MATHEMATICS OF COMPUTATION
Volume 75, Number 255, July 2006, Pages 1561–1583
S 0025-5718(06)01853-9
Article electronically published on May 1, 2006

THE GROUP OF WEIERSTRASS POINTS OF A PLANE QUARTIC WITH AT LEAST EIGHT HYPERFLEXES

MARTINE GIRARD

Abstract. The group generated by the Weierstrass points of a smooth curve in its Jacobian is an 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 property of being geometrically intrinsic. Curves of genus 0 or 1 have no Weierstrass points, and for hyperelliptic curves, the Weierstrass points can easily be 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 the images of the Weierstrass points under the Abel-Jacobi map, cannot be characterized so easily. This structure is known for curves with many automorphisms ([10], [12], [13]), 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 nontrivial 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 ([7], [13]). We show:

Theorem 3.1. *Let Ω_1 be the plane quartic*

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

and let Ω_2 be its conjugate. The group generated by the Weierstrass points of any of the two curves Ω_i is $W = (\mathbb{Z}/4\mathbb{Z})^5 \times \mathbb{Z}^5$.

Received by the editor March 6, 2003 and, in revised form, April 1, 2005.
2000 *Mathematics Subject Classification.* Primary 11G30, 14H55, 14Q05; Secondary 14H40.
Key words and phrases. Algebraic curves, Jacobian, Weierstrass points, quartics, elliptic curves.
This research was carried out while the author was a postdoctoral fellow at Leiden University within the European Research Training Network Galois Theory and Explicit Methods in Arithmetic.

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.*

Theorem 5.1. *Let Σ be the smooth projective curve*

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

The Weierstrass subgroup of the curve Σ is $W=\mathbb{Z}^5 \times (\mathbb{Z}/4\mathbb{Z})^5$.

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 [15], 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 (the only strata with eight or nine hyperflexes are Ω_i, Σ and $\mathbb{Z}_1$, which correspond to nine hyperflexes, eight hyperflexes on three lines, and four conics tangent to the curve at eight hyperflexes, respectively). 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 [3], we showed that for a generic quartic, it is a free abelian group of rank at least 11. In in Section 6, we pursue the study carried out in [4], [3] and improve some of the bounds previously obtained.

We first recall the definitions of Weierstrass points and of the object of our study. In Section 2, we state two theorems fundamental to the present study. We then compute the Weierstrass subgroup for curves with eight or nine hyperflexes.

We proceed in several steps: we first search for elementary geometric configurations involving the Weierstrass points—they usually arise from lines or conics meeting the curve only at these points. They translate into relations between the images of the Weierstrass points in the Jacobian and enable us to restrict the number of generators (starting from $g(g^2-1)$). We then use the fact that the Jacobians of these curves are isogenous to the product of three elliptic curves: degree 0 divisors with support in the set of Weierstrass points which correspond to an extra relation will be mapped to the identity on each elliptic curve. We thus deduce all possible relations between the remaining Weierstrass points, and we use geometric arguments to determine their correctness.

By convention, we choose models of our curves over a number field and consider the geometric points on these curves and their Jacobians (in some fixed algebraic closure).

1. Definitions and notation

1.1. **Weierstrass points.** For properties of the Weierstrass points, we refer to [8, exercise A.4.14, p. 89] or [1, exercise E, p. 41]. Let $\mathcal{C}$ be a smooth projective curve of genus $g \geq 2$ defined over a number field k 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 $\{f \in k(\mathcal{C}) \mid \mathrm{div}(f)+D \geq 0\}$ and let $\ell(D)$ be its dimension. We define the

gap sequence associated to P to be the set $G(P)=\{n\in\mathbb{Z}_{>0} \mid \ell(nP)=\ell((n-1)P)\}$. We can define the *weight* of a point to be $w(P) = \sum_{n\in G(P)} n - g(g+1)/2$. If $K_{\mathcal{C}}$ is a canonical divisor on $\mathcal{C}$, then $\sum_{P\in\mathcal{C}} w(P)P$ is linearly equivalent to $g(g+1)/2K_{\mathcal{C}}$, and thus 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.** We identify the Jacobian of $\mathcal{C}$ and $\mathrm{Pic}^\circ(\mathcal{C})$, and define the *Weierstrass subgroup* W to be the subgroup of $\mathrm{Pic}^\circ(\mathcal{C})$ generated by the differences of two Weierstrass points. Its elements are thus degree 0 divisors with support in $\mathcal{W}$. This group is defined over k, the field of definition of the curve, since $\mathcal{W}$ is invariant under the absolute Galois group of k. Nevertheless, its elements are defined over some finite extension of k, as are the Weierstrass points.

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 nonhyperelliptic 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. We will call the Weierstrass points of weight one *ordinary flexes*. As we have seen before, there are 24 points counted with multiplicity equal to the weight, i.e., $r + 2s = 24$, where s is the number of hyperflexes and r is the number of ordinary flexes.

The difference of two hyperflexes has order 4 in the Jacobian. Indeed, if L_P (resp. L_Q) is the linear form defining the tangent line to the curve at P (resp. Q), we have $\mathrm{div}(L_P/L_Q) = 4(P) - 4(Q)$. Hence the order of $P - Q$ divides 4, and it cannot be 2; otherwise, the curve would be hyperelliptic. We thus obtain that W is a quotient of $\mathbb{Z}^r \times (\mathbb{Z}/4\mathbb{Z})^{s-1}$, since s hyperflexes generate at most $s-1$ points of order 4. Moreover, if P_0 is a hyperflex, $4P_0$ is a canonical divisor, and we have $\sum w(P)P - 24\ P_0 = 0$. 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 $\mathbb{Z}$-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 divisors 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 [9] or Laksov-Thorup [11]; the second part is classic (see [8, Theorem C.1.4]). □

Both of 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. This specialization theorem applies to special families of abelian varieties as follows: 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 nonsingular, the specialization map is defined by $\sigma_t : A(C) \to A_t(\overline{K})$, $P \mapsto P_t$.

Theorem 2.2 (Silverman [14])**.** *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 [15]. These are the curve Ω_1 given by the projective equation

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

and its conjugate Ω_2. This curve has fifteen Weierstrass points, nine of which are hyperflexes. The hyperflexes lie on three lines. We will show that the naïve 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 $W = (\mathbb{Z}/4\mathbb{Z})^5 \times \mathbb{Z}^5$.*

3.1. **Weierstrass points.** Using `magma` [2], we determine that the Weierstrass points are defined over the number field M of degree 48, 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 $j = (-1 + i\sqrt{3})/2$.

For simplicity, we will consider the alternative model Ω given by the 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 Ω is given by

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

We will see that $\mathrm{Aut}(\Omega)$ is generated by two automorphisms, ρ and σ (see 3.2.1), which we can use to define the Weierstrass points: the hyperflexes are

$$P_3 = (-a-2 : a+4j^2-2 : a+4j-2), \qquad P_4 = (-b-2 : b+4j^2-2 : b+4j-2),$$
$$P_5 = (-j : j^2 : 1), \qquad P_1 = \rho(P_5), \qquad P_2 = \sigma(P_5), \qquad P_6 = \sigma(P_3),$$
$$P_7 = \sigma(P_4), \qquad P_8 = \rho(P_3), \qquad P_9 = \rho(P_4),$$

with $a = (\sqrt{7}+1)(i+1)$ and $b = (\sqrt{7}+1)(-i+1)$. The ordinary flexes of the curve Ω are the six points

$$Q_1 = (r : r^2 : 7), \qquad Q_5 = \sigma(Q_1), \qquad Q_4 = \rho(Q_1),$$
$$Q_2 = \sigma(Q_4), \qquad Q_3 = \rho(Q_5), \qquad \text{and} \quad Q_6 = \rho(Q_2) = \sigma(Q_3).$$

The four 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. $\{P_2, P_5, P_8, P_9\}$). Dividing these linear forms by the one corresponding to the tangent line at a hyperflex gives rational functions whose divisors are in W. The last relation is a consequence of the relation between all Weierstrass points as seen at the end of Section 1.3.

Proposition 3.2. *The Weierstrass points satisfy the relations*

- $4(P_m - P_n) = 0$,
- $P_2 + P_3 + P_4 - 3P_1 = 0$,
- $P_5 + P_6 + P_7 - 3P_1 = 0$,
- $P_5 + P_8 + P_9 - 3P_2 = 0$,
- $2\,(Q_1 + Q_2 + Q_3 + Q_4 + Q_5 + Q_6) - 12P_1 = 0$.

A set of generators of W is $P_m - P_1$ and $Q_n - P_1$. From the above relations, we see that $P_4 - P_1$, $P_7 - P_1$, and $P_9 - P_1$ are linear combinations of the other $P_m - P_1$. There are thus at most five independent differences of hyperflexes. The last relation implies that the sum of $Q_n - P_1$ has order two, hence we obtain:

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 $Q_n - P_1$ is equal to twice the sum of some differences of 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 isogenous to the product of three elliptic curves, which we determine.

Proposition 3.4. *The Jacobian of the curve Ω is isogenous 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 $\mathcal{E}_1 \cong \mathcal{E}_2$.*

Proof. We check that the pullbacks of differential forms on each elliptic curve are independent on Ω. 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 Ω 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

$$\phi_1^*(\omega_1) = c_1(y-1)\omega_0, \quad \phi_2^*(\omega_2) = c_2(2y + 1 + i\sqrt{3})\omega_0, \quad \phi_3^*(\omega_3) = c_3x\omega_0,$$

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

3.2.1. *Automorphisms of the curve.* The automorphism group of Ω is S_3. More precisely, this group is generated by the two automorphisms ρ and σ given respectively by

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

They act on the Weierstrass points in the following manner:

$$\rho = (P_1P_5)(P_6P_7)(P_3P_8)(P_4P_9)(Q_1Q_4)(Q_2Q_6)(Q_3Q_5),$$
$$\sigma = (P_2P_5)(P_3P_6)(P_4P_7)(P_8P_9)(Q_1Q_5)(Q_2Q_4)(Q_3Q_6).$$

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 Ω to the same elliptic curve.

Proposition 3.5. *The degree* 2 *morphism* ϕ_1 *from* Ω *to the elliptic curve* $\mathcal{E}_1 = \Omega/\langle\rho\rangle$ *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*

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

The degree 2 *morphism* ϕ_2 *from* Ω *to the elliptic curve* $\mathcal{E}_2 = \Omega/\langle\sigma\rangle$ *is given by* $\phi_2(X : Y : Z) = \phi_1(X : j^2Y : jZ)$.

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 3.6. *The degree* 3 *morphism from the curve* Ω *to the elliptic curve* $\mathcal{E}_3 = \Omega/\langle\tau\rangle$ *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* $\mathcal{E}_1$. 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 $\mathcal{E}_1$:

$$P_{1,1} = \phi_1(P_1), \quad P_{1,3} = \phi_1(P_3), \quad P_{1,4} = \phi_1(P_4), \quad P_{1,6} = \phi_1(P_6),$$
$$Q_{1,1} = \phi_1(Q_1), \quad Q_{1,2} = \phi_1(Q_2), \quad Q_{1,3} = \phi_1(Q_3), \quad \text{and} \quad \mathcal{O} = \phi_1(P_2),$$

which satisfy the following relations on the elliptic curve $\mathcal{E}_1$:

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

where 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 $T_2 = (-6 + 2\sqrt{7}, 0)$.

To show the independence of points on the elliptic curve, we will use the following lemma suggested by Jean-François Mestre:

Lemma 3.7. *Let P and Q be two K-rational points on an elliptic curve. Suppose there exist places of good reduction $\mathfrak{p}_1$ and $\mathfrak{p}_2$ and a prime l such that the reductions $\widetilde{P}_i$ and $\widetilde{Q}_i$ are of order l and $\widetilde{Q}_i \equiv \alpha_i \widetilde{P}_i \bmod \mathfrak{p}_i$ with $\alpha_1 \not\equiv \alpha_2 \bmod l$. If moreover, there exists no K-rational point of order l, then P and Q are $\mathbb{Z}$-independent.*

Proof. Suppose there was a minimal relation $mP + nQ = 0$. Looking at the reductions, we obtain that $m\widetilde{P}_i + n\widetilde{Q}_i \equiv (m + n\alpha_i)\widetilde{P}_i \equiv 0 \bmod \mathfrak{p}_i$, hence $m + n\alpha_i \equiv 0 \bmod l$, i.e., $m \equiv n \equiv 0 \bmod l$. But then $R = m/lP + n/lQ$ is a K-rational point of order l, which gives a contradiction. □

Proposition 3.8. *The two points $Q_{1,1}$ and $Q_{1,2}$ 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 inertial 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 $\#\widetilde{\mathcal{E}}_1(\mathbb{F}_{2797}) = 2^5 \cdot 89$, $\widetilde{Q}_{1,1}$ has order $4 \cdot 89$, and $\widetilde{Q}_{1,2}$ has order $2 \cdot 89$. For the second prime, $\#\widetilde{\mathcal{E}}_1(\mathbb{F}_{16333}) = 2^5 \cdot 509$, $\widetilde{Q}_{1,1}$ has order $4 \cdot 509$, and $\widetilde{Q}_{1,2}$ has order $2 \cdot 509$. Thus $Q_{1,1}$ and $Q_{1,2}$ are of infinite order. Moreover, there are no K-rational points of order 53.

We apply Lemma 3.7 to $P = 2^5 \cdot 3 \cdot 7Q_{1,1}$, $Q = 2^5 \cdot 3 \cdot 7Q_{1,2}$, $l = 53$, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ primes of inertial degree 1 over 4993 and 5881 respectively, $\alpha_1 = 19$, and $\alpha_2 = 25$: taking the following values

p	i	$\sqrt{3}$	j	$\sqrt{7}$	$\sqrt{3-\sqrt{7}}$	s	r
4993	158	1266	2650	212	2011	4277	2692
5881	1098	1451	5604	497	5077	3218	357

we obtain that

p	$\widetilde{\mathcal{E}}_1 : [a_1, a_2, a_3, a_4, a_6]$	$\#\widetilde{\mathcal{E}}_1(\mathbb{F}_p)$	$\widetilde{Q}'_{1,1} = 672\,\widetilde{Q}_{1,1}$	$672\,\widetilde{Q}_{1,2}$	α
4993	$[0, 4155, 0, 1517, 1964]$	$2^5 \cdot 3 \cdot 53$	$(2854, 1656)$	$(2100, 4807)$	19
5881	$[0, 3903, 0, 3442, 3400]$	$2^4 \cdot 7 \cdot 53$	$(3190, 5299)$	$(5530, 1666)$	25

□

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

$$P_{1,1} = \phi_2(P_5), \quad P_{1,4} = \phi_2(P_3), \quad P_{1,3} = \phi_2(P_4), \quad P_{1,6} = \phi_2(P_8),$$
$$Q_{1,1} = \phi_2(Q_3), \quad Q_{1,2} = \phi_2(Q_1), \quad Q_{1,3} = \phi_2(Q_2), \quad \text{and} \quad \mathcal{O} = \phi_2(P_1).$$

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

$$P_{3,1} = \phi_3(P_1),\ P_{3,4} = \phi_3(P_4),\ Q_{3,1} = \phi_3(Q_1),\ Q_{3,4} = \phi_3(Q_4), \text{and } \phi_3(P_3) = \mathcal{O},$$

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

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

Lemma 3.9. *The point $Q_{3,1}$ is of infinite order.*

Proof. For a prime of residue class degree 1 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 $Q_{3,1}$ is the point $\widetilde{Q}_{3,1} = (34, 14)$ 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 $Q_{3,1}$ is the point $\widetilde{Q}_{3,1} = (24, 54)$ which is of order 60. Hence the point $Q_{3,1}$ 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 0 divisor with support in the set of Weierstrass points, say $m_1P_1 + m_2P_2 + m_3P_3 + m_5P_5 + m_6P_6 + m_8P_8 + n_1Q_1 + n_2Q_2 + n_3Q_3 + n_4Q_4 + n_5Q_5 + n_6Q_6$ where $\sum m_i + \sum n_i = 0$. 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 factors, of the Jacobian.

On the first factor of the Jacobian $\mathcal{E}_1$, we get the following relation:

$$\begin{aligned}(m_1 + m_5)P_{1,1} + (m_3 + m_8)P_{1,3} + m_6P_{1,6} \\ + \ (n_1 + n_4)Q_{1,1} + (n_2 + n_6)Q_{1,2} + (n_3 + n_5)Q_{1,3} = \mathcal{O},\end{aligned}$$

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:

$$\begin{aligned}(m_2 + m_5)P_{1,1} + (m_3 + m_6)P_{1,4} + m_8P_{1,6} \\ + \ (n_3 + n_6)Q_{1,1} + (n_1 + n_5)Q_{1,2} + (n_2 + n_4)Q_{1,3} = \mathcal{O},\end{aligned}$$

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:

$$\begin{aligned}(m_1 + m_2 + m_5)P_{3,1} + (m_6 + m_8)P_{3,4} \\ + \ (n_1 + n_2 + n_3)Q_{3,1} + (n_4 + n_5 + n_6)Q_{3,4} = \mathcal{O},\end{aligned}$$

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

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

The only degree 0 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 3.10. *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 Ω at P_1, P_2, and P_5 with multiplicity two and at Q_1, Q_2, Q_3, Q_4, Q_5, and Q_6.

This completes the proof.

4. Family with eight hyperflexes

There is a one-dimensional family of curves with eight hyperflexes [15]. We show

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.*

We will work with another model for the curve: the curve $Z_{1,t}$ is isomorphic to the curve $\mathcal{Z}_t$ 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 $Z_{1,t}$ to $\mathcal{Z}_t$ is given by

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

and the map from $\mathcal{Z}_t$ to $Z_{1,t}$ is given by

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

4.1. **Weierstrass points.** We will see (in Section 4.2.1) that the automorphisms of $\mathcal{Z}_t$ are ρ, σ, and τ. We can use them to define the Weierstrass points: the hyperflexes are

$$P_1 = (-1 : t : 2t-1), \quad P_2 = \rho^2(P_1), \quad P_3 = (-i-1 : (i+1)t : 2t+i-1),$$
$$P_4 = \rho^2(P_3), \quad P_5 = \sigma(P_1), \quad P_6 = \sigma(P_2), \quad P_7 = \sigma(P_3), \quad \text{and} \quad P_8 = \sigma(P_4).$$

Let s be a square root of $(t-2)/(4t-2)$, and let

$$\begin{cases} x_1 &= \dfrac{b(s)(c(s)(1+2s^2)-2\,ia(s)(s^2-1))(2\,s+1)}{8\,s^5-4\,s^3+6\,s^2+2\,s-3}, \\ y_1 &= 2\,\dfrac{(4\,s^4-4\,s^3-2\,s^2+4\,s-2+ia(s)c(s)(1+2s^2))(s^2-1)}{(2\,s-1)(8\,s^5-4\,s^3+6\,s^2+2\,s-3)}, \\ x_3 &= \dfrac{a(s)(c(s)(1+2s^2)-2\,ib(s)(s^2-1))(2\,s-1)}{8\,s^5-4\,s^3-6\,s^2+2\,s+3}, \quad \text{and} \\ y_3 &= 2\,\dfrac{(4\,s^4+4\,s^3-2\,s^2-4\,s-2+ib(s)c(s)(1+2s^2))(s^2-1)}{(2\,s+1)(8\,s^5-4\,s^3-6\,s^2+2\,s+3)}, \end{cases}$$

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 other square root $-s$ will interchange Q_1 and Q_3). We can express the ordinary flexes in the following way:

$$\begin{gathered} Q_1=(x_1,y_1), \qquad Q_3=(x_3,y_3), \qquad Q_5=\sigma(Q_1), \\ Q_2=\rho^2(Q_5), \qquad Q_6=\sigma(Q_2), \qquad Q_3=\rho(Q_3), \\ Q_7=\sigma(Q_3), \qquad Q_4=\rho^2(Q_7), \qquad \text{and} \quad Q_8=\sigma(Q_4). \end{gathered}$$

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:*

- $P_1+P_2+P_3-3P_4=0$,
- $P_5+P_6+P_7-3P_8=0$,
- $4(P_n-P_m)=0$,
- $Q_1+Q_2+Q_3+Q_4+Q_5+Q_6+Q_7+Q_8-8P_1=0$,
- $Q_8+Q_1+Q_6+Q_3-P_3-P_4-P_5-P_6=0$,
- $Q_1+Q_2+Q_5+Q_6-P_1-P_2-P_5-P_6=0$.

Proof. The points P_1, P_2, P_3, and P_4 lie on a line as do 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 $\{P_3,P_4,P_7,P_8\}$.

The first four relations 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). The family of conics passing through P_3, P_4, P_5, and P_6 is given by

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

and

$$\lambda=-\frac{(2\,s+1)^2(2\,s-1)^2(2\,s^2+ia(s)b(s)-1)}{(4\,s^4-2\,s^2+1)(1+2\,s^2)}$$

gives the result.

The conic passing through Q_1, Q_2, Q_5, Q_6, and P_1 is given by

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

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 preceding remark and the following proposition. □

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

Proof. 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 are 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.**

4.2.1. *Automorphisms of the curve.* The group of automorphisms of $\mathcal{Z}_t$ is a dihedral group of order 8 (see [15]) generated by the two involutions whose action on the Weierstrass points is the following:

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

The two automorphisms σ and τ are given respectively by

$$\sigma: \quad (X:Y:Z) \mapsto (-X:Y:Z) \qquad \text{and}$$
$$\tau: \quad (X:Y:Z) \mapsto (-Y:t^2X:t^2X + it(Z-Y)).$$

Also, the automorphism $\rho = \sigma\tau$ satisfies $\rho^2(X:Y:Z) = (X:Y:2Y-Z)$.

4.2.2. *Elliptic factors of the Jacobian.* For the proofs of the statements in this part, see the preprint [6]. For each of these automorphisms, we obtain a map to an elliptic curve by identifying points which are in the same orbit:

Proposition 4.5. *Let $\mathcal{E}_1 = \mathcal{Z}_t/\langle\sigma\rangle$, $\mathcal{E}_2 = \mathcal{Z}_t/\langle\tau\rangle$, and $\mathcal{E}_3 = \mathcal{Z}_t/\langle\rho^2\rangle$. The Jacobian is isogenous to the product of the three elliptic curves, and these elliptic curves have respective equations:*

$$\mathcal{E}_1: \qquad v^2 = u^3 - (2t^2+1)\,u^2 + (1+t^2)t^2\,u,$$
$$\mathcal{E}_2: \qquad v^2 = u^3 + (4i-3)(t^2+6it-1)\,u^2 + (96-28i)t(i+t)^2\,u,$$
$$\mathcal{E}_3: \qquad v^2 = u^3 - (t+1)^2\,u^2 + 2t(1+t^2)\,u.$$

4.3. **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 4.6. *For the specialization $t = 2/5$, the group generated by the Weierstrass points is $W_{2/5} = (\mathbb{Z}/4\mathbb{Z})^4 \times \mathbb{Z}^5$.*

The curve $Z_{1,2/5}$ has the following equation:

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

The map from $Z_{1,2/5}$ to $\mathcal{Z}_{2/5}$ is given by

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

and the map from $\mathcal{Z}_{2/5}$ to $Z_{1,2/5}$ is given by

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

The curve $\mathcal{Z}_{2/5}$ 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 $\mathcal{Z}_{2/5}$ have the following coordinates:

$$P_1 = (5 : -2 : 1), \quad P_2 = \rho^2(P_1), \quad P_3 = (15i - 10 : -6i + 4 : 13),$$
$$P_4 = \rho^2(P_3), \quad P_5 = \sigma(P_1), \quad P_6 = \sigma(P_2), \quad P_7 = \sigma(P_3), \quad P_8 = \sigma(P_4),$$
$$Q_1 = ((3\sqrt{35} - 10i)\sqrt{65} : 6i\sqrt{35} + 20 : 83), \quad Q_5 = \sigma(Q_1), \quad Q_2 = \rho^2(Q_5),$$
$$Q_6 = \sigma(Q_2), \quad Q_3 = (-2i\sqrt{65} + 3\sqrt{35} : 6/25i\sqrt{35}\sqrt{65} + 52/5 : 23),$$
$$Q_7 = \sigma(Q_3), \quad Q_4 = \rho^2(Q_7), \quad \text{and} \quad Q_8 = \sigma(Q_4).$$

4.3.1. *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 $\mathcal{Z}_{2/5}$ 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

$$P_{1,1} = \varphi_1(P_1), \quad P_{1,2} = \varphi_1(P_2), \quad P_{1,3} = \varphi_1(P_3), \quad P_{1,4} = \varphi_1(P_4),$$
$$Q_{1,1} = \varphi_1(Q_1), \quad Q_{1,2} = \varphi_1(Q_2), \quad Q_{1,3} = \varphi_1(Q_3), \quad \text{and} \quad Q_{1,4} = \varphi_1(Q_4).$$

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 4.7. *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 $Q_{1,3}$. We apply Lemma 3.7 to $P = 16\,Q_{1,1}$, $Q = 16\,Q_{1,3}$, $l = 23$, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ primes of inertial degree 1 above 353 and 389, $\alpha_1 = 12$, and $\alpha_2 = 14$: choosing the values

p	i	$\sqrt{35}$	$\sqrt{65}$
389	274	206	125
353	42	68	154

we compute that

p	$\widetilde{\mathcal{E}}_1'$	$\#\widetilde{\mathcal{E}}_1'(\mathbb{F}_p)$	$\widetilde{P}_1 = 16\,\widetilde{Q}_{1,1}$	$\widetilde{Q}_1 = 16\,\widetilde{Q}_{1,3}$	α
389	$y^2 = x^3 + 142x + 170$	$2^4 \cdot 23$	$(362, 185)$	$(168, 145)$	12
353	$y^2 = x^3 + 106x + 26$	$2^4 \cdot 23$	$(35, 108)$	$(14, 148)$	14

□

Remark 4.8. We can show the independence of the points by computing their heights and the regulator using an implementation of the height pairing [5] in `magma` [2]. Indeed, we find that the regulator is nonzero since

$$\det\begin{pmatrix} \langle Q_{1,1}, Q_{1,1}\rangle & \langle Q_{1,1}, Q_{1,3}\rangle \\ \langle Q_{1,3}, Q_{1,1}\rangle & \langle Q_{1,3}, Q_{1,3}\rangle \end{pmatrix} = \begin{vmatrix} 4.33930257 & 0 \\ 0 & 3.87097356 \end{vmatrix} \neq 0.$$

4.3.2. *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 $\mathcal{Z}_{2/5}$ to $\mathcal{E}_2'$ is $(X : Y : Z) \mapsto (u, v)$, where

$$\begin{aligned} u = {} & \frac{1}{(119 + 120i)(6X + 5(i+2)Y + 10(i-1)Z)^2} \\ & \times \Big(342732X^2 + 60(-6008i + 20699)XY - 1680(i + 239)XZ \\ & \quad + 25(568i - 178419)Y^2 + 200(4877i + 23163)YZ - 200(4948i + 11571)Z^2\Big), \\ v = {} & 4\,\frac{(2671 - 10027i)(6X + 5(5i-2)Y + 10(-i+1)Z)}{13(119 + 120i)(6X + 5(i+2)Y + 10(i-1)Z)^3} \\ & \times \Big(780X^2 + 15(-16i + 197)XY + 6(139i - 188)XZ \\ & \quad - 50(9i + 137)Y^2 + 5(744i + 1207)YZ - 10(327i + 406)Z^2\Big). \end{aligned}$$

The images of the Weierstrass points are

$$\begin{gathered} P_{2,1} = \varphi_2(P_1), \quad P_{2,2} = \varphi_2(P_2), \quad P_{2,3} = \varphi_2(P_3), \quad P_{2,4} = \varphi_2(P_4), \\ Q_{2,1} = \varphi_2(Q_1), \quad Q_{2,2} = \varphi_2(Q_2), \quad Q_{2,3} = \varphi_2(Q_3), \quad \text{and} \quad Q_{2,5} = \varphi_2(Q_5), \end{gathered}$$

which 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 4.9. *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 $Q_{2,5}$. We then apply Lemma 3.7 to $P = 16\,Q_{2,1}$, $Q = 16\,Q_{2,5}$, $l = 23$, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ primes of inertial degree 1 above 389 and 353, $\alpha_1 = 20$, and $\alpha_2 = 10$:

p	$\widetilde{\mathcal{E}}_2'$	$\#\widetilde{\mathcal{E}}_2'(\mathbb{F}_p)$	l	$\widetilde{P}_2 = 16\,\widetilde{Q}_{2,1}$	$\widetilde{Q}_2 = 16\,\widetilde{Q}_{2,5}$	α
389	$y^2 = x^3 + 253x + 327$	$2^4 \cdot 23$	23	$(337, 156)$	$(81, 222)$	20
353	$y^2 = x^3 + 253x + 68$	$2^4 \cdot 23$	23	$(35, 308)$	$(294, 73)$	10

□

Remark 4.10. As above, we can show the independence of the points by computing their heights and the regulator. We find that the regulator is nonzero since

$$\det \begin{pmatrix} \langle Q_{2,1}, Q_{2,1} \rangle & \langle Q_{2,1}, Q_{2,2} \rangle \\ \langle Q_{2,2}, Q_{2,1} \rangle & \langle Q_{2,2}, Q_{2,2} \rangle \end{pmatrix} = \begin{vmatrix} 4.10513807 & -0.11708225 \\ -0.11708225 & 4.10513807 \end{vmatrix} \neq 0.$$

4.3.3. *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 $\mathcal{Z}_{2/5}$ 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

$$P_{3,1} = \varphi_3(P_1), \quad P_{3,3} = \varphi_3(P_3), \quad P_{3,5} = \varphi_3(P_5), \quad P_{3,7} = \varphi_3(P_7),$$
$$Q_{3,1} = \varphi_3(Q_1), \quad Q_{3,5} = \varphi_3(Q_2), \quad Q_{3,3} = \varphi_3(Q_3), \quad \text{and} \quad Q_{3,4} = \varphi_3(Q_4).$$

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 4.11. *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. □

Remark 4.12. Here again, we compute the height which is nonzero. Indeed, $\hat{h}(Q_{3,1}) = 1.03540318$.

4.3.4. *Proof of Theorem* 4.6. We will show that there exists no relation between the remaining ten Weierstrass points. Let us consider a degree 0 divisor whose support is in the set of Weierstrass points, say

$$\begin{aligned} D = {} & m_1P_1 + m_2P_2 + m_3P_3 + m_6P_6 + m_8P_8 \\ & + \ n_1Q_1 + n_2Q_2 + n_3Q_3 + n_4Q_4 + n_5Q_5, \end{aligned}$$

where $\sum m_i + \sum n_i = 0$. Let us suppose that this divisor is in the kernel of the isogeny from the Jacobian to the product of the three elliptic curves $\mathcal{E}_1' \times \mathcal{E}_2' \times \mathcal{E}_3'$.

Looking at the images of D on each elliptic curve, we obtain

$$n_1 = n_5 = n_2 = n_3 = n_4 = 0, m_6 \equiv m_3 \equiv m_8 \equiv 2\varepsilon + 2\varepsilon' \bmod 4, \quad \text{and} \quad m_2 \equiv 2\varepsilon.$$

Hence a degree 0 divisor with support in the Weierstrass points is in the kernel of the isogeny only if it is in the subgroup of $W[2]$ generated by $(2P_2+2P_3-2P_6-2P_8)$ and $(2P_3 + 2P_1 - 2P_6 - 2P_8)$, which has order four by the following lemma. Thus 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* $2P_3 + 2P_1 - 2P_8 - 2P_6$*, nor* $2P_2 - 2P_1$ *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 conics 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 $\mathcal{L}(2P_6 + 2P_8)$ 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 $\mathcal{L}(2P_6 + 2P_8)$. Finally, there does not exist a bitangent through P_2 and P_1, hence $2P_2 - 2P_1$ is not zero in J. □

4.4. **Proof of Theorem 4.1.** To prove the theorem, we apply Silverman's specialization theorem, Theorem 2.2, to $A = \mathrm{Jac}(Z_{1,t})$, $C = \mathbb{P}^1$ (parametrized by t), and J_t the Jacobian of $Z_{1,t}$. We have to check that the hypothesis of the theorem is satisfied. If J_t had a constant part, say A_0, we would have a nonconstant map $\phi_t : A_0 \hookrightarrow J_t$, hence the composition with one of the three maps $\pi_i : J_t \to \mathcal{E}_i$ would be nonconstant, hence surjective. But none of the three j-invariants of the elliptic curves is constant, hence a contradiction. Indeed,

$$j(\mathcal{E}_1) = 256\,\frac{(t^2 - t + 1)^3(t^2 + t + 1)^3}{t^4(t - i)^2(t + i)^2},$$

$$j(\mathcal{E}_2) = -16\,\frac{(t^2 - 4t + 1)^3(t^2 + 4t + 1)^3}{t^2(t - i)^4(t + i)^4}$$

and

$$j(\mathcal{E}_3) = 64\,\frac{(t^4 - 2t^3 + 6t^2 - 2t + 1)^3}{t^2(t - 1)^4(t - i)^2(t + i)^2}.$$

5. Curve with eight hyperflexes

There is exactly one curve not in the family of the preceding section with eight hyperflexes [15]. 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

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

We will consider another model of the curve. Let Σ' 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 Σ' is given by

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

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

We will see in Section 5.2.1 that the automorphism group is a dihedral group of order 8 generated by ρ and σ. Let $\tau=\sigma\rho^2$. We can define the Weierstrass points using these automorphisms: The hyperflexes are given by

$$\begin{gathered}P_1=(1:1:2),\qquad P_5=((-\sqrt{7}-1)i-\sqrt{7}+1:(\sqrt{7}-1)i-\sqrt{7}-1:8),\\ P_2=\tau(P_1),\qquad P_3=\rho(P_1),\qquad P_4=\sigma(P_3),\\ P_7=\sigma(P_5),\qquad P_6=\tau(P_7),\qquad P_8=\rho(P_5).\end{gathered}$$

The ordinary flexes are

$$\begin{aligned}&Q_1=(x_0,b),\qquad Q_4=\rho(Q_1),\qquad Q_5=\sigma(Q_1),\qquad Q_7=\tau(Q_1),\\ &Q_8=\rho(Q_5),\qquad Q_2=\sigma(Q_8),\qquad Q_3=\sigma(Q_7),\qquad Q_6=\sigma(Q_4),\end{aligned}$$

where $49\cdot x_0=-((-160i\sqrt{7}+32\cdot 7)\,a+140(i\sqrt{7}+1))\,b^3$.

5.1.1. *Relations between the Weierstrass points.* 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 relations*

- $4(P_n-P_m)=0$,
- $Q_1+Q_2+Q_3+Q_4+Q_5+Q_6+Q_7+Q_8-8P_8=0$,
- $P_1+P_2+P_3+P_4-2P_5-2P_6=0$,
- $P_1+P_2+P_3+P_4-2P_7-2P_8=0$,
- $P_5+P_6+P_7+P_8-2P_1-2P_2=0$,
- $Q_1+Q_3+Q_5+Q_7-P_5-P_6-P_7-P_8=0$,
- $Q_2+Q_4+Q_5+Q_7-2P_7-2P_8=0$.

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

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

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 isogenous 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 Σ' 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

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

Hence, the result follows. □

5.2.1. *Automorphisms of the curve.* The group of automorphisms of the curve is a dihedral group of order 8 ([15]). This group is generated by ρ and σ given by

$$\rho : (X : Y : Z) \mapsto (iX : -iY : Z) \qquad \text{and} \qquad \sigma : (X : Y : Z) \mapsto (Y : X : Z).$$

They act on the Weierstrass points in the following manner:

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

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 4 from Σ' to the elliptic curve $\mathcal{E}_1 = \Sigma'/\langle\rho\rangle$ 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 Σ' to the elliptic curve $\mathcal{E}_2 = \Sigma'/\langle\sigma\rangle$ 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 Σ' to the elliptic curve $\mathcal{E}_3 = \Sigma'/\langle\sigma\rho^2\rangle = \Sigma'/\langle\tau\rangle$ 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,

$$2^8\,a = 70 - 30i\sqrt{7} + 16i\sqrt{7}\sqrt{3i\sqrt{7}+1} \qquad \text{and} \quad b = a^4.$$

5.3.1. *Images of the Weierstrass points on the first elliptic curve.* 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 $\mathcal{E}_1$:

$$P_{1,1} = \phi_1(P_1), \quad P_{1,5} = \phi_1(P_5), \quad Q_{1,1} = \phi_1(Q_1), \quad \text{and} \quad Q_{1,5} = \phi_1(Q_5),$$

which satisfy the following relations

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

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

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

Proof. For primes of inertial degree 1 in M, we compute the reduction of the elliptic curve:

p	i	$\sqrt{7}$	γ	a	$\widetilde{\mathcal{E}}_1$	$\widetilde{Q}_{1,1}$	Order$(\widetilde{Q}_{1,1})$
337	189	218	172	233	$y^2 = x^3 + 318x + 307$	$(236, 139)$	28
569	483	24	270	499	$y^2 = x^3 + 550x + 539$	$(337, 109)$	$8 \cdot 17$

Hence $Q_{1,1}$ has infinite order. □

Remark 5.9. We can also compute the height of the point $Q_{1,1}$ to show it is of infinite order. We do so using an implementation of the height pairing [5] in `magma` [2] and find that $\hat{h}(Q_{1,1}) = 0.53455429$.

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:

$$P_{2,1} = \phi_2(P_1), \quad \phi_2(P_2) = \mathcal{O}, \quad P_{2,3} = \phi_2(P_3), \quad P_{2,5} = \phi_2(P_5), \quad P_{2,6} = \phi_2(P_6),$$
$$Q_{2,1} = \phi_2(Q_1), \quad Q_{2,2} = \phi_2(Q_2), \quad Q_{2,3} = \phi_2(Q_3), \quad Q_{2,4} = \phi_2(Q_4),$$

which satisfy the following relations:

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

where

$$T_0 = ((i\sqrt{7} + 1)/2, 0), \qquad T_1 = ((i\sqrt{7} - 1)/2, 0), \qquad \text{and} \quad T_2 = (-i\sqrt{7}, 0)$$

are the three points of order 2.

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

Proof. We reduce the curve modulo primes of inertial degree 1 in M and compute the orders of the reduced points:

p	i	α	γ	δ	a	b	$\#\widetilde{\mathcal{E}}_2(\mathbb{F}_p)$	Orders$(\widetilde{Q}_{2,1}, \widetilde{Q}_{2,2})$
2657	163	703	2436	1377	2495	2337	$2^6 \cdot 43$	$(2 \cdot 43, 4 \cdot 43)$
569	483	24	270	287	499	214	$2^4 \cdot 37$	$(4 \cdot 37, 4 \cdot 37)$

where

$$\alpha = \sqrt{7}, \qquad \gamma = \sqrt{3i\sqrt{7} + 1}, \qquad \text{and} \quad \delta = \sqrt[4]{70 - 30i\sqrt{7} + 16i\sqrt{7}}\sqrt{3i\sqrt{7} + 1}.$$

Hence, both points $Q_{2,1}$ and $Q_{2,2}$ are of infinite order. Moreover, there are no points of order 23 in $\mathcal{E}_2'(M)$.

We can apply Lemma 3.7 to $P = 2^8\,Q_{2,1}$, $Q = 2^8\,Q_{2,2}$, $l = 23$, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ primes of inertial degree 1 above 337 and 5737, $a_1 = 4$ and $a_2 = 16$: choosing

p	i	α	γ	δ	a	b
337	189	218	172	226	233	225
5737	1126	1033	4903	2889	5361	5025

we obtain that

p	$\widetilde{\mathcal{E}}_2'$	$\#\widetilde{\mathcal{E}}_2'(\mathbb{F}_p)$	l	$\widetilde{P}_1 = 2^8\,\widetilde{Q}_{2,1}$	$\widetilde{Q}_1 = 2^8\,\widetilde{Q}_{2,2}$	α
337	$y^2 = x^3 + 5x + 161$	$2^4 \cdot 23$	23	$(323, 268)$	$(240, 173)$	4
5737	$y^2 = x^3 + 5x + 2906$	$2^8 \cdot 23$	23	$(1347, 718)$	$(267, 4597)$	16

□

Remark 5.11. Here again directly computing the heights of the points and then the regulator shows the independence of the two points. We use the fact that the field of definition of the Weierstrass points is Galois to speed up the computations of the local minimal models at the places over 2 and find that the regulator is nonzero since

$$\det\begin{pmatrix} \langle Q_{2,1}, Q_{2,1}\rangle & \langle Q_{2,1}, Q_{2,2}\rangle \\ \langle Q_{2,2}, Q_{2,1}\rangle & \langle Q_{2,2}, Q_{2,2}\rangle \end{pmatrix} = \begin{vmatrix} 1.04226455 & 0 \\ 0 & 1.04226455 \end{vmatrix} \neq 0.$$

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:

$$\phi_3(P_1) = \mathcal{O}, \quad P_{3,3} = \phi_3(P_3), \quad P_{3,4} = \phi_3(P_4), \quad P_{3,5} = \phi_3(P_5), \quad P_{3,6} = \phi_3(P_6),$$
$$Q_{3,1} = \phi_3(Q_1), \quad Q_{3,2} = \phi_3(Q_2), \quad Q_{3,3} = \phi_3(Q_3), \quad Q_{3,4} = \phi_3(Q_4),$$

which satisfy the following relations:

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

where the two-torsion points T_i are defined in the preceding section.

Lemma 5.12. *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 eleven Weierstrass points. Let us consider a degree 0 divisor whose support is in the set of Weierstrass points, say $m_1P_1 + m_2P_2 + m_3P_3 + m_5P_5 + m_7P_7 + m_8P_8 + n_1Q_1 + n_2Q_2 + n_4Q_4 + n_5Q_5 + n_6Q_6$ 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. We obtain that

$$n_1 = n_2 = n_4 = n_5 = n_6 = 0, \quad 2m_3 \equiv 2m_5 \equiv 0 \bmod 4, \quad m_1 \equiv m_2 \bmod 4,$$
$$m_5 \equiv m_8 - m_7 \bmod 4, \quad \text{and} \quad 2m_1 \equiv 2m_8 + m_3 \bmod 4.$$

If one of the m_i is odd, then twice the divisor is also in the kernel of the isogeny. As before we show that none of the possible divisors with only even coefficients can occur as they would either correspond to a bitangent through two hyperflexes, or give rise to a degree 2 map to the projective line or translate into the existence of a conic tangent to the curve at P_1 or P_2 and two of the three points P_5, P_7, and P_8, which is ruled out by the fifth relation of Proposition 5.2.

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 [15] 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 [3].

Let $\mathcal{M}_3^\circ$ be $\{[C] \in \mathcal{M}_3 \mid C \text{ is nonhyperelliptic}\}$, $M_s = \{[C] \in \mathcal{M}_3^\circ \mid C \text{ has at least } s \text{ hyperflexes}\}$, and $M_s^\circ = \{[C] \in \mathcal{M}_3^\circ \mid C \text{ has exactly } s \text{ hyperflexes}\}$. We follow the definitions and notations of Vermeulen [15] for the irreducible components of M_s°. 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 [13]) 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 [7]).

There are no quartics with either 10 or 11 hyperflexes. There are two curves with exactly nine 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, Theorem 2.1, we can deduce that 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 four 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 $\mathcal{C}$ be a smooth quartic having exactly four hyperflexes. If three 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 four 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 four points.*

The set of curves with four hyperflexes M_4 consists of five 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 $5 \le r \le 15$ 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 $Z_{1,t}$ of Theorem 4.1 is in both Y_3 and Y_4. The curves Ω_i of Theorem 3.1 are in Y_5. The specialization theorem, 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 four hyperflexes. Moreover, the curve $Z_{1,t}$ of Theorem 4.1 is in Y_2. The above lemma and the specialization theorem, Theorem 2.1, give the result. □

Proposition 6.4 ([3])**.** *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 three hyperflexes consists of two irreducible components X_2 and X_3. The set X_1 is in M_3, hence if a curve has three hyperflexes on a line, it lies in X_1 and has at least four 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 three hyperflexes is $(\mathbb{Z}/4\mathbb{Z})^2$, according to the above lemma. Proposition 6.2(i) and the specialization theorem, Theorem 2.1, give the result. □

For completeness, we recall the previous results obtained in [3] for the generic quartic and for the two irreducible strata M_1 and M_2:

Theorem 6.6 ([3])**.** (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 one 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* $F \subset (\mathbb{Z}/4\mathbb{Z})$.

Acknowledgments

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

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I.* Springer-Verlag, New York, 1985. MR0770932 (86h:14019)

[2] W. Bosma and J. Cannon, editors. *Handbook of Magma Functions*, Sydney, 2002. `http://magma.maths.usyd.edu.au/`.

[3] M. Girard. Géométrie du groupe des points de Weierstrass d'une quartique lisse, *Journal of Number Theory*, **94** (2002), 103–135. MR1904965 (2003c:11069)

[4] M. Girard. Groupe des points de Weierstrass sur une famille de quartiques lisses. *Acta Arithmetica*, **105** (2002), 305–321. MR1932565 (2003h:11067)

[5] M. Girard. Code for computing heights of elliptic curves on number fields, `http://www.institut.math.jussieu.fr/~girard/magma/`.
[6] M. Girard. Group of Weierstrass points of a plane quartic with eight hyperflexes or more. Technical report of the Mathematical Institute, Leiden University, June 2002. `http://www.math.leidenuniv.nl/reports/2002-14.shtml`.
[7] M. Girard and P. Tzermias. Group generated by the Weierstrass points of a plane quartic, *Proc. Amer. Math. Soc.*, **130** (2002), 667–672. MR1866017 (2002h:14053)
[8] M. Hindry and J. H. Silverman. *Diophantine Geometry, An Introduction*. Springer-Verlag, New York, 2000. Graduate Texts in Mathematics, 201. MR1745599 (2001e:11058)
[9] J. H. Hubbard. Sur les sections analytiques de la courbe universelle de Teichmüller. *Mem. Amer. Math. Soc.*, 4(166):ix+137, 1976. MR0430321 (55:3326)
[10] M. J. Klassen and E. F. Schaefer. Arithmetic and geometry of the curve $y^3 + 1 = x^4$. *Acta Arith.*, **74** (1996), 241–257. MR1373711 (96k:11081)
[11] D. Laksov and A. Thorup. Weierstrass points and gap sequences for families of curves. *Ark. Mat.*, **32** (1994), 393–422. MR1318539 (96b:14041)
[12] D. T. Prapavessi. On the Jacobian of the Klein curve. *Proc. Amer. Math. Soc.*, **122** (1994), 971–978. MR1212286 (95b:14023)
[13] D. E. Rohrlich. Points at infinity on the Fermat curves. *Invent. Math.*, **39** (1977), 95–127. MR0441978 (56:367)
[14] J. H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, **342** (1983), 197–211. MR0703488 (84k:14033)
[15] A. M. Vermeulen. *Weierstrass points of weight two on curves of genus three*. Ph.D. thesis, Universiteit van Amsterdam, 1983. MR0715084 (84j:14036)

Universiteit Leiden, Mathematisch Instituut, 2300 R. A. Leiden, The Netherlands
Current address: School of Mathematics and Statistics, The University of Sydney, New South Wales, NSW 2006, Australia
E-mail address: `girard@maths.usyd.edu.au`