



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

René Schoof

Dipartimento di Matematica  
2<sup>a</sup> Università di Roma “Tor Vergata”  
I-00133 Roma ITALY  
Email: [schoof@science.uva.nl](mailto:schoof@science.uva.nl)

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

This result is 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  $\mathbf{Q}$  that has good reduction outside the prime  $11$  is isogenous to a power of  $J_0(11)$ .*

See [22] for a related result in a geometric context.

Our second result concerns abelian varieties over  $\mathbf{Q}$  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  $\mathbf{Q}$  that have good reduction at every prime different from  $l$  and acquire semi-stable reduction at  $l$  over an extension of  $\mathbf{Q}$  that is at most tamely ramified at  $l$ .*

This result is 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 [4 Cor.4.4]. When  $l \geq 7$ , these are non-zero abelian varieties.

The curve  $X(7)$  has genus 3. Its Jacobian  $J(7)$  is isogenous (over  $\mathbf{Q}$ ) to a product of the Jacobian  $J_0(49)$  of the modular curve  $X_0(49)$  and a 2-dimensional simple abelian variety  $B$ . The variety  $B$  is isogenous to  $J_0(49) \times J_0(49)$  over the real subfield of the cyclotomic field  $\mathbf{Q}(\zeta_7)$ . Under assumption of the Generalized Riemann Hypothesis for zeta functions of number fields, I can show [18] that any abelian variety over  $\mathbf{Q}$  with good reduction outside 7 and acquiring semi-stable reduction over a tamely ramified extension at 7, is necessarily isogenous (over  $\mathbf{Q}$ ) 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 J.-F. Mestre [12, III]. Mestre's methods are analytic in nature. He assumes that the  $L$ -functions associated to abelian varieties over  $\mathbf{Q}$  admit analytic continuations to  $\mathbf{C}$  and he applies A. Weil's explicit formulas. Our results do not depend on any unproved hypotheses. In a recent paper [3] A. Brumer and K. Kramer prove Theorem 1.1 for primes  $l \leq 7$ . 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 the one by 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 J.-M. Fontaine in [7]. When  $l = 2, 3, 5, 7$  or  $13$  we show for every  $n \geq 1$  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 F. Calegari's work [5]. Under 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  $\mathbf{Q}$  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 section 2 two categories  $\underline{C}$  and  $\underline{D}$  of finite flat group schemes of  $p$ -power order over the ring  $\mathbf{Z}[\frac{1}{l}]$ . In terms of these we

formulate in section 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  $\mu_p$  by  $\mathbf{Z}/p\mathbf{Z}$  over the ring  $\mathbf{Z}[\frac{1}{l}]$ . We determine these in section 4. The other is concerned with the simple objects in the categories  $\underline{D}$  and  $\underline{C}$  respectively. In sections 5 and 6 we determine these for a very short list of pairs of primes  $(p, l)$ . Theorems 1.1 and 1.3 follow from this. We deal with the prime  $l = 11$  in section 7. Here we prove Theorem 1.2. Section 8 contains a theorem concerning  $p$ -divisible groups that is essential for the proof.

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  $X(l)$ .

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

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  $\mathbf{Z}[\frac{1}{l}]$ . In this section we introduce two full subcategories of  $\underline{Gr}$ . In terms of these we formulate in the next section 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  $G(\overline{\mathbf{Q}})$ .

(ii) The category  $\underline{D}$  is the full subcategory of  $\underline{Gr}$  of group schemes  $G$  for which we have that  $(\sigma - \text{id})^2 = 0$  on  $G(\overline{\mathbf{Q}})$  for all  $\sigma$  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  $(\sigma - \text{id})^2 = 0$  implies that  $\sigma^{p^n} = \text{id}$  for some  $n \geq 0$ . This implies that every inertia group acts through a finite  $p$ -group on  $G(\overline{\mathbf{Q}})$ . Since  $p \neq l$ , this action is tame and hence  $\underline{D}$  is a full subcategory of  $\underline{C}$ :

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

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.

1. By A. Grothendieck's semi-stable reduction Theorem [8, Exp.IX, (3.5.3)], the subgroup schemes  $A[p^n]$  of  $p^n$ -torsion points of semi-stable abelian varieties  $A$  over  $\mathbf{Q}$  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  $\mathbf{Q}$  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. 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  $\mathbf{F}_p$ . For any representation  $\varrho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}(V)$  we obtain a Galois module with underlying group  $V$ . If  $\varrho$  is unramified outside  $l$  and infinity, this module is the group of points of an étale group scheme  $V(\varrho)$  over  $\mathbf{Z}[\frac{1}{l}]$ . If  $\varrho$  is at most tamely ramified at  $l$ , the group scheme  $V(\varrho)$  is an object of  $\underline{C}$ . If  $(\varrho(\sigma) - \text{id})^2 = 0$  for every  $\sigma$  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  $V = \mathbf{F}_p^{l-1}$  and  $\varrho : \text{Gal}(\mathbf{Q}(\zeta_l)/\mathbf{Q}) \longrightarrow \text{GL}(V)$  the permutation representation, the group scheme  $V(\varrho)$  is an object of  $\underline{C}$ . Its points generate the field  $\mathbf{Q}(\zeta_l)$ . Another example is given by  $V = \mathbf{F}_p^2$  and  $\varrho$  a homomorphism

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

This time the group scheme  $V(\varrho)$  is an object in  $\underline{D}$ , because  $(\varrho(\sigma) - \text{id})^2 = 0$  for every  $\sigma$ . 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.

**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*

$$\text{Ext}_{\underline{D}}^1(G_1, G_2)$$

of the group  $\text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(G_1, G_2)$  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  $\text{Ext}_{\underline{C}}^1(G_1, G_2) = \text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(G_1, G_2)$ . Indeed, there is some exponent  $e$  that is prime to  $l$  and has the property that for all  $\sigma$  in an inertia group of any of the primes lying over  $l$ , the automorphism  $\sigma^e$  acts trivially on the points of  $G_1$  and  $G_2$ . It follows that  $(\sigma^e - \text{id})^2 = 0$  on the points of  $G$  and hence that  $\sigma^{ep^s} = \text{id}$  for some  $s \geq 0$ . This implies that every inertia group acts through its tame quotient.

It is in general not true that  $\text{Ext}_{\underline{D}}^1(G_1, G_2) = \text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(G_1, G_2)$ . 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

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

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

**4.** N. Katz and B. Mazur construct in their book [9, Interlude 8.7] certain explicit extensions of  $\mathbf{Z}/p\mathbf{Z}$  by  $\mu_p$ . These are objects in  $\underline{D}$ . We recall the construction in our situation. For any unit  $\varepsilon \in \mathbf{Z}[\frac{1}{l}]^*$  Katz and Mazur define a finite flat  $p$ -group scheme  $G_\varepsilon$  over  $\mathbf{Z}[\frac{1}{l}]$  of order  $p^2$ . It is killed by  $p$  and fits in an exact sequence

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

Two group schemes  $G_\varepsilon$  and  $G_{\varepsilon'}$  are isomorphic if and only if  $\varepsilon/\varepsilon' = u^p$  for some  $u \in \mathbf{Z}[\frac{1}{l}]^*$ . The points of  $G_\varepsilon$  generate the number field  $\mathbf{Q}(\zeta_p, \sqrt[p]{\varepsilon})$ . For  $p = 2$  and  $\varepsilon = -1$ , we recover the group scheme  $D$  in [11, Prop.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  $\mathbf{Z}/p\mathbf{Z}$  and  $\mu_p$ ;*
- *we have  $\text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z}) = 0$ .*

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

**Proof.** The proof is very similar to the one in [7, section 3.4.3]. We briefly sketch it. Let  $A$  be a  $g$ -dimensional abelian variety over  $\mathbf{Q}$  that has good reduction at every prime different from  $l$  and has semi-stable reduction at  $l$ . Let  $n \geq 1$  and consider the closed subgroup scheme  $A[p^n]$  of  $p^n$ -torsion points over  $\mathbf{Z}[\frac{1}{l}]$ . 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  $\mathbf{Z}/p\mathbf{Z}$  and  $\mu_p$ . By the second assumption, any extension

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

splits over  $\mathbf{Z}[\frac{1}{l}]$ . Therefore we can modify the filtration of  $A[p^n]$  and obtain for every  $n \geq 1$  an exact sequence of finite flat  $\mathbf{Z}[\frac{1}{l}]$ -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  $\mu_p$  and  $C_n$  an extension of copies of  $\mathbf{Z}/p\mathbf{Z}$ . It follows that  $C_n$  is étale and that the fundamental group of  $\mathbf{Z}[\frac{1}{l}]$  acts on its points through a finite  $p$ -group  $P$ . Since the maximal abelian  $p$ -extension of  $\mathbf{Q}$  that is unramified outside  $l \cdot \infty$  is contained in the cyclic extension  $\mathbf{Q}(\zeta_l)$ , 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  $\mathbf{Q}(\zeta_l)$  over  $\mathbf{Q}$ . It follows that  $C_n$  becomes *constant* over the ring  $\mathbf{Z}[\frac{1}{l}, \zeta_l]$ . Similarly, it follows from Cartier duality that  $M_n$  becomes diagonalizable over this ring.

Pick a non-zero prime  $\mathfrak{p}$  of  $\mathbf{Z}[\frac{1}{l}, \zeta_l]$  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  $\#A(k_{\mathfrak{p}}) \geq \#C_n$ . Taking Cartier duals of the exact sequence above, we see that the abelian variety  $A^{\text{dual}}/C_n^{\vee}$  has at least  $\#M_n^{\vee}$  points over  $k_{\mathfrak{p}}$ . Since  $A$  is isogenous to  $A^{\text{dual}}/C_n^{\vee}$ , we see that  $\#A(k_{\mathfrak{p}}) \geq \#M_n^{\vee} = \#M_n$ . 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  $n \rightarrow \infty$  unless  $g = 0$ . This proves the proposition.

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

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

Then there do not exist any non-zero abelian varieties over  $\mathbf{Q}$  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  $\underline{\mathcal{C}}$ . Up to replacing the category  $\underline{\mathcal{D}}$  by  $\underline{\mathcal{C}}$ , the proof is *identical* to the proof of Proposition 3.1.

#### 4. Extensions of $\mu_p$ by $\mathbf{Z}/p\mathbf{Z}$ over $\mathbf{Z}[\frac{1}{l}]$ .

The criteria of the previous section involve the group  $\text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$  of extensions of the group scheme  $\mu_p$  by  $\mathbf{Z}/p\mathbf{Z}$  over the ring  $\mathbf{Z}[\frac{1}{l}]$ . In this section we determine this group for any pair of distinct primes  $p$  and  $l$ . For  $p = 2$  see also [11, Prop.5.1].

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

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

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

**Proof.** We work with the following base rings.

$$\begin{array}{ccc} & \mathbf{Z}_p & \\ & \nearrow & \searrow \\ \mathbf{Z}[\frac{1}{l}] & & \mathbf{Q}_p \\ & \searrow & \nearrow \\ & \mathbf{Z}[\frac{1}{pl}] & \end{array}$$

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

Therefore the Mayer-Vietoris exact sequence of [16, Prop.2.4]. provides us with the following exact sequence. Since the group schemes  $\mu_p$  and  $\mathbf{Z}/p\mathbf{Z}$  are étale over the rings  $\mathbf{Z}[\frac{1}{pl}]$  and  $\mathbf{Q}_p$ , this sequence gives a description of the group  $\text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$  in terms of groups of extensions of Galois modules.

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

Next we adjoin the  $p$ -th roots of unity to the rings  $\mathbf{Z}[\frac{1}{pl}]$  and  $\mathbf{Q}_p$ . The Galois group  $\Delta$  introduced above, acts naturally on the group  $\text{Ext}_{\mathbf{Q}_p(\zeta_p)}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$  of extensions of  $\mu_p$

by  $\mathbf{Z}/p\mathbf{Z}$  over  $\mathbf{Q}(\zeta_p)$ . Since  $\Delta$  has order prime to  $p$ , the extensions that are defined over  $\mathbf{Q}_p$  correspond precisely to the  $\Delta$ -invariant elements of  $\text{Ext}_{\mathbf{Q}_p(\zeta_p)}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ .

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

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

We express the rightmost extension group in terms of Galois cohomology. In order to do this we apply the functor  $\text{Hom}_{\mathbf{Q}_p(\zeta_p)}(-, \mu_p)$  to the exact sequence  $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow 0$  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  $\mathbf{F}_p[\Delta]$ -modules

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mu_p & \longrightarrow & \text{Ext}_{\mathbf{Z}[\frac{1}{pl}, \zeta_p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) & \longrightarrow & H^1(G_{\mathbf{Z}[\frac{1}{pl}, \zeta_p]}, \mu_p) \longrightarrow 0 \\ & & \parallel & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mu_p & \longrightarrow & \text{Ext}_{\mathbf{Q}_p(\zeta_p)}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) & \longrightarrow & H^1(G_{\mathbf{Q}_p(\zeta_p)}, \mu_p) \longrightarrow 0 \end{array}$$

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

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

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

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

Here  $Cl(\mathbf{Z}[\frac{1}{pl}, \zeta_p])$  denotes the ideal class group of the ring  $\mathbf{Z}[\frac{1}{pl}, \zeta_p]$ . It is naturally isomorphic to the ideal class group of  $\mathbf{Z}[\zeta_p]$  modulo the ideal classes supported in the primes lying over  $l$ . We take  $\omega^2$ -eigenspaces. By Herbrand's Theorem [23, Thm.6.17] the  $\omega^2$ -eigenspace of the  $p$ -part of the class group of the ring  $\mathbf{Z}[\zeta_p]$  vanishes. This implies that the  $\omega^2$ -eigenspace of  $Cl(\mathbf{Z}[\frac{1}{pl}, \zeta_p])$  is also trivial. A second application of the Snake Lemma leads then to the required exact sequence.

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

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

**Proof.** Note that  $\frac{l^2-1}{24}$  is  $p$ -integral since  $p \neq l$ . The condition  $\frac{l^2-1}{24} \equiv 0 \pmod{p}$  is just a compact way of saying that  $l \equiv \pm 1 \pmod{p}$  when  $p \geq 5$ , 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  $\Delta$  is trivial and  $\omega = 1$ . The middle and rightmost groups in the exact sequence of Prop. 4.1 are each of dimension 3 over  $\mathbf{F}_2$ . 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 2 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  $\Delta$  has order 2, so that  $\omega^2 = 1$  and the  $\omega^2$ -eigenspace is simply the group of  $\Delta$ -invariants. The middle and rightmost groups in the exact sequence of Prop. 4.1. are each of dimension 2 over  $\mathbf{F}_3$ . 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  $\text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(\mu_3, \mathbf{Z}/3\mathbf{Z})$  is a 1-dimensional  $\mathbf{F}_3$ -vector space when  $l$  is a 3-adic cube, i.e. when  $l \equiv \pm 1 \pmod{9}$ , while it is zero otherwise.

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

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

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

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

We identify the Galois group  $\Delta$  with  $\mathbf{F}_p^*$  via the cyclotomic character  $\omega$ . By [23, Prop. 8.13] the  $\mathbf{F}_p[\Delta]$ -module  $\mathbf{Z}[\frac{1}{p}, \zeta_p]^* / (\mathbf{Z}[\frac{1}{p}, \zeta_p]^*)^p$  is isomorphic to  $\mu_p \times \mathbf{F}_p[\Delta / \langle -1 \rangle]$ . So, its  $\omega^2$ -eigenspace has  $\mathbf{F}_p$ -dimension 1. The module  $\bigoplus_{\mathfrak{l}|l} \mathbf{F}_p$  is a permutation module isomorphic to  $\mathbf{F}_p[\Delta / \langle l \rangle]$ . Its  $\chi$ -eigenspaces are trivial for the characters  $\chi$  of  $\Delta$  for which  $\chi(l) \neq 1$ . They have dimension 1 if  $\chi(l) = 1$ . Since  $\omega$  generates the group of characters, the  $\omega^2$ -eigenspace is 1-dimensional precisely when  $l \equiv \pm 1 \pmod{p}$ . This shows that the group in the middle of the exact sequence has dimension 2 or 1 over  $\mathbf{F}_p$  depending on whether  $l \equiv \pm 1 \pmod{p}$  or not.

Since  $p \geq 5$ , the  $\omega^2$ -eigenspace of  $\mathbf{Q}_p(\zeta_p)^* / (\mathbf{Q}_p(\zeta_p)^*)^p$  has dimension 1. This follows from a short computation. By [23, Thm.8.25], the  $\omega^2$ -eigenspace of the cyclotomic units

in  $\mathbf{Z}[\frac{1}{p}, \zeta_p]^*$  maps surjectively onto it. It follows that the rightmost arrow in the exact sequence of Prop. 4.1 is surjective and hence that  $\text{Ext}_{\mathbf{Z}[\frac{1}{l}]}^1(\mu_p, \mathbf{Z}/p\mathbf{Z})$  has  $\mathbf{F}_p$ -dimension 1 or 0 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 section 2 we introduced the categories  $\underline{C}$  and  $\underline{D}$  of  $p$ -group schemes over  $\mathbf{Z}[\frac{1}{l}]$ . In this section we give two criteria for the group schemes  $\mathbf{Z}/p\mathbf{Z}$  and  $\mu_p$  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  $\mathbf{Q}(\zeta_l)$ . When not, we put  $F = \mathbf{Q}$ . Suppose that any Galois extension  $L$  of  $\mathbf{Q}$  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  $\delta_L$  of  $L$  is strictly smaller than  $1 + \frac{1}{p-1}$ ,

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

**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 section 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 section 2 with  $V = \mathbf{F}_p^2$  and

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

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  $\mathbf{Q}$  generated by the points of  $G'$ . It is a Galois extension of  $\mathbf{Q}$  that is unramified outside  $pl$  and  $\infty$ . 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  $(\sigma - \text{id})^2 = 0$  on  $G'(\overline{\mathbf{Q}})$  for every  $\sigma$  in the inertia subgroup  $I_l$  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  $\sigma^p = \text{id}$  on  $G'(\overline{\mathbf{Q}})$ . 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 and Fontaine [1, 7] for the ramification at the prime  $p$  imply that the third condition is satisfied. Therefore  $[L : \mathbf{Q}(\zeta_p)]$  is a power of  $p$ .

The subgroup  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_p))$  of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  acts on the group of points  $G(\overline{\mathbf{Q}})$  through the finite  $p$ -group  $\text{Gal}(L/\mathbf{Q}(\zeta_p))$ . Since  $G(\overline{\mathbf{Q}})$  is a simple Galois module of  $p$ -power order, it is fixed by the  $p$ -group  $\text{Gal}(L/\mathbf{Q}(\zeta_p))$ . Therefore  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  acts on  $G(\overline{\mathbf{Q}})$  through the

group  $\Delta = \text{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$  of order  $p - 1$ . The group  $G(\overline{\mathbf{Q}})$  is a product of eigenspaces. Since  $G$  is simple and since the  $p - 1$ -st roots of unity are in  $\mathbf{F}_p$ , the group  $G(\overline{\mathbf{Q}})$  is itself equal to one of the eigenspaces and has dimension 1 over  $\mathbf{F}_p$ . It follows that  $G$  has order  $p$ . Since  $p$  is prime in the ring  $\mathbf{Z}[\frac{1}{l}]$ , the classification of Oort-Tate [20] implies that  $G \cong \mathbf{Z}/p\mathbf{Z}$  or  $\mu_p$  possibly twisted by a character  $\chi$  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  $\chi$  must be a power of  $p$ . Therefore  $\chi$  is a character of  $\mathbf{Q}$  that is only ramified at  $\infty$ . This implies that it is trivial. This proves the theorem.

The following theorem is a variant of Proposition 5.1. Although the conditions have the appearance of being similar to those of Prop. 5.1, they are actually much stronger. In the course of the proof we'll see that they imply that either  $l$  or  $p$  is equal to 2. In section 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  $\mathbf{Q}$  for which the following four conditions hold:*

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

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

**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  $V = (\mathbf{F}_p)^{l-1}$  twisted by the permutation representation  $\varrho : \text{Gal}(\mathbf{Q}(\zeta_l)/\mathbf{Q}) \rightarrow \text{GL}(V)$ . The points of  $V(\varrho)$  generate the field  $\mathbf{Q}(\zeta_l)$ . 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  $\mathbf{Z}[\frac{1}{l}]$ , 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  $I_l$  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 Abraškin-Fontaine. Since the four conditions are satisfied, the degree  $[L : \mathbf{Q}(\zeta_p)]$  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  $\mathbf{Z}/p\mathbf{Z}$  or  $\mu_p$  possibly twisted by a character  $\chi$  that is unramified outside  $l\infty$ . The order of such a character necessarily divides  $l - 1 = [\mathbf{Q}(\zeta_l) : \mathbf{Q}]$  as well as  $p - 1 = \#\text{Aut}(\mathbf{Z}/p\mathbf{Z})$ . Since  $\zeta_l \in L$ , the degree  $l - 1 = [\mathbf{Q}(\zeta_p, \zeta_l) : \mathbf{Q}(\zeta_p)]$  is a power of  $p$ . It follows that  $\text{gcd}(l - 1, p - 1) = 1$ , so that there are no non-trivial twists of  $\mathbf{Z}/p\mathbf{Z}$  or  $\mu_p$  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 Theorem 1.3. We first deal with 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  $\frac{l^2-1}{24} \not\equiv 0 \pmod{p}$  and Corollary 4.2 implies that all extensions of  $\mu_p$  by  $\mathbf{Z}/p\mathbf{Z}$  over  $\mathbf{Z}[\frac{1}{l}]$  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  $\mathbf{Z}/p\mathbf{Z}$  and  $\mu_p$ . 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  $n$ -th root of the absolute value of its discriminant. The first, third and fourth property of the number field  $L$  that occurs Proposition 5.2 imply that the root discriminant  $\delta_L$  satisfies

$$\delta_L < lp^{1+\frac{1}{p-1}}.$$

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  $\delta_L$  of the field  $L$  of Proposition 5.2 satisfies  $\delta_L < 2 \cdot 3^{3/2} = 10.49\dots$ . Odlyzko's bounds [10, p.187] or [13] imply that  $[L : \mathbf{Q}] < 24$ . Therefore the degree of  $L$  over  $K = \mathbf{Q}(\zeta_3, \sqrt[3]{2})$  is at most 3. 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  $\mathbf{F}_3^*$  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  $[L : \mathbf{Q}(\zeta_3)]$  is a power of 3 as required.

**Case  $l = 3, p = 2$ .** The root discriminant  $\delta_L$  of the field  $L$  of Proposition 5.2 satisfies  $\delta_L < 3 \cdot 2^2 = 12$ . Odlyzko's bounds imply that  $[L : \mathbf{Q}] < 32$ . Therefore the degree of  $L$  over  $\mathbf{Q}(i, \sqrt{-3}) = \mathbf{Q}(\zeta_{12})$  is at most 7. Let  $\pi = \text{Gal}(L/\mathbf{Q})$ . Since the 2-adic valuation of the root discriminant of  $\mathbf{Q}(\zeta_{24})$  is not strictly smaller than 2, the fourth condition of Prop. 5.2 implies that the field  $\mathbf{Q}(\zeta_{12})$  is the largest abelian extension of  $\mathbf{Q}$  inside  $L$ . It is the fixed field of the commutator subgroup  $\pi'$  of  $\pi$ . Since its class number is 1 (see [23, Ch.11]), the field  $\mathbf{Q}(\zeta_{12})$  admits no non-trivial everywhere unramified extension inside  $L$ . In addition,  $\zeta_3$  generates the multiplicative group  $\mathbf{F}_4^*$  of the residue field of the unique prime over 2 and the multiplicative group  $\mathbf{F}_9^*$  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  $\mathbf{Q}(\zeta_{12})$  admits no non-trivial odd degree abelian extensions inside  $L$ . Therefore  $\pi'/\pi''$  is a 2-group.

We conclude the proof by showing that  $\pi''$  is trivial. We have  $\#\pi' \leq 7$ . Therefore we are done when  $[\pi' : \pi''] = 1$  or 4. When  $[\pi' : \pi''] = 2$ , the group  $\pi''$  has order at most 3 and is cyclic. Therefore  $\text{Aut}(\pi'')$  is abelian and  $\pi'$  is in the kernel of the homomorphism  $\pi \rightarrow \text{Aut}(\pi'')$  induced by conjugation. This implies that  $\pi''$  is contained in the center

of  $\pi'$ . Since  $\pi'/\pi''$  is cyclic, this implies that  $\pi'$  is abelian and hence that  $\pi''$  is trivial, as required.

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

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

*Proof.* By [23, Ch. 11] the class number of  $\mathbf{Q}(\zeta_{20})$  is 1, the multiplicative group  $\mathbf{F}_{16}^*$  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 4. By class field theory the field  $\mathbf{Q}(\zeta_{20})$  admits therefore no non-trivial odd degree abelian extensions inside  $L$ . It follows that the group  $\pi'/\pi'' = \text{Gal}(K/\mathbf{Q}(\zeta_{20}))$  and all its characters have 2-power order. By the first condition of Prop. 5.2, the conductors of the characters divide  $(1-\zeta_5)(1-i)^a$  for some  $a \geq 0$ . Since the 2-adic valuation of  $\delta_L$  is strictly smaller than 2, it follows from the conductor discriminant formula that  $a \leq 3$ . Since the multiplicative group  $(\mathbf{Z}[\zeta_{20}]/(1-\zeta_5))^* \cong \mathbf{F}_5^* \times \mathbf{F}_5^*$  is generated by the units  $\zeta_{20}$  and  $1-\zeta_{20}$ , the ray class field of  $\mathbf{Q}(\zeta_{20})$  of conductor  $(1-\zeta_5)$  is equal to  $\mathbf{Q}(\zeta_{20})$  and there are no characters of conductor  $(1-\zeta_5)$ . Since the primes over 2 are wildly ramified, this implies that  $a \geq 2$ .

Suppose that  $\chi$  is a character of  $\text{Gal}(K/\mathbf{Q}(\zeta_{20}))$  of conductor  $(1-\zeta_5)(1-i)^3$  or  $(1-i)^3$ . Then  $\chi$  has order 4. Since  $\chi^2$  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  $\chi$  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  $\mathbf{Q}(\zeta_{20})$ . 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  $\mathbf{Q}(\zeta_{20})$  of conductor  $1-\zeta_5$  is equal to  $\mathbf{Q}(\zeta_{20})$  itself. The unit group of  $\mathbf{Z}[\zeta_{20}]$  is generated by  $\zeta_{20}$  and by  $1-\zeta_{20}^a$  for  $a \in (\mathbf{Z}/20\mathbf{Z})^*$ . They generate a subgroup of  $(\mathbf{Z}[\zeta_{20}]/(2))^*$  of index 2. This implies that the ray class field  $F_2$  of  $\mathbf{Q}(\zeta_{20})$  of conductor 2 has degree 2. It is not difficult to see that one has  $F_2 = \mathbf{Q}(\zeta_{20}, \sqrt{\eta})$  where  $\eta = (1+\sqrt{5})/2$ . Similarly, one shows that  $(\mathbf{Z}[\zeta_{20}]/(2(1-\zeta_5)))^*$  modulo the image of the unit group  $\mathbf{Z}[\zeta_{20}]^*$  is a group of type  $2 \times 2$ . It follows that the ray class field  $F_{2(1-\zeta_5)}$  of conductor  $2(1-\zeta_5)$  is a biquadratic extension of  $\mathbf{Q}(\zeta_{20})$ . 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  $5^{7/8}2^{7/4} = 13.75\dots$  as required.

*Step 3.* The group  $\pi''/\pi'''$  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  $\mathbf{Q}$ , 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  $\mathbf{Q}(\zeta_{20})$  contained in  $F_{2(1-\zeta_5)}$ . Since  $F_2 = \mathbf{Q}(\zeta_{20}, \sqrt{\eta})$  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  $\mathbf{F}_{16}$ ,  $\mathbf{F}_{25}$  and  $\mathbf{F}_{25}$  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  $\mathbf{F}_{16}^* \times \mathbf{F}_{25}^* \times \mathbf{F}_{25}^*$  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  $\mathbf{Q}(\zeta_{20})$  contained in it, admit an odd degree extension inside  $L$ . We conclude that  $\pi''/\pi'''$  is a 2-group as required.

*Step 4.* The group  $\pi'''$  is trivial.

*Proof.* By Step 2, the index  $[\pi' : \pi'']$  divides 4. When  $\pi'/\pi''$  is trivial, we are done. If it has order 2, then the order of  $\pi''/\pi'''$  is odd by the Burnside basis theorem. It follows from Step 3 that  $\pi''/\pi'''$  is trivial. This implies that  $\pi''$  is trivial and we are done. When  $\pi'/\pi''$  has order 4, it is of type  $2 \times 2$  and the order of  $\pi''$  is at most 14. By Step 3 and Taussky's theorem [21], the group  $\pi''/\pi'''$  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  $\pi'''/\pi''''$  is cyclic and hence has an abelian automorphism group. Therefore  $\pi''$  is in the kernel of the homomorphism  $\pi' \rightarrow \text{Aut}(\pi'''/\pi''')$  that is induced by conjugation. It follows that  $\pi'''/\pi''''$  is contained in the center of  $\pi''/\pi''''$ , so that  $\pi''/\pi''''$  modulo its center is cyclic. This implies that  $\pi''/\pi''''$  is abelian and hence that  $\pi'''$  is trivial, as required.

This completes the proof of Theorem 1.3. Next we prove 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  $\frac{l^2-1}{24} \not\equiv 0 \pmod{p}$ , Corollary 4.2 implies that all extensions of  $\mu_p$  by  $\mathbf{Z}/p\mathbf{Z}$  over  $\mathbf{Z}[\frac{1}{l}]$  are trivial. It remains to show that the other condition is verified as well: the only simple objects in the category  $\underline{C}$  are  $\mathbf{Z}/p\mathbf{Z}$  and  $\mu_p$ . 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  $\delta_L$  satisfies

$$\delta_L < l^{1-\frac{1}{p}} p^{1+\frac{1}{p-1}}.$$

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

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

We have  $[\pi : \pi'] \leq 14$ . If  $[\pi : \pi'] = 1$  or 9, the group  $\pi$  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  $3^{25/18}7^{2/3} = 16.82\dots$ . 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  $\mathbf{Q}(\zeta_3)$ . We already saw 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  $\mathbf{Q}(\zeta_3)$  that is at most tamely ramified at 3. This is impossible and hence  $[L : \mathbf{Q}(\zeta_3)]$  is a power of 3, as required.

**Case  $l = 13, p = 2$ .** The root discriminant  $\delta_L$  of the extension  $L$  satisfies  $\delta_L < 2^2 \cdot 13^{1/2} = 14.422\dots$ . Odlyzko's bounds imply that  $[L : \mathbf{Q}] < 60$  so that the degree of  $L$  over  $\mathbf{Q}(i, \sqrt{13})$  is at most 14. Let  $\pi = \text{Gal}(L/\mathbf{Q})$ . Since the root discriminant of  $\mathbf{Q}(\zeta_8, \sqrt{13})$  is equal to  $4\sqrt{13} > \delta_L$ , the strict inequality of the fourth condition of Prop. 5.1 implies that the largest abelian extension of  $\mathbf{Q}$  inside  $L$  is the field  $\mathbf{Q}(i, \sqrt{13})$ . This implies that  $\mathbf{Q}(i, \sqrt{13})$  is the fixed field of  $\pi'$ . The class number of  $\mathbf{Q}(i, \sqrt{13})$  is 1 and since  $\mathbf{F}_4^*$  is generated by the global unit  $\eta = (3 + \sqrt{13})/2$ , the ray class field of  $\mathbf{Q}(i, \sqrt{13})$  of conductor  $(1 + i)$  is trivial. It follows from class field theory  $\pi'/\pi''$  is a 2-group. Suppose that  $\chi$  is a quadratic character of  $\pi'/\pi''$ . Then  $\text{cond}(\chi) = (1 + i)^a$  for some  $a \leq 2$ . Since  $v_2(\delta_L) < 2$ , we have  $a \leq 3$ . 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 2 over  $\mathbf{Q}(i, \sqrt{13})$ . It is the field generated by  $\sqrt{\eta}$ . Any larger abelian extension of  $\mathbf{Q}(i, \sqrt{13})$  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  $\pi'/\pi''$  has order at most 2.

If  $\#\pi'/\pi'' = 1$ , it follows that  $\pi' = 1$  and hence that  $\pi$  is a 2-group. If  $\#\pi'/\pi'' = 2$ , we know that  $K = \mathbf{Q}(i, \sqrt{13}, \sqrt{\eta})$  is the fixed field of  $\pi''$  and that  $\pi''/\pi'''$  has odd order. However,  $K$  admits no odd degree abelian extensions inside  $L$ . Indeed,  $\delta_K$  is equal to  $2^{3/2}\sqrt{13} = 10.198\dots$  so that Odlyzko's bounds imply that the absolute degree of its Hilbert class field is at most 22. Since  $[K : \mathbf{Q}] = 8$ , 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  $\mathbf{F}_4$  of the prime  $i + 1$  in  $\mathbf{Q}(i, \sqrt{13})$ , its unit group is generated by the global unit  $\eta$  and hence the ray class field of  $K$  of conductor  $\mathfrak{p}$  is equal to  $K$  itself. This implies that  $K = L$  and that  $[L : \mathbf{Q}]$  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  $\mathbf{Z}[\frac{1}{11}]$  in the category  $\underline{D}$  introduced in section 2. The 2-torsion points  $E[2]$  of  $E$  form a 2-group scheme that is an object in  $\underline{D}$ . The natural map  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{Aut}(E[2](\overline{\mathbf{Q}}))$  is surjective. Indeed, the points in  $E[2]$  generate the sextic field  $F = \mathbf{Q}(\sqrt{-11}, \alpha)$  where  $\alpha$  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  $\mathbf{Z}_2$ .

**Proposition 7.1.** *The simple objects in the category  $\underline{D}$  are the group schemes  $\mathbf{Z}/2\mathbf{Z}$ ,  $\mu_2$  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  $G_\varepsilon$  for the units  $\varepsilon = -1$  and  $11$  of  $\mathbf{Z}[\frac{1}{11}]$ . Then  $G'$  is killed by 2 and is again an object of  $\underline{D}$ . Therefore the root discriminant  $\delta_L$  of the extension  $L$  generated by the points of  $G'$  satisfies  $\delta_L < 4\sqrt{11} = 13.266\dots$ . Odlyzko's bounds imply that  $[L : \mathbf{Q}] < 44$ . We have the inclusions

$$\mathbf{Q} \subset_4 \mathbf{Q}(i, \sqrt{-11}) \subset_3 F(i) \subset_{\leq 3} L.$$

It follows that  $[L : F(i)] \leq 3$ . If  $[L : F(i)] = 3$ , the field  $L$  is abelian over  $\mathbf{Q}(i, \sqrt{-11})$ . Since the class number of  $\mathbf{Q}(i, \sqrt{-11})$  is 1 and since the ray class field of conductor 2 of  $\mathbf{Q}(i, \sqrt{-11})$  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,  $\text{Gal}(L/F(i))$  and hence  $\text{Gal}(L/F)$  is a 2-group and hence fixes the points of the simple 2-group scheme  $G$ . Therefore  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  acts on  $G(\overline{\mathbf{Q}})$  through  $\text{Gal}(F/\mathbf{Q}) \cong S_3$ . It follows from the structure of simple  $\mathbf{F}_2[S_3]$ -modules that the Galois module  $G(\overline{\mathbf{Q}})$  is either a group of order 2 with trivial action or is isomorphic to  $E[2](\overline{\mathbf{Q}})$ .

If  $G$  has order 2, it follows from the Oort-Tate classification [20] that  $G \cong \mathbf{Z}/2\mathbf{Z}$  or  $\mu_2$ . If  $G(\overline{\mathbf{Q}}) \cong E[2](\overline{\mathbf{Q}})$ , 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 [15, section 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  $\mathbf{Z}_2$ . This leads to an isomorphism of local Galois modules  $G(\overline{\mathbf{Q}}_2) \cong E(\overline{\mathbf{Q}}_2)$ . Since the only Galois equivariant automorphism of  $E[2]$  is the identity morphism, the isomorphisms  $G(\overline{\mathbf{Q}}) \cong E[2](\overline{\mathbf{Q}})$  and  $G(\overline{\mathbf{Q}}_2) \cong E[2](\overline{\mathbf{Q}}_2)$  are unique and therefore compatible. It follows from the equivalence of categories of [16, Prop.2.4] that  $G \cong E[2]$  over the ring  $\mathbf{Z}[\frac{1}{11}]$ . 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  $\mathbf{Z}[\frac{1}{11}]$  we have the following.*

- (i) *The groups  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}]}^1(\mu_2, \mathbf{Z}/2\mathbf{Z})$ ,  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}]}^1(E[2], \mathbf{Z}/2\mathbf{Z})$  and  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}]}^1(\mu_2, E[2])$  are all trivial.*
- (ii) *The group of extensions  $\text{Ext}_{\underline{D}}^1(E[2], E[2])$  has dimension 1 over  $\mathbf{F}_2$ . It is generated by the extension  $E[4]$  above.*

**Proof.** (i) Any extension

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

is split over  $\mathbf{Z}_2$  by the connected component. Therefore  $G$  is killed by 2 and its 2-adic Galois representation is trivial. It follows that  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  acts on  $G(\overline{\mathbf{Q}})$  through a quadratic character  $\chi$  that is at most ramified at  $11 \cdot \infty$ . There is exactly one such  $\chi$  that is non-trivial. The prime 2 is *inert* in the corresponding field  $\mathbf{Q}(\sqrt{-11})$ . Therefore  $\chi = 1$  and  $G$  is generically split. The Mayer-Vietoris sequence [16, Cor.2.4] implies then that  $G$  is split over  $\mathbf{Z}[\frac{1}{11}]$ , as required.

The proof that every extension  $0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow E[2] \longrightarrow 0$  splits, is similar. Over  $\mathbf{Z}_2$  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  $\alpha$  generate the unit group  $(O_F/(\sqrt{-11}))^*$  modulo squares as a  $\text{Gal}(F/\mathbf{Q})$ -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 [16, Cor.2.4] implies then that  $G$  is split over  $\mathbf{Z}[\frac{1}{11}]$ , as required.

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

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

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

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

The proof now proceeds in two steps.

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

Let  $\Gamma = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  and let  $\text{Ext}_{\text{ab}}^q$  and  $\text{Ext}_{\mathbf{Q}}^q$  denote the  $q$ -th Ext-groups in the category of abelian groups and  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ -modules respectively. From the spectral sequence

$$H^p(\Gamma, \text{Ext}_{\text{ab}}^q(E[2], E[2])) \implies \text{Ext}_{\mathbf{Q}}^{p+q}(E[2], E[2])$$

we deduce the following commutative diagram with exact rows

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

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

Any extension  $G$  of  $E[2]$  by  $E[2]$  over  $\mathbf{Z}[\frac{1}{11}]$  that is killed by 2 over  $\mathbf{Q}$ , is itself killed by 2. Therefore the left hand square is Cartesian. It follows that the rightmost vertical arrow is injective. Since the  $\Gamma$ -modules  $\text{Ext}_{\text{ab}}^1(E[2], E[2])$  and  $\text{Hom}_{\text{ab}}(E[2], E[2])$  are dual to one another, the orders of  $\text{Ext}_{\text{ab}}^1(E[2], E[2])^\Gamma$  and  $\text{Hom}_{\text{ab}}(E[2], E[2])^\Gamma = \text{Hom}_\Gamma(E[2], E[2])$  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 2. It follows that the index of  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}],2}^1(E[2], E[2])$  in  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}]}^1(E[2], E[2])$  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  $\mathbf{Z}[\frac{1}{11}]$  that is annihilated by 2, is trivial.*

We have already seen that the field  $F = \mathbf{Q}(\sqrt{-11}, \alpha)$  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  $\text{Gal}(L/\mathbf{Q})$  of the primes over 11, have order at most 2. Since the ramification index is equal to 2 in the extension  $F$  of  $\mathbf{Q}$ , this implies that  $L$  is actually *unramified* over  $F$  at the primes over 11. By [16, Prop.6.4], the field  $L$  is a biquadratic extension of  $F$  of conductor dividing  $\pi^2$ . Since the global unit  $\alpha$  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 [16, Prop.6.4] (or rather the proof of its part (ii)) that then the extension is necessarily locally trivial. The Mayer-Vietoris sequence implies then that  $G$  is split, as required.

Part (ii) now follows. Indeed, since  $\text{Ext}_{\underline{D},2}^1(E[2], E[2])$  is precisely the intersection of  $\text{Ext}_{\underline{D}}^1(E[2], E[2])$  and  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}],2}^1(E[2], E[2])$ , Step 1 implies that the group  $\text{Ext}_{\underline{D}}^1(E[2], E[2])$  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  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}]}^1(E[2], E[2])$  of *all* extensions of  $E[2]$  by  $E[2]$  does *not* have dimension 1. 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 [2, p.97] of conductor  $11^2$ . Over the ring  $\mathbf{Z}[\frac{1}{11}]$  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  $F = \mathbf{Q}(\sqrt{-11}, \alpha)$  with  $\alpha^3 + \alpha^2 + \alpha - 1 = 0$ . A theorem of Raynaud's [15, section 3.3.5] implies then that  $E'[2] \cong E[2]$  over  $\mathbf{Z}_2$  and it follows [16, Prop.2.4] that the same is true over  $\mathbf{Z}[\frac{1}{11}]$ . Therefore  $E'[2] \cong E[2]$  is an object in  $\underline{D}$ .

This is in agreement with the fact that in the short table below [2, 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  $\text{Ext}_{\underline{D}}^1(E[2], E[2])$  is 1-dimensional, we conclude that  $E'[4]$  is *not* an object of  $\underline{D}$  and hence that the dimension of  $\text{Ext}_{\mathbf{Z}[\frac{1}{11}]}^1(E[2], E[2])$  is at least 2. 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 Prop. 7.2 it is *not* an object of  $\underline{D}$ .

$p$	2	3	5	7
$a_p$	-2	-1	1	-2
$b_p$	0	-1	-3	0

**Proof of Theorem 1.1.** Let  $A$  be a semi-stable abelian variety over  $\mathbf{Q}$  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 Prop. 7.2 (i) we may modify the filtration and obtain a filtration of the form

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

with  $G_1$  an extension of group schemes isomorphic to  $\mu_2$ , with  $A[2]/G_2$  an extension of copies of  $\mathbf{Z}/2\mathbf{Z}$  and  $G_2/G_1$  admitting a filtration with copies of  $E[2]$ . We claim that actually, there are no subquotients isomorphic to  $\mathbf{Z}/2\mathbf{Z}$  or  $\mu_2$  in this filtration. Indeed, suppose that there is a subquotient isomorphic to  $\mathbf{Z}/2\mathbf{Z}$ . Using Prop. 7.2 (i) to ‘move the subquotients that are isomorphic to  $\mathbf{Z}/2\mathbf{Z}$  to the right’, we find that for each  $n \geq 1$  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  $\mathbf{Z}/2\mathbf{Z}$ . Then  $C_n$  is étale and the fundamental group of  $\mathbf{Z}[\frac{1}{11}]$  acts on  $C_n(\overline{\mathbf{Q}})$  through a 2-group  $P$ . Since the maximal abelian 2-extension of  $\mathbf{Q}$  that is unramified outside 11 is the quadratic field  $\mathbf{Q}(\sqrt{-11})$ , the groups  $P/P'$  and hence  $P$  are cyclic and the group schemes  $C_n$  become constant over the ring  $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}, \frac{1}{11}]$ . Now choose a non-zero prime  $\mathfrak{p}$  of the ring  $\mathbf{Z}[\frac{1+\sqrt{-11}}{2}, \frac{1}{11}]$ . 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  $n \rightarrow \infty$ . Therefore there are no subquotients isomorphic to  $\mathbf{Z}/2\mathbf{Z}$  in the filtration. By Cartier duality there are none isomorphic to  $\mu_2$  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  $\mathbf{Z}_2$ . Indeed, the  $\mathbf{Z}_2$ -algebra generated by the image of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  inside the ring  $\text{End}_{\mathbf{Z}_2}(T_2E)$  of endomorphisms of the Tate module  $T_2E$ , is equal to the full ring  $\text{End}_{\mathbf{Z}_2}(T_2E)$ , since it is so modulo 2. Therefore the image of the injective homomorphism  $\mathbf{Z}_2 \hookrightarrow \text{End}(G) \hookrightarrow \text{End}_{\text{Gal}}(T_2E)$  is precisely the subalgebra  $\mathbf{Z}_2$  of scalar matrices.

An application of Theorem 8.3 of the next section to the 2-divisible group  $H$  of  $A$  over the ring  $O = \mathbf{Z}[\frac{1}{11}]$  shows that the 2-divisible groups of  $A$  and  $E^g$  are isomorphic. By Faltings’ theorem [6, Sect. 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 section 7 of this paper. See [14, 17] 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  $0 \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow 0$  in  $\underline{D}$  and any object  $H \in \underline{D}$  a six term exact sequence

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

Indeed, there is a functorial such exact sequence 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  $\mathrm{Ext}_O^1(H, G_i)$  rather than  $\mathrm{Ext}_{\underline{D}}^1(H, G_i)$ .

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  $\pi$  and residue field  $k = R/\pi R$ . Suppose that*

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

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

*associated above to the exact sequence  $0 \rightarrow G[\pi] \rightarrow G[\pi^2] \rightarrow G[\pi] \rightarrow 0$  is an isomorphism of 1-dimensional  $k$ -vector spaces.*

Then

- (i) For all  $m, m' \geq 1$  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  $m \geq 1$  the group  $\mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi^m])$  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  $k \geq 0$ . 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  $\mathbf{Z}_p$ -linear homomorphism  $\gamma : T_p G \rightarrow T_p G$  for which  $T_p f = p^n \cdot \gamma$ . By Tate's Theorem [19, Thm.4], the homomorphism  $\gamma$  is induced by a morphism  $g : G \rightarrow G$  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  $a \geq 0$  be such that  $\pi^{m'+a}$  is equal to  $p^b u$  for some  $b \geq 0$  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  $\pi^a$ , we see that  $f$  is divisible by  $\pi^{m'}$  as required. This shows that the maps in (i) are injective.

To prove surjectivity of the maps in (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

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

Therefore it suffices to show that  $\mathrm{Hom}_O(G[\pi], G[\pi^m])$  and  $\mathrm{Hom}_O(G[\pi^m], G[\pi])$  both are 1-dimensional  $k$ -vector spaces for all  $m \geq 1$ . 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  $f : G[\pi] \rightarrow G[\pi^m]$  commutes with  $\pi$ . We show contemporarily that the natural maps  $\mathrm{Hom}_O(G[\pi], G[\pi]) \rightarrow \mathrm{Hom}_O(G[\pi], G[\pi^m])$  are isomorphisms and that the natural maps  $\mathrm{Ext}_D^1(G[\pi], G[\pi^{m+1}]) \rightarrow \mathrm{Ext}_D^1(G[\pi], G[\pi^m])$  are injections. Since by assumption  $\mathrm{Ext}_D^1(G[\pi], G[\pi])$  has dimension 1, this shows that  $\dim \mathrm{Ext}_D^1(G[\pi], G[\pi^{m+1}]) = 1$  for all  $m \geq 1$ . The fact that the natural homomorphisms  $\mathrm{Hom}_O(G[\pi^m], G[\pi]) \rightarrow \mathrm{Hom}_O(G[\pi], G[\pi])$  are isomorphism follows in a similar way. It can also be deduced from Cartier duality.

Consider the infinite commutative diagram with exact columns

$$\begin{array}{ccccccc} & 0 & & 0 & & 0 & \\ & \downarrow & & \downarrow & & \downarrow & \\ G[\pi] & = & G[\pi] & = & G[\pi] & = & \dots \\ & \downarrow & & \downarrow & & \downarrow & \\ G[\pi^2] & \hookrightarrow & G[\pi^3] & \hookrightarrow & G[\pi^4] & \hookrightarrow & \dots \\ & \downarrow \pi & & \downarrow \pi & & \downarrow \pi & \\ G[\pi] & \hookrightarrow & G[\pi^2] & \hookrightarrow & G[\pi^3] & \hookrightarrow & \dots \\ & \downarrow & & \downarrow & & \downarrow & \\ & 0 & & 0 & & 0 & \end{array}$$

apply the functor  $\mathrm{Hom}_O(G[\pi], -)$  and form the associated long sequences of  $\mathrm{Ext}_D^1$ -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 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.

$$\begin{array}{ccccccc}
& 0 & & 0 & & 0 & \\
& \downarrow & & \downarrow & & \downarrow & \\
\mathrm{Hom}_O(G[\pi], G[\pi]) & = & \mathrm{Hom}_O(G[\pi], G[\pi]) & = & \mathrm{Hom}_O(G[\pi], G[\pi]) & = & \cdots \\
& \downarrow \cong & & \downarrow f_1 & & \downarrow & \\
\mathrm{Hom}_O(G[\pi], G[\pi^2]) & \xrightarrow{g_1} & \mathrm{Hom}_O(G[\pi], G[\pi^3]) & \rightarrow & \mathrm{Hom}_O(G[\pi], G[\pi^4]) & \rightarrow & \cdots \\
& \downarrow 0 & & \downarrow f_2 & & \downarrow & \\
\mathrm{Hom}_O(G[\pi], G[\pi]) & \xrightarrow{g_2} & \mathrm{Hom}_O(G[\pi], G[\pi^2]) & \xrightarrow{g_3} & \mathrm{Hom}_O(G[\pi], G[\pi^3]) & \rightarrow & \cdots \\
& \downarrow \cong & & \downarrow f_3 & & \downarrow & \\
\mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi]) & = & \mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi]) & = & \mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi]) & = & \cdots \\
& \downarrow 0 & & \downarrow f_4 & & \downarrow & \\
\mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi^2]) & \rightarrow & \mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi^3]) & \rightarrow & \mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi^4]) & \rightarrow & \cdots \\
& \downarrow & & \downarrow f_5 & & \downarrow & \\
\mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi]) & \rightarrow & \mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi^2]) & \rightarrow & \mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi^3]) & \rightarrow & \cdots
\end{array}$$

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  $\pi$  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

$$\mathrm{Ext}_{\underline{D}}^1(G[\pi], \bigoplus_{i=1}^r G[\pi^{n_i}]) \cong \bigoplus_{i=1}^r \mathrm{Ext}_{\underline{D}}^1(G[\pi], G[\pi^{n_i}]) \cong \mathbf{F}_2^r$$

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  $\mathbf{F}_2^r$ . 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  $0 \rightarrow G_1 \rightarrow E \rightarrow G_2 \rightarrow 0$  and  $0 \rightarrow G_1 \rightarrow E' \rightarrow G_2 \rightarrow 0$  is the kernel of a morphism  $E \times E' \rightarrow G_2$  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.

Let therefore

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

be a homomorphism of group schemes. By Lemma 8.1 (i) there are endomorphisms  $f_{ij} \in R = \text{End}_O(G)$  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 commutative diagram

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

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

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

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

associated to the exact sequence  $0 \rightarrow G[\pi] \rightarrow G[\pi^2] \rightarrow G[\pi] \rightarrow 0$  is an isomorphism of 1-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  $g \geq 0$ .

**Proof.** By Cor. 8.2. the group scheme  $H[p^n]$  is for each  $n \geq 1$  isomorphic to a group scheme of the shape  $\bigoplus_{i=1}^r G[\pi^{n_i}]$ . Let  $\bar{F}$  be an algebraic closure of the quotient field  $F$  of  $O$ .

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

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

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

## Bibliography

- [1] Abraškin, V.A.: Galois moduli of period  $p$  group schemes over a ring of Witt vectors, *Izv. Ak. Nauk CCCP*, Ser. Matem. **51**, (1987). English translation in *Math. USSR Izvestiya* **31** (1988) 1–46.
- [2] Birch, B. and Kuyk, W. Eds.: *Modular functions in one variable IV*. Lecture Notes in Math. **476**, Springer-Verlag, New York 1975.
- [3] Brumer, A. and Kramer, K.: Non-existence of certain semistable abelian varieties, *Manuscripta Math.* **106** (2001) 291–304.
- [4] Bouw, I. and Wewers, S.: Stable reduction of modular curves, pp. 1–22 in: Cremona, J., Lario, J.-C., Quer, J. and Ribet, K. (eds.): *Modular Curves and Abelian Varieties*, Progress in Mathematics **224**, Birkhäuser, Basel 2004.
- [5] Calegari, F.: Semistable abelian varieties over  $\mathbf{Q}$ , to appear in *Manuscripta Math.*  
<http://www.math.uiuc.edu/Algebraic-Number-Theory/0284/index.html>
- [6] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983) 349–366.
- [7] Fontaine, J.-M.: Il n’y a pas de variété abélienne sur  $\mathbf{Z}$ , *Invent. Math.* **81**, (1985) 515–538.
- [8] Grothendieck, A.: Modèles de Néron et monodromie, Exp IX in *Groupes de monodromie en géométrie algébrique*, SGA 7, Part I, Lecture Notes in Mathematics **288** (1971) Springer-Verlag, New York.
- [9] Katz, N. and Mazur, B.: *Arithmetic moduli of elliptic curves*, Annals of Math. Studies **108**, Princeton University Press, Princeton 1985.
- [10] Martinet, J.: Petits discriminants des corps de nombres, in J.V. Armitage, *Journées Arithmétiques 1980*, CUP Lecture Notes Series **56**, Cambridge University Press, Cambridge 1981.
- [11] Mazur, B.: Modular curves and the Eisenstein ideal, *Publ. Math. IHES*, **47** (1976), 33–186.
- [12] Mestre, J.-F.: Formules explicites et minorations de conducteurs de variétés algébriques, *Compositio Math.* **58** (1986), 209–232.
- [13] Odlyzko, A.M.: Unconditional bounds for discriminants, 1976. <http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table2>
- [14] Oort, F.: Minimal  $p$ -divisible groups, Manuscript 3-IX-2002.
- [15] Raynaud, M.: Schémas en groupes de type  $(p, \dots, p)$ , *Bull. Soc. Math. France* **102** (1974) 241–280.
- [16] Schoof, R.: Abelian varieties over cyclotomic fields with good reduction everywhere, *Math. Annalen.* **325** (2003/), 413–448.
- [17] Schoof, R.: Abelian varieties over  $\mathbf{Q}(\sqrt{6})$  with good reduction everywhere, pp. 287–306 in: Miyake, K.: *Class Field Theory — Its Centenary and Prospect*, Advanced Studies in Pure Mathematics **148**, Math. Soc. Japan, Tokyo 2001.
- [18] Schoof, R.: Abelian varieties over  $\mathbf{Q}$  with good reduction outside 7, manuscript 2003.
- [19] Tate J.T.:  $p$ -divisible groups, *Proc. Conf. on local fields (Driebergen 1966)*, 118–131. Springer-Verlag, Berlin.
- [20] Tate, J.T. and Oort, F.: Group schemes of prime order, *Ann. Scient. École Norm. Sup.* **3** (1970) 1–21.
- [21] Taussky, O.: A remark on the class field tower, *J. London Math. Soc.* **12** (1937), 82–85.

- [22] Viehweg, E. and Zuo, K.: A characterization of certain Shimura curves in the moduli stack of abelian varieties, manuscript 2003.
- [23] Washington, L.C.: *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York 1982.