Group of Weierstrass points of a plane quartic with eight hyperflexes or more

Martine Girard*
girard@math.leidenuniv.nl

Abstract The group generated by the Weierstrass points of a smooth curve in its Jacobian is an interesting intrinsic invariant of the curve. We determine this group for all smooth quartics with eight hyperflexes or more. Since Weierstrass points are closely related to moduli spaces of curves, as an application, we get bounds on both the rank and the torsion part of this group for a generic quartic having a fixed number of hyperflexes in the moduli space $\mathcal{M}_3$ of curves of genus 3.

The Weierstrass points of an algebraic curve, which can be defined over some extension of the base field, form a distinguished set of points of the curve having the unique property of being geometrically intrinsic. Curves of genus 0 or 1 have no Weierstrass points and for hyperelliptic curves, the Weierstrass points can be easily characterized as the ramification points under the hyperelliptic involution, which generate the 2-torsion subgroup of the Jacobian. For nonhyperelliptic curves of genus 3, which admit a plane quartic model, the structure of the Weierstrass subgroup, i.e. the subgroup of the Jacobian generated by these points under the Abel-Jacobi map, cannot be characterized that easily. This structure is known for curves with many automorphisms ([7], [9], [10]), in which cases, the groups are finite. As with Weierstrass points, the Weierstrass subgroup is a geometric invariant of the curve, which we study in this paper. More precisely, we determine the structure of this group for all curves having either eight (Theorems 4.1 and 5.1) or nine hyperflexes (Theorem 3.1) i.e. points at which the tangent line to the curve meets the curve with multiplicity four. These are the first non-trivial cases of interest since there are no curves with either ten or eleven hyperflexes and the two possible cases of curves with twelve hyperflexes have already been treated ([4], [10]).

*This research was carried out while a postdoctoral fellow at Leiden University within the European Research Training Network Galois Theory and Explicit Methods in Arithmetic

Weierstrass points are used to construct various stratifications of moduli spaces of curves. In particular, there exists a stratification of the moduli space $\mathcal{M}_3$ of genus 3 curves, due to Vermeulen [12], in terms of the number of hyperflexes. This stratification determines certain intrinsic families of quartics, corresponding to the strata of $\mathcal{M}_3$, characterized by the number of hyperflexes and their geometric configuration. Using specialization of curves in these families, we obtain bounds both on the rank and on the torsion part of the group generated by the Weierstrass points for a generic quartic in these strata. In particular, in [2], we showed that for a generic quartic, it is a free abelian group of rank at least 11. In this paper, we pursue the study carried out in [3], [2] and improve some of the bounds previously obtained.

We will first recall the definitions of Weierstrass points and of the object of our study. In section 2, we will state two theorems fundamental to the present study. We will then compute the Weierstrass subgroup for curves with eight or nine hyperflexes. In order to do so, we first restrict the number of generators by exhibiting elementary relations (arising from lines or conics throught these points), we then use the fact that the Jacobians are isogeneous to the product of three elliptic curves and reduction on these elliptic curves to prove independence of points. Finally, in section 6, we will deduce the above-mentioned results on the strata of $\mathcal{M}_3$.

Acknowledgements: I would like to thank Marc Hindry and David Kohel for all their helpful comments during the elaboration of this paper.

1 Definitions and notations

1.1 Weierstrass points

Let $\mathcal{C}$ be a smooth projective curve of genus $g \geq 2$ and let P be any point on $\mathcal{C}$. We will say that P is a *Weierstrass point* if and only if there exists a differential form $\omega \in H^\circ(C, \Omega_C)$, such that $\mathrm{ord}_P(\omega) \geq g$. Let $\mathcal{W}$ be the set of Weierstrass points on $\mathcal{C}$.

We can attach to a point a notion of weight, which will give an alternative characterization of Weierstrass points: $P \in \mathcal{W}$ if and only if $w(P) \geq 1$. The weight is defined as follows: for any divisor D on $\mathcal{C}$, let $\mathcal{L}(D)$ be the Riemann-Roch space $\{f \in k(\mathcal{C}), \mathrm{div}\,(f) + D \geq 0\}$ and let $l(D)$ be its dimension. The gap sequence associated to P is then defined to be the set $G(P) = \{n \in \mathbb{Z}_{>0}, l(nP) = l((n-1)P)\}$. We can define the *weight* of a point to be

$w(P) = \sum_{n \in G(P)} n - g(g+1)/2.$

The number of Weierstrass points is finite. More precisely, the number of Weierstrass points counted with multiplicities equal to their weights is $\sum_{P \in \mathcal{C}} w(P) = g(g^2-1)$.

1.2 The group W

Choose $\infty \in \mathcal{W}$, the Abel-Jacobi map is given by

$$\jmath : \begin{array}{ccc} \mathcal{C} & \to & J = \mathrm{Pic}^\circ(\mathcal{C}) \\ P & \mapsto & [P - \infty] \cdot \end{array}$$

We define the *Weierstrass subgroup* W to be the group generated by the images of the Weierstrass points under this map. It is independent of the base point of the Abel-Jacobi map, hence it defines an interesting geometric invariant of the curve.

For hyperelliptic curves, the Weierstrass points are well-known: they are the ramification points of the curve. Moreover, the group they generate in the Jacobian is the whole 2-torsion group, that is $W = (\mathbb{Z}/2\mathbb{Z})^{2g}$, for a hyperelliptic curve of genus g.

1.3 Plane quartics

We will henceforth restrict ourselves to the case of smooth plane quartics. Indeed, they are the non-hyperelliptic curves of smaller genus, i.e. genus 3. The Weierstrass points are the *flexes* of the curve, i.e. the points where the tangent line to the curve meets the curve with multiplicity at least 3. The *hyperflexes* are then the points for which this multiplicity equals 4; they correspond to Weierstrass points of weight 2. As we have seen before, there are 24 points counted with multiplicity equal to the weight, i.e. $r + 2s = 24$ if s is the number of hyperflexes and r is the number of ordinary flexes.
Convention. We assume for the rest of the paper that the curve $\mathcal{C}$ has a hyperflex, which we take as base point of the Abel-Jacobi map $\jmath$.

Remark. If the base point ∞ of $\jmath$ is a hyperflex, then the image of any hyperflex is a point of order 4 in the Jacobian. Indeed, if L_P (resp. L_∞) is the linear form defining the tangent line to the curve at P (resp. ∞), we have $\mathrm{div}\,(L_P/L_\infty) = 4(P) - 4(\infty)$, hence the order of $\jmath(P)$ divides 4, and it cannot be 2 otherwise the curve would be hyperelliptic. Moreover, there is an extra relation between the images of the Weierstrass points, that is $\sum w(P)\jmath(P) = 0$. We thus obtain that W is a quotient of $\mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^{s-1}$.

Hence, we get a "naïve" bound for the rank: $\mathrm{rank}(W) \leq 24-2s-1$ if $s \neq 12$. For $s = 12$, all points are hyperflexes, they are thus all of order 4 and the rank is 0.

2 Specialization

In this section, we review the tools we use to obtain results both on particular curves and on families. In particular, we state two theorems concerning the behavior under specialization.

Let $\mathcal{C} \to \mathcal{S}$ be a family of smooth projective curves of genus g. Let W_η (resp. W_s) be the group generated by the Weierstrass points in the generic fiber (resp. a special fiber). The divisor of Weierstrass points form an algebraic family. More precisely, we have

Theorem 2.1.
(i) W_s is a group quotient of W_η.
(ii) The specialization is injective on the torsion part.

Proof: For the first part, see Hubbard [6] or Laksov-Thorup [8], the second part is classic (see [5] Theorem C.1.4). ∎

Both these properties and the following theorem of Silverman are essential to deduce results for families of curves and also to obtain bounds on the rank and the torsion part of a generic quartic in the moduli space of curves of genus 3, as we will see in section 6.

Theorem 2.2 (Silverman [11]). *Let $A \to C$ be a (flat) family of abelian varieties, all defined over a global field K, where C is a smooth projective curve. At a point $t \in C(\overline{K})$ for which the fibre A_t is non-singular, the specialization map is defined by $\sigma_t : A(C) \to A_t(\overline{K}),\quad P \mapsto P_t$.*

Assume that A has no constant part, then the set

$$\{t \in C(\overline{K}) \mid \sigma_t \text{ is not injective }\}$$

is a set of bounded height in $C(\overline{K})$. In particular, if K is a number field and $d \geq 1$ is an integer, then σ_t is injective for all but finitely many $t \in \bigcup_{[L:K]\leq d} C(L)$.

3 Curve with nine hyperflexes

There are exactly two curves with precisely nine hyperflexes [12]. These are the curve Ω_1 given by the following projective equation and its conjugate Ω_2

$$(X^2 - YZ)^2 + (-3 + \sqrt{7})YZ(-2X + Y + Z)(-X + Y + Z) = 0.$$

This curve has fifteen Weierstrass points, nine of which are hyperflexes. The hyperflexes are lying on three lines. We will show that the "naive" bound on the rank is attained in this case:

Theorem 3.1. *The group generated by the Weierstrass points of any of the two curves Ω_i is $W = (\mathbb{Z}/4\mathbb{Z})^5 \times \mathbb{Z}^5$.*

We will consider another model for the curve. Let $\mathcal{C}$ be the curve given by the following equation

$$(8\sqrt{7} - 21)X^4 + 6(2 - \sqrt{7})X^2YZ + (\sqrt{7} - 3)(Y^3 + Z^3)X + 3Y^2Z^2 = 0.$$

The map from Ω_1 to $\mathcal{C}$ is given by

$$\psi : (X : Y : Z) \mapsto \left(X - Y - Z : 2jX + Y + j^2Z : 2j^2X + Y + jZ\right).$$

3.1 Weierstrass points

Using `magma` [1], we get that the Weierstrass points are defined over the number field M of degree 144 where $K = \mathbb{Q}(i, \sqrt{7}, \sqrt{3})$, $L = K(s)$ and $M = L(r)$ where $s^2 + 2\sqrt{7}s + 3\sqrt{7} - 2 = 0$ and $r^3 = -24s^3 + 51s^2 + 636s + 794$. Let $j = (-1 + i\sqrt{3})/2$.

3.1.1 Weierstrass points of weight two

The hyperflexes are
$P_1 = (j + 1 : j : 1)$, $P_3 = (-a - 2 : a + 4j^2 - 2 : a + 4j - 2)$,
$P_2 = (-1 : 1 : 1)$, $P_4 = (b - 2 : -b + 4j^2 - 2 : -b + 4j - 2)$,
$P_5 = (-j : j^2 : 1)$, $P_6 = (-2 : -(\sqrt{7} - 2)\sqrt{3} - 1 : (\sqrt{7} - 2)\sqrt{3} - 1)$,
$P_7 = (-2 : (\sqrt{7} - 2)\sqrt{3} - 1 : -(\sqrt{7} - 2)\sqrt{3} - 1)$,
$P_8 = (-a - 2 : a + 4j - 2 : a + 4j^2 - 2)$, and
$P_9 = (b - 2 : -b + 4j - 2 : -b + 4j^2 - 2)$ with $a = (\sqrt{7} + 1)(i + 1)$ and $b = (\sqrt{7} + 1)(i + 1)$.

The 4 points of intersection of the curve with the line $X = j^2Y + jZ$ (resp. $X = Y + Z$, resp. $X = jY + j^2Z$) are $\{P_1, P_2, P_3, P_4\}$ (resp. $\{P_1, P_5, P_6, P_7\}$, resp. $\{P_2, P_5, P_8, P_9\}$).

3.1.2 Weierstrass points of weight one

The Weierstrass points of weight one of the curve $\mathcal{C}$ are the six points $Q_1 = (r : r^2 : 7)$, $Q_2 = (rj : r^2j^2 : 7)$, $Q_3 = (rj^2 : r^2j : 7)$,
$Q_4 = (r : 7 : r^2)$, $Q_5 = (rj : 7 : r^2j^2)$ and $Q_6 = (rj^2 : 7 : r^2j)$.

3.1.3 Relations between the Weierstrass points

Convention. From now on, we take P_2 as base-point for the Abel-Jacobi map and we will write P for the image $[P - P_2]$ of P under $\jmath$.

Since the hyperflexes lie on three lines and the base-point is a hyperflex, there are some straighforward relations (see the remark at the end of section 1.3).

Proposition 3.2. *The Weierstrass points satisfy the following relations*

- $4P_i = 0$,
- $P_1 + P_2 + P_3 + P_4 = 0$,
- $P_1 + P_5 + P_6 + P_7 = 0$,
- $P_2 + P_5 + P_8 + P_9 = 0$,
- $2\,(Q_1 + Q_2 + Q_3 + Q_4 + Q_5 + Q_6) = 0$.

From these relations, we deduce that

Proposition 3.3. *The group W is a quotient of $\mathbb{Z}^5 \times (\mathbb{Z}/4\mathbb{Z})^5 \times (\mathbb{Z}/2\mathbb{Z})$.*

We will show that the sum of the Weierstrass points of weight one is already equal to twice the sum of some hyperflexes, and that there are no other relations between the Weierstrass points, hence the theorem.

3.2 Structure of the Jacobian

In this section, we show that the Jacobian is isogeneous to the product of three elliptic curves, that we determine.

Proposition 3.4. *The Jacobian of the curve $\mathcal{C}$ is isogeneous to the product of two copies of an elliptic curve by a third elliptic curve, i.e. $\mathcal{J} \simeq \mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$, with $\mathcal{E}_1 \simeq \mathcal{E}_2$.*

Proof: We check that the pullbacks of differential forms on each elliptic curve are independent on $\mathcal{C}$. For the definitions of both the curves and the maps, see section 3.2.2 below. On the elliptic curve $\mathcal{E}_i$, a differential form is given by $\omega_i = du/v$. A basis of the differential forms on $\mathcal{C}$ is ω_0, $x\omega_0$ and $y\omega_0$ with

$$\omega_0 = \frac{dx}{x^2 + \sqrt{7}x^2 - 3y + y^2x - y\sqrt{7}}.$$

The pullbacks of the three differential forms are respectively

$$\phi_1^*(\omega_1) = c_1(y-1)\omega_0, \quad \phi_2^*(\omega_2) = c_2(2y+1+i\sqrt{3})\omega_0, \quad \phi_3^*(\omega_3) = c_3 x\omega_0$$

where the c_i's are constants, hence the result. ∎

3.2.1 Automorphisms of the curve

The automorphism group of the curve is equal to S_3. More precisely, this group is generated by the two automorphisms ρ and σ given respectively by

$$\begin{aligned} &\rho : (X:Y:Z) \mapsto (X:Z:Y) \\ \text{and} \qquad &\sigma : (X:Y:Z) \mapsto (jX : j^2Z : Y). \end{aligned}$$

They act on the Weierstrass points in the following manner:

$$\begin{aligned} \rho &= (P_1P_5)(P_6P_7)(P_3P_8)(P_4P_9)(Q_1Q_4)(Q_2Q_6)(Q_3Q_5) \\ \sigma &= (P_2P_5)(P_3P_6)(P_4P_7)(P_8P_9)(Q_1Q_5)(Q_2Q_4)(Q_3Q_6). \end{aligned}$$

3.2.2 Elliptic factors of the Jacobian

By identifying points which are in the same orbit for the action of these two automorphisms, we obtain two maps from $\mathcal{C}$ to the same elliptic curve.

Proposition 3.5. *The degree 2 morphism ϕ_1 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_1 = \mathcal{C}/\langle\rho\rangle$ can be described as $(X:Y:Z) \mapsto (u,v)$ where*

$$\begin{cases} u = 2\,\dfrac{(-3+\sqrt{7})(-4X+Y+Z)}{(2X+Y+Z)} \\ v = 4\,\dfrac{(13-5\sqrt{7})((XZ+YX+2YZ)(1-\sqrt{7})+6(X^2-YZ))}{(2X+Y+Z)^2} \end{cases}$$

writing $\mathcal{E}_1$ as

$$v^2 = u^3 - \left(4\sqrt{7}-10\right)u^2 - \left(-296+112\sqrt{7}\right)u - 1040\sqrt{7} + 2752.$$

Proposition 3.6. *The degree 2 morphism ϕ_2 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_2 = \mathcal{C}/\langle\sigma\rangle$ is given by $(X:Y:Z) \mapsto (u,v)$ where*

$$\begin{cases} u = 2\,\dfrac{(-3+\sqrt{7})(-4X+j^2Y+jZ)}{(2X+j^2Y+jZ)} \\ v = 4\,\dfrac{(13-5\sqrt{7})((XjZ+j^2YX+2YZ)(1-\sqrt{7})+6(X^2-YZ))}{(2X+j^2Y+jZ)^2} \end{cases}$$

writing $\mathcal{E}_2$ as

$$v^2 = u^3 - \left(4\sqrt{7}-10\right)u^2 - \left(-296+112\sqrt{7}\right)u - 1040\sqrt{7} + 2752.$$

Let $\tau = \sigma\rho$. This automorphism is of order three with two fixed points $(0:1:0)$ and $(0:0:1)$. By identifying points in the same orbit, we also obtain a map to a second elliptic curve.

Proposition 3.7. *The degree 3 morphism from the curve $\mathcal{C}$ to the elliptic curve $\mathcal{E}_3 = \mathcal{C}/\langle\tau\rangle$ is given by*
$\phi_3 : (X:Y:Z) \mapsto (u = X_3/Z_3, v = Y_3/Z_3)$ *with*

$$\begin{aligned} (X_3:Y_3:Z_3) = \Big(&2(141-42\sqrt{7})X^2YZ + (267\sqrt{7}+633)X(Y^3+Z^3) \\ &+ (141\sqrt{7}+399)\sqrt{3}X(Y^3-Z^3) + 2(39\sqrt{7}+114)Y^2Z^2 : \\ &2(378-189\sqrt{7})X^2YZ + (351\sqrt{7}-945)X(Y^3+Z^3) + 2(54\sqrt{7}+378)Y^2Z^2 : \\ &2X^2YZ + (45\sqrt{7}+119)\sqrt{3}X(Y^3-Z^3) \\ &+2(39\sqrt{7}+103)X(Y^3+Z^3) + 4(3\sqrt{7}+8)Y^2Z^2\Big), \end{aligned}$$

writing $\mathcal{E}_3$ as $v^2 = u^3 + (26460\sqrt{7} - 70038)u + (12057201 - 4557168\sqrt{7})$.

3.3 Study of the Weierstrass points

We will compute the images of the Weierstrass points on each of these three elliptic curves.

3.3.1 Images of the Weierstrass points on $\mathcal{E}_1$

Recall that the orbits under the action of ρ are $\{P_1, P_5\}$, $\{P_6, P_7\}$, $\{P_3, P_8\}$ $\{P_4, P_9\}$, $\{Q_1, Q_4\}$, $\{Q_2, Q_6\}$ and $\{Q_3, Q_5\}$, the point P_2 being fixed. Thus, the images of the Weierstrass points are the following eight points on the elliptic curve $\mathcal{E}_1$,

$$\begin{gathered}A=\phi_1(\{P_1,P_5\}),\quad B=\phi_1(\{P_3,P_8\}),\quad C=\phi_1(\{P_4,P_9\}),\\ D=\phi_1(\{P_6,P_7\}),\quad R_1=\phi_1(\{Q_1,Q_4\}),\quad R_2=\phi_1(\{Q_2,Q_6\}),\\ R_3=\phi_1(\{Q_3,Q_5\})\quad\text{and}\quad\mathcal{O}=\phi_1(P_2).\end{gathered}$$

The three points of order 2 are $T_0=(-2+\sqrt{7}+11i-4i\sqrt{7},0)$, $T_1=(-2+\sqrt{7}-11i+4i\sqrt{7},0)$ and $T_2=(-6+2\sqrt{7},0)$.

On the elliptic curve $\mathcal{E}_1$, the following relations hold:

$$\begin{gathered}A+D=\mathcal{O},\quad 2A=T_2,\quad 2B=T_0,\quad A+B+C=\mathcal{O},\\ \text{and}\quad R_1+R_2+R_3=T_2.\end{gathered}$$

Proposition 3.8. *The two points R_1 and R_2 are of infinite order and are $\mathbb{Z}$-independent.*

Proof: In order to prove the proposition, we will compute the images of these two points when we reduce the curve modulo primes of residue class degree 1 in $K=\mathbb{Q}(i,\sqrt{3},\sqrt{7},a,b)$. There are such primes above 2797 and 16333 in K. We have $\#\widetilde{\mathcal{E}}_1(\mathbb{F}_{2797})=2^5\cdot 89$, $\widetilde{R_1}$ has order $4\cdot 89$ and $\widetilde{R_2}$ has order $2\cdot 89$. For the second prime, $\#\widetilde{\mathcal{E}}_1(\mathbb{F}_{16333})=2^5\cdot 509$, $\widetilde{R_1}$ has order $4\cdot 509$ and $\widetilde{R_2}$ has order $2\cdot 509$. Thus R_1 and R_2 are of infinite order. Moreover, there are no K-rational points of order 53.

$p=4993$

Take 158 as a square root of -1 mod 4993, 1266 as a square root of 3 mod 4993 (hence $j\equiv 2650 \mod 4993$), 212 as a square root of 7 mod 4993, 2011 as a square root of $3-212$ mod 4993 (hence $s\equiv 4277 \bmod 4993$) and 2692 as a cubic root of $-24\cdot 4277^3+51\cdot 4277^2+636\cdot 4277+794 \bmod 4993$.

The reduction $\widetilde{\mathcal{E}}_1$ of the elliptic curve is given by $y^2=x^3+4155x^2+1517x+1964$, and one has $\#\widetilde{\mathcal{E}}_1(\mathbb{F}_{4993})=2^5\cdot 3\cdot 53$. The reduction of the point $2^5\cdot 3\,R_1$ is the point $\widetilde{R}_1'=2^5\cdot 3\,\widetilde{R}_1=(2585,2705)$ which is of order 53 and the reduction of the point $2^5\cdot 3\,R_2$ is the point $\widetilde{R}_2'=2^5\cdot 3\,\widetilde{R}_2=(1055,2466)=19\,\widetilde{R}_1'$.

$p=5881$

Take 1098 as a square root of -1 mod 5881, 1451 as a square root of 3 mod 5881 (hence $j\equiv 5604 \mod 5881$), 497 as a square root of 7 mod 5881, 5077 as a square root of $3-497$ mod 5881 (hence

$s \equiv 3218 \bmod 5881$) and 357 as a cubic root of $-24 \cdot 3218^3 + 51 \cdot 3218^2 + 636 \cdot 3218 + 794 \bmod 5881$.
The reduction $\widetilde{\mathcal{E}}_1$ of the elliptic curve is defined by $y^2 = x^3 + 3903x^2 + 3442x + 3400$, and $\#\widetilde{\mathcal{E}}_1(\mathbb{F}_{5881}) = 2^4 \cdot 7 \cdot 53$. The reduction of the point $2^4 \cdot 7\, R_1$ is the point $\widetilde{R}_1' = 2^4 \cdot 7\, \widetilde{R}_1 = (5649, 3306)$ which has order 53 and the reduction of the point $2^4 \cdot 7\, R_2$ is the point $\widetilde{R}_2' = 2^4 \cdot 7\, \widetilde{R}_2 = (2510, 4342)$ which is equal to $25\, \widetilde{R}_1'$.

The lemma 3.9 applied to $P = 2^5 \cdot 3 \cdot 7R_1$, $Q = 2^5 \cdot 3 \cdot 7R_2$, $l = 53$, $\mathfrak{p}_1$ a suitable prime above 4993, $\mathfrak{p}_2$ a suitable prime above 5881, $a_1 = 19$ and $a_2 = 25$ gives the result. ∎

Lemma 3.9. *Let P and Q be two K-rational points on an elliptic curve. Suppose there exists two places of good reduction $\mathfrak{p}_1$ and $\mathfrak{p}_2$ and a prime l such that the reductions $\widetilde{P}$ and $\widetilde{Q}$ are of order l, and $\widetilde{Q} \equiv a_i \widetilde{P} \bmod \mathfrak{p}_i$ with $a_1 \not\equiv a_2 \bmod l$. If moreover, there are no K-rational point of order l, then P and Q are $\mathbb{Z} -$ independent.*

Proof: Suppose there were a relation $mP + nQ = 0$, that we choose minimal amongst such relations. Looking at the reductions, we get that $m\widetilde{P} + n\widetilde{Q} \equiv (m + na_i)\widetilde{P} \equiv 0 \bmod \mathfrak{p}_i$, hence $m + na_i \equiv 0 \bmod l$ i.e. $m \equiv n \equiv 0 \bmod l$, which means that there should be a M-rational point of order l (i.e. $m/lP + n/lQ$), which is not the case. ∎

3.3.2 Images of the Weierstrass points on $\mathcal{E}_2$

Recall that the orbits under the action of σ are:
$\{P_2, P_5\}$, $\{P_4, P_7\}$ $\{P_3, P_6\}$ $\{P_8, P_9\}$, $\{Q_1, Q_5\}$, $\{Q_2, Q_4\}$ and $\{Q_3, Q_6\}$, the point P_1 being fixed. Thus the images of the Weierstrass points are the same distinguished points on the elliptic curve with

$$A = \phi_2(\{P_5, P_2\}), \quad C = \phi_2(\{P_3, P_6\}), \quad B = \phi_2(\{P_4, P_7\}),$$
$$D = \phi_2(\{P_8, P_9\}), \quad R_1 = \phi_2(\{Q_3, Q_6\}), \quad R_2 = \phi_2(\{Q_1, Q_5\}),$$
$$R_3 = \phi_2(\{Q_2, Q_4\}), \quad \text{and} \quad \mathcal{O} = \phi_2(P_1).$$

3.3.3 Images of the Weierstrass points on $\mathcal{E}_3$

Recall that the orbits under the action of τ are: $\{P_1, P_2, P_5\}$, $\{P_3, P_7, P_9\}$, $\{P_4, P_6, P_8\}$, $\{Q_1, Q_2, Q_3\}$ and $\{Q_4, Q_5, Q_6\}$. The images of the Weierstrass points by ϕ_3 are thus the following five points

$$A = \phi_3(\{P_1, P_2, P_5\}), \quad B = \phi_3(\{P_4, P_6, P_8\}), \quad C = \phi_3(\{Q_1, Q_2, Q_3\}),$$
$$D = \phi_3(\{Q_4, Q_5, Q_6\}), \quad \text{and} \quad \phi_3(\{P_3, P_7, P_9\}) = \mathcal{O}.$$

These points satisfy the following relations on the elliptic curve $\mathcal{E}_3$:

$$2A = B, \quad 2B = \mathcal{O}, \quad \text{and} \quad C + D = B.$$

Lemma 3.10. *The point C is of infinite order.*

Proof: For a prime of residue class degree 1 in in $\mathbb{Q}(i, \sqrt{3}, \sqrt{7}, s)$, one can compute the reduction $\mathcal{E}_3$ of the elliptic curve. For $p = 37$, the reduction $\widetilde{\mathcal{E}_3}$ of the elliptic curve is given by $y^2 = x^3 + 32x + 23$, and the reduction of the point C is the point $\widetilde{C} = (34, 14)$ which has order 11. For $p = 109$, the reduction $\widetilde{\mathcal{E}'_3}$ of the elliptic curve is given by $y^2 = x^3 + 80x + 34$ and the reduction of the point C is the point $\widetilde{C} = (24, 54)$ which is of order 60. Hence the point C is of infinite order. ∎

3.4 Proof of theorem 3.1

In order to see if there exist extra relations between the Weierstrass points, we will determine which elements of W are in the kernel of the isogeny from J to the product of the three elliptic curves. Indeed, if a divisor with support in the set of Weierstrass points is in this kernel, it is either already zero in the Jacobian (and thus there exists an extra relation between the Weierstrass points) or it is nonzero in the Jacobian.

Consider a degree zero divisor with support in the set of Weierstrass points, say $m_1P_1 + m_2P_2 + m_3P_3 + m_5P_5 + m_6P_6 + m_8P_8 + n_1Q_1 + n_2Q_2 + n_3Q_3 + n_4Q_4 + n_5Q_5 + n_6Q_6$ with m_2 such that $\sum m_i + \sum n_i = 0$. Assume that this divisor is in the kernel of the isogeny to the product of the three elliptic curves. We compute the images of this divisor on each of the elliptic factor of the Jacobian.

On the first factor of the Jacobian $\mathcal{E}_1$, we get the following relation $(m_1+m_5)A+(m_3+m_8)B+m_6D+(n_1+n_4)R_1+(n_2+n_6)R_2+(n_3+n_5)R_3 = \mathcal{O}$, which implies (using the relations between the points on the elliptic curve) that $m_1+m_5-m_6-2n_3-2n_5 \equiv 0 \bmod 4$, $m_3+m_8 \equiv 0 \bmod 4$ and $n_1+n_4 = n_2 + n_6 = n_3 + n_5$.

On the second factor $\mathcal{E}_2$, we get the following relation $(m_2 + m_5)A + (m_3 + m_6)C + m_8D + (n_3 + n_6)R_1 + (n_1 + n_5)R_2 + (n_2 + n_4)R_3 = \mathcal{O}$, which implies (using the relations between the points on the elliptic curve) that

$m_2+m_5-m_3-m_6-m_8-2n_2-2n_4 \equiv 0 \bmod 4$, $m_3+m_6 \equiv 0 \bmod 4$ and $n_1+n_5=n_3+n_6=n_2+n_4$.

On the third factor $\mathcal{E}_3$, we get the following relation $(m_1+m_2+m_5)A+(m_6+m_8)B+(n_1+n_2+n_3)C+(n_4+n_5+n_6)D=\mathcal{O}$, which implies (using the relations between the points on the elliptic curve) that $m_1+m_2+m_5+2m_6+2m_8+2n_4+2n_5+2n_6 \equiv 0 \bmod 4$ and $n_1+n_2+n_3=n_4+n_5+n_6$.

The coefficients thus satisfy

$$n_1=n_2=n_3=n_4=n_5=n_6, \quad m_3 \equiv m_6 \equiv m_8 \equiv 0 \bmod 4,$$
$$m_1 \equiv -m_5 \equiv 2n_1 \bmod 4.$$

The only degree zero divisors with support in the set of Weierstrass points that are in the kernel of the isogeny are $2P_1-2P_5+Q_1+Q_2+Q_3+Q_4+Q_5+Q_6-6P_2$ and its multiples. We still have to show whether (or not) this divisor is zero in the Jacobian, which corresponds to the existence (or not) of a cubic curve tangent to the curve at the three points P_1, P_2 and P_5 and passing through the six Weierstrass points of weight one. Such a curve exists as we will see in the next proposition.

Proposition 3.11. *The cubic curve given by the affine equation* $35x^3+9x^3\sqrt{7}-33xy-9xy\sqrt{7}+1+y^3=0$ *meets the curve* $\mathcal{C}$ *at* 2 P_1, 2 P_2, $2P_5$, Q_1, Q_2, Q_3, Q_4, Q_5 *and* Q_6.

Proof: It is a straightforward computation. ∎

4 Family with eight hyperflexes

There is a one-dimensional family of curves with eight hyperflexes [12]. We show that

Theorem 4.1. *Let* $Z_{1,t}$ *be the smooth projective curve birational to the affine curve* $(t^2+1)(x^2-y)^2-y(2x-y-1)(2tx-y-t^2)=0$ *where* $t \notin \{0,1,-1,3,\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2}\}$. *For any number field* K, *there is a finite set* S_K *such that for each* $t \in K \setminus S_K$ *we have* $W_{Z_{1,t}} \cong \mathbb{Z}^5 \times (\mathbb{Z}/4\mathbb{Z})^4$. *For instance,* $t=2/5$ *is not in* S_K.

For the rest of the section, we will write $\mathcal{C}$ for the curve $Z_{1,t}$.

4.1 Weierstrass points

4.1.1 Weierstrass points of weight two

This curve possess eight hyperflexes, which are:
$P_1=(0:0:1)$, $P_2=(0:1:0)$, $P_3=(0:it:1)$, $P_4=(0:-it:1)$,

$P_5 = (1 : 1 : 1)$, $P_6 = (t : t^2 : 1)$, $P_7 = ((1+i)t : t(it+1) : t+i)$ and $P_8 = ((1-i)t : t(1-it) : t-i)$.

These eight points are in a particular configuration: the points P_1, P_2, P_3 and P_4 are lying on a line and so are the points P_5, P_6, P_7 and P_8; moreover, there exist conics tangent to the curve at the 4 points $\{P_1, P_2, P_5, P_6\}$, $\{P_1, P_2, P_7, P_8\}$, $\{P_3, P_4, P_5, P_6\}$ or $\{P_3, P_4, P_7, P_8\}$.

4.1.2 Weierstrass points of weight one

In order to compute all the Weierstrass points, we will work with another model for the curve.
The curve $\mathcal{C}$ is isomorphic to the curve $\mathcal{C}'$ given by the equation

$$\begin{aligned} t^4(t-1)^2X^4 &+ 2t(t-1)(3t^2-2t+1)X^2Y^2 \\ &+ 4t^3(1-t^2)X^2YZ + 2t^3(t^2-1)X^2Z^2 + (t^2+1)Y^4 \\ &- 4t^3(t^2+1)Y^3Z + 2t(5t^2+1)Y^2Z^2 - 8t^3YZ^3 + 2t^3Z^4 = 0. \end{aligned}$$

The map from $\mathcal{C}$ to $\mathcal{C}'$ is given by

$$(X : Y : Z) \mapsto (2tX - Y - Zt : -(2X - Y - Zt)t : -2tX + Y + 2t^2Z - Zt),$$

and the map from $\mathcal{C}'$ to $\mathcal{C}$ is given by

$$(X : Y : Z) \mapsto (tX + Y : tX + 2tY - Zt : X + Z).$$

Notation. We denote by P' the point on $\mathcal{C}'$ corresponding to the point P on $\mathcal{C}$.

If $t = 2(s-1)(s+1)/(2s-1)(2s+1)$, we can express the ordinary flexes in the following way $Q'_1 = (x_1, y_1)$, $Q'_2 = (x_2, y_2)$, $Q'_3 = (x_3, y_3)$, $Q'_4 = (x_4, y_4)$, $Q'_5 = (-x_1, y_1)$, $Q'_6 = (-x_2, y_2)$, $Q'_7 = (-x_3, y_3)$ and $Q'_8 = (-x_4, y_4)$, where

$$\left\{\begin{array}{lcl} x_1 &=& \dfrac{b(s)(c(s)(1+2s^2) - 2\,ia(s)(s^2-1))(2\,s+1)}{8\,s^5 - 4\,s^3 + 6\,s^2 + 2\,s - 3}, \\ x_2 &=& \dfrac{b(s)(c(s)(1+2s^2) + 2\,ia(s)(s^2-1))(2\,s+1)}{8\,s^5 - 4\,s^3 + 6\,s^2 + 2\,s - 3}, \\ x_3 &=& \dfrac{a(s)(c(s)(1+2s^2) - 2\,ib(s)(s^2-1))(2\,s-1)}{8\,s^5 - 4\,s^3 - 6\,s^2 + 2\,s + 3}, \\ x_4 &=& \dfrac{a(s)(c(s)(1+2s^2) + 2\,ib(s)(s^2-1))(2\,s-1)}{8\,s^5 - 4\,s^3 - 6\,s^2 + 2\,s + 3}, \end{array}\right.$$

and

$$\begin{cases} y_1 &= 2\,\dfrac{(4\,s^4-4\,s^3-2\,s^2+4\,s-2+ia(s)c(s)(1+2s^2))(s^2-1)}{(2\,s-1)(8\,s^5-4\,s^3+6\,s^2+2\,s-3)}, \\ y_2 &= 2\,\dfrac{(4\,s^4-4\,s^3-2\,s^2+4\,s-2-ia(s)c(s)(1+2s^2))(s^2-1)}{(2\,s-1)(8\,s^5-4\,s^3+6\,s^2+2\,s-3)}, \\ y_3 &= 2\,\dfrac{(4\,s^4+4\,s^3-2\,s^2-4\,s-2+ib(s)c(s)(1+2s^2))(s^2-1)}{(2\,s+1)(8\,s^5-4\,s^3-6\,s^2+2\,s+3)}, \\ y_4 &= 2\,\dfrac{(4\,s^4+4\,s^3-2\,s^2-4\,s-2-ib(s)c(s)(1+2s^2))(s^2-1)}{(2\,s+1)(8\,s^5-4\,s^3-6\,s^2+2\,s+3)}, \end{cases}$$

with $a(s)=\sqrt{2\,s^2-2\,s+1}$, $b(s)=\sqrt{2\,s^2+2\,s+1}$ and $c(s)=\sqrt{2\,s^2-1}$.

The hyperflexes are then $P'_1=(-1:t:2t-1)$, $P'_2=(-1:t:1)$, $P'_3=(-i-1:(i+1)t:2t+i-1)$, $P'_4=(i-1:(-i+1)t:2t-i-1)$, $P'_5=(1:t:2t-1)$, $P'_6=(1:t:1)$, $P'_7=(i+1:(i+1)t:2t+i-1)$ and $P'_8=(-i+1:(-i+1)t:2t-i-1)$.

4.1.3 First relations between the Weierstrass points

Convention. From now on, we take P_1 as base-point for the Abel-Jacobi map and we will write P for the image $[P-P_1]$ of P under $\jmath$.

There exist relations between the Weierstrass points arising from lines or conics passing through certain of these points. More precisely, we have

Proposition 4.2. *The Weierstrass points satisfy the following relations:*

- $P_1+P_2+P_3+P_4=0$,
- $P_5+P_6+P_7+P_8=0$,
- $4P_j=0$,
- $Q_1+Q_2+Q_3+Q_4+Q_5+Q_6+Q_7+Q_8=0$,
- $P_3+P_4+P_5+P_6+Q_8+Q_1+Q_6+Q_3=0$,
- $P_1+P_2+P_5+P_6+Q_1+Q_2+Q_5+Q_6=0$.

Proof: We can prove these relations either for the points on $\mathcal{C}$ or for the points on $\mathcal{C}'$. The four first relations come are consequences of the fact that the hyperflexes lie on two lines and that the base-point is a hyperflex (see the remark at the end of section 1.3). For the two remainings relations, we consider the Weierstrass points on the model $\mathcal{C}'$: the family of conics passing through P'_3, P'_4, P'_5 and P'_6 is given by

$$X^2=\frac{\lambda(1+2s^2)^2XY}{2(s^2-1)(4s^2-1)}-\frac{(4(\lambda-4)s^4+8(1-\lambda)s^2+4\lambda-1)Y^2}{4(s^2-1)^2}+\lambda(2Y-Z)$$

and $\lambda = -\dfrac{(2\,s+1)^2(2\,s-1)^2(2\,s^2+ia(s)b(s)-1)}{(4\,s^4-2\,s^2+1)(1+2\,s^2)}$ gives the result.
The conic passing through Q_1', Q_2', Q_5', Q_6' and P_1' is given by

$$\frac{s\left(1+2s^2\right)X^2}{(2s-1)\,(2s+1)^2} - \frac{\left(2s^2-2s-3\right)(2s-1)\,Y^2}{4\,(s+1)\,(s-1)^2} + Z\,(2Y-Z) = 0.$$

∎

Proposition 4.3. *The group W generated by the Weierstrass points is a quotient of $W_0 = (\mathbb{Z}/4\mathbb{Z})^4 \times \mathbb{Z}^5$.*

Proof: The statement follows from the preceeding remark and the following proposition. ∎

Proposition 4.4. *We have $P_5 - P_1 + P_2 - P_6 + 2P_3 - 2P_8 = 0$.*

Proof: Let us prove that for the curve $\mathcal{C}'$. The line through P_1' and P_5' (given by $(2t-1)Y - tZ = 0$) meets the curve at two other points R_1' and R_2' (of respective x-coordinates $\pm\sqrt{(4-3t)t}/(t(2t-1))$). The conic through P_2', $2\ P_3'$ and $2\ P_7'$ meets the curve at P_6', R_1' and R_2'; the equation of this conic is

$$t^3(t-1)X^2 - (t+i)(t+i-1)Y^2 + 2it(t+i)YZ + (1-i)t^2Z^2 = 0.$$

Hence $P_1' + P_5' + R_1' + R_2' = 0$ and $R_1' + R_2' + P_2' + P_6' + 2P_3' + 2P_7' = 0$. Since P_5', P_6', P_7' and P_8' lie on a line, we have the desired result. ∎

We will show that there is no more relations between the generators of W. In order to do so, we will compute the group W_{t_0} for a suitable specialization and show that $W_{t_0} = W_0$. Then, we will apply Silverman's theorem 2.2 to conclude.

4.2 Structure of the Jacobian

We show that the Jacobian is isogeneous to the product of three elliptic curves, that we determine.

Proposition 4.5. *The Jacobian is isogeneous to the product of three elliptic curves.*

Proof: If we consider the pullbacks of differential forms on the $\mathcal{D}_i$, we show that they are independent. For the definitions of both the curves and the maps, see section 4.2.2 below. The differential forms on the $\mathcal{D}_i$ are respectively equal to

$$\omega_1 = \frac{dy_1}{x_1}, \qquad \omega_2 = \frac{dy_2}{x_2} \qquad \text{and} \qquad \omega_3 = \frac{dx_3}{z_3}.$$

A basis of the differential forms on $\mathcal{C}$ is given by ω_0, $x\omega_0$ and $y\omega_0$ where

$$\omega_0 = \frac{dy}{2\,(1+t^2)\,x^3 - 2\,(t+1)^2\,yx + (t+1)\,y^2 + (t+1)\,t\,y}.$$

we obtain that

$$\begin{aligned} \psi_1^*(\omega_1) &= c_1(y + t - 2tx)\,\omega_0, \\ \psi_2^*(\omega_2) &= c_2(y + t + (i-1)(t+i)x)\,\omega_0 \\ \text{and} \qquad \psi_3^*(\omega_3) &= c_3(y - t)\,\omega_0 \end{aligned}$$

where the c_i are constants. We see that these differential forms are independent. ∎

4.2.1 Automorphisms of the curve

The group of automorphisms of this curve is a dihedral group of order 8 (see [12]) generated by the two involutions whose action on the Weierstrass points is the following

$$\begin{aligned} \sigma &= (P_1P_5)(P_2P_6)(P_3P_7)(P_4P_8)(Q_1Q_5)(Q_2Q_6)(Q_3Q_7)(Q_4Q_8) \\ \text{and} \quad \tau &= (P_1P_7)(P_2P_8)(P_3P_6)(P_4P_5)(Q_1Q_8)(Q_2Q_4)(Q_3Q_6)(Q_5Q_7). \end{aligned}$$

The automorphism σ is given by

$$(X:Y:Z) \mapsto \Big(-t((t+1)X - Y - Zt) : t^2(-2X + Y + Z) : t^2Z - 2tX + Y\Big).$$

The automorphism τ is given by

$$\begin{aligned} (X:Y:Z) \mapsto \Big(&-2\,(t+1)tX + 2tY + 2t^2Z : \\ &- 2\,(t^2+1)tX + (t+i)(1-i)tY + (t-i)(1+i)t^2Z : \\ &-2\,(t^2+1)X + (t-i)(1+i)Y + (t+i)(1-i)tZ\Big). \end{aligned}$$

Finally, the automorphism $\rho = \sigma\tau$ is given by

$$\begin{aligned} (X:Y:Z) \mapsto \Big(&2\,tX : (2\,(t+1)X - t(1+i)Z + (i-1)Y)t : \\ &2\,(t+1)X - t(1-i)Z - (i+1)Y\Big). \end{aligned}$$

4.2.2 Elliptic factors of the Jacobian

For each of these automorphisms, we obtain a map to an elliptic curve by identifying points which are in the same orbit.

Proposition 4.6. *The morphism ϕ_1 of degree 2 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_1 = \mathcal{C}/\langle\sigma\rangle$ can be described as*

$$(x,y) \mapsto \left(u = \frac{g_1(x,y)}{(x-y)^2}, v = \frac{g_1(x,y)(x-t)}{(x-y)^3}\right)$$

with $g_1(x,y) = (t^2+1)(x-y)^2 + (x-t)^2 + t^2(x^2-y)$, writing $\mathcal{E}_1$ as

$$v^2 = u^3 - (2t^2+1)\,u^2 + (1+t^2)t^2\,u.$$

Proof: Both

$$X_1 = -\frac{(2tx-y-t)^2}{(2tx-y-2t^2+t)^2}$$

and

$$Y_1 = 2\frac{(2x-y-t)t}{(2tx-y-2t^2+t)}$$

are invariant by σ, hence a map from $\mathcal{C}$ to the curve $\mathcal{D}_1$ given by

$$\begin{aligned}16t^6(t-1)^2{x_1}^2 + (-8t^4+12t^3-9t^2+4t-1){y_1}^4 \\ + 8t^2(2t^3+t^2-2t+1){y_1}^3 - 8t^2(2t^4+2t^3+3t^2-2t+1){y_1}^2 \\ + 32t^4(1+t^2)y_1 - 16t^4(1+t^2) = 0.\end{aligned}$$

The map ψ_1 from $\mathcal{C}$ to $\mathcal{D}_1$ is given by

$$(x,y) \mapsto \left(X_1 - \frac{\left(3\,t^2-2\,t+1\right)Y_1{}^2}{4t^3\,(t-1)} + \frac{(t+1)\,Y_1}{t\,(t-1)} - \frac{t+1}{t\,(t-1)}, Y_1\right).$$

After some transformation, we obtain the elliptic curve $\mathcal{E}_1$ given by the equation $v^2 = u^3 - (2t^2+1)u^2 + (1+t^2)t^2u$, the map from $\mathcal{D}_1$ to $\mathcal{E}_1$ being

$$(x_1,y_1) \mapsto \left(-\frac{h_1(x_1,y_1)}{((2t-1)\,y_1-2\,t)^2}, \frac{h_1(x_1,y_1)(y_1-2t)}{((2t-1)\,y_1-2\,t)^3}\right),$$

where

$$\begin{aligned}h_1(x_1,y_1) = (4t^3-4t^4-3t^2+2\,t-1){y_1}^2 + 4t^2(2t^2-t+1)y_1 \\ - 4t^2(t^2+1) + 4t^3(t-1)x_1.\end{aligned}$$

∎

Proposition 4.7. *The morphism ϕ_2 of degree 2 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_2 = \mathcal{C}/\langle\tau\rangle$ can be described as $(x,y) \mapsto (u,v)$ with*

$$u = \frac{g_2(x,y)}{((i-1)y+(t-i)x)^2}, v = \frac{(1+2i)g_2(x,y)(it-t+tx-ix)(t-i)}{((i-1)y+(t-i)x)^3}$$

and

$$\begin{aligned} g_2(x,y) = (8+6i)\,t\,\big(&t\,(t-i)^2 - (1+i)(t-i)^3x + i(t+i)(t-i)y \\ &-4\,iy^2 + 4(t-i)^2x^2 + 4(i-1)(t-i)xy\big) \end{aligned}$$

writing $\mathcal{E}_2$ as

$$v^2 = u^3 + (4i-3)(t^2+6it-1)\,u^2 + (96-28i)t(i+t)^2\,u.$$

Proof: Both

$$X_2 = -4\frac{((t+i)(1+i)x - i(y+t))^2t^2}{(2ix(1+t^2)+y(t-i)(1-i)-it^2+3t-3t^2-it)^2}$$

and

$$Y_2 = 4\frac{((-t+i)(1-i)x - i(y+t))t}{(2ix(1+t^2)+y(t-i)(1-i)-it^2+3t-3t^2-it)}$$

are τ-invariant.
We thus obtain a degree 2 map ψ_2 from $\mathcal{C}$ to a genus 1 curve $\mathcal{D}_2$ given by $(x,y) \mapsto (X_2', Y_2)$ with

$$X_2' = X_2 - \frac{\left(t^2-2t+2it-i\right){Y_2}^2}{2\,(i+t)\,(t-1)} - \frac{2it^2\,(t+1)}{(t^2+1)\,(t-1)} + \frac{(1+i)\,t\,(t+1)\,Y_2}{(t-i)\,(t-1)},$$

the curve $\mathcal{D}_2$ being

$$\begin{aligned} 8\,(t-1)^2(1+t^2)^2{x_2}^2 + 64\,t^5 + 64(i-1)t^4(t+i)y_2 \\ -16\,it^2(t^4+t^3+6\,it^2-t-1){y_2}^2 \\ +(8+8\,i)t\,(t^3+(i-1)t^2+(i-1)t-i)(t+i)(t-i){y_2}^3 \\ -(t^2+(3i-2)\,t-2\,i)(2\,t^2+(2i-3)\,t-i)(t-i)^2{y_2}^4 = 0. \end{aligned}$$

After transformation, we obtain the elliptic curve $\mathcal{E}_2$ given by the equation

$$v^2 = u^3 - (3-4i)(t^2+6it-1)u^2 - (-96+28i)t(i+t)^2u,$$

the map from $\mathcal{D}_2$ to $\mathcal{E}_2$ being $(x_2, y_2) \mapsto (u, v)$ with

$$u = \frac{h_2(x_2, y_2)}{((5t + 3i - 4)\, y_2 - 2t(3i + 1))^2},$$
$$v = 5\, \frac{h_2(x_2, y_2)\,(2t(i - 1) + (t - i)\, y_2)\,(t - i)}{((5t + 3i - 4)\, y_2 - 2t(3i + 1))^3}$$

and

$$\begin{aligned} h_2(x_2, y_2) = {} & 50(1 - i)(2\,(t + i)(t - 1)(t - i)^2 x_2 - 8(1 + i)t^3 \\ & + (6\,it^3 - 9\,t^2 + 6\,t + i - 9\,it^2 + t^4){y_2}^2 \\ & - 2(1 + i)t(t^2 - 3\,t + 3\,it - i)(t + i)y_2). \end{aligned}$$

∎

Proposition 4.8. *The morphism ϕ_3 of degree 2 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_3 = \mathcal{C}/\langle\rho^2\rangle$ can be described as*

$$(x, y) \mapsto \left(u = \frac{g_3(x, y)}{x^2}, v = -\frac{g_3(x, y)((t + 1)x - y - t)}{x^3}\right)$$

with $g_3(x, y) = (t - (t + 1)\,x)^2 + (y - (t + 1)\,x)^2$, writing $\mathcal{E}_3$ as

$$v^2 = u^3 - (t + 1)^2\, u^2 + 2t(1 + t^2)\, u.$$

Proof: The action of ρ^2 is $(x, y, z) \mapsto (tx, t^2 z, y)$.
Both $X_3 = 4\dfrac{xt}{y + t}$ and $Z_3 = -\dfrac{(y - t)^2}{(y + t)^2}$ are ρ^2-invariant, hence a map ψ_3 from $\mathcal{C}$ to the curve $\mathcal{D}_3$ whose equation is

$$\begin{aligned} -64\,{z_3}^2 t^4 + (t^4 + 2\,t^3 + 6\,t^2 + 2\,t + 1){x_3}^4 - 8\,t\,(t + 1)^3 {x_3}^3 \\ +32\,t^2 (t + 1)^2 {x_3}^2 - 64\,t^3 (t + 1)x_3 + 64\,t^4 = 0, \end{aligned}$$

the map ψ_3 being

$$(x, y) \mapsto \left(X_3, Z_3 - \frac{(t + 1)^2 {X_3}^2}{8t^2} + \frac{(t + 1)X_3}{2t}\right).$$

After some transformation, we obtain the elliptic curve $\mathcal{E}_3$ given by the equation $v^2 = u^3 - (t + 1)^2 u^2 + 2(1 + t^2)tu$, the map from $\mathcal{D}_3$ to $\mathcal{E}_3$ being

$$(x_3, z_3) \mapsto \left(\frac{h_3(x_3, z_3)}{{x_3}^2}, -\frac{h_3(x_3, z_3)\,((t + 1)x_3 - 4\,t)}{{x_3}^3}\right)$$

where $h_3(x_3, z_3) = x_3^2 (t + 1)^2 - 4x_3 t(t + 1) + 8t^2(1 - z_3)$. ∎

4.3 Images of the Weierstrass points on the elliptic factors of the Jacobian

The Jacobian is isogenous to the product of three elliptic curves. Computing the images of the hyperflexes on each of these elliptic factors will give us some relations between these hyperflexes.

4.3.1 Images on the first elliptic curve

The first elliptic curve is given by the equation

$$y^2 = x^3 - (2t^2+1)x^2 + (t^4+t^2)x.$$

The images of the Weierstrass points are
$P_{1,1} = \phi_1(\{P_1, P_5\}) = (0:1:0)$
$P_{1,2} = \phi_1(\{P_2, P_6\}) = (t^2+1:0:1)$
$P_{1,3} = \phi_1(\{P_3, P_7\}) = (t^2+it:-it^2+t:1)$
$P_{1,4} = \phi_1(\{P_4, P_8\}) = (t^2-it:it^2+t:1)$.
We have the following relation $P_{1,3} + P_{1,4} = P_{1,2}$.

4.3.2 Images on the second elliptic curve

The second elliptic curve is given by the equation

$$y^2 = x^3 + (-3+4i)(t^2+6it-1)x^2 + (96-28i)\,t\,(i+t)^2 x.$$

The images of the Weierstrass points are
$P_{2,1} = \phi_2(\{P_1, P_7\}) = (0:1:0)$
$P_{2,2} = \phi_2(\{P_2, P_8\}) = ((12i+16)t:0:1)$
$P_{2,3} = \phi_2(\{P_3, P_6\}) = ((6i+8)t+8i-6:(4i+22)t^2+4i+22:1)$
$P_{2,4} = \phi_2(\{P_4, P_5\}) = ((-8i+6)t^2+(6i+8)t:(22i-4)t^3+(22i-4)t:1)$.
We have the following relation $P_{2,3} + P_{2,4} = P_{2,2}$.

4.3.3 Images on the third elliptic curve

The third elliptic curve is given by the equation

$$y^2 = x^3 - (t+1)^2x^2 + 2t(t+1)x.$$

The images of the Weierstrass points are
$P_{3,1} = \phi_3(\{P_1, P_2\}) = (0:1:0)$
$P_{3,3} = \phi_3(\{P_3, P_4\}) = (0:0:1)$
$P_{3,5} = \phi_3(\{P_5, P_6\}) = (t^2+1:0:1)$
$P_{3,7} = \phi_3(\{P_7, P_8\}) = (2t:0:1)$.

4.4 Specialization at $t = 2/5$

We will show that for a suitable specialization, the group generated by the Weierstrass points is equal to W_0.

Theorem 4.9. *For the specialization $t = 2/5$, the group generated by the Weierstrass points is $W_{\mathcal{C}_{2/5}} = (\mathbb{Z}/4\mathbb{Z})^4 \times \mathbb{Z}^5$.*

The curve $\mathcal{C}_{2/5}$ has the following equation

$$29X^4 - 98X^2YZ + 28YZ^2X + 70Y^2ZX - 25Y^3Z - 4Z^3Y = 0,$$

and the hyperflexes are $P_1 = (0 : 0 : 1)$, $P_2 = (0 : 1 : 0)$, $P_3 = (0 : 2i : 5)$, $P_4 = (0 : -2i : 5)$, $P_5 = (1 : 1 : 1)$, $P_6 = (10 : 4 : 25)$, $P_7 = (5(-6i + 14) : (-42i + 40) : 145)$ and $P_8 = (5(6i + 14) : (42i + 40) : 145)$.

The map from $\mathcal{C}_{2/5}$ to $\mathcal{C}'_{2/5}$ is given by

$$(X : Y : Z) \mapsto (-20X + 25Y + 10Z : 20X - 10Y - 4Z : 20X - 25Y + 2Z),$$

and the map from $\mathcal{C}'_{2/5}$ to $\mathcal{C}_{2/5}$ is given by

$$(X : Y : Z) \mapsto (2X + 5Y : 2X + 4Y - 2Z : 5X + 5Z).$$

The curve $\mathcal{C}'_{2/5}$ has the following equation

$$144X^4 - 5100X^2Y^2 + 3360X^2YZ - 1680X^2Z^2 + 18125Y^4 - \\ 29000Y^3Z + 22500Y^2Z^2 - 8000YZ^3 + 2000Z^4 = 0.$$

The Weierstrass points on $\mathcal{C}'_{2/5}$ have the following coordinates:
$P'_1 = (5 : -2 : 1)$, $P'_2 = (-5 : 2 : 5)$, $P'_3 = (15i - 10 : -6i + 4 : 13)$, $P'_4 = (-15i - 10 : 6i + 4 : 13)$, $P'_5 = (-5 : -2 : 1)$, $P'_6 = (5 : 2 : 5)$, $P'_7 = (-15i + 10 : -6i + 4 : 13)$ and $P'_8 = (15i + 10 : 6i + 4 : 13)$.
$Q'_1 = ((3\sqrt{35} - 10i)\sqrt{65} : 6i\sqrt{35} + 20 : 83)$,
$Q'_2 = ((3\sqrt{35} + 10i)\sqrt{65} : -6i\sqrt{35} + 20 : 83)$,
$Q'_3 = (-2i\sqrt{65} + 3\sqrt{35} : 6/25i\sqrt{35}\sqrt{65} + 52/5 : 23)$ and
$Q'_4 = (2i\sqrt{65} + 3\sqrt{35} : -6/25i\sqrt{35}\sqrt{65} + 52/5 : 23)$.

4.4.1 Images of the Weierstrass points on the first elliptic curve

The first elliptic curve has a minimal model $\mathcal{E}'_1$ given by

$$y^2 = x^3 - 247x - 1386.$$

The map φ_1 from $\mathcal{C}'_{2/5}$ to $\mathcal{E}'_1$ is $(X:Y:Z) \mapsto (u,v)$ where

$$\begin{cases} u = -\dfrac{(24X^2 - 743Y^2 + 508YZ - 212Z^2)}{(Y+2Z)^2} \\ v = -10\,\dfrac{(5Y-2Z)(12X^2 - 377Y^2 + 232YZ - 128Z^2)}{(Y+2Z)^3}. \end{cases}$$

The images of the Weierstrass points are

$$P_{1,1} = \varphi_1(\{P'_1, P'_5\}), \quad P_{1,2} = \varphi_1(\{P'_2, P'_6\}), \quad P_{1,3} = \varphi_1(\{P'_3, P'_7\}),$$
$$P_{1,4} = \varphi_1(\{P'_4, P'_8\}), \quad Q_{1,1} = \varphi_1(\{Q'_1, Q'_5\}), \quad Q_{1,2} = \varphi_1(\{Q'_2, Q'_6\}),$$
$$Q_{1,3} = \varphi_1(\{Q'_3, Q'_7\}), \quad \text{and} \quad Q_{1,4} = \varphi_1(\{Q'_4, Q'_8\}).$$

They satisfy the following relations:

$$2P_{1,2} = P_{1,1} = \mathcal{O}, \quad P_{1,3} + P_{1,4} = Q_{1,1} + Q_{1,2} = Q_{1,3} + Q_{1,4} = P_{1,2}.$$

Lemma 4.10. *The points $Q_{1,1}$ and $Q_{1,3}$ are of infinite order and independent.*

Proof: Since $\#\widetilde{\mathcal{E}'_1}(\mathbb{F}_{97}) = 2^3 \cdot 11$ and $\#\widetilde{\mathcal{E}'_1}(\mathbb{F}_{389}) = 2^4 \cdot 23$, the only points of finite order in $\mathcal{E}'_1(M)$ are of order 2, 4 or 8 which is not the case of either $Q_{1,1}$ and $Q_{1,3}$.

$p = 389$

Take 274 as a square root of -1 mod 389, 206 as a square root of 35 mod 389 and as 125 as a square root of 65 mod 389. The reduction $\widetilde{\mathcal{E}'_1}$ of the elliptic curve is defined by $y^2 = x^3 + 142x + 170$, and we have $\#\widetilde{\mathcal{E}'_1}(\mathbb{F}_{389}) = 2^4 \cdot 23$.
The reduction of the point $16\,Q_{1,1}$ is the point $\widetilde{Q}'_{1,1} = 16\,\widetilde{Q}_{1,1} = (362, 185)$, which is of order 23 and the reduction of the point $16\,Q_{1,3}$ is the point $\widetilde{Q}'_{1,3} = 16\,\widetilde{Q}_{1,3} = (168, 145)$, which is equal to $12\,\widetilde{Q}'_{1,1}$.

$p = 353$

Take 42 as a square root of -1 mod 353, 68 as a square root of 35 mod 353 and as 154 as a square root of 65 mod 353. The reduction $\widetilde{\mathcal{E}'_1}$ of the elliptic curve is defined by $y^2 = x^3 + 106x + 26$, and we have $\#\widetilde{\mathcal{E}'_1}(\mathbb{F}_{353}) = 2^4 \cdot 23$.
The reduction of the point $16\,Q_{1,1}$ is the point $\widetilde{Q}'_{1,1} = 16\,\widetilde{Q}_{1,1} = (35, 108)$, which is of order 23 and the reduction of the point $16\,Q_{1,3}$ is the point $\widetilde{Q}'_{1,3} = 16\,\widetilde{Q}_{1,3} = (14, 148)$, which is equal to $14\,\widetilde{Q}'_{1,1}$.

Applying the lemma 3.9 to $P = 16\,Q_{1,1}$, $Q = 16\,Q_{1,3}$, $l = 23$, $\mathfrak{p}_1$ a suitable prime above 389, $\mathfrak{p}_2$ a suitable prime above 353, $a_1 = 12$ and $a_2 = 14$ gives the result. ∎

4.4.2 Images of the Weierstrass points on the second elliptic curve

The second elliptic curve has a minimal model $\mathcal{E}_2'$ given by the equation

$$y^2 = x^3 + 253x - 6286.$$

The map φ_2 from $\mathcal{C}_{2/5}'$ to $\mathcal{E}_2'$ is $(X : Y : Z) \mapsto (u, v)$ where

$$u = \frac{1}{(119+120i)(6X+5(i+2)Y+10(i-1)Z)^2}\Big(342732X^2 + 60(-6008i+20699)XY - 1680(i+239)XZ + 25(568i-178419)Y^2 + 200(4877i+23163)YZ - 200(4948i+11571)Z^2\Big),$$

$$v = 4\,\frac{(2671-10027i)(6X+5(5i-2)Y+10(-i+1)Z)}{13(119+120i)(6X+5(i+2)Y+10(i-1)Z)^3}\Big(780X^2 + 15(-16i+197)XY + 6(139i-188)XZ - 50(9i+137)Y^2 + 5(744i+1207)YZ - 10(327i+406)Z^2\Big).$$

The images of the Weierstrass points are

$$P_{2,1} = \varphi_2(\{P_1', P_7'\}),\quad P_{2,2} = \varphi_2(\{P_2', P_8'\}),\quad P_{2,3} = \varphi_2(\{P_3', P_6'\}),$$
$$P_{2,4} = \varphi_2(\{P_4', P_5'\}),\quad Q_{2,1} = \varphi_2(\{Q_1', Q_8'\}),\quad Q_{2,2} = \varphi_2(\{Q_2', Q_4'\}),$$
$$Q_{2,3} = \varphi_2(\{Q_3', Q_6'\}),\quad \text{and}\quad Q_{2,5} = \varphi_2(\{Q_5', Q_7'\}).$$

They satisfy the following relations:

$$2P_{2,2} = P_{2,1} = \mathcal{O},\quad P_{2,3} + P_{2,4} = Q_{2,1} + Q_{2,3} = Q_{2,2} + Q_{2,5} = P_{2,2}.$$

Lemma 4.11. *The points $Q_{2,1}$ and $Q_{2,5}$ are of infinite order and independent.*

Proof: Since $\#\widetilde{\mathcal{E}_2'}(\mathbb{F}_{73}) = 2^3 \cdot 9$ and $\#\widetilde{\mathcal{E}_2'}(\mathbb{F}_{97}) = 2^3 \cdot 11$, the only points of finite order in $\mathcal{E}_3(M)$ are of order 2, 4 or 8 which is not the case of either $Q_{2,1}$ and $Q_{2,5}$.

$p = 389$

Take 274 as a square root of -1 mod 389, 206 as a square root of 35 mod 389 and 125 as a square root of 65 mod 389. The reduction $\widetilde{\mathcal{E}}'_2$ of the elliptic curve is defined by $y^2 = x^3 + 253x + 327$, and we have $\#\widetilde{\mathcal{E}}'_2(\mathbb{F}_{389}) = 2^4 \cdot 23$.

The reduction of the point $16\,Q_{2,1}$ is the point $\widetilde{Q}'_{2,1} = 16\,\widetilde{Q}_{2,1} = (337, 156)$, which is of order 23 and the reduction of the point $16\,Q_{2,5}$ is the point $\widetilde{Q}'_{2,5} = 16\,\widetilde{Q}_{2,5} = (81, 222)$, which is equal to $20\,\widetilde{Q}'_{2,1}$.

$p = 353$

Take 42 as a square root of -1 mod 353, 68 as a square root of 35 mod 353 and 154 as a square root of mod 353. The reduction $\widetilde{\mathcal{E}}'_2$ of the elliptic curve is defined by $y^2 = x^3 + 253x + 68$, and we have $\#\widetilde{\mathcal{E}}'_2(\mathbb{F}_{353}) = 2^4 \cdot 23$.

The reduction of the point $16\,Q_{2,1}$ is the point $\widetilde{Q}'_{2,1} = 16\,\widetilde{Q}_{2,1} = (35, 308)$, which is of order 23 and the reduction of the point $16\,Q_{2,5}$ is the point $\widetilde{Q}'_{2,5} = 16\,\widetilde{Q}_{2,5} = (294, 73)$, which is equal to $10\,\widetilde{Q}'_{2,1}$.

Applying the lemma 3.9 to $P = 16\,Q_{2,1}$, $Q = 16\,Q_{2,5}$, $l = 23$, $\mathfrak{p}_1$ a suitable prime above 389, $\mathfrak{p}_2$ a suitable prime above 353, $a_1 = 20$ and $a_2 = 10$ gives the result. ∎

4.4.3 Images of the Weierstrass points on the third elliptic curve

The third elliptic curve has a minimal model $\mathcal{E}'_3$ given by the equation

$$y^2 = x^3 - x^2 - 220x + 832.$$

The map φ_3 from $\mathcal{C}'_{2/5}$ to $\mathcal{E}'_3$ is $(X : Y : Z) \mapsto (u, v)$ where

$$\begin{cases} u = -2\,\dfrac{(16X^2 - 40XY - 525Y^2 + 200YZ - 100Z^2)}{(2X+5Y)^2} \\ v = 6\,\dfrac{(2X - 5Y)(16X^2 + 200XY + 725Y^2 - 200YZ + 100Z^2)}{(2X+5Y)^3}. \end{cases}$$

The images of the Weierstrass points are

$$P_{3,1} = \varphi_3(\{P'_1, P'_2\}), \quad P_{3,3} = \varphi_3(\{P'_3, P'_4\}), \quad P_{3,5} = \varphi_3(\{P'_5, P'_6\}),$$
$$P_{3,7} = \varphi_3(\{P'_7, P'_8\}), \quad Q_{3,1} = \varphi_3(\{Q'_1, Q'_6\}), \quad Q_{3,5} = \varphi_3(\{Q'_2, Q'_5\}),$$
$$Q_{3,3} = \varphi_3(\{Q'_3, Q'_8\}), \quad \text{and} \quad Q_{3,4} = \varphi_3(\{Q'_4, Q'_7\}).$$

They satisfy the following relations:

$$Q_{3,1}+Q_{3,5}=P_{3,5}, \quad Q_{3,1}+Q_{3,3}=Q_{3,4}+Q_{3,5}=P_{3,7},$$
$$2P_{3,5}=2P_{3,7}=2P_{3,3}=P_{3,1}=\mathcal{O}.$$

Lemma 4.12. *The point $Q_{3,1}$ is of infinite order.*

Proof: Since $\#\widetilde{\mathcal{E}}_3'(\mathbb{F}_{577}) = 2^4 \cdot 139$ and $\#\widetilde{\mathcal{E}}_3'(\mathbb{F}_{97}) = 2^2 \cdot 5^2$ and since the point $Q_{3,1}$ is neither of order 2 nor of order 4, it is of infinite order. ∎

4.4.4 Proof of theorem 4.9

We will show that there exists no relation between the remaining ten Weierstrass points. Let us consider a degree zero divisor whose support is in the set of Weierstrass points, say $m_1P_1'+m_2P_2'+m_3P_3'+m_6P_6'+m_8P_8'+n_1Q_1'+n_2Q_2'+n_3Q_3'+n_4Q_4'+n_5Q_5'$ with m_1 such that $\sum m_i+\sum n_i=0$. Let us suppose that this divisor is in the kernel of the isogeny from the Jacobian to the product of the three elliptic curves $\mathcal{E}_1'\times\mathcal{E}_2'\times\mathcal{E}_3'$.

On the first elliptic factor $\mathcal{E}_1'$, we obtain the following relation $(m_2+m_6+m_3+n_2+n_4)\,P_{1,3}+(m_2+m_6+m_8+n_2+n_4)\,P_{1,4}+(n_1+n_5-n_2)\,Q_{1,1}+(n_3-n_4)\,Q_{1,3}=\mathcal{O}$ which yields $n_1+n_5=n_2$, $n_3=n_4$, $m_2+m_6+m_3+n_2+n_4\equiv 2\varepsilon \bmod 4$ and $m_2+m_6+m_8+n_2+n_4\equiv 2\,\varepsilon \bmod 4$.

On the second elliptic factor $\mathcal{E}_2'$, we obtain the following relation $(m_3+m_6+m_2+m_8-n_2-n_4-n_3)\,P_{2,3}+(m_2+m_8-n_2-n_4-n_3)\,P_{2,4}+(n_1-n_3)\,Q_{2,1}+n_3\,Q_{2,3}+(n_5-n_2-n_4)\,Q_{2,5}=\mathcal{O}$ which yields $n_1=n_3$, $n_5=n_2+n_4$, $m_3+m_6+m_2+m_8-n_2-n_4-n_3\equiv 2\,\varepsilon' \bmod 4$ and $m_2+m_8-n_2-n_4-n_3\equiv 2\varepsilon' \bmod 4$.

On the third elliptic factor $\mathcal{E}_3'$, we obtain the following relation $(m_6+m_3+n_2+n_5-n_4)\,P_{3,5}+(m_8+m_3+n_3+n_4)\,P_{3,7}+(n_1-n_3-n_2-n_5+n_4)\,Q_{3,1}=\mathcal{O}$ which yields $n_1+n_4=n_3+n_2+n_5$, $m_6+m_3+n_2+n_5-n_4\equiv 2\,\varepsilon'' \bmod 4$ and $m_8+m_3+n_3+n_4\equiv 2\,\varepsilon''' \bmod 4$.

Hence $n_2=n_1+n_5$, $n_1=n_3=n_4=n_1+2n_5$ and $n_5=n_5+2n_1$ that is $n_1=n_5=n_2=n_3=n_4=0$.

Moreover, $\varepsilon''=0$, $m_6\equiv m_3\equiv m_8\equiv 2\varepsilon+2\varepsilon' \bmod 4$, and $m_2\equiv 2\varepsilon$. Hence a degree zero divisor with support in the Weierstrass points is in the kernel of the isogeny if it is of the following form $\varepsilon\,(2P_2'+2P_3'-2P_6'-2P_8')+\varepsilon'\,(2P_3'+2P_1'-2P_6'-2P_8')$.

$\varepsilon'=0$ it is the divisor $2P_2'+2P_3'-2P_6'-2P_8'$, which is non zero in J, as we check in the following lemma.

$\varepsilon = 0$ it is the divisor $2P_3' + 2P_1' - 2P_8' - 2P_6'$, which is non zero in J, as we check in the following lemma.

$\varepsilon\varepsilon' \neq 0$ it is the divisor $2P_2' - 2P_1'$, which is non zero in J (otherwise there would exist a bitangent through P_2' and P_1').

We conclude that there are no extra relations between the Weierstrass points.

Lemma 4.13. *Neither* $2P_2' + 2P_3' - 2P_6' - 2P_8'$ *nor* $2P_3' + 2P_1' - 2P_8' - 2P_6'$ *is zero in* J.

Proof: The tangent line at P_8' is given by $4X + 10iZ - (25+10i)Y = 0$ and the tangent line at P_6' is given by $X = Z$. The family of conic tangent to the curve at P_8' and P_6' is given by

$$\begin{aligned}\mathcal{Q}_a(X,Y,Z) = 10(5i-2)aZY - 4(5+2i)aZX + 25(-2ia+5)Y^2 \\ + 20aZ^2 + 20X^2 + 10(2a - ia - 10)XY,\end{aligned}$$

the value $a = -5i/2$ corresponding to the degenerate case. An element of the Riemann-Roch space $L(2P_6' + 2P_8')$ is thus of the form

$$\frac{\mathcal{Q}_a(X,Y,Z)}{(4X + 10iZ - (25+10i)Y)(X - Z)}.$$

We check that neither $2P_3' + 2P_1'$ nor $2P_2' + 2P_3'$ is in $L(2P_6' + 2P_8')$. ∎

4.5 Proof of theorem 4.1

We prove the theorem, we apply Silverman's specialization theorem 2.2 to $A = \mathrm{Jac}(\mathcal{C}_t)$, $C = \mathbb{P}^1$ (parametrized by t), and J_t the Jacobian of $\mathcal{C}_t$. We have to check that the hypothesis of the theorem are satisfied. If J_t had a constant part, say A_0, we would have a non-constant map $A_0 \overset{\phi_t}{\hookrightarrow} J_t$, hence one of the three maps $A_0 \overset{\phi_t}{\hookrightarrow} J_t \overset{\pi_i}{\to} \mathcal{E}_i$ would be non-constant, hence surjective. But none of the three j-invariants of the elliptic curves is constant, hence a contradiction. Indeed,

$$\begin{aligned} j(\mathcal{E}_1) &= 256\,\frac{(t^2-t+1)^3(t^2+t+1)^3}{t^4(t-i)^2(t+i)^2}, \\ j(\mathcal{E}_2) &= -16\,\frac{(t^2-4t+1)^3(t^2+4t+1)^3}{t^2(t-i)^4(t+i)^4} \\ \text{and} \qquad j(\mathcal{E}_3) &= 64\,\frac{(t^4-2t^3+6t^2-2t+1)^3}{t^2(t-1)^4(t-i)^2(t+i)^2}. \end{aligned}$$

5 Curve with eight hyperflexes

There is exactly one curve not in the family of the preceeding section with eight hyperflexes [12]. It is the curve Σ given by the following equation:

$$(1-3(\sqrt{-7}+1)/2)(X^2-YZ)^2+YZ(-2X+Y+Z)(2X+Y+Z)=0.$$

We show that

Theorem 5.1. *The group generated by the Weierstrass points of the curve Σ is $W=\mathbb{Z}^5\times(\mathbb{Z}/4\mathbb{Z})^4$.*

We will consider another model of the curve. Let $\mathcal{C}$ be the projective plane curve defined by

$$4(X^4+Y^4)+24i\sqrt{7}X^2Y^2+12(1-i\sqrt{7})XYZ^2-\frac{(7-3i\sqrt{7})}{2}Z^4=0.$$

The map from Σ to $\mathcal{C}$ is given by

$$(X:Y:Z)\mapsto(-2iX-Y+Z:2iX-Y+Z:2Y+2Z).$$

5.1 Weierstrass points

Using `magma` [1], we obtain that the Weierstrass points are defined over the number field M of degree 32, where M is defined as follows: let $K=\mathbb{Q}(\sqrt{7},i)$, $L=K(a)$, $M=L(b)$ where $8192\,a^2+128(15\sqrt{7}i-35)\,a+(147\sqrt{7}i+49)=0$ and $b^4=a$.

5.1.1 Weierstrass points of weight two

The hyperflexes are given by
$P_1=(1:1:2)$, $P_2=(-1:-1:2)$, $P_3=(-i:i:2)$, $P_4=(i:-i:2)$, $P_5=((-\sqrt{7}-1)i-\sqrt{7}+1:(\sqrt{7}-1)i-\sqrt{7}-1:8)$, $P_6=((\sqrt{7}+1)i+\sqrt{7}-1:(-\sqrt{7}+1)i+\sqrt{7}+1:8)$, $P_7=((\sqrt{7}-1)i-\sqrt{7}-1:(-\sqrt{7}-1)i-1\sqrt{7}+1:8)$ and $P_8=((-\sqrt{7}+1)i+\sqrt{7}+1:(\sqrt{7}+1)i+\sqrt{7}-1:8)$.

5.1.2 Weierstrass points of weight one

The Weierstrass points of weight one are given by
$Q_1=(x_0,y_0)$, $Q_2=(-ix_0,iy_0)$, $Q_3=(-x_0,-y_0)$, $Q_4=(ix_0,-iy_0)$, $Q_5=(y_0,x_0)$, $Q_6=(-iy_0,ix_0)$, $Q_7=(-y_0,-x_0)$ and $Q_8=(iy_0,-ix_0)$, where $y_0=b$ and $49\cdot x_0=-((-160i\sqrt{7}+32\cdot 7)\,a+140(i\sqrt{7}+1))\,y_0^3$.

5.1.3 Relations between the Weierstrass points

Convention. From now on, we take P_8 as base-point for the Abel-Jacobi map and we will write P for the image $[P - P_8]$ of P under $\jmath$.

There are some straightforward relations arising from conics intersecting the curve at the Weierstrass points. More precisely,

Proposition 5.2. *The Weierstrass points satisfy the following relations*

- $4P_i = 0$
- $Q_1 + Q_2 + Q_3 + Q_4 + Q_5 + Q_6 + Q_7 + Q_8 = 0$
- $P_1 + P_2 + P_3 + P_4 + 2P_5 + 2P_6 = 0$
- $P_1 + P_2 + P_3 + P_4 + 2P_7 + 2P_8 = 0$
- $2P_1 + 2P_2 + P_5 + P_6 + P_7 + P_8 = 0$
- $P_5 + P_6 + P_7 + P_8 + Q_1 + Q_3 + Q_5 + Q_7 = 0$
- $2P_7 + 2P_8 + Q_2 + Q_4 + Q_5 + Q_7 = 0.$

Proof: The first relation comes from the definition of hyperflexes. It is easy to check that each of the following conics meets the curve at the said points with the correct multiplicities:

- $16XY = (i\sqrt{7} + 7)Z^2$
- $X^2 = (i + \sqrt{7})XY + Y^2 - (i + \sqrt{7})/4Z^2$
- $X^2 + (i + \sqrt{7})XY - Y^2 + (-i - \sqrt{7})/4Z^2 = 0$
- $X^2 - (i\sqrt{7} + 1)XY + Y^2 + (i\sqrt{7} - 1)/4Z^2 = 0$
- $X^2 + ((-32/7i\sqrt{7} + 96/7)a + (40/7i\sqrt{7} - 4))b^2XY + Y^2 + (-32/7a + (-23/28i\sqrt{7} + 13/4))b^2Z^2 = 0$
- $X^2 + (((32i\sqrt{7} - 96)a + (-40i\sqrt{7} - 28))/7b^2 + (-3/2i + 1/2\sqrt{7}))XY - Y^2 + ((32/7a + (37/28i\sqrt{7} - 7/4))b^2 + (7/16i - 5/16\sqrt{7}))Z^2 = 0$

∎

From these relations, we deduce that

Proposition 5.3. *The group W is a quotient of $\mathbb{Z}^5 \times (\mathbb{Z}/4\mathbb{Z})^4$.*

We will show that there are no other relations between the Weierstrass points, hence the theorem. In order to do so, we will determine the elliptic factors of the Jacobian and compute the images of the Weierstrass points on each on these factors in order to show the independence of the remaining points.

5.2 Structure of the Jacobian

Proposition 5.4. *The Jacobian is isogeneous to the product of two copies on an elliptic curve by a third one, i.e.* $\mathcal{J} \simeq \mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$*, with* $\mathcal{E}_2 \simeq \mathcal{E}_3$*.*

Proof: Indeed, if we consider the pullbacks of differential forms on each of these elliptic curves, we see that they are independent. For the definitions of both the curves and the maps, see section 5.2.2 below. On each elliptic curve $\mathcal{E}_i$, a differential form is $\omega_i = du/2v$. A basis of the differential forms on $\mathcal{C}$ is given by ω_0, $x\omega_0$ and $y\omega_0$ with

$$\omega_0 = \frac{dx}{3x + 4y^3 + 12i\sqrt{7}x^2y - 3i\sqrt{7}x}.$$

The pullbacks of the three differential forms are respectively

$$\begin{aligned} \phi_1^*(\omega_1) &= (1 - i\sqrt{7})\,\omega_0, \\ \phi_2^*(\omega_2) &= (i\sqrt{7} - 1)(y - x)\,\omega_0 \\ \text{and} \qquad \phi_3^*(\omega_3) &= -(i + \sqrt{7})(x + y)\,\omega_0. \end{aligned}$$

Hence, the result. ∎

5.2.1 Automorphisms of the curve

The group of automorphisms of the curve is a dihedral group of order 8 ([12]). This group is generated by ρ and σ, whose action on the Weierstrass points is the following:

$$\begin{aligned} \rho &= (P_1, P_4, P_2, P_3)(P_5, P_8, P_6, P_7)(Q_1, Q_4, Q_3, Q_2)(Q_5, Q_8, Q_7, Q_6) \\ \sigma &= (P_3, P_4)(P_5, P_7)(P_6, P_8)(Q_1, Q_5)(Q_2, Q_8)(Q_3, Q_7)(Q_4, Q_6). \end{aligned}$$

The automorphism ρ is given by $(X : Y : Z) \mapsto (iX : -iY : Z)$.
The automorphism σ is given by $(X : Y : Z) \mapsto (Y : X : Z)$.
The automorphism $\tau = \sigma\rho^2$ is given by $(X : Y : Z) \mapsto (-Y : -X : Z)$.

5.2.2 Elliptic factors of the Jacobian

By identifying points which are in the same orbit under the action of these automorphisms, we obtain maps to some elliptic curves.

Proposition 5.5. *The morphism ϕ_1 of degree 2 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_1 = \mathcal{C}/\langle\rho\rangle$ can be described as $(X : Y : Z) \mapsto (u, v)$ where*

$$\begin{cases} u = \dfrac{-2X^3 + i\sqrt{7}XY^2}{X^3} \\ v = \dfrac{24i\sqrt{7}XY^2 + 7(-i\sqrt{7}+1)YZ^2}{4X^3} \end{cases}$$

writing $\mathcal{E}_1$ as $v^2 = u^3 - 19\,u - 30$.

Proposition 5.6. *The morphism ϕ_2 of degree 2 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_2 = \mathcal{C}/\langle\sigma\rangle$ can be described as $(X : Y : Z) \mapsto (u, v)$ where*

$$\begin{cases} u = \dfrac{(i\sqrt{7}+2)(X+Y)^2 + (i\sqrt{7}+1)(X+Y)Z - Z^2}{(X+Y+Z)^2} \\ v = \dfrac{2\,(-i\sqrt{7}+1)(X-Y)^2 + (3i\sqrt{7}+9)(-4XY+Z^2)}{2\,(X+Y+Z)^2} \end{cases}$$

writing $\mathcal{E}_2$ as $v^2 = u^3 + 5\,u - 2i\sqrt{7}$.

With the third automorphism, we obtain a second map to the same elliptic curve.

Proposition 5.7. *The morphism ϕ_3 of degree 2 from $\mathcal{C}$ to the elliptic curve $\mathcal{E}_3 = \mathcal{C}/\langle\sigma\rho^2\rangle$ can be described as $(X : Y : Z) \mapsto (u, v)$ where*

$$\begin{cases} u = \dfrac{-2\,(X-Y)^2 + (i\sqrt{7}+1)(4XY - Z^2)}{2\,(X+Y+Z)(X+Y-Z)} \\ v = \dfrac{(i+\sqrt{7})(Y-X)Z}{(X+Y+Z)(X+Y-Z)} \end{cases}$$

writing $\mathcal{E}_3$ as $v^2 = u^3 + 5\,u - 2i\sqrt{7}$.

5.3 Study of the Weierstrass points

We compute the images of the Weierstrass points on each of the elliptic factors. Recall that, by definition, $2^8\,a = 70 - 30i\sqrt{7} + 16i\sqrt{7}\sqrt{3i\sqrt{7}+1}$ and $b = a^4$.

5.3.1 Images of the Weierstrass points on the first elliptic curve

Recall that the orbits under the action of ρ are as follows $\{P_1, P_2, P_3, P_4\}$, $\{P_5, P_6, P_7, P_8\}$, $\{Q_1, Q_2, Q_3, Q_4\}$ and $\{Q_5, Q_6, Q_7, Q_8\}$. Thus, the images of the Weierstrass points are the following four points on the elliptic curve $\mathcal{E}_1$,

$$\begin{aligned} P_{1,1} = \phi_1(\{P_1, P_2, P_3, P_4\}), \quad & P_{1,5} = \phi_1(\{P_5, P_6, P_7, P_8\}), \\ Q_{1,1} = \phi_1(\{Q_1, Q_2, Q_3, Q_4\}), \quad \text{and} \quad & Q_{1,5} = \phi_1(\{Q_5, Q_6, Q_7, Q_8\}). \end{aligned}$$

The three points of order 2 are $T_0 = (-2, 0)$, $T_1 = (-3, 0)$ and $T_2 = (5, 0)$.

On the elliptic curve, the following relations hold

$$Q_{1,1} + Q_{1,5} = T_0 = 2P_{1,1} \quad \text{and} \quad P_{1,1} - P_{1,5} = T_1.$$

Lemma 5.8. *The point $Q_{1,1}$ is of infinite order.*

Proof: For a prime of residue class degree 1 in M, we can compute the reduction of the elliptic curve. For $p = 337$, we pick 189 as a square root of -1 mod 337, 218 as a square root of 7 mod 337 and 172 as a square root of $3 \cdot 189 \cdot 218 + 1$ mod 337; hence $a = 233$ mod 337. The reduction $\widetilde{\mathcal{E}_1}$ of the elliptic curve is defined by $y^2 = x^3 + 318x + 307$, the reduction of the point $Q_{1,1}$ is the point $\widetilde{Q}_{1,1} = (236, 139)$, which is of order 28. For $p = 569$, we take 483 as a square root of -1 mod 569, 24 as a square root of 7 mod 569, and 270 as a square root of $3 \cdot 483 \cdot 24 + 1$ mod 569; hence $a = 499$ mod 569. The reduction $\widetilde{\mathcal{E}_1}$ of the elliptic curve is defined by $y^2 = x^3 + 550x + 539$, the reduction of the point $Q_{1,1}$ is the point $\widetilde{Q}_{1,1} = (337, 109)$, which is of order $8 \cdot 17$. Hence $Q_{1,1}$ is of infinite order. ∎

5.3.2 Images of the Weierstrass points on the second elliptic curve

Recall that the orbits under the action of σ are: $\{P_3, P_4\}$, $\{P_5, P_7\}$, $\{P_6, P_8\}$, $\{Q_1, Q_5\}$, $\{Q_2, Q_8\}$, $\{Q_3, Q_7\}$, and $\{Q_4, Q_6\}$, P_1 and P_2 being fixed. Thus, the Weierstrass points have the following images under ϕ_2

$$\begin{aligned} P_{2,1} = \phi_2(P_1) = T_0, \quad & P_{2,2} = \phi_2(P_2) = \mathcal{O}, \quad P_{2,3} = \phi_2(\{P_3, P_4\}), \\ P_{2,5} = \phi_2(\{P_5, P_7\}), \quad & P_{2,6} = \phi_2(\{P_6, P_8\}), \quad Q_{2,1} = \phi_2(\{Q_1, Q_5\}), \\ Q_{2,2} = \phi_2(\{Q_2, Q_8\}), \quad & Q_{2,3} = \phi_2(\{Q_3, Q_7\}), \quad Q_{2,4} = \phi_2(\{Q_4, Q_6\}). \end{aligned}$$

The points of order 2 are $T_0 = (1/2i\sqrt{7} + 1/2, 0)$ $T_1 = (1/2i\sqrt{7} - 1/2, 0)$ and $T_2 = ((-i\sqrt{7}, 0)$. The following relations hold on the elliptic curve

$$2P_{2,3} = T_0 = Q_{2,2} + Q_{2,4} = Q_{2,1} + Q_{2,3} = P_{2,6} + P_{2,5}$$
$$\text{and} \quad 2P_{2,5} = T_2.$$

Lemma 5.9. *The points $Q_{2,1}$ and $Q_{2,2}$ are of infinite order and independent.*

Proof: In order to prove the proposition, we will compute the images of these two points when we reduce the curve modulo primes of residue class degree 1 in M. There are such primes above 2657 and 569. We have $\#\widetilde{\mathcal{E}}_2(\mathbb{F}_{2657}) = 2^6 \cdot 43$, $\widetilde{Q}_{2,1}$ is of order $2 \cdot 43$ and $\widetilde{Q}_{2,2}$ is of order $4 \cdot 43$ — for 163 a square root of -1 mod 2657, 703 a square root of 7 mod 2657, 2436 a square root of $3 \cdot 163 \cdot 703 + 1$ mod 2657 and 1377 a fourth root of $70 - 30 \cdot 163 \cdot 703 + 16 \cdot 163 \cdot 703 \cdot 2436$ mod 2657, hence $a = 2495$ mod 2657 and $b = 2337$ mod 2657. For the second prime, $\#\widetilde{\mathcal{E}}_2(\mathbb{F}_{569}) = 2^4 \cdot 37$, $\widetilde{Q}_{2,1}$ is of order $4 \cdot 37$ and $\widetilde{Q}_{2,2}$ is of order $4 \cdot 37$ (for 483 a square root of -1 mod 569, 24 a square root of 7 mod 569, 270 a square root of $(3 \cdot 483 \cdot 24 + 1)$ mod 569 and 287 a fourth root of $70 - 30 \cdot 483 \cdot 24 + 16 \cdot 483 \cdot 24 \cdot 270$ mod 569, hence $a = 499$ mod 569 and $b = 214$ mod 569). Hence, both points $Q_{2,1}$ and $Q_{2,2}$ are of infinite order. Moreover, there are no points of order 23 in $\mathcal{E}_2'(M)$.

$p = 337$

Take 189 as a square root of -1 mod 337, 218 as a square root of 7 mod 337, 172 as a square root of $(3 \cdot 189 \cdot 218 + 1)$ mod 337 and 226 as a fourth root of $70 - 30 \cdot 189 \cdot 218 + 16 \cdot 189 \cdot 218 \cdot 172$ mod 337; hence $a = 233$ mod 337 and $b = 225$ mod 337. The reduction $\widetilde{\mathcal{E}}_2$ of the elliptic curve is defined by $y^2 = x^3 + 5x + 161$, and we have $\#\widetilde{\mathcal{E}}_2(\mathbb{F}_{337}) = 2^4 \cdot 23$.
The reduction of the point $16\,Q_{2,1}$ is the point $\widetilde{Q}'_{2,1} = 16\,\widetilde{Q}_{2,1} = (262, 199)$, which is of order 23 and the reduction of the point $16\,Q_{2,2}$ is the point $\widetilde{Q}'_{2,2} = 16\,\widetilde{Q}_{2,2} = (23, 131)$, which is equal to $4\,\widetilde{Q}'_{2,1}$.

$p = 5737$

Pick 1126 as a square root of -1 mod 5737, 1033 as a square root of 7 mod 5737, 4903 as a square root of $(3 \cdot 1126 \cdot 1033 + 1)$ mod 5737 and 2889 as a fourth root of $70 - 30 \cdot 1126 \cdot 1033 + 16 \cdot 1126 \cdot 1033 \cdot 4903 + 1$ mod 5737; hence $a = 5361$ mod 5737 and $b = 5025$ mod 5737.
The reduced elliptic curve $\widetilde{\mathcal{E}}_2$ is defined by $y^2 = x^3 + 5x + 2906$ and we have $\#\widetilde{\mathcal{E}}_2(\mathbb{F}_{5737}) = 2^8 \cdot 23$.
The reduction of the point $2^8\,Q_{2,1}$ is the point $\widetilde{Q}'_{2,1} = 2^8\,\widetilde{Q}_{2,1} =$

$(1347, 718)$, which is of order 23 and the reduction of the point $2^8\, Q_{2,2}$ is the point $\widetilde{Q}'_{2,2} = 2^8\, \widetilde{Q}_{2,2} = (267, 4597)$, which is equal to $16\, \widetilde{Q}'_{2,1}$.

Applying the lemma 3.9 to $P = 2^8\, Q_{2,1}$, $Q = 2^8\, Q_{2,2}$, $l = 23$, $\mathfrak{p}_1$ a prime above 337, $\mathfrak{p}_2$ a prime above 5737, $a_1 = 4$ and $a_2 = 16$ gives the result. ∎

5.3.3 Images of the Weierstrass points on the third elliptic curve

Recall that the orbits under the action of τ are:
$\{P_1, P_2\}$, $\{P_5, P_8\}$, $\{P_6, P_7\}$, $\{Q_1, Q_7\}$, $\{Q_2, Q_6\}$, $\{Q_3, Q_5\}$, and $\{Q_4, Q_8\}$, P_3 and P_4 being fixed. The images of the Weierstrass points by ϕ_3 are thus the following five points

$$P_{3,1} = \phi_3(\{P_1, P_2\}) = \mathcal{O}, \quad P_{3,3} = \phi_3(P_3), \quad P_{3,4} = \phi_3(P_4),$$
$$P_{3,5} = \phi_3(\{P_5, P_8\}), \quad P_{3,6} = \phi_3(\{P_6, P_7\}), Q_{3,1} = \phi_3(\{Q_1, Q_7\}),$$
$$Q_{3,2} = \phi_3(\{Q_2, Q_6\}), \quad Q_{3,3} = \phi_3(\{Q_3, Q_5\}), \quad Q_{3,4} = \phi_3(\{Q_4, Q_8\}).$$

The following relations hold on the elliptic curve

$$Q_{3,1} + Q_{3,3} = Q_{3,2} + Q_{3,4} = P_{3,5} + P_{3,6} = P_{3,3} + P_{3,4} = \mathcal{O}$$
$$2P_{3,3} = T_0, 2P_{3,5} = T_1 \quad \text{and} \quad P_{3,4} = P_{2,3}.$$

Lemma 5.10. *The points $Q_{3,1}$ and $Q_{3,2}$ are of infinite order and independent.*

Proof: Indeed, $Q_{3,1} + P_{3,3} = -Q_{2,4}$ and $Q_{3,2} + P_{3,3} = -Q_{2,1}$. ∎

5.4 Proof of theorem 5.1

We will show that there exists no relation between the remaining nine Weierstrass points. Let us consider a degree zero divisor whose support is in the set of Weierstrass points, say $m_2P_2 + m_3P_3 + m_5P_5 + m_7P_7 + m_8P_8 + n_1Q_1 + n_2Q_2 + n_4Q_4 + n_5Q_5 + n_6Q_6$ with m_8 such that $\sum m_i + \sum n_i = 0$. Suppose that this divisor is in the kernel of the isogeny from the Jacobian to the product of the three elliptic curves $\mathcal{E}_1 \times \mathcal{E}_2 \times \mathcal{E}_3$ and compute its images on each elliptic factor.

On the first elliptic factor $\mathcal{E}_1$, we obtain the following relation $(m_2 + m_3)P_{1,1} + (m_5 + m_7 + m_8)P_{1,5} + (n_1 + n_2 + n_4)Q_{1,1} + (n_5 + n_6)Q_{1,5} = \mathcal{O}$ which yields $m_2 + m_3 + m_5 + m_7 + m_8 + 2(n_5 + n_6) \equiv 0 \bmod 4$, $m_5 + m_7 + m_8 \equiv 0 \bmod 2$ and $n_1 + n_2 + n_4 = n_5 + n_6$.

On the second elliptic factor $\mathcal{E}_2$, we obtain the following relation $m_3P_{2,3}+(m_5+m_7)P_{2,5}+m_8P_{2,6}+(n_1+n_5)Q_{2,1}+n_2Q_{2,2}+(n_4+n_6)Q_{2,4}=\mathcal{O}$ which yields $m_3-2m_8+2(n_4+n_6)\equiv 0 \bmod 4$, $m_5+m_7\equiv m_8 \bmod 4$, $n_1+n_5=0$ and $n_2=n_4+n_6$.

On the third elliptic factor $\mathcal{E}_3$, we obtain the following relation $m_3P_{3,3}+(m_5+m_8)P_{3,5}+m_7P_{3,6}+n_1Q_{3,1}+(n_2+n_6)Q_{3,2}+n_5Q_{3,3}+n_4Q_{3,4}=\mathcal{O}$ which yields $m_3\equiv 0 \bmod 4$, $m_5+m_8\equiv m_7 \bmod 4$, $n_1=n_5$ and $n_2+n_6=n_4$.

Hence the coefficients satisfy

$$
\begin{gathered}
n_1=n_5=0, \quad n_2=n_4, \quad n_6=0, \quad n_2+n_4=0 \\
m_3\equiv m_2\equiv 0 \bmod 4 \quad m_8\equiv m_5\equiv m_7\equiv 0 \bmod 2.
\end{gathered}
$$

A degree zero divisor with support in the set of Weierstrass points is thus in the kernel of the isogeny if it is of the following form $m_5P_5+m_7P_7-(m_5+m_7)P_8$ with $m_5=m_7=2\,\varepsilon$.

Let us suppose that this divisor is already zero in the Jacobian (which will mean that there is another relation between the nine remaining Weierstrass points). If m_5 or m_7 is zero, that means that there is some relation of the form $2P-2Q\sim 0$, which will imply that the curve is hyperelliptic which is not the case. If $m_5=m_7=2$, then the relation $2P_5+2P_7-4P_8$ means that there is a bitangent through P_5 and P_7, which is not possible, since both points are hyperflexes.

6 Moduli space of curves

In this section, we will use Vermeulen's stratification of the moduli space $\mathcal{M}_3$ of curves of genus 3 [12] and the determination of the group W for particular curves to deduce some bounds on the rank and on the torsion part of a generic quartic having a fixed number of hyperflexes in a particular geometric configuration. We improve some of the results obtained in [2]

Let $\mathcal{M}_3^\circ$ be $\{[C]\in\mathcal{M}_3,\ C$ non-hyperelliptic$\}$, $M_s=\{[C]\in\mathcal{M}_3^\circ,\ C$ has at least s hyperflexes$\}$, and $M_s^\circ=\{[C]\in\mathcal{M}_3^\circ,\ C$ has exactly s hyperflexes$\}$.

The reference for all statements concerning the strata is Vermeulen's thesis [12], as for the notations. In particular, the X_i have dimension 3, and the Y_i's dimension 2. In all the statements, groups called F are always finite.

There are two quartics with 12 hyperflexes, the Fermat quartic, for which the Weierstrass subgroup is $(\mathbb{Z}/4\mathbb{Z})^5\times\mathbb{Z}/2\mathbb{Z}$ (see [10]) and the curve Ψ (given by the equation $X^4+Y^4+Z^4+3\,(X^2Y^2+X^2Z^2+Y^2Z^2)=0$) for which the Weierstrass subgroup is $(\mathbb{Z}/4\mathbb{Z})^5$ (see [4]).

There are no quartics with either 10 or 11 hyperflexes. There are two curves with exactly 9 hyperflexes and we studied the group the Weierstrass points generate in section 3.

The set of curves with exactly eight hyperflexes M_8° consists of the 1-dimensional family $Z_{1,t}$, and of the curve Σ which we studied in sections 4 and 5 respectively. From these results, using the specialization theorem 2.1 we can deduce than the rank is at least 5 and the torsion part is at most $(\mathbb{Z}/4\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^5$ for all strata containing one of the above curves. For curves with 4 hyperflexes or less, we obtain sharper results.

A straightforward study of the Riemann-Roch spaces corresponding to multiples of the base point of the Abel-Jacobi map yields the following lemma

Lemma 6.1. *Let C be a smooth quartic having exactly 4 hyperflexes. If 3 of these points lie on a line, the fourth point lies also on this line and the group they generate is $(\mathbb{Z}/4\mathbb{Z})^2$. Otherwise, the group generated by these 4 points is $(\mathbb{Z}/4\mathbb{Z})^3$ or $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$. More precisely, this group is $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$ if and only if there exists a conic curve tangent to the curve at these 4 points.*

The set of curves with 4 hyperflexes M_4 consists of 5 irreducible components X_1, Y_2, Y_3, Y_4 and Y_5, for which we state the following results:

Proposition 6.2.
(i) The Weierstrass subgroup of a generic quartic of Y_3 or Y_4 is of the form $W_\eta = \mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^3 \times F$ with $5 \leq r \leq 15$ and $F \subset (\mathbb{Z}/4\mathbb{Z})$.
(ii) The Weierstrass subgroup of a generic quartic in Y_5 is of the form $W_\eta = \mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^3 \times F$ with $5 \leq r \leq 15$ and $F \subset (\mathbb{Z}/4\mathbb{Z})^2$.

Proof: Indeed, according to the above lemma, the group generated by the hyperflexes is $(\mathbb{Z}/4\mathbb{Z})^3$. The curve Σ of Theorem 5.1 is in both Y_3 and Y_4. The curves Ω_i's of Theorem 3.1 are in Y_5. The specialization theorem 2.1 implies that the torsion part is at most $(\mathbb{Z}/4\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^5$ respectively, and gives bounds on the rank. ∎

Proposition 6.3. *The Weierstrass subgroup of a generic quartic of Y_2 is of the form $W_\eta = \mathbb{Z}^r \times F$ with $5 \leq r \leq 15$ and $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z}) \subset F \subset (\mathbb{Z}/4\mathbb{Z})^4$.*

Proof: A curve in Y_2 has the property that there is a conic curve which is tangent at 4 hyperflexes. Moreover, the curve Σ of Theorem 5.1 is in Y_2. The above lemma and the specialization theorem 2.1 give the result. ∎

Proposition 6.4 ([2]). *The Weierstrass subgroup of a generic quartic of* X_1 *is of the form* $W_\eta = \mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^2$ *with* $9 \leq r \leq 15$.

The set M_3° of curves with exactly 3 hyperflexes consists of 2 irreducible components X_2 and X_3. The set X_1 is in M_3, hence if a curve has 3 hyperflexes on a line, it lies in X_1 and has at least 4 hyperflexes.

Proposition 6.5. *The Weierstrass subgroup of a generic quartic of either* X_2 *or* X_3 *is of the form* $W_\eta = \mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^2 \times F$ *with* $5 \leq r \leq 17$ *and* $F \subset (\mathbb{Z}/4\mathbb{Z})^2$.

Proof: Both components contain Y_3 and the group generated by 3 hyperflexes is $(\mathbb{Z}/4\mathbb{Z})^2$, according to the above lemma. Proposition 6.2((i)) and the specialization theorem 2.1 give the result. ∎

Since M_1 et M_2 are irreducible, we obtained in [2] the following results:

Theorem 6.6 ([2]).
(i) The Weierstrass subgroup of a generic quartic is of the form $W_\eta = \mathbb{Z}^r$ *with* $11 \leq r \leq 23$.
(ii) The Weierstrass subgroup of a generic quartic with at least 1 hyperflex is of the form $W_\eta = \mathbb{Z}^r$ *with* $11 \leq r \leq 21$.
(iii) The Weierstrass subgroup of a generic quartic of M_2 *is of the form* $W_\eta = \mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z}) \times F$ *with* $9 \leq r \leq 19$ *and* $F \subset (\mathbb{Z}/4\mathbb{Z})$.

References

[1] W. Bosma and J. Cannon, editors. *Handbook of Magma Functions*, Sydney, 2001. `http://magma.maths.usyd.edu.au/`.

[2] M. Girard. Géométrie du groupe des points de Weierstrass d'une quartique lisse, *Journal of Number Theory*, **94**, $n^\circ 1$ (2002), 103–135.

[3] M. Girard. Groupe des points de Weierstrass sur une famille de quartiques lisses. to appear in *Acta Arithmetica*.

[4] M. Girard and P. Tzermias. Group Generated by the Weierstrass Points of a Plane Quartic, *Proc. Amer. Math. Soc.*, **130**, $n^\circ 3$ (2002), 667–672

[5] M. Hindry and J. H. Silverman. *Diophantine Geometry, An Introduction.* Springer-Verlag, New York, 2000. Graduate Texts in Mathematics, 201.

[6] J. H. Hubbard. Sur les sections analytiques de la courbe universelle de Teichmüller. *Mem. Amer. Math. Soc.*, 4(166):ix+137, 1976.

[7] M. J. Klassen and E. F. Schaefer. Arithmetic and geometry of the curve $y^3 + 1 = x^4$. *Acta Arith.*, **74**, $n°3$ (1996), 241–257.

[8] D. Laksov and A. Thorup. Weierstrass points and gap sequences for families of curves. *Ark. Mat.*, **32**, $n°2$ (1994), 393–422.

[9] D. T. Prapavessi. On the Jacobian of the Klein curve. *Proc. Amer. Math. Soc.*, **122**, $n°4$ (1994), 971–978.

[10] D. E. Rohrlich. Points at infinity on the Fermat curves. *Invent. Math.*, **39**, $n°2$ (1977), 95–127.

[11] J. H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, **342** (1983), 197–211.

[12] A. M. Vermeulen. *Weierstrass points of weight two on curves of genus three*. PhD thesis, Universiteit van Amsterdam, 1983.