathbb{Q}}[x, y]$. □

Now we will prove a property of these two fibrations that will allow us to translate the results obtained for ψ_1 into results for ψ_2 (and viceversa).

Proposition 1.1.2. *Let* ψ_1 *and* ψ_2 *the fibration from* W *to* $\mathbb{P}^1$ *defined as in in* (1.2) *and* (1.3). *Consider the automorphism of* $\mathbb{P}^3$ *defined by:*

$$\chi \colon (x : y : z : w) \mapsto (x : y : z : -w).$$

The automorphism χ *induces an automorphism of* W*; with an abuse of notation we call* χ *the automorphism of* W. *The automorphism* χ *makes the following diagram*

commute.

$$\begin{array}{ccc} W & \xrightarrow{\chi} & W \\ {\scriptstyle\psi_1}\downarrow & & \downarrow{\scriptstyle\psi_2} \\ \mathbb{P}^1 & = & \mathbb{P}^1 \end{array}$$

Proof. Trivial. □

1.2 Lines on W

Now we will find the equations of the 48 lines lying on W.
Let $W = W_{c_1,-c_2} \subset \mathbb{P}^3$ be the surface of the family $A148$ given by the equation (1.1):

$$x^4 - 4c_1^2y^4 + c_2z^4 + 4c_2w^4 = 0.$$

The surface W contains 48 lines, L_k, given by the following equations:

$$L_{l+4j} = \begin{cases} x &= -\sqrt{2}\gamma_1\zeta_8^{2l}y \\ z &= -\sqrt{2}\zeta_8^{2j+1}w \end{cases},$$

$$L_{16+l+4j} = \begin{cases} x &= -\gamma_2\zeta_8^{2l+1}z \\ y &= -\frac{\gamma_2}{\gamma_1}\zeta_8^{2j}w \end{cases},$$

$$L_{32+l+4j} = \begin{cases} x &= -\sqrt{2}\gamma_2\zeta_8^{2l+1}w \\ y &= -\frac{\gamma_2}{\sqrt{2}\gamma_1}\zeta_8^{2j}w \end{cases},$$

where ζ_8 is a primitive 8-th root of unity, $\sqrt{2} = \zeta_8 - \zeta_8^3$ and $l, j \in \{0, 1, 2, 3\}$; furthermore γ_1 and γ_2 are elements of $\overline{\mathbb{Q}}$ such that $\gamma_1^2 = c_1$ and $\gamma_2^4 = c_2$, and let $i = \zeta_8^2$.

If we define

$$\begin{aligned} \alpha &= x^2 - 2c_1y^2, \\ \beta &= z^2 + 2zw + 2w^2, \\ \overline{\alpha} &= x^2 + 2c_1y^2, \\ \overline{\beta} &= z^2 - 2zw + 2w^2; \end{aligned}$$

then it follows that on W we have $\alpha\overline{\alpha} = -c_2\beta\overline{\beta}$,
and let ψ_j, with $j = 1, 2$, be the fibrations from W to $\mathbb{P}^1$ defined as in (1.2) and (1.3), given by:

$$\psi_1 \colon (x : y : z : w) \mapsto (\alpha : \beta) = (-c_2\overline{\beta} : \overline{\alpha}), \tag{1.4}$$

$$\psi_2 \colon (x : y : z : w) \mapsto (\alpha : \overline{\beta}) = (-c_2\beta : \overline{\alpha}). \tag{1.5}$$

We want to see where the 48 lines are mapped by those fibrations.

1.3 Lines mapped by ψ_1

In this section we study the image of the 48 lines on the surface W via the fibrations ψ_1 and ψ_2.
It is very easy to see that the four lines given by the conditions $\alpha = 0, \beta \neq 0$ or, equivalently, $\alpha = 0, \overline{\beta} = 0$, namely L_4, L_6, L_8, L_{10} are mapped to $(0 : 1)$, and in fact the fiber above $(0 : 1)$ is given by the union of these 4 lines. To show this, it is enough to recall that

$$\alpha = x^2 - 2c_1y^2 = (x - \sqrt{2}\gamma_1 y)(x + \sqrt{2}\gamma_1 y),$$
$$\overline{\beta} = z^2 - 2zw + 2w^2 = (z - \zeta_8\sqrt{2}w)(z + \zeta_8^3\sqrt{2}w),$$

and from $\alpha\overline{\alpha} = -c_2\beta\overline{\beta}$ it follows that $\alpha = 0, \beta \neq 0$ is equivalent to $\alpha = 0, \overline{\beta} = 0$, from which the equations of our lines follow.

With an analogous argument we show that the fiber above the point $(1 : 0)$ is given by the union of the lines L_1, L_3, L_{13}, L_{15}. In this case the conditions are $\alpha \neq 0, \beta = 0$, i.e. $\overline{\alpha} = 0, \beta = 0$.

We can summarize these results in the following Proposition.

Proposition 1.3.1. *The fiber of ψ_1 above $(0 : 1)$ is the union of the lines L_4, L_6, L_8, L_{10}.*
The fiber of ψ_1 above $(1 : 0)$ is the union of the lines L_1, L_3, L_{13}, L_{15}.
Both fibers have type I_4, i.e. the four lines of each fiber form a tetragon: each line of the fiber intersects the next line cyclically (see also [16, p. 365]).

In order to study the case of the other lines it is useful to recall that the surface W defined in (1.1) is a K3 surface (see [4, II.2.2]), and to prove the following Lemma.

Lemma 1.3.2. *Let s and t be two rationals, not both zero. Then the fiber of ψ_1 above $(s : t)$ on W is linearly equivalent to the fiber above $(0 : 1)$.*

Proof. The fiber F of ψ_1 above $(s : t)$ is given by the equations:

$$\begin{cases} t(x^2 - 2c_1y^2) & = s(z^2 + 2zw + 2w^2) \\ c_2t(z^2 - 2zw + 2w^2) & = s(x^2 + 2c_1y^2) \end{cases}.$$

Let F_0 be the fiber of ψ_1 above $(0 : 1)$ and consider then the function

$$f = \frac{t(x^2 - 2c_1y^2) - s(z^2 + 2zw + 2w^2)}{\alpha}.$$

The divisor of f is $F - F_0$ and the statement follows. □

This reult holds more in general for any map from V to $\mathbb{P}^1$.

Let F_0 denote the fiber of ψ_1 above $(0 : 1)$; from Lemma 1.3.2 it follows that, for any fiber F of ψ_1 and any $k \in 0, \dots, 47$, the following identity of intersection numbers holds: $F \cdot L_k = F_0 \cdot L_k$.
On the other hand, it is very easy to compute the 48×48 matrix $A = (a_{j,k})_{0 \le j,k \le 47}$ where $a_{j,k} = L_j \cdot L_k$, since we have to compute the intersection number of lines, and so it can only be either 0 if the two lines does not intersect, or 1 if they intersect; for any j we have that the self-intersection number $L_j \cdot L_j$ equals -2, using [8, Prop.V.1.5, pag. 361] and recalling that by definition the canonical divisor of a K3 surface is $K = 0$. It also turns out that $\operatorname{rank}(A) = 20$.

Proposition 1.3.3. *Let $j \in \{0, \dots, 47\}$ be such that L_j is not in the fiber of ψ_1 above $(0 : 1)$ nor $(1 : 0)$ (see 1.3.1).*
If $j \le 15$ then L_j is surjectively mapped to $\mathbb{P}^1$ via ψ_1 with a 2-to-1 correspondence.
If $j \ge 16$ then L_j is surjectively mapped to $\mathbb{P}^1$ via ψ_1 with a 1-to-1 correspondence.

Proof. Let s be a non zero rational and let F denote the fiber of ψ_1 above $(s : 1)$. To show that any line is surjectively mapped to $\mathbb{P}^1$ it is enough to show that the intersection number $F \cdot L_j$ is greater than zero. But by 1.3.2 we have that $F \cdot L_j = F_0 \cdot L_j$, and by 1.3.1 we know that $F_0 = L_4 + L_6 + L_8 + L_{10}$. So by bilinearity of the intersection pairing we have that

$$F \cdot L_j = L_4 \cdot L_j + L_6 \cdot L_j + L_8 \cdot L_j + L_{10} \cdot L_j = a_{4,j} + a_{6,j} + a_{8,j} + a_{10,j}$$

for any j as in the hypotheses and $s \in \mathbb{Q}^\times$, where the $a_{i,j}{}'s$ are the entries of the intersection number matrix A computed before.
If $j \leq 15$ the sum above turns out to be 2: hence any fiber F has two intersections with L_j, i.e. L_j is surjectively mapped to $\mathbb{P}^1$ via ψ_1 with a 2-to-1 correspondence.
If $j \geq 16$ then the sum above turns out to be 1: hence any fiber F intersects L_j in a point, i.e. L_j is surjectively mapped to $\mathbb{P}^1$ via ψ_1 with a 1-to-1 correspondence. □

1.4 Lines mapped by ψ_2

Thanks to 1.1.2 it is easy to restate the results of the prevoius section for ψ_2. In any proposition we just have to substitute the line L_k with the line $\chi(L_k)$, where χ is defined as in 1.1.2.
In this way we get the following Propositions.

Proposition 1.4.1. *The fiber of ψ_2 above* $(0:1)$ *is the union of the lines L_0, L_2, L_{12}, L_{14}.*
The fiber of ψ_2 above $(1:0)$ *is the union of the lines L_5, L_7, L_9, L_{11}.*

Proposition 1.4.2. *Let L_j with $j \in \{0, \ldots, 47\}$ be a line on W not in the fiber of ψ_2 above* $(0:1)$ *nor* $(1:0)$ *(see 1.4.1).*
If $j \leq 15$ then L_j is surjectively mapped to $\mathbb{P}^1$ via ψ_2 with a 2*-to-*1 *correspondence.*
If $j \geq 16$ then L_j is surjectively mapped to $\mathbb{P}^1$ via ψ_2 with a 1*-to-*1 *correspondence.*

Chapter 2

Elliptic fibers

Let W be a surface defined as in (1.1),

$$W = W_{c_1,c_2} \colon x^4 - 4c_1^2y^4 - c_2z^4 - 4c_2w^4 = 0$$

with its elliptic fibrations ψ_j, $ji = 1, 2$ defined as in (1.2) and (1.3),

$$\psi_1 \colon (x : y : z : w) \mapsto (x^2 - 2c_1y^2 : z^2 + 2zw + 2w^2) = (c_2(z^2 - 2zw + 2w^2) : x^2 + 2c_1y^2),$$
$$\psi_2 \colon (x : y : z : w) \mapsto (x^2 - 2c_1y^2 : z^2 - 2zw + 2w^2) = (c_2(z^2 + 2zw + 2w^2) : x^2 + 2c_1y^2).$$

Let F be a smooth fiber of ψ_1. In this chapter we will see that F has genus 1 and we will find the Weierstrass equation and the j-invariant of the Jacobian of F. If we assume that F is smooth and there is a rational point on it, then the Jacobian of F is isomorphic to F; taking the given rational point as nutral element, F inherits the structure of an elliptic curve.
In order to do this we will follow the procedure presented in [1].
First we will consider the case for $W = W_{\frac{1}{2},1}$ and then the general case for $W = W_{c_1,c_2}$ where c_1, c_2 run in $\mathbb{Q}^\times$.

2.1 $W = W_{\frac{1}{2},1}$

Let $W = W_{\frac{1}{2},1}$ be the surface defined as in (1.1). Namely:

$$W \colon x^4 - y^4 = z^4 + 4w^4,$$

and consider the two fibrations from W to $\mathbb{P}^1$ defined as in (1.2) and (1.3):

$$\psi_1 \colon (x : y : z : w) \mapsto (x^2 - y^2 : z^2 + 2zw + 2w^2) = (z^2 - 2zw + 2w^2, x^2 + y^2),$$
$$\psi_2 \colon (x : y : z : w) \mapsto (x^2 - y^2 : z^2 - 2zw + 2w^2) = (z^2 + 2zw + 2w^2, x^2 + y^2).$$

We start considering the fibers of ψ_1. Let F denote the fiber of ψ_1 above the point $(s : 1)$; then F is given by:

$$\begin{cases} x^2 - y^2 & = s(z^2 + 2zw + 2w^2) \\ z^2 - 2zw + 2w^2 & = s(x^2 + y^2) \end{cases} \iff \begin{cases} x^2 - y^2 - sz^2 - 2szw - 2sw^2 & = 0 \\ sx^2 + sy^2 - z^2 + 2zw - 2w^2 & = 0 \end{cases}.$$

Notice that by the equations above we can deduce that F has genus 1, since they are intersection of two quadrics in $\mathbb{P}^3$. Let U and V denote the quadric forms given by

$$U(x, y, z, w) = x^2 - y^2 - sz^2 - 2szw - 2sw^2, \tag{2.1}$$
$$V(x, y, z, w) = sx^2 + sy^2 - z^2 + 2zw - 2w^2. \tag{2.2}$$

Let A and B be two 4×4 square symmetric matrices such that

$$U(x, y, z, w) = (x, y, z, w) \cdot A \cdot {}^t(x, y, z, w),$$
$$V(x, y, z, w) = (x, y, z, w) \cdot B \cdot {}^t(x, y, z, w).$$

Then we have that

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -s & -s \\ 0 & 0 & -s & -2s \end{pmatrix}, \tag{2.3}$$

$$B = \begin{pmatrix} s & 0 & 0 & 0 \\ 0 & s & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -2 \end{pmatrix}. \tag{2.4}$$

Let $\Delta, \Theta, \Phi, \Theta', \Delta'$ be defined by the following identity:

$$\det(\lambda A + B) = \Delta\lambda^4 + \Theta\lambda^3 + \Phi\lambda^2 + \Theta'\lambda + \Delta'. \tag{2.5}$$

(Doing the easy computations) we find that they are

$$\Delta = -s^2$$
$$\Theta = -6s$$
$$\Phi = s^4 - 1$$
$$\Theta' = 6s^3$$
$$\Delta' = s^2.$$

Then we define the following quantities:

$$\begin{aligned} a_0 &= \Delta \\ a_1 &= -\frac{\Theta}{4} \\ a_2 &= \frac{\Phi}{6} \\ a_3 &= -\frac{\Theta'}{4} \\ a_4 &= \Delta' \\ h &= a_0a_4 - 4a_1a_3 + 3a_2^2 \\ k &= a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3. \end{aligned}$$

By the result in [1, III.3], we have that the Jacobian of F is isomorphic to the elliptic curve E defined by

$$y^2 = x^3 - 4hx - 16k,$$

namely:

$$E\colon y^2 = x^3 - \frac{s^8 + 94s^4 + 1}{3}x + \frac{2s^{12} - 582s^8 + 582s^4 - 2}{27}. \tag{2.6}$$

If we assume that there is a rational point P on F , then F is isomorphic to its Jacobian, hence to E. In this way we can look at (F, P) as an elliptic curve, isomorphic to E. The j-invariant of E is given by:

$$j = \frac{2(s^8 + 94s^4 + 1)^3}{s^4(s^2 - 2s - 1)^2(s^2 + 2s - 1)^2(s^4 + 6s^2 + 1)^2}. \tag{2.7}$$

and whose discriminant d is

$$d = 2048s^4(s^2 - 2s - 1)^2(s^2 + 2s - 1)^2(s^4 + 6s^2 + 1)^2 = 0 \tag{2.8}$$

So in our case, finding the values of s such that the fiber above $(s : 1)$ is singular means finding the roots of

$$s^4(s^2 - 2s - 1)^2(s^2 + 2s - 1)^2(s^4 + 6s^2 + 1)^2 = 0$$

Since we already computed the fibers above $(0 : 1)$ and $(1 : 0)$, we can reduce to consider the following equation:

$$(s^2 - 2s - 1)(s^2 + 2s - 1)(s^4 + 6s^2 + 1) = 0 \tag{2.9}$$

whose roots are $\{\pm 1 \pm \sqrt{2}, i(\pm 1 \pm \sqrt{2})\}$.
So we can conclude that in the case of the fibration ψ_1 we have exactly 10 singular fibers, namely the fibers above $(1:0), (0:1), (s:1)$ where $s \in \{\pm 1 \pm \sqrt{2}, i(\pm 1 \pm \sqrt{2})\}$. The fibers above the latter eight points turn out to have type I_2, as we will see in the next section.

Beacuse of the involution χ in 1.1.2, the same result holds for the fibers of ψ_2

2.2 $W = W_{c_1,c_2}$

Now we will to do the same computations in the general setting: take W defined by:

$$W = W_{c_1,c_2} \colon x^4 - 4c_1^2y^4 - c_2z^4 - 4c_2w^4 = 0$$

with its elliptic fibrations ψ_j, $j = 1, 2$ defined by:

$$\psi_1 \colon (x:y:z:w) \mapsto (x^2 - 2c_1y^2 : z^2 + 2zw + 2w^2) = (c_2(z^2 - 2zw + 2w^2) : x^2 + 2c_1y^2),$$
$$\psi_2 \colon (x:y:z:w) \mapsto (x^2 - 2c_1y^2 : z^2 - 2zw + 2w^2) = (c_2(z^2 + 2zw + 2w^2) : x^2 + 2c_1y^2).$$

And consider the point $(s:1) \in \mathbb{P}^1$ with $s \neq 0$. Then the fiber of ψ_1 above $(s:1)$, say F, is given by:

$$\begin{cases} x^2 - 2c_1y^2 &= s(z^2 + 2zw + 2w^2) \\ c_2(z^2 - 2zw + 2w^2) &= s(x^2 + 2c_1y^2) \end{cases} \iff \begin{cases} x^2 - 2c_1y^2 - sz^2 - 2szw - 2sw^2 &= 0 \\ sx^2 + 2sc_1y^2 - c_2z^2 + 2c_2zw - 2c_2w^2 &= 0 \end{cases}.$$

Notice that the fiber has genus 1, since it is give by the intersection of two quadrics in $\mathbb{P}^3$.
If we denote by U and V the quadric forms given by

$$U(x,y,z,w) = x^2 - 2c_1y^2 - sz^2 - 2szw - 2sw^2, \tag{2.10}$$
$$V(x,y,z,w) = sx^2 + 2sc_1y^2 - c_2z^2 + 2c_2zw - 2c_2w^2. \tag{2.11}$$

then the matrices A, B defined as in the previous section, are given by

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2c_1 & 0 & 0 \\ 0 & 0 & -s & -s \\ 0 & 0 & -s & -2s \end{pmatrix}, \tag{2.12}$$

$$B = \begin{pmatrix} s & 0 & 0 & 0 \\ 0 & 2sc_1 & 0 & 0 \\ 0 & 0 & -c_2 & c_2 \\ 0 & 0 & c_2 & -2c_2 \end{pmatrix}. \tag{2.13}$$

It follows that

$$\begin{aligned}\Delta &= -2s^2c_1\\ \Theta &= -12sc_1c_2\\ \Phi &= 2s^4c_1 - 2c_1c_2^2\\ \Theta' &= 12c_1c_2s^3\\ \Delta' &= 2s^2c_1c_2^2;\end{aligned}$$

and finally

$$\begin{aligned}h &= \frac{s^8c_1^2 + 94s^4c_1^2c_2^2 + c_1^2c_2^4}{3}\\ k &= \frac{s^{12}c_1^3 + 291s^8c_1^3c_2^2 - 291s^4c_1^3c_2^4 + c_1^3c_2^6}{27}.\end{aligned}$$

and so, by the result in [1, III.3], the Jacobian of F is isomorphic to the curve E given by:

$$\begin{aligned}E = E(s,c_1,c_2)\colon y^2 &= x^3 - 4hx - 16k\\ &= x^3 - \frac{4}{3}(s^8c_1^2 + 94s^4c_1^2c_2^2 + c_1^2c_2^4)x + \frac{16}{27}(s^{12}c_1^3 + 291s^8c_1^3c_2^2 - 291s^4c_1^3c_2^4 + c_1^3c_2^6)\\ &= x^3 - \frac{4c_1^2}{3}(s^8 + 94s^4c_2^2 + c_2^4)x + \frac{16c_1^3}{27}(s^{12} + 291s^8c_2^2 - 291s^4c_2^4 + c_2^6)\end{aligned}$$

Moving the rational 2-torsion point $(\frac{4c_1(s^4-c_2^2)}{3}, 0)$ to $(0,0)$ we can write:

$$E\colon y^2 = x^3 + 4c_1(c_2^2 - s^4)x^2 + 4c_1^2(c_2^4 - 34s^4c_2^2 + s^8)x. \tag{2.14}$$

If we assume that on F there is a rational point, then F is isomorphic to its Jacobian, hence to E.

In other words, we have shown the following theorem:

Theorem 2.2.1. *Let W be the surface defined as in* (1.1) *and ψ_1 its fibration defined in* (1.2)*. Let s be a non zero rational and F the fiber of ψ_1 above $(s:1)$ on W.*
Then the Jacobian of F is isomorphic over the rationals to the elliptic curve given by:

$$y^2 = x^3 + 4c_1(c_2^2 - s^4)x^2 + 4c_1^2(c_2^4 - 34s^4c_2^2 + s^8)x.$$

Corollary 2.2.2. *Let W, ψ_1, s and F defined as in 2.2.1, and assume there is a rational point on F.*
Then F is isomorphic over the rationals to the elliptic curve given by:

$$y^2 = x^3 + 4c_1(c_2^2 - s^4)x^2 + 4c_1^2(c_2^4 - 34s^4c_2^2 + s^8)x.$$

From now until the end of the chapter assume that F admits a rational point. Then we may ask when F is a singular curve, and we already know that the fibers above $(0:1)$ and $(1:0)$ are singular curves (namely, union of four lines of type I_4, as we will see). In order to answer this question it is useful to compute the discriminant of E in terms of s.

The j-invariant of E is:

$$j = j(s, c_2) = \frac{2(s^8 + 94s^4c_2^2 + c_2^4)^3}{c_2^2 s^4 (s^4 - 6s^2c_2 + c_2^2)^2 (s^4 + 6s^2c_2 + c_2^2)^2}, \tag{2.15}$$

and the discriminant d is:

$$d = d(s, c_2) = 2^{17} s^4 c_1^6 c_2^4 (s^4 - 6s^2c_2 + c_2^2)^2 (s^4 + 6s^2c_2 + c_2^2)^2. \tag{2.16}$$

Notice that the roots of both the j-invariant and the discrminant of E are indipendent of c_1.
Finding the values of $s = s(c_2)$ for which F is singular means finding the roots of the equation (in the variable s over $\mathbb{Q}(c_2)$)

$$c_2^6 s^4 (s^4 - 6s^2c_2 + c_2^2)^2 (s^4 + 6s^2c_2 + c_2^2)^2 = 0.$$

Recalling that we assumed $s, c_2 \neq 0$ this is equivalent to solving the equation

$$(s^4 - 6s^2c_2 + c_2^2)(s^4 + 6s^2c_2 + c_2^2) = 0.$$

The set of roots of the above equation is: $\{(\pm 1 \pm \sqrt{2})\gamma_2^2, i(\pm 1 \pm \sqrt{2})\gamma_2^2\}$.
So we can conclude that in the case of the fibration ψ_1 we have exactly 10 singular fibers, namely the fibers above $(1:0), (0:1), (s:1)$ with

$$s \in \{(\pm 1 \pm \sqrt{2})\gamma_2^2, i(\pm 1 \pm \sqrt{2})\gamma_2^2\},$$

where γ_2 is such that $\gamma_2^4 = c_2$ (see 1.2).
But not all of these fibers admit rational points.
In fact let $P = (x_0 : y_0 : z_0 : w_0)$ be a rational point of F, then $\psi_1(P)$ will have rational coordinates: hence $\psi_1(P) \neq (s:1)$ with $s \in \{(\pm 1 \pm \sqrt{2})\gamma_2^2, i(\pm 1 \pm \sqrt{2})\gamma_2^2\}$.
Indeed for any s in that set, s is not rational: for example let $s = (1 + \sqrt{2})\gamma_2^2$ and assume it is rational. Then

$$s^2 = (1 + \sqrt{2})^2 \gamma_2^4 = (1 + \sqrt{2})^2 c_2,$$

from which it follows that

$$3 + 2\sqrt{2} = \frac{s^2}{c_2}.$$

The righthand side of the above identity is a rational, while the lefthand side is not, getting a contradiction. With the same argument we show that also the other roots cannot be rationals. We claim that the following Proposition holds.

Proposition 2.2.3. *Let W and ψ_1 defined as before. Assume that $|2c_1|$ is not a square in $\mathbb{Q}$ and let F be a fiber of ψ_1 on W. Assume F has a rational point. Then F is not singular.*
If $2c_1$ is a square in $\mathbb{Q}$ then there are exactly two rational points on the fiber above $(0:1)$ and this is the only singular fiber with rational points.
If $-2c_1$ is a square in $\mathbb{Q}$ then there are exactly two rational points on the fiber above $(1:0)$ and this is the only singular fiber with rational points.

Proof. We have already seen that the only fibers that may be singular are the fibers above $(1:0), (0:1), (s:1)$ with $s \in \{(\pm 1 \pm \sqrt{2})\gamma_2^2, i(\pm 1 \pm \sqrt{2})\gamma_2^2\}$ and that the fibers above $(s:1)$ admit no rational points.
Now assume that $|2c_1|$ is not a square in $\mathbb{Q}$. We need to check that also the fibers above $(1:0)$ and $(0:1)$ have no rational points.
Indeed first assume that $P = (x_0 : y_0 : z_0 : w_0)$ is a rational point of W sent to $(0:1)$ via ψ_1. Then we have that $0 = x_0^2 - 2c_1 y_0^2$, but since $2c_1$ is not a square the equality can hold only if $x_0 = y_0 = 0$. Recalling that P lies on W it follows that

$$c_2(z_0^4 + 4w_0^4) = 0$$

which implies that $z_0 = w_0 = 0$, getting a contradiction.
Now assume that P is sent to $(1:0)$ via ψ_1: then $z_0^2 + 2z_0w_0 + 2w_0^2 = 0$, which implies that $z_0 = w_0 = 0$. But P is on W, then it follows that

$$0 = x_0^4 - 4c_1^2 y_0^4 = (x_0^2 + 2c_1 y_0^2)(x_0^2 - 2c_1 y_0^2),$$

from which we can conclude, since none of $\pm 2c_1$ is a rational square, that $x_0 = y_0 = 0$. Then we get another contradiction. In this way we have proved that if $|2c_1|$ is not a square in $\mathbb{Q}$ then the fibers above $(1:0)$ and $(0:1)$ have no rational points.
Assume now that $2c_1$ is a rational square: then the points $(\pm\sqrt{2c_1} : 1 : 0 : 0)$ are rational points on W sent to $(0:1)$. We can use the same argument as before to show that the fiber above $(1:0)$ has no rational points.
Finally, assume that $-2c_1$ is a rational square: then the points $(\pm\sqrt{-2c_1} : 1 : 0 : 0)$ are rational points on W sent to $(1:0)$. As before we can show that there are no rational points on the fiber above $(0:1)$. □

As in the previous section, taking ψ_2 instead of ψ_1 one gets exactly the same results, thanks to the involution χ defined in the proof of 1.1.2.

It may be interesting investigate the intersection points of the fibers of ψ_1 and ψ_2 above $(0:1)$ and $(1:0)$.

Let F_0 and F_∞ be the fibers of ψ_1 above $(0:1)$ and $(1:0)$ respectively; let G_0 and G_∞ be the analogue for ψ_2. Then the following result holds:

Lemma 2.2.4. *The intersection of the fibers above* $(0:1)$ *and* $(1:0)$ *are the following:*

$$\begin{aligned} F_0 \cap G_0 &= \{(\pm\sqrt{2}\gamma_1 : 1 : 0 : 0)\}, \\ F_0 \cap G_\infty &= \{(0:0:\sqrt{2}\zeta_8 : 1), (0:0:-\sqrt{2}\zeta_8^3 : 1)\}, \\ F_\infty \cap G_0 &= \{(0:0:-\sqrt{2}\zeta_8 : 1), (0:0:\sqrt{2}\zeta_8^3 : 1)\}, \\ F_\infty \cap G_\infty &= \{(\pm\sqrt{2}\gamma_1 i : 1 : 0 : 0)\}, \end{aligned}$$

where i *and* γ_1 *are defined as in section 1.2.*

Proof.

- $F_0 \cap G_0$: recall that F_0 is given by the conditions $\alpha = \overline{\beta} = 0$ while G_0 is given by the conditions $\alpha = \beta = 0$. Then their intersection is given by the conditions $\alpha = \beta = \overline{\beta} = 0$. The conditions $\beta = \overline{\beta} = 0$ imply $z = w = 0$. The condition $\alpha = 0$ gives the desired result.

- $F_0 \cap G_\infty$: recall that G_∞ is given by the conditions $\overline{\alpha} = \overline{\beta} = 0$; then the intersection with F_0 is given by the conditions $\alpha = \overline{\alpha} = \overline{\beta} = 0$. From $\alpha = \overline{\alpha} = 0$ it follows that $x = y = 0$; from $\overline{\beta} = 0$ the desired conclusion does.

- $F_\infty \cap G_0$: as in the case of $F_0 \cap G_\infty$, but with β in the place of $\overline{\beta}$.

- $F_\infty \cap G_\infty$: as in the case of $F_0 \cap G_0$, but with $\overline{\alpha}$ in the place of α.

□

Notice that, using Lemma 2.2.4, we can see that the points in $F_0 \cap G_\infty$ and $F_\infty \cap G_0$ are not rational for any choice of c_1; the points in $F_0 \cap G_0$ are rational if and only if $2c_1$ is a rational square; the points in $F_\infty \cap G_\infty$ are rationals if and only if $-2c_1$ is a rational square.

Although not in this work, it is often very useful to know which type the singular fibers have.

Proposition 2.2.5. *Let* F_0 *and* F_∞ *be the singular fibers of* ψ_1 *above* $(0:1)$ *and* $(1:0)$ *respectively. Then they both have type* I_4.
Let s *be an element of* $\{(\pm 1 \pm \sqrt{2})\gamma_2^2, i(\pm 1 \pm \sqrt{2})\gamma_2^2\}$, *and let* F_s *denote the singular fiber of* ψ_1 *above* $(s:1)$. *Than* F_s *has type* I_2.

Proof. We explicitely computed the fibers F_0 and F_∞, and so it is easy to see that they have type I_4.
To show that the fiber F_s has type I_2 it is enough to recall the table in [16, p. 365] and to notice that the valuation of the j-invariant and the discriminant of F_s at s is -2 and 2 respectively, as one can deduce from (2.15) and (2.16) respectively. Looking at the table, we can conclude that F_s has type I_2. □

Chapter 3

Torsion Points

Let W be a surface defined as in (1.1),

$$W = W_{c_1,c_2} \colon x^4 - 4c_1^2y^4 - c_2z^4 - 4c_2w^4 = 0$$

with its elliptic fibrations $\psi_i, i = 1, 2$ defined as in (1.2) and (1.3),

$$\psi_1 \colon (x : y : z : w) \mapsto (x^2 - 2c_1y^2 : z^2 + 2zw + 2w^2) = (c_2(z^2 - 2zw + 2w^2) : x^2 + 2c_1y^2),$$
$$\psi_2 \colon (x : y : z : w) \mapsto (x^2 - 2c_1y^2 : z^2 - 2zw + 2w^2) = (c_2(z^2 + 2zw + 2w^2) : x^2 + 2c_1y^2).$$

In this chapter we will study the subgroup of the group of rational points formed by the rational torsion points on each but finitely many fibers with at least one rational point on it. We will treat only the fibers of ψ_1, but thanks to Proposition 1.1.2 all the results hold for the fibers of ψ_2 as well.

Our claim is that on each smooth fiber with at least one rational point (used as 0 to make the fiber an elliptic curve), the rational torsion subgroup of the fiber is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We will see that in order to prove this, using Mazur's theorem, it is enough to show that on these fibers there is only one non trivial rational 2-torsion point and no nontrivial rational 3,4 and 5-torsion points.

3.1 2-torsion points

We will start our study considering the fibers of ψ_1, but because of the involution χ the same results hold for ψ_2 as well.

Assume there is a rational point on W, call it $P = (x_0 : y_0 : z_0 : w_0) \in W(\mathbb{Q})$, such that $\psi_1(P) = (s : 1)$ for some nonzero rational s (recall that we already know what are the fibers above $(0 : 1)$ and $(1 : 0)$).
Let F denote the fiber of ψ_1 passing through P; then we have an isomorphism between F and the elliptic curve E given in 2.2.2 sending P to the zero element of E. So we can think about F, P as an elliptic curve having P as zero element. With an abuse of notation, we will write E when we want to consider F, P as an elliptic curve, and we will write simply F when we consider F just as a curve.
Thanks to the result of the previous chapter, we could easily compute the rational 2-torsion points of E using its Weierstrass equation computed in 2.2.2. We prefer to use another argument, to better understand the arithmetic of these surfaces.

Consider the following isomorphisms of W defined by:

$$\sigma\colon (x : y : z : w) \mapsto (-x : y : z : w), \tag{3.1}$$
$$\tau\colon (x : y : z : w) \mapsto (x : -y : z : w). \tag{3.2}$$

They both respect the fibration, i.e. the following diagrams commute for $j = 1, 2$.

$$\begin{array}{ccc} W & \xrightarrow{\sigma} & W \\ {\scriptstyle\psi_j}\downarrow & & \downarrow{\scriptstyle\psi_j} \\ \mathbb{P}^1 & = & \mathbb{P}^1 \end{array} \qquad \begin{array}{ccc} W & \xrightarrow{\tau} & W \\ {\scriptstyle\psi_j}\downarrow & & \downarrow{\scriptstyle\psi_j} \\ \mathbb{P}^1 & = & \mathbb{P}^1 \end{array}$$

By the definition of σ and τ it is easy to see that $\sigma(P), \tau(P), \sigma \circ \tau(P) \in F(\mathbb{Q})$. Notice that σ is an automorphism of F, but not of E, since it does not fix the point P. Recall the following results:

Lemma 3.1.1. *Let F be defined as before, P a rational point on F and let E denote (F, P) viewed as elliptic curve over $\mathbb{Q}$.*
Consider the following short sequence

$$0 \longrightarrow E(\mathbb{Q}) \xrightarrow{T} \mathrm{Aut}_{\mathbb{Q}}(F) \xrightarrow{\Upsilon} \mathrm{Aut}_{\mathbb{Q}}(E) \longrightarrow 0.$$

where T is the map sending a point Q of $E(\mathbb{Q})$ to the translation (using the group structure on E) by Q; the map Υ sends an automorphism of F, say ω, to the automorphism of E given by $T_{-\omega(P)} \circ \omega$.
The sequence is exact. In fact it splits.

Proof. The injectivity of the map T is trivial, as well as the surjectivity of the map Υ. So we just need to show that $ImT = \ker\Upsilon$.

Let $\omega \in \mathrm{Im}T$, then ω is a translation, say $\omega = T_Q$. Then

$$\begin{aligned}\Upsilon(\omega) &= T_{-\omega(P)} \circ \omega \\ &= T_{-Q} \circ T_Q \\ &= \mathrm{id}_E\end{aligned}$$

Now assume that $\omega \in ker\Upsilon$. It implies that $T_{-\omega(P)} \circ \omega = id_E$ and hence

$$\omega = (T_{-\omega(P)})^{-1} = T_{\omega(P)}.$$

Hence ω is the translation by the point $\omega(P)$.
To show that the sequence splits just notice that $\mathrm{Aut}_{\mathbb{Q}}(E)$ is contained in $\mathrm{Aut}_{\mathbb{Q}}(F)$.
With this the proof is completed. □

Proposition 3.1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$, then*

$$\mathrm{Aut}_{\mathbb{Q}}(E) \simeq \begin{cases} \{\pm 1\} & \text{if } j(E) \neq 0, 1728 \\ \{\pm 1, \pm i\} & \text{if } j(E) = 1728 \\ \langle \zeta_6 \rangle & \text{if } j(E) = 0 \end{cases}$$

where $j(E)$ denotes the j-invariant of E and ζ_6 is a primitive 6-th root of unity.

Proof. See [14], pag. 104, Corollary III.10.2. □

We are interested in the image of σ and τ in $\mathrm{Aut}_{\mathbb{Q}}(E)$.

Lemma 3.1.3. *Let $E = (F, P)$ be smoth a fiber of W with at least a rational point viewed as elliptic curve over $\mathbb{Q}$, and let σ and τ be the elements of $\mathrm{Aut}_{\mathbb{Q}}(F)$ defined as in* (3.1) *and* (3.2).
Then there are rational points R_σ and R_τ on F such that, for any point Q on F we have:

$$\begin{aligned}\sigma(Q) &= R_\sigma - Q, \\ \tau(Q) &= R_\tau - Q.\end{aligned}$$

In particular $R_\sigma = \sigma(P)$ and $R_\tau = \tau(P)$.

Proof. We start considering σ.
First notice that since σ is an involution, it has order 2, and so, by 3.1.2, its image under Υ can only be either 1 or -1. So we have only these two cases:

- σ is mapped to 1: then σ is a translation by a point, and since σ is an involution, it is a translation by a 2-torsion point; in this case σ does not admit fixed points. Recall that σ cannot be the identity, since it does not fix P.

- σ is mapped to -1: then by Lemma 3.1.1 we have that there is an $R_\sigma \in E(\mathbb{Q})$ such that for any $Q \in E, \sigma(Q) = R_\sigma - Q$.
  Let R' be a point on $E(\overline{\mathbb{Q}})$ such that $2R' = R_\sigma$, then we get that $\sigma(R') = R'$, hence the fixed points for σ are given by $R' + E[2]$, i.e. the points of the form $R' + T$ where T is a 2-torsion point of E.

But now notice that σ admits fixed points if and only if $F \cap \{x = 0\} \neq \emptyset$, indeed

$$\sigma(x : y : z : w) = (x : y : z : w) \iff (-x : y : z : w) = (x : y : z : w) \iff x = 0$$

But actually $F \cap \{x = 0\} \neq \emptyset$ (for example consider the point $(0 : \frac{\xi}{\sqrt{2}\gamma_1} : z_0 : w_0)$, where $\xi \in \overline{\mathbb{Q}}$ is a square root of $-s$), and so we have that σ is mapped to -1. Using the same argument but considering $F \cap \{y = 0\}$ we can show that also τ is mapped to -1.
Hence we can conclude that there are $R_\sigma, R_\tau, \in E_\mathbb{Q}$ such that for any $Q \in E$ we have that $\sigma(Q) = R_\sigma - Q$ and $\tau(Q) = R_\tau - Q$. Notice that $R_\sigma = \sigma(P)$ and $R_\tau = \tau(P)$. □

Now consider $\sigma\tau = \sigma \circ \tau$:

$$\sigma\tau(Q) = \sigma(R_\tau - Q) = (R_\sigma - R_\tau) + Q;$$

hence $\sigma\tau$ is a translation, but it is also an involution: indeed

$$\sigma\tau(x : y : z : w) = (-x : -y : z : w).$$

Then it is a translation by a 2-torsion point, so we can conclude that

$$T_0 := R_\sigma - R_\tau = \sigma\tau(P) = (-x_0 : -y_0 : z : w) \in E(\mathbb{Q})[2]. \tag{3.3}$$

In order to find the other two 2-torsion points take the following two maps from W to W, which also respect the fibration ψ_1:

$$\rho_1 \colon (x : y : z : w) \mapsto (\sqrt{2}x : \sqrt{2}y : 2w : z)$$
$$\rho_2 \colon (x : y : z : w) \mapsto (-\sqrt{2}x : -\sqrt{2}y : 2w : z).$$

They are both involutions but they also have fixed points, namely the points such that $z = \sqrt{2}w$ for ρ_1 and the points such that $z = -\sqrt{2}w$ for ρ_2. So, as before, there are $R_1, R_2 \in E$ such that:

$$\rho_1(Q) = R_1 - Q, \text{ where } R_1 = \rho_1(Q), \tag{3.4}$$
$$\rho_2(Q) = R_2 - Q, \text{ where } R_2 = \rho_1(Q). \tag{3.5}$$

Notice that R_1 and R_2 are nonrational since ρ_1 and ρ_2 map P to a non rational point: indeed $\rho_1(P) = (\sqrt{2}x_0 : \sqrt{2}y_0 : 2w_0 : z_0)$ is rational if and only if $x_0 = y_0 = 0$, but in this case P would be sent either to $(0 : 1)$ or $(1 : 0)$, while we assumed that F were a fiber above $(s : 1)$ with s nonzero rational; the same argument works for ρ_2 as well.
Moreover, looking at their definitions, we see that $\rho_1\rho_2 = \sigma\tau$, from which it follows that $R_1 - R_2 = T_0$. But consider $\rho_1\sigma$:

$$\rho_1\sigma(Q) = \rho_1(R_\sigma - Q) = (R_1 - R_\sigma) + Q; \tag{3.6}$$

so $\rho_1\sigma$ is an involution (since composition of two commuting involutions) and a translation, then it is a translation by a 2-torsion point. We can hence conclude that:

$$T_1 := (R_1 - R_\sigma) = \rho_1\sigma(P) = (-\sqrt{2}x_0 : \sqrt{2}y_0 : 2w_0 : z_0) \in E[2]. \tag{3.7}$$

The last torsion point is then $T_2 := T_1 + T_0$.
To compute it explicitely we can use the same argument used to compute T_1, but considering $\rho_2\sigma(= \rho_1\tau)$. Then we have that:

$$T_2 = \rho_2\sigma(P) = (\sqrt{2}x_0 : -\sqrt{2}y_0 : 2w_0 : z_0)\,(= \rho_1\tau(P)). \tag{3.8}$$

To check that in fact $T_0 + T_1 + T_2 = P$, recalling the definition of these points, it is enough to check that

$$(\rho_2\sigma)(\rho_1\sigma)(\sigma\tau) = id_F,$$

but this is straightforward using the definitions of $\sigma, \tau, \rho_1, \rho_2$.

So we have found that

$$E[2] = \{P, T_0, T_1, T_2\}.$$

Recalling that P is rational, (3.3) shows that $T_0 \in E(\mathbb{Q})[2]$; instead (3.7) and (3.8) show that T_1 and T_2 are not rational. Hence we have proved the following Theorem.

Theorem 3.1.4. *Let $E = (F, P)$ be a smooth fiber of ψ_1 on W with a rational point P, viewed as elliptic curve. Then*

$$E(\mathbb{Q})[2] = \{P, T_0\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

where $\sigma\tau(P) = T_0 = R_\sigma - R_\tau$, with R_σ, R_τ defined as in 3.1.3.

Proof. We already proved that $E(\mathbb{Q})[2] = \{P, T_0\}$. Then to show that $\{P, T_0\} \simeq \mathbb{Z}/2\mathbb{Z}$ it is enough to show that $P \neq T_0$. Let $P \in W$ be the point with coordinates $(x_0 : y_0 : z_0 : w_0)$, then we have seen that $T_0 = (-x_0 : -y_0 : z_0 : w_0)$. It follows that $P = T_0$ if and only if either $x_0 = y_0 = 0$ or $z_0 = w_0 = 0$. But for each of these two cases it follows that then P lies on a singular fiber, while we assumed that P was on a smooth fiber. □

3.2 4-torsion points

Let $s \in \mathbb{Q}^\times$, and let F denote the fiber on W of ψ_1 above $(s : 1)$. Assume that on F there is a rational point. Then by Corollary 2.2.2 we have that F is isomorphic to the elliptic curve E given by

$$E\colon y^2 = x^3 + 4c_1(c_2^2 - s^4)x^2 + 4c_1^2(c_2^4 - 34s^4c_2^2 + s^8)x =: g(x).$$

So looking for the 4-torsion points on F is equivalent to looking for the 4-torsion points on E. Notice that $g(x) = xg_1(x)$, where

$$g_1(x) = x^2 + 4c_1(c_2^2 - s^4)x + 4c_1^2(c_2^4 - 34s^4c_2^2 + s^8).$$

Let $f_4(x)$ be the 4-division polynomial of E:

$$f_4(x) = 8xh_1(x)h_2(x)h_3(x), \tag{3.9}$$

where

$$\begin{aligned}
h_1(x) &= g_1(x),\\
h_2(x) &= x^2 - 4c_1^2(s^8 - 34s^4c_2^2 + c_2^4),\\
h_3(x) &= x^4 + 8c_1(c_2^2 - s^4)x^3 + 24c_1^2(s^8 - 34s^4c_2^2 + c_2^4)x^2 +\\
&\quad + 32c_1^3(-s^{12} + 35s^8c_2^2 - 35s^4c_2^4 + 32c_2^6)x +\\
&\quad + 16c_1^4(s^{16} - 68s^{12}c_2^2 + 1158s^8c_2^4 - 68s^4c_2^6 - c_2^8).
\end{aligned}$$

The roots of $h_1(x) = g_1(x)$ are the first coordinate of the two non rational 2-torsion points (since the two rational ones are give by the point at infinity and $(0,0)$).
We claim that the roots of h_3 are the first coordinates of those 4-torsion points mapped to T_1 and T_2 under multiplication by 2 and the roots of h_2 are the first coordinates of the 4-torsion points mapped to $(0,0)$ under multiplication by 2: to see this notice that h_3 splits over $\mathbb{Q}(\sqrt{2})$, and so its roots are conjugated under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. Instead the polynomial h_2 splits over $\mathbb{Q}(\gamma_s)$, where γ_s is such that $\gamma_s^2 = 4c_1^2(s^8 - 34s^4c_2^2 + c_2^4)$. Notice that $\sqrt{2}$ is not an element of $\mathbb{Q}(\gamma_s)$. This implies that, if we consider the extension field $\mathbb{Q}(\sqrt{2}, \gamma_S)$, the roots of h_2 are fixed by the map $\sqrt{2} \mapsto -\sqrt{2}$. Recalling that T_1 and T_2 are conjugated under the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, our claim follows. But then the 4-torsion points mapped to T_1 and T_2 under multiplication by 2 cannot be rational, since T_1 and T_2 are not.
We still need to check the four 4-torsion points given by h_2: in order to prove that they are not rational it is enough to prove that their first coordinate is not rational, i.e. $h_2(x)$ admits no rational roots for any $s, c_2 \in \mathbb{Q}^\times$.

Lemma 3.2.1. *Let s, c_2 be nonzero rationals, then the equation*

$$h_2(x) = 0$$

has no rational roots.

Proof. Asking whenever the equation $h_2(x) = 0$ has a rational solution is equivalent to asking whenever $4c_1^2(s^8 - 34s^4c_2^2 + c_2^4)$ is a rational square, but notice that it is a rational square if and only if $\frac{s^4}{c_2^2} - 34 + (\frac{s^4}{c_2^2})^{-1}$ is a rational square.
In other words, we are looking for rational points on the surface $D \subset \mathbb{A}^3(z, s, c_2) \cap \{sc_2 \neq 0\} =: \mathcal{U}$ given by:

$$D\colon z^2 - \frac{s^4}{c_2^2} - 34 + \left(\frac{s^4}{c_2^2}\right)^{-1} = 0.$$

Let θ denote the map from $\mathcal{U}$ to $\mathbb{A}^2(p, q)$ defined by:

$$\theta\colon (z, s, c_2) \mapsto \left(z\frac{s^2}{c_2}, \frac{s^2}{c_2}\right). \tag{3.10}$$

The map θ maps D to the curve $C \subset \mathbb{A}^2(p, q)$ defined by:

$$C\colon p^2 = q^4 - 34q^2 + 1, \tag{3.11}$$

whose projective closure is given by:

$$\overline{C}\colon X^2Z^2 = Y^4 - 34Y^2Z^2 + Z^4, \tag{3.12}$$

where $p = \frac{X}{Z}$ and $q = \frac{Y}{Z} \subset \mathbb{P}^2(X, Y, Z)$.
Hence we can look at θ as the map from D to $\overline{C}$ defined by:

$$(z, s, c_2) \mapsto (zs^2 : s^2 : c_2) \tag{3.13}$$

The map θ sends rational points to rational points, so to show that there are no rational points on D it is enough to show that there are no rational points on $\overline{C}$ coming from D via θ for any admissible choice of s and c_2.
Again using the procedure shown in [1] it turns out that the Jacobian of $\overline{C}$ is isomorphic to the elliptic curve H given by:

$$H\colon y^2 = x^3 - x^2 - 24x - 36.$$

On $\overline{C}$ there are rational points, namely $(1 : 0 : 1), (1 : 0 : -1)$ and $(1 : 0 : 0)$, but since it is singular (in $(1 : 0 : 0)$) what we can say is that H is isomorphic to the desingularization of $\overline{C}$. Blowing up $\overline{C}$ at $(1 : 0 : 0)$ we can see that $(1 : 0 : 0)$ corresponds to two distinct rational points on the desingularization of $\overline{C}$. Hence we have at least four rational points on the desingularization of $\overline{C}$.
It is easy to compute the rank of H, which turns out to be 0, and so we have that $H_{\mathbb{Q}} = H^{Tor}(\mathbb{Q})$. But one can see that $\#H^{Tor}(\mathbb{Q}) = 4$.
It follows that on the desingularization of $\overline{C}$ there exactly four points, two corresponding to $(1 : 0 : 1)$ and $(1 : 0 : -1)$ and two corresponding to $(1 : 0 : 0)$ on $\overline{C}$. Looking at (3.13) we can see that none of these points comes from any point of D via θ. This means that we have no rational points on D, hence we have no rational roots of h_2. □

From the Lemma 3.2.1 we can deduce that the four 4-torsion points coming from h_2 have nonrational first coordinate, from which it follows that they are nonrational. With this we have shown the following:

Theorem 3.2.2. *Let $E = (F, P)$ be a smooth fiber of ψ_1 on W with a rational point P, viewed as elliptic curve. Then there are no nontrivial rational 4-torsion points on E, i.e.*

$$E(\mathbb{Q})[4] = E(\mathbb{Q})[2].$$

Recall that $E(\mathbb{Q})[2]$ is explicitely given in 3.1.4.

3.3 5-torsion points

In this section we will show that any smooth fiber of ψ_1 on W with at least one rational point, viewed as elliptic curve, admits no nontrivial rational 5-torsion

points.

In our strategy to show this, the j-invariant of the fiber plays a crucial role. Let s be a non-zero rational, then from (2.15) we know that the j-invariant of the fiber F of ψ_1 above $(s : 1)$ is given by:

$$j = j(s, c_2) = \frac{2(s^8 + 94s^4c_2^2 + c_2^4)^3}{c_2^2 s^4 (s^4 - 6s^2c_2 + c_2^2)^2 (s^4 + 6s^2c_2 + c_2^2)^2}. \tag{3.14}$$

Now assume that on F, viewed as an elliptic curve, there is a rational nontrivial 5-torsion point, P. Then we can consider the following Lemma.

Lemma 3.3.1. *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$, and $P \in E(\mathbb{Q})$ a 5-torsion point. Then there is a number $b \in \mathbb{Q}$ and an isomorphism $\varphi\colon E \to E'$, where E' is the curve defined by*

$$E'\colon y^2 + (b+1)xy + by = x^3 + bx^2, \tag{3.15}$$

such that $\varphi(P) = (0, 0)$.

Proof. See [6], proposition 8.2.8. □

In fact this Lemma shows that $X_1(5) \cong \mathbb{P}^1(b)$. From the Lemma 3.3.1 it follows that the j-invariant of the elliptic fiber F is given by

$$j = -\frac{b^2 + 12b + 14 - 12b^{-1} + b^{-2}}{b + 11 + b^{-1}} \tag{3.16}$$

for some $b \in \mathbb{Q}^\times$. It follows that there is a $b \in \mathbb{Q}^\times$ such that

$$\begin{aligned} g(b) := -\frac{b^2 + 12b + 14 - 12b^{-1} + b^{-2}}{b + 11 + b^{-1}} &= \frac{2(s^8 + 94s^4c_2^2 + c_2^4)^3}{c_2^2 s^4 (s^4 - 6s^2c_2 + c_2^2)^2 (s^4 + 6s^2c_2 + c_2^2)^2} \\ &= \frac{2(c_2^{-2}s^4 + 94 + c_2^2 s^{-4})^3}{(c_2^{-2}s^4 - 34 + c_2^2 s^{-4})^2} =: f(s). \end{aligned}$$

This means that we have a rational point on the affine curve $C' \subset \mathbb{A}^2(s, b) \cap \{sb \neq 0\} =: \mathcal{U}$ defined by

$$C'\colon g(b) = f(s). \tag{3.17}$$

We are interested then in understanding the set of rational points of C'. We claim that the curve C' has no rational points. In order to prove this, consider the following map from C' to $C \subset \mathbb{A}^2(u, c)$:

$$\nu\colon (s, b) \mapsto ((c_2^{-1}s^2 - c_2 s^{-2})^2, b - b^{-1}). \tag{3.18}$$

where C is given by

$$C\colon 2(u+96)^3(c+11) = -(c^2+12c+16)^3(u-32)^2. \tag{3.19}$$

Now we have to give two remarks: the first is that the map ν sends rational points to rational points, hence if we have that there are no rational points on C it follows that there are no rational points on C'; the second remark is that, by (3.18), the first coordinate of the image of the rational points of C' on C via ν must be a rational square, namely

$$u = (c_2^{-1}s^2 - c_2 s^{-2})^2 =: v^2.$$

Lemma 3.3.2. *Let $\overline{C} \subset \mathbb{P}^2(X,Y,Z)$ be the projective closure of the curve C defined in* (3.19)*, where $u = X/Z$ and $c = Y/Z$, then there exist a birational morphism*

$$\varphi\colon \mathbb{P}^1 \to \overline{C}, (p:q) \mapsto (X(p,q) : Y(p,q) : Z(p,q))$$

with

$$\begin{aligned}
X(p,q) =& 2^5(p-7168q)^2(p^2-10240pq+20971520q^2)^2(p^2-\frac{73728}{5}pq+54525952q^2),\\
Y(p,q) =& -11(p-8192q)^4(p-\frac{36864}{5}q)\\
&(p^3-22528p^2q+\frac{1862270976}{11}pq^2-\frac{4668629450752}{11}q^3),\\
Z(p,q) =& (p-8192q)^5(p-7168q)^2(p-\frac{36864}{5}q);
\end{aligned}$$

Its inverse $(X:Y:Z) \mapsto (p(X,Y,Z) : q(X,Y,Z))$ is given by:

$$\begin{aligned}
p(X,Y,Z) =& (XY^9+60XY^8Z-32Y^9Z+1520XY^7Z^2-1920Y^8Z^2+21104XY^6Z^3-34304Y^7Z^3+\\
&+2X^2Y^4Z^4+174528XY^5Z^4+88576Y^6Z^4+70X^2Y^3Z^5+877696XY^4Z^5+\\
&+11028480Y^5Z^5+880X^2Y^2Z^6+2659200XY^3Z^6+160147456Y^4Z^6+4608X^2YZ^7+\\
&+4824064XY^2Z^7+1086945280Y^3Z^7+8096X^2Z^8+5496832XYZ^8+3710566400Y^2Z^8+\\
&+3602432XZ^9+5761662976YZ^9+3261759488Z^{10})/2,\\
q(X,Y,Z) =& Z^3(Y+11Z)(Y^2+12YZ+16Z^2)^2(Y^2+18YZ+76Z^2).
\end{aligned}$$

Proof. The map is obtained using MAGMA, but one can check that the compositions of the two maps are the identity maps. □

This parametrization helps us in finding rational points on $\overline{C}$ coming from C'. In fact, using the parametrization, we have that

$$u = \frac{X(p,q)}{Z(p,q)},$$

but $u = v^2$; hence the existence of a rational point on $\overline{C}$ coming from C' would imply the existence of rational p, q, v such that

$$v^2 = \frac{2^5(p - 7168q)^2(p^2 - 10240pq + 20971520q^2)^2(p^2 - \frac{73728}{5}pq + 54525952q^2)}{(p - 8192q)^5(p - 7168q)^2(p - \frac{36864}{5}q)}$$

that is equivalent to the existence of rational p, q, r such that

$$q^2r^2 = 2(p^2 - \frac{73728}{5}pq + 54525952q^2)(p - 8192q)(p - \frac{36864}{5}q). \qquad (3.20)$$

Let $M \subset \mathbb{P}^2(q, r, p)$ be the curve defined by (3.20). Notice that $(1 : 0 : 8192)$ and $(5 : 0 : 36864)$ are rational points on M. Are there more rational points on M? Again using the results presented in [1] we can see that M is isomorphic (since there are rational points on it) to the elliptic curve

$$G\colon y^2z = x^3 - 4x^2z + 20xz^2,$$

which has rank 0 and torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. This means that $G(\mathbb{Q}) = G^{Tor}(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0)\}$. Hence we have only two rational points also on M, namely $(1 : 0 : 8192)$ and $(5 : 0 : 36864)$. These two points correspond to the points $(8192 : 1), (36864 : 5) \in \mathbb{P}^1(p : q)$. So in correspondence of these two points, via φ, we should have two rational points on $\overline{C}$ coming from C'. Both points are mapped to $(1 : 0 : 0) \in \overline{C}$. This means that the only rational points on C coming from C' have $u = \infty$. But this is impossible since

$$u = (c_2^{-1}s^2 - c_2s^{-2})^2,$$

with $c_2, s \in \mathbb{Q}^\times$. So there are no rational points on C coming from C', hence there are no rational points on C'. In other words we have proven the following Proposition.

Proposition 3.3.3. *Let C' be the curve defined in* (3.17)*. C' has no rational points.*

But this is a contradiction to the assumption of the existence of a rational 5-torsion point on the fiber F (viewed as an elliptic curve), then the assumption must be false. This is the proof of the following Theorem.

Theorem 3.3.4. *Let $s \in \mathbb{Q}^\times$ and F be the fiber of ψ_1 over $(s : 1)$, and assume there is at least one rational point on F. Then F viewed as elliptic curve has no nontrivial rational 5-torsion points.*

3.4 3-torsion points

After having proven that there are no non trivial rational 4- and 5-torsion points on the smooth fibers of ψ_1 on W with at least one rational point, we show that there are not even nontrivial rational 3-torsion points.

Lemma 3.4.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ and P a rational 3-torsion point; assume E has nonzero j-invariant. Then there exist an element $b \in \mathbb{Q}^\times$ such that the pair (E, P) is isomorphic to the pair $(E_b, (0,0))$, where E_b is the elliptic curve defined by*

$$y^2 + xy + \frac{b}{27}y = x^3.$$

Proof. First reduce E to the Weierstrass form. Then E can be expressed as

$$E\colon y^2 + a'xy + b'y = x^3 + c'x^2 + d'x + e'.$$

By means of the translation given sending P to $(0,0)$ we have that E is isomorphic to the curve given by

$$E''\colon y^2 + a''xy + b''y = x^3 + c''x^2 + d''x.$$

Now notice that $b'' \neq 0$ otherwise the tangent to E' at $(0,0)$ would be $x = 0$ implying that $(0,0)$ has order 2, while from the hypotheses it follows that $(0,0)$ is of order 3. So we can consider the following automorphism of $\mathbb{A}^2(a_1, a_2)$

$$(a_1, a_2) \mapsto (a_1, b''a_2 - d''a_1),$$

which sends E'' to E' defined by

$$E'\colon y^2 + axy + b'''y = x^3 + cx^2.$$

Since E is an elliptic curve, it is non singular; hence E' is non singular. It follows that $b''' \neq 0$, otherwise $(0,0)$ would be a singular point for E'.
Now consider the 3-division polynomial of E', say φ_3:

$$\varphi_3 = 3x^4 + (a^2 + 4c)x^3 + 3ab'''x^2 + 3b'''^2x + b'''^2c.$$

By hypotheses we have that P is 3-torsion. This implies that $(0,0)$ is 3-torsion on E', hence 0 is a zero of φ_3. From this follows that $b'''^2c = 0$, but since $b''' \neq 0$ we can deduce that $c = 0$.
Then we can write E' as

$$y^2 + axy + b'''y = x^3.$$

Now suppose that $a = 0$, then the $j-$invariant of E' turns out to be 0, which contradicts the hypotheses. So we may assume that $a \neq 0$. Applying the automorphism of $\mathbb{A}^2(x, y)$ sending y to a^3y and x to a^2x we can write E' as

$$y^2 + xy + \frac{b'''}{a^3}y = x^3.$$

For $b = 27\frac{b'''}{a^3}$ we get the desired expression. □

Let s be a nonzero rational, and F the fiber of ψ_1 over $(s : 1)$ on W. Assume that on F viewed as an elliptic curve there is a rational 3-torsion points. Then by 3.4.1 we have that the j-invariant of F is given by:

$$g(b) := 2^9 3^3 \frac{(b - 9/8)^3}{b^4 - b^3} \tag{3.21}$$

for some $b \in \mathbb{Q}^\times$.
But from (2.15) we know that the j-invariant of F is also give by:

$$\frac{2(c_2^{-2}s^4 + 94 + c_2^2 s^{-4})^3}{(c_2^{-2}s^4 - 34 + c_2^2 s^{-4})^2} =: f(s) \tag{3.22}$$

Then assuming the existence of a rational 3-torsion point on F is equivalent to assuming the existence of a rational point on the curve $C' \subset \mathbb{A}^2(b, s) \cap \{bs \neq 0\} =: \mathcal{U}$:

$$C' : g(b) = f(s) \iff 2^8 3^3 (b-9/8)^3 (c_2^{-2}s^4 - 34 + c_2^2 s^{-4})^2 = (c_2^{-2}s^4 + 94 + c_2^2 s^{-4})^3 (b^4 - b^3) \tag{3.23}$$

Consider the map ϵ from $\mathbb{A}^2(b, s)$ to $\mathbb{A}^2(p, q)$ defined by:

$$\epsilon : (b, s) \mapsto (b, c_2^{-1}s^2 + c_2 s^{-2}). \tag{3.24}$$

Notice that ϵ sends rational points to rational points. The curve C' is mapped to the curve $C \subset \mathbb{A}^2(p, q)$ defined by:

$$C : 2^8 3^3 (p - 9/8)^3 (q^2 - 36)^2 = (q^2 + 92)^3 (p^4 - p^3) \tag{3.25}$$

For this curve we have the following result:

Lemma 3.4.2. *Let $C \subset \mathbb{A}^2(p, q)$ be the curve defined in* (3.25)*. Then there are no rational points on C coming from C' via ϵ.*

Proof. To show this Lemma we use the software MAGMA. The following is not really exactly a proof since the author does not yet know the theory and the algorithm beyond the MAGMA functions. Nevertheless we will try to give a basic idea.
Consider the curve C given in (3.25). It is easy to see that $(0, \pm 6), (1, \pm 6)$ are rational points on C, and in particular that the points $(0, \pm 6)$ are also singular. We will show that these are the only rational points on the curve.
Using MAGMA the curve turns out to be isomorphic over the rational to the hyperelliptic curve H defined by:

$$H\colon y^2 = 4x^5 - 14x^4 - 8x^3 + 36x^2 + 36x + 9 \tag{3.26}$$

Also in this case it is easy to see that $(1 : 0 : 0), (0 : \pm 3 : 1), (-1 : 0 : 2), (4 : \pm 27 : 1)$ are rational points on H. Let $\tilde{H}$ be the desingularization of H. Then we have at least six rational points on $\tilde{H}$. Let $J = J(\tilde{H})$ denote the Jacobian of $\tilde{H}$. Since we have rational points on $\tilde{H}$, let R be one of them, we have that $\tilde{H}$ can be embedded in $J(\tilde{H})$ via the canonical map $\iota\colon Q \mapsto (P) - (R)$. By Mordell-Weil theorem we know that $J(\tilde{H})$ is isomorphic to $\mathbb{Z}^r \oplus J^{Tor}$, where r is a nonnegative integer and J^{Tor} is the torsion subgroup of J. Using MAGMA we can compute J^{Tor} and r, getting that $J^{Tor} \simeq \mathbb{Z}/4\mathbb{Z}$ and $r = 1$. Then let $\overline{D}$ be a generator of J/J^{Tor}; it follows that $J = \langle D \rangle \oplus J^{Tor}$.
Now we introduce the concepts of *naive height* and *Neron-Tate height* of a point in J. Notice that we are working with elements of the Jacobian of a curve, and so it is not clear what are the coordinates of these points. As coordinates we use the standard model of the associated singular Kummer surface (see [5]). This surface can be embedded in $\mathbb{P}^3$, and so we define the height for elements of $\mathbb{P}^3$.
Let $Q = (x_0 : y_0 : z_0 : w_0)$ be a rational point of $\mathbb{P}^3$. Without loss of generality we can assume all the coordinates to be integers. Then we define the *height* of Q, denoted by $H(Q)$ as

$$H(Q) = max\{|x_0|, |y_0|, |z_0|, |w_0|\}. \tag{3.27}$$

Using the definition of the height we can now define the *naive height* of Q, to be:

$$h(Q) = \log H(Q). \tag{3.28}$$

We can now define the *Neron-Tate height* to be:

$$\hat{h}(Q) = \lim_{n\to\infty} \frac{h(2^n Q)}{4^n}. \tag{3.29}$$

It is a fact that the Neron-Tate height is well defined and that it is a quadratic form on the Mordell-Weil group of rational points of an abelian variety (J in our case). It is also true that $|h - \hat{h}|$ is bounded, and using MAGMA we can even compute

a bound for it in our case, call it b_2, getting $b_2 \approx 2.47$. For more details about Neron-Tate height see [21]; it may be also useful to read [15, III.1,2] .
Let $\mathcal{B}$ be the set of rational points Q of J such that $H(Q) \leq 250$:

$$\mathcal{B} = \{Q \in J(\mathbb{Q}) \colon H(Q) \leq 250\},$$

and let B the subgroup of J generated by $\mathcal{B}$. We can use MAGMA to compute $B^{Tor} \simeq \mathbb{Z}/4\mathbb{Z}$, and also a basis for B/B^{Tor}, that turns out to be generated by a single element, say $\overline{P}$. Then it follows that

$$B = \langle P \rangle \oplus B^{Tor}.$$

Using MAGMA we can also compute the height of P, getting $H(P) \approx 0.17$. Suppose now that $\langle \overline{P} \rangle$ is strictly contained in $J/J^{Tor} = \langle \overline{D} \rangle$. Then there is an $m \in \mathbb{Z}_{\geq 2}$ such that $P = m \cdot D$ (modulo torsion). Recalling that the Neron-Tate height is a quadratic form and that $m \geq 2$ it follows that

$$\hat{h}(D) \leq \frac{\hat{h}(P)}{4},$$

and hence, recalling that $|h - \hat{h}| \leq b_2 \approx 2.78$ we have that

$$h(D) \leq \frac{\hat{h}(P)}{4} + b_2,$$

and so finally we get

$$H(D) \leq \exp\left(\frac{\hat{h}(P)}{4} + b_2\right) \approx 249.04 < 250.$$

But then $D \in \mathcal{B}$, that is a contradiction with the assumption that $\langle \overline{P} \rangle$ is strictly contained in $J/J^{Tor} = \langle \overline{D} \rangle$. So we have that actually $B = J$.
By Chabauty's method (see [12] for more details) one has that

$$\iota(\tilde{H}(\mathbb{Q})) = \iota(\tilde{H}(\mathbb{Q}_p)) \cap J(\mathbb{Q}).$$

Using $p = 17, 23$ MAGMA shows that $\iota(\tilde{H}(\mathbb{Q})) = \{(1 : 0 : 0), (0 : \pm 3 : 1), (-1 : 0 : 2), (4 : \pm 27 : 1)\}$. Recall that $\tilde{H}(\mathbb{Q})$ is in a 1-to-1 correspondence with $\iota(\tilde{H}(\mathbb{Q}))$: hence there are only six rational points on $\tilde{H}$.
Using MAGMA we can compute the pullback on C for each of these points: MAGMA returns the points that are actually in the preimage of the given point together with the points at which the birational map from C to H is not defined. For all the six points we get that the preimage is given by $\{(0, \pm 6), (1, \pm 6)\}$. Since the map is birational this implies that these four points are the only rational points

on C.
Now we need to show that none of these points comes from C' via ϵ. By the definition of ϵ asking when one of these points comes from C' via ϵ is equivalent to asking when the equation

$$c_2^{-1}s^2 + c_2 s^{-2} = \pm 6 \tag{3.30}$$

has nonzero rational solutions in s, c_2. Let $e = \frac{s^2}{c_2}$; since s and c_2 are nonzero rationals, we have that e is a nonzero rational. Notice that finding nonzero rational solutions in s, c_2 for the equation (3.30) is equivalent to finding nonzero rational roots in e of the equations

$$e^2 \pm 6e + 1 = 0, \tag{3.31}$$

whose solutions are $\{\pm 3 \pm 2\sqrt{2}\}$, none of which is rational.
The statement follows. □

Then, since the map from C' to C sends rational points to rational points, 3.4.2 implies that there are no rational points on C' either. But this contradicts our initial assumption, that is the existence of a rational 5-torsion point on F. In this way, assuming that MAGMA's computations are correct, we have shown the following Theorem.

Theorem 3.4.3. *Let $s \in \mathbb{Q}^\times$ and F be the fiber of ψ_1 over $(s : 1)$, and assume there is at least one rational point on F. Then F, viewed as elliptic curve, has no nontrivial rational 5-torsion points.*

3.5 Torsion subgroup

Using the results obtained in the prevoius sections, in this one we will finally give an explicit description of the torsion subgroup of the smooth fibers of W.
In order to do this it is important to recall Mazur's Theorem.

Theorem 3.5.1 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup $E^{Tor}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \quad & \textit{with} \quad 1 \le N \le 10, N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad & \textit{with} \quad 1 \le N \le 4. \end{aligned}$$

Further, each of these group occurs as $E^{Tor}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

Proof. See [10, 11]. □

Let s be a non zero rational, and let F the fiber of ψ_1 over $(s : 1)$ on W. Assume that F has at least a rational point $P = (x_0 : y_0 : z_0 : w_0)$. Denote by $E = (F, P)$ the fiber viewed as elliptic curve. By 3.1.4 we know that $E^{Tor}(\mathbb{Q})$ has at most one element of order 2 and hence $E^{Tor}(\mathbb{Q}) \neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, where $1 \leq N \leq 4$. More in particular 3.1.4 tells us that $E^{Tor}(\mathbb{Q})[2]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. This implies that $E^{Tor}(\mathbb{Q}) \neq \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}$; by 3.2.2 we know that there are no non trivial rational 4-torsion points, from which we can deduce that $E^{Tor}(\mathbb{Q}) \neq \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}$; by 3.3.4 we know that there are no 5-torsion points, hence $E^{Tor}(\mathbb{Q}) \neq \mathbb{Z}/10\mathbb{Z}$; finally 3.4.3 shows that there are no 3-torsion points and so we have that $E^{Tor}(\mathbb{Q}) \neq \mathbb{Z}/6\mathbb{Z}$. The only case left is then that $E^{Tor}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. In other words, we have proved the following Theorem.

Theorem 3.5.2. *Let $s \in \mathbb{Q}^\times$ and F be the fiber of ψ_1 over $(s : 1)$ on W. Assume that F has at least one rational point, $P = (x_0 : y_0 : z_0 : w_0)$. Denote by $E = (F, P)$ the fiber viewed as elliptic curve. Then*

$$E^{Tor}(\mathbb{Q}) = \{(x_0 : y_0 : z_0 : w_0), (-x_0 : -y_0 : z_0 : w_0)\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

By 1.1.2 we have that the same results hold for ψ_2 as well.

Chapter 4

Density of Rational Points

In this chapter we present our main result. It is deeply linked with the Theorem 3.4 in [9] proved by Van Luijk, Logan and McKinnon.

4.1 The main results

Theorem 4.1.1. *Let c_1, c_2 be two nonzero rationals and W be the surface defined as*

$$W\colon\ x^4 - 4c_1^2y^4 - c_2z^4 - 4c_2w^4 = 0.$$

Let $P = (x_0 : y_0 : z_0 : w_0)$ be a rational point on W with x_0 and y_0 both nonzero. If $|2c_1|$ is a square in $\mathbb{Q}^\times$, then also assume that z_0, w_0 are not both zero. Then the set of rational points on the surface is Zariski dense.

Proof. First assume $|2c_1|$ not to be a square in $\mathbb{Q}^\times$. From this assumption and from the fact that the point P is a rational point, using Lemma 2.2.4, it follows that P does not lie on the intersection of two singular fibers. So let F be a smooth fiber passing through P. Without loss of generality we may assume that F is a fiber of ψ_1. Let $E = (F, P)$ be the fiber viewed as an elliptic curve.
Consider the point $P' = (-x_0 : y_0 : z_0 : w_0)$: Since x_0 is nonzero, it is different from P. The point P' is a rational point on F, and by Theorem 3.5.2, since x_0 and y_0 are both nonzero, it has infinite order. So we have infinitely many rational points on E, which implies that the set $E(\mathbb{Q})$ is Zariski dense in E. It may happen that some rational points on E lie on a singular fiber of ψ_2, but recalling that E is a

smooth fiber and using Proposition 1.3.3, it follows that this can happen for only finitely many points on E. Notice that only fnitely many points among those we obtained can have the product of the first two coordinates equal to zero: indeed assume that there are infinitely many rational points on F having as first coordinate $x = 0$, then the fiber F and the curve over W given by $x = 0$ has infinitely many points of intersection. Since F has only one irreducible component this implies that F is contained in the curve $x = 0$. But this is a contradiction to the assumption of the existence of the point $P = (x_0 : y_0 : z_0 : w_0)$ with x_0 and y_0 nonzero. So for infinitely many points on $E(\mathbb{Q})$, consider the fiber of ψ_2 passing through it. To each of these fibers we can apply the same argument as above, getting that each of these fibers have a Zariski dense set of rational points. So we have infinitely many fibers with infinitely many rational points on each of them. Zariski density follows.
Assume now that $|2c_1|$ is a square in the rationals. By hypotheses we have that z_0 and w_0 are not both zero, then from Lemma 2.2.4 it follows that P does not lie on the intersection of two singular fibers. Hence we can apply the same argument as before and the conclusion follows. □

From the theorem 4.1.1 we can easily deduce the following Corollary.

Corollary 4.1.2. *Let c_1, c_2 be two nonzero rationals such that*

$$4c_1^2 + 5c_2 = 1$$

and let $W = W_{c_1,c_2}$ be the surface defined as in (1.1)*. Then the set of rational points of the surface is Zariski dense.*

Proof. The point (1:1:1:1) lies on W, and so we can apply theorem 4.1.1. The statement follows. □

4.2 Bad points

As we have seen in the proof of Theorem 4.1.1, the assumption of the existence of a rational point on a smooth elliptic fiber having infinite order is crucial. So one may ask what are the points that satisfy this assumption or, equivalently, what are the points that do not satisfy this request and hence do not ensure the Zariski density of the set of rational points on the surface.
Van Luijk gives an answer to this question in [18], with the following Theorem.

Theorem 4.2.1 (Theorem 2.2)**.** *Let k be a number field and let $\overline{k}$ be an algebraic closure of k. Let V be a projective smooth surface over k. For each integer d there exists an explicitly computable closed subset $Z \subseteq V$ such that for each field extension K of k of degree at most d over $\mathbb{Q}$ and for each twist W of V, with corresponding isomorphism $\phi\colon W_{\overline{k}} \mapsto V_{\overline{k}}$, the set $W(K)$ is Zariski dense in W as soon as it contains any point outside $\phi^{-1}(Z)$.*

In this section we give an expicit example of such a subset. Notice that in our case we consider $d = 1$.

Let $W \subset \mathbb{P}^3$ be a diagonal quartic surface defined as in 1.1 and consider the trivial twist of W, i.e. W itself together with the identity map $\mathrm{id}_W\colon W \to W$. Taking $d = 1$, Theorem 4.2.1 implies that there exists an explicitely computable closed subset $Z \subseteq W$ such that the set $W(\mathbb{Q})$ is Zariski dense in W as soon as it contains any point outside Z. We will now compute this subset Z.
Assume that $|2c_1|$ is not a square in $\mathbb{Q}^\times$: then Theorem 4.1.1 shows that the rational points not ensuring the Zariski density are just the rational points with one of the two first coordinates equal to zero, i.e. $Z = \{xy = 0\}$. Instead if $|2c_1|$ is a rational square, then, again from Theorem 4.1.1, we can deduce that $Z = \{xy = 0\} \cup \{z = w = 0\}$.

Chapter 5

Further Developments

In this chapter we start showing how the results we got for the family A148 can be used to get similar results for another family of diagonal quartic surfaces.

5.1 Another family: A25

Consider the family of diagonal quartic surfaces, named $A25$ in [4], given by:

$$V_{c_1,c_2}\colon x^4 + c_1^2y^4 - c_2z^4 - 4c_2w^4 = 0 \tag{5.1}$$

where c_1, c_2 are non zero rationals. When the values of c_1 and c_2 are clear from the context, we will denote V_{c_1,c_2} by V.
We start by considering the following two fibrations from the surface V to $\mathbb{P}^1$:

$$\phi_1\colon (x:y:z:w) \mapsto (x^2-ic_1y^2 : z^2+2izw-2w^2) = (c_2(z^2-2izw-2w^2) : x^2+ic_1y^2) \tag{5.2}$$

$$\phi_2\colon (x:y:z:w) \mapsto (x^2-ic_1y^2 : z^2-2izw-2w^2) = (c_2(z^2+2izw-2w^2) : x^2+ic_1y^2) \tag{5.3}$$

defined over $\mathbb{Q}(i)$, where ζ_8 is a primitive 8-th root of unity and $i = \zeta_8^2$.

Proposition 5.1.1. *The fibrations defined in* (5.2) *and* (5.3) *are well defined over* V.

Proof. Start by considering ϕ_1: we can use the same arguments to prove the proposition in the case of ϕ_2.

We need to prove that the quantities $x^2 - ic_1y^2, z^2 + 2izw - 2w^2, z^2 - 2izw - 2w^2$ and $x^2 + ic_1y^2$ are not all zero for any $(x : y : z : w)$ on V. Consider $P = (x_0 : y_0 : z_0 : w_0)$ on V and assume that

$$x_0^2 - ic_1y_0^2 = 0 = z_0^2 + 2iz_0w_0 - 2w_0^2.$$

Recall that since P is an element of the projective space, its coordinates cannot be all zero. Now notice that $x^2 - ic_1y^2$ and $x^2 + ic_1y^2$ have no common factors in $\overline{\mathbb{Q}}[x, y]$; the same holds for $z^2 + 2izw - 2w^2$ and $z^2 - 2izw - 2w^2$ in $\overline{\mathbb{Q}}[z, w]$. From

$$z_0^2 + 2iz_0w_0 - 2w_0^2 = 0$$

it follows then that either $z_0 = 0 = w_0$ or $z_0^2 - 2iz_0w_0 - 2w_0^2 \neq 0$.
If $z_0^2 - 2iz_0w_0 - 2w_0^2 \neq 0$ then we are done.
So assume $z_0 = w_0$: then

$$z_0^2 - 2iz_0w_0 - 2w_0^2 = 0$$

and at least one of x_0 and y_0 is nonzero. But from $x_0^2 - ic_1y_0^2 = 0$ we have that then both are nonzero. It follows that $x_0^2 + ic_1y_0^2$ is nonzero, since $x^2 - ic_1y^2$ and $x^2 + ic_1y^2$ have no common factors in $\overline{\mathbb{Q}}[x, y]$. □

Proposition 5.1.2. *Let ϕ_1 and ϕ_2 the fibration from V to $\mathbb{P}^1$ defined as in* (5.2) *and* (5.3). *Consider the automorphism of $\mathbb{P}^3$ defined by:*

$$\Xi\colon (x : y : z : w) \mapsto (x : y : z : -w).$$

The automorphism Ξ induces an automorphism of V; with an abuse of notation we call Ξ the automorphism of V. The automorphism Ξ makes the following diagram commute:

$$\begin{array}{ccc} W & \xrightarrow{\Xi} & W \\ {\scriptstyle\phi_1}\downarrow & & \downarrow{\scriptstyle\phi_2} \\ \mathbb{P}^1 & = & \mathbb{P}^1 \end{array}$$

Proof. Trivial. □

This proposition will allow us to translate the results obtained for the fibration ϕ_1 into results for ϕ_2, and viceversa.

Let G be the Galois group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma\}$, where $\sigma\colon i \mapsto -i$. Notice then that σ induces an automorphism of $V(\mathbb{Q}(i))$.

Proposition 5.1.3. *The map σ sends fibers of ϕ_1 to fibers of ϕ_1.*

Proof. Let $P = (x_0 : y_0 : z_0 : w_0)$ be a point on V, and let $(s : t) = \phi_1(P)$. Then

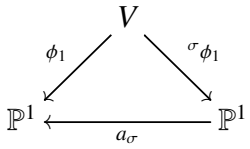
$$({}^{\sigma}\phi_1)(P) = (x_0^2 + ic_1y_0^2 : z_0^2 - 2iz_0w_0 - 2w_0^2) = (c_2t : s).$$

Hence σ sends the fiber above $(s : t)$ to the fiber above $(c_2t : s)$. □

By Proposition 5.1.2 the same result holds for ϕ_2.
Notice that the involution a_σ of $\mathbb{P}^1$, where

$$a_\sigma \colon (s : t) \mapsto (c_2t : s),$$

makes the following diagram commute:



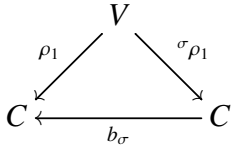
Since we are interested in working on rational points, it is more useful to have a fibration defined over $\mathbb{Q}$. In order to get such a fibration we may consider one from V to some projective curve defined over $\mathbb{Q}$, but isomorphic to $\mathbb{P}^1$ over $\overline{\mathbb{Q}}$. So let $\psi \colon \mathbb{P}^1 \to \mathbb{P}^2$ the map given by $\psi \colon (s : t) \mapsto (s^2 : st : t^2)$. Consider the composition of ϕ_1 with ψ and denote this composition by $\rho_1 \colon V \to \mathbb{P}^2$. Let C denote the image of ρ_1 in $\mathbb{P}^2$. It is easy to see that C is curve defined by

$$C \colon XZ = Y^2. \tag{5.4}$$

So we have two fibrations: ρ_1 from V to C and ${}^{\sigma}\rho_1$ from V to ${}^{\sigma}C = C$ (since C is defined over $\mathbb{Q}$). Let b_σ be the automorphism of $\mathbb{P}^2$ defined as:

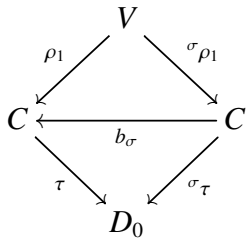
$$b_\sigma \colon (p : q : r) \mapsto (c_2r : q : p/c_2);$$

b_σ induces an automorphism of C: with an abuse of notation we denote the induced automorphism of C with b_σ as well.
It is easy to see that $b_\sigma \circ {}^{\sigma}\rho_1 = \rho_1$, i.e. the following diagram commutes.



If we represent points of $\mathbb{P}^2$ as column vectors then b_σ can be represented by an element of $\mathrm{PGL}_3(K)$. Notice that the representative of the class is not uniquely determined.
In our case we choose as representative of b_σ the matrix $M_\sigma := \begin{pmatrix} 0 & 0 & c_2 \\ 0 & 1 & 0 \\ c_2^{-1} & 0 & 0 \end{pmatrix}$.

We want to find an automorphism τ of $\mathbb{P}^2$ defined over $\overline{\mathbb{Q}}$ such that the diagram below commutes,



i.e. τ must be such that $\tau \circ b_\sigma = {}^\sigma\tau$, where D_0 is a conic in $\mathbb{P}^2$ isomorphic to $\mathbb{P}^1$ over the rationals. This means that if τ is represented by the invertible matrix T (in the analogous sense of b_σ with respect to M_σ) we require that ${}^\sigma T = T \cdot M_\sigma$. Finding such a T means finding the desired τ.

Lemma 5.1.4. *Let K be a field extension of $\mathbb{Q}$; let H denote the galois group $\mathrm{Gal}(K/\mathbb{Q})$. Assume that there exist a map $h \mapsto M_h$ such that it is a 1-cocycle, i.e. $M_{kh} = M_k \cdot {}^k M_h$ for any $h, k \in H$. Consider $S = \sum_{h\in H} M_h \cdot {}^h N$ for some choice of N in $\mathrm{GL}_3(K)$. Then, for any $g \in H$, we have that*

$$M_g \cdot {}^g S = S.$$

Proof.

$$\begin{aligned} M_g \cdot {}^g S &= M_g \cdot {}^g\Big(\sum_{h\in H} M_h \cdot {}^h N\Big) && (5.5)\\ &= M_g \cdot \sum_{h\in H} {}^g M_h \cdot {}^g({}^h N) && (5.6)\\ &= \sum_{h\in H} M_g \cdot {}^g M_h \cdot {}^{gh} N && (5.7)\\ &= \sum_{h\in H} M_{gh} \cdot {}^{gh} N && (5.8)\\ &= \sum_{h'\in H} M_{h'} \cdot {}^{h'} N && (5.9)\\ &= S && (5.10) \end{aligned}$$

Notice that the identity (5.8) follows from the hypotheses that the map $h \mapsto M_h$ is a 1-cocycle. □

From Lemma 5.1.4 one can easily deduce the following Corollary.

Corollary 5.1.5. *Let K, H, S be defined as in 5.1.4. Assume that S is invertible and denote with $T = S^{-1}$ its inverse. Then for any $g \in H$ we have that*

$$^{g}T = T \cdot M_g.$$

It is easy to show that the hypoteses of Lemma 5.1.4 hold in our case: since ρ_1 is defined over $\mathbb{Q}(i)$, we can consider $K = \mathbb{Q}(i)$, then $H = G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma\}$. Consider then the map from G to $GL_3(\mathbb{Q}(i))$ sending 1 to the identity matrix $\mathbb{I}$ and σ to the matrix M_σ defined as before. It is easy to see that this map is a 1-cocycle. So we can apply the previous results to our case.
To keep the computations simple we take

$$N = \begin{pmatrix} 1 & 0 & i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

getting

$$S = \begin{pmatrix} ic_2 & 0 & -ic_2^2 + c_2 \\ 0 & 1 & 0 \\ -i & 0 & ic_2 + 1 \end{pmatrix}$$

and hence

$$T = S^{-1} = \begin{pmatrix} 1 - i/c_2 & 0 & c_2 + i \\ 0 & 2 & 0 \\ 1/c_2 & 0 & 1 \end{pmatrix}.$$

By Corollary 5.1.5 this is the desired T, i.e. $^{\sigma}T = T \cdot M_\sigma$.
The automoprhism τ is hence given by sending:

$$(p : q : r) \mapsto ((1 - i/c_2)p + (c_2 + i)r : 2q : p/c_2 + r), \tag{5.11}$$

and its inverse is given by:

$$(p : q : r) \mapsto (c_2(r + i(p - c_2 r)) : q : r - i(p - c_2 r)). \tag{5.12}$$

Now we can write the equation defining the image of the curve C under τ, the curve $D_0 := \tau(C)$ ($= {}^{\sigma}\tau(C)$). Using (5.12) and recalling that C is defined by $Y^2 = XZ$ we get that D_0 is defined by

$$D_0 \colon Y^2 = c_2(Z^2 + (X - c_2 Z)^2). \tag{5.13}$$

Finding two fibrations from V to a curve described by a simpler equation might be useful; for this reason consider the automorphism of $\mathbb{P}^2$ defined over $\mathbb{Q}$ by

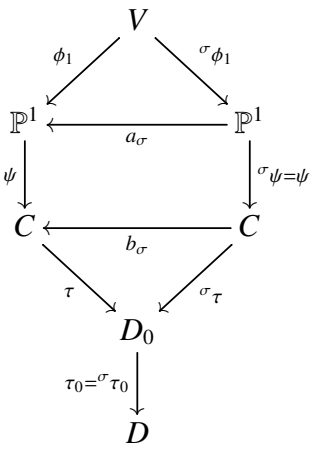
$$(p : q : r) \mapsto (c_2(p - c_2 r) : q : c_2 r), \tag{5.14}$$

call it τ_0. Notice that, since it is defined over the rationals, ${}^{\sigma}\tau_0 = \tau_0$.
It follows that the image of D_0 via τ_0, call it $D := \tau_0(D_0)$, is the curve given by:

$$c_2 Y^2 = X^2 + Z^2. \tag{5.15}$$

In this way we have found two fibrations from V to D, namely:

$$\Phi_1 := \tau_0 \circ \tau \circ \psi \circ \phi_1$$
$${}^{\sigma}\Phi_1 := \tau_0 \circ {}^{\sigma}\tau \circ \psi \circ {}^{\sigma}\phi_1$$



Lemma 5.1.6. *Using the above notations, we have that*

$${}^{\sigma}\Phi_1 = \Phi_1,$$

i.e. the diagram above is commutative.

Proof. The proof is straightforward from the construction and follows from the commutativity of the diagram above. Indeed

$$\begin{aligned}
{}^{\sigma}\Phi_1 &= {}^{\sigma}(\tau_0 \circ \tau \circ \psi \circ \phi_1) \\
&= {}^{\sigma}\tau_0 \circ {}^{\sigma}\tau \circ {}^{\sigma}\psi \circ {}^{\sigma}\phi_1 \\
&= \tau_0 \circ (\tau \circ b_\sigma) \circ {}^{\sigma}\psi \circ {}^{\sigma}\phi_1 \\
&= \tau_0 \circ \tau \circ (b_\sigma \circ {}^{\sigma}\psi) \circ {}^{\sigma}\phi_1 \\
&= \tau_0 \circ \tau \circ (\psi \circ a_\sigma) \circ {}^{\sigma}\phi_1 \\
&= \tau_0 \circ \tau \circ \psi \circ (a_\sigma \circ {}^{\sigma}\phi_1) \\
&= \tau_0 \circ \tau \circ \psi \circ \phi_1 = \Phi_1.
\end{aligned}$$

□

Lemma 5.1.6 shows that in fact the fibration Φ_1 is defined over the rationals, but we still do not have an explicit expression for it that is defined over the rationals. If we call

$$\begin{aligned}\alpha &= x^2 - ic_2y^2,\\ \beta &= z^2 + 2izw - 2w^2,\\ \overline{\alpha} &= x^2 + ic_2y^2,\\ \overline{\beta} &= z^2 - 2izw - 2w^2;\end{aligned}$$

then it follows that on V we have that $\alpha\overline{\alpha} = c_2\beta\overline{\beta}$.
Using this notation we can write

$$(s : t) = \phi_1(x : y : z : w) = (\alpha : \beta)$$

from which it follows that

$$(p : q : r) = \psi(s : t) = (s^2 : st : t^2) = (\alpha^2 : \alpha\beta : \beta^2).$$

Then applying τ:

$$\tau(\alpha^2 : \alpha\beta : \beta^2) = ((1 - i/c_2)\alpha^2 + (c_2 + i)\beta^2 : 2\alpha\beta : \alpha^2/c_2 + \beta^2)$$

and finally

$$\begin{aligned}\tau_0((1 - i/c_2)\alpha^2 + (c_2 + i)\beta^2 : 2\alpha\beta : \alpha^2/c_2 + \beta^2) &=\\ &= (c_2(((1 - i/c_2)\alpha^2 + (c_2 + i)\beta^2) - c_2(\alpha^2/c_2 + \beta^2)) : 2\alpha\beta : c_2(\alpha^2/c_2 + \beta^2))\\ &= (ic_2\beta^2 - i\alpha^2 : 2\alpha\beta : \alpha^2 + c_2\beta^2).\end{aligned}$$

So the fibration Φ_1 can be expressed by:

$$(x : y : z : w) \mapsto (ic_2\beta^2 - i\alpha^2 : 2\alpha\beta : \alpha^2 + c_2\beta^2), \tag{5.16}$$

from wich it follows that ${}^{\sigma}\Phi_1 = \Phi_1$ can be expressed by:

$$(x : y : z : w) \mapsto (-ic_2\overline{\beta}^2 + i\overline{\alpha}^2 : 2\overline{\alpha}\overline{\beta} : \overline{\alpha}^2 + c_2\overline{\beta}^2). \tag{5.17}$$

Although the fibration is defined over the rationals, we still have nonrational expressions for it, since i is involved in (5.16) and (5.17) and also in the expression of α and β.
In order to find rational expressions recall the following property:

$$\text{If } \frac{x}{y} = \frac{z}{w} \text{ then } \frac{x}{y} = \frac{z}{w} = \frac{x+z}{y+w}$$

where K is a field and $x, y, z, w \in K$, $y, w \neq 0$, $y + w \neq 0$.
So we can consider the expressions of Φ_1 from V to D given by the sum and the difference divided by i of the expressions in (5.16) and (5.17), getting

$$(x : y : z : w) \mapsto (P : Q : R) = (P' : Q' : R') \tag{5.18}$$

where

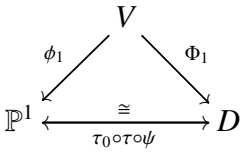
$$P = -4c_2zw(z^2 - 2w^2) - 2c_2x^2y^2, \tag{5.19}$$
$$Q = 2(x^2z^2 - 2x^2w^2 + 2c_2y^2zw), \tag{5.20}$$
$$R = (x^4 - c_2y^4) + c_2(z^4 - 4z^2w^2 + w^2 - 2z^2w^2), \tag{5.21}$$

and

$$P' = c_2(z^4 - 4z^2w^2 + w^2 - 2z^2w^2) - (x^4 - c_2y^4), \tag{5.22}$$
$$Q' = 2(2x^2zw - c_2y^2z^2 + c_2y^2w^2), \tag{5.23}$$
$$R' = 4c_2zw(z^2 - 2w^2) + 2c_2x^2y^2. \tag{5.24}$$

We can summarize these results in the following Proposition.

Proposition 5.1.7. *Let V be the projective surface defined as in* (5.1) *and D the projective curve defined as in* (5.15)*. Then there is rational fibration Φ_1 from V to D defined by* (5.18)*. Furthermore, the following diagram commutes.*



Doing the same construction, but starting with the fibration ϕ_2, we get another fibration from V to D defined over the rationals. Call it Φ_2. Recalling Lemma 5.1.2 one can easily check that Φ_2 is given by

$$(x : y : z : w) \mapsto (P : Q : R) = (P' : Q' : R') \tag{5.25}$$

where

$$P = 4c_2zw(z^2 - 2w^2) - 2c_2x^2y^2, \tag{5.26}$$
$$Q = 2(x^2z^2 - 2x^2w^2 - 2c_2y^2zw), \tag{5.27}$$
$$R = (x^4 - c_2y^4) + c_2(z^4 - 4z^2w^2 + w^2 - 2z^2w^2), \tag{5.28}$$

and

$$P' = c_2(z^4 - 4z^2w^2 + w^2 - 2z^2w^2) - (x^4 - c_2y^4), \tag{5.29}$$
$$Q' = 2(-2x^2zw - c_2y^2z^2 + c_2y^2w^2), \tag{5.30}$$
$$R' = -4c_2zw(z^2 - 2w^2) + 2c_2x^2y^2. \tag{5.31}$$

5.2 An isomorphism between the two families

In this section we want to find an isomorhism between the two families defined over some algebraic extension of $\mathbb{Q}$. This isomorphism will allow us to translate any geometric result for the family A148 into a result for the family A25.
In particular we want an isomorphism which respects the fibrations given by (1.2) and (1.3) for the family A148 and given by (5.2) and (5.3) for the family A25 and viceversa.
Let c_1, c_2 be in $\mathbb{Q}^\times$ and consider the surface $V = V_{c_1,c_2}$ of the family A25 defined as in (5.1) with the fibrations ϕ_1 and ϕ_2 be its fibrations defined in (5.2) and (5.3); let $W = W_{c_1,c_2}$ be the surface of the family A148 defined as in (1.1), and ψ_1 and ψ_2 its fibration defined as in (1.2) and (1.3) respectively. We want to find an isomorphism Θ from V to W such that the following diagrams commute for $k = 1, 2$:

$$\begin{array}{ccc} V & \xrightarrow{\Theta} & W \\ {\scriptstyle \phi_k}\downarrow & & \downarrow{\scriptstyle \psi_k} \\ \mathbb{P}^1 & = & \mathbb{P}^1 \end{array}$$

Proposition 5.2.1. *Let Θ denote the map from V to W defined as*

$$\Theta\colon (x : y : z : w) \mapsto (x : \frac{\zeta_8 y}{\sqrt{2}} : z : iw). \tag{5.32}$$

Then Θ makes the previous diagram commute.

Proof. It is easy to see that it is well defined, i.e. any point on V is sent to a point on W, and bijective; we need to check that the diagram is commutative, that is $\psi_k \circ \Theta = \phi_k$, with $k = 1, 2$:

$$\begin{aligned} \psi_1 \circ \Theta(x : y : z : w) &= \psi_1(x : \frac{\zeta_8 y}{\sqrt{2}} : z : iw) \\ &= (x^2 - 2c_1\frac{iy^2}{2} : z^2 + 2izw - 2w^2) \\ &= (x^2 - c_1 iy^2 : z^2 + 2izw - 2w^2) \\ &= \phi_1(x : y : z : w). \end{aligned}$$

Recalling Lemmas 1.1.2 and 5.1.2, the commutativity of the diagram for $k = 2$ follows. □

So the Θ is the desired isomorphism. Notice that it is induced on V by an automorphism of $\mathbb{P}^3$ that does not depend on c_1, c_2.

Bibliography

[1] S. An, S. Kim, D. Marshall, S. Marshall, W. McCallum, and A. Perlis. Jacobians of genus one curves. *Journal of Number Theory*, 90(2):304–315, 2001.

[2] F. A. Bogomolov and A. Tschinkel. Density of rational points on elliptic K3 surfaces. *Asian J. Math.*, 4(2):351–368, June 2000.

[3] F. A. Bogomolov and A. Tschinkel. Rational curves and points on elliptic K3 surfaces. *Amer. J. Math.*, 4(127):825–835, 2005.

[4] M. Bright. Computations on diagonal quartic surfaces. Phd thesis, Cambridge University.

[5] J. Cassels and E. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230. Cambridge Univ Pr, 1996.

[6] B. Edixhoven and J.-M. Couveignes. *Computational Aspects of Modular Forms and Galois Representations*. Princeton University Press.

[7] N. Elkies. On $a^4+b^4+c^4 = d^4$. *Mathematics of Computation*, pages 825–835, 1988.

[8] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag.

[9] A. Logan, D. McKinnon, and R. Van Luijk. Density of rational points on diagonal quartic surfaces. *Algebra Number Theory*, 4(1):1–20, 2008.

[10] B. Mazur. Rational isogenies of prime degree. *Inventiones Math.44*.

[11] B. Mazur. Modular curves and the Eisenstein Ideal. *Inst. Hautes Études Sci. Publ. Math*, 47:129–162, 1977.

[12] W. Mccallum and B. Poonen. The method of Chabauty and Coleman. *preprint*, 2007.

[13] R. G. E. Pinch and H. Swinnerton-Dyer. *Arithmetic of diagonal quartic surfaces*. Cambridge University Press.

[14] J. H. Silverman. *Arithmetic of Elliptic Curves, 2nd edition*. Springer-Verlag.

[15] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer-Verlag.

[16] J. Silvermann. Advanced topics in the arithmetic of elliptic curves, January 1994.

[17] P. Swinnerton-Dyer. Arithmetic of diagonal quartic surfaces. *Proc. London Math. Soc*.

[18] R. van Luijk. Density of rational points on elliptic surfaces. *Journal*.

[19] R. van Luijk. Rational points on K3 surfaces. Phd thesis, University of California, Berkeley.

[20] Wikipedia. K3 surfaces.

[21] Wikipedia. Neron-tate heigh.