Formal groups, supersingular abelian varieties and tame ramification[1]

Sara Arias-de-Reyna[2]

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.

Keywords: Tame ramification, Formal group, Supersingular abelian variety.
MSC (2010): 14L05, 11G10, 11S15

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 $\overline{\mathbb{Q}}_\ell$ 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

[1]Preprint version. A final version is published in *J. Algebra* **334** (2011), 84–100.

[2]Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Ellernstraße 29, 45326 Essen, Germany.

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 maps 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 5.9). 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 construct 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 [6], §2, for the family of linear groups $\mathrm{GL}_2(\mathbb{F}_\ell)$. In [3], the results in this paper are used 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 $\ell \geq 5$.

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 $v(K^\times) = \mathbb{Z}$, $\mathcal{O}$ 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 start by recalling that an n-dimensional *formal group law* defined over $\mathcal{O}$ is an n-tuple of power series

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

satisfying:

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

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

To a formal group law 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 $\oplus_{\mathbf{F}}$ by

$$\begin{aligned} \oplus_{\mathbf{F}} : \overline{\mathfrak{m}}^{\times n} \times \overline{\mathfrak{m}}^{\times n} &\to \overline{\mathfrak{m}}^{\times n}, \\ (\mathbf{x},\mathbf{y}) &\mapsto (F_1(\mathbf{x},\mathbf{y}),\dots,F_n(\mathbf{x},\mathbf{y})) \end{aligned}$$

(which is well defined since $F_i(\mathbf{x},\mathbf{y})$ converges to an element of $\overline{\mathfrak{m}}$, for all $i = 1,\dots,n$). 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

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

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 spaces 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 the case of a formal group law attached to an elliptic curve with good supersingular reduction, 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 $\alpha = 1/(\ell^2 - 1)$.

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 $(x_1,\dots,x_n) \in V$, 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 wild inertia group* I_{w} *acts trivially on* V*.*

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 $\lambda_1 y_1 + \cdots + \lambda_n y_n$ 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

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

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 $\varphi(\lambda_1, \ldots, \lambda_n)(Q) = y_j + \overline{\mathfrak{m}}_\alpha^+ \neq 0 + \overline{\mathfrak{m}}_\alpha^+$.

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

$$\mathbf{f}\left(F_1(\mathbf{X}, \mathbf{Y}), \ldots, F_n(\mathbf{X}, \mathbf{Y})\right) = \left(G_1(f_1(\mathbf{X}), \ldots, f_n(\mathbf{X}), f_1(\mathbf{Y}), \ldots, f_n(\mathbf{Y})\right), \ldots, \\ G_n\left(f_1(\mathbf{X}), \ldots, f_n(\mathbf{X}), f_1(\mathbf{Y}), \ldots, f_n(\mathbf{Y})\right)).$$

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

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

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 $i = 1, \ldots, n$.

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:

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

Remark 4.4. A 2-dimensional formal group law $\mathbf{F}$ is symmetric if and only if the pair of formal power series $(e_1(Z_1, Z_2), e_2(Z_1, Z_2))$ defined as $e_1(Z_1, Z_2) = Z_2$ and $e_2(Z_1, Z_2) = Z_1$ define a morphism from $\mathbf{F}$ into itself. In particular, a symmetric formal group law has an involution.

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 4.5. *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 4.6. *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 $f(Z_2, Z_1) = -f(Z_1, Z_2)$ and which can be written as*

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

where $\ell \nmid a$. Then if $(x_0, y_0) \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ 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 $1/(r-1)$.

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 ℓ^r, 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:
  $$a \cdot \left(x_0^{\ell^r} - y_0^{\ell^r}\right) = a \cdot \left((x_0 - y_0)^{\ell^r} - B\right) = a \cdot (x_0 - y_0)^{\ell^r} - a \cdot B,$$
  where $B = (x_0 - y_0)^{\ell^r} - (x_0^{\ell^r} - y_0^{\ell^r})$.

  On the one hand, $v\left(a \cdot (x_0 - y_0)^{\ell^r}\right) = v(a) + \ell^r \beta = \ell^r \beta$, 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 4.7. *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 $f(Z_2, Z_1) = f(Z_1, Z_2)$ and which can be written as*

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

where $\ell \nmid a$. Then if $(x_0, y_0) \in \overline{\mathfrak{m}} \times \overline{\mathfrak{m}}$ 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 $v(x_0 + y_0)$ is $1/(\ell^r - 1)$.

Proof. Analogous to that of Lemma 4.6 □

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

Definition 4.9. 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 $\mathcal{O}$.

The following lemma, which is valid for every field k, will be useful to compute the height of a formal group law.

Lemma 4.10. *Let $f_1, \ldots, f_n$ be formal power series in $k[\![Z_1, \ldots, Z_n]\!]$ without constant term. Call $I = \langle f_1, \ldots, f_n \rangle$ the ideal of $k[\![Z_1, \ldots, Z_n]\!]$ they generate. Then $k[\![Z_1, \ldots, Z_n]\!]$ is finitely generated as a module over $k[\![f_1, \ldots, f_n]\!]$ if and only if $k[\![Z_1, \ldots, Z_n]\!]/I$ is a finite dimensional k-vector space. Moreover,*

$$\operatorname{rank}(k[\![Z_1, \ldots, Z_n]\!], k[\![f_1, \ldots, f_n]\!]) = \dim(k[\![Z_1, \ldots, Z_n]\!]/I).$$

Proof. Assume $k[\![Z_1, \ldots, Z_n]\!]$ is generated by $a_1, \ldots, a_r$ as a module over $k[\![f_1, \ldots, f_n]\!]$. Take any element of $k[\![Z_1, ..., Z_n]\!]/I$, say $a + I$. We can express $a = b_1 a_1 + \cdots + b_r a_r$, for some $b_1, \ldots, b_r \in k[\![f_1, \ldots, f_n]\!]$. That is to say, for each $i = 1, \ldots, r$, there is a formal power series $g_i(\mathbf{Z}) \in k[\![Z_1, \ldots, Z_n]\!]$ such that $b_i = g_i(f_1, \ldots, f_n)$. So if λ_i is the constant term of g_i, we may write $b_i = \lambda_i + c_i$, where $c_i \in I$. Therefore

$$a = b_1 a_1 + \cdots + b_r a_r = (\lambda_1 a_1 + \cdots + \lambda_r a_r) + (c_1 a_1 + \cdots + c_r a_r).$$

This shows that the k-vector space $k[\![Z_1, ..., Z_n]\!]/I$ is generated by the elements $a_1 + I, \ldots, a_r + I$. Therefore it has finite dimension and furthermore

$$\operatorname{rank}(k[\![Z_1, ..., Z_n]\!], k[\![f_1, \ldots, f_n]\!]) \geq \dim(k[\![Z_1, \ldots, Z_n]\!]/I).$$

Assume now that $k[\![Z_1, \ldots, Z_n]\!]/I$ is a finite dimensional k-vector space, and fix a basis $a_1 + I, \ldots, a_r + I$. We wish to see that $a_1, \ldots, a_r$ generate $k[\![Z_1, \ldots, Z_n]\!]$ as a module over $k[\![f_1, \ldots, f_n]\!]$.

Take therefore some $a \in k[\![Z_1, \dots, Z_n]\!]$. Our assumption assures us that there exist $\lambda_1, \dots, \lambda_r \in k$ such that $a - (\lambda_1 a_1 + \cdots + \lambda_r a_r) \in I$. Therefore, there exist $b_1, \dots, b_n \in k[\![Z_1, \dots, Z_n]\!]$ such that we can write

$$a = \sum_{j=1}^{r} \lambda_j a_j + \sum_{i=1}^{n} b_i f_i. \tag{4.1}$$

Now we can apply the same procedure to each b_i, and express it as $b_i = \sum_{j=1}^{r} \lambda'_{i,j} a_j + \sum_{s=1}^{n} b'_{i,s} f_s$. Replacing this expression in (4.1), we get

$$a = \sum_{j=1}^{r} \left(\lambda_j + \sum_{i=1}^{n} \lambda'_{i,j} f_i \right) a_j + \sum_{i=1}^{n} \sum_{s=1}^{n} b'_{i,s} f_i f_s.$$

Iterating this procedure, we will express a as a sum

$$a = \sum_{j=1}^{r} g_j(f_1, \dots, f_n) a_j,$$

for some $g(\mathbf{Z}) \in k[\![Z_1, \dots, Z_n]\!]$, thus proving that $k[\![Z_1, \dots, Z_n]\!]$ is finitely generated as a module over $k[\![f_1, \dots, f_n]\!]$, and moreover that

$$\operatorname{rank}\left(k[\![Z_1, \dots, Z_n]\!], k[\![f_1, \dots, f_n]\!]\right) \leq \left(\dim k[\![Z_1, \dots, Z_n]\!]/I\right).$$

□

Therefore, to compute the height of $\overline{\mathbf{F}}$, one seeks the dimension of the k-vector space

$$k[\![\mathbf{Z}]\!]/\langle \overline{[\ell]}_1(\mathbf{Z}), \dots, \overline{[\ell]}_n(\mathbf{Z}) \rangle.$$

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], [5]. If I is an ideal of $k[\![\mathbf{Z}]\!]$, then the dimension of $k[\![\mathbf{Z}]\!]/I$ as a k-vector space is determined in this way: Fix an admissible ordering, take a standard basis S of I with respect to this ordering, and consider the set M of monomials t such that, for all $g \in S$, $\operatorname{LT}(g) \nmid t$, where LT denotes the leading term with respect to the prefixed ordering. Then the cardinality of M is the required dimension (of course, it need not be finite).

In the case when the formal group law is of dimension 1, another definition of height is used (see for instance [10], (18.3.3)). 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], (18.3.9), the reasonings in (18.3.1) can be carried out in arbitrary dimension, yielding the following result:

Proposition 4.11. *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*

$$\overline{\mathbf{f}}(\mathbf{Z}) = \left(\overline{f}_1(\mathbf{Z}), \dots, \overline{f}_n(\mathbf{Z})\right).$$

If u is the smallest exponent such that, in some $\overline{f}_i(\mathbf{Z})$, for some j, Z_j^u occurs in a non-zero monomial, 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

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

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

Proof. Since $\overline{\mathbf{f}}$ is a homomorphism of formal group laws, it holds that

$$\overline{f}_i\left(\overline{F}_1(\mathbf{X},\mathbf{Y}), \ldots, \overline{F}_n(\mathbf{X},\mathbf{Y})\right) = \overline{G}_i\left(\overline{f}_1(\mathbf{X}), \ldots, \overline{f}_n(\mathbf{X}), \overline{f}_1(\mathbf{Y}), \ldots, \overline{f}_n(\mathbf{Y})\right), \tag{4.2}$$

for each $i = 1, \ldots, n$.

Let us differentiate (4.2) with respect to Y_j. Applying the chain rule, we obtain

$$\sum_{m=1}^{n} \frac{\partial \overline{f}_i}{\partial Z_m}\left(\overline{\mathbf{F}}(\mathbf{X},\mathbf{Y}\right) \cdot \frac{\partial \overline{F}_m}{\partial Y_j}(\mathbf{X},\mathbf{Y})) = \sum_{m=1}^{n} \frac{\partial \overline{G}_i}{\partial Y_m}\left(\overline{\mathbf{f}}(\mathbf{X}), \overline{\mathbf{f}}(\mathbf{Y})\right) \cdot \frac{\partial \overline{f}_m}{\partial Z_j}(\mathbf{Y}),$$

for each $i = 1, \ldots, n$, $j = 1, \ldots, n$.

Substitute $\mathbf{Y} = (0, 0, \ldots, 0)$. We obtain that

$$\sum_{m=1}^{n} \frac{\partial \overline{f}_i}{\partial Z_m}(\mathbf{X}) \cdot \frac{\partial \overline{F}_m}{\partial Y_j}(\mathbf{X}, 0, \ldots, 0) = \sum_{m=1}^{n} \frac{\partial \overline{G}_i}{\partial Y_m}\left(\overline{\mathbf{f}}(\mathbf{X}), 0, \ldots, 0\right) \cdot \frac{\partial \overline{f}_m}{\partial Z_j}(0, \ldots, 0), \tag{4.3}$$

for each $i = 1, \ldots, n$, $j = 1, \ldots, n$.

Eq. (4.3), $i = 1, \ldots, n$, $j = 1, \ldots, n$, can be summarized in the following expression: if we denote by

$$A_{ij} = \frac{\partial \overline{f}_i}{\partial Z_j}(\mathbf{X}), \qquad F_{ij} = \frac{\partial \overline{F}_i}{\partial Y_j}(\mathbf{X}, 0, \ldots, 0),$$
$$a_{ij} = \frac{\partial \overline{f}_i}{\partial Z_j}(0, \ldots, 0), \qquad G_{ij} = \frac{\partial \overline{G}_i}{\partial Y_j}\left(\overline{\mathbf{f}}(\mathbf{X}), 0, \ldots, 0\right)$$

and by M_A, M_F, M_G and M_a the matrices with coefficients $(A_{ij})_{i,j}$, $(F_{ij})_{i,j}$, $(G_{ij})_{i,j}$ and $(a_{ij})_{i,j}$ respectively, then $M_A \cdot M_F = M_G \cdot M_a$.

If there exist $i, j \in \{1, \ldots, n\}$ such that $a_{ij} = 0$, then the formal power series $\overline{f}_i$ has a monomial aZ_j, where $a \in k^\times$. Therefore $r = 0$ and obviously all the formal power series $\overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z})$ can be expressed as formal power series in the variables $Z_1, \ldots, Z_n$, so there would be nothing to prove.

Assume that, on the contrary, all $a_{ij} = 0$. Then $M_A \cdot M_F = 0$. But M_F is invertible. (Write $M_F = \mathrm{Id} + B$, where all entries of B are formal power series without constant term. Then the sum $1 - B + B^2 - B^3 + \cdots$ defines a formal power series, which is the inverse of M_F.) Therefore all the A_{ij} must vanish. But this means that, for all $i = 1, \ldots, n$, the monomials of the power series $\overline{f}_i(\mathbf{Z})$, say $Z_1^{e_1} \cdot Z_2^{e_2} \cdots Z_n^{e_n}$, with some exponent e_m not divisible by ℓ, cannot occur with non-zero coefficient. Thus there exist $\overline{g}_i(\mathbf{Z})$, $i = 1, \ldots, n$, such that

$$\overline{f}_i(\mathbf{Z}) = \overline{g}_i(\mathbf{Z}^\ell).$$

We now wish to proceed by induction. To apply the same reasoning to the power series $\overline{\mathbf{g}}(\mathbf{Z}) = (\overline{g}_1(\mathbf{Z}), \ldots, \overline{g}_n(\mathbf{Z}))$, we must view $\overline{\mathbf{g}}$ as a homomorphism between formal group laws. Only the formal group laws will not be $\overline{\mathbf{F}}$ and $\overline{\mathbf{G}}$. Namely, if we consider the formal group law $\overline{\mathbf{F}}'(\mathbf{X}, \mathbf{Y})$, obtained from $\overline{\mathbf{F}}(\mathbf{X}, \mathbf{Y})$ by raising all coefficients to the ℓ-th power, then it is immediate to check that $(\overline{F}_i(\mathbf{X}, \mathbf{Y}))^\ell = \overline{F}'_i(\mathbf{X}, \mathbf{Y})$ for $i = 1, 2, \ldots, n$. Therefore,

$$\overline{\mathbf{g}}\left(\overline{\mathbf{F}}'\left(\mathbf{X}^\ell, \mathbf{Y}^\ell\right)\right) = \overline{\mathbf{g}}\left(\overline{\mathbf{F}}\left(\mathbf{X}, \mathbf{Y}\right)^\ell\right) = \overline{\mathbf{f}}(\overline{\mathbf{F}}(\mathbf{X}, \mathbf{Y})) = \overline{\mathbf{G}}\left(\overline{\mathbf{f}}(\mathbf{X}), \overline{\mathbf{f}}(\mathbf{Y})\right) = \overline{\mathbf{G}}\left(\overline{\mathbf{g}}(\mathbf{X}^\ell), \overline{\mathbf{g}}(\mathbf{Y}^\ell)\right).$$

Thus we conclude that

$$\overline{\mathbf{g}}\left(\overline{\mathbf{F}}'(\mathbf{X}, \mathbf{Y})\right) = \overline{\mathbf{G}}\left(\overline{\mathbf{g}}(\mathbf{X}), \overline{\mathbf{g}}(\mathbf{Y})\right),$$

which shows that the induction step can be taken.

This proves that there exist $\overline{g}_1(\mathbf{Z}), \ldots, \overline{g}_n(\mathbf{Z}) \in k[\![\mathbf{Z}]\!]$ and a natural number r such that

$$\overline{f}_i(\mathbf{Z}) = \overline{g}_i\left(\mathbf{Z}^{\ell^r}\right),$$

for $i = 1, \ldots, n$. Moreover, either $\overline{g}_1(\mathbf{Z})$ or $\overline{g}_2(\mathbf{Z})$ or $\ldots$ or $\overline{g}_n(\mathbf{Z})$ have a term of degree 1 with non-zero coefficient. That is to say, a monomial in some $Z_j^{\ell^r}$ does appear in at least one of the power series $\overline{f}_i(\mathbf{Z})$. And it is clear that it is the term of least degree of $\overline{f}_i(\mathbf{Z})$. □

Remark 4.12. 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 is a finite number (in Chapter IV, (18.3.9), p. 151 of [10], there is an example of such a formal group law). The following proposition deals with this matter.

Proposition 4.13. *Let $\overline{\mathbf{F}}$ be an n-dimensional formal group law defined over $\mathbb{F}_\ell$, and assume that there exist n power series in $\mathbb{F}_\ell[\![Z_1, \ldots, Z_n]\!]$, say $\overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z})$, such that the formal power series that give the multiplication by ℓ map $\overline{[\ell]}$ can be written as $\overline{[\ell]}_1(Z_1, \ldots, Z_n) = \overline{f}_1(Z_1^{\ell^r}, \ldots, Z_n^{\ell^r})$, $\ldots$, $\overline{[\ell]}_n(Z_1, \ldots, Z_n) = \overline{f}_n(Z_1^{\ell^r}, \ldots, Z_n^{\ell^r})$. Then the height of $\overline{\mathbf{F}}$ is greater than or equal to nr.*

Proof. Let us fix an admissible ordering and compute a standard basis S of the ideal

$$I = \langle \overline{f}_1(\mathbf{Z}), \ldots, \overline{f}_n(\mathbf{Z}) \rangle \subset \mathbb{F}_\ell[\![\mathbf{Z}]\!]$$

with respect to this ordering. Let M be the set of monomials t such that, for all $g \in S$, $\mathrm{LT}(g) \nmid t$. Then $\dim(\mathbb{F}_\ell[\![\mathbf{Z}]\!]/I) = |M|$. Now consider the set $S' = \{g(Z_1^{\ell^r}, \ldots, Z_n^{\ell^r}) : g \in S\}$. This is a standard basis of the ideal they generate (since the s-series of the pairs of elements of S' can be obtained from the s-series of the pairs of elements of S by replacing $(Z_1, \ldots, Z_n)$ by $(Z_1^{\ell^r}, \ldots, Z_n^{\ell^r})$).

Call M' the set of monomials t' such that, for all $g' \in S'$, $\mathrm{LT}(g') \nmid t'$. Then $|M'| = \ell^{nr}|M|$, and therefore $\dim(\mathbb{F}_\ell[\![\mathbf{Z}]\!]/\langle \overline{[\ell]}_1(\mathbf{Z}), \ldots, \overline{[\ell]}_n(\mathbf{Z}) \rangle) = \ell^{nr}|M|$. But we know that this dimension must be a power of ℓ (see Definition 4.8), say $\ell^{nr}\ell^s$. Hence the height of $\overline{\mathbf{F}}$ is $nr + s$, which is greater than or equal to nr. □

Remark 4.14. We are interested in the case when the dimension of the formal group law is 2 and the height is 4. In this case, only two possibilities might occur:

- The exponent r in Proposition 4.13 is 2. Hence $s = 0$.
- The exponent r in Proposition 4.13 is 1. Hence $s = 2$.

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

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

Note that the determinant of the matrix $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ is non-zero. This can be seen from the proof of Proposition 4.13. Indeed, let $\overline{f}_1(\mathbf{Z})$ and $\overline{f}_2(\mathbf{Z})$ be such that $\overline{[\ell]}_i(Z_1, Z_2) = \overline{f}_i(Z_1^{\ell^r}, Z_2^{\ell^r})$, $i = 1, 2$. If the vectors $(\overline{a}, \overline{b})$ and $(\overline{c}, \overline{d})$ are linearly dependent, then there would exist a linear combination of $\overline{f}_1(\mathbf{Z})$ and $\overline{f}_2(\mathbf{Z})$, say $\overline{g}(\mathbf{Z})$, such that all terms would be of degree strictly greater than 1. Assume, to fix ideas, that the coefficient of $\overline{f}_2$ in this combination is non-zero. Then if S is the reduced standard basis of $\langle \overline{f}_1(\mathbf{Z}), \overline{g}(\mathbf{Z})\rangle = \langle \overline{f}_1(\mathbf{Z}), \overline{f}_2(\mathbf{Z})\rangle$ with respect to the graduated lexicographical ordering, then the set M of monomials t such that, for all $\overline{f} \in S$, $\mathrm{LT}(\overline{f}) \nmid t$ has cardinality greater than 1, which contradicts that $s = 0$.

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

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 4.13 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 non-zero $(x_0, y_0) \in V$,

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

Proof. First of all, let us recall that, since the formal group law $\mathbf{F}$ has height 4 and $r = 2$, it follows from Remark 4.14 that the coefficients of all the monomials in $[\ell]_1(Z_1, Z_2)$ and $[\ell]_2(Z_1, Z_2)$ of degree smaller than ℓ^2 are divisible by ℓ. Moreover, the monomials of degree ℓ^2 which are not pure in Z_1 or Z_2 also have coefficient divisible by ℓ. Furthermore, by Example 4.2, the only term of degree 1 of $[\ell]_1(Z_1, Z_2)$ is ℓZ_1, and the only term of degree 1 of $[\ell]_2(Z_1, Z_2)$ is ℓZ_2. Taking also into account that $\mathbf{F}$ is symmetric, we can write the two formal power series that comprise the multiplication by ℓ map in the following way:

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

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

Take a non-zero 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 4.6 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

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

  and $\ell \nmid (a - b)$. Nothing prevents us now from applying Lemma 4.6 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 4.6 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 4.7 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 4.16. *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 4.13 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 4.16. Let us fix an odd prime number ℓ.

Given a hyperelliptic equation of a genus 2 curve C, say

$$y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \tag{5.4}$$

with non-zero discriminant, one can define an embedding of the Jacobian surface attached to C into a projective space of dimension 15. This construction is carried out in Chapter 2 of [9]. The first step is to identify the Jacobian of C with $\mathrm{Pic}^2(C)$, and then the embedding is defined as a map from the symmetric product of C with itself into $\mathbb{P}^{15}$, $\mathbf{z} = (z_0, z_1, \ldots, z_{15}) : C^{(2)} \to \mathbb{P}^{15}$ (the expressions of the z_i, $0 \leq i \leq 15$, are given in the first section of Chapter 2 of [9]). The projective locus of the image of $\mathbf{z}$, which shall be written as $J(C)$, is the Jacobian of C. $J(C)$ can be expressed by means of equations as a variety of $\mathbb{P}^{15}$. Furthermore, it is proven in Chapter 7 of [9] that the pair $\mathbf{s} = (s_1, s_2)$, where $s_1 = z_1/z_0$ and $s_2 = z_2/z_0$, is a local parameter for $J(C)$, and the first terms of the expression of the formal group law with respect to this local parameter are computed.

Now consider the hyperelliptic equation

$$y^2 = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_4x^2 + f_5x + f_6. \tag{5.5}$$

Note that the transformation $(x, y) \mapsto (1/x, y/x^3)$ brings Eq. (5.4) into Eq. (5.5), and so this is just another equation that represents the curve C. In any case, we can consider the formal group law $\widetilde{\mathbf{F}}$ computed from Eq. (5.5), which shall be denoted by $\widetilde{\mathbf{F}} = (\widetilde{F}_1, \widetilde{F}_2)$, and the algebraic variety of $\mathbb{P}^{15}$, $\widetilde{J}(C)$, attached to C via Eq. (5.5).

In my PhD thesis [1] the following result is proven, by making use of an explicit isomorphism between $J(C)$ and $\widetilde{J}(C)$ as varieties inside $\mathbb{P}^{15}$.

Theorem 5.1. *With the notations introduced in this section, the following relations hold*

$$\begin{cases} \widetilde{F}_2(s_2, s_1, t_2, t_1) = F_1(s_1, s_2, t_1, t_2), \\ \widetilde{F}_1(s_2, s_1, t_2, t_1) = F_2(s_1, s_2, t_1, t_2). \end{cases}$$

This result motivates the following definition.

Definition 5.2. 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.

As a corollary of Theorem 5.1, we obtain the following result.

Theorem 5.3. *Let $f(x) = f_0x^6 + f_1x^5 + f_2x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$ 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, $J(C)$ is isogenous to $E \times E$ (cf. [9], 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 $H_\ell(x) = \sum_{k=0}^{\frac{\ell-1}{2}} \binom{\frac{\ell-1}{2}}{k} x^k$ 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 $a \in \mathbb{F}_\ell^\times$, provided $\ell > 3$ (see Theorem 1-(b) of [8], cf. Corollary 3.6 of [2]). We exploit this fact in the following proposition.

Proposition 5.4. *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 5.5. 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 4.16 to the curves provided by Proposition 5.4, we need to check that the exponent in Proposition 4.13 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 5.6. *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 $\Psi : A \to B$ 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 homomorphisms 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 2 (for m is invertible in $\mathbb{F}_\ell$). Taking into account Proposition 4.11, 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 also need of the following result (cf. Proposition 3 of [11]).

Proposition 5.7. *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:

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

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

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

Note that it is compatible with the action of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. In order to apply Proposition 5.7, 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 5.7 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 5.6 and conclude that the Jacobian of C satisfies that the exponent in Proposition 4.11 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 5.8. *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 5.9. *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 4.16, 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 $f_0, \dots, f_6 \in \mathbb{Z}_\ell$, whose discriminant is not divisible by ℓ, and consider the genus 2 curve $C'/\mathbb{Q}_\ell$ given by the equation

$$y^2 = f_6'x^6 + f_5'x^5 + f_4'x^4 + f_3'x^3 + f_2'x^2 + f_1'x + f_0'$$

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

$$y^2 = f_6'x^6 + f_5'x^5 + f_4'x^4 + f_3'x^3 + f_2'x^2 + f_1'x + f_0'$$

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 $\mathbb{Z}_\ell[f_0, \dots, f_6]$ (resp. $\mathbf{Z}_\ell[f_0', \dots, f_6']$), $i = 1, 2$.

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 [7], 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 separated 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,

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

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

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

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 $i = 1, \dots, n$. We will apply the following result (cf. Corollary 1 in [7], Chapter III, §4, n° 5).

Corollary 6.2. *Let* $\mathbf{f} = (f_1, \dots, f_n)$ *be a tuple of elements in* $A[\![X_1, \dots, X_n]\!]$*, and let* $\mathbf{a} \in \mathfrak{m}^{\times n}$*. Call* $e = J_{\mathbf{f}}(\mathbf{a})$*. If* $\mathbf{f}(\mathbf{a}) \equiv 0 \pmod{e^2\mathfrak{m}}$*, then there exists* $\mathbf{b} \in \mathfrak{m}^{\times n}$ *such that* $\mathbf{f}(\mathbf{b}) = 0$ *and* $\mathbf{b} \equiv \mathbf{a} \pmod{e\mathfrak{m}}$*. Furthermore, assume that there exists another tuple* $\mathbf{b}' \in \mathfrak{m}^{\times n}$ *such that* $\mathbf{f}(\mathbf{b}') = 0$ *and* $\mathbf{b}' \equiv \mathbf{a} \pmod{e\mathfrak{m}}$*. 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

$$\begin{cases} [\ell]_1(Z_1, Z_2) = 0, \\ [\ell]_2(Z_1, Z_2) = 0 \end{cases} \quad \text{and} \quad \begin{cases} [\ell]'_1(Z_1, Z_2) = 0, \\ [\ell]'_2(Z_1, Z_2) = 0 \end{cases} \tag{6.6}$$

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 Eqs. (6.6) 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 (6.6). 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 separated and complete with respect to the $\mathfrak{m}$-adic topology.

Let us call V' the set of pairs $(x', y') \in \mathfrak{m} \times \mathfrak{m}$ 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

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

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 $(x', y') \in \mathfrak{m}^{\times 2}$ satisfying the equations

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

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

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

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 Theorems 5.9 and 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.*

Acknowledgments:

The contents of this paper are part of my PhD thesis. I want to thank my advisor, Prof. Núria Vila, for her constant support and helpful conversations. I also want to thank the referee for his suggestions to improve the presentation of this manuscript.

The author is a research fellow of the Alexander von Humboldt Foundation. This research was supported by an FPU predoctoral grant AP-20040601 of the MEC and partially supported by MEC grant MTM2009-07024.

References

[1] S. Arias-de-Reyna, *Galois representations and tame Galois realizations*, PhD thesis, Universitat de Barcelona, Departament d'Àlgebra i Geometria, 2009, available at `http://www.tesisenxarxa.net/TDX-0612109-101019/`.

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

[3] S. Arias-de-Reyna, N. Vila, *Tame Galois realizations of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *over* $\mathbb{Q}$, Int. Math. Res. Not. IMRN **2011**, no. 9, 2028–2046.

[4] T. Becker, *Standard bases and some computations in rings of power series*, J. Symbolic Comput. **10** (1990) 165–178.

[5] T. Becker, *Standard bases in power series rings: uniqueness and superfluous critical pairs*, J. Symbolic Comput. **15** (1996) 251–265.

[6] B. Birch, *Noncongruence subgroups, covers and drawings*, in: L. Schneps (Ed.), *The Grothendieck Theory of Dessins d'Enfants*, Cambridge Univ. Press, 1994, pp. 25–46.

[7] N. Bourbaki, *Algèbre commutative*, in: *Éléments de mathématique*. Fascicule XXVIII, in: Actualités Sci. Indust., vol. 1293, Hermann, 1961.

[8] J. Brillhart, P. Morton, *Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial*, J. Number Theory **106** (2004) 79–111.

[9] J.W.S. Cassels, E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, London Math. Soc. Lecture Note Ser., vol. 230, Cambridge Univ. Press, 1996.

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

[11] E.W. Howe, F. Leprévost, B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000) 315–364.

[12] D. Mumford, *Abelian Varieties*, Tata Inst. Fund. Res. Stud. Math., Oxford Univ. Press, 1974.

[13] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259–331.

[14] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math., vol. 106, Springer, 1986.

[15] J.T. Tate, *p-divisible groups*, in: Proc. Conf. Local Fields, Driebergen, 1966, Springer, 1967, pp. 158–183.