ANNALES

DE

L'INSTITUT FOURIER

Florence GILLIBERT & Gabriele RANIERI

On the local-global divisibility over abelian varieties

Tome 68, nº 2 (2018), p. 847-873.

<http://aif.cedram.org/item?id=AIF_2018__68_2_847_0>

Ann. Inst. Fourier, Grenoble
68, 2 (2018) 847-873

ON THE LOCAL-GLOBAL DIVISIBILITY OVER ABELIAN VARIETIES

by Florence GILLIBERT & Gabriele RANIERI (*)

Abstract. — Let $p \geqslant 2$ be a prime number and let k be a number field. Let $\mathcal{A}$ be an abelian variety defined over k. We prove that if $\mathrm{Gal}(k(\mathcal{A}[p])/k)$ contains an element g of order dividing $p-1$ not fixing any non-trivial element of $\mathcal{A}[p]$ and $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$ is trivial, then the local-global divisibility by p^n holds for $\mathcal{A}(k)$ for every $n \in \mathbb{N}$. Moreover, we prove a similar result without the hypothesis on the triviality of $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$, in the particular case where $\mathcal{A}$ is a principally polarized abelian variety. Then, we get a more precise result in the case when $\mathcal{A}$ has dimension 2. Finally, we show that the hypothesis over the order of g is necessary, by providing a counterexample.

In the Appendix, we explain how our results are related to a question of Cassels on the divisibility of the Tate–Shafarevich group, studied by Ciperiani and Stix and Creutz.

Résumé. — Soit $p \neq 2$ un nombre premier et k un corps de nombres. Soit $\mathcal{A}$ une variété abélienne définie sur k. Dans cet article nous prouvons le résultat suivant : si $\mathrm{Gal}(k(\mathcal{A}[p])/k)$ contient un élément g d'ordre divisant $p-1$ ne fixant aucun élément non nul de $\mathcal{A}[p]$ et que $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$ est trivial, alors $\mathcal{A}(k)$ satisfait le principe de divisibilité locale globale par p^n pour tout $n \in \mathbb{N}$. En outre nous démontrons un résultat similaire sans la condition $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p]) = 0$, dans le cas particulier où $\mathcal{A}$ est une variété abélienne principalement polarisée. Ensuite nous obtenons un résultat plus précis lorsque $\mathcal{A}$ est de dimension 2. Enfin nous démontrons que l'hypothèse sur l'ordre de g est nécessaire par un contre-exemple.

Dans l'Appendice, nous expliquons le lien entre nos résultats et une question de Cassels sur la divisibilité du groupe de Tate–Shafarevich, qui fut également étudiée par Ciperiani et Stix ainsi que Creutz.

Keywords: Local-global, Galois cohomology, abelian varieties, abelian surfaces.
2010 *Mathematics Subject Classification:* 11R34, 11G10.
(*) The first author was supported by the project Fondecyt Iniciación 11130409. The second author was supported by the project Fondecyt Regular 1140946. The authors kindly thank the Laboratoires Mathématiques Nicolas Oresme of the University of Caen, where they found a very friendly and stimulating ambient for their research. In particular many thanks to Philippe Satgé for his constant help and disponibility. The authors also thank Jean and Pierre Gillibert, Max Karoubi, José Pantoja and the anonimous referee. Finally, many thanks to Luis Lomelí who read a preliminary version of this article.

1. Introduction

Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. Several papers have been written on the following classical question, known as the *Local-Global Divisibility Problem*.

Problem. — *Let $P \in \mathcal{A}(k)$. Assume that for all but finitely many valuations v of k, there exists a $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$, where q is a positive integer. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = qD$?*

By Bézout's identity, to get answers for a general integer it is sufficient to solve it for powers p^n of a prime. In the classical case of $\mathcal{A} = \mathbb{G}_m$ and $k = \mathbb{Q}$, the answer is positive for p odd and q dividing 4, and negative for $q = 2^m$ for every integer $m \geqslant 3$ (see for example [1, 22]).

For general commutative algebraic groups, Dvornicich and Zannier gave a cohomological interpretation of the problem (see [8, 10]) that we shall explain. Let Γ be a group and let M be a Γ-module. We say that a cocycle $Z\colon \Gamma \to M$ satisfies the local conditions if for every $\gamma \in \Gamma$ there exists $m_\gamma \in M$ such that $Z_\gamma = \gamma(m_\gamma) - m_\gamma$. The set of the class of cocycles in $H^1(\Gamma, M)$ that satisfy the local conditions is a subgroup of $H^1(\Gamma, M)$. We call it the first local cohomology group $H^1_{\text{loc}}(\Gamma, M)$. Equivalently,

$$H^1_{\text{loc}}(\Gamma, M) = \cap_{C \leqslant \Gamma} \ker(H^1(\Gamma, M) \to H^1(C, M)),$$

where C varies among the cyclic subgroups of Γ and the above maps are the restrictions. Dvornicich and Zannier [8, Proposition 2.1] proved the following result.

Proposition 1.1. — *Let p be a prime number, let n be a positive integer, let k be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over k. If $H^1_{\text{loc}}(\text{Gal}(k(\mathcal{A}[p^n])/k), \mathcal{A}[p^n]) = 0$, then local-global divisibility by p^n over $\mathcal{A}(k)$ holds.*

The converse of Proposition 1.1 is not true. However, in the case when the group $H^1_{\text{loc}}(\text{Gal}(k(\mathcal{A}[p^n])/k), \mathcal{A}[p^n])$ is not trivial, we can find an extension L of k, k-linearly disjoint with $k(\mathcal{A}[p^n])$, in which the local-global divisibility by p^n over $\mathcal{A}(L)$ does not hold (see [10, Theorem 3] for the details).

From now on let p be a prime number, let k be a number field and let $\mathcal{E}$ be an elliptic curve defined over k. Dvornicich and Zannier (see [10, Theorem 1]) found a geometric criterion for the validity of the local-global divisibility principle by a power of p over $\mathcal{E}(k)$. In [17] and [18] Paladino, Viada and the second author refined this criterion. Ciperiani and Stix [3, Theorems A and B] also proved a similar criterion to give an answer to a question of Cassels on elliptic curves (see the Appendix). Moreover, very recently, Lawson and Wuthrich [12] obtained a very strong criterion for the vanishing of the first cohomology group of the Galois module of the torsion points of an elliptic curve defined over $\mathbb{Q}$ that allowed them to find a simpler proof of the main result of [18]. Creutz [5] found a counterexample to the local-global divisibility by 3^n for an elliptic curve defined over $\mathbb{Q}$, for every integer $n \geqslant 2$. From this result, the examples of Dvornicich and Zannier [9] and Paladino [15, 16] and the main result of [18], it follows that the set of prime numbers l for which there exists an elliptic curve $\mathcal{E}'$ defined over $\mathbb{Q}$ and $n \in \mathbb{N}$ such that the local-global divisibility by l^n does not hold over $\mathcal{E}'(\mathbb{Q})$ is just $\{2, 3\}$.

Let us now consider an arbitrary abelian variety. To our knowledge the unique known geometric criterion for the validity of the local-global divisibility principle by a power of p for an abelian variety of dimension > 1 over a number field was proved by Ciperiani and Stix (see [3, Theorem D]). For a connection with this result and the local-global divisibility problem see [3, Remark 20] and the Appendix.

The results on elliptic curves and this last result gave a motivation to look for other geometric criteria for the local-global divisibility principle, over the family of abelian varieties. From now on, let $\mathcal{A}$ be an abelian variety defined over k of dimension $d \in \mathbb{N}^*$. Moreover, for every positive integer n, we set $K_n = k(\mathcal{A}[p^n])$ and $G_n = \mathrm{Gal}(K_n/k)$. We prove the following result.

Theorem 1.2. — *Suppose that G_1 contains an element g whose order divides $p-1$ and not fixing any non-trivial element of $\mathcal{A}[p]$. Moreover, suppose that $H^1(G_1, \mathcal{A}[p]) = 0$. Then $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$ for every positive integer n. Hence, local-global divisibility by p^n holds for $\mathcal{A}(k)$.*

Let us now fix a polarization on $\mathcal{A}$ over k and let us suppose that p does not divide the degree of the polarization. We prove the following result, in which there is no hypothesis on $H^1(G_1, \mathcal{A}[p])$. However, we need a hypothesis on the field k.

Theorem 1.3. — *Let $\mathcal{A}$ be a polarized abelian variety of dimension d defined over k and let p be a prime not dividing the degree of the polarization. Suppose that $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. Set $i = ((2d)!, p-1)$ and k_i the subfield of $k(\zeta_p)$ of degree i over k. If for every non-zero $P \in \mathcal{A}[p]$ the field $k(P) \cap k(\zeta_p)$ strictly contains k_i, then for every positive integer n, the group $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$. Hence, local-global divisibility by p^n holds for $\mathcal{A}(k)$.*

Suppose now that $\mathcal{A}$ has dimension 2. By using Theorems 1.2, 1.3 and the results of Sections 2 and 3, we shall give a much more precise criterion, which is a weak generalization to abelian surfaces of the main result of [17] on elliptic curves.

Theorem 1.4. — *Let $\mathcal{A}$ be a polarized abelian surface defined over k. For every prime number $p > 3\,840$ such that $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ and not dividing the degree of the polarization, if there exists $n \in \mathbb{N}$ such that $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) \neq 0$, then there exists a finite extension $\widetilde{k}$ of k of degree $\leqslant 24$ such that $\mathcal{A}$ is $\widetilde{k}$-isogenous to an abelian surface with a torsion point of order p defined over $\widetilde{k}$.*

Merel [14] made the following conjecture on the torsion of abelian varieties over a number field and proved it in the case of dimension 1.

Conjecture 1.5 (Merel's Conjecture). — *Let d and m be positive integers. There exists a positive constant $C(d,m)$, only depending on d and m, such that for every abelian variety of dimension d defined on a number field k of degree m, and for every prime number $p > C(d,m)$, $\mathcal{A}$ does not admit any point of order p defined over k.*

Then, we have the following Corollary of Theorem 1.4.

Corollary 1.6. — *If Merel's Conjecture is true, then for every positive integer m, there exists a constant $C(m)$, only depending on m, such that for every principally polarized abelian surface $\mathcal{A}$ defined over a number field k of degree m over $\mathbb{Q}$ and for every prime number $p > C(m)$, for every positive integer n the local-global divisibility by p^n holds for $\mathcal{A}(k)$.*

Here is the plan of this paper. In Section 2 we prove some algebraic results necessary for the proof of Theorem 1.2, Theorem 1.3 and Theorem 1.4. Moreover we prove Theorem 1.2.

For every prime number p not dividing the degree of the polarization of a polarized abelian variety, the image of the absolute Galois group on the group of the automorphism of the p-torsion is contained in the group of the symplectic similitudes for the Weil-pairing. In Section 3 we describe such a group and we prove Theorem 1.3. For the proof of Theorem 1.4 is necessary a very precise study of the properties of the group $\mathrm{GSp}_4(\mathbb{F}_p)$. We do this in Section 4 and then we finish such section by proving Theorem 1.4. In Section 5 we give an example that shows that the hypothesis on the order of g in Theorem 1.2 is necessary. Finally we explain in the Appendix the connection with the local-global divisibility problem and a question of Cassels studied in particular by Ciperiani and Stix [3] and Creutz [4, 5].

2. Algebraic preliminaries

2.1. Coprime groups and cohomology

Classical Frattini's theory (see for instance [2]) is very useful to prove the following Proposition, which is the first step to prove Theorem 1.2. First, let us give a Definition.

Definition 2.1. — *Let H be a p-group. The Frattini subgroup $\phi(H)$ of H (see* [2, p. 105]*), is the intersection of all maximal subgroups of H.*

Proposition 2.2. — *Let p be a prime number and let G be a finite group such that $G = \langle g, H\rangle$, where g has order dividing $p-1$ and H is a p-group, which is normal in G. There exists $r \in \mathbb{N}$ and a generator set $\{h_1, h_2, \dots, h_r\}$ of H such that, for every $1 \leqslant i \leqslant r$, there exists $\lambda_i \in \mathbb{Z}$ such that*

$$gh_ig^{-1} = h_i^{\lambda_i}.$$

Proof. — Suppose $|H| = p^m$ with $m \in \mathbb{N}$. The proof is by induction on m.

If $m = 1$ we have that H is cyclic generated by an element h_1. Since H is normal in G, we have $gh_1g^{-1} = h_1^{\lambda_1}$ for a $\lambda_1 \in \mathbb{Z}$ and there is nothing to prove.

Suppose that the assumption is true for every natural number $j < m$. The Frattini subgroup $\phi(H)$ (see Definition 2.1) is normal in H and $H/\phi(H)$ is elementary abelian (i.e. is isomorphic to a finite product of groups isomorphic to $\mathbb{Z}/p\mathbb{Z}$, see [2, p. 105] for the details).

Let us show that $\phi(H)$ is normal in G. Let M be a maximal subgroup of H. We have $gMg^{-1} \subseteq H$ because H is normal. Then the action by conjugation of g permutes the maximal subgroups of H. Then, since $\phi(H)$ is the intersection of every maximal subgroup of H, it is normal in G.

We use the following well-known result.

Theorem 2.3 (Burnside basis theorem). — *Let H be a finite p-group. A subset of H is a set of generators for H if and only if its image in $H/\phi(H)$ is a set of generators for $H/\phi(H)$.*

Consider $H/\phi(H)$. Since $\phi(H)$ is normal in G and $H/\phi(H)$ is abelian, the function

$$f\colon H/\phi(H) \to H/\phi(H)$$

that sends $h\phi(H)$ to $ghg^{-1}\phi(H)$ is well-defined and it is actually a $\mathbb{Z}/p\mathbb{Z}$-linear isomorphism. Since g has order dividing $p-1$, also the order of f

divides $p-1$ and so f is diagonalizable on the $\mathbb{Z}/p\mathbb{Z}$-vector space $H/\phi(H)$. Then there exist $v_1, v_2, \dots, v_k \in H$ such that $\{v_i\phi(H) : 1 \leqslant i \leqslant k\}$ is a $\mathbb{Z}/p\mathbb{Z}$-basis of $H/\phi(H)$ and there exist $\lambda_i \in \mathbb{Z}$ such that $gv_ig^{-1}\phi(H) = v_i^{\lambda_i}\phi(H)$.

Suppose that $k=1$. Then $H/\phi(H)$ has a unique generator $v_1\phi(H)$. By Burnside basis theorem, H is then generated by v_1 and it is cyclic. Since H is normal in G, we have that $gv_1g^{-1} = v_1^{\lambda}$ for a $\lambda \in \mathbb{Z}$, which is the thesis.

Suppose $k > 1$. Consider the two groups H_1, $H_2 \subseteq H$, such that

$$H_1 = \langle v_1, \phi(H)\rangle, \quad H_2 = \langle v_2, v_3, \dots, v_k, \phi(H)\rangle.$$

Then set Γ_1 the subgroup of G generated by g and H_1 and Γ_2 the subgroup of G generated by g and H_2. We remark that H_1 is normal in Γ_1 and H_2 is normal in Γ_2. In fact, as $H_1/\phi(H)$ is generated by v_1, all element of H_1 is in $v_1^a\phi(H)$ for some integer a. In the same way we can prove that H_2 is normal in Γ_2.

We now prove that Γ_1 and Γ_2 are not G. Since H_1 and H_2 are respectively normal over Γ_1 and Γ_2 and Γ_1 and Γ_2 are generated by such groups and an element of order not divisible by p, H_1 is the unique p-Sylow subgroup of Γ_1 and H_2 is the unique p-Sylow subgroup of Γ_2. Since H_1 and H_2 are properly contained in H, we have that Γ_1 and Γ_2 are properly contained in G.

Then we can apply the inductive hypothesis to Γ_1 and Γ_2. Since H is generated by H_1 and H_2, a union of a set of generators of H_1 with a set of generators of H_2 gives a set of generators of H. This concludes the proof. □

The following Corollary relates Proposition 2.2 with the vanishing of the first local cohomology group.

Corollary 2.4. — *Let $V_{n,d}$ be the group $(\mathbb{Z}/p^n\mathbb{Z})^{2d}$ and let G be a subgroup of $\mathrm{GL}_{2d}(\mathbb{Z}/p^n\mathbb{Z})$ acting on $V_{n,d}$ in the usual way. Suppose that the normalizer of a p-Sylow subgroup H of G contains an element g of order dividing $p-1$ such that $g - \mathrm{Id}$ is bijective. Then $H^1_{\mathrm{loc}}(G, V_{n,d}) = 0$.*

Proof. — Consider the two restrictions

$$H^1(G, V_{n,d}) \to H^1(\langle g, H\rangle, V_{n,d}) \to H^1(H, V_{n,d}).$$

Notice $H^1(G, V_{n,d}) \to H^1(H, V_{n,d})$ is injective since $V_{n,d}$ is a p-group, and H a p-Sylow subgroup of G. We deduce that $H^1(G, V_{n,d}) \to H^1(\langle g, H\rangle, V_{n,d})$ is also injective. Moreover such maps induce maps on the first local cohomology group. Then the restriction $H^1_{\mathrm{loc}}(G, V_{n,d}) \to H^1_{\mathrm{loc}}(\langle g, H\rangle, V_{n,d})$ is injective and so, to prove the Corollary, it is sufficient to prove that

$H^1_{\mathrm{loc}}(\langle g, H\rangle, V_{n,d}) = 0$. Apply Proposition 2.2 to $\langle g, H\rangle$. Then there exists $r \in \mathbb{N}$ and generators $h_1, h_2, \ldots, h_r$ of H such that, for every $1 \leqslant i \leqslant r$, gh_ig^{-1} is a power of h_i. For every i between 1 and r, set $\Gamma_i = \langle g, h_i\rangle$ and H_i the cyclic group generated by h_i. For every $1 \leqslant i \leqslant r$, H_i is the p-Sylow subgroup of Γ_i. Then we have that $H^1_{\mathrm{loc}}(\Gamma_i, V_{n,d}) \to H^1_{\mathrm{loc}}(H_i, V_{n,d})$ is injective. Moreover, since H_i is cyclic, $H^1_{\mathrm{loc}}(H_i, V_{n,d}) = 0$, and so $H^1_{\mathrm{loc}}(\Gamma_i, V_{n,d}) = 0$. Then, if Z is a cocycle of $\langle g, H\rangle$ satisfying the local conditions, for every i between 1 and r, it is a coboundary over Γ_i and so, for every $\gamma_i \in \Gamma_i$, there exists $v_i \in V_{n,d}$ such that $Z_{\gamma_i} = \gamma_i(v_i) - v_i$. Since $g \in \Gamma_i$ for every $1 \leqslant i \leqslant r$, for every i, j we have $g(v_i) - v_i = g(v_j) - v_j$. The injectivity of $g - \mathrm{Id}$ implies that for every i, j, $v_i = v_j$. Since $g, h_1, h_2, \ldots, h_r$ generate $\langle g, H\rangle$ we get that Z is a coboundary over $\langle g, H\rangle$. □

Remark 2.5. — Let N be the normal subgroup of G consisting of the elements congruent to the identity modulo p (here we use the notation of Corollary 2.4). We shall prove (see Lemma 2.6) that if there exists $\widetilde{g}$ in $G_1 = G/N$ such that $\widetilde{g}$ is in the normalizer of a p-Sylow subgroup of G_1, $\widetilde{g}$ has order dividing $p-1$ and $\widetilde{g} - \mathrm{Id}$ is bijective, then there exists $g \in G$ in the normalizer of a p-Sylow subgroup of G, such that g has order dividing $p-1$ and $g - \mathrm{Id}$ is bijective.

The existence of an element $h \in G$ such that $h\widetilde{g}^{-1} \in N$, and h in the normalizer of a p-Sylow of G, comes from the Lemma 2.6 below. By raising h to an adequate power of p we find an element g fulfilling the conditions.

Lemma 2.6. — *Let G be a group, let N be a normal subgroup of G and let H be a p-Sylow subgroup of G. Let g be an element of G such that its class in G/N is in the normalizer of the p-Sylow subgroup HN/N of G/N. Then there exists an element of the class gN, which is in the normalizer of H.*

In particular, if the p-Sylow subgroup H is contained in a normal subgroup N of G, then for every class of G/N, there exists an element of the class which is in the normalizer of H.

Proof. — Let $\widetilde{g}$ be the class of g modulo N. By hypothesis $\widetilde{g}(HN/N)\widetilde{g}^{-1} = HN/N$. We deduce that $gHNg^{-1}/N = HN/N$, then $gHg^{-1}N = HN$. So gHg^{-1} and H are two p-Sylow subgroups of HN. Then they are conjugate by some element x of HN. There exists $h \in H$ and $n \in N$ such that $x = nh$. So $gHg^{-1} = nhH(nh)^{-1}$, from which we deduce that $n^{-1}g$ is in the class gN and in the normalizer of H. □

Lemma 2.6 does not give precise information on the order of the elements of the normalizer of H. Neverthless, if H is contained in a normal subgroup N such that $|N|$ and $|G/N|$ are coprime, we have a coprime action (see [2, Chapter 8]) and so there exists a subgroup of G isomorphic to G/N with trivial intersection with N. Then in this case the normalizer contains a group isomorphic to G/N. The next Corollary treats the case when $(|G/N|, |N|)$ is small (a sort of near coprime action) and it is crucial for proving Theorem 1.3.

Corollary 2.7. — *Let V_d be the group $(\mathbb{Z}/p\mathbb{Z})^{2d}$ and let G be a subgroup of the group $\mathrm{GL}(2d, \mathbb{Z}/p\mathbb{Z})$ acting on V_d in the usual way. Let H be a p-Sylow subgroup of G. Suppose that there exists a normal subgroup N of G such that G/N is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$. Let i be $((2d)!, p-1)$. Then the normalizer of H contains an element of order $p-1$, whose class modulo N has order divisible by $(p-1)/i$.*

Proof. — Since $|G/N|$ is not divisible by p, it is clear that $H \subseteq N$. Let g be in G such that the class of g modulo N is a generator of G/N. By Lemma 2.6 there exists an element in the class of g modulo N (we call it g by abuse of notation) such that g is in the normalizer of H. Since the class of g has order $p-1$ in G/N, the order of g is $(p-1)r$, where r is a positive integer. Then g^r is in the normalizer of H, has order $p-1$ and the order of its class in G/N is $(p-1)/(p-1, r)$. Then it is sufficient to prove that $(p-1, r)$ divides i. Since p does not divide $p-1$ we can suppose that r is not divisible by p. Then the action of g is semisimple and so there exists $c \in \mathbb{N}$ such that a matrix associated to g can be decomposed in c blocks of matrices $l_j \times l_j$ acting irreducibly over a sub-space of V_d, such that $\sum_{j=1} l_j = 2d$ and the order of the jth block divides $p^{l_j} - 1$. Then the order of g is the least common multiple of the order of the blocks and so r divides the least common multiple of the $(p^{l_j} - 1)/(p-1)$. Observe that

$$\frac{p^{l_j} - 1}{p - 1} = p^{l_j - 1} + p^{l_j - 2} + \cdots + 1.$$

We have

$$p^{l_j-1} + p^{l_j-2} + \cdots + 1 - (p-1)(p^{l_j-2} + 2p^{l_j-3} + \cdots + (l_j - 1)) = l_j.$$

Then $(p^{l_j} - 1)/(p-1), (p-1)) = (l_j, p-1)$. Since, for every j, $l_j \leqslant 2d$, the least common multiple of the $(l_j, (p-1))$ divides $(2d)!$, which proves the lemma. □

2.2. Cocycles satisfying the local conditions and cohomology of the p-torsion

For every r between 1 and n, let $V_{r,d}$ be the group $(\mathbb{Z}/p^r\mathbb{Z})^d$.

Lemma 2.8. — *Let G be a subgroup of $\mathrm{GL}_{2d}(\mathbb{Z}/p^n\mathbb{Z})$ acting on $V_{n,d}$ in the usual way. Suppose that G contains an element δ such that $\delta-\mathrm{Id}$ is a bijective automorphism of $V_{n,d}$. Then the homomorphism $H^1(G,V_{n,d}[p])\to H^1(G,V_{n,d})$ induced by the exact sequence of G-modules*

$$0\to V_{n,d}[p]\to V_{n,d}\xrightarrow{p} V_{n,d}[p^{n-1}]\to 0,$$

is injective and its image is $H^1(G,V_{n,d})[p]$. In other words it induces an isomorphism between $H^1(G,V_{n,d}[p])$ and $H^1(G,V_{n,d})[p]$.

Proof. — The following exact sequence of G-modules

$$0\to V_{n,d}[p]\to V_{n,d}\xrightarrow{p} V_{n,d}[p^{n-1}]\to 0$$

(here the first map is inclusion and the second map is multiplication by p) induces a long exact sequence of cohomology groups:

$$\begin{aligned}\ldots\to H^0(G,V_{n,d}[p^{n-1}])\to H^1(G,V_{n,d}[p])\to H^1(G,V_{n,d})\\ \to H^1(G,V_{n,d}[p^{n-1}]).\end{aligned}$$

Since G contains an element δ such that $\delta-\mathrm{Id}$ is bijective over $V_{n,d}$, then $H^0(G,V_{n,d}[p^{n-1}])=0$. Hence we have the exact sequence

$$0\to H^1(G,V_{n,d}[p])\to H^1(G,V_{n,d})\to H^1(G,V_{n,d}[p^{n-1}]). \tag{2.1}$$

In particular $H^1(G,V_{n,d}[p])\to H^1(G,V_{n,d})$ is injective.

Let Z be a cocycle from G to $V_{n,d}$, representing a class $[Z]$ in $H^1(G,V_{n,d})$ of order p. Then there exists $v\in V_{n,d}$ such that $pZ_\sigma=\sigma(v)-v$ for every $\sigma\in G$. Since there exists $\delta\in G$ such that $\delta-\mathrm{Id}$ is bijective over $V_{n,d}$ and $pZ_\delta=\delta(v)-v\in V_{n,d}[p^{n-1}]$, we get that $v\in V_{n,d}[p^{n-1}]$. Then the cocycle from G to $V_{n,d}[p^{n-1}]$ sending σ to pZ_σ for every $\sigma\in G$ is a coboundary and so the image of $[Z]$ over $H^1(G,V_{n,d}[p^{n-1}])$ is 0. Then there exists $[W]\in H^1(G,V_{n,d}[p])$ such that the image of $[W]$ by $H^1(G,V_{n,d}[p])\to H^1(G,V_{n,d})$ is $[Z]$ (see the sequence (2.1)). This proves that $H^1(G,V_{n,d}[p])\to H^1(G,V_{n,d})[p]$ is surjective and concludes the proof. □

The next Lemma gives the key step to prove Therorem 1.2 and it will be very useful to study the local-global divisibility problem on abelian surfaces.

Lemma 2.9. — *Let G be a subgroup of $\mathrm{GL}_{2d}(\mathbb{Z}/p^n\mathbb{Z})$ acting on $V_{n,d}$ in the usual way and let H be the normal subgroup of G of the elements acting like the identity over $V_{n,d}[p]$. Suppose that G contains an element δ such that $\delta-\mathrm{Id}$ is a bijective automorphism of $V_{n,d}$. Let $Z\colon G\to V_{n,d}$ be a cocycle whose restriction to H is a coboundary. If $H^1(G/H,V_{n,d}[p])=0$, then Z is a coboundary.*

Proof. — Consider the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \to & H^1(G,V_{n,d}[p]) & \to & H^1(G,V_{n,d})[p] & \to & 0 \\ & & \downarrow & & \downarrow & & \\ 0 & \to & H^1(\langle\delta,H\rangle,V_{n,d}[p]) & \to & H^1(\langle\delta,H\rangle,V_{n,d})[p] & \to & 0, \end{array}$$

where the isomorphisms on the lines are the functions of Lemma 2.8, and the functions on the columns are the restrictions. Since the restriction $H^1(\langle\delta,H\rangle,V_{n,d}) \to H^1(H,V_{n,d})$ is injective, if $\ker(H^1(G,V_{n,d}) \to H^1(H,V_{n,d})$ is not trivial, then there exists a non-trivial $[W] \in H^1(G,V_{n,d}[p])$, which is the kernel of the restriction to $H^1(H,V_{n,d}[p])$. Since H is normal in G, we have the inflation-restriction sequence

$$0 \to H^1(G/H,V_{n,d}[p]) \to H^1(G,V_{n,d}[p]) \to H^1(H,V_{n,d}[p]).$$

Then $[W]$ is the image by the inflation of a non-trivial element of $H^1(G/H,V_{n,d}[p])$. Since $H^1(G/H,V_{n,d}[p]) = 0$, we get a contradiction. Then $H^1(G,V_{n,d}) \to H^1(H,V_{n,d})$ is injective. □

THEOREM 2.10 (Theorem 1.2). — *Suppose that G_1 contains an element g whose order divides $p-1$ and not fixing any non-trivial element of $\mathcal{A}[p]$. Moreover suppose that $H^1(G_1,\mathcal{A}[p]) = 0$. Then $H^1_{\mathrm{loc}}(G_n,\mathcal{A}[p^n]) = 0$ for every positive integer n. Hence, local-global divisibility by p^n holds for $\mathcal{A}(k)$.*

Proof. — Let n be a positive integer and consider $H^1_{\mathrm{loc}}(G_n,\mathcal{A}[p^n])$. Let $\widetilde{g} \in G_n$ be such that the restriction of $\widetilde{g}$ to K_1 is g. By applying Corollary 2.4 with $\widetilde{g}$ in the place of g, $\mathrm{Gal}(K_n/K_1)$ in the place of H and $\langle\widetilde{g},H\rangle$ in the place of G, we get that $H^1_{\mathrm{loc}}(\langle\widetilde{g},H\rangle,\mathcal{A}[p^n]) = 0$. Then for any $[Z] \in H^1_{\mathrm{loc}}(G_n,\mathcal{A}[p^n]) = 0$, $[Z]$ is in the kernel of the restriction to $H^1(H,\mathcal{A}[p^n])$. We conclude the proof by applying Lemma 2.9. □

Remark 2.11. — We would like to remove the hypothesis on the triviality of $H^1(G_1,\mathcal{A}[p])$ in Theorem 1.2. Observe that to do that, by Corollary 2.4 and Remark 2.5, it would be sufficient to prove the following fact: let p be a prime number, let d be a positive integer and G be a subgroup of $\mathrm{GL}_{2d}(\mathbb{Z}/p\mathbb{Z})$. Then there exists a p-Sylow subgroup of G such that g is in its normalizer.

In [3], Ciperiani and Stix found an interesting relation between the irreducible subquotients of $\mathrm{End}(\mathcal{A}[p])$ and $\mathcal{A}[p]$ as Galois modules and the triviality of a certain Tate–Shafarevich group (see [3, Theorem 4] and the Appendix for the details). To study the local-global divisibility problem we need a similar result in which we replace the group studied by Ciperiani and Stix with the first local-cohomology group. We do this in the following Proposition, that is also inspired by Section 6 of [12].

Proposition 2.12. — *Let G be a subgroup of $\mathrm{GL}_{2d}(\mathbb{Z}/p^n\mathbb{Z})$ acting on $V_{n,d}$ in the usual way. Let H be the normal subgroup of G of the elements acting like the identity on $V_{n,d}[p]$. Suppose that G contains an element δ such that $\delta - \mathrm{Id}$ is a bijective automorphism of $V_{n,d}$ and let $\overline{\delta}$ be its class in G/H. If $H^1(G/H, V_{n,d}[p]) = 0$, and both $V_{n,d}[p]$ and $\mathrm{End}(V_{n,d}[p])$ have no common irreducible $\mathbb{Z}/p\mathbb{Z}[\langle\overline{\delta}\rangle]$-submodules (the action of $\overline{\delta}$ over $\mathrm{End}(V_{n,d}[p])$ is induced by the conjugation), then $H^1(G, V_{n,d}) = 0$.*

Proof. — Consider the inflation-restriction sequence

$$0 \to H^1(G/H, V_{n,d}[p]) \to H^1(G, V_{n,d}[p]) \to H^1(H, V_{n,d}[p])^{G/H}.$$

Since $H^1(G/H, V_{n,d}[p]) = 0$, $H^1(G, V_{n,d}[p])$ is isomorphic to a subgroup of $H^1(H, V_{n,d}[p])^{G/H}$. Let $\phi(H)$ be the Frattini sub-group of H (see Definition 2.1). In particular recall (or see [2, p. 105]) that $H/\phi(H)$ is an elementary p-abelian group. Since H acts like the identity over $V_{n,d}[p]$ and $V_{n,d}[p]$ is a commutative group with exponent p, $H^1(H, V_{n,d}[p])^{G/H} = \mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[G/H]}\{H/\phi(H), V_{n,d}[p]\}$ where G/H has an action induced by coniugacy over $H/\phi(H)$. We shall prove that $\mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[\overline{\delta}]}\{H/\phi(H), V_{n,d}[p]\}$, and so $\mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[G/H]}\{H/\phi(H), V_{n,d}[p]\}$ is trivial.

By possibly replacing $\overline{\delta}$ with its p-power, we can suppose that p does not divide the order of $\overline{\delta}$. Then the action of $\langle\overline{\delta}\rangle$ is semisimple and $H/\phi(H)$ is isomorphic to a direct sum of irreducible $\langle\overline{\delta}\rangle$-modules.

Take W an irreducible $\mathbb{Z}/p\mathbb{Z}[\langle\overline{\delta}\rangle]$-submodule of $H/\phi(H)$. For every non-zero $w \in W$, let $i_w \in \mathbb{N}$ be the largest integer such that there exists $h \in H$ such that $h\phi(H) = w$ and $h \equiv \mathrm{Id} \mod (p^{i_w})$. Then $h \not\equiv \mathrm{Id} \mod (p^{i_w+1})$. Since W is irreducible, every non-zero element of W is a generator of W. Then observe that i_w is the same for every $w \neq 0$. Thus W is isomorphic to a $\mathbb{Z}/p\mathbb{Z}[\langle\overline{\delta}\rangle]$-submodule of

$$\begin{aligned} M_{i_w+1} = \{\mathrm{Id} + p^{i_w+1}M \ \mid M \in \mathrm{Mat}_{2d}(\mathbb{Z}/p^n\mathbb{Z})\} \\ /\{\mathrm{Id} + p^{i_w+2}M' \ \mid M' \in \mathrm{Mat}_{2d}(\mathbb{Z}/p^n\mathbb{Z})\}. \end{aligned}$$

Since M_{i_w+1} is isomorphic, as $\mathbb{Z}/p\mathbb{Z}[\langle\overline{\delta}\rangle]$-module, to $\mathrm{End}(V_{n,d}[p])$, W is isomorphic to a submodule of $\mathrm{End}(V_{n,d}[p])$. Since, by hypothesis, $V_{n,d}[p]$ and $\mathrm{End}(V_{n,d}[p])$ have no common irreducible $\mathbb{Z}/p\mathbb{Z}[\langle\overline{\delta}\rangle]$-submodules, then $\mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[\overline{\delta}]}\{H/\phi(H), V_{n,d}[p]\} = 0$. Hence,

$$\mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[G/H]}\{H/\phi(H), V_{n,d}[p]\} = 0.$$

Thus $H^1(G, V_{n,d}[p]) = 0$. Since the groups $H^1(G, V_{n,d}[p])$ and $H^1(G, V_{n,d})[p]$ are isomorphic (see Lemma 2.8), we get $H^1(G, V_{n,d})[p] = 0$, which implies $H^1(G, V_{n,d}) = 0$. □

The following Lemma gives a useful criterion to see if an element δ of G satisfies the hypothesis of Proposition 2.12.

Lemma 2.13. — *Let $\delta \in \mathrm{GL}_{2d}(\mathbb{Z}/p\mathbb{Z})$ be with order not divisible by p and let $\lambda_1, \lambda_2, \dots, \lambda_{2d}$ the eigenvalues of δ. Suppose that for every i, j between 1 and $2d$, λ_i/λ_j is not an eigenvalue of δ. Then $V_{1,d}$ and $\mathrm{End}(V_{1,d})$ have no common irreducible $\mathbb{Z}/p\mathbb{Z}[\langle\delta\rangle]$-submodules.*

Proof. — Observe that the Lemma is evident if δ is diagonalizable over $\mathbb{F}_p$. Since p does not divide the order of δ, δ is diagonalizable in a finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$. Since the irreducible $\mathbb{Z}/p\mathbb{Z}[\langle\delta\rangle]$-modules are direct sums of irreducible $\mathbb{F}_q[\langle\delta\rangle]$-modules, the result follows. □

3. The group of the symplectic similitudes and proof of Theorem 3

We start by a description of the Galois action over the p-torsion of a polarized abelian variety $\mathcal{A}$ of dimension $d \in \mathbb{N}$. The referencies that we use for that are [13, Section 2] and [7].

Let $\mathcal{A}$ be an abelian variety admitting a polarization with degree not divisible by p. The Tate module $T_p(\mathcal{A})$ has a skew-symmetric, bilinear, Galois-equivariant form (called Weil pairing)

$$\langle\ ,\ \rangle\colon T_p(\mathcal{A}) \times T_p(\mathcal{A}) \to \mathbb{Z}_p(1),$$

where $\mathbb{Z}_p(1)$ is the 1-dimensional Galois module, in which the action is given by the cyclotomic character $\chi_p\colon\ \mathrm{Gal}(\overline{k}/k) \to \mathbb{Z}_p^*$. This is not degenerate over $\mathcal{A}[p]$ because p does not divide the degree of the polarization. The fact that the Weil pairing is not degenerate means that the Galois group over k of the field generated by all the torsion points of order a power of p is a subgroup of the group of the symplectic similitudes of $T_p(\mathcal{A})$, with respect to the Weil pairing $\mathrm{GSp}(T_p(\mathcal{A}), \langle\ ,\ \rangle)$. Choosing a basis of $\mathcal{A}[p]$ we can consider G_1 (recall that $G_1 = \mathrm{Gal}(k(\mathcal{A}[p])/k)$) as a subgroup of $\mathrm{GSp}_{2d}(\mathbb{F}_p)$.

For every $\sigma \in G_1$, we define the multiplier of σ as the element $\nu(\sigma) \in \mathbb{F}_p^*$ such that, for every P_1, P_2 in $\mathcal{A}[p]$, $\langle\sigma(P_1), \sigma(P_2)\rangle = \nu(\sigma)\langle P_1, P_2\rangle$. Then $\nu(\sigma) = \chi_p(\sigma)$ and the determinant of σ is just $\nu(\sigma)^d = \chi_p(\sigma)^d$.

Theorem 3.1 (Theorem 1.3). — *Let $\mathcal{A}$ be a polarized abelian variety of dimension d defined over k and let p be a prime not dividing the degree of the polarization. Suppose that $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. Set $i = ((2d)!, p-1)$ and k_i the subfield of $k(\zeta_p)$ of degree i over k. If for every non-zero $P \in \mathcal{A}[p]$ the field $k(P) \cap k(\zeta_p)$ strictly contains k_i, then for every positive integer n, the group $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$. Hence, local-global divisibility by p^n holds for $\mathcal{A}(k)$.*

Proof. — Since $\mathcal{A}$ is a polarized abelian variety and p does not divide the degree of the polarization, $k(\zeta_p) \subseteq K_1$. Moreover since by hypothesis $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, we have that $\mathrm{Gal}(k(\zeta_p)/k)$ is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$. Let N be the group $\mathrm{Gal}(K_1/k(\zeta_p))$. By elementary Galois theory, then N is a normal subgroup of G_1, containing all p-Sylow subgroups of G_1 because $[G_1 : N] = p-1$, which is not divisible by p. Let H be a p-Sylow subgroup of G_1. Let i be $((2d)!, p-1)$. By Corollary 2.7, there exists $g \in G_1$ of order $(p-1)$ such that its restriction to $k(\zeta_p)$ has order divisible by $(p-1)/i$. By hypothesis, for every point P of order p of $\mathcal{A}$ we have that $k(P) \cap k(\zeta_p)$ strictly contains the subfield of degree i over k, which is fixed by the restriction of g to $k(\zeta_p)$. Then g does not fix any point of order p and so $g - \mathrm{Id}$ is bijective as endomorphism of $\mathcal{A}[p]$. We conclude the proof by applying Corollary 2.4. □

4. Proof of Theorem 1.4

The proof of Theorem 1.4 requires the study of some properties of $\mathrm{GSp}_4(\mathbb{F}_p)$. We do this in the next subsection.

4.1. Some properties of the group $\mathrm{GSp}_4(\mathbb{F}_p)$

In the next Lemma we list some well-known properties of the group $\mathrm{GSp}_4(\mathbb{F}_p)$.

Lemma 4.1. — *Let $p \geqslant 3$ be a prime number.*

(1) *The order of $\mathrm{GSp}_4(\mathbb{F}_p)$ is $p^4(p-1)^3(p+1)^2(p^2+1)$;*
(2) *Let B be an element of $\mathrm{GSp}_4(\mathbb{F}_p)$. The eigenvalues of B can be written as λ_1, λ_2, $\nu(B)\lambda_1^{-1}$, $\nu(B)\lambda_2^{-1}$, where ν is the multiplier (see Section 3).*

Proof. — (1) is well-known.

For (2), we can use that every $M \in \mathrm{Sp}_4(\mathbb{F}_p)$ has eigenvalues $\alpha, \beta, \alpha^{-1}, \beta^{-1}$ (see [6] or [7, Lemma 2.2]), and the exact sequence

$$1 \to \mathrm{Sp}_4(\mathbb{F}_p) \to \mathrm{GSp}_4(\mathbb{F}_p) \to (\mathbb{Z}/p\mathbb{Z})^* \to 1,$$

where the last map is $\nu\colon\ \mathrm{GSp}_4(\mathbb{F}_p) \to (\mathbb{Z}/p\mathbb{Z})^*$. □

The next Theorem, proved by Lombardo (see [13, Section 3.1]), gives a very precise list of the maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_p)$ not containing $\mathrm{Sp}_4(\mathbb{F}_p)$ and it is one of the main ingredients of our proof.

Theorem 4.2. — *Let $p > 7$ be a prime number. Let G be a proper subgroup of $\mathrm{GSp}_4(\mathbb{F}_p)$ not containing $\mathrm{Sp}_4(\mathbb{F}_p)$. Then G is contained in a maximal proper subgroup Γ of $\mathrm{GSp}_4(\mathbb{F}_p))$ such that one of the following holds:*

(1) *Γ stabilizes a subspace;*
(2) *There exist 2-dimensional subspaces V_1, V_2 of $\mathbb{F}_p^4$ such that $\mathbb{F}_p^4 = V_1 \bigoplus V_2$ and*

$$\Gamma = \{A \in \mathrm{GSp}_4(\mathbb{F}_p) \mid \exists\, \gamma \in S_2 \mid AV_i \subseteq V_{\gamma(i)}\ i = 1, 2\};$$

(3) *There exists an $\mathbb{F}_{p^2}$-structure on $\mathbb{F}_p^4$ such that*

$$\Gamma = \{A \in \mathrm{GSp}_4(\mathbb{F}_p) \mid \exists\, \rho \in \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) \\ \mid \forall\, \lambda \in \mathbb{F}_{p^2}, \forall\, v \in \mathbb{F}_p^4\ A(\lambda * v) = \rho(\lambda) * A(v)\},$$

where $*$ is the multiplication map $\mathbb{F}_{p^2} \times \mathbb{F}_p^4 \to \mathbb{F}_p^4$. In this case, the set

$$\{A \in \mathrm{GSp}_4(\mathbb{F}_p) \mid \forall\, \lambda \in \mathbb{F}_{p^2}, \forall\, v \in \mathbb{F}_p^4\ A(\lambda * v) = \lambda * A(v)\},$$

is a subgroup of Γ of index 2;

(4) *Γ contains a group H isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$ such that the projective image of Γ is identical to the projective image of H. Moreover, for every $\sigma \in H$, the eigenvalues of σ can be written as $\lambda_1^3, \lambda_1^2\lambda_2, \lambda_1\lambda_2^2, \lambda_2^3$, with λ_1 and λ_2 roots of a second degree polynomial with coefficients in $\mathbb{F}_p$. Here λ_1 and λ_2 are the eigenvalues of the element of $\mathrm{GL}_2(\mathbb{F}_p)$ corresponding to σ;*
(5) *The projective image of Γ has order at most 3 840.*

Proof. — See [13, Definitions 3.1 and 3.2, Theorem 3.3, Lemma 3.4]. □

4.2. Subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$

Let q be a power of p. To prove Theorem 1.4, in many cases we can reduce to study a group isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ (see the next subsection), or to a subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$. Then we recall the well-known classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$ that we often use in the next subsection.

Proposition 4.3. — *Let G be a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ of order not divisible by p. If G is neither cyclic nor dihedral, then G is isomorphic to either A_4, S_4 or A_5.*

Proof. — See [20, Proposition 16]. □

Proposition 4.4. — *Let G be a subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$ and suppose that $p \geqslant 5$ and p divides the order of G. Then either there exists $r \geqslant 1$ such that G contains $\mathrm{SL}_2(\mathbb{F}_{p^r})$ or G has a unique abelian p-Sylow subgroup H such that G/H is cyclic of order dividing $q-1$.*

Proof. — See [21, Chapter 3.6, Theorem 6.17]. □

The following Corollary of Propositions 4.3 and 4.4 will be often used in the next subsection.

Corollary 4.5. — *Let $p \geqslant 5$ be a prime number and let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ such that G contains an element σ of order > 2 and dividing $p+1$, and such that the image of the determinant of G in $\mathbb{F}_p^*$ has order i. Then G contains a scalar matrix of order $i/(i,60)$.*

Proof. — Suppose first that p divides the order of G. Since by hypothesis σ has order not dividing $p-1$ and not divisible by p, by Proposition 4.4 G contains $\mathrm{SL}_2(\mathbb{F}_p)$. Since the image of the determinant of G in $\mathbb{F}_p^*$ has order i, then G contains a scalar matrix of order at least $i/(i,2)$.

Suppose that p does not divide the order of G. Let $\delta \in G$ be such that its determinant has order i. Then, since i divides $p-1$ and $(p-1,p+1)=2$, by possibly considering a suitable power g of δ, we can suppose that g is diagonalizable and it has determinant of order divisible by $i/(i,2)$. Let PG denote the image of G by the projection over $\mathrm{PGL}_2(\mathbb{F}_p)$ and $\overline{g}$, respectively $\overline{\sigma}$, the images of g respectively σ in PG. By Proposition 4.3 either PG is cyclic, or PG is dihedral or PG is a group with exponent dividing 60.

Suppose that PG is cyclic. Then $\overline{g}$ and $\overline{\sigma}$ commute. Hence $g\sigma g^{-1}\sigma^{-1}$ is a scalar matrix with determinant 1. Since g is diagonalizable and σ is not diagonalizable because its order does not divide $p-1$, a simple calculation shows that g^2 is a scalar matrix. Then G contains a scalar matrix of order $i/(i,4)$.

Suppose that PG is dihedral. We call a rotation a power of the element of largest order in PG and a symmetry any element of order 2 that anti-commutes with the rotations. If $\overline{g}$ and $\overline{\sigma}$ commute, then like in the previous case, we prove that g^2 is a scalar matrix. Moreover, if $\overline{g}$ is a symmetry, then it has order 2 and so g^2 is a scalar matrix. Then G contains a scalar matrix of order $i/(i,4)$. Thus it only remains the case where $\overline{\sigma}$ is a symmetry and $\overline{g}$ is a rotation. In this case $\overline{\sigma g \sigma}^{-1} = \overline{g}^{-1}$ and so $\sigma g \sigma^{-1} g$ is a scalar matrix $\mu\,\mathrm{Id}$ with $\mu \in \mathbb{F}_p^*$. Observe that the determinant of $\mu\,\mathrm{Id}$ is equal to the square of the determinant of g. Then also in this case G contains a scalar matrix of order $i/(i,4)$.

It is well-knwown that A_4 has exponent 6, S_4 has exponent 12 and A_5 has exponent 30. Since $(30,12) = 60$, and 4 divides 60, in particular G contains a scalar matrix of order $i/(i,60)$. □

4.3. End of the proof

We first recall the statement of Theorem 1.4.

Theorem 4.6 (Theorem 1.4). — *Let $\mathcal{A}$ be a polarized abelian surface defined over k. For every prime number $p > 3840$ such that $k \cap \mathbb{Q}(\zeta_p) = k$ and not dividing the degree of the polarization, if there exists $n \in \mathbb{N}$ such that $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) \neq 0$, then there exists a finite extension $\widetilde{k}$ of k of degree $\leqslant 24$ such that $\mathcal{A}$ is $\widetilde{k}$-isogenous to an abelian surface with a torsion point of order p defined over $\widetilde{k}$.*

Proof. — Suppose that there exists $n \in \mathbb{N}$ such that $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) \neq 0$. The proof is divided in some distinct steps. The first is the following simple lemma.

Lemma 4.7. — *The group G_1 is isomorphic to its projective image to $\mathrm{PGL}_4(\mathbb{F}_p)$. Moreover the function ν from G_1 to $(\mathbb{Z}/p\mathbb{Z})^*$ sending $\sigma \in G_1$ to its multiplier $\nu(\sigma)$ is surjective and G_1 contains an element g of order $p-1$ and multiplier divisible by $(p-1)/2$.*

Proof. — If G_1 is not isomorphic to its projective image, then it contains a scalar matrix whose eigenvalue is distinct of 1. Then, by Theorem 1.2, $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$ for every positive integer n (actually $H^1(G_n, \mathcal{A}[p^n]) = 0$ for every positive integer n, see for instance [10, p. 29]).

Since by hypothesis $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ and $k(\zeta_p)$ is the subfield of K_1 fixed by the kernel of the multiplier ν (see Section 3), we have $G_1/\ker(\nu)$ isomorphic to $\mathrm{Gal}(k(\zeta_p)/k)$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$.

Finally, since $G_1/\ker(\nu)$ is a cyclic group of order $(p-1)$, every element of G_1 whose class generates $G_1/\ker(\nu)$ has order divisible by $(p-1)$. □

The following Proposition shows that a large subgroup of G_1 has a stable proper subspace of $\mathcal{A}[p]$.

Proposition 4.8. — *There exists a subgroup Γ of G_1 of index at most 4 and a proper subspace V of $\mathcal{A}[p]$ such that $\sigma(V) = V$ for every $\sigma \in \Gamma$.*

Proof. — By Lemma 4.7, G_1 is isomorphic to its projective image and so it does not contain $\mathrm{Sp}_4(\mathbb{F}_p)$, because $-\mathrm{Id} \in \mathrm{Sp}_4(\mathbb{F}_p)$. Moreover, see Lemma 4.7, G_1 has order at least $p-1$ and recall that $p > 3840$. Then, by Theorem 4.2, either G_1 stabilizes a proper subspace of $\mathbb{F}_p^4$, or G_1 is contained in a maximal subgroup of type 2., 3., or 4. in the list of Theorem 4.2.

Suppose that G_1 is contained in a subgroup of type 2. Then, there exists V_1 and V_2 subspaces of $\mathcal{A}[p]$ of dimension 2 such that, for every $\sigma \in G_1$, either σ permutes V_1 and V_2 or σ stabilizes V_1 and V_2. Let Γ be the subgroup of G_1 that stabilizes V_1 and V_2. Observe that it is a normal subgroup of index at most 2. Then Γ stabilizes two proper subspaces.

Suppose that G_1 is contained in a subgroup of type 3. Then G_1 has a subgroup Γ of index at most 2 such that there exists a $\mathbb{F}_{p^2}$-structure on $\mathbb{F}_p^4$ such that Γ is contained in the group

$$\{A \in \mathrm{GSp}_4(\mathbb{F}_p) \mid \forall\, \lambda \in \mathbb{F}_{p^2}, \forall\, v \in \mathbb{F}_p^4\ A(\lambda * v) = \lambda * A(v)\},$$

where $*$ is the multiplication map $\mathbb{F}_{p^2} \times \mathbb{F}_p^4 \to \mathbb{F}_p^4$. Then, by choosing a $\mathbb{F}_p^2$-basis of $\mathbb{F}_p^4$, we get an injective homomorphism of $\phi\colon \Gamma \to \mathrm{GL}_2(\mathbb{F}_{p^2})$. Also observe that for every $\sigma \in \Gamma$, $\phi(\sigma)$ has the same eigenvalues of σ (with multiplicity divided by 2). Then $\phi(\Gamma)$ is contained in $\mathrm{PGL}_2(\mathbb{F}_{p^2})$. Suppose first that p does not divide the order of Γ. Then, by Proposition 4.3 and the fact that $p-1$ divides the order of G_1, either Γ is cyclic or Γ is dihedral. If Γ is cyclic, then, since the generator of Γ has two eigenvalues with multiplicity 2, it stabilizes two subspaces of dimension 2. If Γ is dihedral, then it contains a normal cyclic subgroup Γ' of index 2. Thus, by replacing Γ with Γ', we reduce to the previous case. Also observe that $[G_1 : \Gamma']$ divides 4. Suppose now that p divides the order of Γ. Then, by Proposition 4.4 and the fact that $\phi(\Gamma)$ is isomorphic to its projective image, $\phi(\Gamma) \cap \mathrm{SL}_2(\mathbb{F}_{p^2})$ is contained in a Borel subgroup. Since the p-Sylow subgroup is normal, actually $\phi(\Gamma)$ is contained in a Borel subgroup and so Γ stabilizes a subspace of dimension 2.

Suppose that G_1 is contained in a maximal subgroup of type 4. Then, since G_1 is isomorphic to its projective image, G_1 is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Observe that (see Theorem 4.2) the isomorphism sends the projective image of G_1 to $\mathrm{PGL}_2(\mathbb{F}_p)$ and so actually G_1 is isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$. If p does not divide the order of G_1, then by Proposition 4.3 and since $p-1$ divides the order of G_1, we get that G_1 is either cyclic or dihedral. If G_1 is cyclic and since $\mathrm{PGL}_2(\mathbb{F}_p)$ has order $p(p-1)(p+1)$, we get that G_1 stabilizes a subspace. If G_1 is dihedral, then G_1 has a normal cyclic subgroup Γ of index 2 and so, by replacing G_1 with Γ, we get the same result. Suppose that p divides the order of G_1. In this case, by Proposion 4.4, G_1 has a unique non-trivial p-Sylow subgroup and so it stabilizes a subspace. □

From the next Proposition and a deep result of Katz (see Theorem 4.11) it will easily follow Theorem 1.4.

Proposition 4.9. — *There exists a subgroup Γ of G_1 of index $\leqslant 24$ such that every $\gamma \in \Gamma$ has at least an eigenvalue equal to* 1.

Proof. — By Proposition 4.8, by possibly replacing G_1 with a subgroup Γ of index 2 or 4, there exists V a proper subspace of $\mathcal{A}[p]$ stable by the action of Γ. Then, by Lemma 4.7, Γ contains a diagonal element g with order dividing $p-1$ and multiplier with order divisible by $(p-1)/(p-1,8)$. By abuse of notation, from now on we set $G_1 = \Gamma$. Let $V^\perp$ be the subspace of $\mathcal{A}[p]$ of the $w \in \mathcal{A}[p]$ such that, for every $v \in V$, we have $\langle v, w\rangle = 0$. Then, since the Weil pairing $\langle\ ,\ \rangle$ is Galois-equivariant, also $V^\perp$ is stable by the action of G_1. Suppose first that V has dimension 1. Then $V \subseteq V^\perp$ and $V^\perp$ has dimension 3. On the other hand, if V has dimension 3, then $V^\perp$ has dimension 1 and $V^\perp \subseteq V$. By possibly replacing V with $V^\perp$, we have two cases: either V has dimension 3 or V has dimension 2.

The case when V has dimension 3. — Suppose that V has dimension 3 and so $V^\perp$ has dimension 1 and it is contained in V. Then we have the following G_1-modules: $V^\perp \subseteq V \subseteq \mathcal{A}[p]$ of dimension 1, $V \subseteq \mathcal{A}[p]$ of dimension 3, $V/V^\perp$ of dimension 2 and $\mathcal{A}[p]/V$ of dimension 1. In particular, observe that the exponent of G_1 is coprime with $(p^2+1)/2$. Let H be a p-Sylow subgroup of G_1. Then H is the identity over $V^\perp$ and over $\mathcal{A}[p]/V$. Then, for every $\tau \in G_1$, if the projection of τ over $V/V^\perp$ is in the normalizer of the projection of H, then τ is in the normalizer of H. Since $V/V^\perp$ has dimension 2 and for every subgroup Δ of $\mathrm{GL}_2(\mathbb{F}_p)$, every element of order dividing $p-1$ is in the normalizer of a p-Sylow subgroup of Δ, every element of G_1 of order dividing $p-1$ is in the normalizer of a p-Sylow subgroup of G_1. Then, see Corollary 2.4 and Remark 2.5, every element of order dividing $p-1$ has at least an eigenvalue equal to 1. Let σ be in G_1 such that σ has all the eigenvalues distinct from 1. Then, since σ stabilizes $V^\perp$ and $A[p]/V$, the unique possibility is that the automorphism of $V/V^\perp$ induced by σ has order divisible by a divisor of $(p+1)$ not dividing $(p-1)$. On the other hand choose v and w in V such that $\{v, w\}$ is sent by the projection to a basis of $V/V^\perp$. Let us remark that v is not orthogonal to w. In fact, if v were orthogonal to w, then $\langle v\rangle^\perp$ would be equal to V, and so $V^\perp$ would be $\langle v\rangle$. But $v \notin V^\perp$. Then we have a contradiction. Thus, for every $\tau \in G_1$, the determinant of the projection of τ over $V/V^\perp$ is equal to the multiplier of τ and so, by Corollary 4.5 and the fact that the image of the multiplier has index dividing 4 over $\mathbb{F}_p^*$, we have that there exists $\delta \in G_1$ such that the projection of δ over $V/V^\perp$ is a scalar matrix $\lambda\,\mathrm{Id}$ with λ of order $(p-1)/(p-1,60)$. Then, since the order of δ divides $p-1$, one of its eigenvalues is 1. Then the eigenvalues of δ are $1, \lambda, \lambda, \lambda^2$. Observe that the eigenvalues distinct from λ are one the eigenvalue of the restriction of δ to $V^\perp$, and the other the eigenvalue of the projection of δ to $\mathcal{A}[p]/V$. Suppose that δ is the identity over $V^\perp$ (the other case is identical). Let $\gamma \in G_1$ be any element of order dividing $p-1$ and suppose that the eigenvalues of γ are $\lambda_1, \lambda_2, \lambda_3, \lambda_4$. Then observe that since the projection of δ to $V/V^\perp$ is in the center of the projection of G_1, by possibly permuting the eigenvalues of γ, for every integer i we have that the eigenvalues of $\delta^i g$ are $\lambda_1, \lambda^i\lambda_2, \lambda^i\lambda_3, \lambda^{2i}\lambda_4$. Moreover, $\delta^i\gamma$ has order dividing $(p-1)p^r$ for a certain integer r. But raising a power of p of an element does not change the eigenvalues and so we can suppose that $\delta^i\gamma$ has order dividing $p-1$. Since λ has order $p-1$ and $p > 3840$, if $\lambda_1 \neq 1$, then we can choose i such that $\delta^i\gamma$ has all the eigenvalues distinct from 1. But this is not possible and so every element of order dividing $p-1$ is the identity over $V^\perp$. Let again σ be an element with all eigenvalues distinct from 1 and so such that $\overline{\sigma}$ has order divisible by a divisor of $(p+1)$ not dividing $(p-1)$. Since we can suppose that p does not divide the order of σ, then σ^{p+1} has order dividing $(p-1)$. Thus σ^{p+1} is the identity over $V^\perp$. But $(p+1, p-1) = 2$ and so the restriction of σ to $V^\perp$ is either the identity or $-\mathrm{Id}$. Thus the subgroup Γ of G_1 that fixes $V^\perp$ has index 2. This concludes the proof in the case that V has dimention 3.

The case when V has dimension 2 and $V \cap V^\perp = \{0\}$. — Since $V \cap V^\perp = \{0\}$, then $\mathcal{A}[p]$ is isomorphic as G_1-module to the direct sum of V and $V^\perp$. Moreover, we can suppose that V and $V^\perp$ are irreducible because, if not, $\mathcal{A}[p]$ has G_1-submodule of dimension 1 and we are in the previous case.

Suppose that the order of G_1 is coprime with $(p+1)/2$. Then G_1 has a unique p-Sylow subgroup and, by Corollary 2.4 and Remark 2.5, we have that every element of G_1 of order dividing $p-1$ has at least an eigenvalue equal to 1. Since G_1 has order coprime with $(p+1)/2$ and it stabilizes two spaces of dimension 2, G_1 has exponent dividing $(p-1)p^2$. Since, for every $\tau \in G_1$, τ and τ^p have the same eigenvalues, all the elements of G_1 have at least an eigenvalue equal to 1. Then we can suppose that there exists $\sigma \in G_1$ of order dividing $p+1$ and not dividing $(p-1)$. In particular the restriction of σ to either V or $V^\perp$ should have the same property and so suppose that this is the case for the restriction to V (the other case is identical). Since $V \cap V^\perp = \{0\}$, for every $\tau \in G_1$ the determinant of the restriction of τ to V is the multiplier of τ. Since the multiplier has index dividing 4 over $\mathbb{F}_p^*$, by Corollary 4.5 there exists $\delta \in G_1$ such that the restriction of δ to V is a scalar matrix $\lambda\,\mathrm{Id}$ with λ of order $(p-1)/(p-1,60)$. By possibly replacing δ with its power, since $(p-1,p+1)=2$, we can suppose that δ has order dividing $p-1$, but then we have just that λ has order divisible by $(p-1)/(p-1,120)$. In particular observe that since the restriction of δ to V is a scalar matrix, δ is diagonalizable over $V^\perp$ and $V^\perp$ has dimension 2, then δ is in the normalizer of a p-Sylow subgroup of G_1. Hence, by Corollary 2.4 and Remark 2.5, the eigenvalues of the restriction of δ to $V^\perp$ are 1 and λ^2. Consider now the restriction $G_{1,\perp}$ of G_1 to $V^\perp$. If there exists $\tau \in G_1$ whose restriction to $V^\perp$ has order dividing $p+1$ and not divisible by $p-1$, then by Corollary 4.5 there exists $\delta' \in G_1$, which is a scalar matrix over $V^\perp$ with order dividing $(p-1)/(p-1,120)$. Then δ' commutes with δ and by taking the product of suitable powers of δ and δ', we get an element of G_1 of order dividing $p-1$, with all the eigenvalues distinct from 1. Moreover, since V and $V^\perp$ have dimension 2, such an element is in the normalizer of a p-Sylow subgroup and so $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$ for every positive integer n, by Corollary 2.4 and Remark 2.5. Then the restriction of $G_{1,\perp}$ has order dividing $2p(p-1)^2$. If p divides the order of $G_{1,\perp}$, by Proposition 4.4 either $G_{1,\perp}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$ (and so $p+1$ divides the order of $G_{1,\perp}$) or $G_{1,\perp}$ has a unique p-Sylow subgroup of order p. But in the last case $V^\perp$ is reducible and then we get a contradiction. Hence $G_{1,\perp}$ has order dividing $2(p-1)^2$. Since $V^\perp$ is irreducible, the unique possibility is that $G_{1,\perp}$ has a commutative normal subgroup Δ of index 2 with order dividing $(p-1)^2$. Take Γ the subgroup of G_1 of the elements whose restrictions to $V^\perp$ are in Δ. Then G_1 has index 2 over Γ and Γ stabilizes a subspace of dimension 1 and its orthogonal (then a space of dimension 3). Then we are in the previous case already studied: the case when V has dimension 3.

The case when $V = V^{\perp}$. — First observe that if V is not irreducible, then we are in the case when V has dimension 3 (or 1) and so we suppose that V is an irreducible G_1-module. Let W be the G_1-module $\mathcal{A}[p]/V$. Let us call I_V, respectively I_W, the normal subgroup of G_1 fixing all the elements of V, respectively W. Suppose that p divides the order of G_1/I_V. Then there is $\sigma \in G_1$ of order p and a basis $\{v_1, v_2\}$ of V such that $\sigma(v_1) = v_1$ and $\sigma(v_2) = v_1 + v_2$. Let w_1, w_2 be in $\mathcal{A}[p]$, such that w_i is not orthogonal to v_i and w_i is orthogonal to v_j for $i \neq j$ and $i, j \in \{1, 2\}$. Then $\{v_1, v_2, w_1, w_2\}$ is a basis of $\mathcal{A}[p]$. Moreover, let $\overline{w_1}$ and $\overline{w_2}$ be the class (modulo V) of w_1, respectively w_2. Then $\{\overline{w_1}, \overline{w_2}\}$ is a basis of W. Let us show that the class of σ in G_1/I_W has order p. If the class of σ were not of order p, it would be the identity. Then, there would exist $v \in V$ such that $\sigma(w_1)$ should be equal to $w_1 + v$. Thus

$$\langle \sigma(v_2), \sigma(w_1) \rangle = \langle v_1 + v_2, w_1 \rangle = \langle v_1, w_1 \rangle.$$

But $\langle \sigma(v_2), \sigma(w_1) \rangle = \langle v_2, w_1 \rangle$, which is distinct from $\langle v_1, w_1 \rangle$ because v_1 and w_1 are not orthogonal and v_2, w_1 are orthogonal. In the same way we can prove that if p divides G_1/I_W, then there exists $\sigma \in G_1$ of order p such that the restriction of σ to V has order p. Since V and W are irreducible, if their p-Sylow subgroup is not the identity, then their p-Sylow subgroup cannot be normal and so, by Proposition 4.4, G_1/I_V and G_1/I_W contain the group $\mathrm{SL}_2(\mathbb{F}_p)$. Then, observe that there exists $\tau_1 \in G_1$ whose restriction over V is $-\mathrm{Id}$ and $\tau_2 \in G_1$ whose projection over W is $-\mathrm{Id}$. By Lemma 4.1, then the other eigenvalues of τ_1 are identical and so a p power of τ_1 is a diagonal matrix with two eigenvalues equal to -1 and the others equal to a $\lambda \in \mathbb{F}_p^*$. In the same way we can prove that a p-power of τ_2 is a diagonal matrix with two eigenvalues equal to -1 and the others equal to μ for a certain $\mu \in \mathbb{F}_p^*$. Then either τ_1, τ_2 or $\tau_1\tau_2$ has order dividing $p-1$, has all the eigenvalues distinct from 1 and is in the normalizer of a p-Sylow subgroup because is a scalar matrix over V and over W. Then, by Corollary 2.4 and Remark 2.5, for every positive integer n we have $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$. Thus G_1/I_V and G_1/I_W have orders not divisible by p and so G_1 has a normal p-Sylow subgroup N such that $N \subseteq I_V$ and $N \subseteq I_W$. Thus, if G_1 has order coprime with $(p+1)/2$, by Corollary 2.4 and Remark 2.5, for every positive integer n we have $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$. Then, there exists $\sigma \in G_1$ with order dividing $p + 1$ and not dividing $p - 1$. Since $(p - 1, p + 1) = 2$, by Lemma 4.1 we can suppose that the eigenvalues of σ are either μ, μ^p (both with multiplicity 2) or μ, μ^p, $-\mu$, $-\mu^p$. The following Lemma, whose proof is similar to the proof of Proposition 2.12, gives a strong restriction to the order of σ.

Lemma 4.10. — *If there exists $n \in \mathbb{N}$ such that $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) \neq 0$, then σ has order dividing* 6.

Proof. — First observe that $\sigma - \mathrm{Id}$ is bijective as endomorphism of $\mathcal{A}[p]$ because $\mu \notin \mathbb{F}_p$. Moreover, by using Lemma 2.13, we can prove that $\mathcal{A}[p]$ and $\mathrm{End}(\mathcal{A}[p])$ have a common $\mathbb{Z}/p\mathbb{Z}[\langle\sigma\rangle]$-module only if σ has order dividing 6. Then by Proposition 2.12, if $H^1(G_1, \mathcal{A}[p]) = 0$, we immediately get the result. Then let us prove that $H^1(G_1, \mathcal{A}[p]) = 0$ (actually the proof is similar to the proof of Proposition 2.12). Consider the exact sequence of G_1-modules:

$$0 \to V \to \mathcal{A}[p] \to W \to 0,$$

where the first map is the inclusion and the second is the projection. Since $\delta - \mathrm{Id}$ is bijective over $\mathcal{A}[p]$, we have $H^0(G_1, W) = 0$ and so we get the following cohomology exact sequence

$$0 \to H^1(G_1, V) \to H^1(G_1, \mathcal{A}[p]) \to H^1(G_1, W).$$

Then, to prove the triviality of $H^1(G_1, \mathcal{A}[p])$, it is sufficient to prove the triviality of $H^1(G_1, V)$ and $H^1(G_1, W)$. Let us prove the triviality of $H^1(G_1, V)$ (the proof of the triviality of $H^1(G_1, W)$ is identical). Recall that N is the p-Sylow subgroup of G_1 and N fixes V and W. Then we have the following inflation-restriction sequence:

$$0 \to H^1(G_1/N, V) \to H^1(G_1, V) \to H^1(N, V)^{G_1/N}.$$

Since p does not divide the order of G_1/N, we have $H^1(G_1/N, V) = 0$. Since N fixes V, we get that $H^1(N, V)^{G_1/N}$ is isomorphic to $\mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}[G_1/N]}(N, V)$ where G_1 acts over N by conjugation (recall that since N fixes V and W, N is an abelian group with exponent dividing p). By Lemma 2.13, the action of δ by conjugation over N is given by an automorphism with eigenvalues contained in the set either $\{1, \mu^{p-1}, \mu^{1-p}\}$ or $\{1, -1, \mu^{p-1}, -\mu^{p-1}, \mu^{1-p}, -\mu^{1-p}\}$. On the other hand, over V the element δ has eigenvalues either $\{\mu, \mu^p\}$ or $\{\mu, -\mu, \mu^p, -\mu^p\}$. But $\{1, -1, \mu^{p-1}, -\mu^{p-1}, \mu^{1-p}, -\mu^{1-p}\} \cap \{\mu, -\mu, \mu^p, -\mu^p\}$ is not empty only if μ has order dividing 6. Hence, if σ does not have order dividing 6, then $H^1(G_1, \mathcal{A}[p]) = 0$. □

Observe that if σ has order 3 or 6, then σ^2 has order 3 and it has eigenvalues λ, λ^p (both with multiplicity 2) and λ of order 3. Now recall that G_1 contains an element g of order dividing $p-1$ and multiplier divisible by $(p-1)/(p-1, 8)$. By Corollary 2.4 and Remark 2.5, G_1 has at least an eigenvalue equal to 1. Suppose that the corresponding eigenvector is in V (the case when it is in W is identical). By Proposition 4.3, since p does not divide the order of G_1/I_V, the projective image of G_1/I_V is either cyclic, dihedral or isomorphic to an exceptional subgroup (either A_4, S_4, or A_5). If this last case is verified, then G_1/I_V contains an element τ which act like $-\operatorname{Id}$ over V. By Corollary 2.4 and Remark 2.5, it acts like the identity over W. Then a suitable p-power of τ commutes with g and by choosing $i=1$ or 2, $g^i\tau$ has all the eigenvalues distinct from 1, because g has multiplier divided by $(p-1)/(p-1,8)$ and $p>3840$. Thus either the projective image of G_1/I_V is cyclic of order 3 or it is dihedral of order 6 (in the two cases generated by the class of σ^2 of order 3 and the class of g that can have order 1 or 2). Since g has an eigenvalue equal to 1 over V the unique possibility is that g is either the identity or it has order 2 over V. Then G_1/I_V is generated by σ^2, g and possibly $\delta\in G_1$, which is a scalar matrix over V. But in this case take a suitable power of g^2 multiplied by δ and get a matrix with order dividing $p-1$ and all eigenvalues distinct from 1. Then G_1 has either index 3 or index 6 over I_V. Hence, $K_1^{I_V}$ is an extension of degree dividing 6 of k in which all the elements of I_V fix all the elements of a subspace of V of dimension 2. □

The last result we need to finish the proof is the following deep result of Katz.

Theorem 4.11. — *Let $\mathcal{B}$ be an abelian surface defined over a number field F. If for all but finitely many prime numbers r, we have that a prime number q divides the order of $\mathcal{B}(\mathbb{F}_r)$, then there exists an abelian surface $\mathcal{B}'$ defined over F and F-isogenous to $\mathcal{B}$ such that $\mathcal{B}'$ admits a point of order q over F.*

Proof. — See [11, Introduction]. □

Observe that if all elements of G_1 have at least an eigenvalue equal to 1, then, by Chebotarev density Theorem, for all but finitely many prime numbers q, we have that p divides the order of $\mathcal{A}(\mathbb{F}_q)$. By Proposition 4.9, there exists an extension L of k of degree $\leqslant 24$ such that every element of $\operatorname{Gal}(K_1/L)$ fixes at least a non-trivial element of $\mathcal{A}[p]$. By applying Theorem 4.11, we conlude the proof. □

5. The counterexample

Let p be a prime number such that $p\equiv 2 \mod (3)$. Consider the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$:

$$H_2=\left\{h(a,b)=\begin{pmatrix}1+p(a-2b) & 3p(b-a)\\ -pb & 1-p(a-2b)\end{pmatrix}\ a,b\in\mathbb{Z}/p^2\mathbb{Z}\right\}$$

and

$$G_2 = \left\langle g = \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix},\ H_2 \right\rangle.$$

A simple calculation gives that g has order 3, which does not divide $p-1$. A simple verification gives that for every a, b, we have

$$gh(a,b)g^{-1} = h(-b, a-b),\ g^2h(a,b)g^{-2} = h(b-a, -a).$$

Then H_2 is a normal abelian subgroup of G_2.

We shall prove that $H^1_{\mathrm{loc}}(G_2, (\mathbb{Z}/p^2\mathbb{Z})^2) \neq 0$, by explicitly costructing a cocycle from G_2 to $(\mathbb{Z}/p^2\mathbb{Z})^2$ that satisfies the local conditions, but it is not a coboundary. Observe that H_2 is a $\mathbb{Z}/p\mathbb{Z}[\langle g\rangle]$-module, with g that acts by conjugation. Let Z be a cocycle from G_2 to $(p\mathbb{Z}/p^2\mathbb{Z})^2$. By cocycle relations and the fact that H_2 acts like the identity over $(p\mathbb{Z}/p^2\mathbb{Z})^2$, we have that Z is a homomorphism of $\mathbb{Z}/p\mathbb{Z}[\langle g\rangle]$-modules from H_2 to $(p\mathbb{Z}/p^2\mathbb{Z})^2$. Using that $gh(a,b)g^{-1} = h(-b, a-b)$, a simple calculation shows that the group of homomorphisms of $\mathbb{Z}/p\mathbb{Z}[\langle g\rangle]$-modules from H_2 to $(p\mathbb{Z}/p^2\mathbb{Z})$ is cyclic generated by $Z\colon H_2 \to (p\mathbb{Z}/p^2\mathbb{Z})^2$, with $Z_{h(a,b)} = (p(a-2b), p(a-b))$. Then, extending Z to G_2 by sending g to $(0,0)$ and using the properties of cocycles, we have a cocycle from G_2 to $(\mathbb{Z}/p^2\mathbb{Z})^2$.

Let us show that Z satisfies the local conditions. In other words we shall prove that for every (a,b) the system $h(a,b) - \mathrm{Id}(x,y) = Z_{h(a,b)}$ has a solution. Observe that, by definition of $h(a,b)$, it is sufficient to prove that if $a \neq 0$ or $b \neq 0$, then

$$\begin{pmatrix} a-2b & 3(b-a) \\ -b & 2b-a \end{pmatrix}$$

has determinant distinct from 0 in $\mathbb{Z}/p\mathbb{Z}$. A simple calculation shows that the determinant is $\Delta((a,b)) = a^2+b^2-ab$. Since $\Delta((a,b))$ is a homogenous polynomial in a and in b and a and b are symmetric, if it has a non-zero solution, it has a solution of the form $(-1,\beta)$. Then $\beta^2+\beta+1=0$ that gives that β has order 3 in $(\mathbb{Z}/p\mathbb{Z})^*$. This is not possible because $p \equiv 2 \mod (3)$. Then Z satisfies the local conditions.

We show that Z is not a coboundary. Observe that $(h(1,1)-\mathrm{Id})(x,y) = Z_{h(1,1)}$ if and only if $(x,y) = (1,1)$. Moreover $(h(2,1)-\mathrm{Id})(x,y) = Z_{h(2,1)}$ if and only if $(x,y) = (-1,0)$. Then Z is not a coboundary.

Let k be a number field and let $\mathcal{E}$ be a not CM elliptic curve defined over k. By the main result of [20], for every large enough prime number l, the representation of $\mathrm{Gal}(\overline{k}/k)$ over the group of the automorphisms on the Tate l-module of $\mathcal{E}$ is surjective. Choose a large enough prime $p \equiv 2 \mod (3)$. Then $\mathrm{Gal}(k(\mathcal{E}[p^2])/k) = \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. Let L be the field contained in $k(\mathcal{E}[p^2])$ fixed by G_2. Then $\mathrm{Gal}(L(\mathcal{E}[p^2])/L) = G_2$ and $H^1_{\mathrm{loc}}(\mathrm{Gal}(L(\mathcal{E}[p^2])/L), \mathcal{E}[p^2])$ is not trivial. Then by [10, Theorem 3], by possibly replacing L with a field L' such that $L \subseteq L'$ and $L(\mathcal{E}[p^2]) \cap L' = L$, we get a counterexample to local-global divisibility by p^2 over $\mathcal{E}(L')$. Observe that $\mathrm{Gal}(L'(\mathcal{E}[p])/L')$ is generated by an element of order 3, then of order not dividing $p-1$. Moreover $H^1(\mathrm{Gal}(L'(\mathcal{E}[p])/L'), \mathcal{E}[p]) = 0$ because p and 3 are distinct.

6. Appendix

Ciperiani and Stix [3] and Creutz [4] studied the following question of Cassels, which is related to the local-global divisibility problem: let k be a number field and let $\mathcal{A}$ be an abelian variety defined over k. For every prime number q we say that the Tate–Shafarevich group $Ш(\mathcal{A}/k)$ is q-divisible in $H^1(k, \mathcal{A})$ if $Ш(\mathcal{A}/k) \subseteq \cap_{n \in \mathbb{N}^*} q^n H^1(k, \mathcal{A})$. What is the set of prime numbers q such that $Ш(\mathcal{A}/k)$ is q-divisible ?

We explain the criterion found by Ciperiani and Stix to answer to this question. Define

$$Ш^1(k, \mathcal{A}[p^n]) = \cap_{v \in M_k} \ker(H^1(\mathrm{Gal}(\overline{k}/k), \mathcal{A}[p^n]) \\ \to H^1(\mathrm{Gal}(\overline{k}_v/k_v), \mathcal{A}[p^n])).$$

Let $\mathcal{A}^t$ be the dual variety of $\mathcal{A}$. Ciperiani and Stix (see [3, Proposition 13]) proved the following result.

Theorem 6.1. — *If $Ш^1(k, \mathcal{A}^t[p^n])$ is trivial for every positive integer n, then $Ш(\mathcal{A}/k)$ is p-divisible over $H^1(k, \mathcal{A})$.*

Then, in their paper found very interesting criteria for the triviality of $Ш^1(k, \mathcal{A}^t[p^n])$ (see [3, Theorems A, B, C, D]). We applied some of their ideas in this paper, in particular in the second subsection of Section 2.

We now explain the relation with Cassels question and the local-global divisibility problem (observe that Ciperiani and Stix [3, Remark 20] already substantially observed the connection. Here we just want to make it precise). Let Σ be a subset of the set of places M_k of k. By following [19, p. 15] with $G = \mathcal{A}[p^n]$, we define

$$Ш^1_\Sigma(k, \mathcal{A}[p^n]) = \cap_{v \notin \Sigma} \ker(H^1(\mathrm{Gal}(\overline{k}/k), \mathcal{A}[p^n]) \to H^1(\mathrm{Gal}(\overline{k}_v/k_v), \mathcal{A}[p^n])),$$

$$Ш^1_\omega(k, \mathcal{A}[p^n]) = \cup_{\Sigma \text{ finite}} Ш^1_\Sigma(k, \mathcal{A}[p^n]).$$

Observe that $Ш^1(k, \mathcal{A}[p^n]) = Ш^1_\emptyset(k, \mathcal{A}[p^n])$ and obviously $Ш^1(k, \mathcal{A}[p^n]) \subseteq Ш^1_\omega(k, \mathcal{A}[p^n])$. The Lemma [19, Lemme 1.2] applied with $B = \mathcal{A}[p^n]$ implies that $Ш^1_\omega(k, \mathcal{A}[p^n])$ is isomorphic to $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n])$. Then if the group $H^1_{\mathrm{loc}}(G_n, \mathcal{A}[p^n]) = 0$, we have $Ш^1(k, \mathcal{A}[p^n]) = 0$. By Theorem 6.1 we then get the following Corollaries of Theorem 1.2, Theorem 1.3 and Theorem 1.4 respectively.

Corollary 6.2. — *Suppose that* $\mathrm{Gal}(k(\mathcal{A}^t[p])/k)$ *contains an element* g *whose order divides* $p-1$ *and not fixing any non-trivial element of* $\mathcal{A}[p]$*. Moreover suppose that* $H^1(\mathrm{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p]) = 0$*. Then* $Ш(\mathcal{A}/k)$ *is* p*-divisible in* $H^1(k, \mathcal{A})$*.*

Corollary 6.3. — *Let* $\mathcal{A}$ *be a principally polarized abelian variety of dimension* d *defined over* k *and suppose that* $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$*. Set* $i = ((2d)!, p-1)$ *and* k_i *the subfield of* $k(\zeta_p)$ *of degree* i *over* k*. If for every* $P \in \mathcal{A}[p]$ *of order* p *the field* $k(P) \cap k(\zeta_p)$ *strictly contains* k_i*, then* $Ш(\mathcal{A}/k)$ *is* p*-divisible in* $H^1(k, \mathcal{A})$*,*

Corollary 6.4. — *Let* $\mathcal{A}$ *be a principally polarized abelian surface defined over* k*. For every prime number* $p > 3840$ *such that* $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$*, if* $Ш^1(\mathcal{A}, k)$ *is not* p*-divisible over* $H^1(k, \mathcal{A})$*, then there exists a finite extension* $\widetilde{k}$ *of* k *of degree* $\leqslant 24$ *such that* $\mathcal{A}$ *is* $\widetilde{k}$*-isogenous to an abelian surface with a torsion point of order* p *defined over* $\widetilde{k}$

BIBLIOGRAPHY

[1] E. Artin & J. Tate, *Class field Theory*, Benjamin, 1968, xxvi+259 pages.

[2] M. Aschbacher, *Finite group theory*, Cambridge Studies in Advanced Mathematics, vol. 10, Cambridge University Press, 2000, xi+304 pages.

[3] M. Ciperiani & J. Stix, "Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels", *J. Reine Angew. Math.* **700** (2015), p. 175-207.

[4] B. Creutz, "Locally trivial torsors that are not Weil-Châtelet divisible", *Bull. Lond. Math. Soc* **45** (2013), no. 5, p. 935-942.

[5] ———, "On the local-global principle for divisibility in the cohomology of elliptic curves", *Math. Res. Lett.* **23** (2016), no. 2, p. 377-387.

[6] L. E. Dickson, "Canonical forms of Quaternary Abelian Substitutions in an Arbitrary Galois Field", *Trans. Am. Math. Soc.* **2** (1901), p. 103-138.

[7] L. V. Dieleufait, "Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$", *Exp. Math.* **11** (2002), no. 4, p. 503-512.

[8] R. Dvornicich & U. Zannier, "Local-global divisibility of rational points in some commutative algebraic groups", *Bull. Soc. Math. Fr.* **129** (2001), no. 3, p. 317-338.

[9] ———, "An analogue for elliptic curves of the Grunwald-Wang example", *C. R., Math., Acad. Sci. Paris* **338** (2004), no. 1, p. 47-50.

[10] ———, "On local-global principle for the divisibility of a rational point by a positive integer", *Bull. Lond. Math. Soc.* **39** (2007), p. 27-34.

[11] N. M. Katz, "Galois properties of torsion points on abelian varieties", *Invent. Math.* **62** (1981), p. 481-502.

[12] T. Lawson & C. Wuthrich, "Vanishing of some Galois cohomology groups of elliptic curves", in *Elliptic Curves, Modular Forms and Iwasawa Theory (Cambridge, 2015)*, Springer Proceedings in Mathematics and Statistics, vol. 188, Springer, 2017, p. 373-399.

[13] D. Lombardo, "Explicity surjectivity of Galois representations for abelian surfaces and GL_2-type varieties", *J. Algebra* **460** (2016), p. 26-59.

[14] L. Merel, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124** (1996), no. 1-3, p. 437-449.

[15] L. Paladino, "Local-global divisibility by 4 in elliptic curves defined over $\mathbb{Q}$", *Ann. Mat. Pura Appl.* **189** (2010), no. 4, p. 17-23.

[16] ———, "On counterexamples to local-global divisibility in commutative algebraic groups", *Acta Arith.* **148** (2011), no. 1, p. 21-29.

[17] L. Paladino, G. Ranieri & E. Viada, "Local-Global Divisibility by p^n in elliptic curves", *Bull. Lond. Math. Soc.* **44** (2012), no. 4, p. 789-802.

[18] ———, "On the minimal set for counterexamples to the Local-Global Divisibility principle", *J. Algebra* **415** (2014), p. 290-304.

[19] J.-J. Sansuc, "Groupe de Brauer et arithméthique des groupes linéaires sur un corps de nombres", *J. Reine Angew. Math.* **327** (1981), p. 12-80.

[20] J.-P. Serre, "Proprietés Galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), p. 259-331.

[21] M. Suzuki, *Group Theory I*, Grundlehren der mathematischen Wissenschaften, vol. 247, Springer, 1982, xiv+434 pages.

[22] E. Trost, "Zur theorie des Potenzreste", *Nieuw Arch. Wiskd.* **18** (1948), no. 2, p. 58-61.

Manuscrit reçu le 30 novembre 2016,
révisé le 17 mai 2017,
accepté le 15 juin 2017.

Florence GILLIBERT
Pontificia Universidad Católica de Valparaíso
Instituto de Matemáticas
Blanco Viel 596,
Valparaíso (Chile)
florence.gillibert@pucv.cl

Gabriele RANIERI
Pontificia Universidad Católica de Valparaíso
Instituto de Matemáticas
Blanco Viel 596,
Valparaíso (Chile)
gabriele.ranieri@pucv.cl