Compositio Math. 141 (2005) 847–868
doi:10.1112/S0010437X05001107

Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only

René Schoof

Abstract

We show that for the primes $l = 2, 3, 5, 7$ or 13, there do not exist any non-zero abelian varieties over $\mathbb{Q}$ that have good reduction at every prime different from l and are semi-stable at l. We show that any semi-stable abelian variety over $\mathbb{Q}$ with good reduction outside $l = 11$ is isogenous to a power of the Jacobian variety of the modular curve $X_0(11)$. In addition, we show that for $l = 2, 3$ and 5, there do not exist any non-zero abelian varieties over $\mathbb{Q}$ with good reduction outside l that acquire semi-stable reduction at l over a tamely ramified extension.

1. Introduction

In this paper we study abelian varieties over $\mathbb{Q}$ that have good reduction at all but a single prime. Denoting this one bad prime by l, our first results are concerned with abelian varieties that have semi-stable reduction at l.

Theorem 1.1. *For the primes $l = 2, 3, 5, 7$ or 13, there do not exist any non-zero abelian varieties over $\mathbb{Q}$ that have good reduction at every prime different from l and have semi-stable reduction at l.*

This result is the best possible, because the Jacobian varieties $J_0(l)$ of the modular curves $X_0(l)$ have good reduction at all primes different from l and are semi-stable at l. When l is not one of 2, 3, 5, 7 or 13, these are non-zero abelian varieties.

For the prime $l = 11$ we show the following.

Theorem 1.2. *Every semi-stable abelian variety over $\mathbb{Q}$ that has good reduction outside the prime 11 is isogenous to a power of $J_0(11)$.*

See [VZ04] for a related result in a geometric context.

Our second result concerns abelian varieties over $\mathbb{Q}$ that have good reduction outside l and acquire semi-stable reduction at l over a tamely ramified extension.

Theorem 1.3. *For the primes $l = 2, 3$ or 5, there do not exist any non-zero abelian varieties over $\mathbb{Q}$ that have good reduction at every prime different from l and acquire semi-stable reduction at l over an extension of $\mathbb{Q}$ that is at most tamely ramified at l.*

This result is the best possible, because the Jacobian varieties $J(l)$ of the modular curves $X(l)$ have good reduction at all primes different from l and acquire semi-stable reduction at l over a tamely ramified extension [BW04, Corollary 4.4]. When $l \geqslant 7$, these are non-zero abelian varieties.

The curve $X(7)$ has genus three. Its Jacobian $J(7)$ is isogenous (over $\mathbb{Q}$) to a product of the Jacobian $J_0(49)$ of the modular curve $X_0(49)$ and a two-dimensional simple abelian variety B.

Received 15 June 2003, accepted in final form 14 April 2004, published online 21 June 2005.
2000 Mathematics Subject Classification 11G10, 14L15.
Keywords: abelian varieties, number fields, group schemes, semi-stable reduction.

The variety B is isogenous to $J_0(49) \times J_0(49)$ over the real subfield of the cyclotomic field $\mathbb{Q}(\zeta_7)$. Under the assumption of the Generalized Riemann Hypothesis for zeta functions of number fields, I can show [Sch03a] that any abelian variety over $\mathbb{Q}$ with good reduction outside 7 and acquiring semi-stable reduction over a tamely ramified extension at 7, is necessarily isogenous (over $\mathbb{Q}$) to a product of copies of the abelian varieties $J_0(49)$ and B. The proof follows the lines of the proof of Theorem 1.2.

Our results are consistent with conditional results obtained by Mestre [Mes86, § III]. Mestre's methods are analytic in nature. He assumes that the L-functions associated to abelian varieties over $\mathbb{Q}$ admit analytic continuations to $\mathbf{C}$ and he applies Weil's explicit formulas. Our results do not depend on any unproved hypotheses. In a recent paper [BK01] Brumer and Kramer prove Theorem 1.1 for primes $l \leqslant 7$. In this paper we take care of the prime 13. For the primes $l = 2, 3$ and 5 we prove the somewhat stronger Theorem 1.3. Our proof, like that of Brumer and Kramer, proceeds by studying, for a suitable small prime $p \neq l$, the p^n-torsion points $A[p^n]$ of abelian varieties A that have good reduction at every prime different from l and that either have semi-stable reduction at l or acquire it over a tamely ramified extension. The way in which the main result is obtained differs from Brumer and Kramer's method. Our method is closer to the approach taken by Fontaine in [Fon85]. When $l = 2, 3, 5, 7$ or 13 we show for every $n \geqslant 1$ that the group scheme $A[p^n]$ is an extension of a constant group scheme by a diagonalizable one. This leads to a contradiction when $\dim(A) > 0$.

For $l = 11$ things are more complicated. In this case there exist group schemes of p-power order that are not extensions of a constant group scheme by a diagonalizable one. Indeed, for $p = 2$, the 2-torsion subgroup scheme of $J_0(11)$ is an example of such an 'exotic' group scheme.

Finally we mention Calegari's work [Cal04]. Under the assumption of the Generalized Riemann Hypothesis, he determines all squarefree integers $n > 0$ for which there do not exist any non-zero abelian varieties over $\mathbb{Q}$ with good reduction at all primes not dividing n while the reduction at the primes dividing n is semi-stable. These turn out to be the squarefree integers n for which the genus of $X_0(n)$ is zero: $n = 1, 2, 3, 5, 6, 7, 10$ and 13.

For any pair of distinct primes p and l we introduce in § 2 two categories $\underline{C}$ and $\underline{D}$ of finite flat group schemes of p-power order over the ring $\mathbb{Z}[\frac{1}{l}]$. In terms of these we formulate in § 3 two simple criteria for Theorem 1.1 or 1.3 to hold. Each criterion has two parts. One involves the extensions of the group schemes μ_p by $\mathbb{Z}/p\mathbb{Z}$ over the ring $\mathbb{Z}[\frac{1}{l}]$. We determine these in § 4. The other is concerned with the simple objects in the categories $\underline{D}$ and $\underline{C}$, respectively. In §§ 5 and 6 we determine these for a very short list of pairs of primes (p, l). Theorems 1.1 and 1.3 then follow. We deal with the prime $l = 11$ in § 7. Here we prove Theorem 1.2. Section 8 contains a theorem concerning p-divisible groups that is essential for the proof.

2. Two categories of finite flat group schemes over $\mathbb{Z}[\frac{1}{l}]$

Let p and l be two distinct primes. By $\underline{Gr}$ we denote the category of finite flat commutative p-power order group schemes, or *p-group schemes* for short, over the ring $\mathbb{Z}[\frac{1}{l}]$. In this section we introduce two full subcategories of $\underline{Gr}$. In terms of these, in the next section, we formulate two criteria for Theorems 1.1 and 1.3 to hold.

Definition 2.1. Let p and l be two distinct primes.

(i) The category $\underline{C}$ is the full subcategory of $\underline{Gr}$ of group schemes G for which the inertia group of every prime over l acts tamely on the group of points $G(\overline{\mathbb{Q}})$.

(ii) The category $\underline{D}$ is the full subcategory of $\underline{Gr}$ of group schemes G for which we have that $(\sigma - \mathrm{id})^2 = 0$ on $G(\overline{\mathbb{Q}})$ for all σ in the inertia groups of any of the primes lying over l.

Since every group scheme G in the category $\underline{D}$ has p-power order, the relation $(\sigma - \mathrm{id})^2 = 0$ implies that $\sigma^{p^n} = \mathrm{id}$ for some $n \geqslant 0$. This implies that every inertia group acts through a finite p-group on $G(\overline{\mathbb{Q}})$. Since $p \neq l$, this action is tame and hence $\underline{D}$ is a full subcategory of $\underline{C}$:

$$\underline{D} \quad \subset \quad \underline{C} \quad \subset \quad \underline{Gr}.$$

We now exhibit several objects in the categories $\underline{C}$ and $\underline{D}$. The first example explains why we are interested in these two categories of group schemes.

2.1 By A. Grothendieck's semi-stable reduction Theorem [Gro71, Exp. IX, (3.5.3)], the subgroup schemes $A[p^n]$ of p^n-torsion points of semi-stable abelian varieties A over $\mathbb{Q}$ that have good reduction outside l are objects of $\underline{D}$ and hence of $\underline{C}$. More generally, the subgroup schemes $A[p^n]$ of abelian varieties A over $\mathbb{Q}$ that have good reduction outside l and acquire semi-stable reduction at l over some tamely ramified extension, are objects of $\underline{C}$ and need not be objects of $\underline{D}$.

2.2 Constant and diagonalizable group schemes of p-power order are objects of $\underline{D}$ and hence of $\underline{C}$. So are certain *twists* of these group schemes that are unramified outside l. Let V be a finite-dimensional vector space over $\mathbb{F}_p$. For any representation $\varrho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(V)$ we obtain a Galois module with underlying group V. If ϱ is unramified outside l and infinity, this module is the group of points of an étale group scheme $V(\varrho)$ over $\mathbb{Z}[\frac{1}{l}]$. If ϱ is at most tamely ramified at l, the group scheme $V(\varrho)$ is an object of $\underline{C}$. If $(\varrho(\sigma) - \mathrm{id})^2 = 0$ for every σ in an inertia group of any of the primes lying over l, then $V(\varrho)$ is even an object of $\underline{D}$.

For instance, taking $V = \mathbb{F}_p^{l-1}$ and $\varrho : \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \longrightarrow \mathrm{GL}(V)$ as the permutation representation, the group scheme $V(\varrho)$ is an object of $\underline{C}$. Its points generate the field $\mathbb{Q}(\zeta_l)$. Another example is given by $V = \mathbb{F}_p^2$ where ϱ is a homomorphism,

$$\varrho : \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \longrightarrow \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_p \right\} \quad \subset \quad \mathrm{GL}(V).$$

This time the group scheme $V(\varrho)$ is an object in $\underline{D}$, because $(\varrho(\sigma) - \mathrm{id})^2 = 0$ for every σ. For this twist to be non-trivial, it is necessary that $l \equiv 1 \pmod{p}$. Taking Cartier duals we obtain unramified twists of diagonalizable group schemes that are objects in $\underline{C}$ and $\underline{D}$, respectively.

2.3 Cartier duals $G^\vee$ of objects G in $\underline{D}$ are also in $\underline{D}$. Any closed flat subgroup scheme and any quotient by such a group scheme of an object in $\underline{D}$ is again in $\underline{D}$. The product of any two objects in $\underline{D}$ is again in $\underline{D}$. It follows from the definition of the Baer sum that if G_1 and G_2 are objects in $\underline{D}$, then the extension classes of G_1 by G_2 that are themselves objects of $\underline{D}$ make up a *subgroup* $\mathrm{Ext}^1_{\underline{D}}(G_1, G_2)$ of the group $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(G_1, G_2)$ of *all* extensions of G_1 by G_2 in the category $\underline{Gr}$.

All these remarks also hold for the category $\underline{C}$. However, an extension G of an object $G_1 \in \underline{C}$ by another object $G_2 \in \underline{C}$ is *automatically* an object of $\underline{C}$. In other words, we have $\mathrm{Ext}^1_{\underline{C}}(G_1, G_2) = \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(G_1, G_2)$. Indeed, there is some exponent e that is prime to l and has the property that, for all σ in an inertia group of any of the primes lying over l, the automorphism σ^e acts trivially on the points of G_1 and G_2. It follows that $(\sigma^e - \mathrm{id})^2 = 0$ on the points of G and hence that $\sigma^{ep^s} = \mathrm{id}$ for some $s \geqslant 0$. This implies that every inertia group acts through its tame quotient.

It is, in general, not true that $\mathrm{Ext}^1_{\underline{D}}(G_1, G_2) = \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(G_1, G_2)$. It is true, however, when the inertia groups of the primes over l act trivially on the points of G_1 and G_2. We have for instance that

$$\mathrm{Ext}^1_{\underline{D}}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Ext}^1_{\underline{C}}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}).$$

See § 7 for an example of two group schemes G_1, G_2 in the category $\underline{D}$ for which $\mathrm{Ext}^1_{\underline{D}}(G_1, G_2)$ is strictly smaller than $\mathrm{Ext}^1_{\underline{C}}(G_1, G_2) = \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(G_1, G_2)$.

2.4 Katz and Mazur construct in their book [KM85, Interlude 8.7], certain explicit extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p. These are objects in $\underline{D}$. We recall the construction in our situation. For any unit $\varepsilon \in \mathbb{Z}[\frac{1}{l}]^*$, Katz and Mazur define a finite flat p-group scheme G_ε over $\mathbb{Z}[\frac{1}{l}]$ of order p^2. It is killed by p and fits in an exact sequence

$$0 \longrightarrow \mu_p \longrightarrow G_\varepsilon \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

Two group schemes G_ε and $G_{\varepsilon'}$ are isomorphic if and only if $\varepsilon/\varepsilon' = u^p$ for some $u \in \mathbb{Z}[\frac{1}{l}]^*$. The points of G_ε generate the number field $\mathbb{Q}(\zeta_p, \sqrt[p]{\varepsilon})$. For $p = 2$ and $\varepsilon = -1$, we recover the group scheme D in [Maz76, Proposition 4.2].

3. Two criteria

In this section we formulate criteria for Theorems 1.1 and 1.3 to hold. Let l and p be two distinct primes. A *simple* object in any of the categories $\underline{Gr}$, $\underline{C}$ or $\underline{D}$ of the previous section is an object in that category that does not admit any non-trivial closed flat subgroup schemes.

PROPOSITION 3.1. *Let l be a prime and suppose there exists a prime $p \neq l$ for which:*

- *the only simple objects in the category $\underline{D}$ are the group schemes $\mathbb{Z}/p\mathbb{Z}$ and μ_p;*
- *we have $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = 0$.*

Then there do not exist any non-zero abelian varieties over $\mathbb{Q}$ that have good reduction at every prime different from l and have semi-stable reduction at l.

Proof. The proof is very similar to that in [Fon85, § 3.4.3]. We briefly sketch it. Let A be a g-dimensional abelian variety over $\mathbb{Q}$ that has good reduction at every prime different from l and has semi-stable reduction at l. Let $n \geqslant 1$ and consider the closed subgroup scheme $A[p^n]$ of p^n-torsion points over $\mathbb{Z}[\frac{1}{l}]$. This is an object of the category $\underline{D}$. We filter $A[p^n]$ with flat closed subgroup schemes and successive *simple* subquotients. The simple steps are by assumption isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and μ_p. By the second assumption, any extension

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow G \longrightarrow \mu_p \longrightarrow 0$$

splits over $\mathbb{Z}[\frac{1}{l}]$. Therefore, we can modify the filtration of $A[p^n]$ and obtain for every $n \geqslant 1$ an exact sequence of finite flat $\mathbb{Z}[\frac{1}{l}]$-group schemes

$$0 \longrightarrow M_n \longrightarrow A[p^n] \longrightarrow C_n \longrightarrow 0$$

with M_n an extension of group schemes isomorphic to μ_p and C_n an extension of copies of $\mathbb{Z}/p\mathbb{Z}$. It follows that C_n is étale and that the fundamental group of $\mathbb{Z}[\frac{1}{l}]$ acts on its points through a finite p-group P. Since the maximal abelian p-extension of $\mathbb{Q}$ that is unramified outside $l \cdot \infty$ is contained in the cyclic extension $\mathbb{Q}(\zeta_l)$, the group P/P' is cyclic. This implies that P itself is cyclic and hence that the fundamental group acts through the Galois group of $\mathbb{Q}(\zeta_l)$ over $\mathbb{Q}$. It follows that C_n becomes *constant* over the ring $\mathbb{Z}[\frac{1}{l}, \zeta_l]$. Similarly, it follows from Cartier duality that M_n becomes diagonalizable over this ring.

Pick a non-zero prime $\mathfrak{p}$ of $\mathbb{Z}[\frac{1}{l}, \zeta_l]$ and let $k_\mathfrak{p}$ denote its residue field. The abelian variety A/M_n has at least $\#C_n$ rational points over $k_\mathfrak{p}$. Since A is isogenous to A/M_n, it has the same number of points over $k_\mathfrak{p}$ as A/M_n. This implies that $\#A(k_\mathfrak{p}) \geqslant \#C_n$. Taking Cartier duals of the exact sequence above, we see that the abelian variety $A^{\mathrm{dual}}/C_n^\vee$ has at least $\#M_n^\vee$ points over $k_\mathfrak{p}$. Since A is

isogenous to $A^{\mathrm{dual}}/C_n^\vee$, we see that $\#A(k_\mathfrak{p}) \geqslant \#M_n^\vee = \#M_n$. It follows that $\#A(k_\mathfrak{p})^2$ is at least the product of the orders of M_n and C_n, which is equal to $\#A[p^n] = p^{2ng}$. This leads to a contradiction when $n \to \infty$ unless $g = 0$. This proves the proposition. □

PROPOSITION 3.2. *Let l be a prime and suppose that there exists a prime $p \neq l$ for which:*

- *the only simple objects in the category $\underline{C}$ are the group schemes $\mathbb{Z}/p\mathbb{Z}$ and μ_p;*
- *we have $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = 0$.*

Then there do not exist any non-zero abelian varieties over $\mathbb{Q}$ that have good reduction at every prime different from l and acquire semi-stable reduction at l over a tamely ramified extension.

Proof. This time the group scheme $A[p^n]$ is an object of the category $\underline{C}$. Up to replacing the category $\underline{D}$ by $\underline{C}$, the proof is *identical* to the proof of Proposition 3.1. □

4. Extensions of μ_p by $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Z}[\frac{1}{l}]$

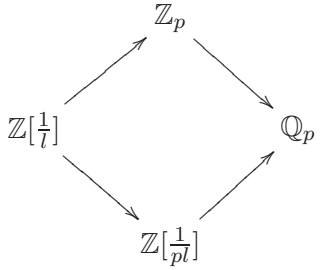
The criteria of the previous section involve the group $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ of extensions of the group scheme μ_p by $\mathbb{Z}/p\mathbb{Z}$ over the ring $\mathbb{Z}[\frac{1}{l}]$. In this section we determine this group for any pair of distinct primes p and l. For $p = 2$ see also [Maz76, Proposition 5.1].

For any prime p, let ζ_p denote a primitive pth root of unity and let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let $\omega : \Delta \longrightarrow \mathbb{F}_p^*$ denote the cyclotomic (or Teichmüller) character defined by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$ for every $\sigma \in \Delta$. By M_{ω^i} we denote the ω^i-eigenspace of an $\mathbb{F}_p[\Delta]$-module M.

PROPOSITION 4.1. *Let l and p be distinct primes. Then there is a natural exact sequence*

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \longrightarrow (\mathbb{Z}[\tfrac{1}{pl}, \zeta_p]^*/(\mathbb{Z}[\tfrac{1}{pl}, \zeta_p]^*)^p)_{\omega^2} \longrightarrow (\mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p)_{\omega^2}.$$

Proof. We work with the following base rings.



Since the group scheme μ_p is connected, while $\mathbb{Z}/p\mathbb{Z}$ is étale, the group $\mathrm{Hom}_{\mathbb{Z}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ vanishes. Therefore $\mathrm{Hom}_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is zero as well. The natural homomorphism $\mathrm{Hom}_{\mathbb{Z}[\frac{1}{p}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Q}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is an isomorphism. More precisely, both groups are zero when p is odd, while they both have order two when $p = 2$. Finally, the group $\mathrm{Ext}^1_{\mathbb{Z}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is trivial because any extension of μ_p by $\mathbb{Z}/p\mathbb{Z}$ over the ring of p-adic integers $\mathbb{Z}_p$ is split by the connected component.

Therefore, the Mayer–Vietoris exact sequence of [Sch03b, Proposition 2.4] provides us with the exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{pl}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{Ext}^1_{\mathbb{Q}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z}).$$

Since the group schemes μ_p and $\mathbb{Z}/p\mathbb{Z}$ are étale over the rings $\mathbb{Z}[\frac{1}{pl}]$ and $\mathbb{Q}_p$, this sequence gives a description of the group $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ in terms of groups of extensions of Galois modules.

Next we adjoin the pth roots of unity to the rings $\mathbb{Z}[\frac{1}{pl}]$ and $\mathbb{Q}_p$. The Galois group Δ, introduced above, acts naturally on the group $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ of extensions of μ_p by $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Q}(\zeta_p)$. Since Δ has order prime to p, the extensions that are defined over $\mathbb{Q}_p$ correspond precisely to the Δ-invariant elements of $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.

Since $\mathbb{Q}_p(\zeta_p)$ contains ζ_p, the Galois modules μ_p and $\mathbb{Z}/p\mathbb{Z}$ are isomorphic! This implies that $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ and $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ are also isomorphic. However, under this isomorphism the Δ-invariant extensions of μ_p by $\mathbb{Z}/p\mathbb{Z}$ correspond to the extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p that are contained in the ω^2-eigenspace of $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$. Exactly the same occurs for the extension groups over the ring $\mathbb{Z}[\frac{1}{pl}, \zeta_p]$ and its subring of Δ-invariants $\mathbb{Z}[\frac{1}{pl}]$. These considerations lead to the exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{pl}, \zeta_p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p)_{\omega^2} \longrightarrow \mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)_{\omega^2}.$$

We express the rightmost extension group in terms of Galois cohomology. In order to do this we apply the functor $\mathrm{Hom}_{\mathbb{Q}_p(\zeta_p)}(-, \mu_p)$ to the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$ and compute the long exact sequence of Ext-groups. Proceeding in the same way with the extension group in the middle, we obtain the following diagram of $\mathbb{F}_p[\Delta]$-modules.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mu_p & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{pl}, \zeta_p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p) & \longrightarrow & H^1(G_{\mathbb{Z}[\frac{1}{pl}, \zeta_p]}, \mu_p) & \longrightarrow & 0 \\
 & & \| & & \downarrow & & & & \\
0 & \longrightarrow & \mu_p & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p) & \longrightarrow & H^1(G_{\mathbb{Q}_p(\zeta_p)}, \mu_p) & \longrightarrow & 0
\end{array}$$

The rows of this diagram are exact, and $G_{\mathbb{Q}_p(\zeta_p)}$ denotes the absolute Galois group of $\mathbb{Q}_p(\zeta_p)$ and $G_{\mathbb{Z}[\frac{1}{pl}, \zeta_p]}$ is the fundamental group of $\mathbb{Z}[\frac{1}{pl}, \zeta_p]$. By the Snake Lemma there is an exact sequence of $\mathbb{F}_p[\Delta]$-modules,

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(G_{\mathbb{Z}[\frac{1}{pl}, \zeta_p]}, \mu_p)_{\omega^2} \longrightarrow H^1(G_{\mathbb{Q}_p(\zeta_p)}, \mu_p)_{\omega^2}.$$

The Kummer sequences over the rings $\mathbb{Z}[\frac{1}{pl}, \zeta_p]$ and $\mathbb{Q}_p(\zeta_p)$ give rise to the following commutative diagram of $\mathbb{F}_p[\Delta]$-modules with exact rows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}[\frac{1}{pl}, \zeta_p]^*/(\mathbb{Z}[\frac{1}{pl}, \zeta_p]^*)^p & \longrightarrow & H^1(G_{\mathbb{Z}[\frac{1}{pl}, \zeta_p]}, \mu_p) & \longrightarrow & Cl(\mathbb{Z}[\frac{1}{pl}, \zeta_p])[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p & \xrightarrow{\cong} & H^1(G_{\mathbb{Q}_p(\zeta_p)}, \mu_p) & & & &
\end{array}$$

Here $Cl(\mathbb{Z}[\frac{1}{pl}, \zeta_p])$ denotes the ideal class group of the ring $\mathbb{Z}[\frac{1}{pl}, \zeta_p])$. It is naturally isomorphic to the ideal class group of $\mathbb{Z}[\zeta_p]$ modulo the ideal classes supported in the primes lying over l. We take ω^2-eigenspaces. By Herbrand's Theorem [Was82, Theorem 6.17], the ω^2-eigenspace of the p-part of the class group of the ring $\mathbb{Z}[\zeta_p]$ vanishes. This implies that the ω^2-eigenspace of $Cl(\mathbb{Z}[\frac{1}{pl}, \zeta_p])$ is also trivial. A second application of the Snake Lemma then leads to the required exact sequence. □

COROLLARY 4.2. *Let l and p be distinct primes. We have that*

$$\dim_{\mathbb{F}_p} \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} 1, & \text{if } (l^2-1)/24 \equiv 0 \pmod{p}; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Note that $(l^2-1)/24$ is p-integral since $p \neq l$. The condition $(l^2-1)/24 \equiv 0 \pmod{p}$ is just a compact way of saying that $l \equiv \pm 1 \pmod{p}$ when $p \geqslant 5$, that $l \equiv \pm 1 \pmod{9}$ when $p = 3$ and that $l \equiv \pm 1 \pmod{8}$ when $p = 2$.

When $p = 2$, the group Δ is trivial and $\omega = 1$. The middle and rightmost groups in the exact sequence of Proposition 4.1 are each of dimension three over $\mathbb{F}_2$. The middle one is generated by 2, -1 and l while the rightmost group is generated by 2, -1 and 5. This implies that the extension group on the left is cyclic of order two when $\pm l$ is a 2-adic square, i.e. when $l \equiv \pm 1 \pmod 8$, while it is trivial otherwise.

When $p = 3$, the group Δ has order two, so that $\omega^2 = 1$ and the ω^2-eigenspace is simply the group of Δ-invariants. The middle and rightmost groups in the exact sequence of Proposition 4.1. are each of dimension two over $\mathbb{F}_3$. The middle one is generated by 3 and l, while the rightmost one is generated by 3 and the unit 4. This implies that the group $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_3, \mathbb{Z}/3\mathbb{Z})$ is a one-dimensional $\mathbb{F}_3$-vector space when l is a 3-adic cube, i.e. when $l \equiv \pm 1 \pmod 9$, while it is zero otherwise.

When $p \geqslant 5$, we first compute the group in the middle of the exact sequence of Proposition 4.1. Consider the natural exact sequence

$$0 \longrightarrow \mathbb{Z}[\tfrac{1}{p}, \zeta_p]^* \longrightarrow \mathbb{Z}[\tfrac{1}{pl}, \zeta_p]^* \xrightarrow{v} \bigoplus_{\mathfrak{l}|l} \mathbb{Z} \longrightarrow Cl(\mathbb{Z}[\tfrac{1}{p}, \zeta_p]) \longrightarrow Cl(\mathbb{Z}[\tfrac{1}{pl}, \zeta_p]) \longrightarrow 0.$$

Here v is the map that sends a unit $\varepsilon \in \mathbb{Z}[\frac{1}{pl}, \zeta_p]^*$ to its valuations at the primes $\mathfrak{l}$ of $\mathbb{Z}[\zeta_p]$ that lie over l. We tensor with $\mathbb{Z}_p$ and take ω^2-eigenspaces. By Herbrand's Theorem, the ω^2-eigenspace of the p-part of the class group of $\mathbb{Z}[\frac{1}{p}, \zeta_p]$ is trivial. Therefore, we obtain a three-term exact sequence. It is $\mathbb{Z}_p$-split, because the rightmost term is free over $\mathbb{Z}_p$. Taking quotients by pth powers, we obtain therefore the following exact sequence of ω^2-eigenspaces,

$$0 \longrightarrow (\mathbb{Z}[\tfrac{1}{p}, \zeta_p]^*/(\mathbb{Z}[\tfrac{1}{p}, \zeta_p]^*)^p)_{\omega^2} \longrightarrow (\mathbb{Z}[\tfrac{1}{pl}, \zeta_p]^*/(\mathbb{Z}[\tfrac{1}{pl}, \zeta_p]^*)^p)_{\omega^2} \xrightarrow{v} \left(\bigoplus_{\mathfrak{l}|l} \mathbb{F}_p\right)_{\omega^2} \longrightarrow 0.$$

We identify the Galois group Δ with $\mathbb{F}_p^*$ via the cyclotomic character ω. By [Was82, Proposition 8.13] the $\mathbb{F}_p[\Delta]$-module $\mathbb{Z}[\frac{1}{p}, \zeta_p]^*/(\mathbb{Z}[\frac{1}{p}, \zeta_p]^*)^p$ is isomorphic to $\mu_p \times \mathbb{F}_p[\Delta/\langle -1\rangle]$. So, its ω^2-eigenspace has $\mathbb{F}_p$-dimension one. The module $\bigoplus_{\mathfrak{l}|l} \mathbb{F}_p$ is a permutation module isomorphic to $\mathbb{F}_p[\Delta/\langle l\rangle]$. Its χ-eigenspaces are trivial for the characters χ of Δ for which $\chi(l) \neq 1$. They have dimension one if $\chi(l) = 1$. Since ω generates the group of characters, the ω^2-eigenspace is one-dimensional precisely when $l \equiv \pm 1 \pmod p$. This shows that the group in the middle of the exact sequence has dimension two or one over $\mathbb{F}_p$ depending on whether $l \equiv \pm 1 \pmod p$ or not.

Since $p \geqslant 5$, the ω^2-eigenspace of $\mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p$ has dimension one. This follows from a short computation. By [Was82, Theorem 8.25], the ω^2-eigenspace of the cyclotomic units in $\mathbb{Z}[\frac{1}{p}, \zeta_p]^*$ maps surjectively onto it. It follows that the rightmost arrow in the exact sequence of Proposition 4.1 is surjective and hence that $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{l}]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ has $\mathbb{F}_p$-dimension one or zero depending on whether $l \equiv \pm 1 \pmod p$ or not. This proves the proposition. □

5. Simple objects in the categories $\underline{C}$ and $\underline{D}$

Let l and p be distinct primes. In § 2 we introduced the categories $\underline{C}$ and $\underline{D}$ of p-group schemes over $\mathbb{Z}[\frac{1}{l}]$. In this section we give two criteria for the group schemes $\mathbb{Z}/p\mathbb{Z}$ and μ_p to be the only *simple* objects in $\underline{C}$ or $\underline{D}$. For any prime q, the q-adic valuation v_q is normalized by putting $v_q(q) = 1$.

PROPOSITION 5.1. *Let l and p be distinct primes. When p divides $l-1$, we let F denote the degree p subfield F of $\mathbb{Q}(\zeta_l)$. When not, we put $F = \mathbb{Q}$. Suppose that any Galois extension L of $\mathbb{Q}$ for which each of the following three conditions hold:*

- *the field $F(\zeta_{2p}, \sqrt[p]{l})$ is contained in L,*
- *the extension $F(\zeta_{2p}, \sqrt[p]{l}) \subset L$ is unramified at all primes not lying over p,*
- *the p-adic valuation of the root discriminant δ_L of L is strictly smaller than $1 + [1/(p-1)]$,*

has the property that the degree $[L : \mathbb{Q}(\zeta_p)]$ *is a power of* p*. Then the only* simple *objects in the category* $\underline{D}$ *are the group schemes* $\mathbb{Z}/p\mathbb{Z}$ *and* μ_p*.*

Proof. Let G be a simple object of $\underline{D}$. When $p = 2$, we put $G' = G \times G_l \times G_{-1}$. Here G_l and G_{-1} denote the Katz–Mazur group schemes of § 2 associated to the units $\varepsilon = l$ and -1, respectively. When $p \neq 2$ we put $G' = G \times G_l \times V(\varrho)$. Here $V(\varrho)$ is the twisted constant group scheme introduced in § 2 with $V = \mathbb{F}_p^2$ and

$$\varrho : \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \longrightarrow \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_p \right\} \quad \subset \quad \mathrm{GL}(V)$$

is any non-trivial representation when $l \equiv 1 \pmod{p}$, but is trivial otherwise. The points of $V(\varrho)$ generate the field F. Let L be the extension of $\mathbb{Q}$ generated by the points of G'. It is a Galois extension of $\mathbb{Q}$ that is unramified outside pl and ∞. By construction, the first condition of the proposition is satisfied.

Since the group scheme G' is a product of objects in $\underline{D}$, it is itself an object in $\underline{D}$. Therefore, we know that $(\sigma - \mathrm{id})^2 = 0$ on $G'(\overline{\mathbb{Q}})$ for every σ in the inertia subgroup $I_\mathfrak{l}$ of any of the primes $\mathfrak{l}$ over l. Since G is simple, it is killed by p. Therefore, G' is also killed by p and we have that $\sigma^p = \mathrm{id}$ on $G'(\overline{\mathbb{Q}})$. Since tame ramification groups are cyclic, it follows that the ramification indices of the primes over l divide p. Since the ramification indices of the primes over l in the subfield $F(\zeta_{2p}, \sqrt[p]{l})$ are actually *equal* to p, the field L must be unramified over $F(\zeta_{2p}, \sqrt[p]{l})$ at the primes lying over l. Therefore, the second condition is satisfied. The estimates of Abraškin [Abr87] and Fontaine [Fon85] for the ramification at the prime p imply that the third condition is satisfied. Therefore, $[L : \mathbb{Q}(\zeta_p)]$ is a power of p.

The subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_p))$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the group of points $G(\overline{\mathbb{Q}})$ through the finite p-group $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$. Since $G(\overline{\mathbb{Q}})$ is a simple Galois module of p-power order, it is fixed by the p-group $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$. Therefore, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $G(\overline{\mathbb{Q}})$ through the group $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ of order $p - 1$. The group $G(\overline{\mathbb{Q}})$ is a product of eigenspaces. Since G is simple and since the $(p-1)$th roots of unity are in $\mathbb{F}_p$, the group $G(\overline{\mathbb{Q}})$ is itself equal to one of the eigenspaces and has dimension one over $\mathbb{F}_p$. It follows that G has order p. Since p is prime in the ring $\mathbb{Z}[\frac{1}{l}]$, the classification of Tate and Oort [TO70] implies that $G \cong \mathbb{Z}/p\mathbb{Z}$ or μ_p possibly twisted by a character χ that is unramified outside $l\infty$. Such a character necessarily has order dividing $p-1$. However, since G is an object of $\underline{D}$, the ramification index at l of the field cut out by χ must be a power of p. Therefore, χ is a character of $\mathbb{Q}$ that is only ramified at ∞. This implies that it is trivial. This proves the proposition. □

The following proposition is a variant of Proposition 5.1. Although the conditions have the appearance of being similar to those of Proposition 5.1, they are actually much stronger. In the course of the proof we will see that they imply that either l or p is equal to 2. In § 6 we apply Proposition 5.2 only to the pairs $(l, p) = (2, 3)$, $(3, 2)$ and $(5, 2)$.

PROPOSITION 5.2. *Let* l *and* p *be distinct primes. Suppose that any Galois extension* L *of* $\mathbb{Q}$ *for which the following four conditions hold:*

- *the field* L *is unramified outside* pl *and* ∞*,*
- *the field* $\mathbb{Q}(\zeta_{2p}, \zeta_l, \sqrt[p]{l})$ *is contained in* L*,*
- *the* l*-adic valuation of the root discriminant* δ_L *of* L *is strictly smaller than* 1*,*
- *the* p*-adic valuation of* δ_L *of* L *is strictly smaller than* $1 + [1/(p-1)]$*,*

has the property that the degree $[L : \mathbb{Q}(\zeta_p)]$ *is power of* p*. Then the only* simple *objects in the category* $\underline{C}$ *are the group schemes* $\mathbb{Z}/p\mathbb{Z}$ *and* μ_p*.*

Proof. Let G be a simple object of $\underline{C}$. As a first approximation, let G' be as in the proof of Proposition 5.1, but then multiply G' by the étale group scheme corresponding to the Galois module $V = (\mathbb{F}_p)^{l-1}$ twisted by the permutation representation $\varrho : \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \longrightarrow \mathrm{GL}(V)$. The points of $V(\varrho)$ generate the field $\mathbb{Q}(\zeta_l)$. The group scheme G' is an object of $\underline{C}$ that is killed by p.

Since G' is a finite flat p-group scheme over $\mathbb{Z}[\frac{1}{l}]$, the field L generated by the points of G' satisfies the first condition. By construction it satisfies the second condition. The third condition is satisfied because the inertia groups $I_\mathfrak{l}$ of the primes $\mathfrak{l}$ over l act tamely on the points of G', so that the l-adic contribution to the root discriminant of L is of the form $l^{(e-1)/e}$, where e is the ramification index e of any of the primes over l. The fourth condition is verified by the theorem of Abraškina and Fontaine. Since the four conditions are satisfied, the degree $[L : \mathbb{Q}(\zeta_p)]$ must be a power of p. Arguing as in the proof of the previous proposition, one shows that any simple object of the category $\underline{C}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or μ_p possibly twisted by a character χ that is unramified outside $l\infty$. The order of such a character necessarily divides $l-1 = [\mathbb{Q}(\zeta_l) : \mathbb{Q}]$ as well as $p-1 = \#\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$. Since $\zeta_l \in L$, the degree $l-1 = [\mathbb{Q}(\zeta_p, \zeta_l) : \mathbb{Q}(\zeta_p)]$ is a power of p. It follows that $\gcd(l-1, p-1) = 1$, so that there are no non-trivial twists of $\mathbb{Z}/p\mathbb{Z}$ or μ_p by characters that are unramified outside $l\infty$. More precisely, we have that either $l = 2$ or that $p = 2$ and l is a Fermat prime.

This proves the proposition. □

6. Odlyzko bounds and class field theory

In this section we prove Theorems 1.1 and 1.3. We first deal with Theorem 1.3.

Proof of Theorem 1.3. It suffices to check the two conditions of Proposition 3.2. For each of the pairs of primes $(l, p) = (2, 3)$, $(3, 2)$ and $(5, 2)$ we have that $(l^2 - 1)/24 \not\equiv 0 \pmod{p}$ and Corollary 4.2 implies that all extensions of μ_p by $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Z}[\frac{1}{l}]$ are trivial. Therefore, one of the conditions is satisfied. It remains to show that the other condition is satisfied as well: the only simple objects in the category $\underline{C}$ are $\mathbb{Z}/p\mathbb{Z}$ and μ_p. We do this by checking, case by case, that the conditions of Proposition 5.2 are satisfied.

We recall that the *root discriminant* of a number field K of degree n is the nth root of the absolute value of its discriminant. The first, third and fourth properties of the number field L that occurs in Proposition 5.2 imply that the root discriminant δ_L satisfies

$$\delta_L < l p^{1+[1/(p-1)]}.$$

Indeed, since the primes of L that lie over l are at most tamely ramified, the l-adic contribution to the root discriminant of L is of the form $l^{(e-1)/e} < l$ where e is the ramification index e of any of the primes over l.

We proceed case by case.

Case $l = 2$, $p = 3$. The root discriminant δ_L of the field L of Proposition 5.2 satisfies $\delta_L < 2 \cdot 3^{3/2} = 10.49\ldots$. Odlyzko's bounds [Mar81, p. 187] or [Odl76] imply that $[L : \mathbb{Q}] < 24$. Therefore, the degree of L over $K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is at most three. Since the prime over 2 is *tamely* ramified, if $[L : K]$ were 2, the extension $K \subset L$ would be unramified at 2 and hence unramified outside 3. However, the class number of K is 1 and the multiplicative group $\mathbb{F}_3^*$ of the residue field of the unique prime over 3 is generated by the global unit -1. Therefore, class field theory implies that the field K does not admit any quadratic extension that is unramified outside 3.

This proves that $[L : \mathbb{Q}(\zeta_3)]$ is a power of 3 as required.

Case $l = 3$, $p = 2$. The root discriminant δ_L of the field L of Proposition 5.2 satisfies $\delta_L < 3 \cdot 2^2 = 12$. Odlyzko's bounds imply that $[L : \mathbb{Q}] < 32$. Therefore, the degree of L over $\mathbb{Q}(i, \sqrt{-3}) = \mathbb{Q}(\zeta_{12})$ is

at most 7. Let $\pi = \mathrm{Gal}(L/\mathbb{Q})$. Since the 2-adic valuation of the root discriminant of $\mathbb{Q}(\zeta_{24})$ is not strictly smaller than 2, the fourth condition of Proposition 5.2 implies that the field $\mathbb{Q}(\zeta_{12})$ is the largest abelian extension of $\mathbb{Q}$ inside L. It is the fixed field of the commutator subgroup π' of π. Since its class number is 1 (see [Was82, Ch. 11]), the field $\mathbb{Q}(\zeta_{12})$ admits no non-trivial everywhere unramified extension inside L. In addition, ζ_3 generates the multiplicative group $\mathbb{F}_4^*$ of the residue field of the unique prime over 2 and the multiplicative group $\mathbb{F}_9^*$ of the residue field of the unique prime over 3 is a 2-group. Since the prime over 3 is at most tamely ramified in L, it follows from class field theory that $\mathbb{Q}(\zeta_{12})$ admits no non-trivial odd degree abelian extensions inside L. Therefore, π'/π'' is a 2-group.

We conclude the proof by showing that π'' is trivial. We have $\#\pi' \leqslant 7$. Therefore, we are done when $[\pi' : \pi''] = 1$ or 4. When $[\pi' : \pi''] = 2$, the group π'' has order at most three and is cyclic. Therefore, $\mathrm{Aut}(\pi'')$ is abelian and π' is in the kernel of the homomorphism $\pi \longrightarrow \mathrm{Aut}(\pi'')$ induced by conjugation. This implies that π'' is contained in the center of π'. Since π'/π'' is cyclic, this implies that π' is abelian and hence that π'' is trivial, as required.

Case $l = 5$, $p = 2$. Let $\pi = \mathrm{Gal}(L/\mathbb{Q})$. The root discriminant δ_L of the field L of Proposition 5.2 satisfies $\delta_L < 5 \cdot 2^2 = 20$. Odlyzko's bounds imply that $[L : \mathbb{Q}] < 480$ so that the degree of L over $\mathbb{Q}(i, \zeta_5) = \mathbb{Q}(\zeta_{20})$ is less than 60. This implies that $\pi = \mathrm{Gal}(L/\mathbb{Q})$ is a *solvable* group. Since the 2-adic valuation of the root discriminant of $\mathbb{Q}(\zeta_{40})$ is not strictly smaller than 2, the fourth condition of Proposition 5.2 implies that the field $\mathbb{Q}(\zeta_{20})$ is the largest abelian extension of $\mathbb{Q}$ inside L. It is the fixed field of π'. Next we study the maximal abelian extension K of $\mathbb{Q}(\zeta_{20})$ inside L. This is the fixed field of π''.

Step 1. *The field K is contained in the ray class field $F_{2(1-\zeta_5)}$ of $\mathbb{Q}(\zeta_{20})$ of conductor $2(1-\zeta_5)$.*

Proof. By [Was82, Ch. 11] the class number of $\mathbb{Q}(\zeta_{20})$ is 1, the multiplicative group $\mathbb{F}_{16}^*$ of the residue field of the unique prime over 2 is generated by the global unit $1-\zeta_{20}$ and the multiplicative groups of the residue fields of the two primes over 5 both have order four. By class field theory the field $\mathbb{Q}(\zeta_{20})$ admits, therefore, no non-trivial odd degree abelian extensions inside L. It follows that the group $\pi'/\pi'' = \mathrm{Gal}(K/\mathbb{Q}(\zeta_{20}))$ and all its characters have 2-power order. By the first condition of Proposition 5.2, the conductors of the characters divide $(1-\zeta_5)(1-i)^a$ for some $a \geqslant 0$. Since the 2-adic valuation of δ_L is strictly smaller than 2, it follows from the conductor discriminant formula that $a \leqslant 3$. Since the multiplicative group $(\mathbb{Z}[\zeta_{20}]/(1-\zeta_5))^* \cong \mathbb{F}_5^* \times \mathbb{F}_5^*$ is generated by the units ζ_{20} and $1-\zeta_{20}$, the ray class field of $\mathbb{Q}(\zeta_{20})$ of conductor $(1-\zeta_5)$ is equal to $\mathbb{Q}(\zeta_{20})$ and there are no characters of conductor $(1-\zeta_5)$. Since the primes over 2 are wildly ramified, this implies that $a \geqslant 2$.

Suppose that χ is a character of $\mathrm{Gal}(K/\mathbb{Q}(\zeta_{20}))$ of conductor $(1-\zeta_5)(1-i)^3$ or $(1-i)^3$. Then χ has order four. Since χ^2 has conductor divisible by $(1-i)^2$, the conductor discriminant formula implies that the 2-adic valuation of the root discriminant of the field cut out by χ is at least 2. This is impossible by the fourth condition. Therefore, $a = 2$ and K is contained in $F_{2(1-\zeta_5)}$ as required. □

Step 2. *The ray class field $F_{2(1-\zeta_5)}$ is a biquadratic extension of $\mathbb{Q}(\zeta_{20})$. Its root discriminant is equal to $5^{7/8}2^{7/4}$.*

Proof. We already saw in Step 1 that the ray class field of $\mathbb{Q}(\zeta_{20})$ of conductor $1-\zeta_5$ is equal to $\mathbb{Q}(\zeta_{20})$ itself. The unit group of $\mathbb{Z}[\zeta_{20}]$ is generated by ζ_{20} and by $1-\zeta_{20}^a$ for $a \in (\mathbb{Z}/20\mathbb{Z})^*$. They generate a subgroup of $(\mathbb{Z}[\zeta_{20}]/(2))^*$ of index 2. This implies that the ray class field F_2 of $\mathbb{Q}(\zeta_{20})$ of conductor 2 has degree two. It is not difficult to see that one has $F_2 = \mathbb{Q}(\zeta_{20}, \sqrt{\eta})$ where $\eta = (1+\sqrt{5})/2$. Similarly, one shows that $(\mathbb{Z}[\zeta_{20}]/(2(1-\zeta_5)))^*$ modulo the image of the unit group $\mathbb{Z}[\zeta_{20}]^*$ is a group of type 2×2. It follows that the ray class field $F_{2(1-\zeta_5)}$ of conductor $2(1-\zeta_5)$ is a

biquadratic extension of $\mathbb{Q}(\zeta_{20})$. Since the three quadratic characters have conductors 2, $2(1-\zeta_5)$ and $2(1-\zeta_5)$, respectively, the root discriminant of $F_{2(1-\zeta_5)}$ is equal to $5^{7/8}2^{7/4} = 13.75\ldots$ as required. □

STEP 3. *The group π''/π''' is a 2-group.*

Proof. The Odlyzko bounds imply that the absolute degree of the Hilbert class field of $F_{2(1-\zeta_5)}$ is at most 46. Since $F_{2(1-\zeta_5)}$ has degree 32 over $\mathbb{Q}$, the field $F_{2(1-\zeta_5)}$ admits no everywhere unramified extension inside L. Since the prime over 2 is totally ramified in $F_{2(1-\zeta_5)}$, the same is true for the three quadratic extensions of $\mathbb{Q}(\zeta_{20})$ contained in $F_{2(1-\zeta_5)}$. Since $F_2 = \mathbb{Q}(\zeta_{20}, \sqrt{\eta})$ where $\eta = (1+\sqrt{5})/2$, the prime over 5 is inert in the subfield F_2. It follows that the residue fields of the primes in F_2 lying over 2 and 5 are isomorphic to $\mathbb{F}_{16}$, $\mathbb{F}_{25}$ and $\mathbb{F}_{25}$, respectively. The same is true for $F_{2(1-\zeta_5)}$. A computation shows that the units $1-\zeta_{20}$ and $i \pm \sqrt{\eta}$ of the field F_2 together with their conjugates generate a subgroup of the multiplicative group $\mathbb{F}_{16}^* \times \mathbb{F}_{25}^* \times \mathbb{F}_{25}^*$ of index a power of 2. Therefore, by class field theory neither $F_{2(1-\zeta_5)}$ nor any of the three quadratic extensions of $\mathbb{Q}(\zeta_{20})$ contained in it, admit an odd degree extension inside L. We conclude that π''/π''' is a 2-group as required. □

STEP 4. *The group π''' is trivial.*

Proof. By Step 2, the index $[\pi' : \pi'']$ divides 4. When π'/π'' is trivial, we are done. If it has order two, then the order of π''/π''' is odd by the Burnside basis theorem. It follows from Step 3 that π''/π''' is trivial. This implies that π'' is trivial and we are done. When π'/π'' has order four, it is of type 2×2 and the order of π'' is at most 14. By Step 3 and Taussky's theorem [Tau37], the group π''/π''' is a *cyclic* 2-group. If it is trivial we are done. If not, then $\#(\pi'''/\pi'''')$ is odd and at most 7. It follows that π'''/π'''' is cyclic and hence has an abelian automorphism group. Therefore, π'' is in the kernel of the homomorphism $\pi' \longrightarrow \mathrm{Aut}(\pi'''/\pi'''')$ that is induced by conjugation. It follows that π'''/π'''' is contained in the center of π''/π'''', so that π''/π'''' modulo its center is cyclic. This implies that π''/π'''' is abelian and hence that π''' is trivial, as required. □

This completes the proof of Theorem 1.3. □

Next we prove Theorem 1.1.

Proof of Theorem 1.1. The primes $l = 2, 3$ and 5 are taken care of by the stronger Theorem 1.3. We deal with the primes 7 and 13 by checking the conditions of Proposition 5.1 for the pairs $(l,p) = (7,3)$ and $(13,2)$. Since in each case we have that $(l^2-1)/24 \not\equiv 0 \pmod{p}$, Corollary 4.2 implies that all extensions of μ_p by $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Z}[\frac{1}{l}]$ are trivial. It remains to show that the other condition is verified as well: the only simple objects in the category $\underline{C}$ are $\mathbb{Z}/p\mathbb{Z}$ and μ_p. We do this by checking in both cases that the conditions of Proposition 5.1 are satisfied.

The three conditions of Proposition 5.1 imply that the number field L that occurs there has the property that the ramification index of any of the primes over l in L is at most p and that the root discriminant δ_L satisfies

$$\delta_L < l^{1-(1/p)} p^{1+[1/(p-1)]}.$$

We show that the field L is necessarily of p-power degree over $\mathbb{Q}(\zeta_p)$.

Case $l = 7$, $p = 3$. In this case the field F of Proposition 5.1 is equal to $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. The root discriminant δ_L of the field L satisfies $\delta_L < 3^{3/2} \cdot 7^{2/3} = 19.01\ldots$. Odlyzko's bounds imply that $[L : \mathbb{Q}] < 270$ so that the degree of L over $K = \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}, \sqrt[3]{7})$ is at most 14. In particular, $\pi = \mathrm{Gal}(L/K)$ is a solvable group. Since $7 \equiv 1 \pmod 3$, the field $\mathbb{Q}(\zeta_3, \sqrt[3]{7})$ is a cubic extension of conductor $3 \cdot 7$ of $\mathbb{Q}(\zeta_3)$. It follows from the conductor discriminant formula and the relative discriminant formula that the root discriminant of K is equal to $3^{7/6}7^{2/3} = 13.18\ldots$. By Odlyzko's

bounds, any unramified extension of K has relative degree at most $42/18$. This implies that K admits at most an unramified quadratic extension H. By group theory such a field H would be the composite of K with an unramified quadratic extension of $\mathbb{Q}(\zeta_3)$. Since the field $\mathbb{Q}(\zeta_3)$ does not admit any non-trivial unramified extensions, this implies that $K = H$. There lies only one prime $\mathfrak{p}$ over 3 in K. Its residue field has 27 elements. It is easily seen that its unit group is generated by the global units -1 and $\zeta_7 + \zeta_7^{-1}$. It follows, therefore, from class field theory that there is no abelian extension of K inside L that is unramified outside 3 and at most tamely ramified at the prime over 3. This implies that π/π' is a 3-group.

We have $[\pi : \pi'] \leqslant 14$. If $[\pi : \pi'] = 1$ or 9, the group π is a 3-group and we are done. Suppose that $[\pi : \pi'] = 3$. Let $\mathfrak{p}$ denote the unique prime over 3 in K and let $\mathfrak{p}^a$ be the conductor of the corresponding cubic extension K' of K. By the conductor discriminant formula, the root discriminant of K' is equal to $3^{a/9+7/6}7^{2/3}$. Since $\delta_{K'}$ is at most $\delta_L < 3^{3/2}7^{2/3}$, we must have that $a = 2$. This implies that the root discriminant of K' is at most $3^{25/18}7^{2/3} = 16.82\ldots$. Odlyzko's bounds imply that any unramified extension of K' has relative degree smaller than $120/36 < 4$. If K' admitted an everywhere unramified quadratic extension, then this would be the composite of K' and an unramified quadratic extension of $\mathbb{Q}(\zeta_3)$. We have already seen that this is impossible. Similarly, any abelian extension of K' that is unramified at 3 and at most tamely ramified at the unique prime over 3 is cyclic and is the composite of K' and a cyclic extension of $\mathbb{Q}(\zeta_3)$ that is at most tamely ramified at 3. This is impossible and hence $[L : \mathbb{Q}(\zeta_3)]$ is a power of 3, as required.

Case $l = 13$, $p = 2$. The root discriminant δ_L of the extension L satisfies $\delta_L < 2^2 \cdot 13^{1/2} = 14.422\ldots$. Odlyzko's bounds imply that $[L : \mathbb{Q}] < 60$ so that the degree of L over $\mathbb{Q}(i, \sqrt{13})$ is at most 14. Let $\pi = \mathrm{Gal}(L/\mathbb{Q})$. Since the root discriminant of $\mathbb{Q}(\zeta_8, \sqrt{13})$ is equal to $4\sqrt{13} > \delta_L$, the strict inequality of the fourth condition of Proposition 5.1 implies that the largest abelian extension of $\mathbb{Q}$ inside L is the field $\mathbb{Q}(i, \sqrt{13})$. This implies that $\mathbb{Q}(i, \sqrt{13})$ is the fixed field of π'. The class number of $\mathbb{Q}(i, \sqrt{13})$ is 1 and, since $\mathbb{F}_4^*$ is generated by the global unit $\eta = (3 + \sqrt{13})/2$, the ray class field of $\mathbb{Q}(i, \sqrt{13})$ of conductor $(1 + i)$ is trivial. It follows from class field theory that π'/π'' is a 2-group. Suppose that χ is a quadratic character of π'/π''. Then $\mathrm{cond}(\chi) = (1 + i)^a$ for some $a \leqslant 2$. Since $v_2(\delta_L) < 2$, we have $a \leqslant 3$. Since the unique prime over 2 is wildly ramified and since there are no quadratic characters of conductor $(1+i)^3$, we must have that $a = 2$. Since the unit i is not congruent to 1 modulo $(1+i)^2$, the ray class field of conductor $(1+i)^2$ has degree two over $\mathbb{Q}(i, \sqrt{13})$. It is the field generated by $\sqrt{\eta}$. Any larger abelian extension of $\mathbb{Q}(i, \sqrt{13})$ inside L has relative discriminant at least $(i+1)^{2+3+3}$ and hence root discriminant at least $4\sqrt{13}$. This is impossible and hence π'/π'' has order at most two.

If $\#\pi'/\pi'' = 1$, it follows that $\pi' = 1$ and hence that π is a 2-group. If $\#\pi'/\pi'' = 2$, we know that $K = \mathbb{Q}(i, \sqrt{13}, \sqrt{\eta})$ is the fixed field of π'' and that π''/π''' has odd order. However, K admits no odd degree abelian extensions inside L. Indeed, δ_K is equal to $2^{3/2}\sqrt{13} = 10.198\ldots$ so that Odlyzko's bounds imply that the absolute degree of its Hilbert class field is at most 22. Since $[K : \mathbb{Q}] = 8$, this implies that the class number of K is at most 2. Since the residue field of the unique prime $\mathfrak{p}$ over 2 in K is equal to the residue field $\mathbb{F}_4$ of the prime $i + 1$ in $\mathbb{Q}(i, \sqrt{13})$, its unit group is generated by the global unit η and hence the ray class field of K of conductor $\mathfrak{p}$ is equal to K itself. This implies that $K = L$ and that $[L : \mathbb{Q}]$ is a power of 2 as required. □

7. The case $l = 11$

In this section we prove Theorem 1.2. The modular curve $X_0(11)$ has genus 1 and is given by the equation

$$Y^2 + Y = X^3 - X^2 - 10X - 20.$$

Its Jacobian $E = J_0(11)$ has good reduction at every prime except at $l = 11$, where the reduction is semi-stable. We take $p = 2$ and study p-group schemes over $\mathbb{Z}[\frac{1}{11}]$ in the category $\underline{D}$ introduced in § 2. The 2-torsion points $E[2]$ of E form a 2-group scheme that is an object in $\underline{D}$. The natural map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[2](\overline{\mathbb{Q}}))$ is surjective. Indeed, the points in $E[2]$ generate the sextic field $F = \mathbb{Q}(\sqrt{-11}, \alpha)$ where α satisfies the equation $\alpha^3 + \alpha^2 + \alpha - 1 = 0$. This implies that $E[2]$ is a *simple* object of $\underline{D}$. It is isomorphic to its Cartier dual. Since the elliptic curve E is supersingular modulo 2, the group scheme $E[2]$ is local over $\mathbb{Z}_2$.

PROPOSITION 7.1. *The simple objects in the category $\underline{D}$ are the group schemes $\mathbb{Z}/2\mathbb{Z}$, μ_2 and $E[2]$.*

Proof. We modify the proof of Proposition 5.1. Let G be simple and let G' be the product of G by $E[2]$ and by the Katz–Mazur group schemes G_ε for the units $\varepsilon = -1$ and 11 of $\mathbb{Z}[\frac{1}{11}]$. Then G' is killed by 2 and is again an object of $\underline{D}$. Therefore, the root discriminant δ_L of the extension L generated by the points of G' satisfies $\delta_L < 4\sqrt{11} = 13.266\ldots$. Odlyzko's bounds imply that $[L : \mathbb{Q}] < 44$. We have the inclusions

$$\mathbb{Q} \underset{4}{\subset} \mathbb{Q}(i, \sqrt{-11}) \underset{3}{\subset} F(i) \underset{\leqslant 3}{\subset} L.$$

It follows that $[L : F(i)] \leqslant 3$. If $[L : F(i)] = 3$, the field L is abelian over $\mathbb{Q}(i, \sqrt{-11})$. Since the class number of $\mathbb{Q}(i, \sqrt{-11})$ is 1 and since the ray class field of conductor 2 of $\mathbb{Q}(i, \sqrt{-11})$ is $F(i)$, class field theory implies that $[L : F(i)]$ cannot be equal to 3 and must therefore be 1 or 2. In either case, $\mathrm{Gal}(L/F(i))$ and hence $\mathrm{Gal}(L/F)$ is a 2-group and hence fixes the points of the simple 2-group scheme G. Therefore, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $G(\overline{\mathbb{Q}})$ through $\mathrm{Gal}(F/\mathbb{Q}) \cong S_3$. It follows from the structure of simple $\mathbb{F}_2[S_3]$-modules that the Galois module $G(\overline{\mathbb{Q}})$ is either a group of order two with trivial action or is isomorphic to $E[2](\overline{\mathbb{Q}})$.

If G has order two, it follows from the Tate and Oort classification [TO70] that $G \cong \mathbb{Z}/2\mathbb{Z}$ or μ_2. If $G(\overline{\mathbb{Q}}) \cong E[2](\overline{\mathbb{Q}})$, the inertia group I_2 of the prime over 2 acts irreducibly, so G is local and has local Cartier dual. By Raynaud's theorem [Ray74, § 3.3.5], the group scheme G is therefore determined by its Galois module and hence we have that $G \cong E[2]$ as group schemes over $\mathbb{Z}_2$. This leads to an isomorphism of local Galois modules $G(\overline{\mathbb{Q}}_2) \cong E(\overline{\mathbb{Q}}_2)$. Since the only Galois equivariant automorphism of $E[2]$ is the identity morphism, the isomorphisms $G(\overline{\mathbb{Q}}) \cong E[2](\overline{\mathbb{Q}})$ and $G(\overline{\mathbb{Q}}_2) \cong E[2](\overline{\mathbb{Q}}_2)$ are unique and therefore compatible. It follows from the equivalence of categories of [Sch03b, Proposition 2.4], that $G \cong E[2]$ over the ring $\mathbb{Z}[\frac{1}{11}]$. This proves the proposition. □

Next we study extensions of the simple group schemes with one another. Note that the group scheme $E[4]$ fits in the non-split exact sequence

$$0 \longrightarrow E[2] \longrightarrow E[4] \longrightarrow E[2] \longrightarrow 0$$

and is an object of $\underline{D}$, because E has semi-stable reduction at 11.

PROPOSITION 7.2. *Over the ring $\mathbb{Z}[\frac{1}{11}]$ we have the following.*

(i) *The groups $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(\mu_2, \mathbb{Z}/2\mathbb{Z})$, $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], \mathbb{Z}/2\mathbb{Z})$ and $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(\mu_2, E[2])$ are all trivial.*

(ii) *The group of extensions $\mathrm{Ext}^1_{\underline{D}}(E[2], E[2])$ has dimension one over $\mathbb{F}_2$. It is generated by the extension $E[4]$ above.*

Proof. (i) Any extension

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0$$

is split over $\mathbb{Z}_2$ by the connected component. Therefore, G is killed by 2 and its 2-adic Galois representation is trivial. It follows that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $G(\overline{\mathbb{Q}})$ through a quadratic character χ that is at most ramified at $11 \cdot \infty$. There is exactly one such χ that is non-trivial. The prime 2 is *inert*

in the corresponding field $\mathbb{Q}(\sqrt{-11})$. Therefore, $\chi = 1$ and G is generically split. The Mayer–Vietoris sequence [Sch03b, Corollary 2.4] implies then that G is split over $\mathbb{Z}[\frac{1}{11}]$, as required.

The proof that every extension $0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow G \longrightarrow E[2] \longrightarrow 0$ splits, is similar. Over $\mathbb{Z}_2$ the extension is split by the connected component. So G is killed by 2 and its 2-adic Galois representation is trivial. Therefore, the points of G generate a Galois extension K of the field F that is unramified outside 11. The field K is a composite of at most two quadratic extensions. There are three primes lying over 11 in F. A computation shows that the global units -1 and α generate the unit group $(O_F/(\sqrt{-11}))^*$ modulo squares as a $\mathrm{Gal}(F/\mathbb{Q})$-module. Using Odlyzko's bounds one shows that the class number of F is 1. Therefore, class field theory implies that K is actually equal to F. Therefore, G is split as a Galois module. The Mayer–Vietoris sequence [Sch03b, Corollary 2.4] implies then that G is split over $\mathbb{Z}[\frac{1}{11}]$, as required.

The fact that $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(\mu_2, E[2])$ vanishes follows by Cartier duality.

(ii) Since the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[2](\overline{\mathbb{Q}}))$ is surjective, the only Galois equivariant endomorphisms of the group scheme $E[2]$ are scalar multiplications. This is true over any of the rings $\mathbb{Z}_2$, $\mathbb{Q}_2$, $\mathbb{Z}[\frac{1}{11}]$ and $\mathbb{Z}[\frac{1}{22}]$.

It follows from the Mayer–Vietoris sequence that there is an exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], E[2]) \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}_2}(E[2], E[2]) \times \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{22}]}(E[2], E[2]) \longrightarrow \mathrm{Ext}^1_{\mathbb{Q}_2}(E[2], E[2]).$$

The proof now proceeds in two steps.

Step 1. The group $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], E[2])$ *is generated by* $E[4]$ *and by the extensions of* $E[2]$ *by itself that are killed by 2.*

Let $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and let $\mathrm{Ext}^q_{\mathrm{ab}}$ and $\mathrm{Ext}^q_{\mathbb{Q}}$ denote the qth Ext-groups in the category of abelian groups and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules respectively. From the spectral sequence

$$H^p(\Gamma, \mathrm{Ext}^q_{\mathrm{ab}}(E[2], E[2])) \quad \Longrightarrow \quad \mathrm{Ext}^{p+q}_{\mathbb{Q}}(E[2], E[2])$$

we deduce the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}],2}(E[2], E[2]) & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], E[2]) & \longrightarrow & \mathrm{cok} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Q},2}(E[2], E[2]) & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Q}}(E[2], E[2]) & \longrightarrow & \mathrm{Ext}^1_{\mathrm{ab}}(E[2], E[2])^\Gamma & &
\end{array}$$

By $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}],2}(E[2], E[2])$ and $\mathrm{Ext}^1_{\mathbb{Q},2}(E[2], E[2])$ we indicate the subgroups of the groups $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], E[2])$ and $\mathrm{Ext}^1_{\mathbb{Q}}(E[2], E[2])$, respectively, of extensions of $E[2]$ by $E[2]$ that are annihilated by 2.

Any extension G of $E[2]$ by $E[2]$ over $\mathbb{Z}[\frac{1}{11}]$ that is killed by 2 over $\mathbb{Q}$ is itself killed by 2. Therefore, the left-hand square is Cartesian. It follows that the rightmost vertical arrow is injective. Since the Γ-modules $\mathrm{Ext}^1_{\mathrm{ab}}(E[2], E[2])$ and $\mathrm{Hom}_{\mathrm{ab}}(E[2], E[2])$ are dual to one another, the orders of $\mathrm{Ext}^1_{\mathrm{ab}}(E[2], E[2])^\Gamma$ and $\mathrm{Hom}_{\mathrm{ab}}(E[2], E[2])^\Gamma = \mathrm{Hom}_\Gamma(E[2], E[2])$ are equal. Since the Galois representation on the points of $E[2]$ is surjective, the latter group consists of the scalar matrices and has order two. It follows that the index of $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}],2}(E[2], E[2])$ in $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], E[2])$ is at most 2. It is exactly 2, because of the existence of the group scheme $E[4]$.

Step 2. Any extension in the category $\underline{D}$ *of* $E[2]$ *by* $E[2]$ *over* $\mathbb{Z}[\frac{1}{11}]$ *that is annihilated by 2, is trivial.*

We have already seen that the field $F = \mathbb{Q}(\sqrt{-11}, \alpha)$ has class number 1. Let $\pi \in F$ be a prime over 2. We have that $(\pi)^3 = (2)$. Let G be an extension of $E[2]$ by $E[2]$ that is an object in $\underline{D}$ and that is annihilated by 2. The field extension L generated by the points of G is of exponent 2 over F and is at most ramified at the primes over 2 and 11. Since G is an object in $\underline{D}$ of exponent 2, the inertia groups in $\mathrm{Gal}(L/\mathbb{Q})$ of the primes over 11, have order at most two. Since the ramification index is equal to 2 in the extension F of $\mathbb{Q}$, this implies that L is actually *unramified* over F at the primes over 11. By [Sch03b, Proposition 6.4], the field L is a biquadratic extension of F of conductor dividing π^2. Since the global unit α generates the group $(1+(\pi))/(1+(\pi^2))$ and since F admits no non-trivial unramified extensions, class field theory implies that $F = L$. Therefore, the extension G is split as an extension of Galois modules. It follows from [Sch03b, Proposition 6.4] (or rather the proof of its part (ii)) that the extension is then necessarily locally trivial. The Mayer–Vietoris sequence then implies that G is split, as required.

Part (ii) now follows. Indeed, since $\mathrm{Ext}^1_{\underline{D},2}(E[2], E[2])$ is precisely the intersection of $\mathrm{Ext}^1_{\underline{D}}(E[2], E[2])$ and $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}],2}(E[2], E[2])$, Step 1 implies that the group $\mathrm{Ext}^1_{\underline{D}}(E[2], E[2])$ is generated by $E[4]$ and by the subgroup extensions in $\underline{D}$ of $E[2]$ by itself that are killed by 2. By Step 2 the latter subgroup is trivial. □

Note that the space $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], E[2])$ of *all* extensions of $E[2]$ by $E[2]$ does *not* have dimension one. Indeed, consider the elliptic curve E' given by the Weierstrass equation $Y^2 + Y = X^3 - X^2 - 7X + 10$. It is the curve 121D in [BK75, p. 97] of conductor 11^2. Over the ring $\mathbb{Z}[\frac{1}{11}]$ the subgroup scheme $E'[2]$ of 2-torsion points is isomorphic to the subgroup scheme of 2-torsion points of the semi-stable abelian variety $E = J_0(11)$. This follows from the fact that the points of each of the two group schemes generate the field $F = \mathbb{Q}(\sqrt{-11}, \alpha)$ with $\alpha^3 + \alpha^2 + \alpha - 1 = 0$. A theorem of Raynaud's [Ray74, § 3.3.5] then implies that $E'[2] \cong E[2]$ over $\mathbb{Z}_2$ and it follows [Sch03b, Proposition 2.4] that the same is true over $\mathbb{Z}[\frac{1}{11}]$. Therefore, $E'[2] \cong E[2]$ is an object in $\underline{D}$.

p	2	3	5	7
$a(p)$	-2	-1	1	-2
$b(p)$	0	-1	-3	0

This is in agreement with the fact that in the short table above [BK75, Table 3], the coefficients $a(p)$ and $b(p)$ of the L-functions of E' and E are congruent modulo 2. The coefficients are visibly *not* congruent modulo 4. This implies that the group scheme $E'[4]$ is *not* isomorphic to $E[4]$. Since $\mathrm{Ext}^1_{\underline{D}}(E[2], E[2])$ is one-dimensional, we conclude that $E'[4]$ is *not* an object of $\underline{D}$ and hence that the dimension of $\mathrm{Ext}^1_{\mathbb{Z}[\frac{1}{11}]}(E[2], E[2])$ is at least two. Of course, the group scheme $E'[4]$ is an object of the category $\underline{C}$.

The Baer sum of $E[4]$ and $E'[4]$ is a non-trivial extension of $E[2]$ by $E[2]$ that is killed by 2. By Proposition 7.2 it is *not* an object of $\underline{D}$.

Proof of Theorem 1.1. Let A be a semi-stable abelian variety over $\mathbb{Q}$ with good reduction outside 11. We show that the subgroup scheme $A[2]$ of 2-torsion points admits a filtration with successive subquotients isomorphic to $E[2]$. Consider an arbitrary filtration of $A[2]$ with simple subquotients. By Proposition 7.2(i) we may modify the filtration and obtain a filtration of the form

$$0 \quad \subset \quad G_1 \quad \subset \quad G_2 \quad \subset \quad A[2]$$

with G_1 an extension of group schemes isomorphic to μ_2, with $A[2]/G_2$ an extension of copies of $\mathbb{Z}/2\mathbb{Z}$ and G_2/G_1 admitting a filtration with copies of $E[2]$. We claim that, actually, there are no

subquotients isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or μ_2 in this filtration. Indeed, suppose that there is a subquotient isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Using Proposition 7.2(i) to 'move the subquotients that are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ to the right', we find that for each $n \geqslant 1$ there is an exact sequence

$$0 \longrightarrow H_n \longrightarrow A[2^n] \longrightarrow C_n \longrightarrow 0$$

with C_n admitting a filtration of length n with subquotients isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Then C_n is étale and the fundamental group of $\mathbb{Z}[\frac{1}{11}]$ acts on $C_n(\overline{\mathbb{Q}})$ through a 2-group P. Since the maximal abelian 2-extension of $\mathbb{Q}$ that is unramified outside 11 is the quadratic field $\mathbb{Q}(\sqrt{-11})$, the groups P/P' and hence P are cyclic and the group schemes C_n become constant over the ring $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}, \frac{1}{11}]$. Now choose a non-zero prime $\mathfrak{p}$ of the ring $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}, \frac{1}{11}]$. The abelian varieties A/H_n are all isogenous to A and have, therefore, the same number of points modulo $\mathfrak{p}$. On the other hand, they have at least 2^n rational points. This leads to a contradiction when $n \to \infty$. Therefore, there are no subquotients isomorphic to $\mathbb{Z}/2\mathbb{Z}$ in the filtration. By Cartier duality there are none isomorphic to μ_2 either. It follows that $A[2^n]$ is filtered with group schemes isomorphic to $E[2]$.

The endomorphism ring of the 2-divisible group G of E is isomorphic to $\mathbb{Z}_2$. Indeed, the $\mathbb{Z}_2$-algebra generated by the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ inside the ring $\mathrm{End}_{\mathbb{Z}_2}(T_2E)$ of endomorphisms of the Tate module T_2E is equal to the full ring $\mathrm{End}_{\mathbb{Z}_2}(T_2E)$, since it is so modulo 2. Therefore, the image of the injective homomorphism $\mathbb{Z}_2 \hookrightarrow \mathrm{End}(G) \hookrightarrow \mathrm{End}_{\mathrm{Gal}}(T_2E)$ is precisely the subalgebra $\mathbb{Z}_2$ of scalar matrices.

An application of Theorem 8.3 of the next section to the 2-divisible group H of A over the ring $O = \mathbb{Z}[\frac{1}{11}]$ shows that the 2-divisible groups of A and E^g are isomorphic. By Faltings' Theorem [Fal83, § 5] this implies that A is isogenous to E^g as required. □

8. *p*-divisible groups

The main result of this section is Theorem 8.3. It is a general result about p-divisible groups, used in § 7 of this paper. See [Oor02, Sch01] for related statements.

Let O be a Noetherian domain of characteristic 0, let p be a prime and let $\underline{D}$ be a full subcategory of the category of p-group schemes over O that is closed under taking products, closed flat subgroup schemes and quotients by closed flat subgroup schemes.

There is for every short exact sequence $0 \to G_1 \to G_2 \to G_3 \to 0$ in $\underline{D}$ and any object $H \in \underline{D}$ a six-term exact sequence

$$0 \longrightarrow \mathrm{Hom}_O(H, G_1) \longrightarrow \mathrm{Hom}_O(H, G_2) \longrightarrow \mathrm{Hom}_O(H, G_3) \xrightarrow{\delta}$$
$$\xrightarrow{\delta} \mathrm{Ext}^1_{\underline{D}}(H, G_1) \longrightarrow \mathrm{Ext}^1_{\underline{D}}(H, G_2) \longrightarrow \mathrm{Ext}^1_{\underline{D}}(H, G_3).$$

Indeed, there is a functorial exact sequence of this type involving extension groups classifying extensions in the *abelian* category of sheaves for the flat topology over the ring O. Since every extension class is represented by a finite flat group scheme over O, this leads to a six-term exact sequence involving extension groups $\mathrm{Ext}^1_O(H, G_i)$ rather than $\mathrm{Ext}^1_{\underline{D}}(H, G_i)$.

Since the category $\underline{D}$ is closed under the formation of products, closed subgroup schemes and quotients by closed flat subgroup schemes, one easily obtains the exact sequence above. For instance, the extension $\delta(g)$ of H by G_1 corresponding to a homomorphism $g \in \mathrm{Hom}_O(H, G_3)$ is a closed subgroup scheme of the product $G_2 \times H$ and is therefore an object of $\underline{D}$. We leave the other verifications to the reader.

We first prove a lemma.

LEMMA 8.1. *Let $G = \{G_n\}$ be a p-divisible group over O. Suppose that $R = \mathrm{End}(G)$ is a discrete valuation ring with uniformizer π and residue field $k = R/\pi R$. Suppose that:*

- *every group scheme G_n is an object in the category $\underline{D}$;*
- *the map*

$$\mathrm{Hom}_O(G[\pi], G[\pi]) \xrightarrow{\delta} \mathrm{Ext}^1_{\underline{D}}(G[\pi], G[\pi])$$

associated above to the exact sequence $0 \to G[\pi] \to G[\pi^2] \to G[\pi] \to 0$ is an isomorphism of one-dimensional k-vector spaces.

Then

(i) *for all $m, m' \geqslant 1$ the canonical map*

$$(R/\pi^{m'}R)[\pi^m] \longrightarrow \mathrm{Hom}_O(G[\pi^{m'}], G[\pi^m])$$

is an isomorphism;

(ii) *for every $m \geqslant 1$ the group $\mathrm{Ext}^1_{\underline{D}}(G[\pi], G[\pi^m])$ is generated by the class of the extension*

$$0 \longrightarrow G[\pi^m] \longrightarrow G[\pi^{m+1}] \xrightarrow{\pi^m} G[\pi] \longrightarrow 0.$$

Proof. First suppose that $f \in R$ restricts to the zero morphism on $G[p^k]$ for some $k \geqslant 0$. This means that the image of the endomorphism $T_p f$ of the Tate module $T_p G$ of G induced by f is contained in $p^k T_p G$. Since the Galois module $p^k T_p G$ is isomorphic to $T_p G$, it follows that there exists a Galois equivariant $\mathbb{Z}_p$-linear homomorphism $\gamma : T_p G \longrightarrow T_p G$ for which $T_p f = p^n \cdot \gamma$. By Tate's Theorem [Tat67, Theorem 4], the homomorphism γ is induced by a morphism $g : G \longrightarrow G$ of p-divisible groups. We have that $f = p^n \cdot g$.

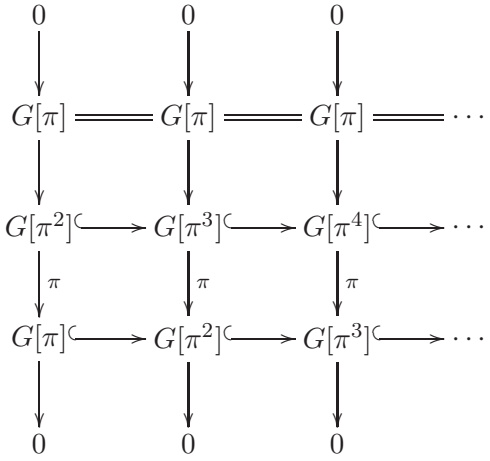
To prove the injectivity of the homomorphisms in part (i), we assume that $f \in R$ restricts to the zero morphism on $G[\pi^{m'}]$. Let $a \geqslant 0$ be such that $\pi^{m'+a}$ is equal to $p^b u$ for some $b \geqslant 0$ and some unit in R. Then $f \cdot \pi^a \in R$ restricts to the zero morphism on $G[p^b]$. By the discussion above, we have that $f \cdot \pi^a = p^b \cdot g$ for some $g \in R$. Dividing by π^a, we see that f is divisible by $\pi^{m'}$ as required. This shows that the maps in part (i) are injective.

To prove surjectivity of the maps in part (i), we observe that both sides are finite groups and we count their orders. The left-hand side has order $q^{\min(m,m')}$ where $q = \#k$. It follows from the multiplicativity of orders in exact sequences that

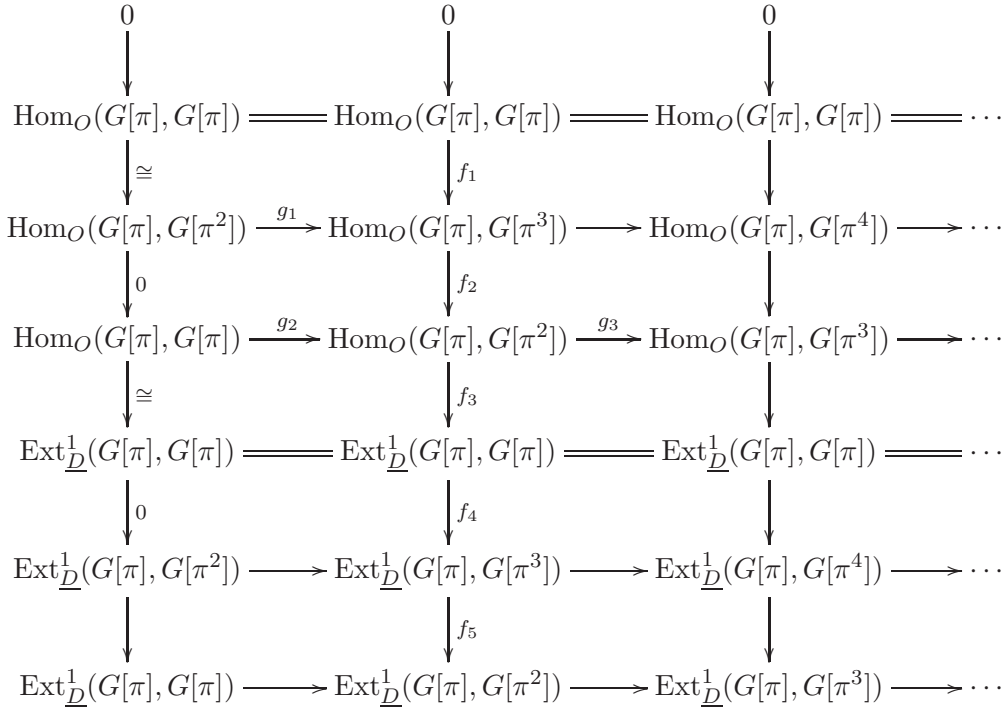
$$\#\mathrm{Hom}_O(G[\pi^m], G[\pi^{m'}]) \leqslant \begin{cases} \#\mathrm{Hom}_O(G[\pi], G[\pi^{m'}])^m, \\ \#\mathrm{Hom}_O(G[\pi^m], G[\pi])^{m'}. \end{cases}$$

Therefore, it suffices to show that $\mathrm{Hom}_O(G[\pi], G[\pi^m])$ and $\mathrm{Hom}_O(G[\pi^m], G[\pi])$ are both one-dimensional k-vector spaces for all $m \geqslant 1$. By assumption, this is so for $m = 1$. It is not clear for $m > 1$, because we do not know *a priori* that an arbitrary morphism of group schemes $f : G[\pi] \longrightarrow G[\pi^m]$ commutes with π. We show contemporarily that the natural maps $\mathrm{Hom}_O(G[\pi], G[\pi]) \longrightarrow \mathrm{Hom}_O(G[\pi], G[\pi^m])$ are isomorphisms and that the natural maps $\mathrm{Ext}^1_{\underline{D}}(G[\pi], G[\pi^{m+1}]) \longrightarrow \mathrm{Ext}^1_{\underline{D}}(G[\pi], G[\pi^m])$ are injections. Since, by assumption, $\mathrm{Ext}^1_{\underline{D}}(G[\pi], G[\pi])$ has dimension one, this shows that $\dim \mathrm{Ext}^1_{\underline{D}}(G[\pi], G[\pi^{m+1}]) = 1$ for all $m \geqslant 1$. The fact that the natural homomorphisms $\mathrm{Hom}_O(G[\pi^m], G[\pi]) \longrightarrow \mathrm{Hom}_O(G[\pi], G[\pi])$ are isomorphisms follows in a similar way. It can also be deduced from Cartier duality.

Consider the infinite commutative diagram with exact columns.



Apply the functor $\mathrm{Hom}_O(G[\pi], -)$ and form the associated long sequences of $\mathrm{Ext}^1_{\underline{D}}$-groups. The resulting diagram has exact columns. The isomorphisms and zero maps in the exact first column are a direct consequence of the assumptions. The statement for $m = 2$ follows at once. The map g_2 is the same map as the first morphism in the first column. So g_2 is an isomorphism and it follows at once that f_3 is an isomorphism as well. This implies that f_2 and f_4 are both zero and that f_1 is an isomorphism. Finally, f_5 is injective and g_1 is an isomorphism. This implies the statement for $m = 3$. Note that the map g_3 is the same map as g_1. Now one proceeds inductively.



This proves the lemma. □

COROLLARY 8.2. *Let the ring O and the category $\underline{D}$ be as above and let $G = \{G_n\}$ be a p-divisible group over O. Suppose that $R = \mathrm{End}(G)$ is a discrete valuation ring with uniformizer π and residue field $k = R/\pi R$. Suppose that the conditions of Lemma 8.1 are satisfied. Then every p-group scheme in $\underline{D}$ that admits a filtration with closed flat subgroup schemes and successive subquotients*

isomorphic to $G[\pi]$ is isomorphic to a group scheme of the shape

$$\bigoplus_{i=1}^{r} G[\pi^{n_i}].$$

Proof. Let J be a such a group scheme. Proceeding by induction we may assume that there is an exact sequence

$$0 \longrightarrow \bigoplus_{i=1}^{r} G[\pi^{n_i}] \longrightarrow J \longrightarrow G[\pi] \longrightarrow 0.$$

The class of this extension is an element in the group

$$\operatorname{Ext}^1_{\underline{D}}\left(G[\pi], \bigoplus_{i=1}^{r} G[\pi^{n_i}]\right) \cong \bigoplus_{i=1}^{r} \operatorname{Ext}^1_{\underline{D}}(G[\pi], G[\pi^{n_i}]) \cong \mathbb{F}_2^r.$$

The second isomorphism follows from Lemma 8.1(ii). The extensions of the form

$$0 \longrightarrow G[\pi^{n_j}] \times W \longrightarrow G[\pi^{n_j+1}] \times W \longrightarrow G[\pi] \longrightarrow 0$$

with $W = \bigoplus_{i \neq j} G[\pi^{n_i}]$ form a basis for the vector space $\mathbb{F}_2^r$. These extensions have the required shape. Therefore, if we show that the Baer sum of two extensions of the right shape is again of the right shape, we are done. The Baer sum of two extensions $0 \to G_1 \to E \to G_2 \to 0$ and $0 \to G_1 \to E' \to G_2 \to 0$ is the kernel of a morphism $E \times E' \longrightarrow G_2$ modulo a closed flat subgroup scheme isomorphic to G_1. Therefore, it suffices to show that kernels and cokernels of morphisms between group schemes of the shape $\bigoplus_{i=1}^{r} G[\pi^{n_i}]$ are again of that shape. By duality, it is enough to show this for kernels.

Therefore, let

$$\bigoplus_{i=1}^{r} G[\pi^{n_i}] \xrightarrow{g} \bigoplus_{j=1}^{s} G[\pi^{m_j}]$$

be a homomorphism of group schemes. By Lemma 8.1(i) there are endomorphisms $f_{ij} \in R = \operatorname{End}_O(G)$ that induce g. Hence the kernel K of g is isomorphic to the kernel of the restriction of the homomorphism

$$\begin{pmatrix} f_{11} & \cdots & f_{r1} \\ \vdots & & \vdots \\ f_{1s} & \cdots & f_{rs} \end{pmatrix} : G^r \longrightarrow G^s$$

to the subgroup scheme $\bigoplus_{i=1}^{r} G[\pi^{n_i}]$ of G. Consider the following commutative diagram.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & K & & K_1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \bigoplus_{i=1}^{r} G[\pi^{n_i}] & \longrightarrow & G^r & \xrightarrow{(\pi^{n_i})} & G^r & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle A} & & \| & & \\
0 & \longrightarrow & G^s & \longrightarrow & G^s \times G^r & \longrightarrow & G^r & \longrightarrow & 0
\end{array}$$

Here (π^{n_i}) and A denote the homomorphisms

$$\begin{pmatrix} \pi^{n_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \pi^{n_r} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} f_{11} & \cdots & f_{r1} \\ \vdots & & \vdots \\ f_{1s} & \cdots & f_{rs} \\ \pi^{n_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \pi^{n_r} \end{pmatrix},$$

respectively. The diagram has exact rows and columns and, working in the *abelian* category of sheaves for the flat topology, we deduce that

$$K \cong K_1 = \ker(G^{r} \xrightarrow{A} G^{r+s}).$$

Since the ring R is a principal ideal domain, there exist an invertible $(r \times r)$ matrix B and an invertible $(r+s) \times (r+s)$ matrix B' both with entries in R so that

$$B'AB = \begin{pmatrix} g_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & g_r \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

for certain $g_i \in R$. This shows that K is isomorphic to the kernel of the map

$$\begin{pmatrix} g_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & g_r \end{pmatrix} : G^r \longrightarrow G^r.$$

This proves the corollary. □

THEOREM 8.3. *Let the ring O and the category $\underline{D}$ be as above and let $G = \{G_n\}$ be a p-divisible group over O. Suppose that $R = \mathrm{End}(G)$ is a discrete valuation ring with uniformizer π and residue field $k = R/\pi R$. Suppose that:*

- *every group scheme G_n is an object in the category $\underline{D}$;*
- *the map*

$$\mathrm{Hom}_O(G[\pi], G[\pi]) \xrightarrow{\delta} \mathrm{Ext}^1_{\underline{D}}(G[\pi], G[\pi])$$

associated to the exact sequence $0 \to G[\pi] \to G[\pi^2] \to G[\pi] \to 0$ is an isomorphism of one-dimensional k-vector spaces.

Let $H = \{H_n\}$ be a p-divisible group over O for which the following hold:

- *every group scheme H_n is an object in $\underline{D}$;*
- *each H_n admits a filtration with flat closed subgroup schemes and successive quotients isomorphic to $G[\pi]$.*

Then H is isomorphic to G^g for some $g \geqslant 0$.

Proof. By Corollary 8.2 the group scheme $H[p^n]$ is, for each $n \geqslant 1$, isomorphic to a group scheme of the shape $\bigoplus_{i=1}^{r} G[\pi^{n_i}]$. Let $\overline{F}$ be an algebraic closure of the quotient field F of O. The $\overline{F}$-points

of $H[p^n]$ form a group isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^g$ where $g = \dim H$. Therefore, every direct summand of $H[p^n](\overline{F})$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. This implies that

$$H[p^n] \cong \bigoplus_{i=1}^{r} G[\pi^{en}] \cong G^r[p^n].$$

Here e denotes the ramification index of R over $\mathbb{Z}_p$ and we have $r\,e \dim G[\pi](\overline{F}) = g$. Since the groups $\mathrm{Hom}_O(H[p^n], G^g[p^n])$ are finite, a compactness argument shows that there is a cofinal projective system of such isomorphisms and hence an isomorphism $H \longrightarrow G^g$ as required. □

Acknowledgements

I thank Frank Calegari for pointing out that the methods used to prove Theorem 1.1 could also be used to prove Theorem 1.3 and James Parson for informing me about the ramification properties of the Galois representations associated to the modular curves $X(l)$.

References

Abr87 V. A. Abraškin, *Galois moduli of period p group schemes over a ring of Witt vectors*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987) (English translation: Math. USSR Izvestiya **31** (1988), 1–46).

BK75 B. Birch and W. Kuyk (eds), *Modular functions in one variable IV*, Lecture Notes in Mathematics, vol. 476 (Springer, New York, 1975).

BK01 A. Brumer and K. Kramer, *Non-existence of certain semistable abelian varieties*, Manuscripta Math. **106** (2001), 291–304.

BW04 I. Bouw and S. Wewers, *Stable reduction of modular curves*, in *Modular curves and abelian varieties*, Progress in Mathematics, vol. 224, eds J. Cremona, J.-C. Lario, J. Quer and K. Ribet (Birkhäuser, Basel, 2004), 1–22.

Cal04 F. Calegari, *Semistable abelian varieties over* $\mathbb{Q}$, Manuscripta Math. **113** (2004), 507–529.

Fal83 G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

Fon85 J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. Math. **81** (1985), 515–538.

Gro71 A. Grothendieck, *Modèles de Néron et monodromie, exp. IX*, in *Groupes de monodromie en géométrie algébrique*, SGA 7, Part I, Lecture Notes in Mathematics, vol. 288 (Springer, New York, 1971).

KM85 N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematical Studies, vol. 108 (Princeton University Press, Princeton, 1985).

Mar81 J. Martinet, *Petits discriminants des corps de nombres*, in *Journées Arithmétiques 1980*, London Math. Soc. Lecture Notes Series, vol. 56, ed. J. V. Armitage (Cambridge University Press, Cambridge, 1981).

Maz76 B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci. **47** (1976), 33–186.

Mes86 J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.

Odl76 A. M. Odlyzko, *Unconditional bounds for discriminants*, unpublished (1976). Available at http://www.dtc.umn.edu/∼odlyzko/unpublished/discr.bound.table2.

Oor02 F. Oort, *Minimal p-divisible groups*, unpublished manuscript (2002). Available at http://www.math.ruu.nl/people/oort/A-Min5Rev.ps.

Ray74 M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

Sch01 R. Schoof, *Abelian varieties over* $\mathbb{Q}(\sqrt{6})$ *with good reduction everywhere*, in *Class field theory – its centenary and prospect*, Advanced Studies in Pure Mathematics, vol. 30, ed. K. Miyake (Mathematical Society Japan, Tokyo, 2001), 287–306.

Sch03a R. Schoof, *Abelian varieties over $\mathbb{Q}$ with good reduction outside* 7, unpublished manuscript (2003).

Sch03b R. Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Ann. **325** (2003), 413–448.

Tat67 J. T. Tate, *p-divisible groups*, in *Proc. conf. on local fields*, Driebergen, 1966 (Springer, Berlin, 1967), 118–131.

TO70 J. T. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

Tau37 O. Taussky, *A remark on the class field tower*, J. London Math. Soc. **12** (1937), 82–85.

VZ04 E. Viehweg and K. Zuo, *A characterization of certain Shimura curves in the moduli stack of abelian varieties*, J. Differential Geom. **66** (2004), 233–288.

Was82 L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83 (Springer, Berlin, 1982).

René Schoof schoof@science.uva.nl
Dipartimento di Matematica, 2ª Università di Roma 'Tor Vergata', I-00133, Roma, Italy