Formal groups, supersingular abelian varieties and tame ramification

Sara Arias-de-Reyna

Abstract

Let us consider an abelian variety defined over $\mathbb{Q}_\ell$ with good supersingular reduction. In this paper we give explicit conditions that ensure that the action of the wild inertia group on the ℓ-torsion points of the variety is trivial. Furthermore we give a family of curves of genus 2 such that their Jacobian surfaces have good supersingular reduction and satisfy these conditions. We address this question by means of a detailed study of the formal group law attached to abelian varieties.

1 Introduction

Let ℓ be a prime number and $A/\mathbb{Q}_\ell$ be an abelian variety with good supersingular reduction. In this paper we study the action of the wild inertia group $I_{\mathrm{w}} \subset \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ on the ℓ-torsion points of A. More precisely, we will address the problem of finding explicit conditions that ensure that the Galois extension $\mathbb{Q}_\ell(A[\ell])/\mathbb{Q}_\ell$ obtained by adjoining to the field of ℓ-adic numbers the coordinates of the ℓ-torsion points of A is tamely ramified.

Let $E/\mathbb{Q}_\ell$ be an elliptic curve. If it has good supersingular reduction, then the field extension $\mathbb{Q}_\ell(E[\ell])/\mathbb{Q}_\ell$ is tamely ramified (cf. [13], § 1). The proof relies on a detailed study of the formal group law attached to E. This formal group law has dimension 1 and height 2. The set of elements of

2010 Mathematics Subject Classification: 14L05, 11G10, 11S15
Key words and phrases: tame ramification, formal group, supersingular abelian variety
Research supported by a FPU predoctoral grant AP-20040601 of the MEC and partially supported by MEC grant MTM2006-04895.

$\overline{\mathbb{Q}}_\ell$ with positive ℓ-adic valuation can be endowed with a group structure by means of this formal group law. Call V the $\mathbb{F}_\ell$-vector space of ℓ-torsion points of this group (which is isomorphic to the group of ℓ-torsion points of E as $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-module). One essential ingredient in the proof is the fact that the ℓ-adic valuation of the points of V can be explicitly computed (see Proposition 9, § 1.9 of [13]). This fact allows one to define an embedding of V into a certain 1-dimensional $\overline{\mathbb{F}}_\ell$-vector space (called V_α in [13]) where the wild inertia group acts trivially, and in turn this compels the wild inertia group to act trivially upon V. When the dimension n of the formal group law is greater than 1 the situation becomes more complicated. It is no longer possible to compute the ℓ-adic valuation of the n coordinates of the elements of V, which now denotes the group of ℓ-torsion points of the corresponding formal group. In this paper we give a condition, Hypothesis 3.2, under which we can prove that the wild inertia group acts trivially on V. The key point is that this hypothesis allows us to define several different embeddings of V into V_α.

In the rest of the paper we apply this result to the case of dimension 2, and produce non-trivial examples of abelian surfaces defined over $\mathbb{Q}_\ell$ such that the ramification of $\mathbb{Q}_\ell(A[\ell])/\mathbb{Q}_\ell$ is tame. We introduce the notion of *symmetric* 2-dimensional formal group law, and prove that such a formal group law satisfies Hypothesis 3.2 under a certain condition. Furthermore, using this result we explicitly construct, for each $\ell \geq 5$, genus 2 curves over $\mathbb{Q}_\ell$ such that the formal group law attached to their Jacobians satisfy Hypothesis 3.2 (cf. Theorem 5.8). Finally we formulate a condition that allows us to deform the curves and enlarge the family of genus 2 curves such that the Galois extension defined by the ℓ-torsion points of their Jacobians is tamely ramified, which enables us to obtain Theorem 6.4.

Given a prime ℓ, in [2] the authors contruct certain semistable elliptic curves defined over $\mathbb{Q}$ with good supersingular reduction at ℓ. When $\ell \geq 11$, these curves provide tame Galois realizations of the group $\mathrm{GL}_2(\mathbb{F}_\ell)$. In this way, the authors give an affirmative answer to the tame inverse Galois problem posed by B. Birch in [5], Section 2, for the family of linear groups $\mathrm{GL}_2(\mathbb{F}_\ell)$.

In [3], we will use the results in this paper in order to realize the groups in the family $\mathrm{GSp}_4(\mathbb{F}_\ell)$ as the Galois group of a tamely ramified extension for each prime $\ell \geq 5$.

The contents of this paper are part of my Ph.D. thesis. I want to thank my advisor, Prof. Núria Vila, for her constant support and helpful conversations.

2 Notation

We will denote by K a local field of characteristic zero and residual characteristic ℓ, v the corresponding discrete valuation, normalized so that $v(K^*) = \mathbb{Z}$, $\mathcal{O}$ the ring of integers of the valuation and k the residue field. Further, we will assume that $v(\ell) = 1$ (that is to say, K will be an unramified extension of $\mathbb{Q}_\ell$). We fix an algebraic closure $\overline{K}$ of K, and denote by v the extension of v to this algebraic closure. Finally, $\overline{k}$ denotes the algebraic closure of k obtained through the reduction of $\mathcal{O}_{\overline{K}}$, the ring of integers of $\overline{K}$ with respect to v, modulo its maximal ideal. Later in the paper, we will take $K = \mathbb{Q}_\ell$.

We will denote by $I \subset \mathrm{Gal}(\overline{K}/K)$ the inertia group, and by I_{w} the wild inertia group.

To ease notation, we will denote the tuples of elements in boldface. For instance, we will write $\mathbf{X} = (X_1, \ldots, X_n)$, $\mathbf{Y} = (Y_1, \ldots, Y_n)$, $\mathbf{Z} = (Z_1, \ldots, Z_n)$ to denote n-tuples of variables, and $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ will denote tuples of elements of $\overline{K}$.

3 Inertia action and the formal group law

We will start by recalling that an *n-dimensional formal group law* defined over $\mathcal{O}$ is a n-tuple of power series

$$(F_1(\mathbf{X}, \mathbf{Y}), \ldots, F_n(\mathbf{X}, \mathbf{Y})) \in \mathcal{O}[[X_1, \ldots, X_n, Y_1, \ldots, Y_n]]^{\times n}$$

satisfying:

- $F_i(\mathbf{X}, \mathbf{Y}) \equiv X_i + Y_i \pmod{\text{terms of degree two}}$,
  for all $i = 1, \ldots, n$.
- $F_i(F_1(\mathbf{X}, \mathbf{Y}), \ldots, F_n(\mathbf{X}, \mathbf{Y}), \mathbf{Z}) = F_i(\mathbf{X}, F_1(\mathbf{Y}, \mathbf{Z}), \ldots, F_n(\mathbf{Y}, \mathbf{Z}))$
  for all $i = 1, \ldots, n$.

Besides, if $F_i(\mathbf{X}, \mathbf{Y}) = F_i(\mathbf{Y}, \mathbf{X})$ for all $i = 1, \ldots, n$, then the formal group law is said to be *commutative*.

To a formal power series one can attach a group. Let us denote by $\overline{\mathfrak{m}}$ the set of elements of $\overline{K}$ with positive valuation, and denote by $\overline{\mathfrak{m}}^{\times n}$ the cartesian product of $\overline{\mathfrak{m}}$ with itself n times. For this set one can define an addition law

$\oplus_F$ by

$$\oplus_{\mathbf{F}} : \overline{\mathfrak{m}}^{\times n} \times \overline{\mathfrak{m}}^{\times n} \to \overline{\mathfrak{m}}^{\times n}$$
$$(\mathbf{x}, \mathbf{y}) \mapsto (F_1(\mathbf{x}, \mathbf{y}), \ldots, F_n(\mathbf{x}, \mathbf{y}))$$

(which is well defined since $F_i(\mathbf{x}, \mathbf{y})$ converges to an element of $\overline{\mathfrak{m}}$, for all $i = 1, \ldots n$). The set $\overline{\mathfrak{m}}^{\times n}$, endowed with this sum, turns out to be a group, which will be denoted by $\mathbf{F}(\overline{\mathfrak{m}})$. Let us call V the $\mathbb{F}_\ell$-vector space of ℓ-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$.

In [13], § 8, an auxiliary object is introduced.

Definition 3.1. Let $\alpha \in \mathbb{Q}$ be a positive rational number. Consider the sets

$$\overline{\mathfrak{m}}_\alpha = \{x \in \overline{\mathfrak{m}} : v(x) \geq \alpha\} \quad \text{and} \quad \overline{\mathfrak{m}}_\alpha^+ = \{x \in \overline{\mathfrak{m}} : v(x) > \alpha\}.$$

We define V_α as the quotient group

$$V_\alpha := \overline{\mathfrak{m}}_\alpha / \overline{\mathfrak{m}}_\alpha^+.$$

V_α has a natural structure of $\overline{k}$-vector space, and its dimension as such is 1. Moreover, the absolute Galois group of K acts on V_α: for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, and for each $x + \overline{\mathfrak{m}}_\alpha^+ \in \overline{\mathfrak{m}}_\alpha / \overline{\mathfrak{m}}_\alpha^+$, we have $\sigma(x + \overline{\mathfrak{m}}_\alpha^+) := \sigma(x) + \overline{\mathfrak{m}}_\alpha^+$. In general, this action does not respect the $\overline{k}$-vector space structure. But if we take an element σ in the inertia group I, it induces a morphism of $\overline{k}$-vector space on V_α, and in turn this implies that the wild inertia group I_{w} acts trivially on V_α (cf. § 1.8 in [13]). The main point in the proof, in dimension 1, that the wild inertia group acts trivially on V is to define an embedding of V into V_α, taking advantage of the fact that the valuation of the points of V is equal to $\alpha = \frac{1}{\ell^2 - 1}$.

But, in the case when $n > 1$, each point has n coordinates, and we have to admit the possibility that the valuations of the coordinates of the ℓ-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$ have different values. Our idea is to formulate a weaker assumption about the valuations of the coordinates, but which is strong enough to imply the desired result about the action of the wild inertia group I_{w} on $\mathbf{F}(\overline{\mathfrak{m}})$.

Hypothesis 3.2. *There exists a positive $\alpha \in \mathbb{Q}$ such that, for all non-zero $(x_1, \ldots, x_n) \in V$, it holds that*

$$\min_{1 \leq i \leq n} \{v(x_i)\} = \alpha.$$

Under this hypothesis, we are able to prove the desired result:

Theorem 3.3. *Let* $\mathbf{F}$ *be a formal group law such that the* $\mathbb{F}_\ell$*-vector space* V *of the* ℓ*-torsion points of* $\mathbf{F}(\overline{\mathfrak{m}})$ *satisfies Hypothesis 3.2. Then the image of the wild inertia group* I_{w} *by the Galois representation attached to* V *is trivial.*

Proof. Let $P = (x_1, \ldots, x_n) \in V$. We are going to show that each $\sigma \in I_{\mathrm{w}}$ acts trivially on P, that is, $\sigma(P) = P$.

According to Hypothesis 3.2, we have that, for each non-zero point $Q = (y_1, \ldots, y_n) \in V$,

$$\min_{1 \leq i \leq n} \{v(y_i)\} = \alpha.$$

Therefore, for each n-tuple $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$, we know that either $\lambda_1 y_1 + \cdots \lambda_n y_n = 0$ or else it belongs to $\overline{\mathfrak{m}}_\alpha$. This allows us to consider the following map:

$$\begin{aligned} \varphi_{(\lambda_1,\ldots,\lambda_n)} : V &\to V_\alpha = \overline{\mathfrak{m}}_\alpha / \overline{\mathfrak{m}}_{\alpha^+} \\ (y_1, \ldots, y_n) &\mapsto \lambda_1 y_1 + \cdots \lambda_n y_n + \overline{\mathfrak{m}}_\alpha^+. \end{aligned}$$

It is clear that $\varphi_{(\lambda_1,\ldots,\lambda_n)}$ is a group morphism, when we consider on V the sum given by the formal group law, and on V_α the sum induced by that of $\overline{K}$. As a matter of fact, it is a morphism of $\mathbb{F}_\ell$-vector spaces (for the structure of $\mathbb{F}_\ell$-vector space is determined by the sum). Besides, it is compatible with the Galois action.

Now let us take an element $\sigma \in I_{\mathrm{w}}$. Then

$$\varphi_{(\lambda_1,\ldots,\lambda_n)}(\sigma(P)) = \sigma(\varphi_{(\lambda_1,\ldots,\lambda_n)}(P)) = \varphi_{(\lambda_1,\ldots,\lambda_n)}(P),$$

where the last equation holds because I_{w} acts trivially upon V_α. In other words, for each n-tuple $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$, $\sigma(P) - P$ belongs to the kernel of $\varphi_{(\lambda_1,\ldots,\lambda_n)}$. But no point of V can belong to all these kernels save the zero vector. This, again, is a consequence of Hypothesis 3.2. Any non-zero point $Q = (y_1, \ldots, y_n) \in V$ satisfies that there exists $j \in \{1, \ldots, n\}$ such that $v(y_j) = \alpha$. If we take $\lambda_i = 0$ for all $i \neq j$, $\lambda_j = 1$, then $\varphi_{(\lambda_1,\ldots,\lambda_n)}(P) = x_j + \overline{\mathfrak{m}}_\alpha^+ \neq 0 + \overline{\mathfrak{m}}_\alpha^+$.

To sum up, for each $P \in V$ and each $\sigma \in I_{\mathrm{w}}$, $\sigma(P) - P = (0, \ldots, 0)$, and so σ acts trivially on P.

□

4 Symmetric formal group laws of dim 2

Let $\mathbf{F}$ be a formal group law over $\mathbb{Q}_\ell$ of dimension 2. Our aim is to analyze the valuation of the ℓ-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$, and try to obtain explicit conditions that ensure that Hypothesis 3.2 holds. The property of being ℓ-torsion provides us with two equations in two variables. Let us briefly recall these equations. We begin by recalling the definition of homomorphism between formal group laws of dimension n.

Definition 4.1. Let $\mathbf{F} = (F_1(\mathbf{X}, \mathbf{Y}), \dots, F_n(\mathbf{X}, \mathbf{Y}))$ and $\mathbf{G} = (G_1(\mathbf{X}, \mathbf{Y}), \dots G_n(\mathbf{X}, \mathbf{Y}))$ be two formal group laws over $\mathcal{O}$ of dimension n. A *homomorphism* f is a n-tuple of formal power series in $\mathcal{O}[[Z_1, \dots, Z_n]]$ without constant term, say $(f_1(\mathbf{Z}), \dots, f_n(\mathbf{Z}))$, such that

$$\begin{aligned} f(F_1(\mathbf{X}, \mathbf{Y}), \dots, F_n(\mathbf{X}, \mathbf{Y})) = \\ = (G_1(f_1(\mathbf{X}), \dots, f_n(\mathbf{X}), f_1(\mathbf{Y}), \dots, f_n(\mathbf{Y})), \\ \dots, G_n(f_1(\mathbf{X}), \dots, f_n(\mathbf{X}), f_1(\mathbf{Y}), \dots, f_n(\mathbf{Y}))). \end{aligned}$$

Example 4.2. For each $m \in \mathbb{N}$, one can define the multiplication by m map in the following way:

$$\begin{cases} [0](\mathbf{Z}) = (0, 0, \dots, 0) \\ [1](\mathbf{Z}) = \mathbf{Z} \\ [m+1](\mathbf{Z}) = \mathbf{F}([1](\mathbf{Z}), [m](\mathbf{Z})) \text{ for } m \geq 1. \end{cases}$$

It is easy to prove by induction that the shape of the n power series $[m]_i(\mathbf{Z})$ that constitute the multiplication by m map is the following:

$$[m]_i(\mathbf{Z}) = m \cdot Z_i + \text{ terms of degree } \geq 2,$$

for all $i = 1, \dots, n$.

When $n = 2$, the multiplication by ℓ map is defined by two equations in two variables, and this complicates our attempt to compute the valuations of the two coordinates of the points of V. In order to avoid this inconvenience, we are going to restrict our attention to a special kind of formal group laws. Namely, we will consider formal group laws such that the two equations have a certain relationship that allows us to reduce the problem to studying a single equation.

Definition 4.3. Let $\mathbf{F} = (F_1(X_1, X_2, Y_1, Y_2), F_2(X_1, X_2, Y_1, Y_2))$ be a formal group law of dimension 2 over $\mathbb{Q}_\ell$. We will say that $\mathbf{F}$ is a *symmetric formal group law* if the following relationship holds:

$$F_2(X_2, X_1, Y_2, Y_1) = F_1(X_1, X_2, Y_1, Y_2).$$

The symmetry is reflected in the power series $[\ell]_1(Z_1, Z_2)$ and $[\ell]_2(Z_1, Z_2)$. By induction on m, one can prove the following lemma.

Lemma 4.4. *Let $\mathbf{F}(\mathbf{X}, \mathbf{Y})$ be a symmetric formal group law of dimension 2. For all $m \geq 1$, it holds that*

$$[m]_2(Z_2, Z_1) = [m]_1(Z_1, Z_2).$$

Next we will establish two technical lemmas which will be useful.

Lemma 4.5. *Let $\ell > 2$ be a prime number, $r \in \mathbb{N}$, and let $f(Z_1, Z_2) \in \mathbb{Z}_\ell[[Z_1, Z_2]]$ be a formal power series such that $f(Z_2, Z_1) = -f(Z_1, Z_2)$, which can be written as:*

$$\begin{aligned} f(Z_1, Z_2) = \ell \cdot (Z_1 - Z_2) + \ell \cdot (&\textit{terms of total degree} \geq 2 \textit{ and} < \ell^r) \\ &+ a \cdot (Z_1^{\ell^r} - Z_2^{\ell^r}) + \textit{ terms of total degree} \geq \ell^r + 1, \end{aligned}$$

where $\ell \nmid a$. Then if $(x_0, y_0) \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ with $x_0 \neq y_0$ satisfies $f(x_0, y_0) = 0$ and furthermore $v(x_0), v(y_0) \geq v(x_0 - y_0)$, then the ℓ-adic valuation $v(x_0 - y_0)$ is $1/(\ell^r - 1)$.

Proof. Let us call $\beta = v(x_0 - y_0)$. We will compute the valuations of the different terms that appear in the equality $f(x_0, y_0) = 0$.

- $v(\ell \cdot (x_0 - y_0)) = 1 + \beta$.
- Let us consider a term of total degree between 2 and $\ell^r - 1$, say $\ell \cdot c x_0^n y_0^m$. Compute its valuation: $v(\ell \cdot c x_0^n y_0^m) = 1 + v(c) + nv(x_0) + mv(y_0) \geq 1 + (n + m)\beta > 1 + \beta$, since $n + m \geq 2$.
- Let us consider the term $a(x_0^{\ell^r} - y_0^{\ell^r})$. Let us split it into the sum of two terms, in the following way:

$$a \cdot (x_0^{\ell^r} - y_0^{\ell^r}) = a \cdot ((x_0 - y_0)^{\ell^r} - B) = a \cdot (x_0 - y_0)^{\ell^r} - a \cdot B,$$

where $B = (x_0 - y_0)^{\ell^r} - (x_0^{\ell^r} - y_0^{\ell^r})$.

On the one hand, $v(a \cdot (x_0 - y_0)^{\ell^r}) = v(a) + \ell^r \beta = \ell^r \beta$, since ℓ does not divide a.

On the other hand, note that

$$(x_0 - y_0)^{\ell^r} = x_0^{\ell^r} - \binom{\ell^r}{1} x_0^{\ell^r - 1} y_0 + \binom{\ell^r}{2} x_0^{\ell^r - 2} y_0^2 + \cdots \\ - \binom{\ell^r}{2} x_0^2 y_0^{\ell^r - 2} + \binom{\ell^r}{1} x_0 y_0^{\ell^r - 1} - y_0^{\ell^r}.$$

Therefore, each of the terms $\binom{\ell^r}{i}(-1)^i x_0^{\ell^r - i} y_0^i$ has a valuation strictly greater than $1 + \beta$. (For $v(x_0^{\ell^r - i} y_0^i) \geq \beta(\ell^r - i + i) = \ell^r \beta$, and hence $v(\binom{\ell^r}{i}(-1)^i x_0^{\ell^r - i} y_0^i) \geq 1 + \beta \ell^r > 1 + \beta$).

- Since $v(x_0), v(y_0) \geq \beta$, it is clear that the valuation of the terms of degree greater than ℓ^r is greater than $\ell^r \beta$.

But obviously there must be (at least) two terms with minimal valuation, since they must cancel out. Therefore $v(\ell \cdot (x_0 - y_0)) = v(a \cdot (x_0 - y_0)^{\ell^r})$, that is to say, $1 + \beta = \ell^r \beta$, hence $\beta = 1/(\ell^r - 1)$, as was to be proven.

□

Lemma 4.6. *Let $\ell > 2$ be a prime number, $r \in \mathbb{N}$, and let $f(Z_1, Z_2) \in \mathbb{Z}_\ell[[Z_1, Z_2]]$ be a formal power series such that $f(Z_2, Z_1) = f(Z_1, Z_2)$, which can be written as:*

$$f(Z_1, Z_2) = \ell \cdot (Z_1 + Z_2) + \ell \cdot (\textit{terms of total degree} \geq 2 \textit{ and} < \ell^r) \\ + a \cdot (Z_1^{\ell^r} + Z_2^{\ell^r}) + \textit{ terms of total degree} \geq \ell^r + 1,$$

where $\ell \nmid a$. Then if $(x_0, y_0) \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ satisfies $f(x_0, y_0) = 0$ and furthermore $v(x_0), v(y_0) \geq v(x_0 + y_0)$, then $v(x_0 + y_0)$ is $1/(\ell^r - 1)$.

Proof. Analogous to that of Lemma 4.5. □

We want to apply the previous lemmas to the formal power series defined by $[\ell]_1(Z_1, Z_2) - [\ell]_2(Z_1, Z_2)$ and $[\ell]_1(Z_1, Z_2) + [\ell]_2(Z_1, Z_2)$. In order to do this, we need to know the value of the parameter r that appears in these formal power series. This parameter is related to the height of the formal group law.

Let us recall this notion (see [10], Chapter IV, (18.3.8)). Firstly, we need to define this concept for formal group laws defined over k, and then we will transfer this definition to formal group laws over $\mathcal{O}$ through the reduction map.

Definition 4.7. Let $\overline{\mathbf{F}}$ be a formal group law of dimension n over k, and let $\overline{[\ell]} = (\overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z}))$ be the multiplication by ℓ map. Then $\overline{\mathbf{F}}$ is of *finite height* if the ring $k[[Z_1, \ldots, Z_n]]$ is finitely generated as a module over the subring $k[[\overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z})]]$.

When $\overline{\mathbf{F}}$ is of finite height, it holds that $k[[Z_1, \ldots, Z_n]]$ is a free module over $k[[\overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z})]]$ of rank equal to a power of ℓ, say ℓ^h. This h shall be called the *height of* $\overline{\mathbf{F}}$.

Definition 4.8. Let $\mathbf{F}$ be a formal group law of dimension n over $\mathcal{O}$. We define the *height* of $\mathbf{F}$ as the height of the reduction $\overline{\mathbf{F}}$ of $\mathbf{F}$ modulo the maximal ideal of $\mathcal{O}$.

Remark 4.9. A few words concerning the way to compute the height of a formal group law are in order. Let $\overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z})$ be n formal power series in $k[[Z_1, \ldots, Z_n]]$ without constant term. Note that the following statements are equivalent:

- $k[[Z_1, \ldots, Z_n]]$ is generated by h elements as a module over the subring $k[[\overline{f}_1, \ldots, \overline{f}_n]]$.
- $k[[Z_1, \ldots, Z_n]]/\langle \overline{f}_1, \ldots, \overline{f}_n \rangle$ is a k-vector space of finite dimension less than or equal to h.

Therefore, to compute the height of $\overline{\mathbf{F}}$, one seeks the least h that satisfies the last property, that is, the dimension of the k-vector space

$$k[[Z_1, \ldots, Z_n]]/\langle \overline{f}_1, \ldots, \overline{f}_n \rangle.$$

But this can be easily done by means of standard bases. For the definition and some properties of standard bases in power series rings we refer the reader to [4]. If I is an ideal of $k[[X_1, \ldots, X_n]]$, then the dimension of $k[[X_1, \ldots, X_n]]/I$ as a k-vector space is determined in this way: Take a standard basis S of I, and consider the set of terms $M = \{t \in T : \text{ for all } g \in S, \mathrm{LT}(g) \nmid t\}$. Then the cardinal of M is the required dimension (of course, it need not be finite).

Now, if we have a formal group law $\overline{\mathbf{F}}$ over k of dimension n, its height is the dimension of $k[[Z_1, \ldots, Z_n]]/\langle \overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z}) \rangle$, so we can compute it in an explicit way.

In the case when the formal group law is of dimension 1, another definition of height is used (see for instance [14], Chapter IV, § 7). Namely, if $\overline{F}(X,Y)$ is a formal group law defined over k, the height of $\overline{F}$ is defined as the largest r such that the multiplication by ℓ map, $\overline{[\ell]}(Z)$, can be expressed as $\overline{[\ell]}(Z) = \overline{g}(Z^{\ell^r})$, for some formal power series $\overline{g}(Z) \in k[[Z]]$. One can prove, following a simple reasoning, that the first term of g with non-zero coefficient is precisely a constant times Z^{ℓ^r}. Now what happens if we try to imitate this reasoning in dimension n? As is stated in [10], the reasonings in (18.3.1) can be carried out in arbitrary dimension, yielding the following result:

Proposition 4.10. *Let $\overline{\mathbf{F}}$, $\overline{\mathbf{G}}$ be formal group laws over k of dimension n, and $\overline{\mathbf{f}} : \overline{\mathbf{F}} \to \overline{\mathbf{G}}$ a non-zero homomorphism. Let us write*

$$\overline{\mathbf{f}}(\mathbf{Z}) = (\overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z})).$$

If u is the smallest exponent such that, in some $\overline{f}_i(\mathbf{Z})$, some variable Z_j occurs in a non-zero monomial raised to the u-th power, then $u = \ell^r$ for some $r \geq 0$. Furthermore, there exist $\overline{g}_1(\mathbf{Z}), \ldots, \overline{g}_n(\mathbf{Z}) \in k[[Z_1, \ldots, Z_n]]$ such that

$$\overline{f}_i(\mathbf{Z}) = \overline{g}_i(\mathbf{Z}^{\ell^r}), \text{ for all } i = 1, \ldots, n,$$

where $\mathbf{Z}^{\ell^r} = (Z_1^{\ell^r}, \ldots, Z_n^{\ell^r})$.

Remark 4.11. We can apply this proposition to the homomorphism $\overline{[\ell]}$ of multiplication by ℓ in a formal group law $\overline{\mathbf{F}}$, and conclude that there exists an $r \geq 0$ (in fact r will be greater than or equal to 1) such that the formal power series $\overline{[\ell]}_i(\mathbf{Z})$, $i = 1, \ldots, n$, can be expressed as formal power series in the variables $Z_1^{\ell^r}, \ldots, Z_n^{\ell^r}$. But this r might not be determined by the height of $\overline{\mathbf{F}}$. For instance, it might be the case that the height of $\overline{\mathbf{F}}$ is infinite, while the exponent r must always be a finite number. The following proposition deals with this matter.

Proposition 4.12. *Let $\overline{\mathbf{F}}$ be a 2-dimensional formal group law defined over $\mathbb{F}_\ell$, and assume that there exist two power series in $\mathbb{F}_\ell[[Z_1, Z_2]]$, say $\overline{f}_1, \overline{f}_2$, such that the formal power series that give multiplication by ℓ map $\overline{[\ell]}$ can be written as*

$$\begin{cases} \overline{[\ell]}_1(Z_1, Z_2) = \overline{f}_1(Z_1^{\ell^r}, Z_2^{\ell^r}), \\ \overline{[\ell]}_2(Z_1, Z_2) = \overline{f}_2(Z_1^{\ell^r}, Z_2^{\ell^r}). \end{cases}$$

Then the height of $\overline{\mathbf{F}}$ is greater than or equal to $2r$.

Proof. Let us write

$$\begin{cases} \overline{f}_1(Z_1, Z_2) = a_{11}Z_1 + a_{12}Z_2 + \text{terms of degree} \geq 2 \\ \overline{f}_2(Z_1, Z_2) = a_{21}Z_1 + a_{22}Z_2 + \text{terms of degree} \geq 2. \end{cases}$$

We may assume that one element (at least) of the set $\{a_{11}, a_{12}, a_{21}, a_{22}\}$ does not vanish, say $a_{11} \neq 0$ (the other cases are analogous).

Consider the graduated lexicographical ordering on $\mathbb{F}_\ell[[Z_1, Z_2]]$ with $Z_1 < Z_2$, that is to say, the relation $\leq$ determined by the following rules:

$$Z_1^a Z_2^b < Z_1^c Z_2^d \leftrightarrow \begin{cases} a + b < c + d \text{ or} \\ a + b = c + d \text{ and } a > c. \end{cases}$$

Let I be the ideal generated by $\overline{f}_1(Z_1, Z_2)$ and $\overline{f}_2(Z_1, Z_2)$. In order to compute the height of $\overline{\mathbf{F}}$, we need to find a standard basis for I. Now the smallest monomial with respect to this ordering is Z_1. And this monomial appears in $\overline{f}_1(Z_1, Z_2)$. We can therefore use it to eliminate all monomials under a given degree of $\overline{f}_2(Z_1, Z_2)$, save those which are pure in Z_2. In fact, if $\overline{f}_2(Z_1, Z_2)$ is not a multiple of $\overline{f}_1(Z_1, Z_2)$, we will reach a point where the power series $\overline{g}_2(Z_1, Z_2)$ obtained from $\overline{f}_2$ by eliminating the terms divisible by Z_1 up to a certain degree has as leading term a monomial which is pure in Z_2, say $\overline{g}_2(Z_1, Z_2) = b_{0,t}Z_2^t +$ terms of degree $\geq t + 1$. Then it is easily seen that $\{\overline{f}_1, \overline{g}_2\}$ is a standard basis for I, and the rank of $\mathbb{F}_\ell[[Z_1, Z_2]]/I$ as a $\mathbb{F}_\ell$-module is t.

Recall that the height of $\overline{\mathbf{F}}$ is the rank of $\mathbb{F}_\ell[[Z_1, Z_2]]/\langle \overline{[\ell]}_1, \overline{[\ell]}_2 \rangle$. Clearly this rank is $\ell^r \cdot (\ell^r t) = \ell^{2r} t$. But we know that t must be a power of ℓ (see Definition 4.7), say t is of the form ℓ^s for some $s \in \mathbb{N}$. Hence the height of $\overline{\mathbf{F}}$ is $2r + s$, which is greater than (or equal to) $2r$.

□

Remark 4.13. Note that the height of a formal group law of dimension 2 must be comprised between 2 and 4. Actually, the case that interests us is when the height is 4. In this case, only two possibilities might occur:

- The exponent r in Proposition 4.10 is 2. By Proposition 4.12, there exists an $s \in \mathbb{N}$ such that $4 = 2r + s = 4 + s$. Hence $s = 0$.
- The exponent r in Proposition 4.10 is 1. Then by Proposition 4.12, there exists an $s \in \mathbb{N}$ such that $4 = 2r + s = 2 + s$. Hence $s = 2$.

Assume $s = 0$. If we write the multiplication by ℓ map as

$$\begin{cases} \overline{[\ell]}_1(Z_1, Z_2) = \overline{a} Z_1^{\ell^2} + \overline{b} Z_2^{\ell^2} + \text{terms of degree} \geq \ell^2 \\ \overline{[\ell]}_2(Z_1, Z_2) = \overline{c} Z_1^{\ell^2} + \overline{d} Z_2^{\ell^2} + \text{terms of degree} \geq \ell^2 \end{cases}$$

then the determinant of the matrix $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ is non-zero.

We will finally state and prove the main theorem of this section:

Theorem 4.14. *Let $\ell > 2$ be a prime number and let $\mathbf{F} = (F_1, F_2)$ be a 2-dimensional symmetric formal group law over $\mathbb{Z}_\ell$. Assume it has height 4 and the exponent in Proposition 4.10 is $r = 2$. Let us denote by V the $\mathbb{F}_\ell$-vector space of ℓ-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$, $\alpha = 1/(\ell^2 - 1)$.*

Then for all $(x_0, y_0) \in V$,

$$\min\{v(x_0), v(y_0)\} = \alpha.$$

Proof. First of all, let us recall that, since the formal group law $\mathbf{F}$ is symmetric and of height 4 with $r = 2$, Remark 4.13 allows us to write the two formal power series that comprise the multiplication by ℓ map in the following way:

$$\begin{cases} [\ell]_1(Z_1, Z_2) = \ell Z_1 + \ell \cdot (\text{terms of total degree} \geq 2 \text{ and} < \ell^2) \\ \qquad\qquad + a \cdot Z_1^{\ell^2} + b \cdot Z_2^{\ell^2} + \text{ terms of degree} \geq \ell^2 + 1 \\ [\ell]_2(Z_1, Z_2) = \ell Z_2 + \ell \cdot (\text{terms of total degree} \geq 2 \text{ and} < \ell^2) \\ \qquad\qquad + b \cdot Z_1^{\ell^2} + a \cdot Z_2^{\ell^2} + \text{ terms of degree} \geq \ell^2 + 1 \end{cases}$$

with $\ell \nmid a^2 - b^2$.

Take a point $P = (x_0, y_0) \in V$. We split the proof in two cases.

Case 1: $v(x_0) \neq v(y_0)$. Assume that $v(x_0) < v(y_0)$ (otherwise we proceed analogously). Then $v(x_0 - y_0) = v(x_0)$. We will apply Lemma 4.5 with $r = 2$. The point (x_0, y_0) satisfies both equations $[\ell]_1(x_0, y_0) = 0$ and $[\ell]_2(x_0, y_0) = 0$. Therefore it also satisfies that $f(x_0, y_0) = [\ell]_1(x_0, y_0) - [\ell]_2(x_0, y_0) = 0$. Furthermore, taking into account the previous considerations, we can write

$$\begin{aligned} f(Z_1, Z_2) = \ell(Z_1 - Z_2) + \\ + \ell \cdot (\text{terms of total degree} \geq 2 \text{ and} < \ell^2) + (a - b) \cdot (Z_1^{\ell^2} - Z_2^{\ell^2}) + \\ + \text{ terms of degree greater than or equal to } \ell^2 + 1, \end{aligned}$$

and $\ell \nmid a - b$. Nothing prevents us now from applying Lemma 4.5 and concluding that $v(x_0 - y_0) = \alpha$. But then $\alpha = v(x_0) < v(y_0)$, hence $\min\{v(x_0), v(y_0)\} = \alpha$.

Case 2: $v(x_0) = v(y_0)$. Then either $v(x_0 - y_0) = v(x_0)$ or $v(x_0 + y_0) = v(x_0)$. (For both must be greater than or equal to $v(x_0)$. And taking into account that $\ell \neq 2$, we obtain $v(x_0) = v(2x_0) = v((x_0 + y_0) + (x_0 - y_0))$, so both $v(x_0 + y_0)$ and $v(x_0 + y_0)$ cannot be greater than $v(x_0)$). If $v(x_0 - y_0) = v(x_0)$, we can apply Lemma 4.5 as in the previous case and conclude that $v(x_0) = v(y_0) = \alpha$. If $v(x_0 + y_0) = v(x_0)$, we make use of Lemma 4.6 with $f = [\ell]_1 + [\ell]_2$ and $r = 2$, thus concluding that $v(x_0) = v(y_0) = \alpha$. This completes the proof.

□

Combining this theorem with Theorem 3.3, we obtain the following result:

Theorem 4.15. *Let $\ell > 2$ be a prime number, and let $\mathbf{F} = (F_1, F_2)$ be a 2-dimensional symmetric formal group law over $\mathbb{Z}_\ell$. Assume it has height 4 and the exponent in Proposition 4.10 is $r = 2$. Then the wild inertia group I_w acts trivially on the $\mathbb{F}_\ell$-vector space of ℓ-torsion points of $\mathbf{F}(\overline{\mathfrak{m}})$.*

5 Symmetric genus 2 curves

In this section we are going to present a certain kind of genus 2 curves such that their Jacobians are abelian surfaces with good supersingular reduction, and moreover the corresponding formal group law satisfies the hypotheses of Theorem 4.15. Let us fix an odd prime number ℓ.

Definition 5.1. We shall call a genus 2 curve *symmetric* if it can be expressed through an equation $y^2 = f(x)$, where $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ is a polynomial of degree 6 and non-zero discriminant.

In my PhD thesis [1] the following result is proven.

Theorem 5.2. *Let $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Q}_\ell[x]$ be a polynomial of degree 6 and non-zero discriminant, and let $\mathbf{F} = (F_1, F_2)$ be the formal group law attached to the Jacobian variety of the curve defined by $y^2 = f(x)$. Then*

$$F_2(s_2, s_1, t_2, t_1) = F_1(s_1, s_2, t_1, t_2).$$

In this way we can control the symmetry of the formal group law. With respect to the height, it is well known that the formal group law attached to an abelian surface with good supersingular reduction has height 4 (cf. [15]). We will say that a genus 2 curve defined over $\mathbb{F}_\ell$ is supersingular if its Jacobian is a supersingular abelian surface.

Our aim is to construct, for a given prime number $\ell > 3$, a symmetric genus 2 curve over $\mathbb{Q}_\ell$ with supersingular reduction. In fact, what we shall construct is a supersingular genus 2 curve, defined over $\mathbb{F}_\ell$ by an equation $y^2 = \overline{f}(x)$, where $\overline{f}(x) = \overline{f}_0x^6 + \overline{f}_1x^5 + \overline{f}_2x^4 + \overline{f}_3x^3 + \overline{f}_2x^2 + \overline{f}_1x + \overline{f}_0 \in \mathbb{F}_\ell[x]$ is a polynomial of degree 6 with non-zero discriminant. Lifting this equation to $\mathbb{Q}_\ell$ in a suitable way we will obtain the curve we were seeking.

Fix $\ell > 3$, and assume we have a supersingular elliptic curve E defined by $y^2 = x^3 + bx^2 + bx + 1$ for a certain $b \in \mathbb{F}_\ell$. Then the bielliptic curve C defined by the equation $y^2 = x^6 + bx^4 + bx^2 + 1$ is a supersingular genus 2 curve. For the discriminant Δ_f of $f(x) = x^6 + bx^4 + bx^2 + 1$ and the discriminant Δ_g of $g(x) = x^3 + bx^2 + bx + 1$ are related by the equation $\Delta_f = -64\Delta_g$ and the characteristic of our base field is different from 2. On the other hand, C is isogenous to $E \times E$ (cf. [8], Chapter 14), hence the supersingularity of C. Therefore, our problem boils down to finding a supersingular elliptic curve defined by an equation of the form $y^2 = x^3 + bx^2 + bx + 1$.

Recall that an elliptic curve in Legendre form $y^2 = x(x-1)(x-\lambda)$ defined over a finite field of characteristic ℓ is supersingular if and only if $H_\ell(\lambda) = 0$, where $H_\ell(x) = \sum_{k=0}^{\frac{\ell-1}{2}} \binom{\frac{\ell-1}{2}}{k}^2 x^k$ is the Deuring polynomial (see Theorem 4.1-(b) in Chapter IV of [14]). Moreover, there is always a quadratic factor of $H_\ell(x)$ of the form $x^2 - x + a$ for a certain $a \in \mathbb{F}_\ell^*$, provided $\ell > 3$ (see Theorem 1-(b) of [7], cf. Corollary 3.6 of [2]). We exploit this fact in the following proposition.

Proposition 5.3. *Let $a \in \mathbb{F}_\ell$ be such that $x^2 - x + a$ divides $H_\ell(x)$. Then the equation*

$$y^2 = x^3 + \frac{1-a}{a}x^2 + \frac{1-a}{a}x + 1$$

defines a supersingular elliptic curve over $\mathbb{F}_\ell$.

Proof. The discriminant of $g(x) = x^3 + \frac{1-a}{a}x^2 + \frac{1-a}{a}x + 1$ is $\Delta_g = -\frac{(-1+4a)^3}{a^4}$, which does not vanish (if $\Delta_g = 0$, then $a = 1/4$, and the polynomial $x^2 - x + a$ would have a double root. But the Deuring polynomial $H_\ell(x)$ does not have double roots). Moreover, one can easily transform this equation into Legendre form with $\lambda = \frac{1}{2} + \frac{\sqrt{1-4a}}{1}$. □

Remark 5.4. Assume $\ell = 3$. The only supersingular elliptic curve over $\mathbb{F}_3$ is given by the equation $y^2 = x(x-1)(x+1)$. We can study all the changes of variables which turn this equation into a symmetric one, but we only obtain the curve given by $y^2 = x^3 + 1$, which is a singular curve. Therefore, there is no symmetric polynomial $f(x) \in \mathbb{F}_3[x]$ such that the curve defined by $y^2 = f(x)$ is a supersingular elliptic curve. This is the reason why we exclude the prime $\ell = 3$ from our reasonings.

In order to apply Theorem 4.15 to the curves provided by Proposition 5.3, we need to check that the exponent in Proposition 4.10 is $r = 2$. Let us work with the reductions of the Jacobians. First of all, note that this property is preserved by isogenies of degree prime to the characteristic ℓ.

Lemma 5.5. *Let A and B be abelian varieties defined over k, and $\Phi : B \to A$ an isogeny of degree prime to ℓ. Assume moreover that the formal group law attached to B has $r = 2$. Then the formal group law attached to A has $r = 2$ too.*

Proof. Let m be the degree of Φ. We know that there exists an isogeny $\Psi : A \to B$ (the dual isogeny of Φ) such that $\Psi \circ \Phi = \overline{[m]}_B$.

Consider the following commutative diagram:

$$\begin{array}{ccc} B & \xrightarrow{\overline{[\ell]}_B} & B \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} \\ A & \xrightarrow{\overline{[\ell]}_A} & A \end{array}$$

Since $\Phi \circ \overline{[\ell]}_B = \overline{[\ell]}_A \circ \Phi$, $\Phi \circ \overline{[\ell]}_B \circ \Psi = \overline{[\ell]}_A \circ \Phi \circ \Psi$; and thus $\Phi \circ \overline{[\ell]}_B \circ \Psi = \overline{[\ell]}_A \circ \overline{[m]}_A$.

Consider now the homomorphism these arrows induce on the formal group laws on A and B (we will not change their names). Since $\overline{[\ell]}_B$ modulo ℓ can be expressed by means of formal power series in $Z_1^{\ell^2}, Z_2^{\ell^2}$, the same is true of the composition $\Phi \circ \overline{[\ell]}_B \circ \Psi = \overline{[\ell]}_A \circ \overline{[m]}_A$. But since the multiplication by m map in the formal group law of A is defined by

$$\begin{cases} \overline{[m]}_1(Z_1, Z_2) = mZ_1 + \cdots \\ \overline{[m]}_2(Z_1, Z_2) = mZ_2 + \cdots \end{cases}$$

neither of the formal power series that define $\overline{[\ell]}_A$ can possess a term of degree smaller than ℓ^2 (for m is invertible in $\mathbb{F}_\ell$). Taking into account Proposition

4.10, we conclude that the multiplication by ℓ map in A must also be expressible as a formal power series in $Z_1^{\ell^2}, Z_2^{\ell^2}$. $\square$

We will now see that the natural isogeny from $E \times E$ to the Jacobian of C (cf. [8], Chapter 14) satisfies the conditions of the lemma above. We will make use of the following result (cf. Proposition 3 of [11]).

Proposition 5.6. *Let E and F be two elliptic curves over $\mathbb{F}_\ell$, let A be the polarized abelian surface $E \times F$, and let $G \subset A[2](\overline{\mathbb{F}}_\ell)$ be the graph of a group isomorphism $\psi : E[2](\overline{\mathbb{F}}_\ell) \to F[2](\overline{\mathbb{F}}_\ell)$. Then G is a maximal isotropic subgroup of $A[2](\overline{\mathbb{F}}_\ell)$, and furthermore the quotient polarized abelian variety A/G is isomorphic to the Jacobian of a curve C over $\overline{\mathbb{F}}_\ell$, unless ψ is the restriction to $E[2](\overline{\mathbb{F}}_\ell)$ of an isomorphism $E \to F$ over $\overline{\mathbb{F}}_\ell$. Moreover, the curve C and the isomorphisms are defined over $\mathbb{F}_\ell$ if ψ is an isomorphism of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$-modules.*

Let us consider the elliptic curve E defined by the Weierstrass equation $y^2 = x^3 + bx^2 + bx + 1$. The 2-torsion points of E are the following:

$$\begin{aligned} &O \\ &P_1 := (-1, 0) \\ &P_2 := (\frac{1}{2}(1 - b + \sqrt{-3 - 2b + b^2}), 0) \\ &P_3 := (\frac{1}{2}(1 - b - \sqrt{-3 - 2b + b^2}), 0). \end{aligned}$$

Let us consider the group morphism $\psi : E[2](\overline{\mathbb{F}}_\ell) \to E[2](\overline{\mathbb{F}}_\ell)$ defined as

$$O \mapsto O, \;\; P_1 \mapsto P_1, \;\; P_2 \mapsto P_3, \;\; P_3 \mapsto P_2.$$

Note that it is compatible with the action of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. In order to apply Proposition 5.6, we need to check that ψ is not induced from an automorphism of E.

But the group of automorphisms of E is well known (cf. [14], Chapter III, § 10). Namely, if E is an elliptic curve with j-invariant different from 0 or 1728 (that is to say, with b different from 0 or $-3/2$), then the group of automorphisms of E has order 2, and the non-trivial automorphism corresponds to $(x, y) \mapsto (x, -y)$. Therefore, it cannot restrict to the morphism ψ.

In the other cases, the order of $\mathrm{Aut}(E)$ is 4 or 6: it is easy to compute these automorphisms explicitly and check that they cannot restrict to ψ.

Therefore, for each $b \in \mathbb{F}_\ell$ such that the equation $y^2 = x^3 + bx^2 + bx + 1$ defines an elliptic curve E (i.e., $b \neq 3, -1$), Proposition 5.6 tells us that there exists a genus 2 curve C and an isogeny

$$\Phi : E \times E \to J(C)$$

which is separable (because of the definition of the quotient of abelian varieties, cf. § 7 Chapter 2, Theorem on p. 66 of [12]) of degree 4. Moreover, the isogeny can be defined over $\mathbb{F}_\ell$. Therefore, if E is a supersingular elliptic curve we can apply Lemma 5.5 and conclude that the Jacobian of C satisfies that the exponent in Proposition 4.10 is 2. But can C be explicitly determined? Fortunately, Proposition 4 of [11] gives a very explicit recipe for computing C. As a conclusion, we can state the following result.

Proposition 5.7. *Let $b \in \mathbb{F}_\ell$ be such that the Weierstrass equation $y^2 = x^3 + bx^2 + bx + 1$ defines a supersingular elliptic curve over $\mathbb{F}_\ell$. Then the formal group law attached to the Jacobian of the genus 2 curve C defined by a lifting of the hyperelliptic equation*

$$y^2 = x^6 + bx^4 + bx^2 + 1$$

has exponent $r = 2$.

This provides us with all the ingredients to give a family of genus 2 curves such that the action of the wild inertia group on the ℓ-torsion points of their Jacobians is trivial.

Theorem 5.8. *Let $\ell > 3$ be a prime number. Let $\overline{a} \in \mathbb{F}_\ell$ be such that $x^2 - x + \overline{a}$ divides the Deuring polynomial $H_\ell(x)$, and lift it to $a \in \mathbb{Z}_\ell$. Let $f_0, f_1, f_2, f_3 \in \mathbb{Z}_\ell$ such that $f_0 - 1, f_1, f_2 - (1-a)/a, f_3 \in (\ell)$. Then the equation $y^2 = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}_\ell[x]$ defines a genus 2 curve C such that the Galois extension $\mathbb{Q}_\ell(J(C))/\mathbb{Q}_\ell$ is tamely ramified.*

6 Approximation to symmetry

The results in the previous section provide, for each $\ell > 3$, a symmetric genus 2 curve with good supersingular reduction such that its formal group

law satisfies the hypotheses of Theorem 4.15, and in consequence also the hypotheses of Theorem 3.3. But one might argue that these curves are not a good example to illustrate Theorem 3.3, in the sense that they are actually isogenous over $\mathbb{Q}_\ell$ to a product of elliptic curves with good supersingular reduction, and surely one can prove in a more direct fashion that the wild inertia group at ℓ acts trivially. Our aim now is to enlarge this class of curves, and provide other more complicated examples in which Theorem 3.3 applies. The key idea is that we are going to take curves which are "approximately symmetric", that is to say, symmetric up to a certain order with respect to the ℓ-adic valuation. More specifically, we wish to determine how close the coefficients of a hyperelliptic equation of C' must be to those of a hyperelliptic symmetric equation for the condition in Hypothesis 3.2 to be preserved. The main result of this section is the following.

Theorem 6.1. *Let C be a genus 2 curve given by a hyperelliptic equation*

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

where $f_0, \dots, f_6 \in \mathbb{Z}_\ell$, and consider the genus 2 curve $C'/\mathbb{Q}_\ell$ given by the equation

$$y^2 = f'_6x^6 + f'_5x^5 + f'_4x^4 + f'_3x^3 + f'_2x^2 + f'_1x + f'_0$$

with $f'_0, \dots, f'_6 \in \mathbb{Z}_\ell$ and satisfying $f_i - f'_i \in (\ell^4)$. Then if the formal group law attached to the Jacobian of C satisfies Hypothesis 3.2 with $\alpha = \frac{1}{\ell^2-1}$, so does the formal group law attached to the Jacobian of C'.

The rest of the section is devoted to proving this result. Fix a genus 2 curve $C/\mathbb{Q}_\ell$, given by a hyperelliptic equation

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

where $f_0, \dots, f_6 \in \mathbb{Z}_\ell$, and consider the genus 2 curve $C'/\mathbb{Q}_\ell$ given by the equation

$$y^2 = f'_6x^6 + f'_5x^5 + f'_4x^4 + f'_3x^3 + f'_2x^2 + f'_1x + f'_0$$

with $f'_0, \dots, f'_6 \in \mathbb{Z}_\ell$.

Denote by $\mathbf{F} = (F_1, F_2)$ (resp. $\mathbf{F}' = (F'_1, F'_2)$) the formal group law attached to C (resp. C'). It can be proven that the coefficients of F_i (resp. F'_i) lie in $\mathbb{Z}[f_0, \dots, f_6]$ (resp. $\mathbb{Z}[f'_0, \dots, f'_6]$), $i = 1, 2$.

Therefore, if we assume that, for all $i = 0, \dots, 6$, $f_i - f'_i \in (\ell^s)$, then the difference $F_i(s_1, s_2, t_1, t_2) - F'_i(s_1, s_2, t_1, t_2)$ has coefficients in (ℓ^s). Hence we

may drop the curves and work in the formal group setting, since all we have to determine is the exponent s which preserves Hypothesis 3.2.

Denote by $\overline{\mathbb{Q}}_\ell$ an algebraic closure of $\mathbb{Q}_\ell$, and $\overline{\mathfrak{m}} \subset \overline{\mathbb{Q}}_\ell$ the set of elements with positive valuation. If the coefficients of the power series $[\ell]_1(Z_1, Z_2)$, $[\ell]_2(Z_1, Z_2)$ are close (with respect to the ℓ-adic valuation) to the coefficients of the series $[\ell]'_1(Z_1, Z_2), [\ell]'_2(Z_1, Z_2)$, does this imply that the solutions of the system of equations $[\ell]_1(Z_1, Z_2) = [\ell]_2(Z_1, Z_2) = 0$ are close to the solutions of the system of equations $[\ell]'_1(Z_1, Z_2) = [\ell]'_2(Z_1, Z_2) = 0$?

A precise answer to this question can be found in [6], chapter III, § 4, n° 5. The reasoning is carried out in the context of restricted formal power series, but it can be adapted to this setting.

Namely, let A be a commutative ring, and fix an ideal $\mathfrak{m}$ of A. Assume that A is separable and complete with respect to the $\mathfrak{m}$-adic topology. As usual, we will denote the tuples of elements in boldface.

Consider a system of n power series in n variables,

$$\mathbf{f} = (f_1, \ldots, f_n), \quad f_i \in A[[X_1, \ldots, X_n]].$$

We will denote by $J_{\mathbf{f}}$ the determinant of the Jacobian matrix, that is to say,

$$J_{\mathbf{f}} = \det \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{X_n} \\ \cdots & \cdots & \cdots \\ \frac{\partial f_n}{\partial X_1} & \cdots & \frac{\partial f_n}{X_n} \end{pmatrix}.$$

By $\mathfrak{m}^{\times n}$ we shall mean the cartesian product of $\mathfrak{m}$ with itself n times. We will say that two n-tuples $\mathbf{a}$ and $\mathbf{b}$ are congruent modulo an ideal I of A if they are so coordinatewise, that is to say, $a_i - b_i \in I$ for $i = 1, \ldots, n$. We will apply the following result (cf. Corollary 1 in [6], chapter III, § 4, n° 5).

Corollary 6.2. *Let $\mathbf{f} = (f_1, \ldots, f_n)$ be a tuple of elements in $A[[X_1, \ldots, X_n]]$, and let $\mathbf{a} \in \mathfrak{m}^{\times n}$. Call $e = J_{\mathbf{f}}(\mathbf{a})$. If $\mathbf{f}(\mathbf{a}) \equiv 0 \mod e^2\mathfrak{m}$, then there exists $\mathbf{b} \in \mathfrak{m}^{\times n}$ such that $\mathbf{f}(\mathbf{b}) = 0$ and $\mathbf{b} \equiv \mathbf{a} \mod e\mathfrak{m}$. Furthermore, assume that there exists another tuple $\mathbf{b}' \in \mathfrak{m}^{\times n}$ such that $\mathbf{f}(\mathbf{b}') = 0$ and $\mathbf{b}' \equiv \mathbf{a} \mod e\mathfrak{m}$. Then, if A has no zero divisors, $\mathbf{b} = \mathbf{b}'$.*

Let us go back now to our approximation problem. We have two formal group laws $\mathbf{F}$, $\mathbf{F}'$, defined over $\mathbb{Z}_\ell$. We consider the two systems of equations

$$\begin{cases} [\ell]_1(Z_1, Z_2) = 0 \\ [\ell]_2(Z_1, Z_2) = 0 \end{cases} \quad \text{and} \quad \begin{cases} [\ell]'_1(Z_1, Z_2) = 0 \\ [\ell]'_2(Z_1, Z_2) = 0 \end{cases} \tag{1}$$

where we know that for $i = 1, 2$, it holds that

$$[\ell]_i(Z_1, Z_2) - [\ell]'_i(Z_1, Z_2) \in \ell^s \cdot \mathbb{Z}_\ell[[Z_1, Z_2]].$$

Furthermore, since the systems of equations (1) describe the ℓ-torsion points of the Jacobians of curves of genus 2, the set of solutions in $\overline{\mathfrak{m}}^{\times 2}$ is finite. We may thus consider a finite extension $K \supset \mathbb{Q}_\ell$ that contains all the coordinates of all the solutions of the systems in (1). Let us denote by $\mathcal{O}_K$ the ring of integers of K and by $\mathfrak{m}$ its maximal ideal. It is clear that $\mathcal{O}_K$ is separable and complete with respect to the $\mathfrak{m}$-adic topology.

Let us call V' the set of pairs $(x', y') \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ such that $[\ell]'_1(x', y') = [\ell]'_2(x', y') = 0$. Our first claim is the following:

Lemma 6.3. *For all $(x', y') \in V'$, $[\ell]_1(x', y'), [\ell]_2(x', y') \in \ell^s\mathfrak{m}$.*

Proof. Since $[\ell]'_1(x', y') = 0$, we can write

$$[\ell]_1(x', y') = [\ell]_1(x', y') - [\ell]'_1(x', y').$$

Furthermore, let us express

$$[\ell]_1(x, y) = \sum_{ij} a_{ij} x^i y^j \text{ and } [\ell]'_1(x, y) = \sum_{ij} a'_{ij} x^i y^j.$$

Hence $[\ell]_1(x', y') = \sum_{ij}(a_{ij} - a'_{ij}) x'^i y'^j$. We know that $a_{ij} - a'_{ij} \in (\ell^s)$, and $x', y' \in \mathfrak{m}$, and also that $[\ell]_1(x, y)$ is a power series without constant term; thus it follows that $[\ell]_1(x', y') \in \ell^s\mathfrak{m}$. A similar reasoning shows that $[\ell]_2(x', y') \in \ell^s\mathfrak{m}$. □

In order to apply Corollary 6.2 to the system of equations $[\ell]_1(Z_1, Z_2) = [\ell]_2(Z_1, Z_2) = 0$, we need to compute the determinant of the Jacobian matrix $e = \det \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix} = \ell^2$. This suggests that we should choose $s = 4$.

Proof of Theorem 6.1. Take $(x', y') \in \overline{\mathfrak{m}}^{\times 2}$ satisfying the equations

$$[\ell]'_1(x', y') = [\ell]'_2(x', y') = 0.$$

We know that $[\ell]_1(x', y'), [\ell]_2(x', y') \in \ell^4 \cdot \mathfrak{m}$. Hence there exists a unique $(x, y) \in \overline{\mathfrak{m}}^{\times 2}$ such that $[\ell]_1(x, y) = [\ell]_2(x, y) = 0$ and furthermore

$$\begin{cases} x' \equiv x \mod \ell^2\mathfrak{m} \\ y' \equiv y \mod \ell^2\mathfrak{m}. \end{cases}$$

In particular, the two conditions $v(x'-x) \geq 2$, $v(y'-y) \geq 2$ are satisfied.

But (x, y) is a point of ℓ-torsion of the Jacobian of C, and therefore we know that

$$\min\{v(x), v(y)\} = \alpha = \frac{1}{\ell^2 - 1}.$$

But if $v(x) = \alpha$ and $v(x'-x) \geq 2 > \alpha$, then it follows that $v(x') = \alpha$. And similarly, if $v(y) = \alpha$, then $v(y') = \alpha$. Also if $v(x) > \alpha$, it cannot happen that $v(x') < \alpha$ (and the same applies to y, y'). We may conclude that $\min\{v(x'), v(y')\} = \alpha$. □

Gathering together Proposition 5.8 and Theorem 6.1 we obtain, for each prime $\ell > 3$, a large family of abelian surfaces such that the action of the wild inertia group upon their ℓ-torsion points is trivial.

Theorem 6.4. *Let $\ell > 3$ be a prime number. Let $\overline{a} \in \mathbb{F}_\ell$ be such that $x^2 - x + \overline{a}$ divides the Deuring polynomial $H_\ell(x)$, and lift it to $a \in \mathbb{Z}_\ell$. Let $f_0, f_1, \ldots, f_6 \in \mathbb{Z}_\ell$ satisfy that $f_6 - f_0, f_5 - f_1, f_4 - f_2 \in (\ell^4)$ and furthermore $f_6 - 1, f_5, f_4 - (1-a)/a, f_3 \in (\ell)$. Then the equation $y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbb{Z}_\ell[x]$ defines a genus 2 curve C such that the Galois extension $\mathbb{Q}_\ell(J(C))/\mathbb{Q}_\ell$ is tamely ramified.*

References

[1] Arias-de-Reyna, S. *Galois representations and tame Galois realizations*, Ph.D. Thesis, Barcelona, June 2009. Available at

`http://www.tesisenxarxa.net/TDX-0612109-101019/`

[2] Arias-de-Reyna, S. and N. Vila. *Tame Galois realizations of* $\mathrm{GL}_2(\mathbb{F}_\ell)$ *over* $\mathbb{Q}$. Journal of Number Theory, Volume **129**, Issue 5, May (2009), pages 1056-1065.

[3] Arias-de-Reyna, S. and N. Vila. *Tame Galois realizations of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *over* $\mathbb{Q}$, preprint.

[4] Becker, T. *Standard bases and some computations in rings of power series*. J. Symbolic Comput. **10** (1990), no. 2, pages 165–178.

[5] Birch, B. *Noncongruence subgroups, Covers and Drawings*, pages 25–46 in *The Grothendieck theory of dessins d'enfants*, Leila Schneps, editor. Cambridge Univ. Press (1994).

[6] Bourbaki, N. *Èléments de mathématique. Fascicule XXVIII. Algèbre commutative*. Actualités Scientifiques et Industrielles, No. 1293 Hermann, Paris (1961).

[7] Brillhart, J. and P. Morton. *Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial*, J. Number Theory **106**, no. 1, pages 79–111 (2004).

[8] Cassels, J. W. S. and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Matematical Society Lecture Note Series 230, Cambridge University Press (1996).

[9] Flynn, E. V. *The Jacobian and Formal Group of a curve of genus* 2 *over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. **107** (1990), no. 3, pages 425–441.

[10] Hazewinkel, M. *Formal Groups and Applications*. Academic Press (1978).

[11] Howe, E. W., F. Leprévost and B. Poonen. *Large torsion subgroups of split Jacobians of curves of genus two or three*. Forum Math. **12** (2000), no. 3, pages 315–364.

[12] Mumford, D. *Abelian Varieties*. Tata Institute of Fundamental Research Studies in Mathematics, Bombay. Oxford University Press (1974).

[13] Serre, J-P. *Proprietes galoisiénnés des points d'ordre fini des courbes elliptiques*, Inventiones math. **15**, pages 259–331 (1972).

[14] Silverman, J. *The Arithmetic of Elliptic Curves*, Graduate texts in mathematics 106, Springer (1986).

[15] Tate, J. T. *p-divisible groups*. 1967 Proc. Conf. Local Fields (Driebergen, 1966) pages 158–183, Springer, Berlin.